ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P1.01
https://doi.org/10.26493/2590-9770.1380.1c9
(Also available at http://adam-journal.eu)

Whitney's connectivity inequalities for directed hypergraphs

Anahy Santiago Arguello*

Bioinformatics Group, Department of Computer Science; and Interdisciplinary Center of Bioinformatics, Leipzig University, Härtelstraße 16-18, D-04107 Leipzig, Germany

Peter F. Stadler†

Bioinformatics Group, Department of Computer Science and *Interdisciplinary Center of Bioinformatics, Leipzig University, Härtelstraße 16-18, D-04107 Leipzig, Germany,* and *Max-Planck-Institute for Mathematics in the Sciences, Inselstraße 22, D-04103 Leipzig, Germany,* and *Department of Theoretical Chemistry, University of Vienna, Währingerstraß 17, A-1090 Wien, Austria,* and *Facultad de Ciencias, Universidad Nacional de Colombia, Sede Bogotá, Colombia Santa Fe Institute, 1399 Hyde Park Rd., Santa Fe NM 87501, USA*

Received 27 August 2020, accepted 26 Janury 2021, published online 7 March 2022

Abstract

Whitney's inequality established an important connection between vertex and edge connectivity, and the degree of a graph, which was later generalized to digraphs and undirected hypergraphs. Here we show, using the most common definitions of connectedness for directed hypergraphs, that an analogous result holds for directed hypergraphs. It relates the vertex connectivity under strong vertex elimination, edge connectivity under weak edge elimination, and a suitable degree-like parameter and it is a proper generalization of the situation in both digraphs and undirected hypergraphs. We furthermore relate the connectivity parameters of directed hypergraphs with those of its directed bipartite König representation.

Keywords: Strong and weak vertex elimination, strong connectedness, unilateral connectedness, directed hypergraph, total degree, connectivity indices.

Math. Subj. Class.: 05C65, 05C40, 05C20

*Consejo Nacional de Ciencia y Tecnología, Mexico, CONACYT PostDoc grant 2019-000012-01EXTV

†Corresponding author.

E-mail addresses: jpscw@hotmail.com (Anahy Santiago Arguello), studla@bioinf.uni-leizpig.de (Peter F. Stadler)

1 Introduction

Directed hypergraphs naturally arose as a model of dependencies e.g. in propositional logic, database theory, and model checking, see e.g. [3, 7] for reviews. Recently they also received increasing attention as models of biological [6, 9], chemical [2, 11], and transportation networks [10]. Connectivity parameters are one of the most fundamental characteristics of a network, and hence are also of directed practical relevance for applications of directed hypergraphs [6].

It is important to note that directed hypergraphs give rise to many different notions of connectedness. Here, we only consider the simplest, least restrictive, construction of hyperpath, requiring only a single vertex in the overlap of the head of one directed hyperedge and the tail of the following one. In particular in chemical reactions networks, much more restrictive notions path and reachability are also of interest, see e.g. [1, 2, 6]. The concepts of connectivity explored here remain closely related to those of bipartite graphs representation of directed hypergraphs [12] and, as we shall see, admit generalizations of well-known results for graphs and digraphs.

The connectivity in an undirected graph G is described by two parameters, the vertex connectivity index κ and the edge connectivity index κ'. They are defined as the minimum number of vertices or edges, respectively, whose removal disconnects G or gives a trivial graph. Hassler Whitney [13] showed that all undirected graphs satisfy the inequality $\kappa \leq \kappa' \leq \delta$, where δ denotes the minimal vertex degree in G. Later Geller and Harary found a generalization to digraphs [8]. In hypergraphs, the situation becomes more complicated because there are different, natural ways to delete vertices and hyperedges and thus to derive sub-hypergraphs [4]. Nevertheless, Whitney's inequalities for the connectivity parameters generalize to (undirected) hypergraphs [5].

In the present contribution we show that analogous results also hold for directed hypergraphs with respect to both strong and unilateral connectedness. In Section 2.1 we introduce the notation and give some simple preliminary results for later use. Section 3 introduces the various connectivity indices and established some universal inequalities between them. For many pairs of indices, however, we show that they are not comparable in general. The main theorem, a generalization of Whitney's inequalities, is the topic of Section 4. In the final Section 5 we explore relations between connectivities of Section 5 we explore relations between connectivities of directed hypergraphs and their bipartite digraph representation.

2 Notation and preliminaries

2.1 Directed hypergraphs

A *directed hypergraph* $H = (V, E)$ consists on a vertex set V and a set of directed hyperedges or hyperarcs $E = \{(T(e), H(e))\} \mid T(e) \subseteq V \text{ and } H(e) \subseteq V\}$, where $H(e) \neq \emptyset$ and $T(e) \neq \emptyset$. The sets $T(e)$ and $H(e)$ are called the *tail* and the *head* of e, respectively. The *support* of a hyperedge $e \in E$ is the pair $\operatorname{supp}(e) = T(e) \cup H(e)$. A directed hypergraph is called k*-uniform* if $|T(e)| = |H(e)| = k$ for all $e \in E$. Two edges $e, e' \in E$ are said to be *parallel* if $T(e) = T(e')$ and $H(e) = H(e')$. A directed hypergraph $H = (V, E)$ is called *simple* if it has neither parallel hyperarcs and nor loops, that is, edges e with $T(e) \cap H(e) = \emptyset$. A (directed) hypergraph is *trivial* if $|V| = 1$ and $E = \emptyset$, i.e., H consists of a single vertex.

We say that $u, v \in V$ are *adjacent* if there exists a hyperarc $e \in E$ such that $u \in T(e)$ and $v \in H(e)$. The *neighborhood* of a vertex v in a hypergraph (or graph) is the set of all the vertices adjacent to v not including v. The *indegree* of a vertex v, denoted as $d^-(v)$ in H, is defined as the number of hyperarcs that contain v in their head. The *outdegree* of a vertex v, denoted as $d^+(v)$ in H, is defined as the number of hyperarcs that contain v in their tail. The *minimum indegree* and *minimum outdegree* of H will be denoted by $\delta^-(H) = \min\{d^-(v)\}_{v\in V}$ and $\delta^+(H) = \min\{d^+(v)\}_{v\in V}$, respectively. The number of arcs parallel to e (including e) is the *multiplicity* of e and it is denoted as $m_H(e)$.

Every directed hypergraph $H = (V, E)$ can be represented as a bipartite digraph $G(H)$ with vertex set $V \cup E$ and directed arcs $x \to e$ iff $x \in T(e)$ and $e \to x$ iff $x \in H(e)$. The arcs of $G(H)$ are called the *bits* of the directed hypergraph. The graph $G(H)$ is called the *incidence digraph, Levi digraph, or König digraph* of H. There is a one-to-one correspondence between directed hypergraphs and bipartite graphs for which one partition (the one corresponding to the hyperarcs E) has neither sources nor sinks (since we do not allow hyperarcs with empty heads or tails.) For details we refer to [12].

2.2 Subhypergraphs

Substructures of directed hypergraphs can be constructed in two ways: In *strong* substructures the hyperedges are either retained or removed as an entity. In *weak substructures*, hyperedges can be restricted to a subset of vertices as long as their heads and tails remain non-empty. More precisely, following [5] we define:

A directed hypergraph $H' = (V', E')$ is a *weak subhypergraph* of the directed hypergraph $H = (V, E)$ if $V' \subset V$ and E' consists of edges e' with $T(e') = \{v \mid v \in T(e) \cap V'\}$ and $H(e') = \{v \mid v \in H(e) \cap V'\}$ for some $e \in E$. A directed hypergraph $H' = (V', E')$ is a *weak induced subhypergraph* of the directed hypergraph $H = (V, E)$ if $V' \subset V$ and edge set $E' = \{(T(e) \cap V', H(e) \cap V')|e \in E \wedge T(e) \cap V' \neq \emptyset \wedge H(e) \cap V' \neq \emptyset\}$. A directed hypergraph $H' = (V', E')$ is called a *strong subhypergraph* of the directed hypergraph $H = (V, E)$ if $V' \subset V$ and $E' \subset E$. A *strong subhypergraph* $H' = (V', E')$ of $H = (V, E)$, is *induced* by V' if $\operatorname{supp}(e) \subseteq V'$ and it is induced by E' if $V' = \bigcup_{e' \in E'} \operatorname{supp}(e')$. $H' = (V', E')$ is a *spanning* subhypergraph of $H = (V, E)$ if $V' = V$.

The deletion of vertices and edges from a directed hypergraph will play a key role in this contribution. Just as the formation of subhypergraphs this can be done in two ways:

Strong vertex deletion of $v \in V$ removes v and all hyperarcs that are incident to v. Thus it creates the strong subhypergraph $H' = (V', E')$ of $H = (V, E)$ with vertex set $V' = V \setminus \{v\}$ and edge set $E' = \{e \in E \mid v \notin T(e) \cup H(e)\}$. For a subset $X \subset V$ we write $H \backslash_S X$ to denote the directed hypergraph formed by strongly deleting all the vertices of X from H.

Weak vertex deletion of $v \in V$ removes v from the vertex set, and all occurrences of v from the hyperarcs of the directed hypergraph H. This creates the hypergraph $H' = (V', E')$ where $V' = V \backslash \{v\}$ and $E' = \{(T(e) \cap V', H(e) \cap V')|e \in E \wedge T(e) \cap V' \neq \emptyset \wedge H(e) \cap V' \neq \emptyset\}$. We use the notation $H \backslash_W v$ to denote the directed hypergraph formed by weakly deleting the vertex v from H. For any subset X of V we write $H \backslash_W X$ to denote the directed hypergraph formed by weakly deleting all the vertices of X from H.

Strong deletion of the hyperarc $e \in E$ removes e from the hypergraph and weakly deletes all the vertices incident with e. Thus it produces the weak subhypergraph $H' = (V', E')$ with $V' = V \backslash supp(e)$ and $E' = \{(T(e) \cap V', H(e) \cap V') | e \in E \wedge T(e) \cap V' \neq \emptyset \wedge H(e) \cap V' \neq \emptyset\}$. We write $H \backslash_S e$ to denote the hypergraph formed by strongly deleting the edge e from H. For any subset F of E, we use $H \backslash_S F$ to denote the directed hypergraph formed by strongly deleting all the hyper arcs of F from H.

Weak deletion of the hyperarc $e \in E$ simply removes the hyperarc e without affecting the rest of the hypergraph. Thus it leads to the strong subhypergraph $H' = (V, E')$ with $E' = E \setminus \{e\}$. We write $H \backslash_W e$ to denote the directed hypergraph formed by weakly deleting the hyperarc e from H. For any subset F of E, we write $H \backslash_W F$ to denote the directed hypergraph formed by weakly deleting all the hyperarcs of F from H.

It follows directly from the definition that the order in which vertices or edges are deleted has no impact on the final result. Thus the hypergraphs $H \backslash_S X$, $H \backslash_W X$, $H \backslash_S F$, and $H \backslash_W F$ are well-defined.

2.3 Connectedness

A *directed walk* in a hypergraph $H = (V, E)$ is a sequence $P_{v_0, v_k} = (v_0, e_1, v_1, e_2, ..., e_k, v_k)$ where $e_1, ..., e_k \in E$ and $v_0, ..., v_k \in V$, such that $v_{i-1} \neq v_i$, $v_{i-1} \in T(e_i)$ and $v_i \in H(e_i)$. A *directed p-path* is a walk where the vertices $v_0, ..., v_k$ are all distinct. A *directed cycle* is a directed walk with k distinct hyperarcs and k distinct vertices such that $v_0 = v_k$. The *length* of a directed walk, directed path, or cycle is the number of hyperarcs in the sequence; i.e., it is k in the foregoing definitions. Let $e \in E$ where $T(e) = \{u_1, ..., u_k\}$ and $H(e) = \{v_1, ..., v_l\}$ then the *reverse hyperarc* of e is $\bar{e} \in E$ such that $H(\bar{e}) = \{u_1, ..., u_k\}$ and $T(\bar{e}) = \{v_1, ..., v_l\}$.

Definition 2.1. We say that y is reachable from x in H if there is a directed p-path from x to y in H. For two hyperarcs e and e' we say that e' is reachable from e in H if there is x in $H(e)$ and $y \in T(e')$ such that y is reachable from x. Furthermore, we say v is reachable from u in $G(H)$ if there is a directed path from u to v.

There are three natural notions of connectedness in digraphs: A digraph is said to be *strongly connected* if, for every pair of vertices $x, y \in V$, x is reachable from y **and** y is reachable from x. It is said to be *unilaterally connected* if, for every pair of vertices $x, y \in V$, x is reachable from y **or** from y is reachable from x. A bipartite graph with vertex set $V_1 \cup V_2$ is *unilaterally connected on* V_1 if for every pair $u, v \in V_1$, v is reachable from u or u is reachable from v. Finally, a digraph is weakly connected if its underlying graph, i.e without direction, is connected. These definitions can be generalized immediately to hypergraphs.

Definition 2.2. A directed hypergraph H is *strongly connected* if for every pair of vertices $u, v \in V$, u is reachable from v and v is reachable from u. It is *unilaterally connected* if for every two pair of vertices $u, v \in V$, v is reachable from u or u is reachable from v. It is *(weakly) connected* if the underlying hypergraph, is connected.

Corollary 2.3. *For every directed hypergraph, "strongly connected" implies "unilaterally connected", which in turn implies "weakly connected".*

Lemma 2.4. *A directed hypergraph H is strongly, unilaterally, or weakly connected if and only if its incidence (di)graph $G(H)$ is strongly connected, unilaterally connected on V, and weakly connected, respectively.*

Proof. An undirected hypergraph is connected if and only if its (undirected) incidence graph is connected, see e.g. [4, 5], hence the statement is true for weak connectedness.

To show the statement for unilateral and strong connectedness we first show that for all $x, y \in V$ there is hyperpath from x to y in H if and only if there is a path from x to y in $G(H)$. First assume that a directed hyperpath $x = v_0, e_1, v_1, e_2, \dots, v_{k-1}, e_k, v_k = y$ in H exists. Then the bits (v_0, e_1), (e_1, v_2), …, (e_{k-1}, v_k) form a directed path for x to y in $G(H)$. Conversely, suppose such a directed path exists in $G(H)$. We note that the arcs (v_{i-1}, e_i) and (e_i, v_i) in $G(H)$ by construction are bits induced by a hyperedge e_i with $v_{i-1} \in T(e_i)$ and $v_i \in H(e_i)$. Thus the sequence $x = v_0, e_1, v_1, e_2, \dots, v_{k-1}, e_k, v_k = y$ is a directed hyperpath in H.

If $G(H)$ is strongly connected then in particular there is a directed hyperpath in H between any pair of vertices, and thus H is strongly connected. Conversely, if H is strongly connected, we know that there is a directed path between any pair x, y in V. To see that every $e \in E$ is reachable from every $x \in V$ in $G(H)$ we recall that every $T(e) \neq \emptyset$, i.e., there is $u \in T(e)$. We already know that there is a directed path from x to u in $G(H)$, which can be extended by the bit (u, e) to a directed path from x to e. Using that $H(e) \neq \emptyset$ we see that every $x \in V$ is reachable from every $e \in E$. Concatenating a directed from e to x and from x to e' we finally see that every $e' \in E$ is reachable from every $e \in E$, and thus $G(H)$ is strongly connected.

It follows immediately that H is unilaterally connected if for every $x, y \in V$ there is a directed path from x to y or from y to x in $G(H)$, i.e., if $G(H)$ is unilaterally connected on V. □

Note that unilateral connectedness of H does not imply unilateral connectedness of $G(H)$. As a counterexample consider the directed (hyper)graph H with $V = \{u, v, w, x\}$ and hyperarcs $e_1 = (u, v)$, $e_2 = (v, w)$, $e_3 = (w, x)$, and $e_4 = (u, x)$. H is unilaterally but not strongly connected but there is no directed path from e_2 to e_4 or *vice versa* in $G(H)$.

In the following we say that $H = (V, E)$ is $\mathscr{C}$-connected with $\mathscr{C} \in \{\mathscr{S}, \mathscr{U}, \mathscr{W}\}$ is strongly, unilaterally, or (weakly) connected. Correspondingly, we shall say that H is $\mathscr{C}$-disconnected if it is not $\mathscr{C}$-connected.

3 Connectivity in directed hypergraphs

The degree of connectedness in an undirected hypergraph H is described by invariants describing the minimal number of vertices or edges that must be removed by either weak or strong elimination to disconnect the hypergraph or leave on a trivial hypergraph behind [5]. The situation becomes even more involved because each of these invariants or indices can be defined with respect to each of the three concepts of connectedness. We write $\kappa_{x\mathscr{C}}$ and $\kappa'_{x\mathscr{C}}$, where the prime refers to edge deletion, $x \in \{s, w\}$ indicates strong or weak vertex/edge deletion and refers to strong, unilateral, or weak connectedness. The numbers $\kappa_{x\mathscr{C}}$ and $\kappa'_{x\mathscr{C}}$, are the minimum numbers of vertices and hyperedges, respectively, such that their x-elimination leaves a hypergraph $\mathscr{C}$-disconnected or trivial.

Let $H = (V, E)$ be a directed hypergraph. A vertex $v \in V$ is called *a strong (weak) $\mathscr{C}$-cut vertex* of H if $H\backslash_s v$ ($H\backslash_w v$) is $\mathscr{C}$-disconnected or trivial. X is a *strong (weak) vertex*

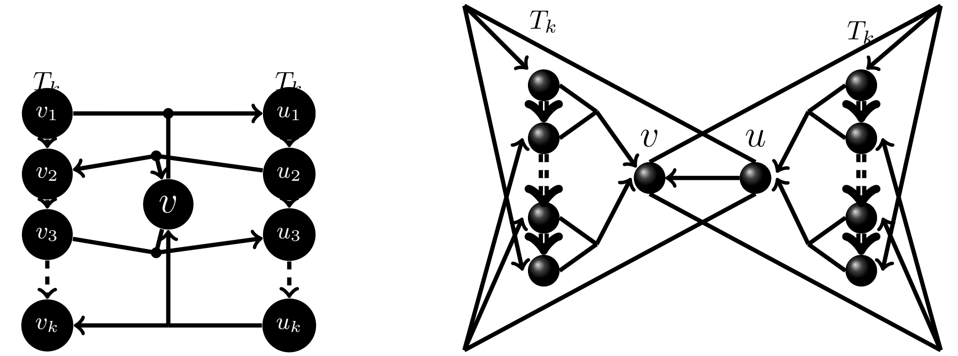


Figure 1: **Left:** T_k is the tournament of k vertices, where k is even. In this hypergraph $\kappa_{s\mathscr{S}} = 1$, $\kappa_{w\mathscr{S}} = \frac{k}{2}$, $\kappa_{s\mathscr{U}} = 1$, $\kappa_{w\mathscr{U}} = k$, the minimum strong vertex, for $s\mathscr{S}$ and $s\mathscr{U}$ cut is $\{v\}$ and a minimum weak vertex cut for $w\mathscr{S}$ is $\{u_1, u_3, ..., u_{k-1}\}$ and a weak vertex cut for $w\mathscr{U}$ is $\{u_1, v_2, u_3, v_4, ..., v_k\}$. As k increases, an infinite family of hypergraphs for which this difference grows linearly is obtained. **Right:** T_k is the tournament of k vertices, where k is even. In this hypergraph $\kappa'_{s\mathscr{S}} = \kappa'_{s\mathscr{U}} = 1$ ((u, v) is a disconnecting arc), $\kappa'_{w\mathscr{S}} = \frac{k}{2}$(all the arcs that have tail v), $\kappa'_{w\mathscr{U}} = k + 1$(all the arcs that have tail or head u).

$\mathscr{C}$-cut of H if $H\backslash_s X$ ($H\backslash_w X$) is $\mathscr{C}$-disconnected or trivial. We adopt the convention that $\kappa_{x\mathscr{C}} = 1$ for trivial hypergraphs and $\kappa_{x\mathscr{C}} = 0$ for null hypergraphs. A subset $F \subseteq E$ is called *a strong (weak) $\mathscr{C}$-disconnecting set* of H if $H\backslash_s F$ ($H\backslash_w F$) is $\mathscr{C}$-disconnected or trivial. We set $\kappa'_{x\mathscr{C}} = 1$ for trivial hypergraphs and $\kappa'_{x\mathscr{C}} = 0$ for null hypergraphs.

The following inequalities hold for all directed hypergraphs as an immediate consequence of the definition and the implications between the connectedness classes for both $x = s$ and $x = w$.

$$\kappa_{x\mathscr{S}} \leq \kappa_{x\mathscr{U}} \leq \kappa_{x\mathscr{W}} \qquad\qquad \kappa'_{x\mathscr{S}} \leq \kappa'_{x\mathscr{U}} \leq \kappa'_{x\mathscr{W}} \tag{3.1}$$

Since $\mathscr{W}$-connectedness coincides with the connectedness of undirected hypergraphs we focus on $\mathscr{C} \in \{\mathscr{S}, \mathscr{U}\}$ in the following. The case of undirected hypergraphs is studied in detail in [5]. We first consider the relationships between strong and weak elimination:

Lemma 3.1. *Let $H = (V, E)$ be a directed hypergraph. Then $\kappa_{s\mathscr{C}} \leq \kappa_{w\mathscr{C}}$ for $\mathscr{C} \in \{\mathscr{S}, \mathscr{U}\}$.*

Proof. If H is trivial or null, there is nothing to show. If H is $\mathscr{C} - disconnected$, then $\kappa_{x\mathscr{C}} = \kappa'_{x\mathscr{C}} = 0$, and the inequalities hold trivially. Now suppose that H is nontrivial and $\mathscr{C}$-connected. We note that $H\backslash_s X$ is a spanning strong subhypergraph of $H \backslash_w X$ for all $X \subseteq V$. This implies immediately that $\kappa_{s\mathscr{C}} \leq \kappa_{w\mathscr{C}}$ for $\mathscr{C} \in \{\mathscr{S}, \mathscr{U}\}$. □

It is worth noting that $\kappa_{w\mathscr{C}}$ is a poor upper bound for $\kappa_{s\mathscr{C}}$. Indeed, the difference between $\kappa_{w\mathscr{C}} - \kappa_{s\mathscr{C}}$ can become arbitrarily large as shown in Figure 1(left). It is important to notice that not every strong vertex cut is contained in a weak vertex cut. The situation on the left hand side of Figure 1 is an example.

Whitney's inequalities [5] and their generalization to directed graphs [8] and undirected hypergraphs [13] relate the connectivity indices with each other. In the case of directed

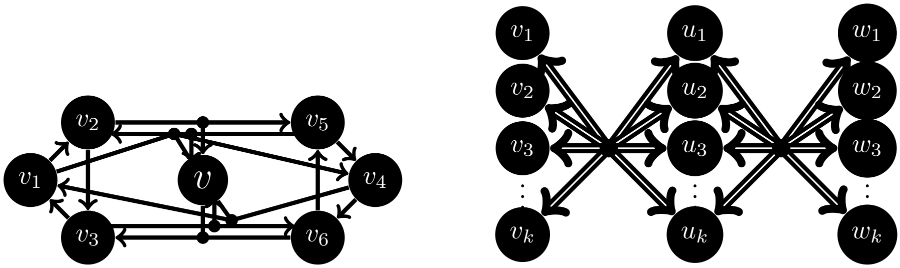


Figure 2: **Left:** In this hypergraph $\kappa_{s\mathscr{S}} = \kappa_{s\mathscr{U}} = 1$ since v is a cut vertex; $\kappa_{w\mathscr{S}} = 2$ since $\{v_2, v_4\}$ is a minimum weak vertex cut; $\kappa'_{s\mathscr{U}} = \kappa'_{s\mathscr{S}} = 2$ since $\{(v_5, v_4), (v_2, v_3)\}$ is a strong disconnecting set. **Right:** The hyperarcs in this hypergraph are $e_1 = (\{v_1, ..., v_k\}, \{u_1, ..., u_k\})$, $\bar{e_1}$, $e_2 = (\{u_1, ..., u_k\}, \{w_1, ..., w_k\})$, $\bar{e_2}$. We have $\kappa'_{w\mathscr{S}} = 1$ by removal of any hyperarc and $\kappa_{w\mathscr{S}} = k$ since $\{u_1, ..., u_k\}$ is the minimal weak vertex.

hypergraphs, however, some of these quantities do not fulfill universal inequalities. We give some simple counterexamples:

$\kappa_{s\mathscr{U}} \overset{\leq}{>} \kappa_{w\mathscr{S}}$. In a directed cycle C_n of length $n > 3$ we have $\kappa_{s\mathscr{U}} = 2$ and $\kappa_{w\mathscr{S}} = 1$. Therefore $\kappa_{s\mathscr{U}} > \kappa_{w\mathscr{S}}$. On the other hand, the left hand side of figure 2 shows an example where $\kappa_{s\mathscr{U}} = 1$ and $\kappa_{w\mathscr{S}} = 2$, i.e., $\kappa_{s\mathscr{U}} < \kappa_{w\mathscr{S}}$.

$\kappa'_{s\mathscr{U}} \overset{\leq}{>} \kappa'_{w\mathscr{S}}$. In a directed cycle C_n of length $n > 4$ we have $\kappa'_{w\mathscr{S}} = 1$ and $\kappa'_{s\mathscr{U}} = 2$. Therefore $\kappa'_{s\mathscr{U}} > \kappa'_{w\mathscr{S}}$. The hypergraph on the right hand side of Figure 1 has $\kappa'_{s\mathscr{U}} = 1$ and $\kappa'_{w\mathscr{S}} = \frac{k}{2}$. For $k > 3$ we therefore have $\kappa'_{s\mathscr{U}} < \kappa'_{w\mathscr{S}}$.

$\kappa_{s\mathscr{S}} \overset{\leq}{>} \kappa'_{s\mathscr{U}}$. The hypergraph in Figure 2(left) satisfies $\kappa_{s\mathscr{S}} < \kappa'_{s\mathscr{U}}$. Now consider the hypergraph in Figure 1(right) with all reverse hyperarcs added. Here, $\kappa'_{s\mathscr{U}} = 1$ and $\kappa_{s\mathscr{S}} = 2$ since $\{u, v\}$ is a vertex cut. Thus $\kappa'_{s\mathscr{U}} < \kappa_{s\mathscr{S}}$.

$\kappa_{s\mathscr{U}} \overset{\leq}{>} \kappa'_{s\mathscr{U}}$. The hypergraph in Figure 2(left) satisfied $\kappa_{s\mathscr{U}} < \kappa'_{s\mathscr{U}}$, while the hypergraph in Figure 1(right) satisfies $\kappa_{s\mathscr{U}} = 2$ ($\{u, v\}$ is a minimal strong the vertex cut) and $\kappa'_{s\mathscr{U}} = 1$. Therefore $\kappa'_{s\mathscr{U}} < \kappa_{s\mathscr{U}}$.

$\kappa'_{s\mathscr{U}} \overset{\leq}{>} \kappa_{w\mathscr{S}}$. In a directed cycle C_n of length $n > 4$ we have $\kappa_{w\mathscr{S}} = 1$ and $\kappa'_{s\mathscr{U}} = 2$, i.e., $\kappa_{w\mathscr{S}} < \kappa'_{s\mathscr{U}}$. Again, we consider the hypergraph in Figure 1(right) with the reverse hyperarcs added. It satisfies $\kappa'_{s\mathscr{U}} = 1$ and $\kappa_{w\mathscr{S}} = 2$, i.e., $\kappa'_{s\mathscr{U}} < \kappa_{w\mathscr{S}}$.

$\kappa_{w\mathscr{S}} \overset{\leq}{>} \kappa'_{w\mathscr{S}}$. The hypergraph in Figure 2(right) satisfies $\kappa'_{w\mathscr{S}} = 1$ and $\kappa_{w\mathscr{S}} = k$, i.e., $\kappa'_{w\mathscr{S}} < \kappa_{w\mathscr{S}}$. For the hypergraph in Figure 1(right) we have $\kappa_{w\mathscr{S}} = 2$ due to the weak way the vertex cut $\{u, v\}$. Furthermore, for $k \geq 4$ we have $\kappa'_{w\mathscr{S}} = \frac{k}{2}$ and thus $\kappa_{w\mathscr{S}} < \kappa'_{w\mathscr{S}}$.

$\kappa'_{w\mathscr{U}} \overset{\leq}{>} \kappa_{w\mathscr{S}}$. The hypergraph in Figure 1(right) satisfies $\kappa_{w\mathscr{S}} = 2$, the set $\{u, v\}$ being a minimum vertex cut. On the other hand, we have $\kappa'_{w\mathscr{U}} = k+1$ in the same example, hence, for $k > 2$, we have $\kappa_{w\mathscr{S}} < \kappa'_{w\mathscr{U}}$. The hypergraph in Figure 2(right) satisfies $\kappa_{w\mathscr{S}} = k$ and $\kappa'_{w\mathscr{U}} = 2$, since $\{e_1, \bar{e_1}\}$ is a minimal disconnecting set. Thus, for $k > 2$, we have $\kappa'_{w\mathscr{U}} < \kappa_{w\mathscr{S}}$.

$\kappa_{w\mathscr{S}} \overset{\leq}{>} \kappa'_{s\mathscr{U}}$. The hypergraph in Figure 2(right) satisfied $\kappa'_{s\mathscr{U}} = 1$ since every hyperarc contains a strong cut vertex. On the other hand we have $\kappa_{w\mathscr{S}} = k$ and this, for

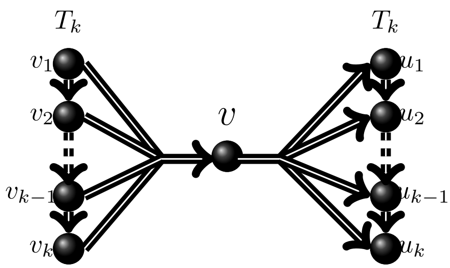


Figure 3: In this hypergraph with even k we have $\kappa_{w\mathscr{S}} = \kappa_{w\mathscr{U}} = 1$ since the vertex v is a cut vertex; $\kappa'_{s\mathscr{U}} = \kappa'_{s\mathscr{S}} = 1+\frac{k}{2}$ since $\{(v,\{u_1,...,u_k\}),(v_1,v_2),(v_3,v_4),...,(v_{k-1},v_k)\}$ is a strong disconnecting set.

$k > 1$, $\kappa'_{s\mathscr{U}} < \kappa_{w\mathscr{S}}$. In a directed cycle C_n with $n > 5$ we have $\kappa_{w\mathscr{S}} = 1$ and $\kappa_{s\mathscr{U}} = 2$ and therefore $\kappa_{w\mathscr{S}} < \kappa_{s\mathscr{U}}$.

$\kappa_{w\mathscr{U}} \lesseqgtr \kappa'_{w\mathscr{S}}$. In a directed cycle of length $n > 3$ we have $\kappa'_{w\mathscr{S}} = 1$ and $\kappa_{w\mathscr{U}} = 2$ and this $\kappa'_{w\mathscr{S}} < \kappa_{w\mathscr{U}}$. The hypergraph in Figure 1(right) satisfied $\kappa'_{w\mathscr{S}} = \frac{k}{2}$ and $\kappa_{w\mathscr{U}} = 2$ since the set $\{u,v\}$ is a weak vertex cut. Thus, for $k > 4$, we have $\kappa_{w\mathscr{U}} < \kappa'_{w\mathscr{S}}$.

$\kappa_{w\mathscr{U}} \lesseqgtr \kappa'_{w\mathscr{U}}$. The hypergraph in Figure 2(right) satisfies $\kappa'_{w\mathscr{U}} = 2$ and $\kappa_{w\mathscr{U}} = k$. Thus, for $k > 2$ we have $\kappa'_{w\mathscr{U}} < \kappa_{w\mathscr{U}}$. The hypergraph in Figure 1(right) satisfied $\kappa_{w\mathscr{U}} = 2$ and $\kappa'_{w\mathscr{U}} = k+1$. This, for $k > 2$ we have $\kappa_{w\mathscr{U}} < \kappa'_{w\mathscr{U}}$.

$\kappa_{s\mathscr{U}} \lesseqgtr \kappa'_{w\mathscr{S}}$. In a directed cycle C_n of length $n > 3$ we have $\kappa'_{w\mathscr{S}} = 1$ and $\kappa_{s\mathscr{U}} = 2$, i.e., $\kappa'_{w\mathscr{S}} < \kappa_{s\mathscr{U}}$. The hypergraph in Figure 1(right) satisfies $\kappa_{s\mathscr{U}} = 2$ and $\kappa'_{w\mathscr{S}} = \frac{k}{2}$. Thus, for $k > 4$ we have $\kappa_{s\mathscr{U}} < \kappa'_{w\mathscr{S}}$.

$\kappa'_{s\mathscr{S}} \lesseqgtr \kappa_{s\mathscr{U}}$. The hypergraph in Figure 1(right) satisfied $\kappa'_{s\mathscr{S}} = 1$ and $\kappa_{s\mathscr{U}} = k+1$, i.e., $\kappa'_{s\mathscr{S}} < \kappa_{s\mathscr{U}}$. For the hypergraph in Figure 2(left) we have $\kappa_{s\mathscr{U}} = 1$ and $\kappa'_{s\mathscr{S}} = 2$ and thus $\kappa_{s\mathscr{U}} < \kappa'_{s\mathscr{S}}$.

$\kappa'_{s\mathscr{S}} \lesseqgtr \kappa_{s\mathscr{S}}$. The hypergraph in Figure 1(right) satisfies $\kappa'_{s\mathscr{S}} = 1$ and $\kappa_{s\mathscr{S}} = 2$, and thus $\kappa'_{s\mathscr{S}} < \kappa_{s\mathscr{S}}$. For the hypergraph in Figure 2(left) we have $\kappa_{s\mathscr{S}} = 1$ and $\kappa'_{s\mathscr{S}} = 2$, and therefore $\kappa_{s\mathscr{S}} < \kappa'_{s\mathscr{S}}$.

$\kappa'_{s\mathscr{C}} \lesseqgtr \kappa_{w\mathscr{C}}$. The hypergraph in Figure 3 satisfies that $\kappa'_{s\mathscr{C}} = 1+\frac{k}{2}$ and $\kappa_{w\mathscr{C}} = 1$, hence for $k > 2$ we have $\kappa'_{s\mathscr{C}} > \kappa_{w\mathscr{C}}$. The hypergraph in Figure 2(right) satisfies $\kappa'_{s\mathscr{C}} = 1$ and $\kappa_{w\mathscr{C}} = k$, thus for $k > 1$ we have $\kappa'_{s\mathscr{C}} < \kappa_{w\mathscr{C}}$.

$\kappa'_{s\mathscr{S}} \lesseqgtr \kappa_{w\mathscr{U}}$. The hypergraph in Figure 3 satisfies $\kappa'_{s\mathscr{S}} = 1+\frac{k}{2}$ and $\kappa_{w\mathscr{U}} = 1$ thus for $k > 2$ we have $\kappa'_{s\mathscr{S}} > \kappa_{w\mathscr{U}}$. The hypergraph in Figure 2(right) satisfies $\kappa'_{s\mathscr{S}} = 1$ and $\kappa_{w\mathscr{U}} = k$, hence for $k > 1$ we have $\kappa'_{s\mathscr{S}} < \kappa_{w\mathscr{U}}$.

$\kappa'_{s\mathscr{C}} \lesseqgtr \kappa'_{w\mathscr{C}}$. The hypergraph in Figure 3 satisfies $\kappa'_{s\mathscr{C}} = 1+\frac{k}{2}$ and $\kappa'_{w\mathscr{C}} = 1$, hence for $k > 2$ we have $\kappa'_{s\mathscr{C}} > \kappa_{w\mathscr{C}}$. The hypergraph in Figure 1(left) satisfies $\kappa'_{s\mathscr{C}} = 1$ and $\kappa'_{w\mathscr{C}} = \frac{k}{2}$, hence for $k > 1$ we have $\kappa'_{s\mathscr{C}} < \kappa'_{w\mathscr{C}}$.

$\kappa'_{s\mathscr{S}} \lesseqgtr \kappa'_{w\mathscr{U}}$. The hypergraph in Figure 3 satisfies $\kappa'_{s\mathscr{S}} = 1+\frac{k}{2}$ and $\kappa'_{w\mathscr{U}} = 1$, hence for $k > 2$ we have $\kappa'_{s\mathscr{S}} > \kappa_{w\mathscr{U}}$. The hypergraph in Figure 1(left) satisfies $\kappa'_{s\mathscr{S}} = 1$ and $\kappa'_{w\mathscr{U}} = \frac{k}{2}$, hence for $k > 1$ we have $\kappa'_{s\mathscr{S}} < \kappa'_{w\mathscr{U}}$.

4 Whitney's theorem for directed hypergraphs

Let $H = (V, E)$ a directed hypergraph (or digraph) and $v \in V$. The *total degree of the vertex* v is $d^t(v) = d^+(v) + d^-(v)$. Denote by δ_{id}, δ_{od}, and $\delta_{\mathscr{W}}$ the minimum of d^-, d^+ and d^t over all $v \in V$, respectively. Furthermore we introduce

$$\delta_{id}^{\mathscr{U}} = \min_{v \in V}\{d^-(v) + \delta_{id}(H \setminus_w v)\} \qquad \text{and} \qquad \delta_{od}^{\mathscr{U}} = \min_{v \in V}\{d^+(v) + \delta_{od}(H \setminus_w v)\}.$$

With this notation we define $\delta_{\mathscr{S}} = \min\{\delta_{id}, \delta_{od}\}$ and $\delta_{\mathscr{U}} = \min\{\delta_{id}^{\mathscr{U}}, \delta_{id}^{\mathscr{U}}\}$. These parameters are direct generalizations of the corresponding quantities for directed hypergraphs, see e.g. [8].

The next theorem is a generalization of Whitney's inequalities for directed hypergraphs. The proof follows ideas from [8] for the analogous result for digraphs.

Theorem 4.1. *Let $H = (V, E)$ a directed hypergraph. Then $\kappa_{s\mathscr{U}}(H) \leq \kappa'_{w\mathscr{U}}(H) \leq \delta_{\mathscr{U}}(H)$ and $\kappa_{s\mathscr{S}}(H) \leq \kappa'_{w\mathscr{S}}(H) \leq \delta_{\mathscr{S}}(H)$.*

Proof. If H is trivial or null, the statements of the theorem are obviously valid.

Let H be a $\mathscr{U}$-connected hypergraph and let $u, v \in V$ such that $d^-(u) = \delta_{id}(H)$ and $d^-(v) = \delta_{id}(H \setminus_w u)$. Weakly eliminate the hyperarcs such that their heads contain u and v; in this way, there is no (u, v)-directed path and there is no (v, u)-directed path on H. So $\kappa'_{w\mathscr{U}}(H) \leq \delta_{in}^{\mathscr{U}}$. Applying the same dual argument we conclude that $\kappa'_{w\mathscr{U}}(H) \leq \delta_{od}^{\mathscr{U}}$ and so $\kappa'_{w\mathscr{U}}(H) \leq \delta_{\mathscr{U}}$.

On the other hand, if $\kappa'_{w\mathscr{U}}(H) = 1$, there is $e \in E$, such that $H \setminus_w e$ is not $\mathscr{U}$-connected. If we eliminate in a strong way the vertex $v \in T(e) \cup H(e)$ then $H \setminus_s v$ is not $\mathscr{U}$-connected, so $\kappa_{s\mathscr{U}}(H) = 1$ and the result is valid. Let $\kappa'_{w\mathscr{U}}(H) > 1$, for proving that $\kappa_{s\mathscr{U}}(H) \leq \kappa'_{w\mathscr{U}}(H)$ let weakly eliminate set of hyperarcs F, the cardinality of F is $\kappa'_{w\mathscr{U}}(H) - 1$ such that the directed hypergraph $H' = (V', E') = H \setminus_w F$ has $\kappa'_{w\mathscr{U}}(H') = 1$. Let $e \in (E')$ a hyperarc such that $H' \setminus_w e$ is not unilaterally connected. Now we strongly eliminate the set of vertices $X \in V$ such that each vertex on X is in exactly one hyperarc of F (there are enough vertices due to $\mid e \mid > 1$ for all $e \in E$), we denote this directed hypergraph $H'' = (V'', E'')$. If $e \notin E''$ then H'' is not unilaterally connected, so $\kappa_{s\mathscr{U}}(H) < \kappa'_{w\mathscr{U}}(H)$. If $e \in E''$ then $\kappa'_{w\mathscr{U}}(H'') = 1$ and $\kappa_{s\mathscr{U}}(H'') = \kappa'_{w\mathscr{U}}(H'') = 1$ so $\kappa_{s\mathscr{U}}(H) = \kappa'_{w\mathscr{U}}(H)$.

Let H be $\mathscr{S}$-connected hypergraph and let $v \in V$ such that $d^-(v) = \delta_{id}(H)$. Weakly eliminate the hyperarcs such that their heads contain v; in this way, there is no (u, v)-directed path on H for all $u \in V$. So $\kappa'_{w\mathscr{S}}(H) \leq \delta_{in}$. Applying the same dual argument we conclude that $\kappa'_{w\mathscr{S}}(H) \leq \delta_{od}$ and so $\kappa'_{w\mathscr{S}}(H) \leq \delta_{\mathscr{S}}$.

The proof that $\kappa_{s\mathscr{S}}(H) \leq \kappa'_{w\mathscr{S}}(H)$ parallels the proof of the inequality $\kappa_{s\mathscr{U}}(H) \leq \kappa'_{w\mathscr{U}}(H)$. □

Note that Theorem 4.1 reduces the corresponding statement for digraphs whenever all $e \in E$ hyperarcs satisfy $|T(e)| = |H(e)| = 1$.

Corollary 4.2. *Let $H = (V, E)$ a directed hypergraph. Then $\kappa_{s\mathscr{S}} \leq \kappa_{w\mathscr{U}}$ and $\kappa_{s\mathscr{S}} \leq \kappa'_{w\mathscr{U}}$.*

Proof. The first inequality follows from the note at the beginning of the previous section and Lemma 3.1. The second inequality follows from Theorem 4.1 and Equation 3.1. □

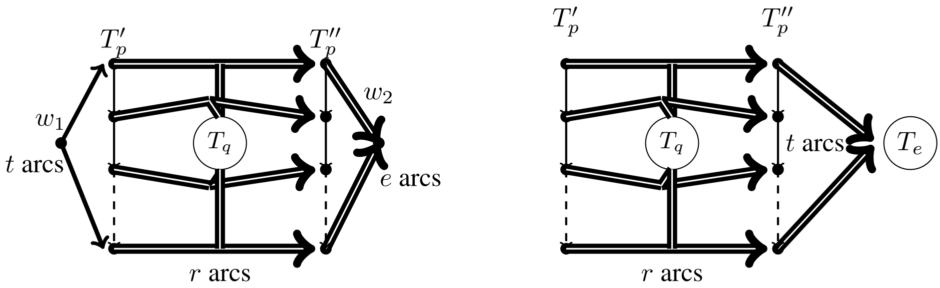


Figure 4: Left: Construction (A); Right: Construction (B)

We next show that the parameters $\kappa_{s\mathscr{C}}(H)$, $\kappa'_{s\mathscr{C}}(H)$, $\kappa_{w\mathscr{C}}(H)$ and $\kappa'_{w\mathscr{C}}(H)$ are independent for strongly or unilaterally connected directed hypergraphs satisfying $\kappa_{s\mathscr{C}}(H) \leq \min\{\kappa_{w\mathscr{C}}(H), \kappa'_{w\mathscr{C}}(H)\}$.

Theorem 4.3. *For every choice of natural numbers a, b, c, d, and e with $a \leq \min\{c, d\}$, $b \leq c$ and $\max\{b, c, d\} \leq e$ and connectedness classes $\mathscr{C} \in \{\mathscr{S}, \mathscr{U}, \mathscr{W}\}$ there exists a directed hypergraph such that $\kappa_{s\mathscr{C}}(H) = a$, $\kappa'_{s\mathscr{C}}(H) = b$, $\kappa_{w\mathscr{C}}(H) = c$, $\kappa'_{w\mathscr{C}}(H) = d$ and $\delta_{\mathscr{C}}(H) = e$.*

Proof. We explicitly construct hypergraphs with the desired properties.

Consider unilateral connectedness, i.e., $\mathscr{C} = \mathscr{U}$. We construct a hypergraph A form by five disjoint components: Two tournaments T'_p and T''_p on p vertices, a tournament T_q, and two single vertices w_1 and w_2; each arc in the tournaments T'_p and T''_p has multiplicity $e-p+1$ and each arc in T_q has multiplicity $e-q+1$. We then insert r hyperarcs consisting of one vertex from T'_p and T_q in its tail and a vertex from T''_p in its head involved, with all reverse hyperarcs added and with one of these hyperarcs with multiplicity t. Finally, we insert t arcs from w_1 to T'_p and e arcs from w_2 to T''_p with all reverse arcs added. The arcs are inserted in such a way that the vertices of the tournaments are covered as uniformly as possible. The construction is illustrated in Figure 4(left).

Let $a = q, b = r, c = p, d = t$. The minimum strong vertex cut in A is $V(T_q)$, the minimum strong disconnecting set is the r different hyperarcs, a minimum weak vertex cut is the set $V(T'_p)$ and the minimum weak disconnecting set is the t arcs (recall that one of the r hyperarcs has multiplicity t); then $q = \kappa_{s\mathscr{U}}$, $r = \kappa'_{s\mathscr{U}}$, $p = \kappa_{w\mathscr{U}}$ and $t = \kappa'_{w\mathscr{U}}$. Finally $\delta_{\mathscr{U}} = e$ because $d^-(w_1) = 0$ and $d^-(w_2) = e$, since all the vertices in the tournaments have in-degree and out-degree at least e, because of the multiplicities of the arcs inside the tournaments.

Next we consider strongly connectedness, $\mathscr{C} = \mathscr{S}$. We construct a hypergraph B form by five disjoint components: Two tournaments T'_p and T''_p on p vertices, a tournament T_q, and a tournament T_e; each arc in the tournaments T'_p and T''_p has multiplicity $e - p + 1$ and each arc in T_q has multiplicity $e - q + 1$. We then insert r hyperarcs consisting of one vertex from T'_p and T_q in its tail and a vertex from T''_p in its head involved, with all reverse hyperarcs added and with all of these hyperarcs with multiplicity t. The arcs are inserted in such a way that the vertices of the tournaments are covered as uniformly as possible. Finally, we insert t hyperarcs consisting of at least one vertex from T_e in its tail and a vertex from T''_p in its head involved, all vertices in T_e are in a head of these hyperarcs, all the reverse hyperarcs are added. The construction is illustrated in Figure 4(right).

Let $a = q$, $b = r$, $c = p$, and $d = t$. The minimum strong vertex cut in B is $V(T_q)$, the minimum strong disconnecting set is the r different hyperarcs, the minimum weak vertex cut is the set $V(T''_p)$ and a minimum weak disconnecting set is the t arcs from T_e to T''_p (don't forget that each of the r hyperarcs has multiplicity t); then $q = \kappa_{s\mathscr{S}}$, $r = \kappa'_{s\mathscr{S}}$, $p = \kappa_{w\mathscr{S}}$ and $t = \kappa'_{w\mathscr{U}}$. Finally $\delta_{\mathscr{S}} = e$ because all the vertices in T_e have indegree and outdegree e (all the vertices in the other tournaments have indegree and outdegree at least e, because of the multiplicities of the arcs inside the tournaments).

Next, we consider weak connectedness, $\mathscr{C} = \mathscr{W}$. We construct a hypergraph C form by five disjoint components: Two complete graphs K'_p and K''_p on p vertices, a complete graph K_q, and a complete graph K_e; each edge in the complete graphs K'_p and K''_p has multiplicity $e-p+1$ and each edge in K_q has multiplicity $e-q+1$. We then insert r edges consisting of one vertex from K'_p, K_q and K''_p, with all of these edges with multiplicity t. The edges are inserted in such a way that the vertices of the complete graphs are covered as uniformly as possible.

Finally, we insert t edges consisting of at least one vertex from T_e and one vertex from T''_p, all vertices in T_e are incident with these edges. The explanation of why this hypergraph has the desired parameters is analogous to the strong case. □

5 König digraph of a directed hypergraph

The connectivity invariants in digraphs are defined in the same way as in directed hypergraphs, the difference is that the weak or strong elimination of vertices or arcs is not relevant so we only have to consider a single connectivity index for each connectedness class, which we denote by $\kappa_{\mathcal{C}}$ and $\kappa'_{\mathcal{C}}$ with $\mathcal{C} \in \{\mathcal{S}, \mathcal{U}\}$.

Lemma 5.1. *Let $H = (V, E)$ be a directed hypergraph and let $G(H) = (V \cup E, A)$ be its König digraph. Then*

$$\kappa_{s\mathscr{C}}(H) \leq \kappa_{\mathcal{C}}(G(H)) \leq \min\{\kappa_{w\mathscr{C}}(H), \kappa'_{w\mathscr{C}}(H)\} \tag{5.1}$$

holds for $C \in \{U, S\}$.

Proof. Let $S \subseteq V \cup E$ be a vertex cut in $G(H)$ with $|S| = \kappa_{\mathcal{C}}(G(H))$.
Case 1: $S \subseteq V$, then $S = \{v_1, ..., v_k\}$ is a weak vertex cut in H and so it is a strong vertex cut in H, so $\kappa_{s\mathscr{C}}(H) \leq \kappa_{\mathcal{C}}(G(H))$.
Case 2: Suppose $S \subseteq E$. We step-wisely construct a vertex cut S' as follows by interacting over the hyperedges in S. In each step we add to S' a single vertex $v_i \in e_i$ that is not contained in $\bigcup_{j<i} \operatorname{supp}(e_j)$. By construction we have $|S'| \leq |S|$. Since $H \setminus_s S'$ is not strongly or unilaterally connected we have $\kappa_{s\mathscr{C}}(H) \leq \kappa_{\mathcal{C}}(G(H))$.
Case 3: Suppose $S \cap V \neq \emptyset$ and $S \cap E \neq \emptyset$. We write $S = \{v_1, ..., v_l, e_{l+1}, ..., e_k\}$ where $v_i \in V$ for $i \in \{1, ..., l\}$ and $e_i \in E$ for $i \in \{l+1, ..., k\}$. Let $S' = \{v_1, .., v_l\}$. We iterate over the $e_i \in S \cap E$ and, in each step, we add to S', if it exists, a vertex $v_i \in e_i$ satisfying $v_i \notin S \cap V$ and $v_i \notin \bigcup_{j<i} \operatorname{supp}(e_j)$. This yields a strong vertex cut containing $S \cap V$ and at most one vertex from each $e_i \in S \cap E$, thus $|S'| \leq |S|$. So $H \setminus_s S'$ is not strongly or unilaterally connected and $\kappa_{s\mathscr{C}}(H) \leq \kappa_{\mathcal{C}}(G(H))$.

Considering the other inequality, let $S \subseteq V$ be a minimal weak vertex cut in H with $|S| = \kappa_{w\mathscr{C}}(H)$. Since $H \setminus_w S$ is not strongly or unilaterally connected, then by Lemma 2.4,

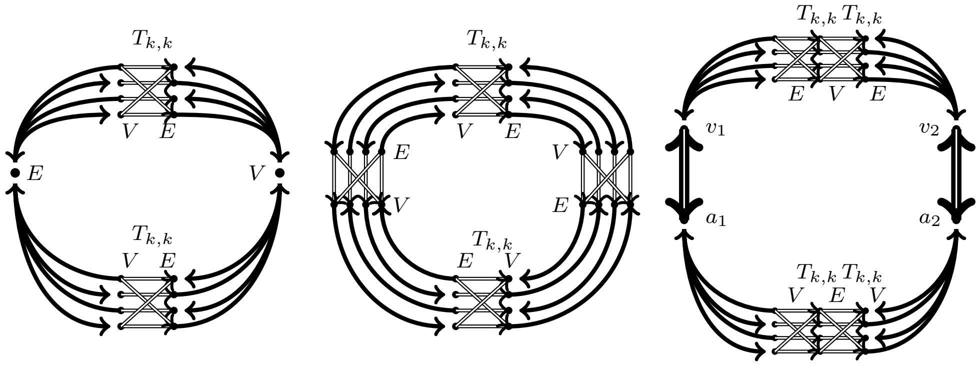


Figure 5: **Left**: König graph $G(H)$ of a hypergraph with $\kappa'_{w\mathscr{U}}(H) = \kappa_{w\mathscr{U}}(H) = k+1$ and $\kappa'_{w\mathscr{S}}(H) = \kappa_{w\mathscr{S}}(H) = \frac{k}{2}+1$. **Middle:** König graph $G(H)$ of a hypergraph with $\kappa_{s\mathscr{C}}(H) = \kappa'_{s\mathscr{C}} = 1$, $\kappa_{\mathcal{U}}(G(H)) = k+1$ and $\kappa_{\mathscr{S}}(G(H)) = k$. **Right:** König graph $G(H)$ of a hypergraph with $\kappa_{w_{\mathscr{C}}}(H) = \kappa'_{w\mathscr{C}}(H) = 2$, $\kappa'_{\mathcal{U}}(G(H)) = 2k$ and $\kappa'_{\mathcal{S}}(G(H)) = k+\frac{k}{2}$.

$G_H \setminus S$ is not strongly or unilaterally connected on $V \setminus S$, so $\kappa_{\mathcal{C}}(G(H)) \leq \kappa_{w\mathscr{C}}(H)$. Let $F \subseteq E$ be a minimal weak disconnecting set in H with $|S| = \kappa_{w\mathscr{C}}(H)$, as $H \setminus_w F$ is not strongly or unilaterally connected, then by Lemma 2.4, $G_H \setminus F$ is not unilaterally connected on V, so $\kappa_{\mathcal{C}}(G(H)) \leq \kappa'_{w\mathscr{C}}(H)$. Then $\kappa_{\mathcal{C}}(G(H)) \leq \min\{\kappa_{w\mathscr{C}}(H), \kappa'_{w\mathscr{C}}(H)\}$. □

In practice, however, $\min\{\kappa_{w\mathscr{C}}(H), \kappa'_{w\mathscr{C}}(H)\}$ is not a particularly good upper bound for $\kappa_{\mathcal{C}}(G(H))$ for either strong or unilateral connectedness. We show that the difference, in fact, can become arbitrarily large. Similarly, the difference $\kappa_{\mathcal{C}}(G(H)) - \kappa_{s\mathscr{C}}(H)$ can also become arbitrarily large for both strong and unilateral connectedness.

The graph in the left panel of Figure 5 is the König digraph $G(H)$ of a directed hypergraph $H = (V, E)$ with $\kappa_{\mathcal{U}}(G(H)) = \kappa_{\mathcal{S}}(G(H)) = 2$ (as seen by removing the vertices that are not in any $T_{k,k}$ subgraph). On the other hand, removing only vertices in V, we need to eliminate $k+1$ vertices for $G(H)$ to destroy unilateral connectedness, namely k vertices in one of the $T_{k,k}$ in the V set partition, and one vertex V that is not in these complete digraphs. We need to remove $\frac{k}{2}+1$ vertices for $G(H)$ not being strongly connected, $\frac{k}{2}$ vertices in any of the $T_{k,k}$ in the V set (the ones that are in- or out-neighbors of a vertex in E that is not in any $T_{k,k}$), and a vertex V that is not in any $T_{k,k}$ digraph. Therefore $\kappa_{w_U}(H) = k+1$ and $\kappa_{w\mathscr{S}}(H) = \frac{k}{2}+1$. The same argument is correct for eliminating vertices only in E so $\kappa'_{w\mathscr{U}}(H) = k+1$ and $\kappa'_{w\mathscr{S}}(H) = \frac{k}{2}+1$. As k increases, an infinite family of hypergraphs for which the difference $\min\{\kappa_{w\mathscr{C}}(H), \kappa'_{w\mathscr{C}}(H)\} - \kappa_{\mathcal{C}}(G(H))$ grows linearly is obtained.

The middle panel of Figure 5 shows the König graph $G(H)$ of a directed hypergraph $H = (V, E)$ with $\kappa_{\mathcal{U}}(G(H)) = k+1$ (removing the k vertices in of one partition set in $T_{k,k}$ and one in the same partition set in the adjacent complete digraph) and $\kappa_{\mathscr{S}}(G(H)) = k$ (removing the k vertices in of one partition set in $T_{k,k}$ subgraph and then any neighbor of any vertex in the other partition set of the same subgraph). In the hypergraph, on the other hand, it suffices to strongly eliminate any vertex in $G(H)$ to destroy strong connectedness, since this amount to removing a vertex together with its neighborhood from $G(H)$. Thus $\kappa_{s_{\mathscr{C}}}(H) = 1$. Therefore, $\kappa_{\mathcal{C}}(G(H)) - \kappa_{s\mathscr{C}}(H)k$. As k increases, we obtain an infinite family of hypergraphs for which this difference grows linearly.

Lemma 5.2. *Let $H = (V, E)$ be a directed hypergraph and $G(H) = (V \cup E, A)$ its König digraph. Then for $\mathscr{C} \in \{\mathscr{U}, \mathscr{S}\}$ holds*

$$\max\{\kappa_{w\mathscr{C}}(H), \kappa'_{w\mathscr{C}}(H)\} \leq \kappa'_{\mathcal{C}}(G(H)) \leq \delta_{\mathcal{C}}(G(H)). \tag{5.2}$$

Proof. Let $S \subseteq A$ be a minimal disconnecting set in $G(H)$ with $\mid S \mid = \kappa'_C(G(H)) = k$ and let $S' = \{v \in V | v \in \text{supp}(e) \wedge e \in S\}$. Note that $\mid S' \mid \leq \mid S \mid$. $G(H) \setminus S'$ is not strong or unilaterally connected (and in particular not unilaterally connected on V). Therefore S' is a weak disconnecting set in H by Lemma 2.4, and thus we have $\kappa_{w\mathscr{C}}(H) \leq \mid S' \mid \leq \mid S \mid = \kappa'_C(G(H))$. An analogous argument using $F = \{e \in E | e \in \text{supp}(e') \wedge e' \in S\}$ yields $\kappa'_{w\mathscr{C}}(H) \leq \mid S \mid = \kappa'_C(G(H))$. The remaining inequalities are the Whitney inequalities for digraphs [8]. □

Recall that in general we have $\delta_{\mathscr{C}}(H) \leq \delta_{\mathscr{C}}(G(H))$. The inequality is strict for some hypergraphs. This is the case even if $\max\{\kappa'_{w\mathscr{C}}(H), \kappa_{w\mathscr{C}}\} = \kappa_{w\mathscr{C}}$. For example in Figure 2 (right) we have $\kappa_{w\mathscr{C}}(H) = k$ and $\delta_{\mathscr{C}}(H) = 1$ for both unilateral and strong connectedness assuming $\max\{\kappa'_{w\mathscr{C}}(H), \kappa_{w\mathscr{C}}\} = \kappa_{w\mathscr{C}}$.

We note, finally, that the difference $\kappa'_{\mathcal{C}}(G(H)) - \max\{\kappa_{w\mathscr{C}}(H), \kappa'_{w\mathscr{C}}(H)\}$ can be arbitrarily large. The right panel of Figure 5 shows the König digraph $G(H)$ of a directed hypergraph $H = (V, E)$ with even k is even and the arcs (v_1, a_1), (v_2, a_2) are k parallel arcs of each direction between these vertices. We $\kappa'_{\mathcal{U}}(G(H)) = 2k$ (due to removal of the $2k$ arcs incident with v_1 or v_2 or a_1 or a_2) and $\kappa'_{\mathcal{S}}(G(H)) = k + \frac{k}{2}$ (due to removal of the k arcs with tail (or head) any of the vertices v_1, v_2, a_1, a_2). In the hypergraph H, $\{v_1, v_2\}$ is a weak vertex cut, hence $\kappa_{w_{\mathscr{C}}}(H) = 2$. The same is true for removing $\{a_1, a_2\}$, thus $\kappa'_{w\mathscr{C}}(H) = 2$. Thus $\kappa'_{\mathcal{C}}(G(H)) - \max\{\kappa_{w\mathscr{C}}(H), \kappa'_{w\mathscr{C}}(H)\} \geq k + \frac{k}{2} - 2$. We therefore obtain an infinite family of hypergraphs for which this difference grows linearly with k.

6 Concluding remarks

We have seen that some of the connectivity invariants of directed hypergraphs are "ill-behaved" in the sense that they are not bounded by any other connectivity invariant. This is in particular the case for $\kappa'_{s\mathscr{C}}$. It is an interesting open question, therefore, whether there are interesting structural constraints on the directed hypergraph for which $\kappa'_{s\mathscr{C}}$ is bounded by some of the other connectivity parameters. A class of hypergraphs that is relevant in this context are those whose minimal cut sets are covered by collections of hyperedges that form a disconnecting set. It remains a question for future research whether such connectivity properties are related to classes of hypergraphs that have already received attention in the literature.

ORCID iDs

Anahy Santiago Arguello https://orcid.org/0000-0001-6574-0446
Peter F. Stadler https://orcid.org/0000-0002-5016-5191

References

[1] X. Allamigeon, On the complexity of strongly connected components in directed hypergraphs, *Algorithmica* **69** (2014), 335–369, doi:10.1007/s00453-012-9729-0.

[2] J. L. Andersen, C. Flamm, D. Merkle and P. F. Stadler, Chemical transformation motifs — modelling pathways as integer hyperflows, *IEEE/ACM Trans. Comp. Biol.* **16** (2019), 510–523, doi:10.1109/TCBB.2017.2781724.

[3] G. Ausiello and L. Laura, Directed hypergraphs: Introduction and fundamental algorithms—a survey, *Theor. Comp. Sci.* **658** (2017), 293–306, doi:10.1016/j.tcs.2016.03.016.

[4] M. A. Bahmanian and M. Sajna, Connection and separation in hypergraphs, *Theory Appl. Graphs* **2** (2015), 5, doi:10.20429/tag.2015.020205.

[5] M. Dewar, D. Pike and J. Proos, Connectivity in hypergraphs, *Canadian Math. Bull.* **61** (2018), 252–271, doi:10.4153/CMB-2018-005-9.

[6] N. Franzese, A. Groce, T. M. Murali and A. Ritz, Hypergraph-based connectivity measures for signaling pathway topologies, *PLoS Comput Biol* **15** (2019), e1007384, doi:doi.org/10.1371/journal.pcbi.1007384.

[7] G. Gallo, G. Longo, S. Pallottino and S. Nguyen, Directed hypergraphs and applications, *Discr. Appl. Math.* **42** (1993), 177–201, doi:10.1016/0166-218X(93)90045-P.

[8] D. Geller and F. Harary, Connectivity in digraphs, in: M. Capobianco, J. B. Frechen and M. Krolik (eds.), *Recent Trends in Graph Theory*, Springer, Berlin, volume 186, pp. 105–115, 1971, doi:10.1007/BFb0059429.

[9] S. Klamt, U. U. Haus and F. Theis, Hypergraphs and cellular networks, *PLoS Comput Biol.* **5** (2009), e1000385, doi:10.1371/journal.pcbi.1000385.

[10] S. Nguyen, S. Pallottino and M. Gendreau, Implicit enumeration of hyperpaths in a logit model for transit networks, *Transportation Science* **32** (1998), 54–64, doi:10.1287/trsc.32.1.54.

[11] C. C. Özturan, On finding hypercycles in chemical reaction networks, *Appl. Math. Lett.* **21** (2008), 881–884, doi:10.1016/j.aml.2007.07.031.

[12] T. R. S. Walsh, Hypermaps versus bipartite maps, *J. Comb. Theory B* **18** (1975), 155–163, doi:10.1016/0095-8956(75)90042-8.

[13] H. Whitney, Congruent graphs and the connectivity of graphs, *Amer. J. Math.* **54** (1932), 150–168, doi:10.1007/978-1-4612-2972-8_4.

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P1.02
https://doi.org/10.26493/2590-9770.1364.48b
(Also available at http://adam-journal.eu)

Minimizing vertex-degree function index for k-generalized quasi-unicyclic graphs*

Ioan Tomescu
Faculty of Mathematics and Computer Science, Bucharest University, Str. Academiei, 14, 010014 Bucharest, Romania

Received 05 March 2020, accepted 23 January 2021, published online 7 March 2022

Abstract

In this paper the problem of minimizing vertex-degree function index $H_f(G)$ for k-generalized quasi-unicyclic graphs of order n is solved for $k \geq 1$ and $n \geq 2k+2$ if the function f is strictly increasing and strictly convex. These conditions are fulfilled by general first Zagreb index ${}^0R_\alpha(G)$ if $\alpha > 1$, second multiplicative Zagreb index $\prod_2(G)$ and sum lordeg index $SL(G)$. The extremal graph is unique for $k=1, n=4$ and for $k \geq 2$ and it consists from a path $x_1, x_2, \ldots, x_{n-1}$ and a new vertex x_n adjacent with x_k, x_{k+1} and x_{k+2}.

Keywords: Vertex-degree function index, general first Zagreb index, second multiplicative Zagreb index, sum lordeg index, k-generalized quasi-unicyclic graph, Jensen inequality.

Math. Subj. Class.: 05C35, 05C75, 05C09

1 Introduction

Let G be a simple graph. By $V(G)$ and $E(G)$ we denote the vertex set and the edge set of G, respectively. Let $e(G)$ be the number of edges of G. For any $x \in V(G)$, we denote by $d_G(x)$ the degree of x, i.e., the number of neighbors of x in G. If the graph G is clear under the context, then we use $d(x)$ instead of $d_G(x)$. A vertex with degree one will also be referred as a *pendant vertex*. Suppose that $V(G) = \{v_1, v_2, \ldots, v_n\}$ and the degree of vertex v_i equals d_i for $i = 1, 2, \ldots, n$, then $\pi = (d_1, d_2, \ldots, d_n)$ is called the *degree sequence* of G. We always will enumerate the degrees in non-increasing order, i.e., $d_1 \geq d_2 \geq \ldots \geq d_n$. P_n and C_n will denote the path and cycle on n vertices.

*The author thanks the referees for valuable comments.
E-mail address: ioan@fmi.unibuc.ro (Ioan Tomescu)

For $S \subset V(G)$, the subgraph induced by S is denoted $G[S]$. For two vertex disjoint subsets $S, T \subset V(G)$, the induced bipartite graph between S and T is denoted by $G[S,T]$. For graph G and a subset X of $V(G)$, $G - X$ is the graph obtained from G by removing the vertices of X and all edges incident to any of them. In particular, when X consists of only one vertex v, $G - \{v\}$ is always abbreviated to $G - v$. Similar notation is $G - uv$, where $uv \in E(G)$.

A unicyclic graph G of order n is connected and has n edges. It consists of a cycle C_r, where $3 \le r \le n$ and some vertex-disjoint trees having each a vertex common with C_r. A bicyclic graph G of order n is a connected graph of size $e(G) = n + 1$. It has two linearly independent cycles which have a common vertex or a common path P_a with $a \ge 2$ or they are connected by a path P_b with $b \ge 2$. The *quasi-tree* is a graph G in which there exists a vertex $v \in V(G)$ such that $G - v$ is a tree. Similarly, if graph G has the property that $G - v$ induces a unicyclic graph for a suitable vertex v, then G is called a *quasi-unicyclic graph.* In [14], Xu et. al. generalized the concept of quasi-tree to *k-generalized quasi-tree* as:

Definition 1.1 ([14])**.** For any integer $k \ge 1$, the connected graph G is called a k-generalized quasi-tree, if there exists a subset $V_k \subseteq V(G)$ with cardinality k such that $G - V_k$ is a tree but for every subset V_{k-1} of cardinality $k-1$ of $V(G)$, the graph $G - V_{k-1}$ is not a tree.

In [14], the authors pointed out that any tree is a quasi-tree since the deletion of any pendant vertex will produce another tree. Thus, they called any tree a trivial quasi-tree, and other quasi-tree graphs as non-trivial quasi-trees. With the similar reason, any unicyclic graph with at least one pendant vertex is also a quasi-unicyclic graph. Motivated from Definition 1.1, Javaid et. al. [7] generalized the concept of quasi-unicyclic graph to *k-generalized quasi-unicyclic graph* as:

Definition 1.2 ([7])**.** For any integer $k \ge 1$, the connected graph G is called a k-generalized quasi-unicyclic graph, if there exists a subset $V_k \subseteq V(G)$ of cardinality k such that $G - V_k$ is a unicyclic graph but for every subset V_{k-1} of cardinality $k-1$ of $V(G)$, the graph $G - V_{k-1}$ is not unicyclic.

It is easily checked that a quasi-unicyclic graph which is not unicyclic is just a 1-generalized quasi-unicyclic graph. In what follows, we call the vertex set V_k of Definitions 1.1 and 1.2 as a *k-quasi-vertex set*, and we use the symbol $\mathcal{U}_n^k$ to denote the class of k-generalized quasi-unicyclic graphs with n vertices.

Notice that a graph may by a k-generalized quasi-unicyclic graph for several non-consecutive values of k.

For other notations in graph theory, we refer [13].

Among all (vertex) degree-based graph invariants, the first Zagreb index $M_1(G)$ [4] is a famous topological index. It is defined as

$$M_1(G) = \sum_{v \in V(G)} d^2(v).$$

The general first Zagreb index (sometimes referred as ”zeroth-order general Randić index” [8]), denoted by ${}^0R_\alpha(G)$ was defined [9] as

$${}^0R_\alpha(G) = \sum_{v \in V(G)} d(v)^\alpha,$$

where α is a real number, $\alpha \notin \{0,1\}$. For $\alpha = 2$ it is the first Zagreb index $M_1(G)$.

Extremal results concerning the first Zagreb index for trees, unicyclic and bicyclic graphs were obtained in [1, 3, 16].

The second multiplicative Zagreb index or modified Narumi-Katayama index [2, 6] is defined as

$$\prod_2(G) = \prod_{v\in V(G)} d(v)^{d(v)} = \prod_{uv\in E(G)} d(u)d(v).$$

This index is minimum if and only if $\ln \prod_2(G) = \sum_{v\in V(G)} d(v)\ln d(v)$ is minimum.

The sum lordeg index is one of the Adriatic indices introduced in [12] and it is defined by

$$SL(G) = \sum_{v\in V(G)} d(v)\sqrt{\ln d(v)} = \sum_{v\in V(G):d(v)\geq 2} d(v)\sqrt{\ln d(v)}.$$

The vertex-degree function index $H_f(G)$ was defined in [15] as

$$H_f(G) = \sum_{v\in V(G)} f(d(v))$$

for a function $f(x)$ defined on positive real numbers. In this paper we will impose to function $f(x)$ to be (i) strictly increasing and (ii) strictly convex. All indices mentioned above are vertex-degree function indices $H_f(G)$: ${}^0R_\alpha(G)$ corresponds to $f(x) = x^\alpha$ which satisfies (i)–(ii) for $\alpha > 1$; the natural logarithm of the second multiplicative Zagreb index $\prod_2(G)$ to $f(x) = x\ln x$ which satisfies (i)–(ii) for $x \geq 1$ and sum lordeg index to $f(x) = x\sqrt{\ln x}$ satisfying (i)–(ii) for $x \geq 2$ (see [5]).

The rest of the paper is organized as follows. In Section 2, we introduce a function defined on the partitions of n and give some properties concerning the minimum of this function. In Section 3, we solve the problem of minimizing the vertex-degree function index $H_f(G)$, where $f(x)$ verifies (i)–(ii) for k-generalized quasi-unicyclic graphs of order n for $k \geq 1$ and $n \geq 2k+2$. Section 4 includes an extremal result of this type for k-generalized quasi-trees when $k \geq 2$ and $n \geq 3k$.

2 Preliminary results

In what follows we shall suppose that function $f(x)$ satisfies requirements (i)–(ii). The following lemmas will be used in our proofs.

Lemma 2.1. *Let $y > 0$ and $x \geq y+2$. Then*

$$f(x) + f(y) > f(x-1) + f(y+1).$$

Proof. The function $f(x)$ being strictly convex, $\varphi(x) = f(x+1) - f(x)$ is a strictly increasing function. Since $x-1 \geq y+1 > y$ it follows that $\varphi(x-1) > \varphi(y)$, or $f(x) - f(x-1) > f(y+1) - f(y)$. □

For integers n, p such that $n \geq 1$ and $p \geq n$ denote by $D_{n,p}$ the set of n-tuples $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ such that $x_1 \geq x_2 \geq \ldots \geq x_n \geq 1$ and $\sum_{i=1}^n x_i = p$. Let the function $F(\mathbf{x}) = \sum_{i=1}^n f(x_i)$. By Lemma 2.1 the minimum of $F(\mathbf{x})$ is reached if and only if

$|x_i - x_j| \leq 1$ for every $1 \leq i < j \leq n$, or equivalently, if and only if $x_1 + x_2 + \ldots + x_n$ is an equipartition of p, having almost equal parts. It follows that the point of minimum of $F(\mathbf{x})$ on $D_{n,p}$ is unique.

Lemma 2.2. *If $q > p \geq n$ then*

$$\min_{\mathbf{x} \in D_{n,q}} F(\mathbf{x}) > \min_{\mathbf{x} \in D_{n,p}} F(\mathbf{x}).$$

Proof. If $p = kn + r$, where $0 \leq r \leq n-1$, then the point $\mathbf{x}^* = (x_1^*, \ldots, x_n^*)$ where $F(\mathbf{x})$ reaches its minimum is $x^* = (k, k, \ldots, k)$ for $r = 0$. Otherwise, $x_1^* = \ldots = x_r^* = k+1$ and $x_{r+1}^* = \ldots = x_n^* = k$. If $\mathbf{x}^* = (x_1^*, \ldots, x_n^*)$ and $\mathbf{y}^* = (y_1^*, \ldots, y_n^*)$ denote the points of minimum of $F(\mathbf{x})$ in $D_{n,p}$ and in $D_{n,p+1}$, respectively, it follows that there is an index $t, 1 \leq t \leq n$ such that $y_t^* = x_t^* + 1$ and $y_i^* = x_i^*$ for $i \neq t$. We get $F(\mathbf{y}^*) > F(\mathbf{x}^*)$, therefore

$$\min_{\mathbf{x} \in D_{n,q}} F(\mathbf{x}) > \min_{\mathbf{x} \in D_{n,q-1}} F(\mathbf{x}) > \ldots > \min_{\mathbf{x} \in D_{n,p}} F(\mathbf{x}).$$

□

For a natural number s, $1 \leq s \leq n-1$, denote by $D_{n,p}^s \subset D_{n,p}$ the set of n-tuples $(x_1, x_2, \ldots, x_n) \in D_{n,p}$ such that the last s components are equal to 1: $x_{n-s+1} = x_{n-s+2} = \ldots = x_n = 1$. The following property also holds by Lemma 2.1:

Lemma 2.3. *If $s < t \leq n-1$ and $p \geq 2n - t + 1$ then*

$$\min_{\mathbf{x} \in D_{n,p}^s} F(\mathbf{x}) < \min_{\mathbf{x} \in D_{n,p}^t} F(\mathbf{x}).$$

Proof. Let $\mathbf{x}^* = (x_1^*, \ldots, x_n^*)$ be the point of minimum of $F(\mathbf{x})$ in $D_{n,p}^t$. It follows that $x_{n-t+1}^* = \ldots = x_n^* = 1$. Since $p \geq 2n - t + 1$, we deduce that $x_1^* \geq 3$. By rearranging the numbers $x_1^* - 1, x_2^*, \ldots, x_{n-t}^*, 2, 1, \ldots, 1$ in decreasing order we get the vector denoted by $\mathbf{y}^*$, which belongs to $D_{n,p}^{t-1}$. We get that $F(\mathbf{x}^*) > F(\mathbf{y}^*) \geq \min_{D_{n,p}^s} F(\mathbf{x})$ and lemma holds. □

Since $\sum_{i=1}^n d_i = 2e(G)$ we get:

Lemma 2.4. *We have*

$$H_f(G) \geq \min_{\mathbf{x} \in D_{n,2e(G)}} F(\mathbf{x}).$$

Equality may hold only if the point of minimum $(x_1^*, x_2^*, \ldots, x_n^*)$ of $F(x_1, x_2, \ldots, x_n)$ in $D_{n,2e(G)}$ is graphical, i.e., if there exists a graph G with degrees $d_i = x_i^*$ for $i = 1, \ldots, n$.

