ARS MATHEMATICA CONTEMPORANEA

Volume 21, Number 2, Fall/Winter 2021, Pages 151–317

Covered by:
Mathematical Reviews
zbMATH (formerly Zentralblatt MATH)
COBISS
SCOPUS
Science Citation Index-Expanded (SCIE)
Web of Science
ISI Alerting Service
Current Contents/Physical, Chemical & Earth Sciences (CC/PC & ES)
dblp computer science bibliography

The University of Primorska

The Society of Mathematicians, Physicists and Astronomers of Slovenia
The Institute of Mathematics, Physics and Mechanics
The Slovenian Discrete and Applied Mathematics Society

The publication is partially supported by the Slovenian Research Agency from the Call for co-financing of scientific periodical publications.

ARS MATHEMATICA
CONTEMPORANEA

Contents

Volume 21, Number 2, Fall/Winter 2021, Pages 151–317

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.01 / 151–173
https://doi.org/10.26493/1855-3974.2129.ac1
(Also available at http://amc-journal.eu)

Classification of skew morphisms of cyclic groups which are square roots of automorphisms*

Kan Hu †

Department of Mathematics, Zhejiang Ocean University, Zhoushan, Zhejiang 316022, P.R. China, and
Key Laboratory of Oceanographic Big Data Mining & Application of Zhejiang Province, Zhoushan, Zhejiang 316022, P.R. China

Young Soo Kwon ‡

Department of Mathematics, Yeungnam University, Gyeongsan, 712-749, Republic of Korea

Jun-Yang Zhang §

School of Mathematical Sciences, Chongqing Normal University, Chongqing 401331, P.R. China

Received 29 September 2019, accepted 28 April 2021, published online 18 September 2021

Abstract

The auto-index of a skew morphism φ of a finite group A is the smallest positive integer h such that φ^h is an automorphism of A. In this paper we develop a theory of auto-index of skew morphisms, and as an application we present a complete classification of skew morphisms of finite cyclic groups which are square roots of automorphisms.

Keywords: Skew morphism, auto-index, period, square root.

Math. Subj. Class. (2020): 20B25, 05C10, 14H57

*The authors would like to thank Marston Conder for his suggestion of the concept of 'auto-index', and Kai Yuan for his help in verifying our examples by the Magma program.

†Supported by Natural Science Foundation of Zhejiang Province (LY16A010010, LQ17A010003).

‡Supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2018R1D1A1B05048450).

§Corresponding author. Supported by Basic Research and Frontier Exploration Project of Chongqing (No. cstc2018jcyjAX0010), Science and Technology Research Program of Chongqing Municipal Education Commission (No.KJQN201800512) and National Natural Science Foundation of China (11671276).

E-mail addresses: hukan@zjou.edu.cn (Kan Hu), ysookwon@ynu.ac.kr (Young Soo Kwon), jyzhang@cqnu.edu.cn (Jun-Yang Zhang)

1 Introduction

Throughout the paper, groups considered are all finite. A *skew morphism* of a group A is a permutation φ on A fixing the identity element of A and for which there is a function $\pi\colon A \to \mathbb{Z}_{|\varphi|}$ on A, called the *power function* of φ, such that $\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$ for all $a, b \in A$. It is apparent the notion of skew morphism is a generalization of that of group automorphism. A skew morphism of A is called *proper* if it is not an automorphism. Two skew morphisms φ and φ' of A are *conjugate* if there exists an automorphism θ of A such that $\varphi' = \theta\varphi\theta^{-1}$.

The concept of skew morphism was first introduced by Jajcay and Širáň in [13] as an algebraic tool to study regular Cayley maps, which are regular embeddings of graphs on orientable closed surfaces admitting a regular subgroup of automorphisms on the vertices of the embedded graph. In this direction, regular Cayley maps of cyclic groups and dihedral groups have been classified, see [8, 21] and [14, 15, 16, 19, 28, 27]. In contrast, classification of regular Cayley maps of non-cyclic abelian groups and other metacyclic groups is still in progress; see [4, 5, 7, 20, 22, 26] for details.

The connection between skew morphisms and regular Cayley maps reveals a deep relationship between skew morphisms and group factorizations with cyclic complements. Indeed, if a group G is expressible as a product $A\langle y\rangle$ of a subgroup A and a cyclic subgroup $\langle y\rangle$ with $A \cap \langle y\rangle = 1$, then left multiplication of elements of A by y gives rise to a skew morphism φ of A, determined by $ya = \varphi(a)y^{\pi(a)}$ for all $a \in A$. Conversely, if φ is a skew morphism of a group A, then for any $a, b \in A$, we have

$$\varphi L_a(b) = \varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b) = L_{\varphi(a)}\varphi^{\pi(a)}(b),$$

so $\langle\varphi\rangle L_A \subseteq L_A\langle\varphi\rangle$, where $L_A = \{L_a \mid a \in A\}$ is the left regular representation of A. Since $\langle\varphi\rangle \cap L_A = 1$, we have $|\langle\varphi\rangle L_A| = |L_A\langle\varphi\rangle|$, and hence $\langle\varphi\rangle L_A = L_A\langle\varphi\rangle$. Therefore, $G = L_A\langle\varphi\rangle$ is a factorization of a transitive permutation group with a cyclic complement, which is often referred to as the *skew-product group* of φ. The interested reader is referred to [6, 17] for more details.

A prominent problem in this field is the classification of skew morphisms of cyclic groups, which is closely related to regular Cayley maps [8] as well as edge-transitive embeddings of complete bipartite graphs [11]. Kovács and Nedela [17] showed that if $n = n_1n_2$ such that $\gcd(n_1, n_2) = 1$ and $\gcd(n_1, \phi(n_2)) = \gcd(\phi(n_1), n_2) = 1$, then every skew morphism φ of the cyclic additive group $\mathbb{Z}_n$ is a direct product $\varphi = \varphi_1 \times \varphi_2$ of skew morphisms φ_i of $\mathbb{Z}_{n_i}$, $i = 1, 2$. In a subsequent paper [18] the authors classified all skew morphisms of the cyclic groups $\mathbb{Z}_{p^e}$, where p is an odd prime. As for the case $p = 2$, the associated skew product groups are classified by Du and Hu in [9].

Recently, Bachratý and Jajcay introduced the notion of period of skew morphisms [1]. More precisely, the *period* of a skew morphism φ is the smallest positive integer d such that $\pi\big(\varphi^d(a)\big) = \pi(a)$ for all $a \in A$. In particular, if $d = 1$ then the skew morphism is said to be *smooth* (or *coset-preserving*). In [1, 23], it was shown that if φ is a skew morphism of period d, then φ^d is a smooth skew morphism. The smooth skew morphisms of cyclic groups and of dihedral groups were classified in [2] and [23] respectively. Let φ be a skew morphism of a group A with power function π. If for any $a \in A$ either $\pi(a) = \pi(\varphi(a)) = \cdots = \pi(\varphi^{|\varphi|-1}(a)) = 1$ or $\pi(a) = \pi(\varphi(a)) = \cdots = \pi(\varphi^{|\varphi|-1}(a)) = t$ where $|\varphi|$ is the order of φ and t is a fixed integer with $1 \le t < |\varphi|$, then φ is called *t-balanced*. Observe that every t-balanced skew morphism φ of a group A is necessarily smooth, and in particular φ^{t+1} is an automorphism of A (see [10] and Remark 3.2 in Section 3). Thus, any t-balanced skew morphism is a $(t+1)$-*th root* of a group automorphism.

Inspired by those results above, we propose the following two related problems:

Problem 1.1. Let A be a given group, and d a given positive integer.

(a) Classify all skew morphisms of A which are d-th roots of automorphisms of A.

(b) Classify all skew morphisms of A which have period d.

For $A = \mathbb{Z}_n$ and $d = 2$, the following main result of this paper is a solution to the first problem, and by Theorem 3.8 (a) in Section 4 it is also a partial solution to the second one (skew morphisms of period 2 of $\mathbb{Z}_n$ whose square is an automorphism are determined).

Theorem 1.2. *Every proper skew morphism of the cyclic additive group $\mathbb{Z}_n$ which is a square root of an automorphism is conjugate to a skew morphism of the form*

$$\varphi(x) \equiv sx - \frac{x(x-1)n}{2k} \pmod{n},$$

where the pair (k, s) of positive integers satisfy the following conditions:

(a) *k^2 divides n and $s \in \mathbb{Z}_n^*$ if k is odd, and $2k^2$ divides n and $s \in \mathbb{Z}_{n/2}^*$ if k is even,*

(b) *$s \equiv -1 \pmod{k}$, s has multiplicative order 2ℓ in $\mathbb{Z}_{n/k}$ and $\gcd(w, k) = 1$ where*

$$w = \frac{k}{n}(s^{2\ell} - 1) - \frac{s(s-1)}{2}\ell.$$

The power function of φ is given by $\pi(x) \equiv 1+2xw'\ell \pmod{m}$, where $w'w = 1 \pmod{k}$ and $m = 2k\ell$ is the order of φ. Moreover, two such skew morphisms corresponding to distinct integer pairs are not conjugate.

The paper is organized as follows. After a summary of preliminary results in Section 2, we develop a more comprehensive theory of powers of skew morphisms by defining a new notion called auto-index in Section 3. In Section 4 we show that if φ is a proper skew morphism of a group A which is a square root of an automorphism, then its power function has the property $\pi(xy) \equiv \pi(x) + \pi(y) - 1 \pmod{|\varphi|}$ for all $x, y \in A$; in particular, if $A = \mathbb{Z}_n$, then $\pi(x) \equiv (\pi(1) - 1)x + 1 \pmod{|\varphi|}$ for all $x \in \mathbb{Z}_n$. As an application of the theory, we present a proof of Theorem 1.2 in Section 5. Finally, for the special case when $n = p^e$ is a prime power, we enumerate proper skew morphisms of $\mathbb{Z}_n$ which are square roots of automorphisms in Section 6.

2 Preliminaries

In this section we summarize some preliminary results on skew morphisms for future reference.

Proposition 2.1 ([1, 13])**.** *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. Then for any positive integer k,*

$$\varphi^k(ab) = \varphi^k(a)\varphi^{\sigma(a,k)}(b), \qquad \textit{for all} \quad a, b \in A,$$

where $\sigma(a,k) = \sum_{i=1}^{k} \pi(\varphi^{i-1}(a))$; moreover, φ^k is a skew morphism if and only if the congruence $kx \equiv \sigma(a,k) \pmod{m}$ is solvable for every $a \in A$.

Proposition 2.2 ([13])**.** *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. Then for any $a, b \in A$,*

$$\pi(ab) \equiv \sum_{i=1}^{\pi(a)} \pi(\varphi^{i-1}(b)) \pmod m.$$

Proposition 2.3 ([23])**.** *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. Then for any automorphism θ of A, $\varphi' = \theta\varphi\theta^{-1}$ is a skew morphism of A with power function $\pi' = \pi\theta^{-1}$.*

It follows that the automorphism group $\mathrm{Aut}(A)$ of A acts by conjugation on the set $\mathrm{Skew}(A)$ of all skew morphisms of A. Two skew morphisms of A are conjugate if they belong to the same orbit under such action.

An important subgroup related to skew morphisms is the *kernel* of φ defined by

$$\mathrm{Ker}\,\varphi = \{a \in A \mid \pi(a) \equiv 1 \pmod m\}.$$

It is well known that, for any $a, b \in A$, $\pi(a) \equiv \pi(b) \pmod m$ if and only if $ab^{-1} \in \mathrm{Ker}\,\varphi$, so π takes exactly $|A : \mathrm{Ker}\,\varphi|$ distinct values in $\mathbb{Z}_m$. The index $|A : \mathrm{Ker}\,\varphi|$ is called the *skew-type* of φ. It is obvious that φ is an automorphism if and only if it has skew-type 1. A skew morphism which is not an automorphism will be called *proper*.

The subset

$$\mathrm{Fix}\,\varphi = \{a \in A \mid \varphi(a) = a\}$$

of fixed-points of φ forms a subgroup of A. A subgroup N of A is *φ-invariant* if $\varphi(N) = N$. Clearly, $\mathrm{Fix}\,\varphi$ is φ-invariant, but $\mathrm{Ker}\,\varphi$ may not be. However, the subset

$$\mathrm{Core}\,\varphi = \bigcap_{i=1}^{m} \varphi^i(\mathrm{Ker}\,\varphi)$$

forms the largest φ-invariant subgroup of A contained in $\mathrm{Ker}\,\varphi$, and in particular, it is normal in A [28]. Thus $\mathrm{Ker}\,\varphi$ is φ-invariant if and only if $\mathrm{Ker}\,\varphi = \mathrm{Core}\,\varphi$, in which case the skew morphism is called *kernel-preserving*. It is apparent that if φ is kernel-preserving, then the restriction of φ to $\mathrm{Ker}\,\varphi$ is an automorphism of $\mathrm{Ker}\,\varphi$. The following result is well known.

Proposition 2.4 ([5])**.** *Every skew morphism of an abelian group is kernel-preserving.*

The importance of φ-invariant normal subgroups is reflected by the following result.

Proposition 2.5 ([29])**.** *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. If N a φ-invariant normal subgroup of A, then $\overline{\varphi}$ defined by $\overline{\varphi}(\overline{x}) = \overline{\varphi(x)}$ is a skew morphism of the quotient group $\overline{A} := A/N$. In particular, the order m_1 of $\overline{\varphi}$ is a divisor of m, and the power function $\overline{\pi}$ of $\overline{\varphi}$ is determined by $\overline{\pi}(\overline{a}) \equiv \pi(a) \pmod{m_1}$ for all $a \in A$.*

Since $\mathrm{Core}\,\varphi$ is a normal subgroup of A, φ induces a skew morphism $\overline{\varphi}$ of the quotient group $\overline{A} = A/\mathrm{Core}\,\varphi$. Define

$$\mathrm{Smooth}\,\varphi = \{a \in A \mid \overline{\varphi}(\overline{a}) = \overline{a}\},$$

which is the preimage of the fixed-point subgroup $\mathrm{Fix}\,\overline{\varphi}$ of $\overline{\varphi}$ under the natural epimorphism of A onto $A/\mathrm{Core}\,\varphi$. Since $\mathrm{Fix}\,\overline{\varphi}$ is a $\overline{\varphi}$-invariant subgroup of $\overline{A}$, $\mathrm{Smooth}\,\varphi$ is a φ-invariant subgroup of A.

In the extremal case that $\mathrm{Smooth}\,\varphi = A$, the skew morphism φ is called *smooth*. In [23] it is shown that a skew morphism φ of A is smooth if and only if $\pi(a) \equiv \pi(\varphi(a)) \pmod m$ for all $a \in A$. More generally, the *period* of φ is the smallest positive integer d such that $\pi(\varphi^d(a)) \equiv \pi(a) \pmod m$ for all $a \in A$. Thus, φ is smooth if and only if it has period 1. The following properties on the periodicity of skew morphisms are fundamental, see [23] for details.

Proposition 2.6 ([23]). *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. If φ has period d, then the following hold:*

(a) *d is equal to the order of the induced skew morphism $\overline{\varphi}$ of $\overline{A} = A/\mathrm{Core}\,\varphi$;*

(b) *d is the smallest positive integer such that φ^d is a smooth skew morphism of A;*

(c) *for any $a \in A$, $\sum_{i=1}^{d} \pi(\varphi^{i-1}(a)) \equiv 0 \pmod d$;*

(d) *conjugate skew morphisms have identical periods.*

Note that for any positive integer k, by Proposition 2.6 (a), if φ^k is a smooth skew morphism, then the period d of φ divides k.

3 Skew morphisms and automorphisms

Lemma 3.1. *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. Then for any positive integer k, φ^k is a group automorphism if and only if*

$$\sum_{i=1}^{k} \pi\big(\varphi^{i-1}(a)\big) \equiv k \pmod m$$

for all $a \in A$. In particular, if φ is smooth, then φ^k is an automorphism if and only if $k\pi(a) \equiv k \pmod m$ for all $a \in A$.

Proof. By Proposition 2.1, φ^k is a skew morphism of A if and only if the congruences

$$kx \equiv \sigma(a,k) \pmod m \tag{3.1}$$

are solvable for all $a \in A$, where

$$\sigma(a,k) = \sum_{i=1}^{k} \pi\big(\varphi^{i-1}(a)\big).$$

Note that if π_μ is the power function of $\mu := \varphi^k$, then $\pi_\mu(a)$ is the solution of (3.1), and therefore μ is an automorphism if and only if $\sigma(a,k) \equiv k \pmod m$ for all $a \in A$. In addition, if φ is smooth, then $\sigma(a,k) = k\pi(a)$, so μ is an automorphism if and only if $k\pi(a) \equiv k \pmod m$ for all $a \in A$. □

Remark 3.2. If φ is a t-balanced skew morphism of a group A, then φ is smooth and for all $a \in A \setminus \operatorname{Ker}\varphi$, $\pi(a) \equiv t \pmod{m}$ where $t^2 \equiv 1 \pmod{m}$ [5]. Therefore $(t+1)t \equiv t+1 \pmod{m}$. By Lemma 3.1, φ^{t+1} is a group automorphism. This is a generalization of [10, Lemma 3.4].

Definition 3.3. For a skew morphism φ of a group A, the *auto-index* of φ is defined to be the smallest positive integer h such that φ^h is a group automorphism of A.

Clearly, φ is an automorphism if and only if it has auto-index 1. Lower and upper bounds of the auto-index of a skew morphism are given as follows.

Lemma 3.4. *Let φ be a skew morphism of a group A. Suppose that φ has order m, period d and auto-index h, then d divides h and h divides m.*

Proof. Note that d is the smallest positive integer such that φ^d is a smooth skew morphism. Since φ^h is an automorphism which is necessarily smooth, the minimality of d implies that $d \mid h$. Since $\varphi^m = 1$ is the identity automorphism, the minimality of h implies that $h \mid m$, as required. □

Corollary 3.5. *If φ is a proper skew morphism of prime order, then it is smooth with auto-index equal to its order.*

Proof. Let d and h denote the period and auto-index of φ, respectively. As φ is proper, $d \leq |A : \operatorname{Ker}\varphi| < |\varphi|$ and $h > 1$. By Lemma 3.4, d divides h and h divides $|\varphi|$. Since $|\varphi| = p$ is prime, we obtain $d = 1$ and $h = p$, as required. □

As an example of Corollary 3.5, $\varphi = (0)(153)(2)(4)$ is a proper skew morphism of the cyclic group $\mathbb{Z}_6$. It is smooth, and both its order and auto-index are equal to 3.

Lemma 3.6. *Let φ be a skew morphism of the cyclic group $\mathbb{Z}_n$ and let $\pi : \mathbb{Z}_n \to \mathbb{Z}_m$ be the associated power function, where m is the order of φ. If φ has period 2 and auto-index h, then h is an even positive divisor of m and there exists some $u \in \mathbb{Z}_h$ such that*

$$\pi(x) \equiv \big(\pi(1) - 1\big) \sum_{i=1}^{x} \Big(1 + \frac{um}{h}\Big)^{i-1} + 1 \pmod{m}, \quad \textit{for all } x \in \mathbb{Z}_n. \tag{3.2}$$

Proof. Since φ has period 2, by Proposition 2.6 (c), $\pi(x) + \pi(\varphi(x)) \equiv 0 \pmod{2}$ for all $x \in \mathbb{Z}_n$. By Lemma 3.4, h is an even positive divisor of m. By Lemma 3.1, we have

$$h \equiv \sum_{i=1}^{h} \pi(\varphi^{i-1}(1)) \equiv \frac{1}{2}\Big(\pi(1) + \pi\big(\varphi(1)\big)\Big)h \pmod{m},$$

and then

$$\frac{1}{2}\Big(\pi(1) + \pi\big(\varphi(1)\big)\Big) = 1 + um/h,$$

for some $u \in \mathbb{Z}_h$.

Moreover, since φ has period 2, by Proposition 2.6 (a), $\overline{\varphi}$ is an automorphism of order 2. Thus, $\pi(1) \equiv \overline{\pi}(\overline{1}) \equiv 1 \pmod 2$. Consequently, by Proposition 2.1, we have

$$\begin{aligned}\pi(2) \equiv &\sum_{i=1}^{\pi(1)} \pi\big(\varphi^{i-1}(1)\big)\\ \equiv &\pi(1) + \frac{\pi(1)-1}{2}\Big(\pi(1) + \pi\big(\varphi(1)\big)\Big)\\ \equiv &\pi(1) + \big(\pi(1)-1\big)(1+um/h)\\ \equiv &\big(\pi(1)-1\big)\big(1+(1+um/h)\big)+1 \pmod m.\end{aligned}$$

By induction, we obtain (3.2), as required. □

In what follows we study skew morphisms of auto-index 2. These skew morphisms are all square roots of automorphisms. Clearly, every permutation of order 2 on A is a square root of the identity automorphism of A. Generally, a square root of an automorphism of A maybe not a skew morphism of A. It seems too difficult to determine all square roots of automorphisms for a family of groups. In the following example, all square roots of nonidentity automorphisms of $\mathbb{Z}_8$ are determined.

Example 3.7. The cyclic group $\mathbb{Z}_8$ has three nonidentity automorphisms as follows:

$\sigma_1 = (0)(2)(4)(6)(1,5)(3,7)$, $\sigma_2 = (0)(4)(2,6)(1,3)(5,7)$, $\sigma_3 = (0)(4)(2,6)(1,7)(5,3)$.

Since the square of every permutation of order 4 on $\mathbb{Z}_8$ either fixes no element or fixes 4 elements, σ_2 and σ_3 have no square roots. Set $\mu = (0)(2)(4)(6)(1,3,5,7)$ and use C_μ to denote the set of all square roots of the identity automorphism of $\mathbb{Z}_8$ which commute with μ. Then every square root of σ_1 can be represented as a product $\tau\mu$ where $\tau \in C_\mu$. It is straightforward to check that μ and μ^3 are the only two square roots of σ_1 which are skew morphisms. Since $\mu^3 = \sigma_3^{-1}\mu\sigma_3$, $\mathbb{Z}_8$ has a unique conjugate class of skew morphism of auto-index 2.

We are only concerned with square roots of automorphisms which are also skew morphisms. For convenience, skew morphisms of auto-index 2 are called *proper square roots of automorphisms* throughout this paper.

Theorem 3.8. *Let φ be a skew morphism of a group A, and let $\pi : A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. If φ is a proper square root of an automorphism, then*

(a) *φ is kernel-preserving of period at most 2;*

(b) *$\pi(x)$ is odd for all $x \in A$;*

(c) *$\pi(xy) \equiv \pi(x) + \pi(y) - 1 \pmod m$ for all $x, y \in A$;*

Proof. Take an arbitrary element $x \in A$. Since φ^2 is an automorphism and φ is not an automorphism, by Lemma 3.1, we have

$$\pi(x) + \pi(\varphi(x)) \equiv 2 \pmod m \quad \text{and} \quad \pi\big(\varphi(x)\big) + \pi\big(\varphi^2(x)\big) \equiv 2 \pmod m. \tag{3.3}$$

(a) From (3.3) we deduce $\pi(x) \equiv \pi\big(\varphi^2(x)\big) \pmod{m}$, so the period of φ is at most 2. In particular, we see that $\pi\big(\varphi(x)\big) = 1$ whenever $\pi(x) = 1$. It follows that φ is kernel-preserving.

(b) If φ has period 1, then $\pi(x) \equiv \pi\big(\varphi(x)\big) \pmod{m}$, and hence $2\pi(x) \equiv \pi(x) + \pi\big(\varphi(x)\big) \equiv 2 \pmod{m}$. Since φ is not an automorphism, m must be even. Since π is a group homomorphism from A to $\mathbb{Z}_m^*$ [23, Theorem 4.9], $\pi(x)$ is an odd integer. Now assume φ has period 2. Since φ is kernel-preserving, $\operatorname{Ker}\varphi = \operatorname{Core}\varphi$ is normal in A. By Proposition 2.6 (a), the induced skew morphism $\overline{\varphi}$ of $A/\operatorname{Ker}\varphi$ is an automorphism of order 2. Thus, $\pi(x) \equiv \overline{\pi}(\overline{x}) \equiv 1 \pmod{2}$, and $\pi(x)$ is also odd.

(c) By Proposition 2.2, we have

$$\begin{aligned}\pi(xy) \equiv &\sum_{i=1}^{\pi(x)} \pi(\varphi^{i-1}(y)) \\ \equiv &\pi(y) + \frac{\pi(x)-1}{2}\big(\pi(y) + \pi(\varphi(y))\big) \\ \equiv &\pi(x) + \pi(y) - 1 \pmod{m}\end{aligned}$$

for all $x, y \in A$. □

Corollary 3.9. *Let φ be a proper square root of an automorphism of a group A, and let $\pi : A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. Then*

(a) *if φ is smooth, then it has skew-type two, 4 divides m, and $\pi(x) = 1 + m/2$ for all $x \in A \setminus \operatorname{Ker}\varphi$;*

(b) *if φ is not smooth, then it has skew-type at least* 3.

Proof. If φ is smooth, then from the proof of Theorem 3.8, we see that m is even and $2\pi(x) \equiv 2 \pmod{m}$ for any $x \in A$. Hence $\pi(x) = 1$ or $1 + m/2$. Since φ is proper and $\pi(x)$ is odd, 4 divides m. If φ is not smooth, then the skew-type of φ is at least 3 since φ is kernel-preserving of period 2. □

Example 3.10 ([25])**.** The cyclic group $\mathbb{Z}_9$ has four skew morphisms of period 2:

$$\begin{aligned}
\varphi_1 &= (0)(1,2,7,5,4,8)(3,6), &\quad \pi_1 &= [1][3,5,3,5,3,5][1,1];\\
\varphi_2 &= (0)(1,5,4,2,7,8)(3,6), &\quad \pi_2 &= [1][3,5,3,5,3,5][1,1];\\
\varphi_3 &= (0)(1,8,4,5,7,2)(3,6), &\quad \pi_3 &= [1][5,3,5,3,5,3][1,1];\\
\varphi_4 &= (0)(1,8,7,2,4,5)(3,6), &\quad \pi_4 &= [1][5,3,5,3,5,3][1,1].
\end{aligned}$$

It can be directly verified that φ_i^2 $(i = 1,2,3,4)$ are automorphisms of $\mathbb{Z}_9$, so that all of these skew morphisms are proper square roots of automorphisms. Note that up to conjugation by automorphisms they are divided into two classes $\{\varphi_1, \varphi_4\}$ and $\{\varphi_2, \varphi_3\}$.

Example 3.11. Define two functions φ and π on the cyclic group $\mathbb{Z}_{8n}$ where n is a positive integer as follows:

$$\varphi(x) \equiv \begin{cases} 2i \pmod{8n}, & \text{if } x = 2i;\\ 2(n+i)+1 \pmod{8n}, & \text{if } x = 2i+1 \end{cases}$$

and

$$\pi(x) = \begin{cases} 1, & \text{if } x = 2i; \\ 3, & \text{if } x = 2i+1. \end{cases}$$

It is straightforward to check that φ is a skew morphism of $\mathbb{Z}_{8n}$ with power function π whose square is an involutory automorphism.

4 Technical lemmas

In what follows we restrict our discussion to proper square roots of automorphisms of the cyclic groups.

Lemma 4.1. *Let φ be a skew morphism of the cyclic group $\mathbb{Z}_n$, and let $\pi\colon \mathbb{Z}_n \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. If φ is a proper square root of an automorphism and it has skew-type k, then the following hold:*

(a) *there is some integer $\ell \geq 1$ such that $m = 2k\ell$;*

(b) *there is some integer $u \in \mathbb{Z}_k^*$ such that $\pi(x) \equiv 1 + 2xu\ell \pmod{m}$ for all $x \in \mathbb{Z}_n$;*

(c) *the number $r = \varphi^2(1)$ is coprime to n and there exists some integer $v \in \mathbb{Z}_k^*$ such that $r^\ell \equiv 1 + vn/k \pmod{n}$;*

(d) *k^2 is a divisor of n;*

(e) *the multiplicative order of r in $\mathbb{Z}_{n/k}$ is equal to ℓ.*

Proof. By Theorem 3.8, φ has period 1 or 2 and

$$\pi(x+y) \equiv \pi(x) + \pi(y) - 1 \pmod{m}$$

for all $x, y \in \mathbb{Z}_n$. Thus $\pi(2) \equiv 2\pi(1) - 1 \equiv 2\big(\pi(1) - 1\big) + 1 \pmod{m}$ and by induction

$$\pi(x) \equiv x\big(\pi(1) - 1\big) + 1 \pmod{m}, \quad \forall x \in \mathbb{Z}_n.$$

In particular, $\pi(m) \equiv m\big(\pi(1) - 1\big) + 1 \equiv 1 \pmod{m}$, and therefore $m \in \operatorname{Ker}\varphi$. Since φ is of skew-type k, $\operatorname{Ker}\varphi = \langle k \rangle$, and hence $k \mid m$. Noting that

$$1 \equiv \pi(k) \equiv k\big(\pi(1) - 1\big) + 1 \pmod{m},$$

we get $\pi(1) = 1 + um/k$ for some $u \in \mathbb{Z}_k$. Consequently, $\pi(x) \equiv 1 + xum/k \pmod{m}$. Since π takes k distinct values of the form $1 + im/k$ $(i = 0, 1, \ldots, k-1)$ in $\mathbb{Z}_m$, we have $u \in \mathbb{Z}_k^*$. By Theorem 3.8, $1 + m/k$ is odd, that is, m/k is even. Thus we can write $m = 2k\ell$, where ℓ is a positive integer. Then $\pi(x) \equiv 1 + 2xu\ell \pmod{m}$.

Set $r = \varphi^2(1)$. Since $\varphi^2 \in \operatorname{Aut}(\mathbb{Z}_n)$, r is coprime to n and $\varphi^2(x) \equiv rx \pmod{n}$ for all $x \in \mathbb{Z}_n$. In particular, $\varphi^{2\ell}(k) \equiv r^\ell k \pmod{n}$. On the other hand, there exists $u' \in \mathbb{Z}_n$ such that $\pi(u') \equiv 1 + 2\ell \pmod{m}$. Therefore

$$\varphi(k) + \varphi(u') \equiv \varphi(k + u') \equiv \varphi(u' + k) \equiv \varphi(u') + \varphi^{1+2\ell}(k) \pmod{n}$$

and then $\varphi^{2\ell}(k) = k$. Thus, $r^\ell \equiv 1 \pmod{n/k}$. Write $r^\ell = 1 + vn/k$. Recalling that φ has period at most 2, we have $\pi\big(\varphi^{2\ell}(1)\big) \equiv \pi(1) \pmod{m}$ and hence $\varphi^{2\ell}(1) \equiv 1$

$\pmod{k}$. It follows that $1 + vn/k \equiv r^\ell \equiv \varphi^{2\ell}(1) \equiv 1 \pmod{k}$, and hence k is a divisor of vn/k. Note that

$$\varphi^{2\ell j}(1) \equiv r^{\ell j} \equiv \Big(1 + \frac{vn}{k}\Big)^j \equiv 1 + \frac{jvn}{k} + \sum_{i=2}^{j} \binom{j}{i} \Big(\frac{vn}{k}\Big)^i \equiv 1 + \frac{jvn}{k} \pmod{n}$$

for any positive integer j. By [29, Lemma 3.1], the length of the orbit of 1 under φ is equal to the order $m = 2k\ell$ of φ. If $0 < j < k$, then $1 \not\equiv \varphi^{2j\ell}(1) \equiv 1 + jvn/k \pmod{n}$. Consequently, $v \in \mathbb{Z}_k^*$ and k^2 divides n.

If the multiplicative order of r in $\mathbb{Z}_{n/k}$ is i, then $r^i = 1+tn/k$ for some positive integer t. Since $r^\ell \equiv 1 \pmod{n/k}$, we have $i \mid \ell$. On the other hand, since $k^2 \mid n$ for all $x \in \mathbb{Z}_n$, we have

$$\varphi^{2ik}(x) \equiv r^{ik} x \equiv (1 + tn/k)^k x \equiv x \pmod{n}.$$

Since the order of φ is $2k\ell$, we get $\ell \mid i$, and therefore $\ell = i$. □

Corollary 4.2. *Let φ be a skew morphism of the cyclic group $\mathbb{Z}_n$. If φ is a proper square root of an automorphism, then the induced skew morphism $\overline{\varphi}$ of $\mathbb{Z}_n/\mathrm{Ker}\,\varphi$ maps each $\overline{x}$ to $-\overline{x}$.*

Proof. Let m and k be the order and the skew-type of φ, respectively. By Lemma 4.1, $m = 2k\ell$ for some positive integer ℓ, and

$$2 \equiv \pi(x) + \pi\big(\varphi(x)\big) \equiv 2 + 2\big(x + \varphi(x)\big)u\ell \pmod{2k\ell}$$

for all $x \in \mathbb{Z}_n$, where $u \in \mathbb{Z}_k^*$. Thus $2\big(x + \varphi(x)\big)u\ell \equiv 0 \pmod{2k\ell}$ and then $\varphi(x) \equiv -x \pmod{k}$, as required. □

The converse of Corollary 4.2 is generally not true, see [6, Theorem 6.5] for a counterexample. However, we have the following result.

Lemma 4.3. *Let φ be a proper skew morphism of the cyclic group $\mathbb{Z}_n$. If the induced skew morphism $\overline{\varphi}$ of $\mathbb{Z}_n/\mathrm{Ker}\,\varphi$ maps each $\overline{x}$ to $-\overline{x}$, then φ^2 is a skew morphism of skew-type at most 2. In particular, if the skew-type of φ is odd, then φ^2 is an automorphism of $\mathbb{Z}_n$.*

Proof. Throughout the proof, we denote the order and the skew-type of φ by m and k, and the power functions of φ and $\overline{\varphi}$ by π and $\overline{\pi}$, respectively.

If $k = 2$, then the result is obviously true. In what follows we assume $k > 2$. Since $\overline{\varphi}$ maps each $\overline{x}$ to $-\overline{x}$, $\overline{\varphi}$ is an automorphism of order 2. By Proposition 2.6 (a), φ has period 2. It follows that m is even, $\pi\big(\varphi^2(x)\big) \equiv \pi(x) \pmod{m}$ and $\pi\big(\varphi(x)\big) \equiv \pi(-x) \pmod{m}$ for all $x \in \mathbb{Z}_n$. Since $\pi(x) \equiv \overline{\pi}(\overline{x}) \equiv 1 \pmod{2}$, $\pi(x)$ is odd.

Take two arbitrary elements $x, y \in \mathbb{Z}_n$. By Proposition 2.2, we have

$$\pi(x + y) \equiv \sum_{i=1}^{\pi(x)} \pi(\varphi^{i-1}(y)) \equiv \pi(y) + \frac{\pi(x) - 1}{2}\big(\pi(y) + \pi(-y)\big) \pmod{m}.$$

In particular,

$$1 = \pi(x-x) \equiv \pi(-x) + \frac{\pi(x)-1}{2}\big(\pi(x)+\pi(-x)\big) \pmod{m}, \tag{4.1}$$

$$1 = \pi(-x+x) \equiv \pi(x) + \frac{\pi(-x)-1}{2}\big(\pi(x)+\pi(-x)\big) \pmod{m}, \tag{4.2}$$

$$\pi(2x) \equiv \pi(x) + \frac{\pi(x)-1}{2}\big(\pi(x)+\pi(-x)\big) \pmod{m}, \tag{4.3}$$

$$\pi(-2x) \equiv \pi(-x) + \frac{\pi(-x)-1}{2}\big(\pi(x)+\pi(-x)\big) \pmod{m}, \tag{4.4}$$

$$\pi(2x+1) \equiv \pi(2x) + \frac{\pi(1)-1}{2}\big(\pi(2x)+\pi(-2x)\big) \pmod{m}, \tag{4.5}$$

$$\pi(-2x-1) \equiv \pi(-2x) + \frac{\pi(-1)-1}{2}\big(\pi(2x)+\pi(-2x)\big) \pmod{m}. \tag{4.6}$$

Adding (4.1) to (4.2) and (4.3) to (4.4), we get

$$\frac{1}{2}\big(\pi(x)+\pi(-x)\big)^2 \equiv 2 \pmod{m}$$

and

$$\frac{1}{2}\big(\pi(x)+\pi(-x)\big)^2 \equiv \pi(2x)+\pi(-2x) \pmod{m}.$$

Thus,

$$\pi(2x)+\pi(-2x) \equiv 2 \pmod{m}. \tag{4.7}$$

Substituting 2 for $\pi(2x)+\pi(-2x)$ in (4.5) and (4.6) we obtain

$$\pi(2x+1) \equiv \pi(2x)+\pi(1)-1 \pmod{m}$$

and

$$\pi(-2x-1) \equiv \pi(-2x)+\pi(-1)-1 \pmod{m}.$$

It follows that

$$\pi(2x+1)+\pi(-2x-1) \equiv \pi(1)+\pi(-1) \pmod{m}. \tag{4.8}$$

From (4.7) and (4.8) we deduce that

$$\varphi^2(x+y) = \varphi^2(x)+\varphi^2(y)$$

if x is even, and

$$\varphi^2(x+y) = \varphi^2(x)+\varphi^{\pi(1)+\pi(-1)}(y)$$

if x is odd. Thus, φ^2 is a skew morphism of skew-type at most 2. In particular, if the skew-type k of φ is an odd number, then

$$\pi(1)+\pi(-1) \equiv \pi(k+1)+\pi(k-1) \equiv 2 \pmod{m}$$

and therefore φ^2 is an automorphism, as claimed. □

5 Classification

In this section, we classify proper square roots of automorphisms of $\mathbb{Z}_n$.

Theorem 5.1. *Define a quadratic polynomial over the ring* $(\mathbb{Z}_n, +, \times)$ *by*

$$\varphi(x) \equiv sx - \frac{x(x-1)n}{2k} \pmod n, \ \ x \in \mathbb{Z}_n, \tag{5.1}$$

where k and s are positive integers satisfying the following conditions:

(a) *k^2 divides n and $s \in \mathbb{Z}_n^*$ if k is odd, and $2k^2$ divides n and $s \in \mathbb{Z}_{n/2}^*$ if k is even,*

(b) *$s \equiv -1 \pmod k$, s has multiplicative order 2ℓ in $\mathbb{Z}_{n/k}$ and* $\gcd(w,k) = 1$ *where*

$$w = \frac{k}{n}(s^{2\ell} - 1) - \frac{s(s-1)}{2}\ell.$$

Then φ is a proper square root of an automorphism of the cyclic additive group $\mathbb{Z}_n$ whose skew-type is k and power function is given by

$$\pi(x) \equiv 1 + 2xw'\ell \pmod m,$$

where $w'w \equiv 1 \pmod k$ and $m = 2k\ell$ is the order of φ. Moreover, up to conjugation φ is uniquely determined by the parameters k and s.

Proof. First, we show that φ is a permutation on $\mathbb{Z}_n$. Assume $\varphi(x) \equiv \varphi(y) \pmod n$ where $x, y \in \mathbb{Z}_n$. Then it suffices to prove that $x \equiv y \pmod n$. Since

$$sx - \frac{x(x-1)n}{2k} \equiv sy - \frac{y(y-1)n}{2k} \pmod n,$$

we get

$$s(x-y) \equiv \frac{(x-y)(x+y-1)n}{2k} \pmod n.$$

By (a) and (b) we have $s \in \mathbb{Z}_n^*$. Thus, from the above equation we deduce that $x - y \equiv 0 \pmod{n/k}$. By (a) again we obtain

$$\frac{(x-y)(x+y-1)n}{2k} \equiv 0 \pmod n,$$

and hence $x \equiv y \pmod n$.

Second, we show that φ^2 is an automorphism of $\mathbb{Z}_n$. By (a) and (b), we derive from formula (5.1) that

$$\varphi\Big(\frac{jn}{k}\Big) \equiv \frac{sjn}{k} - \frac{jn(jn-k)n}{2k^3} \equiv -\frac{jn}{k} \pmod n \tag{5.2}$$

for all positive integers j. Now for any $x, y \in \mathbb{Z}_n$,

$$\begin{aligned}\varphi(x+y) &\equiv s(x+y) - \frac{(x+y)(x+y-1)n}{2k} \\ &\equiv sx - \frac{x(x-1)n}{2k} + sy - \frac{y(y-1)n}{2k} - \frac{xyn}{k} \\ &\equiv \varphi(x) + \varphi(y) - \frac{xyn}{k} \pmod n.\end{aligned}$$

It follows that

$$\begin{aligned}
\varphi^2(x) &\equiv \varphi\Big(sx - \frac{x(x-1)n}{2k}\Big) \\
&\equiv \varphi(sx) + \varphi\Big(-\frac{x(x-1)n}{2k}\Big) + \frac{n}{k}\frac{sx^2(x-1)n}{2k} \\
&\equiv \varphi(sx) + \varphi\Big(-\frac{x(x-1)n}{2k}\Big) \\
&\overset{(5.2)}{\equiv} s^2x - \frac{sx(sx-1)n}{2k} + \frac{x(x-1)n}{2k} \\
&\equiv \Big(s^2 - \frac{s(s-1)n}{2k}\Big)x - \frac{(s^2-1)x(x-1)n}{2k} \\
&\overset{(b)}{\equiv} \Big(s^2 - \frac{s(s-1)n}{2k}\Big)x \pmod{n}.
\end{aligned}$$

Since $s \in \mathbb{Z}_n^*$ and $k^2 \mid n$, we have $\gcd\big(s^2 - \frac{s(s-1)n}{2k}, n\big) = 1$. Thus, φ^2 is an automorphism of $\mathbb{Z}_n$.

Next we show that φ is a skew morphism of $\mathbb{Z}_n$ with associated power function π defined by $\pi(x) \equiv 1 + 2w'\ell \pmod{m}$ for any $x \in \mathbb{Z}_n$, where $w'w \equiv 1 \pmod{k}$. Take arbitrary $x, y \in \mathbb{Z}_n$. By the conditions (a) and (b), we have

$$\begin{aligned}
\varphi(x) + \varphi^{\pi(x)}(y) &\equiv \varphi(x) + \varphi^{1+2xw'\ell}(y) \equiv \varphi(x) + \varphi^{2xw'\ell}(\varphi(y)) \\
&\equiv \varphi(x) + \varphi(y)\Big(s^2 - \frac{s(s-1)n}{2k}\Big)^{\ell w' x} \\
&\equiv \varphi(x) + \varphi(y)\Big(s^{2\ell} - \frac{s(s-1)\ell n}{2k}\Big)^{w' x} \\
&\equiv \varphi(x) + \varphi(y)\Big(1 + \frac{wn}{k}\Big)^{w' x} \\
&\equiv \varphi(x) + \varphi(y)\Big(1 + \frac{nx}{k}\Big) \pmod{n}
\end{aligned}$$

and

$$\begin{aligned}
\varphi(x+y) &\equiv \varphi(x) + \varphi(y) - \frac{nxy}{k} \equiv \varphi(x) + \Big(sy - \frac{y(y-1)n}{2k}\Big) - \frac{nxy}{k} \\
&\equiv \varphi(x) + \Big(sy - \frac{y(y-1)n}{2k}\Big) + \frac{snxy}{k} \\
&\equiv \varphi(x) + \Big(sy - \frac{y(y-1)n}{2k}\Big)\Big(1 + \frac{nx}{k}\Big) \\
&\equiv \varphi(x) + \varphi(y)\Big(1 + \frac{nx}{k}\Big) \pmod{n}.
\end{aligned}$$

Therefore, $\varphi(x+y) \equiv \varphi(x) + \varphi^{\pi(x)}(y)$ and thus φ is a skew morphism of $\mathbb{Z}_n$.