3 Main results

Let $k \geq 1$ and $n \geq 2k+2$. By $F_{n,k}$ we denote the graph consisting of a path $x_1, x_2, \ldots, x_{n-1}$ and a new vertex x_n which is adjacent to x_k, x_{k+1} and x_{k+2}. For $k \geq 2$ and $n \geq 2k+2$, this bicyclic graph belongs to the class $\mathcal{U}_n^k$ of k-generalized quasi-unicyclic graphs with n vertices. For $k = 1$ and $n = 4$ this graph, denoted $F_{4,1}$, consists of two cycles C_3 having a common edge and belongs to the class $\mathcal{U}_4^1$. For $k \geq 2$ we have $H_f(F_{n,k}) = 4f(3) + (n-6)f(2) + 2f(1)$ and this expression does not depend on k.

Theorem 3.1. *If $G \in \mathcal{U}_n^1$ and $n \geq 4$, then we have $H_f(G) \geq 2f(3) + (n-2)f(2)$. The equality is reached if and only if G has two vertices of degree three and $n-2$ vertices of degree two, i.e., it consists of two vertex disjoint cycles joined by a path P_s or two cycles having a common path P_t,where $s, t \geq 2$. The extremal graph is unique only for $n = 4$, when it coincides to $F_{4,1}$.*

Proof. Suppose that $G \in \mathcal{U}_n^1$ has minimum $H_f(G)$. Since $G \in \mathcal{U}_n^1$, there exists a vertex v_0 such that $G - v_0$ is a connected unicyclic graph with $n-1$ vertices and $n-1$ edges. We first will prove that $d_G(v_0) = 2$. Since $k = 1$, by Definition 1.2, G is not a unicyclic graph and so $d_G(v_0) \geq 2$. We assume that $d_G(v_0) \geq 3$. If v_0u is an edge of G, denote $G_1 = G - v_0u$. Let $H = G - v_0 = G_1 - v_0$, which is a unicyclic graph. G_1 is not unicyclic because its number of edges equals $|E(H)| + d_G(v_0) - 1 \geq n+1$. It follows that $G_1 \in \mathcal{U}_n^1$. Since $G_1 = G - v_0u$ we get $H_f(G) > H_f(G_1)$, a contradiction, since function $f(x)$ is strictly increasing.
Consequently, G has $n - 1 + 2 = n + 1$ edges. In $D_{n,2n+2}$ the minimum of the function $F(\mathbf{x})$ is reached for the n-tuple $(3, 3, 2, 2, \ldots, 2)$, since $3+3+2+\ldots+2$ is an equipartition of $2n + 2$ with n almost equal parts. The degree sequence $(3^2, 2^{n-2})$ is graphical and any graphical realization consists of two vertex disjoint cycles joined by a path P_s or two cycles having a common path P_t, where $s, t \geq 2$ since G is connected. All these graphs belong to $\mathcal{U}_n^1$ and we are done. For $n = 4$ the extremal graph is $F_{4,1}$, composed from two C_3 with a common edge, for $n = 5$ there are two extremal graphs: G_1 and G_2, consisting of C_4 and a new vertex adjacent to two adjacent and nonadjacent vertices, respectively, of C_4. For $n = 6$ there exist five extremal graphs and so on. □

The following result was proved in [10]:

Theorem 3.2 ([10])**.** *If $k \geq 2, n \geq 2k + 2$ and $G \in \mathcal{U}_n^k$, then $M_1(G) \geq 4n + 14$, with equality if and only if $G = F_{n,k}$.*

An extension of this result is:

Theorem 3.3. *For $k \geq 2$ and $n \geq 2k + 2$, if $G \in \mathcal{U}_n^k$ then we have*

$$H_f(G) \geq 4f(3) + (n-6)f(2) + 2f(1).$$

The equality is reached if and only if $G = F_{n,k}$.

Proof. Let $G \in \mathcal{U}_n^k$ such that $H_f(G)$ is minimum. By Definition 1.2, there exists a k-quasi-vertex set, which is a subset $V_k \subseteq V(G)$ with cardinality k such that $G - V_k$ is a unicyclic graph but for every subset V_{k-1} of cardinality $k-1$ of $V(G)$, the graph $G - V_{k-1}$ is not unicyclic. Let $W_{n-k} = G - V_k$. If there exists a vertex $v \in V_k$ which is adjacent with a single vertex from W_{n-k}, then $V_{k-1} = V_k - v$ has the property that $G - V_{k-1}$ is unicyclic, which contradicts the Definition 1.2. It follows that every vertex of V_k is not adjacent to any vertex of W_{n-k} or is adjacent to at least two vertices from W_{n-k}. Suppose that the subgraph $G[V_k]$ has $r \geq 1$ connected components $A_1, A_2, \ldots, A_r$. Since G is connected, we deduce that in each component there is at least one vertex which is adjacent with at least two vertices from W_{n-k}. Indeed, since G is connected, it follows that for every $i, 1 \leq i \leq r$, in component A_i of $G[V_k]$ there is a vertex v_i which is adjacent to at least one vertex in W_{n-k}. If v_i would be adjacent to a single vertex in W_{n-k}, this would contradict the property that every vertex of V_k is not adjacent to any vertex or is adjacent to at least two vertices of W_{n-k}. Each component i has at least $|A_i| - 1$ edges and equality holds if and only if this component is a tree. It follows that the number of edges of G having at least one end in V_k is at least $2r + \sum_{i=1}^{r}(|A_i| - 1) = 2r + k - r = k + r \geq k+1$. Since W_{n-k} is a unicyclic graph it has $n - k$ edges. We get that the number of edges of G is at least $k + 1 + n - k = n + 1$. Equality holds only if $r = 1$ and $G[V_k]$ has exactly $|V_k| - 1$ edges, i.e., $G[V_k]$ is a tree. In other words, this happens when $G[V_k]$ is a tree with k vertices and exactly one vertex, say w of this tree is adjacent with exactly two vertices of W_{n-k}. In this case G is bicyclic, having $e(G) = n + 1$ edges.

Now the proof splits into the following two cases: Case 1. $e(G) = n + 1$ and Case 2. $e(G) \geq n + 2$.

Case 1. In this case G has at least one pendant vertex, since $G[V_k]$ is a tree with $k \geq 2$ vertices and exactly one vertex of this tree, denoted by w is adjacent to two vertices from W_{n-k}. Other four subcases may hold: Subcase 1.1. G has one pendant vertex. Subcase 1.2. G has two pendant vertices. Subcase 1.3. G has three pendant vertices. Subcase 1.4. G has at least four pendant vertices.

Subcase 1.1. Since G is a connected bicyclic graph of size $n + 1$ with one pendant vertex one obtains that $G[V_k]$ is a path $w, y_1, y_2, \ldots, y_{k-1}$ and $d_G(w) = 3, d_G(y_1) = 2, \ldots, d_G(y_{k-2}) = 2$ and $d_G(y_{k-1}) = 1$. The degree sequence may be $\pi_1 = (3^3, 2^{n-4}, 1)$, $\pi_2 = (4, 3, 2^{n-3}, 1)$ or $\pi_3 = (5, 2^{n-2}, 1)$. We shall prove that in all cases $G \notin \mathcal{U}_n^k$. If the degree sequence is π_1 then G contains two cycles C_r and C_s having a common path $P = u, \ldots, v$ where $u \neq v$ or C_r and C_s are vertex disjoint and they are joined by P and $w \neq u, v$. In this case we can find a vertex $z \neq w, y_1, y_2, \ldots, y_{k-1}, u, v$ such that if $V_{k-1} = \{y_2, \ldots, y_{k-1}, z\}$ then $G - V_{k-1}$ is unicyclic, a contradiction. If the degree sequence of G is π_2, then C_r and C_s have a common vertex and a similar conclusion as for π_1 holds. In case of π_3, w coincides with the common vertex of C_r and C_s, but in this situation $G - V_k$ is not a unicyclic graph being disconnected, which contradicts the hypothesis.

Subcase 1.2. In this case G has two pendant vertices. We further prove that the unique graph in this situation belonging to $\mathcal{U}_n^k$ is $F_{n,k}$. We consider other two subcases: Subcase 1.2.1. $G[V_k]$ is a path, as in the subcase 1.1. Subcase 1.2.2. The tree $G[V_k]$ has two pendant vertices and the vertex w is adjacent to two vertices of W_{n-k}.

Subcase 1.2.1. In this case, as in the subcase 1.1, G consists of two cycles, C_r and C_s, where $r, s \geq 3$, a path $P = u, \ldots, v$ connecting cycles C_r and C_s or being a common path of C_r and C_s and a path $w, y_1, \ldots, y_{k-1}$. Since G has two pendant vertices there exists another path having an end denoted by $q \neq w$, where $w, q \in V(C_r) \cup V(C_s) \cup V(P)$. If cycles C_r and C_s are disjoint or $\max\{r, s\} \geq 4$ and cycles have a common path or cycles have only a common vertex we can always find a vertex z such that $G - V_{k-1}$ is unicyclic, where $V_{k-1} = \{y_2, \ldots, y_{k-1}, z\}$, a contradiction. The remaining case is when $C_r = C_s = C_3$ and the cycles have a common edge. In this last case $G = F_{n,k} \in \mathcal{U}_n^k$.

Subcase 1.2.2. In this situation $G[V_k]$ consists of two paths having a common vertex w or it contains one vertex of degree three different from w. In both cases we can find a subset $X \subset V_k$ of cardinality $k-2$ such that $G[V_k - X]$ is an edge with an end w. As in the previous cases, G contains two cycles C_r and C_s having a common path $P = u, \ldots, v$ or C_r and C_s are vertex disjoint and they are joined by P, or the cycles have only a common vertex (when $u = v$), $w \in V(C_r) \cup V(C_s) \cup V(P)$ and $w \neq u, v$. In this case we can find a vertex $z \notin V_k \cup \{u, v\}$ such that $G - V_{k-1}$ is unicyclic, where $V_{k-1} = X \cup \{z\}$, a contradiction.

Subcase 1.3. Since $k \geq 2$ we have $n \geq 2k+2 \geq 6$. We shall consider the cases $n = 6$; $n = 7$ and $n \geq 8$.

If $n = 6$ then $\min_{\mathbf{x} \in D^3_{6,14}} F(\mathbf{x})$ is reached for $\mathbf{x}^* = (4^2, 3, 1^3)$ by Lemma 2.1 and $H_f(G) \geq F(\mathbf{x}^*) = 2f(4) + f(3) + 3f(1) > H_f(F_{6,2}) = 4f(3) + 2f(1)$, a contradiction, since this inequality is equivalent to

$$2f(4) + f(1) > 3f(3). \tag{3.1}$$

Since f is strictly convex by Jensen inequality we get $f(4) + f(2) > 2f(3)$ and by Lemma 2.1 we deduce $f(4) + f(1) > f(3) + f(2)$. By summing up these inequalities we find (1).

Similarly, for $n = 7$ we deduce $H_f(G) \geq \min_{\mathbf{x} \in D^3_{7,16}} F(\mathbf{x})$. This minimum is reached for $\mathbf{x}^* = (4, 3^3, 1^3)$ by Lemma 2.1 and $F(\mathbf{x}^*) = f(4) + 3f(3) + 3f(1) > H_f(F_{7,2}) = 4f(3) + f(2) + 2f(1)$, a contradiction since this inequality is equivalent to $f(4) + f(1) > f(3) + f(2)$.

If $n \geq 8$ then $\min_{\mathbf{x} \in D^3_{n,2n+2}} F(\mathbf{x})$ is reached for $\mathbf{x}^* = (3^5, 2^{n-8}, 1^3)$ by Lemma 2.1 and $H_f(G) \geq F(\mathbf{x}^*) = 5f(3) + (n-8)f(2) + 3f(1) > H_f(F_{n,k}) = 4f(3) + (n-6)f(2) + 2f(1)$, a contradiction, since this inequality is equivalent to $f(3) + f(1) > 2f(2)$. The last inequality follows by Jensen inequality since f is strictly convex.

Subcase 1.4. Suppose that G has $s \geq 4$ pendant vertices. By Lemma 2.3 we have $\min_{\mathbf{x} \in D^s_{n,2n+2}} F(\mathbf{x}) > \min_{\mathbf{x} \in D^3_{n,2n+2}} F(\mathbf{x})$, which implies $H_f(G) > H_f(F_{n,k})$, which is again a contradiction.

Case 2. If $e(G) = n + 2$ then $\min_{\mathbf{x} \in D_{n,2n+4}} F(\mathbf{x})$ is reached for $\mathbf{x}^* = (3^4, 2^{n-4})$ by Lemma 2.1. We get $H_f(G) \geq F(\mathbf{x}^*) = 4f(3) + (n-4)f(2) > H_f(F_{n,k}) = 4f(3) + (n-6)f(2) + 2f(1)$, or $2f(2) > 2f(1)$, which is true because f is strictly increasing and this fact contradicts the hypothesis about the minimality of G.

If $e(G) \geq n + 3$ Lemmas 2.4 and 2.2 yield that $H_f(G) \geq \min_{\mathbf{x} \in D_{n,2n+6}} F(\mathbf{x}) > \min_{\mathbf{x} \in D_{n,2n+4}} F(\mathbf{x}) > H_f(F_{n,k})$, which contradicts the hypothesis. Thus, the theorem holds. □

4 Concluding remarks

In this paper we have solved a minimization problem concerning the vertex-degree function index $H_f(G)$ in the class of k-generalized quasi-unicyclic graphs of order n for $k \geq 1$ and $n \geq 2k + 2$ if the function f is strictly increasing and strictly convex. This includes the case of general first Zagreb index ${}^0R_\alpha(G)$ if $\alpha > 1$, second multiplicative Zagreb index $\prod_2(G)$ and sum lordeg index $SL(G)$. For general first Zagreb index ${}^0R_\alpha(G)$ this problem was solved in [10] by other means for $\alpha = 2$.

By similar methods one can prove that for $k \geq 2$ and $n \geq 3k$ the k-generalized quasi-trees of order n which reach the minimum of $H_f(G)$ consist of three vertex-disjoint paths $x_1, \ldots, x_k; y_1, \ldots, y_p$ and $z_1, \ldots, z_q$, where $p, q \geq k$ and $p+q = n-k$ and three additional edges x_1y_1, y_1z_1 and z_1x_1. This minimum equals $3f(3) + (n-6)f(2) + 3f(1)$. The same result has been already obtained in [11] by using different arguments.

ORCID iDs

Ioan Tomescu https://orcid.org/0000-0002-4747-9843

References

[1] H. Deng, A unified approach to the extremal Zagreb indices for trees, unicyclic graphs and bicyclic graphs, *MATCH Commun. Math. Comput. Chem.* **57** (2007), 597–616, https://match.pmf.kg.ac.rs/content57n3.htm.

[2] M. Ghorbani, M. Songhori and I. Gutman, Modified narumi-katayama index, *Kragujevac J. Sci.* **34** (2012), 57–64, http://www.pmf.kg.ac.rs/kjs/index.php?option=com_content&view=article&id=41&Itemid=4.

[3] I. Gutman, Graphs with smallest sum of squares of vertex degrees, *Kragujevac J. Math.* **25** (2003), 51–54, https://imi.pmf.kg.ac.rs/kjm/en/index.php?page=vol_25.

[4] I. Gutman and N. Trinajstić, Graph theory and molecular orbitals. total φ-electron energy of alternant hydrocarbons, *Chem. Phys. Lett.* **17** (1972), 535–538, doi:10.1016/0009-2614(72)85099-1.

[5] W. R. Inc., Wolfram alpha, champaign, IL, 2020, https://www.wolframalpha.com.

[6] A. Iranmanesh, M. Hosseinzadeh and I. Gutman, On multiplicative zagreb indices of graphs, *Iranian J. Math. Chem.* **3** (2012), 145–154, doi:10.22052/ijmc.2012.5234.

[7] F. Javaid, M. K. Jamil and I. Tomescu, Extremal k-generalized quasi unicyclic graphs with respect to first and second Zagreb indices, *Discrete Appl. Math.* **270** (2019), 153–158, doi:10.1016/j.dam.2019.06.006.

[8] X. Li and I. Gutman, *Mathematical Aspects of Randić-Type Molecular Structure Descriptors*, Mathematical Chemistry Monographs No. 1, University of Kragujevac and Faculty of Science Kragujevac, 2006, https://match.pmf.kg.ac.rs/mcm1.htm.

[9] X. Li and J. Zheng, A unified approach to the extremal trees for different indices, *MATCH Commun. Math. Comput. Chem.* **54** (2005), 195–208, https://match.pmf.kg.ac.rs/content54n1.htm.

[10] M. Liu, K. Cheng and I. Tomescu, Some notes on the extremal k-generalized quasi-unicyclic graphs with respect to Zagreb indices, *Discrete Appl. Math.* **284** (2020), 616–621, doi:10.1016/j.dam.2020.03.048.

[11] M. Liu, I. Tomescu and J. Liu, Unified extremal results for k-apex unicyclic graphs (trees), *Discrete Appl. Math.* **288** (2021), 35–49, doi:10.1016/j.dam.2020.08.024.

[12] D. Vukičević and M. Gašperov, Bond additive modeling 1. adriatic indices, *Croat. Chem. Acta* **83** (2010), 43–260, https://hrcak.srce.hr/62202.

[13] D. West, *Introduction to Graph Theory*, Prentice Hall, 2001, https://faculty.math.illinois.edu/~west/igt/.

[14] K. Xu, J. Wang and H. Liu, The Harary index of ordinary and generalized quasi-tree graphs, *J. Appl. Math. Comput.* **45** (2014), 365–374, doi:10.1007/s12190-013-0727-4.

[15] Y. Yao, M. Liu, F. Belardo and C. Yang, Unified extremal results of topological indices and spectral invariants of graphs, *Discrete Appl. Math.* **271** (2019), 218–232, doi:10.1016/j.dam.2019.06.005.

[16] S. Zhang and H. Zhang, Unicyclic graphs with the first three smallest and largest first general Zagreb index, *MATCH Commun. Math. Comput. Chem.* **55** (2006), 427–438, https://match.pmf.kg.ac.rs/content55n2.htm.

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P1.03
https://doi.org/10.26493/2590-9770.1374.bf0
(Also available at http://adam-journal.eu)

Distributions of restricted rotation distances

Sean Cleary*

Department of Mathematics, The City College of New York and the CUNY Graduate Center, City University of New York, New York, NY 10031, USA

Haris Nadeem

Department of Computer Science, The City College of New York, City University of New York, New York, NY 10031, USA

Received 17 July 2020, accepted 26 October 2020, published online 21 March 2022

Abstract

Rotation distances measure the differences in structure between rooted ordered binary trees. The one-dimensional skeleta of associahedra are rotation graphs, where two vertices representing trees are connected by an edge if they differ by a single rotation. There are no known efficient algorithms to compute rotation distance between trees and thus distances in rotation graphs. Limiting the allowed locations of where rotations are permitted gives rise to a number of notions related to rotation distance. Allowing rotations at a minimal such set of locations gives restricted rotation distance. There are linear-time algorithms to compute restricted rotation distance, where there are only two permitted locations for rotations to occur. The associated restricted rotation graph has an efficient distance algorithm. There are linear upper and lower bounds on restricted rotation distance with respect to the sizes of the reduced tree pairs. Here, we experimentally investigate the expected restricted rotation distance between two trees selected at random of increasing size and find that it lies typically in a narrow band well within the earlier proven linear upper and lower bounds.

Keywords: Random binary trees, rotation distances.

Math. Subj. Class.: 05C05, 68P05, 05C12

*Corresponding author. This material is based upon work supported by the National Science Foundation under Grant No. #1417820 `http://cleary.ccnysites.cuny.edu`

E-mail addresses: cleary@sci.ccny.cuny.edu (Sean Cleary), haris.nadeem.bsc@gmail.com (Haris Nadeem)

1 Introduction

Binary trees capture hierarchical relationships in a wide range of settings. For example, when there is an order on leaves, binary search trees have broad use, see Knuth [16]. Simple local changes, called rotations, at nodes give rise to rotation distance and the rotation graph, where two trees are connected by an edge in the rotation graph if they differ by a single rotation. There are no known algorithms for computing rotation distance exactly in polynomial time, though there are some estimation algorithms which run in polynomial time of Baril and Pallo [1] and Cleary and St. John [11] and the problem is known to be fixed-parameter tractable, see Cleary and St. John [10]. But there is thus no known algorithm for calculating distances efficiently in rotation graphs. Given the apparent difficulty of computing rotation distance exactly, there are a number of related notions that have been considered, such as restricted rotation distance of Cleary [4], right-arm rotation distances of Cleary and Taback [12] and level-restricted rotation distances of Luccio, Pagli, and Mesa Enriquez [18]. In each of these, the locations where rotations are permitted is restricted in some way. If we only allow rotations either all along the right arm of the tree or only at the root and right child of the root, then there are linear-time algorithms for computing the resulting right-arm rotation and restricted rotation distances, see Cleary [4] and Cleary and Taback [12]. Thus we can explore the properties of distance in the related graph associated to restricted rotation distance. Here, we experimentally study the distributions of restricted rotation distance between randomly selected trees of increasing size and find that the distances appear to grow on average quite linearly with size with a linear coefficient of between three and four, with the distances distributed centrally arranged near the average in relatively narrow spreads.

This gives insight into the distribution of distances between pairs of trees in the restricted rotation graph which is not presently feasible at this scale for the rotation graph, and equivalently into the distribution of distances between vertices of the restricted rotation graph.

2 Background and definitions

In the following, by *tree* we mean a rooted binary tree where each node has either zero or two children, a left child and a right child. Such trees are sometimes called *0-2 trees* or *proper binary trees*, see Knuth [16]. A node with no children is a *leaf*, and a node with two children is an *internal node*. The *size* of a tree T is the number of internal nodes in T. We number the $n+1$ leaves in a tree with n internal nodes from left to right from 0 to n.

We encode binary trees via the standard encoding of a preorder traversal where an internal node is denoted by 1 and a leaf node by 0. So the left hand tree in Figure 1 has encoding 1101100101000 and the right hand tree has encoding 1101110001000. A *rotation* at a node P is the operation depicted in Figure 1 where one grandchild of P is promoted to become a child of P, one child is demoted to become a grandchild, and where one grandchild's parent node is switched in an order-preserving way. In terms of encodings, a left rotation at a node can be regarded as a string substitution of the form $\ldots 1x1yz\ldots$ becoming $\ldots 11xyz\ldots$ where x, y, and z are encodings of subtrees, with a right rotation the inverse string substitution operation.

Given two trees S and T of size n, Culik and Wood [13] showed that there is always at least one sequence of rotations transforming S to T and thus defined rotation distance. *Rotation distance* between S and T, denoted $d(S,T)$, is the minimum number of rotations

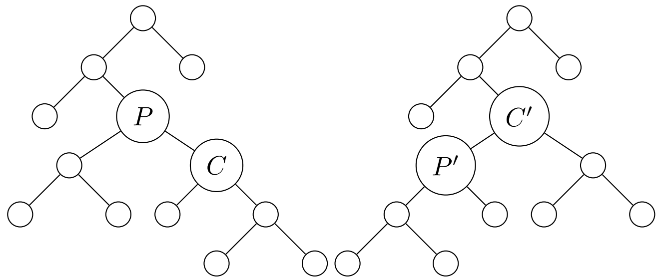


Figure 1: An example of a left rotation at node P, with a rotation promoting child node C to C' and demoting parent node P to P'. The left hand tree has encoding 1101100101000 and the right hand tree is 1101110001000. All other nodes are unaffected by the rotation at P. Right rotation at C' is the inverse operation, taking the tree on the right to the tree on the left.

needed to transform S to T where the rotations are permitted at any nodes present. We need not have rotations permitted at every node to transform any tree to any other- a minimal set of permitted rotations has size 2, as described by Cleary [4]. We take those two locations to be the root and the right child of the root, giving *restricted rotation distance* between S and T, denoted $d_R(S,T)$, as the minimum number of rotations needed to transform S to T where the rotations are permitted only at the root node (always present) and the right child of the root node, if present.

The *rotation graph* $RG(n)$ of size n is the graph whose vertices are rooted binary trees of size n and where two vertices are connected by an undirected edge if there is a single rotation transforming the one tree to the other. The rotation graph is the one-dimensional skeleton of the associahedron of the appropriate size. The notions foundational to the geometric realization of associahedra go back to Tamari [22] and Stasheff [21] and were first published concretely by Lee [17]. Here, we consider distances in the related *restricted rotation graph* $RRG(n)$ where the vertices are again trees and an edge is present between trees S and T if they differ by a single rotation at either the root or the right child of the root. We note that the restricted rotation graph does not enjoy the same set of symmetries as the ordinary rotation graph- in fact, not even the valence is the same for every vertex. Most vertices have valence 4, corresponding to left and right rotations at the root and right child of the root, but some have smaller valence if the right child of the root is not present or if rotation in a direction is not possible at one of those two nodes. There are vertices of valence 1 in this graph, whereas the rotation graph has high symmetry, arising from the dihedral symmetries inherited from the full associahedron.

A *tree pair* (S,T) is a pair of trees of the same size. A tree pair (S,T) is *unreduced* if there are nodes in both S and T such that leaf node children numbered as i and $i+1$, via preorder traversal of the tree, are the same in both trees. A *reduction* in a tree pair is the removal of such a pair of identically numbered siblings in each tree, replacing them with a single leaf i, and then renumbering to get a new tree pair (S',T') of one smaller size, see Cannon, Floyd and Parry [3] for background as well as for connections with Thompson's group F. A tree pair (S,T) is said to be *reduced* if there are no possible reductions. Note that for both rotation distance and restricted rotation distances, the distances between S and T are the same as between the representatives of their reduced tree pair S' and T' as the

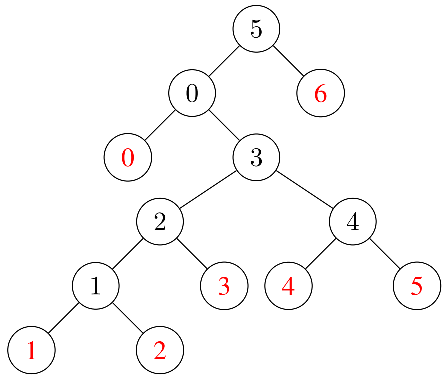


Figure 2: A tree of size 6 with leaves numbered in red from 0 to 6 and with internal nodes numbered from 0 to 5. Nodes 0 and 5 are left nodes and all other internal nodes are interior nodes.

same sequence of rotations will perform the required transformations, see [4]. The *binary address* of a node in a tree is a sequences of 0's and 1's representing the path from the root to the node with a 0 for each left child and 1 for each right child. For example, the address of node C in Figure 1 in the left hand tree is 011 as the path from the root to C is a left edge followed by two right edges.

A *right node* of a tree is one whose binary address consists only of 1's and has at least one 1. A *left node* is one whose binary address consists only of 0's. The root node is thus a left node but not a right node. All non-right and non-left nodes of a tree are *interior nodes*. We number nodes with an in-order traversal of the tree, and a *node pair* from a tree pair (S, T) is a pair of nodes numbered the same in such traversals. Figure 2 shows leaves and nodes numbered in the resulting left-to-right in-order traversals of leaves and interior nodes respectively.

To calculate restricted rotation distance, we use the methods of Fordham [15]. His methods were designed to calculate word length exactly in Thompson's group F with respect to the generating set $\{x_0, x_0^{-1}, x_1, x_1^{-1}\}$, and give minimal length representatives of a word with respect to that generating set. The generator x_0 corresponds to right rotation at the root, with x_0^{-1} correspondingly the inverse which is a left rotation at the root. Similarly, x_1 and its inverse correspond to rotations at the right child of the root. So word length in F translates into restricted rotation distance between trees, as described in [4, 12].

Fordham's method takes as input two trees forming a reduced tree pair, and classifies each interior node as one of seven types as follows:

- L_0: The first node on the left side of the tree.
- L_L: Any left node other than the leftmost node.
- I_0: An interior node with no right child.
- I_R: An interior node with a right child.
- R_I: Any right node numbered k whose immediate successor node $k+1$ is an interior node.

	R_0	R_{NI}	R_I	L_l	I_0	I_R
R_0	0	2	2	1	1	3
R_{NI}	2	2	2	1	1	3
R_I	2	2	2	1	3	3
L_l	1	1	1	2	2	2
I_0	1	1	3	2	2	4
I_R	3	3	3	2	4	4

Table 1: Weights for caret pairs by caret pair types.

.

- R_{NI}: A right node which is not of type R_I but for which there is some successor interior node.
- R_0: A right node with no successor interior node.

A primary result of Fordham [15] is that the word length $|w|$ in Thompson's group F with respect to the standard finite generating set can be calculated by classifying node pairs into those seven types and summing the totals from the Table 1. Note that the first node pair is always of type (L_0, L_0) and adds weight 0, and the single L_0 in each tree must necessarily be paired, so the caret type L_0 is not listed in Table 1.

As described [12], since all non-L_0 carets contribute at least one to word length (and thus at least one to restricted rotation distance), and since a caret can contribute at most 4 to word length, analysis of caret types and configurations give that for two trees forming a reduced pair of size n, the restricted rotation distance between lies between $n-1$ and $4n-8$ and is sharp for $n \geq 3$. Fordham's method goes further and can be in fact used to not only find restricted rotation distances, but also to find and enumerate all possible minimal length paths between the relevant trees. We note that there have been computations to calculate the number of words of Thompson's group F of increasing word length with respect to the standard generating set (and thus restricted rotation distances) of increasing sizes by Burillo, Cleary, and Weist [2] and Elder, Fusy, and Rechnitzer [14], with the latter giving the first 1500 terms of the OEIS sequence A156945 [20] which are the number of elements of increasing word length size. The relationship between word length size and tree size is linear but knowing word length gives only linear bounds on the tree size.

3 Distributions of restricted rotation distance

We study computationally the distribution of restricted rotation distance between rooted binary trees. This is equivalent to analyzing distances in the restricted rotation graph $RRG(n)$ between vertices. Work of Cleary and Maio [6] analyzes distributions of ordinary rotation distances. Here, we address similar questions for restricted rotation distances. The general question is: given two trees of the same size n, what is the expected restricted rotation distance between them? We anticipate that on average, larger tree pairs have larger distances between them, but we would like to estimate the rates of growth as well as the dispersal. Work of Cleary and Taback [12] gave sharp lower and asymptotically sharp upper bounds for restricted rotation distances, and we find that the vast majority of instances are clustered quite centrally and not near the bounds.

Tree size range	# sampled	Avg. red. frac.	Avg. RRD ratio
10–19	138999	0.907533	2.24473
20–29	161500	0.917172	2.64333
30–39	150500	0.920593	2.83326
40–49	133000	0.922663	2.9421
50–59	144000	0.923896	3.00793
60–69	134500	0.924459	3.05513
70–79	129000	0.924884	3.08993
80–89	119000	0.925221	3.1151
90–99	118500	0.925659	3.13679
100–199	685191	0.92646	3.19676
200–299	509390	0.927268	3.24813
300–399	310962	0.927496	3.26887
400–499	111460	0.927678	3.27999
500–599	89580	0.92783	3.28727
600–699	100600	0.927795	3.29198
700–799	102600	0.9279	3.29606
800–899	43600	0.927921	3.29866
900–999	45450	0.928027	3.30121
1000–1249	89200	0.928008	3.30416
1250–1499	86000	0.928002	3.3069
1500–1749	99000	0.928071	3.30908
1750–1999	35600	0.928121	3.31039
2000–2249	20000	0.928089	3.31145
2250–2499	19800	0.928089	3.31235
2500–2749	18764	0.928117	3.31311
2750–2999	13900	0.928124	3.31386
3000–3249	12124	0.928094	3.31407
3250–3499	8044	0.928185	3.31517
3500–3999	3072	0.928024	3.31562
4000–4500	800	0.928023	3.31568

Table 2: Tree pair restricted rotation distances for unreduced tree pairs. Given are the average fractions of the reduced tree pairs size of the originally generated tree pair size and the average ratio of restricted rotation distance to the generated tree pair size.

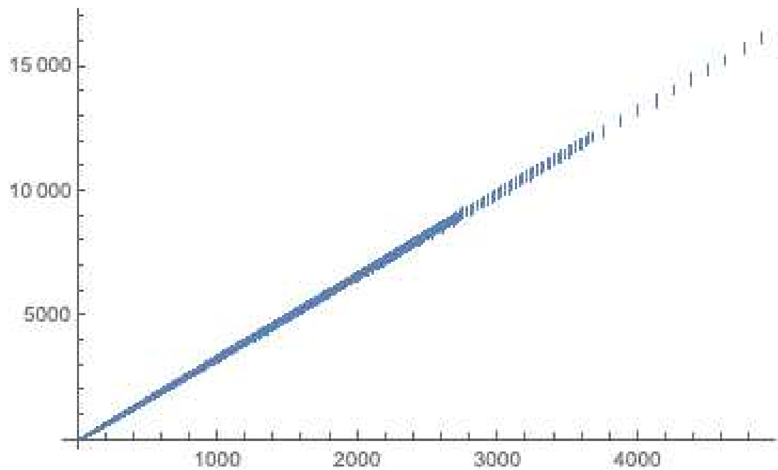


Figure 3: Restricted rotation distance vs. raw size for randomly selected tree pairs of increasing sizes.

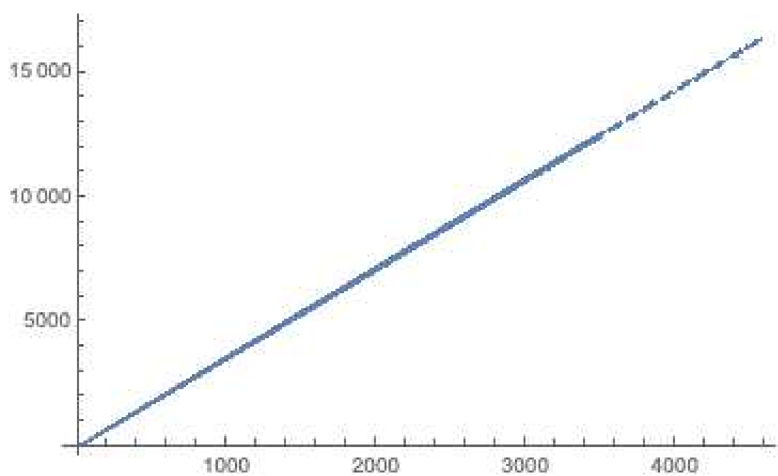


Figure 4: Restricted rotation distance vs. reduced size for randomly selected tree pairs of increasing sizes, by the size of the resulting reduced tree pair after reduction.

Tree size range	Number of tree pairs sampled	Average RRD size
10–19	168846	2.609
20–29	166650	2.96244
30–39	145364	3.12548
40–49	152971	3.22228
50–59	144317	3.28264
60–69	139509	3.32627
70–79	132652	3.35818
80–89	126454	3.38269
90–99	94370	3.40162
100–199	700470	3.45925
200–299	504029	3.50732
300–399	272408	3.52717
400–499	116513	3.53867
500–599	97243	3.54577
600–699	107923	3.55041
700–799	74740	3.55356
800–899	48099	3.55662
900–999	40737	3.55859
1000–1249	94865	3.56172
1250–1499	100074	3.56451
1500–1749	77950	3.56616
1750–1999	22109	3.56769
2000–2249	21630	3.56872
2250–2499	20622	3.5695
2500–2749	15851	3.57045
2750–2999	13158	3.57073
3000–3249	8342	3.57162
3250–3499	2607	3.57268
3500–3999	821	3.57276
4000–4500	717	3.57285

Table 3: Tree pair restricted rotation distances divided by tree pair size, for reduced tree pairs of increasing size ranges. There are examples with ratios as small as 1 and approaching 4 for all n.

We sample rooted binary tree pairs at random using Remy's algorithm [19] for each tree, which guarantees a uniform randomly generated tree of size n. Work on the asymptotic density of isomorphism classes of subgroups of Thompson's group F of Cleary, Elder, Rechnitzer and Taback [5] addresses the question of the expected fraction of tree pairs which are reduced, and later work of Cleary, Rechnitzer and Wong [9] describes the asymptotics of the expected sizes of reduced components of tree pairs.

Here, we study two main questions:

- Given two trees selected at random of size n, what is the expected restricted rotation distance between them?
- Given a reduced tree pair of size n, what is the expected restricted rotation distance between the pair?

We also seek to understand the deviations from the means of these distances. We generated tree pairs (S, T) at random, then calculated the reduced representatives (S', T') of each tree pair, then the corresponding restricted rotation distance, $d_R(S, T) = d_R(S', T')$, which are the same as the reductions reflect commonality which does not change the distance.

We note that generating reduced tree pairs of a specified size is not as feasible as generating tree pairs generally. As described in [9] and [5], a tree pair selected at random is likely to have a number of reductions, and the resulting reduced representative is on average about 10% smaller. But of course there is a (increasingly small) chance that the generated tree is already reduced, and also a (vanishingly small) chance that it reduces all the way down to the empty tree pair. Cleary, Rechnitzer and Wong [9] analyze some properties of the distribution of the resulting sizes of reduced tree pairs. Cleary and Maio [8] have an algorithm which guarantees to produce not only a reduced tree pair of a specified size, but is difficult in an additional sense as well– not having any obvious initial first moves along minimal length paths. Unfortunately, though that algorithm is efficient, it does not choose uniformly from among the possible ones. The particular number of such difficult instances is not even known precisely, though Cleary and Maio [7] calculate the number of such cases exhaustively for small sizes and approximately for larger ones.

By generating large families of trees across a range of sizes and then performing reductions, we get a range of reduced tree pairs to consider and analyze. The resulting reduced tree pairs are necessarily smaller than the generated, possibly reducible, tree pairs, but since the number of reductions vary, there is a dispersal in the resulting sizes of the reduced tree pairs. That is, if we generate 1400 tree pairs of size 1000, the smallest resulting reduced pair may be 896 and the largest 955, with a mean and median of about 928 with the most commonly occurring being 929 with 73 occurrences. The tree pairs were generated of fixed sizes, often 500 apart. Thus, after reductions, these sizes would reduce to different extents which may lead to gaps in the resulting reduced sizes. So we generate many examples across a range of increasing sizes in an effort to get representative samples across a broad range.

4 Experiments and discussion

For the computational experiments we described, we generated about 3.6 million tree pairs of sizes ranging from 10 to 4400. We reduced each tree pair to a reduced representative, and then calculated the restricted rotation distances using Fordham's method.

To compare average restricted rotation distances across a range of sizes, we consider the *RRD ratio*, which for a tree pair (S, T) of size n is $d_R(S, T)/n$. This gives a somewhat normalized measure of the typical contribution of tree carets to the restricted rotation distance and a sense of how quickly the restricted rotation distance grows with increased tree size. We note that trees realizing the lower bound of restricted rotation distance from [12] would have an RRD ratio limiting to 1, and those realizing the upper bound would have an RRD ratio limiting to 4.

Table 2 tabulates the results across a range of unreduced sizes, with Figure 3 plotting the results for these unreduced sampled tree pairs. We see tight linear behavior of distance with respect to raw size, despite the fact that the amount of reductions varies considerably and the resulting sizes have a large influence on the corresponding distances.

Owing to the time of computation, larger size tree pairs were not sampled as extensively as the smaller ones. In Figure 3 the sampling increments of size 500 are visible, and in Figure 4 the fact that those sizes have dispersed somewhat as the reductions in size vary is visible. The fraction of common edges in a more general sense was computed asymptotically by Cleary, Rechnitzer and Wong [9] to be $6 - \frac{16}{\pi} \sim 0.907$, so the observed fractions of reduced size from generated size of about 0.928 is consistent with that. That asymptotic analysis allowed reductions of internal common edges in addition to the peripheral ones relevant to the tree reductions considered here.

In the remaining analyses, we restrict our attention to the resulting generated reduced tree pairs as the distances are more tightly related to the sizes after reduction.

Table 3 tabulates the distances observed across a range of reduced tree pair sizes, and Figure 4 plots these results. We can again see tight linear behavior, where the reduced trees have on average larger rotation distances and a smaller spread in the observed reduced instances relative to the unreduced sizes.

The examples from Cleary and Taback [12] giving the bounds of $n - 1 \leq d_R(S, T) \leq 4n - 8$ are clearly quite constrained, as the vast majority of the sampled lengths lie close to about $3.57n$, well away from the upper and lower bounds. We note that in both cases, the maximum possible distances (about 4 times the size) and minimal possible distances (one less than the size) lie far away from the randomly-generated instances. This is not surprising as those examples to show the sharpness of the bounds were carefully constructed in a very specific manner to realize those bounds.

We note that the only entries in Table 1 that contribute 4 to restricted rotation distance are (I_R, I_0) and (I_R, I_R) which involve interior carets being paired with interior carets. Given that the average distances are well above 3, such caret pairings are necessarily quite common and cannot occur in the examples realizing the lower bounds of $n - 1$.

Not surprisingly, given the strong linear behavior observed, a fitted linear model agrees with the sampled data exceptionally well, giving $d_R(S, T) \sim 3.31941n - 17.0321$ for restricted rotation distance in terms of unreduced tree pair sizes n, and $d_R(S, T) \sim 3.57612n - 16.1551$ correspondingly for reduced tree pairs of size n.

We see that the standard deviations of the observed RRD ratios of restricted rotation distance are relatively small and stable, dropping steadily from about 0.33 for the smallest size trees sampled, to about 0.025 for tree sizes in the hundreds, then dropping to about 0.01 for tree sizes in the hundreds, with an observed average standard deviation of ratios of 0.009 for the largest tree sizes sampled. These are for the normalized ratios- the standard deviations do increase with size, albeit somewhat more slowly.

The distributions of restricted rotation for reduced tree pairs of a fixed size show an

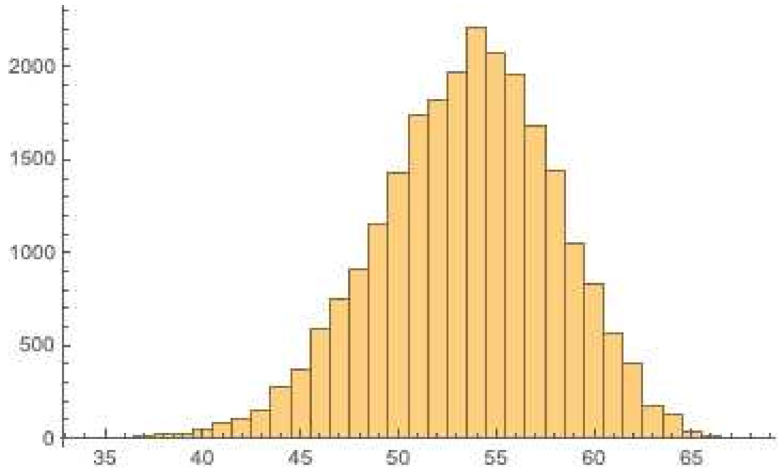


Figure 5: Distribution of restricted rotation distances for 24,067 randomly-produced reduced tree pairs of size 19. The sample mean is about 53.5 and the sample standard deviation is about 4.58.

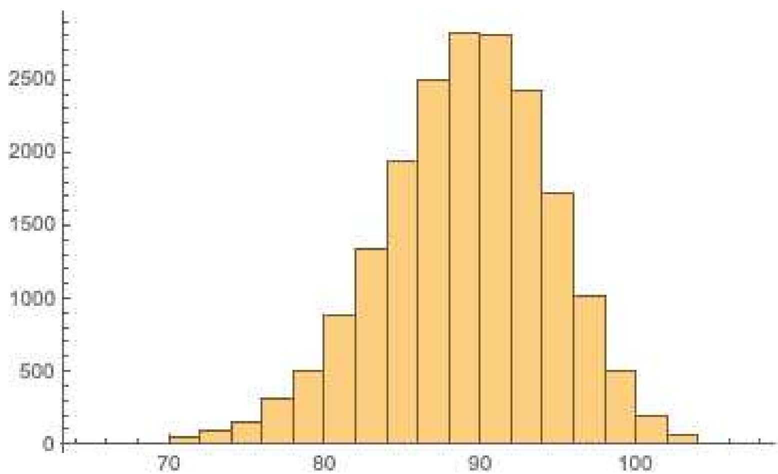


Figure 6: Distribution of restricted rotation distances for 19,307 randomly-produced reduced tree pairs of size 29. The sample mean is about 88.5 and the sample standard deviation is about 5.45.

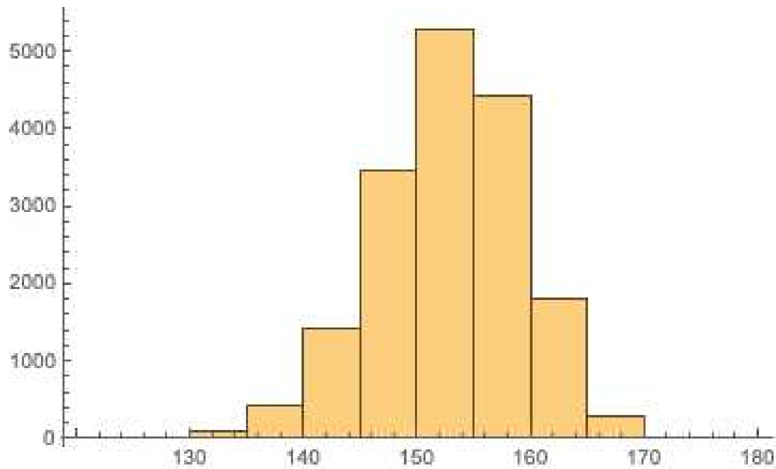


Figure 7: Distribution of restricted rotation distances for 17,196 randomly-produced reduced tree pairs of size 47. The sample mean is about 152.3 and the sample standard deviation is about 6.36.

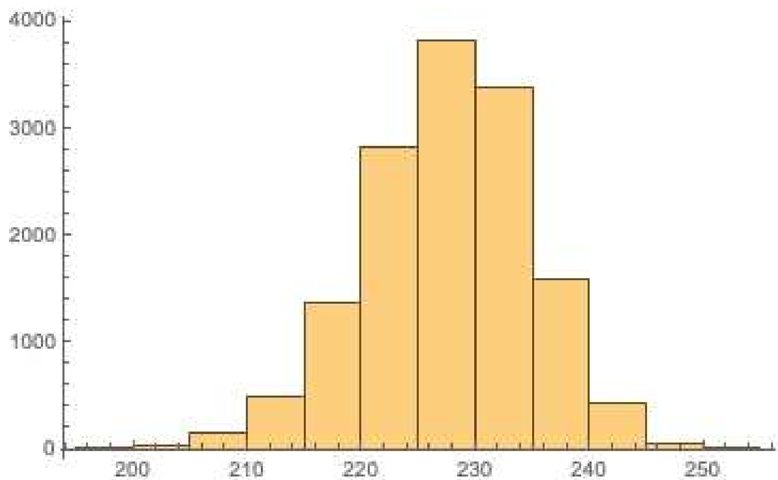


Figure 8: Distribution of restricted rotation distances for 14,155 randomly-produced reduced tree pairs of size 68. The sample mean is about 227.1 and the sample standard deviation is about 7.20.

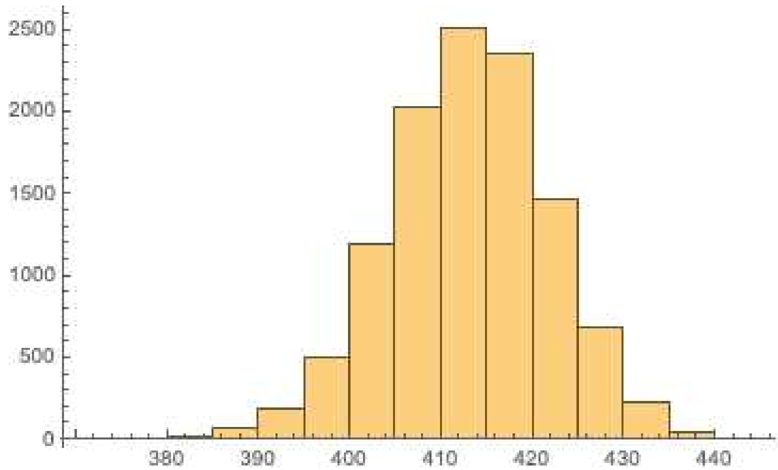


Figure 9: Distribution of restricted rotation distances for 11,258 randomly-produced reduced tree pairs of size 120. The sample mean is about 412.6 and the sample standard deviation is about 8.79.

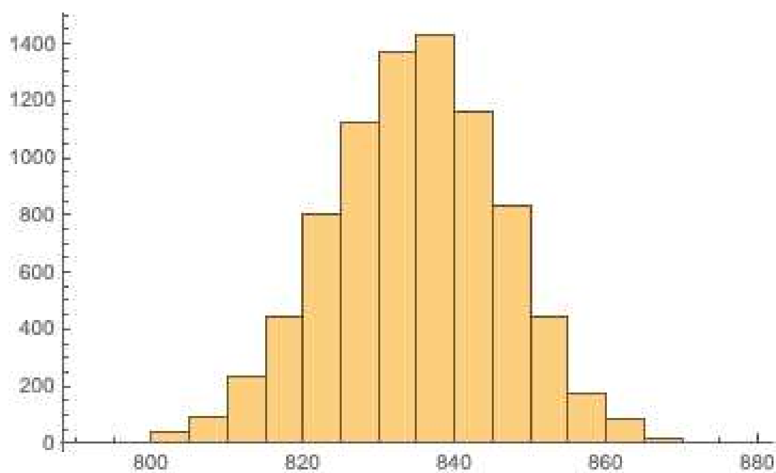


Figure 10: Distribution of restricted rotation distances for 8266 randomly-produced reduced tree pairs of size 238. The sample mean is about 834.3 and the sample standard deviation is about 11.4.

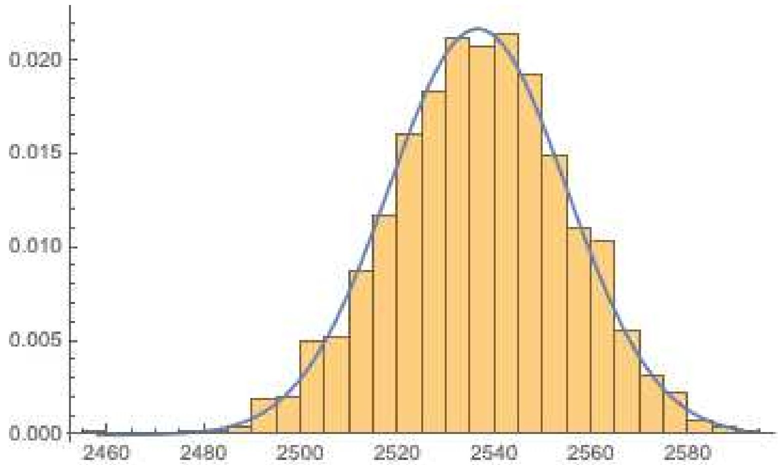


Figure 11: Distribution of restricted rotation distances for 1200 randomly-produced reduced tree pairs of size 714. The sample mean is about 2536.4. and the sample standard deviation is about 18.4. A normal distribution with the same mean and standard deviation is superimposed for comparison.

approximately normal shape, slightly skewed to the left for smaller sizes but less so for larger sizes. Here, we chose a few sizes for which there were a reasonable number of observed instances, shown in Figures 5 to Figure 11. These distributions have characteristic normal shapes, and further suggest that the extremely short and extremely long cases shown earlier to be possible are exceptionally rare. The vast majority of randomly-selected cases lie in relatively narrow bands concentrated on a line well away from the lowest and highest possible bounds. For the largest million tree pairs sampled, less than 175,000 were more than 1% away from the distance predicted by the linear model, and all but 1054 were within 3% of the linear prediction, with the largest observed deviation from the linearly fitted model being less than 5% away from the predicted distance. For the size 714 case illustrated in Figure 11, the lower bound of 713 is nearly 100 standard deviations below the sample mean and the upper bound of 2848 is about 17 standard deviations above the sample mean of 2536.

Thus we have developed some understanding of typical behavior of distances in restricted rotation graphs $RRG(n)$ for a decent range of distances. Note that analyzing the corresponding questions for the rotation graphs $RG(n)$ are not presently feasible beyond size about 20, even experimentally, due to the difficulty of computing ordinary rotation distance exactly, where the best known algorithms have exponential running time in the size of the trees.

ORCID iDs

Sean Cleary https://orcid.org/0000-0002-3123-8658

Haris Nadeem https://orcid.org/0000-0001-9283-2805

References

[1] J.-L. Baril and J.-M. Pallo, Efficient lower and upper bounds of the diagonal-flip distance between triangulations, *Inform. Process. Lett.* **100** (2006), 131–136, doi:10.1016/j.ipl.2006.07.001.

[2] J. Burillo, S. Cleary and B. Wiest, Computational explorations in Thompson's group F, in: *Geometric group theory*, Birkhäuser, Basel, Trends Math., pp. 21–35, 2007, doi:10.1007/978-3-7643-8412-8_2.

[3] J. W. Cannon, W. J. Floyd and W. R. Parry, Introductory notes on Richard Thompson's groups, *Enseign. Math. (2)* **42** (1996), 215–256, https://www.e-periodica.ch/digbib/view?pid=ens-001%3A1996%3A42%3A%3A398#416.

[4] S. Cleary, Restricted rotation distance between binary trees, *Inform. Process. Lett.* **84** (2002), 333–338, doi:10.1016/s0020-0190(02)00315-0.

[5] S. Cleary, M. Elder, A. Rechnitzer and J. Taback, Random subgroups of Thompson's group F, *Groups Geom. Dyn.* **4** (2010), 91–126, doi:10.4171/ggd/76.

[6] S. Cleary and R. Maio, Distributions of rotation distances, in preparation.

[7] S. Cleary and R. Maio, Counting difficult tree pairs with respect to the rotation distance problem, *J. Comb. Math. Comb. Comput.* **115** (2020), 199–213, doi:10.1080/01621459.2018.1537922.

[8] S. Cleary and R. Maio, An efficient sampling algorithm for difficult tree pairs, *Acta Cybern.* (2022), doi:10.14232/actacyb.285522.

[9] S. Cleary, A. Rechnitzer and T. Wong, Common edges in rooted trees and polygonal triangulations, *Electron. J. Combin.* **20** (2013), Paper 39, 22, doi:10.37236/2541.

[10] S. Cleary and K. St. John, Rotation distance is fixed-parameter tractable, *Inform. Process. Lett.* **109** (2009), 918–922, doi:10.1016/j.ipl.2009.04.023.

[11] S. Cleary and K. St. John, A linear-time approximation for rotation distance, *J. Graph Algorithms Appl.* **14** (2010), 385–390, doi:10.7155/jgaa.00212.

[12] S. Cleary and J. Taback, Bounding restricted rotation distance, *Inform. Process. Lett.* **88** (2003), 251–256, doi:10.1016/j.ipl.2003.08.004.

[13] K. Culik and D. Wood, A note on some tree similarity measures, *Inform. Process. Lett.* **15** (1982), 39–42, doi:10.1016/0020-0190(82)90083-7.

[14] M. Elder, É. Fusy and A. Rechnitzer, Counting elements and geodesics in Thompson's group F, *J. Algebra* **324** (2010), 102–121, doi:10.1016/j.jalgebra.2010.02.035.

[15] S. B. Fordham, Minimal length elements of Thompson's group F, *Geom. Dedicata* **99** (2003), 179–220, doi:10.1023/a:1024971818319.

[16] D. E. Knuth, *The art of computer programming. Volume 3*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1973, sorting and searching, Addison-Wesley Series in Computer Science and Information Processing.

[17] C. W. Lee, The associahedron and triangulations of the n-gon, *European J. Combin.* **10** (1989), 551–560, doi:10.1016/s0195-6698(89)80072-1.

[18] F. Luccio, A. Mesa Enriquez and L. Pagli, k-restricted rotation distance between binary trees, *Inform. Process. Lett.* **102** (2007), 175–180, doi:10.1016/j.ipl.2006.12.007.

[19] J.-L. Rémy, Un procédé itératif de dénombrement d'arbres binaires et son application à leur génération aléatoire, *RAIRO Inform. Théor.* **19** (1985), 179–195, www.numdam.org/item/ITA_1985__19_2_179_0/.

[20] N. J. A. Sloane, The on-line encyclopedia of integer sequences (oeis), sequence A156945, http://oeis.org.

[21] J. D. Stasheff, Homotopy associativity of H-spaces. I, II, *Trans. Amer. Math. Soc. 108 (1963), 275-292; ibid.* **108** (1963), 293–312, doi:10.1090/s0002-9947-1963-0158400-5.

[22] D. Tamari, *Monoïdes préordonnés et chaînes de Malcev*, Thèse, Université de Paris, 1951.

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P1.04
https://doi.org/10.26493/2590-9770.1307.cb4
(Also available at http://adam-journal.eu)

Product irregularity strength of graphs with small clique cover number*

Daniil Baldouski
University of Primorska, FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia

Received 19 July 2019, accepted 04 February 2021, published online 21 March 2022

Abstract

For a graph X without isolated vertices and without isolated edges, a *product-irregular labelling* $\omega : E(X) \to \{1, 2, \ldots, s\}$, first defined by Anholcer in 2009, is a labelling of the edges of X such that for any two distinct vertices u and v of X the product of labels of the edges incident with u is different from the product of labels of the edges incident with v. The minimal s for which there exists a product irregular labeling is called *the product irregularity strength* of X and is denoted by $ps(X)$. *Clique cover number* of a graph is the minimum number of cliques that partition its vertex-set. In this paper we prove that connected graphs with clique cover number 2 or 3 have the product-irregularity strength equal to 3, with some small exceptions.

Keywords: Product irregularity strength, clique-cover number.

Math. Subj. Class.: 05C15, 05C70, 05C78

1 Introduction

Throughout this paper let X be a simple graph, that is, a graph without loops or multiple edges, without isolated vertices and without isolated edges. Let $V(X)$ and $E(X)$ denote the vertex set and the edge set of X, respectively. Let $\omega : E(X) \to \{1, 2, \ldots, s\}$ be an integer labelling of the edges of X. Then the *product degree* $pd_X(v)$ of a vertex $v \in V(X)$ in the graph X with respect to the labelling ω is defined by

$$pd_X(v) = \prod_{v \in e} \omega(e).$$

*The author would like to express his gratitude to an anonymous reviewer for carefully reading the manuscript, and for several helpful suggestions that improved the quality of this paper.
E-mail address: d.baldovskiy@mail.ru (Daniil Baldouski)

If the graph X is clear from the context, then we will simply use $pd(v)$. A labelling ω is said to be *product-irregular*, if any two distinct vertices u and v of X have different corresponding product degrees, that is, $pd_X(u) \neq pd_X(v)$ for any u and v in $V(X)$ ($u \neq v$). The *product irregularity strength* $ps(X)$ of X is the smallest positive integer s for which there exists a product-irregular labelling $\omega : E(X) \to \{1, 2, \dots, s\}$.

This concept was first introduced by Anholcer in [1] as a multiplicative version of the well-studied concept of irregularity strength of graphs introduced by Chartrand et al. in [4] and studied later quite extensively (see for example [3, 7, 8, 11]). A concept similar to product-irregular labelling is the *product anti-magic labeling* of a graph, where it is required that the labeling ω is bijective (see [9, 12]). It is clear that every product anti-magic labeling is product-irregular. Another related concept is the so-called *multiplicative vertex-colouring* (see [13, 14]), where it is required that $pd(u) \neq pd(v)$ for every pair of adjacent vertices u and v, while non-adjacent vertices can have the same product degrees. It is easy to see that every product-irregular labelling is a multiplicative vertex-colouring.

In [1] Anholcer gave upper and lower bounds on product irregularity strength of graphs. The main results in [1] are estimates for product irregularity strength of cycles, in particular it was proved that for every $n > 2$

$$ps(C_n) \geq \lceil \sqrt{2n} - \frac{1}{2} \rceil,$$

and that for every $\varepsilon > 0$ there exists n_0 such that for every $n \geq n_0$

$$ps(C_n) \leq \lceil (1 + \varepsilon)\sqrt{2n} \ln n \rceil.$$

Anholcer in [2] considered product irregularity strength of complete bipartite graphs and forests. Anholcer proved that for two integers m and n such that $2 \geq m \geq n$ it holds $ps(K_{m,n}) = 3$ if and only if $n \geq \binom{m+2}{2}$. The main result in [2] is about product irregularity strength of almost all forests F such that $\triangle(F) = D$ for arbitrary integer $D \geq 3$, $n_2 = 0$, $n_0 \leq 0$ and $n_2 = 0$ of the forest F with all pendant edges removed, where n_d denotes the number of vertices of degree d. Anholcer proved that in this case $ps(F) = n_1$.

In [5], Darda and Hujdurović proved that for any graph X of order at least 4 with at most one isolated vertex and without isolated edges we have $ps(X) \leq |V(X)| - 1$. Connections between product irregularity strength of graphs and multidimensional multiplication table problem was established, see [6, 10] for some results on multidimensional multiplication problem.

It is easy to see that the lower bound for the product irregularity strength of any graph is 3. In this paper we will give some sufficient conditions for a graph to have product irregularity strength equal to 3. In particular we will prove that graphs of order at least 3 with clique-cover number 2 have product irregularity strength 3 (see Corollary 3.5), where *clique cover number* of a graph is the minimum number of cliques that partition the vertex set of the graph. Moreover, we will prove that for a connected graph such that its vertex set can be partitioned into 3 cliques of sizes at least 4 then its product irregularity strength is 3 (see Corollary 4.14).

The paper is organized as follows. In section 2 we rephrase the definition of product-irregular labellings in terms of the corresponding weighted adjacency matrices and give some constructions that will be used for proving our main results. In section 3 we will determine the product irregularity strength of graphs with clique cover number 2, while in section 4 we study product irregularity strength of graphs with clique cover number 3.

2 Product-irregular matrices

In this section we will rephrase the definition of product irregular labelling of graphs using weighted adjacency matrices. We start with the definition of a weighted adjacency matrix.

Definition 2.1. Let w be an integer labelling of the edges of a graph X of order n with $V(X) = \{v_1, v_2, \ldots, v_n\}$. Weighted adjacency matrix of X is $n \times n$ matrix M where $M_{ij} = w(\{v_i, v_j\})$ if v_i and v_j are adjacent and $M_{ij} = 0$ otherwise.

Definition 2.2 (Product-irregular matrices and product degree for matrices)**.** Assume that we have weighted adjacency $n \times n$ matrix M $(n \geq 2)$. Then for a k-th row of a matrix M, denoted M_k, define $pd(M_k) := \prod_{M_{k,i} \neq 0} M_{k,i}$ to be the product of all non-zero elements of the k-th row. We say that M is product-irregular if $\forall i, j \in \{1, 2, \ldots, n\}$ for $i \neq j$ $pd(M_i) \neq pd(M_j)$. We will work with matrices with entries $a_{ij} \in \{0, 1, 2, 3\}$ therefore to simplify reading for a row v from matrix M if $pd(v) = 2^a \cdot 3^b$ then we will use notation $pd(v) := (a, b)$. Also define $pd(v)[1] := a$ and $pd(v)[2] := b$.

Observation 2.3. A graph labelling is product-irregular if and only if the corresponding weighted adjacency matrix is product-irregular.

Let $n \geq 4$ and let $M_n(x, y, z)$ be $n \times n$ matrix such that $M_n(x, y, z) = (m_{ij})$ where

$$m_{ij} = \begin{cases} 0, & \text{if } i = j \\ x, & \text{if } j \leq n - i + 1 \text{ and } i \neq j \\ z, & \text{if } (i, j) = (k, n) \text{ or } (i, j) = (n, k) \text{ for } k = \lceil \frac{n}{2} \rceil + 1 \\ y, & \text{otherwise} \end{cases}$$

For example:

$$M_7(x, y, z) = \begin{pmatrix} 0 & x & x & x & x & x & x \\ x & 0 & x & x & x & x & y \\ x & x & 0 & x & x & y & y \\ x & x & x & 0 & y & y & y \\ x & x & x & y & 0 & y & z \\ x & x & y & y & y & 0 & y \\ x & y & y & y & z & y & 0 \end{pmatrix}. \tag{2.1}$$

We will denote with $A \oplus B$ the direct sum of matrices A and B, that is

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

where 0 denotes the zero matrix of appropriate size.

2.1 Properties of M_n

Let x_i, y_i and z_i be the number of x, y and z respectively appearing in the i-th row of matrix $M_n(x, y, z)$. For fixed n with k we denote $k := \lceil \frac{n}{2} \rceil + 1$. Then the rows of the matrix $M_n(x, y, z)$ can be separated into 3 types:

1st type: $(x_k, y_k, z_k) = (\lceil \frac{n-1}{2} \rceil, \lceil \frac{n}{2} \rceil - 2, 1)$, 2nd type: $(x_i, y_i, z_i) = (n-i, i-1, 0)$ for $i < k$ and $(x_i, y_i, z_i) = (n-i+1, i-2, 0)$ for $n > i > k$,

3rd type: $(x_n, y_n, z_n) = (1, n-3, 1)$.

We denote by $m_{(i)}(M)$ a row of type i for $i \in \{1,2,3\}$ of matrix M, where M is matrix $M_n(x,y,z)$ (if the matrix $M_n(x,y,z)$ is clear from the context, then we will simply use $m_{(i)}$). We start by proving the following nice property of matrix M_n.

Proposition 2.4. *If $\{x,y,z\}$ is a set of distinct pairwise relatively prime integers, then $M_n(x,y,z)$ is product irregular matrix for any $n \geq 4$.*

Proof. Suppose contrary, that is there exist m_i and m_j (that are rows of matrix $M_n(x,y,z)$) for some $i \neq j$ such that $pd(m_i) = pd(m_j)$. There are 3 types of rows therefore it is enough to check the equality above not for all rows, but for all types of rows. Observe that for every $i \in \{1,2,\ldots,n\}$ the sum $x_i + y_i + z_i = n-1$ and $pd(m_i) = pd(m_j)$ for some $i \neq j$ if and only if $x_i = x_j$, $y_i = y_j$ and $z_i = z_j$. It follows that:

1. If $pd(m_{(1)}) = pd(m_{(3)})$ then $(\lceil \frac{n-1}{2} \rceil, \lceil \frac{n}{2} \rceil - 2, 1) = (1, n-3, 1)$, so $n = 3$ which is a contradiction.
2. Since rows of second type have value 0 at 3rd coordinate and rows of first and third types have value 1 at 3rd coordinate, then $pd(m_{(2)}) \neq pd(m_{(i)})$ for $i \in \{1,3\}$.
3. It is clear that $(x_i, y_i, z_i) \neq (x_j, y_j, z_j)$ for $i < k$ and $k < j < n$ i.e. product degrees of different rows of type 2 are different.

We were considering different rows, that means we did not have to consider $pd(m_{(i)}) = pd(m_{(i)})$ for every $i \in \{1,3\}$. □

We will define 3 matrices of class $M_n(x,y,z)$ for specific x, y and z. Assign matrix $A_n := M_n(1,2,3)$, $B_n := M_n(2,3,1)$ and $C_n := M_n(3,1,2)$.

2.2 Properties of $A_n \oplus B_m$

Lemma 2.5. *For every $m \geq n \geq 4$, $A_n \oplus B_m$ is product irregular if $(n,m) \notin \{(4,4),(5,5),(6,6)\}$.*

Proof. Suppose contrary, that is there exist a_i and b_j (that are rows of matrices A_n and B_m respectively) for some i and j such that $pd(a_i) = pd(b_j)$. There are 3 types of rows therefore it is enough to check all of the 9 possibilities for different types of rows:

1. If $pd(a_{(1)}) = pd(b_{(1)})$ then $(\lceil \frac{n}{2} \rceil - 2, 1) = (\lceil \frac{m-1}{2} \rceil, \lceil \frac{m}{2} \rceil - 2)$ which contradicts with $m \geq n$.
2. If $pd(a_{(1)}) = pd(b_{(2)})$ then $(\lceil \frac{n}{2} \rceil - 2, 1) = (m-j, j-1)$ or $(\lceil \frac{n}{2} \rceil - 2, 1) = (m-j+1, j-2)$ which contradicts with $m \geq n \geq 4$.
3. If $pd(a_{(1)}) = pd(b_{(3)})$ then $(\lceil \frac{n}{2} \rceil - 2, 1) = (1, m-3)$, so $(n,m) = (5,4)$ or $(n,m) = (6,4)$ which contradicts with $m \geq n$.
4. If $pd(a_{(2)}) = pd(b_{(1)})$ then $(i-1, 0) = (\lceil \frac{m-1}{2} \rceil, \lceil \frac{m}{2} \rceil - 2)$ or $(i-2, 0) = (\lceil \frac{m-1}{2} \rceil, \lceil \frac{m}{2} \rceil - 2)$, so $m = 3$ or $m = 4$, thus $m = n = 4$ which is a contradiction.

5. If $pd(a_{(2)}) = pd(b_{(2)})$ then we have that in both possible cases $((i-1, 0 = (m - j, j-1))$ and $(i-2, 0) = (m-j+1, j-2))$ we get $i = m \geq n$ which is a contradiction.
6. If $pd(a_{(2)}) = pd(b_{(3)})$ then $pd(a_{(2)})[2] = 0$ and $pd(b_{(3)})[2] > 0$ which is a contradiction.
7. If $pd(a_{(3)}) = pd(b_{(1)})$ then $(n-3, 1) = (\lceil \frac{m-1}{2} \rceil, \lceil \frac{m}{2} \rceil - 2)$, so $(n, m) = (5, 5)$ or $(n, m) = (6, 6)$ which is a contradiction.
8. If $pd(a_{(3)}) = pd(b_{(2)})$ then $(n-3, 1) = (m-j, j-1)$ or $(n-3, 1) = (m-j+1, j-2)$, so $n > m$ in both cases which is a contradiction.
9. If $pd(a_{(3)}) = pd(b_{(3)})$ then $(n-3, 1) = (1, m-3)$, so $(n, m) = (4, 4)$ which is a contradiction.

This finishes the proof. □

For the next lemma we need to consider weighted adjacency matrix

$$T := \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 3 \\ 2 & 3 & 0 \end{pmatrix} \tag{2.2}$$

Observe that $pd(T_1) = (1, 0)$, $pd(T_2) = (0, 1)$, $pd(T_3) = (1, 1) \Rightarrow ps(K_3) = 3$.

Lemma 2.6. *Let T be the matrix defined in (2.2). For every $n \geq 5$ $T \oplus B_n$ is product irregular.*

Proof. Observe that $\{pd(T_i) : i \in \{1, 2, 3\}\} \subset \{pd((A_4)_i) : i \in \{1, 2, 3, 4\}\}$ and we know from Lemma 2.5 that $\forall n \geq 5$ $A_4 \oplus B_n$ is product irregular. □

3 Graphs with clique-cover number 2

In this section we consider product irregularity strength of connected graphs with clique cover number two. Suppose that G is a graph with clique-cover number 2, that is the vertex set of G can be partitioned into two cliques C_1 and C_2, of sizes n and m respectively. Then it follows that G has a spanning subgraph isomorphic to $K_n + K_m$, where for two graphs H_1 and H_2, $H_1 + H_2$ denotes the disjoint union of H_1 and H_2. Then by [5, Lemma 1] it follows that $3 \leq ps(G) \leq ps(K_n + K_m)$. Hence we will start by considering product irregularity strength of $K_n + K_m$.

It can be proved that any 4×4 weighted adjacency matrix M (with weights $1, 2$ and 3) is product irregular if and only if there exist row $m \in M$ such that $pd(m) = (1, 1)$. Therefore $ps(K_4 + K_4) > 3$. There are a lot of graphs of the form $K_n + K_m$ for some integers n and m with product irregularity strength greater than 3. But since such graphs are disconnected, we will define operation of adding an edge between components of these graphs, i.e. we will consider minimal connected graphs with clique cover number 2.

Definition 3.1 ($+edge$)**.** Let G_1 and G_2 be two graphs with disjoint vertex sets. With $G_1 + G_2 + edge$ we denote a graph obtained by taking disjoint union of G_1 and G_2 and adding an edge between two vertices of G_1 and G_2.

Lemma 3.2. $\forall n \geq 4$, $ps(K_2 + K_n + edge) = 3$.

Proof. Consider weighted adjacency $(n+2)\times(n+2)$ matrix

$$L = \begin{pmatrix} 0 & 1 & 3 & 0 & \cdots & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 \\ 3 & 0 & & & & \\ \vdots & \vdots & & & & \\ 0 & 0 & & B_n & & \\ \vdots & \vdots & & & & \\ 0 & 0 & & & & \end{pmatrix} \tag{3.1}$$

where $L_{1,3} = L_{3,1} = 3$. Clearly, L is weighted adjacency matrix of the graph $K_2 + K_n$. We will show that L is product-irregular. Since we have that $pd((B_n)_i) = pd(L_{i+2})$ for every $i \in \{2, 3, \dots n\}$ it is enough to show that product degrees of first 3 rows of matrix L are different and do not belong to the set $\{pd((B_n)_i), i \in \{2, 3, \dots, n\}\}$.

1. It is clear that those rows are different and that first two rows of L are not in the set $\{pd((B_n)_i), i \in \{2, 3, \dots, n\}\}$.
2. For the row L_3 we have that $pd(L_3) = pd((B_n)_1) + (0, 1) = (n-1, 1)$. Therefore $pd(L_3)[1] + pd(L_3)[2] = n - 1 + 1 > n - 1 \geq pd((B_n)_j)[1] + pd((B_n)_j)[2]$ for any $j \in \{2, 3, \dots, n\}$.

This finishes the proof. □

Corollary 3.3. *For every $n \geq 4$, $ps(K_1 + K_n + edge) = 3$.*

Proof. Consider matrix L' obtained from matrix L from (3.1) by deleting second row and column. Clearly, L' is product-irregular. □

Theorem 3.4. *For every positive integers n and m such that $n + m > 2$ we have $ps(K_n + K_m + edge) = 3$.*

Proof. Consider some cases that were not covered by previous Lemmas:

(i) $ps(K_5 + K_5) = 3$. For proving this fact we can take direct sum of the following weighted adjacency matrices:

$$T_5 := \begin{pmatrix} 0 & 3 & 1 & 1 & 1 \\ 3 & 0 & 1 & 3 & 2 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 3 & 1 & 0 & 2 \\ 1 & 2 & 1 & 2 & 0 \end{pmatrix} \text{ and } \tilde{T_5} := \begin{pmatrix} 0 & 2 & 2 & 2 & 1 \\ 2 & 0 & 3 & 3 & 3 \\ 2 & 3 & 0 & 2 & 3 \\ 2 & 3 & 2 & 0 & 1 \\ 1 & 3 & 3 & 1 & 0 \end{pmatrix} \tag{3.2}$$

(ii) $ps(K_6 + K_6) = 3$. For proving this fact we can take direct sum of the following weighted adjacency matrices:

$$T_6 := \begin{pmatrix} 0 & 1 & 2 & 3 & 1 & 3 \\ 1 & 0 & 1 & 3 & 1 & 1 \\ 2 & 1 & 0 & 1 & 2 & 2 \\ 3 & 3 & 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 1 & 0 & 1 \\ 3 & 1 & 2 & 1 & 1 & 0 \end{pmatrix} \text{ and } \tilde{T_6} := \begin{pmatrix} 0 & 1 & 2 & 3 & 3 & 3 \\ 1 & 0 & 2 & 3 & 3 & 2 \\ 2 & 2 & 0 & 2 & 1 & 2 \\ 3 & 3 & 2 & 0 & 3 & 1 \\ 3 & 3 & 1 & 3 & 0 & 3 \\ 3 & 2 & 2 & 1 & 3 & 0 \end{pmatrix} \tag{3.3}$$

Also consider some cases that could not be proved without adding edges between cliques.

(iii) $ps(K_4 + K_4 + edge) = 3$. For proving this fact we will consider the following product-irregular matrix:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 3 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 2 & 3 \\ 0 & 0 & 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 3 & 1 & 0 \end{pmatrix} \tag{3.4}$$

(iv) $ps(K_3 + K_4 + edge) = 3$. For proving this fact we will consider the following product-irregular matrix:

$$\begin{pmatrix} 0 & 1 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 \\ 2 & 3 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 2 & 0 & 2 & 3 \\ 0 & 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 3 & 1 & 0 \end{pmatrix} \tag{3.5}$$

Observe that this matrix is obtained from matrix (3.4) by deleting first row and column.

(v) $ps(K_3 + K_3 + edge) = 3$. For proving this fact we will consider the following product-irregular matrix:

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 3 & 2 & 3 & 0 \end{pmatrix} \tag{3.6}$$

(vi) $ps(K_2 + K_3 + edge) = 3$. For proving this fact we will consider the following product-irregular matrix:

$$\begin{pmatrix} 0 & 3 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 0 & 3 \\ 0 & 3 & 2 & 3 & 0 \end{pmatrix} \tag{3.7}$$

Observe that this matrix is obtained from matrix (3.6) by deleting first row and column.

(vii) $ps(K_1 + K_3 + edge) = 3$. For proving this fact we will consider the following product-irregular matrix:

$$\begin{pmatrix} 0 & 0 & 0 & 3 \\ 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 3 \\ 3 & 2 & 3 & 0 \end{pmatrix} \tag{3.8}$$

Observe that this matrix is obtained from matrix (3.7) by deleting first row and column.

We are left with some trivial cases and it is straihtforward to check that $ps(K_2 + K_2 + edge) = ps(P_4) = 3$ and $ps(K_1 + K_2 + edge) = ps(P_3) = 3$.

The proof now follows by Lemmas 2.5, 2.6 and 3.2 and Corollary 3.3. □

Corollary 3.5. *If G is a connected graph of order at least 3 with clique-cover number 2 then $ps(G) = 3$.*

Observe that $K_1 + K_1 + edge = P_2$ is an isolated edge, for which product-irregular labelling is not defined, i.e. 2 is the lower bound of the sum $n + m$ in Theorem 3.4.

4 Graphs with clique-cover number 3

In this section we consider the product irregularity strength of graphs with clique-cover number 3. Observe that a graph G has clique cover number 3, if and only if its complement has chromatic number equal to 3. If G is a graph with clique cover number 3, then its vertex set can be partitioned into three cliques, of sizes n, m and l. Then it follows that G has a spanning subgraph isomorphic to $K_n + K_m + K_l$, hence we will first investigate the product irregularity strength of such graphs.

4.1 Properties of $A_n \oplus B_m \oplus C_l$

Lemma 4.1. *For every $n \geq 7$ and $m \geq 4$, $A_n \oplus C_m$ is product irregular.*

Proof. Suppose contrary, that is $\exists a_i$ and c_j (that are rows of matrices A_n and C_m respectively) for some i and j such that $pd(a_i) = pd(c_j)$. We will use the same type of proof as in the Lemma 2.5.

1. If $pd(a_{(1)}) = pd(c_{(1)})$ then $(\lceil \frac{n}{2} \rceil - 2, 1) = (1, \lceil \frac{m-1}{2} \rceil)$, so $n = 5$ or $n = 6$ and $m = 2$ or $m = 3$ which is a contradiction.
2. If $pd(a_{(1)}) = pd(c_{(2)})$ then $(\lceil \frac{n}{2} \rceil - 2, 1) = (0, m-j)$ or $(\lceil \frac{n}{2} \rceil - 2, 1) = (0, m-j+1)$. In both cases $n = 3$ or $n = 4$ which is a contradiction.
3. If $pd(a_{(1)}) = pd(c_{(3)})$ then $(\lceil \frac{n}{2} \rceil - 2, 1) = (1, 1)$, so $n = 5$ or $n = 6$ which is a contradiction.
4. If $pd(a_{(2)}) = pd(c_{(1)})$ then $(i - 1, 0) = (1, \lceil \frac{m-1}{2} \rceil)$ or $(i - 2, 0) = (1, \lceil \frac{m-1}{2} \rceil)$. In both cases $m = 1$ which is a contradiction.
5. For $pd(a_{(2)}) = pd(c_{(2)})$ we have that $pd(a_{(2)})[2] = 0$ and $pd(c_{(2)})[2] > 0$ which is a contradiction.
6. If $pd(a_{(2)}) = pd(c_{(3)})$ then $(i - 1, 0) = (1, 1)$ or $(i - 2, 0) = (1, 1))$ which is, clearly, a contradiction.

7. If $pd(a_{(3)}) = pd(c_{(1)})$ then $(n-3, 1) = (1, \lceil \frac{m-1}{2} \rceil)$, so $n = 4$ which is a contradiction.
8. If $pd(a_{(3)}) = pd(c_{(2)})$ then $(n-3, 1) = (0, m-j)$ or $(n-3, 1) = (0, m-j+1)$, so $n = 3$ which is a contradiction.
9. If $pd(a_{(3)}) = pd(c_{(3)})$ then $(n-3, 1) = (1, 1)$, so $n = 4$ which is a contradiction.

This finishes the proof. □

Lemma 4.2. *For every $n \geq m \geq 5$, $B_n \oplus C_m$ is product irregular if $(n, m) \notin \{(5, 5), (6, 6)\}$.*

Proof. Suppose contrary, that is there exist b_i and c_j (that are rows of matrices B_n and C_m respectively) for some i and j such that $pd(b_i) = pd(c_j)$. We will use the same type of proof as in the Lemma 2.5.

1. If $pd(b_{(1)}) = pd(c_{(1)})$ then $(\lceil \frac{n-1}{2} \rceil, \lceil \frac{n}{2} \rceil - 2) = (1, \lceil \frac{m-1}{2} \rceil)$, so $n = 2$ or $n = 3$ which is a contradiction.
2. If $pd(b_{(1)}) = pd(c_{(2)})$ then $(\lceil \frac{n-1}{2} \rceil, \lceil \frac{n}{2} \rceil - 2) = (0, m-j)$ or $(\lceil \frac{n-1}{2} \rceil, \lceil \frac{n}{2} \rceil - 2) = (0, m-j+1)$, so $n = 1$, a contradiction.
3. If $pd(b_{(1)}) = pd(c_{(3)})$ then $(\lceil \frac{n-1}{2} \rceil, \lceil \frac{n}{2} \rceil - 2) = (1, 1)$, so $n = 2$ or $n = 3$, a contradiction.
4. If $pd(b_{(2)}) = pd(c_{(1)})$ then $(n-i, i-1) = (1, \lceil \frac{m-1}{2} \rceil)$ or $(n-i+1, i-2) = (1, \lceil \frac{m-1}{2} \rceil)$. In the first case we have that $\lceil \frac{m-1}{2} \rceil = i - 1 = n - 2$, which implies that $2n - 4 \leq m \leq 2n - 3$, so, in particular, $2n - 4 \leq m \leq n$, therefore $n \leq 4$, a contradiction. In the second case we have that $n = i$ which is a contradiction.
5. For $pd(b_{(2)}) = pd(c_{(2)})$ we have that $pd(b_{(2)})[1] > 0$ and $pd(c_{(2)})[1] = 0$ which is a contradiction.
6. If $pd(b_{(2)}) = pd(c_{(3)})$ then $(n-i, i-1) = (1, 1)$ or $(n-i+1, i-2) = (1, 1)$, so $n = 3$ which is a contradiction.
7. If $pd(b_{(3)}) = pd(c_{(1)})$ then $(1, n-3) = (1, \lceil \frac{m-1}{2} \rceil)$, so $m = 2(n-3)$ or $m = 2(n-3)+1$ which is a contradiction because for $n \geq 7$ we have that $m > n$ and for $5 \leq n < 7$ we have that $(n, m) \in \{(5, 5), (6, 6)\}$.
8. If $pd(b_{(3)}) = pd(c_{(2)})$ then $(1, n-3) = (0, m-j)$ or $(1, n-3) = (0, m-j+1)$ which is a contradiction.
9. If $pd(b_{(3)}) = pd(c_{(3)})$ then $(1, n-3) = (1, 1)$, so $n = 4$ which is a contradiction.

This finishes the proof. □

Theorem 4.3. *For every n, m and l such that $m \geq l \geq n \geq 7$ $A_n \oplus B_m \oplus C_l$ is product irregular.*

Proof. Proof follows by Lemmas 2.5, 4.1 and 4.2. □

Corollary 4.4. *For all positive integers n, m and l greater than or equal to 7 it holds that $ps(K_n + K_m + K_l) = 3$.*

Lemma 4.5. *For all positive integers n and m greater than 6 and $k \in \{4, 5, 6\}$, $ps(K_n + K_m + K_k) = 3$.*

Proof. Let $m \geq n$ and consider matrix $A_n \oplus B_m \oplus C_k$. From Lemmas 2.5, 4.1 and 4.2 we can conclude that this matrix is product-irregular. □

Lemma 4.6. *For all positive integer $n \geq 7$ $ps(K_6 + K_6 + K_n) = 3$.*

Proof. Consider $T_6 \oplus \tilde{T_6} \oplus B_n$ which is product-irregular because for every row b of matrix B_n $pd(b)[1] + pd(b)[2] \geq 5$, while for every row t of matrices T_6 and $\tilde{T_6}$ we have that $pd(t)[1] + pd(t)[2] \leq 4$. □

Lemma 4.7. *For all positive integer $n \geq 7$ $ps(K_5 + K_6 + K_n) = 3$.*

Proof. Consider the following matrix:

$$M := \begin{pmatrix} 0 & 2 & 2 & 2 & 1 & 1 \\ 2 & 0 & 3 & 3 & 3 & 1 \\ 2 & 3 & 0 & 2 & 3 & 1 \\ 2 & 3 & 2 & 0 & 1 & 2 \\ 1 & 3 & 3 & 1 & 0 & 1 \\ 1 & 1 & 1 & 2 & 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 3 & 1 & 1 & 1 \\ 3 & 0 & 1 & 3 & 2 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 3 & 1 & 0 & 2 \\ 1 & 2 & 1 & 2 & 0 \end{pmatrix} \oplus B_n \tag{4.1}$$

M is product-irregular because for every row b of matrix B_n $pd(b)[1]+pd(b)[2] \geq 5$, while for every row v of first two blocks of our matrix M we have that $pd(v)[1] + pd(v)[2] \leq 4$. □

Lemma 4.8. *For all positive integers $n \geq 6$, $ps(K_5 + K_5 + K_n) = 3$.*

Proof. Consider weighted adjacency matrices T_5 and $\tilde{T_5}$ from (3.2) in the first item of the proof of Theorem 3.4:

1. $\forall n \geq 7$ we have $T_5 \oplus \tilde{T_5} \oplus B_n$ is product irregular because for every row b of matrix B_n $pd(b)[1] + pd(b)[2] \geq 5$.
2. For $n = 6$ we have that $T_5 \oplus \tilde{T_5} \oplus P_6$ is product-irregular, where

$$P_6 := \begin{pmatrix} 0 & 2 & 2 & 2 & 2 & 1 \\ 2 & 0 & 2 & 2 & 2 & 3 \\ 2 & 2 & 0 & 2 & 3 & 3 \\ 2 & 2 & 2 & 0 & 3 & 1 \\ 2 & 2 & 3 & 3 & 0 & 3 \\ 1 & 3 & 3 & 1 & 3 & 0 \end{pmatrix}. \tag{4.2}$$

This finishes the proof. □

Consider the graph $K_4 + K_4 + K_4$. Suppose that $ps(K_4 + K_4 + K_4) = 3$. Then there exist a product-irregular adjacency matrix K of the form $K = P_1 \oplus P_2 \oplus P_3$ of our graph $K_4 + K_4 + K_4$, where P_i is a product-irregular adjacency matrix of a graph K_4 for every $i \in \{1, 2, 3\}$. Therefore, we have that for every row v of matrix K $pd(v)[1]+pd(v)[2] < 4$. Also, it is clear that for every row v of matrix K we have $pd(v)[1] < 4$ and $pd(v)[2] < 4$. But there exist only 10 different pairs of the form (x, y) such that $0 \leq x, y < 4$ and $x+y < 4$, which implies that there exist two rows v and u of matrix K such that $pd(v) = pd(u)$. Therefore, $ps(K_4 + K_4 + K_4) > 3$.

There are a lot of graphs of the form $K_n + K_m + K_k$ for some integers n, m and k with product irregularity strength greater than 3. But since such graphs are disconnected, we will define operation of adding 2 edges between components of these graphs such that the resulting graph will be connected, i.e. we will consider minimal connected graphs with clique cover number 3.

Definition 4.9 ($+2edges$)**.** Let $+2edges$ for graphs $G_1 + G_2 + G_3$ be the operation of adding edges, i.e. applying two times $+edge$ between any 2 different pairs of different sets $V(G_1), V(G_2)$ and $V(G_3)$. We will use the following notation for that operation: $G_1 + G_2 + G_3 + 2edges$.

Now we will describe this operation using matrix language. Consider weighted adjacency matrices A, B, C of sizes $n \times n$, $m \times m$ and $l \times l$ respectively. Let $T_{12}(A, B, C, i, j, w)$ be $(n+m+l) \times (n+m+l)$ matrix with all zeros except elements with coordinates $(i, n+j)$ and $(n+j, i)$ of value w, where $1 \le i \le n$ and $1 \le j \le m$. In a similar way we can define matrices $T_{13}(A, B, C, i, j, w)$ and $T_{23}(A, B, C, i, j, w)$ for which coordinates of non-zero elements are $(i, n + m + j)$ and $(n + m + j, i)$, where $1 \le i \le n$ and $1 \le j \le l$ and $(n + i, n + m + j)$ and $(n + m + j, n + i)$, where $1 \le i \le m$ and $1 \le j \le l$ respectively.

For example one of the weighted adjacency matrices for graph $K_n + K_m + K_l + 2edges$ where the edges between cliques are between vertices a_i and b_j of weight w_1 and between vertices b_j and c_k of weight w_2 where $a_i \in V(K_n), b_j \in V(K_m)$ and $c_k \in V(K_l)$ is $A_n \oplus B_m \oplus C_l + T_{12}(A_n, B_m, C_l, i, j, w_1) + T_{23}(A_n, B_m, C_l, j, k, w_2)$.

Definition 4.10 (In-degree and in-edges)**.** Consider graph $G := G_1 + G_2 + G_3 + 2edges$. Let $G' := G_1 + G_2 + G_3$ be a subgraph of the graph G. Let $g \in V(G)$ and let $d_{G'}(g)$ be the degree of the vertex $g \in V(G')$. Then define *in-degree* of vertex $g \in V(G)$ to be $d^+(g) := d(g) - d_{G'}(g)$. We say that for some $i \in \{1, 2, 3\}$ G_i has t *in-edges* if and only if

$$\sum_{g \in V(G_i)} d^+(g) = t.$$

For the next theorem we will define the following matrix. Let $\tilde{M}_n(x, y) := M_n(x, y, y)$ and matrices $\tilde{A}_n, \tilde{B}_n$ and $\tilde{C}_n$ to be $\tilde{M}_n(1, 2), \tilde{M}_n(2, 3)$ and $\tilde{M}_n(3, 1)$ respectively.

Theorem 4.11. *For all positive integers n, m and l that are greater than or equal to* 5 *we have that* $ps(K_n + K_m + K_l + 2edges) = 3$.

Proof. Consider some cases that were not covered by previous Lemmas:

1. For $(n, m, l) = (6, 6, 6)$ consider the following product-irregular matrix:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 3 & 1 & 1 & 2 \\ 1 & 3 & 0 & 1 & 2 & 2 \\ 1 & 1 & 1 & 0 & 2 & 2 \\ 1 & 1 & 2 & 2 & 0 & 2 \\ 1 & 2 & 2 & 2 & 2 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 1 & 2 & 2 & 3 \\ 2 & 1 & 0 & 2 & 3 & 3 \\ 2 & 2 & 2 & 0 & 3 & 3 \\ 2 & 2 & 3 & 3 & 0 & 3 \\ 2 & 3 & 3 & 3 & 3 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 3 & 3 & 3 & 3 & 3 \\ 3 & 0 & 2 & 3 & 3 & 1 \\ 3 & 2 & 0 & 3 & 1 & 1 \\ 3 & 3 & 3 & 0 & 1 & 1 \\ 3 & 3 & 1 & 1 & 0 & 1 \\ 3 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \tag{4.3}$$

2. For $(n, m, l) = (5, 6, 6)$ we can consider the same matrix as in (4.3) without first row (and column), i.e. without row (and column) v such that $pd(v) = (0, 0)$.

3. For $(n, m, l) = (5, 5, 5)$ we will consider $\tilde{A}_5 \oplus \tilde{B}_5 \oplus \tilde{C}_5 + 2edges$. Let $\tilde{B}_5$ to have 2 in-edges, then we have:

   (1) If $\tilde{B}_5$ has 2 in-edges from one vertex, then we can take weighted adjacency matrix $\tilde{A}_5 \oplus \tilde{B}_5 \oplus \tilde{C}_5 + T_{12}(\tilde{A}_5, \tilde{B}_5, \tilde{C}_5, 3, 3, 3) + T_{23}(\tilde{A}_5, \tilde{B}_5, \tilde{C}_5, 3, 3, 2)$ which is product-irregular.

   (2) If $\tilde{B}_5$ has 2 in-edges from different vertices then we can take weighted adjacency matrix $\tilde{A}_5 \oplus \tilde{B}_5 \oplus \tilde{C}_5 + T_{12}(\tilde{A}_5, \tilde{B}_5, \tilde{C}_5, 3, 3, 3) + T_{23}(\tilde{A}_5, \tilde{B}_5, \tilde{C}_5, 1, 3, 2)$ which is product-irregular.

The proof now follows by the above argumentation, together with Theorem 4.3 and Lemmas 4.5, 4.6, 4.7 and 4.8. □

Lemma 4.12. *For all positive integers $n \geq 7$ and $m \in \{5, 6\}$ we have that $ps(K_4 + K_n + K_m) = 3$.*

Proof. Consider three different cases for different m:

1. For $m = 6$ and $n \geq 8$ consider matrix $A_4 \oplus B_6 \oplus B_n$ which is product-irregular using Theorem 3.4.
2. For $m = 6$ and $n = 7$ consider matrix $A_4 \oplus B_7 \oplus \tilde{T}_6$ which is product-irregular (where $\tilde{T}_6$ is defined in (3.3)).
3. For $m = 5$ consider matrix $A_4 \oplus B_n \oplus \tilde{T}_5$ which is product-irregular (where $\tilde{T}_5$ is defined in (3.2)). □

Theorem 4.13. *For all positive integers n, m and l that are greater than or equal to 4 we have that $ps(K_n + K_m + K_l + 2edges) = 3$.*

Proof. Consider some cases that were not covered by previous Lemmas and Theorems:

1. For $(n, m, l) = (4, 5, 6)$ consider the following product-irregular matrix:

$$A_4 \oplus \begin{pmatrix} 0 & 2 & 2 & 2 & 1 \\ 2 & 0 & 3 & 1 & 3 \\ 2 & 3 & 0 & 2 & 3 \\ 2 & 1 & 2 & 0 & 1 \\ 1 & 3 & 3 & 1 & 0 \end{pmatrix} \oplus B_6 \tag{4.4}$$

   Notice that the second block of this matrix is obtained from $\tilde{T}_5$ from (3.2) by changing the values t_{24} and t_{42} from 3 to 1.

2. For $(n, m, l) = (4, 6, 6)$ consider the matrix $C_4 + A_6 + \tilde{T}_6$ which is product-irregular (where $\tilde{T}_6$ is defined in (3.3)).

Consider some cases for which we will add some edges between cliques:

3. For $(n, m, l) = (4, 5, 5)$ we will consider $\tilde{A}_4 \oplus \tilde{B}_5 \oplus \tilde{C}_5 + 2edges$.

   ($\tilde{B}_5$) For the case when $d^+(\tilde{B}_5) = 2$ we have two options:

   (1) If $\tilde{B}_5$ has 2 in-edges from one vertex, then we can take weighted adjacency matrix $\tilde{A}_4 \oplus \tilde{B}_5 \oplus \tilde{C}_5 + T_{12}(\tilde{A}_4, \tilde{B}_5, \tilde{C}_5, 2, 3, 3) + T_{23}(\tilde{A}_4, \tilde{B}_5, \tilde{C}_5, 3, 3, 2)$ which is product-irregular.

(2) If $\tilde{B}_5$ has 2 in-edges from different vertices then we can take weighted adjacency matrix $\tilde{A}_5 \oplus \tilde{B}_5 \oplus \tilde{C}_5 + T_{12}(\tilde{A}_4, \tilde{B}_5, \tilde{C}_5, 3, 3, 3) + T_{23}(\tilde{A}_4, \tilde{B}_5, \tilde{C}_5, 1, 3, 2)$ which is product-irregular.

($\tilde{A}_4$) For the case when $d^+(\tilde{A}_4) = 2$ we have two options:

(1) If $\tilde{A}_4$ has 2 in-edges from one vertex then we can take weighted adjacency matrix $\tilde{A}_4 \oplus \tilde{B}_5 \oplus \tilde{C}_5 + T_{12}(\tilde{A}_4, \tilde{B}_5, \tilde{C}_5, 2, 3, 2) + T_{13}(\tilde{A}_4, \tilde{B}_5, \tilde{C}_5, 2, 3, 2)$ which is product-irregular.

(2) If $\tilde{A}_4$ has 2 in-edges from different vertices then we can take weighted adjacency matrix $\tilde{A}_4 \oplus \tilde{B}_5 \oplus \tilde{C}_5 + T_{12}(\tilde{A}_4, \tilde{B}_5, \tilde{C}_5, 2, 3, 2) + T_{13}(\tilde{A}_4, \tilde{B}_5, \tilde{C}_5, 4, 3, 2)$ which is product-irregular.

4. For $(n, m) = (4, 4)$ and $l \geq 5$ we will consider $\tilde{A}_4 \oplus \tilde{B}_l \oplus \tilde{C}_4 + 2edges$.

($\tilde{B}_l$) For the case when $d^+(\tilde{B}_l) = 2$ we have two options:

(1) If $\tilde{B}_l$ has 2 in-edges from one vertex then we can take weighted adjacency matrix $\tilde{A}_4 \oplus \tilde{B}_l \oplus \tilde{C}_4 + T_{12}(\tilde{A}_4, \tilde{B}_l, \tilde{C}_4, 2, 3, 3) + T_{23}(\tilde{A}_4, \tilde{B}_l, \tilde{C}_4, 3, 2, 2)$ which is product-irregular.

(2) If $\tilde{B}_l$ has 2 in-edges from different vertices then we can take weighted adjacency matrix $\tilde{A}_4 \oplus \tilde{B}_l \oplus \tilde{C}_4 + T_{12}(\tilde{A}_4, \tilde{B}_l, \tilde{C}_4, 2, 3, 3) + T_{23}(\tilde{A}_4, \tilde{B}_l, \tilde{C}_4, 1, 2, 2)$ which is product-irregular.

($\tilde{C}_4$) For the case when $d^+(\tilde{C}_4) = 2$ we have two options:

(1) If $\tilde{C}_4$ has 2 in-edges from one vertex then we can take weighted adjacency matrix $\tilde{A}_4 \oplus \tilde{B}_l \oplus \tilde{C}_4 + T_{13}(\tilde{A}_4, \tilde{B}_l, \tilde{C}_4, 2, 2, 3) + T_{23}(\tilde{A}_4, \tilde{B}_l, \tilde{C}_4, 3, 2, 3)$ which is product-irregular.

(2) If $\tilde{C}_4$ has 2 in-edges from different vertices then we can take weighted adjacency matrix $\tilde{A}_4 \oplus \tilde{B}_l \oplus \tilde{C}_4 + T_{13}(\tilde{A}_4, \tilde{B}_l, \tilde{C}_4, 2, 2, 3) + T_{23}(\tilde{A}_4, \tilde{B}_l, \tilde{C}_4, 3, 1, 3)$ which is product-irregular.

5. For $(n, m, l) = (4, 4, 4)$ we will consider $\tilde{A}_4 \oplus \tilde{B}_4 \oplus \tilde{C}_4 + 2edges$. Let $\tilde{C}_4$ to have 2 in-edges.

(1) If $\tilde{C}_4$ has 2 in-edges from one vertex then we can take weighted adjacency matrix $\tilde{A}_4 \oplus \tilde{B}_4 \oplus \tilde{C}_4 + T_{13}(\tilde{A}_4, \tilde{B}_4, \tilde{C}_4, 2, 2, 3) + T_{23}(\tilde{A}_4, \tilde{B}_4, \tilde{C}_4, 3, 2, 3)$ which is product-irregular.

(2) If $\tilde{C}_4$ has 2 in-edges from different vertices then we can take weighted adjacency matrix $\tilde{A}_4 \oplus \tilde{B}_4 \oplus \tilde{C}_4 + T_{13}(\tilde{A}_4, \tilde{B}_4, \tilde{C}_4, 2, 2, 3) + T_{23}(\tilde{A}_4, \tilde{B}_4, \tilde{C}_4, 3, 1, 3)$ which is product-irregular.

The proof now follows by the above argumentation, together with Theorem 4.11 and Lemma 4.12. □

Corollary 4.14. *If G is a connected graph such that its vertex set can be partitioned into 3 cliques of sizes at least 4 then $ps(G) = 3$.*

We would like to conclude the paper with proposing the following problem for possible further research.

Problem 4.15. Are there only finitely many connected graphs with clique cover number 4 and product irregularity strength more than 3?

ORCID iDs

Daniil Baldouski https://orcid.org/0000-0001-5350-9343

References

[1] M. Anholcer, Product irregularity strength of graphs, *Discrete Math.* **309** (2009), 6434–6439, doi:10.1016/j.disc.2008.10.014.

[2] M. Anholcer, Product irregularity strength of certain graphs, *Ars Math. Contemp.* **7** (2014), 23–29, doi:10.26493/1855-3974.258.2a0.

[3] T. Bohman and D. Kravitz, On the irregularity strength of trees, *J. Graph Theory* **45** (2004), 241–254, doi:10.1002/jgt.10158.

[4] G. Chartrand, M. S. Jacobson, J. Lehel, O. R. Oellermann, S. Ruiz and F. Saba, Irregular networks, Graph theory, 250th Anniv. Conf., Lafayette/Indiana 1986, Congr. Numerantium 64, 197-210 (1988)., 1988, https://www.researchgate.net/publication/265701559_Irregular_networks.

[5] R. Darda and A. Hujdurović, On bounds for the product irregularity strength of graphs, *Graphs Comb.* **31** (2015), 1347–1357, doi:10.1007/s00373-014-1458-5.

[6] K. Ford, The distribution of integers with a divisor in a given interval, *Ann. Math. (2)* **168** (2008), 367–433, doi:10.4007/annals.2008.168.367.

[7] A. Frieze, R. J. Gould, M. Karoński and F. Pfender, On graph irregularity strength, *J. Graph Theory* **41** (2002), 120–137, doi:10.1002/jgt.10056.

[8] M. Kalkowski, M. Karoński and F. Pfender, A new upper bound for the irregularity strength of graphs, *SIAM J. Discrete Math.* **25** (2011), 1319–1321, doi:10.1137/090774112.

[9] G. Kaplan, A. Lev and Y. Roditty, Bertrand's postulate, the prime number theorem and product anti-magic graphs, *Discrete Math.* **308** (2008), 787–794, doi:10.1016/j.disc.2007.07.049.

[10] D. Koukoulopoulos, Localized factorizations of integers, *Proc. Lond. Math. Soc. (3)* **101** (2010), 392–426, doi:10.1112/plms/pdp056.

[11] P. Majerski and J. Przybyło, On the irregularity strength of dense graphs, *SIAM J. Discrete Math.* **28** (2014), 197–205, doi:10.1137/120886650.

[12] O. Pikhurko, Characterization of product anti-magic graphs of large order, *Graphs Comb.* **23** (2007), 681–689, doi:10.1007/s00373-007-0748-6.

[13] J. Skowronek-Kaziów, Multiplicative vertex-colouring weightings of graphs, *Inf. Process. Lett.* **112** (2012), 191–194, doi:10.1016/j.ipl.2011.11.009.

[14] J. Skowronek-Kaziów, Graphs with multiplicative vertex-coloring 2-edge-weightings, *J. Comb. Optim.* **33** (2017), 333–338, doi:10.1007/s10878-015-9966-7.

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P1.05
https://doi.org/10.26493/2590-9770.1396.3c7
(Also available at http://adam-journal.eu)

A tight relation between series–parallel graphs and bipartite distance hereditary graphs*

Nicola Apollonio†
Istituto per le Applicazioni del Calcolo, M. Picone, v. dei Taurini 19, 00185 Roma, Italy

Massimiliano Caramia
Dipartimento di Ingegneria dell'Impresa, Università di Roma "Tor Vergata", v. del Politecnico 1, 00133 Roma, Italy

Paolo Giulio Franciosa
Dipartimento di Scienze Statistiche, Sapienza Università di Roma, p.le Aldo Moro 5, 00185 Roma, Italy

Jean-François Mascari‡
Istituto per le Applicazioni del Calcolo, M. Picone, v. dei Taurini 19, 00185 Roma, Italy

Received 25 September 2020, accepted 06 December 2020, published online 21 March 2021

Abstract

Bandelt and Mulder's structural characterization of bipartite distance hereditary graphs asserts that such graphs can be built inductively starting from a single vertex and by repeatedly adding either pendant vertices or twins (i.e., vertices with the same neighborhood as an existing one). Dirac and Duffin's structural characterization of 2–connected series–parallel graphs asserts that such graphs can be built inductively starting from a single edge by adding either edges in series or in parallel. In this paper we give an elementary proof that the two constructions are the same construction when bipartite graphs are viewed as the fundamental graphs of a graphic matroid. We then apply the result to re-prove known results concerning bipartite distance hereditary graphs and series–parallel graphs and to provide a new class of polynomially-solvable instances for the integer multi-commodity flow of maximum value.

Keywords: Series-parallel graphs, bipartite distance hereditary graphs, binary matroids.

Math. Subj. Class.: 05C

*We are sincerely grateful to the referee for the careful reading of the paper and for his comments and detailed suggestions which helped us to improve considerably the manuscript.

†Corresponding Author. Supported by the Italian National Research Council (C.N.R.) under national research project "MATHTECH".

‡Supported by the Italian National Research Council (C.N.R.) under national research project "MATHTECH".

1 Introduction

Distance hereditary graphs are graphs with the *isometric property*, i.e., the distance function of a distance hereditary graph is inherited by its connected induced subgraphs. This important class of graphs was introduced and thoroughly investigated by Howorka in [24, 25]. A bipartite distance hereditary (BDH for short) graph is a distance hereditary graph which is bipartite. Such graphs can be constructed starting from a single vertex by means of the following two operations [6]:

(BDH1) adding a *pendant vertex*, namely a vertex adjacent exactly to an existing vertex;

(BDH2) adding a *twin* of an existing vertex, namely adding a vertex and making it adjacent to all the neighbors of an existing vertex.

Taken together the two operations above will be referred to as Bandelt and Mulder's construction.

A graph is *series–parallel* [7], if it does not contain the complete graph K_4 as a minor; equivalently, if it does not contain a subdivision of K_4. This is Dirac's [14] and Duffin's [15] characterization by forbidden minors. Since both K_5 and $K_{3,3}$ contain a subdivision of K_4, by Kuratowski's Theorem any series–parallel graph is planar. Like BDH graphs, series–parallel graphs admit a constructive characterization which justifies their name: a connected graph is series–parallel if it can be constructed starting from a single edge by means of the following two operations:

(SP1) adding an edge with the same end-vertices as an existing one (*parallel extension*);

(SP2) subdividing an existing edge by the insertion of a new vertex (*series extension*).

Taken together the two operations above will be referred to as Duffin's construction. Here and throughout the rest of the paper we consider only 2–connected series–parallel graphs which can be therefore obtained by starting from a pair of a parallel edges rather than by starting from a single edge.

The close resemblance between operations (BDH1) and (BDH2) and operations (SP1) and (SP2) is apparent. It becomes even more apparent after our Theorem 3.1, which establishes that the constructions defining BDH and series–parallel graphs, namely, Bandelt and Mulder's construction and Duffin's construction, are the same construction when bipartite graphs are viewed as fundamental graphs of a graphic matroid (Theorem 3.1). Although this fact is fairly well known and short proofs can be given using the deep and refined notions of *branch width* and *tree width* of graphs and matroids[1] (combined with classical results on graph minors), neither an elementary proof nor an explicit statement seem to be at hand.

The intimate relationship between BDH graphs and series–parallel graphs was also already observed by Ellis-Monhagan and Sarmiento in [16]. The authors, motivated by the aim of finding polynomially computable classes of instances for the *vertex–nullity interlace polynomial* introduced by Arratia, Bollobás and Sorkin in [5], under the name of *interlace polynomial*, related the two classes of graphs via a topological construction involving the so called *medial graph* of a planar graph. By further relying on the relationships

E-mail addresses: nicola.apollonio@cnr.it (Nicola Apollonio), caramia@disp.uniroma2.it (Massimiliano Caramia), paolo.franciosa@uniroma1.it (Paolo Giulio Franciosa), g.mascari@iac.cnr.it (Jean-François Mascari)

[1] In section 5, we give one of such a proof kindly supplied by an anonymous referee of an earlier version of the paper.

between the *Martin polynomial* and the *symmetric Tutte polynomial* of a planar graph, they proved a relation between the the *symmetric Tutte polynomial* of a planar graph H, namely $t(H;x,x)$—recall that the Tutte polynomial is a two variable polynomial–and the interlace polynomial $q(G;x)$ of a graph G derived from the medial graph of G (Theorem 4.1). Such a relation led to the following three interesting consequences:

– the #P–completeness of the interlace polynomial of Arratia, Bollobás and Sorkin [5] in the general case;

– a characterization of BDH graphs via the so-called γ *invariant*, (i.e., the coefficient of the linear term of the interlace polynomial);

– an effective proof that the interlace polynomial is polynomial-time computable within BDH graphs.

In view of a result due to Aigner and van der Holst (Theorem 4.6), the latter two consequences in the list above are straightforward consequences of Theorem 3.1 (see Section 4.1).

Besides the new direct proofs of these results, Theorem 3.1 has some more applications.

– Syslo's characterization's of series–parallel graphs in terms of *Depth First Search* (DFS) *trees*: the characterization asserts that a connected graph H is series–parallel if and only if every spanning tree of H is a DFS-tree of one of its 2–*isomorphic* copies. In other words, up to 2–*isomorphism*, series–parallel graphs have the characteristic property that their spanning trees can be oriented to become *arborescences* so that the corresponding fundamental cycles become directed circuits (cycles whose arcs are oriented in the same way). Recall that an *arborescence* is a directed tree with a single special node distinguished as the *root* such that, for each other vertex, there is a directed path from the root to that vertex.

– New polynomially solvable instances for the problem of finding *integer multi-commodity flow* of maximum value: if the demand graph of a series–parallel graph is a co–tree, then the maximum value of a multi-commodity flow equals the minimum value of a *multi-terminal cut*; furthermore both a maximizing flow and a minimizing cut can be found in strongly polynomial time.

Organization of the paper. The rest of the paper is organized as follows: in Section 2 we give the basic notions used throughout the rest of the paper. In Section 3 we prove our main result (Theorem 3.1) (two more proofs are given in Section 5) and discuss how it fits within *circle graphs* and how it relates with edge-pivoting. Theorem 3.1 is then applied in Section 4: in Section 4.1, we re-prove the previously mentioned couple of results in [16]; in Section 4.2 we re-prove Syslo's characterization of series–parallel graphs and give a sort of hierarchy of characterizations of 2–connected planar graphs by the properties of their spanning trees; finally in Section 4.3, we give an application to multi-commodity flow in series–parallel graphs.

2 Preliminaries

For a graph G the edge e with endvertices x and y will be denoted by xy. The graph induced by $U \subseteq V(G)$ is denoted by $G[U]$. If $F \subseteq E(G)$, the graph $G - F$ is the graph $(V(G), E(G) - F)$.

A *digon* is a pair of parallel edges, namely a cycle with two edges. A *hole* in a bipartite graph is an induced subgraph isomorphic to C_n for some $n \geq 6$. A *domino* is a subgraph isomorphic to the graph obtained from C_6 by joining two antipodal vertices by a chord. The domino is denoted by $\boxminus$. A bipartite graph G is a *chordal bipartite graph* if G has no hole. Let $\mathcal{F}$ be a family of graphs. We say that G is $\mathcal{F}$–free if G does not contain any induced copy of a member of $\mathcal{F}$. If G is $\mathcal{F}$–free and $\mathcal{F} = \{G_0\}$, then we say that G is G_0–free.

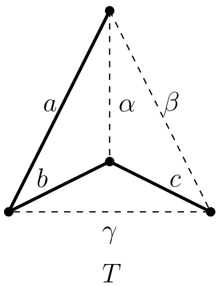
Graphs dealt with in this paper are, in general, not assumed to be vertex-labeled. However, when needed, vertices are labeled by the first n naturals where n is the order of G. We denote labeled and unlabeled graphs with the same symbol. If u and v are two vertices of G, then a *label swapping* at u and v (or simply uv-swapping) is the labeled graph obtained by interchanging the labels of u and v. For a bipartite graph G with color classes A and B, let $\mathsf{A} \in \{0,1\}^{A\times B}$ be the *reduced adjacency matrix of* G, namely, A is the matrix whose rows are indexed by the vertices of A, whose columns are indexed by the vertices of B and where $\mathsf{A}_{u,v} = 1$ if and only if u and v are adjacent vertices of G. The *incidence graph* of a matrix $\mathsf{A} \in \{0,1\}^{A\times B}$ is the bipartite graph with color classes A and B and where $u \in A$ and $v \in B$ are adjacent if and only $a_{u,v} = 1$.

We review very briefly some basic notions in matroid theory [28, 36, 37]. For a $\{0,1\}$-matrix A the *binary matroid generated by* A, denoted by $M(\mathsf{A})$, is the matroid whose elements are the indices of the columns of A and whose independent sets are those subsets of elements whose corresponding columns are linearly independent over $GF(2)$. A *binary matroid* is a matroid isomorphic to the binary matroid generated by some $\{0,1\}$-matrix A. If T is a basis of a binary matroid M and $f \notin T$, then $T \cup \{f\}$ contains a unique minimal non independent set $C(f,T)$. Thus, if F is a proper subset of $C(f,T)$, then F is an independent set of M. Such a set $C(f,T)$ is the so called *fundamental circuit through* f *with respect to* T and $C(f,T) - \{f\}$ is the corresponding *fundamental path*. A *partial representation* of a binary matroid M is a $\{0,1\}$-matrix $\widetilde{\mathsf{A}}$ whose columns are the incidence vectors over the elements of a basis of the fundamental circuits with respect to that basis.

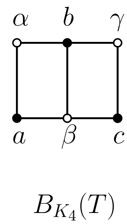
A *fundamental graph of a binary matroid* M is simply the incidence bipartite graph of any of its partial representations. Therefore a bipartite graph G is the fundamental graph of a binary matroid M if G is isomorphic to the graph $B_M(T)$ with color classes T and $\overline{T}$ for some basis T and co-basis $\overline{T}$ (i.e., the complement of a basis) of M and where there is an edge of G between $e \in T$ and $f \in \overline{T}$ if $e \in C(f,T)$, where $C(f,T)$ is the fundamental circuit through f with respect to T. If $\widetilde{\mathsf{A}}$ is a partial representation of a binary matroid M, then $M \cong M([\,\mathsf{I}\,|\,\widetilde{\mathsf{A}}\,])$, that is M is isomorphic to the matroid generated by $[\,\mathsf{I}\,|\,\widetilde{\mathsf{A}}\,]$. Clearly, $\widetilde{\mathsf{A}}$ is a partial representation of M with rows and columns indexed by the elements of the basis T and of the co-basis $\overline{T}$, respectively, if and only if $\widetilde{\mathsf{A}}$ is the reduced adjacency matrix of $B_T(M)$, where the color class T indexes the rows of $\widetilde{\mathsf{A}}$.

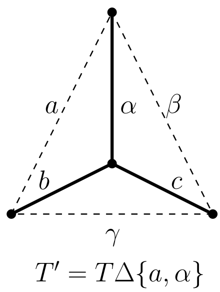
The *cycle matroid* (also known as *graphic matroid)* of a graph H, denoted by $M(H)$, is the matroid whose elements are the edges of H and whose independent sets are the forests of H. If H is connected, then the bases of $M(H)$ are precisely the spanning trees of H and its co-bases are precisely the *co-trees*, namely the subgraphs spanned by the complement of the edge–set of a spanning tree. A matroid M is a *cycle matroid* if it is isomorphic to the cycle matroid of some graph H. Cycle matroids are binary: if M is a cycle matroid, then there are a graph H and a spanning forest of H such that $M \cong M([\,\mathsf{I}\,|\,\widetilde{\mathsf{A}}\,])$ where $\widetilde{\mathsf{A}}$ is the $\{0,1\}$-matrix whose columns are the incidence vectors over the edges of a spanning forest of the fundamental cycles with respect to that spanning forest.

A *fundamental graph of a graph H* is simply the fundamental graph of its cycle matroid $M(H)$. For a graph H and one of its spanning forests T, we abridge the notation $B_{M(H)}(T)$ into $B_H(T)$ to denote the fundamental graph of H with respect to T (see Figure 1, where $H \cong K_4$). If H is 2–connected, then $B_H(T)$ is connected. Moreover, $B_H(T)$ does not determine H in the sense that non-isomorphic graphs may have isomorphic fundamental graphs. This because, while it is certainly true that isomorphic graphs have isomorphic cycle matroids, the converse is not generally true (see Figure 2). Two graphs having isomorphic cycle matroids are called 2–*isomorphic*.



	α	β	γ
a	1	1	0
b	1	1	1
c	0	1	1





	a	β	γ
α	1	1	0
b	1	0	1
c	0	1	1

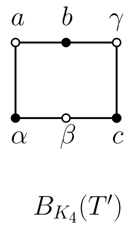


Figure 1: Two fundamental graphs of K_4 with respect to two spanning trees T and T' along with the corresponding matrices and the respective fundamental graphs. The fundamental graph with respect to T' arises from the one with respect to T by pivoting along edge αa.

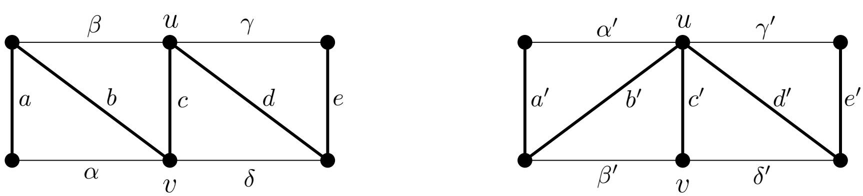


Figure 2: Two 2–isomorphic graphs that are not isomorphic: $x \mapsto x'$ maps bijectively fundamental cycles of the graph on the left to fundamental cycles of the graph on the right.

3 BDH graphs are fundamental graphs of series parallel graphs

In this section we prove our main result.

Theorem 3.1. *A connected bipartite graph G is a bipartite distance hereditary graph if and only if G is a fundamental graph of a 2–connected series–parallel graph.*

Proof. For a bipartite graph G let M^G denote the binary matroid generated by the reduced adjacency matrix of G. Let us examine preliminarily the effect induced on a fundamental graph $B_H(T)$ of a 2–connected graph H by series and parallel extensions and, conversely (and in a sense "dually"), the effect induced on M^G by extending a connected bipartite graph G through the addition of violated vertices and twins. If M^G is a graphic matroid and H is one of the 2–isomorphic graphs whose cycle matroid is isomorphic to M^G, then Table 1 summarizes these effects.

Operation on H		Operation on $B_H(T)$
Parallel extension on edge a of T	$\leftrightarrow$	adding a pendant vertex in color class $\overline{T}$ adjacent to a
Series extension on edge a of T	$\leftrightarrow$	adding a twin of a in color class T
Parallel extension on edge β of $\overline{T}$	$\leftrightarrow$	adding a twin of β in color class $\overline{T}$
Series extension on edge β of $\overline{T}$	$\leftrightarrow$	adding a pendant vertex in color class T adjacent to β.

Table 1: The effects of series and parallel extension on H on its fundamental graph $B_H(T)$.

We can now proceed with the proof. The *only if direction* is proved by induction on the order of G. The assertion is true when G has two vertices because K_2 is a BDH graph and at the same time is also the fundamental graph of a digon. Let now G have $n \geq 3$ vertices and assume that the assertion is true for BDH graphs with $n-1$ vertices. By Bandelt and Mulder's construction G is obtained from a BDH graph G' either by adding a pendant vertex or a twin. Let H' be a series–parallel graph having G' as fundamental graph with respect to some spanning tree. Since, by Table 1, the last two operations correspond to series or parallel extension of H', the result follows by Duffin's construction of series–parallel graphs. For the *if direction*, let G be the fundamental graph of a series–parallel graph H with respect to some tree T. By Duffin's construction of series–parallel graphs and Table 1, G can be constructed starting from a single edge by either adding twins or pendant vertices. Therefore, G is a BDH graph by Bandelt and Mulder's construction. □

Before going through applications, let us discuss how Theorem 3.1 relates to *circle graphs*, a thoroughly investigated class of graphs which we now briefly describe.

A *double occurrence word* $\mathbf{w}$ over a finite alphabet Σ is a word in which each letter appears exactly twice, where $\mathbf{w}$ is cyclic word, namely, it is the equivalence class of a linear word modulo cyclic shifting and reversal of the orientation. Two distinct symbols of Σ in $\mathbf{w}$ are *interlaced* if one appears precisely once between the two occurrences of the other. By wrapping $\mathbf{w}$ along a circle and by joining the two occurrences of the same symbol of $\mathbf{w}$ by a chord labeled by the same symbols whose occurrences it joins, one obtains a pair $(S, \mathcal{C})$ consisting of a circle S and a set $\mathcal{C}$ of chords of S. In knot theory terminology, such a pair is usually called a *chord diagram* and its intersection graph, namely the graph whose vertex set is $\mathcal{C}$ and where two vertices are adjacent if and only if the corresponding chords intersects, is called *the interlacement graph of the chord diagram* or the *interlacement graph of the double occurrence word*.

A graph is an *interlacement graph* if it is the interlacement graph of some chord diagram or of some double occurrence words. Interlacement graphs are probably better known as *circle graphs*. The name *interlacement graph* comes historically from the *Gauss Realization Problem of double occurrence words* [13, 31, 34].

Distance hereditary graphs are circle graphs [8]. Thus BDH graphs form a proper subclass of bipartite circle graphs. De Fraysseix [11, 12] proved the following.

Theorem 3.2 ([11, 12]). *A bipartite graph is a bipartite circle graph if and only if it is the fundamental graph of a planar graph.*

Therefore Theorem 3.1 specializes de Fraysseix's Theorem to the subclass of series–parallel graphs.

3.1 BDH graphs and edge–pivoting

It follows from Theorem 3.1 that with every 2–isomorphism class of 2–connected series–parallel graphs one can associate all the BDH graphs that are fundamental graphs of each member in the class. Therefore BDH graphs that correspond to the same 2–isomorphism class are graphs in the same "orbit". In this section we make precise the latter sentence and draw the graph-theoretical consequences of this fact.

Given a $\{0,1\}$-matrix A, pivoting A over $GF(2)$ on a nonzero entry (the pivot element) means replacing

$$\tilde{A} = \begin{pmatrix} 1 & \mathsf{a} \\ \mathsf{b} & \mathsf{D} \end{pmatrix} \quad \text{by} \quad \tilde{A} = \begin{pmatrix} 1 & \mathsf{a} \\ \mathsf{b} & \mathsf{D} + \mathsf{ba} \end{pmatrix}$$

where a is a row vector, b is a column vector, D is a submatrix of A and the rows and columns of A have been permuted so that the pivot element is $a_{1,1}$ ([10, p. 69], [32, p. 280]). If A is the partial representation of the cycle matroid of a graph H (or more generally a binary matroid), then pivoting on a nonzero entry, $C(e,f)$, say, yields a new tree (basis) with f in the tree (basis) and e in the co-tree (co-basis) and the matrix obtained after pivoting is a new partial representation matrix of the same matroid. Clearly the fundamental graphs associated with the two bases change accordingly so that pivoting on $\{0,1\}$-matrices induces an operation on bipartite graphs whose concrete interpretation is a change of basis in the associated binary matroid. The latter operation on bipartite graph will be still referred to as *edge–pivoting* or simply to as *pivoting* in analogy to what happens for matrices (see also Figure 1). In the context of circle graphs, the operation of pivoting is a specialization to bipartite graph of the so called *edge–local complementation*. Since any bipartite graph is a fundamental graph of some binary matroid, the operation of *pivoting* can be described more abstractly as follows.

Given a bipartite graph with color classes A and B, *pivoting on edge* $uv \in E(G)$ is the operation that takes G into the graph G^{uv} on the same vertex set of G obtained by complementing the edges between $N_G(u) \setminus \{u\}$ and $N_G(v) \setminus \{v\}$ and then by swapping the labels of u and v (if G is labeled). More formally, if $\ell_G \colon V(G) \to \mathbb{N}$ is a labeling of the vertices of G, then

$$G^{uv} = (V(G), E(G)\Delta((N_G(u) \setminus \{u\}) \times (N_G(v) \setminus \{v\})))$$

and $\ell_{G^{uv}}$ is defined by $\ell_{G^{uv}}(u) = \ell_G(v)$, $\ell_{G^{uv}}(v) = \ell_G(u)$ and $\ell_{G^{uv}}(w) = \ell_G(w)$ if $w \notin \{u,v\}$. If $e \in E(G)$ has endpoints uv, then we use G^e in place of G^{uv}.

We say that a graph $\widetilde{G}$ is *pivot-equivalent* to a graph G, written $\widetilde{G} \sim G$, if for some $k \in \mathbb{N}$, there is a sequence $G_1, \ldots, G_k$ of graphs such that $G_1 \cong G$, $G_k \cong \widetilde{G}$ and, for $i = 1, \ldots, k-1$, $G_{i+1} \cong G_i^{e_i}$, $e_i \in E(G_i)$. The *orbit of* G, denoted by $[G]$, consists of all graphs that are pivot-equivalent to G.

For later reference, we state as a lemma the easy though important facts discussed above. Figure 1 illustrates the contents of the lemma.

Lemma 3.3. *Let M be a connected graphic matroid. Then M determines both a class $[G]$ of pivot-equivalent graphs and a class $[H]$ of 2–isomorphic graphs. In particular, any graph in $[G]$ is the fundamental graph of some 2–isomorphic copy of H and the fundamental graph of any graph in $[H]$ is pivot-equivalent to G.*

The operations of pivoting and of taking induced subgraphs commute in (bipartite) graphs.

Lemma 3.4 (see [5])**.** *Let G a bipartite graph, $U \subseteq V(G)$ and e be an edge whose end-vertices are in U. Then $G^e[U] \cong (G[U])^e$.*

The next lemma relates in the natural way minors of a cycle matroid to the induced subgraphs of the fundamental graphs associated with the matroid.

Lemma 3.5. *Let M and N be cycle matroids. Let G be any of the fundamental graphs of M and let K be any of the fundamental graphs of N. Then N is a minor of M if and only if K is an induced subgraph in some bipartite graph in the orbit of G. Equivalently, N is a minor of M if and only if G contains some induced copy of a graph in the orbit of K.*

To get acquainted with pivoting, the reader may check Lemma 3.6 with the help of Figure 3. Refer to Section 2 for the definition of *domino* and *hole*.

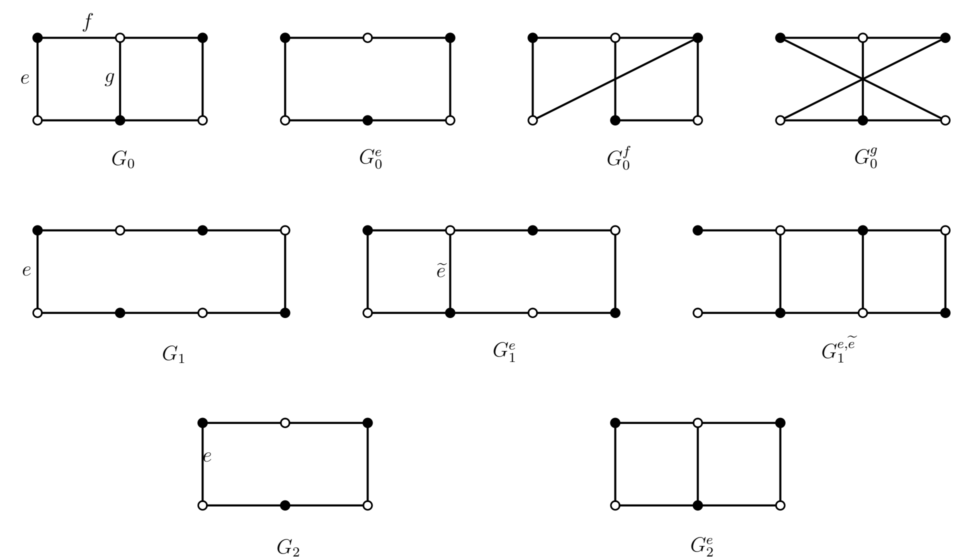


Figure 3: The effect of pivoting a graph G along some of its edges when $G \cong$ ⊟$, C_8, C_6$.

Lemma 3.6. *Let $k \geq 6$ be an even integer.*

- *If either $H \cong \boxminus$ or $H \cong C_k$, then for each $uv \in E(H)$ there exists an induced subgraph H' of H^{uv} such that either $H' \cong \boxminus$ or $H' \cong C_k$.*
- *If $G \cong C_k$, then there is a graph $\widetilde{G}$ in the orbit of H such that $\widetilde{G}$ contains an induced copy of either $\boxminus$ or C_6.*

Proof. By inspecting Figure 3 one checks that if $G \cong \boxminus$, then either $G^e \cong \boxminus$ or $G^e \cong C_6$. If $G \cong C_6$, then $G^e \cong \boxminus$ for every $e \in E(G)$. If $G \cong C_k$, $k > 6$, then by pivoting on $uv \in E(G)$ and deleting u and v results in a graph $G' \cong C_{k-2}$. In particular, by repeatedly pivoting on new formed edges (like edge $\widetilde{e}$ of graph G_1^e in Figure 3), one obtains a graph in the orbit of G which contains an induced copy of either $\boxminus$ or C_6. The second part of the proof is left to the reader. □

We are ready to extract the graph-theoretical consequence of Theorem 3.1. To this end let us recall that besides their constructive characterization, Bandelt and Mulder characterized the class of BDH graphs also by forbidden induced subgraphs as follows.

Theorem 3.7 ([6, Corollaries 3 and 4])**.** *Let G be a connected bipartite graph. Then G is BDH if and only if G contains neither holes nor induced dominoes.*

The following two corollaries follow straightforwardly from Theorem 3.1 after Theorem 3.7 and assert that the class of BDH graphs–that is, of $\{hole, domino\}$–free graphs–is closed under pivoting, namely, that the orbit of a bipartite $\{hole, domino\}$–free graph consists of $\{hole, domino\}$–free graphs.

Corollary 3.8. *The following statements about a chordal bipartite graph G are equivalent:*

(i) *G does not contain any induced domino;*

(ii) *any graph in the orbit of G is a chordal bipartite graph.*

Corollary 3.9. *Let G be a bipartite domino-free graph. If G is chordal, then so is any other graph in its orbit.*

4 Applications

4.1 BDH graphs and the interlace polynomial

As already mentioned, Ellis-Monaghan and Sarmiento related series–parallel graphs and BDH graphs topologically, via the medial graph. Let H be a plane graph (or even a 2-cell embedded graph in an oriented surface). For our purposes, we can assume that H is 2–connected. The medial graph $m(H)$ of H is the graph obtained as follows: first place a vertex v_e into the interior of each edge e of H. Then, for each face F of H, join v_e to v_f by an edge lying in F if and only if the edges e and f are consecutive on the boundary of F. Notice that if F is bounded by a digon $\{e, e'\}$ or if e and e' share a degree-2 endpoint in H, then vertices v_e and $v_{e'}$ are joined by two parallel edges. Let $m(H)$ be the plane (2-cell embedded) graph obtained in this way. The graph underlying $m(H)$ is the medial graph of H. The medial graph is clearly 4-regular, as each face creates two adjacencies for each edge on its boundary. Moreover, it can be oriented so that each vertex is entered by 2 arcs and left by 2 arcs. Given a 4-regular labeled graph N and one of its Eulerian circuits

C, we can associate with N a double occurrence word $\mathbf{w}$ which is the word consisting of the labels of the vertices of C cyclically met during the tour on C. The circle graph formed from C and chords between repeated pairs of letters of $\mathbf{w}$ is called the *the circle graph of* N. Ellis-Monaghan and Sarmiento, building also on the relations between the *Martin polynomial* and the symmetric *Tutte polynomial*, proved the following relation between the symmetric Tutte polynomial $t(H; x, x)$ of a planar graph H and the vertex nullity interlace polynomial $q(G; x)$ of a graph G derived, as described in the theorem below, from the medial graph of any of its plane embedding.

Theorem 4.1 ([16])**.** *If H is a plane embedding of a planar graph and G is the circle graph of some Eulerian circuit of the medial graph of H, then $q(G; x) = t(H; x, x)$.*

The results were then specialized so as to give the following characterization of BDH graphs.

Theorem 4.2 ([16])**.** *G is a BDH graph with at least two vertices if and only if it is the circle graph of an Euler circuit in the medial graph of a plane embedding of a series–parallel graph H.*

Using Theorem 4.1 and Theorem 4.2, the authors deduced the following consequences stated below as Corollary 4.3, Corollary 4.4 and Corollary 4.5.

Corollary 4.3. *Computing the vertex-nullity interlace polynomial is #P-hard in general.*

Corollary 4.4. *If G is a BDH graph, then $q(G; x)$ is polynomial-time computable.*

Corollary 4.4 follows because the Tutte polynomial is polynomial-time computable for series–parallel graphs [29].

Corollary 4.5. *A connected graph G is a BDH graph if and only if the coefficient of the linear term of $q(G; x)$ equals 2.*

The latter coefficient referred to in Corollary 4.5, denoted by $\gamma(G)$, is called the γ-invariant of G in analogy with the Crapo invariant $\beta(G)$ which is the common value of the coefficients of the linear terms of $t(G; x, y)$ where G has at least two edges. By a result due to Brylawski [9] (in the more general context of matroids) series–parallel graphs can be characterized by the value of the Crapo invariant as follows: a graph G is a series–parallel graph if and only if $\beta(G) = 1$. Both the corollaries above can be deduced directly by Theorem 3.1 after the following result due to Aigner and van der Holst [1].

Theorem 4.6 ([1])**.** *If G is a bipartite graph, then*

$$q(G; x) = t(M^G; x, x)$$

where M^G is the binary matroid generated by the reduced adjacency matrix of G and $t(M^G; x, x)$ is the Tutte polynomial of M^G.

Theorem 3.1 and Theorem 4.6 have the following straightforward consequence which re-proves directly Corollary 4.4 and Corollary 4.5.

Corollary 4.7. *If G is BDH graph, then*

$$q(G; x) = t(H; x, x)$$

for some series–parallel graph H having G as fundamental graph and where $t(H; x, x)$ is the Tutte polynomial of H, namely the Tutte polynomial of the cycle matroid of H.

4.2 Characterizing series–parallel graphs by DFS-trees

As credited by Syslo [35], Shinoda, Chen, Yasuda, Kajitani, and Mayeda, proved that series–parallel graphs can be completely characterized as in Theorem 4.8 by a property of their spanning trees, and Syslo himself gave a constructive algorithmic proof of the result [35].

Theorem 4.8 (S. Shinoda et al., 1981; Syslo, 1984). *Every spanning tree of a connected graph H is a DFS-tree of one of its 2–isomorphic copies if and only if H is a series–parallel graph.*

When H is assumed to be 2–connected (an assumption that guarantees the connectedness of its fundamental graphs), Theorem 4.8 will be equivalently stated as statement (1) below.

Let $\mathcal{T}$ be a family of trees (or a family of oriented trees) and let G be a bipartite graph with color classes A and B. We say that G is a *path/$\mathcal{T}$ bipartite graph on A* if there exist a member T of $\mathcal{T}$ and a bijection $\xi\colon A \to E(T)$ such that, for each $v \in B$, $\{\xi w \mid w \in N_G(v)\}$ is the edge–set (arc–set if T is oriented) of a simple cycle (directed circuit if T is oriented) in the (oriented) graph $(V(T), A \cup B)$. *Path/$\mathcal{T}$ bipartite graphs on B* are defined similarly. G is a *path/$\mathcal{T}$ bipartite graph* if it is a path/$\mathcal{T}$ bipartite graph on A or on B. G is a *self–dual path/$\mathcal{T}$* bipartite graph if it is a path/$\mathcal{T}$ bipartite graph on both A and B. In any case T will be referred to as a *supporting tree* for G. For instance, if $G \cong K_{1,3}$ and G has color classes $A = \{a\}$ and $B = \{\alpha, \beta, \gamma\}$ and if $\mathcal{T}$ is any family of paths containing paths of order 2 and order 4, then G is a path/$\mathcal{T}$ bipartite graph: G is supported on A by a path of order 2 whose unique edge is labeled a and G is supported on B by a path of order 4 with three edges labeled α, β and γ.

Recall that an *arborescence* is a directed tree with a single special node distinguished as the *root* such that, for each other vertex, there is a directed path from the root to that vertex. A *DFS tree* for a connected graph H (in the sense of [35]), is a pair (T, ϕ) consisting of a spanning tree T and an orientation ϕ of H, such that ϕT is a spanning arborescence of ϕH and for each $f \in E(H) \setminus E(T)$, $\phi C(f, T)$ is a directed circuit in ϕH (i.e, all arcs of $\phi C(f, T)$ are oriented in the same way). By choosing for $\mathcal{T}$ the class **arborescence** of arborescences, one can reformulate Theorem 4.8 in the following way

(1) H is series–parallel if and only if for each spanning tree T of H the fundamental graph $B_T(H)$ is a self–dual path/**arborescence** bipartite graph.

Indeed, if (T, ϕ) is a DFS-tree in a 2–isomorphic copy H' of H, then T is a spanning tree of graph H' whose cycle matroid is $M(H)$; hence $B_H(T) \cong B_{H'}(T)$ and ϕT is a supporting arborescence for $B_H(T)$. Conversely, suppose that G is a fundamental graph of H and that G is a path/**arborescence** bipartite graph. Let G have color classes A and B. Since G is a path/**arborescence** bipartite graph, then there is a supporting arborescence $\overrightarrow{T}$ for G that induces an orientation ϕ of the graph $H' = (V(T), A \cup B)$, T being the underlying undirected graph of $\overrightarrow{T}$. Clearly (T, ϕ) is a DFS tree in H' which in turn is 2–isomorphic to H because G is one of its fundamental graphs (i.e., H and H' have the same cycle matroid).

Statement (1) is now a rather straightforward consequence of Corollary 3.8 and the fact that BDH graphs are self–dual path/**arborescence** bipartite graphs as shown by the following result proved in [4].

Theorem 4.9 ([4])**.** *Every connected BDH graph is a self–dual path/**arborescence** bipartite graph.*

Proof of (1). Let H be a 2–connected series–parallel graph. Then, by Theorem 3.1 $B_H(T)$ is BDH for each spanning tree T of H. Hence, for every spanning tree T of H, $B_H(T)$ is a self–dual path/**arborescence** bipartite graph by Theorem 4.9. Conversely, suppose that for every spanning tree T of a 2–connected graph H, the fundamental graph $B_H(T)$ is a path/**arborescence** bipartite graph. Thus $B_H(T)$ is chordal (see, e.g., [8]). Moreover, since if T' is any other spanning tree of H, then $B_H(T')$ is in the orbit of $B_H(T)$, we conclude that each bipartite graph in the orbit of $B_H(T)$ is a chordal bipartite graph. Therefore $B_H(T)$ is a BDH graph by Corollary 3.8 and, consequently, H is a series–parallel graph. □

It is worth observing that, in the same way as Theorem 3.1 specializes de Fraysseix's Theorem 3.2, Statement (1) specializes the following statement (see also [12]):

(2) a bipartite graph is a bipartite circle graph if and only if it is a self–dual path/**tree** bipartite graph, **tree** being the class of trees.

Proof. By Whitney's planarity criterion [38] a graph is planar if and only if its cycle matroid is also *co-graphic*, namely, it is the dual matroid of another cycle matroid. Let now G be the fundamental graph of a 2–connected graph H with respect to some spanning tree T of H. Let A be the reduced adjacency matrix of G with rows indexed by the edges of T and columns indexed by the edges of $\overline{T}$. Then, while $[\,\mathsf{I}\,|\,\mathsf{A}\,]$ generates $M(H)$, $[\,\mathsf{I}\,|\,\mathsf{A}^t\,]$ generates $M^*(H)$, the dual of $M(H)$. Hence, when H is planar, by Whitney's planarity criterion, $M^*(H)$ is the cycle matroid of a 2–isomorphic copy of a plane dual H^* of H. Therefore the neighbors of each vertex in the color class T spans a path in the co-tree $\overline{T}$ which is in turn a spanning tree of a 2–isomorphic copy of plane dual H^* of H. □

In view of such a discussion it is reasonable to wonder whether there is a class of self dual path/ $\mathcal{T}_0$ bipartite graphs closed under edge–pivoting, where $\mathcal{T}_0$ is a family of trees sandwiched between **trees** and **arborescences**. The next result gives a negative answer in a sense. In what follows **di-tree** is the class of oriented trees.

Theorem 4.10. *If G is a connected bipartite graph whose orbit consists of self–dual path/**di-tree** bipartite graphs, then the orbit of G consists of path/**arborescence** bipartite graphs.*

Proof. Path/**di-tree** bipartite graphs are *balanced* (see [2]). Recall that a bipartite graph Γ is *balanced* if its reduced adjacency matrix does not contain the vertex-edge adjacency matrix of a chordless cycle of odd order. Equivalently, Γ is *balanced* if each hole of Γ has order congruent to zero modulo 4. Hence, since G and any other graph in its orbit is a self–dual path/**di-tree** bipartite graph, then G, and any other graph in its orbit must be balanced as well. Let $\widetilde{G}$ be any member of $[G]$ and suppose that $\widetilde{G}$ contains a hole C. Let $e \in E(C)$. The order t of C is at least eight, because $\widetilde{G}$ is balanced. Nevertheless $\widetilde{G}^e$ contains a hole of order $t-2$ by Lemma 3.6. Since $t-2 \equiv 2 \pmod 4$ we conclude that any graph in the orbit of G must be hole-free. Therefore G is BDH by Corollary 3.9, and, by Theorem 3.1, it is the fundamental graph of a series–parallel graph. The thesis now follows by Statement (1). □

Remark 4.11. It is worth observing that by the proof above, if $\mathbf{A}$ is a class of balanced matrices closed under pivoting over $GF(2)$, then $\mathbf{A}$ consists of totally balanced matrices, namely those matrices whose bipartite incidence graph is hole-free. Actually, and more sharply, in view of Corollary 3.9, every member of $\mathbf{A}$ is the incidence matrix of a γ-acyclic hypergraph [3].

4.3 Packing paths and multi-commodity flows in series–parallel graphs

In this section we give an application of Theorem 3.1 in Combinatorial Optimization. We show that a notoriously hard problem contains polynomially solvable instances when restricted to series–parallel graphs. Let $H = (V, E)$ be a graph and let $F \subseteq E$ be a set of prescribed edges of H called the *nets* of H. Following [19] a path P of H will be called F*-admissible* if it connects two vertices s, t of V with $st \in F$ and $E(P) \subseteq E - F$. Let U be the set of end-vertices of the nets. In the context of network-flow, vertices of U are thought of as terminals to be connected by a flow of some commodity (the nets are in fact also known as *commodities*). Let $\mathcal{P}_F$ denote the family of all F-admissible paths of G and let $\mathcal{P}_{F,f} \subseteq \mathcal{P}_F$ be the family of those F-admissible paths connecting the endpoints s,t of net f. An F*-multiflow* (see e.g. [33]), is a function $\lambda\colon \mathcal{P}_F \to \mathbb{R}_+$, $P \mapsto \lambda_P$. The multiflow is integer if λ is integer valued. The value of the F*-multiflow on the net* f is $\phi_f = \sum_{P\in\mathcal{P}_{F,f}} \lambda_P$. The total value of the multiflow is the number $\phi = \sum_{f\in F} \phi_f$. Let $w\colon E - F \to \mathbb{Z}_+$ be a function to be though of as a capacity function. An F*-multiflow subject to* w in H is an F-multiflow such that,

$$\sum_{P\in\mathcal{P}_F : E(P)\ni e} \lambda_P \le w(e), \;\; \forall e \in E - F \tag{4.1}$$

When $w(e) = 1$ for all $e \in E - F$, an integer multiflow is simply a collection of edge–disjoint F-admissible paths of H. The F*-Max- Multiflow Problem* is the problem of finding, for a given capacity function w, an F-multiflow subject to w of maximum total value. An F*-multicut* of H is a subset of B edges of $E - F$ that intersects the edge–set of each F-admissible path. The name F-multicut is due to the fact that the removal of the edges of B from H leaves a graph with no F-admissible path: in the graph $H - B$ it is not possible to connect the terminals of any net. The *capacity of the* F*-multicut* B is the number $\sum_{e\in B} w(e)$.

Multiflow Problems are very difficult problems (see [18], [19] and Vol. C, Chapter 70 in [33]). In [20] it has been shown that the Max-Multiflow Problem is NP-hard even for trees and even for $\{1, 2\}$-valued capacity functions. The problem though is shown to be polynomial time solvable for constant capacity functions by a dynamic programming approach. However, even for constant functions, the linear programming problem of maximizing the value of the multiflow over the system of linear inequalities (4.1) has not even, in general, $\frac{1}{2}\mathbb{Z}$-valued optimal solutions. In [26], the NP-completeness of the Edge–Disjoint–Multi commodity Path Problem for series–parallel graphs (and partial 2–trees) has been established while, previously in [39], the polynomial time solvability of the same problem for partial 2–trees was proved under some restriction either on the number of the commodities (required to be a logarithmic function of the order of the graph) or on the location of the nets.

Theorem 4.12. *Let $H = (V, E)$ be a 2–connected series–parallel graph and let F be the edge–set of any of its spanning co-trees. Then the maximum total value of an F-multiflow* *equals the minimum capacity of an F-multicut. Furthermore, both a maximizing multiflow and a minimizing multicut can be found in strongly polynomial time.*

Proof. Let A be a $\{0,1\}^{m\times n}-$valued matrix and $\mathsf{b} \in \mathbb{Z}_+^m$ be a vector. Let 1_d be the all ones vector in $\mathbb{R}^d$. Consider the linear programming problem

$$\max_{\mathsf{x}\in\mathbb{R}_+^n} \left\{1_n^T \mathsf{x} \mid \mathsf{A}\mathsf{x} \leq \mathsf{b}\right\} \tag{4.2}$$

and its dual

$$\min_{\mathsf{y}\in\mathbb{R}_+^m} \left\{\mathsf{b}^T \mathsf{y} \mid \mathsf{A}^T\mathsf{y} \geq 1_n\right\}. \tag{4.3}$$

By the results of Hoffman, Kolen and Sakarovitch [23] and Farber [17], if A is a totally balanced matrix (i.e., A is the reduced adjacency matrix of a bipartite chordal graph), then both the linear programming problems above have integral optimal solutions and, by linear programming duality, the two problems have the same optimum value. Furthermore, an integral optimal solution x^* to the maximization problem in (4.2) satisfying the additional constraint

$$\mathsf{x}^* \leq 1_n \tag{4.4}$$

and an integral optimal solution y^* to the minimization problem in (4.3) satisfying the additional constraint

$$\mathsf{y}^* \leq 1_n \tag{4.5}$$

can be found in strongly polynomial time.

Let now H be a 2–connected graph and let F be the edge–set of a co–tree $\overline{T}$ of some spanning T tree of H. By giving a total order on the edge–set of T, one can define a vector b whose entries are the values of the capacity function $w\colon E(H) - F \to \mathbb{Z}_+$. If A is the incidence matrix of $\mathcal{P}_F$, namely the matrix whose columns are the incidence vectors of the F-admissible paths of H, then A is a partial representation of $M(H)$. Moreover, if H is series–parallel, then A is totally balanced: by Theorem 3.1, A is the reduced adjacency matrix of a BDH graph which is chordal being hole-free (by Theorem 3.7). On the other hand, integral solutions to the problem in (4.2) satisfying constraint (4.4) and to the problem in (4.3) satisfying constraint (4.5) are incidence vectors of F-multiflows and F-multicuts, respectively. Hence, both an F-multiflow of maximum value and an F-multicut of minimum capacity can be found in strongly polynomial-time by solving the linear programming problems above. Moreover, linear programming duality implies that the maximum value of an F-multiflow and the minimum capacity of an F-multicut coincide. □

5 Two more proofs of Theorem 3.1

In this section, we give two more proofs of Theorem 3.1: one is due to an anonymous referee of an earlier version of the paper and it relies on the deep and refined notion of *branch*- and *rank-width* of a matroid (for the undefined terms given in the proof we address the reader to the references therein); the other fits the theory of double occurrences words and relies on a result in [5].

Second proof of Theorem 3.1. Suppose that a connected bipartite graph G is a fundamental graph of a 2-connected series parallel graph H. Since 2-connected graphs of branch-width at most 2 are exactly 2-connected series parallel graphs ([30]), the branch-width of H is at most 2. As proved in [22], the branch-width of a graph equals that of its cycle matroid. Hence, the branch-width of H equals the branch-width of $M(H)$. By a result in [27], the branch-width of a binary matroid (in particular of a cycle matroid) equals the rank-width of any of its fundamental graphs plus 1. By definition, G is a fundamental graph of $M(H)$ and thus $\mathrm{rw}(G)+1 = \mathrm{bw}(M(H)) = \mathrm{bw}(H) \leq 2$, where $\mathrm{rw}(\cdot)$ and $\mathrm{bw}(\cdot)$ denote the rank-width and branch-width parameters, respectively. Hence the rank-width of G is at most 1 and we conclude that G is bipartite distance hereditary because, still by a result in [27], distance hereditary graphs are precisely the graphs of rank-width at most 1.

For the other direction, suppose that a connected bipartite graph G is distance-hereditary. Let M^G be the binary matroid generated by the reduced adjacency matrix of G. By the same reasons (and the same notation) given above, it holds that $\mathrm{bw}(M^G) = \mathrm{rw}(G)+1 \leq 2$. By a result in [21], M^G is a *series parallel matroid* (see [36] for the definition) and any such a matroid is the cycle matroid of a series parallel graph (see Lemma 4.2.12 in [36]). Hence $M^G = M(H)$ for some series parallel graph H. Furthermore, H is 2-connected, otherwise, G is disconnected. □

The third proof will require a result in [5]. Let C be an Eulerian cycle in a 4-regular labeled graph H and let $\mathbf{w}$ be the double occurrence word it induces (Section 3, following the first proof of Theorem 3.1). Recall that two vertices, say labeled a and b, are interlaced in $\mathbf{w}$ if $\mathbf{w} = \mathbf{u}a\mathbf{x}b\mathbf{y}a\mathbf{z}$ for some (possibly empty) intervals $\mathbf{u}$, $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ of $\mathbf{w}$. For two vertices u and v, labeled a and b, respectively, the uv-transposition of $\mathbf{w}$ is the word $\mathbf{w}^{uv} = \mathbf{u}a\mathbf{y}b\mathbf{x}a\mathbf{z}$ [5]. Thus a uv-transposition of $\mathbf{w}$ amounts to replace one of the subpaths of C connecting u and v with the other one. The relation between uv-transposition and uv pivoting is given in the next lemma which specializes a more general result in [5] (see also [13]).