Finally, we prove that up to conjugation φ is uniquely determined by the parameters k and s. It is evident that if two such skew morphism are conjugate, then they must have the same skew-type k. Suppose now that φ_i $(i = 1, 2)$ are two conjugate skew morphisms of $\mathbb{Z}_n$ defined by

$$\varphi_i(x) \equiv s_i x - \frac{x(x-1)n}{2k} \pmod{n},$$

where n, k and s_i satisfy the stated conditions. Then there exists an automorphism θ of $\mathbb{Z}_n$ such that $\varphi_1\theta = \theta\varphi_2$. Set $r = \theta(1)$. Then

$$s_1 rx - \frac{rx(rx-1)n}{2k} \equiv \varphi_1\theta(x) \equiv \theta\varphi_2(x) \equiv s_2 rx - \frac{rx(x-1)n}{2k} \pmod{n}.$$

Since $\gcd(r, n) = 1$, this is reduced to

$$s_1 x - \frac{x(rx-1)n}{2k} \equiv s_2 x - \frac{x(x-1)n}{2k} \pmod{n},$$

or equivalently,

$$(s_1 - s_2)x \equiv \frac{x(rx-1)n}{2k} - \frac{x(x-1)n}{2k} \equiv \frac{x^2(r-1)n}{2k} \pmod{n}.$$

If we choose $x = \pm 1$, then $\pm(s_1 - s_2) \equiv (r-1)n/2k \pmod{n}$. Therefore $2(s_1 - s_2) \equiv 0 \pmod{n}$ and $r \equiv 1 \pmod{k}$. If k is even, so is n, and hence $s_1 \equiv s_2 \pmod{n/2}$. If both k and n are odd, then $s_1 \equiv s_2 \pmod{n}$. If k is odd but n is even, then r is odd. Since $r \equiv 1 \pmod{k}$, we obtain $r - 1 \equiv 0 \pmod{2k}$. Thus, we also get $s_1 \equiv s_2 \pmod{n}$, as required. $\square$

Now we are ready to prove the main result of the paper.

Proof of Theorem 1.2. By Theorem 5.1, the quadratic polynomial of the stated form is a proper square root of an automorphism of $\mathbb{Z}_n$, and distinct pairs (k, s) correspond to disconjugate skew morphisms.

Conversely, suppose that φ is a proper square root of an automorphism of $\mathbb{Z}_n$ of skew-type $k > 1$. By Lemma 4.1, $k^2 \mid n$, $|\varphi| = 2k\ell$ for some positive integer ℓ, and the power function of φ is given by $\pi(x) \equiv 1 + 2xu\ell \pmod{2k\ell}$ for some $u \in \mathbb{Z}_k^*$. Set $s = \varphi(1)$. By Lemma 3.1, we have

$$2 \equiv \pi(1) + \pi(\varphi(1)) \equiv (1 + 2u\ell) + (1 + 2su\ell) \equiv 2 + 2(1+s)u\ell \pmod{2k\ell},$$

which implies $2(1+s)u\ell \equiv 0 \pmod{2kl}$. Since $u \in \mathbb{Z}_k^*$, we obtain $s \equiv -1 \pmod{k}$.

Since φ^2 is an automorphism of $\mathbb{Z}_n$, $\varphi^2(x) \equiv rx \pmod{n}$ for some r coprime to n. By Lemma 4.1, $r^\ell \equiv 1 + vn/k \pmod{n}$ for some $v \in \mathbb{Z}_k^*$. Then

$$\begin{aligned}\varphi(x) \equiv& \varphi(x-1) + \varphi^{\pi(x-1)}(1) \equiv \varphi(x-1) + \varphi^{2\ell u(x-1)+1}(1)\\ \equiv& \varphi(x-1) + \varphi^{2\ell u(x-1)}(s) \equiv \varphi(x-1) + sr^{\ell u(x-1)}\\ \equiv& \varphi(x-1) + s\Big(1 + \frac{vn}{k}\Big)^{u(x-1)} \pmod{n}.\end{aligned}$$

By induction we obtain

$$\varphi(x) \equiv s\sum_{i=1}^{x}\Big(1 + \frac{vn}{k}\Big)^{u(i-1)} \pmod{n}, \quad x \in \mathbb{Z}_n.$$

Since $k^2 \mid n$, for any positive integer j, we have

$$\Big(1 + \frac{vn}{k}\Big)^j \equiv 1 + \frac{jvn}{k} + \sum_{i=2}^{j}\binom{j}{i}\Big(\frac{vn}{k}\Big)^i \equiv 1 + \frac{jvn}{k} \pmod{n}.$$

Thus,

$$\begin{aligned}\varphi(x) \equiv& s\sum_{i=1}^{x}\Big(1+\frac{vn}{k}\Big)^{u(i-1)} \equiv s\sum_{i=1}^{x}\Big(1+\frac{uvn(i-1)}{k}\Big)\\ \equiv& s\Big(x+\frac{uvnx(x-1)}{2k}\Big) \equiv sx-\frac{uvnx(x-1)}{2k} \pmod{n}.\end{aligned}$$

It follows that

$$r=\varphi^2(1)=\varphi(s)\equiv s^2-\frac{uvns(s-1)}{2k} \pmod{n}. \tag{5.3}$$

Hence, $r\equiv s^2 \pmod{n/k}$ and by Lemma 4.1 (e), s has multiplicative order 2ℓ in $\mathbb{Z}_{n/k}$.

Since

$$\begin{aligned}1+\frac{vn}{k} \equiv& r^\ell \equiv \Big(s^2-\frac{s(s-1)uvn}{2k}\Big)^\ell\\ \equiv& s^{2\ell}-\binom{\ell}{1}s^{2(\ell-1)}\frac{s(s-1)uvn}{2k}+\sum_{i=2}^{\ell}\binom{\ell}{i}s^{2(\ell-i)}\Big(-\frac{s(s-1)uvn}{2k}\Big)^i\\ \equiv& s^{2\ell}-\frac{s^{2(\ell-1)}s(s-1)\ell uvn}{2k} \equiv s^{2\ell}-\frac{s(s-1)\ell uvn}{2k} \pmod{n},\end{aligned}$$

we have

$$s^{2\ell}\equiv 1+\Big(1+\frac{s(s-1)\ell u}{2}\Big)\frac{vn}{k} \pmod{n/k}.$$

By [12, Lemma 1], there exists $c\in\mathbb{Z}_n^*$ such that $c\equiv uv \pmod{k}$. Define $\varphi':=\theta_c\varphi\theta_c^{-1}$, where θ_c is the automorphism of $\mathbb{Z}_n$ taking 1 to c. By Proposition 2.3, φ' is a skew morphism of $\mathbb{Z}_n$. For all $x\in\mathbb{Z}_n$, we have

$$\begin{aligned}\varphi'(x) =& \theta_c\varphi\theta_c^{-1}(x)=\theta_c\varphi(c^{-1}x)\equiv c\Big(sc^{-1}x-\frac{c^{-1}x(c^{-1}x-1)cn}{2k}\Big)\\ \equiv& sx-\frac{x(x-c)n}{2k} \equiv \Big(s+\frac{(c-1)n}{2k}\Big)x-\frac{x(x-1)n}{2k} \pmod{n}.\end{aligned}$$

Let $s'=s+\frac{(c-1)n}{2k}$, then it is easily seen that $s'\equiv -1 \pmod{k}$, $s'\in\mathbb{Z}_n^*$, and s' has multiplicative order 2ℓ in $\mathbb{Z}_{n/k}$. Therefore, up to conjugation we can assume

$$\varphi(x)\equiv sx-\frac{x(x-1)n}{2k} \pmod{n} \quad \text{and} \quad \pi(x)\equiv 1+2w'\ell x \pmod{2k\ell},$$

where $s\equiv -1 \pmod{k}$, $s\in\mathbb{Z}_n^*$, $w'\in\mathbb{Z}_k^*$, and 2ℓ is the multiplicative order of s in $\mathbb{Z}_{n/k}$.

We show that $ww'\equiv 1 \pmod{k}$, that is, w' is the modular inverse of w in $\mathbb{Z}_k$. Noting that the congruence

$$w\equiv \frac{k}{n}(s^{2\ell}-1)-\frac{s(s-1)}{2}\ell \pmod{k}$$

is equivalent to

$$s^{2\ell}-\frac{s(s-1)\ell n}{2k}\equiv 1+\frac{nw}{k} \pmod{n},$$

we have

$$\begin{aligned}
2s-\frac{n}{k} &\equiv \varphi(2) \equiv \varphi(1)+\varphi^{\pi(1)}(1)\\
&\equiv s+\varphi^{2w'\ell}(s)\\
&\equiv s+s\Big(s^2-\frac{s(s-1)n}{2k}\Big)^{\ell w'}\\
&\equiv s+s\Big(s^{2\ell}-\frac{s(s-1)\ell n}{k}\Big)^{w'}\\
&\equiv s+s\Big(1+\frac{nw}{k}\Big)^{w'}\\
&\equiv 2s+\frac{sww'n}{k} \equiv 2s-\frac{nww'}{k} \pmod{n},
\end{aligned}$$

which is reduced to $ww' \equiv 1 \pmod{k}$.

In what follows we consider the particular case that k is even. We have

$$\varphi^2(2)=2\varphi^2(1)\equiv 2s^2-\frac{s(s-1)n}{k}\equiv 2s^2-\frac{2n}{k} \pmod{n}$$

and

$$\begin{aligned}
\varphi^2(2) &\equiv \varphi\Big(2s-\frac{n}{k}\Big) \equiv s\Big(2s-\frac{n}{k}\Big)-\Big(2s-\frac{n}{k}\Big)\big(2s-\frac{n}{k}-1\big)\frac{n}{2k}\\
&\equiv 2s^2-\frac{sn}{k}-\Big(s-\frac{n}{2k}\Big)(2s-1)\frac{n}{k}\\
&\equiv 2s^2-\frac{sn}{k}-\Big(2s^2-s-\frac{sn}{k}+\frac{n}{2k}\Big)\frac{n}{k}\\
&\equiv 2s^2-\frac{2s^2n}{k}-\frac{n^2}{2k^2}\equiv 2s^2-\frac{2n}{k}-\frac{n^2}{2k^2} \pmod{n}.
\end{aligned}$$

Thus,

$$2s^2-\frac{2n}{k}\equiv 2s^2-\frac{2n}{k}-\frac{n^2}{2k^2} \pmod{n},$$

and therefore $2k^2 \mid n$. Moreover, if $s > n/2$, then we write $s' = s - n/2$ and define

$$\varphi'(x)\equiv s'x-\frac{x(x-1)n}{2k} \pmod{n}, \qquad x\in\mathbb{Z}_n.$$

It is easily seen that φ' is also a square root of an automorphism of $\mathbb{Z}_n$. We show that φ' is conjugate to φ. Since $2k^2 \mid n$, $n = 2^e k n_1$ where $e \geq 1$ and $2 \nmid n_1$. Note that the number $c := kn_1 + 1$ is coprime to n. Let θ_c be the automorphism of $\mathbb{Z}_n$ taking x to cx. Then, for any $x \in \mathbb{Z}_n$,

$$\begin{aligned}
\varphi'\theta_c(x) &\equiv s'cx-\frac{cx(cx-1)n}{2k}\\
&\equiv (s-\frac{n}{2})cx-\frac{\big(cx(x-1)+c(c-1)x^2\big)n}{2k}\\
&\equiv scx-\frac{cx(x-1)n}{2k}+\frac{nx}{2}-\frac{c(c-1)x^2n}{2k}\\
&\equiv scx-\frac{cx(x-1)n}{2k}\equiv \theta_c\varphi(x) \pmod{n}.
\end{aligned}$$

Thus, φ is conjugate to φ', as required. $\square$

Corollary 5.2. *Every smooth proper square root of an automorphism of the cyclic group $\mathbb{Z}_n$ is conjugate to a skew morphism of the form*

$$\varphi(x) \equiv sx - \frac{x(x-1)n}{4} \pmod{n}, \quad x \in \mathbb{Z}_n,$$

with the associated power function given by

$$\pi(x) \equiv 1 + 2\ell x \pmod{4\ell}, \quad x \in \mathbb{Z}_n,$$

where $8 \mid n$, both s and $\frac{2}{n}(s^{2\ell}-1) - \frac{s(s-1)}{2}\ell$ are odd numbers, and the multiplicative order of s in $\mathbb{Z}_{n/2}$ is equal to 2ℓ. In particular, φ has order 4ℓ and skew-type 2.

Proof. By Corollary 3.9, every smooth proper square root of an automorphism has skew-type 2. The result follows immediately from Theorem 1.2. $\square$

Remark 5.3. Note that if φ is proper skew morphism of $\mathbb{Z}_n$ and φ^2 is an involutory automorphism, then $|\varphi| = 4$, and by Theorem 1.2, $k = 2$, $\ell = 1$ and φ is smooth.

Corollary 5.4. *Let φ be a non-smooth skew morphism of the cyclic group $\mathbb{Z}_n$. If φ has skew-type 3, then it is conjugate to a skew morphism of the form*

$$\varphi(x) \equiv sx - \frac{n}{6}x(x-1) \pmod{n}, \qquad x \in \mathbb{Z}_n,$$

where $9 \mid n$, $s \in \mathbb{Z}_n^*$ has multiplicative order 2ℓ in $\mathbb{Z}_{n/3}$, $s \equiv -1 \pmod{3}$ and

$$\frac{3}{n}(s^{2\ell} - 1) - \ell \equiv w' \not\equiv 0 \pmod{3}.$$

Moreover, the order of φ is $m = 6\ell$ and the power function of φ is given by

$$\pi(x) \equiv 1 + \frac{m}{3}w'x \pmod{m}.$$

Proof. Since φ is a non-smooth skew morphism of $\mathbb{Z}_n$ of skew-type 3, the induced skew morphism $\overline{\varphi}$ of $\mathbb{Z}_n/\mathrm{Ker}\,\varphi$ is an automorphism of the form $\overline{\varphi} = (\overline{0})(\overline{1}, -\overline{1})$. By Lemma 4.3, φ^2 is an automorphism. The result then follows from Theorem 1.2. $\square$

By Theorem 1.2, we have the following special property of a square root of an automorphism of the cyclic group $\mathbb{Z}_n$.

Corollary 5.5. *Let φ be a proper square root of an automorphism of the cyclic group $\mathbb{Z}_n$. Then every subgroup of $\mathbb{Z}_n$ is φ-invariant.*

Proof. Let $H = \langle h \rangle$ be a subgroup of $\mathbb{Z}_n$. If φ and φ' are conjugate by an automorphism of $\mathbb{Z}_n$ and H is φ-invariant, then H is also φ'-invariant. So it suffices to consider the skew morphisms φ given by Theorem 1.2. Let k be the skew-type of φ. For any integer j,

$$\varphi(jh) \equiv sjh - \frac{jh(jh-1)n}{2k} \equiv h\left(sj - \frac{j(jh-1)n}{2k}\right) \pmod{n}.$$

If n is even, $\frac{n}{2k}$ is a positive integer, and if n is odd, then h is also odd and $\frac{j(jh-1)n}{2k}$ is a positive integer. This means that $\varphi(jh) \in H$, and hence H is φ-invariant. $\square$

6 The prime power case

In this section, for the case where $n = p^e$ is a prime power, we enumerate the conjugacy classes of proper square roots of automorphisms of $\mathbb{Z}_n$.

We need a technical result from number theory.

Proposition 6.1 ([3, 24]). *Suppose that $n = p^e$, where p is a prime and $e \geq 1$. Then*

(a) *if $p > 2$, then $\mathbb{Z}_{p^e}^* \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{e-1}}$ is cyclic of order $p^{e-1}(p-1)$. In particular, for each i, $1 \leq i \leq e-1$, an element of the form $1 + up^{e-i}$ in $\mathbb{Z}_{p^e}^*$ has order p^i if and only if $p \nmid u$,*

(b) *if $p = 2$, then $\mathbb{Z}_{2^e}^*$ is trivial if $e = 1$, $\mathbb{Z}_{2^e}^* \cong \mathbb{Z}_2$ if $e = 2$, and $\mathbb{Z}_{2^e}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$ if $e \geq 3$. In particular, in the last case for each i, $2 \leq i \leq e-1$, an element of the form $\pm 1 + u2^i$ in $\mathbb{Z}_{2^e}^*$ has order 2^{e-i} if and only if $2 \nmid u$.*

Let $N(p^e)$ denote the number of conjugacy classes of proper square roots of automorphisms of $\mathbb{Z}_{p^e}$. Then $N(p^e)$ is determined in the following theorem.

Theorem 6.2. *Suppose that p is a prime and $e \geq 1$. If $p \neq 2$, then*

$$N(p^e) = \begin{cases} \frac{1}{p-1}(p^{\frac{e}{2}} - 1)^2, & \text{if } e \text{ is even} \\ \frac{1}{p-1}(p^{\frac{e+1}{2}} - 1)(p^{\frac{e-1}{2}} - 1), & \text{if } e \text{ is odd,} \end{cases}$$

while if $p = 2$, then

$$N(2^e) = \begin{cases} 0, & \text{if } e < 3 \\ 1, & \text{if } e = 3 \\ 2^{e-1} - 3 \cdot 2^{\frac{e-2}{2}}, & \text{if } e > 3 \text{ is even} \\ 2^{e-1} - 2^{\frac{e+1}{2}}, & \text{if } e > 3 \text{ is odd.} \end{cases}$$

Proof. Denote $n = p^e$ and $k = p^f$. Then for fixed prime p and integer $e \geq 1$, by Theorem 1.2, $N(p^e)$ is equal to the number of pairs (f, s) which satisfy the following conditions:

(a) $2 \leq 2f \leq e$ and $s \in \mathbb{Z}_{p^e}^*$ if $p \neq 2$, and $2 \leq 2f \leq e-1$ and $s \in \mathbb{Z}_{2^{e-1}}^*$ if $p = 2$,

(b) $s \equiv -1 \pmod{p^f}$, s has multiplicative order 2ℓ in $\mathbb{Z}_{p^{e-f}}$ and $p \nmid w$, where

$$w = p^{f-e}(s^{2\ell} - 1) - \frac{1}{2}s(s-1)\ell.$$

For each admissible value of the parameter f, let $N(p^e, p^f)$ denote the number of admissible values of the parameter s. In what follows, we first determine $N(p^e, p^f)$, and then determine $N(p^e)$. We divide the proof into two cases according to the parity of p.

Case (A). $p \neq 2$.

Since $s \equiv -1 \pmod{p^f}$, we may write $s = tp^h - 1$ where $1 \leq f \leq h \leq e$ and $t \in \mathbb{Z}_{p^{e-h}}^*$. Then $s^2 = 1 + tp^h(tp^h - 2)$. According to the multiplicative order 2ℓ of s in $\mathbb{Z}_{p^{e-f}}$, we distinguish two subcases as follows.

If $h < e - f$, by Proposition 6.1 we have $\ell = p^{e-f-h}$. Since s has multiplicative ordr 2ℓ in $\mathbb{Z}_{p^{e-f}}$, we have $p^{e-f} \parallel s^{2\ell} - 1$. Since $p \mid \frac{1}{2}s(s-1)\ell$, we have $p \nmid w$.

If $h \geq e-f$, then $\ell = 1$. Recalling that $1 \leq f \leq h \leq e$, we have

$$w \equiv tp^{f+h-e}(tp^h - 2) - \frac{1}{2}(tp^h - 1)(tp^h - 2) \equiv -1 - 2tp^{f+h-e} \pmod{p}.$$

Thus, $p \mid w$ if and only if $h = e - f$ and $p \mid 1 + 2t$, where $t \in \mathbb{Z}^*_{p^f}$, in which case the number of such t is equal to p^{f-1}.

Consequently,

$$N(p^e, p^f) = \sum_{h=f}^{e} \phi(p^{e-h}) - p^{f-1} = 1 + \sum_{h=f}^{e-1} p^{e-h-1}(p-1) - p^{f-1} = p^{e-f} - p^{f-1},$$

where ϕ is the Euler's totient function. Therefore,

$$N(p^e) = \sum_{f=1}^{\lfloor e/2 \rfloor} N(p^e, p^f) = \sum_{f=1}^{\lfloor e/2 \rfloor} (p^{e-f} - p^{f-1}) = \frac{1}{p-1}(p^{\lfloor e/2 \rfloor} - 1)(p^{e-\lfloor e/2 \rfloor} - 1).$$

Note that $\lfloor e/2 \rfloor = e/2$ if e is even, and $\lfloor e/2 \rfloor = (e-1)/2$ if e is odd. The stated formula follows from substitution.

Case (B). $p = 2$.

It is straightforward to check that $N(2^2) = 0$, $N(2^3) = N(2^3, 2^1) = 1$ and $N(2^4) = N(2^4, 2^1) = 2$. In what follows, we assume $e \geq 5$ and distinguish two subcases.

Subcase (a). $s \equiv 1 \pmod{4}$.

Since $s \equiv -1 \pmod{2^f}$, we have $f = 1$. Since $s \in \mathbb{Z}^*_{2^{e-1}}$, we may write $s = 1 + 2^h t$ where $2 \leq h \leq e-2$ and $t \in \mathbb{Z}^*_{2^{e-h-1}}$. By Proposition 6.1 (b), s has multiplicative order 2^{e-h-1} in $\mathbb{Z}_{2^{e-1}}$, and so $\ell = 2^{e-h-2}$. We have $2 \nmid w$ since

$$2^{e-1} \parallel (s^{2\ell} - 1) \quad \text{and} \quad 2 \mid \frac{1}{2}s(s-1)\ell.$$

Subcase (b). $s \equiv -1 \pmod{4}$.

We may write $s = -1 + 2^h t$, where $2 \leq h \leq e-1$ and $t \in \mathbb{Z}^*_{2^{e-h-1}}$. Since $s \equiv -1 \pmod{2^f}$, we have $f \leq h$. Recall that s has multiplicative order 2ℓ in $\mathbb{Z}_{2^{e-f}}$.

If $h < e - f - 1$, then $e > f + h + 1 \geq 4$. By Proposition 6.1, s has multiplicative order 2^{e-f-h} in $\mathbb{Z}_{2^{e-f}}$, and hence $\ell = 2^{e-f-h-1}$. We also have $2 \nmid w$ since

$$2^{e-f} \parallel (s^{2\ell} - 1) \quad \text{and} \quad 2 \mid \frac{1}{2}s(s-1)\ell.$$

If $h \geq e - f - 1$, then $\ell = 1$ and hence

$$\begin{aligned} w &\equiv 2^{f-e}\big((-1+2^h t)^2 - 1\big) - (-1+2^h t)(-1+2^{h-1}t) \\ &\equiv (-1+2^{h-1}t)(2^{f-e+h+1}t - 2^h t + 1) \\ &\equiv 2^{f-e+h+1}t + 1 \pmod{2}. \end{aligned}$$

It follows that $2 \nmid w$ if and only if $h > e - f - 1$. Therefore the case $h = e - f - 1$ should be excluded.

From the above discussion, we obtain

$$N(2^e, 2^1) = \sum_{h=2}^{e-2} \phi(2^{e-h-1}) + \sum_{h=2}^{e-1} \phi(2^{e-h-1}) - \phi(2) = 2^{e-2} - 2,$$

and for $f > 1$,

$$N(2^e, 2^f) = \sum_{h=f}^{e-f-2} \phi(2^{e-h-1}) + \sum_{h=e-f}^{e-1} \phi(2^{e-h-1}) = 2^{e-f-1} - 2^{f-1}.$$

Consequently, for $e \geq 5$, we get

$$\begin{aligned} N(2^e) = \sum_{f=1}^{\lfloor \frac{e-1}{2} \rfloor} N(2^e, 2^f) &= 2^{e-2} - 2 + \sum_{f=2}^{\lfloor \frac{e-1}{2} \rfloor} (2^{e-f-1} - 2^{f-1}) \\ &= 2^{e-2} - 2 + (2^{\lfloor \frac{e-1}{2} \rfloor - 1} - 1)(2^{e-1-\lfloor \frac{e-1}{2} \rfloor)} - 2). \end{aligned}$$

Note that $\lfloor \frac{e-1}{2} \rfloor = (e-2)/2$ if e if even, and $\lfloor \frac{e-1}{2} \rfloor = (e-1)/2$ if e is odd. The result follows from substitution for $\lfloor \frac{e-1}{2} \rfloor$ in the above formula, as required. □

Remark 6.3. By Theorem 1.2, one can enumerate the conjugacy classes of proper square roots of automorphisms of $\mathbb{Z}_n$ for any positive integer n in the following steps:

(a) Find the set of all positive integers k satisfying that k^2 divides n if k is odd, and $2k^2$ divides n if k is even. Denote this set by $A(n)$.

(b) For any $k \in A(n)$, find the set of all s satisfying (i) $s \equiv -1 \pmod{k}$ and (ii) $s \in \mathbb{Z}_n^*$ if k is odd, and $s \in \mathbb{Z}_{n/2}^*$ if k is even. Denote this set by $S(n, k)$.

(c) For any $s \in S(n, k)$, calculate the smallest positive integer ℓ such that $s^{2\ell} \equiv 1 \pmod{n/k}$ and check whether $\frac{k}{n}(s^{2\ell} - 1) - \frac{1}{2}s(s-1)\ell$ is coprime to k or not. Let $A(n, k)$ be the set of all $s \in S(n, k)$ satisfying that $\frac{k}{n}(s^{2\ell} - 1) - \frac{1}{2}s(s-1)\ell$ is coprime to k.

(d) Now (k, s) is admissible for proper square root of automorphism of $\mathbb{Z}_n$ if and only if $k \in A(n)$ and $s \in A(n, k)$. The number $N(n)$ of the conjugacy classes of proper square roots of automorphisms of $\mathbb{Z}_n$ is $\sum_{k \in A(n)} |A(n, k)|$.

Using the method above, we obtain $N(18) = 2$, $N(24) = 2$, $N(40) = 2$ and $N(72) = 16$. In each case the parameters (n, k, s) are given below (details are omitted):

(n, k)	$(18, 3)$	$(24, 2)$	$(40, 2)$	$(72, 2)$	$(72, 3)$	$(72, 6)$
s	$11, 17$	$7, 11$	$11, 19$	$7, 11, 19, 23, 31, 35$	$11, 17, 29, 35, 47, 53, 65, 71$	$23, 35$

We close the paper by attaching a full list of conjugacy classes of proper square roots of automorphisms of $\mathbb{Z}_n$ for some small values of n.

Table 1: Proper square roots of automorphisms of $\mathbb{Z}_n$.

n	$\varphi(x)$	$\pi(x)$	$\varphi^2(x)$
8	$6x^2+5x \pmod 8$	$1+2x \pmod 4$	$5x \pmod 8$
9	$3x^2+2x \pmod 9$	$1+2x \pmod 6$	$4x \pmod 9$
9	$3x^2+4x \pmod 9$	$1+2x \pmod 6$	$4x \pmod 9$
16	$12x^2+9x \pmod{16}$	$1+2x \pmod 4$	$9x \pmod{16}$
16	$12x^2+11x \pmod{16}$	$1+2x \pmod 4$	$9x \pmod{16}$
18	$15x^2+2x \pmod{18}$	$1+2x \pmod 6$	$13x \pmod{18}$
18	$15x^2+14x \pmod{18}$	$1+2x \pmod 6$	$7x \pmod{18}$
24	$18x^2+13x \pmod{24}$	$1+2x \pmod 4$	$23x \pmod{24}$
24	$18x^2+17x \pmod{24}$	$1+2x \pmod 4$	$13x \pmod{24}$
27	$9x^2+2x \pmod{27}$	$1+6x \pmod{18}$	$4x \pmod{27}$
27	$9x^2+5x \pmod{27}$	$1+6x \pmod{18}$	$25x \pmod{27}$
27	$9x^2+8x \pmod{27}$	$1+2x \pmod 6$	$10x \pmod{27}$
27	$9x^2+11x \pmod{27}$	$1+6x \pmod{18}$	$13x \pmod{27}$
27	$9x^2+14x \pmod{27}$	$1+12x \pmod{18}$	$7x \pmod{27}$
27	$9x^2+17x \pmod{27}$	$1+4x \pmod 6$	$19x \pmod{27}$
27	$9x^2+20x \pmod{27}$	$1+6x \pmod{18}$	$22x \pmod{27}$
27	$9x^2+23x \pmod{27}$	$1+12x \pmod{18}$	$16x \pmod{27}$
32	$24x^2+11x \pmod{32}$	$1+4x \pmod 8$	$25x \pmod{32}$
32	$24x^2+13x \pmod{32}$	$1+4x \pmod 8$	$25x \pmod{32}$
32	$24x^2+17x \pmod{32}$	$1+2x \pmod 4$	$17x \pmod{32}$
32	$24x^2+19x \pmod{32}$	$1+4x \pmod 8$	$9x \pmod{32}$
32	$24x^2+21x \pmod{32}$	$1+4x \pmod 8$	$9x \pmod{32}$
32	$24x^2+23x \pmod{32}$	$1+2x \pmod 4$	$17x \pmod{32}$
32	$28x^2+11x \pmod{32}$	$1+2x \pmod 8$	$9x \pmod{32}$
32	$28x^2+19x \pmod{32}$	$1+6x \pmod 8$	$25x \pmod{32}$
40	$30x^2+21x \pmod{40}$	$1+2x \pmod 4$	$31x \pmod{40}$
40	$30x^2+29x \pmod{40}$	$1+2x \pmod 4$	$21x \pmod{40}$
64	$48x^2+19x \pmod{64}$	$1+8x \pmod{16}$	$41x \pmod{64}$
64	$48x^2+21x \pmod{64}$	$1+8x \pmod{16}$	$25x \pmod{64}$
64	$48x^2+23x \pmod{64}$	$1+4x \pmod 8$	$17x \pmod{64}$
64	$48x^2+25x \pmod{64}$	$1+4x \pmod 8$	$17x \pmod{64}$
64	$48x^2+27x \pmod{64}$	$1+8x \pmod{16}$	$25x \pmod{64}$
64	$48x^2+29x \pmod{64}$	$1+8x \pmod{16}$	$41x \pmod{64}$
64	$48x^2+33x \pmod{64}$	$1+2x \pmod 4$	$33x \pmod{64}$
64	$48x^2+35x \pmod{64}$	$1+8x \pmod{16}$	$9x \pmod{64}$
64	$48x^2+37x \pmod{64}$	$1+4x \pmod{16}$	$57x \pmod{64}$
64	$48x^2+39x \pmod{64}$	$1+4x \pmod 8$	$49x \pmod{64}$
64	$48x^2+41x \pmod{64}$	$1+4x \pmod 8$	$49x \pmod{64}$
64	$48x^2+43x \pmod{64}$	$1+8x \pmod{16}$	$57x \pmod{64}$
64	$48x^2+45x \pmod{64}$	$1+8x \pmod{16}$	$9x \pmod{64}$
64	$48x^2+47x \pmod{64}$	$1+2x \pmod 4$	$33x \pmod{64}$
64	$56x^2+11x \pmod{64}$	$1+12x \pmod{16}$	$25x \pmod{64}$
64	$56x^2+19x \pmod{64}$	$1+4x \pmod{16}$	$9x \pmod{64}$
64	$56x^2+23x \pmod{64}$	$1+2x \pmod 8$	$17x \pmod{64}$
64	$56x^2+27x \pmod{64}$	$1+12x \pmod{16}$	$57x \pmod{64}$
64	$56x^2+35x \pmod{64}$	$1+4x \pmod{16}$	$41x \pmod{64}$
64	$56x^2+39x \pmod{64}$	$1+6x \pmod 8$	$49x \pmod{64}$

ORCID iDs

Kan Hu https://orcid.org/0000-0003-4775-7273
Young Soo Kwon https://orcid.org/0000-0002-1765-0806
Jun-Yang Zhang https://orcid.org/0000-0002-0871-2059

References

[1] M. Bachratý and R. Jajcay, Powers of skew-morphisms, in: *Symmetries in Graphs, Maps, and Polytopes*, Springer International Publishing, volume 159, pp. 1–25, 2016, doi:10.1007/978-3-319-30451-9.

[2] M. Bachratý and R. Jajcay, Classification of coset-preserving skew-morphisms of finite cyclic groups, *Australas. J. Comb.* **67** (2017), 259–280, `https://ajc.maths.uq.edu.au/?page=get_volumes&volume=67`.

[3] B. G. Basmaji, On the ismorphisms of two metacyclic groups, *Proc. Amer. Math. Soc.* **22** (1969), 175–182, doi:10.2307/2036947.

[4] M. Conder, R. Jajcay and T. Tucker, Regular Cayley maps for finite abelian groups, *J. Algebraic Combin.* **25** (2007), 259–283, doi:10.1007/s10801-006-0037-0.

[5] M. Conder, R. Jajcay and T. Tucker, Regular t-balanced Cayley maps, *J. Combin. Theory Ser. B* **97** (2007), 453–473, doi:10.1016/j.jctb.2006.07.008.

[6] M. D. E. Conder, R. Jajcay and T. W. Tucker, Cyclic complements and skew morphisms of groups, *J. Algebra* **453** (2016), 68–100, doi:10.1016/j.jalgebra.2015.12.024.

[7] M. D. E. Conder, Y. S. Kwon and J. Širáň, Reflexibility of regular Cayley maps for abelian groups, *J. Combin. Theory Ser. B* **99** (2009), 254–260, doi:10.1016/j.jctb.2008.07.002.

[8] M. D. E. Conder and T. W. Tucker, Regular Cayley maps for cyclic groups, *Trans. Amer. Math. Soc.* **366** (2014), 3585–3609, doi:10.1090/s0002-9947-2014-05933-3.

[9] S. Du and K. Hu, Skew-morphisms of cyclic 2-groups, *J. Group Theory* **22** (2019), 617–635, doi:10.1515/jgth-2019-2046.

[10] R. Feng, R. Jajcay and Y. Wang, Regular t-balanced Cayley maps for abelian groups, *Discrete Math.* **311** (2011), 2309–2316, doi:10.1016/j.disc.2011.04.012.

[11] Y.-Q. Feng, K. Hu, R. Nedela, M. Škoviera and N.-E. Wang, Complete regular dessins and skew-morphisms of cyclic groups, *Ars Math. Contemp.* **18** (2020), 289–307, doi:10.26493/1855-3974.1748.ebd.

[12] K. Hu, R. Nedela and N.-E. Wang, Nilpotent groups of class two which underly a unique regular dessin, *Geom. Dedicata* **179** (2015), 177–186, doi:10.1007/s10711-015-0074-8.

[13] R. Jajcay and J. Širáň, Skew-morphisms of regular Cayley maps, *Discrete Math.* **244** (2002), 167–179, doi:10.1016/s0012-365x(01)00081-4.

[14] I. Kovács and Y. S. Kwon, Regular Cayley maps on dihedral groups with the smallest kernel, *J. Algebraic Combin.* **44** (2016), 831–847, doi:10.1007/s10801-016-0689-3.

[15] I. Kovács and Y. S. Kwon, Classification of reflexible Cayley maps for dihedral groups, *J. Combin. Theory Ser. B* **127** (2017), 187–204, doi:10.1016/j.jctb.2017.06.002.

[16] I. Kovács and Y. S. Kwon, Regular Cayley maps for dihedral groups, *J. Comb. Theory Ser. B* **148** (2021), 84–124, doi:10.1016/j.jctb.2020.12.002.

[17] I. Kovács and R. Nedela, Decomposition of skew-morphisms of cyclic groups, *Ars Math. Contemp.* **4** (2011), 329–349, doi:10.26493/1855-3974.157.fc1.

[18] I. Kovács and R. Nedela, Skew-morphisms of cyclic p-groups, *J. Group Theory* **20** (2017), 1135–1154, doi:10.1515/jgth-2017-0015.

[19] J. H. Kwak, Y. S. Kwon and R. Feng, A classification of regular t-balanced Cayley maps on dihedral groups, *European J. Combin.* **27** (2006), 382–393, doi:10.1016/j.ejc.2004.12.002.

[20] J. H. Kwak and J.-M. Oh, A classification of regular t-balanced Cayley maps on dicyclic groups, *European J. Combin.* **29** (2008), 1151–1159, doi:10.1016/j.ejc.2007.06.023.

[21] Y. S. Kwon, A classification of regular t-balanced Cayley maps for cyclic groups, *Discrete Math.* **313** (2013), 656–664, doi:10.1016/j.disc.2012.12.012.

[22] J.-M. Oh, Regular t-balanced Cayley maps on semi-dihedral groups, *J. Combin. Theory Ser. B* **99** (2009), 480–493, doi:10.1016/j.jctb.2008.09.006.

[23] N.-E. Wang, K. Hu, K. Yuan and J.-Y. Zhang, Smooth skew morphisms of dihedral groups, *Ars Math. Contemp.* **16** (2019), 527–547, doi:10.26493/1855-3974.1475.3d3.

[24] M. Xu and Q. Zhang, A classification of metacyclic 2-groups, *Algebra Colloq.* **13** (2006), 25–34, doi:10.1142/s1005386706000058.

[25] K. Yuan, Y. Wang and J. H. Kwak, Enumeration of skew-morphisms of groups of small orders and their corresponding Cayley maps, *Adv. Math. (China)* **45** (2016), 21–36, doi:10.1103/physrevd.45.21.

[26] J.-Y. Zhang, Regular Cayley maps of skew-type 3 for abelian groups, *European J. Combin.* **39** (2014), 198–206, doi:10.1016/j.ejc.2014.01.006.

[27] J.-Y. Zhang, A classification of regular Cayley maps with trivial Cayley-core for dihedral groups, *Discrete Math.* **338** (2015), 1216–1225, doi:10.1016/j.disc.2015.01.036.

[28] J.-Y. Zhang, Regular Cayley maps of skew-type 3 for dihedral groups, *Discrete Math.* **338** (2015), 1163–1172, doi:10.1016/j.disc.2015.01.038.

[29] J.-Y. Zhang and S. Du, On the skew-morphisms of dihedral groups, *J. Group Theory* **19** (2016), 993–1016, doi:10.1515/jgth-2016-0027.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.02 / 175–200
https://doi.org/10.26493/1855-3974.2373.c02
(Also available at http://amc-journal.eu)

Trivalent dihedrants and bi-dihedrants*

Mi-Mi Zhang

School of Mathematical Sciences, Hebei Normal University, Shijiazhuang, 050024, China

Jin-Xin Zhou †

Department of Mathematics, Beijing Jiaotong University, Beijing, 100044, China

Received 3 July 2020, accepted 22 February 2021, published online 21 October 2021

Abstract

A Cayley (resp. bi-Cayley) graph on a dihedral group is called a *dihedrant* (resp. *bi-dihedrant*). In 2000, a classification of trivalent arc-transitive dihedrants was given by Marušič and Pisanski, and several years later, trivalent non-arc-transitive dihedrants of order $4p$ or $8p$ (p a prime) were classified by Feng et al. As a generalization of these results, our first result presents a classification of trivalent non-arc-transitive dihedrants. Using this, a complete classification of trivalent vertex-transitive non-Cayley bi-dihedrants is given, thus completing the study of trivalent bi-dihedrants initiated in our previous paper [Discrete Math. 340 (2017) 1757–1772]. As a by-product, we generalize a theorem in [The Electronic Journal of Combinatorics 19 (2012) #P53].

Keywords: Cayley graph, non-Cayley, bi-Cayley, dihedral group, dihedrant, bi-dihedrant.

Math. Subj. Class. (2020): 05C25, 20B25

1 Introduction

In this paper we describe an investigation of trivalent Cayley graphs on dihedral groups as well as vertex-transitive trivalent bi-Cayley graphs over dihedral groups. To be brief, we shall say that a Cayley (resp. bi-Cayley) graph on a dihedral group a *dihedrant* (resp. *bi-dihedrant*).

Cayley graphs are usually defined in the following way. Given a finite group G and an inverse closed subset $S \subseteq G \setminus \{1\}$, the *Cayley graph* $\mathrm{Cay}(G, S)$ on G with respect to S is a graph with vertex set G and edge set $\{\{g, sg\} \mid g \in G, s \in S\}$. For any $g \in G$, $R(g)$ is the

*This work was supported by the National Natural Science Foundation of China (11671030, 12101181) and the Natural Science Foundation of Hebei Province (A2019205180)

†Corresponding author.
E-mail addresses: mmzhang@hebtu.edu.cn (Mi-Mi Zhang), jxzhou@bjtu.edu.cn (Jin-Xin Zhou)

permutation of G defined by $R(g) : x \mapsto xg$ for $x \in G$. Set $R(G) := \{R(g) \mid g \in G\}$. It is well-known that $R(G)$ is a subgroup of $\mathrm{Aut}\,(\mathrm{Cay}(G, S))$. We say that the Cayley graph $\mathrm{Cay}(G, S)$ is *normal* if $R(G)$ is normal in $\mathrm{Aut}\,(\mathrm{Cay}(G, S))$ (see [19]).

In 2000, Marušič and Pisanski [13] initiated the study of automorphisms of dihedrants, and they gave a classification of trivalent arc-transitive dihedrants. Following this work, highly symmetrical dihedrants have been extensively studied, and one of the remarkable achievements is the complete classification of 2-arc-transitive dihedrants (see [7, 12]). In contrast, however, relatively little is known about the automorphisms of non-arc-transitive dihedrants. In [1], the authors claimed that every trivalent non-arc-transitive dihedrant is normal. However, this is not true. There exist non-arc-transitive and non-normal dihedrants. Actually, in [22, 26], the automorphism groups of trivalent dihedrants of order $4p$ and $8p$ are determined for each prime p, and the result reveals that every non-arc-transitive trivalent dihedrant of order $4p$ or $8p$ is either a normal Cayley graph, or isomorphic to the so-called cross ladder graph. For an integer $m \geq 2$, the *cross ladder graph*, denoted by CL_{4m}, is a trivalent graph of order $4m$ with vertex set $V_0 \cup V_1 \cup \ldots V_{2m-2} \cup V_{2m-1}$, where $V_i = \{x_i^0, x_i^1\}$, and edge set $\{\{x_{2i}^r, x_{2i+1}^r\}, \{x_{2i+1}^r, x_{2i+2}^s\} \mid i \in \mathbb{Z}_m, r, s \in \mathbb{Z}_2\}$ (see Fig. 1 for CL_{4m}). It is worth mentioning that the cross ladder graph plays an important role in the

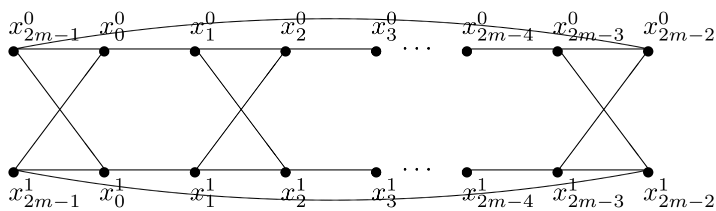


Figure 1: The cross ladder graph CL_{4m}

study of automorphisms of trivalent graphs (see, for example, [5, 21, 26]). Motivated by the above mentioned facts, we shall focus on trivalent non-arc-transitive dihedrants. Our first theorem generalizes the results in [22, 26] to all trivalent dihedrants.