Lemma 5.1. *Let H be a 4-regular graph and let $\mathbf{w}$ be any of the double occurrence words it induces. Further, let $G(H,\mathbf{w})$ denote the interlacement graph of $\mathbf{w}$. Suppose that $G(H,\mathbf{w})$ is a bipartite graph. Then, for any edge uv of $G(H,\mathbf{w})$ of H, one has $G(H,\mathbf{w})^{uv} = G(H,\mathbf{w}^{uv})$.*

Third proof of Theorem 3.1. If G is a fundamental graph of a series–parallel graph, then M^G is a binary matroid with no $M(K_4)$ minor by Dirac and Duffin's characterization. Dominoes are fundamental graphs of K_4 and holes can be pivoted to either dominoes or C_6 (recall Lemma 3.6)—notice that C_6 is a fundamental graph of K_4 as well (Figure 1)–it follows that G is BDH-free by Lemma 3.3. Conversely, if G is BDH, then by Theorem 4.2 (in the language of Lemma 5.1), $G \cong G(m(H),\mathbf{w})$ for some series–parallel graph H (observe that $m(H)$ is a 4-regular graph) and some code $\mathbf{w}$. By Lemma 5.1, pivoting on edges G affects neither H nor $m(H)$. Consequently, every graph in $[G]$ is a BDH. Therefore M^G has no $M(K_4)$ minor by Lemma 3.3 and Lemma 3.5 and G is a fundamental graph of such a matroid and therefore the fundamental graph of a series–parallel graph. □

ORCID iDs

Nicola Apollonio https://orcid.org/0000-0001-6089-1333
Massimiliano Caramia https://orcid.org/0000-0002-9925-1306
Paolo Giulio Franciosa https://orcid.org/0000-0002-5464-4069
Jean-François Mascari https://orcid.org/0000-0002-0210-3375

References

[1] M. Aigner and H. van der Holst, Interlace polynomials, *Linear Algebra Appl.* **377** (2004), 11–30, doi:10.1016/j.laa.2003.06.010.

[2] N. Apollonio, Integrality properties of edge path tree families, *Discrete Math.* **309** (2009), 4181–4184, doi:10.1016/j.disc.2008.10.004.

[3] N. Apollonio, M. Caramia and P. G. Franciosa, On the Galois lattice of bipartite distance hereditary graphs, *Discrete Appl. Math.* **190/191** (2015), 13–23, doi:10.1016/j.dam.2015.03.014.

[4] N. Apollonio and P. G. Franciosa, On computing the Galois lattice of bipartite distance hereditary graphs, *Discrete Appl. Math.* **226** (2017), 1–9, doi:10.1016/j.dam.2017.04.004.

[5] R. Arratia, B. Bollobás and G. B. Sorkin, The interlace polynomial: a new graph polynomial, in: *Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 2000)*, ACM, New York, 2000 pp. 237–245.

[6] H.-J. Bandelt and H. M. Mulder, Distance-hereditary graphs, *J. Combin. Theory Ser. B* **41** (1986), 182–208, doi:10.1016/0095-8956(86)90043-2.

[7] M. Bodirsky, O. Giménez, M. Kang and M. Noy, Enumeration and limit laws for series–parallel graphs, *European J. Combin.* **28** (2007), 2091–2105, doi:10.1016/j.ejc.2007.04.011.

[8] A. Brandstädt, V. B. Le and J. P. Spinrad, *Graph classes: a survey*, SIAM Monographs on Discrete Mathematics and Applications, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1999, doi:10.1137/1.9780898719796.

[9] T. H. Brylawski, A combinatorial model for series–parallel networks, *Trans. Amer. Math. Soc.* **154** (1971), 1–22, doi:10.2307/1995423.

[10] G. Cornuéjols, *Combinatorial Optimization: Packing and Covering*, SIAM Monographs on Discrete Mathematics and Applications, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2001, doi:10.1137/1.9780898717105.

[11] H. de Fraysseix, Local complementation and interlacement graphs, *Discrete Math.* **33** (1981), 29–35, doi:10.1016/0012-365x(81)90255-7.

[12] H. de Fraysseix, A characterization of circle graphs, *European J. Combin.* **5** (1984), 223–238, doi:10.1016/s0195-6698(84)80005-0.

[13] H. de Fraysseix and P. Ossona de Mendez, On a characterization of Gauss codes, *Discrete Comput. Geom.* **22** (1999), 287–295, doi:10.1007/pl00009461.

[14] G. A. Dirac, A property of 4-chromatic graphs and some remarks on critical graphs, *J. London Math. Soc.* **27** (1952), 85–92, doi:10.1112/jlms/s1-27.1.85.

[15] R. J. Duffin, Topology of series–parallel networks, *J. Math. Anal. Appl.* **10** (1965), 303–318, doi:10.1016/0022-247x(65)90125-3.

[16] J. A. Ellis-Monaghan and I. Sarmiento, Distance hereditary graphs and the interlace polynomial, *Combin. Probab. Comput.* **16** (2007), 947–973, doi:10.1017/s0963548307008723.

[17] M. Farber, Domination, independent domination, and duality in strongly chordal graphs, *Discrete Appl. Math.* **7** (1984), 115–130, doi:10.1016/0166-218x(84)90061-1.

[18] A. Frank, Packing paths, circuits, and cuts—a survey, in: B. Korte, L. Lovász, H. J. Prömel and A. Schrijver (eds.), *Paths, flows, and VLSI-layout*, Springer, Berlin, volume 9 of *Algorithms Combin.*, pp. 47–100, 1990.

[19] A. Frank, A. V. Karzanov and A. Sebő, On integer multiflow maximization, *SIAM J. Discrete Math.* **10** (1997), 158–170, doi:10.1137/s0895480195287723.

[20] N. Garg, V. V. Vazirani and M. Yannakakis, Primal-dual approximation algorithms for integral flow and multicut in trees, *Algorithmica* **18** (1997), 3–20, doi:10.1007/bf02523685.

[21] J. F. Geelen, A. M. H. Gerards, N. Robertson and G. P. Whittle, On the excluded minors for the matroids of branch-width k, *J. Combin. Theory Ser. B* **88** (2003), 261–265, doi:10.1016/s0095-8956(02)00046-1.

[22] I. V. Hicks and N. B. McMurray, Jr., The branchwidth of graphs and their cycle matroids, *J. Combin. Theory Ser. B* **97** (2007), 681–692, doi:10.1016/j.jctb.2006.12.007.

[23] A. J. Hoffman, A. W. J. Kolen and M. Sakarovitch, Totally-balanced and greedy matrices, *SIAM J. Algebraic Discrete Methods* **6** (1985), 721–730, doi:10.1137/0606070.

[24] E. Howorka, A characterization of distance-hereditary graphs, *Quart. J. Math. Oxford Ser. (2)* **28** (1977), 417–420, doi:10.1093/qmath/28.4.417.

[25] E. Howorka, A characterization of Ptolemaic graphs; survey of results, in: *Proceedings of the Eighth Southeastern Conference on Combinatorics, Graph Theory and Computing*, 1977 pp. 355–361.

[26] T. Nishizeki, J. Vygen and X. Zhou, The edge-disjoint paths problem is NP-complete for series-parallel graphs, *Discrete Appl. Math.* **115** (2001), 177–186, doi:10.1016/s0166-218x(01)00223-2.

[27] S.-i. Oum, Rank-width and vertex-minors, *J. Combin. Theory Ser. B* **95** (2005), 79–100, doi:10.1016/j.jctb.2005.03.003.

[28] J. G. Oxley, *Matroid theory*, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1992.

[29] J. G. Oxley and D. J. A. Welsh, Tutte polynomials computable in polynomial time, *Discrete Math.* **109** (1992), 185–192, doi:10.1016/0012-365x(92)90289-r.

[30] N. Robertson and P. D. Seymour, Graph minors. X. Obstructions to tree-decomposition, *J. Combin. Theory Ser. B* **52** (1991), 153–190, doi:10.1016/0095-8956(91)90061-n.

[31] P. Rosenstiehl, A new proof of the Gauss interlace conjecture, *Adv. in Appl. Math.* **23** (1999), 3–13, doi:10.1006/aama.1999.0643.

[32] A. Schrijver, *Theory of linear and integer programming*, Wiley-Interscience Series in Discrete Mathematics, John Wiley & Sons, Ltd., Chichester, 1986.

[33] A. Schrijver, *Combinatorial optimization*, volume 24 of *Algorithms and Combinatorics*, Springer-Verlag, Berlin, 2003.

[34] B. Shtylla, L. Traldi and L. Zulli, On the realization of double occurrence words, *Discrete Math.* **309** (2009), 1769–1773, doi:10.1016/j.disc.2008.02.035.

[35] M. M. Sysło, Series-parallel graphs and depth-first search trees, *IEEE Trans. Circuits and Systems* **31** (1984), 1029–1033, doi:10.1109/tcs.1984.1085460.

[36] K. Truemper, *Matroid decomposition*, Academic Press, Inc., Boston, MA, 1992, doi:10.1016/c2013-0-11622-4.

[37] D. J. A. Welsh, *Matroid theory*, Academic Press, London-New York, 1976.

[38] H. Whitney, Non-separable and planar graphs, *Trans. Amer. Math. Soc.* **34** (1932), 339–362, doi:10.2307/1989545.

[39] X. Zhou, S. Tamura and T. Nishizeki, Finding edge-disjoint paths in partial k-trees, *Algorithmica* **26** (2000), 3–30, doi:10.1007/s004539910002.

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P1.06
https://doi.org/10.26493/2590-9770.1402.d50
(Also available at http://adam-journal.eu)

Sierpiński products of r-uniform hypergraphs

Mark Budden*

Department of Mathematics and Computer Science, Western Carolina University
Cullowhee, NC, 28723, USA

Josh Hiller

Department of Mathematics and Computer Science, Adelphi University
Garden City, NY 11530-0701, USA

Received 8 August 2020, accepted 9 February 2021, published online 4 April 2022

Abstract

If H_1 and H_2 are r-uniform hypergraphs and f is a function from the set of all $(r-1)$-element subsets of $V(H_1)$ into $V(H_2)$, then the Sierpiński product $H_1 \otimes_f H_2$ is defined to have vertex set $V(H_1) \times V(H_2)$ and hyperedges falling into two classes:

$$(g, h_1)(g, h_2) \cdots (g, h_r), \quad \text{such that } g \in V(H_1) \text{ and } h_1 h_2 \cdots h_r \in E(H_2),$$

and

$$(g_1, f(\{g_2, g_3, \ldots, g_r\}))(g_2, f(\{g_1, g_3, \ldots, g_r\})) \cdots (g_r, f(\{g_1, g_2, \ldots, g_{r-1}\})),$$

such that $g_1 g_2 \cdots g_r \in E(H_1)$. We develop the basic structure possessed by this product and offer proofs of numerous extremal properties involving connectivity, clique numbers, and strong chromatic numbers.

Keywords: Hypergraph products, cliques, chromatic numbers.

Math. Subj. Class.: 05C65, 05C15, 05C40

1 Introduction

Sierpiński graphs were first introduced in 1997 by Klavžar and Milutinović [8] stemming from their work on the Tower of Hanoi problem. Since then, numerous properties and generalizations of Sierpiński graphs have been extensively studied (e.g., see [6, 7, 9, 10, 12, 13], and [14]). Recently, Kovič, Pisanski, Zemljič, and Žitnik [11] have used Sierpiński graphs

*Corresponding author.
E-mail addresses: mrbudden@email.wcu.edu (Mark Budden), johiller@adelphi.edu (Josh Hiller)

as a motivation for a graph product structure, which they referred to as a Sierpiński product. Their introductory work on this product included proofs of the product's basic properties involving connectivity, planarity, automorphism groups, and a consideration of the product with multiple factors. The present paper seeks to generalize the Sierpiński product to the setting of r-uniform hypergraphs and to describe its structure, with an emphasis on extremal properties.

We begin with the construction of a Sierpiński product in the setting of graphs. Given graphs G_1 and G_2, and a function $f : V(G_1) \longrightarrow V(G_2)$, the Sierpiński product $G_1 \otimes_f G_2$ is defined to have vertex set $V(G_1) \times V(G_2)$ and edge set consisting of edges that fall into two classes:

$$\begin{aligned} (g,h)(g,h'), &\quad \text{such that } g \in V(G_1) \text{ and } hh' \in E(G_2), \\ (g,f(g'))(g',f(g)), &\quad \text{such that } gg' \in E(G_1). \end{aligned}$$

Edges in these classes are referred to as inner and connecting edges, respectively. Observe that regardless of the choice of function f, the graph $G_1 \otimes_f G_2$ is a subgraph of the lexicographic product $G_1[G_2]$, defined to have vertex set $V(G_1) \times V(H_2)$ and edge set

$$E(G_1[G_2]) = \{(g,h)(g',h') \mid (g = g' \text{ and } hh' \in E(G_2)) \text{ or } gg' \in E(G_1)\}.$$

Like the lexicographic product, the Sierpiński product is not commutative in general.

For each vertex $g \in V(G_1)$, the subgraph induced by the set

$$gG_2 = \{(g,h) \mid h \in V(G_2)\}$$

is isomorphic to G_2. It follows that when $|V(G_1)| = 1$, the Sierpiński product $G_1 \otimes_f G_2$ is isomorphic to G_2, regardless of the choice of f. It is also easily confirmed that when $|V(G_2)| = 1$, the function f must be constant and the Sierpiński product $G_1 \otimes_f G_2$ is isomorphic to G_1. Among these properties, it was proven in [11] that $G_1 \otimes_f G_2$ is connected if and only if G_1 and G_2 are both connected.

In Section 2, we consider a generalization of the Sierpiński product to r-uniform hypergraphs and prove several properties regarding connectivity. In Section 3, we turn our attention to clique numbers and the strong chromatic number. We note that in the case of the strong chromatic number, Theorems 3.2 and 3.4 and Corollary 3.5 are stated to include the case $r = 2$, offering new results involving the chromatic number of Sierpiński products of graphs. In Section 4, we conclude by offering some directions for future research and an alternate generalization of the Sierpiński product of r-uniform hypergraphs.

2 The Sierpiński product of r-uniform hypergraphs

Recall that an r-uniform hypergraph H consists of a nonempty vertex set $V(H)$ and a hyperedge set $E(H)$, consisting of unordered r-tuples of distinct elements from $V(H)$. For our purposes, we assume that all r-uniform hypergraphs are simple (i.e., we do not allow multi-hyperedges). When $r = 2$, this definition coincides with that of simple graphs.

If H_1 and H_2 are r-uniform hypergraphs, then denote by $\binom{V(H_1)}{r-1}$ the set of all unordered $(r-1)$-tuples of elements in $V(H_1)$. For a function

$$f : \binom{V(H_1)}{r-1} \longrightarrow V(H_2),$$

the Sierpiński product $H_1 \otimes_f H_2$ has vertex set $V(H_1) \times V(H_2)$. The hyperedges in $E(H_1 \otimes_f H_2)$ have the following forms:

$$(g, h_1)(g, h_2) \cdots (g, h_r), \quad \text{such that } g \in V(H_1) \text{ and } h_1 h_2 \cdots h_r \in E(H_2),$$

and

$$(g_1, f(\{g_2, g_3, \ldots, g_r\}))(g_2, f(\{g_1, g_3, \ldots, g_r\})) \cdots (g_r, f(\{g_1, g_2, \ldots, g_{r-1}\})),$$

such that $g_1 g_2 \cdots g_r \in E(H_1)$. Hyperedges in the first class are called inner hyperedges, while those in the second class are called connecting hyperedges. This product agrees with the definition in Section 1 in the case where $r = 2$.

For each $g \in V(H_1)$, the subhypergraph of $H_1 \otimes_f H_2$ induced by

$$gH_2 = \{(g, h) \mid h \in V(H_2)\}$$

is isomorphic to H_2. Among any r distinct $g_1 H_2, g_2 H_2, \ldots, g_r H_2$ chosen, there exists at most a single connecting hyperedge. In total, we find that $H_1 \otimes_f H_2$ contains $|V(H_1)| \cdot |E(H_2)|$ inner hyperedges and $|E(H_1)|$ connecting hyperedges.

Before considering examples and properties involving connectivity, we must recall some definitions. Recall that a Berge path of length ℓ is a sequence of $\ell + 1$ distinct vertices $v_1, v_2, \ldots, v_{\ell+1}$ and distinct hyperedges $e_1, e_2, \ldots, e_\ell$ such that $v_i, v_{i+1} \in e_i$ for all $i \in \{1, 2, \ldots, \ell\}$. We write such a path as

$$P = v_1 e_1 v_2 e_2 \cdots e_\ell v_{\ell+1}$$

and observe that although the hyperedges are distinct, each pair of hyperedges may have numerous vertices in common. A Berge path $P = v_1 e_1 v_2 e_2 \cdots e_\ell v_{\ell+1}$ forms a loose path if all vertices in P other than $v_2, v_3, \ldots, v_\ell$ have degree 1. In this case, all vertices are necessarily distinct and P has order $r + (r-1)(\ell-1)$. While we have defined Berge paths and loose paths as "stand alone" hypergraphs, we also refer to subhypergraphs isomorphic to these hypergraph constructions by the same names.

An r-uniform hypergraph H is called connected if for any distinct pair of vertices, there exists a Berge path that contains them both. An r-uniform hypergraph that is not connected is called disconnected. When an r-uniform hypergraph is connected, but the removal of any hyperedge (while retaining all vertices) disconnects it, then it is called minimally connected (e.g., see [2]). Given a Berge path $P = v_1 e_1 v_2 e_2 \cdots e_\ell v_{\ell+1}$, if there exists a hyperedge $e_{\ell+1}$ distinct from $e_1, e_2, \ldots, e_\ell$ such that $v_1, v_{\ell+1} \in e_{\ell+1}$, then we say that

$$C = v_1 e_1 v_2 e_2 \cdots e_\ell v_{\ell+1} e_{\ell+1} v_1$$

is a Berge cycle. An r-uniform hypergraph is an r-uniform tree if it is connected and does not contain any Berge cycles. Other equivalent definitions for an r-uniform tree are given in [2] and [3]. In particular, note that every r-uniform tree is minimally connected, but not every minimally connected r-uniform hypergraph is an r-uniform tree.

Example 2.1. For example, consider $K_4^{(3)}$, the complete 3-uniform hypergraph of order 4, and denote by P the 3-uniform loose path of size 2. Then if

$$f : \binom{V(K_4^{(3)})}{2} \longrightarrow V(P)$$

is any constant function that maps to a vertex of degree 1 in P, the Sierpiński product $K_4^{(3)} \otimes_f P$ is given in Figure 1. Observe that each copy of gP is isomorphic to P and the hypergraph spanned by the connecting hyperedges (dashed in Figure 1) is isomorphic to $K_4^{(3)}$.

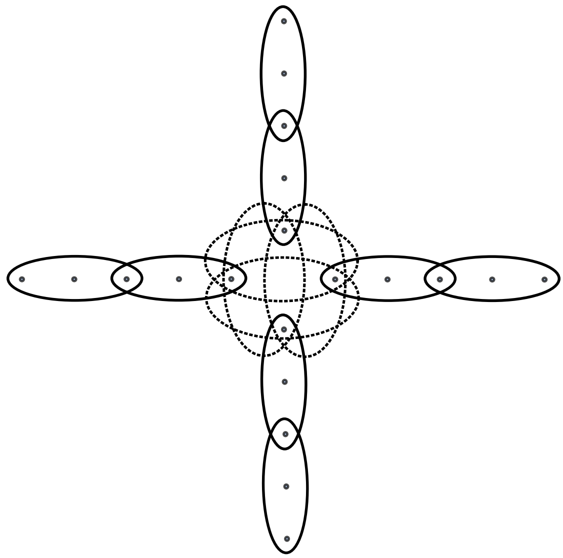


Figure 1: The Sierpiński Product $K_4^{(3)} \otimes_f P$, where P is a 3-uniform loose path of length 2 and f is a constant function whose range consists of a single vertex of degree 1 in P. The inner hyperedges are solid while the connecting hyperedges are dashed.

Example 2.2. Let C denote the 3-uniform Berge cycle of size 2 and order 4 containing exactly two vertices of degree 1. Suppose that $V(C) = \{x_1, x_2, x_3, x_4\}$, where x_1 and x_4 have degree 1. Also, let P be the loose path described in Example 2.1, with vertex set $V(P) = \{y_1, y_2, y_3, y_4, y_5\}$ such that y_3 is the unique vertex of degree 2. Define the function $f : \binom{V(C)}{2} \longrightarrow V(P)$ by

$$\begin{aligned} f(\{x_1, x_2\}) &= y_1, & f(\{x_1, x_3\}) &= y_2, & f(\{x_1, y_4\}) &= y_3, \\ f(\{x_2, x_3\}) &= y_3, & f(\{x_2, x_4\}) &= y_4, & f(\{x_3, x_4\}) &= y_5. \end{aligned}$$

Then the connecting hyperedges in $C \otimes_f P$ are given by

$$e_1 = (x_1, y_3)(x_2, y_2)(x_3, y_1) \quad \text{and} \quad e_2 = (x_2, y_5)(x_3, y_4)(x_4, y_3).$$

Since f is nonconstant, such a hypergraph becomes more difficult to illustrate. So in Figure 2, we represent the connecting hyperedges by drawing segments from each hyperedge to the vertices they include. Also, note that the vertex (x_i, y_j) is labeled ij in this figure.

Examples 2.1 and 2.2 provide illustrations of some 3-uniform Sierpiński products when the underlying hypergraphs are connected. We note that when f is a constant function (as

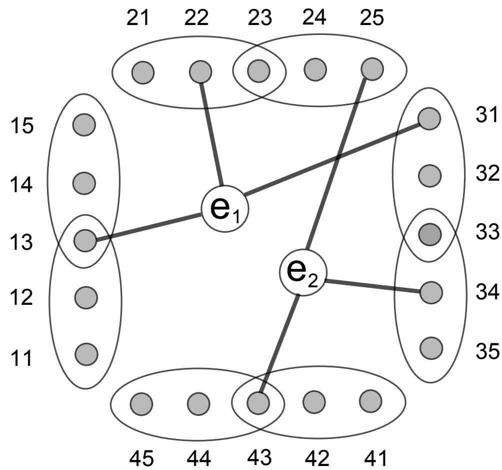


Figure 2: The Sierpiński Product $C \otimes_f P$, where C is a 3-uniform Berge cycle of size 2 and order 4 containing exactly two vertices of degree 1, P is a 3-uniform loose path of length 2, and f is the surjective function described in Example 2.2.

in Example 2.1), the resulting Sierpiński product may be considered a hypergraph generalization of a rooted product graph (for example, see [5]). In Proposition 2.10 of [11], it was shown that when G_1 and G_2 are graphs, then $G_1 \otimes_f G_2$ is connected if and only if G_1 and G_2 are connected. The following theorem considers connectivity for higher uniformity.

Theorem 2.3. *Assume that $r \geq 3$, H_1 and H_2 are r-uniform hypergraphs, and $f : \binom{V(H_1)}{r-1} \longrightarrow V(H_2)$ is a function. If H_1 and H_2 are connected, then $H_1 \otimes_f H_2$ is connected. If $H_1 \otimes_f H_2$ is connected, then H_1 is connected. If $H_1 \otimes_f H_2$ is connected and f is a constant function, then H_2 is connected.*

Proof. First, suppose that H_1 and H_2 are connected and let (g, h) and (g', h') be vertices in $H_1 \otimes_f H_2$. If $g = g'$, then there exists a Berge path that contains both (g, h) and (g, h') since gH_2 is isomorphic to H_2. Otherwise, suppose that $g \neq g'$. Since H_1 is connected, there exists a Berge path

$$P = ge_0g_1e_1g_2e_2 \cdots g_{\ell-1}e_{\ell-1}g'$$

in H_1 (and we may write $g = g_0$ and $g' = g_\ell$). Each hyperedge e_i in P corresponds with a unique hyperedge E_i in $H_1 \otimes_f H_2$. Suppose that $(g_i, h_i) \in E_{i-1}$ while $(g_i, k_i) \in E_i$. If $h_i = k_i$, then E_{i-1} and E_i are adjacent. If $h_i \neq k_i$, then there must exist a Berge path Q_i connecting (g_i, h_i) to (g_i, k_i) in g_iH_2. Thus, we are able to form a Berge path from (g, h) to (g', h') in $H_1 \otimes_f H_2$ by following along the hyperedges $E_0, E_1, \ldots, E_{\ell-1}$ and taking a detour along the Berge path Q_i in g_iH_2 whenever

$$E_{i-1} \cap g_iH_2 \neq E_i \cap g_iH_2.$$

Finally, if $(g', k) \in E_{\ell-1}$ and $k \neq h'$, then we again follow the Berge path connecting (g', k) to (g', h') in $g'H_2$. Thus, $H_1 \otimes_f H_2$ is connected. Now assume that $H_1 \otimes_f H_2$ is connected. For any pair $g, g' \in V(H_1)$, there exists a Berge path from gH_2 to $g'H_2$ in $H_1 \otimes_f H_2$ that corresponds with a Berge path from g to g' in H_1. Thus, H_1 is connected. Now assume that $H_1 \otimes_f H_2$ is connected, f is a constant function, and $k, k' \in E(H_2)$ are distinct. Then there exists a Berge path from (g, k) to (g, k') that does not contains any of the connecting hyperedges in $H_1 \otimes_f H_2$ since all such hyperedges intersect gH_2 at a single vertex. Such a Berge path necessarily corresponds with a Berge path in gH_2, from which it follows that H_2 must be connected. □

Theorem 2.3 is not as strong as in the case of graphs. This is demonstrated in Example 2.4, where a case is given in which $H_1 \otimes_f H_2$ is connected, but H_2 is disconnected.

Example 2.4. Consider the Sierpiński product $K_4^{(3)} \otimes_f 2K_3^{(3)}$, where $2K_3^{(3)}$ is the disjoint union of two 3-uniform hyperedges and $f : \binom{V(K_4^{(3)})}{2} \longrightarrow V(2K_3^{(3)})$ by

$$\begin{aligned} f(\{x_1, x_2\}) &= y_6, & f(\{x_1, x_3\}) &= y_1, & f(\{x_1, y_4\}) &= y_1, \\ f(\{x_2, x_3\}) &= y_1, & f(\{x_2, x_4\}) &= y_6, & f(\{x_3, x_4\}) &= y_6. \end{aligned}$$

Here, $V(K_4^{(3)}) = \{x_1, x_2, x_3, x_4\}$ and $2K_3^{(3)}$ consists of the hyperedges $y_1y_2y_3$ and $y_4y_5y_6$. The connecting hyperedges are given by

$$\begin{aligned} e_1 &= (x_1, y_1)(x_2, y_1)(x_3, y_6) \\ e_2 &= (x_1, y_6)(x_2, y_1)(x_4, y_6) \\ e_3 &= (x_1, y_6)(x_3, y_1)(x_4, y_1) \\ e_4 &= (x_2, y_6)(x_3, y_6)(x_4, y_1). \end{aligned}$$

From Figure 3, it is clear that $K_4^{(3)} \otimes_f 2K_3^{(3)}$ is connected even though $2K_3^{(3)}$ is disconnected.

Consider the case where $H_1 \otimes_f H_2$ is minimally connected and H_2 is assumed to be connected. Then by Theorem 2.3, H_1 is also connected. When an inner hyperedge of $H_1 \otimes_f H_2$ is removed, the removal of the corresponding hyperedge in H_2 disconnects H_2. When a connecting hyperedge is removed, the removal of the corresponding hyperedge in H_1 disconnects H_1. We obtain the following corollary.

Corollary 2.5. *Assume that $r \geq 3$, H_1 and H_2 are r-uniform hypergraphs, and $f : \binom{V(H_1)}{r-1} \longrightarrow V(H_2)$ is a function. If $H_1 \otimes_f H_2$ is minimally connected and H_2 is connected, then H_1 and H_2 are minimally connected.*

In the more restrictive class of r-uniform trees, we obtain the following theorem.

Theorem 2.6. *Assume that $r \geq 3$, H_1 and H_2 are r-uniform hypergraphs, and $f : \binom{V(H_1)}{r-1} \longrightarrow V(H_2)$ is a function. If $H_1 \otimes_f H_2$ is an r-uniform tree and H_2 is connected, then, H_2 is an r-uniform tree.*

Proof. Assume that H_2 is connected. Since $H_1 \otimes_f H_2$ contains a subhypergraph isomorphic to H_2, $H_1 \otimes_f H_2$ will contain a Berge cycle whenever H_2 contains a Berge cycle. It follows that H_2 is an r-uniform tree whenever $H_1 \otimes_f H_2$ is an r-uniform tree. □

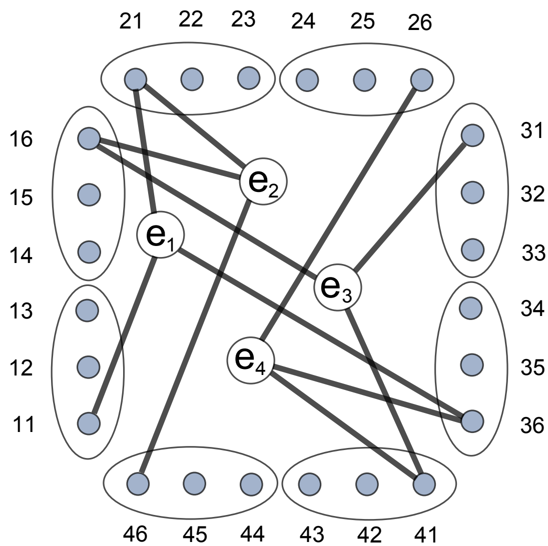


Figure 3: The Sierpiński Product $K_4^{(3)} \otimes_f 2K_3^{(3)}$, where f is the function described in Example 2.4. Observe that $K_4^{(3)} \otimes_f 2K_3^{(3)}$ is connected even though $2K_3^{(3)}$ is disconnected.

3 Cliques and strong chromatic numbers

In this section, we focus on the clique numbers and chromatic numbers of Sierpiński products. These parameters serve as measures of connectivity and they play important roles in various extremal aspects of the study of hypergraphs. If H is any r-uniform hypergraph, then the clique number $\omega(H)$ is the maximum order of a complete subhypergraph of H. When $r = 2$, it is well-known that $\omega(G_1[G_2]) = \omega(G_1)\omega(G_2)$ (e.g., see [4]), and since $G_1 \otimes_f G_2$ is a subgraph of $G_1[G_2]$ for all f, it follows that

$$\omega(G_1 \otimes_f G_2) \leq \omega(G_1)\omega(G_2).$$

When $r \geq 3$, we obtain the following theorem.

Theorem 3.1. *Let $r \geq 3$. If H_1 and H_2 are r-uniform hypergraphs and $f : \binom{V(H_1)}{r-1} \longrightarrow V(H_2)$ is a function, then*

$$\omega(H_1 \otimes_f H_2) \leq \max\{\omega(H_1), \omega(H_2)\}.$$

If $\omega(H_2) \geq \omega(H_1)$, then

$$\omega(H_1 \otimes_f H_2) = \omega(H_2).$$

If f is a constant function, then

$$\omega(H_1 \otimes_f H_2) = \max\{\omega(H_1), \omega(H_2)\}.$$

Proof. The statement

$$\omega(H_1 \otimes_f H_2) \leq \max\{\omega(H_1), \omega(H_2)\}$$

follows from Theorem 3 of [1], where it was proved that the lexicographic product satisfies

$$\omega(H_1[H_2]) = \max\{\omega(H_1), \omega(H_2)\},$$

and the observation that $H_1 \otimes_f H_2$ is a subhypergraph of $H_1[H_2]$. Since each gH_2 contained in $H_1 \otimes_f H_2$ is isomorphic to H_2, we find that $H_1 \otimes_f H_2$ contains a complete subhypergraph at least as large as a clique in H_2. It follows that

$$\omega(H_1 \otimes_f H_2) = \omega(H_2)$$

whenever $\omega(H_2) \geq \omega(H_1)$. Finally, if f is a constant function, then the subhypergraph induced by

$$H_1 h = \{(g, h) \mid g \in V(H_1)\}$$

is isomorphic to H_1 for the unique vertex h in the image of f. So, $H_1 \otimes_f H_2$ contains complete subgraphs of orders equal to both $\omega(H_1)$ and $\omega(H_2)$, giving us

$$\omega(H_1 \otimes_f H_2) = \max\{\omega(H_1), \omega(H_2)\}$$

in this case. □

In the setting of r-uniform hypergraphs, there are many ways to generalize chromatic numbers. In this paper, we will focus on the strong chromatic number of an r-uniform hypergraph H. First, define a *strong proper vertex coloring* of an r-uniform hypergraph H to be a map

$$c : V(H) \longrightarrow \{1, 2, \ldots, n\}$$

such that no two adjacent vertices in H receive the same color. Then the least n for which a strong proper vertex coloring exists is called the *strong chromatic number* of H, and is denoted $\chi_s(H)$. Our reasoning for focusing on this generalization is due to the relationship between the strong chromatic number and the existence of certain hypergraph homomorphisms. Recall that if H_1 and H_2 are two r-uniform hypergraphs, then a *homomorphism* is a function $\phi : V(H_1) \longrightarrow V(H_2)$ such that if $x_1 x_2 \cdots x_r \in E(H_1)$, then $\phi(x_1)\phi(x_2)\cdots\phi(x_r) \in E(H_2)$.

For any strong proper vertex coloring $c : V(H) \longrightarrow \{1, 2, \ldots, n\}$, there is a natural homomorphism $\phi : V(H) \longrightarrow V(K_n^{(r)})$ given by mapping each vertex $h \in V(H)$ to a vertex $\phi(h) \in V(K_n^{(r)})$ identified with the color class of h under c. This identification of strong proper vertex colorings of r-uniform hypergraphs with homomorphisms leads to a useful property. Specifically, if H_1 and H_2 are any r-uniform hypergraphs and if $\phi : V(H_1) \longrightarrow V(H_2)$ is a homomorphism, then

$$\chi_s(H_1) \leq \chi_s(H_2), \tag{3.1}$$

since any strong proper vertex coloring of H_2 can be applied to H_1 under ϕ.

Theorem 3.2. *For $r \geq 2$, let H_1 and H_2 be r-uniform hypergraphs such that $\chi_s(H_2) = n$. Let $\phi : V(H_2) \longrightarrow V(K_n^{(r)})$ be a homomorphism. For any function $f : \binom{V(H_1)}{r-1} \longrightarrow V(H_2)$,*

$$\chi_s(H_1 \otimes_f H_2) \leq \chi_s(H_1 \otimes_{f^*} K_n^{(r)}),$$

where $f^* := \phi \circ f$.

Proof. Let $c : V(H_2) \longrightarrow \{1, 2, \dots, n\}$ be a strong proper vertex coloring of H_2 such that $\chi_s(H_2) = n$. Note that c is necessarily surjective. Such a coloring naturally extends to the surjective homomorphism $\phi : V(H_2) \longrightarrow K_n^{(r)}$ given by sending each vertex in $h \in V(H_2)$ to a vertex in $K_n^{(r)}$ identified with the color class of h under c. Consider the map

$$\phi^* : V(H_1 \otimes_f H_2) \longrightarrow V(H_1 \otimes_{f^*} K_n^{(r)})$$

given by $\phi^*(g, h) = (g, \phi(h))$. We claim that ϕ^* is a homomorphism. To prove this claim, let

$$(g_1, h_1)(g_2, h_2) \cdots (g_r, h_r) \in E(H_1 \otimes_f H_2)$$

and consider

$$(g_1, \phi(h_1))(g_2, \phi(h_2)) \cdots (g_r, \phi(h_r)) \in E(H_1 \otimes_{f^*} K_n^{(r)}).$$

Then either $g_1 = g_2 = \cdots = g_r$ (in which case, $\phi(h_1)\phi(h_2) \cdots \phi(h_r) \in E(K_n^{(r)})$ since $h_1 h_2 \cdots h_r \in E(H_2)$ and ϕ is a homomorphism) or $g_1 g_2 \cdots g_r \in E(H_1)$ and

$$\begin{aligned}
\phi(h_1) &= \phi(f(\{g_2, g_3, \dots, g_r\})) = f^*(\{g_2, g_3, \dots, g_r\}) \\
\phi(h_2) &= \phi(f(\{g_1, g_3, \dots, g_r\})) = f^*(\{g_1, g_3, \dots, g_r\}) \\
&\vdots \\
\phi(h_r) &= \phi(f(\{g_1, g_2, \dots, g_{r-1}\})) = f^*(\{g_1, g_2, \dots, g_{r-1}\}).
\end{aligned}$$

It follows that ϕ^* is a homomorphism, from which we conclude that

$$\chi_s(H_1 \otimes_f H_2) \leq \chi_s(H_1 \otimes_{f^*} K_n^{(r)})$$

by (3.1). □

Note that in the previous theorem, the case $r = 2$ is included. In this case, χ_s is the usual chromatic number for graphs. We find that in general, Theorem 3.2 is the strongest statement that can be made, as the following example demonstrates a case where a strict inequality is satisfied.

Example 3.3. Consider the complete 3-uniform hypergraph $K_4^{(3)}$ with vertex set $V(K_4^{(3)}) = \{x_1, x_2, x_3, x_4\}$ and the 3-uniform loose path P of length 2 with vertex set $V(P) = \{y_1, y_2, y_3, y_4, y_5\}$, where y_3 is the unique vertex in P with degree 2. Let $f : \binom{V(K_4^{(3)})}{2} \longrightarrow V(P)$ be the function

$$\begin{aligned}
&f(\{x_1, x_2\}) = y_1, \qquad f(\{x_1, x_3\}) = y_2, \qquad f(\{x_1, y_4\}) = y_3, \\
&f(\{x_2, x_3\}) = y_4, \qquad f(\{x_2, x_4\}) = y_5, \qquad f(\{x_3, x_4\}) = y_5.
\end{aligned}$$

Then the Sierpiński product $K_4^{(3)} \otimes_f P$ is given in Figure 4, with vertex (x_i, y_i) labelled ij. The connecting hyperedges are given by

$$\begin{aligned}
e_1 &= (x_1, y_4)(x_2, y_2)(x_3, y_1) \\
e_2 &= (x_1, y_5)(x_2, y_3)(x_4, y_1) \\
e_3 &= (x_1, y_5)(x_3, y_3)(x_4, y_2) \\
e_4 &= (x_2, y_5)(x_3, y_5)(x_4, y_4).
\end{aligned}$$

Since every strong proper vertex coloring of a hypergraph containing at least one hyperedge requires at least 3 colors, the coloring given in Figure 4 implies that $\chi_s(K_4^{(3)} \otimes_f P) = 3$. Note that $\chi_s(P) = 3$, and we can identify a strong proper vertex coloring of P with the

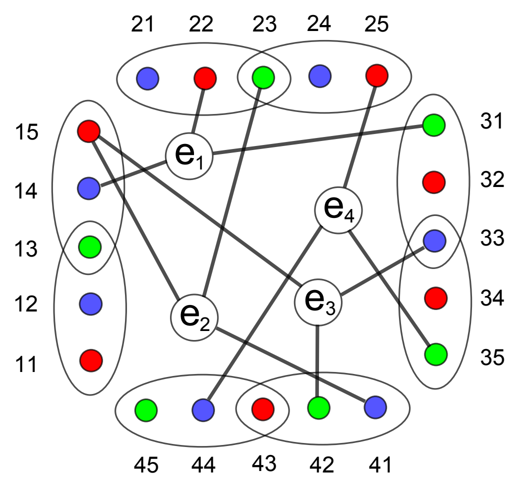


Figure 4: The Sierpiński product $K_4^{(3)} \otimes_f P$, where P is a 3-uniform loose path of length 2 and f is the function given in Example 3.3. The strong proper vertex coloring given shows that this hypergraph has a strong chromatic number of 3.

homomorphism $\phi : V(P) \longrightarrow K_3^{(3)}$ that maps

$$\phi(y_1) = \phi(y_5) = z_1, \quad \phi(y_2) = \phi(y_4) = z_2, \quad \text{and} \quad \phi(y_3) = z_3,$$

where $V(K_3^{(3)}) = \{z_1, z_2, z_3\}$. Then $f^* := \phi \circ f$ and the connecting hyperedges in $K_4^{(3)} \otimes_{f^*} K_3^{(3)}$ are given by

$$\begin{aligned} e'_1 &= (x_1, z_2)(x_2, z_2)(x_3, z_1) \\ e'_2 &= (x_1, z_1)(x_2, z_3)(x_4, z_1) \\ e'_3 &= (x_1, z_1)(x_3, z_3)(x_4, z_2) \\ e'_4 &= (x_2, z_1)(x_3, z_1)(x_4, z_2). \end{aligned}$$

The resulting hypergraph $K_4^{(3)} \otimes_{f^*} K_3^{(3)}$ is given in Figure 5.

To obtain a strong proper vertex coloring, we begin by focusing on the connecting hyperedges e'_2 and e'_3. Without loss of generality, suppose that (x_1, z_1) is red and (x_4, z_2) is blue. This forces (x_4, z_1) and (x_3, z_3) to be green and (x_2, z_3) to be blue. Then (x_3, z_1) must be red and (x_2, z_1) must be green. At this point, no color is available for (x_2, z_2) as (x_2, z_1) and (x_2, z_3) require it to be different from blue and green, but e'_1 already contains a red vertex. So, $\chi_s(K_4^{(3)} \otimes_{f^*} K_3^{(3)}) \geq 4$, and one can continue with this process to obtain

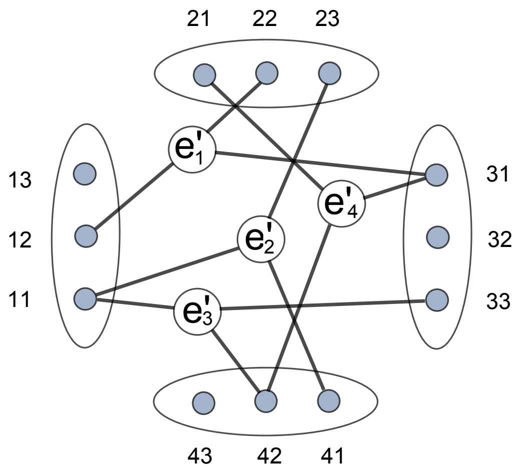


Figure 5: The Sierpiński product $K_4^{(3)} \otimes_{f^*} K_3^{(3)}$ given in Example 3.3.

a strong proper vertex 4-coloring of $K_4^{(3)} \otimes_{f^*} K_3^{(3)}$, showing that $\chi_s(K_4^{(3)} \otimes_{f^*} K_3^{(3)}) = 4$. Thus, our example demonstrates that there are cases where equality is not obtained in Theorem 3.2.

While we can not be precise with the evaluation of the strong chromatic number in general, an exact evaluation can be found when f is assumed to be constant.

Theorem 3.4. *Let $r \geq 2$ and suppose that H_1 and H_2 are r-uniform hypergraphs. If $f : \binom{V(H_1)}{r-1} \longrightarrow V(H_2)$ is a constant function, then*

$$\chi_s(H_1 \otimes_f H_2) = \max\{\chi_s(H_1), \chi_s(H_2)\}.$$

Proof. When $f : \binom{V(H_1)}{r-1} \longrightarrow V(H_2)$ is a constant function, the subhypergraph spanned by the connecting hyperedges is isomorphic to H_1 and each gH_2 is isomorphic to H_2. It follows that

$$\chi_s(H_1 \otimes_f H_2) \geq \max\{\chi_s(H_1), \chi_s(H_2)\}.$$

To prove the opposite inequality, observe that all connecting hyperedges include at most one vertex from each gH_2. Begin with a strong proper vertex coloring of the vertices spanned by the connecting hyperedges using at most $\chi_s(H_1)$. The specific color assigned for at most one vertex in each gH_2 does not affect the number of colors needed to form a strong proper vertex coloring of each gH_2. Hence, it is possible to color $H_1 \otimes_f H_2$ using $\max\{\chi_s(H_1), \chi_s(H_2)\}$ colors, completing the proof. □

An immediate consequence of this theorem is the following corollary.

Corollary 3.5. *Let $r \geq 2$ and suppose that H_1 and H_2 are r-uniform hypergraphs with $\chi_s(H_2) = n$. If $f : \binom{V(H_1)}{r-1} \longrightarrow V(H_2)$ is a constant function, then*

$$\chi_s(H_1 \otimes_f H_2) = \chi_s(H_1 \otimes_{f^*} K_n^{(r)}).$$

4 Conclusion

We conclude our investigation of Sierpiński products of r-uniform hypergraphs by identifying numerous directions for future study. Our primary focus has been on measures of connectivity, but there are many additional parameters (e.g., independence numbers, diameters, etc...) and applications worthy of inquiry. As subhypergraphs of lexicographic products, Sierpiński products may offer new results in Ramsey theory or bounds for certain Turán numbers (e.g., see [1]). Several of the topics studied in Kovič, Pisanski, Zemljič, and Žitnik's paper [11], such as automorphism groups and products involving more than two factors, have not been considered here and should be considered for hypergraphs.

Finally, the generalization of Sierpiński products to r-uniform hypergraphs that we have used seemed like the natural choice, but there are other ways in which one can make such a generalization. For example, let H_1 and H_2 be r-uniform hypergraphs. For a function $f : V(H_1) \longrightarrow V(H_2)$, define the product $H_1 \otimes^f H_2$ to have vertex set $V(H_1) \times V(H_2)$. The hyperedges in $E(H_1 \otimes^f H_2)$ have the following forms:

$$(g, h_1)(g, h_2) \cdots (g, h_r), \quad \text{such that } g \in V(H_1) \text{ and } h_1 h_2 \cdots h_r \in E(H_2),$$

and

$$(g_1, f(\pi(g_1)))(g_2, f(\pi(g_2))) \cdots (g_r, f(\pi(g_r))),$$

such that $g_1 g_2 \cdots g_r \in E(H_1)$ and π is any nontrivial permutation on $\{g_1, g_2, \ldots, g_r\}$. Observe that we have denoted this generalization of the Sierpiński product by writing f as a superscript rather than a subscript. Perhaps many of the results proved in this paper hold for this product as well. We leave its investigation for future work.

ORCID iDs

Mark Budden https://orcid.org/0000-0002-4065-6317
Josh Hiller https://orcid.org/0000-0001-5747-4061

References

[1] M. Bruce, M. Budden and J. Hiller, Lexicographic products of r-uniform hypergraphs and some applications to hypergraph Ramsey theory, *Australas. J. Comb.* **70** (2018), 390–401, https://ajc.maths.uq.edu.au/?page=get_volumes&volume=70.

[2] M. Budden, J. Hiller and A. Penland, Minimally connected r-uniform hypergraphs, *Australas. J. Comb.* **82** (2022), 1–20, https://ajc.maths.uq.edu.au/?page=get_volumes&volume=82.

[3] M. Budden and A. Penland, Trees and n-good hypergraphs, *Australas. J. Comb.* **72** (2018), 329–349, https://ajc.maths.uq.edu.au/?page=get_volumes&volume=72.

[4] D. Geller and S. Stahl, The chromatic number and other functions of the lexicographic product, *J. Comb. Theory Ser. B* **19** (1975), 87–95, doi:10.1016/0095-8956(75)90076-3.

[5] C. D. Godsil and B. D. McKay, A new graph product and its spectrum, *Bull. Austral. Math. Soc.* **18** (1978), 21–28, doi:10.1017/s0004972700007760.

[6] A. M. Hinz, S. Klavžar and S. S. Zemljič, Sierpiński graphs as spanning subgraphs of Hanoi graphs, *Cent. Eur. J. Math.* **11** (2013), 1153–1157, doi:10.2478/s11533-013-0227-7.

[7] M. Jakovac and S. Klavžar, Vertex-, edge-, and total-colorings of Sierpiński-like graphs, *Discrete Math.* **309** (2009), 1548–1556, doi:10.1016/j.disc.2008.02.026.

[8] S. Klavžar and U. Milutinović, Graphs $S(n, k)$ and a variant of the Tower of Hanoi problem, *Czechoslov. Math. J.* **47(122)** (1997), 95–104, doi:10.1023/a:1022444205860.

[9] S. Klavžar, U. Milutinović and C. Petr, 1-perfect codes in Sierpiński graphs, *Bull. Austral. Math. Soc.* **66** (2002), 369–384, doi:10.1017/s0004972700040235.

[10] S. Klavžar and S. S. Zemljič, On distances in Sierpiński graphs: almost-extreme vertices and metric dimension, *Appl. Anal. Discrete Math.* **7** (2013), 72–82, doi:10.2298/aadm130109001k.

[11] J. Kovič, T. Pisanski, S. Zemljič and A. Žitnik, The Sierpiński product of graphs, *Ars Math. Contemp.* (2022), doi:10.26493/1855-3974.1970.29e.

[12] D. Parisse, On some metric properties of the Sierpiński graphs $S(n, k)$, *Ars Comb.* **90** (2009), 145–160.

[13] B. Xue, L. Zuo and G. Li, The Hamiltonicity and path t-coloring of Sierpiński-like graphs, *Discrete Appl. Math.* **160** (2012), 1822–1836, doi:10.1016/j.dam.2012.03.022.

[14] B. Xue, L. Zuo, G. Wang and G. Li, Shortest paths in Sierpiński graphs, *Discrete Appl. Math.* **162** (2014), 314–321, doi:10.1016/j.dam.2013.08.029.

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P1.07
https://doi.org/10.26493/2590-9770.1373.60a
(Also available at http://adam-journal.eu)

Groups for which it is easy to detect graphical regular representations*

Dave Witte Morris†, Joy Morris

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta. T1K 3M4, Canada

Gabriel Verret‡

Department of Mathematics, The University of Auckland, Private Bag 92019, Auckland 1142, New Zealand

Received 08 July 2020, accepted 09 December 2020, published online 4 April 2022

Abstract

We say that a finite group G is *DRR-detecting* if, for every subset S of G, either the Cayley digraph $\operatorname{Cay}(G, S)$ is a digraphical regular representation (that is, its automorphism group acts regularly on its vertex set) or there is a nontrivial group automorphism φ of G such that $\varphi(S) = S$. We show that every nilpotent DRR-detecting group is a p-group, but that the wreath product $\mathbb{Z}_p \wr \mathbb{Z}_p$ is not DRR-detecting, for every odd prime p. We also show that if G_1 and G_2 are nontrivial groups that admit a digraphical regular representation and either $\gcd\big(|G_1|, |G_2|\big) = 1$, or G_2 is not DRR-detecting, then the direct product $G_1 \times G_2$ is not DRR-detecting. Some of these results also have analogues for graphical regular representations.

Keywords: Cayley graph, GRR, DRR, automorphism group, normalizer.

Math. Subj. Class.: 05C25,20B05

*This work was supported in part by the Natural Science and Engineering Research Council of Canada (grant RGPIN-2017-04905). The authors thank two anonymous referees for helpful comments.

†Corresponding author.

‡The author is grateful to the N.Z. Marsden Fund for its support (via grant UOA1824).

E-mail address: dave.morris@uleth.ca (Dave Witte Morris), joy.morris@uleth.ca (Joy Morris), g.verret@auckland.ac.nz (Gabriel Verret)

1 Introduction

All groups and graphs in this paper are finite. Recall [1] that a digraph Γ is said to be a *digraphical regular representation (DRR)* of a group G if the automorphism group of Γ is isomorphic to G and acts regularly on the vertex set of Γ. If a DRR of G happens to be a graph, then it is also called a *graphical regular representation (GRR)* of G. Other terminology and notation can be found in Section 2.

It is well known that if Γ is a GRR (or DRR) of G, then Γ must be a Cayley graph (or Cayley digraph, respectively), so there is a subset S of G such that $\Gamma \cong \mathrm{Cay}(G, S)$ (and S is inverse-closed if Γ is a graph). It is traditional [5, p. 243] to let

$$\mathrm{Aut}(G, S) = \{\, \varphi \in \mathrm{Aut}(G) \mid \varphi(S) = S \,\}.$$

Since $\mathrm{Aut}(G, S) \subseteq \mathrm{Aut}\big(\mathrm{Cay}(G, S)\big)$, it is obvious (and well known) that if $\mathrm{Aut}(G, S)$ is nontrivial, then $\mathrm{Cay}(G, S)$ is not a GRR (or DRR). In this paper, we discuss groups for which the converse holds:

Definition 1.1. We say that a group G is *GRR-detecting* if, for every inverse-closed subset S of G, $\mathrm{Aut}(G, S) = \{1\}$ implies that $\mathrm{Cay}(G, S)$ is a GRR. Similarly, a group G is *DRR-detecting* if for every subset S of G, $\mathrm{Aut}(G, S) = \{1\}$ implies that $\mathrm{Cay}(G, S)$ is a DRR.

Remark 1.2. Every Cayley graph is a Cayley digraph, so every DRR-detecting group is GRR-detecting.

Definition 1.3. We say that a Cayley (di)graph $\Gamma = \mathrm{Cay}(G, S)$ on a group G *witnesses that G is not GRR-detecting* (respectively, not DRR-detecting) if $\mathrm{Aut}(G, S) = \{1\}$ but Γ is not a GRR (respectively, not a DRR) for G.

An important class of DRR-detecting groups was found by Godsil. His result actually deals with vertex-transitive digraphs, rather than only the more restrictive class of Cayley graphs, but here is a special case of his result in our terminology:

Theorem 1.4 (Godsil, cf. [5, Corollary 3.9])**.** Let G be a p-group and let $\mathbb{Z}_p$ be the cyclic group of order p. If G admits no homomorphism onto the wreath product $\mathbb{Z}_p \wr \mathbb{Z}_p$ then G is DRR-detecting (and therefore also GRR-detecting).

Since $\mathbb{Z}_p \wr \mathbb{Z}_p$ is nonabelian, the following statement is an immediate consequence:

Corollary 1.5. Every abelian p-group is DRR-detecting (and therefore also GRR-detecting).

Remark 1.6. It is obvious (without reference to Theorem 1.4) that most abelian p-groups are GRR-detecting. Indeed, it is well known that every abelian group is GRR-detecting (unless it is an elementary abelian 2-group), because the nontrivial group automorphism $x \mapsto x^{-1}$ is an automorphism of $\mathrm{Cay}(G, S)$.

The following result shows that the bound in Godsil's theorem is sharp, in the sense that $\mathbb{Z}_p \wr \mathbb{Z}_p$ cannot be replaced with a larger p-group (when p is odd):

Theorem 1.7. If p is an odd prime, then the wreath product $\mathbb{Z}_p \wr \mathbb{Z}_p$ is not GRR-detecting (and is therefore also not DRR-detecting).

Remark 1.8. The conclusion of Theorem 1.7 is not true for $p = 2$, because $\mathbb{Z}_2 \wr \mathbb{Z}_2$ is GRR-detecting. This is a special case of the fact that if a group has no GRR, then it is GRR-detecting [4, Theorem 1.4].

The following two results provide additional examples, by showing that direct products often yield groups that are not DRR-detecting:

Theorem 1.9. If G_1 and G_2 are nontrivial groups that admit a DRR (a GRR, respectively) and $\gcd\big(|G_1|, |G_2|\big) = 1$, then $G_1 \times G_2$ is not DRR-detecting (not GRR-detecting, respectively).

Theorem 1.10. If G_1 admits a DRR (a GRR, respectively) and G_2 is not DRR-detecting (not GRR-detecting, respectively), then $G_1 \times G_2$ is not DRR-detecting (not GRR-detecting, respectively).

These two results are the main ingredients in the proof of the following theorem:

Theorem 1.11. Every nilpotent DRR-detecting group is a p-group.

Remark 1.12. The phrase "DRR-detecting" in Theorem 1.11 cannot be replaced with "GRR-detecting." For example, every abelian group is GRR-detecting (unless it is an elementary abelian 2-group), as was pointed out in Remark 1.6.

Here is an outline of the paper. A few definitions and basic results are recalled in Section 2. Theorem 1.7 is proved in Section 3. A generalization of Theorem 1.9 is proved in Section 4, by using wreath products of digraphs. In Section 5, we recall some fundamental facts about cartesian products of digraphs and use them to prove Theorem 1.10. Theorem 1.11 is proved in Section 6.

2 Preliminaries

Definition 2.1. Recall that if S is a subset of a group G, then the *Cayley digraph of G (with respect to the connection set S)* is the digraph $\mathrm{Cay}(G, S)$ whose vertex set is G, such that there is a directed edge from g_1 to g_2 if and only if $g_2 = sg_1$ for some $s \in S$. If S is closed under inverses, then $Cay(G, S)$ is a graph, and is called a *Cayley graph*.

See Remark 4.4 for a general definition of the wreath product of two groups. The following special case is less complicated:

Definition 2.2. Let $\mathbb{Z}_p \wr \mathbb{Z}_p = \mathbb{Z}_p \ltimes (\mathbb{Z}_p)^p$, where $\mathbb{Z}_p$ acts on $(\mathbb{Z}_p)^p$ by cyclically permuting the coordinates: for $(v_1, v_2, \ldots, v_p) \in (\mathbb{Z}_p)^p$ and $g \in \mathbb{Z}_p$, we have

$$(v_1, v_2, \ldots, v_p)^g = (v_{g+1}, v_{g+2}, \ldots, v_p, v_1, v_2, \ldots, v_g).$$

We will use the following well-known results.

Theorem 2.3 (Babai [1, Theorem 2.1])**.** If a finite group does not admit a DRR, then it is isomorphic to

$$Q_8,\ (\mathbb{Z}_2)^2,\ (\mathbb{Z}_2)^3,\ (\mathbb{Z}_2)^4, \text{ or } (\mathbb{Z}_3)^2,$$

where Q_8 is the quaternion group of order 8, which means

$$Q_8 = \langle\, i, j, k \mid i^2 = j^2 = k^2 = -1,\ ij = k \,\rangle.$$

Lemma 2.4. Let $\widehat{G}$ be the right regular representation of G. Then:

1. $\widehat{G}$ is contained in $\mathrm{Aut}\big(\mathrm{Cay}(G,S)\big)$ for every subset S of G.
2. The normalizer of $\widehat{G}$ in $\mathrm{Aut}\big(\mathrm{Cay}(G,S)\big)$ is $\mathrm{Aut}(G,S) \ltimes \widehat{G}$.

The latter has the following simple consequence:

Lemma 2.5. If Γ is a Cayley digraph on G (a Cayley graph on G, respectively), then Γ witnesses that G is not DRR-detecting (not GRR-detecting, respectively) if and only if the regular representation of G is a proper self-normalizing subgroup of $\mathrm{Aut}(\Gamma)$.

3 Proof of Theorem 1.7

Let p be an odd prime. In this section, we show that $\mathbb{Z}_p \wr \mathbb{Z}_p$ is not GRR-detecting. (This proves Theorem 1.7.) To do this, we will construct a Cayley graph Γ on $\mathbb{Z}_p \wr \mathbb{Z}_p$ such that Γ is not a GRR, but the regular representation of $\mathbb{Z}_p \wr \mathbb{Z}_p$ is self-normalizing in $\mathrm{Aut}(\Gamma)$. In order to construct this graph, we first construct a certain group G that properly contains $\mathbb{Z}_p \wr \mathbb{Z}_p$. We will then define Γ in such a way that G is contained in $\mathrm{Aut}(\Gamma)$.

Let $A \cong \mathbb{Z}_p$ be a cyclic group of order p, and choose an irreducible representation of A on a vector space $Q \cong (\mathbb{Z}_2)^n$ over the finite field with 2 elements, such that $n \geq 2$. Now construct the corresponding semidirect product $A \ltimes Q$, which is a nonabelian group of order $2^n p$.

Choose a nontrivial 1-dimensional representation $\chi\colon Q \to \{\pm 1\} \subseteq \mathbb{Z}_p^\times$ (where $\mathbb{Z}_p^\times$ denotes the multiplicative group of nonzero elements of $\mathbb{Z}_p$), and induce it to a representation of $A \ltimes Q$ on a vector space V over $\mathbb{Z}_p$ [10, §3.3, pp. 28–30]. Since Q has index p in $A \ltimes Q$, the vector space V has dimension p, so $V \cong (\mathbb{Z}_p)^p$. Let

$$G = (A \ltimes Q) \ltimes V.$$

Since the representation of $A \ltimes Q$ on V is induced from a one-dimensional representation of the normal subgroup Q, the restriction to Q decomposes as a direct sum of one-dimensional representations: $V = V_1 \oplus \cdots \oplus V_p$, where each V_i is a subgroup of order p that is normalized by Q (cf. [10, Proposition 22, p. 58]). (More precisely, for each $i \in \{1,\ldots,p\}$, there is some $a \in A$, such that the representation of Q on V_i is given by χ^a, where $\chi^a(g) = \chi(g^{a^{-1}})$ for $g \in Q$, and $g^h = h^{-1}gh$ for $g,h \in G$.) Note that, since A normalizes Q, it must (cyclically) permute the Q-irreducible summands $V_1,\ldots,V_p$, so the Sylow p-subgroup $A \ltimes V$ of G is isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$.

Fix a nonidentity element a of A. Since A normalizes Q, we know that the coset Qa is fixed by the action of Q on the space $Q\backslash G$ of right cosets of Q. Also fix some nonzero $v_1 \in V_1$. Then, for each $i \in \{1,\ldots,p\}$, let $v_i = v_1^{a^{i-1}}$, so v_i is a nonzero element of V_i, and define $z = v_1 + v_2 + \cdots + v_p$, so z is a generator of the center $\mathrm{Z}(A \ltimes V)$.

Now let

$$S = \big(\langle v_1, v_2\rangle \smallsetminus \langle v_1\rangle\big) \cup (a\, z^Q)^{\pm 1} \subseteq A \ltimes V \subseteq G,$$

and let

$$\Gamma = \mathrm{Cay}(A \ltimes V, S).$$

Since Q normalizes $\langle v_1\rangle$ and $\langle v_2\rangle$, and fixes the coset Qa in $Q\backslash G$, it is clear that $SQ = QS$. Therefore, after identifying the vertex set $A \ltimes V$ of Γ with $Q\backslash QAV = Q\backslash G$ in the natural way, we have $G \subseteq \mathrm{Aut}(\Gamma)$, via the natural action of G on $Q\backslash G$. (Note that the action of G on $Q\backslash G$ is faithful, because Q does not contain any nontrivial, normal subgroup of G. Otherwise, since the action of A on Q is irreducible, the entire subgroup Q would have to be normal, which would mean that Q acts trivially on $Q\backslash G$. But this is false, because the representation of Q on V is nontrivial.) So Γ is not a GRR.

Therefore, in order to show that $\mathbb{Z}_p \wr \mathbb{Z}_p \cong A \ltimes V$ is not GRR-detecting, it will suffice to show that $\operatorname{Aut}(A \ltimes V, S)$ is trivial. To this end, let φ be an automorphism of $A \ltimes V$ that fixes S. We will show that φ is trivial.

Since V is characteristic in $A \ltimes V$ (for example, it is the only abelian subgroup of order p^p), we know that

$$\varphi(V \cap S) = V \cap S = \langle v_1, v_2 \rangle \smallsetminus \langle v_1 \rangle \subseteq \langle v_1, v_2 \rangle.$$

So

$$\varphi\big(\langle v_1, v_2 \rangle\big) = \varphi\big(\langle v_1 v_2, v_2 \rangle\big) = \langle \varphi(v_1 v_2), \varphi(v_2) \rangle \subseteq \langle \varphi(V \cap S) \rangle \subseteq \langle v_1, v_2 \rangle.$$

Since φ is injective, we conclude that φ fixes $\langle v_1, v_2 \rangle$ (setwise). Then φ also fixes $\langle v_1, v_2 \rangle \smallsetminus S = \langle v_1 \rangle$.

We have $\varphi(a) \notin V$ (because $a \notin V$ and φ fixes V), which means $\varphi(a) = a^k v'$ for some $k \in \mathbb{Z}_p^\times$ and $v' \in V$. Then (since v' centralizes V, because V is abelian) we have

$$\langle v_1, v_2 \rangle = \varphi\big(\langle v_1, v_2 \rangle\big) \ni \varphi(v_2) = \varphi(v_1^a) = \varphi(v_1)^{\varphi(a)} \in \langle v_1 \rangle^{a^k} = \langle v_{k+1} \rangle,$$

so $k \in \{0,1\} \cap \mathbb{Z}_p^\times = \{1\}$, which means

$$\varphi(a) = av'.$$

Note that (since $\varphi(V) = V$) this implies

$$\varphi(aV) = aV.$$

Since φ fixes $\langle v_1 \rangle$, we have $\varphi(v_1) = \ell v_1$ for some $\ell \in \mathbb{Z}_p^\times$. For every $i \in \{1, \ldots, p\}$, this implies

$$\varphi(v_i) = \varphi(v_1^{a^{i-1}}) = \varphi(v_1)^{\varphi(a^{i-1})} = (\ell v_1)^{a^{i-1}} = \ell v_i.$$

Since $\{v_1, \ldots, v_p\}$ generates V, we conclude that

$$\varphi(v) = \ell v \text{ for all } v \in V.$$

To complete the proof, we will show that v' is trivial and $\ell = 1$. (This means that φ fixes a, and also fixes every element of V. So φ is the trivial automorphism, as desired.) For all $z_0 \in z^Q$, we have

$$\begin{aligned} a \cdot (v' + \ell z_0) &= a\, v' \cdot (\ell z_0) = \varphi(a)\, \varphi(z_0) = \varphi(a\, z_0) \\ &\in \varphi(S \cap aV) = \varphi(S) \cap \varphi(aV) = S \cap aV = a\, z^Q. \end{aligned}$$

Therefore, if we write $v' = \sum_{i=1}^p s_i v_i$ (with $s_i \in \mathbb{Z}_p$) and $z_0 = \sum_{i=1}^p t_i v_i$ (with $t_i \in \{\pm 1\}$), then we have

$$s_i + \ell t_i \in \{\pm 1\} \pmod{p} \text{ for every } i.$$

For any given i, the representation of Q on V_i is nontrivial, so we may choose z_0 so that $t_i = -1$. Therefore, we have $s_i - \ell \equiv \pm 1 \pmod{p}$. On the other hand, by letting $z_0 = z$ (and noting that $s_i - \ell \not\equiv s_i + \ell \pmod{p}$) we see that we also have $s_i + \ell \equiv \mp 1 \pmod{p}$. Adding these two equations and dividing by 2 yields $s_i = 0$ (for all i). So v' is trivial (which means $\varphi(a) = a$).

All that remains is to show that $\ell = 1$ (which means that φ acts trivially on V). Suppose this is not true. (That is, suppose $\ell \neq 1$.) We have

$$\pm\ell = 0 + \ell(\pm 1) = s_i + \ell t_i \in \{\pm 1\} \pmod{p},$$

so this implies $\ell = -1$.

For convenience, let $Z = \langle z \rangle = \mathrm{Z}(A \ltimes V)$. Note that, since $\varphi(a) = a$, we have

$$a \cdot (-z) = a \cdot (\ell z) = \varphi(az) \in \varphi(S \cap aV) = S \cap aV = a\, z^Q,$$

so there is some $g \in Q$, such that $z^g = -z$. Since $Z = \langle z \rangle$, this implies that g is an element of the normaliser $\mathrm{N}_Q(Z)$ of Z in Q. Also note that g is nontrivial, because $z^g = -z \neq z$. Then, since $\mathrm{N}_Q(Z)$ is normalized by A (because A normalizes Q and Z), the irreducibility of the representation of A on Q implies that $\mathrm{N}_Q(Z) = Q$.

Hence, Q acts on Z by conjugation, so $Q/C_Q(Z)$ embeds in the cyclic group $\mathrm{Aut}(Z) \cong \mathbb{Z}_p^\times$. Since Q is an elementary abelian 2-group, this implies that $|Q/C_Q(Z)| \leq 2$. It is clear that $|Q| \geq 4$ (because $Q \cong (\mathbb{Z}_2)^n$ and $n \geq 2$), so we conclude that $C_Q(Z)$ is nontrivial. Using once again the fact that the representation of A on Q is irreducible, we conclude that $C_Q(Z) = Q$, which means that Q centralizes Z. However, since

$$Z = \langle z \rangle = \langle v_1 + v_2 + \cdots + v_p \rangle,$$

and each $\langle v_i \rangle = V_i$ is a Q-invariant subspace, this implies that Q centralizes each v_i, and is therefore trivial on V. On the other hand, we have $z^g = -z \neq z$, and $g \in Q$. This is a contradiction.

4 Using wreath products to construct witnesses

In this section, we prove Corollary 4.11, which is a generalization of Theorem 1.9.

Notation 4.1. In this section, N always denotes a normal subgroup of a group G. We let $\overline{G} = G/N$, and use $\overline{}\colon G \to \overline{G}$ to denote the natural homomorphism.

Notation 4.2. For each $c \in G$ and each function $f\colon \overline{G} \to N$, we let $\varphi_{c,f}$ be the permutation on G that is defined by

$$\varphi_{c,f}(x) = xc\, f(\overline{x}) \text{ for } x \in G.$$

Let $W(G, N)$ be the set of all such permutations of G.

Remark 4.3. Informally speaking, an element of $W(G, N)$ is defined by choosing an element of $\overline{G}$ (or, more accurately, by choosing a coset representative) to permute the cosets of N, and then choosing an element of N to act on each coset. (The elements of N can be chosen independently on each coset.)

We have $\varphi_{c,f} = \varphi_{c',f'}$ if and only if there is some $n \in N$, such that $c' = cn$ and $f'(\overline{x}) = n^{-1} f(x)$ for all $\overline{x}$. From this, it follows that $|W(G, N)| = |\overline{G}| \cdot |N|^{|\overline{G}|}$.

Remark 4.4. The usual definition of the *wreath product* of two groups K and H is essentially:

$$K \wr H = W(K \times H, \{1\} \times H).$$

Definition 4.5. Recall that the *wreath product* $X \wr Y$ of two (di)graphs X and Y is the (di)graph whose vertex set is the cartesian product $V(X) \times V(Y)$, and with a (directed) edge from (x_1, y_1) to (x_2, y_2) if and only if either there is a (directed) edge from x_1 to x_2 or $x_1 = x_2$ and there is a (directed) edge from y_1 to y_2. This is also known as the *lexicographic product* of X and Y.

The following two observations are well known (and fairly immediate from the definitions). The first is a concrete version of the Universal Embedding Theorem, which states that G is isomorphic to a subgroup of $(G/N) \wr N$.

Lemma 4.6. $W(G, N)$ is a subgroup of the symmetric group on G. It is isomorphic to the wreath product $\overline{G} \wr N$, and contains the regular representation of G.

Lemma 4.7. Suppose $\operatorname{Cay}(\overline{G}, \overline{S_1})$ is a loopless Cayley digraph on $\overline{G}$, and $\operatorname{Cay}(N, S_2)$ is a Cayley digraph on N. Let $S_1 = \{\, g \in G \mid \overline{g} \in \overline{S_1} \,\}$. Then

$$\operatorname{Cay}(G, S_1 \cup S_2) \cong \operatorname{Cay}(\overline{G}, \overline{S_1}) \wr \operatorname{Cay}(N, S_2),$$

and $W(G, N)$ is contained in the automorphism group of $\operatorname{Cay}(G, S_1 \cup S_2)$.

The following result is a special case of the general principle that the automorphism group of a wreath product of digraphs is usually the wreath product of the automorphism groups. We have stated it only for DRRs, making use of some straightforward observations about the automorphism group of a DRR on more than 2 vertices, but the much more general statement in [3] applies to all vertex-transitive digraphs.

Lemma 4.8 (cf. Dobson-Morris [3, Theorem 5.7])**.** Assume that the graphs $\operatorname{Cay}(\overline{G}, \overline{S_1})$ and $\operatorname{Cay}(N, S_2)$ are loopless DRRs, and let S_1 be as in Lemma 4.7. If either $|\overline{G}| \neq 2$ or $|N| \neq 2$, then

$$\operatorname{Aut}\bigl(\operatorname{Cay}(G, S_1 \cup S_2)\bigr) = W(G, N).$$

In light of Lemmas 2.5 and 4.8, it is of obvious interest to us to determine when the regular representation of G is self-normalizing in $W(G, N)$. Our next result is the answer to this question. Recall that the *abelianization* of a group H is the largest abelian quotient of H, or, in other words, the quotient group $H/[H, H]$, where $[H, H]$ is the commutator subgroup of H.

Theorem 4.9. Let N be a normal subgroup of G. Then the regular representation of G is self-normalizing in $W(G, N)$ if and only if

1. $Z(N) \leq Z(G)$, and
2. the order of the abelianization of G/N is relatively prime to $|Z(N)|$.

Proof. ($\Rightarrow$) We prove the contrapositive. (1) If $Z(N) \not\leq Z(G)$, then there exists $n \in Z(N)$ such that $n \notin Z(G)$. Conjugation by n is an element of $W(G, N)$ that normalizes the right regular representation of G, but is not in the right regular representation of G. (2) If the order of the abelianization of G/N is not relatively prime to $|Z(N)|$, then there is a nontrivial homomorphism $f \colon \overline{G} \to \mathrm{Z}(N)$. We may assume that hypothesis (1) is satisfied, and then it is straightforward to verify that the corresponding element $\varphi_{f,1}$ of $W(G,N)$ normalizes the right regular representation of G:

$$\begin{aligned} \varphi_{f,1}(xg) &= xg\, f(\overline{xg}) && \text{(definition of } \varphi_{f,1}) \\ &= x\, f(\overline{xg})\, g && (f(\overline{xg}) \in f(\overline{G}) \subseteq \mathrm{Z}(N) \subseteq \mathrm{Z}(G)) \\ &= x\, f(\overline{x})\, f(\overline{g})\, g && (f \text{ is a homomorphism}) \\ &= \varphi_{f,1}(x) \cdot f(\overline{g})\, g && \text{(definition of } \varphi_{f,1}). \end{aligned}$$

($\Leftarrow$) By Lemma 2.4, it suffices to show that $\mathrm{Aut}(G) \cap W(G,N)$ is trivial. To this end, let $\varphi \in \mathrm{Aut}(G) \cap W(G,N)$. Since $\varphi \in W(G,N)$, there exist $c \in G$ and $f \colon \overline{G} \to N$, such that

$$\varphi(x) = xc\, f(\overline{x}) \text{ for all } x \in G.$$

Since φ is a group automorphism we know $\varphi(1) = 1 \in N$, so we may assume $c = 1$, after multiplying c on the right by an element of N. Then we must have $f(\overline{1}) = 1$. Now, for each $n \in N$, we have $\overline{n} = \overline{1}$, so

$$\varphi(n) = n \cdot f(\overline{n}) = n \cdot f(\overline{1}) = n \cdot 1 = n.$$

Therefore, for all $g \in G$ and $n \in N$, we have

$$gn \cdot f(\overline{g}) = gn \cdot f(\overline{gn}) = \varphi(gn) = \varphi(g)\, \varphi(n) = g\, f(\overline{g}) \cdot n,$$

so $n \cdot f(\overline{g}) = f(\overline{g}) \cdot n$. Since this is true for all $n \in N$, we conclude that $f(\overline{g}) \in \mathrm{Z}(N)$. Since $\mathrm{Z}(N) \subseteq \mathrm{Z}(G)$, this implies $f(\overline{g}) \in \mathrm{Z}(G)$ for all $\overline{g}$. Therefore, for all $g, h \in G$, we have

$$gh \cdot f(\overline{gh}) = \varphi(gh) = \varphi(g)\, \varphi(h) = g\, f(\overline{g}) \cdot h\, f(\overline{h}) = gh \cdot f(\overline{g})\, f(\overline{h}).$$

So f is a group homomorphism. Since $f(\overline{G})$ is contained in $\mathrm{Z}(N)$, which is abelian, we see from (2) that f must be trivial. Since c is also trivial, we conclude that $\varphi(x) = x$ for all x. Since φ is an arbitrary element of $\mathrm{Aut}(G) \cap W(G,N)$, this completes the proof. □

Remark 4.10. A slight modification of the proof of Theorem 4.9 shows that if $\widehat{G}$ is the right regular representation of G, then the normalizer of $\widehat{G}$ in $W(G,N)$ is

$$\{\, \varphi_{c,f} \mid c \in G, f \in Z^1\big(\overline{G}, \mathrm{Z}(N)\big) \,\},$$

where

$$Z^1\big(\overline{G}, \mathrm{Z}(N)\big) = \{\, f \colon \overline{G} \to \mathrm{Z}(N) \mid f(\overline{gh}) = f(\overline{g})^{\overline{h}}\, f(\overline{h}) \text{ for all } \overline{g}, \overline{h} \in \overline{G} \,\}$$

is the set of all "1-cocycles" or "crossed homomorphisms" from $\overline{G}$ to $\mathrm{Z}(N)$ (in the terminology of group cohomology [12]). This fact is presumably known.