Theorem 1.1. *Let* $\Sigma = \mathrm{Cay}(H, S)$ *be a connected trivalent Cayley graph, where* $H = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1}\rangle (n \geq 3)$. *If* Σ *is non-arc-transitive and non-normal, then* n *is even and* $\Sigma \cong \mathrm{CL}_{4\cdot\frac{n}{2}}$ *and* $S^\alpha = \{b, ba, ba^{\frac{n}{2}}\}$ *for some* $\alpha \in \mathrm{Aut}\,(H)$.

Recall that for an integer $m \geq 2$, the cross ladder graph CL_{4m} has vertex set $V_0 \cup V_1 \cup \ldots V_{2m-2} \cup V_{2m-1}$, where $V_i = \{x_i^0, x_i^1\}$. The *multi-cross ladder graph*, denoted by $\mathrm{MCL}_{4m,2}$, is the graph obtained from CL_{4m} by blowing up each vertex x_i^r of CL_{4m} into two vertices $x_i^{r,0}$ and $x_i^{r,1}$. The edge set is $\{\{x_{2i}^{r,s}, x_{2i+1}^{r,t}\}, \{x_{2i+1}^{r,s}, x_{2i+2}^{s,r}\} \mid i \in \mathbb{Z}_m, r, s, t \in \mathbb{Z}_2\}$ (see Fig. 2 for $\mathrm{MCL}_{20,2}$).

Note that the multi-cross ladder graph $\mathrm{MCL}_{4m,2}$ is just the graph given in [23, Definition 7]. From [6, Proposition 3.3] we know that every $\mathrm{MCL}_{4m,2}$ is vertex-transitive. However, not all multi-cross ladder graphs are Cayley graphs. Actually, in [23, Theorem 9], it is proved that $\mathrm{MCL}_{4p,2}$ is a vertex-transitive non-Cayley graph for each prime $p > 7$. Our second theorem generalizes this result to all multi-cross ladder graphs.

Theorem 1.2. *The multi-cross ladder graph* $\mathrm{MCL}_{4m,2}$ *is a Cayley graph if and only if either* m *is even, or* m *is odd and* $3 \mid m$.

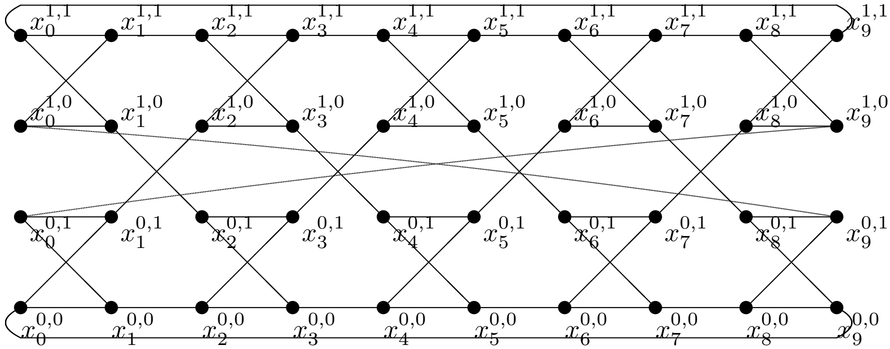


Figure 2: The multi-cross ladder graph $\mathrm{MCL}_{20,2}$

Both of the above two theorems are crucial in attacking the problem of classification of trivalent vertex-transitive non-Cayley bi-dihedrants. Before proceeding, we give some background to this topic, and set some notation.

Let R, L and S be subsets of a group H such that $R = R^{-1}$, $L = L^{-1}$ and $R \cup L$ does not contain the identity element of H. The *bi-Cayley graph* $\mathrm{BiCay}(H, R, L, S)$ over H relative to R, L, S is a graph having vertex set the union of the *right part* $H_0 = \{h_0 \mid h \in H\}$ and the *left part* $H_1 = \{h_1 \mid h \in H\}$, and edge set the union of the *right edges* $\{\{h_0, g_0\} \mid gh^{-1} \in R\}$, the *left edges* $\{\{h_1, g_1\} \mid gh^{-1} \in L\}$ and the *spokes* $\{\{h_0, g_1\} \mid gh^{-1} \in S\}$. If $|R| = |L| = s$, then $\mathrm{BiCay}(H,\ R,\ L,\ S)$ is said to be an *s-type bi-Cayley graph.*

In [20] we initiated a program to investigate the automorphism groups of the trivalent vertex-transitive bi-dihedrants. This was partially motivated by the following facts. As one of the most important finite graphs, the Petersen graph is a bi-circulant, but it is not a Cayley graph. Note that a *bi-circulant* is a bi-Cayley graph over a cyclic group. The Petersen graph is the initial member of a family of graphs $P(n, t)$, known now as the *generalized Petersen graphs* (see [17]), which can be also constructed as bi-circulants. Let $n \geq 3$, $1 \leq t < n/2$ and set $H = \langle a \rangle \cong \mathbb{Z}_n$. The generalized Petersen graph $P(n, t)$ is isomorphic to the bi-circulant $\mathrm{BiCay}(H,\ \{a, a^{-1}\},\ \{a^t, a^{-t}\},\ \{1\})$. The complete classification of vertex-transitive generalized Petersen graphs has been worked out in [8, 14]. Latter, this was generalized by Marušič et al. in [13, 15] where all trivalent vertex-transitive bi-circulants were classified, and more recently, all trivalent vertex-transitive bi-Cayley graphs over abelian groups were classified in [24]. The characterization of trivalent vertex-transitive bi-dihedrants is the next natural step.

Another motivation for us to consider trivalent vertex-transitive bi-dihedrants comes from the excellent work in a highly cited article [16], where the authors give a census of trivalent vertex-transitive graphs of order up to 1280. This is very important in the study of trivalent vertex-transitive graphs. Actually, by checking this census of graphs of order up to 1000, we find out that there are 981 non-Cayley graphs, and among these graphs, 233 graphs are non-Cayley bi-dihedrants. This may suggest bi-dihedrants form an important class of trivalent vertex-transitive non-Cayley graphs.

In [20], we gave a classification of trivalent arc-transitive bi-dihedrants, and we also proved that every trivalent vertex-transitive 0- or 1-type bi-dihedrant is a Cayley graph, and gave a classification of trivalent vertex-transitive non-Cayley bi-dihedrants of order $4n$ with

n odd. The goal of this paper is to complete the classification of trivalent vertex-transitive non-Cayley bi-dihedrants.

Before stating the main result, we need the following concepts. For a bi-Cayley graph $\Gamma = \mathrm{BiCay}(H,\ R,\ L,\ S)$ over a group H, we can assume that the identity 1 of H is in S (see Proposition 2.3 (2)). The triple (R, L, S) of three subsets R, L, S of a group H is called *bi-Cayley triple* if $R = R^{-1}, L = L^{-1}$, and $1 \in S$. Two bi-Cayley triples (R, L, S) and (R', L', S') of a group H are said to be *equivalent*, denoted by $(R, L, S) \equiv (R', L', S')$, if either $(R', L', S') = (R, L, S)^\alpha$ or $(R', L', S') = (L, R, S^{-1})^\alpha$ for some automorphism α of H. The bi-Cayley graphs corresponding to two equivalent bi-Cayley triples of the same group are isomorphic (see Proposition 2.3 (3)-(4)).

Theorem 1.3. *Let* $\Gamma = \mathrm{BiCay}(R, L, S)$ *be a trivalent vertex-transitive bi-dihedrant where* $H = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1}\rangle$ *is a dihedral group. Then either* Γ *is a Cayley graph or one of the following occurs:*

(1) $(R, L, S) \equiv (\{b,\ ba\}, \{a,\ a^{-1}\}, \{1\})$, *where* $n = 5$.

(2) $(R, L, S) \equiv (\{b,\ ba^{\ell+1}\}, \{ba,\ ba^{\ell^2+\ell+1}\}, \{1\})$, *where* $n \geq 5$, $\ell^3 + \ell^2 + \ell + 1 \equiv 0 \pmod n$, $\ell^2 \not\equiv 1 \pmod n$.

(3) $(R, L, S) \equiv (\{ba^{-\ell},\ ba^{\ell}\}, \{a,\ a^{-1}\}, \{1\})$, *where* $n = 2m$ *and* $\ell^2 \equiv -1 \pmod m$. *Furthermore,* Γ *is also a bi-Cayley graph over an abelian group* $\mathbb{Z}_n \times \mathbb{Z}_2$.

(4) $(R, L, S) \equiv (\{b, ba\}, \{b, ba^{2m}\}, \{1\})$, *where* $n = 2(2m + 1)$, $m \not\equiv 1 \pmod 3$, *and the corresponding graph is isomorphic the multi-cross ladder graph* $\mathrm{MCL}_{4m,2}$.

(5) $(R, L, S) \equiv (\{b, ba\}, \{ba^{24\ell}, ba^{12\ell-1}\}, \{1\})$, *where* $n = 48\ell$ *and* $\ell \geq 1$.

Moreover, all of the graphs arising from (1)-(4) *are vertex-transitive non-Cayley.*

2 Preliminaries

All groups considered in this paper are finite, and all graphs are finite, connected, simple and undirected. For the group-theoretic and graph-theoretic terminology not defined here we refer the reader to [3, 18].

2.1 Definitions and notations

For a positive integer, let $\mathbb{Z}_n$ be the cyclic group of order n and $\mathbb{Z}_n^*$ be the multiplicative group of $\mathbb{Z}_n$ consisting of numbers coprime to n. For two groups M and N, $N \rtimes M$ denotes a semidirect product of N by M. For a subgroup H of a group G, denote $C_G(H)$ the centralizer of H in G and by $N_G(H)$ the normalizer of H of G. Let G be a permutation group on a set Ω and $\alpha \in \Omega$. Denote by G_α the stabilizer of α in G. We say that G is *semiregular* on Ω if $G_\alpha = 1$ for every $\alpha \in \Omega$ and *regular* if G is transitive and semiregular.

For a finite, simple and undirected graph Γ, we use $V(\Gamma)$, $E(\Gamma)$, $A(\Gamma)$, $\mathrm{Aut}\,(\Gamma)$ to denote its vertex set, edge set, arc set and full automorphism group, respectively. For any subset B of $V(\Gamma)$, the subgraph of Γ induced by B will be denoted by $\Gamma[B]$. For any $v \in V(\Gamma)$ and a positive integer i no more than the diameter of Γ, denote by $\Gamma_i(v)$ be the set of vertices at distance i from v. Clearly, $\Gamma_1(v)$ is just the neighborhood of v. We shall often abuse the notation by using $\Gamma(v)$ to replace $\Gamma_1(v)$.

A graph Γ is said to be *vertex-transitive*, and *arc-transitive* (or *symmetric*) if $\mathrm{Aut}\,(\Gamma)$ acts transitively on $V(\Gamma)$ and $A(\Gamma)$, respectively. Let Γ be a connected vertex-transitive graph, and let $G \leq \text{Aut}(\Gamma)$ be vertex-transitive on Γ. For a G-invariant partition $\mathcal{B}$ of $V(\Gamma)$, the *quotient graph* $\Gamma_{\mathcal{B}}$ is defined as the graph with vertex set $\mathcal{B}$ such that, for any two different vertices $B, C \in \mathcal{B}$, B is adjacent to C if and only if there exist $u \in B$ and $v \in C$ which are adjacent in Γ. Let N be a normal subgroup of G. Then the set $\mathcal{B}$ of orbits of N in $V(\Gamma)$ is a G-invariant partition of $V(\Gamma)$. In this case, the symbol $\Gamma_{\mathcal{B}}$ will be replaced by Γ_N. The original graph Γ is said to be a N*-cover* of Γ_N if Γ and Γ_N have the same valency.

2.2 Cayley graphs

Let $\Gamma = \text{Cay}(G, S)$ be a Cayley graph on G with respect to S. Then Γ is vertex-transitive due to $R(G) \leq \text{Aut}(\Gamma)$. In general, we have the following proposition.

Proposition 2.1 ([2, Lemma 16.3])**.** *A vertex-transitive graph Γ is isomorphic to a Cayley graph on a group G if and only if its automorphism group has a subgroup isomorphic to G, acting regularly on the vertex set of Γ.*

In 1981, Godsil [9] proved that the normalizer of $R(G)$ in $\text{Aut}(\text{Cay}(G, S))$ is $R(G) \rtimes \text{Aut}(G, S)$, where $\text{Aut}(G, S)$ is the group of automorphisms of G fixing the set S setwise. This result has been successfully used in characterizing various families of Cayley graphs $\text{Cay}(G, S)$ such that $R(G) = \text{Aut}(\text{Cay}(G, S))$ (see, for example, [9, 10]). Recall that a Cayley graph $\text{Cay}(G, S)$ is said to be *normal* if $R(G)$ is normal in $\text{Aut}(\text{Cay}(G, S))$ (see [19]).

Proposition 2.2 ([19, Proposition 1.5])**.** *The Cayley graph $\Gamma = \text{Cay}(G, S)$ is normal if and only if $A_1 = \text{Aut}(G, S)$, where A_1 is the stabilizer of the identity 1 of G in $\text{Aut}(\Gamma)$.*

2.3 Basic properties of bi-Cayley graphs

In this subsection, we let Γ be a connected bi-Cayley graph $\text{BiCay}(H, R, L, S)$ over a group H. It is easy to prove some basic properties of such a Γ, as in [24, Lemma 3.1].

Proposition 2.3. *The following hold.*

(1) *H is generated by $R \cup L \cup S$.*

(2) *Up to graph isomorphism, S can be chosen to contain the identity of H.*

(3) *For any automorphism α of H,* $\text{BiCay}(H,\ R,\ L,\ S) \cong \text{BiCay}(H,\ R^\alpha,\ L^\alpha,\ S^\alpha)$.

(4) $\text{BiCay}(H,\ R,\ L,\ S) \cong \text{BiCay}(H,\ L,\ R,\ S^{-1})$.

Next, we collect several results about the automorphisms of bi-Cayley graph $\Gamma = \text{BiCay}(H,\ R,\ L,\ S)$. For each $g \in H$, define a permutation as follows:

$$\mathcal{R}(g) : h_i \mapsto (hg)_i, \quad \forall i \in \mathbb{Z}_2,\ h \in H. \tag{2.1}$$

Set $\mathcal{R}(H) = \{\mathcal{R}(g) \mid g \in H\}$. Then $\mathcal{R}(H)$ is a semiregular subgroup of $\text{Aut}(\Gamma)$ with H_0 and H_1 as its two orbits.

For an automorphism α of H and $x, y, g \in H$, define two permutations of $V(\Gamma) = H_0 \cup H_1$ as follows:

$$\begin{aligned} \delta_{\alpha,x,y} &: \ h_0 \mapsto (xh^\alpha)_1,\ h_1 \mapsto (yh^\alpha)_0,\ \forall h \in H, \\ \sigma_{\alpha,g} &: \ h_0 \mapsto (h^\alpha)_0,\ h_1 \mapsto (gh^\alpha)_1,\ \forall h \in H. \end{aligned} \tag{2.2}$$

Set

$$\begin{aligned} I &= \{\delta_{\alpha,x,y} \mid \alpha \in \text{Aut}(H) \ s.t.\ R^\alpha = x^{-1}Lx,\ L^\alpha = y^{-1}Ry,\ S^\alpha = y^{-1}S^{-1}x\}, \\ F &= \{\sigma_{\alpha,g} \mid \alpha \in \text{Aut}(H) \ s.t.\ R^\alpha = R,\ L^\alpha = g^{-1}Lg,\ S^\alpha = g^{-1}S\}. \end{aligned} \tag{2.3}$$

Proposition 2.4 ([25, Theorem 1.1])**.** *Let $\Gamma = \text{BiCay}(H, R, L, S)$ be a connected bi-Cayley graph over the group H. Then $N_{\text{Aut}(\Gamma)}(\mathcal{R}(H)) = \mathcal{R}(H) \rtimes F$ if $I = \emptyset$ and $N_{\text{Aut}(\Gamma)}(\mathcal{R}(H)) = \mathcal{R}(H)\langle F,\ \delta_{\alpha,x,y}\rangle$ if $I \neq \emptyset$ and $\delta_{\alpha,x,y} \in I$. Furthermore, for any $\delta_{\alpha,x,y} \in I$, we have the following:*

(1) *$\langle \mathcal{R}(H),\ \delta_{\alpha,x,y}\rangle$ acts transitively on $V(\Gamma)$;*

(2) *if α has order 2 and $x = y = 1$, then Γ is isomorphic to the Cayley graph Cay($\bar{H}$, $R \cup \alpha S$), where $\bar{H} = H \rtimes \langle \alpha \rangle$.*

3 Cross ladder graphs

The goal of this section is to prove Theorem 1.1.

Proof of Theorem 1.1. Suppose that $\Sigma = \text{Cay}(H, S)$ is a connected trivalent Cayley graph which is neither normal nor arc-transitive, where $H = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1}\rangle (n \geq 3)$. Then S is a generating subset of H and $|S| = 3$. So S must contain an involution of H outside $\langle a\rangle$. As $\text{Aut}(H)$ is transitive on the coset $b\langle a\rangle$, we may assume that $S = \{b, x, y\}$ for $x, y \in H \setminus \langle b\rangle$.

Suppose first that x is not an involution. Then we must have $y = x^{-1}$. Since S generates H, one has $\langle a\rangle = \langle x\rangle$, and so $bxb = x^{-1}$. Then there exists an automorphism of H sending b, x to b, a respectively. So we may assume that $S = \{b, a, a^{-1}\}$. Now it is easy to check that Σ is isomorphic to the generalized Petersen graph $P(n, 1)$. Since Σ is not arc-transitive, by [8, 14], we have $|\text{Aut}(\Sigma)| = 2|H|$, and so Σ would be a normal Cayley graph of H, a contradiction.

Therefore, both x and y must be involutions. Suppose that $x \in \langle a\rangle$. Then n is even and $x = a^{n/2}$. Again since S generates H, one has $y = ba^j$, where $1 \leq j \leq n-1$ and either $(j, n) = 1$ or $(j, n) = 2$ and $\frac{n}{2}$ is odd. Note that the subgroup of $\text{Aut}(H)$ fixing b is transitive on the set of generators of $\langle a\rangle$ and that $\langle a^{n/2}\rangle$ is the center of H. There exists $\alpha \in \text{Aut}(H)$ such that

$$S^\alpha = \{b, ba, a^{\frac{n}{2}}\} \text{ or } \{b, ba^2, a^{\frac{n}{2}}\}.$$

Without loss of generality, we may assume that $S = \{b, ba, a^{\frac{n}{2}}\}$ or $\{b, ba^2, a^{\frac{n}{2}}\}$. If $S = \{b, ba^2, a^{\frac{n}{2}}\}$, we shall prove that $\Sigma \cong P(n, 1)$. Note that the generalized Petersen graph $P(n, 1)$ has vertex set $\{u_i, v_i \mid i \in \mathbb{Z}_n\}$ and edge set $\{\{u_i, u_{i+1}\}, \{v_i, v_{i+1}\}, \{u_i, v_i\} \mid i \in \mathbb{Z}_n\}$. Define a map from $V(\Sigma)$ to $V(P(n, 1))$ as follows:

$$\begin{aligned} \varphi: \quad & a^{2i} \mapsto u_{2i}, & a^{2i+\frac{n}{2}} \mapsto v_{2i}, \\ & ba^{2i} \mapsto u_{2i-1}, & ba^{2i+\frac{n}{2}} \mapsto v_{2i-1}, \end{aligned}$$

where $0 \leq i \leq \frac{n}{2} - 1$. It is easy to see that φ is an isomorphism form Σ to $P(n, 1)$. Since Σ is not arc-transitive, by [8, 14], we have $|\text{Aut}(\Sigma)| = 2|H|$, and so Σ would be a normal Cayley graph of H, a contradiction. If $S = \{b, ba, a^{\frac{n}{2}}\}$, then Σ has a connected subgraph $\Sigma_1 = \text{Cay}(H, \{b, ba\})$ which is a cycle of length $2n$, and Σ is just the graph obtained from

Σ_1 by adding a 1-factor such that each vertex g of Σ_1 is adjacent to its antipodal vertex $a^{\frac{n}{2}}g$. Then $R(H) \rtimes \mathbb{Z}_2 \cong \mathrm{Aut}\,(\Sigma_1) \leq \mathrm{Aut}\,(\Sigma)$, and then since Σ is assumed to be not arc-transitive, $\mathrm{Aut}\,(\Sigma)$ will fix the 1-factor $\{\{g, a^{\frac{n}{2}}g\} \mid g \in H\}$ setwise. This implies that $\mathrm{Aut}\,(\Sigma) \leq \mathrm{Aut}\,(\Sigma_1)$ and so $\mathrm{Aut}\,(\Sigma) = \mathrm{Aut}\,(\Sigma_1)$. Consequently, we have Σ is a normal Cayley graph of H, a contradiction.

Similarly, we have $y \notin \langle a \rangle$. Then we may assume that $x = ba^i$ and $y = ba^j$ for some $1 \leq i, j \leq n-1$ and $i \neq j$. Then $S = \{b, ba^i, ba^j\} \subseteq b\langle a \rangle$. This implies that Σ is a bipartite graph with $\langle a \rangle$ and $b\langle a \rangle$ as its two partition sets. Since Σ is not arc-transitive, $\mathrm{Aut}\,(\Sigma)_1$ is intransitive on the neighbourhood S of 1, and since Σ is not a normal Cayley graph of H, there exists a unique element, say $s \in S$, such that $\mathrm{Aut}\,(\Sigma)_1 = \mathrm{Aut}\,(\Sigma)_s$. Considering the fact that $\mathrm{Aut}\,(H)$ is transitive on $b\langle a \rangle$, without loss of generality, we may assume that $\mathrm{Aut}\,(\Sigma)_1 = \mathrm{Aut}\,(\Sigma)_b$ and $\mathrm{Aut}\,(\Sigma)_1$ swaps ba^i and ba^j. Then for any $h \in H$, we have

$$\mathrm{Aut}\,(\Sigma)_h = (\mathrm{Aut}\,(\Sigma)_1)^{R(h)} = (\mathrm{Aut}\,(\Sigma)_b)^{R(h)} = \mathrm{Aut}\,(\Sigma)_{bh}.$$

Direct computation shows that

$$\begin{aligned}
&\Sigma_2(1) = \{a^{-i}, a^{-j}, a^i, a^{i-j}, a^j, a^{j-i}\},\\
&\Sigma_3(1) = \{ba^{-i}, ba^{j-i}, ba^{-j}, ba^{i-j}, ba^{2i}, ba^{j+i}, ba^{2i-j}, ba^{2j}, ba^{2j-i}\}.
\end{aligned}$$

Let $\mathrm{Aut}\,(\Sigma)_1^*$ be the kernel of $\mathrm{Aut}\,(\Sigma)_1$ acting on S. Take an $\alpha \in \mathrm{Aut}\,(\Sigma)_1^*$. Then α fixes every element in S. As $\mathrm{Aut}\,(\Sigma)_h = \mathrm{Aut}\,(\Sigma)_{bh}$ for any $h \in H$, α will fix $b(ba^i) = a^i$ and $b(ba^j) = a^j$. Note that $\Sigma(ba^i) \setminus \{1, a^i\} = \{a^{i-j}\}$ and $\Sigma(ba^j) \setminus \{1, a^j\} = \{a^{j-i}\}$. Then α also fixes a^{i-j} and a^{j-i}, and then α also fixes ba^{i-j} and ba^{j-i}.

If $|\Sigma_2(1)| = 6$, then it is easy to check that a^{-i} is the unique common neighbor of b and ba^{j-i}. So α also fixes a^{-i}. Now one can see that α fixes every vertex in $\Sigma_2(1)$. If $|\Sigma_2(1)| < 6$ and either $|\Sigma_1(b) \cap \Sigma_1(ba^i)| > 1$ or $|\Sigma_1(b) \cap \Sigma_1(ba^j)| > 1$, then α also fixes every vertex in $\Sigma_2(1)$. In the above two cases, by the connectedness and vertex-transitivity of Σ, α would fix all vertices of Σ, implying that $\alpha = 1$. Hence, $\mathrm{Aut}\,(\Sigma)_1^* = 1$ and $\mathrm{Aut}\,(\Sigma)_1 \cong \mathbb{Z}_2$. This forces that Σ is a normal Cayley graph of H, a contradiction.

Thus, we have $|\Sigma_2(1)| < 6$ and $|\Sigma_1(b) \cap \Sigma_1(ba^i)| = |\Sigma_1(b) \cap \Sigma_1(ba^j)| = 1$. This implies that $\Sigma_1(ba^i) \cap \Sigma_1(ba^j) = \{1, a^{i-j}\} = \{1, a^{j-i}\}$, and so $a^{i-j} = a^{j-i}$. It follows that a^{i-j} is an involution, and hence n is even and $a^{i-j} = a^{n/2}$. So $S = \{b, ba^i, ba^{i+n/2}\}$. As S generates H, one has $\langle a^i, a^{n/2} \rangle = \langle a \rangle$. So either $(i, n) = 1$ or $(i, n) = 2$ and $\frac{n}{2}$ is odd. Note that the subgroup of $\mathrm{Aut}\,(H)$ fixing b is transitive on the set of generators of $\langle a \rangle$ and that $\langle a^{n/2} \rangle$ is the center of H. There exists $\alpha \in \mathrm{Aut}\,(H)$ such that

$$S^\alpha = \{b, ba, ba^{1+\frac{n}{2}}\} \text{ or } \{b, ba^2, ba^{2+\frac{n}{2}}\}.$$

Let β_ϵ be the automorphism of H induced by the map $a \mapsto a^{-1}, b \mapsto ba^\epsilon$, where $\epsilon \in \mathbb{Z}_2$. Then

$$\{b, ba, ba^{1+\frac{n}{2}}\}^{\beta_1} = \{b, ba, ba^{\frac{n}{2}}\}, \text{and } \{b, ba^2, ba^{2+\frac{n}{2}}\}^{\beta_2} = \{b, ba^2, ba^{\frac{n}{2}}\}.$$

If $\frac{n}{2}$ is odd, then the map $\eta : a \mapsto a^{2+\frac{n}{2}}, b \mapsto ba^{\frac{n}{2}}$ induces an automorphism of H, and $\{b, ba, ba^{\frac{n}{2}}\}^\eta = \{b, ba^2, ba^{\frac{n}{2}}\}$. So there always exists $\gamma \in \mathrm{Aut}\,(H)$ such that $S^\gamma = \{b, ba, ba^{\frac{n}{2}}\}$, completing the proof of the first part of our theorem.

Finally, we shall prove $\Sigma \cong \mathrm{CL}_{4\cdot\frac{n}{2}}$. Without loss of generality, assume that $S = \{b, ba, ba^{\frac{n}{2}}\}$. Recall that $V(\mathrm{CL}_{4\cdot\frac{n}{2}}) = \{x_i^r \mid i \in \mathbb{Z}_{2n}, r \in \mathbb{Z}_2\}$ and $E(\mathrm{CL}_{4\cdot\frac{n}{2}}) =$

$\{\{x_i^r, x_{i+1}^r\}, \{x_{2i}^r, x_{2i+1}^{r+1}\}, \mid i \in \mathbb{Z}_{2n}, r \in \mathbb{Z}_2\}$. Let ϕ be a map from $V(\Sigma)$ to $V(\mathrm{CL}_{4\cdot\frac{n}{2}})$ as following:

$$\begin{aligned}\phi:\quad & a^i \mapsto x_{2i}^0, && a^{i+\frac{n}{2}} \mapsto x_{2i}^1,\\ & ba^j \mapsto x_{2j-1}^0, && ba^{j+\frac{n}{2}} \mapsto x_{2j-1}^1,\end{aligned}$$

where $0 \leq i \leq \frac{n}{2} - 1$ and $1 \leq j \leq \frac{n}{2}$. It is easy to check that ϕ is an isomorphism from Σ and $X(\mathrm{CL}_{4\cdot\frac{n}{2}})$, as desired. □

4 Multi-cross ladder graphs

The goal of this section is to prove Theorem 1.2. We first show that each $\mathrm{MCL}_{4m,2}$ is a bi-Cayley graph.

Lemma 4.1. *The multi-cross ladder graph* $\mathrm{MCL}_{4m,2}$ *is isomorphic to the bi-Cayley graph* $\mathrm{BiCay}(H, \{c, ca\}, \{ca, ca^2b\}, \{1\})$*, where*

$$H = \langle a, b, c \mid a^m = b^2 = c^2 = 1, a^b = a, a^c = a^{-1}, b^c = b\rangle.$$

Proof. For convenience, let Γ be the bi-Cayley graph given in our lemma, and let $X = \mathrm{MCL}_{4m,2}$. Let ϕ be a map from $V(X)$ to $V(\Gamma)$ defined by the following rule:

$$\begin{aligned}\phi:\quad & x_{2t}^{1,1} \mapsto (a^t)_0, && x_{2t+1}^{1,1} \mapsto (ca^{t+1})_0, && x_{2t}^{1,0} \mapsto (ca^{t+1})_1, && x_{2t+1}^{1,0} \mapsto (a^t)_1,\\ & x_{2t}^{0,1} \mapsto (ca^{t+1}b)_1, && x_{2t+1}^{0,1} \mapsto (a^tb)_1, && x_{2t}^{0,0} \mapsto (a^tb)_0, && x_{2t+1}^{0,0} \mapsto (ca^{t+1}b)_0,\end{aligned}$$

where $t \in \mathbb{Z}_m$.

It is easy to see that ϕ is an adjacency preserving isomorphism from X to Γ. □

Remark 1 Let m be odd, let $e = ab$ and $f = ca$. Then the group given in Lemma 4.1 has the following presentation:

$$H = \langle e, f \mid e^{2m} = f^2 = 1, e^f = e^{-1}\rangle.$$

Clearly, in this case, H is a dihedral group. Furthermore, the corresponding bi-Cayley graph given in Lemma 4.1 will be

$$\mathrm{BiCay}(H, \{f, fe\}, \{f, fe^{m-1}\}, \{1\}).$$

Proof of Theorem 1.2. By Lemma 4.1, we may let $\Gamma = \mathrm{MCL}_{4m,2}$ be just the bi-Cayley graph $\mathrm{BiCay}(H, R, L, S)$, where

$$\begin{aligned}&H = \langle a, b, c \mid a^m = b^2 = c^2 = 1, a^b = a, a^c = a^{-1}, b^c = b\rangle,\\ &R = \{c, ca\}, L = \{ca, ca^2b\}, S = \{1\}.\end{aligned}$$

We first prove the sufficiency. Assume first that m is even. Then the map

$$a \mapsto ab, b \mapsto b, c \mapsto cb$$

induces an automorphism, say α of H of order 2. Furthermore, $R^\alpha = \{c, ca\}^\alpha = caLca$, $L^\alpha = \{ca, ca^2b\}^\alpha = caRca$ and $S^\alpha = \{1\}^\alpha = ca\{1\}ca = S^{-1}$. By Proposition 2.4, $\delta_{\alpha,ca,ca} \in \mathrm{Aut}(\Gamma)$ and $\mathcal{R}(H) \rtimes \langle\delta_{\alpha,ca,ca}\rangle$ acts regularly on $V(\Gamma)$. Consequently, by Proposition 2.1, Γ is a Cayley graph.

Assume now that m is odd and $3 \mid m$. In this case, we shall use the bi-Cayley presentation for Γ as in Remark 5.1, that is,

$$\Gamma = \mathrm{BiCay}(H, \{f, fe\}, \{f, fe^{m-1}\}, \{1\}),$$

where

$$H = \langle e, f \mid e^{2m} = f^2 = 1, e^f = e^{-1} \rangle.$$

Let β be a permutation of $V(\Gamma)$ defined as following:

$$\begin{array}{lll} \beta: & (f^i e^{3t+1})_i \leftrightarrow (f^i e^{m+3t+1})_i, & (f^{i+1} e^{3t+1})_i \leftrightarrow (f^i e^{m+3t+1})_{i+1}, \\ & (f^{i+1} e^{3t+2})_i \leftrightarrow (f^{i+1} e^{m+3t+2})_i, & (f^i e^{3t+2})_i \leftrightarrow (f^{i+1} e^{m+3t+2})_{i+1}, \\ & (e^{3t})_i \leftrightarrow (fe^{3t})_{i+1}, & (e^{m+3t})_i \leftrightarrow (fe^{m+3t})_{i+1}, \end{array}$$

where $t \in \mathbb{Z}_{\frac{m}{3}}$ and $i \in \mathbb{Z}_2$. It is easy to check that β is an automorphism of Γ of order 2. Furthermore, $\mathcal{R}(e), \mathcal{R}(f)$ and β satisfy the following relations:

$$\begin{array}{l} \mathcal{R}(e)^{2m} = \mathcal{R}(f)^2 = \beta^2 = 1,\ \mathcal{R}(f)^{-1}\mathcal{R}(e)\mathcal{R}(f) = \mathcal{R}(e)^{-1},\ \mathcal{R}(f)^{-1}\beta\mathcal{R}(f) = \beta, \\ \mathcal{R}(e)^6\beta = \beta\mathcal{R}(e)^6,\ \mathcal{R}(e)^2\beta = \beta\mathcal{R}(e)^4\beta\mathcal{R}(e)^{-2}. \end{array}$$

Let $G = \langle \mathcal{R}(e^2), \mathcal{R}(f), \beta \rangle$ and $P = \langle \mathcal{R}(e^2), \beta \rangle$. Then $\mathcal{R}(f) \notin P$ and $G = P\langle \mathcal{R}(f) \rangle$. Since $\mathcal{R}(e)^6\beta = \beta\mathcal{R}(e)^6$, we have $\mathcal{R}(e^6) \in Z(P)$. Since $\mathcal{R}(e)^2\beta = \beta\mathcal{R}(e)^4\beta\mathcal{R}(e)^{-2}$, it follows that

$$(\mathcal{R}(e)^2\beta)^3 = \mathcal{R}(e)^2\beta[\beta\mathcal{R}(e)^4\beta\mathcal{R}(e)^{-2}]\mathcal{R}(e)^2\beta = \mathcal{R}(e^6).$$

Let $N = \langle \mathcal{R}(e^6) \rangle$. Clearly, N is a normal subgroup of G. Furthermore,

$$P/N = \langle \mathcal{R}(e^2)N, \beta N \mid \mathcal{R}(e^2)^3 N = \beta^2 N = (\mathcal{R}(e^2)\beta)^3 N = N \rangle \cong A_4.$$

Therefore, $|P| = 4m$ and $|G| \le 8m$.

Let

$$\begin{array}{ll} \Delta_{00} = \{x_0 \mid x \in \langle e^2, f \rangle\}, & \Delta_{10} = \{(ex)_0 \mid x \in \langle e^2, f \rangle\}, \\ \Delta_{01} = \{x_1 \mid x \in \langle e^2, f \rangle\}, & \Delta_{11} = \{(ex)_1 \mid x \in \langle e^2, f \rangle\}. \end{array}$$

Then Δ_{ij}'s $(i, j \in \mathbb{Z}_2)$ are four orbits of $\langle \mathcal{R}(e^2), \mathcal{R}(f) \rangle$. Moreover,

$$1_0^{\beta\mathcal{R}(f)} = 1_1 \in \Delta_{01},\ e_0^{\beta} = (e^{m+1})_0 \in \Delta_{00},\ e_1^{\beta} = (fe^{m+1})_0 \in \Delta_{00}.$$

This implies that G is transitive on $V(\Gamma)$. Hence, $|G| = 8m$ and so G is regular on $V(\Gamma)$, and by Proposition 2.1, Γ is a Cayley graph.

To prove the necessity, it suffices to prove that if m is odd and $3 \nmid m$, then Γ is a non-Cayley graph. In this case, we shall use the original definition of $\Gamma = \mathrm{MCL}_{4m,2}$. Suppose that m is odd and $3 \nmid m$. We already know from [6, Proposition 3.3] that Γ is vertex-transitive. Let $A = \mathrm{Aut}(\Gamma)$. For $m = 5$ or 7, using Magma [4], Γ is a non-Cayley graph. In what follows, we assume that $m \ge 11$.

For each $j \in \mathbb{Z}_m$, $\mathrm{C}_j^0 = (x_{2j}^{0,0}, x_{2j+1}^{0,0}, x_{2j}^{0,1}, x_{2j+1}^{0,1})$ and $\mathrm{C}_j^1 = (x_{2j}^{1,1}, x_{2j+1}^{1,1}, x_{2j}^{1,0}, x_{2j+1}^{1,0})$ are two 4-cycles. Set $\mathcal{F} = \{\mathrm{C}_j^i \mid i \in \mathbb{Z}_2, j \in \mathbb{Z}_m\}$. From the construction of $\Gamma = \mathrm{MCL}_{4m,2}$, it is easy to see that in $\Gamma = \mathrm{MCL}_{4m,2}$ passing each vertex there is exactly one 4-cycle, which belongs to $\mathcal{F}$. Clearly, any two distinct 4-cycles in $\mathcal{F}$ are vertex-disjoint. This implies that $\Delta = \{V(\mathrm{C}_j^i) \mid i \in \mathbb{Z}_2, j \in \mathbb{Z}_m\}$ is an A-invariant partition of $V(\Gamma)$. Consider the quotient graph Γ_Δ, and let T be the kernel of A acting on Δ. Then $\Gamma_\Delta \cong \mathrm{C}_m[2K_1]$, the lexicographic product of a cycle of length m and an empty graph of order 2. Hence $A/T \leq \mathrm{Aut}\,(\mathrm{C}_m[2K_1]) \cong \mathbb{Z}_2^m \rtimes D_{2m}$. Note that between any two adjacent vertices of Γ_Δ there is exactly one edge of $\Gamma = \mathrm{MCL}_{4m,2}$. Then T fixes each vertex of Γ and hence $T = 1$. So we may view A as a subgroup of $\mathrm{Aut}\,(\Gamma_\Delta) \cong \mathrm{Aut}\,(\mathrm{C}_m[2K_1]) \cong \mathbb{Z}_2^m \rtimes D_{2m}$.

For convenience, we will simply use the C_j^i's to represent the vertices of Γ_Δ. Then Γ_Δ has vertex set

$$\{\mathrm{C}_j^0, \mathrm{C}_j^1 \mid j \in \mathbb{Z}_m\}$$

and edge set

$$\{\{\mathrm{C}_j^0, \mathrm{C}_{j+1}^0\}, \{\mathrm{C}_j^1, \mathrm{C}_{j+1}^1\}, \{\mathrm{C}_j^0, \mathrm{C}_{j+1}^1\}, \{\mathrm{C}_j^1, \mathrm{C}_{j+1}^0\} \mid j \in \mathbb{Z}_m\}.$$

Let $\mathcal{B} = \{\{\mathrm{C}_j^0, \mathrm{C}_j^1\} \mid j \in \mathbb{Z}_m\}$. Then $\mathcal{B}$ is an $\mathrm{Aut}\,(\Gamma_\Delta)$-invariant partition of $V(\Gamma_\Delta)$. Let K be the kernel of $\mathrm{Aut}\,(\Gamma_\Delta)$ acting on $\mathcal{B}$. Then $K = \langle k_0\rangle \times \langle k_2\rangle \times \cdots \times \langle k_{m-1}\rangle$, where we use k_i to denote the transposition $(\mathrm{C}_j^0\ \mathrm{C}_j^1)$ for $j \in \mathbb{Z}_m$. Clearly, K is the maximal normal 2-subgroup of $\mathrm{Aut}\,(\Gamma_\Delta)$.

Suppose to the contrary that $\Gamma = \mathrm{MCL}_{4m,2}$ is a Cayley graph. By Proposition 2.1, A has a subgroup, say G acting regularly on $V(\Gamma)$. Then G has order $8m$, and

$$G/(G \cap K) \cong GK/K \leq \mathrm{Aut}\,(\Gamma_\Delta)/K \lesssim D_{2m}.$$

Since m odd, it follows that $|G \cap K| = 4$ or 8, and so $G \cap K \cong \mathbb{Z}_2^2$ or $\mathbb{Z}_2^3$.

If $G \cap K \cong \mathbb{Z}_2^2$, then $|GK/K| = 2m$ and $GK/K = \mathrm{Aut}\,(\Gamma_\Delta)/K \cong D_{2m}$. So $GK = \mathrm{Aut}\,(\Gamma_\Delta) \cong \mathbb{Z}_2^m \rtimes D_{2m}$. Let M be a Hall $2'$-subgroup of G. Then $M \cong \mathbb{Z}_m$ and M is also a Hall $2'$-subgroup of $\mathrm{Aut}\,(\Gamma_\Delta)$. Clearly, $\mathrm{Aut}\,(\Gamma_\Delta)$ is solvable, so all Hall $2'$-subgroups of $\mathrm{Aut}\,(\Gamma_\Delta)$ are conjugate. Without loss of generality, we may let $M = \langle\alpha\rangle$, where α is the following permutation on $V(\Gamma_\Delta)$:

$$\alpha = (\mathrm{C}_0^0\ \mathrm{C}_1^0 \ldots \mathrm{C}_{m-1}^0)(\mathrm{C}_0^1\ \mathrm{C}_1^1 \ldots \mathrm{C}_{m-1}^1).$$

Then $K \rtimes \langle\alpha\rangle$ acts transitively on $V(\Gamma_\Delta)$. Clearly, $C_K(\alpha)$ is contained in the center of $K \rtimes \langle\alpha\rangle$. So $C_K(\alpha)$ is semiregular on $V(\Gamma_\Delta)$. This implies that

$$C_K(\alpha) = \langle k_0 k_1 \ldots k_{m-1}\rangle \cong \mathbb{Z}_2.$$

On the other hand, let $L = (G \cap K)M$. Clearly, $G \cap K \trianglelefteq G$, so L is a subgroup of G of order $4m$. For any odd prime factor p of m, let P be a Sylow p-subgroup of M. Then P is also a Sylow p-subgroup of L, and since M is cyclic, one has $M \leq N_L(P)$. By Sylow theorem, we have $|L : N_L(P)| = kp + 1 \mid 4$ for some integer k. Since $3 \nmid m$, one has $L = N_L(P)$. It follows that $M \trianglelefteq L$ and so $L = M \times (G \cap K)$. This implies that $G \cap K \leq C_K(M) = C_K(\alpha) \cong \mathbb{Z}_2$, a contradiction.

If $G \cap K \cong \mathbb{Z}_2^3$, then $|GK/K| = m$. Furthermore, $GK/K \cong \mathbb{Z}_m$ and GK/K acts on $\mathcal{B}$ regularly. Since G is transitive on $V(\Gamma)$, there exists $g \in G$ such that $(x_0^{1,1})^g = x_1^{1,1}$, where $x_0^{1,1}, x_1^{1,1} \in \mathrm{C}_0^1$. As $V(\Gamma_\Delta) = \{\mathrm{C}_j^i \mid i \in \mathbb{Z}_2, j \in \mathbb{Z}_m\}$, g fixes the 4-cycle $\mathrm{C}_0^1 = (x_0^{1,1}, x_1^{1,1}, x_0^{1,0}, x_1^{1,0})$. Since $\mathcal{B} = \{\{\mathrm{C}_j^0, \mathrm{C}_j^1\} \mid j \in \mathbb{Z}_m\}$ is also A-invariant, g fixes $\{\mathrm{C}_0^0, \mathrm{C}_0^1\}$ setwise. Since GK/K acts on $\mathcal{B}$ regularly, g fixes $\{\mathrm{C}_j^0, \mathrm{C}_j^1\}$ setwise for every $j \in \mathbb{Z}_m$. Observe that $\{x_0^{1,1}, x_{2m-1}^{1,1}\}$ and $\{x_1^{1,1}, x_2^{1,1}\}$ are the unique edges of Γ between C_0^1 and C_{m-1}^1, C_0^1 and C_2^1, respectively. This implies that g will map C_{m-1}^1 to C_2^1, contradicting that g fixes $\{\mathrm{C}_j^0, \mathrm{C}_j^1\}$ setwise for every $j \in \mathbb{Z}_m$. □

5 A family of trivalent VNC bi-dihedrants

The goal of this section is to prove the following lemma which gives a new family of trivalent vertex-transitive non-Cayley bi-dihedrants. To be brief, a vertex-transitive non-Cayley graph is sometimes simply called a *VNC graph*.

Lemma 5.1. *Let* $H = \langle a, b \mid a^n = b^2 = 1, a^b = a^{-1}\rangle$ *be a dihedral group, where* $n = 48\ell$ *and* $\ell \geq 1$*. Then* $\Gamma = \mathrm{BiCay}(H, \{b, ba\}, \{ba^{24\ell}, ba^{12\ell-1}\}, \{1\})$ *is a VNC dihedrant.*

Proof. We first define a permutation on $V(\Gamma)$ as follows:

$$\begin{array}{llll} g: & (a^{3r})_0 \mapsto (a^{3r})_0, & (a^{3r})_1 \mapsto (ba^{3r})_0, & (a^{3r+1})_0 \mapsto (ba^{3r+1})_1, \\ & (a^{3r+1})_1 \mapsto (a^{24\ell+3r+1})_1, & (a^{3r+2})_i \mapsto (ba^{12\ell+3r+2})_{i+1}, & (ba^{3r})_0 \mapsto (a^{3r})_1, \\ & (ba^{3r})_1 \mapsto (ba^{24\ell+3r})_1, & (ba^{3r+1})_0 \mapsto (ba^{3r+1})_0, & (ba^{3r+1})_1 \mapsto (a^{3r+1})_0, \\ & (ba^{3r+2})_i \mapsto (a^{-12\ell+3r+2})_{i+1}, & & \end{array}$$

where $r \in \mathbb{Z}_{16\ell},\ i \in \mathbb{Z}_2$.

It is easy to check that g is an involution, and furthermore, for any $t \in \mathbb{Z}_{16\ell}$, we have

$$\begin{array}{l} \Gamma((a^{3r})_0)^g = \{(a^{3r})_1, (ba^{3r})_0, (ba^{3r+1})_0\} = \Gamma((a^{3r})_0), \\ \Gamma((a^{3r})_1)^g = \{(ba^{3r})_1, (a^{3r})_0, (a^{3r-1})_0\} = \Gamma((ba^{3r})_0), \\ \Gamma((ba^{3r})_1)^g = \{(ba^{24\ell+3r})_0, (a^{3r})_1, (a^{12\ell+3r+1})_1\} = \Gamma((ba^{24\ell+3r})_1), \\ \Gamma((a^{3r+1})_0)^g = \{(ba^{3r+1})_0, (a^{24\ell+3r+1})_1, (a^{36\ell+3r+2})_1\} = \Gamma((ba^{3r+1})_1), \\ \Gamma((a^{3r+1})_1)^g = \{(a^{24\ell+3r+1})_0, (ba^{3r+1})_1, (ba^{36\ell+3r})_1\} = \Gamma((a^{24\ell+3r+1})_1), \\ \Gamma((ba^{3r+1})_0)^g = \{(ba^{3r+1})_1, (a^{3r+1})_0, (a^{3r})_0\} = \Gamma((ba^{3r+1})_0), \\ \Gamma((a^{3r+2})_0)^g = \{(ba^{12\ell+3r+2})_0, (a^{36\ell+3r+2})_1, (a^{3r+3})_1\} = \Gamma((ba^{12\ell+3r+2})_1), \\ \Gamma((a^{3r+2})_1)^g = \{(ba^{12\ell+3r+2})_1, (a^{12\ell+3r+2})_0, (a^{12\ell+3r+1})_0\} = \Gamma((ba^{12\ell+3r+2})_0). \end{array}$$

This implies that g is an automorphism of Γ. Observing that g maps 1_1 to b_0, it follows that $\langle \mathcal{R}(H), g\rangle$ is transitive on $V(\Gamma)$, and so Γ is a vertex-transitive graph.

Below, we shall first prove the following claim.

Claim. $\mathrm{Aut}\,(\Gamma)_{1_0} = \langle g\rangle$.

Let $A = \mathrm{Aut}\,(\Gamma)$. It is easy to see that g fixes 1_0, and so $g \in A_{1_0}$. To prove the Claim, it suffices to prove that $|A_{1_0}| = 2$.

Note that the neighborhood $\Gamma(1_0)$ of 1_0 in Γ is $= \{1_1, b_0, (ba)_0\}$. By a direct computation, we find that in Γ there is a unique 8-cycle passing through 1_0, 1_1 and b_0, that is,

$$\mathrm{C}_0 = (1_0, 1_1, (ba^{24\ell})_1, (ba^{24\ell})_0, (a^{24\ell})_0, (a^{24\ell})_1, b_1, b_0, 1_0).$$

Furthermore, in Γ there is no 8-cycle passing through 1_0 and $(ba)_0$. So A_{1_0} fixes $(ba)_0$.

If A_{1_0} also fixes 1_1 and b_0, then A_{1_0} will fix every neighbor of 1_0, and the connectedness and vertex-transitivity of Γ give that $A_{1_0} = 1$, a contradiction. Therefore, A_{1_0} swaps 1_1 and b_0, and $(ba)_0$ is the unique neighbor of 1_0 such that $A_{1_0} = A_{(ba)_0}$. It follows that $\{1_0, (ba)_0\}$ is a block of imprimitivity of A acting on $V(\Gamma)$. Since Γ is vertex-transitive, every $v \in V(\Gamma)$ has a unique neighbor, say u such that $A_u = A_v$. Then the set

$$\mathcal{B} = \{\{u, v\} \in E(\Gamma) \mid A_u = A_v\}$$

forms an A-invariant partition of $V(\Gamma)$. Clearly, $\{1_0, (ba)_0\} \in \mathcal{B}$. Similarly, since C_0 is also the unique 8-cycle of Γ passing through 1_0, 1_1 and b_0, A_{1_1} swaps 1_0 and b_0, and

$(ba^{12\ell-1})_1$ is the unique neighbor of 1_1 such that $A_{1_1} = A_{(ba^{12\ell-1})_1}$. So $\{1_1, (ba^{12\ell-1})_1\} \in \mathcal{B}$. Set

$$\mathcal{B}_0 = \{\{1_0, (ba)_0\}^{\mathcal{R}(h)} \mid h \in H\} \text{ and } \mathcal{B}_1 = \{\{1_1, (ba^{12\ell-1})_1\}^{\mathcal{R}(h)} \mid h \in H\}.$$

Clearly, $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_1$.

Now we consider the quotient graph $\Gamma_{\mathcal{B}}$ of Γ relative to $\mathcal{B}$. It is easy to see that $\langle \mathcal{R}(a) \rangle$ acts semiregularly on $\mathcal{B}$ with $\mathcal{B}_0$ and $\mathcal{B}_1$ as its two orbits. So $\Gamma_{\mathcal{B}}$ is isomorphic to a bi-Cayley graph over $\langle a \rangle$. Set $B_0 = \{1_0, (ba)_0\}$ and $B_1 = \{1_1, (ba^{12\ell-1})_1\}$. Then one may see that the neighbors of B_0 in $\Gamma_{\mathcal{B}}$ are: $B_0^{\mathcal{R}(a)}, B_0^{\mathcal{R}(a^{-1})}, B_1, B_1^{\mathcal{R}(a^{-12\ell+2})}$, and the neighbors of B_1 in $\Gamma_{\mathcal{B}}$ are: $B_1^{\mathcal{R}(a^{12\ell+1})}, B_1^{\mathcal{R}(a^{-12\ell-1})}, B_0, B_0^{\mathcal{R}(a^{12\ell-2})}$. So

$$\Gamma_{\mathcal{B}} \cong \Gamma' = \mathrm{BiCay}(\langle a \rangle, \{a, a^{-1}\}, \{a^{12\ell+1}, a^{-12\ell-1}\}, \{1, a^{-12\ell+2}\}).$$

Observe that there is one and only one edge of Γ between B_0 and any one of its neighbors in $\Gamma_{\mathcal{B}}$. Clearly, A acts transitively on $V(\Gamma_{\mathcal{B}})$, so there is one and only one edge of Γ between every two adjacent blocks of $\mathcal{B}$. It follows that A acts faithfully on $V(\Gamma_{\mathcal{B}})$, and hence we may view A as a subgroup of $\mathrm{Aut}\,(\Gamma_{\mathcal{B}})$. Recall that $g \in A_{1_0} = A_{(ba)_0}$. Moreover, g swaps the two neighbors 1_1 and b_0 of 1_0. Clearly, $1_1 \in B_1$ and $b_0 \in B_0^{\mathcal{R}(a^{-1})}$, so g swaps the two blocks B_1 and $B_0^{\mathcal{R}(a^{-1})}$. Similarly, g swaps the two neighbors $(ba)_1$ and a_0 of $(ba)_0$. Clearly, $(ba)_1 \in B_1^{\mathcal{R}(a^{-12\ell+2})}$ and $a_0 \in B_0^{\mathcal{R}(a)}$, so g swaps the two blocks $B_1^{\mathcal{R}(a^{-12\ell+2})}$ and $B_0^{\mathcal{R}(a)}$. Note that $\mathcal{R}(ab)$ swaps the two vertices in B_0. So $\langle g, \mathcal{R}(ab) \rangle$ acts transitively on the neighborhood of B_0 in $\Gamma_{\mathcal{B}}$. This implies that A acts transitively on the arcs of $\Gamma_{\mathcal{B}}$, and so Γ' is a tetravalent arc-transitive bi-circulant. In [11], a characterization of tetravalent edge-transitive bi-circulants is given. It is easy to see that our graph Γ' belongs to Class 1(c) of [11, Theorem 1.1]. By checking [11, Theorem 4.1], we see that the stabilizer $\mathrm{Aut}\,(\Gamma')_u$ of $u \in V(\Gamma')$ has order 4. This implies that $|A| = 4|V(\Gamma_{\mathcal{B}})| = 8n$. Consequently, $|A_{1_0}| = 2$ and so our claim holds.

Now we are ready to finish the proof. Suppose to the contrary that Γ is a Cayley graph. By Proposition 2.1, A contains a subgroup, say J acting regularly on $V(\Gamma)$. By Claim, J has index 2 in A, and since $g \in A_{1_0}$, one has $A = J \rtimes \langle g \rangle$. It is easy to check that $\mathcal{R}(a), \mathcal{R}(b)$ and g satisfy the following relations:

$$(g\mathcal{R}(b))^4 = \mathcal{R}(a^{24\ell}),\ g\mathcal{R}(a^3) = \mathcal{R}(a^3)g,\ g\mathcal{R}(ba) = \mathcal{R}(ba)g,\ g = \mathcal{R}(a)(g\mathcal{R}(b))^2\mathcal{R}(a^{12\ell-1}).$$

Suppose that $\mathcal{R}(H) \nleq J$. Then $A = J\mathcal{R}(H)$. Since $|J|/|\mathcal{R}(H)| = 2$, it follows that $|\mathcal{R}(H) : J \cap \mathcal{R}(H)| = 2$. Thus, $J \cap \mathcal{R}(H) = \langle \mathcal{R}(a) \rangle$ or $\langle \mathcal{R}(a^2), \mathcal{R}(b) \rangle$. If $\mathcal{R}(H) \cap J = \langle \mathcal{R}(a) \rangle$, then we have $\mathcal{R}(b) \notin J, \mathcal{R}(a) \in J$, and hence $A = J \cup J\mathcal{R}(b) = J \cup Jg$, implying that $J\mathcal{R}(b) = Jg$. It follows that $g\mathcal{R}(b) \in J$, and then $g = \mathcal{R}(a)(g\mathcal{R}(b))^2\mathcal{R}(a^{12\ell-1}) \in J$ due to $\mathcal{R}(a) \in J$, a contradiction. If $\mathcal{R}(H) \cap J = \langle \mathcal{R}(a^2), \mathcal{R}(b) \rangle$, then $\mathcal{R}(a) \notin J$, and again we have $A = J \cup J\mathcal{R}(a) = J \cup Jg$, implying that $J\mathcal{R}(a) = Jg$. So, $\mathcal{R}(a)g, g\mathcal{R}(a^{-1}) \in J$. Then

$$g = \mathcal{R}(a)g\mathcal{R}(b)g\mathcal{R}(b)\mathcal{R}(a^{12\ell-1}) = (\mathcal{R}(a)g)\mathcal{R}(b)(g\mathcal{R}(a^{-1}))\mathcal{R}(ba^{12\ell-2}) \in J,$$

a contradiction.

Suppose that $\mathcal{R}(H) \leq J$. Then $|J : \mathcal{R}(H)| = 2$ and $\mathcal{R}(H) \trianglelefteq J$. Since J is regular on $V(\Gamma)$, by Proposition 2.4, there exists a $\delta_{\alpha,x,y} \in J$ such that $1_0^{\delta_{\alpha,x,y}} = 1_1$, where $\alpha \in$

Aut (H) and $x, y \in H$. By the definition of $\delta_{\alpha,x,y}$, we have $1_1 = 1_0^{\delta_{\alpha,x,y}} = (x \cdot 1^\alpha)_1 = x_1$, implying that $x = 1$. Furthermore, we have the following relations:

$$R^\alpha = x^{-1}Lx, L^\alpha = y^{-1}Ry, S^\alpha = y^{-1}S^{-1}x,$$

where $R = \{b, ba\}, L = \{ba^{24\ell}, ba^{12\ell-1}\}, S = \{1\}$. In particular, the last equality implies that $x = y$ due to $S = \{1\}$. So we have $x = y = 1$. From the proof of Claim we know that $B_0 = \{1_0, (ba)_0\}$ and $B_1 = \{1_1, (ba^{12\ell-1})_1\}$ are two blocks of imprimitivity of A acting on $V(\Gamma)$. So we have $((ba)_0)^{\delta_{\alpha,1,1}} = (ba^{12\ell-1})_1$. It follows that $(ba)^\alpha = ba^{12\ell-1}$, and then from $R^\alpha = L$ we obtain that $b^\alpha = ba^{24\ell}$. Consequently, we have $a^\alpha = a^{36\ell-1}$. One the other hand, we have $\{b, ba\} = R = L^\alpha = \{b, ba^{24\ell+1}\}$. This forces that $ba = ba^{24\ell+1}$, which is clearly impossible. □

6 Two families of trivalent Cayley bi-dihedrants

In this section, we shall prove two lemmas which will be used the proof of Theorem 1.3.

Lemma 6.1. *Let $H = \langle a, b \mid a^{12m} = b^2 = 1, a^b = a^{-1}\rangle$ be a dihedral group with m odd. Then for each $i \in \mathbb{Z}_{12m}$, $\Gamma = \mathrm{BiCay}(H, \{b, ba^i\}, \{ba^{6m}, ba^{3m-i}\}, \{1\})$ is a Cayley graph whenever $\langle a^i, a^{3m}\rangle = \langle a\rangle$.*

Proof. Let g be a permutation of $V(\Gamma)$ defined as follows:

$$\begin{array}{lll}
g: & (a^{6km+3ri})_j \mapsto (ba^{6(k+1)m+3ri})_{j+1}, & (ba^{6km+3ri})_j \mapsto (a^{6km+3ri})_{j+1},\\
& (a^{3km+(3r+1)i})_0 \mapsto (a^{3(k+1)m+(3r+1)i})_0, & (ba^{3km+(3r+1)i})_0 \mapsto (a^{3(k+1)m+(3r+1)i})_1,\\
& (a^{3km+(3r+1)i})_1 \mapsto (ba^{3(k+1)m+(3r+1)i})_0, & (ba^{3km+(3r+1)i})_1 \mapsto (ba^{3(k-1)m+(3r+1)i})_1,\\
& (a^{3km+(3r+2)i})_0 \mapsto (ba^{3(k+1)m+(3r+2)i})_1, & (ba^{3km+(3r+2)i})_0 \mapsto (ba^{3(k+1)m+(3r+2)i})_0,\\
& (a^{3km+(3r+2)i})_1 \mapsto (a^{3(k-1)m+(3r+2)i})_1, & (ba^{3km+(3r+2)i})_1 \mapsto (a^{3(k+1)m+(3r+2)i})_0,
\end{array}$$

where $r \in \mathbb{Z}_m$, $k \in \mathbb{Z}_4$ and $j \in \mathbb{Z}_2$.

It is easy to check that $g \in \mathrm{Aut}\,(\Gamma)$. Furthermore, one may check that g and $\mathcal{R}(a^2)$ satisfy the following relations:

$$\begin{array}{l}
\mathcal{R}(a^{12m}) = g^4 = 1,\ g^2 = \mathcal{R}(a^{6m}),\ \mathcal{R}(a^6)g = g\mathcal{R}(a^6),\\
\mathcal{R}(b^{-1})g\mathcal{R}(b) = g\mathcal{R}(a^{6m}),\ \mathcal{R}(a^2)g = g\mathcal{R}(a^4)g\mathcal{R}(a^{-2}).
\end{array}$$

By the last equality, we have

$$(\mathcal{R}(a^2)g)^3 = [g\mathcal{R}(a^4)g\mathcal{R}(a^{-2}))]\mathcal{R}(a^2)g\mathcal{R}(a^2)g = g\mathcal{R}(a^4)g^2\mathcal{R}(a^2)g.$$

It then follows from the second and third equalities that

$$g\mathcal{R}(a^4)g^2\mathcal{R}(a^2)g = g\mathcal{R}(a^{6+6m})g = g^2\mathcal{R}(a^{6+6m}) = \mathcal{R}(a^6).$$

Therefore, $(\mathcal{R}(a^2)g)^3 = \mathcal{R}(a^6)$.

Let $G = \langle\mathcal{R}(a^2), \mathcal{R}(b), g\rangle$ and $T = \langle\mathcal{R}(a^6)\rangle$. Then $T \trianglelefteq G$ and

$$\begin{aligned}
G/T &= \langle\mathcal{R}(a^2)T, \mathcal{R}(b)T, gT\rangle\\
&= \langle\mathcal{R}(a^2)T, gT \mid \mathcal{R}(a^2)^3T = g^2T = (\mathcal{R}(a^2)g)^3T = T\rangle \rtimes \langle\mathcal{R}(b)T\rangle\\
&\cong A_4 \rtimes \mathbb{Z}_2.
\end{aligned}$$

So $|G| = 48m$.

Let

$$\begin{array}{ll}\Omega_{00} = \{t_0 \mid t \in \langle a^2, b\rangle\}, & \Omega_{01} = \{t_1 \mid t \in \langle a^2, b\rangle\},\\ \Omega_{10} = \{(at)_0 \mid t \in \langle a^2, b\rangle\}, & \Omega_{11} = \{(at)_1 \mid t \in \langle a^2, b\rangle\}.\end{array}$$

Then Ω_{ij}'s $(0 \leq i, j \leq 1)$ are orbits of T and $V(\Gamma) = \bigcup_{0\leq i,j\leq 1} \Omega_{ij}$. Since $1_0^g = (ba^{6m})_1 \in \Omega_{01}$, $a_0^g = (a^{3m+1})_0 \in \Omega_{00}$ and $a_1^g = (ba^{3m+1})_1 \in \Omega_{01}$, it follows that G is transitive, and so regular on $V(\Gamma)$. By Proposition 2.1, Γ is a Cayley graph on G, as required. $\square$

Lemma 6.2. *Let $H = \langle a, b \mid a^{12m} = b^2 = 1, a^b = a^{-1}\rangle$ be a dihedral group with m even and $4 \nmid m$. Then the following two bi-Cayley graphs:*

$$\begin{array}{l}\Gamma_1 = \mathrm{BiCay}(H, \{b, ba\}, \{ba^{6m}, ba^{3m-1}\}, \{1\}),\\ \Gamma_2 = \mathrm{BiCay}(H, \{b, ba\}, \{ba^{6m}, ba^{9m-1}\}, \{1\})\end{array}$$

are both Cayley graphs.

Proof. Let $V = H_0 \cup H_1$. Then $V(\Gamma_1) = V(\Gamma_2) = V$. We first define two permutations on V as follows:

$$\begin{array}{lll} g_1: & (a^{4r})_i \mapsto (ba^{6m+4r})_{i+1}, & (ba^{4r})_i \mapsto (a^{4r})_{i+1},\\ & (a^{4r+1})_i \mapsto (ba^{9m+4r+1})_{i+1}, & (ba^{4r+1})_i \mapsto (a^{3m+4r+1})_{i+1},\\ & (a^{4r+2})_i \mapsto (ba^{4r+2})_{i+1}, & (ba^{4r+2})_i \mapsto (a^{6m+4r+2})_{i+1},\\ & (a^{4r+3})_i \mapsto (ba^{3m+4r+3})_{i+1}, & (ba^{4r+3})_i \mapsto (a^{9m+4r+3})_{i+1},\end{array}$$

$$\begin{array}{lll} g_2: & (a^{4r})_i \mapsto (ba^{6m+4r})_{i+1}, & (ba^{4r})_i \mapsto (a^{4r})_{i+1},\\ & (a^{4r+1})_i \mapsto (ba^{3m+4r+1})_{i+1}, & (ba^{4r+1})_i \mapsto (a^{9m+4r+1})_{i+1},\\ & (a^{4r+2})_i \mapsto (ba^{4r+2})_{i+1}, & (ba^{4r+2})_i \mapsto (a^{6m+4r+2})_{i+1},\\ & (a^{4r+3})_i \mapsto (ba^{9m+4r+3})_{i+1}, & (ba^{4r+3})_i \mapsto (a^{3m+4r+3})_{i+1},\end{array}$$

where $r \in \mathbb{Z}_{3m}$ and $i \in \mathbb{Z}_2$.

It is easy to check that $g_j \in \mathrm{Aut}(\Gamma_j)$ for $j = 1$ or 2. Furthermore, $\mathcal{R}(a^2), \mathcal{R}(b)$ and g_j $(j = 1$ or $2)$ satisfy the following relations:

$$\begin{array}{l}\mathcal{R}(a^{12m}) = \mathcal{R}(b^2) = g_j^4 = 1, \mathcal{R}(b)\mathcal{R}(a^2)\mathcal{R}(b) = \mathcal{R}(a^{-2}),\\ g_j^2 = \mathcal{R}(a^{6m}), \mathcal{R}(b)g_j\mathcal{R}(b) = g_j^{-1},\\ g_1^{-1}\mathcal{R}(a)g_1 = \mathcal{R}(a^{3m+1}), g_2^{-1}\mathcal{R}(a)g_2 = \mathcal{R}(a^{9m+1}).\end{array}$$

For $j = 1$ or 2, let $G_j = \langle \mathcal{R}(a), \mathcal{R}(b), g_j\rangle$. From the above relations it is east to see that

$$G_j = (\langle \mathcal{R}(a)\rangle\langle g_j\rangle) \rtimes \langle \mathcal{R}(b)\rangle$$

has order at most $48m$. Observe that $1_0^{g_j} = (ba^{6m})_1 \in H_1$ for $j = 1$ or 2. It follows that G_j is transitive on $V(\Gamma_j)$, and so G_j acts regularly on $V(\Gamma_j)$. By Proposition 2.1, each Γ_j is a Cayley graph. $\square$

7 Vertex-transitive trivalent bi-dihedrants

In this section, we shall give a complete classification of trivalent vertex-transitive non-Cayley bi-dihedrants. For convenience of the statement, throughout this section, we shall make the following assumption.

Assumption I.

- H: the dihedral group $D_{2n} = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1}\rangle (n \geq 3)$,
- $\Gamma = \mathrm{BiCay}(H,\ R,\ L,\ \{1\})$: a connected trivalent 2-type vertex-transitive bi-Cayley graph over the group H (in this case, $|R| = |L| = 2$),
- G: a minimum group of automorphisms of Γ subject to that $\mathcal{R}(H) \leq G$ and G is transitive on the vertices but intransitive on the arcs of Γ.

The following lemma given in [20] shows that the group G must be solvable.

Lemma 7.1 ([20, Lemma 6.2])**.** *$G = \mathcal{R}(H)P$ is solvable, where P is a Sylow 2-subgroup of G.*

7.1 H_0 and H_1 are blocks of imprimitivity of G

The case where H_0 and H_1 are blocks of imprimitivity of G has been considered in [20], and the main result is the following proposition.

Proposition 7.2 ([20, Theorem 1.3])**.** *If H_0 and H_1 are blocks of imprimitivity of G on $V(\Gamma)$, then either Γ is Cayley or one of the following occurs:*

(1) $(R, L, S) \equiv (\{b,\ ba^{\ell+1}\}, \{ba,\ ba^{\ell^2+\ell+1}\}, \{1\})$, *where* $n \geq 5$, $\ell^3 + \ell^2 + \ell + 1 \equiv 0 \pmod{n}$, $\ell^2 \not\equiv 1 \pmod{n}$*;*

(2) $(R, L, S) \equiv (\{ba^{-\ell},\ ba^{\ell}\}, \{a,\ a^{-1}\}, \{1\})$, *where* $n = 2k$ *and* $\ell^2 \equiv -1 \pmod{k}$. *Furthermore, Γ is also a bi-Cayley graph over an abelian group $\mathbb{Z}_n \times \mathbb{Z}_2$.*

Furthermore, all of the graphs arising from (1)-(2) are vertex-transitive non-Cayley.

In particular, it is proved in [20] that if n is odd and Γ is not a Cayley graph, then H_0 and H_1 are blocks of imprimitivity of G on $V(\Gamma)$. Consequently, we can get a classification of trivalent vertex-transitive non-Cayley bi-Cayley graphs over a dihedral group D_{2n} with n odd.

Proposition 7.3 ([20, Proposition 6.4])**.** *If n is odd, then either Γ is a Cayley graph, or H_0 and H_1 are blocks of imprimitivity of G on $V(\Gamma)$.*

7.2 H_0 and H_1 are not blocks of imprimitivity of G

In this subsection, we shall consider the case where H_0 and H_1 are not blocks of imprimitivity of G on $V(\Gamma)$. We begin by citing a lemma from [20].

Lemma 7.4 ([20, Lemma 6.3])**.** *Suppose that H_0 and H_1 are not blocks of imprimitivity of G on $V(\Gamma)$. Let N be a normal subgroup of G, and let K be the kernel of G acting on $V(\Gamma_N)$. Let Δ be an orbit of N. If N fixes H_0 setwise, then one of the following holds:*

(1) $\Gamma[\Delta]$ *has valency* 1, $|V(\Gamma_N)| \geq 3$ *and* Γ *is a Cayley graph;*

(2) $\Gamma[\Delta]$ *has valency* 0, Γ_N *has valency* 3, *and* $K = N$ *is semiregular.*

The following lemma deals with the case where $\mathrm{Core}_G(\mathcal{R}(H)) = 1$, and in this case we shall see that Γ is just the cross ladder graph.

Lemma 7.5. *Suppose that H_0 and H_1 are not blocks of imprimitivity of G on $V(\Gamma)$. If $\mathrm{Core}_G(\mathcal{R}(H)) = \bigcap_{g\in G}\mathcal{R}(H) = 1$, then Γ is isomorphic to the cross ladder graph CL_{4n} with n odd, and furthermore, for any minimal normal subgroup N of G, we have the following:*

(1) *N is a 2-group which is non-regular on $V(\Gamma)$;*

(2) *N does not fix H_0 setwise;*

(3) *every orbit of N consists of two non-adjacent vertices.*

Proof. Let N be a minimal normal subgroup of G. By Lemma 7.1, G is solvable. It follows that N is an elementary abelian r-subgroup for some prime divisor r of $|G|$. Clearly, $N \nleq \mathcal{R}(H)$ due to $\mathrm{Core}_G(\mathcal{R}(H)) = 1$. Then $|N\mathcal{R}(H)|/|\mathcal{R}(H)| \mid |G|/|\mathcal{R}(H)|$. From Lemma 7.1 it follows that $|G|/|\mathcal{R}(H)|$ is a power of 2, and hence N is a 2-group.

Suppose that N is regular on $V(\Gamma)$. Then $N\mathcal{R}(H)$ is transitive on $V(\Gamma)$ and $\mathcal{R}(H)$ is also a 2-group. Therefore, $N\mathcal{R}(H)$ is not transitive on the arcs of Γ. The minimality of G gives that $G = N\mathcal{R}(H)$. Since n is even, $\mathcal{R}(a^{\frac{n}{2}})$ is in the center of $\mathcal{R}(H)$. Set $Q = N\langle\mathcal{R}(a^{\frac{n}{2}})\rangle$. Then $Q \trianglelefteq G$ and then $1 \neq N \cap Z(Q) \trianglelefteq G$. Since N is a minimal normal subgroup of G, one has $N \leq Z(Q)$, and hence Q is abelian. It follows that $\langle\mathcal{R}(a^{\frac{n}{2}})\rangle \trianglelefteq G$, contrary to the assumption that $\mathrm{Core}_G(\mathcal{R}(H)) = 1$. Thus, N is not regular on $V(\Gamma)$. (1) is proved.

For (2), by way of contradiction, suppose that N fixes H_0 setwise. Consider the quotient graph Γ_N of Γ relative to N, and let K be the kernel of G acting on $V(\Gamma_N)$. Take Δ to be an orbit of N on $V(\Gamma)$. Then either (1) or (2) of Lemma 7.4 happens.

For the former, $\Gamma[\Delta]$ has valency 1 and $|V(\Gamma_N)| \geq 3$. Then Γ_N is a cycle. Moreover, any two neighbors of $u \in \Delta$ are in different orbits of N. It follows that the stabilizer N_v of v in N fixes every neighbor of u. The connectedness of Γ implies that $N_v = 1$. Thus, $K = N$ is semiregular and Γ_N is a cycle of length $\ell = 2|\mathcal{R}(H)|/|N|$. So $G/N \leq \mathrm{Aut}(\Gamma_N) \cong D_{2\ell}$. If $G/N < \mathrm{Aut}(\Gamma_N)$, then $|G : N| = \ell$ and so $|G| = 2|\mathcal{R}(H)|$. This implies that $\mathcal{R}(H) \trianglelefteq G$, contrary to the assumption that $\mathrm{Core}_G(\mathcal{R}(H)) = 1$. If $G/N = \mathrm{Aut}(\Gamma_N)$, then $|G : \mathcal{R}(H)| = 4$. Since $N \nleq \mathcal{R}(H)$ and since N fixes H_0 setwise, one has $|G : \mathcal{R}(H)N| = 2$. It follows that $\mathcal{R}(H)N \trianglelefteq G$. Clearly, H_0 and H_1 are just two orbits of $\mathcal{R}(H)N$, and they are also two blocks of imprimitivity of G on $V(\Gamma)$, a contradiction.

For the latter, $\Gamma[\Delta]$ has valency 0, Γ_N has valency 3 and $N = K$ is semiregular. Let $\bar{H}_i$ be the set of orbits of N contained in H_i with $i = 1, 2$. Then $\Gamma_N[\bar{H}_0]$ and $\Gamma_N[\bar{H}_1]$ are of valency 2 and the edges between $\bar{H}_0$ and $\bar{H}_1$ form a perfect matching. Without loss of generality, we may assume that $1_0 \in \Delta$. Since $\mathcal{R}(H)$ acts on H_0 by right multiplication, we have the subgroup of $\mathcal{R}(H)$ fixing Δ setwise is just $\mathcal{R}(H)_\Delta = \{\mathcal{R}(h) \mid h_0 \in \Delta\}$. If $\mathcal{R}(H)_\Delta \leq \langle\mathcal{R}(a)\rangle$, then $\mathcal{R}(H)_\Delta \trianglelefteq \mathcal{R}(H)$, and the transitivity of $\mathcal{R}(H)$ on H_0 implies that $\mathcal{R}(H)_\Delta$ will fix all orbits of N contained in H_0. Since the edges between $\bar{H}_0$ and $\bar{H}_1$ are independent, $\mathcal{R}(H)_\Delta$ fixes all orbits of N. It follows that $\mathcal{R}(H)_\Delta \leq N$, namely, $\mathcal{R}(H)N/N$ acts regularly on $\bar{H}_0$. Then $|\mathcal{R}(H)/(\mathcal{R}(H)\cap N)| = |\mathcal{R}(H)N/N| = |H_0/N|$, and so $|N| = |\mathcal{R}(H) \cap N|$, forcing $N \leq \mathcal{R}(H)$, a contradiction. Thus, $\mathcal{R}(H)_\Delta \nleq \langle\mathcal{R}(a)\rangle$, and so $\langle\mathcal{R}(a)\rangle\mathcal{R}(H)_\Delta = \mathcal{R}(H)$. This implies that $\langle\mathcal{R}(a), N\rangle/N$ is transitive and so regular on $\bar{H}_0$. Similarly, $\langle\mathcal{R}(a), N\rangle/N$ is also regular on $\bar{H}_1$. Thus, Γ_N is a trivalent 2-type bi-Cayley graph over $\langle\mathcal{R}(a), N\rangle/N$. By [24, Lemma 5.3], $\bar{H}_0$ and $\bar{H}_0$ are blocks of imprimitivity of G/N, and so H_0 and H_1 are blocks of imprimitivity of G, a contradiction.

So far, we have completed the proof of (2). Then N does not fix H_0 setwise, and then $N\mathcal{R}(H)$ is transitive on $V(\Gamma)$. The minimality of G gives that $G = N\mathcal{R}(H)$. Let P and P_1 be Sylow 2-subgroups of G and $\mathcal{R}(H)$, respectively, such that $P_1 \leq P$. Then $N \leq P$ and $P = NP_1$.

If n is even, then by a similar argument to the second paragraph, a contradiction occurs. Thus, n is odd. As $H \cong D_{2n}$, $P_1 \cong \mathbb{Z}_2$ and P_1 is non-normal in $\mathcal{R}(H)$. So $N \cap \mathcal{R}(H) = 1$. Clearly, $|V(\Gamma)| = 4n$. If N is semiregular on $V(\Gamma)$, then $N \cong \mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$, and then $|G| = |\mathcal{R}(H)||N| = 2|\mathcal{R}(H)|$ or $4|\mathcal{R}(H)|$. Since $\mathrm{Core}_G(\mathcal{R}(H)) = 1$, we must have $|G : \mathcal{R}(H)| = 4$ and $G \lesssim \mathrm{Sym}(4)$. Since n is odd, one has $n = 3$ and $H \cong \mathrm{Sym}(3)$. So $G \cong \mathrm{Sym}(4)$ and hence $G_{1_0} \cong \mathbb{Z}_2$. Then all involutions of $G(\cong \mathrm{Sym}(4))$ not contained in N are conjugate. Take $1 \neq g \in G_{1_0}$. Then g is an involution which is not contained in N because N is semiregular on $V(\Gamma)$. Since $\mathcal{R}(H) \cap N = 1$, every involution in $\mathcal{R}(H)$ would be conjugate to g. This is clearly impossible because $\mathcal{R}(H)$ is semiregular on $V(\Gamma)$. Thus, N is not semiregular on $V(\Gamma)$. (3) is proved.

Since n is odd, we have $|V(\Gamma_N)| > 2$. Since N is not semiregular on $V(\Gamma)$, Γ_N has valency 2 and $\Gamma[\Delta]$ has valency 0. This implies that the subgraph induced by any two adjacent two orbits of N is either a union of several cycles or a perfect matching. Thus, Γ_N has even order. As Γ has order $4n$ with n odd, every orbit of N has length 2. It is easy to see that Γ is isomorphic to the cross ladder graph CL_{4n}. □

The following is the main result of this section.

Theorem 7.6. *Suppose that H_0 and H_1 are not blocks of imprimitivity of G on $V(\Gamma)$. Then $\Gamma = \mathrm{BiCay}(H, R, L, S)$ is vertex-transitive non-Cayley if and only if one of the followings occurs:*

(1) $(R, L, S) \equiv (\{b, ba\}, \{b, ba^{2m}\}, \{1\})$, *where* $n = 2(2m + 1)$, $m \not\equiv 1 \pmod 3$, *and the corresponding graph is isomorphic the multi-cross ladder graph* $\mathrm{MCL}_{4m,2}$*;*

(2) $(R, L, S) \equiv (\{b, ba\}, \{ba^{24\ell}, ba^{12\ell-1}\}, \{1\})$, *where* $n = 48\ell$ *and* $\ell \geq 1$.

Proof. The sufficiency can be obtained from Theorem 1.2 and Lemma 5.1. We shall prove the necessity in the following subsection by a series of lemmas. □

7.3 Proof of the necessity of Theorem 7.6

The purpose of this subsection is to prove the necessity of Theorem 7.6. Throughout this subsection, we shall always assume that H_0 and H_1 are not blocks of imprimitivity of G on $V(\Gamma)$ and that $\Gamma = \mathrm{BiCay}(H, R, L, S)$ is vertex-transitive non-Cayley. In this subsection, we shall always use the following notation.

Assumption II. Let $N = \mathrm{Core}_G(\mathcal{R}(H))$.

Our first lemma gives some properties of the group N.

Lemma 7.7. $1 < N < \langle\mathcal{R}(a)\rangle$, $|\langle\mathcal{R}(a)\rangle : N| = n/|N|$ *is odd and the quotient graph* Γ_N *of* Γ *relative to* N *is isomorphic to the cross ladder graph* $\mathrm{CL}_{4n/|N|}$.

Proof. If $N = 1$, then from Lemma 7.5 it follows that $\Gamma \cong \mathrm{CL}_{4n}$ which is a Cayley graph by Theorem 1.1, a contradiction. Thus, $N > 1$. Since H_0 and H_1 are not blocks of imprimitivity of G on $V(\Gamma)$, one has $N < \mathcal{R}(H)$.

Consider the quotient graph Γ_N. Clearly, N fixes H_0 setwise. Recall that H_0 and H_1 are not blocks of imprimitivity of G on $V(\Gamma)$ and that Γ is non-Cayley. Applying Lemma 7.4, we see that Γ_N is a trivalent 2-type bi-Cayley graph over $\mathcal{R}(H)/N$. This implies that $|\mathcal{R}(H) : N| > 2$, and since H is a dihedral group, one has $N < \langle \mathcal{R}(a) \rangle$.

Again, by Lemma 7.4, $\mathcal{R}(H)/N$ acts semiregularly on $V(\Gamma_N)$ with two orbits, $\bar{H}_0$ and $\bar{H}_1$, where $\bar{H}_i$ is the set of orbits of N contained in H_i with $i = 1, 0$. Furthermore, N is just the kernel of G acting on $V(\Gamma_N)$ and N acts semiregularly on $V(\Gamma)$. Then G/N is also a minimal vertex-transitive automorphism group of Γ_N containing $\mathcal{R}(H)/N$. If $\bar{H}_0$ and $\bar{H}_1$ are blocks of imprimitivity of G/N on $V(\Gamma_N)$, then H_0 and H_1 will be blocks of imprimitivity of G on $V(\Gamma)$, which is impossible by our assumption. Thus, $\bar{H}_0$ and $\bar{H}_1$ are not blocks of imprimitivity of G/N on $V(\Gamma_N)$. Since $N = \mathrm{Core}_G(\mathcal{R}(H))$, $\mathrm{Core}_{G/N}(\mathcal{R}(H)/N)$ is trivial. Then from Lemma 7.5 it follows that $\Gamma_N \cong \mathrm{CL}_{\frac{4n}{|N|}}$, where $\frac{n}{|N|}$ is odd. □

Next, we introduce another notation which will be used in the proof.

Assumption III. Take M/N to be a minimal normal subgroup of G/N.

We shall first consider some basic properties of the quotient graph Γ_M of Γ relative to M.

Lemma 7.8. *The quotient graph Γ_M of Γ relative to M is a cycle of length $n/|N|$. Furthermore, every orbit of M on $V(\Gamma)$ is a union of an orbit of N on H_0 and an orbit of N on H_1, and these two orbits of N are non-adjacent.*

Proof. Applying Lemma 7.5 to Γ_N and G/N, we obtain the following facts:

(a) M/N is an elementary abelian 2-group which is not regular on $V(\Gamma_N)$,

(b) M/N does not fix $\bar{H}_0$ setwise,

(c) every orbit of M/N on $V(\Gamma_N)$ consists of two non-adjacent vertices of Γ_N.

From (b) and (c) it follows that every orbit of M on $V(\Gamma)$ is just a union of an orbit of N on H_0 and an orbit of N on H_1, and these two orbits are non-adjacent. Since every orbit of N on $V(\Gamma)$ is an independent subset of $V(\Gamma)$, each orbit of M on $V(\Gamma)$ is also an independent subset.

Recall that $\Gamma_N \cong \mathrm{CL}_{4m}$ where $m = \frac{n}{|N|}$ is odd. The quotient graph of Γ_N relative to M/N is just a cycle of length m, and so the quotient graph Γ_M of Γ relative to M is also a cycle of length m. □

By Lemma 7.8, each orbit of M on $V(\Gamma)$ is an independent subset. It follows that the subgraph induced by any two adjacent orbits of M is either a perfect matching or a union of several cycles. For convenience of the statement, the following notations will be used in the remainder of the proof:

Assumption IV.

(1) Let Δ and Δ' be two adjacent orbits of M on $V(\Gamma)$ such that $\Gamma[\Delta \cup \Delta']$ is a union of several cycles.