It may also be of interest to note that hypotheses (1) and (2) in Theorem 4.9 are obviously satisfied when $\mathrm{Z}(N)$ is trivial.

Combining the results of this section, we obtain the following.

Corollary 4.11. Let N be a nontrivial, proper, normal subgroup of G, such that N and G/N each admit a DRR (or, respectively, a GRR). If

1. $Z(N) \leq Z(G)$, and
2. the order of the abelianization of G/N is relatively prime to $|Z(N)|$,

then G is not DRR-detecting (respectively, not GRR-detecting).

More precisely, if we let Γ_1 be a DRR (respectively, GRR) on G/N and Γ_2 be a DRR (respectively, GRR) on N, then $\Gamma_1 \wr \Gamma_2$ witnesses that G is not DRR-detecting (respectively, not GRR-detecting).

Proof. Clearly, either $|\overline{G}| \neq 2$ or $|N| \neq 2$. It then follows by Lemma 4.7 and Lemma 4.8 that $\operatorname{Aut}(\Gamma_1 \wr \Gamma_2) = W(G,N)$. By Theorem 4.9, the regular representation of G is self-normalizing in $W(G,N)$, therefore $\Gamma_1 \wr \Gamma_2$ witnesses that G is not DRR-detecting (respectively, not GRR-detecting). □

Note that Theorem 1.9 can be obtained from Corollary 4.11 by letting $G = G_1 \times G_2$ and $N = G_2$.

5 Using cartesian products to construct witnesses

Definition 5.1. Recall that the *cartesian product* $X \,\square\, Y$ of two (di)graphs X and Y is the (di)graph whose vertex set is the cartesian product $X \times Y$, such that there is a (directed) edge from (x_1, y_1) to (x_2, y_2) if and only if either $x_1 = x_2$ and there is a (directed) edge from y_1 to y_2, or $y_1 = y_2$, and there is a (directed) edge from x_1 to x_2.

We say that a (di)graph is *prime* (with respect to cartesian product) if it has more than one vertex, and is not isomorphic to the cartesian product of two (di)graphs, each with more than one vertex. It is well known that every (di)graph can be written uniquely as a cartesian product of prime factors (up to a permutation of the factors), but we do not need this fact.

To avoid the need to consider permutations of the factors, the following result includes the hypothesis that the factors are pairwise non-isomorphic. (This is not assumed in [11], which also considers isomorphisms between two different cartesian products, instead of only automorphisms of a single digraph.) The upshot is that, in this situation, the automorphism group of the cartesian product is the direct product of the automorphism groups.

Theorem 5.2 (Walker, cf. [11, Theorem 10])**.** Let $\Gamma_1, \ldots, \Gamma_k$ be weakly connected prime digraphs that are pairwise non-isomorphic. If φ is an automorphism of $\Gamma_1 \,\square \cdots \square\, \Gamma_k$, then for each i, there is an automorphism φ_i of Γ_i such that, for every vertex $(v_1, \ldots, v_k)$ of $\Gamma_1 \,\square \cdots \square\, \Gamma_k$, we have

$$\varphi(v_1, \ldots, v_k) = \big(\varphi_1(v_1), \ldots, \varphi_k(v_k)\big).$$

Prime graphs are quite abundant:

Theorem 5.3 (Imrich [7, Theorem 1])**.** If Γ is a graph (with more than one vertex), such that neither Γ nor its complement $\overline{\Gamma}$ is prime, then Γ is one of the following:

1. the cycle of length 4 or its complement (two disjoint copies of K_2);
2. the cube or its complement (the graph $K_2 \times K_4$);

3. $K_3 \,\square\, K_3$ (which is self-complementary); or
4. $K_2 \,\square\, \Delta$, where Δ is the graph obtained by deleting an edge from K_4 (which is self-complementary).

The following is an analogous result for digraphs. (Recall that a digraph is *proper* if it is not a graph.)

Theorem 5.4 (Grech-Imrich-Krystek-Wojakowski [6, Theorem 1.2] and Morgan-Morris-Verret [8, Theorem 2.2])**.** If Γ is a proper digraph, then at least one of Γ or $\overline{\Gamma}$ is prime.

Corollary 5.5. If a nontrivial group G admits a DRR (respectively, GRR), then it admits a DRR (respectively, GRR) that is prime (and weakly connected). Furthermore, if G is not DRR-detecting (respectively, not GRR-detecting), then there is a witness that is prime (and weakly connected).

Proof. First, note that Γ and $\overline{\Gamma}$ have the same automorphism group, so Γ is a DRR (GRR, respectively) for G if and only if $\overline{\Gamma}$ is. Similarly, Γ is a witness that G is not DRR-detecting (GRR-detecting, respectively) if and only if $\overline{\Gamma}$ is.

Also note that if a prime digraph Γ is not weakly connected, and is either a DRR or a witness that some group is not DRR-detecting, then $\overline{\Gamma} = K_2$ (so $\overline{\Gamma}$ is prime and weakly connected). This is because any vertex-transitive digraph is isomorphic to $\Gamma_0 \,\square\, \overline{K_n}$, where Γ_0 is a weakly connected component of the digraph, and n is the number of components.

Suppose that Γ is a GRR for G. By Theorem 5.3, at least one of Γ or $\overline{\Gamma}$ is prime with respect to cartesian product, unless Γ is one of the graphs listed in that theorem, but none of those graphs is a GRR, because the automorphism group does not act regularly on the set of vertices:

1. the automorphism group of a cycle of length 4 (or its complement) is the dihedral group of order 8;
2. the automorphism group of the cube (or its complement) is $\mathbb{Z}_2 \times \mathrm{Sym}(4)$, of order 48;
3. the automorphism group of $K_3 \,\square\, K_3$ is $\mathbb{Z}_2 \wr \mathrm{Sym}(3)$, of order 72; and
4. the graph $K_2 \,\square\, \Delta$ is not vertex-transitive (it is not even true that all vertices have the same valency).

Now, suppose that Γ is a DRR for G. We may assume that Γ is a proper digraph. (Otherwise, Γ is a GRR, so the preceding paragraph applies.) Then, by Theorem 5.4, either Γ or $\overline{\Gamma}$ is prime with respect to cartesian product.

Finally, suppose Γ is a witness that G is not DRR-detecting (or not GRR-detecting, respectively), such that neither Γ nor $\overline{\Gamma}$ is prime. This implies that Γ is one of the graphs listed in Theorem 5.3. (So G is not GRR-detecting.)

However, it is easy to see that none of the graphs listed in Theorem 5.3 is a witness. First, recall that a p-subgroup of a group cannot be self-normalizing unless it is a Sylow subgroup. Therefore (by Lemma 2.5), if a graph Γ of prime-power order p^k is a witness that some group is not GRR-detecting, then p^k must be the largest power of p that divides $\mathrm{Aut}(\Gamma)$. This shows that the graphs in (1) and (2) are not witnesses. If Γ is as described in (3), then the only regular subgroup of $\mathrm{Aut}(\Gamma)$ is the unique (Sylow) subgroup of order 9, which is normal, and is therefore obviously not self-normalizing. Finally, as noted above, the graphs in (4) are not vertex-transitive. □

Proof of Theorem 1.10. For simplicity, we consider only DRRs (because the proof is the same for GRRs). Let $\Gamma_1 = \mathrm{Cay}(G_1, S_1)$ be a DRR for G_1, and let $\Gamma_2 = \mathrm{Cay}(G_2, S_2)$ be a witness that G_2 is not DRR-detecting. By Corollary 5.5, we may assume that Γ_1 and Γ_2 are prime with respect to cartesian product (and are weakly connected). Since Γ_1 is a DRR, but Γ_2 is not, we know that $\Gamma_1 \not\cong \Gamma_2$. Therefore, we see from Theorem 5.2 that $\mathrm{Aut}(\Gamma_1 \,\square\, \Gamma_2) = \mathrm{Aut}(\Gamma_1) \times \mathrm{Aut}(\Gamma_2)$.

Since Γ_2 is not a DRR, $\Gamma_1 \,\square\, \Gamma_2$ is not a DRR. Similarly, since the regular representation of G_1 is all of $\mathrm{Aut}(\Gamma_1)$ and the regular representation of G_2 is self-normalizing in $\mathrm{Aut}(\Gamma_2)$, the regular representation of $G_1 \times G_2$ is self-normalizing in $\mathrm{Aut}(\Gamma_1 \,\square\, \Gamma_2)$. So $\Gamma_1 \,\square\, \Gamma_2$ is a witness that $G_1 \times G_2$ is not DRR-detecting. □

6 Nilpotent DRR-detecting groups are p-groups

In this section, we prove Theorem 1.11, which states that if a nilpotent group is not a p-group, then it is not DRR-detecting. In most cases, this follows easily from Theorems 1.9 and 1.10, but there is one special case that requires a different proof:

Lemma 6.1. If H is a nontrivial group of odd order and $H \not\cong \mathbb{Z}_3 \times \mathbb{Z}_3$, then $Q_8 \times H$ is not DRR-detecting.

Proof. From Theorem 2.3, we see that H admits a DRR (because it has odd order, but is not $\mathbb{Z}_3 \times \mathbb{Z}_3$), so we may let $\mathrm{Cay}(H, S_1)$ be a DRR. Let $S = S_1 \cup \{i\} \cup jH \subseteq G$. It suffices to show that $\mathrm{Aut}(G, S) = \{1\}$ and that $\mathrm{Cay}(G, S)$ is not a DRR.

Let $\varphi \in \mathrm{Aut}(G, S)$. We can characterise S_1 as the set of all elements of S that have odd order. Thus, we must have $\varphi(S_1) = S_1$, so $H = \langle S_1 \rangle$ is fixed setwise by φ. Since the identity vertex is also fixed and the induced subgraph on H is a DRR, every element of H must be fixed by φ. We can use this fact to distinguish i from the elements of jH (all of which differ from each other by elements of H), so i is fixed by φ. Finally, j is the unique element of order 4 in jH, so it too is fixed by φ. We now know that φ is an automorphism of G that fixes every element of a generating set for G. So φ must be trivial.

All that remains is to show that $\mathrm{Cay}(G, S)$ is not a DRR. Fix a nontrivial element $h \in H$, and define a permutation τ of G by

$$\tau(x) = \begin{cases} x & \text{if } x \in \langle H, i \rangle; \\ xh & \text{if } x \in j\langle H, i \rangle. \end{cases}$$

Note that τ is a permutation of G, because right multiplication by h is a permutation of G that fixes $\langle H, i \rangle$ setwise.

We claim that τ is an automorphism of $\mathrm{Cay}(G, S)$. First, note that a directed edge of the form $g \to s_1 g$ or $g \to ig$ either has both of its endpoints in $\langle H, i \rangle$, or has both of its endpoints in $j\langle H, i \rangle$. Since right multiplication by h is an automorphism of $\mathrm{Cay}(G, S)$, it is clear that τ preserves such directed edges. The remaining directed edges are of the form $g \to gjh'$ for some $h' \in H$. Multiplying either g or gjh' on the right by h results in another such directed edge. This completes the proof that τ is an automorphism of $\mathrm{Cay}(G, S)$. □

Proof of Theorem 1.11. Let G be a nilpotent group, and assume that G is not a p-group. (Note that $|G|$ is divisible by at least two distinct primes.) We will show that G is not DRR-detecting.

Case 1. $|G|$ is divisible by at least three distinct primes. Let p be the largest prime divisor of $|G|$ and let P be a Sylow p-subgroup of G. Since G is nilpotent, we may write $G = P \times H$ for some subgroup H with $\gcd\big(|P|, |H|\big) = 1$. Since p is the largest of at least three primes dividing $|G|$, neither P nor H is a 2-group or a 3-group, so we see from Theorem 2.3 that P and H each admit a DRR. Therefore, Theorem 1.9 implies that $G = P \times H$ is not DRR-detecting.

Case 2. $|G|$ is divisible by precisely two distinct primes p and q. Since G is nilpotent, we have $G = P \times Q$, where P is a Sylow p-subgroup and Q is a Sylow q-subgroup of G. If P and Q each admit a DRR, then Theorem 1.9 implies that $G = P \times Q$ is not DRR-detecting.

We may thus assume, without loss of generality, that P does not admit a DRR. Using Theorem 2.3 and Lemma 6.1 and interchanging P and Q if necessary, we may assume that P is isomorphic to one of $(\mathbb{Z}_2)^2$, $(\mathbb{Z}_2)^3$, $(\mathbb{Z}_2)^4$, or $(\mathbb{Z}_3)^2$. Thus, we may write $P = (\mathbb{Z}_p)^r$, with $r \geq 2$.

Since $(\mathbb{Z}_p)^{r-1} \times Q$ is not a p-group, we may assume, by induction on $|G|$, that it is not DRR-detecting. Also note that $\mathbb{Z}_p$ admits a DRR. (Take the directed p-cycle $\overrightarrow{C_p}$ if $p \geq 3$; or take K_2 if $p = 2$.) Therefore, by applying Theorem 1.10 with $G_1 = \mathbb{Z}_p$ and $G_2 = (\mathbb{Z}_p)^{r-1} \times Q$, we see that the group $G = \mathbb{Z}_p \times \big((\mathbb{Z}_p)^{r-1} \times Q\big)$ is not DRR-detecting. □

ORCID iDs

Joy Morris https://orcid.org/0000-0003-2416-669X
Gabriel Verret https://orcid.org/0000-0003-1766-4834

References

[1] L. Babai, Finite digraphs with given regular automorphism groups, *Period. Math. Hungar.* **11** (1980), 257–270, doi:10.1007/bf02107568.

[2] J. Dixon and B. Mortimer, *Permutation Groups*, volume 163 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1996, doi:10.1007/978-1-4612-0731-3.

[3] E. Dobson and J. Morris, Automorphism groups of wreath product digraphs, *Electron. J. Combin.* **16** (2009), Research Paper 17, 30, doi:10.37236/106.

[4] C. D. Godsil, GRRs for nonsolvable groups, in: *Algebraic methods in graph theory, Vol. I, II (Szeged, 1978)*, North-Holland, Amsterdam-New York, volume 25 of *Colloq. Math. Soc. János Bolyai*, pp. 221–239, 1981, https://www.elsevier.com/books/algebraic-methods-in-graph-theory/sos/978-0-444-85442-1.

[5] C. D. Godsil, On the full automorphism group of a graph, *Combinatorica* **1** (1981), 243–256, doi:10.1007/bf02579330.

[6] M. Grech, W. Imrich, A. D. Krystek and L. u. J. Wojakowski, Direct product of automorphism groups of digraphs, *Ars Math. Contemp.* **17** (2019), 89–101, doi:10.26493/1855-3974.1498.77b.

[7] W. Imrich, On products of graphs and regular groups, *Israel J. Math.* **11** (1972), 258–264, doi:10.1007/bf02789317.

[8] L. Morgan, J. Morris and G. Verret, Digraphs with small automorphism groups that are Cayley on two nonisomorphic groups, *Art Discrete Appl. Math.* **3** (2020), Paper No. 1.01, 11, doi:10.26493/2590-9770.1254.266.

[9] J. Morris and P. Spiga, Classification of finite groups that admit an oriented regular representation, *Bull. Lond. Math. Soc.* **50** (2018), 811–831, doi:10.1112/blms.12177.

[10] J. Serre, *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1977, doi:10.1007/978-1-4684-9458-7.

[11] J. W. Walker, Strict refinement for graphs and digraphs, *J. Combin. Theory Ser. B* **43** (1987), 140–150, doi:10.1016/0095-8956(87)90018-9.

[12] Wikipedia, Group cohomology — Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Group_cohomology, 2021.

THE ART OF DISCRETE AND APPLIED MATHEMATICS

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P1.08
https://doi.org/10.26493/2590-9770.1414.f67
(Also available at http://adam-journal.eu)

Circulant almost cross intersecting families

Michal Parnas*

The Academic College of Tel-Aviv-Yaffo, Tel-Aviv, Israel

Received 16 July 2020, accepted 29 April 2021, published online 4 April 2022

Abstract

Let $\mathcal{F}$ and $\mathcal{G}$ be two t-uniform families of subsets over $[k] = \{1, 2, ..., k\}$, where $|\mathcal{F}| = |\mathcal{G}|$, and let C be the adjacency matrix of the bipartite graph whose vertices are the subsets in $\mathcal{F}$ and $\mathcal{G}$, where there is an edge between $A \in \mathcal{F}$ and $B \in \mathcal{G}$ if and only if $A \cap B \neq \emptyset$. The pair $(\mathcal{F}, \mathcal{G})$ is q-almost cross intersecting if every row and column of C has exactly q zeros.

We further restrict our attention to q-almost cross intersecting pairs that have a circulant intersection matrix $C_{p,q}$, determined by a column vector with $p > 0$ ones followed by $q > 0$ zeros. This family of matrices includes the identity matrix in one extreme, and the adjacency matrix of the bipartite crown graph in the other extreme.

We give constructions of pairs $(\mathcal{F}, \mathcal{G})$ whose intersection matrix is $C_{p,q}$, for a wide range of values of the parameters p and q, and in some cases also prove matching upper bounds. Specifically, we prove results for the following values of the parameters: (1) $1 \leq p \leq 2t-1$ and $1 \leq q \leq k-2t+1$. (2) $2t \leq p \leq t^2$ and any $q > 0$, where $k \geq p+q$. (3) p that is exponential in t, for large enough k.

Using the first result we show that if $k \geq 4t-3$ then $C_{2t-1,k-2t+1}$ is a maximal isolation submatrix of size $k \times k$ in the $0,1$-matrix $A_{k,t}$, whose rows and columns are labeled by all subsets of size t of $[k]$, and there is a one in the entry on row x and column y if and only if subsets x, y intersect.

Keywords: Circulant matrix, intersecting sets, Boolean rank, isolation set.

Math. Subj. Class.: 05D05, 15B34

1 Introduction

One of the fundamental results of extremal set theory is the theorem of Erdős, Ko and Rado [8], which shows that the size of an intersecting t-uniform family of subsets over

*The author would like to thank the referee for the useful comments that helped improve the presentation of the paper.

E-mail address: michalp@mta.ac.il (Michal Parnas)

$[k] = \{1, 2, ..., k\}$ is bounded above by $\binom{k-1}{t-1}$. Numerous variations of the original problem have been suggested and studied over the years. Among them is the problem of cross intersecting families of subsets (e.g. [4, 10, 14, 17, 21]). Specifically, if $\mathcal{F}$ and $\mathcal{G}$ are two t-uniform families of subsets over $[k]$, then the pair $(\mathcal{F}, \mathcal{G})$ is cross intersecting if every subset in $\mathcal{F}$ intersects with every subset in $\mathcal{G}$ and vice versa. Pyber [21] proved that in this case $|\mathcal{F}| \cdot |\mathcal{G}| \leq \binom{k-1}{t-1}^2$.

Many of the extremal combinatorial problems considered so far can be inferred as results about maximal submatrices of the $0,1$-matrix $A_{k,t}$ of size $\binom{k}{t} \times \binom{k}{t}$, whose rows and columns are labeled by all subsets of size t of $[k]$, and there is a one in the entry on row x and column y if and only if subsets x, y intersect. Hence, in this setting, the result of Erdős, Ko and Rado can be inferred as stating the size of the largest all-one square principal submatrix of $A_{k,t}$, and the result of Pyber states the size of the largest all-one submatrix of $A_{k,t}$. We note that considering the classic results of extremal combinatorics as maximal submatrices of $A_{k,t}$, allows us to employ tools from algebra in addition to the combinatorial techniques.

Another variation of the problem of cross intersecting families was introduced by Gerbner et al. [11], which defined the notion of a q-almost cross intersecting pair $(\mathcal{F}, \mathcal{G})$. Here every subset in $\mathcal{F}$ does not intersect with exactly q subsets in $\mathcal{G}$ and vice versa. If $\mathcal{F} = \mathcal{G}$ then $\mathcal{F}$ is called a q-almost intersecting family of subsets. Hence, if C is the submatrix of $A_{k,t}$ whose rows are indexed by the subsets of $\mathcal{F}$ and columns by the subsets of $\mathcal{G}$, then every row and column of C has exactly q zeros. Using a classic theorem of Bollobás [3], it is possible to prove that the largest square submatrix C of $A_{k,t}$, representing a 1-almost cross intersecting pair, is of size $\binom{2t}{t} \times \binom{2t}{t}$. A theorem proved in [11] shows that if C is a submatrix of size $n \times n$ of $A_{k,t}$, with exactly q zeros in each row and column, then $n \leq (2q-1)\binom{2t}{t}$.

In this paper we consider the problem of finding maximal *circulant* submatrices of $A_{k,t}$, representing an almost cross intersecting pair, for a range of parameters. A circulant matrix is a matrix in which each row is shifted one position to the right compared to the preceding row (or alternatively, each column is shifted one position compared to the preceding column). Therefore, such a matrix C is determined completely by its first row or first column. Circulant matrices were studied extensively in the context of the multiplicative commutative semi-group of circulant Boolean matrices and also when discussing Cayley graphs of cyclic groups (see e.g. [1, 5, 6, 7, 22]). However, they were not studied in the context of extremal combinatorics, besides some special cases that will be discussed shortly.

$$C_{4,4} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Figure 1: The circulant matrix $C_{p,q}$, where $p = q = 4$.

Our focus will be on circulant matrices that are determined by a column vector with

p ones followed by q zeros. Such a matrix will be denoted by $C_{p,q}$. See Figure 1 for an example. Thus, in one extreme, if $p = 1$ and $q > 0$, then $C_{p,q}$ is the identity matrix. The other extreme is $q = 1$ and $p > 0$, and then $C_{p,q}$ is the adjacency matrix of a crown graph (where a crown graph is a complete bipartite graph from which the edges of a perfect matching have been removed). Hence, the structure of the circulant matrix $C_{p,q}$ forms a bridge which connects these two extreme cases, and it is interesting to find a unifying theorem which determines the maximal size of the matrix $C_{p,q}$ as a function of p, q, k and t.

We note that two trivial examples of circulant submatrices of $A_{k,t}$ include the case of $q = 0$, where we get an all-one submatrix of $A_{k,t}$ of maximal size $\binom{k-1}{t-1} \times \binom{k-1}{t-1}$, and the case of $p = 0$, where we get an all-zero submatrix of $A_{k,t}$ of maximal size $\binom{k/2}{t} \times \binom{k/2}{t}$. Hence, the problem of studying the size of circulant submatrices $C_{p,q}$ of $A_{k,t}$ is interesting only if both $p, q > 0$. Furthermore, we must require that $k \geq 2t$, as otherwise, $A_{k,t}$ is the all-one matrix itself.

As we discuss shortly, one of our results also provides a simple construction of maximal isolation submatrices of $A_{k,t}$, thus providing simple small witnesses to the Boolean rank of $A_{k,t}$. The *Boolean rank* of a $0,1$-matrix A of size $n \times m$ is equal to the smallest integer r, such that A can be factorized as a product of two $0,1$-matrices, $X \cdot Y = A$, where X is a matrix of size $n \times r$ and Y is a matrix of size $r \times m$, and all additions and multiplications are Boolean (that is, $1+1 = 1, 1+0 = 0+1 = 1, 1\cdot 1 = 1, 1\cdot 0 = 0\cdot 1 = 0$). A $0,1$-matrix B of size $s \times s$ is called an *isolation matrix*, if we can select s ones in B, so that no two of the selected ones are in the same row or column of B, and no two of the selected ones are contained in a 2×2 all-one submatrix of B. It is well known that if B is an isolation submatrix of size $s \times s$ in a given $0,1$-matrix A, then s bounds below the Boolean rank of A (see [2, 16]). However, computing the Boolean rank or finding a maximal isolation submatrix in general is an NP-hard problem (see [13, 18, 24]). Hence, it is interesting to find and characterize families of maximal isolation sets for specific given matrices.

1.1 Our results

Our main goal is to determine the range of parameters, p and q, for which $C_{p,q}$ is a submatrix of $A_{k,t}$. The constructions and upper bounds we present differ in their structure and proof methods according to the size of p, q compared to t, k.

We first consider the range of values of relatively small p, that is $1 \leq p \leq 2t - 1$, and prove in Section 2 the following positive result.

Theorem 1.1. *Let $k \geq 2t$, $1 \leq p \leq 2t - 1$ and $1 \leq q \leq k - 2t + 1$. Then $C_{p,q}$ is a submatrix of $A_{k,t}$.*

In the extreme case of $p = 1$ and $q = k - 2t + 1$, this construction gives the identity submatrix of size $(k-2t+2) \times (k-2t+2)$. Recently, [20] proved that this is the maximal size of an identity submatrix in $A_{k,t}$.

The other extreme is $p = 2t - 1$ and $q = k - 2t + 1$, in which case we get a circulant submatrix of size $k \times k$. As we show in Section 2, if $k \geq 4t - 3$ then $C_{2t-1,k-2t+1}$ is a maximal isolation submatrix of size $k \times k$ in $A_{k,t}$. Since the Boolean rank of $A_{k,t}$ is k for $k \geq 2t$ (see [19]), then the size of a maximal isolation submatrix of $A_{k,t}$ is upper bounded by $k \times k$, and thus, our result is optimal in this case.

Furthermore, for $k = 2t + p - 2$ and $p \geq 2$, the construction described in Theorem 1.1 provides an isolation submatrix of size $(2p - 1) \times (2p - 1)$. We note that [20] gave constructions of isolation submatrices in $A_{k,t}$, of the same size as achieved here. However, the constructions described in [20] are quite complex, and thus, the result described in Theorem 1.1 provides an alternative simpler construction of a maximal isolation submatrix in $A_{k,t}$, for large enough k.

We then prove the following upper bound that matches the size of the construction given in Theorem 1.1, for the range of values of $1 \le p \le 2t-1$ and $q \ge p-1$. The proof of this result characterizes the structure of the Boolean decompositions of $C_{p,q}$ for this range of parameters.

Theorem 1.2. *Let $C_{p,q}$ be a submatrix of $A_{k,t}$, where $k \ge 2t$, $1 \le p \le 2t-1$ and $q > 0$. If $q \ge p-1$ then $q \le k-2t+1$.*

In Section 3 we address the range of slightly larger values of p, that is, $2t \le p \le t^2$, and provide a different construction of circulant submatrices of $A_{k,t}$ of the form $C_{p,q}$. As we show, for this range of values of p, there is no upper bound on the size of q, as we had in Theorem 1.1 and Theorem 1.2, as long as $k \ge p+q$.

Furthermore, the proof for this range of parameters provides a decomposition of $C_{p,q}$ into a product of two Boolean circulant matrices X, Y, where X has t ones in each row and Y has t ones in each column. If we view the rows of X and the columns of Y as the characteristic vectors of subsets of size t, then X and Y each represents a *circulant t-uniform family*. Thus, the construction used in the proof of the next theorem, uses a pair $\mathcal{F}, \mathcal{G}$ of circulant families to construct $C_{p,q}$.

Theorem 1.3. *Let $2t \le p \le t^2$ and $q > 0$. Then $C_{p,q}$ is a submatrix of $A_{k,t}$ for $k \ge q+p$.*

Finally, in Section 4, we consider the range of large p. Using the result of [11] stated above, we know that if $C_{p,q}$ is a submatrix of $A_{k,t}$ of size $n \times n$, then $n \le (2q-1)\binom{2t}{t}$, and [23] proved a conjecture of [12] and showed that for large enough q and t, the size of a q-almost intersecting family $\mathcal{F}$ is bounded by $(q+1)\binom{2t-2}{t-1}$. Note that this last result refers to q-almost cross intersecting pairs $(\mathcal{F}, \mathcal{G})$ in which $\mathcal{F} = \mathcal{G}$. Furthermore, the constructions presented in [23], which achieve this bound, do not have a circulant intersection matrix.

Indeed, we can get a better upper bound for circulant submatrices of the form $C_{p,q}$. Using a theorem of Frankl [9] and Kalai [15] about skew matrices, it is possible to show that $p \le \binom{2t}{t} - 1$. Hence, if $C_{p,q}$ is a submatrix of size $n \times n$ of $A_{k,t}$ then $n \le \binom{2t}{t} + q - 1$.

In the extreme case of $p = \binom{2t}{t} - 1$ and $q = 1$, the simple construction that takes all subsets of size t of $[2t]$ as row and column indices, results in a submatrix $C_{p,q}$ of size $\binom{2t}{t} \times \binom{2t}{t}$. This is optimal, as it matches the upper bound of $\binom{2t}{t} + q - 1$.

For larger q, we give a simple construction of $C_{p,q}$ for $p = q \cdot (\binom{2t/q}{t/q} - 1)$, when $t \bmod q = 0$ and k is large enough. Note that there is a relatively large gap between the size of $C_{p,q}$ stated here, and the upper bound of $\binom{2t}{t} + q - 1$. As we prove, this gap can be slightly narrowed for $q = 2$:

Theorem 1.4. *Let $q = 2$ and $p = 2^t + 2^{t-2} - 2$, where $t > 2$. Then $C_{p,q}$ is a submatrix of $A_{k,t}$ for large enough k.*

We conclude by considering the case of $t = 2$ and $p = \binom{2t}{t} - 1 = 5$ and fully characterize it. As we show, in this case, $C_{p,q}$ is a submatrix of $A_{k,t}$, for $q = 1$ and $k \ge 5$, or for $q = 3$ and $k \ge 6$. Thus, for $t = 2, p = 5$ and $q = 1, 3$, we get a result which matches the upper bound of $\binom{2t}{t} + q - 1$. However, as we prove, for $t = 2, p = 5$ and

$q > 0$, $q \neq 1, 3$, there is no k for which $C_{p,q}$ is a submatrix of $A_{k,t}$. This implies that the upper bound of $\binom{2t}{t} + q - 1$ is not tight in general. It remains an open problem to determine for what values of $q > 1$ is $C_{p,q}$ a submatrix of $A_{k,t}$, given that $p = \binom{2t}{t} - 1$ and $t > 2$.

2 The range of $1 \leq p \leq 2t - 1$

In this section we prove Theorems 1.1 and 1.2, which address the range of small p, that is, $1 \leq p \leq 2t - 1$. As stated above, this range of values includes the identity matrix, as well as allows us to provide a simple construction of maximal isolation sets for large enough k.

It will be useful to identify subsets of $[k]$ with their characteristic vectors. Thus, a subset of size t of $[k]$ will be represented by a $0, 1$-vector of length k with exactly t ones. Furthermore, in order to show that some matrix C of size $n \times m$ is a submatrix of $A_{k,t}$, it will be enough to show that there exists a Boolean decomposition $C = X \cdot Y$, where X is a Boolean matrix of size $n \times k$ with exactly t ones in each row, and Y is a Boolean matrix of size $k \times m$ with exactly t ones in each column, and all operations are Boolean.

2.1 A construction of $C_{p,q}$ for $1 \leq p \leq 2t - 1$

The following lemma will be useful in proving Theorem 1.1. It shows that it is possible to decompose a matrix of the form $C_{p,q}$ into a product of two circulant matrices of the same type, for a wide range of parameters.

Lemma 2.1. *Let i, j, z be three integers, such that $i, j \geq 1$ and $i + j - 1 \leq z$. Then*

$$C_{i,z-i} \cdot C_{j,z-j} = C_{i+j-1,z-i-j+1}.$$

Proof. It is well known that the product of two circulant Boolean matrices is a circulant Boolean matrix (where all operations are Boolean). Thus, it is enough to determine the first column $c = (c_1, c_2, ..., c_z)$ of the product matrix $C_{i,z-i} \cdot C_{j,z-j}$, and to show that it has $i + j - 1$ ones, followed by $z - i - j + 1$ zeros. The proof follows directly from the definition of matrix multiplication using the Boolean operations.

Specifically, it is clear that $c_s = 1$ for $1 \leq s \leq i$, since the first element in each of the first i rows of $C_{i,z-i}$ is a 1, and the first element of the first column of $C_{j,z-j}$ is also a 1 (since $i, j \geq 1$). Next consider element c_{i+s} for $1 \leq s \leq j - 1$. Note that row $i + s$ of $C_{i,z-i}$ begins with s zeros and then has i ones, and the first j elements of the first column of $C_{j,z-j}$ are ones. Since $s \leq j - 1$, then the result of multiplying row $i + s$ of $C_{i,z-i}$ with the first column of $C_{j,z-j}$, is a one.

It remains to show that the remaining elements of c are all zeros. But the last $z-i-j+1$ rows of $C_{i,z-i}$ begin with at least j zeros. Therefore, multiplying any of these rows with the first column of $C_{j,z-j}$, results in a zero. □

Using Lemma 2.1, we can now prove Theorem 1.1.

Proof of Theorem 1.1. Let $1 \leq i, j \leq t$ such that $i + j - 1 = p$. Let $J_{n,m}$ be the all-one matrix of size $n \times m$, and $O_{n,m}$ the all-zero matrix of size $n \times m$. Define, two matrices X and Y as follows:

$$X = [C_{i,p+q-i} O_{p+q,t-j} J_{p+q,t-i}], \qquad Y = \begin{bmatrix} C_{j,p+q-j} \\ J_{t-j,p+q} \\ O_{t-i,p+q} \end{bmatrix}.$$

Using Lemma 2.1, where $z = p + q$, we have that

$$X \cdot Y = C_{i,p+q-i} \cdot C_{j,p+q-j} = C_{i+j-1,p+q-i-j+1} = C_{p,q}.$$

Furthermore, each row of X and each column of Y is a vector with exactly t ones, whose length is:

$$(p+q)+(t-j)+(t-i) = p+q+2t-i-j = p+q+2t-(p+1) = q+2t-1.$$

Therefore, if $k \geq q + 2t - 1$, then we can view the rows of X and columns of Y as the characteristic vectors of subsets in $\binom{[k]}{t}$. Thus, $X \cdot Y = C_{p,q}$ is a submatrix of $A_{k,t}$ as claimed. □

As we show next, if $k \geq 4t - 3$ then the construction described in the proof of Theorem 1.1, provides a maximal isolation submatrix of size $k \times k$ in $A_{k,t}$. This result is optimal since the Boolean rank of $A_{k,t}$ is k for $k \geq 2t$ (see [19]).

Corollary 2.2. *Let $2 \leq p \leq 2t - 1$ and let $k = 2t + p - 2$. Then $C_{p,p-1}$ is an isolation submatrix of size $(2p-1) \times (2p-1)$ in $A_{k,t}$. Furthermore, if $k \geq 4t-3$ then $C_{2t-1,k-2t+1}$ is an isolation submatrix of size $k \times k$ in $A_{k,t}$.*

Proof. Let $k = 2t+p-2$. If we set $q = k-2t+1 = (2t+p-2)-2t+1 = p-1$, then by Theorem 1.1, $C_{p,q}$ is a submatrix of $A_{k,t}$ of size $(2p-1) \times (2p-1)$ since $p + q = 2p - 1$. It is easy to verify that in this case, since $q = p - 1$, the ones on the main diagonal of $C_{p,q}$ form an isolation set of size $p + q$.

In the extreme case of $p = 2t-1$, and if $k \geq 4t-3$, then $q = k-2t+1 \geq 2t-2 \geq p-1$, and we get an isolation matrix $C_{p,q}$ of size $k \times k$, since $p + k - 2t + 1 = k$. □

2.2 Upper bounds on the size of $C_{p,q}$ for $1 \leq p \leq 2t - 1$

We now turn to prove Theorem 1.2, which provides a matching upper bound to the size of the construction given in Theorem 1.1, for $1 \leq p \leq 2t - 1$ and $q \geq p - 1$. We note that if $q \geq p - 1$ then $p + q \leq k$ (for any value of p), since in this case $C_{p,q}$ is an isolation submatrix of $A_{k,t}$. Thus, its Boolean rank, which is $p + q$, is bounded above by k, which is the Boolean rank of $A_{k,t}$. However, the proof of Theorem 1.2, which provides a tight upper bound on $p + q$, will require a more elaborate proof.

The following simple claim is easy to verify, and will be needed for the proof of Theorem 1.2.

Claim 2.3. *Let B be an all-one submatrix of size $i \times j$ of $C_{p,q}$, where $p, q > 0$. Then, $1 \leq i, j \leq p$ and $i + j \leq p + 1$.*

The next lemma is a generalization of a claim proved in [19], which characterizes the Boolean decompositions of the identity matrix. Here we characterize the Boolean decompositions of circulant isolation matrices of the form $C_{p,q}$.

Denote by $|x|$ the number of ones in a vector x, and let $x \otimes y$ denote the outer product of a column vector x and a row vector y, where both x, y are of length n. That is, $x \otimes y$ is a matrix of size $n \times n$.

Lemma 2.4. *Let $p, q > 0$ and $n = p + q$. Let $X \cdot Y = C_{p,q}$ be a Boolean decomposition of $C_{p,q}$, where X is an $n \times r$ Boolean matrix and Y is an $r \times n$ Boolean matrix. Denote by $x_1, \ldots, x_r$ the columns of X, and by $y_1, \ldots, y_r$ the rows of Y. Then:*

1. *For each $i \in [r]$, if x_i has more than p ones then y_i is the all-zero vector, and if y_i has more than p ones then x_i is the all-zero vector.*
2. *For each $i \in [r]$, if $|x_i|, |y_i| > 0$, then $|x_i| + |y_i| \leq p + 1$.*
3. *If $q \geq p - 1$, then there exist n indices $i_1, ..., i_n$, such that $|x_{i_j}|, |y_{i_j}| > 0$ for every $j \in [n]$.*

Proof. For simplicity, denote $C = C_{p,q}$. If we write the decomposition $X \cdot Y = C$ with outer products, then $C = \sum_{i=1}^{r} x_i \otimes y_i$.

First note that if we have an i such that x_i has more than p ones, and y_i is not the all-zero vector, then $x_i \otimes y_i$ has a column with more than p ones. Since the addition is the Boolean addition, then $\sum_{i=1}^{r} x_i \otimes y_i \neq C$. A similar argument shows that if y_i has more than p ones then x_i is the all-zero vector. Thus, item (1) follows.

Assume now, by contradiction, that item (2) does not hold. Thus, there exists an i, such that $|x_i|, |y_i| > 0$ and $|x_i|+|y_i| > p+1$. Let $|x_i| = s$ and $|y_i| = \ell$, where by our assumption $\ell \geq p - s + 2$. Thus, the matrix $x_i \otimes y_i$ has an all-one submatrix B of size $s \times \ell$. Since the addition is Boolean, $C_{p,q}$, also has an all-one submatrix of size $s \times \ell \geq s \times (p - s + 2)$, in contradiction to Claim 2.3.

It remains to prove item (3). Since $q \geq p - 1$, then C is an isolation matrix. Therefore, its Boolean rank is $n = p + q$. Assume by contradiction that there are strictly less than n pairs x_i, y_i such that $|x_i|, |y_i| > 0$. Note that if x_i or y_i is the all-zero vector then $x_i \otimes y_i$ is the all-zero matrix. Thus, we can remove from X any column x_i which is the all-zero vector, and remove the corresponding row y_i from Y, and similarly, remove from Y any row y_j which is the all-zero vector, and remove the corresponding column x_j from X. We get two new matrices X', Y', such that $X' \cdot Y' = C$, where the size of X' is $n \times \ell$, the size of Y' is $\ell \times n$, and by our assumption $\ell < n$. Therefore, the Boolean rank of C is strictly less than n, and we get a contradiction. □

Lemma 2.5. *Let $p, q > 0$ and $q \geq p-1$, and let $n = p+q$. Let $X \cdot Y = C_{p,q}$ be a Boolean decomposition of $C_{p,q}$, where X is an $n \times r$ Boolean matrix and Y is an $r \times n$ Boolean matrix. Then the sum of the number of ones in X and the number of ones in Y is at most $(p + 1)n + (r - n)n$.*

Proof. Let $x_1, \ldots, x_r$ be the columns of X, and $y_1, \ldots, y_r$ the rows of Y. By Lemma 2.4, there exist n indices $i_1, ..., i_n$, such that $|x_{i_j}|, |y_{i_j}| > 0$ for every $j \in [n]$. Furthermore, for these indices it holds that $|x_{i_j}| + |y_{i_j}| \leq p + 1$. Assume, without loss of generality, that these are indices $1, ..., n$.

As for the remaining pairs, x_i, y_i, for $n < i \leq r$: by Lemma 2.4, if $|x_i|, |y_i| > 0$ then $|x_i| + |y_i| \leq p + 1$, and if $|x_i| \geq p + 1$ then y_i is the all-zero vector, and similarly if $|y_i| \geq p + 1$ then x_i is the all-zero vector. Thus, $|x_i| + |y_i|$ is maximized when x_i or y_i is the all-zero vector and the other is the all-one vector, since in this case $|x_i| + |y_i| = n = p + q \geq p + 1$.

Hence, the sum of the number of ones in X and the number of ones in Y is at most $(p + 1)n + (r - n)n$. □

Proof of Theorem 1.2. Consider the Boolean decomposition $X \cdot Y = A_{k,t}$, where X is a matrix of size $\binom{k}{t} \times k$ and Y is a matrix of size $k \times \binom{k}{t}$, and X and Y each contain all characteristic vectors of subsets in $\binom{[k]}{t}$.

Since $C_{p,q}$ is a submatrix of $A_{k,t}$ then there exist two matrices $X' \subseteq X, Y' \subseteq Y$, such that $X' \cdot Y' = C_{p,q}$. Notice that X' is an $n \times k$ matrix and Y' is an $k \times n$ matrix, where $n = p + q$, and the sum of the number of ones in X and the number of ones in Y is exactly $2nt$. But, by Lemma 2.5, the total number of 1's in both X' and Y' is at most $(p+1)n + (k-n)n$. Thus, $2nt \leq (p+1)n + (k-n)n$. Hence, $p+q = n \leq k - 2t + p + 1$, as claimed. □

3 The range of $2t \leq p \leq t^2$

The circulant decomposition given in Lemma 2.1 is not suitable for $p \geq 2t$, since if we take the decomposition $C_{i+j-1,z-i-j+1} = C_{i,z-i} \cdot C_{j,z-j}$, and let $p = i + j - 1$ and $p \geq 2t$, then $i + j \geq 2t + 1$. Thus, either i or j are strictly larger than t, and therefore, the rows of $C_{i,z-i}$ or the columns of $C_{j,z-j}$ cannot represent subsets of size t of $[k]$.

However, Theorem 1.3 stated in Section 1.1 and proved next, shows that when $2t \leq p \leq t^2$, there exists a different circulant decomposition $C_{p,q} = X \cdot Y$, in which each row of X and each column of Y has exactly t ones as required. See Figure 2 for an illustration, and note also that since $2t \leq p \leq t^2$ then $t \geq 2$.

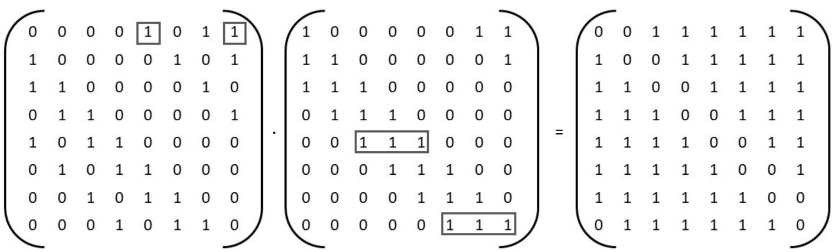


Figure 2: The construction described in Theorem 1.3 for $t = 3, p = 6, q = 2$. The matrices presented are $X \cdot Y = W$, where W is achieved from $C_{p,q}$ by moving the last row of $C_{p,q}$ as defined in the introduction to be first. The first row x_1 of X begins with $q + t - 1$ zeros, and then every t positions there is a one outlined with a rectangle. The remaining positions of x_1 contain zeros and ones for a total of t ones in x_1. The matrix $Y = C_{t,p+q-t}$. The ones in the columns of Y that intersect the outlined ones in x_1 are also outlined with rectangles.

Proof of Theorem 1.3. Let W be the matrix achieved from $C_{p,q}$ by moving the last row of $C_{p,q}$ as defined in the introduction to be first. Hence, the first row of W has q zeros followed by p ones. It is enough to show that there exist two square matrices X, Y, of size $p + q$, such that each row of X and each column of Y has exactly t ones, and $X \cdot Y = W$.

The matrix Y is just the matrix $C_{t,p+q-t}$ as defined in the introduction, and thus each column has t ones as required. The matrix X is also circulant and is defined as follows. The first row x_1 of X begins with $q + t - 1$ zeros. The remaining $p - t + 1 \geq 2t - t + 1 = t + 1$ coordinates of x_1 start with a one and then there is a one every t positions, and a one in the last position of x_1. The remaining positions have ones and zeros in an arbitrary order, for a total of t ones in x_1. Note that there are at most $t - 1$ zeros between every two consecutive ones in x_1, and in the extreme case of $p = t^2$, there are exactly $t - 1$ zeros between every two consecutive ones.

Finally, we must show that $X \cdot Y = W$. Since both X and Y are circulant, the resulting product matrix $X \cdot Y$ is circulant. Thus, it is sufficient to prove that the first row of $X \cdot Y$ is equal to the first row $(0, 0, ..., 0, 1, 1, ..., 1)$ of W. Let $y_1, ..., y_{p+q}$ be the columns of Y.

- Columns $y_1, ..., y_q$ have ones only in positions at most $q + t - 1$, whereas x_1 has zeros in the first $q + t - 1$ positions. Hence, $x_1 \cdot y_i = 0$, for $1 \le i \le q$, as required.
- Now consider the last p columns of Y. Note that for each such column y_j, at least one of the t consecutive ones of y_j avoids the $q + t - 1$ consecutive zeros of x_1. Furthermore, every t consecutive columns of Y have a one in a common row. It is easy to verify that columns y_j, for $q + 1 \le j \le q + t$, intersect with the first one in x_1, as they all have a one in position $q + t$. The next t columns of Y all have a one in position $q + 2t$, and since x_1 has a one every t coordinates, these columns also intersect with x_1, and so on. The last t columns of Y intersect with the last one of x_1.

Hence, $X \cdot Y = W$ as claimed, and the theorem follows. □

4 The range of large p

Bollobás [3] proved that for any m pairs of subsets (A_i, B_i), such that $|A_i| = a, |B_i| = b$ for $1 \le i \le m$, and $A_i \cap B_j = \emptyset$ if and only if $i = j$, it holds that $m \le \binom{a+b}{a}$. An immediate corollary of this theorem is that the largest circulant submatrix $C_{p,q}$ of $A_{k,t}$, for $q = 1$, is of size $\binom{2t}{t} \times \binom{2t}{t}$. This result is tight.

This theorem has several generalizations. Among them is a result of Frankl [9] and Kalai [15] that considered the skew version of the problem, and showed that the same bound holds even under the following relaxed assumptions: Let (A_i, B_i) be pairs of sets, such that $|A_i| = a, |B_i| = b$ for $1 \le i \le m$, $A_i \cap B_i = \emptyset$ for every $1 \le i \le m$, and $A_i \cap B_j \ne \emptyset$ if $i > j$. Then $m \le \binom{a+b}{a}$.

We immediately get the following corollary, where here and throughout this section we assume that the first row of $C_{p,q}$ has q zeros followed by p ones.

Corollary 4.1. *Let $C_{p,q}$ be a submatrix of $A_{k,t}$ of size $n \times n$, for a given fixed q. Then, $n \le \binom{2t}{t} + q - 1$, that is, $p \le \binom{2t}{t} - 1$.*

Proof. Consider the submatrix B of $C_{p,q}$ that is defined by the first $p+1$ rows and columns of $C_{p,q}$. The matrix B maintains the conditions of the Theorem of Frankl and Kalai, and, thus, its size is at most $\binom{2t}{t} \times \binom{2t}{t}$. Hence, $n \le \binom{2t}{t} + q - 1$ as claimed, and $p \le \binom{2t}{t} - 1$. □

The following lemma presents a simple construction of a large circulant submatrix $C_{p,q}$ of $A_{k,t}$ for a given fixed q. See also Figure 3 for an illustration.

Lemma 4.2. *Let $q > 0$, $t \ge q$, where $t \bmod q = 0$. Then $C_{p,q}$ is a submatrix of $A_{k,t}$, for $p = q \cdot (\binom{2t/q}{t/q} - 1)$ and $k \ge 3t - t/q$.*

Proof. Let $n = \binom{2t/q}{t/q}$. The matrix $C_{p,q}$, where $p + q = q \cdot n$, can be partitioned into q disjoint submatrices of size $n \times (p + q)$, as follows. The ith submatrix, $1 \le i \le q$, contains rows $i + j \cdot q$, $0 \le j \le n - 1$, of $C_{p,q}$. Each such submatrix is a blowup of $C_{n-1,1}$, since we can partition each row of these q submatrices into blocks of q consecutive entries, where the blocks of the ith submatrix are shifted by one position compared to the blocks of the

$C_{10,2}$ =

1 2 a b	1 2 a c	1 3 a c	1 3 a d	1 4 a d	1 4 b c	2 3 b c	2 3 b d	2 4 b d	2 4 c d	3 4 c d	3 4 a b	
0	0	1	1	1	1	1	1	1	1	1	1	3, 4
1	0	0	1	1	1	1	1	1	1	1	1	b, d
1	1	0	0	1	1	1	1	1	1	1	1	2, 4
1	1	1	0	0	1	1	1	1	1	1	1	b, c
1	1	1	1	0	0	1	1	1	1	1	1	2, 3
1	1	1	1	1	0	0	1	1	1	1	1	a, d
1	1	1	1	1	1	0	0	1	1	1	1	1, 4
1	1	1	1	1	1	1	0	0	1	1	1	a, c
1	1	1	1	1	1	1	1	0	0	1	1	1, 3
1	1	1	1	1	1	1	1	1	0	0	1	a, b
1	1	1	1	1	1	1	1	1	1	0	0	1, 2
0	1	1	1	1	1	1	1	1	1	1	0	c, d

Figure 3: The construction described in Lemma 4.2, for $t = 4, p = 10, q = 2$. The matrix $C_{10,2}$ is composed of two submatrices, one containing the odd rows and one the even rows. Each row of these submatrices is partitioned into $n = 6$ blocks of size $q = 2$, as outlined by rectangles. The first submatrix is the intersection matrix of all subsets of size 2 of $[4]$, and the second submatrix is the intersection matrix of all subsets of size 2 of $\{a, b, c, d\}$, where in both cases each of the subsets assigned to the columns appears twice (in columns belonging to the same block). Since the subsets assigned to the first submatrix are disjoint from the subsets assigned to the second submatrix, and the blocks in the two submatrices are shifted, this defines an assignment of different subsets of $\{1, 2, 3, 4, a, b, c, d\}$, each of size at most 4, to the columns and rows of $C_{10,2}$.

previous submatrix (in a circulant way). Thus, the entries in each block are identical (either all ones or all zeros). For example, the first row of the first submatrix starts with a block of q zeros, followed by $n - 1$ blocks of q ones.

Hence, we can view each of these q submatrices as the intersection matrix of the two families of all subsets of size t/q of $[2t/q]$ (since each subset intersects with all subsets but one), where columns belonging to the same block in a submatrix are assigned the same subset. Now, if we take disjoint copies of the subsets assigned to each submatrix, and label each column in $C_{p,q}$ with the subset that is the union of all subsets of size t/q assigned to this column, then we get $q \cdot n$ different subsets, each of size t, assigned to the columns (the subsets are different because the blocks in each submatrix are shifted compared to the other submatrices). As to the rows, each row is assigned a different subset of size t/q, and therefore, we can define $t - t/q$ additional new elements that do not belong to any of the subsets, and add them to each row, so that the rows are also assigned subsets of size t. Finally, by taking the union of all subsets, we get that $k \geq 2t + t - t/q = 3t - t/q$. □

The size of the construction given in Lemma 4.2 is quite far from the upper bound given in Corollary 4.1. As we show in the next subsection, there exists a slightly larger construction for $q = 2$. Finally, in Subsection 4.2, we show that the upper bound of Corollary 4.1 is tight for $t = 2, p = \binom{2t}{t} - 1 = 5$ and $q = 1, 3$, but there is no k for which $C_{5,2}$ is a submatrix of $A_{k,2}$ when $q \neq 1, 3$.

4.1 The values $q = 2$ and $p = 2^t + 2^{t-2} - 2$

We now prove Theorem 1.4 and show a construction of $C_{p,q}$ for $q = 2$ and p that is exponential in t. The construction we present is recursive in nature, and exploits the fact that $C_{p,2}$ has two blocks on the main diagonal, such that each one of these blocks is half the size of $C_{p,2}$, and the structure of each block is almost identical to that of $C_{p,q}$, where the only difference is that there is a 1 in the first position of the last row instead of a zero in $C_{p,q}$. This small difference complicates the recursive argument. The details of the proof follow. See Figure 4 for an illustration of the proof of Theorem 1.4.

$C_{8,2}$ =

1 5 8	1 2 8	3 2 8	3 5 8	3 7 8	1 6 9	1 2 9	4 2 9	4 6 9	4 7 9	
0	0	1	1	1	1	1	1	1	1	7, 3, 9
1	0	0	1	1	1	1	1	1	1	7, 5, 9
1	1	0	0	1	1	1	1	1	1	7, 1, 9
1	1	1	0	0	1	1	1	1	1	2, 1, 9
1	1	1	1	0	0	1	1	1	1	2, 5, 4
1	1	1	1	1	0	0	1	1	1	7, 4, 8
1	1	1	1	1	1	0	0	1	1	7, 6, 8
1	1	1	1	1	1	1	0	0	1	7, 1, 8
1	1	1	1	1	1	1	1	0	0	2, 1, 8
0	1	1	1	1	1	1	1	1	0	2, 6, 3

Figure 4: The construction of $C_{p,q}$ described in Theorem 1.4, for $q = 2$ and $p = 2^t + 2^{t-2} - 2$, where $t = 3$. The column indices are written above the matrix $C_{8,2}$ and the row indices to the right of the matrix.

Proof of Theorem 1.4. Let $h = (p + q)/2$. We prove by induction on t that $C_{p,q}$ is the intersection matrix of two families of t-subsets

$$\mathcal{F}_{a,b} = \{F_1, ..., F_{p+q}\}, \qquad \mathcal{G}_{a,b} = \{G_1, ..., G_{p+q}\},$$

where the subsets in $\mathcal{F}_{a,b}$ are the row indices and the subsets in $\mathcal{G}_{a,b}$ are the column indices, and a, b are two integers with the following properties:

- $a \in G_1, ..., G_h$, and $a \in F_{h+1}, ..., F_{p+q-1}$.
- $b \in G_{h+1}, ..., G_{p+q}$, and $b \in F_1, ..., F_{h-1}$.
- a, b appear only in the subsets specified above. In particular, $a, b \notin F_{p+q}$.

Let $\tilde{C}_{p,q}$ be the matrix that is achieved from $C_{p,q}$, by modifying to 1 the first position of the last row of $C_{p,q}$, and let $\tilde{\mathcal{F}}_{a,b}$ be a family that is identical to $\mathcal{F}_{a,b}$ with one difference: the subset F_{p+q} also contains the element a. It is not hard to verify that if $C_{p,q}$ is the intersection matrix of $\mathcal{F}_{a,b}$ and $\mathcal{G}_{a,b}$, then $\tilde{C}_{p,q}$ is the intersection matrix of $\tilde{\mathcal{F}}_{a,b}$ and $\mathcal{G}_{a,b}$.

The base of the induction is $t = 3$, and the construction of $C_{8,2}$ is given in Figure 4, where in this case $a = 8, b = 9$. Note that if we modify the last row index $\{2, 6, 3\}$ to be $\{2, 6, 3, 8\}$, then we get a construction of $\tilde{C}_{8,2}$ as claimed.

Assume now that $t > 3$, let $p_t = 2^t + 2^{t-2} - 2$ and $p_{t-1} = 2^{t-1} + 2^{t-3} - 2$, and consider $C_{p_t,q}$. Then it has the following structure: there are two matrices of the form $\tilde{C}_{p_{t-1},q}$ on the main diagonal, and two blocks of size $(p_t + q)/2$ that are all one, but the leftmost entry on the bottom row of each of these blocks that is a 0.

By the induction hypothesis there exist, as specified above, two families of $(t-1)$-subsets

$$\mathcal{F}_{a,b} = \{F_1, ..., F_{p_{t-1}+q}\}, \qquad \mathcal{G}_{a,b} = \{G_1, ..., G_{p_{t-1}+q}\},$$

whose intersection matrix is $C_{p_{t-1},q}$.

Let $\mathcal{F}'_{b,a} = \{F'_1, ..., F'_{p_{t-1}+q}\}$ be a family of subsets that is identical to $\mathcal{F}_{a,b}$, but a, b are interchanged in all subsets. That is, for $1 \leq i \leq p_{t-1} + q$:

$$F'_i = \begin{cases} F_i \setminus \{a\} \cup \{b\}, & \text{if } a \in F_i, \\ F_i \setminus \{b\} \cup \{a\}, & \text{if } b \in F_i, \\ F_i, & \text{if } a, b \notin F_i. \end{cases}$$

Similarly define $\mathcal{G}'_{b,a} = \{G'_1, ..., G'_{p_{t-1}+q}\}$, which is identical to $\mathcal{G}_{a,b}$, but a, b are interchanged in all subsets. Note that since a, b appear only in subsets as specified above, then it also holds that $C_{p_{t-1},q}$ is the intersection matrix of the two families $\mathcal{F}'_{b,a}$ and $\mathcal{G}'_{b,a}$.

Now let c, d be two new elements that do not appear in any of the above families, and define the following families:

$$\begin{aligned} \mathcal{F}_d &= \{F_1 \cup \{d\}, F_2 \cup \{d\}, ..., F_{p_{t-1}+q-1} \cup \{d\}, F_{p_{t-1}+q} \cup \{a\}\}, \\ \mathcal{F}_c &= \{F'_1 \cup \{c\}, F'_2 \cup \{c\}, ..., F'_{p_{t-1}+q-1} \cup \{c\}, F'_{p_{t-1}+q} \cup \{b\}\}, \\ \mathcal{G}_c &= \{G_1 \cup \{c\}, G_2 \cup \{c\}, ..., G_{p_{t-1}+q} \cup \{c\}\}, \\ \mathcal{G}_d &= \{G'_1 \cup \{d\}, G'_2 \cup \{d\}, ..., G'_{p_{t-1}+q} \cup \{d\}\}. \end{aligned}$$

Finally, define the families $\mathcal{F}_{c,d}, \mathcal{G}_{c,d}$ as follows:

$$\mathcal{F}_{c,d} = \mathcal{F}_d \cup \mathcal{F}_c, \qquad \mathcal{G}_{c,d} = \mathcal{G}_c \cup \mathcal{G}_d.$$

It is clear that $\mathcal{F}_{c,d}, \mathcal{G}_{c,d}$ are two families of t-sets, each of size $p_t + q$, and their structure is as claimed above, where c and d are in the role of a and b, respectively. It remains to prove that $C_{p_t,q}$ is the intersection matrix of $\mathcal{F}_{c,d}, \mathcal{G}_{c,d}$. First note that by the induction hypothesis, and using the structure of the subsets we defined, $\tilde{C}_{p_{t-1},q}$ is the intersection matrix of $\mathcal{F}_d, \mathcal{G}_c$, as well as the intersection of $\mathcal{F}_c, \mathcal{G}_d$.

Consider now the matrix C which is the intersection matrix of $\mathcal{F}_d, \mathcal{G}_d$. It is clear that the first $p_{t-1} + q - 1$ rows of C are all ones, since the first $p_{t-1} + q - 1$ families of $\mathcal{F}_d, \mathcal{G}_d$ all contain d. We next show that the last row of C is of the form $(0, 1, 1, ..., 1)$. By the induction hypothesis, the intersection of $F_{p_{t-1}+q}$ with all subsets of $\mathcal{G}_{a,b}$ gives a vector of the form $(0, 1, 1, ...1, 0)$. Thus, since $a, b \notin F_{p_{t-1}+q}$ and $\mathcal{G'}_{b,a}$ is identical to $\mathcal{G}_{a,b}$, but a, b are interchanged in all subsets, then the intersection of of $F_{p_{t-1}+q}$ with all subsets of $\mathcal{G'}_{b,a}$ results also with the vector $(0, 1, 1, ...1, 0)$. Since the last subset of $\mathcal{F}_d$ is defined as $F_{p_{t-1}+q} \cup \{a\}$ and the last subset of $\mathcal{G}_d$ is $G'_{p_{t-1}+q} \cup \{d\}$, and $a \in G'_{p_{t-1}+q}$, then we get that $F_{p_{t-1}+q} \cup \{a\}$ and $G'_{p_{t-1}+q} \cup \{d\}$ also intersect as required.

A similar argument shows that the intersection matrix of $\mathcal{F}_d, \mathcal{G}_d$ is also a matrix that is all one, but the first element on the last row of this matrix, which is a zero. This completes the proof of the theorem. □

4.2 The values $t = 2, p = \binom{2t}{t} - 1, q > 0$

Finally, we address the range of values of $t = 2$ and $p = \binom{2t}{t} - 1 = 5$. We first show that $C_{p,q}$ is a submatrix of $A_{k,t}$ for these values of p and t, and for $q = 1, 3$.

Lemma 4.3. *Let $t = 2$ and $p = \binom{2t}{t} - 1 = 5$. Then $C_{p,q}$ is a submatrix of $A_{k,t}$ for $q = 1$ and $k \geq 5$, or for $q = 3$ and $k \geq 6$.*

Proof. If $t = 2, p = 5, q = 1$, then $C_{5,1}$ is a submatrix of $A_{5,2}$. Simply take as row/column indices all subsets of size 2 of $[4]$. As to the case of $t = 2, p = 5, q = 3$, Figure 5 shows that $C_{5,3}$ is a submatrix of $A_{k,2}$, for any $k \geq 6$. □

$$
\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1
\end{pmatrix}
\cdot
\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
=
\begin{pmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}
$$

Figure 5: A construction of $C_{p,q}$ for $t = 2, p = 5, q = 3$.

We conclude by proving that $C_{p,q}$ is not a submatrix of $A_{k,t}$ for $t = 2, p = 5$ and $q \neq 1, 3$. Unfortunately, this proof cannot be generalized to the case of $p = \binom{2t}{t} - 1$ and $t > 2$. Thus, it remains an open problem to determine for what values of $q > 1$ is $C_{p,q}$ a submatrix of $A_{k,t}$, when $p = \binom{2t}{t} - 1$ and $t > 2$.

Lemma 4.4. *Let $t = 2$, $p = \binom{2t}{t} - 1 = 5, q \neq 1, 3$, $q > 0$. Then $C_{p,q}$ is not a submatrix of $A_{k,t}$ for any k.*

Proof. Assume by contradiction that $C_{5,q}$ is a submatrix of $A_{k,2}$ for some k, where the first row of $C_{5,q}$ starts with $q \neq 1, 3$ zeros, followed by p ones. Let $n = p + q = q + 5 \geq 7$ be the size of $C_{5,q}$, and let A_i, B_i, $0 \leq i \leq n-1$, be the 2-uniform subsets defining the row and column indices, respectively, of $C_{5,q}$.

Assume first that there exists some i such that $B_i \cap B_{(i+1) \bmod n} = \emptyset$, that is, two consecutive column indices are disjoint. Since $C_{5,q}$ is circulant, then we can assume that $i = 0$, that is, $B_0 \cap B_1 = \emptyset$. Since B_0 and B_1 both intersect with A_3, A_4, A_5, then each of these three subsets contains one element from each of B_0, B_1. Furthermore, as all subsets are different and of size 2, then each element of B_0, B_1 is contained in at most two of these three subsets.

Next consider B_2. It also intersects with A_3, A_4, A_5, and since there is no common element of B_0, B_1 in these three subsets, then B_2 also includes two elements from $B_0 \cup B_1$ (although here B_2 can contain two elements from the same subset B_0 or B_1).

Now, consider $A_{7 \bmod n}$, where if $q = 2$ then $A_{7 \bmod n} = A_0$ and otherwise, $A_{7 \bmod n} = A_7$. In both cases, since $p = 5$, the row labeled by $A_{7 \bmod n}$ starts with two zeros followed by a one. Thus, since $A_{7 \bmod n} \cap B_2 \neq \emptyset$, then $A_{7 \bmod n}$ contains an element from $B_0 \cup B_1$, in contradiction to the fact that $A_{7 \bmod n} \cap B_0 = A_{7 \bmod n} \cap B_1 = \emptyset$.

Hence, we can assume from now on that $B_i \cap B_{(i+1) \bmod n} \neq \emptyset$, and similarly that $A_i \cap A_{(i+1) \bmod n} \neq \emptyset$, for $0 \leq i \leq n-1$. There are two cases:

- There exists an i such that $B_i \cap B_{(i+1) \bmod n} \cap B_{(i+2) \bmod n} \neq \emptyset$. Since $C_{p,q}$ is circulant, then assume that $i = 0$, and let $b \in B_0, B_1, B_2$. Thus, $B_0 = \{b_0, b\}, B_1 = \{b_1, b\}, B_2 = \{b_2, b\}$. From this and the structure of $C_{5,q}$, we can deduce the following:

  1. $b_0 \in A_1$, $A_2 = \{b_0, b_1\}$, and $b \in A_3, A_4, A_5$.
  2. The row labeled by A_6 starts with a zero followed by 5 ones, and so $b \notin A_6$. But $A_6 \cap B_1 \neq \emptyset, A_6 \cap B_2 \neq \emptyset$. Thus, $A_6 = \{b_1, b_2\}$.
  3. $b \notin B_3$ as $B_3 \cap A_3 = \emptyset$. But $B_3 \cap B_2 \neq \emptyset$, and therefore, $b_2 \in B_3$.
  4. $b, b_0, b_1 \notin B_3$ as also $B_3 \cap A_2 = \emptyset$. But $B_3 \cap A_5 \neq \emptyset$ and $A_5 \cap A_6 \neq \emptyset$. Therefore, $b_2 \in A_5$.
  5. Since $b, b_0, b_1 \notin B_3$ and $B_3 \cap A_4 \neq \emptyset$, then there exists a new element $b_3 \in B_3 \cap A_4$.
  6. $A_4 \cap B_4 = \emptyset$ and so $b \notin B_4$. Hence, $b_2 \in B_4$ since $B_4 \cap A_5 \neq \emptyset$. In a similar way, $b_1 \in B_5$.

  Hence, the subsets defining the first seven rows and columns of $C_{5,q}$ have the following structure so far, where they are written to the left and above the submatrix:

	b_0, b	b_1, b	b_2, b	b_2, b_3	b_2	b_1	
	0	0					
b_0	1	0	0				
b_0, b_1	1	1	0	0			
b	1	1	1	0	0		
b, b_3	1	1	1	1	0	0	
b, b_2	1	1	1	1	1	0	0
b_1, b_2	0	1	1	1	1	1	0

Now, if $q \geq 4$, we already get a contradiction, since in $C_{5,q}$ it holds that $A_2 \cap B_5 = \emptyset$, whereas here $b_1 \in A_2 \cap B_5$.

Therefore, assume that $q = 2$, and so all remaining entries in the submatrix above are ones. From the structure of the submatrix and the information we have so far, we can deduce that $A_1 = \{b_0, b_3\}$ and hence $B_5 = \{b_1, b_0\}$ (since $B_5 \cap A_1 \neq \emptyset$ and $B_5 \cap A_4 = \emptyset$ and so $b_3 \notin B_5$). But then since $b_0, b_1 \notin A_0$, we get a contradiction since $A_0 \cap B_5 \neq \emptyset$.

- $B_i \cap B_{(i+1) \bmod n} \cap B_{(i+2) \bmod n} = \emptyset$, but $B_i \cap B_{(i+1) \bmod n} \neq \emptyset$, for $0 \leq i \leq n-1$. Thus, $B_i = \{b_i, b_{(i+1) \bmod n}\}$, where some of the b_i's may be identical.

  If all b_i's in the subsets $B_q, B_{q+1}, B_{q+2}, B_{q+3}, B_{q+4}$ are different, then A_0 cannot intersect with these subsets, since $|A_0| = 2$. Hence, there exist $0 \leq i \neq j \leq 4$ such that $b_{q+i} = b_{q+j}$. Assume, without loss of generality, that $i = 0$ (as the matrix is circulant). Since the intersection of every three consecutive subsets is empty, and each subset contains two different elements, then $j \neq 1, 2$. If $j = 3$ then $b_q = b_{q+3}$, and since A_2 does not intersect with B_q, B_{q+1} then $b_q, b_{q+1}, b_{q+2} \notin A_2$. But A_2 intersects with $B_{q+2} = \{b_{q+2}, b_{q+3} = b_q\}$, and we get a contradiction. A similar contradiction is achieved if $j = 4$ when considering A_5.

Thus, in all cases we get a contradiction and the lemma follows. □

ORCID iDs

Michal Parnas https://orcid.org/0000-0003-0189-6999

References

[1] B. Alspach, Isomorphism and cayley graphs on abelian groups, in: *Graph Symmetry*, Springer, volume 497 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pp. 1–22, 1997, doi:10.1007/978-94-015-8937-6_1.

[2] L. B. Beasley, Isolation number versus Boolean rank, *Linear Algebra Appl.* **436** (2012), 3469–3474, doi:10.1016/j.laa.2011.12.013.

[3] B. Bollobás, On generalized graphs, *Acta Math. Acad. Sci. Hungar.* **16** (1965), 447–452, doi:10.1007/bf01904851.

[4] P. Borg, The maximum sum and the maximum product of sizes of cross-intersecting families, *European J. Comb.* **35** (2014), 117–130, doi:10.1016/j.ejc.2013.06.029.

[5] K. Butler and J. R. Krabill, Circulant Boolean relation matrices, *Czechoslovak Math. J.* **24** (1974), 247–251.

[6] K. Butler and Š. Schwarz, The semigroup of circulant Boolean matrices, *Czechoslovak Math. J.* **26** (1976), 632–635.

[7] H. Daode, On circulant Boolean matrices, *Linear Algebra Appl.* **136** (1990), 107–117, doi:10.1016/0024-3795(90)90022-5.

[8] P. Erdős, C. Ko and R. Rado, Intersection theorems for systems of finite sets, *Q. J. Math.* **12** (1961), 313–320, doi:10.1093/qmath/12.1.313.

[9] P. Frankl, An extremal problem for two families of sets, *European J. Comb.* **3** (1982), 125–127, doi:10.1016/s0195-6698(82)80025-5.

[10] P. Frankl and N. Tokushige, Some best possible inequalities concerning cross-intersecting families, *J. Comb. Theory Ser. A* **61** (1992), 87–97, doi:10.1016/0097-3165(92)90054-x.

[11] D. Gerbner, N. Lemons, C. Palmer, D. Pálvölgyi, B. Patkós and V. Szécsi, Almost cross-intersecting and almost cross-sperner pairs of families of sets, *Graphs Comb.* **29** (2013), 489–498, doi:10.1007/s00373-012-1138-2.

[12] D. Gerbner, N. Lemons, C. Palmer, B. Patkós and V. Szécsi, Almost intersecting families of sets, *SIAM J. Discrete Math.* **26** (2012), 1657–1669, doi:10.1137/120878744.

[13] H. Gruber and M. Holzer, Inapproximability of nondeterministic state and transition complexity assuming $\mathrm{P} \neq \mathrm{NP}$, in: *Developments in language theory*, Springer, Berlin, volume 4588 of *Lecture Notes in Comput. Sci.*, pp. 205–216, 2007, doi:10.1007/978-3-540-73208-2_21.

[14] A. J. Hilton and E. C. Milner, Some intersection theorems for systems of finite sets, *Quart. J. Math. Oxford Ser. (2)* **18** (1967), 369–384, doi:10.1093/qmath/18.1.369.

[15] G. Kalai, Intersection patterns of convex sets, *Israel J. Math.* **48** (1984), 161–174, doi:10.1007/bf02761162.

[16] E. Kushilevitz and N. Nisan, *Communication Complexity*, Cambridge University Press, Cambridge, 1996, doi:10.1017/cbo9780511574948.

[17] M. Matsumoto and N. Tokushige, The exact bound in the erdös-ko-rado theorem for cross-intersecting families, *J. Combin. Theory Ser. A* **52** (1989), 90–97, doi:10.1016/0097-3165(89)90065-4.

[18] J. Orlin, Contentment in graph theory: covering graphs with cliques, *Indag. Math.* **80** (1977), 406–424, doi:10.1016/1385-7258(77)90055-5.

[19] M. Parnas, D. Ron and A. Shraibman, The Boolean rank of the uniform intersection matrix and a family of its submatrices, *Linear Algebra Appl.* **574** (2019), 67–83, doi:10.1016/j.laa.2019.03.027.

[20] M. Parnas and A. Shraibman, On maximal isolation sets in the uniform intersection matrix, *Australas. J. Comb.* **77** (2020), 285–300, https://ajc.maths.uq.edu.au/?page=get_volumes&volume=77.

[21] L. Pyber, A new generalization of the Erdős-Ko-Rado theorem, *J. Comb. Theory Ser. A* **43** (1986), 85–90, doi:10.1016/0097-3165(86)90025-7.

[22] Š. Schwarz, Circulant Boolean relation matrices, *Czechoslovak Math. J.* **24** (1974), 252–253.

[23] A. Scott and E. Wilmer, Hypergraphs of bounded disjointness, *SIAM J. Discrete Math.* **28** (2014), 372–384, doi:10.1137/130925670.

[24] Y. Shitov, On the complexity of Boolean matrix ranks, *Linear Algebra Appl.* **439** (2013), 2500–2502, doi:10.1016/j.laa.2013.06.033.

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P1.09
https://doi.org/10.26493/2590-9770.1377.8e9
(Also available at http://adam-journal.eu)

On avoiding 1233

Toufik Mansour*
Department of Mathematics, University of Haifa, 3498838 Haifa, Israel

Mark Shattuck
Department of Mathematics, University of Tennessee, 37996 Knoxville, TN

Received 12 August 2020, accepted 16 June 2021, published online 11 April 2022

Abstract

In this paper, we establish a recurrence relation for finding the generating function for the number of k-ary words of length n that avoid 1233 for arbitrary k. Comparable generating function formulas may also be found counting words where a single permutation pattern of length three is avoided in addition to 1233.

Keywords: k-ary words, Kernel method, Avoiding 1233.

Math. Subj. Class.: 05A15, 05A05

1 Introduction

We denote the set of all words of length n over the alphabet $[k] = \{1, \dots, k\}$ by $[k]^n$ and refer to members of $[k]^n$ as k-ary words. Let $\pi = \pi_1 \cdots \pi_n \in [k]^n$ and $\tau = \tau_1 \cdots \tau_m \in [\ell]^m$ such that each letter from $[\ell]$ appears at least once in τ (possibly with repetitions). We say that π *contains* τ if there exist indices $1 \leq i_1 < \cdots < i_m \leq n$ such that $\pi_{i_a} \Phi \pi_{i_b}$ if and only if $\tau_a \Phi \tau_b$, for any relation $\Phi \in \{<, =, >\}$ and $a, b \in [m]$. In this context, the word τ is called a *pattern*, and it is said that π *avoids* τ if π fails to contain τ per the preceding definition.

The area of permutation pattern avoidance has received considerable attention in recent decades; see, e.g., [13] and references therein. Alon and Friedgut [2] extended this study to avoidance on k-ary words in obtaining an upper bound on the number of permutations of length n that avoid a given pattern. The question of pattern avoidance on permutations was initiated by Knuth [6], who found that the number of permutations of length n that avoid the pattern τ for any $\tau \in S_3$ is given by the n-th Catalan number $\frac{1}{n+1}\binom{2n}{n}$. Later, Simion and Schmidt [12] extended this result by determining the number of permutations

*Corresponding author.
E-mail addresses: tmansour@univ.haifa.ac.il (Toufik Mansour), mshattuc@utk.edu (Mark Shattuck)

of length n that avoid all patterns in any subset T of S_3. Comparable results involving k-ary words were found by Burstein [4] and Albert et al. [1], and later by Burstein and Mansour [5], who allowed patterns to contain repeated letters. See also [11, 14] concerning the avoidance of 123 by words as well as [9] for general enumeration schemes for words avoiding a permutation pattern.