(2) Let $\Delta = \Delta_0 \cup \Delta_1$ and $\Delta' = \Delta'_0 \cup \Delta'_1$, where $\Delta_0, \Delta'_0 \subseteq H_0$ and $\Delta_1, \Delta'_1 \subseteq H_1$ are four orbits of N on $V(\Gamma)$.

(3) $1_0 \in \Delta_0$.

Since $\Gamma[\Delta]$ and $\Gamma[\Delta']$ are both null graphs and since $\Gamma[\Delta \cup \Delta']$ is a union of several cycles, we have the following easy observation.

Lemma 7.9. *$\Gamma[\Delta_i \cup \Delta'_j]$ is a perfect matching for any $0 \le i, j \le 1$.*

The following lemma tells us the possibility of R (Recall that we assume that $\Gamma = \mathrm{BiCay}(H, R, L, \{1\})$).

Lemma 7.10. *Up to graph isomorphism, we may assume that $R = \{b, ba^i\}$ with $i \in \mathbb{Z}_n \setminus \{0\}$ and that $b_0 \in \Delta'_0$. Furthermore, we have*

$$\Delta_0 = \{h_0 \mid \mathcal{R}(h) \in N\}, \Delta'_0 = \{(bh)_0 \mid \mathcal{R}(h) \in N\},$$
$$\Delta'_1 = \{h_1 \mid \mathcal{R}(h) \in N\}, \Delta_1 = \{(bh)_1 \mid \mathcal{R}(h) \in N\},$$

and 1_1 is adjacent to $(ba^l)_1 \in \Delta_1$ for some $\mathcal{R}(a^l) \in N$.

Proof. Recall that N is a proper subgroup of $\langle \mathcal{R}(a) \rangle$ and that $n/|N|$ is odd. Since n is even by Proposition 7.3, it follows that N is of even order, and so the unique involution $\mathcal{R}(a^{n/2})$ of $\langle \mathcal{R}(a) \rangle$ is contained in N. As $1_0 \in \Delta_0$ and $N \le \langle \mathcal{R}(a) \rangle$ acts on H_0 by right multiplication, one has $\Delta_0 = \{h_0 \mid h \in N\}$. Since $\Gamma[\Delta_0]$ is an empty graph, one has $a^{n/2} \notin R$. By Proposition 2.3 (1), we have $\langle R \cup L \rangle = H$, and since R and L are both self-inverse, either $R \subseteq b\langle a \rangle$ or $L \subseteq b\langle a \rangle$. By Proposition 2.3 (4), we may assume that $R \subseteq b\langle a \rangle$.

Recall that $\Gamma[\Delta_i \cup \Delta'_j]$ is a perfect matching for any $0 \le i, j \le 1$. Then 1_0 is adjacent to $r_0 \in \Delta'_0$ for some $r \in R$. Since $R \subseteq b\langle a \rangle$ and $\mathrm{Aut}\,(H)$ is transitive on $b\langle a \rangle$, by Proposition 2.3 (3), we may assume that $r = b$. So 1_0 is adjacent to $b_0 \in \Delta'_0$. Since $N \le \langle \mathcal{R}(a) \rangle$ acts on H_i with $i = 0$ or 1 by right multiplication, we see that the two orbits Δ_0, Δ'_0 of N are just the form as given in the lemma. Since $S = \{1\}$, the edges between H_0 and H_1 form a perfect matching. This enables us to obtain another two orbits Δ_1, Δ'_1 of N which have the form as given in the lemma.

By Lemma 7.9, $\Gamma[\Delta_1 \cup \Delta'_1]$ is a perfect matching. So we may assume that 1_1 is adjacent to $(ba^l)_1 \in \Delta_1$ for some $\mathcal{R}(a^l) \in N$. □

Now we shall introduce some new notations which will be used in the following.

Assumption V.

(1) Let $T = \langle \mathcal{R}(a^l) \rangle$ be of order t, where a^l is given in the above lemma.

(2) Let

$$\Omega_0 = \{(a^{i\frac{n}{t}})_0 \mid 0 \le i \le t-1\}, \quad \Omega_1 = \{(ba^{i\frac{n}{t}})_1 \mid 0 \le i \le t-1\},$$
$$\Omega'_0 = \{(ba^{i\frac{n}{t}})_0 \mid 0 \le i \le t-1\}, \quad \Omega'_1 = \{(a^{i\frac{n}{t}})_1 \mid 0 \le i \le t-1\}.$$

(3) $\mathcal{B} = \{B^{\mathcal{R}(h)} \mid h \in H\}$, where $B = \Omega_0 \cup \Omega_1$.

(4) Let $B' = \Omega'_0 \cup \Omega'_1$. Then $B' = B^{\mathcal{R}(b)}$.

Lemma 7.11. *The followings hold.*

(1) $T \le N$.

(2) $\Omega_0, \Omega_1, \Omega'_0, \Omega'_1$ *are four orbits of* T.

(3) $\Gamma[\Omega_0 \cup \Omega_1 \cup \Omega'_0 \cup \Omega'_1]$ *is a cycle of length* $4t$.

(4) $\mathcal{B}$ *is a* G*-invariant partition of* $V(\Gamma)$.

Proof. By Lemma 7.10, we see that $\mathcal{R}(a^l) \in N$, and so $T \leq N$. (1) holds. Since $T = \langle \mathcal{R}(a^l) \rangle$ is assumed to be of order t, one has $T = \langle \mathcal{R}(a^{n/t}) \rangle$, and then one can obtain (2). By the adjacency rule of bi-Cayley graph, we can obtain (3).

Set $\Omega = \Omega_0 \cup \Omega_1 \cup \Omega'_0 \cup \Omega'_1$ and $B = \Omega_0 \cup \Omega_1$. By Lemma 7.8, $\Gamma[\Delta]$ is a null graph, and so $B = \Delta \cap \Omega$. Since Γ has valency 3, it follows that $\Delta \cup \Delta'$ is a block of imprimitivity of G on $V(\Gamma)$, and hence Ω is also a block of imprimitivity of G on $V(\Gamma)$ since $\Gamma[\Omega]$ is a component of $\Gamma[\Delta \cup \Delta']$. Since Δ is also a block of imprimitivity of G on $V(\Gamma)$, $B(= \Delta \cap \Omega)$ is a block of imprimitivity of G on $V(\Gamma)$. Then $\mathcal{B} = \{B^{\mathcal{R}(h)} \mid h \in H\}$ is a G-invariant partition of $V(\Gamma)$. □

Lemma 7.12. *$T < N$ and the quotient graph $\Gamma_{\mathcal{B}}$ of Γ relative to $\mathcal{B}$ is isomorphic to the cross ladder graph $\mathrm{CL}_{\frac{4n}{2t}}$. Moreover, T is the kernel of G acting on $\mathcal{B}$.*

Proof. Let $K_{\mathcal{B}}$ be the kernel of G acting on $\mathcal{B}$. Clearly, $T \leq K_{\mathcal{B}}$. Let $B' = \Omega'_0 \cup \Omega'_1$. Then $B' = B^{\mathcal{R}(b)} \in \mathcal{B}$. Let $B^{\mathcal{R}(h)} \in \mathcal{B}$ be adjacent to B and $B^{\mathcal{R}(h)} \neq B'$.

Suppose that $\Gamma[B \cup B^{\mathcal{R}(h)}]$ is a perfect matching. Since G is transitive on $\mathcal{B}$, $\Gamma_{\mathcal{B}}$ is a cycle of length $\frac{2n}{t}$. Clearly, $G/K_{\mathcal{B}}$ is vertex-transitive but not edge-transitive on $\Gamma_{\mathcal{B}}$, so $G/K_{\mathcal{B}} \cong D_{2n/t}$. If $t = 1$, then it is easy to see that $\Gamma \cong \mathrm{CL}_{4n}$ which is a Cayley graph by Theorem 1.1, a contradiction. If $t > 1$, then since $\Gamma[\Omega] = \Gamma[B \cup B']$ is a cycle of length $4t$, $K_{\mathcal{B}}$ acts faithfully on B, and so $K_{\mathcal{B}} \leq \mathrm{Aut}\,(\Gamma[B \cup B']) \cong D_{8t}$. Since $K_{\mathcal{B}}$ fixes B, one has $|K_{\mathcal{B}}| \mid 4t$, implying that $|G| = |K_{\mathcal{B}}| \cdot \frac{2n}{t} \mid 8n$. As $|R(H)| = 2n$ and $\mathcal{R}(H)$ is non-normal in G, one has $|K_{\mathcal{B}}| = 4t$ due to $T \leq K_{\mathcal{B}}$. In view of the fact that $K_{\mathcal{B}} \lesssim D_{8t}$, $K_{\mathcal{B}}$ has a characteristic cyclic subgroup, say J, of order $2t$. Then we have $J \trianglelefteq G$ because $K_{\mathcal{B}} \trianglelefteq G$. Clearly, J is regular on B and $J \cap N = T$, so $J\mathcal{R}(H)$ is regular on $V(\Gamma)$. It follows from Proposition 2.1 that Γ is a Cayley graph, a contradiction.

Therefore, $\Gamma[B \cup B^{\mathcal{R}(h)}]$ is not a perfect matching. If $N = T$, then $B = \Delta$ and $B' = \Delta'$ are orbits of M, and then $\Gamma[B \cup B^{\mathcal{R}(h)}]$ will be a perfect matching, a contradiction. Thus, $N > T$.

Now we are going to prove that $\Gamma_{\mathcal{B}} \cong \mathrm{CL}_{\frac{n}{2t}}$. Since B is adjacent to $B^{\mathcal{R}(h)}$, Ω_i is adjacent to $\Omega_j^{\mathcal{R}(h)}$ for some $i, j \in \{0, 1\}$. Then because Ω_i and $\Omega_j^{\mathcal{R}(h)}$ are orbits of T, $\Gamma[\Omega_i \cup \Omega_j^{\mathcal{R}(h)}]$ is a perfect matching. This implies that $\Gamma_{\mathcal{B}}$ is of valency 3, and so $K_{\mathcal{B}}$ is intransitive on B. As every $B^h \in \mathcal{B}$ is a union of two orbits of T on $V(\Gamma)$, $K_{\mathcal{B}}$ fixes every orbit of T. Since N is cyclic, the normality of N in G implies that $T \trianglelefteq G$. Clearly, Ω_0 is adjacent to three pair-wise different orbits of T, so the quotient graph Γ_T of Γ relative to T is of valency 3. Consequently, the kernel of G acting on $V(\Gamma_T)$ is T. Then $K_{\mathcal{B}} = T$. Now $\mathcal{R}(H)/T \cong D_{2n/t}$ is regular on $\mathcal{B}$, and so $\Gamma_{\mathcal{B}}$ is a Cayley graph over $\mathcal{R}(H)/T$. Furthermore, G/T is not arc-transitive on $\Gamma_{\mathcal{B}}$. Since $\mathcal{R}(H)/T$ is non-normal in G/T, $\Gamma_{\mathcal{B}}$ is a non-normal Cayley graph over $\mathcal{R}(H)/T$. If $\Gamma_{\mathcal{B}}$ is arc-transitive, then by [13, Theorem 1], either $|\mathrm{Aut}\,(\Gamma_{\mathcal{B}})| = 3k|\mathcal{R}(H)/T|$ with $k \leq 2$, or $\Gamma_{\mathcal{B}}$ has order $2 \cdot p$ with $p = 3$ or 7. For the former, since G/T is not arc-transitive on $\Gamma_{\mathcal{B}}$, one has $|G/T : \mathcal{R}(H)/T| \leq 2$, implying $\mathcal{R}(H) \trianglelefteq G$, a contradiction. For the latter, we have $\frac{2n}{t} = 6$ or 14, implying $\frac{n}{t} = 3$ or 7. It follows that T is a maximal subgroup of $\langle \mathcal{R}(a) \rangle$, and so $T = N$, a contradiction.

Therefore, $\Gamma_{\mathcal{B}}$ is not arc-transitive. Since $\mathcal{R}(H)/T$ is non-normal in G/T, by Theorem 1.1, one has $\Gamma_{\mathcal{B}} \cong \mathrm{CL}_{\frac{4n}{2t}}$, as required. □

Proof of Theorem 7.6. By Lemma 7.12, we have $\Gamma_{\mathcal{B}} \cong \mathrm{CL}_{\frac{4n}{2t}}$. By the definition of $\mathrm{CL}_{\frac{4n}{2t}}$, we may partition the vertex set of $\Gamma_{\mathcal{B}}$ in the following way:

$$V(\Gamma_{\mathcal{B}}) = V_0 \cup V_1 \cup \cdots V_{\frac{2n}{2t}-2} \cup V_{\frac{2n}{2t}-1}, \text{ where } V_i = \{B_i^0, B_i^1\}, i \in \mathbb{Z}_{\frac{2n}{2t}}$$

and

$$E(\Gamma_{\mathcal{B}}) = \{\{B_{2i}^r, B_{2i+1}^r\}, \{B_{2i+1}^r, B_{2i+2}^s\} \mid i \in \mathbb{Z}_{\frac{n}{2t}}, r, s \in \mathbb{Z}_2\}.$$

Assume that $B_0^0 = B$ and $B_1^0 = B'$. Recall that $B = \Omega_0 \cup \Omega_1$ and $B' = \Omega_0' \cup \Omega_1' = B^{\mathcal{R}(b)}$. Moreover, $\Omega_0, \Omega_1, \Omega_0'$ and Ω_1' are four orbits of T. Then every $B_i^j \in \mathcal{B}$ is just a union of two orbits of T. For convenience, we may let

$$B_i^j = \Omega_{i0}^j \cup \Omega_{i1}^j, i \in \mathbb{Z}_{\frac{2n}{2t}}, j \in \mathbb{Z}_2,$$

where $\Omega_{i0}^j, \Omega_{i1}^j$ are two orbits of T. For $B = B_0^0$, we let $\Omega_0 = \Omega_{00}^0$ and $\Omega_1 = \Omega_{01}^0$, and for $B' = B_1^0$, we let $\Omega_0' = \Omega_{10}^0$ and $\Omega_1' = \Omega_{11}^0$.

For convenience, in the remainder of the proof, we shall use C_{4t} to denote a cycle of length $4t$, and we also call C_{4t} a $4t$-cycle. Recall that $\Gamma[B \cup B'] = \Gamma[B_0^0 \cup B_1^0] \cong \mathrm{C}_{4t}$, and that the edges between $\Omega_{0i}^0 (= \Omega_i)$ and $\Omega_{1j}^0 (= \Omega_j')$ form a perfect matching for all $i, j \in \mathbb{Z}_2$. Since $T \trianglelefteq G$, the quotient graph Γ_T of Γ relative to T has valency 3. So the edges between any two adjacent orbits of T form a perfect matching.

From the construction of $\Gamma_{\mathcal{B}}$, one may see that there exists $g \in G$ such that $\{V_0, V_1\}^g = \{V_{2i}, V_{2i+1}\}$ for each $i \in \mathbb{Z}_{\frac{n}{2t}}$. So for each $i \in \mathbb{Z}_{\frac{n}{2t}}, r \in \mathbb{Z}_2$, we may assume that $\Gamma[B_{2i}^r \cup B_{2i+1}^r] \cong \mathrm{C}_{4t}$, and $\Omega_{(2i)s}^r \sim \Omega_{(2i+1)t}^r$ for all $s, t \in \mathbb{Z}_2$. (Here $\Omega_{(2i)s}^r \sim \Omega_{(2i+1)t}^r$ means that $\Omega_{(2i)s}^r$ and $\Omega_{(2i+1)t}^r$ are adjacent in $\Gamma_{\mathcal{B}}$.) Again, from the construction of $\Gamma_{\mathcal{B}}$, we may assume that

$$\Omega_{(2i+2)0}^0 \sim \Omega_{(2i+1)0}^0, \Omega_{(2i+2)1}^0 \sim \Omega_{(2i+1)0}^1, \Omega_{(2i+2)1}^1 \sim \Omega_{(2i+1)0}^1, \Omega_{(2i+2)1}^1 \sim \Omega_{(2i+1)0}^0,$$

for each $i \in \mathbb{Z}_{\frac{n}{2t}}$. We draw a local subgraph of $\Gamma_{\mathcal{B}}$ in Figure 3. Observing that every

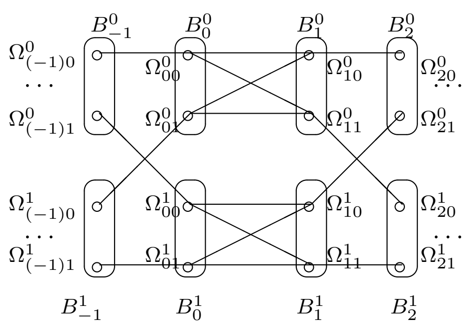


Figure 3: The sketch graph of $\Gamma_{\mathcal{B}}$

$V_i = \{B_i^0, B_i^1\}$ with $i \in \mathbb{Z}_{\frac{2n}{2t}}$ is a block of imprimitivity of $G/K_{\mathcal{B}}$ acting on $V(\Gamma_{\mathcal{B}})$. So every $B_i^0 \cup B_i^1$ with $i \in \mathbb{Z}_{\frac{2n}{2t}}$ is a block of imprimitivity of G acting on $V(\Gamma)$. Let E be the kernel of G acting on the block system $\Lambda = \{B_i^0 \cup B_i^1 \mid i \in \mathbb{Z}_{\frac{2n}{2t}}\}$. Then $G/E \cong D_{\frac{n}{t}}$

acts regularly on Λ. Clearly, $\mathcal{R}(H)$ is also transitive on Ω, so $G/E = \mathcal{R}(H)E/E$. By Lemma 7.12, T is a the kernel of G acting on $\mathcal{B}$. So E/T is an elementary 2-group. From $\mathcal{R}(H)/(\mathcal{R}(H) \cap E) \cong D_{\frac{n}{t}}$ it follows that $\mathcal{R}(H) \cap E = \langle \mathcal{R}(a^{\frac{n}{2t}}) \rangle \cong \mathbb{Z}_{2t}$, and so $(\mathcal{R}(H) \cap E)/T$ is a normal subgroup of G/T of order 2. This implies that $B_i^1 = (B_i^0)^{\mathcal{R}(a^{\frac{n}{2t}})}$ for $i \in \mathbb{Z}_{\frac{2n}{2t}}$. We may further assume that $\Omega_{01}^1 = (\Omega_{00}^0)^{\mathcal{R}(a^{\frac{n}{2t}})} \subseteq B_0^1$. So $\Omega_{00}^0 \cup \Omega_{01}^1$ is just the orbit of $\langle \mathcal{R}(a^{\frac{n}{2t}}) \rangle$ containing 1_0.

Observing that $\Omega_{10}^0 \sim \Omega_{20}^0$ and the edges between them are of the form $\{g_0, (ba^i g)_0\}$ with $g_0 \in \Omega_{10}^0$, one has $\Omega_{20}^0 = ba^i \Omega_{10}^0 = ba^i(\Omega_{00}^0)^{\mathcal{R}(b)} = (\Omega_{00}^0)^{\mathcal{R}(a^{-i})}$. So $\Omega_{20}^1 \subseteq (B_0^1)^{\mathcal{R}(a^{-i})}$.

Since $B_1^0 = B' = B^{\mathcal{R}(b)} = (B_0^0)^{\mathcal{R}(b)}$, one has $B_1^1 = (B_0^1)^{\mathcal{R}(b)}$. Recall that $1_1 \in \Omega_{11}^0 = \Omega_1'$ and 1_1 is adjacent to $1_0 \in \Omega_{00}^0 = \Omega_0$ and $(ba^l)_1 \in \Omega_{01}^0 = \Omega_1$. As we assume that $\Omega_{11}^0 \sim \Omega_{20}^1$, 1_1 is adjacent to some vertex in Ω_{20}^1. So $\Omega_{20}^1 \subseteq H_1$ and hence

$$\begin{aligned}\Omega_{20}^1 &= (\Omega_{00}^1)^{\mathcal{R}(a^{-i})}\\ &= (\Omega_{01}^0)^{\mathcal{R}(a^{\frac{n}{2t}})\mathcal{R}(a^{-i})}\\ &= (\Omega_{01}^0)^{\mathcal{R}(a^{\frac{n}{2t}-i})}\\ &= \{(ba^{k\frac{n}{t}})_1 \mid 0 \le k \le t-1\}^{\mathcal{R}(a^{\frac{n}{2t}-i})}.\end{aligned}$$

So we have the following claim.

Claim 1 $L = \{ba^l, ba^{k\frac{n}{t}+\frac{n}{2t}-i}\}$ and $R = \{ba^i, b\}$, where $|\mathcal{R}(a^l)| = t$, $i \in \mathbb{Z}_n$ and $0 \le k \le t-1$.

Let $G_{1_0}^*$ be the kernel of G_{1_0} acting on the neighborhood of 1_0 in Γ. Then $G_{1_0}^* \le E_{1_0}$. Recall that for each $i \in \mathbb{Z}_{\frac{n}{2t}}, r \in \mathbb{Z}_2$, $\Gamma[B_{2i}^r \cup B_{2i+1}^r] \cong \mathrm{C}_{4t}$ and the edges between $B_{2i+1}^0 \cup B_{2i+1}^1$ and $B_{2i+2}^0 \cup B_{2i+2}^1$ form a perfect matching. It follows that E acts faithfully on each $B_i^0 \cup B_i^1$. Clearly, $G_{1_0}^* \le E_{1_0}$, so $G_{1_0}^*$ acts faithfully on each $B_i^0 \cup B_i^1$.

Claim 2 If $t > 2$ then $G_{1_0}^* = 1$, and if $t = 2$ then $G_{1_0}^* \le \mathbb{Z}_2$ and $3 \mid n$.

Assume that $t \ge 2$. Since $\Gamma[B_0^0 \cup B_1^0] \cong \mathrm{C}_{4t}$, $G_{1_0}^*$ fixes every vertex in B_0^0, and so fixes every vertex in $\Omega_{(-1)0}^0$ since $\Omega_{(-1)0}^0 \sim \Omega_{00}^0$ (see Figure 3). This implies that $G_{1_0}^*$ fixes $\Omega_{(-1)1}^0$ setwise, and so fixes Ω_{00}^1 setwise since $\Omega_{(-1)1}^0 \sim \Omega_{00}^1$. Consequently, $G_{1_0}^*$ also fixes Ω_{01}^1 setwise. Similarly, by considering the edges between $B_1^0 \cup B_1^1$ and $B_2^0 \cup B_2^1$, we see that $G_{1_0}^*$ fixes both Ω_{10}^1 and Ω_{11}^1 setwise. Recall that the edges between Ω_{0i}^1 and Ω_{1j}^1 form a perfect matching for $i, j \in \mathbb{Z}_2$. As $\Gamma[B_1^0 \cup B_1^1] \cong \mathrm{C}_{4t}$, $G_{1_0}^*$ acts faithfully on Ω_{00}^1 (or Ω_{01}^1), and so $G_{1_0}^* \le \mathbb{Z}_2$.

If $t > 2$, then since $\Gamma[B_{-2}^0 \cup B_{-1}^0] \cong \mathrm{C}_{4t}$, $G_{1_0}^*$ will fix every vertex in this cycle, and in particular, $G_{1_0}^*$ will fix every vertex in $\Omega_{(-1)1}^0$. As $\Omega_{(-1)1}^0 \sim \Omega_{00}^1$, $G_{1_0}^*$ will fix every vertex in Ω_{00}^1. Since $G_{1_0}^*$ acts faithfully on Ω_{00}^1, one has $G_{1_0}^* = 1$.

Let $t = 2$. We shall show that $3 \mid n$. Then $T = \langle \mathcal{R}(a^{\frac{n}{2}}) \rangle$. Recall that $(\mathcal{R}(H) \cap E)/T$ is a normal subgroup of G/T of order 2. Let $M = \mathcal{R}(H) \cap E$. Then M is a normal subgroup of G of order 4. Since $\mathcal{R}(H)$ is dihedral, one has $M = \langle \mathcal{R}(a^{\frac{n}{4}}) \rangle$. Let $C = C_G(M)$. Then $\mathcal{R}(a) \in C$ and $\mathcal{R}(b) \notin C$. It follows that C is a proper subgroup of G. Since G/E acts regularly on Λ, C_{1_0} fixes every element in Λ. Since C_{1_0} centralizes M, C_{1_0} fixes every vertex in the orbit $\Omega_{00}^0 \cup \Omega_{01}^1$ of M containing 1_0. Clearly, $C_{1_0} \le G_{1_0}$, so $C_{1_0}/(C_{1_0} \cap G_{1_0}^*) \le \mathbb{Z}_2$. As we have shown that $G_{1_0}^*$ acts faithfully on Ω_{01}^1, it follows that

$C_{1_0} \cap G^*_{1_0} = 1$ since C_{1_0} fixes Ω^1_{01} pointwise, and hence $C_{1_0} \leq \mathbb{Z}_2$. On the other hand, as $G^*_{1_0} \leq \mathbb{Z}_2$, one has $|G| \mid 4 \cdot 4n = 16n$. Since $C < G$ and $\mathcal{R}(a) \in C$, one has $|C| = kn$ with $k \mid 8$.

Suppose that $3 \nmid n$. For any odd prime divisor p of n, let P be a Sylow p-subgroup of $\langle \mathcal{R}(a) \rangle$. Then P is also a Sylow p-subgroup of C. If P is not normal in C, then by Sylow's theorem, we have $|C : N_C(P)| = k'p + 1 \mid 8$ for some integer k'. Since $p \neq 3$, one has $p = 7$ and $k' = 1$. This implies that $|C| = 8|N_C(P)|$, and so $|C| = 8n$ due to $\mathcal{R}(a) \in C$ and $C < G$. Since $C_{1_0} \leq \mathbb{Z}_2$, one has $|C : C_{1_0}| \geq 4n$, and so C is transitive on $V(\Gamma)$. Moreover, we have $C_C(P) = N_C(P) = \langle \mathcal{R}(a) \rangle$. By Burnside theorem, C has a normal subgroup M such that $C = M \rtimes P$. Then the quotient graph Γ_M of Γ relative to M would be a cycle of length $|P|$, and the subgraph induced by each orbit of M is just a perfect matching. This implies that M is just the kernel of G acting on $V(\Gamma_M)$. Furthermore, C/M is a vertex-transitive subgroup of $\mathrm{Aut}\,(\Gamma_M)$. Since Γ_M is a cycle, C/M must contain a subgroup, say B/M acting regularly on $V(\Gamma_M)$. Then B will be regular on $V(\Gamma)$, and so by Proposition 2.1, Γ is a Cayley graph, a contradiction. Therefore, $P \trianglelefteq C$, and since $C \trianglelefteq G$, one has $P \trianglelefteq G$, implying $P \leq N$. By the arbitrariness of P, $n/|N|$ must be even, contrary to Lemma 7.7. Thus, $3 \mid n$, as claimed.

The following claim shows that $t = 1$ or 2.

Claim 3 $t \leq 2$.

By way of contradiction, suppose that $t > 2$. Let $C = C_G(T)$. Then $\langle \mathcal{R}(a) \rangle \leq C$ and $\mathcal{R}(H) \nleq C$ since $|T| = t > 2$. Clearly, $C_{1_0} \leq E_{1_0}$. As C_{1_0} centralizes T, C_{1_0} will fixes every vertex in Ω^0_{00} since Ω^0_{00} is an orbit of T containing 1_0. Since $\Gamma[B^0_0 \cup B^0_1] \cong \mathrm{C}_{4t}$, C_{1_0} fixes every vertex in this $4t$-cycle, and so $C_{1_0} \leq G^*_{1_0} = 1$ (by Claim 2). Thus, C acts semiregularly on $V(\Gamma)$. If $C = \langle \mathcal{R}(a) \rangle$, then by N/C-theorem, we have $G/\langle \mathcal{R}(a) \rangle = G/C \leq \mathrm{Aut}\,(T)$. Since $T \leq N \leq \langle \mathcal{R}(a) \rangle$ is cyclic, $\mathrm{Aut}\,(T)$ is abelian. It then follows that $\mathcal{R}(H)/C \trianglelefteq G/C$, and hence $\mathcal{R}(H) \trianglelefteq G$, a contradiction. If $C > \langle \mathcal{R}(a) \rangle$, then $|C| = 2n$ because Γ is non-Cayley. Since H_0 and H_1 are not blocks of imprimitivity of G on $V(\Gamma)$, C does not fix H_0 setwise, and so $\mathcal{R}(H)C$ is transitive on $V(\Gamma)$. Clearly, $\mathcal{R}(H) \cap C = \langle \mathcal{R}(a) \rangle$, so $|\mathcal{R}(H)C| = |\mathcal{R}(H)||C|/|\langle \mathcal{R}(a) \rangle| = 4n$. It follows that $\mathcal{R}(H)C$ is regular on $V(\Gamma)$, contradicting that Γ is non-Cayley.

By Claim 3, we only need to consider the following two cases:

Case 1 $t = 1$.

In this case, by Claim 1, we have $R = \{b, ba^i\}$ and $L = \{b, ba^{\frac{n}{2}-i}\}$. For convenience, we let $n = 2\ell$. Then $R = \{b, ba^i\}$ and $L = \{b, ba^{\ell-i}\}$.

By Proposition 2.3 (1), the connectedness of Γ implies that $\langle a^i, a^\ell \rangle = \langle a \rangle$. Then either $(i, 2\ell) = 1$, or $i = 2k$ with $(k, 2\ell) = 1$ and ℓ is odd. Recall that $H = \langle a, b \mid a^{2\ell} = b^2 = 1, bab = a^{-1} \rangle$. For any $\lambda \in \mathbb{Z}^*_{2\ell}$, let α_λ be the automorphism of H induced by the map

$$a^\lambda \mapsto a,\ b \mapsto b.$$

So if $(i, 2\ell) = 1$, then we have

$$(R, L)^{\alpha_i} = (\{b, ba\}, \{b, ba^{\ell-1}\}),$$

and if $i = 2k$ with $(k, 2\ell) = 2$ and ℓ is odd, then we have

$$(R, L)^{\alpha_k} = (\{b, ba^2\}, \{b, ba^{\ell-2}\}).$$

So by Proposition 2.3 (3), we have

$$(R, L, S) \equiv (\{b, ba\}, \{b, ba^{\ell-1}\}, \{1\}) \text{ or } (\{b, ba^2\}, \{b, ba^{\ell-2}\}, \{1\})(\ell \text{ is odd}).$$

Suppose that ℓ is even. Then $(R, L, S) \equiv (\{b, ba\}, \{b, ba^{\ell-1}\}, \{1\})$. Since ℓ is even, one has $(2\ell, \ell+1) = 1$ and $(\ell+1)^2 \equiv 1 \pmod{2\ell}$. Then it is easy to check that $\alpha_{\ell+1}$ is an automorphism of H of order 2 that swaps $\{b, ba\}$ and $\{b, ba^{\ell-1}\}$. By Proposition 2.4, we have $\delta_{\alpha_{\ell+1},1,1} \in I$, and then $\Gamma \cong \mathrm{BiCay}(H, \{b, ba\}, \{b, ba^{\ell+1}\}, \{1\})$ is a Cayley graph, a contradiction.

Now we assume that $n = 2\ell$ with $\ell = 2m + 1$ for some integer m. Let

$$\Gamma_1 = \mathrm{BiCay}(H, \{b, ba\}, \{b, ba^{2m}\}, \{1\}), \Gamma_2 = \mathrm{BiCay}(H, \{b, ba^2\}, \{b, ba^{2m-1}\}, \{1\}).$$

Direct calculation shows that $(n, 2m-1) = 1$, and $2m(2m-1) \equiv 2 \pmod{n}$. Then the automorphism $\alpha_{2m-1} : a \mapsto a^{2m-1},\ b \mapsto b$ maps the pair of two subsets $(\{b, ba\}, \{b, ba^{2m}\})$ to $(\{b, ba^{2m-1}\}, \{b, ba^2\})$. So, we have $(R, L, S) \equiv (\{b, ba\}, \{b, ba^{2m}\}, \{1\})$. By Lemma 4.1 and Theorem 1.2, $\Gamma \cong \mathrm{MCL}(4m, 2)$ and Γ is non-Cayley if and only if $3 \nmid (2m+1)$. Note that $3 \nmid (2m+1)$ is equivalent to $m \not\equiv 1 \pmod 3$. So we obtain the first family of graphs in Theorem 7.6.

Case 2 $t = 2$.

In this case, by Claim 1, we have $R = \{b, ba^i\}$ and $L = \{ba^{\frac{n}{2}}, ba^{\frac{3n}{4}-i}\}$ or $\{ba^{\frac{n}{2}}, ba^{\frac{n}{4}-i}\}$. We still use the following notation: For any $\lambda \in \mathbb{Z}_{2\ell}^*$, let α_λ be the automorphism of H induced by the map

$$a^\lambda \mapsto a,\ b \mapsto b.$$

Note that

$$(\{b, ba^i\}, \{ba^{\frac{n}{2}}, ba^{\frac{3n}{4}-i}\})^{\alpha_{-1}} = (\{b, ba^{-i}\}, \{ba^{\frac{n}{2}}, ba^{\frac{n}{4}-(-i)}\}).$$

By replacing $-i$ by i, we may always assume that

$$(R, L) = (\{b, ba^i\}, \{ba^{\frac{n}{2}}, ba^{\frac{n}{4}-i}\}).$$

By Claim 2, we have $3 \mid n$. So we may assume that $n = 12m$ for some integer m. Then we have

$$(R, L) = (\{b, ba^i\}, \{ba^{6m}, ba^{3m-i}\}).$$

Since Γ is connected, by Proposition 2.3, we have $\langle a^i, a^{3m}\rangle = \langle a\rangle$. If m is odd, by Lemma 6.1, Γ will be a Cayley graph which is impossible. Thus, m is even. It then follows that $\langle a^i\rangle \cap \langle a^{3m}\rangle > 1$ since $\langle a^i, a^{3m}\rangle = \langle a^i\rangle\langle a^{3m}\rangle = \langle a\rangle$. Since $\langle a^{3m}\rangle \cong \mathbb{Z}_4$, one has $|\langle a^i\rangle \cap \langle a^{3m}\rangle| = 2$ or 4. For the former, we would have $|\langle a^i\rangle| = 6m$, and since m is even, one has $4 \mid |\langle a^i\rangle|$, and hence $a^{3m} \in \langle a^i\rangle$, a contradiction. Thus, we have $|\langle a^i\rangle \cap \langle a^{3m}\rangle| = 4$, that is, $\langle a^i\rangle = \langle a\rangle$. So $(i, 12m) = 1$, and then $\alpha_i \in \mathrm{Aut}\,(H)$ which maps $(\{b, ba^i\}, \{ba^{6m}, ba^{3m-i}\})$ to $(\{b, ba\}, \{ba^{6m}, ba^{3m-1}\})$ or $(\{b, ba\}, \{ba^{6m}, ba^{-3m-1}\})$. Then

$$(R, L, S) \equiv (\{b, ba\}, \{ba^{6m}, ba^{3m-1}\}, \{1\}) \text{ or } (\{b, ba\}, \{ba^{6m}, ba^{-3m-1}\}), \{1\}.$$

If $m \equiv 2 \pmod 4$, then by Lemma 6.2, we see that Γ will be a Cayley graph, a contradiction. Thus, $m \equiv 0 \pmod 4$. Clearly, $(3m-1, 12m) = 1$, and hence the map $a \mapsto a^{3m-1}, b \mapsto ba^{6m}$ induces an automorphism, say β of H. It is easy to check that

$$(\{b, ba\}, \{ba^{6m}, ba^{3m-1}\})^\beta = (\{ba^{6m}, ba^{-3m-1}\}, \{b, ba\}).$$

Thus,

$$(R, L, S) \equiv (\{b, ba\}, \{ba^{6m}, ba^{3m-1}\}, \{1\}).$$

By Proposition 5.1, Γ is a non-Cayley graph. Let $m = 4\ell$ for some integer ℓ. Then $n = 48\ell$ and then we get the second family of graphs in Theorem 7.6. This completes the proof of Theorem 7.6. □

7.4 Proof of Theorem 1.3

By [20, Theorem 1.2], if Γ is 0- or 1-type, then Γ is a Cayley graph. Let Γ be of 2-type. Suppose that Γ is a non-Cayley graph. Let $G \leq \mathrm{Aut}(\Gamma)$ be minimal subject to that $\mathcal{R}(H) \leq G$ and G is transitive on $V(\Gamma)$. If Γ is arc-transitive or H_0 and H_1 are blocks of imprimitivity of G on $V(\Gamma)$, then by [20, Theorem 1.1] and Proposition 7.2, we obtain the graphs in part (1)–(3) of Theorem 1.3. Otherwise, Γ is not arc-transitive and H_0 and H_1 are not blocks of imprimitivity of G on $V(\Gamma)$, by Theorem 7.6, we obtain the last two families of graphs of Theorem 1.3. □

ORCID iDs

Mi-Mi Zhang https://orcid.org/0000-0002-8719-5888
Jin-Xin Zhou https://orcid.org/0000-0002-8353-896X

References

[1] M. Alaeiyan, M. Ghasemi and G. R. Safakish, The normality of cubic Cayley graphs for dihedral groups, *Vietnam J. Math.* **37** (2009), 43–48, `http://www.math.ac.vn/publications/vjm/VJM_37/43.htm`.

[2] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, 1993.

[3] J. Bondy and U. Murty, *Graph Theory with Applications*, Elsevier Science Ltd/North-Holland, 1976.

[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265, doi:10.1006/jsco.1996.0125, computational algebra and number theory (London, 1993).

[5] P. Cameron, J. Sheehan and P. Spiga, Semiregular automorphisms of vertex-transitive cubic graphs, *European J. Combin.* **27** (2006), 924–930, doi:10.1016/j.ejc.2005.04.008.

[6] E. Dobson, A. Malnič, D. Marušič and L. A. Nowitz, Semiregular automorphisms of vertex-transitive graphs of certain valencies, *J. Combin. Theory Ser. B* **97** (2007), 371–380, doi:10.1016/j.jctb.2006.06.004.

[7] S. Du, A. Malnič and D. Marušič, Classification of 2-arc-transitive dihedrants, *J. Combin. Theory Ser. B* **98** (2008), 1349–1372, doi:10.1016/j.jctb.2008.02.007.

[8] R. Frucht, J. E. Graver and M. E. Watkins, The groups of the generalized Petersen graphs, *Proc. Cambridge Philos. Soc.* **70** (1971), 211–218, doi:10.1017/s0305004100049811.

[9] C. D. Godsil, On the full automorphism group of a graph, *Combinatorica* **1** (1981), 243–256, doi:10.1007/bf02579330.

[10] C. D. Godsil, The automorphism groups of some cubic Cayley graphs, *European J. Combin.* **4** (1983), 25–32, doi:10.1016/s0195-6698(83)80005-5.

[11] I. Kovács, B. Kuzman, A. Malnič and S. Wilson, Characterization of edge-transitive 4-valent bicirculants, *J. Graph Theory* **69** (2012), 441–463, doi:10.1002/jgt.20594.

[12] D. Marušič, On 2-arc-transitivity of Cayley graphs, *J. Combin. Theory Ser. B* **87** (2003), 162–196, doi:10.1016/s0095-8956(02)00033-3, dedicated to Crispin St. J. A. Nash-Williams.

[13] D. Marušič and T. Pisanski, Symmetries of hexagonal molecular graphs on the torus, *Croat. Chem. Acta* **73** (2000), 969–981, `https://hrcak.srce.hr/131972`.

[14] R. Nedela and M. Škoviera, Which generalized Petersen graphs are Cayley graphs?, *J. Graph Theory* **19** (1995), 1–11, doi:10.1002/jgt.3190190102.

[15] T. Pisanski, A classification of cubic bicirculants, *Discrete Math.* **307** (2007), 567–578, doi:10.1016/j.disc.2005.09.053.

[16] P. Potočnik, P. Spiga and G. Verret, Cubic vertex-transitive graphs on up to 1280 vertices, *J. Symbolic Comput.* **50** (2013), 465–477, doi:10.1016/j.jsc.2012.09.002.

[17] M. E. Watkins, A theorem on Tait colorings with an application to the generalized Petersen graphs, *J. Combinatorial Theory* **6** (1969), 152–164.

[18] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

[19] M.-Y. Xu, Automorphism groups and isomorphisms of Cayley digraphs, *Discrete Math.* **182** (1998), 309–319, doi:10.1016/s0012-365x(97)00152-0, graph theory (Lake Bled, 1995).

[20] M.-M. Zhang and J.-X. Zhou, Trivalent vertex-transitive bi-dihedrants, *Discrete Math.* **340** (2017), 1757–1772, doi:10.1016/j.disc.2017.03.017.

[21] W.-J. Zhang, Y.-Q. Feng and J.-X. Zhou, Cubic vertex-transitive non-Cayley graphs of order $12p$, *Sci. China Math.* **61** (2018), 1153–1162, doi:10.1007/s11425-016-9095-8.

[22] C. Zhou and Y.-Q. Feng, Automorphism groups of connected cubic Cayley graphs of order $4p$, *Algebra Colloq.* **14** (2007), 351–359, doi:10.1142/s100538670700034x.

[23] J.-X. Zhou and Y.-Q. Feng, Cubic vertex-transitive non-Cayley graphs of order $8p$, *Electron. J. Combin.* **19** (2012), Paper 53, 13, doi:10.37236/2087.

[24] J.-X. Zhou and Y.-Q. Feng, Cubic bi-Cayley graphs over abelian groups, *European J. Combin.* **36** (2014), 679–693, doi:10.1016/j.ejc.2013.10.005.

[25] J.-X. Zhou and Y.-Q. Feng, The automorphisms of bi-Cayley graphs, *J. Combin. Theory Ser. B* **116** (2016), 504–532, doi:10.1016/j.jctb.2015.10.004.

[26] J.-X. Zhou and M. Ghasemi, Automorphisms of a family of cubic graphs, *Algebra Colloq.* **20** (2013), 495–506, doi:10.1142/s1005386713000461.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.03 / 201–217
https://doi.org/10.26493/1855-3974.2260.c0e
(Also available at http://amc-journal.eu)

A generalization of balanced tableaux and marriage problems with unique solutions

Brian Tianyao Chan *

KeyFi, First Floor, First St. Vincent Bank Ltd. Building James Street, Kingstown, St. Vincent and the Grenadines

Received 22 February 2020, accepted 24 February 2021, published online 30 September 2021

Abstract

We consider families of finite sets that we call flagged and that have been characterized by Chang as being the families of sets that admit unique solutions to Hall's marriage problem and we consider generalizations of Edelman and Greene's balanced tableaux previously investigated by Viard. In this paper, we introduce a natural generalization of Edelman and Greene's balanced tableaux that involves families of sets that satisfy Hall's marriage condition and certain words in $[m]^n$, then prove that flagged families can be characterized by a strong existence condition relating to this generalization. As a consequence of this characterization, we show that the arithmetic mean of the sizes of subclasses of such generalized tableaux is given by a generalization of the hook-length formula.