Concerning avoidance of patterns of length four by k-ary words, only the following more general results are known:

- Regev [10] showed that the number of k-ary words of length n that avoid $12\cdots(\ell+1)$ is asymptotic to
$$\frac{n^{\ell(k-\ell)}\ell^n}{\ell^{\ell(k-\ell)}\prod_{i=1}^{\ell}\prod_{j=1}^{k-\ell}(i+j-1)}.$$
This result was re-derived by Brändén and Mansour [3].
- The patterns $11\cdots1$ and $11\cdots121\cdots11$ have been considered in [5].
- Brändén and Mansour [3] (see also [8]) suggested an automaton for the enumeration of k-ary words of length n that avoid a fixed pattern for a given k.

We remark that it is a challenging problem in general to enumerate the k-ary words of length n that avoid a given pattern where k is arbitrary. Even in the case of a pattern of length four, the task at hand is still not a simple one. Here, we consider the problem of enumerating the members of $[k]^n$ that avoid 1233 for arbitrary k. The main purpose of this paper is to provide a recurrence relation on k for finding the number k-ary words of length n that avoid 1233, see Theorem 2.2 below. This recurrence represents an improvement in the case of 1233 over the general procedure described in [3, 8], which was derived using automata theory. Some further results are found involving avoidance of 1233 and a single pattern of length three.

2 k-ary words that avoid 1233

Let $a_{n,k}$ denote the number of k-ary words π of length n that avoid 1233. In order to write recurrences, we must refine $a_{n,k}$ according to the prefix of a word π. Given $s \geq 1$ and $i_1, \ldots, i_s \in [k]$, let $a_{n,k}(i_1, \ldots, i_s)$ denote the number of 1233-avoiding k-ary words π of length n having the form $\pi = i_1 \cdots i_s\pi'$, where π' is possibly empty. Clearly, we have $a_{n,1} = 1$ and $a_{n,2} = 2^n$. Henceforth, we may assume $k \geq 3$. By the definitions, for all $1 \leq i \leq k-2$,

$$a_{n,k}(i) = a_{n,k}(i,k) + \sum_{j=1}^{i} a_{n,k}(i,j) + \sum_{j=i+1}^{k-1} a_{n,k}(i,j).$$

Note that $a_{n,k}(i,k) = a_{n-1,k}(i)$ and $a_{n,k}(i,j) = a_{n-1,k}(j)$ for all $1 \leq j \leq i \leq k-2$. Thus,

$$a_{n,k}(i) = a_{n-1,k}(i) + \sum_{j=1}^{i} a_{n-1,k}(j) + \sum_{j=i+1}^{k-1} a_{n,k}(i,j).$$

Next observe that a k-ary word of the form $\pi = ij\pi'$ with $1 \le i < j \le k-1$ must have any letters from $[j+1,k] = \{j+1, j+2, \ldots, k\}$ distinct in order to avoid 1233. If we assume that exactly ℓ letters of π belong to $[j+1,k]$, then there are $\binom{k-j}{\ell}$ choices for these letters, $\binom{n-2}{\ell}$ choices for their positions within π and $\ell!$ ways in which to order these letters within their positions. Thus,

$$a_{n,k}(i,j) = \sum_{\ell=0}^{k-j} \ell! \binom{n-2}{\ell}\binom{k-j}{\ell} a_{n-1-\ell,j}(i).$$

Hence, for all $1 \le i \le k-2$,

$$a_{n,k}(i) = a_{n-1,k}(i) + \sum_{j=1}^{i} a_{n-1,k}(j) + \sum_{j=i+1}^{k-1}\sum_{\ell=0}^{k-j} \ell! \binom{n-2}{\ell}\binom{k-j}{\ell} a_{n-1-\ell,j}(i), \tag{2.1}$$

with $a_{n,k}(k) = a_{n,k}(k-1) = a_{n-1,k}$.

In order to study the sequence determined by recurrence (2.1), we define the distribution polynomial

$$A_{n,k}(v) = \sum_{i=1}^{k} a_{n,k}(i) v^{i-1}, \qquad n,k \ge 1,$$

with $A_{0,k}(v) = 1$ and the generating function

$$A_k(x,v) = \sum_{n\ge 0} A_{n,k}(v) x^n, \qquad k \ge 1.$$

Multiplying both sides of (2.1) by v^{i-1}, and summing over $i = 1, 2, \ldots, k-2$, yields for $n,k \ge 3$ the recurrence

$$\begin{aligned} A_{n,k}(v) &- a_{n-1,k}(v^{k-1}+v^{k-2}) \\ &= A_{n-1,k}(v) - a_{n-2,k}(v^{k-1}+v^{k-2}) \\ &\quad + \sum_{i=1}^{k-1} a_{n-1,k}(i) \frac{v^{i-1}-v^{k-2}}{1-v} \\ &\quad + \sum_{j=2}^{k-1}\sum_{\ell=0}^{k-j} \ell! \binom{n-2}{\ell}\binom{k-j}{\ell} (A_{n-1-\ell,j}(v) - a_{n-2-\ell,j} v^{j-1}), \end{aligned}$$

which, by $a_{n,k} = A_{n,k}(1)$, leads to

$$\begin{aligned} A_{n,k}(v) &= \frac{1}{1-v}(A_{n-1,k}(v) - v^k A_{n-1,k}(1)) \\ &\quad + \sum_{j=2}^{k}\sum_{\ell=0}^{k-j} \ell! \binom{n-2}{\ell}\binom{k-j}{\ell} (A_{n-1-\ell,j}(v) - v^{j-1} A_{n-2-\ell,j}(1)), \end{aligned}$$

with $A_{1,k}(v) = \alpha_k(v) = \sum_{i=1}^{k} v^{i-1}$ and $A_{2,k}(v) = k\alpha_k(v)$.

Multiplying both sides of the last equation by x^n, and summing over $n \geq 3$, we obtain

$$\begin{aligned}A_k(x,v) &= 1 + \alpha_k(v)x(1+kx) \\ &\quad + \frac{x}{1-v}(A_k(x,v) - \alpha_k(v)x - 1 - v^k A_k(x,1) + v^k + kv^k x) \\ &\quad + x(A_k(x,v) - 1 - \alpha_k(v)x) - v^{k-1}x^2(A_k(x,1)-1) \\ &\quad + \sum_{j=2}^{k-1}\left(x(A_j(x,v) - 1 - \alpha_j(v)x) - v^{j-1}x^2(A_j(x,1)-1)\right) \\ &\quad + \sum_{j=2}^{k-1}\sum_{\ell=1}^{k-j} x^{\ell+2}\binom{k-j}{\ell}\frac{\partial^\ell}{\partial x^\ell}\left(x^{\ell-1}A_j(x,v) - v^{j-1}x^\ell A_j(x,1)\right). \qquad (2.2)\end{aligned}$$

Example 2.1 (Case $k = 3$)**.** Note that $A_1(x,v) = 1 + \frac{x}{1-x}$ and $A_2(x,v) = 1 + \frac{x(1+v)}{1-2x}$, by the definitions. For $k = 3$, we have

$$\begin{aligned}&A_3(x,v) = 1 + (1+v+v^2)x(1+3x) \\ &+ \frac{x}{1-v}(A_3(x,v) - (1+v+v^2)x - 1 - v^3A_3(x,1) + v^3 + 3v^3x) \\ &+ x(A_3(x,v) - 1 - (1+v+v^2)x) - v^2x^2(A_3(x,1)-1) \\ &+ x(A_2(x,v) - 1 - (1+v)x) - vx^2(A_2(x,1)-1) + x^3\frac{\partial}{\partial x}\left(A_2(x,v) - vxA_2(x,1)\right).\end{aligned}$$

To solve this functional equation, we make use of the kernel method and take $v = \frac{1-2x}{1-x}$ to obtain

$$\begin{aligned}&1 + (1+v+v^2)x(1+3x) + \frac{x}{1-v}(-(1+v+v^2)x - 1 - v^3A_3(x,1) + v^3 + 3v^3x) \\ &+ x(-1 - (1+v+v^2)x) - v^2x^2(A_3(x,1)-1) \\ &+ x(A_2(x,v) - 1 - (1+v)x) - vx^2(A_2(x,1)-1) \\ &+ x^3\frac{\partial}{\partial x}\left(A_2(x,v) - vxA_2(x,1)\right) = 0.\end{aligned}$$

Hence, $A_3(x,1) = \frac{(1-x)(1-4x+5x^2)}{(1-2x)^4}$. Substituting this expression into the one above for $A_3(x,v)$ then yields

$$A_3(x,v) = \frac{(1-x)(1-4x+5x^2)(1+(v-1)(v+2)x)}{(1-2x)^4}.$$

Following Example 2.1, to solve the functional equation (2.2), we use the kernel method. Taking $v = v_0 = \frac{1-2x}{1-x}$ in (2.2) yields

$$\begin{aligned}A_k(x,1) &= \frac{(1-x)^{k-3}}{(1-2x)^{k-1}} \\ &\quad \cdot\left(1 - (k-1)x + \sum_{j=2}^{k-1}\sum_{\ell=0}^{k-j} x^{\ell+2}\binom{k-j}{\ell}\frac{\partial^\ell}{\partial x^\ell}(x^{\ell-1}A_j(x,v) - v^{j-1}x^\ell A_j(x,1))\,|_{v=v_0}\right).\end{aligned}$$

Substituting this expression for $A_k(x,1)$ into (2.2), and observing the identity

$$x\sum_{j=2}^{k}\alpha_{j-1}(v)=(1+kx)\alpha_k(x)-\frac{1+x\alpha_k(v)-v^k(1+kx)}{1-v},\qquad k\geq 2,$$

we obtain our main result.

Theorem 2.2. *The generating function $A_k(x,v)$ for $k\geq 3$ is given by*

$$A_k(x,v)=\frac{(1-v)(1-(k-1)x)}{1-2x-v(1-x)}-\frac{(x+v(1-x))xv^{k-1}}{1-2x-v(1-x)}A_k(x,1)$$
$$+(1-v)\sum_{j=2}^{k-1}\sum_{\ell=0}^{k-j}x^{\ell+2}\binom{k-j}{\ell}\frac{\frac{\partial^\ell}{\partial x^\ell}(x^{\ell-1}A_j(x,v)-v^{j-1}x^\ell A_j(x,1))}{1-2x-v(1-x)},$$

where $A_1(x,v)=\frac{1}{1-x}$, $A_2(x,v)=1+\frac{x(1+v)}{1-2x}$ and

$$A_k(x,1)=\frac{(1-x)^{k-3}}{(1-2x)^{k-1}}$$
$$\cdot\left(1-(k-1)x+\sum_{j=2}^{k-1}\sum_{\ell=0}^{k-j}x^{\ell+2}\binom{k-j}{\ell}\frac{\partial^\ell}{\partial x^\ell}(x^{\ell-1}A_j(x,v)-v^{j-1}x^\ell A_j(x,1))\mid_{v=v_0}\right),$$

where $v_0=\frac{1-2x}{1-x}$.

Note that Theorem 2.2 provides a recurrence formula for finding the generating function $A_k(x,1)$ (even, more generally, for finding $A_k(x,v)$). For instance, upon making use of software such as Maple or Mathematica, one can obtain from Theorem 2.2 the following explicit formulas for $k=3,4,5,6$:

$$A_3(x,1)=\frac{(1-x)(1-4x+5x^2)}{(1-2x)^4},$$
$$A_4(x,1)=\frac{1-10x+44x^2-104x^3+140x^4-100x^5+31x^6}{(1-2x)^7},$$
$$A_5(x,1)=\frac{1-15x+105x^2-435x^3+1175x^4-2129x^5+2595x^6-2041x^7+946x^8-190x^9}{(1-2x)^{10}},$$
$$A_6(x,1)=\frac{1-20x+192x^2-1136x^3+4604x^4-13380x^5+28599x^6-45154x^7+52338x^8-43320x^9+24401x^{10}-8386x^{11}+1391x^{12}}{(1-2x)^{13}}.$$

Remarks: By Theorem 2.2 and induction on k, one can show that the generating function $A_k(x,v)$ for $k\geq 2$ may be expressed in the form $P_k(x,v)/(1-2x)^{\alpha_k}$, where $\alpha_k\geq 1$ and $P_k(x,v)$ is a polynomial in x and v (and not divisible by $1-2x$). Upon taking $v=1$, it is seen that there exists a constant c_k such that the number of k-ary words of length n that avoid 1233 is asymptotic to $c_kn^{\beta_k}2^n$ for some $1\leq\beta_k<\alpha_k$, which was also shown in [8]. We conjecture that $\alpha_k=3k-5=\beta_k+1$ for all k, the fact of which is demonstrated by programming for $3\leq k\leq 15$. Note that Theorem 2.2 provides a recurrence relation for finding an explicit formula for the generating function $A_k(x,1)$ and is an improvement in the case of 1233 over the more general procedure described in [3, 8].

We close this section with some remarks concerning avoidance of the general pattern 123^m, where $m \geq 2$. Let $a_{n,k}^{(m)}$ denote the number of k-ary words of length n that avoid 123^m, with $a_{n,k}^{(m)}(i_1,\ldots,i_s)$ defined analogously as before. If $1 \leq i \leq k-2$, then

$$a_{n,k}^{(m)}(i) = a_{n-1,k}^{(m)}(i) + \sum_{j=1}^{i} a_{n-1,k}^{(m)}(j) + \sum_{j=i+1}^{k-1} a_{n,k}^{(m)}(i,j).$$

To determine a formula for $a_{n,k}^{(m)}(i,j)$, we consider enumerating a restricted class of finite functions as follows. Given $a,b,c \geq 0$, let $d_{a,b}^{(c)}$ denote the number of functions $f : [b] \to [a]$ such that $|\{x \in [b] : f(x) = i\}| \leq c$ for all $i \in [a]$. Such functions could be described as being at most c-to-1. Upon considering the number ℓ of letters in a word belonging to $[j+1,k]$, we have

$$a_{n,k}^{(m)}(i,j) = \sum_{\ell=0}^{k-j} d_{k-j,\ell}^{(m-1)} \binom{n-2}{\ell} a_{n-1-\ell,j}^{(m)}(i),$$

if $i < j < k$. Note that the $d_{k-j,\ell}^{(m-1)}$ factor accounts for the number of ways in which to select and arrange the elements of $[j+1,k]$ within ℓ preselected positions such that none of these elements occur m or more times. Hence, for all $1 \leq i \leq k-2$,

$$a_{n,k}^{(m)}(i) = a_{n-1,k}^{(m)}(i) + \sum_{j=1}^{i} a_{n-1,k}^{(m)}(j) + \sum_{j=i+1}^{k-1} \sum_{\ell=0}^{k-j} d_{k-j,\ell}^{(m-1)} \binom{n-2}{\ell} a_{n-1-\ell,j}^{(m)}(i),$$

with $a_{n,k}^{(m)}(k) = a_{n,k}^{(m)}(k-1) = a_{n-1,k}^{(m)}$.

To write a recurrence for the array $d_{a,b}^{(c)}$, consider the number j of elements in $[a]$ whose pre-image cardinality is exactly c. This implies for $a,b,c \geq 1$,

$$d_{a,b}^{(c)} = \sum_{j=0}^{t} \binom{a}{j} \binom{b}{c,\ldots,c,b-jc} d_{a-j,b-jc}^{(c-1)},$$

where $t = \min\{a, \lfloor b/c \rfloor\}$ and the c index appears exactly j times in the multinomial coefficient of order $j+1$. One may verify the initial conditions $d_{a,0}^{(c)} = 1$ for all $a,c \geq 0$ and $d_{a,b}^{(c)} = 0$ if $ac = 0$ and $b \geq 1$. Note that from the recurrence when $c = 1$, we have $d_{a,b}^{(1)} = 0$ if $b > a$, which is in agreement with the pigeonhole principle, whereas if $b \leq a$, then $d_{a,b}^{(1)} = b!\binom{a}{b} = a(a-1)\cdots(a-b+1)$, as it should. Finding a simple explicit formula for $d_{a,b}^{(c)}$ in general appears not to be an easy task. Note that by induction on c using the recurrence, one has the following multi-sum expression for $d_{a,b}^{(c)}$:

$$d_{a,b}^{(c)} = \sum_{j_c=0}^{\min\{a,\lfloor \frac{b}{c} \rfloor\}} \sum_{j_{c-1}=0}^{\min\{a-j_c,\lfloor \frac{b-cj_c}{c-1} \rfloor\}} \cdots \sum_{j_2=0}^{\min\{a-\sum_{p=3}^{c} j_p,\lfloor \frac{b-\sum_{p=3}^{c} pj_p}{2} \rfloor\}} R_{a,b}(j_2,\ldots,j_c),$$

where

$$R_{a,b}(j_2,\ldots,j_c)=\frac{b!}{2!^{j_2}\cdots c!^{j_c}}\binom{a-\sum_{p=2}^{c}j_p}{b-\sum_{p=2}^{c}pj_p}\prod_{i=2}^{c}\binom{a-\sum_{p=i+1}^{c}j_p}{j_i}.$$

3 Further results

As the previous section illustrates, it is challenging in general to ascertain formulas, either explicitly or by a recurrence, for the number of k-ary words for all k that avoid a single fixed pattern of length four (or of arbitrary length). Another possible direction to pursue is that of enumerating words which avoid 1233 and a second pattern τ. Here, we present two cases when τ is of length three demonstrating that even this problem is highly non-trivial. In particular, we consider the cases when $\tau = 132$ or $\tau = 213$ and leave the remaining cases when τ is a permutation pattern of length three as exercises for the interested reader (the patterns 231 and 321 apparently requiring a lengthier analysis than the others).

3.1 Case 132

Let $A_k(x)$ denote the generating function (g.f.) for the number of k-ary words of length n that avoid $\{132, 1233\}$ for each $k \geq 1$ and define $A(x,y) = \sum_{k\geq 0} A_k(x)y^k$, where $A_0(x) = 1$. In order to find a formula for $A(x,y)$, we let $A'(x,y) = \frac{(1-y)A(x,y)-1}{y}$ and $A''(x,y) = \frac{(1-y)A(x,y)-1}{y(1-y)}$, in accordance with [7, Notation 2.2]. Note that $yA''(x,y)$ represents the restriction of the g.f. $A(x,y)$ to nonempty k-ary words, whereas $yA'(x,y)$ is the further restriction to such words that contain 1.

We wish to write an equation for $A(x,y)$. Let π be a nonempty k-ary word that avoids $\{132, 1233\}$. We represent π by $\pi = \pi^{(1)}k\cdots\pi^{(s)}k\pi^{(s+1)}$, where each $\pi^{(j)}$ is $(k-1)$-ary and $s \geq 0$. Proceeding according to [7, Proposition 2.1], we consider the cases $s = 0$, $s = 1$ and $s \geq 2$. This yields the following:

- If $s = 0$, then one has a contribution of $yA(x,y)$.
- If $s = 1$, then $\frac{xy}{1-y} + \frac{xy^2A''(x,y)}{A'(x,y)}((A'(x,y)+1)^2-1)$.
- If $s \geq 2$, then

$$\sum_{s\geq 2}\frac{x^sy}{1-y}+\sum_{s\geq 2}\sum_{d=1}^{s-1}x^sy^2\binom{s-1}{d}B'^{d-1}B''$$
$$+2\sum_{s\geq 2}\sum_{d=0}^{s-1}x^sy^2\binom{s-1}{d}B'^{d}A''(x,y)$$
$$+\sum_{s\geq 2}\sum_{d=0}^{s-1}x^sy^2\binom{s-1}{d}B'^{d}A'(x,y)A''(x,y),$$

where $B' = \frac{(1-y)B(x,y)-1}{y}$, $B'' = \frac{(1-y)B(x,y)-1}{y(1-y)}$, and $B(x,y) = \frac{1-x}{1-x-y}$ is the g.f. for the number of k-ary words of length n that avoid 12 for all $n, k \geq 0$.

To realize the last two cases above, first note that yB'' is seen to enumerate nonempty, weakly decreasing k-ary words of length n, whereas yB' counts such words that contain

1. Observe further that various sections $\pi^{(i)}$ of π are accounted for by B' in the $s \geq 2$ case above, instead of by yB', since one must divide by y to compensate for the fact the minimum letter of one section can coincide with the maximum letter of the subsequent nonempty section. The same also applies when considering the $\pi^{(i)}$ blocks accounted for by $A'(x, y)$.

Combining all of the above contributions, and simplifying, we have that $A(x, y)$ satisfies

$$(1-y)A(x,y) = 1 + \frac{xy}{(1-x)(1-y)} - \frac{x^2y^2}{(1-x)(1-y)} + \frac{x^2y^2}{1-2x-y+xy} + \frac{x((y-1)A(x,y)+1)((y-1)A(x,y)-2y+1)(1-x-y)}{(1-y)(1-2x-y+xy)}.$$

Solving for $A(x, y)$ in the last equation, and simplifying, yields the following result.

Theorem 3.1. *The generating function for the number of k-ary words of length n that avoid both 132 and 1233 for all $n, k \geq 0$ is given by*

$$\frac{1-2x^2-y-xy-\sqrt{\frac{(1-2x-y+xy)((1-x-y-xy)^2-x(1-x)(1-y))}{(1-x)(1-y)}}}{2x(1-x-y)}.$$

For example, extracting the coefficient of y^k in the formula for $A(x, y)$ in Theorem 3.1 yields the following formulas for $A_k(x)$ where $1 \leq k \leq 5$:

$$A_1(x) = \frac{1}{1-x},$$
$$A_2(x) = \frac{1}{1-2x},$$
$$A_3(x) = \frac{1-3x+4x^2-x^3}{(1-x)^2(1-2x)^2},$$
$$A_4(x) = \frac{1-4x+9x^2-6x^3+2x^4}{(1-x)^2(1-2x)^3},$$
$$A_5(x) = \frac{1-6x+21x^2-34x^3+32x^4-16x^5+4x^6}{(1-x)^3(1-2x)^4}.$$

3.2 Case 213

By the reverse complement operation, the number of k-ary words of length n that avoid $\{213, 1233\}$ is the same as the number that avoid $\{132, 1123\}$. Here, it is more convenient to enumerate the latter. Let $B_k(x)$ denote the g.f. for the number of k-ary words π of length n that avoid $\{132, 1123\}$ for each $k \geq 1$, with $B_0(x) = 1$. Consider cases based on whether π can be expressed as $\pi = k^\ell\pi'$, where $\ell \geq 0$ and π' is $(k-1)$-ary, or as $\pi = k^\ell\pi''k\pi'''$, where π'' is a word on the alphabet $[i, k-1]$ for some $i \in [k-1]$ such that i occurs at least once and π''' is $(i+1)$-ary on $[i] \cup \{k\}$. Note that π' and π''' both avoid $\{132, 1123\}$, whereas π'' avoids $\{132, 112\}$. This implies

$$B_k(x) = \frac{1}{1-x}B_{k-1}(x) + \frac{1}{1-x}\sum_{j=2}^{k}(M_j(x) - M_{j-1}(x))B_{k+2-j}(x), \qquad k \geq 1,$$

where $M_k(x)$ is the g.f. for the number of k-ary words of the form γk such that γ is $(k-1)$-ary and avoids $\{132, 112\}$. Note that the $M_j(x) - M_{j-1}(x)$ factor accounts for the fact that the letter i must occur at least once in the section π'' of π above.

We now must determine $M_k(x)$. Note that $M_1(x) = x$, so assume $k \geq 2$. Then ρ enumerated by $M_k(x)$ is either of the form $\rho = (k-1)^\ell \rho' k$, where $\ell \geq 0$ and ρ' contains no $k-1$, or of the form $\rho = (k-1)^\ell \rho''(k-1)\rho''' k$, where ρ'' is a word on $[i, k-2]$ for some $i \in [k-2]$ containing at least one i and ρ''' is $(i+1)$-ary on $[i] \cup \{k-1\}$. Note that ρ' and ρ''' both avoid $\{132, 112\}$, whereas ρ'' avoids $\{132, 11\}$. Furthermore, observe that within ρ''', any $(k-1)$'s must occur prior to any i's, for otherwise there would be a 1123 in ρ of the form $ii(k-1)k$, where the first i occurs in ρ''. Concerning ρ''', we therefore consider additional cases based on whether ρ''' contains (i) neither i nor $k-1$, (ii) exactly one of $i, k-1$ or (iii) both i and $k-1$. Note that all $(k-1)$'s in ρ''' occur as an initial run in case (iii), for otherwise a 132 would occur. Hence, we get contributions of $M_i(x)$, $2(M_{i+1}(x) - M_i(x))$ and $\frac{x}{1-x}(M_{i+1}(x) - M_i(x))$ for (i), (ii) and (iii), respectively. Considering all possible i, and replacing i with $k-i$, then gives for all $k \geq 2$ the recurrence

$$M_k(x) = \frac{1}{1-x} M_{k-1}(x) + \frac{1}{1-x} \sum_{i=2}^{k-1} (L_i(x) - L_{i-1}(x)) \left(\frac{2-x}{1-x} M_{k+1-i}(x) - \frac{1}{1-x} M_{k-i}(x) \right),$$

where $L_k(x)$ is the g.f. for the number of k-ary words of the form γk that avoid $\{132, 11\}$. Since such words correspond to 132-avoiding permutations whose largest letter is last, we have $L_k(x) = \sum_{j=0}^{k-1} C_j \binom{k-1}{j} x^{j+1}$ for $k \geq 1$.

Define the bivariate g.f.'s by $B(x,y) = \sum_{k\geq 0} B_k(x) y^k$, $M(x,y) = \sum_{k\geq 1} M_k(x) y^k$ and $L(x,y) = \sum_{k\geq 1} L_k(x) y^k$. Then the recurrences above for $B_k(x)$ and $M_k(x)$ imply

$$\left(1 - \frac{y}{1-x}\right) B(x,y) = 1 + \frac{1}{(1-x)y^2} \left((1-y)M(x,y) - xy\right) \left(B(x,y) - 1 - \frac{y}{1-x}\right)$$

and

$$\left(1 - \frac{y}{1-x}\right) M(x,y) = xy + \frac{((1-y)L(x,y) - xy)((2-x-y)M(x,y) - (2-x)xy)}{(1-x)^2 y},$$

where $L(x,y) = \frac{xy}{1-y} C\left(\frac{xy}{1-y}\right)$ and $C(z) = \frac{1-\sqrt{1-4z}}{2z} = \sum_{n\geq 0} C_n z^n$ denotes the g.f. for the Catalan number sequence.

Solving the preceding equations for $B(x,y)$ yields after several algebraic steps the following result.

Theorem 3.2. *The generating function for the number of k-ary words of length n that avoid both* 213 *and* 1233 *(*132 *and* 1123*) for all $n, k \geq 0$ is given by*

$$\frac{4(1-2x)(1-x)^2 - 2(1-x)(4-7x+4x^2)y + (4-7x+4x^2)y^2 + xy^2\sqrt{1-\frac{4xy}{1-y}}}{2(2(1-2x)(1-x)^2 - (1-x)(2-x)(3-4x)y + 2(1-x)(3-2x)y^2 - (2-x)y^3)}.$$

By Theorem 3.2, we have for example the following formulas for $B_k(x)$ where $1 \leq k \leq 5$:

$$\begin{aligned}
B_1(x) &= \frac{1}{1-x},\\
B_2(x) &= \frac{1}{1-2x},\\
B_3(x) &= \frac{1-3x+4x^2-x^3}{(1-x)^2(1-2x)^2},\\
B_4(x) &= \frac{1-3x+6x^2+2x^4}{(1-x)(1-2x)^3},\\
B_5(x) &= \frac{1-6x+21x^2-34x^3+32x^4-26x^5+13x^6+8x^7-8x^8}{(1-x)^3(1-2x)^4}.
\end{aligned}$$

ORCID iDs

Toufik Mansour https://orcid.org/0000-0001-8028-2391
Mark Shattuck https://orcid.org/0000-0001-8473-2505

References

[1] M. H. Albert, R. E. L. Aldred, M. D. Atkinson, C. Handley and D. Holton, Permutations of a multiset avoiding permutations of length 3, *European J. Combin.* **22** (2001), 1021–1031, doi:10.1006/eujc.2001.0538.

[2] N. Alon and E. Friedgut, On the number of permutations avoiding a given pattern, *J. Combin. Theory Ser. A* **89** (2000), 133–140, doi:10.1006/jcta.1999.3002.

[3] P. Brändén and T. Mansour, Finite automata and pattern avoidance in words, *J. Combin. Theory Ser. A* **110** (2005), 127–145, doi:10.1016/j.jcta.2004.10.007.

[4] A. Burstein, *Enumeration of words with forbidden patterns*, ProQuest LLC, Ann Arbor, MI, 1998, thesis (Ph.D.)–University of Pennsylvania, http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:9829868.

[5] A. Burstein and T. Mansour, Words restricted by patterns with at most 2 distinct letters, *Electron. J. Combin.* **9** (2002/03), Research paper 3, 14, doi:10.37236/1675, permutation patterns (Otago, 2003).

[6] D. E. Knuth, *The art of computer programming. Volume 3*, Addison-Wesley Series in Computer Science and Information Processing, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1973, sorting and searching.

[7] T. Mansour, Restricted 132-avoiding k-ary words, Chebyshev polynomials, and continued fractions, *Adv. in Appl. Math.* **36** (2006), 175–193, doi:10.1016/j.aam.2005.04.003.

[8] T. Mansour, R. Rastegar and A. Roitershtein, Finite automata, probabilistic method, and occurrence enumeration of a pattern in words and permutations, *SIAM J. Discrete Math.* **34** (2020), 1011–1038, doi:10.1137/19M1262206.

[9] L. Pudwell, Enumeration schemes for words avoiding permutations, in: *Permutation patterns*, Cambridge Univ. Press, Cambridge, volume 376 of *London Math. Soc. Lecture Note Ser.*, pp. 193–211, 2010, doi:10.1017/CBO9780511902499.010.

[10] A. Regev, Asymptotics of the number of k-words with an l-descent, *Electron. J. Combin.* **5** (1998), Research Paper 15, 4, doi:10.37236/1353.

[11] N. Shar and D. Zeilberger, The (ordinary) generating functions enumerating 123-avoiding words with r occurrences of each of $1, 2, \ldots, n$ are always algebraic, *Ann. Comb.* **20** (2016), 387–396, doi:10.1007/s00026-016-0308-y.

[12] R. Simion and F. W. Schmidt, Restricted permutations, *European J. Combin.* **6** (1985), 383–406, doi:10.1016/S0195-6698(85)80052-4.

[13] H. S. Wilf, The patterns of permutations, *Discrete Math.* **257** (2002), 575–583, doi:10.1016/S0012-365X(02)00515-0, kleitman and combinatorics: a celebration (Cambridge, MA, 1999).

[14] D. Zeilberger, A snappy proof that 123-avoiding words are equinumerous with 132-avoiding words, 2005.

THE ART OF DISCRETE AND APPLIED MATHEMATICS

ISSN 2590-9770
The Art of Discrete and Applied Mathematics 5 (2022) #P1.10
https://doi.org/10.26493/2590-9770.1389.fa2
(Also available at http://adam-journal.eu)

Cayley graphs of order $6pq$ and $7pq$ are Hamiltonian

Farzad Maghsoudi*

Carleton University, Ottawa, Canada

Received 25 September 2020, accepted 8 May 2021, published online 11 May 2022

Abstract

Assume G is a finite group, such that $|G| = 6pq$ or $7pq$, where p and q are distinct prime numbers, and let S be a generating set of G. We prove there is a Hamiltonian cycle in the corresponding connected Cayley graph $\mathrm{Cay}(G;S)$.

Keywords: Cayley graphs, Hamiltonian cycles.

Math. Subj. Class.: 05C25, 05C45

1 Introduction

Arthur Cayley [1] introduced the definition of Cayley graph in 1878. All graphs in this paper are undirected (graphs without loops and direction on the edges).

Definition 1.1 ([16, Definition 1.1], cf. [11, p. 34])**.** Let S be a subset of a finite group G. The *Cayley graph* $\mathrm{Cay}(G;S)$ is the graph whose vertices are elements of G, with an edge joining g and gs, for every $g \in G$ and $s \in S$.

Since then, the theory of Cayley graphs has developed into an important branch of algebraic graph theory. It is an interesting topic to work on because not only is it related to pure mathematics problems, but it is connected to fascinating problems studied by computer scientists, molecular biologists, and coding theorists (see [15] for more information).

*Theorem 1.3 and Proposition 1.4 are the main results of this paper. I would like to express my sincere gratitude to my supervisor, professor Joy Morris who always supported me throughout my graduate journey. I am especially grateful to my co-supervisor, professor Dave Morris, for the patient guidance and advice he has provided during my graduate study. I have been extremely lucky to have a co-supervisor who cared so much about my research, and who responded to my questions so promptly. I am also thankful to professor Hadi Kharaghani and professor Amir Akbary and cannot forget their valuable help and motivation during my graduate years. I am truly grateful to my family for their immeasurable love and care.

E-mail address: FARZADMAGHSOUDI@cmail.carleton.ca (Farzad Maghsoudi)

Recall that a *Hamiltonian cycle* is a cycle that visits every vertex of a graph. Finding Hamiltonian cycles is a fundamental question in graph theory, but in general, it is extremely difficult. To be precise, it is an NP-complete problem, which means most mathematicians do not believe there exists an efficient algorithm to determine whether an arbitrary graph contains such a cycle. Because the general case is so hard, it is natural to look at special cases.

Cayley graphs are one of these cases that mathematicians are interested in working on. There have been many papers on the topic of Hamiltonian cycles in Cayley graphs, but it is still an open question whether every connected Cayley graph has a Hamiltonian cycle. (See survey papers [5, 24, 21] for more information. We ignore the trivial counterexamples on 1 or 2 vertices.) The following result combines the main result of this paper with the previous work of several authors (C. C. Chen and N. Quimpo [2], S. J. Curran, J. Morris and D. W. Morris [6], E. Ghaderpour and D. W. Morris [9, 10], D. Jungreis and E. Friedman [13], Kutnar et al. [16], K. Keating and D. Witte [14], D. Li [17], D. W. Morris and K. Wilk [20], and D. Witte [23]).

Theorem 1.2 ([16, 20, 23])**.** *Let G be a finite group. If $|G|$ has any of the forms below (where p, q, and r are distinct primes), then every connected Cayley graph on G has a Hamiltonian cycle.*

1. *kp, where $1 \leqslant k \leqslant 47$,*
2. *kpq, where $1 \leqslant k \leqslant 7$,*
3. *pqr,*
4. *kp^2, where $1 \leqslant k \leqslant 4$,*
5. *kp^3, where $1 \leqslant k \leqslant 2$,*
6. *p^k, where $1 \leqslant k < \infty$.*

Previously, part (2) of Theorem 1.2 was only known for $1 \leqslant k \leqslant 5$, but we improve this condition: we show that 5 can be replaced with 7. This is the new part of the above theorem which is our result. The hard part is when $k = 6$:

Theorem 1.3. *Assume G is a finite group of order $6pq$, where p and q are distinct prime numbers. Then every connected Cayley graph on G contains a Hamiltonian cycle.*

This generalizes [10], which considered only the case where $q = 5$. The proof takes up all of Section 3, after some preliminaries in Section 2.

Unlike Theorem 1.3, the following observation follows easily from known results, and may be known to experts. The proof is on page 8.

Proposition 1.4. *Assume G is a finite group of order $7pq$, where p and q are distinct prime numbers. Then every connected Cayley graph on G contains a Hamiltonian cycle.*

The Introduction of the author's masters thesis [18] provides additional background and a description of the methods that are used in the proof of the main theorem.

2 Preliminaries

This section establishes basic terminology and notation, and proves a number of technical results that will be used in the proof of Theorem 1.3. In particular, it is shown we may assume that $|G|$ is square-free (note $|G| = 6pq$ in Theorem 1.3), so the Sylow subgroups of G are $\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_p$, and $\mathcal{C}_q$, and that $|G'|$ has precisely 2 prime factors, so G' is either $\mathcal{C}_p \times \mathcal{C}_q$ or $\mathcal{C}_3 \times \mathcal{C}_p$.

2.1 Basic notation and definitions

Throughout the paper, we have used standard terminology of graph theory and group theory that can be found in textbooks, such as [11, 12].

The following notation is used throughout the paper:

- The commutator $ghg^{-1}h^{-1}$ of g and h is denoted by $[g, h]$.
- We will always let $G' = [G, G]$ be the commutator subgroup of G.
- We define $\overline{G} = G/G'$, $\overline{g} = gG'$ for any $g \in G$, and $\overline{S} = \{\overline{g}; g \in S\}$ for any $S \subseteq G$.
- $C_{G'}(S)$ denotes the centralizer of S in G'.
- $G \ltimes H$ denotes a semidirect product of groups G and H, where H is normal.
- D_{2n} denotes the dihedral group of order $2n$.
- e denotes the identity element of G.
- For $S \subseteq G$, a sequence $(s_1, s_2, \ldots, s_n)$ of elements of $S \cup S^{-1}$ specifies the walk in the Cayley graph Cay$(G; S)$ that visits the vertices: $e, s_1, s_1s_2, \ldots, s_1s_2 \cdots s_n$. Also, $(s_1, s_2, \ldots, s_n)^{-1} = (s_n^{-1}, s_{n-1}^{-1}, \ldots, s_1^{-1})$.
- We use $(\overline{s_1}, \overline{s_2}, \ldots, \overline{s_n})$ to denote the image of the walk $(s_1, s_2, \ldots, s_n)$ in the Cay$(G/G'; \overline{S})$ = Cay$(\overline{G}; \overline{S})$ which is a Cayley graph on the quotient group G/G'.
- For $k \in \mathbb{Z}^+$, we use $(s_1, s_2, \ldots, s_m)^k$ to denote the concatenation of k copies of the sequence $(s_1, s_2, \ldots, s_m)$.
- p and q are distinct prime numbers.
- $\mathcal{C}_n$ denotes the cyclic group of order n.
- $\widehat{G} = G/\mathcal{C}_p$, when $\mathcal{C}_p$ is a normal subgroup, we also let $\breve{G} = G/\mathcal{C}_q$ when $\mathcal{C}_q$ is a normal subgroup, and let $\overleftrightarrow{G} = G/\mathcal{C}_3$ when $\mathcal{C}_3$ is a normal subgroup. Also, $\widehat{g} = g\mathcal{C}_p$, $\breve{g} = g\mathcal{C}_q$, for any $g \in G$, and $\widehat{S} = \{\widehat{g}; g \in S\}$, $\breve{S} = \{\breve{g}; g \in S\}$ for any $S \subseteq G$.
- We let a_2, a_3, γ_p, and a_q be elements of G that generate $\mathcal{C}_2$, $\mathcal{C}_3$, $\mathcal{C}_p$, and $\mathcal{C}_q$, respectively.

Remark 2.1. When $|G| = 6pq$ and it is square free (as is usually the case in Section 3), the Sylow subgroups are $\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_p$, and $\mathcal{C}_q$. Also, the commutator subgroup G' will usually be either $\mathcal{C}_p \times \mathcal{C}_q$ or $\mathcal{C}_3 \times \mathcal{C}_p$, so $\mathcal{C}_p$ is a normal subgroup and either $\mathcal{C}_q$ or $\mathcal{C}_3$ is also a normal subgroup.

2.2 Basic methods

In this subsection, we explain some of the key ideas in the proof of our main result (Theorem 1.3).

It is easy to see that $\mathrm{Cay}(G; S)$ is connected if and only if S generates G ([11, Lemma 3.7.4]). Also, if S is a subset of S_0, then $\mathrm{Cay}(G; S)$ is a subgraph of $\mathrm{Cay}(G; S_0)$ that contains all of the vertices. Therefore, in order to show that every connected Cayley graph on G contains a Hamiltonian cycle, it suffices to consider $\mathrm{Cay}(G; S)$, where S is a generating set that is *minimal*, which means that no proper subset of S generates G.

The following well known (and easy) result handles the case of Theorem 1.3 where G is abelian.

Lemma 2.2 ([3, Corollary on page 257])**.** *Assume G is an abelian group. Then every connected Cayley graph on G has a Hamiltonian cycle.*

Note $\mathrm{Cay}(\mathcal{C}_2; \{a\})$ is a Cayley graph with two vertices, where $\mathcal{C}_2 = \langle a \rangle$. We consider (a, a) as its Hamiltonian cycle which is:

$$e \xrightarrow{a} a \xrightarrow{a} a^2 = e.$$

Although graph theorists would not typically consider this a cycle, it satisfies the basic property of visiting each vertex exactly once. In some of our inductive proofs, we require a Hamiltonian cycle in a Cayley graph on a quotient group. When this quotient group is $\mathcal{C}_2$, this Hamiltonian cycle provides the structure we need for our inductive arguments to work.

Theorem 2.3 (Marušič [19], Durnberger [7, 8], and Keating-Witte [14])**.** *If the commutator subgroup G' of G is a cyclic p-group, then every connected Cayley graph on G has a Hamiltonian cycle.*

Theorem 2.4 (Chen-Quimpo [4])**.** *Let v and w be two distinct vertices of a connected Cayley graph $\mathrm{Cay}(G; S)$. Assume G is abelian, $|G|$ is odd, and the valency of $\mathrm{Cay}(G; S)$ is at least 3. Then $\mathrm{Cay}(G; S)$ has a Hamiltonian path that starts at v and ends at w.*

The following lemma (and its corollary) often provide a way to lift a Hamiltonian cycle in $\mathrm{Cay}(G/N; \overline{S})$ to a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. Before stating the results, we introduce a useful piece of notation.

Notation 2.5. Suppose N is a normal subgroup of G, and $C = (s_1, s_2, \ldots, s_n)$ is a walk in $\mathrm{Cay}(G; S)$. If the walk $(s_1N, s_2N, \ldots, s_nN)$ in $\mathrm{Cay}(G/N; SN/N)$ is closed, then its *voltage* is the product $\mathbb{V}(C) = s_1 s_2 \cdots s_n$. This is an element of N. In particular, if $C = (\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_n)$ is a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}, \overline{S})$, then $\mathbb{V}(C) = s_1 s_2 \cdots s_n$.

Factor Group Lemma 2.6 ([24, Section 2.2])**.** *Suppose:*

- *S is a generating set of G,*
- *N is a cyclic normal subgroup of G,*
- *$\overline{G} = G/N$,*
- *$C = (\overline{s_1}, \overline{s_2}, \ldots, \overline{s_n})$ is a Hamiltonian cycle in $\mathrm{Cay}(G/N; \overline{S})$, and*
- *the voltage $\mathbb{V}(C)$ generates N.*

Then there is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Corollary 2.7 ([10, Corollary 2.3])**.** *Suppose:*

- *S is a generating set of G,*
- *N is a normal subgroup of G, such that $|N|$ is prime,*
- *$sN = tN$ for some $s, t \in S$ with $s \neq t$, and*
- *there is a Hamiltonian cycle in* $\mathrm{Cay}(G/N; \overline{S})$ *that uses at least one edge labeled $\overline{s}$.*

Then there is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Lemma 2.8. *Assume $G = H \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$, where $G' = \mathcal{C}_p \times \mathcal{C}_q$, and let S be a generating set of G. As usual, let $\overline{G} = G/G' \cong H$. Assume there is a unique element c of S that is not in $H \ltimes \mathcal{C}_q$, and C is a Hamiltonian cycle in* $\mathrm{Cay}(\overline{G}; \overline{S})$ *such that c occurs precisely once in C. Then the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$.*

Proof. Write $C = (\overline{s}_1, \overline{s}_2, \cdots, \overline{s}_n)$, and let $H^+ = H \ltimes \mathcal{C}_q$. By assumption, there is a unique k, such that $s_k = c$, and all other elements of S are in H^+. Therefore,

$$\mathbb{V}(C) = s_1 s_2 \ldots s_n \in H^+ \cdot H^+ \cdots H^+ \cdot c \cdot H^+ \cdot H^+ \cdots H^+ = H^+ c H^+.$$

Since $c \notin H^+$, we conclude that $\mathbb{V}(C) \notin H^+$.

On the other hand, since $\mathbb{V}(C)$ is an element of $G' = \mathcal{C}_p \times \mathcal{C}_q$, we have $\mathbb{V}(C) = a_q^i \gamma_p^j \in H^+ \gamma_p^j$. Since $\mathbb{V}(C) \notin H^+$, this implies $j \not\equiv 0 \pmod{p}$, so $\langle a_q^i \gamma_p^j \rangle$ contains $\mathcal{C}_p$. □

Definition 2.9. The *Cartesian product* $X_1 \,\square\, X_2$ of graphs X_1 and X_2 is a graph such that the vertex set of $X_1 \,\square\, X_2$ is $V(X_1) \times V(X_2) = \{(v, v'); v \in V(X_1), v' \in V(X_2)\}$, and two vertices (v_1, v_2) and (v_1', v_2') are adjacent in $X_1 \,\square\, X_2$ if and only if either

- $v_1 = v_1'$ and v_2 is adjacent to v_2' in X_2 or
- $v_2 = v_2'$ and v_1 is adjacent to v_1' in X_1.

Lemma 2.10 ([4, Lemma 5 on page 28])**.** *The Cartesian product of a path and a cycle is Hamiltonian.*

Corollary 2.11 (cf. [4, Corollary on page 29])**.** *The Cartesian product of two Hamiltonian graphs is Hamiltonian.*

Lemma 2.12 ([16, Lemma 2.27])**.** *Let S generate the finite group G, and let $s \in S$, such that $\langle s \rangle \lhd G$. If* $\mathrm{Cay}(G/\langle s \rangle; \overline{S})$ *has a Hamiltonian cycle, and either*

1. *$s \in Z(G)$, or*
2. *$Z(G) \cap \langle s \rangle = \{e\}$,*

then $\mathrm{Cay}(G; S)$ *has a Hamiltonian cycle.*

2.3 Some facts from group theory

In this subsection, we state some facts in group theory, which are used to prove our main result. The following lemma often makes it possible to use Factor Group Lemma 2.6 for finding Hamiltonian cycles in connected Cayley graphs of G.

Lemma 2.13 ([6, Corollary 4.4]). *Assume $G = \langle a, b\rangle$ and G' is cyclic. Then $G' = \langle [a, b]\rangle$.*

Corollary 2.14. *Assume $G = \langle a, b\rangle$ and $\gcd(k, |a|) = 1$, where $k \in \mathbb{Z}$, and G' is cyclic. Then $G' = \langle [a^k, b]\rangle$.*

Proposition 2.15 ([12, Theorem 9.4.3 on page 146], cf. [10, Lemma 2.11]). *Assume $|G|$ is square-free. Then:*

1. *G' and G/G' are cyclic,*
2. *$Z(G) \cap G' = \{e\}$,*
3. *$G \cong C_n \ltimes G'$, for some $n \in \mathbb{Z}^+$,*
4. *If b and γ are elements of G such that $\langle bG'\rangle = G/G'$ and $\langle\gamma\rangle = G'$, then $\langle b, \gamma\rangle = G$, and there are integers m, n, and τ, such that $|\gamma| = m$, $|b| = n$, $b\gamma b^{-1} = \gamma^\tau$, $mn = |G|$, $\gcd(\tau - 1, m) = 1$, and $\tau^n \equiv 1 \pmod m$.*

Lemma 2.16. *Assume*

- $G = (\mathcal{C}_p \times \mathcal{C}_q) \ltimes (\mathcal{C}_r \times \mathcal{C}_t)$,
- $G' = (\mathcal{C}_r \times \mathcal{C}_t)$,
- $\overline{a} \in \overline{G}$,
- *p, q, r, and t are distinct primes.*

If $|\overline{a}| = pq$, then $|a| = pq$.

Proof. Suppose $|a| \neq pq$. Without loss of generality, assume $|a|$ is divisible by r. Then (after replacing a by a conjugate) the abelian group $\langle a\rangle$ contains $\mathcal{C}_p \times \mathcal{C}_q$ and $\mathcal{C}_r$, so $\mathcal{C}_r$ centralizes $\mathcal{C}_p \times \mathcal{C}_q$. Since $\mathcal{C}_r$ also centralizes $\mathcal{C}_t$, this implies that $\mathcal{C}_r \subseteq Z(G)$. This contradicts the fact that $G' \cap Z(G) = \{e\}$ (see Proposition 2.15(2)). □

Lemma 2.17 ([22, Exercise 19 on page 43]). *Assume $|G| = 2k$, where k is odd. Then G has a subgroup of index 2.*

Corollary 2.18. *Assume $|G| = 2k$, where k is odd. Then $|G'|$ is odd.*

Proof. By Lemma 2.17, there is a normal subgroup H of G such that $[G : H] = 2$. Now since G/H has order 2, then G/H is abelian, so $G' \subseteq H$. Therefore, $|G'|$ is odd. □

Notation 2.19. For τ as defined in Proposition 2.15(4), we use τ^{-1} to denote the inverse of τ modulo m (so $\tau^{-1} \equiv \tau^{n-1} \pmod m$).

2.4 Cayley graphs that contain a Hamiltonian cycle

We show, throughout this subsection, that there exists a Hamiltonian cycle in some connected Cayley graphs with additional assumptions. The following proposition shows that in our proof of Theorem 1.3 we can assume $|G|$ is square-free, since the cases where $|G|$ is not square-free have already been dealt with. At the end of this subsection we prove Proposition 1.4.

Proposition 2.20. *Assume:*

- $|G| = 6pq$, *where p and q are distinct prime numbers, and*
- $|G|$ *is not square-free (i.e. $\{p, q\} \cap \{2, 3\} \neq \emptyset$).*

Then every connected Cayley graph on G has a Hamiltonian cycle.

Proof. Without loss of generality we may assume $q \in \{2, 3\}$. Then $|G| \in \{12p, 18p\}$. Therefore, Theorem 1.2(1) applies. □

Proposition 2.21 ([25, Proposition 5.5])**.** *If n is divisible by at most 3 distinct primes, then every Cayley diagram (directed Cayley graph) in D_{2n} has a Hamiltonian cycle.*

The following proposition demonstrates that we can assume $|G'|$ in Theorem 1.3 is a product of two distinct prime numbers.

Proposition 2.22. *Assume $|G| = 2pqr$, where p, q and r are distinct odd prime numbers. If $|G'| \in \{1, pqr\}$ or $|G'|$ is prime, then every connected Cayley graph on G has a Hamiltonian cycle.*

Proof. If $|G'| = 1$, then $G' = \{e\}$. So G is an abelian group. Therefore, Lemma 2.2 applies. If $|G'|$ is prime, then Theorem 2.3 applies. Finally, if $|G'| = pqr$, then

$$G = \mathcal{C}_2 \ltimes (\mathcal{C}_p \times \mathcal{C}_q \times \mathcal{C}_r) \cong D_{2pqr}.$$

So Proposition 2.21 applies. □

The following lemmas show that some special Cayley graphs have a Hamiltonian cycle, and we use these facts in Section 3 in order to prove our main result.

Lemma 2.23. *Assume $G = (\mathcal{C}_2 \times \mathcal{C}_r) \ltimes G'$, and $G' = \mathcal{C}_p \times \mathcal{C}_q$, where p, q and r are distinct odd prime numbers and let $S = \{a, b\}$ be a generating set of G. Additionally, assume $|\overline{a}| \in \{2, 2r\}$, $|\overline{b}| = r$ and $\gcd(|b|, r-1) = 1$. Then $\mathrm{Cay}(G; S)$ contains a Hamiltonian cycle.*

Proof. We have $C = (\overline{b}^{r-1}, \overline{a}, \overline{b}^{-(r-1)}, \overline{a}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage

$$\mathbb{V}(C) = b^{r-1} a b^{-(r-1)} a^{-1} = [b^{r-1}, a].$$

Since $\gcd(|b|, r-1) = 1$, then by Lemma 2.14 we have $[b^{r-1}, a] = G'$. Therefore, Factor Group Lemma 2.6 applies. □

Lemma 2.24 (cf. [10, Case 2 of proof of Theorem 1.1, pages 3619-3620])**.** *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_r) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $\widehat{S}$ *is a minimal generating set of* $\widehat{G} = G/\mathcal{C}_p$,
- $\mathcal{C}_r$ *centralizes* $\mathcal{C}_q$,
- $\mathcal{C}_2$ *inverts* $\mathcal{C}_q$.

Then, $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

Lemma 2.25 ([10, Lemma 2.6])**.** *Assume:*

- $G = \langle a \rangle \ltimes \langle S_0 \rangle$, *where* $\langle S_0 \rangle$ *is an abelian subgroup of odd order,*
- $|(S_0 \cup S_0^{-1})| \geqslant 3$, *and*
- $\langle S_0 \rangle$ *has a nontrivial subgroup* H*, such that* $H \lhd G$ *and* $H \cap Z(G) = \{e\}$.

Then $\mathrm{Cay}(G; S_0 \cup \{a\})$ *has a Hamiltonian cycle.*

Lemma 2.26 ([10, Lemma 2.9])**.** *If* $G = D_{2pq} \times \mathcal{C}_r$*, where* p, q *and* r *are distinct odd primes, then every connected Cayley graph on* G *has a Hamiltonian cycle.*

Now we prove Proposition 1.4 which is on page 2.

Proof of Proposition 1.4. If $p \neq 7$ and $q \neq 7$, then Theorem 1.2(3) applies. So we may assume $q = 7$, which means $|G| = 49p$ (and $p \neq 7$). We may also assume that G is not abelian, for otherwise Lemma 2.2 applies.

If a Sylow p-subgroup P of G is normal, then $|G/P| = 49$, so the quotient G/P is abelian. (Because if q is prime, then every group of order q^2 is abelian). Therefore, since P is normal and G/P is abelian, then G' is contained in P. So $|G'| = p$. Therefore, Theorem 2.3 applies.

Now we may assume P is not normal in G. Then by Sylow's Theorem, $n_p | 49$ and $n_p \equiv 1 \pmod p$, where n_p is the number of Sylow p-subgroups in G. Thus, $p \in \{2, 3\}$, so $|G| \in \{14q, 21q\}$. Therefore, Theorem 1.2(1) applies. □

2.5 Some specific sets that generate G

This Subsection presents a few results that provide conditions under which certain 2-element subsets generate G. Obviously, no 3-element minimal generating set can contain any of these subsets.

Lemma 2.27. *Assume* $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes G'$*, and* $G' = \mathcal{C}_p \times \mathcal{C}_q$*. Also, assume* $C_{G'}(\mathcal{C}_3) = \mathcal{C}_q$ *and* $\mathcal{C}_q \nsubseteq C_{G'}(\mathcal{C}_2)$*. If* (a, b) *is one of the following ordered pairs*

1. $(a_3 a_q, a_2 a_3^j a_q^k \gamma_p)$,
2. $(a_2 a_3, a_3^j a_q^k \gamma_p)$, *where* $k \not\equiv 0 \pmod q$,
3. $(a_2 a_3 a_q, a_3^j a_q^k \gamma_p)$, *where* $k \not\equiv 0 \pmod q$,
4. $(a_2 a_3 a_q, a_2 a_3^j a_q^k \gamma_p)$, *where* $k \not\equiv 1 \pmod q$,

then $\langle a, b \rangle = G$.

Proof. It is easy to see that $(\overline{a}, \overline{b}) = \overline{G}$, so it suffices to show that $\langle a, b \rangle$ contains $\mathcal{C}_p$ and $\mathcal{C}_q$. Thus, it suffices to show that $\breve{G}$ and $\check{G}$ are nonabelian, where $\breve{G} = G/(\mathcal{C}_3 \ltimes \mathcal{C}_p) \cong D_{2q}$ and $\check{G} = G/C_q$.

Since a_3 does not centralize $\mathcal{C}_p$, it is clear in each of $(1) - (4)$ that $\breve{a}$ does not centralize γ_p (and γ_p is one of the factors in $\check{b}$), so $\check{G}$ is not abelian.

The pair $(\breve{a}, \breve{b})$ is either $(a_q, a_2 a_q^k)$, (a_2, a_q^k) where $k \not\equiv 0 \pmod q$, $(a_2 a_q, a_q^k)$ where $k \not\equiv 0 \pmod q$, or $(a_2 a_q, a_2 a_q^k)$ where $k \not\equiv 1 \pmod q$. Each of these is either a reflection and a nontrivial rotation or two different reflections, and therefore generates the (nonabelian) dihedral group $D_{2q} = \breve{G}$. ☐

Lemma 2.28. *Assume* $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes G'$*, and* $G' = \mathcal{C}_p \times \mathcal{C}_q$*. Also, assume* $C_{G'}(\mathcal{C}_3) = \{e\}$*. If* (a, b) *is one of the following ordered pairs*

1. $(a_2 a_3, a_2^i a_3^j a_q^k \gamma_p)$*, where* $k \not\equiv 0 \pmod q$*,*
2. $(a_3 a_q, a_2 a_3^j \gamma_p)$*, where* $j \not\equiv 0 \pmod 3$*,*
3. $(a_3, a_2 a_3^j a_q^k \gamma_p)$*, where* $k \not\equiv 0 \pmod q$*,*
4. $(a_2 a_3 a_q, a_2^i a_3^j \gamma_p)$*, where* $j \not\equiv 0 \pmod 3$*,*

then $\langle a, b \rangle = G$.

Proof. It is easy to see that $(\overline{a}, \overline{b}) = \overline{G}$, so it suffices to show that $\langle a, b \rangle$ contains $\mathcal{C}_p$ and $\mathcal{C}_q$. we need to show that $\widehat{G}$ and $\check{G}$ are nonabelian, where $\widehat{G} = G/\mathcal{C}_p$ and $\check{G} = G/\mathcal{C}_q$, as usual.

As in the proof of Lemma 2.27, since a_3 does not centralize $\mathcal{C}_p$, it is clear in each of $(1) - (4)$ that $\breve{a}$ does not centralize γ_p (and γ_p is one of the factors in $\check{b}$), so $\check{G}$ is not abelian.

In $(1) - (4)$, a_q appears in one of the generators in $(\widehat{a}, \widehat{b})$, but not the other, and the other generator does have an occurrence of a_3. Since a_3 does not centralize a_q, this implies that $\widehat{G}$ is not abelian. ☐

Lemma 2.29. *Assume* $G = (\mathcal{C}_2 \times \mathcal{C}_q) \ltimes G'$*, and* $G' = \mathcal{C}_3 \times \mathcal{C}_p$*. Also, assume* $C_{G'}(\mathcal{C}_q) = \mathcal{C}_3$ *and* $\mathcal{C}_3 \nsubseteq C_{G'}(\mathcal{C}_2)$*. If* (a, b) *is one of the following ordered pairs*

1. $(a_2 a_q, a_2^i a_q^j a_3^k \gamma_p)$*, where* $k \not\equiv 0 \pmod q$*,*
2. $(a_q a_3, a_2 a_q^j a_3^k \gamma_p)$*,*
3. $(a_2^i a_q^m a_3, a_2 a_q^j \gamma_p)$*, where* $m \not\equiv 0 \pmod q$*,*

then $G = \langle a, b \rangle$.

Proof. It is easy to see that $(\overline{a}, \overline{b}) = \overline{G}$, so it suffices to show that $\langle a, b \rangle$ contains $\mathcal{C}_p$ and $\mathcal{C}_3$. We need to show that $\breve{G}$ and $\overleftrightarrow{G}$ are nonabelian, where $\breve{G} = G/(\mathcal{C}_q \ltimes \mathcal{C}_p) \cong D_6$ and $\overleftrightarrow{G} = G/\mathcal{C}_3$.

In each of $(1) - (4)$, a_q appears in $\overleftrightarrow{a}$, and γ_p appears in $\overleftrightarrow{b}$ (but not in $\overleftrightarrow{a}$). Since a_q does not centralize γ_p, this implies that $\overleftrightarrow{G}$ is not abelian.

In each of $(1) - (4)$, $(\overleftrightarrow{a}, \overleftrightarrow{b})$ consists of either a reflection and a nontrivial rotation or two different reflections, so it generates the (nonabelian) dihedral group $D_6 = \overleftrightarrow{G}$. ☐

3 Proof of the main result

In this section, we prove Theorem 1.3, which is the main result. We are given a generating set S of a finite group G of order $6pq$, where p and q are distinct prime numbers, and we wish to show $\mathrm{Cay}(G; S)$ contains a Hamiltonian cycle. The proof is a long case-by-case analysis (see Figures 1, 2 and 3 for outlines of the many cases that are considered). Here are our main assumptions throughout the whole section.

Assumption 3.1. *We assume:*

1. $p, q > 7$, *otherwise* Theorem 1.2(1) *applies.*
2. $|G|$ *is square-free, otherwise* Proposition 2.20 *applies.*
3. $G' \cap Z(G) = \{e\}$, *by* Proposition 2.15(2).
4. $G \cong \mathcal{C}_n \ltimes G'$, *by* Proposition 2.15(3).
5. $|G'| \in \{pq, 3p\}$, *by* Corollary 2.18.
6. *For every element* $\overline{s} \in \overline{S}$, $|\overline{s}| \neq 1$. *Otherwise, if* $|\overline{s}| = 1$, *then* $s \in G'$, *so* $G' = \langle s \rangle$ *or* $|s|$ *is prime. In each case* $\mathrm{Cay}(G/\langle s\rangle; \overline{S})$ *has a Hamiltonian cycle by* part 2 or 3 *of* Theorem 1.2. *By* Assumption 3.1(3), $\langle s \rangle \cap Z(G) = \{e\}$, *therefore,* Lemma 2.12(2) *applies.*
7. *S is a minimal generating set of G. Note that S must generate G, for otherwise* $\mathrm{Cay}(G; S)$ *is not connected. Also, in order to show that every connected Cayley graph on G contains a Hamiltonian cycle, it suffices to consider* $\mathrm{Cay}(G; S)$, *where S is a generating set that is minimal.*

3.1 Assume $|S| = 2$ and $G' = \mathcal{C}_p \times \mathcal{C}_q$

In this subsection, we prove the part of Theorem 1.3 where, $|S| = 2$ and $G' = \mathcal{C}_p \times \mathcal{C}_q$. Recall $\overline{G} = G/G'$ and $\widehat{G} = G/\mathcal{C}_p$.

Proposition 3.2. *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 2$.

Then $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

Proof. Let $S = \{a, b\}$. For every $s \in S$, $|\overline{s}| \neq 1$, by Assumption 3.1(6).

Case 1. Assume $\overline{S}$ is minimal. Then $|\overline{a}|, |\overline{b}| \in \{2, 3\}$. When $|\overline{a}| = |\overline{b}| = 2$ or $|\overline{a}| = |\overline{b}| = 3$, then $\overline{G} \neq \langle \overline{a}, \overline{b} \rangle$. Therefore, $G \neq \langle a, b \rangle$ which contradicts the fact that $G = \langle a, b \rangle$. So we may assume $|\overline{a}| = 2$ and $|\overline{b}| = 3$. Since $|b| \in \{3, 3p, 3q, 3pq\}$, then $\gcd(|b|, 2) = 1$. Thus, Lemma 2.23 applies.

Case 2. Assume $\overline{S}$ is not minimal. Then $\{|\overline{a}|, |\overline{b}|\}$ is either $\{6, 2\}$, $\{6, 3\}$, or $\{6\}$. We may assume $|\overline{a}| = 6$.

I. $|S| = 2$

A. $G' = \mathcal{C}_p \times \mathcal{C}_q$ (Section 3.1).
1. $\overline{S}$ is a minimal generating set.
2. $\overline{S}$ is not a minimal generating set.

B. $G' = \mathcal{C}_3 \times \mathcal{C}_p$ (Section 3.2).
1. $|\overline{a}| = |\overline{b}| = 2q$.
2. $|\overline{a}| = q$.
3. $|\overline{a}| = 2q$ and $|\overline{b}| = 2$.
4. None of the previous cases apply.

Figure 1: Outline of the cases in the proof of Theorem 1.3 where $|S| = 2$

II. $|S| = 3$.

A. $G' = \mathcal{C}_p \times \mathcal{C}_q$.

a. $C_{G'}(\mathcal{C}_3) \neq \{e\}$ or $\widehat{S}$ is minimal.

i. $C_{G'}(\mathcal{C}_3) \neq \{e\}$ (Section 3.3).
1. $a = a_2$ and $b = a_q a_3$.
2. $a = a_2$ and $b = a_2 a_q a_3$.
3. $a = a_2 a_3$ and $b = a_2 a_q$.
4. $a = a_2 a_3$ and $b = a_q a_3$.
5. $a = a_2 a_3$ and $b = a_2 a_3 a_q$.

ii. $\widehat{S}$ is minimal (Section 3.4).
1. $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$.
2. $C_{G'}(\mathcal{C}_2) = \mathcal{C}_q$.
3. $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p$.
4. $C_{G'}(\mathcal{C}_2) = \{e\}$.

b. $C_{G'}(\mathcal{C}_3) = \{e\}$ and $\widehat{S}$ is not minimal.

i. $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$ (Section 3.5).
1. $a = a_3$ and $b = a_2 a_q$.
2. $a = a_3$ and $b = a_2 a_3 a_q$.
3. $a = a_2 a_3$ and $b = a_3 a_q$.
4. $a = a_2 a_3$ and $b = a_2 a_q$.
5. $a = a_2 a_3$ and $b = a_2 a_3 a_q$.

ii. $C_{G'}(\mathcal{C}_2) \neq \{e\}$ (Section 3.6).
1. $a = a_2 a_3$ and $b = a_2 a_3 a_q$.
2. $a = a_2 a_3$ and $b = a_2 a_q$.
3. $a = a_2 a_3$ and $b = a_3 a_q$.
4. $a = a_3$ and $b = a_2 a_q$.

iii. $C_{G'}(\mathcal{C}_2) = \{e\}$ (Section 3.7).
1. $a = a_2 a_3$ and $b = a_2 a_3 a_q$.
2. $a = a_2 a_3$ and $b = a_2 a_q$.
3. $a = a_2 a_3$ and $b = a_3 a_q$.
4. $a = a_3$ and $b = a_2 a_q$.

B. $G' = \mathcal{C}_3 \times \mathcal{C}_p$. (Section 3.8).
1. $a = a_2 a_q$ and $b = a_2 a_q^m a_3$.
2. $a = a_2 a_q$ and $b = a_2 a_3$.
3. $a = a_2 a_q$ and $b = a_q^m a_3$.
4. $a = a_2$ and $b = a_q a_3$.

Figure 2: Outline of the cases in the proof of Theorem 1.3 where $|S| = 3$

III. $|S| \geqslant 4$ (Section 3.9). This part of the proof applies whenever $|G| = pqrt$ with p, q, r, and t distinct primes.

1. $|G'|$ has only two prime factors.
2. $|G'|$ has three prime factors.

Figure 3: Outline of the cases in the proof of Theorem 1.3 where $|S| \geqslant 4$

Subcase 2.1. Assume $|\overline{b}| = 2$. So we have $\overline{b} = \overline{a}^3$, then $b = a^3\gamma$, where $G' = \langle\gamma\rangle$ for otherwise $\langle a, b\rangle = \langle a, a^3\gamma\rangle = \langle a, \gamma\rangle \neq G$ which contradicts the fact that $G = \langle a, b\rangle$. Now by Proposition 2.15(4), we have $\tau \in \mathbb{Z}^+$ such that $a\gamma a^{-1} = \gamma^\tau$ and $\tau^6 \equiv 1 \pmod{pq}$, also $\gcd(\tau - 1, pq) = 1$. This implies that $\tau \not\equiv 1 \pmod p$ and $\tau \not\equiv 1 \pmod q$. We have $C_1 = (\overline{a}^2, \overline{b}, \overline{a}^{-2}, \overline{b}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\mathbb{V}(C_1) = a^2ba^{-2}b^{-1} = a^2a^3\gamma a^{-2}\gamma^{-1}a^{-3} = \gamma^{\tau^5-\tau^3} = \gamma^{\tau^3(\tau^2-1)}.$$

We may assume $\gcd(\tau^2 - 1, pq) \neq 1$ for otherwise Factor Group Lemma 2.6 applies. Without loss of generality let $\tau^2 \equiv 1 \pmod q$, then $\tau \equiv -1 \pmod q$. We may assume $\tau \not\equiv -1 \pmod p$, for otherwise $G \cong D_{2pq} \times \mathcal{C}_3$, so Lemma 2.26 applies.

Consider $\widehat{G} = G/\mathcal{C}_p = \mathcal{C}_6 \ltimes \mathcal{C}_q$. Since $|\overline{a}| = 6$, then by Lemma 2.16 $|a| = 6$, so $|\widehat{a}| = 6$. We may assume $|\widehat{b}| = 2$, for otherwise Corollary 2.7 applies with $s = b$ and $t = b^{-1}$ since $\langle\widehat{a}\rangle \neq \widehat{G}$, so any Hamiltonian cycle must use an edge labeled $\widehat{b}$. Thus, $\widehat{b} = \widehat{a}^3 a_q$, where $\langle a_q\rangle = \mathcal{C}_q$. Since $\tau \equiv -1 \pmod q$, then $\mathcal{C}_3$ centralizes $\mathcal{C}_q$ and $\mathcal{C}_2$ inverts $\mathcal{C}_q$. Therefore, $\widehat{G} \cong D_{2q} \times \mathcal{C}_3$. Now we have

$$C_2 = ((\widehat{a}^5, \widehat{b}, \widehat{a}^{-5}, \widehat{b})^{(q-3)/2}, (\widehat{a}^5, \widehat{b})^3)$$

as a Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 4 on page 13 shows the Hamiltonian cycle when $q = 7$. If in C_2 we change one occurrence of $(\widehat{a}^5, \widehat{b}, \widehat{a}^{-5}, \widehat{b})$ to $(\widehat{a}^{-5}, \widehat{b}, \widehat{a}^5, \widehat{b})$ we have another Hamiltonian cycle. Note that,

$$a^5ba^{-5}b = a^5 \cdot a^3\gamma \cdot a^{-5} \cdot a^3\gamma = a^2\gamma a^{-2}\gamma = \gamma^{\tau^2+1},$$

and

$$a^{-5}ba^5b = a^{-5} \cdot a^3\gamma \cdot a^5 \cdot a^3\gamma = a^{-2}\gamma a^2\gamma = \gamma^{\tau^{-2}+1}.$$

Since $\tau^4 \not\equiv 0 \pmod p$ we see that $\tau^2 + 1 \not\equiv \tau^{-2} + 1 \pmod p$. Therefore, the voltages of these two Hamiltonian cycles are different, so one of these Hamiltonian cycles has a nontrivial voltage. Thus, Factor Group Lemma 2.6 applies.

Subcase 2.2. Assume $|\overline{b}| = 3$. Since $|\overline{b}| = 3$, then $|b| \in \{3, 3p, 3q, 3pq\}$. Since $|\overline{a}| = 6$, then by 2.16 $|a| = 6$. Since $\gcd(|b|, 2) = 1$, then Lemma 2.23 applies.

Subcase 2.3. Assume $|\overline{b}| = 6$. Then we have $\overline{a} = \overline{b}$ or $\overline{a} = \overline{b}^{-1}$. Additionally, by Lemma 2.16 we have $|a| = |b| = 6$. We may assume $\overline{a} = \overline{b}$ by replacing b with its inverse if necessary. Then $b = a\gamma$, where $G' = \langle\gamma\rangle$, because $G = \langle a, b\rangle$. We have $C = (\overline{a}^5, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}, \overline{S})$. Now we calculate its voltage

$$\mathbb{V}(C) = a^5 b = a^5 a\gamma = a^6\gamma = \gamma$$

which generates G'. Therefore, Factor Group Lemma 2.6 applies. □

3.2 Assume $|S| = 2$ and $G' = \mathcal{C}_3 \times \mathcal{C}_p$

In this subsection, we prove the part of Theorem 1.3 where, $|S| = 2$ and $G' = \mathcal{C}_3 \times \mathcal{C}_p$. Recall $\overline{G} = G/G'$ and $\widehat{G} = G/\mathcal{C}_p$.

Proposition 3.3. *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_q) \ltimes (\mathcal{C}_3 \times \mathcal{C}_p)$,
- $|S| = 2$.

Then $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

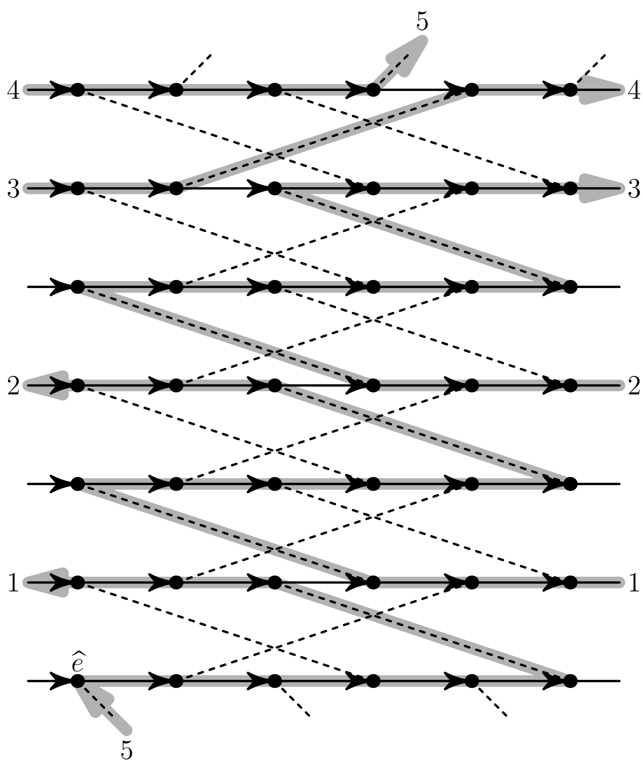


Figure 4: The Hamiltonian cycle C_1: $\hat{a}$ edges are solid and $\hat{b}$ edges are dashed.

Proof. Let $S = \{a, b\}$. Since the only non-trivial automorphism of $\mathcal{C}_3$ is inversion, $\mathcal{C}_q$ centralizes $\mathcal{C}_3$. Since $G' \cap Z(G) = \{e\}$ (see Proposition 2.15(4)), $\mathcal{C}_2$ does not centralize $\mathcal{C}_3$.

Case 1. Assume $|\overline{a}| = |\overline{b}| = 2q$. Then $\overline{b} = \overline{a}^m$, where $1 \leqslant m \leqslant q-1$ by replacing b with its inverse if needed. Therefore, $b = a^m\gamma$, where $G' = \langle\gamma\rangle$. Also, $\gcd(m, 2q) = 1$. So, by Proposition 2.15(4) we have $a\gamma a^{-1} = \gamma^\tau$ where $\tau^{2q} \equiv 1 \pmod{3p}$ and $\gcd(\tau - 1, 3p) = 1$. Consider $\overline{G} = \mathcal{C}_{2q}$.