Keywords: Balanced tableaux, Hall's marriage condition, shelling.

Math. Subj. Class. (2020): 05A20, 05C70, 05E45

1 Introduction

Hall's Marriage Theorem is a combinatorial theorem proved by Hall [11] that asserts that a finite family of sets has a transversal if and only if this family satisfies the marriage condition. This theorem is known to be equivalent to at least six other theorems which include Dilworth's Theorem, Menger's Theorem, and the Max-Flow Min-Cut Theorem [20]. Hall Jr. proved [10] that Hall's Marriage Theorem also holds for arbitrary families of finite sets, where by arbitrary we mean families of finite sets that do not necessarily have a finite number of members. Afterwards, Chang [3] noted how Hall Jr.'s work in [10] can be used to characterize marriage problems with unique solutions.

*The author would like to thank Stephanie van Willigenburg for her guidance and advice during the development of this paper. Furthermore, the author gratefully acknowledges the insightful advice and feedback from the anonymous referees. The author was supported in part by the Natural Sciences and Engineering Research Council of Canada [funding reference number PGSD2 - 519022 - 2018]. https://sites.google.com/view/btchan

E-mail address: bchan600@gmail.com (Brian Tianyao Chan)

Standard skew tableaux are well-known and intensively studied in algebraic combinatorics, for example [15, 18, 19, 21]. Moreover, another class of tableaux was introduced by Edelman and Greene in [5, 4], where they defined balanced tableaux on partition shapes. In investigating the number of maximal chains in the weak Bruhat order of the symmetric group, Edelman and Greene proved [5, 4] that the number of balanced tableaux of a given partition shape equals the number of standard Young tableaux of that shape. Since then, connections to random sorting networks [1], the Lascoux-Schützenberger tree [16], and a generalization of balanced tableaux pertaining to Schubert polynomials [7] have been explored.

In this paper we consider a new perspective for marriage problems with unique solutions by interpreting such objects as shapes for generalized tableaux. Specifically we call the families of finite sets that admit marriage problems with unique solutions *flagged* and give a new characterization of these families of sets in Theorem 3.10. In this characterization, we generalize standard skew tableaux and Edelman and Greene's balanced tableaux to families with systems of distinct representatives, we generalize hook sets to members of such families, and we generalize bijective fillings of tableaux to certain words in $[m]^n$. We then use our characterization of marriage problems with unique solutions to show in Theorem 3.25 that the arithmetic mean of the sizes of subclasses of such generalized tableaux is given by a generalization of the hook-length formula. The *hook-length formula* was discovered by Frame, Robinson, and Thrall and they proved that it enumerates the number of *standard Young tableaux* of a given partition shape [8]. The formula consists of parameters known as *hook-lengths*. Subsequent to Frame, Robinson and Thrall's work, hook-lengths have been shown to be connected to many known properties of tableaux. They are integral, for instance, in work by Edelman and Greene on balanced tableaux [4] and in results established by Morales, Pak, and Panova [17, 18]. Properties of Edelman and Greene's balanced tableaux and related notions are of interest [6, 7]. Moreover, generalizations of balanced tableaux were investigated by Viard. In [24, 23], Viard proved what is equivalent to the following which we state using the terminology in this paper. If $\mathcal{F}$ is a flagged family, if t is a transversal of $\mathcal{F}$, and if f is a configuration of t, then there exists a permutation σ that satisfies f. Moreover, Viard proved [24] what is equivalent to the following which we also state using the terminology in this paper. Let S be a finite subset of $\mathbb{N}^2$ and let $\mathcal{F}$ be the family of hooks $\{H_{(i,j)} : (i,j) \in S\}$ where $H_{(i,j)} = \{(i,j)\} \cup \{(i,j') \in S : j' > j\} \cup \{(i',j) \in S : i' > i\}$. Furthermore, let t be the transversal of $\mathcal{F}$ defined by $t(H_{(i,j)}) = (i,j)$ for all $(i,j) \in S$. Then the average value of $A_{n,n}(f)$ over all configurations f of t satisfying $A_{n,n}(f) \geq 1$ is given by the hook-length formula $n!/\prod_{(i,j)\in S} h_{(i,j)}$ where $h_{(i,j)} = |H_{(i,j)}|$ for all $(i,j) \in S$. Afterwards, we indicate how our generalization of standard skew tableaux and balanced tableaux can be analysed using Naruse's Formula for skew tableaux and how such an approach can be extended to skew shifted shapes [9, 17, 19] and likely to certain d-complete posets [9, 19].

2 Preliminaries

Throughout this paper, let $\mathbb{N}$ denote the set of positive integers and for all $n \in \mathbb{N}$, define $[n] = \{1, 2, \dots, n\}$. For all $X' \subseteq X$, let the *restriction of f to X'*, which we denote by $f|_{X'}$, be the function $g : X' \to Y$ defined by $g(r) = f(r)$ for all $r \in X'$. For all $m, n \in \mathbb{N}$, say that a function $f : [n] \to [m]$ is *order-preserving* if for all $1 \leq i \leq j \leq n$, $f(i) \leq f(j)$. Lastly, we write examples of permutations using one-line notation. When describing families of sets, call $F \in \mathcal{F}$ a *member* of $\mathcal{F}$. We treat families of sets as multisets, so the members of $\mathcal{F}$ are counted with multiplicity. That is, $|\mathcal{F}| = |I|$ if $\mathcal{F} = \{F_i : i \in I\}$.

An illustrative class of examples that we use in this paper will come from skew shapes. Hence, we recall them below and describe the notation we will use. A *partition* λ is a weakly decreasing sequence of positive integers. We write $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_\ell)$ to denote such a partition, where $\lambda_i \in \mathbb{N}$ for all $1 \le i \le \ell$. If λ is a partition, then we will also represent it as a *Young diagram*, which we also denote by λ. Specifically, the *Young diagram of* $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_\ell)$ is a subset of $\mathbb{N}^2$ defined by

$$\bigcup_{i=1}^{\ell} \{(i, j) : 1 \le j \le \lambda_i\}.$$

Moreover, if λ and μ are Young diagrams such that $\mu \subset \lambda$, then define a *skew shape* λ/μ to be the set $\lambda \backslash \mu$. We also consider a Young diagram λ as the skew shape λ/μ where μ is the *empty partition*. We use the English convention for depicting Young diagrams and skew shapes. In order to follow this convention, we call the elements of λ/μ the *cells of* λ/μ, the non-empty subsets of the form $\{(i', j') \in \lambda/\mu : i' = i\}$ the *rows of* λ/μ, and the non-empty subsets of the form $\{(i', j') \in \lambda/\mu : j' = j\}$ the *columns of* λ/μ.

3 Flagged families of sets and words in $[m]^n$

We investigate families of sets that satisfy Hall's marriage condition and generalizations of Edelman and Greene's balanced tableaux by proving relationships between these classes of structures. In Section 3.1, we introduce marriage problems with unique solutions as flagged families and generalizations of balanced tableaux, then we give a new characterization of marriage problems with unique solutions in terms of these tableaux. In Section 3.2, we explain how our results relate to tableaux on skew shapes. Lastly, in Section 3.3, we show that the arithmetic mean of the sizes of subclasses of the above generalized tableaux is given by a generalization of the hook-length formula.

3.1 A new characterization

A well-known notion for families of sets is the following.

Definition 3.1 (Folklore [14])**.** Let $n \in \mathbb{N}$, and let $\mathcal{F}$ be a finite family of subsets of $[n]$. Then a *transversal* of $\mathcal{F}$ is an injective function $t : \mathcal{F} \to [n]$ such that $t(F) \in F$ for all $F \in \mathcal{F}$. The set $\{t(F) : F \in \mathcal{F}\}$ is called a *system of distinct representatives* of $\mathcal{F}$.

Families of sets that have transversals are of great interest. Exemplary of this is *Hall's Marriage Theorem*, which we present below.

Definition 3.2 (Marriage condition, Hall [11])**.** Let $n \in \mathbb{N}$, and let $\mathcal{F}$ be a finite family of subsets of $[n]$. Then $\mathcal{F}$ satisfies the *marriage condition* if for all subfamilies $\mathcal{F}'$ of $\mathcal{F}$,

$$|\mathcal{F}'| \le \left| \bigcup_{F \in \mathcal{F}'} F \right|.$$

Theorem 3.3 (Marriage Theorem, Hall [11])**.** *Let $n \in \mathbb{N}$, and let $\mathcal{F}$ be a family of non-empty subsets of $[n]$. Then $\mathcal{F}$ has a transversal if and only if $\mathcal{F}$ satisfies the marriage condition.*

In order to meaningfully use the families of sets in Hall's Marriage Theorem, we will define more structure on them.

Definition 3.4. Let $n \in \mathbb{N}$, let $\mathcal{F}$ be a family of non-empty subsets of $[n]$, and let t be a transversal of $\mathcal{F}$. Then a *configuration* f of t is a function $f : [n] \to \mathbb{N}$ such that for all $F \in \mathcal{F}$,

$$f(t(F)) \leq |F|.$$

Moreover, for $m \in [n]$, a surjective map $\sigma : [n] \to [m]$ *satisfies* f if for all $F \in \mathcal{F}$, the positive integer $\sigma(t(F))$ is the k^{th} smallest element of the set $\sigma(F)$, where $k = f(t(F))$.

Example 3.5. Let $\mathcal{F} = \{F_1, F_2\}$ be a family of sets on [2] where $F_1 = [2]$ and $F_2 = [2]$. The injective function $t : \mathcal{F} \to [2]$ defined by $t(F_1) = 1$ and $t(F_2) = 2$ is a transversal of $\mathcal{F}$. Consider three configurations f', f'', and f''' of t defined by $f'(1) = 1$ and $f'(2) = 1$, $f''(1) = 1$ and $f''(2) = 2$, and $f'''(1) = 2$ and $f'''(2) = 2$.

Note $\sigma : [2] \to [1]$ satisfies f' because $\sigma(1) = 1$ is the smallest element of $\sigma(F_1) = \sigma([2]) = [1]$ and because $\sigma(2) = 1$ is the smallest element of $\sigma(F_2) = \sigma([2]) = [1]$. However, no permutation $\sigma : [2] \to [2]$ can satisfy f'. It can also be checked that the surjective map $\sigma : [2] \to [1]$ and the permutation $\sigma = 21$ do not satisfy f'' but the permutation $\sigma = 12$ satisfies f''. Moreover, for all $m \in [2]$ and for all surjective maps $\sigma : [2] \to [m]$, σ does not satisfy f'''.

Now, we define the following stronger form of the marriage condition.

Definition 3.6 (cf. [3])**.** Let $n \in \mathbb{N}$, let $\mathcal{F}$ be a finite family of subsets of $[n]$, and write $m = |\mathcal{F}|$. Then $\mathcal{F}$ is *flagged* if there exists a bijection $\sigma_{\mathcal{F}} : [m] \to \mathcal{F}$ such that for all $k \in [m]$,

$$\left| \bigcup_{i=1}^{k} \sigma_{\mathcal{F}}(i) \right| = k. \tag{3.1}$$

Informally, $\sigma_{\mathcal{F}}$ maps each k to a subset, such that the union of the first k subsets has cardinality k.

In [3], Chang noted the following as a simple consequence of Hall Jr.'s work ([10], Theorem 2).

Proposition 3.7 (Chang [3])**.** *If $n \in \mathbb{N}$, then a finite family $\mathcal{F}$ of subsets of $[n]$ has exactly one transversal if and only if $\mathcal{F}$ is flagged.*

In particular, by Theorem 3.3, all flagged families satisfy the marriage condition. The families of sets $\mathcal{F}$ in Proposition 3.7 are referred to as *marriage problems with unique solutions* [13, 12].

Remark 3.8. When describing a flagged family $\mathcal{F}$, we will use total orderings on the members of this family by fixing orderings F_1, F_2, $\ldots$, F_n of the members of $\mathcal{F}$ that satisfy

$$\mathcal{F} = \{F_i : 1 \leq i \leq n\},$$

and, for all $1 \leq k \leq n$,

$$\left| \bigcup_{i=1}^{k} F_i \right| = k.$$

We observe that no flagged family is a multi-set. Let $\mathcal{F}$ be a flagged family and fix an ordering $F_1, F_2, \cdots, F_n$ of the members of $\mathcal{F}$ as described in Remark 3.8. Suppose that $F_j = F_{j'}$ for some $j < j'$. Then,

$$\bigcup_{i=1}^{j} F_i = \bigcup_{i=1}^{j'} F_i,$$

contradicting Equation (3.1) of Definition 3.6.

Before proving the main result of this paper, we prove the following lemma.

Lemma 3.9. *Let $\mathcal{F}$ be a flagged family of subsets of $[n]$. Moreover, let $S \subseteq [n]$ be the set of elements $k \in [n]$ such that $k \in F$ for exactly one member F of $\mathcal{F}$. Then S is not empty.*

Proof. Let $m = |\mathcal{F}|$. Because $\mathcal{F}$ is flagged, Definition 3.6 and Equation (3.1) imply that there exists a bijection $\sigma_{\mathcal{F}} : [m] \to \mathcal{F}$ and an element $k \in [n]$ such that

$$\bigcup_{i=1}^{m-1} \sigma_{\mathcal{F}}(i) \;=\; \left(\bigcup_{i=1}^{m} \sigma_{\mathcal{F}}(i)\right) \setminus \{k\}.$$

So as $k \in \sigma_{\mathcal{F}}(m)$ and as, for all $1 \leq i < m$, $k \notin \sigma_{\mathcal{F}}(i)$, it follows that $k \in S$ and that S is non-empty. □

Now, we prove the main result of this paper.

Theorem 3.10. *Let $n \in \mathbb{N}$, let $\mathcal{F}$ be a family of subsets of $[n]$ such that $|\mathcal{F}| = n$, assume that $\mathcal{F}$ satisfies the marriage condition, and let t be a transversal of $\mathcal{F}$. Moreover, let $S \subseteq [n]$ be the set of elements $k \in [n]$ such that $k \in F$ for exactly one member F of $\mathcal{F}$. Lastly, let m be an integer satisfying*

$$\min(n, n - |S| + 1) \leq m \leq n.$$

Then $\mathcal{F}$ is flagged if and only if for all configurations f of t, there exists a surjective map $\sigma : [n] \to [m]$ such that σ satisfies f.

Proof. Let n, $\mathcal{F}$, t, S, and m be as described in the theorem. First assume that for all configurations f of t, there exists a surjective map $\sigma : [n] \to [m]$ that satisfies f. If $n = 1$, then the only family of $\{1\}$ with a transversal is the family $\mathcal{F} = \{\{1\}\}$, which is flagged.

So assume without loss of generality that $n \geq 2$. Consider the configuration f_1 of t defined by $f_1(t(F)) = |F|$ for all $F \in \mathcal{F}$. By assumption, there exists a surjective map $\sigma' : [n] \to [m]$ that satisfies f_1. Moreover, let $k \in [n-1]$, and assume that we can fix an ordering $\mathcal{F} = \{F'_i : i \in [n]\}$ of $\mathcal{F}$ so that the following holds for all integers $0 \leq j \leq k-1$.

$$\left|\bigcup_{i=1}^{n-j} F'_i\right| = n - j \tag{3.2}$$

Note that Equation (3.2) holds if $k = 1$ because the fact that $\mathcal{F}$ has a transversal implies that $\bigcup_{F \in \mathcal{F}} F = [n]$.

Next, let $1 \leq s \leq n - k + 1$ satisfy

$$\sigma'(t(F'_s)) \;=\; \max_{1 \leq j \leq n-k+1} \sigma'(t(F'_j)). \tag{3.3}$$

Suppose that there exists an element $j \in [n]$ such that $1 \leq j \leq n-k+1$, $j \neq s$, and $t(F'_s) \in F'_j$. By Equation (3.3), $\sigma'(t(F'_j)) \leq \sigma'(t(F'_s))$. So as $t(F'_s) \in F'_j$ and $t(F'_s) \neq t(F'_j)$, it follows that for some $1 \leq \ell \leq |F'_j| - 1$, $\sigma'(t(F'_j))$ is an ℓ^{th} smallest element of $\sigma'(F'_j)$. But then, as $f_1(t(F'_j)) = |F'_j|$, σ' does not satisfy f_1, contradicting the assumption that σ' satisfies f_1.

Hence, $t(F'_s) \notin F'_i$ for all $1 \leq i \leq n-k+1$ satisfying $i \neq s$. In particular, fix an ordering $\mathcal{F} = \{F''_i : i \in [n]\}$ of the members of $\mathcal{F}$ so that $F''_i = F'_i$ if $i > n-k+1$ and $F''_{n-k+1} = F'_s$, where s is as described in the above paragraph. By Equation (3.2) and the fact that $t(F'_s) \notin F'_i$ for all $1 \leq i \leq n-k+1$ satisfying $i \neq s$, it follows that this ordering of the members of $\mathcal{F}$ satisfies the following equation for all integers $0 \leq j \leq k$.

$$\left| \bigcup_{i=1}^{n-j} F''_i \right| = n - j$$

As the choice of $k \in [n-1]$ is arbitrary, it follows that there exists an ordering $\mathcal{F} = \{F_1, F_2, \ldots, F_n\}$ of $\mathcal{F}$ such that

$$\left| \bigcup_{i=1}^{k} F_i \right| = k$$

for all $1 \leq k \leq n$. Hence, $\mathcal{F}$ satisfies Equation (3.1) of Definition 3.6. So, by Definition 3.6, $\mathcal{F}$ is flagged.

Next, assume that $\mathcal{F}$ is flagged. We proceed by strong induction on n. Because $\mathcal{F}$ is flagged, we will use the total orderings as described in Remark 3.8 to describe the members of this family.

If $n = 1$, then the only family of subsets of $\{1\}$ with a transversal is the family $\mathcal{F} = \{\{1\}\}$. Moreover, with t being the transversal of $\mathcal{F}$ defined by mapping $\{1\}$ to 1, the only configuration f of t is the function $f : \{1\} \to \mathbb{N}$ defined by $f(1) = 1$, $S = \{1\}$, $\min(n, n - |S| + 1) = 1$, and the surjective map $\sigma : \{1\} \to \{1\}$ satisfies f.

So assume that $n \geq 2$ and let f be a configuration of t. Since S is not empty by Lemma 3.9, $\min(n, n-|S|+1) = n - |S| + 1$, implying that $n - |S| + 1 \leq m \leq n$. Assume without loss of generality that

$$S = \{n - m' + 1, n - m' + 2, \ldots, n\} \tag{3.4}$$

for some $m' \in [n]$. If $m = 1$, then $n - |S| + 1 \leq 1$, implying that $n = |S|$. Hence, as $|\mathcal{F}| = n$ and $S = [n]$, every element of $[n]$ is contained in exactly one element of $\mathcal{F}$, that is $\mathcal{F} = \{\{k\} : k \in [n]\}$. So in this case, $t(\{k\}) = k$ for all $k \in [n]$, the only configuration f of t is the map defined by $f(k) = 1$ for all $k \in [n]$, and the surjective map $\sigma : [n] \to [m]$, defined by $\sigma(k) = 1$ for all $k \in [n]$, satisfies f. So assume without loss of generality that $m \geq 2$.

Since $n - |S| + 1 \leq m \leq n$, m satisfies the inequality $n - m' + 1 \leq m \leq n$. As $\mathcal{F}$ is flagged, there is an ordering $F'_1, F'_2, \ldots, F'_n$ of the members of $\mathcal{F}$ such that

$$\left| \bigcup_{i=1}^{k} F'_i \right| = k \tag{3.5}$$

for all $1 \leq k \leq n$. Define the following subfamilies of $\mathcal{F}$,

$$\mathcal{F}_0 = \{F \in \mathcal{F} : t(F) \leq m - 1\}$$

and

$$\mathcal{F}_1 = \{F \in \mathcal{F} : t(F) \geq m\}.$$

We first prove that $\mathcal{F}_0$ is flagged. Because S is the set of elements $k \in [n]$ such that $k \in F$ for exactly one member F of $\mathcal{F}$, Equation (3.4) and the fact that $n-m'+1 \leq m \leq n$ implies that for all $m \leq k \leq n$, k is contained in exactly one member of $\mathcal{F}$ and that for all $F \in \mathcal{F}_1$,

$$|F \cap \{m, m+1, \ldots, n\}| = 1.$$

In particular, $\mathcal{F}_0$ is an $(m-1)$-member family of subsets of $[m-1]$.

Assume that there exists an integer $1 \leq j \leq n-1$ such that $F'_j \in \mathcal{F}_1$ and $F'_{j+1} \in \mathcal{F}_0$. Write

$$X_j = \bigcup_{i=1}^{j-1} F'_i,$$

where we assume that $X_j = \emptyset$ if $j = 1$. Since $F'_j \in \mathcal{F}_1$, $t(F'_j) \in \{m, m+1, \ldots, n\}$ and no member of $\mathcal{F}$ other than F'_j contains $t(F'_j)$. Moreover, by Equation (3.5), $|F'_j \cup X_j| = |X_j| + 1$. So as $t(F'_j) \in F'_j$, it follows that $[m-1] \cap (F'_j \cup X_j) = [m-1] \cap X_j$. Since $F'_{j+1} \in \mathcal{F}_0$, $F'_{j+1} \subseteq [m-1]$. Moreover, by Equation (3.5), $|X_j \cup F'_j \cup F'_{j+1}| = |X_j \cup F'_j| + 1$. It follows that $F'_{j+1} \backslash X_j = F'_{j+1} \backslash (X_j \cup F'_j) = \{k\}$ for some $k \in [m-1]$, implying that

$$|F'_{j+1} \cup X_j| = |X_j| + 1. \tag{3.6}$$

So the ordering $\mathcal{F} = \{F''_1, F''_2, \ldots, F''_n\}$ of the members of $\mathcal{F}$, such that $F''_j = F'_{j+1}$, $F''_{j+1} = F'_j$, and $F''_i = F'_i$ for all $i \in [n] \backslash \{j, j+1\}$, satisfies the following by Equation (3.5) and Equation (3.6). For all $1 \leq k \leq n$,

$$\left| \bigcup_{i=1}^{k} F''_i \right| = k. \tag{3.7}$$

Furthermore, $F''_j \in \mathcal{F}_0$ and $F''_{j+1} \in \mathcal{F}_1$. If there exists an integer $1 \leq j' \leq n-1$ such that $F''_{j'} \in \mathcal{F}_1$ and $F''_{j'+1} \in \mathcal{F}_0$, then argue again as above. Repeating this argument at most a finite number of times, we obtain an ordering $\mathcal{F} = \{F_1, F_2, \ldots, F_n\}$ of the members of $\mathcal{F}$ where

$$\left| \bigcup_{i=1}^{k} F_i \right| = k \tag{3.8}$$

for all $1 \leq k \leq n$, $\mathcal{F}_0 = \{F_k : 1 \leq k \leq m-1\}$, and $\mathcal{F}_1 = \{F_k : m \leq k \leq n\}$. In particular, Equation (3.8) holds for all $1 \leq k \leq m-1$, implying that $\mathcal{F}_0$ satisfies Equation (3.1) of Definition 3.6. It follows, by Definition 3.6, that $\mathcal{F}_0$ is a flagged family of subsets of $[m-1]$.

So consider the ordering $F_1, F_2, \ldots, F_n$ of the members of $\mathcal{F}$ as above and assume without loss of generality that for all $m \leq i \leq n$, $t(F_i) = i$. Let t' be the transversal of $\mathcal{F}_0$ defined by $t'(F) = t(F)$ for all $F \in \mathcal{F}_0$. Moreover, let $f' = f|_{[m-1]}$, where $f|_{[m-1]}$ denotes the restriction of f to $[m-1]$. In particular, f' is a configuration of t'.

Since it is assumed in the theorem that $\min(n, n-|S|+1) \leq m \leq n$, and since a surjective map $\sigma : [n] \to [m]$ is a permutation if $m = n$, the following holds. Because $\mathcal{F}_0$ is flagged, because $|\mathcal{F}_0| = m-1$, and because $|[m-1]| < n$, the induction hypothesis implies that there exists a permutation $\sigma' : [m-1] \to [m-1]$ such that σ' satisfies f'.

If there exists an integer $m \leq j \leq n$ such that $f(j) = |F_j|$, then there exists a surjective map $\kappa' : [n] \to [m]$ such that $\kappa'(i) = i$ for all $1 \leq i \leq m-1$ and the following two properties hold for all $m \leq i \leq n$.

- If $f(i) = |F_i|$, then $\kappa'(i) = m$.
- If $f(i) < |F_i|$, then $\kappa'(i)$ is equal to the $f(i)^{th}$ smallest element of $\sigma'(F_i \backslash \{i\})$.

Otherwise, if $f(i) < |F_i|$ for all $m \leq i \leq n$, the following holds. Write $\sigma'(F_n \backslash \{n\}) = \{r_1, r_2, \cdots, r_t\}$ where $t = |F_n| - 1$ and $r_1 < r_2 < \cdots < r_t$. Since $f(n) < |F_n|$, there exists a map $\kappa^* : [m-1] \to [m]$ such that κ^* is injective and order-preserving and such that, with $x \in [m] \backslash \kappa^*([m-1])$, $x < \kappa^*(r_1)$ if $f(n) = 1$ and $\kappa^*(r_{f(n)-1}) < x < \kappa^*(r_{f(n)})$ if $f(n) \geq 2$. So there exists a surjective map $\kappa'' : [n] \to [m]$ such that $\kappa''|_{[m-1]} = \kappa^*$ and such that the following two properties hold.

- If $m \leq i < n$, then $\kappa''(i)$ is equal to the $f(i)^{th}$ smallest element of $\kappa''(\sigma'(F_i \backslash \{i\}))$.
- If $i = n$, then $\kappa''(i) \notin \kappa''([m-1])$ and $\kappa''(i)$ is equal to the $f(i)^{th}$ smallest element of $\kappa''(i) \cup \kappa''(\sigma'(F_i \backslash \{i\}))$.

We note that $\kappa''|_{[m-1]}$ is injective and order-preserving because κ^* is injective and order-preserving.

So define a surjective map $\kappa : [n] \to [m]$ as follows. If there exists an integer $m \leq j \leq n$ such that $f(j) = |F_j|$, then define $\kappa = \kappa'$. Otherwise, if $f(i) < |F_i|$ for all $m \leq i \leq n$, define $\kappa = \kappa''$. Now, define the map $\sigma : [n] \to [m]$ by

$$\sigma(i) = \begin{cases} \kappa(\sigma'(i)) & \text{if } 1 \leq i \leq m-1 \\ \kappa(i) & \text{if } m \leq i \leq n. \end{cases}$$

Because $\sigma' : [m-1] \to [m-1]$ is a bijection, the definition of κ implies that σ is surjective. Moreover, because σ' satisfies f' and because, for all integers $m \leq i \leq n$, i is contained in exactly one member of $\mathcal{F}$ and $F_i \cap \{m, m+1, \ldots, n\} = \{i\}$, the definition of κ and the definition of σ imply that σ satisfies f. From this, the theorem follows. □

A natural consequence of the above is the following which, combined with Theorem 3.10, gives another characterization of flagged families of sets.

Corollary 3.11. *Let $\mathcal{F}$ be a family of subsets of $[n]$ such that $|\mathcal{F}| = n$, assume that $\mathcal{F}$ satisfies the marriage condition, and let t be a transversal of $\mathcal{F}$. Moreover, let S be as in Theorem 3.10. Lastly, let f_0 be the configuration of t defined by $f_0(t(F)) = 1$ for all $F \in \mathcal{F}$. Then f_0 is satisfied by some permutation $\sigma : [n] \to [n]$ if and only if for all integers $n - |S| + 1 \leq m \leq n$ and for all configurations f of t, there exists a surjective map $\sigma : [n] \to [m]$ that satisfies f.*

Proof. Let f_1 be the configuration of t defined by $f_1(t(F)) = |F|$ for all $F \in \mathcal{F}$. Then a permutation $\sigma : [n] \to [n]$ satisfies f_0 if and only if the permutation $\sigma' : [n] \to [n]$ defined by $\sigma'(i) = n - \sigma(i) + 1$ for all $i \in [n]$ satisfies f_1. In particular, f_0 is satisfied by some permutation if and only if f_1 is. The first half of the proof of Theorem 3.10 implies that if f_1 is satisfied by some permutation $\sigma : [n] \to [n]$, then $\mathcal{F}$ is flagged. Furthermore, by Theorem 3.10, if $\mathcal{F}$ is flagged, then for all integers $n - |S| + 1 \leq m \leq n$ and for all configurations f of t, there exists a surjective map $\sigma : [n] \to [m]$ that satisfies f. From this, the corollary follows. □

Remark 3.12. A family $\mathcal{F}$ of subsets of $[n]$ such that $|\bigcup_{F\in\mathcal{F}} F| = |\mathcal{F}| = n$ is called a *critical block* in [10] by Hall Jr.. He used this notion as a very important ingredient in extending Hall's Marriage Theorem to infinite families of finite sets.

3.2 The case of skew shapes

To explain how the results in the previous subsection relate to skew shapes, we will need the following definitions.

Definition 3.13. Let λ/μ be a skew shape with n cells, and let $1 \le m \le n$ be an integer. Then a *surjective tableau of shape* λ/μ is a surjective function $T : \lambda/\mu \to [m]$ and elements in the range of T are called the *entries in* T. In the case $m = n$ a surjective tableau is a *bijective tableau*. Moreover, a *standard skew tableau of shape* λ/μ is a bijective tableau of shape λ/μ such that the entries along every row increase from left to right and the entries along every column increase from top to bottom.

Example 3.14. The tableaux

$$T_1 = \begin{array}{cccc} & & \boxed{3} & \boxed{5} \\ \boxed{6} & \boxed{1} & \boxed{2} & \\ \boxed{4} & & & \end{array}, \quad T_2 = \begin{array}{cccc} & & \boxed{2} & \boxed{3} \\ \boxed{1} & \boxed{5} & \boxed{6} & \\ \boxed{4} & & & \end{array}, \text{ and } T_3 = \begin{array}{cccc} & & \boxed{2} & \boxed{3} \\ \boxed{3} & \boxed{1} & \boxed{2} & \\ \boxed{2} & & & \end{array}$$

have shape $(4,3,1)/(2)$. Here, T_1 and T_2 are bijective and T_2 is standard. All three are surjective. Moreover, for T_1 and T_2, $m = 6$ and for T_3, $m = 3$.

In order to fully relate Definition 3.13 to Definition 3.4, we will use the following standard definitions.

Definition 3.15. Let λ/μ be a skew shape. For any cell $(i,j) \in \lambda/\mu$, define the corresponding *hook* $H_{(i,j)}$ to be

$$H_{(i,j)} = \{(i,j)\} \cup A_{(i,j)} \cup L_{(i,j)},$$

where

$$A_{(i,j)} = \{(i,j') \in \lambda/\mu : j' > j\}$$

is the *arm* of $H_{(i,j)}$ and where

$$L_{(i,j)} = \{(i',j) \in \lambda/\mu : i' > i\}$$

is the *leg* of $H_{(i,j)}$. Define the corresponding *hook-length* $h_{(i,j)}$ to be

$$h_{(i,j)} = |H_{(i,j)}|.$$

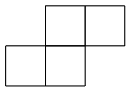
Example 3.16. Consider the following skew shape λ/μ, where $\lambda = (5,4,3,3)$ and $\mu = (2,2,1)$. Then $r = (2,3)$ is the cell of λ/μ depicted below that is filled with a bullet. The entries of H_r are filled with asterisks, bullets or circles, so $h_r = 4$. Moreover, the entry of A_r is filled with an asterisk and the entries of L_r are filled with circles.

$$\begin{array}{ccccc} & & \boxed{} & \boxed{} & \boxed{} \\ & & \boxed{\bullet} & \boxed{\ast} & \\ & \boxed{} & \boxed{\circ} & & \\ \boxed{} & \boxed{} & \boxed{\circ} & & \end{array}$$

Definition 3.17. Let λ/μ be a skew shape. Then define $\mathcal{F}_{\lambda/\mu}$ to be the set

$$\{H_r : r \in \lambda/\mu\}.$$

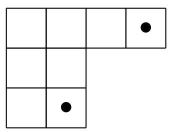
Example 3.18. If λ/μ is the skew shape depicted below


,

then, as $\lambda/\mu = \{(1,2),(1,3),(2,2),(2,3)\}$,

$$\mathcal{F}_{\lambda/\mu} = \{\{(1,2),(2,2),(1,3)\},\{(1,3)\},\{(2,1),(2,2)\},\{(2,2)\}\}.$$

Many families of sets that satisfy the marriage condition are not flagged. For instance, the family $\mathcal{F} = \{F_1, F_2\}$, where $F_1 = F_2 = \{1,2\}$, satisfies the marriage condition but is not flagged. However, Definition 3.6 is a very broad definition. Let λ be a Young diagram. Then an *inner corner of* λ is a cell $r \in \lambda$ such that deleting r from λ results in another Young diagram. For instance, if $\lambda = (4,2,2)$, then the inner corners of λ are the cells filled with bullets.



With this definition in mind, let λ/μ be a skew shape with n cells, and consider the family $\mathcal{F}$ of sets defined by $\mathcal{F} = \mathcal{F}_{\lambda/\mu}$. Let $r_1, r_2, \dots, r_n$ be a sequence of cells in λ/μ such that:

- The cell r_1 is an inner corner of λ.
- For all $k \in [n-1]$, the cell r_{k+1} is an inner corner of $\lambda \backslash \{r_1, r_2, \cdots, r_k\}$.

Define $\sigma_{\mathcal{F}} : [n] \to \mathcal{F}$ by letting $\sigma_{\mathcal{F}}(k) = H_{r_k}$ for all $k \in [n]$. It can be checked that the bijection $\sigma_{\mathcal{F}}$ satisfies Equation (3.1). Now, because the skew shape λ/μ is a finite set, regard λ/μ as being the set $[n]$, where n is the number of cells in λ/μ. In particular, regard $\mathcal{F}_{\lambda/\mu}$ as a family of subsets of $[n]$. Then, by the above and by Definition 3.6, $\mathcal{F}$ is flagged. In particular, by Proposition 3.7, $\mathcal{F}$ has a unique transversal. The unique transversal $t_{\lambda/\mu} : \mathcal{F} \to \lambda/\mu$ of $\mathcal{F}$ is given by $t_{\lambda/\mu}(H_r) = r$ for all $r \in \lambda/\mu$.

As we are regarding the cells of a skew shape with n cells as being the elements of $[n]$, we can regard any surjective tableau T of shape λ/μ as being a surjective function $T : [n] \to [m]$ in which $T(i) = j$ if j is the entry of T in the cell of T corresponding to i. Taking $m = n$, we can also regard any bijective tableau of shape λ/μ as being a permutation $T : [n] \to [n]$. Lastly, as we are regarding the skew shape λ/μ as being the set $[n]$ and as we are regarding $\mathcal{F}_{\lambda/\mu}$ as a family of subsets of $[n]$, we define configurations $f : \lambda/\mu \to \mathbb{N}$ of $t_{\lambda/\mu}$, where $t_{\lambda/\mu}$ is the unique transversal of $\mathcal{F}_{\lambda/\mu}$, and surjective maps $\sigma : \lambda/\mu \to [m]$ that satisfy f analogously to Definition 3.4.

Next, let λ/μ be a skew shape with n cells, consider the flagged family of sets $\mathcal{F}_{\lambda/\mu}$, and let $t_{\lambda/\mu}$ be the unique transversal of $\mathcal{F}$. We define the configuration f_0 of $t_{\lambda/\mu}$ by $f_0(r) = 1$ for all $r \in \lambda/\mu$. It can be seen that the standard skew tableaux of shape λ/μ are the bijective tableaux of shape λ/μ that satisfy f_0. Since we regard λ/μ as being the set $[n]$, we can regard f_0 as being the function $f_0 : [n] \to \mathbb{N}$ defined by $f_0(k) = 1$ for all $k \in [n]$. So as we regard $\mathcal{F}_{\lambda/\mu}$ as being a family of subsets of $[n]$, the standard skew tableaux of shape λ/μ can be regarded as being the permutations $\sigma : [n] \to [n]$ that satisfy f_0.

Example 3.19. Consider the following surjective tableau of shape $\lambda = (4, 3, 2)$.

$$\begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 3 \\ \hline 1 & 2 & 3 \\ \cline{1-3} 3 & 3 \\ \cline{1-2}\end{array}$$

Next, consider $\mathcal{F}_\lambda$. Let t_λ be the unique transversal of $\mathcal{F}_\lambda$, and let $f : \lambda \to \mathbb{N}$ be the configuration of t_λ defined by $f(r) = 1$ for all $r \in \lambda/\mu$. It can be checked that the above tableau satisfies f.

Edelman and Greene introduced the following class of bijective tableaux, which we re-formulate in terms of the configurations we defined in this paper.

Definition 3.20 (Edelman and Greene [5])**.** Let λ be a Young diagram containing n cells. Moreover, let t_λ be the transversal of $\mathcal{F}_\lambda$ defined by $t_\lambda(H_r) = r$ for all $r \in \lambda$ and let f be the configuration defined by

$$f(r) = |L_r| + 1$$

for all $r \in \lambda$. Then a *balanced tableau of shape* λ is a bijective tableau of shape λ that satisfies f.

Example 3.21. Let $\lambda = (4, 3, 2)$, and let t_λ and f be defined from $\mathcal{F}_\lambda$ as described in Definition 3.20. Then

$$T = \begin{array}{|c|c|c|c|}\hline 4 & 5 & 8 & 3 \\ \hline 6 & 7 & 9 \\ \cline{1-3} 1 & 2 \\ \cline{1-2}\end{array}$$

is balanced because T satisfies f. For instance, $f((2,1)) = 2$ since $L_{(2,1)} = \{(3,1)\}$ and $|L_r| + 1 = 2$. So as $T((2,1)) = 6$, $H_{(2,1)} = \{(2,1), (2,2), (2,3), (3,1)\}$, and the set of entries in T that are contained in a cell of $H_{(2,1)}$ is $\{1, 6, 7, 9\}$, it follows that $T((2,1))$ is the $f((2,1))^{th}$-smallest element of $\{1, 6, 7, 9\}$.

Remark 3.22. The surjective tableaux from Definition 3.13 that satisfy the configuration $f : [n] \to \mathbb{N}$ defined by $f(k) = 1$ for all $k \in [n]$ do not correspond to semistandard tableaux, nor do they correspond to the semistandard balanced labelings in [7].

Balanced tableaux can be regarded as permutations $\sigma : [n] \to [n]$ that satisfy $f(r) = |L_r| + 1$. The function $f(r) = |L_r| + 1$ was called the *hook rank* of r by Edelman and Greene and they used it to define balanced tableaux [5].

Lastly, we give examples illustrating Theorem 3.10 and Corollary 3.11.

Example 3.23. We give an example in which the lower bound $\min(n, n - |S| + 1)$ from Theorem 3.10 cannot be improved on. Consider $\lambda = (3, 2, 1)$. Next, let $\mathcal{F} = \mathcal{F}_\lambda$ and let t be the unique transversal of $\mathcal{F}$. As discussed earlier, $\mathcal{F}$ is flagged. Now, let f be the configuration of $\mathcal{F}_\lambda$ defined by $f((1,1)) = 5$, $f((1,2)) = 3$, $f((1,3)) = 1$, $f((2,1)) = 3$, $f((2,2)) = 1$, and $f((3,1)) = 1$. We depict the configuration f with the below diagram.

$$\begin{array}{|c|c|c|}\hline 5 & 3 & 1 \\ \hline 3 & 1 \\ \cline{1-2} 1 \\ \cline{1-1}\end{array}$$

There is exactly one cell in the Young diagram λ, the cell $(1,1)$, that is contained in exactly one member of $\mathcal{F} = \{H_r : r \in \lambda\}$. Hence, $S = \{(1,1)\}$ and $\min(n, n-|S|+1) = n - |S| + 1$. With this in mind, set $n = 6$ and, as $n - |S| + 1 = 6 - 1 + 1 = 6$, assume that m is an integer satisfying $1 \leq m \leq 5$. Suppose that there exists a surjective tableau T of shape λ, and with entries from $[m]$, such that T satisfies the configuration f defined above. The cells $(1,1)$, $(1,2)$ and $(2,1)$ are cells $r \in \lambda$ that satisfy $f(r) = h_r$. Moreover, because T satisfies f, $f(r) = h_r$ implies that no two entries of T in H_r are the same and that the entry of T in cell r is the h_r^{th} smallest element of the set of entries of T that are contained in H_r.

So consider the cell $(2,2)$ of λ. Since $m \leq 5$, some two entries of T in $H_{(1,1)}$ are the same, or the entry of T in cell $(2,2)$ equals to the entry of T in some other cell, (i_1, j_1), in λ. Since $f((1,1)) = 5 = h_{(1,1)}$, no two entries of T in $H_{(1,1)}$ are the same. So the entry of T in cell $(2,2)$ equals to the entry of T in some other cell, (i_1, j_1), in λ. If $(i_1, j_1) = (1,1)$, then the entry of T in cell $(2,2)$ of λ is larger than the entries of T in cells $(1,2)$ and $(2,1)$ of λ. But that is impossible by the above. If $(i_1, j_1) = (2,1)$ or if $(i_1, j_1) = (3,1)$, then the entry of T in cell $(2,1)$ of λ is the k^{th} smallest element of the set of entries of T that are contained in $H_{(2,1)}$ for some $k \leq 2$. But that is impossible by the above. By symmetry, it is impossible for $(i_1, j_1) = (1,2)$ or for $(i_1, j_1) = (1,3)$. Hence, we have reached a contradiction. It follows that there is no such surjective tableau T.

Example 3.24. Consider a skew shape λ/μ with n cells, and let S denote the set of cells of λ/μ that are contained in exactly one member of $\{H_r : r \in \lambda/\mu\}$. The elements of S are also known as the *outer corners* of μ. Clearly, there exists a standard skew tableau of shape λ/μ. Corollary 3.11 implies that such a tableau exists if and only if for all integers $n - |S| + 1 \leq m \leq n$ and for all configurations f of λ/μ, there exists a surjective tableau T of shape λ/μ, with $[m]$ as the set of entries of T, such that T satisfies f.

3.3 The average number of generalized tableaux

Let $S(n,m)$ denote the Stirling number of the second kind, namely the number of set partitions of $[n]$ into m parts. Let $\mathcal{F}$ be a family of subsets of $[n]$ that satisfies the marriage condition, let $m \in [n]$, and let t be a transversal of $\mathcal{F}$. If f is a configuration of t, then let $A_{n,m}(f)$ denote the number of surjective maps $\sigma : [n] \to [m]$ that satisfy f. Moreover, let X be the set of configurations f of t such that $A_{n,m}(f) \geq 1$. Then define the *average value of $A_{n,m}(f)$ over all configurations f of t satisfying $A_{n,m}(f) \geq 1$* to be

$$\frac{1}{|X|} \sum_{f \in X} A_{n,m}(f)$$

if $|X| > 0$, and 0 otherwise.