Subcase 1.1. Assume $m > 3$. Then we have

$$C = (\overline{b}^{-2}, \overline{a}^{-2}, \overline{b}, \overline{a}, \overline{b}, \overline{a}^{-(m-2)}, \overline{b}^{-1}, \overline{a}^{m-4}, \overline{b}^{-1}, \overline{a}^{-(2q-2m-3)})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= b^{-2}a^{-2}baba^{-(m-2)}b^{-1}a^{m-4}b^{-1}a^{-(2q-2m-3)} \\
&= \gamma^{-1}a^{-m}\gamma^{-1}a^{-m}a^{-2}a^m\gamma a a^m\gamma a^{-m+2}\gamma^{-1}a^{-m}a^{m-4}\gamma^{-1}a^{-m}a^{-2q+2m+3} \\
&= \gamma^{-1}a^{-m}\gamma^{-1}a^{-2}\gamma a^{m+1}\gamma a^{-m+2}\gamma^{-1}a^{-4}\gamma^{-1}a^{m+3} \\
&= \gamma^{-1-\tau^{-m}+\tau^{-m-2}+\tau^{-1}-\tau^{-m+1}-\tau^{-m-3}} \\
&= \gamma^{-1+\tau^{-1}-\tau^{-m+1}-\tau^{-m}+\tau^{-m-2}-\tau^{-m-3}}.
\end{aligned}$$

We may assume $\mathbb{V}(C)$ does not generate $G' = \mathcal{C}_3 \times \mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ either does not contain $\mathcal{C}_3$, or does not contain $\mathcal{C}_p$. We already know $\tau \equiv -1 \pmod 3$, then we have

$$-1 + \tau^{-1} - \tau^{-m+1} - \tau^{-m} + \tau^{-m-2} - \tau^{-m-3} \equiv -4 = -1 \pmod 3.$$

This implies that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_3$. So we may assume the subgroup generated by $\mathbb{V}(C)$ does not contain $\mathcal{C}_p$, then

$$0 \equiv -1 + \tau^{-1} - \tau^{-m+1} - \tau^{-m} + \tau^{-m-2} - \tau^{-m-3} \pmod p. \tag{1.1A}$$

Multiplying by $-\tau^{m+3}$ we have

$$0 \equiv \tau^{m+3} - \tau^{m+2} + \tau^4 + \tau^3 - \tau + 1 \pmod p. \tag{1.1B}$$

Replacing $\{\overline{a}, \overline{b}\}$ with $\{\overline{a}^{-1}, \overline{b}^{-1}\}$ replaces τ with τ^{-1}. Therefore, applying the above argument to $\{\overline{a}^{-1}, \overline{b}^{-1}\}$ establishes that 1.1A holds with τ^{-1} in the place of τ, which means we have

$$0 \equiv -\tau^{m+3} + \tau^{m+2} - \tau^m - \tau^{m-1} + \tau - 1 \pmod p. \tag{1.1C}$$

By adding 1.1B and 1.1C we have

$$0 \equiv -\tau^m - \tau^{m-1} + \tau^4 + \tau^3 = \tau^3(\tau + 1)(1 - \tau^{m-4}) \pmod p.$$

If $\tau \equiv -1 \pmod p$, then $\mathcal{C}_{2q}$ inverts $\mathcal{C}_{3p}$, so $\mathcal{C}_q$ centralizes $\mathcal{C}_p$. This implies that $G \cong D_{6p} \times \mathcal{C}_q$, so Lemma 2.26 applies. The only other possibility is $\tau^{m-4} \equiv 1 \pmod p$. Multiplying by τ^4, we have $\tau^m \equiv \tau^4 \pmod p$. We also know that $\tau^{2q} \equiv 1 \pmod p$. So $\tau^d \equiv 1 \pmod p$, where $d = \gcd(m - 4, 2q)$. Since m is odd and $m < q$, then $d = 1$. This contradicts the fact that $\gcd(\tau - 1, 3p) = 1$.

Subcase 1.2. Assume $m \leqslant 3$. Therefore, either $m = 1$ or $m = 3$. If $m = 1$, then $\overline{a} = \overline{b}$ and $b = a\gamma$. So we have $C_1 = (\overline{a}^{2q-1}, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\mathbb{V}(C_1) = a^{2q-1}b = a^{2q-1}a\gamma = \gamma$$

which generates G'. Therefore, Factor Group Lemma 2.6 applies. Now if $m = 3$, then $b = a^3\gamma$ and we have

$$C_2 = (\overline{b}^2, \overline{a}^{-1}, \overline{b}^{-1}, \overline{a}^{-1}, \overline{b}^3, \overline{a}^{-2}, \overline{b}, \overline{a}^{2q-11})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. We calculate its voltage.

$$\begin{aligned}\mathbb{V}(C_2) &= b^2a^{-1}b^{-1}a^{-1}b^3a^{-2}ba^{2q-11}\\ &= a^3\gamma a^3\gamma a^{-1}\gamma^{-1}a^{-3}a^{-1}a^3\gamma a^3\gamma a^3\gamma a^{-2}a^3\gamma a^{-11}\\ &= a^3\gamma a^3\gamma a^{-1}\gamma^{-1}a^{-1}\gamma a^3\gamma a^3\gamma a\gamma a^{-11}\\ &= \gamma^{\tau^3+\tau^6-\tau^5+\tau^4+\tau^7+\tau^{10}+\tau^{11}}\\ &= \gamma^{\tau^{11}+\tau^{10}+\tau^7+\tau^6-\tau^5+\tau^4+\tau^3}\end{aligned}$$

We may assume $\mathbb{V}(C_2)$ does not generate $G' = \mathcal{C}_3 \times \mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ does not contain either $\mathcal{C}_3$, or $\mathcal{C}_p$. We already know $\tau \equiv -1 \pmod 3$, then

$$\tau^{11} + \tau^{10} + \tau^7 + \tau^6 - \tau^5 + \tau^4 + \tau^3 \equiv -1 + 1 - 1 + 1 + 1 + 1 - 1 = 1 \pmod 3.$$

This implies that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_3$. So we may assume the subgroup generated by $\mathbb{V}(C_2)$ does not contain $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.6 applies. Then we have

$$\begin{aligned}0 &\equiv \tau^{11} + \tau^{10} + \tau^7 + \tau^6 - \tau^5 + \tau^4 + \tau^3 \pmod p\\ &= \tau^3(\tau^8 + \tau^7 + \tau^4 + \tau^3 - \tau^2 + \tau + 1).\end{aligned}$$

This implies that

$$0 \equiv \tau^8 + \tau^7 + \tau^4 + \tau^3 - \tau^2 + \tau + 1 \pmod p. \tag{1.2A}$$

We can replace τ with τ^{-1} in the above equation, by replacing $\{\overline{a}, \overline{b}\}$ with $\{\overline{a}^{-1}, \overline{b}^{-1}\}$ if necessary. Then we have

$$0 \equiv \tau^{-8} + \tau^{-7} + \tau^{-4} + \tau^{-3} - \tau^{-2} + \tau^{-1} + 1 \pmod p.$$

Multiplying τ^8, then we have

$$\begin{aligned}0 &\equiv 1 + \tau + \tau^4 + \tau^5 - \tau^6 + \tau^7 + \tau^8 \pmod p\\ &= \tau^8 + \tau^7 - \tau^6 + \tau^5 + \tau^4 + \tau + 1.\end{aligned}$$

Now by subtracting the above equation from 1.2A we have

$$0 \equiv \tau^6 - \tau^5 + \tau^3 - \tau^2 \pmod p$$

$$= \tau^2(\tau - 1)(\tau^3 + 1).$$

This implies that $\tau \equiv 1 \pmod{p}$ or $\tau^3 \equiv -1 \pmod{p}$. If $\tau \equiv 1 \pmod{p}$, then it contradicts the fact that $\gcd(\tau - 1, 3p) = 1$. Now if $\tau^3 \equiv -1 \pmod{p}$, then $\tau^6 \equiv 1 \pmod{p}$. We already know $\tau^{2q} \equiv 1 \pmod{p}$. Then $\tau^d \equiv 1 \pmod{p}$, where $d = \gcd(2q, 6)$. Since $\gcd(2, 6) = 2$ and $\gcd(q, 6) = 1$, then $d = 2$. This implies that $\tau^2 \equiv 1 \pmod{p}$, which means $\mathcal{C}_q$ centralizes $\mathcal{C}_p$. Then we have

$$G = \mathcal{C}_q \times (\mathcal{C}_2 \ltimes \mathcal{C}_{3p}) \cong \mathcal{C}_q \times D_{6p}.$$

So Lemma 2.26 applies.

Case 2. Assume $|\overline{a}| = q$. Then $|\overline{b}| \in \{2, 2q\}$. Thus $|b| \in \{2, 2q, 2p, 2pq\}$. If $|b| = 2pq$, then $\mathcal{C}_q$ centralizes $\mathcal{C}_p$. This implies that

$$G = \mathcal{C}_q \times (\mathcal{C}_2 \ltimes \mathcal{C}_{3p}) \cong \mathcal{C}_q \times D_{6p}$$

so, Lemma 2.26 applies. Therefore, we may assume $\mathcal{C}_q$ does not centralize $\mathcal{C}_p$, so $|a|$ is not divisible by p. If $|b| = 2p$, then Corollary 2.7 applies with $s = b$ and $t = b^{-1}$, because we have a Hamiltonian cycle in $\operatorname{Cay}(\widehat{G}; \widehat{S})$ by Theorem 1.2(3). Since b is the only generator whose order is even, then any Hamiltonian cycle in $\operatorname{Cay}(\widehat{G}; \widehat{S})$ must use some edge labeled $\widehat{b}$.

We may now assume $|b| \in \{2, 2q\}$. We have $C = (\overline{a}^{q-1}, \overline{b}, \overline{a}^{-(q-1)}, \overline{b}^{-1})$ as a Hamiltonian cycle in $\operatorname{Cay}(\overline{G}; \overline{S})$. Now if $|a| = q$, then by Lemma 2.14 we have $G' = \langle [a^{q-1}, b] \rangle$. Therefore, Factor Group Lemma 2.6 applies. So, we may assume $|a| = 3q$. Since $\mathcal{C}_q$ does not centralize $\mathcal{C}_p$, then after conjugation we can assume $a = a_3 a_q$ and $b = a_2 a_q^j \gamma_p$, where $0 \leqslant j \leqslant q - 1$. We already know that C is a Hamiltonian cycle in $\operatorname{Cay}(\overline{G}; \overline{S})$. So we can assume $\gcd(3q, q - 1) \neq 1$ for otherwise Lemma 2.14 applies, which implies that Factor Group Lemma 2.6 applies. This implies that $\gcd(3, q - 1) \neq 1$ which means $q \equiv 1 \pmod{3}$.

Consider $\widehat{G} = G/\mathcal{C}_p$. Then $\widehat{a} = a_3 a_q$ and $\widehat{b} = a_2 a_q^j$. Therefore, there exists $0 \leqslant k \leqslant 3q - 1$ such that $\widehat{b}^{-1}\widehat{a}\widehat{b} = \widehat{a}^k$. Since $\widehat{b}$ inverts a_3 and centralizes a_q, then we must have $\widehat{a} = \widehat{b}\widehat{a}^k\widehat{b}^{-1} = a_3^{-k} a_q^k$, so $k \equiv -1 \pmod{3}$ and $k \equiv 1 \pmod{q}$. Since $q \equiv 1 \pmod{3}$, then $k = q + 1$. Additionally, we have $a\gamma_p a^{-1} = \gamma_p^{\widehat{\tau}}$, where $\widehat{\tau}^q \equiv 1 \pmod{p}$. We also have $\widehat{\tau} \not\equiv 1 \pmod{p}$, because $\mathcal{C}_q$ does not centralize $\mathcal{C}_p$. Now we have

$$b^{-1}ab = \gamma_p^{-1} a_q^{-j} a_2 a a_2 a_q^j \gamma_p = \gamma_p^{-1} a^{q+1} \gamma_p.$$

This implies that

$$b^{-1}a^i b = (b^{-1}ab)^i = (\gamma_p^{-1} a^{q+1} \gamma_p)^i = \gamma_p^{-1} a^{i(q+1)} \gamma_p.$$

Therefore,

$$b^{-1}a^i b = \gamma_p^{-1} a^{i(q+1)} \gamma_p \equiv \gamma_p^{-1} a^i \gamma_p \pmod{\mathcal{C}_3}.$$

We have

$$C_1 = (\widehat{a}^{q-3}, \widehat{b}^{-1}, \widehat{a}^{-(q-2)}, \widehat{b}, \widehat{a}^{-1}, \widehat{b}^{-1}, \widehat{a}, \widehat{b}, \widehat{a}^{q-2}, \widehat{b}^{-1},$$

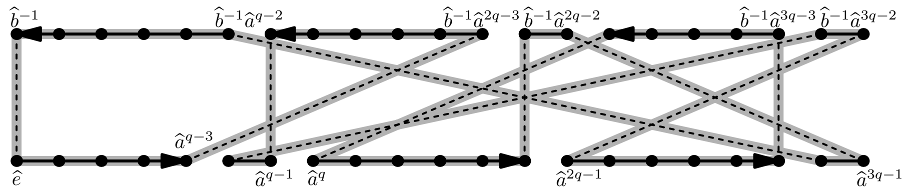


Figure 5: The Hamiltonian cycle C_1: $\hat{a}$ edges are solid and $\hat{b}$ edges are dashed.

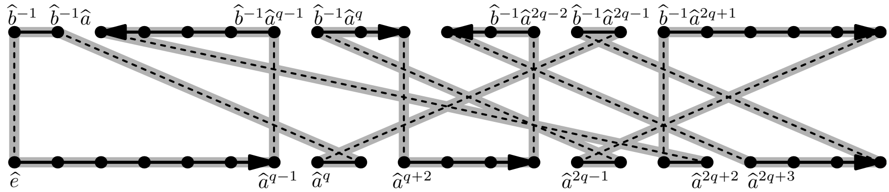


Figure 6: The Hamiltonian cycle C_2: $\hat{a}$ edges are solid and $\hat{b}$ edges are dashed.

$$\hat{a}^{-(q-3)}, \hat{b}, \hat{a}^{q-2}, \hat{b}^{-1}, \hat{a}, \hat{b}, \hat{a}^{-1}, \hat{b}^{-1}, \hat{a}^{-(q-2)}, \hat{b})$$

as our first Hamiltonian cycle in $\operatorname{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 5 on page 17 shows the Hamiltonian cycle. In addition,

$$\begin{aligned} C_2 = (&\hat{a}^{q-1}, \hat{b}^{-1}, \hat{a}^{-(q-3)}, \hat{b}, \hat{a}^{-1}, \hat{b}^{-1}, \hat{a}^{q-2}, \hat{b}, \hat{a}, \hat{b}^{-1}, \hat{a}^{2}, \hat{b}, \\ &\hat{a}^{q-4}, \hat{b}^{-1}, \hat{a}^{-(q-5)}, \hat{b}, \hat{a}^{q-4}, \hat{b}^{-1}, \hat{a}, \hat{b}, \hat{a}, \hat{b}^{-1}, \hat{a}^{-1}, \hat{b}) \end{aligned}$$

is the second Hamiltonian cycle in $\operatorname{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 6 on page 17 shows the Hamiltonian cycle. We calculate the voltage of C_1 in $\overleftrightarrow{G} = G/\mathcal{C}_3$. Since $a^q \equiv e \pmod{\mathcal{C}_3}$, we have

$$\begin{aligned} \mathbb{V}(C_1) &\equiv a^{-3}(b^{-1}a^2b)a^{-1}(b^{-1}ab)a^{-2}(b^{-1}a^3b)a^{-2}(b^{-1}ab)a^{-1}(b^{-1}a^2b) \pmod{\mathcal{C}_3} \\ &= a^{-3}(\gamma_p^{-1}a^2\gamma_p)a^{-1}(\gamma_p^{-1}a\gamma_p)a^{-2}(\gamma_p^{-1}a^3\gamma_p)a^{-2}(\gamma_p^{-1}a\gamma_p)a^{-1}(\gamma_p^{-1}a^2\gamma_p) \\ &= a^{-3}(\gamma_p^{\hat{\tau}^2-1}a^2)a^{-1}(\gamma_p^{\hat{\tau}-1}a)a^{-2}(\gamma_p^{\hat{\tau}^3-1}a^3)a^{-2}(\gamma_p^{\hat{\tau}-1}a)a^{-1}(\gamma_p^{\hat{\tau}^2-1}a^2) \\ &= a^{-3}\gamma_p^{\hat{\tau}^2-1}a\gamma_p^{\hat{\tau}-1}a^{-1}\gamma_p^{\hat{\tau}^3-1}a\gamma_p^{\hat{\tau}^2+\hat{\tau}-2}a^2 \\ &= \gamma_p^{\hat{\tau}^{-3}(\hat{\tau}^2-1)+\hat{\tau}^{-2}(\hat{\tau}-1)+\hat{\tau}^{-3}(\hat{\tau}^3-1)+\hat{\tau}^{-2}(\hat{\tau}^2+\hat{\tau}-2)} \\ &= \gamma_p^{-2\hat{\tau}^{-3}-3\hat{\tau}^{-2}+3\hat{\tau}^{-1}+2}. \end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, so

$$0 \equiv -2\hat{\tau}^{-3} - 3\hat{\tau}^{-2} + 3\hat{\tau}^{-1} + 2 \pmod{p}.$$

Multiplying by $\hat{\tau}^3$, we have

$$0 \equiv 2\hat{\tau}^3 + 3\hat{\tau}^2 - 3\hat{\tau} - 2 = (\hat{\tau} - 1)(\hat{\tau} + 2)(2\hat{\tau} + 1) \pmod{p}.$$

Since $\hat{\tau} \not\equiv 1 \pmod{p}$, then we may assume $\hat{\tau} \equiv -2 \pmod{p}$, by replacing $\hat{a}$ with $\hat{a}^{-1}$ if needed.

Now we calculate the voltage of C_2 in $\overleftrightarrow{G} = G/\mathcal{C}_3$.

$$\begin{aligned}
\mathbb{V}(C_2) &\equiv a^{-1}(b^{-1}a^3b)a^{-1}(b^{-1}a^{-2}b)a(b^{-1}a^2b)\\
&\qquad \cdot a^{-4}(b^{-1}a^5b)a^{-4}(b^{-1}ab)a(b^{-1}a^{-1}b) \pmod{\mathcal{C}_3}\\
&= a^{-1}(\gamma_p^{-1}a^3\gamma_p)a^{-1}(\gamma_p^{-1}a^{-2}\gamma_p)a(\gamma_p^{-1}a^2\gamma_p)\\
&\qquad \cdot a^{-4}(\gamma_p^{-1}a^5\gamma_p)a^{-4}(\gamma_p^{-1}a\gamma_p)a(\gamma_p^{-1}a^{-1}\gamma_p)\\
&= a^{-1}(\gamma_p^{\hat{\tau}^3-1}a^3)a^{-1}(\gamma_p^{\hat{\tau}^{-2}-1}a^{-2})a(\gamma_p^{\hat{\tau}^2-1}a^2)\\
&\qquad \cdot a^{-4}(\gamma_p^{\hat{\tau}^5-1}a^5)a^{-4}(\gamma_p^{\hat{\tau}-1}a)a(\gamma_p^{\hat{\tau}^{-1}-1}a^{-1})\\
&= a^{-1}\gamma_p^{\hat{\tau}^3-1}a^2\gamma_p^{\hat{\tau}^{-2}-1}a^{-1}\gamma_p^{\hat{\tau}^2-1}a^{-2}\gamma_p^{\hat{\tau}^5-1}a\gamma_p^{\hat{\tau}-1}a^2\gamma_p^{\hat{\tau}^{-1}-1}a^{-1}\\
&= \gamma_p^{\hat{\tau}^{-1}(\hat{\tau}^3-1)+\hat{\tau}(\hat{\tau}^{-2}-1)+\hat{\tau}^2-1+\hat{\tau}^{-2}(\hat{\tau}^5-1)+\hat{\tau}^{-1}(\hat{\tau}-1)+\hat{\tau}(\hat{\tau}^{-1}-1)}\\
&= \gamma_p^{\hat{\tau}^3+2\hat{\tau}^2-2\hat{\tau}+1-\hat{\tau}^{-1}-\hat{\tau}^{-2}}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, so

$$0 \equiv \hat{\tau}^3 + 2\hat{\tau}^2 - 2\hat{\tau} + 1 - \hat{\tau}^{-1} - \hat{\tau}^{-2} \pmod{p}.$$

Multiplying by $\hat{\tau}^2$, we have

$$0 \equiv \hat{\tau}^5 + 2\hat{\tau}^4 - 2\hat{\tau}^3 + \hat{\tau}^2 - \hat{\tau} - 1 \pmod{p}.$$

We already know $\hat{\tau} \equiv -2 \pmod{p}$. By substituting this in the equation above, we have

$$0 \equiv (-2)^5 + 2(-2)^4 - 2(-2)^3 + (-2)^2 - (-2) - 1 = 21 = 3 \cdot 7 \pmod{p}.$$

Since $p > 7$, then $21 \not\equiv 0 \pmod{p}$. This is a contradiction.

Case 3. Assume $|\overline{a}| = 2q$ and $|\overline{b}| = 2$. Since $|\overline{a}| = 2q$, then by Lemma 2.16 $|a| = 2q$. We have $b = a^q\gamma$ where $G' = \langle\gamma\rangle$.

By Proposition 2.15(4) we have $a\gamma a^{-1} = \gamma^\tau$, where $\tau^{2q} \equiv 1 \pmod{3p}$ and $\gcd(\tau - 1, 3p) = 1$. This implies that $\tau \not\equiv 0, 1 \pmod{p}$ and $\tau \equiv -1 \pmod{3}$.

Suppose, for the moment, that $\tau \equiv -1 \pmod{p}$. Then $G \cong D_{6p} \times \mathcal{C}_q$, so $\mathrm{Cay}(G; S)$ has a Hamiltonian cycle by Lemma 2.26.

We may now assume that $\tau \not\equiv -1 \pmod{p}$. Recall that $\widehat{G} = G/\mathcal{C}_p = \mathcal{C}_{2q} \ltimes \mathcal{C}_3$. We may assume $\hat{a} = a_2a_q$ and $\hat{b} = a_2a_3$. We have

$$\begin{aligned}
C_1 = ((&\hat{a}, \hat{b}, \hat{a}, \hat{b}, \hat{a}^{-1}, \hat{b}, \hat{a}, \hat{b}, \hat{a}^{-1}, \hat{b}, \hat{a}, \hat{b})^{(q-5)/2}, \hat{a}, \hat{b}, \hat{a}^4,\\
&\hat{b}, \hat{a}^{-3}, \hat{b}, \hat{a}^{-1}, \hat{b}, \hat{a}^2, \hat{b}, \hat{a}^2, \hat{b}, \hat{a}^{-1}, \hat{b}, \hat{a}^{-3}, \hat{b}, \hat{a}^4, \hat{b})
\end{aligned}$$

as the first Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$. The picture in Figure 7 on page 19 shows the Hamiltonian cycle. We also have

$$C_2 = ((\hat{a}, \hat{b}, \hat{a}^{-1}, \hat{b}, \hat{a}, \hat{b})^{q-5}, \hat{a}^3, \hat{b}, \hat{a}^2, \hat{b}, \hat{a}^{-1}, \hat{b}, \hat{a}^{-3}, \hat{b}, \hat{a}^3, \hat{b}, \hat{a}^{-3}, \hat{b}, \hat{a}^{-1}, \hat{b}, \hat{a}^2, \hat{b}, \hat{a}^3, \hat{b})$$

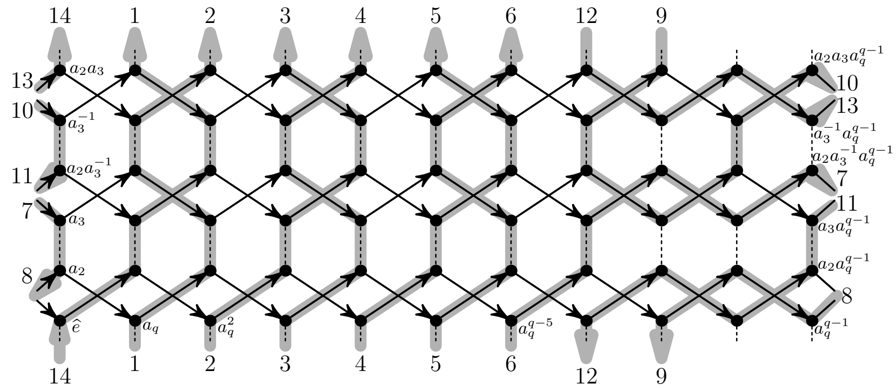


Figure 7: The Hamiltonian cycle C_1: $\widehat{a}$ edges are solid and $\widehat{b}$ edges are dashed.

as the second Hamiltonian cycle in $\mathrm{Cay}(\widehat{G};\widehat{S})$. The picture in Figure 8 on page 21 shows the Hamiltonian cycle. Now we calculate the voltage of C_1.

$$\begin{aligned}
\mathbb{V}(C_1) &= ((ababa^{-1}b)(aba^{-1}bab))^{(q-5)/2}(aba^4ba^{-3}ba^{-1}ba^2ba^2ba^{-1}ba^{-3}ba^4b) \\
&= ((aa^q\gamma aa^q\gamma a^{-1}a^q\gamma)(aa^q\gamma a^{-1}a^q\gamma aa^q\gamma))^{(q-5)/2} \\
&\qquad \cdot (aa^q\gamma a^4a^q\gamma a^{-3}a^q\gamma a^{-1}a^q\gamma a^2a^q\gamma a^2a^q\gamma a^{-1}a^q\gamma a^{-3}a^q\gamma a^4a^q\gamma) \\
&= ((a^{q+1}\gamma a^{q+1}\gamma a^{q-1}\gamma)(a^{q+1}\gamma a^{q-1}\gamma a^{q+1}\gamma))^{(q-5)/2} \\
&\qquad \cdot (a^{q+1}\gamma a^{q+4}\gamma a^{q-3}\gamma a^{q-1}\gamma a^{q+2}\gamma a^{q+2}\gamma a^{q-1}\gamma a^{q-3}\gamma a^{q+4}\gamma) \\
&= ((\gamma^{\tau^{q+1}+\tau^2+\tau^{q+1}}a^{q+1})(\gamma^{\tau^{q+1}+1+\tau^{q+1}}a^{q+1}))^{(q-5)/2} \\
&\qquad \cdot (\gamma^{\tau^{q+1}+\tau^5+\tau^{q+2}+\tau+\tau^{q+3}+\tau^5+\tau^{q+4}+\tau+\tau^{q+5}}a^{q+5}) \\
&= ((\gamma^{2\tau^{q+1}+\tau^2}a^{q+1})(\gamma^{2\tau^{q+1}+1}a^{q+1}))^{(q-5)/2} \\
&\qquad \cdot (\gamma^{\tau^{q+5}+\tau^{q+4}+\tau^{q+3}+\tau^{q+2}+\tau^{q+1}+2\tau^5+2\tau}a^{q+5}) \\
&= ((\gamma^{2\tau^{q+1}+\tau^2+\tau^{q+1}(2\tau^{q+1}+1)}a^2))^{(q-5)/2} \\
&\qquad \cdot (\gamma^{\tau^{q+5}+\tau^{q+4}+\tau^{q+3}+\tau^{q+2}+\tau^{q+1}+2\tau^5+2\tau}a^{q+5}) \\
&= (\gamma^{3\tau^{q+1}+3\tau^2}a^2)^{(q-5)/2}(\gamma^{\tau^{q+5}+\tau^{q+4}+\tau^{q+3}+\tau^{q+2}+\tau^{q+1}+2\tau^5+2\tau}a^{q+5}) \\
&= (\gamma^{(3\tau^{q+1}+3\tau^2)(\tau^{q-5}-1)/(\tau^2-1)}a^{q-5})(\gamma^{\tau^{q+5}+\tau^{q+4}+\tau^{q+3}+\tau^{q+2}+\tau^{q+1}+2\tau^5+2\tau}a^{q+5}) \\
&= \gamma^{(3\tau^{q+1}+3\tau^2)(\tau^{q-5}-1)/(\tau^2-1)+\tau^{q-5}(\tau^{q+5}+\tau^{q+4}+\tau^{q+3}+\tau^{q+2}+\tau^{q+1}+2\tau^5+2\tau)}.
\end{aligned}$$

Since $\tau^{2q} \equiv 1 \pmod p$, we have $\tau^q \equiv \pm 1 \pmod p$.

Let us now consider the case where $\tau^q \equiv 1 \pmod p$, then by substituting this in the formula for the voltage of C_1 we have

$$\begin{aligned}
\mathbb{V}(C_1) &= \gamma^{(3\tau+3\tau^2)(\tau^{-5}-1)/(\tau^2-1)+\tau^{-5}(\tau^5+\tau^4+\tau^3+\tau^2+\tau+2\tau^5+2\tau)} \\
&= \gamma^{3\tau(1+\tau)(\tau^{-5}-1)/(\tau+1)(\tau-1)+(1+\tau^{-1}+\tau^{-2}+\tau^{-3}+\tau^{-4}+2+2\tau^{-4})} \\
&= \gamma^{3\tau(\tau^{-5}-1)/(\tau-1)+(3+\tau^{-1}+\tau^{-2}+\tau^{-3}+3\tau^{-4})}
\end{aligned}$$

$$= \gamma^{(-2+2\tau^{-3})/(\tau-1)}.$$

We may assume this does not generate $\mathcal{C}_p$, then

$$0 \equiv -2 + 2\tau^{-3} \pmod{p}.$$

Multiplying by τ^3, we have

$$0 \equiv -2\tau^3 + 2 \pmod{p}.$$

This implies that $\tau^3 \equiv 1 \pmod{p}$, which contradicts the fact that $\tau^q \equiv 1 \pmod{p}$ but $\tau \not\equiv 1 \pmod{p}$.

Now we may assume $\tau^q \equiv -1 \pmod{p}$, then substituting this in the formula for the voltage of C_1 we have

$$\begin{aligned}\mathbb{V}(C_1) &= \gamma^{(-3\tau+3\tau^2)(-\tau^{-5}-1)/(\tau^2-1)-\tau^{-5}(-\tau^5-\tau^4-\tau^3-\tau^2-\tau+2\tau^5+2\tau)} \\ &= \gamma^{3\tau(\tau-1)(-\tau^{-5}-1)/(\tau+1)(\tau-1)+(1+\tau^{-1}+\tau^{-2}+\tau^{-3}+\tau^{-4}-2-2\tau^{-4})} \\ &= \gamma^{3\tau(-\tau^{-5}-1)/(\tau+1)+(-1+\tau^{-1}+\tau^{-2}+\tau^{-3}-\tau^{-4})} \\ &= \gamma^{(-4\tau+2\tau^{-1}+2\tau^{-2}-4\tau^{-4})/(\tau+1)}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, then

$$0 \equiv -4\tau + 2\tau^{-1} + 2\tau^{-2} - 4\tau^{-4} \pmod{p}.$$

Multiplying by $(-\tau^4)/2$, we have

$$\begin{aligned}0 &\equiv 2\tau^5 - \tau^3 - \tau^2 + 2 \\ &= (\tau+1)(2\tau^4 - 2\tau^3 + \tau^2 - 2\tau + 2) \pmod{p}.\end{aligned}$$

Since we assumed $\tau \not\equiv -1 \pmod{p}$, then the above equation implies that

$$0 \equiv 2\tau^4 - 2\tau^3 + \tau^2 - 2\tau + 2 \pmod{p}. \tag{3A}$$

Now we calculate the voltage of C_2.

$$\begin{aligned}\mathbb{V}(C_2) &= (aba^{-1}bab)^{(q-5)}(a^3ba^2ba^{-1}ba^{-3}ba^3ba^{-3}ba^{-1}ba^2ba^3b) \\ &= (aa^q\gamma a^{-1}a^q\gamma aa^q\gamma)^{(q-5)}(a^3a^q\gamma a^2a^q\gamma \\ &\qquad \cdot a^{-1}a^q\gamma a^{-3}a^q\gamma a^3a^q\gamma a^{-3}a^q\gamma a^{-1}a^q\gamma a^2a^q\gamma a^3a^q\gamma) \\ &= (a^{q+1}\gamma a^{q-1}\gamma a^{q+1}\gamma)^{(q-5)}(a^{q+3}\gamma a^{q+2}\gamma a^{q-1} \\ &\qquad \cdot \gamma a^{q-3}\gamma a^{q+3}\gamma a^{q-3}\gamma a^{q-1}\gamma a^{q+2}\gamma a^{q+3}\gamma) \\ &= (\gamma^{\tau^{q+1}+1+\tau^{q+1}}a^{q+1})^{(q-5)}(\gamma^{\tau^{q+3}+\tau^5+\tau^{q+4}+\tau+\tau^{q+4}+\tau+\tau^q+\tau^2+\tau^{q+5}}a^{q+5}) \\ &= (\gamma^{2\tau^{q+1}+1}a^{q+1})^{(q-5)}(\gamma^{\tau^{q+5}+2\tau^{q+4}+\tau^{q+3}+\tau^q+\tau^5+\tau^2+2\tau}a^{q+5}) \\ &= (\gamma^{(2\tau^{q+1}+1)((\tau^{q+1})^{(q-5)}-1)/(\tau^{q+1}-1)}a^{(q+1)(q-5)}) \\ &\qquad \cdot (\gamma^{\tau^{q+5}+2\tau^{q+4}+\tau^{q+3}+\tau^q+\tau^5+\tau^2+2\tau}a^{q+5})\end{aligned}$$

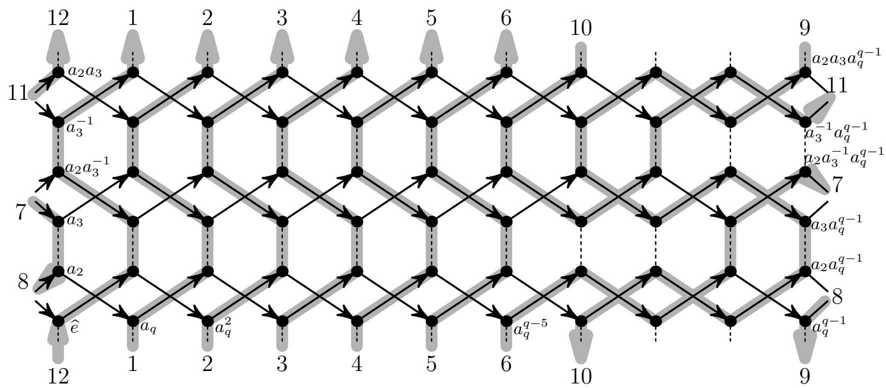


Figure 8: The Hamiltonian cycle C_2: $\widehat{a}$ edges are solid and $\widehat{b}$ edges are dashed.

$$= \gamma^{(2\tau^{q+1}+1)((\tau^{q+1})^{(q-5)}-1)/(\tau^{q+1}-1)+\tau^{(q+1)(q-5)}(\tau^{q+5}+2\tau^{q+4}+\tau^{q+3}+\tau^{q}+\tau^{5}+\tau^{2}+2\tau)}.$$

Since we are assuming $\tau^q \equiv -1 \pmod p$, then by substituting this in the above formula we have

$$\begin{aligned}\mathbb{V}(C_2) &= \gamma^{(-2\tau+1)((-\tau)^{-5}-1)/(-\tau-1)-\tau^{-5}(-\tau^5-2\tau^4-\tau^3-1+\tau^5+\tau^2+2\tau)} \\ &= \gamma^{(2\tau^{-4}+2\tau-\tau^{-5}-1)/(-\tau-1)+1+2\tau^{-1}+\tau^{-2}+\tau^{-5}-1-\tau^{-3}-2\tau^{-4}} \\ &= \gamma^{(2\tau-3-3\tau^{-1}+3\tau^{-3}+3\tau^{-4}-2\tau^{-5})/(-\tau-1)}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, then

$$2\tau - 3 - 3\tau^{-1} + 3\tau^{-3} + 3\tau^{-4} - 2\tau^{-5} \equiv 0 \pmod p.$$

Multiplying by τ^5, we have

$$0 \equiv 2\tau^6 - 3\tau^5 - 3\tau^4 + 3\tau^2 + 3\tau - 2 = (\tau^2 - 1)(2\tau^4 - 3\tau^3 - \tau^2 - 3\tau + 2) \pmod p.$$

Since $\tau^2 \not\equiv 1 \pmod p$, then the above equation implies that

$$0 \equiv 2\tau^4 - 3\tau^3 - \tau^2 - 3\tau + 2 \pmod p.$$

Therefore, by subtracting the above equation from 3A, we have

$$0 \equiv (\tau^3 + 2\tau^2 + \tau) = \tau(\tau+1)^2 \pmod p.$$

This is a contradiction.

Case 4. Assume none of the previous cases apply. Since $\langle \overline{a}, \overline{b} \rangle = \overline{G}$, we may assume $|\overline{a}|$ is divisible by q, which means $|\overline{a}|$ is either q or $2q$. Since Case 2 applies when $|\overline{a}| = q$, we must have $|\overline{a}| = 2q$. Then $|\overline{b}| = q$, since Cases 1 and 3 do not apply. So Case 2 applies after interchanging a and b. □

3.3 Assume $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_3) \neq \{e\}$

In this subsection, we prove the part of Theorem 1.3 where, $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_3) \neq \{e\}$. Recall $\overline{G} = G/G'$, $\breve{G} = G/\mathcal{C}_q$ and $\widehat{G} = G/\mathcal{C}_p$.

Proposition 3.4. *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $C_{G'}(\mathcal{C}_3) \neq \{e\}$.

Then $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

Proof. Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_3) = \mathcal{C}_p \times \mathcal{C}_q$, then since $G' \cap Z(G) = \{e\}$ (see Proposition 2.15(2)), we conclude that $C_{G'}(\mathcal{C}_2) = \{e\}$. So we have

$$G = \mathcal{C}_3 \times (\mathcal{C}_2 \ltimes \mathcal{C}_{pq}) \cong \mathcal{C}_3 \times D_{2pq}.$$

Therefore, Lemma 2.26 applies.

Since $C_{G'}(\mathcal{C}_3) \neq \{e\}$, then we may assume $C_{G'}(\mathcal{C}_3) = \mathcal{C}_q$ by interchanging q and p if necessary. Since $G' \cap Z(G) = \{e\}$, then $\mathcal{C}_2$ inverts $\mathcal{C}_q$. Since $\mathcal{C}_3$ centralizes $\mathcal{C}_q$ and $Z(G) \cap G' = \{e\}$ (by Proposition 2.15(2)), then $\mathcal{C}_2$ inverts $\mathcal{C}_q$. Thus,

$$\widehat{G} = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q \cong (\mathcal{C}_2 \ltimes \mathcal{C}_q) \times \mathcal{C}_3 = D_{2q} \times \mathcal{C}_3.$$

Now if $\widehat{S}$ is minimal, then Lemma 2.24 applies. Therefore, we may assume $\widehat{S}$ is not minimal. Choose a 2-element subset $\{a, b\}$ of S that generates $\widehat{G}$. From the minimality of S, we see that $\langle a, b\rangle = D_{2q} \times \mathcal{C}_3$ after replacing a and b by conjugates. The projection of (a, b) to D_{2q} must be of the form (a_2, a_q) or $(a_2, a_2 a_q)$, where a_2 is reflection and a_q is a rotation. Also note that $\widehat{b} \neq a_q$ because $S \cap G' = \varnothing$ by Assumption 3.1(6). Therefore, (a, b) must have one of the following forms:

1. $(a_2, a_3 a_q)$,
2. $(a_2, a_2 a_3 a_q)$,
3. $(a_2 a_3, a_2 a_q)$,
4. $(a_2 a_3, a_3 a_q)$,
5. $(a_2 a_3, a_2 a_3 a_q)$.

Let c be the third element of S. We may write $c = a_2^i a_3^j a_q^k \gamma_p$ with $0 \leqslant i \leqslant 1, 0 \leqslant j \leqslant 2$ and $0 \leqslant k \leqslant q-1$. Note since $S \cap G' = \varnothing$, we know that i and j cannot both be equal to 0. Additionally, we have $a_3 \gamma_p a_3^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^3 \equiv 1 \pmod{\mathcal{C}_p}$. Also, $\widehat{\tau} \not\equiv 1 \pmod{p}$ since $C_{G'}(\mathcal{C}_3) = \mathcal{C}_q$. Therefore, we conclude that $\widehat{\tau}^2 + \widehat{\tau} + 1 \equiv 0 \pmod{p}$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod{p}$.

Case 1. Assume $a = a_2$ and $b = a_3 a_q$.

Subcase 1.1. Assume $i \neq 0$. Then, $c = a_2 a_3^j a_q^k \gamma_p$. Thus, by Lemma 2.27(1) $\langle b, c\rangle = G$ which contradicts the minimality of S.

Subcase 1.2. Assume $i = 0$. Then $j \neq 0$. We may assume $j = 1$, by replacing c with c^{-1} if necessary. Thus $c = a_3 a_q^k \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. We have $\overline{a} = a_2$, $\overline{b} = a_3$ and $\overline{c} = a_3$. Therefore, $\overline{b} = \overline{c} = a_3$. We have $(\overline{a}, \overline{b}^2, \overline{a}, \overline{b}^{-2})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since we can replace each $\overline{b}$ by $\overline{c}$, then we consider $C_1 = (\overline{a}, \overline{b}^2, \overline{a}, \overline{b}^{-1}, \overline{c}^{-1})$ and $C_2 = (\overline{a}, \overline{b}^2, \overline{a}, \overline{c}^{-2})$ as Hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now since there is one occurrence of c in C_1, then by Lemma 2.8 the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_1) &= ab^2ab^{-1}c^{-1} \\
&\equiv a_2 \cdot a_3^2 a_q^2 \cdot a_2 \cdot a_q^{-1} a_3^{-1} \cdot a_q^{-k} a_3^{-1} \pmod{\mathcal{C}_p} \\
&= a_q^{-2} a_3 a_q^{-1-k} a_3^{-1} \\
&= a_q^{-3-k}.
\end{aligned}$$

We can assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.6 applies. Therefore,

$$-3 - k \equiv 0 \pmod{q}.$$

Thus, $k \equiv -3 \pmod{q}$.

Now we calculate the voltage of C_2.

$$\begin{aligned}
\mathbb{V}(C_2) &= ab^2ac^{-2} \\
&\equiv a_2 \cdot a_3^2 \cdot a_2 \cdot \gamma_p^{-1} a_3^{-1} \gamma_p^{-1} a_3^{-1} \pmod{\mathcal{C}_q} \\
&= a_3^2 \gamma_p^{-1} a_3^{-1} \gamma_p^{-1} a_3^{-1} \\
&= \gamma_p^{-\hat{\tau}^2 - \hat{\tau}}.
\end{aligned}$$

Since $\hat{\tau}^2 + \hat{\tau} + 1 \equiv 0 \pmod{p}$, then $-\hat{\tau}^2 - \hat{\tau} \equiv 1 \pmod{p}$. Thus, $\gamma_p^{-\hat{\tau}^2 - \hat{\tau}} = \gamma_p$ generates $\mathcal{C}_p$.

$$\begin{aligned}
\mathbb{V}(C_2) &= ab^2ac^{-2} \\
&\equiv a_2 \cdot a_3^2 a_q^2 \cdot a_2 \cdot a_q^{-k} a_3^{-1} a_q^{-k} a_3^{-1} \pmod{\mathcal{C}_p} \\
&= a_q^{-2} a_3^2 a_q^{-k} a_3^{-1} a_q^{-k} a_3^{-1} \\
&= a_q^{-2(k+1)}.
\end{aligned}$$

We know $k \equiv -3 \pmod{q}$, therefore, $-2(k+1) \equiv 4 \pmod{q}$, so Factor Group Lemma 2.6 applies.

Case 2. Assume $a = a_2$ and $b = a_2 a_3 a_q$.

Subcase 2.1. Assume $i = 0$, then $j \neq 0$. If $k \neq 0$, then $c = a_3^j a_q^k \gamma_p$. Thus, by Lemma 2.27(3) $\langle b, c\rangle = G$ which contradicts the minimality of S. Therefore, we may assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_3 \gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, thus $\overline{a} = a_2$, $\overline{b} = a_2 a_3$ and $\overline{c} = a_3$. Therefore, $|\overline{a}| = 2$, $|\overline{b}| = 6$ and $|\overline{c}| = 3$. Consider $C = (\overline{b}^2, \overline{c}, \overline{b}, \overline{c}^{-1}, \overline{a})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}\mathbb{V}(C) &= b^2 c b c^{-1} a \\ &\equiv a_2 a_3 a_q a_2 a_3 a_q \cdot a_3 \cdot a_2 a_3 a_q \cdot a_3^{-1} \cdot a_2 \pmod{\mathcal{C}_p} \\ &= a_q^{-1}\end{aligned}$$

which generates $\mathcal{C}_q$. By considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not, we have

$$\begin{aligned}\mathbb{V}(C) &= b^2 c b c^{-1} a \\ &\equiv a_2 a_3 a_2 a_3 \cdot a_3 \gamma_p \cdot a_2 a_3 \cdot \gamma_p^{-1} a_3^{-1} \cdot a_2 \pmod{\mathcal{C}_q} \\ &= \gamma_p a_3 \gamma_p^{\mp 1} a_3^{-1} \\ &= \gamma_p^{1 \mp \hat{\tau}}.\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Subcase 2.2. Assume $j = 0$. Then $i \neq 0$. If $k \neq 1$, then $c = a_2 a_q^k \gamma_p$. Thus, by Lemma 2.27(4) $\langle b, c \rangle = G$ which contradicts the minimality of S. We may therefore assume $k = 1$. Then $c = a_2 a_q \gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = \overline{c} = a_2$ and $\overline{b} = a_2 a_3$. Thus, $|\overline{a}| = |\overline{c}| = 2$ and $|\overline{b}| = 6$. We have $C = (\overline{b}^2, \overline{c}, \overline{b}^{-2}, \overline{a})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= b^2 c b^{-2} a \\ &\equiv a_2 a_3 a_q a_2 a_3 a_q \cdot a_2 a_q \cdot a_q^{-1} a_3^{-1} a_2 a_q^{-1} a_3^{-1} a_2 \cdot a_2 \pmod{\mathcal{C}_p} \\ &= a_q^{-1} a_3 a_q a_3 a_q^{-1} a_3^{-1} a_q a_3^{-1} a_q^{-1} \\ &= a_q^{-1}.\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Subcase 2.3. Assume $i \neq 0$ and $j \neq 0$. We may assume $j = 1$, by replacing c with c^{-1} if necessary. So $c = a_2 a_3 a_q^k \gamma_p$. If $k \neq 1$, then by Lemma 2.27(4) $\langle b, c \rangle = G$ which contradicts the minimality of S. We may now assume $k = 1$. Then $c = a_2 a_3 a_q \gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then $\overline{a} = a_2$ and $\overline{b} = \overline{c} = a_2 a_3$. Therefore, $|\overline{b}| = |\overline{c}| = 6$ and $|\overline{a}| = 2$. We have $C = (\overline{c}, \overline{a}, (\overline{b}, \overline{a})^2)$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ is $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= ca(ba)^2 \\ &\equiv a_2 a_3 a_q \cdot a_2 \cdot a_2 a_3 a_q \cdot a_2 \cdot a_2 a_3 a_q \cdot a_2 \pmod{\mathcal{C}_p} \\ &= a_3 a_q^{-2} a_3 a_q^{-1} a_3 \\ &= a_q^{-3}\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Case 3. Assume $a = a_2a_3$ and $b = a_2a_q$. Since $b = a_2a_q$ is conjugate to a_2 via an element of $\mathcal{C}_q$ (which centralizes $\mathcal{C}_3$), then $\{a, b\}$ is conjugate to $\{a_2a_3a_q^m, a_2\}$ for some nonzero m. So Case 2 applies (after replacing a_q with a_q^m).

Case 4. Assume $a = a_2a_3$ and $b = a_3a_q$.

Subcase 4.1. Assume $i \neq 0$. Then $c = a_2a_3^ja_q^k\gamma_p$. Thus, by Lemma 2.27(1) $\langle b, c\rangle = G$ which contradicts the minimality of S.

Subcase 4.2. Assume $i = 0$. Then $j \neq 0$ and $c = a_3^ja_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.27(2) $\langle a, c\rangle = G$ which contradicts the minimality of S. So we may assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_3\gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Therefore, $\overline{a} = a_2a_3$ and $\overline{b} = \overline{c} = a_3$. In addition, $|\overline{a}| = 6$ and $|\overline{b}| = |\overline{c}| = 3$. We have $C = (\overline{c}, \overline{b}, \overline{a}, \overline{b}^{-2}, \overline{a}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= cbab^{-2}a^{-1} \\
&\equiv a_3 \cdot a_3a_q \cdot a_2a_3 \cdot a_q^{-2}a_3^{-2} \cdot a_3^{-1}a_2 \pmod{\mathcal{C}_p} \\
&= a_3a_qa_3^2a_q^2 \\
&= a_q^3
\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. Thus, Factor Group Lemma 2.6 applies.

Case 5. Assume $a = a_2a_3$, $b = a_2a_3a_q$.

Subcase 5.1. Assume $i = 0$. Then $j \neq 0$ and $c = a_3^ja_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.27(3) $\langle b, c\rangle = G$ which contradicts the minimality of S. So we may assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_3\gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Therefore, $\overline{a} = \overline{b} = a_2a_3$ and $\overline{c} = a_3$. Thus, $|\overline{a}| = |\overline{b}| = 6$ and $|\overline{c}| = 3$. We have $C = (\overline{a}, \overline{c}^2, \overline{b}^{-1}, \overline{c}^{-2})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= ac^2b^{-1}c^{-2} \\
&\equiv a_2a_3 \cdot a_3^2 \cdot a_q^{-1}a_3^{-1}a_2 \cdot a_3^{-2} \pmod{\mathcal{C}_p} \\
&= a_3^{-1}a_qa_3^{-2} \\
&= a_q
\end{aligned}$$

which generates $\mathcal{C}_q$. Also

$$\begin{aligned}
\mathbb{V}(C) &= ac^2b^{-1}c^{-2} \\
&\equiv ac^2a^{-1}c^{-2} \pmod{\mathcal{C}_q} \text{ (because } a \equiv b \pmod{\mathcal{C}_q}) \\
&= ac^{-1}a^{-1}c \text{ (because } |c| = 3) \\
&= [a, c^{-1}].
\end{aligned}$$

This generates $\mathcal{C}_p$, because $\{a, c\}$ generates $G/\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Subcase 5.2. Assume $i \neq 0$. Then $c = a_2 a_3^j a_q^k \gamma_p$. If $k \neq 1$, then by Lemma 2.27(4) $\langle b, c\rangle = G$ which contradicts the minimality of S. So we may assume $k = 1$. Then $c = a_2 a_3^j a_q \gamma_p$. We show that $\langle a, c\rangle = G$. Now, we have

$$\begin{aligned}
\langle a, c\rangle &= \langle a_2, a_3, c\rangle \text{ (because } \langle a\rangle = \langle a_2 a_3\rangle = \langle a_2, a_3\rangle) \\
&= \langle a_2, a_3, a_2 a_3^j a_q \gamma_p\rangle \\
&= \langle a_2, a_3, a_q \gamma_p\rangle \\
&= \langle a_2, a_3, a_q, \gamma_p\rangle \\
&= G,
\end{aligned}$$

which contradicts the minimality of S. □

3.4 Assume $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $\widehat{S}$ is minimal

In this subsection, we prove the part of Theorem 1.3 where, $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_3) = \{e\}$. Recall $\overline{G} = G/G'$ and $\widehat{G} = G/\mathcal{C}_p$.

Proposition 3.5. *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $\widehat{S}$ *is minimal.*

Then $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

Proof. Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_3) \neq \{e\}$, then Proposition 3.4 applies. Hence we may assume $C_{G'}(\mathcal{C}_3) = \{e\}$. Then we have four different cases.

Case 1. Assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$, thus $G = \mathcal{C}_2 \times (\mathcal{C}_3 \ltimes \mathcal{C}_{pq})$. Since $\widehat{S}$ is minimal, then all three elements belonging to $\widehat{S}$ must have prime order. There is an element $\widehat{a} \in \widehat{S}$, such that $|\widehat{a}| = 2$, otherwise all elements of S belong to a subgroup of index 2 of G, so $\langle a, b, c\rangle \neq G$ which is a contradiction. If $|a| = 2p$, then Corollary 2.7 applies with $s = a$ and $t = a^{-1}$, because there is a Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$ (see Theorem 1.2(3)) which uses at least one labeled edge $\widehat{a}$ because $\widehat{S}$ is minimal.

Now we may assume $|a| = 2$. Replacing a by a conjugate we may assume $\langle a\rangle = \mathcal{C}_2$. Thus, $\langle b, c\rangle = \mathcal{C}_3 \ltimes \mathcal{C}_{pq}$. By Theorem 1.2(3), there is a Hamiltonian path L in $\mathrm{Cay}(\mathcal{C}_3 \ltimes \mathcal{C}_{pq}, \{b, c\})$. Therefore, $LaL^{-1}a^{-1}$ is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$.

Case 2. Assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_q$. Therefore,

$$\widehat{G} = G/\mathcal{C}_p = \mathcal{C}_6 \ltimes \mathcal{C}_q \cong \mathcal{C}_2 \times (\mathcal{C}_3 \ltimes \mathcal{C}_q).$$

There is some $a \in S$ such that $|\widehat{a}| = 2$. Thus, we can assume $|a| = 2$, for otherwise Corollary 2.7 applies with $s = a$ and $t = a^{-1}$. (Note since $\widehat{S}$ is minimal, then $\widehat{a}$ must be used in any Hamiltonian cycle in $\mathrm{Cay}(\widehat{G};\widehat{S})$.) We may assume $a = a_2$. Since $\widehat{S}$ is minimal, $S \cap G' = \varnothing$ (see Assumption 3.1(6)) and each element belonging to $\widehat{S}$ has prime order, then $|\widehat{b}| = |\widehat{c}| = 3$. We may assume $\widehat{a} = a_2$, $\widehat{b} = a_3$ and $\widehat{c} = a_3 a_q$. We have the following two Hamiltonian paths in $\mathrm{Cay}(\mathcal{C}_3 \ltimes \mathcal{C}_q; \{\widehat{b}, \widehat{c}\})$:

$$L_1 = ((\widehat{c}, \widehat{b}^2)^{q-1}, \widehat{c}, \widehat{b})$$

and

$$L_2 = ((\widehat{b}, \widehat{c}, \widehat{b})^{q-1}, \widehat{b}, \widehat{c}).$$

These lead to the following two Hamiltonian cycles in $\mathrm{Cay}(\widehat{G};\widehat{S})$:

$$C_1 = (L_1, \widehat{a}, L_1^{-1}, \widehat{a})$$

and

$$C_2 = (L_2, \widehat{a}, L_2^{-1}, \widehat{a}).$$

Then if we let

$$\prod L_1 = (cb^2)^{q-1}cb = (cb^2)^q b^{-1} \in a_3^{-1}\mathcal{C}_p$$

and

$$\prod L_2 = (bcb)^{q-1}bc = (bcb)^q b^{-1} = b(cb^2)^q b^{-2} = b(\prod L_1)b^{-1}$$

then it is clear that $V(C_i) = [\prod L_i, a]$ for $i = 1, 2$. Therefore, we may assume a centralizes $\prod L_1$ and $\prod L_2$, for otherwise Factor Group Lemma 2.6 applies. Now, since a centralizes $\prod L_1$, and $\prod L_1 \in a_3^{-1}\mathcal{C}_p$, we must have $\prod L_1 = a_3^{-1}$. So $\prod L_2 = ba_3^{-1}b^{-1}$. If b does not centralize a_3, then $\mathbb{V}(C_1) \neq \mathbb{V}(C_2)$, so the voltage of C_1 or C_2 cannot both be equal to identity. Therefore, Factor Group Lemma 2.6 applies. Now if b centralizes a_3, then we can assume $b = a_3$. Therefore, $c = a_3 a_q \gamma_p$. We calculate the voltage of C_1. We have

$$\begin{aligned}
\mathbb{V}(C_1) &= (cb^2)^q b^{-1} a((cb^2)^q b^{-1})^{-1} a \\
&= (a_3 a_q \gamma_p \cdot a_3^2)^q \cdot a_3^{-1} \cdot a_2 \cdot ((a_3 a_q \gamma_p \cdot a_3^2)^q \cdot a_3^{-1})^{-1} \cdot a_2 \\
&= (a_3 a_q \gamma_p a_3^{-1})^q a_3^{-1} a_2 ((a_3 a_q \gamma_p a_3^{-1}) a_3^{-1})^{-1} a_2 \\
&= a_3 a_q^q \gamma_p^q a_3^{-1} a_3^{-1} a_2 (a_3 a_q^q \gamma_p^q a_3^{-1} a_3^{-1})^{-1} a_2 \\
&= a_3 \gamma_p^q a_3^{-2} a_2 (a_3 \gamma_p^q a_3^{-2})^{-1} a_2 \\
&= a_3 \gamma_p^q a_3^{-2} a_2 a_3^2 \gamma_p^{-q} a_3^{-1} a_2 \\
&= a_3 \gamma_p^{2q} a_3^{-1}
\end{aligned}$$

which generates $\mathcal{C}_p$. Thus, Factor Group Lemma 2.6 applies.

Case 3. Assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p$. Therefore,

$$\breve{G} = G/\mathcal{C}_q = \mathcal{C}_6 \ltimes \mathcal{C}_p \cong \mathcal{C}_2 \times (\mathcal{C}_3 \ltimes \mathcal{C}_p).$$

Now since $S \cap G' = \varnothing$ (see Assumption 3.1(6)) and $\mathcal{C}_3$ does not centralize $\mathcal{C}_p$, then for all $a \in S$, we have $|\breve{a}| \in \{2, 3, 6, 2p\}$. If $|\breve{a}| = 6$, then $|\widehat{a}|$ is divisible by 6 which contradicts the minimality of $\widehat{S}$. Note that every element belong to $\widehat{S}$ has prime order. If $|\breve{a}| = 2p$, then $|\widehat{a}| = 2$ (because $\widehat{S}$ is minimal). Therefore, Corollary 2.7 applies with $s = a$ and $t = a^{-1}$. Note that since $\widehat{S}$ is minimal, then there is a Hamiltonian cycle in $\mathrm{Cay}(\widehat{G}; \widehat{S})$ uses at least one labeled edge $\widehat{a}$. Thus, $|\breve{a}| \in \{2, 3\}$ for all $a \in S$. This implies that $\breve{S}$ is minimal, because we need an a_2 and an a_3 to generate $\mathcal{C}_2 \times \mathcal{C}_3$ and two elements whose order divisible by 2 or 3 to generate $\mathcal{C}_p$. So by interchanging p and q the proof in Case 2 applies.

Case 4. Assume $C_{G'}(\mathcal{C}_2) = \{e\}$. Consider

$$\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q.$$

Now since $\widehat{S}$ is minimal, every element of $\widehat{S}$ has prime order. Since $S \cap G' = \varnothing$ (see Assumption 3.1(6)), then for every $\widehat{s} \in \widehat{S}$, we have $|\widehat{s}| \in \{2, 3\}$. Since $C_{G'}(\mathcal{C}_2) = \{e\}$ and $C_{G'}(\mathcal{C}_3) = \{e\}$, this implies that for every $s \in S$, we have $|s| \in \{2, 3\}$. From our assumption we know that $S = \{a, b, c\}$. Now we may assume $|a| = 2$ and $|b| = 3$. Also, we know that $|c| \in \{2, 3\}$.

If $|c| = 2$, then $c = a\gamma$, where $\gamma \in G'$. Suppose, for the moment, $\langle\gamma\rangle \neq G'$. Since $\langle\gamma\rangle \lhd G$, then we have

$$G = \langle a, b, c\rangle = \langle a, b, \gamma\rangle = \langle a, b\rangle\langle\gamma\rangle.$$

Now since $\widehat{S}$ is minimal, $\langle a, b\rangle$ does not contain $\mathcal{C}_q$. So this implies that $\langle\gamma\rangle$ contains $\mathcal{C}_q$. Since $\langle\gamma\rangle$ does not contain G', then $\langle\gamma\rangle = \mathcal{C}_q$. Thus, we may assume that $a = a_2$ (by conjugation if necessary), $b = a_3\gamma_p$ and $c = a_2 a_q$. So $\langle b, c\rangle = \langle a_3\gamma_p, a_2 a_q\rangle = G$ (since $a_3\gamma_p$ and $a_2 a_q$ clearly generate $\overline{G}$ and do not commute modulo p or modulo q, they must generate G). This contradicts the minimality of S. Therefore, $\langle\gamma\rangle = G'$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then $\overline{a} = \overline{c}$. We have $|\overline{a}| = |\overline{c}| = 2$ and $|\overline{b}| = 3$. We also have $C_1 = (\overline{c}^{-1}, \overline{b}^{-2}, \overline{a}, \overline{b}^2)$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\mathbb{V}(C_1) = c^{-1}b^{-2}ab^2 = \gamma^{-1}a^{-1}b^{-2}ab^2.$$

Now, $a^{-1}b^{-2}ab^2 \in G'$. Since $\langle a, b\rangle \neq G$, we have $a^{-1}b^{-2}ab^2 \in \{e, \gamma_p\}$. If $a^{-1}b^{-2}ab^2 = e$, then a and b^2 commute, so a and b commute. Hence $b = a_3$, so $\langle b, c\rangle = G$, a contradiction. So $a^{-1}b^{-2}ab^2 = \gamma_p$, and $\mathbb{V}(C_1) = \gamma^{-1}\gamma_p$ which generates G'. Therefore, Factor Group Lemma 2.6 applies.

Now we can assume $|c| = 3$. Then $c = b\gamma$, where $\gamma \in G'$ (after replacing c with its inverse if necessary). Suppose, for the moment, $\langle\gamma\rangle \neq G'$. Since $\langle\gamma\rangle \lhd G$, then we have

$$G = \langle a, b, c\rangle = \langle a, b, \gamma\rangle = \langle a, b\rangle\langle\gamma\rangle.$$

Now since $\widehat{S}$ is minimal, then $\langle a, b\rangle$ does not contain $\mathcal{C}_q$. So this implies that $\langle\gamma\rangle$ contains $\mathcal{C}_q$. Since $\langle\gamma\rangle$ does not contain G', then $\langle\gamma\rangle = \mathcal{C}_q$. Therefore, we may assume that $a = a_2\gamma_p$ (by conjugation if necessary), $b = a_3$ and $c = a_3 a_q$. So $\langle a, c\rangle = \langle a_2\gamma_p, a_3 a_q\rangle = G$ (since $a_2\gamma_p$ and $a_3 a_q$ clearly generate $\overline{G}$ and do not commute modulo p or modulo q, they must generate G). This contradicts the minimality of S. So $\langle\gamma\rangle = G'$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then $\overline{b} = \overline{c}$. We have $|\overline{a}| = 2$ and $|\overline{b}| = |\overline{c}| = 3$. We also have $C_2 = (\overline{c}^{-1}, \overline{b}^{-1}, \overline{a}^{-1}, \overline{b}^{2}, \overline{a})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\mathbb{V}(C_2) = c^{-1}b^{-1}a^{-1}b^2a = \gamma^{-1}b^{-1}b^{-1}a^{-1}b^2a.$$

Now, $b^{-2}a^{-1}b^2a \in G'$. Since $\langle a, b\rangle \neq G$, we have $b^{-2}a^{-1}b^2a \in \{e, \gamma_p\}$. If $b^{-2}a^{-1}b^2a = e$, then a and b^2 commute, so a and b commute. Hence $a = a_2$, so $\langle a, c\rangle = G$, a contradiction. So $b^{-2}a^{-1}b^2a = \gamma_p$, and $\mathbb{V}(C_2) = \gamma^{-1}\gamma_p$ which generates G'. Therefore, Factor Group Lemma 2.6 applies. □

3.5 Assume $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$

In this subsection, we prove the part of Theorem 1.3 where, $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$, $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$, and neither $C_{G'}(\mathcal{C}_3) \neq \{e\}$ nor $\widehat{S}$ is minimal holds. Recall $\overline{G} = G/G'$, $\breve{G} = G/\mathcal{C}_q$ and $\widehat{G} = G/\mathcal{C}_p$.

Proposition 3.6. *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$.

Then $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

Proof. Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_3) \neq \{e\}$, then Proposition 3.4 applies. So we may assume $C_{G'}(\mathcal{C}_3) = \{e\}$. Now if $\widehat{S}$ is minimal, then Proposition 3.5 applies. So we may assume $\widehat{S}$ is not minimal. Consider

$$\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q \cong (\mathcal{C}_3 \ltimes \mathcal{C}_q) \times \mathcal{C}_2.$$

Choose a 2-element $\{a, b\}$ subset of S that generates $\widehat{G}$. From the minimality of S, we see that

$$\langle a, b\rangle = (\mathcal{C}_3 \ltimes \mathcal{C}_q) \times \mathcal{C}_2,$$

after replacing a and b by conjugates. The projection of (a, b) to $\mathcal{C}_3 \ltimes \mathcal{C}_q$ must be of the form (a_3, a_q) or (a_3, a_3a_q) (perhaps after replacing a and/or b with its inverse; also note that $\widehat{b} \neq a_q$ because $S \cap G' = \varnothing$). Therefore, (a, b) must have one of the following forms:

1. (a_3, a_2a_q),
2. $(a_3, a_2a_3a_q)$,
3. (a_2a_3, a_3a_q),
4. (a_2a_3, a_2a_q),
5. $(a_2a_3, a_2a_3a_q)$.

Let c be the third element of S. We may write $c = a_2^i a_3^j a_q^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant 2$ and $0 \leqslant k \leqslant q-1$. Note since $S \cap G' = \varnothing$, we know that i and j cannot both be equal to 0. Additionally, we have $a_3 \gamma_p a_3^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^3 \equiv 1 \pmod{p}$ and $\widehat{\tau} \not\equiv 1 \pmod{p}$. Thus $\widehat{\tau}^2 + \widehat{\tau} + 1 \equiv 0 \pmod{p}$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod{p}$. Also we have $a_3 a_q a_3^{-1} = a_q^{\check{\tau}}$. By using the same argument we can conclude that $\check{\tau} \not\equiv 1 \pmod{q}$ and $\check{\tau}^2 + \check{\tau} + 1 \equiv 0 \pmod{q}$. Note that this implies $\check{\tau} \not\equiv -1 \pmod{q}$. Combining these facts with $\widehat{\tau}^3 \equiv 1 \pmod{p}$ and $\check{\tau}^3 \equiv 1 \pmod{q}$, we conclude that $\widehat{\tau}^2 \not\equiv \pm 1 \pmod{p}$, and $\check{\tau}^2 \not\equiv \pm 1 \pmod{q}$.

Case 1. Assume $a = a_3$ and $b = a_2 a_q$.

Subcase 1.1. Assume $i = 0$. Then $j \neq 0$ and $c = a_3^j a_q^k \gamma_p$. For future reference in Subcase 4.1 of Proposition 3.7, we note that the argument here does not require our current assumption that $\mathcal{C}_2$ centralizes $\mathcal{C}_p$. We may assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_3 a_q^k \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = \overline{c} = a_3$, $\overline{b} = a_2$. We have $C_1 = (\overline{c}, \overline{a}, \overline{b}, \overline{a}^{-2}, \overline{b})$ and $C_2 = (\overline{c}^2, \overline{b}, \overline{a}^{-2}, \overline{b})$ as Hamiltonian cycles in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C_1, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_1) &= caba^{-2}b \\
&\equiv a_3 a_q^k \cdot a_3 \cdot a_2 a_q \cdot a_3^{-2} \cdot a_2 a_q \pmod{\mathcal{C}_p} \\
&= a_q^{k\check{\tau} + \check{\tau}^2 + 1} \\
&= a_q^{\check{\tau}^2 + k\check{\tau} + 1}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.6 applies. Therefore,

$$0 \equiv \check{\tau}^2 + k\check{\tau} + 1 \pmod{q}. \tag{1.1A}$$

We also have

$$0 \equiv \check{\tau}^2 + \check{\tau} + 1 \pmod{q}. \tag{1.1B}$$

By subtracting the above equation from 1.1A, we have $0 \equiv (k-1)\check{\tau} \pmod{q}$. This implies that $k = 1$.

Now we calculate the voltage of C_2.

$$\begin{aligned}
\mathbb{V}(C_2) &= c^2 ba^{-2}b \\
&\equiv a_3 \gamma_p a_3 \gamma_p \cdot a_2 \cdot a_3^{-2} \cdot a_2 \pmod{\mathcal{C}_q} \\
&= \gamma_p^{\widehat{\tau} + \widehat{\tau}^2}
\end{aligned}$$

which generates $\mathcal{C}_p$. Also

$$\begin{aligned}
\mathbb{V}(C_2) &= c^2 ba^{-2}b \\
&\equiv a_3 a_q \cdot a_3 a_q \cdot a_2 a_q \cdot a_3^{-2} \cdot a_2 a_q \pmod{\mathcal{C}_p} \\
&= a_q^{\check{\tau} + \check{\tau}^2 + \check{\tau}^2 + 1} \\
&= a_q^{2\check{\tau}^2 + \check{\tau} + 1}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.6 applies. Then

$$0 \equiv 2\check{\tau}^2 + \check{\tau} + 1 \pmod{q}.$$

By subtracting 1.1B from the above equation we have

$$0 \equiv \check{\tau}^2 \pmod{q}$$

which is a contradiction.

Subcase 1.2. Assume $j = 0$. Then $i \neq 0$ and $c = a_2 a_q^k \gamma_p$. For future reference in Subcase 4.2 of Proposition 3.7, we note that the argument here does not require our current assumption that $\mathcal{C}_2$ centralizes $\mathcal{C}_p$. If $k \neq 0$, then by Lemma 2.28(3) $\langle a, c \rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = a_3$ and $\overline{b} = \overline{c} = a_2$. This implies that $|\overline{a}| = 3$ and $|\overline{b}| = |\overline{c}| = 2$. We have $C = (\overline{c}^{-1}, \overline{a}^2, \overline{b}, \overline{a}^{-2})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Similarly, since there is one occurrence of b in C, and it is the only generator of G that contains a_q, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Subcase 1.3. Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2 a_3^j a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.28(3) $\langle a, c \rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_2 a_3 \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = a_3$, $\overline{b} = a_2$ and $\overline{c} = a_2 a_3$. This implies that $|\overline{a}| = 3$, $|\overline{b}| = 2$ and $|\overline{c}| = 6$. We have $C = (\overline{c}, \overline{b}, \overline{a}, \overline{c}, \overline{a}^{-1}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= cbaca^{-1}c \\
&\equiv a_2 a_3 \cdot a_2 a_q \cdot a_3 \cdot a_2 a_3 \cdot a_3^{-1} \cdot a_2 a_3 \pmod{\mathcal{C}_p} \\
&= a_3 a_q a_3^2 \\
&= a_q^{\check{\tau}}
\end{aligned}$$

which generates $\mathcal{C}_q$. Also

$$\begin{aligned}
\mathbb{V}(C) &= cbaca^{-1}c \\
&\equiv a_2 a_3 \gamma_p \cdot a_2 \cdot a_3 \cdot a_2 a_3 \gamma_p \cdot a_3^{-1} \cdot a_2 a_3 \gamma_p \pmod{\mathcal{C}_q} \\
&= a_3 \gamma_p a_3^2 \gamma_p^2 \\
&= \gamma_p^{\hat{\tau}+2}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.6 applies. Then $\hat{\tau} \equiv -2 \pmod{p}$. By substituting this in

$$0 \equiv \hat{\tau}^2 + \hat{\tau} + 1 \pmod{p},$$

we have

$$\begin{aligned} 0 &\equiv 4 - 2 + 1 \pmod{p} \\ &= 3. \end{aligned}$$

This contradicts the fact that $p > 3$.

Case 2. Assume $a = a_3$ and $b = a_2a_3a_q$.

Subcase 2.1. Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2a_3^ja_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.28(3) $\langle a, c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$. Then $c = a_2a_3^j\gamma_p$. Thus, by Lemma 2.28(4) $\langle b, c\rangle = G$ which contradicts the minimality of S.

Subcase 2.2. Assume $i = 0$. Then $j \neq 0$. We may assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_3a_q^k\gamma_p$.

Suppose, for the moment, that $k \neq 1$. Then $c = a_3a_q^k\gamma_p$. We have $\langle\overline{b}, \overline{c}\rangle = \langle\overline{a}_2\overline{a}_3, \overline{a}_3\rangle = \overline{G}$. Consider $\{\widehat{b}, \widehat{c}\} = \{a_2a_3a_q, a_3a_q^k\}$. Since $\mathcal{C}_2$ centralizes $\mathcal{C}_q$, then

$$\begin{aligned} [a_2a_3a_q, a_3a_q^k] = [a_3a_q, a_3a_q^k] = a_3a_qa_3a_q^ka_q^{-1}a_3^{-1}a_q^{-k}a_3^{-1} &= a_q^{\check{\tau}+k\check{\tau}^2-\check{\tau}^2-k\check{\tau}} \\ &= a_q^{\check{\tau}(k-1)(\check{\tau}-1)} \end{aligned}$$

which generates $\mathcal{C}_q$. Now consider $\{\check{b}, \check{c}\} = \{a_2a_3, a_3\gamma_p\}$. Since $\mathcal{C}_2$ centralizes $\mathcal{C}_p$, then

$$[a_2a_3, a_3\gamma_p] = [a_3, a_3\gamma_p] = a_3a_3\gamma_pa_3^{-1}\gamma_p^{-1}a_3^{-1} = \gamma_p^{\hat{\tau}^2-\hat{\tau}} = \gamma_p^{\hat{\tau}(\hat{\tau}-1)}$$

which generates $\mathcal{C}_p$. Therefore, $\langle b, c\rangle = G$ which contradicts the minimality of S.

Now we can assume $k = 1$. Then $c = a_3a_q\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. We have $\overline{a} = \overline{c} = a_3$ and $\overline{b} = a_2a_3$. This implies that $|\overline{a}| = |\overline{c}| = 3$ and $|\overline{b}| = 6$. We have $C = (\overline{c}, \overline{b}, \overline{a}^2, \overline{b}, \overline{a})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ is $\mathcal{C}_p$. Also,

$$\begin{aligned} \mathbb{V}(C) &= cba^2ba \\ &\equiv a_3a_q \cdot a_2a_3a_q \cdot a_3^2 \cdot a_2a_3a_q \cdot a_3 \pmod{\mathcal{C}_p} \\ &= a_3a_qa_3a_q^2a_3 \\ &= a_q^{\check{\tau}+2\check{\tau}^2} \\ &= a_q^{\check{\tau}(1+2\check{\tau})}. \end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.6 applies. Therefore, $1 + 2\check{\tau} \equiv 0 \pmod{q}$. This implies that $\check{\tau} \equiv -1/2 \pmod{q}$. By substituting $\check{\tau} \equiv -1/2 \pmod{q}$ in

$$\check{\tau}^2 + \check{\tau} + 1 \equiv 0 \pmod{q},$$

then we have $3/4 \equiv 0 \pmod{q}$, which contradicts Assumption 3.1(1).

Subcase 2.3. Assume $j = 0$. Then $i \neq 0$ and $c = a_2 a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.28(3) $\langle a, c\rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = a_3$, $\overline{b} = a_2a_3$ and $\overline{c} = a_2$. This implies that $|\overline{a}| = 3$, $|\overline{b}| = 6$ and $|\overline{c}| = 2$. We have $C = (\overline{c}, \overline{a}, \overline{b}, \overline{a}^{-1}, \overline{b}^2)$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= caba^{-1}b^2\\ &\equiv a_2 \cdot a_3 \cdot a_2a_3a_q \cdot a_3^{-1} \cdot a_2a_3a_qa_2a_3a_q \pmod{\mathcal{C}_p}\\ &= a_3^2a_q^2a_3a_q\\ &= a_q^{2\check{\tau}^2+1}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.6 applies. Thus, $\check{\tau}^2 \equiv -1/2 \pmod q$. By substituting this in

$$\check{\tau}^2 + \check{\tau} + 1 \equiv 0 \pmod q,$$

we have $\check{\tau} \equiv -1/2 \pmod q$ which contradicts $\check{\tau}^2 \equiv -1/2 \pmod q$.

Case 3. Assume $a = a_2a_3$ and $b = a_3a_q$. Since $b = a_3a_q$ is conjugate to a_3 via an element of $\mathcal{C}_q$, then $\{a, b\}$ is conjugate to $\{a_2a_3a_q^m, a_3\}$ for some nonzero m. So Case 2 applies (after replacing a_q with a_q^m).

Case 4. Assume $a = a_2a_3$ and $b = a_2a_q$.

Subcase 4.1. Assume $i = 0$. Then $j \neq 0$ and $c = a_3^j a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.28(1) $\langle a, c\rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_3\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Thus, $\overline{a} = a_2a_3$, $\overline{b} = a_2$ and $\overline{c} = a_3$. This implies that $|\overline{a}| = 6$, $|\overline{b}| = 2$ and $|\overline{c}| = 3$. We have $C = (\overline{a}^2, \overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of b in C, and it is the only generator of G that contains a_q, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Also,

$$\begin{aligned}\mathbb{V}(C) &= a^2bcac^{-1}\\ &\equiv a_3^2 \cdot a_2 \cdot a_3\gamma_p \cdot a_2a_3 \cdot \gamma_p^{-1}a_3^{-1} \pmod{\mathcal{C}_q}\\ &= \gamma_pa_3\gamma_p^{-1}a_3^{-1}\\ &= \gamma_p^{1-\hat{\tau}}\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Subcase 4.2. Assume $j = 0$. Then $i \neq 0$ and $c = a_2a_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.28(1) $\langle a, c\rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_2a_3$ and $\overline{b} = \overline{c} = a_2$. This implies that $|\overline{a}| = 6$ and $|\overline{b}| = |\overline{c}| = 2$. We have $C = ((\overline{a}, \overline{b})^2, \overline{a}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= (ab)^2ac \\ &\equiv (a_2a_3 \cdot a_2a_q)^2 \cdot a_2a_3 \cdot a_2 \pmod{\mathcal{C}_p} \\ &= a_3a_qa_3a_qa_3 \\ &= a_q^{\check{\tau}+\check{\tau}^2}.\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. Thus, Factor Group Lemma 2.6 applies.

Subcase 4.3. Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2a_3^ja_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.28(1) $\langle a, c\rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_2a_3\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Thus, $\overline{a} = \overline{c} = a_2a_3$ and $\overline{b} = a_2$. This implies that $|\overline{a}| = |\overline{c}| = 6$ and $|\overline{b}| = 2$. We have $C = (\overline{a}, \overline{c}, \overline{b}, \overline{a}^{-2}, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= acba^{-2}b \\ &\equiv a_2a_3 \cdot a_2a_3 \cdot a_2a_q \cdot a_3^{-2} \cdot a_2a_q \pmod{\mathcal{C}_p} \\ &= a_3^2a_qa_3^{-2}a_q \\ &= a_q^{\check{\tau}^2+1}\end{aligned}$$

which generates $\mathcal{C}_q$, because $\check{\tau}^2 \not\equiv -1 \pmod{q}$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Case 5. Assume $a = a_2a_3$ and $b = a_2a_3a_q$. If $k \neq 0$, then by Lemma 2.28(1) $\langle a, c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$. Also, if $j \neq 0$, then by Lemma 2.28(4) $\langle b, c\rangle = G$ which contradicts the minimality of S. So we may also assume $j = 0$. Then $i \neq 0$. Therefore, $c = a_2\gamma_p$. So Case 4 applies, after interchanging b and c, and interchanging p and q. □

3.6 Assume $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_2) \neq \{e\}$

In this subsection, we prove the part of Theorem 1.3 where, $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$, $C_{G'}(\mathcal{C}_2) \neq \{e\}$, and neither $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$ nor $C_{G'}(\mathcal{C}_3) \neq \{e\}$ nor $\widehat{S}$ is minimal holds. Recall $\overline{G} = G/G'$, $\check{G} = G/\mathcal{C}_q$ and $\widehat{G} = G/\mathcal{C}_p$.

Proposition 3.7. *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $C_{G'}(\mathcal{C}_2) \neq \{e\}$.

Then $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

Proof. Let $S = \{a, b, c\}$. If $C_{G'}(\mathcal{C}_3) \neq \{e\}$, then Proposition 3.4 applies. Therefore, we may assume $C_{G'}(\mathcal{C}_3) = \{e\}$. Now if $C_{G'}(\mathcal{C}_2) = \mathcal{C}_p \times \mathcal{C}_q$, then Proposition 3.6 applies. Since $C_{G'}(\mathcal{C}_2) \neq \{e\}$, then we may assume $C_{G'}(\mathcal{C}_2) = \mathcal{C}_q$, by interchanging q and p if necessary. This implies that $\mathcal{C}_2$ inverts $\mathcal{C}_p$. Now if $\widehat{S}$ is minimal, then Proposition 3.5 applies. So we may assume $\widehat{S}$ is not minimal. Consider

$$\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q.$$

Choose a 2-element subset $\{a, b\}$ in S that generates $\widehat{G}$. From the minimality of S, we see that

$$\langle a, b \rangle = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q$$

after replacing a and b by conjugates. We may assume $|\overline{a}| \geqslant |\overline{b}|$ and (by conjugating if necessary) a is an element of $\mathcal{C}_2 \times \mathcal{C}_3$. Then the projection of (a, b) to $\mathcal{C}_2 \times \mathcal{C}_3$ has one of the following forms after replacing a and b with their inverses if necessary.

- (a_2a_3, a_2a_3),
- (a_2a_3, a_2),
- (a_2a_3, a_3),
- (a_3, a_2).

So there are four possibilities for (a, b):

1. $(a_2a_3, a_2a_3a_q)$,
2. (a_2a_3, a_2a_q),
3. (a_2a_3, a_3a_q),
4. (a_3, a_2a_q).

Let c be the third element of S. We may write $c = a_2^i a_3^j a_q^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant 2$ and $0 \leqslant k \leqslant q-1$. Note since $S \cap G' = \varnothing$, we know that i and j cannot both be equal to 0. Additionally, we have $a_3\gamma_p a_3^{-1} = \gamma_p^{\widehat{\tau}}$ where $\widehat{\tau}^3 \equiv 1 \pmod p$ and $\widehat{\tau} \not\equiv 1 \pmod p$. Thus $\widehat{\tau}^2 + \widehat{\tau} + 1 \equiv 0 \pmod p$. Note that this implies $\widehat{\tau} \not\equiv -1 \pmod p$. Also we have $a_3a_qa_3^{-1} = a_q^{\check{\tau}}$. By using the same argument we can conclude that $\check{\tau} \not\equiv 1 \pmod q$ and $\check{\tau}^2 + \check{\tau} + 1 \equiv 0 \pmod q$. Note that this implies $\check{\tau} \not\equiv -1 \pmod q$. Therefore, we conclude that $\widehat{\tau}^2 \not\equiv \pm 1 \pmod p$, and $\check{\tau}^2 \not\equiv \pm 1 \pmod q$.

Case 1. Assume $a = a_2a_3$ and $b = a_2a_3a_q$. If $k \neq 0$, then by Lemma 2.28(1), $\langle a, c \rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$. Now if $j \neq 0$, then by Lemma 2.28(4), $\langle b, c \rangle = G$ which contradicts the minimality of S. Therefore, we may assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Thus $\overline{a} = \overline{b} = a_2a_3$ and $\overline{c} = a_2$. Therefore, $|\overline{a}| = |\overline{b}| = 6$ and $|\overline{c}| = 2$. We have $C = (\overline{a}, \overline{b}, \overline{c}, \overline{a}^{-2}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of b in C, and it is the only generator of G that contains a_q, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Also,

$$\begin{aligned}\mathbb{V}(C) &= abca^{-2}c \\ &\equiv a_2a_3 \cdot a_2a_3 \cdot a_2\gamma_p \cdot a_3^{-2} \cdot a_2\gamma_p \pmod{\mathcal{C}_q} \\ &= a_3^2\gamma_p^{-1}a_3^{-2}\gamma_p \\ &= \gamma_p^{-\hat{\tau}^2+1}\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Case 2. Assume $a = a_2a_3$ and $b = a_2a_q$.

Subcase 2.1. Assume $i = 0$. Then $j \neq 0$ and $c = a_3^j a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.28(1), $\langle a, c\rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_3\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Thus, $\overline{a} = a_2a_3$, $\overline{b} = a_2$ and $\overline{c} = a_3$. Therefore, $|\overline{a}| = 6$, $|\overline{b}| = 2$ and $|\overline{c}| = 3$. We have $C = (\overline{a}^2, \overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of b in C, and it is the only generator of G that contains a_q, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Also,

$$\begin{aligned}\mathbb{V}(C) &= a^2bc^{-1}ac \\ &\equiv a_3^2 \cdot a_2 \cdot a_3\gamma_p \cdot a_2a_3 \cdot \gamma_p^{-1}a_3^{-1} \pmod{\mathcal{C}_q} \\ &= \gamma_p^{-1}a_3\gamma_p^{-1}a_3^{-1} \\ &= \gamma_p^{-1-\hat{\tau}}\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Subcase 2.2. Assume $j = 0$. Then $i \neq 0$ and $c = a_2a_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.28(1), $\langle a, c\rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_2a_3$ and $\overline{b} = \overline{c} = a_2$. We have $C = ((\overline{a}, \overline{b})^2, \overline{a}, \overline{c})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Now we calculate its voltage. Also,

$$\begin{aligned}\mathbb{V}(C) &= (ab)^2ac \\ &\equiv (a_2a_3 \cdot a_2a_q)^2 \cdot a_2a_3 \cdot a_2 \pmod{\mathcal{C}_p} \\ &= a_3a_qa_3a_qa_3 \\ &= a_q^{\check{\tau}+\check{\tau}^2}.\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ generates G'. So, Factor Group Lemma 2.6 applies.

Subcase 2.3. Assume $i \neq 0$ and $j \neq 0$. If $k \neq 0$, then $c = a_2 a_3^j a_q^k \gamma_p$. Thus, by Lemma 2.28(1), $\langle a, c \rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_2 a_3 \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Thus, $\overline{a} = \overline{c} = a_2 a_3$ and $\overline{b} = a_2$. Therefore, $|\overline{a}| = |\overline{c}| = 6$ and $|\overline{b}| = 2$. We have $C = (\overline{a}, \overline{c}, \overline{b}, \overline{a}^{-2}, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= acba^{-2}b \\
&\equiv a_2 a_3 \cdot a_2 a_3 \cdot a_2 a_q \cdot a_3^{-2} \cdot a_2 a_q \pmod{\mathcal{C}_p} \\
&= a_3^2 a_q a_3^{-2} a_q \\
&= a_q^{\check{\tau}^2 + 1}.
\end{aligned}$$

Since $\check{\tau}^2 \not\equiv -1 \pmod{q}$, Factor Group Lemma 2.6 applies.

Case 3. Assume $a = a_2 a_3$ and $b = a_3 a_q$.

Subcase 3.1. Assume $i \neq 0$ and $j \neq 0$. If $k = 0$, then $c = a_2 a_3^j \gamma_p$. Thus, by Lemma 2.28(2), $\langle b, c \rangle = G$ which contradicts the minimality of S. So we can assume $k \neq 0$. Then $c = a_2 a_3^j a_q^k \gamma_p$. Thus, by Lemma 2.28(1), $\langle a, c \rangle = G$ which contradicts the minimality of S.

Subcase 3.2. Assume $i = 0$. Then $j \neq 0$ and $c = a_3^j a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.28(1), $\langle a, c \rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_3 \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_2 a_3$, $\overline{b} = \overline{c} = a_3$. Therefore, $|\overline{a}| = 6$ and $|\overline{b}| = |\overline{c}| = 3$. We have $C = (\overline{c}, \overline{b}, \overline{a}, \overline{b}^{-2}, \overline{a}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= cbab^{-2}a^{-1} \\
&\equiv a_3 \cdot a_3 a_q \cdot a_2 a_3 \cdot a_q^{-1} a_3^{-1} a_q^{-1} a_3^{-1} \cdot a_3^{-1} a_2 \pmod{\mathcal{C}_p} \\
&= a_3^2 a_q a_3 a_q^{-1} a_3^{-1} a_q^{-1} a_3^{-2} \\
&= a_q^{\check{\tau}^2 - 1 - \check{\tau}^{-1}} \\
&= a_q^{\check{\tau}^2 - 1 - \check{\tau}^2} \\
&= a_q^{-1}
\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Subcase 3.3. Assume $j = 0$. Then $i \neq 0$ and $c = a_2 a_q^k \gamma_p$. If $k \neq 0$, then by Lemma 2.28(1), $\langle a, c \rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. Then $c = a_2 \gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_2 a_3$, $\overline{b} = a_3$ and $\overline{c} = a_2$. Therefore, $|\overline{a}| = 6$, $|\overline{b}| = 3$ and $|\overline{c}| = 2$. We have $C = (\overline{a}, \overline{c}, \overline{b}, \overline{a}, \overline{b}^{-1}, \overline{a})$

as a Hamiltonian cycle in $\operatorname{Cay}(\overline{G};\overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= acbab^{-1}a\\ &\equiv a_2a_3 \cdot a_2 \cdot a_3a_q \cdot a_2a_3 \cdot a_q^{-1}a_3^{-1} \cdot a_2a_3 \pmod{\mathcal{C}_p}\\ &= a_3^2a_qa_3a_q^{-1}\\ &= a_q^{\check{\tau}^2-1}.\end{aligned}$$

Since $\check{\tau}^2 \not\equiv 1 \pmod{q}$, Factor Group Lemma 2.6 applies.

Case 4. Assume $a = a_3$ and $b = a_2a_q$.

Subcase 4.1. Assume $i = 0$. Then $j \neq 0$ and $c = a_3^ja_q^k\gamma_p$. Thus, the argument in Subcase 1.1 of Proposition 3.6 applies.

Subcase 4.2. Assume $j = 0$. Then $i \neq 0$ and $c = a_2a_q^k\gamma_p$. Thus, the argument in Subcase 1.2 of Proposition 3.6 applies.

Subcase 4.3. Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2a_3^ja_q^k\gamma_p$. If $k \neq 0$, then by Lemma 2.28(3) $\langle a, c\rangle = G$ which contradicts the minimality of S.

So we can assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_2a_3\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = a_3$, $\overline{b} = a_2$ and $\overline{c} = a_2a_3$. This implies that $|\overline{a}| = 3$, $|\overline{b}| = 2$ and $|\overline{c}| = 6$. We have $C = (\overline{c}, \overline{b}, \overline{a}, \overline{c}, \overline{a}^{-1}, \overline{c})$ as a Hamiltonian cycle in $\operatorname{Cay}(\overline{G};\overline{S})$. Since there is one occurrence of b in C, and it is the only generator of G that contains a_q, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Also, since a_2 inverts $\mathcal{C}_p$

$$\begin{aligned}\mathbb{V}(C) &= cbaca^{-1}c\\ &\equiv a_2a_3\gamma_p \cdot a_2 \cdot a_3 \cdot a_2a_3\gamma_p \cdot a_3^{-1} \cdot a_2a_3\gamma_p \pmod{\mathcal{C}_q}\\ &= a_3\gamma_p^{-1}a_3^2\\ &= \gamma_p^{-\hat{\tau}}\end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies. □

3.7 Assume $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$ and $C_{G'}(\mathcal{C}_2) = \{e\}$

In this subsection, we prove the part of Theorem 1.3 where, $|S| = 3$, $G' = \mathcal{C}_p \times \mathcal{C}_q$, $C_{G'}(\mathcal{C}_2) = \{e\}$, and neither $C_{G'}(\mathcal{C}_3) \neq \{e\}$ nor $\widehat{S}$ is minimal holds. Recall $\overline{G} = G/G'$, $\check{G} = G/\mathcal{C}_q$ and $\widehat{G} = G/\mathcal{C}_p$.

Proposition 3.8. *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes (\mathcal{C}_p \times \mathcal{C}_q)$,
- $|S| = 3$,
- $C_{G'}(\mathcal{C}_2) = \{e\}$.

Then $\mathrm{Cay}(G;S)$ *contains a Hamiltonian cycle.*

Proof. Let $S = \{a,b,c\}$. If $C_{G'}(\mathcal{C}_3) \neq \{e\}$, then Proposition 3.4 applies. So we may assume $C_{G'}(\mathcal{C}_3) = \{e\}$. Now if $\widehat{S}$ is minimal, then Proposition 3.5 applies. So we may assume $\widehat{S}$ is not minimal. Consider

$$\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q.$$

Choose a 2-element subset $\{a,b\}$ in S that generates $\widehat{G}$. From the minimality of S, we see

$$\langle a,b\rangle = (\mathcal{C}_2 \times \mathcal{C}_3) \ltimes \mathcal{C}_q.$$

after replacing a and b by conjugates. We may assume $|a| \geqslant |b|$ and (by conjugating if necessary) a is in $\mathcal{C}_2 \times \mathcal{C}_3$. Then the projection of (a,b) to $\mathcal{C}_2 \times \mathcal{C}_3$ is one of the following forms after replacing a and b with their inverses if necessary.

- (a_2a_3, a_2a_3),
- (a_2a_3, a_2),
- (a_2a_3, a_3),
- (a_3, a_2).

There are four possibilities for (a,b):

1. $(a_2a_3, a_2a_3a_q)$,
2. (a_2a_3, a_2a_q),
3. (a_2a_3, a_3a_q),
4. (a_3, a_2a_q).

Let c be the third element of S. We may write $c = a_2^i a_3^j a_q^k \gamma_p$ with $0 \leqslant i \leqslant 1$, $0 \leqslant j \leqslant 2$ and $0 \leqslant k \leqslant q-1$. Note since $S \cap G' = \varnothing$, we know that i and j cannot both be equal to 0. Additionally, we have $a_3\gamma_p a_3^{-1} = \gamma_p^{\hat{\tau}}$ where $\hat{\tau}^3 \equiv 1 \pmod p$ and $\hat{\tau} \not\equiv 1 \pmod p$. Thus $\hat{\tau}^2 + \hat{\tau} + 1 \equiv 0 \pmod p$. Note that this implies $\hat{\tau} \not\equiv -1 \pmod p$. We have $a_3a_qa_3^{-1} = a_q^{\check{\tau}}$. By using the same argument we can conclude that $\check{\tau} \not\equiv 1 \pmod q$ and $\check{\tau}^2 + \check{\tau} + 1 \equiv 0 \pmod q$. Note that this implies $\check{\tau} \not\equiv -1 \pmod q$. Therefore, we conclude that $\hat{\tau}^2 \not\equiv \pm 1 \pmod p$, and $\check{\tau}^2 \not\equiv \pm 1 \pmod q$.

Case 1. Assume $a = a_2a_3$ and $b = a_2a_3a_q$. If $k \neq 0$, then by Lemma 2.28(1) $\langle a,c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$. Now if $j \neq 0$, then by Lemma 2.28(4), $\langle b,c\rangle = G$ which contradicts the minimality of S. Therefore, we may assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. We have $\langle \overline{b},\overline{c}\rangle = \langle \overline{a}_2\overline{a}_3, \overline{a}_2\rangle = \overline{G}$. Consider $\{\breve{b},\breve{c}\} = \{a_2a_3, a_2\gamma_p\}$. Therefore,

$$[a_2a_3, a_2\gamma_p] = a_2a_3a_2\gamma_p a_3^{-1} a_2\gamma_p^{-1} a_2 = a_3\gamma_p a_3^{-1}\gamma_p = \gamma_p^{\hat{\tau}+1}.$$

which generates $\mathcal{C}_p$. Now consider $\{\widehat{b},\widehat{c}\} = \{a_2a_3a_q, a_2\}$, then

$$[a_2a_3a_q, a_2] = a_2a_3a_qa_2a_q^{-1}a_3^{-1}a_2a_2 = a_3a_q^{-2}a_3^{-1} = a_q^{-2\check{\tau}}$$

which generates $\mathcal{C}_q$. Therefore, $\langle b,c\rangle = G$ which contradicts the minimality of S.

Case 2. Assume $a = a_2a_3$ and $b = a_2a_q$. If $k \neq 0$, then by Lemma 2.28(1), $\langle a, c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$.

Subcase 2.1. Assume $j \neq 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_2^i a_3 \gamma_p$. We have $\langle \overline{b}, \overline{c}\rangle = \langle \overline{a}_2, \overline{a}_2^i \overline{a}_3\rangle = \overline{G}$. Consider $\{\widehat{b}, \widehat{c}\} = \{a_2a_q, a_2^i a_3\}$. We have

$$\begin{aligned}[a_2a_q, a_2^i a_3] &= a_2a_qa_2^i a_3 a_q^{-1} a_2 a_3^{-1} a_2^i = a_q^{-1} a_2^{i+1} a_3 a_q^{-1} a_3^{-1} a_2^{i+1} \\ &= a_q^{-1} a_3 a_q^{\mp 1} a_3^{-1} = a_q^{-1 \mp \check{\tau}}\end{aligned}$$

which generates $\mathcal{C}_q$. Now consider $\{\check{b}, \check{c}\} = \{a_2, a_2^i a_3 \gamma_p\}$. We have

$$[a_2, a_2^i a_3 \gamma_p] = a_2 a_2^i a_3 \gamma_p a_2 \gamma_p^{-1} a_3^{-1} a_2^i = a_2^{i+1} a_3 \gamma_p^2 a_3^{-1} a_2^{i+1} = \gamma_p^{\pm 2\hat{\tau}}$$

which generates $\mathcal{C}_p$. Therefore, $\langle b, c\rangle = G$ which contradicts the minimality of S.

Subcase 2.2. Assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_2a_3$ and $\overline{b} = \overline{c} = a_2$. Thus, $|\overline{a}| = 6$ and $|\overline{b}| = |\overline{c}| = 2$. We have $C = ((\overline{a}, \overline{b})^2, \overline{a}, \overline{c})$ as a Hamiltonian cycle in Cay$(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C) &= (ab)^2(ac) \\ &\equiv a_2a_3 \cdot a_2a_q \cdot a_2a_3 \cdot a_2a_q \cdot a_2a_3 \cdot a_2 \pmod{\mathcal{C}_p} \\ &= a_3a_qa_3a_qa_3 \\ &= a_q^{\check{\tau} + \check{\tau}^2}\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Case 3. Assume $a = a_2a_3$ and $b = a_3a_q$. If $k \neq 0$, then by Lemma 2.28(1), $\langle a, c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$.

Subcase 3.1. Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2a_3^j\gamma_p$. Thus, by Lemma 2.28(2), $\langle b, c\rangle = G$ which contradicts the minimality of S.

Subcase 3.2. Assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. We have $\langle \overline{b}, \overline{c}\rangle = \langle \overline{a}_3, \overline{a}_2\rangle = \overline{G}$. Consider $\{\check{b}, \check{c}\} = \{a_3, a_2\gamma_p\}$. Then we have

$$[a_3, a_2\gamma_p] = a_3a_2\gamma_pa_3^{-1}\gamma_p^{-1}a_2 = a_3\gamma_p^{-1}a_3^{-1}\gamma_p = \gamma_p^{-\hat{\tau}+1}$$

which generates $\mathcal{C}_p$. Now consider $\{\widehat{b}, \widehat{c}\} = \{a_3a_q, a_2\}$. Thus,

$$[a_3a_q, a_2] = a_3a_qa_2a_q^{-1}a_3^{-1}a_2 = a_3a_q^2a_3^{-1} = a_q^{2\check{\tau}}$$

which generates $\mathcal{C}_q$. Therefore, $\langle b, c\rangle = G$ which contradicts the minimality of S.

Subcase 3.3. Assume $i = 0$. Then $j \neq 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_3\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then we have $\overline{a} = a_2a_3$, $\overline{b} = \overline{c} = a_3$. Thus, $|\overline{a}| = 6$ and $|\overline{b}| = |\overline{c}| = 3$. We have $C = (\overline{c}, \overline{b}, \overline{a}, \overline{b}^{-2}, \overline{a}^{-1})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C) &= cbab^{-2}a^{-1} \\
&\equiv a_3 \cdot a_3a_q \cdot a_2a_3 \cdot a_q^{-1}a_3^{-1}a_q^{-1}a_3^{-1} \cdot a_3^{-1}a_2 \pmod{\mathcal{C}_p} \\
&= a_3^2a_qa_3a_qa_3^{-1}a_qa_3^{-2} \\
&= a_q^{\check{\tau}^2+1+\check{\tau}^{-1}} \\
&= a_q^{\check{\tau}^2+1-\check{\tau}^2} \\
&= a_q
\end{aligned}$$

which generates $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Case 4. Assume $a = a_3$ and $b = a_2a_q$.

Subcase 4.1. Assume $i = 0$. Then $j \neq 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_3a_q^k\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$. Then we have $\overline{a} = \overline{c} = a_3$ and $\overline{b} = a_2$. This implies that $|\overline{a}| = |\overline{c}| = 3$ and $|\overline{b}| = 2$. We have $C = (\overline{c}^{-2}, \overline{b}, \overline{a}^2, \overline{b})$ as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= c^{-2}ba^2b \\
&\equiv \gamma_p^{-1}a_3^{-1}\gamma_p^{-1}a_3^{-1} \cdot a_2 \cdot a_3^2 \cdot a_2 \pmod{\mathcal{C}_q} \\
&= \gamma_p^{-1}a_3^{-1}\gamma_p^{-1}a_3 \\
&= \gamma_p^{-1-\hat{\tau}^{-1}}
\end{aligned}$$

which generates $\mathcal{C}_p$. Also

$$\begin{aligned}
\mathbb{V}(C) &= c^{-2}ba^2b \\
&\equiv a_q^{-k}a_3^{-1}a_q^{-k}a_3^{-1} \cdot a_2a_q \cdot a_3^2 \cdot a_2a_q \pmod{\mathcal{C}_p} \\
&= a_q^{-k}a_3^{-1}a_q^{-k}a_3^{-1}a_q^{-1}a_3^2a_q \\
&= a_q^{-k-k\check{\tau}^{-1}-\check{\tau}^{-2}+1}.
\end{aligned}$$

If $k = 2$, then

$$a_q^{-k-k\check{\tau}^{-1}-\check{\tau}^{-2}+1} = a_q^{-2-2\check{\tau}^{-1}-\check{\tau}^{-2}+1} = a_q^{-(\check{\tau}^{-1}+1)^2}$$

which generates $\mathcal{C}_q$. So we may assume $k \neq 2$ and the subgroup generated by $\mathbb{V}(C)$ does not contain $\mathcal{C}_q$, for otherwise Factor Group Lemma 2.6 applies. Therefore,

$$\begin{aligned}
0 &\equiv -k - k\check{\tau}^{-1} - \check{\tau}^{-2} + 1 \pmod{q} \\
&= (1-k) - k\check{\tau}^{-1} - \check{\tau}^{-2}.
\end{aligned}$$

Multiplying by $\check{\tau}^2$, we have

$$0 \equiv (1-k)\check{\tau}^2 - k\check{\tau} - 1 \pmod q. \tag{4.1A}$$

We can replace $\check{\tau}$ with $\check{\tau}^{-1}$ in the above equation, by replacing a_3,a and c with their inverses.

$$0 \equiv (1-k)\check{\tau}^{-2} - k\check{\tau}^{-1} - 1 \pmod q.$$

Multiplying by $\check{\tau}^2$, then

$$0 \equiv (1-k) - k\check{\tau} - \check{\tau}^2 \pmod q.$$

By subtracting 4.1A from the above equation, we have

$$0 \equiv (k-2)\check{\tau}^2 + (2-k) \pmod q.$$

This implies that $\check{\tau}^2 \equiv 1 \pmod q$, a contradiction.

Subcase 4.2. Assume $j = 0$. Then $i \neq 0$. If $k \neq 0$, then $c = a_2 a_q^k \gamma_p$. Thus, by Lemma 2.28(3), $\langle a, c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$. Then $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_3$, then $\overline{a} = a_3$ and $\overline{b} = \overline{c} = a_2$. We have $C = (\overline{a}^2, \overline{b}, \overline{a}^{-2}, \overline{c})$ as a Hamiltonian cycle in Cay$(\overline{G}; \overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Similarly, since there is one occurrence of b in C, and it is the only generator of G that contains a_q, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_q$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Subcase 4.3. Assume $i \neq 0$ and $j \neq 0$. If $k \neq 0$, then $c = a_2 a_3^j a_q^k \gamma_p$. Thus, by Lemma 2.28(3), $\langle a, c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$. We may also assume $j = 1$, by replacing c with c^{-1} if necessary. Then $c = a_2 a_3 \gamma_p$. We have $\langle \overline{b}, \overline{c}\rangle = \langle \overline{a}_2, \overline{a}_2\overline{a}_3\rangle = \overline{G}$. Consider $\{\widehat{b}, \widehat{c}\} = \{a_2 a_q, a_2 a_3\}$. Then we have

$$[a_2 a_q, a_2 a_3] = a_2 a_q a_2 a_3 a_q^{-1} a_2 a_3^{-1} a_2 = a_q^{-1} a_3 a_q^{-1} a_3^{-1} = a_q^{-1-\check{\tau}}$$

which generates $\mathcal{C}_q$. Now consider $\{\check{b}, \check{c}\} = \{a_2, a_2 a_3 \gamma_p\}$. Then

$$[a_2, a_2 a_3 \gamma_p] = a_2 a_2 a_3 \gamma_p a_2 \gamma_p^{-1} a_3^{-1} a_2 = a_3 \gamma_p^2 a_3^{-1} = \gamma_p^{2\hat{\tau}}$$

which generates $\mathcal{C}_p$. Therefore, $\langle b, c\rangle = G$ which contradicts the minimality of S. □

3.8 Assume $|S| = 3$ and $G' = \mathcal{C}_3 \times \mathcal{C}_p$

In this subsection, we prove the part of Theorem 1.3 where, $|S| = 3$ and $G' = \mathcal{C}_3 \times \mathcal{C}_p$. Recall $\overline{G} = G/G'$, $\widehat{G} = G/\mathcal{C}_p$ and $\overleftrightarrow{G} = G/\mathcal{C}_3$.

Proposition 3.9. *Assume*

- $G = (\mathcal{C}_2 \times \mathcal{C}_q) \ltimes (\mathcal{C}_3 \times \mathcal{C}_p)$,

- $|S| = 3$.

Then $\mathrm{Cay}(G; S)$ *contains a Hamiltonian cycle.*

Proof. Let $S = \{a, b, c\}$. Since $\mathcal{C}_q$ centralizes $\mathcal{C}_3$ and $Z(G) \cap G' = \{e\}$ (by Proposition 2.15(2)), then $\mathcal{C}_2$ inverts $\mathcal{C}_3$. Now if $\widehat{S}$ is minimal, then Lemma 2.24 applies. So we may assume $\widehat{S}$ is not minimal. Consider

$$\widehat{G} = G/\mathcal{C}_p = (\mathcal{C}_2 \times \mathcal{C}_q) \ltimes \mathcal{C}_3.$$

Choose a 2-element subset $\{a, b\}$ in S that generates $\widehat{G}$. From the minimality of S we see

$$\langle a, b\rangle = (\mathcal{C}_2 \times \mathcal{C}_q) \ltimes \mathcal{C}_3.$$

after replacing a and b with conjugates. Then the projection of (a, b) to $\mathcal{C}_2 \times \mathcal{C}_q$ has one of the following forms:

- $(a_2a_q, a_2a_q^m)$, where $1 \leqslant m \leqslant q-1$,
- (a_2a_q, a_2),
- (a_2a_q, a_q^m), where $1 \leqslant m \leqslant q-1$,
- (a_2, a_q).

Thus, there are four different possibilities for (a, b) after assuming, without loss of generality, that $a \in \mathcal{C}_2 \times \mathcal{C}_q$:

1. $(a_2a_q, a_2a_q^m a_3)$,
2. (a_2a_q, a_2a_3),
3. $(a_2a_q, a_q^m a_3)$,
4. (a_2, a_qa_3).

Let c be the third element of S. We may write $c = a_2^i a_q^j a_3^k \gamma_p$ with $0 \leqslant i \leqslant 1, 0 \leqslant j \leqslant q-1$ and $0 \leqslant k \leqslant 2$. Since $\mathcal{C}_q$ centralizes $\mathcal{C}_3$, we may assume $\mathcal{C}_q$ does not centralize $\mathcal{C}_p$, for otherwise Lemma 2.26 applies. Now we have $a_q\gamma_p a_q^{-1} = \gamma_p^{\widehat{\tau}}$, where $\widehat{\tau}^q \equiv 1 \pmod p$. We also have $\widehat{\tau} \not\equiv 1 \pmod p$. Since $\widehat{\tau}^q \equiv 1 \pmod p$, this implies

$$\widehat{\tau}^{q-1} + \widehat{\tau}^{q-2} + \cdots + 1 \equiv 0 \pmod p.$$

Note that this implies $\widehat{\tau} \not\equiv -1 \pmod p$.

Case 1. Assume $a = a_2a_q$ and $b = a_2a_q^m a_3$. If $k \neq 0$, then by Lemma 2.29(1) $\langle a, c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$. Now if $i \neq 0$, then by Lemma 2.29(3) $\langle b, c\rangle = G$ which contradicts the minimality of S. Therefore, we may assume $i = 0$. Then $j \neq 0$ and $c = a_q^j \gamma_p$.

Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2a_q$, $\overline{b} = a_2a_q^m$ and $\overline{c} = a_q^j$. We may assume m is odd by replacing b with b^{-1} (and m with $q-m$) if necessary. Note that this implies $\overline{b} = \overline{a}^m$. Also, we have $|\overline{a}| = |\overline{b}| = 2q$ and $|\overline{c}| = q$.

Subcase 1.1. Assume $m = 1$. Then $\overline{a} = \overline{b}$. We have

$$C = (\overline{c}^{q-1}, \overline{b}, \overline{c}^{-(q-1)}, \overline{a}^{-1})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of b in C, and it is the only generator of G that contains a_3, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_3$. Now by considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not we have

$$\begin{aligned}
\mathbb{V}(C) &= c^{q-1} b c^{-(q-1)} a^{-1} \\
&\equiv (a_q^j \gamma_p)^{q-1} \cdot a_2 a_q \cdot (a_q^j \gamma_p)^{-(q-1)} \cdot a_q^{-1} a_2 \pmod{\mathcal{C}_3} \\
&= \gamma_p^{\hat{\tau}^j + \hat{\tau}^{2j} + \cdots + \hat{\tau}^{(q-1)j}} a_q^{(q-1)j} a_2 a_q a_q^{-(q-1)j} \gamma_p^{-(\hat{\tau}^j + \hat{\tau}^{2j} + \cdots + \hat{\tau}^{(q-1)j})} a_q^{-1} a_2 \\
&= \gamma_p^{\hat{\tau}^j (1 + \hat{\tau}^j + \cdots + \hat{\tau}^{(q-2)j})} a_q \gamma_p^{\mp \hat{\tau}^j (1 + \hat{\tau}^j + \cdots + \hat{\tau}^{(q-2)j})} a_q^{-1}.
\end{aligned}$$

Now if $\hat{\tau}^j \not\equiv 1 \pmod{p}$, then

$$\begin{aligned}
\mathbb{V}(C) &= \gamma_p^{\hat{\tau}^j (1 + \hat{\tau}^j + \cdots + \hat{\tau}^{(q-2)j})} a_q \gamma_p^{\mp \hat{\tau}^j (1 + \hat{\tau}^j + \cdots + \hat{\tau}^{(q-2)j})} a_q^{-1} \\
&= \gamma_p^{\hat{\tau}^j ((\hat{\tau}^j)^{q-1} - 1)/(\hat{\tau}^j - 1) \mp \hat{\tau}^{j+1} ((\hat{\tau}^j)^{q-1} - 1)/(\hat{\tau}^j - 1)} \\
&= \gamma_p^{\hat{\tau}^j ((\hat{\tau}^{-j}) - 1)/(\hat{\tau}^j - 1) \mp \hat{\tau}^{j+1} ((\hat{\tau}^{-j}) - 1)/(\hat{\tau}^j - 1)} \\
&= \gamma_p^{(1 - \hat{\tau}^j)(1 \mp \hat{\tau})/(\hat{\tau}^j - 1)} \\
&= \gamma_p^{-(1 \mp \hat{\tau})}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.6 applies. Therefore, $\hat{\tau}^j \equiv 1 \pmod{p}$ or $\hat{\tau} \equiv \pm 1 \pmod{p}$. The second case is impossible. So we must have $\hat{\tau}^j \equiv 1 \pmod{p}$. We also know that $\hat{\tau}^q \equiv 1 \pmod{p}$. So $\hat{\tau}^d \equiv 1 \pmod{p}$, where $d = \gcd(j, q)$. Since $1 \leqslant j \leqslant q - 1$, then $d = 1$, which contradicts the fact that $\hat{\tau} \not\equiv 1 \pmod{p}$.

Subcase 1.2. Assume $m \neq 1$ and $j = 2$. Then $c = a_q^2 \gamma_p$. We have

$$C = (\overline{b}, \overline{c}^{-(m-1)/2}, \overline{a}, \overline{c}^{(m-1)/2}, \overline{a}^{2q-m-1})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of b in C, and it is the only generator of G that contains a_3, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_3$. Considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not we have

$$\begin{aligned}
\mathbb{V}(C) &= b c^{-(m-1)/2} a c^{(m-1)/2} a^{2q-m-1} \\
&\equiv a_2 a_q^m \cdot (a_q^2 \gamma_p)^{-(m-1)/2} \cdot a_2 a_q \cdot (a_q^2 \gamma_p)^{(m-1)/2} \cdot a_q^{2q-m-1} \pmod{\mathcal{C}_3} \\
&= a_2 a_q^m (\gamma_p^{\hat{\tau}^2 + (\hat{\tau}^2)^2 + \cdots + (\hat{\tau}^2)^{(m-1)/2}} a_q^{(m-1)})^{-1} a_2 a_q \\
&\qquad \cdot (\gamma_p^{\hat{\tau}^2 + (\hat{\tau}^2)^2 + \cdots + (\hat{\tau}^2)^{(m-1)/2}} a_q^{(m-1)}) a_q^{-m-1} \\
&= a_2 a_q^m a_q^{-m+1} \gamma_p^{-\hat{\tau}^2 (1 + \hat{\tau}^2 + \cdots + (\hat{\tau}^2)^{(m-3)/2})} a_2 a_q \gamma_p^{\hat{\tau}^2 (1 + \hat{\tau}^2 + \cdots + (\hat{\tau}^2)^{(m-3)/2})} a_q^{-2} \\
&= a_q \gamma_p^{\pm \hat{\tau}^2 (1 + \hat{\tau}^2 + \cdots + \hat{\tau}^2)^{(m-3)/2}} a_q \gamma_p^{\hat{\tau}^2 (1 + \hat{\tau}^2 + \cdots + \hat{\tau}^2)^{(m-3)/2}} a_q^{-2}
\end{aligned}$$

$$= \gamma_p^{\pm\hat{\tau}^3(\hat{\tau}^{m-1}-1)/(\hat{\tau}^2-1)+\hat{\tau}^4(\hat{\tau}^{m-1}-1)/(\hat{\tau}^2-1)}$$
$$= \gamma_p^{\hat{\tau}^3(\hat{\tau}^{m-1}-1)(\pm 1+\hat{\tau})/(\hat{\tau}^2-1)}.$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.6 applies. Therefore, $\hat{\tau}^{m-1} \equiv 1 \pmod p$. We also know that $\hat{\tau}^q \equiv 1 \pmod p$. So $\hat{\tau}^d \equiv 1 \pmod p$, where $d = \gcd(m-1, q)$. Since $2 \leqslant m \leqslant q-1$, then $d = 1$, which contradicts the fact that $\hat{\tau} \not\equiv 1 \pmod p$.

Subcase 1.3. Assume $m \neq 1$ and $j \neq 2$. We may also assume j is an even number, by replacing c with its inverse and j with $q-j$ if necessary. This implies that $\overline{c} = \overline{a}^j$. We have

$$C = (\overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1}, \overline{b}^{-1}, \overline{a}^{m-2}, \overline{c}, \overline{a}^{-(j-3)}, \overline{c}, \overline{a}^{2q-m-j-2})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2q-m-j-2} \\
&\equiv a_2a_3 \cdot a_2 \cdot a_3^{-1}a_2 \cdot a_2^{m-2} \cdot a_2^{-(j-3)} \cdot a_2^{2q-m-j-2} \quad (\mathrm{mod}\ \mathcal{C}_q \ltimes \mathcal{C}_p) \\
&= a_2a_3a_2a_3^{-1} \\
&= a_3^{-2}
\end{aligned}$$

which generates $\mathcal{C}_3$. Also considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not we have

$$\begin{aligned}
\mathbb{V}(C) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2q-m-j-2} \\
&\equiv a_2a_q^m \cdot a_q^j\gamma_p \cdot a_2a_q \cdot \gamma_p^{-1}a_q^{-j} \cdot a_q^{-m}a_2 \\
&\qquad \cdot a_2a_q^{m-2} \cdot a_q^j\gamma_p \cdot a_q^{-j+3}a_2 \cdot a_q^j\gamma_p \cdot a_2a_q^{2q-m-j-2} \quad (\mathrm{mod}\ \mathcal{C}_3) \\
&= a_q^{m+j}\gamma_p^{\pm 1}a_q\gamma_p^{-1}a_q^{-2}\gamma_pa_q^3\gamma_p^{\pm 1}a_q^{-m-j-2} \\
&= \gamma_p^{\pm\hat{\tau}^{m+j}-\hat{\tau}^{m+j+1}+\hat{\tau}^{m+j-1}\pm\hat{\tau}^{m+j+2}} \\
&= \gamma_p^{\hat{\tau}^{m+j-1}(\pm\hat{\tau}^3-\hat{\tau}^2\pm\hat{\tau}+1)}.
\end{aligned}$$

So we may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.6 applies. Then we have

$$0 \equiv \pm\hat{\tau}^3 - \hat{\tau}^2 \pm \hat{\tau} + 1 \pmod p.$$

Let $t = \hat{\tau}$ if $\mathcal{C}_2$ centralizes $\mathcal{C}_p$ and $t = -\hat{\tau}$ if $\mathcal{C}_2$ inverts $\mathcal{C}_p$. Then

$$0 \equiv t^3 - t^2 + t + 1 \pmod p. \tag{1.3A}$$

We can replace t with t^{-1} in the above equation after replacing $\{a, b, c\}$ with their inverses, then

$$0 \equiv t^{-3} - t^{-2} + t^{-1} + 1 \pmod p.$$

Multiplying by t^3, we have

$$0 \equiv 1 - t + t^2 + t^3 \pmod p$$

$$= t^3 + t^2 - t + 1.$$

By subtracting 1.3A from the above equation, we have

$$\begin{aligned} 0 &\equiv 2t^2 - 2t \pmod{p} \\ &= 2t(t-1) \end{aligned}$$

This implies that $t \equiv 1 \pmod{p}$ which contradicts the fact that $\hat{\tau} \not\equiv \pm 1 \pmod{p}$.

Case 2. Assume $a = a_2 a_q$ and $b = a_2 a_3$. If $k \neq 0$, then by Lemma 2.29(1) $\langle a, c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$.

Subcase 2.1. Assume $i = 0$. Then $j \neq 0$ and $c = a_q^j \gamma_p$. We may assume j is an odd number, by replacing c with its inverse and j with $q-j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2 a_q$, $\overline{b} = a_2$ and $\overline{c} = a_q^j$. Also, we have $|\overline{a}| = 2q$, $|\overline{b}| = 2$ and $|\overline{c}| = q$. Now if $j \neq 1$, then we have

$$C = (\overline{c}, \overline{a}^{-1}, \overline{b}, \overline{a}^2, \overline{b}, \overline{c}^{-1}, \overline{a}^{j-3}, \overline{b}, \overline{a}^{-(q-4)}, \overline{b}, \overline{a}^{q-j-2})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate the voltage of C.

$$\begin{aligned} \mathbb{V}(C) &= ca^{-1}ba^2bc^{-1}a^{j-3}ba^{-(q-4)}ba^{q-j-2} \\ &\equiv a_2 \cdot a_2a_3 \cdot a_2^2 \cdot a_2a_3 \cdot a_2^{j-3} \cdot a_2a_3 \cdot a_2^{-(q-4)} \cdot a_2a_3 \cdot a_2^{q-j-2} \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\ &= a_3a_2a_3a_2a_3a_2a_2a_3 \\ &= a_3^2 \end{aligned}$$

which generates $\mathcal{C}_3$. By considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not, we have

$$\begin{aligned} \mathbb{V}(C) &= ca^{-1}ba^2bc^{-1}a^{j-3}ba^{-(q-4)}ba^{q-j-2} \\ &\equiv a_q^j\gamma_p \cdot a_q^{-1}a_2 \cdot a_2 \cdot a_q^2 \cdot a_2 \cdot \gamma_p^{-1}a_q^{-j} \cdot a_q^{j-3} \cdot a_2 \cdot a_2a_q^{-q+4} \cdot a_2 \cdot a_q^{q-j-2} \pmod{\mathcal{C}_3} \\ &= a_q^j\gamma_p a_q \gamma_p^{\mp 1} a_q^{-j-1} \\ &= \gamma_p^{\hat{\tau}^j \mp \hat{\tau}^{j+1}} \\ &= \gamma_p^{\hat{\tau}^j(1 \mp \hat{\tau})} \end{aligned}$$

which generates $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. Thus, Factor Group Lemma 2.6 applies.

So we may assume $j = 1$, then $c = a_q\gamma_p$ and $\overline{c} = a_q$. We have

$$C_1 = ((\overline{b}, \overline{c})^{q-1}, \overline{b}, \overline{a})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned} \mathbb{V}(C_1) &= (bc)^{q-1}ba \\ &\equiv (a_2a_3)^{q-1} \cdot a_2a_3 \cdot a_2 \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\ &= a_3^{-1} \end{aligned}$$

which generates $\mathcal{C}_3$. If $\mathcal{C}_2$ centralizes $\mathcal{C}_p$, then

$$\begin{aligned}\mathbb{V}(C_1) &= (bc)^{q-1}ba\\ &\equiv (a_2 \cdot a_q\gamma_p)^{q-1} \cdot a_2 \cdot a_2a_q \pmod{\mathcal{C}_3}\\ &= (a_q\gamma_p)^{q-1}a_q\\ &= \gamma_p^{\hat{\tau}+\hat{\tau}^2+\cdots+\hat{\tau}^{q-1}}\\ &= \gamma_p^{-1}\end{aligned}$$

which generates $\mathcal{C}_p$. So in this case, the subgroup generated by $\mathbb{V}(C_1)$ is G'. Thus, Factor Group Lemma 2.6 applies.

Now if $\mathcal{C}_2$ inverts $\mathcal{C}_p$, then

$$\begin{aligned}\mathbb{V}(C_1) &= (bc)^{q-1}ba\\ &\equiv (a_2 \cdot a_q\gamma_p)^{q-1} \cdot a_2 \cdot a_2a_q \pmod{\mathcal{C}_3}\\ &= \gamma_p^{-\hat{\tau}+\hat{\tau}^2-\cdots-\hat{\tau}^{q-2}+\hat{\tau}^{q-1}}.\end{aligned}$$

Since $\hat{\tau} \not\equiv -1 \pmod{p}$, then

$$\begin{aligned}\mathbb{V}(C_1) &= \gamma_p^{-\hat{\tau}+\hat{\tau}^2-\cdots-\hat{\tau}^{q-2}+\hat{\tau}^{q-1}}\\ &= \gamma_p^{(\hat{\tau}^q+1)/(\hat{\tau}+1)-1}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.6 applies. Therefore, since $\hat{\tau}^q \equiv 1 \pmod{p}$, then

$$\begin{aligned}0 &\equiv (\hat{\tau}^q + 1)/(\hat{\tau} + 1) - 1 \pmod{p}\\ &= 2/(\hat{\tau} + 1) - 1.\end{aligned}$$

This implies that $\hat{\tau} \equiv 1 \pmod{p}$, which is impossible.

Subcase 2.2. Assume $j = 0$. Then $i \neq 0$ and $c = a_2\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2a_q$ and $\overline{b} = \overline{c} = a_2$. This implies that $|\overline{a}| = 2q$ and $|\overline{b}| = |\overline{c}| = 2$. We have

$$C = (\overline{c}, \overline{a}^{q-1}, \overline{b}, \overline{a}^{-(q-1)})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Since there is one occurrence of b in C, and it is the only generator of G that contains a_3, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_3$. Similarly, since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C)$ contains $\mathcal{C}_p$. Therefore, the subgroup generated by $\mathbb{V}(C)$ is G'. So, Factor Group Lemma 2.6 applies.

Subcase 2.3. Assume $i \neq 0$ and $j \neq 0$. Then $c = a_2a_q^j\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2a_q$, $\overline{b} = a_2$ and $\overline{c} = a_2a_q^j$. This implies that $|\overline{a}| = |\overline{c}| = 2q$ and $|\overline{b}| = 2$. We may assume j is even by replacing c with its inverse and j with $q - j$ if necessary.

Suppose, for the moment, that $j = q - 1$, then $c = a_2a_q^{-1}\gamma_p$ and $\overline{c} = \overline{a}^{-1}$. We have

$$C_1 = (\overline{c}, \overline{b}, (\overline{a}^{-1}, \overline{b})^{q-1})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G};\overline{S})$. Since there is one occurrence of c in C, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C_1) &= cb(a^{-1}b)^{q-1}\\ &\equiv a_2 \cdot a_2a_3 \cdot (a_2 \cdot a_2a_3)^{q-1} \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p}\\ &= a_3^q\end{aligned}$$

which generates $\mathcal{C}_3$. Therefore, the subgroup generated by $\mathbb{V}(C_1)$ contains G'. Thus, Factor Group Lemma 2.6 applies.

So we may assume $j \neq q-1$. Then we have

$$C_2 = (\overline{c}, \overline{a}^{q-j-1}, \overline{b}, \overline{a}^{-q+j+1}, (\overline{a}^{-1}, \overline{b})^j)$$

and

$$C_3 = (\overline{c}, \overline{a}^{q-j-2}, \overline{b}, \overline{a}^{-q+j+2}, (\overline{a}^{-1}, \overline{b})^{j-1}, \overline{a}^{-2}, \overline{b}, \overline{a})$$

as Hamiltonian cycles in $\mathrm{Cay}(\overline{G};\overline{S})$. Since there is one occurrence of c in C_2, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C_2) &= ca^{q-j-1}ba^{-q+j+1}(a^{-1}b)^j\\ &\equiv a_2 \cdot a_2^{q-j-1} \cdot a_2a_3 \cdot a_2^{-q+j+1} \cdot a_3^j \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p}\\ &= a_3^{j+1}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_3$, for otherwise Factor Group Lemma 2.6 applies. Then $j \equiv -1 \pmod 3$.

Since there is one occurrence of c in C_3, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C_3)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C_3) &= ca^{q-j-2}ba^{-q+j+2}(a^{-1}b)^{j-1}a^{-2}ba\\ &\equiv a_2 \cdot a_2^{q-j-2} \cdot a_2a_3 \cdot a_2^{-q+j+2} \cdot a_3^{j-1} \cdot a_2^{-2} \cdot a_2a_3 \cdot a_2 \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p}\\ &= a_2a_3a_2a_3^{j-1}a_2a_3a_2\\ &= a_3^{j-3}\\ &= a_3^j\end{aligned}$$

Since $j \equiv -1 \pmod 3$, this generates $\mathcal{C}_3$. So, Factor Group Lemma 2.6 applies.

Case 3. Assume $a = a_2a_q$ and $b = a_q^m a_3$. If $k \neq 0$, then by Lemma 2.29(1) $\langle a, c\rangle = G$ which contradicts the minimality of S. So we can assume $k = 0$. Now if $i \neq 0$, then by Lemma 2.29(3) $\langle b, c\rangle = G$ which contradicts the minimality of S. Therefore, we may assume $i = 0$. Then $j \neq 0$ and $c = a_q^j\gamma_p$. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2a_q$, $\overline{b} = a_q^m$ and $\overline{c} = a_q^j$.

Suppose, for the moment, that $m = j$. Then $\overline{b} = \overline{c}$. We have

$$C_1 = (\overline{c}^{-1}, \overline{b}^{-(q-2)}, \overline{a}^{-1}, \overline{b}^{q-1}, \overline{a})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G};\overline{S})$. Since there is one occurrence of c in C_1, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C_1)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}\mathbb{V}(C_1) &= c^{-1}b^{-(q-2)}a^{-1}b^{q-1}a \\ &\equiv a_3^{-(q-2)}\cdot a_2\cdot a_3^{q-1}\cdot a_2 \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\ &= a_3^{-2q+3} \\ &= a_3^{-2q}\end{aligned}$$

which generates $\mathcal{C}_3$, because $\gcd(2q,3)=1$. So, the subgroup generated by $\mathbb{V}(C_1)$ is G'. Therefore, Factor Group Lemma 2.6 applies.

So we may assume $m \neq j$. We may also assume m and j are even, by replacing $\{b,c\}$ with their inverses, m with $q-m$, and j with $q-j$ if necessary. Now suppose, for the moment, $j=2$. Then we have $c=a_q^2\gamma_p$. We also have

$$C_2 = (\overline{b}, \overline{c}^{-(m-2)/2}, \overline{a}^{-1}, \overline{c}^{m/2}, \overline{a}^{2q-m-1})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G};\overline{S})$. Since there is one occurrence of b in C_2, and it is the only generator of G that contains a_3, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_3$. Now by considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not, we have

$$\begin{aligned}\mathbb{V}(C_2) &= bc^{-(m-2)/2}a^{-1}c^{m/2}a^{2q-m-1} \\ &\equiv a_q^m\cdot(a_q^2\gamma_p)^{-(m-2)/2}\cdot a_q^{-1}a_2\cdot(a_q^2\gamma_p)^{m/2}\cdot a_2^{2q-m-1}a_q^{2q-m-1} \pmod{\mathcal{C}_3} \\ &= a_q^m(\gamma_p^{\hat{\tau}^2+(\hat{\tau}^2)^2+\cdots+(\hat{\tau}^2)^{(m-2)/2}}a_q^{(m-2)})^{-1}a_q^{-1}a_2 \\ &\qquad\cdot(\gamma_p^{\hat{\tau}^2+(\hat{\tau}^2)^2+\cdots+(\hat{\tau}^2)^{m/2}}a_q^m)a_2a_q^{-m-1} \\ &= a_q^m a_q^{-(m-2)}\gamma_p^{-\hat{\tau}^2(1+\hat{\tau}^2+\cdots+(\hat{\tau}^2)^{(m-4)/2})} \\ &\qquad\cdot a_q^{-1}\gamma_p^{\pm\hat{\tau}^2(1+\hat{\tau}^2+\cdots+(\hat{\tau}^2)^{(m-2)/2})}a_q^m a_q^{-m-1}.\end{aligned}$$

Since $\hat{\tau}^2-1 \not\equiv 0 \pmod p$, then

$$\begin{aligned}\mathbb{V}(C_2) &= a_q^2\gamma_p^{-\hat{\tau}^2(\hat{\tau}^{m-2}-1)/(\hat{\tau}^2-1)}a_q^{-1}\gamma_p^{\pm\hat{\tau}^2(\hat{\tau}^m-1)/(\hat{\tau}^2-1)}a_q^{-1} \\ &= \gamma_p^{-\hat{\tau}^4(\hat{\tau}^{m-2}-1)/(\hat{\tau}^2-1)\pm\hat{\tau}^3(\hat{\tau}^m-1)/(\hat{\tau}^2-1)} \\ &= \gamma_p^{\hat{\tau}^3(1\mp\hat{\tau})(-\hat{\tau}^{m-1}\mp1)/(\hat{\tau}^2-1)}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.6 applies. Therefore, $\hat{\tau}\equiv\pm1 \pmod p$ or $\hat{\tau}^{m-1}\equiv\pm1 \pmod p$. The first case is impossible. So we may assume $\hat{\tau}^{m-1}\equiv\pm1 \pmod p$. Thus, $\hat{\tau}^{2(m-1)}\equiv 1 \pmod p$. We also know that $\hat{\tau}^q\equiv 1 \pmod p$. So we have $\hat{\tau}^d\equiv 1 \pmod p$, where $d=\gcd(2(m-1),q)$. Since $\gcd(2,q)=1$ and $2\leqslant m\leqslant q-1$, then $d=1$, which contradicts the fact that $\hat{\tau}\not\equiv 1 \pmod p$.

So we may assume $j \neq 2$. We have

$$C_3 = (\overline{b}, \overline{c}, \overline{a}, \overline{c}^{-1}, \overline{b}^{-1}, \overline{a}^{m-2}, \overline{c}, \overline{a}^{-(j-3)}, \overline{c}, \overline{a}^{2q-m-j-2})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G};\overline{S})$. Now we calculate its voltage.

$$\begin{aligned}\mathbb{V}(C_3) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2q-m-j-2}\\ &\equiv a_3\cdot a_2\cdot a_3^{-1}\cdot a_2^{m-2}\cdot a_2^{-j+3}\cdot a_2^{2q-m-j-2} \pmod{\mathcal{C}_q\ltimes\mathcal{C}_p}\\ &= a_3^2\end{aligned}$$

which generates $\mathcal{C}_3$. Also, by considering the fact that $\mathcal{C}_2$ might centralize $\mathcal{C}_p$ or not, we have

$$\begin{aligned}\mathbb{V}(C_3) &= bcac^{-1}b^{-1}a^{m-2}ca^{-(j-3)}ca^{2q-m-j-2}\\ &\equiv a_q^m\cdot a_q^j\gamma_p\cdot a_2a_q\cdot\gamma_p^{-1}a_q^{-j}\cdot a_q^{-m}\cdot a_2^{m-2}a_q^{m-2}\\ &\qquad\cdot a_q^j\gamma_p\cdot a_q^{-j+3}a_2^{-j+3}\cdot a_q^j\gamma_p\cdot a_2^{2q-m-j-2}a_q^{2q-m-j-2} \pmod{\mathcal{C}_3}\\ &= a_q^{m+j}\gamma_p a_2 a_q\gamma_p^{-1}a_q^{-2}\gamma_p a_q^3 a_2\gamma_p a_q^{-m-j-2}\\ &= a_q^{m+j}\gamma_p a_q\gamma_p^{\mp1}a_q^{-2}\gamma_p^{\pm1}a_q^3\gamma_p a_q^{-m-j-2}\\ &= \gamma_p^{\hat{\tau}^{m+j}\mp\hat{\tau}^{m+j+1}\pm\hat{\tau}^{m+j-1}+\hat{\tau}^{m+j+2}}\\ &= \gamma_p^{\hat{\tau}^{m+j-1}(\hat{\tau}^3\mp\hat{\tau}^2+\hat{\tau}\pm1)}.\end{aligned}$$

We may assume this does not generate $\mathcal{C}_p$, for otherwise Factor Group Lemma 2.6 applies. Therefore,

$$0\equiv\hat{\tau}^3\mp\hat{\tau}^2+\hat{\tau}\pm1 \pmod{p}.$$

If $\mathcal{C}_2$ centralizes $\mathcal{C}_p$, then

$$0\equiv\hat{\tau}^3-\hat{\tau}^2+\hat{\tau}+1 \pmod{p}. \tag{3A}$$

We can replace $\hat{\tau}$ with $\hat{\tau}^{-1}$ in the above equation after replacing $\{a,b,c\}$ with their inverses in the Hamiltonian cycle, then

$$0\equiv\hat{\tau}^{-3}-\hat{\tau}^{-2}+\hat{\tau}^{-1}+1 \pmod{p}.$$

Multiplying by $\hat{\tau}^3$, we have

$$\begin{aligned}0&\equiv 1-\hat{\tau}+\hat{\tau}^2+\hat{\tau}^3 \pmod{p}\\ &=\hat{\tau}^3+\hat{\tau}^2-\hat{\tau}+1.\end{aligned}$$

Subtracting 3A from the above equation we have

$$\begin{aligned}0&\equiv 2\hat{\tau}^2-2\hat{\tau} \pmod{p}\\ &=2\hat{\tau}(\hat{\tau}-1)\end{aligned}$$

which is impossible, because $\hat{\tau}\not\equiv 1 \pmod{p}$.

Now if $\mathcal{C}_2$ inverts $\mathcal{C}_p$, then

$$0\equiv\hat{\tau}^3+\hat{\tau}^2+\hat{\tau}-1 \pmod{p}. \tag{3B}$$

We can replace $\widehat{\tau}$ with $\widehat{\tau}^{-1}$ in the above equation after replacing $\{a, b, c\}$ with their inverses. Then

$$0 \equiv \widehat{\tau}^{-3} + \widehat{\tau}^{-2} + \widehat{\tau}^{-1} - 1 \pmod{p}.$$

Multiplying by $\widehat{\tau}^3$, then

$$\begin{aligned} 0 &\equiv 1 + \widehat{\tau} + \widehat{\tau}^2 - \widehat{\tau}^3 \pmod{p} \\ &= -\widehat{\tau}^3 + \widehat{\tau}^2 + \widehat{\tau} + 1. \end{aligned}$$

By adding 3B and the above equation, we have

$$\begin{aligned} 0 &\equiv 2(\widehat{\tau}^2 + \widehat{\tau}) \pmod{p} \\ &= 2\widehat{\tau}(\widehat{\tau} + 1) \end{aligned}$$

which is also impossible, because $\widehat{\tau} \not\equiv -1 \pmod{p}$.

Case 4. Assume $a = a_2$ and $b = a_q a_3$.

Subcase 4.1. Assume $i \neq 0$. Then $c = a_2 a_q^j a_3^k \gamma_p$. By Lemma 2.29(2) $\langle b, c\rangle = G$ which contradicts the minimality of S.

Subcase 4.2. Assume $i = 0$. Then $j \neq 0$ and $c = a_q^j a_3^k \gamma_p$. We may assume j is even by replacing c with its inverse and j with $q - j$ if necessary. Consider $\overline{G} = \mathcal{C}_2 \times \mathcal{C}_q$. Then we have $\overline{a} = a_2$, $\overline{b} = a_q$ and $\overline{c} = a_q^j$. This implies that $|\overline{a}| = 2$ and $|\overline{b}| = |\overline{c}| = q$. We have

$$C_1 = (\overline{c}, \overline{b}^{q-j-1}, \overline{c}, \overline{b}^{-(j-2)}, \overline{a}, \overline{b}^{q-1}, \overline{a})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. Now we calculate its voltage.

$$\begin{aligned} \mathbb{V}(C_1) &= cb^{q-j-1}cb^{-(j-2)}ab^{q-1}a \\ &\equiv a_q^j\gamma_p \cdot a_q^{q-j-1} \cdot a_q^j\gamma_p \cdot a_q^{-j+2} \cdot a_2 \cdot a_q^{q-1} \cdot a_2 \pmod{\mathcal{C}_3} \\ &= a_q^j\gamma_p a_q^{-1}\gamma_p a_q^{-j+1} \\ &= \gamma_p^{\widehat{\tau}^{j-1}(\widehat{\tau}+1)} \end{aligned}$$

which generates $\mathcal{C}_p$. Also

$$\begin{aligned} \mathbb{V}(C_1) &= cb^{q-j-1}cb^{-(j-2)}ab^{q-1}a \\ &\equiv a_3^k \cdot a_3^{q-j-1} \cdot a_3^k \cdot a_3^{-j+2} \cdot a_2 \cdot a_3^{q-1} \cdot a_2 \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\ &= a_3^{k+q-j-1+k-j+2-q+1} \\ &= a_3^{2(k-j+1)}. \end{aligned}$$

We may assume this does not generate $\mathcal{C}_3$, for otherwise Factor Group Lemma 2.6 applies. Then

$$0 \equiv k - j + 1 \pmod{3}. \tag{4.2A}$$

We also have

$$C_2 = (\overline{c}, \overline{a}, (\overline{b}, \overline{a})^{q-j-1}, \overline{b}^j, \overline{a}, \overline{b}^{-(j-1)})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. We calculate its voltage. Since there is one occurrence of c in C_2, and it is the only generator of G that contains γ_p, then by Lemma 2.8 we conclude that the subgroup generated by $\mathbb{V}(C_2)$ contains $\mathcal{C}_p$. Also,

$$\begin{aligned}
\mathbb{V}(C_2) &= ca(ba)^{q-j-1}b^j ab^{-(j-1)} \\
&\equiv a_3^k \cdot a_2 \cdot (a_3 a_2)^{q-j-1} \cdot a_3^j \cdot a_2 \cdot a_3^{-j+1} \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_3^{k-2j+1}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_3$, for otherwise Factor Group Lemma 2.6 applies. Therefore,

$$0 \equiv k - 2j + 1 \pmod{3}.$$

By subtracting the above equation from 4.2A we have $j \equiv 0 \pmod{3}$.

Now we have

$$C_3 = (\overline{c}, \overline{a}, \overline{b}^{q-j-1}, \overline{a}, \overline{b}^{-(q-j-2)}, \overline{c}^{-1}, \overline{b}^{j-2}, \overline{a}, \overline{b}^{-(j-1)}, \overline{a})$$

as a Hamiltonian cycle in $\mathrm{Cay}(\overline{G}; \overline{S})$. We calculate its voltage.

$$\begin{aligned}
\mathbb{V}(C_3) &= cab^{q-j-1}ab^{-(q-j-2)}c^{-1}b^{j-2}ab^{-(j-1)}a \\
&\equiv a_q^j \gamma_p \cdot a_2 \cdot a_q^{q-j-1} \cdot a_2 \cdot a_q^{-q+j+2} \cdot \gamma_p^{-1} a_q^{-j} \cdot a_q^{j-2} \cdot a_2 \cdot a_q^{-j+1} \cdot a_2 \pmod{\mathcal{C}_3} \\
&= a_q^j \gamma_p a_q \gamma_p^{-1} a_q^{-j-1} \\
&= \gamma_p^{\hat{\tau}^j (1-\hat{\tau})}.
\end{aligned}$$

which generates $\mathcal{C}_p$. Also

$$\begin{aligned}
\mathbb{V}(C_3) &= cab^{q-j-1}ab^{-(q-j-2)}c^{-1}b^{j-2}ab^{-(j-1)}a \\
&\equiv a_3^k \cdot a_2 \cdot a_3^{q-j-1} \cdot a_2 \cdot a_3^{-q+j+2} \cdot a_3^{-k} \cdot a_3^{j-2} \cdot a_2 \cdot a_3^{-j+1} \cdot a_2 \pmod{\mathcal{C}_q \ltimes \mathcal{C}_p} \\
&= a_3^{k-q+j+1-q+j+2-k+j-2+j-1} \\
&= a_3^{-2q+4j}.
\end{aligned}$$

We may assume this does not generate $\mathcal{C}_3$, for otherwise Factor Group Lemma 2.6 applies. Then

$$\begin{aligned}
0 &\equiv -2q + 4j \pmod{3} \\
&= q + j
\end{aligned}$$

We already know $j \equiv 0 \pmod{3}$. By substituting this in the above equation, we have $q \equiv 0 \pmod{3}$ which contradicts the fact that $\gcd(q, 3) = 1$. □

3.9 Assume $|S| \geqslant 4$

In this subsection, we prove the following general result that includes the part of Theorem 1.3, where $|S| \geqslant 4$ (see Assumption 3.1). Unlike in the other subsections of this section, we do not assume $|G| = 6pq$.

Proposition 3.10. *Assume $|G|$ is a product of four distinct primes and S is a minimal generating set of G, where $|S| \geqslant 4$. Then $\mathrm{Cay}(G; S)$ contains a Hamiltonian cycle.*

Proof. Suppose $S = \{s_1, s_2, ..., s_k\}$ and let $G_i = \langle s_1, s_2, ..., s_i\rangle$ for $i = 1, 2, ..., k$. Since S is minimal, we know $\{e\} \subset G_1 \subset G_2 \subset ...G_k = G$. Therefore, the number of prime factors of $|G_i|$ is at least i. Since $|G| = p_1p_2p_3q$ is the product of only 4 primes, and $k = |S| \geqslant 4$, we can conclude that $|G_i|$ has exactly i prime factors, for all i. This implies that $|S| = 4$. This also implies every element of S has prime order.

Since $|G|$ is square-free, we know that G' is cyclic (see Proposition 2.15(1)), so $G' \neq G$. We may assume $|G'| \neq 1$, for otherwise G is abelian, so Lemma 2.2 applies. Also, if $|G'|$ is equal to a prime number, then Theorem 2.3 applies. So we may assume $|G'|$ has at least two prime factors. Therefore, the number of prime factors of $|G'|$ is either 2 or 3.

Case 1. Assume $|G'|$ has only two prime factors. This implies $|\overline{G}| = p_1p_2$, where p_1 and p_2 are two distinct primes. Suppose $s \in S$, then $\overline{s} \in \overline{S}$. We know that $|\overline{s}| \neq 1$ (see Assumption 3.1(6)). Now since every element of S has prime order, then $|s|$ is either p_1 or p_2. Also, every element of order p_1 must commute with every element of order p_2, because the subgroup H generated by any element of S that has order p_1, together with any element of S that has order p_2 has exactly two prime factors, so $|H| = p_1p_2$, $H' \subseteq G'$, and $|G'| = p_3p_4$. Thus, $|H'| = 1$. Let S_{p_1} be the elements of order p_1 in S, and let S_{p_2} be the elements of order p_2. Also let H_{p_1} and H_{p_2} be the subgroups generated by S_{p_1} and S_{p_2}, respectively. This implies that $\mathrm{Cay}(G; S) \cong \mathrm{Cay}(G_{p_1}; S_{p_1}) \,\square\, \mathrm{Cay}(G_{p_2}; S_{p_2})$. Therefore, $\mathrm{Cay}(G; S)$ contains a Hamiltonian cycle (see Corollary 2.11).

Case 2. Assume $|G'|$ has three prime factors. We may write (see Proposition 2.15(3))

$$G = \mathcal{C}_q \ltimes G' = \mathcal{C}_q \ltimes (\mathcal{C}_{p_1} \times \mathcal{C}_{p_2} \times \mathcal{C}_{p_3}),$$

where p_1, p_2, p_3 and q are distinct primes. Note that $G' \cap Z(G) = \{e\}$ (see Proposition 2.15(2)). Now we may assume $\langle s_4\rangle = \mathcal{C}_q$. Since $|\langle s_i, s_4\rangle|$ has only two prime factors (for $1 \leqslant i \leqslant 3$), we must have $s_i = s_4^{k_i}a_{p_i}$ (after permuting p_1, p_2, p_3), where a_{p_i} is a generator of $\mathcal{C}_{p_i}$. We may also assume $S \cap G' = \varnothing$ (see Lemma 2.12), so $k_i \not\equiv 0 \pmod q$. Now consider

$$G_2 = \langle s_1, s_2\rangle = \langle s_4^{k_1}a_{p_1}, s_4^{k_2}a_{p_2}\rangle.$$

Since $\mathcal{C}_{p_1}$ is a normal subgroup in G, we can consider $\overline{G}_2 = G_2/\mathcal{C}_{p_1}$, then $\{\overline{s}_1, \overline{s}_2\} = \{\overline{s}_4^{k_1}, \overline{s}_4^{k_2}\overline{a}_{p_2}\}$. We have

$$\overline{s}_4^{k_2^{-1}} = (\overline{s}_4^{k_1})^{k_1^{-1}k_2^{-1}} = \overline{s}_1^{k_1^{-1}k_2^{-1}}.$$

Multiplying by $\overline{s}_2$, then

$$\overline{a}_{p_2} = \overline{s}_4^{k_2^{-1}} \cdot \overline{s}_4^{k_2}a_{p_2} = \overline{s}_1^{k_1^{-1}k_2^{-1}}\overline{s}_2 \in \overline{G}_2.$$

Since a_{p_2} generates $\mathcal{C}_{p_2}$, this implies $|G_2|$ is divisible by p_2. Similarly, we can show that $|G_2|$ is divisible by p_1. Also, $|s_1| = q$, so $|G_2|$ is divisible by q. Therefore, $|G_2|$ has three prime factors, which is a contradiction. □

ORCID iDs

Farzad Maghsoudi https://orcid.org/0000-0002-0482-319X

References

[1] A. Cayley, The theory of groups: Graphical representation, *Am. J. Math.* **1** (1878), 174–176, doi:10.2307/2369306.

[2] C. C. Chen and N. Quimpo, Hamiltonian Cayley graphs of order pq, in: *Combinatorial Mathematics, X (Adelaide, 1982)*, Springer, Berlin, volume 1036 of *Lecture Notes in Math.*, pp. 1–5, 1983, doi:10.1007/BFb0071505.

[3] C. C. Chen and N. F. Quimpo, On some classes of Hamiltonian graphs, *Southeast Asian Bull. Math.* (1979), 252–258, https://scopus.com/inward/record.url?eid=2-s2.0-0041913857&partnerID=10&rel=R3.0.0.

[4] C. C. Chen and N. F. Quimpo, On strongly Hamiltonian abelian group graphs, in: *Combinatorial mathematics, VIII (Geelong, 1980)*, Springer, Berlin-New York, volume 884 of *Lecture Notes in Math.*, pp. 23–34, 1981, doi:10.1007/BFb0091805.

[5] S. J. Curran and J. A. Gallian, Hamiltonian cycles and paths in Cayley graphs and digraphs—a survey, *Discrete Math.* **156** (1996), 1–18, doi:10.1016/0012-365X(95)00072-5.

[6] S. J. Curran, D. W. Morris and J. Morris, Cayley graphs of order $16p$ are Hamiltonian, *Ars Math. Contemp.* **5** (2012), 185–211, doi:10.26493/1855-3974.207.8e0.

[7] E. Durnberger, Connected Cayley graphs of semidirect products of cyclic groups of prime order by abelian groups are Hamiltonian, *Discrete Math.* **46** (1983), 55–68, doi:10.1016/0012-365X(83)90270-4.

[8] E. Durnberger, Every connected Cayley graph of a group with prime order commutator group has a Hamilton cycle, in: *Cycles in Graphs (Burnaby, B.C., 1982)*, North-Holland, Amsterdam, volume 115 of *North-Holland Math. Stud.*, pp. 75–80, 1985, doi:10.1016/S0304-0208(08)72997-9.

[9] E. Ghaderpour and D. W. Morris, Cayley graphs of order $27p$ are Hamiltonian, *Int. J. Comb.* (2011), Art. ID 206930, 16, doi:10.1155/2011/206930.

[10] E. Ghaderpour and D. W. Morris, Cayley graphs of order $30p$ are Hamiltonian, *Discrete Math.* **312** (2012), 3614–3625, doi:10.1016/j.disc.2012.08.017.

[11] C. Godsil and G. Royle, *Algebraic Graph Theory*, Springer, New York, 2001, doi:10.1007/9781461301639.

[12] M. Hall, *The Theory of Groups*, American Mathematical Soc., 1959, https://books.google.com/books?hl=sl&lr=&id=K8hEDwAAQBAJ&oi=fnd&pg=PP1&ots=BE6c1Bzt3u&sig=W90_d6E83hb0OBijkVUNNbHfxJU.

[13] D. Jungreis and E. Friedman, Cayley graphs on groups of low order are Hamiltonian (unpublished).

[14] K. Keating and D. W. Morris, On Hamilton cycles in Cayley graphs in groups with cyclic commutator subgroup, in: *Cycles in Graphs (Burnaby, B.C., 1982)*, North-Holland, Amsterdam, volume 115 of *North-Holland Math. Stud.*, pp. 89–102, 1985, doi:10.1016/S0304-0208(08)72999-2.

[15] E. Konstantinova, Some problems on Cayley graphs, *Linear Algebra Appl.* **429** (2008), 2754–2769, doi:10.1016/j.laa.2008.05.010.

[16] K. Kutnar, D. Marušič, D. W. Morris, J. Morris and P. Šparl, Hamiltonian cycles in Cayley graphs whose order has few prime factors, *Ars Math. Contemp.* **5** (2012), 27–71, doi:10.26493/1855-3974.177.341.

[17] D. Li, Cayley graphs of order pqr are Hamiltonian (chinese), *Acta Math. Sinica* **44** (2001), 351–358, https://www.semanticscholar.org/paper/Cayley-Graphs-of-Order-pqr-are-Hamiltonian-Deng/656ec3b806a0c8aa16ede47660cd9f90dcfff4a4.

[18] F. Maghsoudi, *Cayley graphs of order* $6pq$ *are Hamiltonian*, Master's thesis, University of Lethbridge, 2020, https://hdl.handle.net/10133/5771.

[19] D. Marušič, Hamiltonian circuits in Cayley graphs, *Discrete Math.* **46** (1983), 49–54, doi:10.1016/0012-365X(83)90269-8.

[20] D. W. Morris and K. Wilk, Cayley graphs of order kp are hamiltonian for $k < 48$, *Art Discrete Appl. Math.* **3** (2020), doi:10.26493/2590-9770.1250.763.

[21] I. Pak and R. Radoičić, Hamiltonian paths in Cayley graphs, *Discrete Math.* **309** (2009), 5501–5508, doi:10.1016/j.disc.2009.02.018.

[22] J. S. Robinson, *A Course in the Theory of Groups*, Springer, New York, 1996, doi:10.1007/978-1-4419-8594-1.

[23] D. Witte, Cayley digraphs of prime-power order are Hamiltonian, *J. Comb. Theory Ser. B* **40** (1986), 107–112, doi:10.1016/0095-8956(86)90068-7.

[24] D. Witte and J. A. Gallian, A survey: Hamiltonian cycles in Cayley graphs, *Discrete Math.* **51** (1984), 293–304, doi:10.1016/0012-365X(84)90010-4.

[25] D. S. Witte, On Hamiltonian circuits in Cayley diagrams, *Discrete Math.* **38** (1982), 99–108, doi:10.1016/0012-365X(82)90174-1.