Theorem 3.25. *Let $\mathcal{F}$ be a flagged family of subsets of $[n]$ such that $|\mathcal{F}| = n$ and let t be the transversal of $\mathcal{F}$. Moreover, let $S \subseteq [n]$ be the set of elements $k \in [n]$ such that $k \in F$ for exactly one member F of $\mathcal{F}$, and let m be an integer satisfying*

$$n - |S| + 1 \leq m \leq n.$$

Then the average value of $A_{n,m}(f)$ over all configurations f of t satisfying

$$A_{n,m}(f) \geq 1$$

is

$$\frac{m!\,S(n,m)}{\prod_{F\in\mathcal{F}}|F|}. \tag{3.9}$$

Remark 3.26. Consider the sequence $(p_k(x))_{k=0,1,2,\ldots}$ of polynomials in $\mathbb{Q}[x]$ such that $p_0(x)=1$ and, for all k,

$$p_{k+1}(x)-p_{k+1}(x-1)=x\,p_k(x).$$

If $k=n-m$, then $S(n,m)=p_k(m)$ (see [2, 22]). So if k is fixed, then we can compute closed-form expressions for $S(n,m)$. For instance, Expression 3.9 becomes

$$\frac{m!}{\prod_{F\in\mathcal{F}}|F|}$$

if $n=m$,

$$\binom{m+1}{2}\frac{m!}{\prod_{F\in\mathcal{F}}|F|}$$

if $n=m+1$, and

$$\frac{1}{2}\binom{m+1}{2}\left(\binom{m+1}{2}+\frac{2m+1}{3}\right)\frac{m!}{\prod_{F\in\mathcal{F}}|F|}$$

if $n=m+2$.

In order to prove Theorem 3.25, we prove the following.

Lemma 3.27. *Let $m,n\in\mathbb{N}$ such that $m\leq n$, and let $\mathcal{F}$ be a family of subsets of $[n]$ that has a transversal $t:\mathcal{F}\to[n]$ such that t is surjective. Then every surjective function $\sigma:[n]\to[m]$ satisfies exactly one configuration f of t.*

Proof. Let $\sigma:[n]\to[m]$ be a surjective map. Then σ satisfies the configuration f of t defined by letting, for all $F\in\mathcal{F}$, $f(t(F))=k$ where $\sigma(t(F))$ is the k^{th} smallest element of the set $\sigma(F)$. Now, suppose that σ satisfies more than one configuration of t. Then, let f_1 and f_2 be two distinct configurations of t. Because $f_1\neq f_2$ and because t is surjective, there is an element $F\in\mathcal{F}$ such that $f_1(t(F))\neq f_2(t(F))$. So write $k_1=f_1(t(F))$ and write $k_2=f_2(t(F))$. Since σ satisfies f_1, Definition 3.4 implies that $\sigma(t(F))$ is the k_1^{th} smallest element of $\sigma(F)$. Moreover, since σ satisfies f_2, Definition 3.4 implies that $\sigma(t(F))$ is the k_2^{th} smallest element of $\sigma(F)$. However, this is impossible because $k_1=f_1(t(F))\neq f_2(t(F))=k_2$. □

Now, we prove Theorem 3.25.

Proof. By Definition 3.4, the total number of configurations of $\mathcal{F}$ equals to $\prod_{F\in\mathcal{F}}|F|$. Moreover, it is well-known that the number of surjective maps from $[n]$ to $[m]$ is given by $m!\,S(n,m)$. By Lemma 3.27, every surjective map satisfies exactly one configuration. Moreover, by Theorem 3.10, every configuration of $\mathcal{F}$ is satisfied by some surjective map from $[n]$ to $[m]$. From this, the theorem follows. □

Theorem 3.25 implies the following consequence relating to how the values $A_{n,m}(f)$ are distributed. By Theorem 3.10, every configuration f of t is satisfied by at least one surjective map $\sigma : [n] \to [m]$. Hence, by Theorem 3.25 and the fact that $A_{n,m}(f) \geq 1$ always holds, it follows that for all constants $k \geq 1$ the number of configurations f of t that satisfy

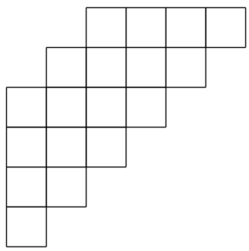
$$A_{n,m}(f) \;\leq\; k \cdot \frac{m!\, S(n,m)}{\prod_{F \in \mathcal{F}} |F|}$$

is at least

$$\left(1 - \frac{1}{k}\right) \prod_{F \in \mathcal{F}} |F|.$$

We now illustrate Theorem 3.25 with some examples and in the process describe its relationship with the hook-length formula.

Example 3.28. Let $\lambda = (6,5,4,3,2,1)$ and $\mu = (1)$. The skew shape λ/μ is depicted below.



Since λ/μ has eighteen cells, let $n = 18$. The cells of λ/μ that are contained in exactly one member of the family $\mathcal{F}_{\lambda/\mu}$ are $(1,3)$, $(2,2)$, and $(3,1)$. Hence, $S = \{(1,3),(2,2),(3,1)\}$ and $n - |S| + 1 = n - 2$. So let $m = n - 2 = 16$. Then by Theorem 3.25 and Remark 3.26, the average value of $A_{n,m}(f)$ over all configurations f of λ/μ satisfying $A_{n,m}(f) \geq 1$ is given by

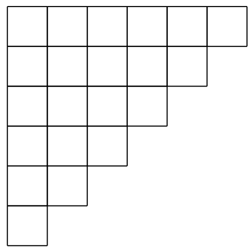
$$\begin{aligned}
\frac{1}{2}\binom{m+1}{2}\left(\binom{m+1}{2} + \frac{2m+1}{3}\right) \frac{m!}{\prod_{F \in \mathcal{F}_{\lambda/\mu}} |F|} &= \\
&= \frac{1}{2}\binom{16+1}{2}\left(\binom{16+1}{2} + \frac{2 \cdot 16 + 1}{3}\right) \frac{16!}{\prod_{r \in \lambda/\mu} h_r} \\
&= \frac{1}{2}\binom{17}{2}\left(\binom{17}{2} + 11\right) \frac{16!}{(7 \cdot 5 \cdot 3 \cdot 1)^3 \cdot 5 \cdot 3 \cdot 1 \cdot 3 \cdot 1 \cdot 1} \\
&= 4014814003 + \frac{1}{5}\,.
\end{aligned}$$

The *hook-length formula*, first proved by Frame, Robinson, and Thrall [8], is well-known. It is as follows. A skew shape λ/μ is a *straight shape* if $\mu = \emptyset$. Given a Young diagram λ, call a standard skew tableau of straight shape λ a *standard Young tableaux of shape* λ. If λ is a Young diagram with n cells, then the number of standard Young tableaux of shape λ equals

$$\frac{n!}{\prod_{r \in \lambda} h_r}.$$

Moreover, the above formula was also proved by Edelman and Greene to equal the number of balanced tableaux of shape λ [5]. Furthermore, the hook-length formula does not hold for skew shapes. Taking $m = n$ in Theorem 3.25, setting $\mathcal{F} = \mathcal{F}_\lambda$, and letting t be the unique transversal of $\mathcal{F}$, we see that the average value of $A_{n,m}(f)$ over all configurations f of t satisfying $A_{n,m}(f) \geq 1$ equals to the number of standard Young tableau of shape λ.

Example 3.29. Let $\lambda = (6, 5, 4, 3, 2, 1)$. The Young diagram λ is depicted below.



Since λ has twenty-one cells, let $n = 21$. The cell of λ that is contained in exactly one member of the family $\mathcal{F}_\lambda$ is $(1, 1)$. Hence, $S = \{(1, 1)\}$ and $n - |S| + 1 = n$. So let $m = n = 21$. Then by Theorem 3.25 and Remark 3.26, the average value of $A_{n,m}(f)$ over all configurations f of λ satisfying $A_{n,m}(f) \geq 1$ is given by the hook-length formula

$$\begin{aligned}\frac{m!}{\prod_{F\in\mathcal{F}_\lambda}|F|} &= \frac{21!}{\prod_{r\in\lambda} h_r}\\ &= \frac{21!}{1^6\cdot 3^5\cdot 5^4\cdot 7^3\cdot 9^2\cdot 11}\\ &= 1100742656\end{aligned}$$

and is, by the hook-length formula, equal to the number of standard Young tableaux of shape λ.

Remark 3.30. Theorem 3.25 is versatile. For instance, possible applications of the special case of Theorem 3.25 in the case of permutations are as follows. There is a formula for the number of standard skew tableaux of shape λ/μ, known as Naruse's formula. Asymptotic properties of Naruse's formula were analysed by Morales, Pak, and Panova in [17]. In particular, it turns out that in general, the number of standard skew tableaux of shape λ/μ divided by

$$\frac{n!}{\prod_{r\in\lambda/\mu} h_r},$$

where n is the number of cells of λ/μ, can be arbitrarily large. Hence, we can apply Theorem 3.25 to Naruse's formula and, using the work of Morales, Pak, and Panova in [17], analyse lower bounds on the number of configurations f of λ/μ such that $A_{n,n}(f) \geq 1$ and $A_{n,n}(f)$ is strictly less than

$$\frac{n!}{\prod_{r\in\lambda/\mu} h_r}.$$

Remark 3.31. Regarding Remark 3.30, there are variants and generalizations of Naruse's formula, the formula mentioned in Remark 3.30, for *skew shifted shapes* [9, 19]. What we observe about these shapes is that the "hook-sets" for skew shifted shapes as defined in [9, 19] also form examples of flagged families. Hence, the results in this section can be replicated verbatim to include *skew shifted shapes*. Moreover, it is claimed by Morales, Pak, and Panova in [17] that their analysis of Naruse's formula can be extended to skew shifted shapes. It also appears that we can even extend the above to involve posets known as *d-complete posets* [19], as there is a generalization of Naruse's formula for such posets and the "hook-sets" in these formulas are a generalization of the "hook-sets" for the skew shifted shapes [19].

We conclude this subsection by asking some natural enumerative questions related to the quantity $A_{n,m}(f)$ in Theorem 3.25.

1. Which configurations f as specified in Theorem 3.25 are such that $A_{n,m}(f)$ is given by Equation (3.9)?
2. Which flagged families $\mathcal{F}$ with transversal t are such that $A_{n,m}(f)$, with m fixed, is independent of the configuration f of t?
3. If the configuration f as specified in Theorem 3.25 is such that $f(F) = 1$ for all $F \in \mathcal{F}$, when is $A_{n,m}(f)$ maximal, and can $A_{n,m}(f)$ be less than or equal to Equation (3.9)?
4. Let $\mathcal{F}$ be a flagged family and let t be a transversal of $\mathcal{F}$. For m fixed, which configurations f of t maximize or minimize the value of $A_{n,m}(f)$?
5. Does the value of m in comparison to n affect answers to any of the above questions?

ORCID iDs

Brian Tianyao Chan https://orcid.org/0000-0003-0525-1362

References

[1] O. Angel, A. E. Holroyd, D. Romik and B. Virág, Random sorting networks, *Adv. Math.* **215** (2007), 839–868, doi:10.1016/j.aim.2007.05.019.

[2] M. Bóna, *A walk through combinatorics*, World Scientific Publishing Co., Inc., River Edge, NJ, 2002, doi:10.1142/4918, an introduction to enumeration and graph theory, With a foreword by Richard Stanley.

[3] G. J. Chang, On the number of SDR of a (t, n)-family, *European J. Combin.* **10** (1989), 231–234, doi:10.1016/s0195-6698(89)80056-3.

[4] P. Edelman and C. Greene, Combinatorial correspondences for Young tableaux, balanced tableaux, and maximal chains in the weak Bruhat order of S_n, in: *Combinatorics and algebra (Boulder, Colo., 1983)*, Amer. Math. Soc., Providence, RI, volume 34 of *Contemp. Math.*, pp. 155–162, 1984, doi:10.1090/conm/034/777699.

[5] P. Edelman and C. Greene, Balanced tableaux, *Adv. in Math.* **63** (1987), 42–99, doi:10.1016/0001-8708(87)90063-6.

[6] N. J. Y. Fan, Standard Rothe tableaux, *Discrete Math.* **342** (2019), 3182–3193, doi:10.1016/j.disc.2019.06.027.

[7] S. Fomin, C. Greene, V. Reiner and M. Shimozono, Balanced labellings and Schubert polynomials, *European J. Combin.* **18** (1997), 373–389, doi:10.1006/eujc.1996.0109.

[8] J. S. Frame, G. d. B. Robinson and R. M. Thrall, The hook graphs of the symmetric groups, *Canad. J. Math.* **6** (1954), 316–324, doi:10.4153/cjm-1954-030-1.

[9] W. Graham and V. Kreiman, Excited Young diagrams, equivariant K-theory, and Schubert varieties, *Trans. Amer. Math. Soc.* **367** (2015), 6597–6645, doi:10.1090/s0002-9947-2015-06288-6.

[10] M. Hall, Jr., Distinct representatives of subsets, *Bull. Amer. Math. Soc.* **54** (1948), 922–926, doi:10.1090/s0002-9904-1948-09098-x.

[11] P. Hall, On representatives of subsets, *J. London Math. Soc* **10** (1935), 26–30, doi:10.1112/jlms/s1-10.37.26.

[12] J. L. Hirst and N. A. Hughes, Reverse mathematics and marriage problems with unique solutions, *Arch. Math. Logic* **54** (2015), 49–57, doi:10.1007/s00153-014-0401-z.

[13] J. L. Hirst and N. A. Hughes, Reverse mathematics and marriage problems with finitely many solutions, *Arch. Math. Logic* **55** (2016), 1015–1024, doi:10.1007/s00153-016-0509-4.

[14] L. Hurwicz and S. Reiter, Transversals, systems of distinct representatives, mechanism design, and matching, in: *Markets, Games, and Organizations*, Springer, Berlin, Heidelberg, 2003, doi:10.1007/978-3-540-24784-5_10.

[15] M. Konvalinka, A bijective proof of the hook-length formula for skew shapes, *European J. Combin.* **88** (2020), 103104, 14, doi:10.1016/j.ejc.2020.103104.

[16] D. P. Little, Combinatorial aspects of the Lascoux-Schützenberger tree, *Adv. Math.* **174** (2003), 236–253, doi:10.1016/s0001-8708(02)00038-5.

[17] A. H. Morales, I. Pak and G. Panova, Asymptotics of the number of standard Young tableaux of skew shape, *European J. Combin.* **70** (2018), 26–49, doi:10.1016/j.ejc.2017.11.007.

[18] A. H. Morales, I. Pak and G. Panova, Hook formulas for skew shapes I. q-analogues and bijections, *J. Combin. Theory Ser. A* **154** (2018), 350–405, doi:10.1016/j.jcta.2017.09.002.

[19] H. Naruse and S. Okada, Skew hook formula for d-complete posets via equivariant K-theory, *Algebr. Comb.* **2** (2019), 541–571, doi:10.5802/alco.54.

[20] P. F. Reichmeider, *The equivalence of some combinatorial matching theorems*, Polygonal Publ. House, Washington, NJ, 1984, doi:10.2307/3615712.

[21] R. P. Stanley, *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 1999, doi:10.1017/cbo9780511609589, with a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.

[22] R. P. Stanley, *Enumerative Combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 2nd edition, 2012, doi:10.1017/cbo9781139058520.

[23] F. Viard, A new family of posets generalizing the weak order on some coxeter groups, 2015, `arXiv:1508.06141 [math.CO]`.

[24] F. Viard, A natural generalization of balanced tableaux, 2016, `arXiv:1407.6217v2 [math.CO]`.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.04 / 219–241
https://doi.org/10.26493/1855-3974.2478.d1b
(Also available at http://amc-journal.eu)

Enumerating symmetric peaks in non-decreasing Dyck paths*

Sergi Elizalde

Department of Mathematics, Dartmouth College, Hanover, NH, U.S.A.

Rigoberto Flórez †

Department of Mathematical Sciences, The Citadel, Charleston, SC, U.S.A.

José Luis Ramírez ‡

Departamento de Matemáticas, Universidad Nacional de Colombia, Bogotá, Colombia

Received 7 November 2020, accepted 25 February 2021, published online 30 September 2021

Abstract

Local maxima and minima of a Dyck path are called *peaks* and *valleys*, respectively. A Dyck path is *non-decreasing* if the heights (y-coordinates) of its valleys increase from left to right. A peak is symmetric if it is surrounded by two valleys (or endpoints of the path) at the same height. In this paper we give multivariate generating functions, recurrence relations, and closed formulas to count the number of symmetric and asymmetric peaks in non-decreasing Dyck paths. Finally, we use Riordan arrays to study weakly symmetric peaks, namely those for which the valley preceding the peak is at least as high as the valley following it.

Keywords: Non-decreasing Dyck path, symmetric peak, generating function, Riordan array, Fibonacci number.

Math. Subj. Class. (2020): 05A15, 05A19

*The authors are grateful to an anonymous referee for helpful comments.

†Corresponding author. The author was partially supported by the Citadel Foundation, Charleston, SC.
‡The author was partially supported by Universidad Nacional de Colombia, Project No. 46240.
E-mail addresses: sergi.elizalde@dartmouth.edu (Sergi Elizalde), rigo.florez@citadel.edu (Rigoberto Flórez), jlramirezr@unal.edu.co (José Luis Ramírez)

1 Introduction

A *Dyck path* is a lattice path in the first quadrant of the xy-plane that starts at the origin, ends on the x-axis, and consists of (the same number of) up-steps $X = (1, 1)$ and down-steps $Y = (1, -1)$. A *peak* is a subpath of the form XY, and a *valley* is a subpath of the form YX. The height of a valley is the y-coordinate of its lowest point. A Dyck path is called *non-decreasing* if the heights of its valleys form a non-decreasing sequence from left to right (see Figure 1 for an example). Non-decreasing Dyck paths have been extensively studied in the literature, see [2, 5, 6, 8, 13, 15, 17, 20]. All the Dyck paths considered in this paper will be non-decreasing. Following the notation from [5, 6, 13, 14], we denote by $\mathcal{D}$ the set of all non-decreasing Dyck paths, and by $\mathcal{D}_n$ the set of all non-decreasing Dyck paths of length $2n$, where the length is defined as the number of steps. For $P \in \mathcal{D}_n$, we write $|P|= n$ to denote its semilength.

A *pyramid* of semilength $h \geq 1$ is a subpath of the form X^hY^h; it is *maximal* if it can not be extended to a pyramid $X^{h+1}Y^{h+1}$.

Flórez and Ramírez [16] introduced the concept of symmetric and asymmetric peaks in Dyck paths, see also recent follow-up work by Elizalde [11] and Flórez et al. [14]. This concept was motivated in part by Asakly's [1] study of symmetric and asymmetric peaks in k-ary words. The concept of symmetric peaks is different from the notion of *degree of symmetry*, which has been considered by Elizalde [9, 10] as a measure of how symmetric a Dyck path is.

In this paper we study symmetric peaks and asymmetric peaks in non-decreasing Dyck paths. A peak is *symmetric* if the maximal pyramid containing the peak is not preceded by an X and is not followed by a Y. A peak is *weakly symmetric* if the maximal pyramid containing the peak is not preceded by an X. A peak is *asymmetric* if the maximal pyramid containing the peak is either preceded by an X or followed by a Y. Geometrically, a peak is symmetric if the maximal pyramid containing the peak is either at ground level or bounded by two valleys at the same height, and it is asymmetric otherwise. For example, in the non-decreasing Dyck path in Figure 1, the first, third, fourth, and sixth peaks are symmetric. The weakly symmetric peaks are the symmetric ones along with the seventh peak. Finally, the second, fifth, and the seventh peaks are asymmetric.

We are also interested in the size of the maximal pyramid containing a peak. We define the *weight* of a pyramid X^hY^h to be equal to h. In [5, 7], the authors refer to this parameter as the height, but we will use the term weight to suggest that it is not affected by the location of the pyramid. We define the *weight* of a peak to be the weight of the maximal pyramid that contains it. The *symmetric weight* of a path is the sum of the weights of its symmetric peaks. Similarly, the *asymmetric weight* of a path is the sum of the weights of its asymmetric peaks. For example, the weights of the symmetric peaks in the path depicted in Figure 1 are 4, 3, 3, 2 from left to right, and so the symmetric weight of the path is 12. The weights of asymmetric peaks are 1, 3, and 1, and the asymmetric weight of the path is 5.

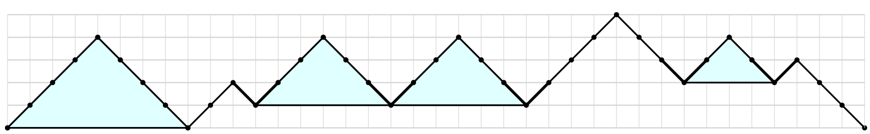


Figure 1: A non-decreasing Dyck path of length 38.

The generating functions that we present throughout the paper, are given using the symbolic method (cf. [12]). In Section 2, we give generating functions, recurrence relations, and closed formulas enumerating symmetric peaks and asymmetric peaks in non-decreasing Dyck paths. In Section 3, we focus on the enumeration of peaks with respect to their weight, and we give a connection to directed column-convex polyominoes. In Section 4, we study weakly symmetric peaks, and we synthesize the results using Riordan arrays. A summary of notation used throughout the paper appears in Tables 1 and 2 in the appendix.

2 Counting symmetric peaks

In this section we study the distribution of the number of symmetric peaks in $\mathcal{D}_n$. We give recurrences, generating functions and closed formulas (in terms of Fibonacci numbers) that enumerate these statistics in non-decreasing Dyck paths. Throughout the paper we will use F_n and L_n to denote the nth Fibonacci number and the nth Lucas number, respectively.

The set $\mathcal{D}_n$ can be partitioned into two disjoint sets $\mathcal{A}_n$ and $\mathcal{B}_n$, where $\mathcal{A}_n$ consists of the paths that have at least one valley of ground level (height 0), and $\mathcal{B}_n = \mathcal{D}_n \setminus \mathcal{A}_n$. Note that

$$\mathcal{D}_n = \mathcal{A}_n \,\dot\cup\, \mathcal{B}_n \quad \text{and} \quad \mathcal{A}_n = \dot{\bigcup_{i=1}^{n-1}} \mathcal{C}_{n,i}, \tag{2.1}$$

where $\mathcal{C}_{n,i}$ consists of those paths whose first valley touches the x-axis at $(2i, 0)$, and $\dot\cup$ denotes disjoint union. There is a natural bijection

$$\begin{array}{ccc} \mathcal{C}_{n,i} & \to & \mathcal{D}_{n-i} \\ P & \mapsto & P \setminus \Delta_i, \end{array} \tag{2.2}$$

obtained by removing the first pyramid $\Delta_i = X^iY^i$ of each $P \in \mathcal{C}_{n,i}$. Similarly, there is a bijection from $\mathcal{B}_n$ to $\mathcal{D}_{n-1}$ obtained by removing the first up-step and last down-step from each path.

From (2.1), a path $Q \in \mathcal{D}$ is either empty or has one of these two forms: $Q = XPY$ or $Q = X^kY^kP$, where $k \geq 1$ and $P \in \mathcal{D}$ is non-empty. This decomposition gives rise to the following equation for the generating function $D(x) = \sum_{P \in \mathcal{D}} x^{|P|} = \sum_{n \geq 0} |\mathcal{D}_n| x^n$:

$$D(x) = 1 + xD(x) + \frac{x}{1-x}(D(x) - 1). \tag{2.3}$$

Solving this equation and removing the empty path, we obtain the generating function for non-decreasing Dyck paths with respect to their semilength:

$$D(x) = \frac{x(1-x)}{1-3x+x^2} = \sum_{n=1}^{\infty} F_{2n-1}x^n.$$

Therefore,

$$|\mathcal{D}_n| = F_{2n-1}. \tag{2.4}$$

Other derivations of this generating function appear in [2, 13].

2.1 A generating function for the number of symmetric and asymmetric peaks

In this section we give a multivariate generating function enumerating symmetric peaks and the number of asymmetric peaks in non-decreasing Dyck paths. We start by introducing some terminology. We define the *insertion vertices* of a path to be the lowest point of each valley YX, the initial point of the path, and, if the path contains no valleys at positive height, the final point of the path. For a path $P \in \mathcal{D}$, we use $\tau(P)$, $\sigma(P)$, $\overline{\sigma}(P)$, $\nu(P)$, and $\iota(P)$ to denote the number of peaks, the number of symmetric peaks, the number of asymmetric peaks, the number of valleys, and the number of insertion points of P, respectively. We are interested in the generating function

$$D_{\sigma,\overline{\sigma}}(t,r,x) = \sum_{P\in\mathcal{D}} t^{\sigma(P)} r^{\overline{\sigma}(P)} x^{|P|}.$$

The coefficient of $t^i r^j x^n$ in $D_{\sigma,\overline{\sigma}}(t,r,x)$ is the number of paths of length $2n$ with i symmetric peaks and j asymmetric peaks.

Theorem 2.1. *The generating function for non-decreasing Dyck paths with respect to the number of symmetric peaks and the number of asymmetric peaks is*

$$D_{\sigma,\overline{\sigma}}(t,r,x) = \frac{1-(3+t)x+(3+2t-r)x^2-(1+t-r-r^2)x^3}{(1-(1+t)x)(1-(t+2)x+(1+t-r)x^2)}.$$

Proof. In order to obtain an expression for $D_{\sigma,\overline{\sigma}}(t,r,x)$, we show that non-decreasing Dyck paths where some of their symmetric peaks have been marked can be constructed by inserting marked symmetric peaks in certain positions of smaller non-decreasing Dyck paths.

First, we refine Equation (2.3) by introducing a variable v that keeps track of the number of valleys in the path. Letting $D_\nu(v,x) = \sum_{P\in\mathcal{D}} v^{\nu(P)} x^{|P|}$, the same decomposition gives

$$D_\nu(v,x) = 1 + xD_\nu(v,x) + \frac{vx}{1-x}(D_\nu(v,x)-1),$$

from where

$$D_\nu(v,x) = \frac{1-(1+v)x}{1-(2+v)x+x^2}.$$

Next we introduce another refinement. Let $\mathcal{D}^\Delta \subseteq \mathcal{D}$ denote the set of paths that consist of a non-empty sequence of pyramids, that is, paths of the form $X^{k_1}Y^{k_1}\cdots X^{k_j}Y^{k_j}$, where $k_i \geq 1$ for $1 \leq i \leq j$, for some $j \geq 1$. Let $D_{\tau,\iota}(p,q,x) = \sum_{P\in\mathcal{D}} p^{\tau(P)} q^{\iota(P)} x^{|P|}$ be the generating function with respect to the number of peaks and the number of insertion vertices. Recall that insertion vertices of P are the bottoms of the valleys, the initial point of P, and, in the case that $P \in \mathcal{D}^\Delta$, the final point of P. Thus, $\iota(P) = \nu(P) + 2$ if $P \in \mathcal{D}^\Delta$, and $\iota(P) = \nu(P) + 1$ otherwise. On the other hand, $\tau(P) = \nu(P) + 1$ unless P is empty, in which case $\tau(P) = 0$. Using that

$$D_\nu^\Delta(v,x) = \sum_{P\in\mathcal{D}^\Delta} v^{\nu(P)} x^{|P|} = \frac{x/(1-x)}{1-vx/(1-x)} = \frac{x}{1-x-vx},$$

it follows that

$$\begin{aligned} D_{\tau,\iota}(p,q,x) &= q + pq(D_\nu(pq,x) - D_\nu^\Delta(pq,x) - 1) + pq^2 D_\nu^\Delta(pq,x) \\ &= q + \frac{pq^2x(1-(2+pq)x+(1+p)x^2)}{(1-x+pqx)(1-(2+pq)x+x^2)}. \end{aligned} \tag{2.5}$$

By construction, the insertion vertices of P are those vertices where the insertion of a pyramid X^kY^k creates a symmetric peak and results in another non-decreasing Dyck path.

Our next step is to enumerate non-decreasing Dyck paths where some of its symmetric peaks have been *marked*. Formally, we are enumerating pairs (P, M) where $P \in \mathcal{D}$ and M is a subset of the symmetric peaks of P. Let $\mathcal{D}^*$ be the set of such pairs (P, M), which we refer to as *non-decreasing Dyck paths with marked symmetric peaks*, and let $D^*_\tau(p, u, x) = \sum_{(P,M)\in\mathcal{D}^*} p^{\tau(P)}u^{|M|}x^{|P|}$. The key observation is that elements of $\mathcal{D}^*$ can be uniquely obtained from paths in $\mathcal{D}$ by inserting a possibly empty sequence of marked pyramids (that is, pyramids whose symmetric peak is marked) at each insertion vertex. Since replacing each insertion vertex with a sequence of marked pyramids corresponds to the substitution

$$q = \frac{1}{1 - upx/(1-x)},$$

we get

$$D^*_\tau(p, u, x) = D_{\tau,\iota}\left(p, \frac{1}{1 - upx/(1-x)}, x\right).$$

In order to have a variable t that keeps track of the total number of symmetric peaks, as opposed to marked symmetric peaks, we make the substitution $u = t - 1$. Note that, if $\Sigma(P)$ is the set of symmetric peaks of a path $P \in D$, then

$$\sum_{M\subseteq\Sigma(P)} (t-1)^{|M|} = ((t-1)+1)^{|\Sigma(P)|} = t^{\sigma(P)}. \tag{2.6}$$

It follows that

$$D_{\tau,\sigma}(p, t, x) = \sum_{P\in\mathcal{D}} p^{\tau(P)}t^{\sigma(P)}x^{|P|} = \sum_{P\in\mathcal{D}}\sum_{M\subseteq\Sigma(P)} p^{\tau(P)}(t-1)^{|M|}x^{|P|} = D^*_\tau(p, t-1, x).$$

Finally, since $\overline{\sigma}(P) = \tau(P) - \sigma(P)$, we have

$$D_{\sigma,\overline{\sigma}}(t, r, x) = D_{\tau,\sigma}(r, t/r, x) = D_{\tau,\iota}\left(r, \frac{1}{1-(t-r)x/(1-x)}, x\right),$$

and the formula in the statement follows now from Equation (2.5). □

Corollary 2.2. *The generating functions for the total number of symmetric peaks and the total number of asymmetric peaks in non-decreasing Dyck paths are, respectively,*

$$S(x) := \sum_{P\in\mathcal{D}} \sigma(P)x^{|P|} = \frac{\partial}{\partial t}D_{\sigma,\overline{\sigma}}(t, 1, x)\bigg|_{t=1} = \frac{x(1-5x+7x^2-x^3-x^4)}{(1-2x)(1-3x+x^2)^2}, \tag{2.7}$$

$$\sum_{P\in\mathcal{D}} \overline{\sigma}(P)x^{|P|} = \frac{\partial}{\partial r}D_{\sigma,\overline{\sigma}}(1, r, x)\bigg|_{r=1} = \frac{x^3(2-6x+3x^2)}{(1-2x)(1-3x+x^2)^2}.$$

2.2 Recurrence relations and Fibonacci numbers

Let $s_n = \sum_{P\in\mathcal{D}_n} \sigma(P)$, that is, the total number of symmetric peaks in all non-decreasing Dyck paths of semilength n. Note that $S(x) = \sum_{n\geq 1} s_n x^n$ is the generating function in Equation (2.7). Next we give a recurrence for s_n that involves the Fibonacci numbers. Define the *level* of a pyramid to be the height of the base of the pyramid.

Theorem 2.3. *The sequence s_n satisfies the recurrence relation*

$$s_n = 3s_{n-1} - s_{n-2} + F_{2(n-2)} - 2^{n-3} \quad \textit{for } n \geq 3,$$

with initial values $s_1 = 1$ and $s_2 = 3$.

Proof. Recall the decomposition given in (2.1). It is clear from the definition of non-decreasing Dyck paths that the first pyramid in every path in $\mathcal{C}_{n,i}$ has a symmetric peak. Applying the bijection $\mathcal{C}_{n,i} \to \mathcal{D}_{n-i}$ from Equation (2.2) to all paths in $\mathcal{C}_{n,i}$ removes a total of $|\mathcal{D}_{n-i}| = F_{2(n-i)-1}$ pyramids (using Equation (2.4)), each having a symmetric peak. This implies that the number of symmetric peaks in $\mathcal{C}_{n,i}$ equals $F_{2(n-i)-1}$ plus the number of symmetric peaks in $\mathcal{D}_{n-i}$. So, the total number of symmetric peaks in $\mathcal{A}_n$ is given by

$$\sum_{i=1}^{n-1} s_{n-i} + \sum_{i=1}^{n-1} F_{2(n-i)-1} = \sum_{i=1}^{n-1} s_i + F_{2(n-1)}. \tag{2.8}$$

We now count the total number of symmetric peaks in $\mathcal{B}_n$, using the fact that $\mathcal{B}_n$ maps bijectively into $\mathcal{D}_{n-1}$ by deleting the first X and the last Y. Note, however, that the first and the last peak of paths in $\mathcal{B}_n$ are not symmetric (unless the path is a pyramid), but they may become symmetric after the first X and the last Y are deleted. This happens when the associated path in $\mathcal{D}_{n-1}$ starts or ends with a pyramid at ground level, without the path being itself the pyramid $\Delta_{n-1} = X^{n-1}Y^{n-1}$, resulting in more symmetric peaks in $\mathcal{D}_{n-1}$ than in $\mathcal{B}_n$. Therefore, to count the number of symmetric peaks in $\mathcal{B}_n$, we take the number of symmetric peaks in $\mathcal{D}_{n-1}$, which is s_{n-1}, and subtract the total number of first and last pyramids at ground level of paths in $\mathcal{D}_{n-1} \setminus \{\Delta_{n-1}\}$.

First of all, we want to know the total number of pyramids at ground level that occur at the end of the paths in $\mathcal{D}_{n-1} \setminus \{\Delta_{n-1}\}$. Note that if the last pyramid of a non-decreasing Dyck path is at ground level, then the path consists of a sequence of pyramids at ground level. From [13, Corollary 6.3], we deduce that the number of paths in $\mathcal{D}_{n-1}$ ending with a pyramid $\Delta_i = X^iY^i$ at ground level, for $1 \leq i \leq n-2$, is $2^{(n-1-i)-1}$. This implies that the total number of last pyramids at ground level in $\mathcal{D}_{n-1} \setminus \{\Delta_{n-1}\}$ is $\sum_{i=0}^{n-3} 2^i = 2^{n-2} - 1$. From a similar analysis as in the first paragraph of this proof, we have that the total number of first pyramids at ground level in $\mathcal{D}_{n-1} \setminus \{\Delta_{n-1}\}$ is $\sum_{i=1}^{n-2} F_{2i-1} = F_{2(n-2)}$. So, the total number of symmetric peaks in $\mathcal{B}_n$ is given by $s_{n-1} - F_{2(n-2)} - 2^{n-2} + 1$. Adding this to (2.8), we get

$$s_n = \left(\sum_{i=1}^{n-1} s_i + F_{2(n-1)} \right) + \left(s_{n-1} - F_{2(n-2)} - 2^{n-2} + 1 \right),$$

with $s_1 = 1$, and $s_2 = 3$. We can simplify the recurrence by computing $s_{n+1} - s_n = 2s_n - s_{n-1} + F_{2(n-1)} - 2^{n-2}$. Therefore,

$$s_{n+1} = 3s_{n-1} - s_{n-2} + F_{2(n-2)} - 2^{n-3}. \qquad \square$$

The first few values of the sequence s_n for $n \geq 1$ are

$$1, \quad 3, \quad 8, \quad 22, \quad 62, \quad 177, \quad 508, \quad 1459, \quad 4182, \quad 11946, \quad \ldots.$$

For example, Figure 2 shows the non-decreasing Dyck paths of length 6, where the total number of symmetric peaks is $s_3 = 8$.

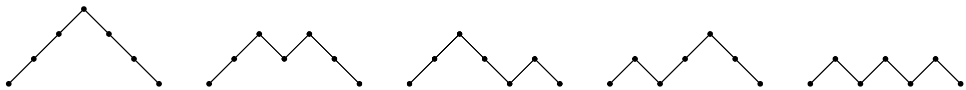


Figure 2: Non-decreasing Dyck paths of length 6.

Next we give another expression for s_n in terms of the Fibonacci and the Lucas numbers.

Theorem 2.4. *The sequence s_n satisfies*

$$s_n = F_{2n} + \sum_{\ell=3}^{n} (F_{2\ell-2} - 2^{\ell-2})F_{2(n-\ell)} = \frac{2F_{2n-2} + (n-1)L_{2n-2}}{5} + 2^{n-1}.$$

Proof. We first consider the generating function of the bisection of the Fibonacci sequence

$$F(x) = \sum_{n\geq 0} F_{2n}x^n = \frac{x}{1-3x+x^2}.$$

By Equation (2.7), the generating function $S(x)$ can be decomposed as

$$\begin{aligned} S(x) &= F(x)\,\frac{1-5x+7x^2-x^3-x^4}{(1-2x)(1-3x+x^2)} = F(x)\left(1+\frac{x^2}{1-3x+x^2}-\frac{x^2}{1-2x}\right) \\ &= F(x)\left(1+xF(x)-\frac{x^2}{1-2x}\right). \end{aligned}$$

Using the Cauchy product of series we obtain the desired result. The second equality follows from the recurrence relation given in Theorem 2.3. □

In [6, Theorem 2], the authors prove that the total number of peaks in $\mathcal{D}_n$ is

$$t_n = \frac{(2n-1)F_{2n} - (n-5)F_{2n-1}}{5}. \tag{2.9}$$

The next corollary is a direct consequence of Theorem 2.4 and Equation (2.9).

Corollary 2.5. *Let $\overline{s}_n$ be the total number of asymmetric peaks in $\mathcal{D}_n$. Then, for $n \geq 2$,*

$$\overline{s}_n = \frac{2F_{2n+1} + (n-2)L_{2n-3}}{5} - 2^{n-1}.$$

The first few values of the sequence $\overline{s}_n$ for $n \geq 1$ are

$$0, \quad 0, \quad 2, \quad 10, \quad 37, \quad 122, \quad 379, \quad 1136, \quad 3326, \quad 9580, \quad \ldots.$$

From the identities in Theorem 2.4 and Corollary 2.5, we obtain some asymptotic results about the proportion of peaks in non-decreasing Dyck paths that are symmetric.

Theorem 2.6. *Among all peaks of non-decreasing Dyck paths, the proportion of those that are symmetric is asymptotically*

$$\lim_{n\to\infty} \frac{s_n}{t_n} = \frac{-1+\sqrt{5}}{2} \approx 0.618034.$$

Proof. From the well-known limits

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \phi = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \lim_{n\to\infty} \frac{L_n}{F_n} = \sqrt{5},$$

we have

$$\begin{aligned}
\lim_{n\to\infty} \frac{s_n}{t_n} &= \lim_{n\to\infty} \frac{(2F_{2n-2} + (n-1)L_{2n-2})/5 + 2^{n-1}}{((2n-1)F_{2n} - (n-5)F_{2n-1})/5} \\
&= \lim_{n\to\infty} \frac{2 + (n-1)L_{2n-2}/F_{2n-2} + 5\cdot 2^{n-1}/F_{2n-2}}{(2n-1)F_{2n}/F_{2n-2} - (n-5)F_{2n-1}/F_{2n-2}} \\
&= \frac{\sqrt{5}}{2\phi^2 - \phi} = \frac{-1+\sqrt{5}}{2}.
\end{aligned}$$

□

Corollary 2.7. *Among all peaks of non-decreasing Dyck paths, the proportion of those that are asymmetric is asymptotically*

$$\lim_{n\to\infty} \frac{\overline{s}_n}{t_n} = \frac{3-\sqrt{5}}{2} \approx 0.381966.$$

We say that a symmetric peak is *low* if the y-coordinate of its top vertex is one, and that it is *high* if this coordinate is greater than 1. Note that every low peak is symmetric. By [6, Corollary 6], the total number of high peaks in $\mathcal{D}_n$ is $((2n-1)F_{2n} - nF_{2n-1})/5$. Together with Corollary 2.5, this implies the following.

Corollary 2.8. *The total number of high symmetric peaks in $\mathcal{D}_n$ is*

$$\frac{1}{5}\left(F_{2n-3} + (n-4)L_{2n-2}\right) + 2^{n-1}.$$

3 Symmetric weight and symmetric height

Recall that the weight of a pyramid $X^h Y^h$ is equal to h and that the weight of a peak is the weight of the maximal pyramid that contains it. In this section we give a multivariate generating function for non-decreasing Dyck paths with respect to the weight of their symmetric peaks, as well a recurrence relation for the total symmetric weight over $\mathcal{D}_n$. We also give a recurrence relation for the total sum of the heights of symmetric peaks over $\mathcal{D}_n$. At the end of the section we describe a connection with polyominoes.

3.1 A generating function for symmetric weight

We introduce an infinite family of variables $\mathbf{t} = (t_1, t_2, \dots)$ in order to keep track of symmetric peaks of a given weight. For $P \in \mathcal{D}$ and $i \geq 1$, let $\omega_i(P)$ be the number of symmetric peaks of weight i in P. Let $\boldsymbol{\omega}(P) = (\omega_1(P), \omega_2(P), \dots)$, and let $\mathbf{t}^{\boldsymbol{\omega}(P)} = \prod_{i\geq 1} t_i^{\omega_i(P)}$. We are interested in the generating function

$$D_{\boldsymbol{\omega}}(\mathbf{t}, x) = \sum_{P\in\mathcal{D}} \mathbf{t}^{\boldsymbol{\omega}(P)} x^{|P|}.$$

Theorem 3.1. *Let $P(\mathbf{t}, x) = \sum_{i\geq 1} t_i x^i$. The generating function for non-decreasing Dyck paths with respect to the weights of their symmetric peaks is*

$$D_{\boldsymbol{\omega}}(\mathbf{t}, x) = \frac{1 - 3x + 2x^2 + x^3 - (1-x)^3 P(\mathbf{t}, x)}{(1-x)(1 - P(\mathbf{t}, x))(1 - 2x - (1-x)^2 P(\mathbf{t}, x))}.$$

Proof. We modify the proof of Theorem 2.1 in order to keep track of the weight of the inserted marked symmetric peaks. Replacing insertion vertices in non-decreasing Dyck paths with sequences of marked pyramids, with variable u_i keeping track of marked pyramids of the form $X^i Y^i$ for each $i \geq 1$, corresponds to the substitution

$$q = \frac{1}{1 - \sum\limits_{i\geq 1} u_i x^i}$$

in $D_{\tau,\iota}(1, q, x)$. A variant of Equation (2.6), where we replace $\Sigma(P)$ with the set of symmetric peaks of weight i, shows that the substitutions $u_i = t_i - 1$ yield the generating function where t_i keeps track of the total number of symmetric peaks of weight i in non-decreasing Dyck paths. It follows that

$$D_{\boldsymbol{\omega}}(\mathbf{t}, x) = D_{\tau,\iota}\left(1, \frac{1}{1 - \sum\limits_{i\geq 1}(t_i - 1)x^i}, x\right) = D_{\tau,\iota}\left(1, \frac{1}{\frac{1}{1-x} - P(\mathbf{t}, x)}, x\right),$$

and the formula is now obtained from Equation (2.5). □

The symmetric weight of a path $P \in \mathcal{D}$ is defined as the sum of the weights of its symmetric peaks, and it is denoted by $\omega(P) = \sum_{i\geq 1} \omega_i(P)$. From Theorem 3.1, one can easily obtain a generating function for this statistic. Let

$$D_{\sigma,\omega}(t, w, x) = \sum_{P\in\mathcal{D}} t^{\sigma(P)} w^{\omega(P)} x^{|P|}$$

be the generating function for non-decreasing Dyck paths with respect to the number of symmetric peaks and the symmetric weight of the path.

Corollary 3.2. *The generating function $D_{\sigma,\omega}(t, w, x)$ is equal to*

$$\frac{(1 - wx)\left(1 - (3 + w + tw)x + (2 + 3w + 3tw)x^2 + (1 - 2w - 3tw)x^3 - (1-t)wx^4\right)}{(1-x)\left(1 - (t+1)wx\right)\left(1 - (2 + w + tw)x + 2(t+1)wx^2 - twx^3\right)}.$$

Proof. By definition, $D_{\sigma,\omega}(t, w, x)$ is obtained from $D_{\boldsymbol{\omega}}(\mathbf{t}, x)$ by making the substitution $t_i = tw^i$ for all $i \geq 1$. When applied to $P(\mathbf{t}, x)$, this substitution yields $\sum_{i\geq 1} tw^i x^i = twx/(1 - wx)$, and so the formula follows immediately from Theorem 3.1. □

Corollary 3.3. *The generating function for the total symmetric weight in non-decreasing Dyck paths is*

$$W(x) := \sum_{P\in\mathcal{D}} \omega(P) x^{|P|} = \frac{\partial}{\partial w} D_{\sigma,\omega}(1, w, x)\bigg|_{w=1} = \frac{x(1 - 5x + 7x^2 - x^3 - x^4)}{(1-x)(1-2x)(1 - 3x + x^2)^2}.$$

Comparing this formula with Equation (2.7), we see that

$$W(x) = \frac{S(x)}{1-x}.$$

Taking the coefficients of x^n on both sides, and letting $w_n = \sum_{P \in \mathcal{D}_n} \omega(P)$ denote the total symmetric weight of $\mathcal{D}_n$, we get

$$w_n = \sum_{k=1}^{n} s_k, \tag{3.1}$$

that is, the total symmetric weight of paths in $\mathcal{D}_n$ equals the total number of symmetric peaks of paths in $\bigcup_{k=1}^{n} \mathcal{D}_k$. Next we give a bijective proof of this equality.

The right-hand side of (3.1) can be interpreted as counting paths in $\bigcup_{k=1}^{n} \mathcal{D}_k$ with a distinguished symmetric peak. Indeed, for each k, the number of ways to choose path in $\mathcal{D}_k$ and select a symmetric peak of such path equals the total number of symmetric peaks of paths in $\mathcal{D}_k$, namely s_k. Similarly, the left-hand side of (3.1) can be interpreted as counting pairs $(\hat{P}, i)$, where $\hat{P}$ is a path in $\mathcal{D}_n$ with a distinguished symmetric peak, and i is an integer between 1 and the weight of the distinguished peak of $\hat{P}$. This is because, for a given path $P \in \mathcal{D}_n$, the number of ways to choose a symmetric peak of P and then an integer i between 1 and the weight of that peak equals the sum of the weights of the symmetric peaks of P, which is $\omega(P)$.

Let us describe a bijection between the sets counted by both sides of (3.1). Given a path in $\mathcal{D}_k$ (for some $k \leq n$) with a distinguished symmetric peak, insert a pyramid $X^{n-k}Y^{n-k}$ at the top of the distinguished peak to obtain a pair $(\hat{P}, i)$, where $\hat{P}$ is a path in $\mathcal{D}_n$ with a distinguished symmetric peak (the same distinguished peak where the pyramid was inserted), and $i = n-k$. Conversely, given such a pair $(\hat{P}, i)$, delete the pyramid X^iY^i around the distinguished peak, to obtain a path in $\mathcal{D}_{n-i}$ with a distinguished symmetric peak (the same distinguished peak from where the pyramid was removed).

3.2 Recurrence relations and Fibonacci numbers

Recall that w_n denotes the sum of the symmetric weights of all paths in $\mathcal{D}_n$. Similarly, let $\overline{w}_n$ denote the sum of the asymmetric weights of all paths in $\mathcal{D}_n$. For example, the paths in Figure 2 give $w_3 = 3+0+3+3+3 = 12$ and $\overline{w}_3 = 2$. The next theorem follows immediately by applying Equation (3.1) to Theorem 2.3.

Theorem 3.4. *The sequence w_n satisfies the recurrence relation*

$$w_n = 3w_{n-1} - w_{n-2} + F_{2n-3} - 2^{n-2} + 1 \quad \textit{for } n \geq 3,$$

with initial values $w_1 = 1$ and $w_2 = 4$.

The first few values of the sequence w_n for $n \geq 1$ are

$$1, \quad 4, \quad 12, \quad 34, \quad 96, \quad 273, \quad 781, \quad 2240, \quad 6422, \quad 18368, \quad \ldots.$$

From the expression for $W(x)$ in Corollary 3.3, we obtain the following corollary.

Corollary 3.5. *We have*

$$w_n = F_{2n} + \sum_{\ell=1}^{n} (F_{2\ell-1} - 2^{\ell-1} + 1) F_{2(n-\ell)}$$

and

$$w_n = \frac{1}{5}\left(nL_{2n-1} - F_{2n}\right) + 2^n - 1.$$

In [5, Theorem 8] the authors prove that the sum of the weights of all peaks in $\mathcal{D}_n$ is

$$\frac{2nF_{2n+1} + (2-n)F_{2n}}{5}.$$

As a direct application of Corollary 3.5, we obtain the following formula for the sum of the asymmetric weights of all paths in $\mathcal{D}_n$.

Corollary 3.6. *We have*

$$\overline{w}_n = \frac{1}{5}\left(3F_{2n} + nL_{2n-2}\right) - 2^n + 1.$$

3.3 Symmetric height

The height of a peak is the y-coordinate of the vertex at the top of the peak. Denote by h_n the total sum of the heights of all symmetric peaks of paths in $\mathcal{D}_n$. For example, from the paths in Figure 2, we see that $h_3 = 12$.

Theorem 3.7. *The sequence h_n satisfies the recurrence relation*

$$h_n = 3h_{n-1} - h_{n-2} + \frac{nL_{2n-5} + 7F_{2n-5}}{5} - 2^{n-2} + 1 \quad \textit{for } n \geq 3,$$

with initial values $h_1 = 1$ and $h_2 = 4$.

Proof. We will find the total sum of the heights of all symmetric peaks of paths in $\mathcal{D}_n = \mathcal{A}_n \uplus \mathcal{B}_n$ by adding the total sum of the heights of all symmetric peaks in $\mathcal{A}_n$ and the total sum of the heights of all symmetric peaks in $\mathcal{B}_n$. Recall that $\mathcal{A}_n = \uplus_{i=1}^{n-1} \mathcal{C}_{n,i}$, and that the first peak of every path in $\mathcal{C}_{n,i}$ is symmetric. From (2.2) we know that every path $P \in \mathcal{C}_{n,i}$ is a concatenation of the pyramid $\Delta_i = X^i Y^i$ with a path $Q \in \mathcal{D}_{n-i}$. So, the total sum of the heights of all symmetric peaks in P is given by the hight of Δ_i (which is equal to i) plus the total sum of the heights of all symmetric peaks in Q. Summing over all paths $P \in \mathcal{C}_{n,i}$, we deduce that the total sum of the heights of all symmetric peaks of $\mathcal{C}_{n,i}$ is $i|\mathcal{D}_{n-i}| + h_{n-i} = iF_{2(n-i)-1} + h_{n-i}$ (using that $|\mathcal{D}_{n-i}| = F_{2(n-i)-1}$, see (2.4)). Therefore, the total sum of the heights of all symmetric peaks in $\mathcal{A}_n$ is given by

$$\sum_{i=1}^{n-1} h_{n-i} + \sum_{i=1}^{n-1} iF_{2(n-i)-1} = \sum_{i=1}^{n-1} h_i + F_{2n-1} - 1. \tag{3.2}$$

We now count the sum of the heights of all symmetric peaks in $\mathcal{B}_n$, using the fact that $\mathcal{B}_n$ is in bijection with $\mathcal{D}_{n-1}$, for which the sum of the heights of all symmetric peaks is h_{n-1}. The bijection is given by removing the first and the last step of the path. Let us carefully analyze how the sum of the heights of the symmetric peaks is changed by this bijection. On the one hand, removing the first and last step of the path decreases the heights of the peaks by one. On the other hand, for paths in $\mathcal{D}_{n-1}$ that begin or end with a pyramid at ground level, those pyramids contain a symmetric peak that does not give a symmetric peak in the corresponding path in $\mathcal{B}_n$. To account for these cases, we subtract, from the total sum of heights of symmetric peaks in $\mathcal{D}_{n-1}$, the heights of the first and last peaks belonging to pyramids at ground level, and then we add one for each symmetric peak whose height has increased.

We recall that the paths in $\mathcal{D}_{n-1} \setminus \{\Delta_{n-1}\}$, whose first pyramid is at ground level have the form $\Delta_i P_{n-1-i}$, where $P_{n-1-i} \in \mathcal{D}_{n-1-i}$ and $1 \leq i \leq n-2$. For fixed i, the height of all first pyramids in all such paths is given by $i\,|\mathcal{D}_{n-1-i}| = i\,F_{2(n-1-i)-1}$. So, the total height of all first pyramids at ground level of paths in $\mathcal{D}_{n-1} \setminus \{\Delta_{n-1}\}$ is given by

$$\sum_{i=1}^{n-2}(n-1-i)F_{2i-1} = F_{2n-3} - 1. \tag{3.3}$$

We count the total height of pyramids at ground level that occur at the end of the paths in $\mathcal{D}_{n-1} \setminus \{\Delta_{n-1}\}$. If the last pyramid of a non-decreasing Dyck path is at ground level, then the whole path consists of a sequence of pyramids at ground level. From [13, Corollary 6.3], we deduce that the number of paths in $\mathcal{D}_{n-1}$ ending with a pyramid Δ_i at ground level, for $1 \leq i \leq n-2$, is $2^{(n-1-i)-1}$. So, the total height of all last pyramids at ground level of paths in $\mathcal{D}_{n-1} \setminus \{\Delta_{n-1}\}$ is given by

$$\sum_{i=1}^{n-2} i\,2^{n-i-2} = 2^{n-1} - n. \tag{3.4}$$

Now, —to account for the increase by one of peak heights caused by the addition of the initial X and the final Y to paths in $\mathcal{D}_{n-1}$— we add the total number of symmetric peaks in $\mathcal{D}_{n-1}$, which equals s_{n-1} (see Theorem 2.4). But this results in some over-counting due to the first and last pyramids at ground level of the paths in $\mathcal{D}_{n-1}$, so we have to subtract F_{2n-4} and $2^{n-2}-1$. All in all, the term that needs to be added to account for the increase in peak heights is

$$\left(\frac{2F_{2n-4} + (n-2)L_{2n-4}}{5} + 2^{n-2}\right) - F_{2n-4} - 2^{n-2} + 1. \tag{3.5}$$

Adding (3.2), h_{n-1}, and (3.5), and subtracting (3.3) and (3.4), we get the recurrence relation

$$\begin{aligned} h_n = {} & \sum_{i=1}^{n-1} h_i + F_{2n-1} - 1 + h_{n-1} + \\ & \left(\frac{2F_{2n-4} + (n-2)L_{2n-4}}{5} + 2^{n-2} - F_{2n-4} - 2^{n-2} + 1\right) - \left(F_{2n-3} - 1 + 2^{n-1} - n\right). \end{aligned}$$

Simplifying, we have that

$$h_n = \sum_{i=1}^{n-1} h_i + h_{n-1} + \frac{F_{2n-1} + nL_{2n-4} + L_{2n-5}}{5} - 2^{n-1} + n + 1,$$

where $h_1 = 1$, and $h_2 = 4$. Now it is easy to see that

$$h_{n+1} - h_n = 2h_n - h_{n-1} + \frac{F_{2n} + nL_{2n-3} + 5F_{2n-3}}{5} - 2^{n-1} + 1.$$

Therefore,

$$h_n = 3h_{n-1} - h_{n-2} + \frac{nL_{2n-5} + 7F_{2n-5}}{5} - 2^{n-2} + 1. \qquad \square$$

The first few values of the sequence h_n for $n \geq 1$ are

$$1, \quad 4, \quad 12, \quad 35, \quad 104, \quad 315, \quad 964, \quad 2957, \quad 9044, \quad 27502, \quad \ldots.$$

3.4 Connections with dccp-polyominoes

Non-decreasing Dyck paths are in bijection with a family of polyominoes called *directed column-convex polyominoes* (dccp). A polyomino is *directed* if each of its cells can be reached from its bottom left-hand corner by a path which is contained in the polyomino and uses only north and east steps. A dccp polyomino is a directed polyomino such that every column consists of contiguous cells [3]. Deutsch and Prodinger [8] give a bijection between the set of non-decreasing Dyck paths of length $2n$ and the set of dccp of area n, where the *area* of a polyomino is defined as its number of cells. Figure 3 shows a dccp of area 19. The numbers in the first (second) row represent the final (initial) altitude of each column.

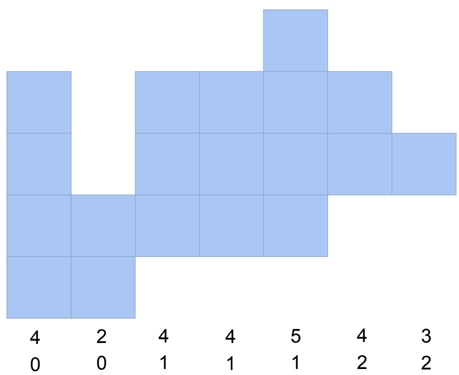


Figure 3: A direct column-convex polyomino (dccp).

The bijection from [8] can be described as follows. Given a dccp whose columns have initial altitudes $A = (0, a_2, \ldots, a_k)$ and final altitudes $B = (b_1, b_2, \ldots, b_k)$, from left to right, its corresponding non-decreasing Dyck path has valleys at heights $(a_2, \ldots, a_k)$, and peaks at heights $(b_1, b_2, \ldots, b_k)$, from left to right. For example, the dccp in Figure 3 is mapped to the path in Figure 1.

We say that two consecutive columns in a dccp polyomino are at the *same level* if their initial altitudes are the same. For example, the polyomino in Figure 3 has 4 pairs of consecutive columns at the same level; columns 1 and 2, columns 3 and 4, columns 4 and 5, and columns 6 and 7. Thus, the sequence s_n that we introduced in Section 2.2 also counts the total number of pairs of consecutive columns at the same level in all dccp polyominoes of area n. Moreover, if we define the weight of a pair of consecutive columns at the same level as the number of cells in the first of these two columns, then the total weight over all dccp polyominoes of area n is given by w_n.

4 Weakly symmetric peaks

In this section we consider a variation of symmetric peaks. We recall from Section 1 that a peak is *weakly symmetric* if the maximal pyramid containing the peak is not preceded by an X. Figure 4 shows different possibilities for the steps preceding and following the maximal pyramid of a weakly symmetric peak. Note that the last configuration in Figure 4 can only occur in the last peak of a path.

In Section 2, we gave generating functions to count symmetric and asymmetric peaks in non-decreasing Dyck paths, in this section we also give generating functions to count the number of weakly symmetric peaks. Surprisingly, the generating functions in this section have a simpler construction.

We will find formulas, involving Fibonacci numbers, for the total number of weakly symmetric peaks, as well as the sum of their weights, using generating functions and recurrence relations. The results in this section are synthesized using Riordan arrays.

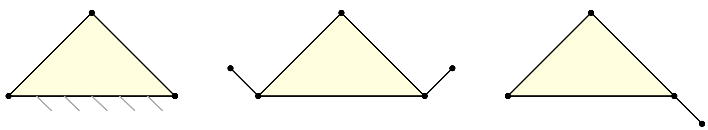


Figure 4: Weakly symmetric peaks.

4.1 A generating function for the number of weakly symmetric peaks

Let $\tilde{s}_n$ be the total number of weakly symmetric peaks in $\mathcal{D}_n$. For example, we see from the paths in Figure 2 that $\tilde{s}_3 = 9$. The first few values of $\tilde{s}_n$ for $n \geq 1$ are

$$1, \quad 3, \quad 9, \quad 27, \quad 80, \quad 234, \quad 677, \quad 1941, \quad 5523, \quad 15615, \quad \dots,$$

which correspond to sequence A059502 in [23].

Given a non-decreasing Dyck path P, we denote by $\tilde{\sigma}(P)$ the number of weakly symmetric peaks of P, and recall that $|P|$ denotes the semilength of P. We introduce the generating function

$$D_{\tilde{\sigma}}(x,y) = \sum_{P\in\mathcal{D}} x^{|P|}y^{\tilde{\sigma}(P)}.$$

Theorem 4.1. *The generating function $D_{\tilde{\sigma}}(x,y)$ is given by*

$$D_{\tilde{\sigma}}(x,y) = \frac{(1-x)xy}{1-(2+y)x+yx^2}.$$

Proof. Recall the decomposition in (2.1). Non-empty paths in $\mathcal{B}_n$ can be written as XY or $XT'Y$, where T' is a non-decreasing Dyck paths. Paths in $\mathcal{A}_n$ are of the form $X\Delta YT''$, where Δ is a pyramid and T'' is a non-decreasing Dyck paths. Figure 5 illustrates the three cases.

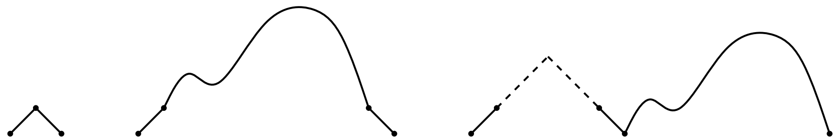


Figure 5: Decomposition of a non-decreasing Dyck path.

Using the symbolic method, we obtain the relation

$$D_{\tilde{\sigma}}(x,y) = xy + x(D_{\tilde{\sigma}}(x,y) \underbrace{-\frac{xy}{1-x}D_{\tilde{\sigma}}(x,y) + \frac{x}{1-x}D_{\tilde{\sigma}}(x,y)}_{(a)}) + \frac{xy}{1-x}D_{\tilde{\sigma}}(x,y).$$

The term (a) corresponds to the case where T' starts with a pyramid, which was symmetric in T' but is no longer weakly symmetric in the big path. This completes the proof. □

Corollary 4.2. *The total number of weakly symmetric peaks in $\mathcal{D}_n$ satisfies these*

(i) *The generating function for $\tilde{s}_n$ is given by*

$$\sum_{n=1}^{\infty} \tilde{s}_n x^n = \frac{(1-x)(1-2x)x}{(1-3x+x^2)^2}.$$

(ii) *The sequence $\tilde{s}_n$ satisfies the recurrence relation*

$$\tilde{s}_n = 6\tilde{s}_{n-1} - 11\tilde{s}_{n-2} + 6\tilde{s}_{n-3} - \tilde{s}_{n-4} \quad \textit{for } n \geq 5,$$

with initial values $\tilde{s}_1 = 1$, $\tilde{s}_2 = 3$, $\tilde{s}_3 = 9$ and $\tilde{s}_4 = 27$.

(iii) *The sequence $\tilde{s}_n$ satisfies the recurrence relation*

$$\tilde{s}_n = 3\tilde{s}_{n-1} - \tilde{s}_{n-2} + F_{2(n-2)} \quad \textit{for } n \geq 3,$$

with initial values $\tilde{s}_1 = 1$ and $\tilde{s}_2 = 3$.

(iv) *For $n \geq 1$, we have the convolution*

$$\tilde{s}_n = \sum_{\ell=0}^{n-1} F_{2\ell-1}F_{2(n-\ell)-1}.$$

(v) *The sequence $\tilde{s}_n$ satisfies that $\tilde{s}_n = (3F_{2n} + nL_{2n-2})/5$.*

Proof. By Theorem 4.1,

$$\sum_{n=0}^{\infty} \tilde{s}_n x^n = \left.\frac{\partial D_{\tilde{\sigma}}(x,y)}{\partial y}\right|_{y=1} = \frac{(1-x)(1-2x)x}{(1-3x+x^2)^2}.$$

This proves part (i). The recurrence in part (ii) is obtained from this rational generating function. The proof of (iii) is similar to the proof of Theorem 2.3, but in this case we do not subtract the last pyramid at ground level of paths in $\mathcal{B}_n$.

To prove part (iv), note that

$$\begin{aligned}\sum_{n=1}^{\infty}\tilde{s}_n x^n &= \left(\frac{(1-x)x}{1-3x+x^2}\right)\left(\frac{1-2x}{1-3x+x^2}\right)\\ &= \left(\sum_{n=1}^{\infty}F_{2n-1}x^n\right)\left(\sum_{n=0}^{\infty}F_{2n-1}x^n\right)\\ &= \sum_{n=1}^{\infty}\left(\sum_{\ell=0}^{n-1}F_{2\ell-1}F_{2(n-\ell)-1}\right)x^n.\end{aligned}$$

Comparing coefficients of x^n yields the identity.

Finally, it is easy to verify that the right side of part (v) satisfies the same recurrence relation as $\tilde{s}_n$ given in part (2), or alternatively in (3). □

From Part (v) of Corollary 4.2 and Equation (2.9), we conclude the following.

Theorem 4.3. *Among all peaks of all non-decreasing Dyck paths, the proportion of those that are weakly symmetric is asymptotically*

$$\lim_{n\to\infty}\frac{\tilde{s}_n}{t_n} = \frac{-1+\sqrt{5}}{2} \approx 0.618034.$$

Notice that this coincides with the asymptotic proportion of symmetric peaks given in Theorem 2.6.

4.2 A connection with Riordan arrays

In this section we use Riordan arrays to describe the distribution of the number of weakly symmetric peaks in non-decreasing Dyck paths. We start by giving some background on Riordan arrays [22]. We will say that an infinite column vector $(a_0, a_1, \dots)^T$ has generating function $f(x)$ if $f(x) = \sum_{n\geq 0} a_n x^n$, and we index rows and columns starting at 0. A *Riordan array* is an infinite lower triangular matrix whose kth column has generating function $g(x)f(x)^k$ for all $k \geq 0$, for some formal power series $g(x)$ and $f(x)$ with $g(0) \neq 0$, $f(0) = 0$, and $f'(0) \neq 0$. Such a Riordan array is denoted by $(g(x), f(x))$. If we multiply this matrix by a column vector $(c_0, c_1, \dots)^T$ having generating function $h(x)$, then the resulting column vector has generating function $g(x)h(f(x))$. This property is known as the fundamental theorem of Riordan arrays, or as the summation property.

The product of two Riordan arrays $(g(x), f(x))$ and $(h(x), l(x))$ is defined by

$$(g(x), f(x)) * (h(x), l(x)) = (g(x)h(f(x)), l(f(x))). \tag{4.1}$$

Under this operation, the set of all Riordan arrays is a group [22]. The identity element is $I = (1, x)$, and the inverse of $(g(x), f(x))$ is

$$(g(x), f(x))^{-1} = \left(1/\left(g\circ f^{<-1>}\right)(x), f^{<-1>}(x)\right), \tag{4.2}$$

where $f^{<-1>}(x)$ denotes the compositional inverse of $f(x)$.

Let $r_{n,k}$ be the number of paths in $\mathcal{D}_n$ with exactly k weakly symmetric peaks, that is,

$$D_{\tilde{\sigma}}(x,y) = \sum_{n,k\geq 1} r_{n,k}x^n y^k.$$

By definition, $\sum_{k=1}^{n} k\, r_{n,k} = \tilde{s}_n$.

Consider the matrix $\mathcal{R} = [r_{n,k}]_{n,k\geq 1}$. The first few rows of $\mathcal{R}$ are

$$\mathcal{R} = [r_{n,k}]_{n,k\geq 1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \\ 2 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & \\ 4 & 5 & 3 & 1 & 0 & 0 & 0 & 0 & \\ 8 & 12 & 9 & 4 & 1 & 0 & 0 & 0 & \cdots \\ 16 & 28 & 25 & 14 & 5 & 1 & 0 & 0 & \\ 32 & 64 & 66 & 44 & 20 & 6 & 1 & 0 & \\ 64 & 144 & 168 & 129 & 70 & 27 & 7 & 1 & \\ \vdots & & & \vdots & & & & & \ddots \end{pmatrix},$$

which correspond to array A105306 in [23]. Even though rows and columns of Riordan arrays are indexed starting at 0, the elements of $\mathcal{R}$ are shifted so that the entry in row 0 and column 0 is in fact $r_{1,1}$. The goal of this shift is to simplify some of our formulas.

Theorem 4.4. *The matrix $\mathcal{R}$ is a Riordan array given by*

$$\mathcal{R} = \left(\frac{1-x}{1-2x}, \frac{x(1-x)}{1-2x}\right).$$

Proof. Multiplying the right-hand side of the equality by the vector $(1, y, y^2, \dots)^T$, which has generating function $\frac{1}{1-xy}$, and using the summation property, the resulting vector has bivariate generating function

$$\begin{aligned}\left(\frac{1-x}{1-2x}, \frac{x(1-x)}{1-2x}\right)\frac{1}{1-xy} &= \frac{1-x}{1-2x}\frac{1}{1-\dfrac{x(1-x)}{1-2x}y} \\ &= \frac{1-x}{1-(2+y)x+yx^2} = \frac{D_{\tilde{\sigma}}(x,y)}{xy},\end{aligned}$$

by Theorem 4.1. □

Theorem 4.5. *For $n, k \geq 0$,*

$$r_{n+1,k+1} = \sum_{\ell=0}^{n} \binom{k+1}{\ell}\binom{n-\ell}{k}(-1)^{\ell}2^{n-k-\ell}.$$

Proof. From the definition of the Riordan array $\mathcal{R}$, we have

$$\begin{aligned} r_{n+1,k+1} &= [x^n]\, \frac{1-x}{1-2x}\left(\frac{x(1-x)}{1-2x}\right)^{k} \\ &= \left[x^{n-k}\right]\left(\frac{1-x}{1-2x}\right)^{k+1} \\ &= \left[x^{n-k}\right]\sum_{n\geq 0}\sum_{\ell=0}^{n}\binom{k+1}{\ell}\binom{k+n-\ell}{n-\ell}(-1)^{\ell}2^{n-\ell}x^n. \end{aligned}$$ □

Let $\mathcal{P} = \left[\binom{n}{k}\right]_{n,k\geq 0}$, often called Pascal's matrix, and let $\overline{\mathcal{P}} = [\overline{p_{i,j}}]$ be the matrix defined by

$$\overline{p_{i,j}} = \begin{cases} \binom{(i+j)/2}{j}, & \text{if } i+j \equiv 0 \pmod 2; \\ 0, & \text{otherwise.} \end{cases}$$

It is easy to show that $\mathcal{P}$ and $\overline{\mathcal{P}}$ are Riordan arrays given by

$$\mathcal{P} = \left(\frac{1}{1-x}, \frac{x}{1-x}\right) \quad \text{and} \quad \overline{\mathcal{P}} = \left(\frac{1}{1-x^2}, \frac{x}{1-x^2}\right).$$

Theorem 4.6. *The matrix $\mathcal{R}$ factors as $\mathcal{R} = \mathcal{P}\overline{\mathcal{P}}$.*

Proof. By Equation (4.1),

$$\begin{aligned} \mathcal{P}\overline{\mathcal{P}} &= \left(\frac{1}{1-x}, \frac{x}{1-x}\right)\left(\frac{1}{1-x^2}, \frac{x}{1-x^2}\right) \\ &= \left(\frac{1}{1-x}\left(\frac{1}{1-\left(\frac{x}{1-x}\right)^2}\right), \frac{\frac{x}{1-x}}{1-\left(\frac{x}{1-x}\right)^2}\right). \end{aligned}$$

Simplifying,

$$\mathcal{P}\overline{\mathcal{P}} = \left(\frac{1-x}{1-2x}, \frac{x(1-x)}{1-2x}\right) = \mathcal{R}.$$ ∎

From above theorem and the product of matrices we obtain the following combinatorial identities.

Theorem 4.7. *For $n, k \geq 0$,*

$$\begin{aligned} r_{n+1,2k+1} &= \sum_{\ell=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2\ell}\binom{\ell+k}{2k}, \\ r_{n+1,2k+2} &= \sum_{\ell=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2\ell+1}\binom{\ell+k+1}{2k+1}. \end{aligned}$$

Rogers [21], observed that every element not belonging to row 0 or column 0 in a Riordan array can be expressed as a fixed linear combination of the elements in the preceding row. The A-sequence is defined to be the sequence coefficients of this linear combination. Similarly, Merlini et al. [19] introduced the Z-sequence, that characterizes the elements in column 0, except for the top one. Therefore, the A-sequence, the Z-sequence and the upper-left element completely characterize a Riordan array. We summarize this characterization in the following two theorems.

Theorem 4.8 ([19]). *An infinite lower triangular array $\mathcal{F} = [d_{n,k}]_{n,k\geq 0}$ is a Riordan array if and only if $d_{0,0} \neq 0$ and there exist two sequences $(a_0, a_1, a_2, \dots)$, with $a_0 \neq 0$, and $(z_0, z_1, z_2, \dots)$ (called the A-sequence and the Z-sequence, respectively), such that*

$$\begin{aligned} d_{n+1,k+1} &= a_0 d_{n,k} + a_1 d_{n,k+1} + a_2 d_{n,k+2} + \cdots && \text{for } n, k \geq 0, \\ d_{n+1,0} &= z_0 d_{n,0} + z_1 d_{n,1} + z_2 d_{n,2} + \cdots && \text{for } n \geq 0. \end{aligned}$$

Theorem 4.9 ([18, 19]). *Let $\mathcal{F} = (g(x), f(x))$ be a Riordan array with inverse $\mathcal{F}^{-1} = (d(x), h(x))$. Then the A-sequence and the Z-sequence of $\mathcal{F}$ have generating functions*

$$A(x) = \frac{x}{h(x)}, \qquad Z(x) = \frac{1}{h(x)}\left(1 - d_{0,0}d(x)\right),$$

respectively.

Next we describe the A-sequence and Z-sequence for the Riordan array $\mathcal{R}$.

Theorem 4.10. *If C_n denotes the n-th Catalan number, then for $n, k \geq 2$,*

$$r_{n,k} = \sum_{\ell=0}^{n} r_{n-1,k-1+\ell}\, c_\ell,$$

where

$$c_n = \begin{cases} 1, & \text{if } n = 0, 1; \\ (-1)^{\frac{n+2}{2}} C_{\frac{n-2}{2}}, & \text{if } n \geq 2 \text{ is even}; \\ 0, & \text{otherwise.} \end{cases}$$

Moreover, for $n \geq 2$

$$r_{n,1} = \sum_{\ell=0}^{n} r_{n-1,k-1+\ell}\, c_{\ell+1},$$

with initial value $r_{1,1} = 1$.

Proof. By Equation (4.2), the inverse of the matrix $\mathcal{R}$ is given by

$$\mathcal{R}^{-1} = \left(\frac{1 + 2x - \sqrt{1+4x^2}}{2x}, \frac{1 + 2x - \sqrt{1+4x^2}}{2}\right).$$

Therefore, by Theorem 4.9, the A-sequence and Z-sequence of the Riordan array $\mathcal{R}$ have generating functions given by

$$A(x) = \frac{1 + 2x + \sqrt{1+4x^2}}{2} \quad \text{and} \quad Z(x) = \frac{-1 + 2x + \sqrt{1+4x^2}}{2x}.$$

We recall that the generating function of the Catalan numbers is given by

$$C(x) = \sum_{n\geq 0} C_n x^n = \frac{1 - \sqrt{1-4x}}{2x}.$$

Therefore, $A(x) = 1 + x + x^2 C(-x^2) = \sum_{n\geq 0} c_n x^n$, where c_n is as in the statement of the theorem. Similarly, $Z(x) = 1 + xC(-x^2)$. The recurrences from Theorem 4.8 now give the desired result. $\square$

The first few values of the sequence c_n for $n \geq 0$ are

$$1, \quad 1, \quad 1, \quad 0, \quad -1, \quad 0, \quad 2, \quad 0, \quad -5, \quad 0, \quad 14, \quad 0, \quad -42, \quad 0, \quad 132, \quad \ldots.$$

So, the recurrence for $r_{n,k}$ starts as

$$r_{n-1,k-1} + r_{n-1,k} + r_{n-1,k+1} - r_{n-1,k+3} + 2r_{n-1,k+5} - 5r_{n-1,k+7} + \cdots.$$

Next we analyze the central diagonal of the matrix $\mathcal{R}$, that is, the sequence $u_n = r_{2n+1,n+1}$ for $n \geq 0$ (recall that the entry in row i and column j of $\mathcal{R}$ is $r_{i+1,j+1}$). The first few values of u_n are

$$1, \quad 2, \quad 9, \quad 44, \quad 225, \quad 1182, \quad 6321, \quad 34232, \quad 187137, \quad 1030490, \quad 5707449, \quad \dots,$$

which correspond to the sequence A176479 in [23].

Barry [4] proved that for any Riordan array $(g(x), f(x)) = [d_{n,k}]_{n,k\geq 0}$ the generating function of its central diagonal is given by

$$\sum_{n\geq 0} d_{2n,n}x^n = \frac{v(x)g(v(x))}{f(v(x))}v'(x),$$

where

$$v(x) = \left(\frac{x^2}{f(x)}\right)^{<-1>}.$$

Therefore, by Theorem 4.4,

$$\sum_{n\geq 0} u_n x^n = \frac{3 - x + \sqrt{1-6x+x^2}}{4\sqrt{1-6x+x^2}}.$$

Other combinatorial interpretations of the sequence u_n are given in [23]. For example, it counts the number of Dyck paths having exactly n peaks at height 1, n peaks at height 2, and no other peaks. It is also equal to $n+1$ times the nth little Schröder number. The little Schröder numbers have several combinatorial interpretations in terms of leaves in plane trees, parenthesizations, and dissections of convex polygons [24].

4.3 A generating function for total weight

Let $\tilde{\omega}(P)$ be the sum of the weights of the weakly symmetric peaks of a path P. Define the generating function

$$D_{\tilde{\omega}}(x,y) = \sum_{P\in\mathcal{D}} x^{|P|}y^{\tilde{\omega}(P)}.$$

Theorem 4.11. *The generating function $D_{\tilde{\omega}}(x,y)$ is given by*

$$D_{\tilde{\omega}}(x,y) = \frac{(1-x)^2xy}{1-2(1+y)x+4yx^2-yx^3}.$$

Proof. We again use the refinement of the decomposition (2.1) illustrated in Figure 5: every non-empty non-decreasing Dyck path can be written as either XY, $XT'Y$, or $X\Delta YT''$, where T' and T'' are non-decreasing Dyck paths and Δ is a pyramid. It follows that

$$D_{\tilde{\omega}}(x,y) = xy + x(D_{\tilde{\omega}}(x,y) \underbrace{- \frac{xy}{1-xy}D_{\tilde{\omega}}(x,y) + \frac{x}{1-x}D_{\tilde{\omega}}(x,y)}_{(a)} - \underbrace{\frac{xy}{1-xy} + \frac{xy^2}{1-xy}}_{(b)})) + \frac{xy}{1-xy}D_{\tilde{\omega}}(x,y).$$

The correction term (a) corresponds to the case where T' consists of a pyramid followed by a non-empty path, whereas the term (b) corresponds to the case where T' is a pyramid. $\square$

From Theorem 4.11 we obtain the following corollary, whose proof is similar to that of Corollary 4.2. Let $\tilde{w}_n$ be the sum of the weights of all weakly symmetric peaks of paths in $\mathcal{D}_n$.

Corollary 4.12. *The sum of the weights of all weakly symmetric peaks in $\mathcal{D}_n$ satisfies the following:*

(i) *The generating function for $\tilde{w}_n$ is given by*

$$\sum_{n=1}^{\infty} \tilde{w}_n x^n = \frac{(1-2x)x}{(1-3x+x^2)^2}.$$

(ii) *The sequence $\tilde{w}_n$ satisfies the recurrence relation*

$$\tilde{w}_n = 6\tilde{w}_{n-1} - 11\tilde{w}_{n-2} + 6\tilde{w}_{n-3} - \tilde{w}_{n-4} \quad \textit{for } n \geq 5,$$

with initial values $\tilde{w}_1 = 1, \tilde{w}_2 = 4, \tilde{w}_3 = 13$ and $\tilde{w}_4 = 40$.

(iii) *For $n \geq 1$, we have the convolution*

$$\tilde{w}_n = \sum_{\ell=0}^{n} F_{2\ell-1} F_{2(n-\ell)} = \frac{4F_{2n} + nL_{2n-1}}{5}.$$

The first few values of $\tilde{w}_n$ for $n \geq 1$ are

$$1, \quad 4, \quad 13, \quad 40, \quad 120, \quad 354, \quad 1031, \quad 2972, \quad 8495, \quad 24110, \quad \dots,$$

which correspond to the sequence A238846 in [23].

Let $q_{n,k}$ be the number of paths in $\mathcal{D}_n$ which have weakly symmetric weight k, that is,

$$D_{\tilde{\omega}}(x,y) = \sum_{n,k\geq 1} q_{n,k} x^n y^k.$$

Notice that $\sum_{k=1}^{n} k\, q_{n,k} = \tilde{w}_n$. Consider the matrix defined by $\mathcal{Q} = [q_{n,k}]_{n,k\geq 1}$. The first few rows of $\mathcal{Q}$ are

$$\mathcal{Q} = [q_{n,k}]_{n,k\geq 1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & \\ 1 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & \\ 2 & 3 & 0 & 8 & 0 & 0 & 0 & 0 & \\ 4 & 6 & 8 & 0 & 16 & 0 & 0 & 0 & \cdots \\ 8 & 13 & 16 & 20 & 0 & 32 & 0 & 0 & \\ 16 & 28 & 37 & 40 & 48 & 0 & 64 & 0 & \\ 32 & 60 & 84 & 98 & 96 & 112 & 0 & 128 & \\ \vdots & & & \vdots & & & & & \ddots \end{pmatrix}.$$

Again, as in the matrix $\mathcal{R}$, the elements of $\mathcal{Q}$ are shifted so that the entry in row 0 and column 0 is $q_{1,1}$. The proof of our last result is similar to that of Theorem 4.4.

Theorem 4.13. *The matrix $\mathcal{Q}$ is a Riordan array given by*

$$\mathcal{Q} = \left(\frac{1-2x+x^2}{1-2x}, \frac{2x-4x^2+x^3}{1-2x} \right).$$

ORCID iDs

Sergi Elizalde https://orcid.org/0000-0003-4116-2455
Rigoberto Flórez https://orcid.org/0000-0002-3644-9358
José Luis Ramírez https://orcid.org/0000-0002-8028-9312

References

[1] W. Asakly, Enumerating symmetric and non-symmetric peaks in words, *Online J. Anal. Comb.* (2018), 7, https://hosted.math.rochester.edu/ojac/articles.html.

[2] E. Barcucci, A. Del Lungo, S. Fezzi and R. Pinzani, Nondecreasing Dyck paths and q-Fibonacci numbers, *Discrete Math.* **170** (1997), doi:10.1016/s0012-365x(97)82778-1.

[3] E. Barcucci, R. Pinzani and R. Sprugnoli, Directed column-convex polyominoes by recurrence relations, in: *TAPSOFT '93: theory and practice of software development (Orsay, 1993)*, Springer, Berlin, volume 668 of *Lecture Notes in Comput. Sci.*, pp. 282–298, 1993, doi:10.1007/3-540-56610-4_71.

[4] P. Barry, On the central coefficients of Riordan matrices, *J. Integer Seq.* **16** (2013), Article 13.5.1, 12pp, https://cs.uwaterloo.ca/journals/JIS/VOL16/Barry1/barry242.html.

[5] E. Czabarka, R. Flórez and L. Junes, Some enumerations on non-decreasing Dyck paths, *Electron. J. Combin.* **22** (2015), Paper 1.3, 22, doi:10.37236/3941.

[6] E. Czabarka, R. Flórez, L. Junes and J. L. Ramírez, Enumerations of peaks and valleys on non-decreasing Dyck paths, *Discrete Math.* **341** (2018), 2789–2807, doi:10.1016/j.disc.2018.06.032.

[7] A. Denise and R. Simion, Two combinatorial statistics on Dyck paths, *Discrete Math.* **137** (1995), 155–176, doi:10.1016/0012-365x(93)e0147-v.

[8] E. Deutsch and H. Prodinger, A bijection between directed column-convex polyominoes and ordered trees of height at most three, *Theoret. Comput. Sci.* **307** (2003), 319–325, doi:10.1016/s0304-3975(03)00222-6, random generation of combinatorial objects and bijective combinatorics.

[9] S. Elizalde, Measuring symmetry in lattice paths and partitions, *Sém. Lothar. Combin.* **84B** (2020), Art. 26, 12pp, https://www.mat.univie.ac.at/~slc/.

[10] S. Elizalde, The degree of symmetry of lattice paths, *Ann. Comb.* (2021), doi:10.1007/s00026-021-00551-6.

[11] S. Elizalde, Symmetric peaks and symmetric valleys in Dyck paths, *Discrete Math.* **344** (2021), 112364, doi:10.1016/j.disc.2021.112364.

[12] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press, Cambridge, 2009.

[13] R. Flórez, L. Junes and J. L. Ramírez, Enumerating several aspects of non-decreasing Dyck paths, *Discrete Math.* **342** (2019), 3079–3097, doi:10.1016/j.disc.2019.06.018.

[14] R. Flórez, L. Junes and J. L. Ramírez, Counting asymmetric weighted pyramids in non-decreasing Dyck paths, *Australas. J. Combin.* **79** (2021), 123–140, https://ajc.maths.uq.edu.au/?page=get_volumes&volume=79.

[15] R. Flórez and J. L. Ramírez, Some enumerations on non-decreasing Motzkin paths, *Australas. J. Combin.* **72** (2018), 138–154, https://ajc.maths.uq.edu.au/?page=get_volumes&volume=72.

[16] R. Flórez and J. L. Ramírez, Enumerating symmetric and asymmetric peaks in Dyck paths, *Discrete Math.* **343** (2020), 112118, doi:10.1016/j.disc.2020.112118.

[17] R. Flórez and J. L. Ramírez, Enumerations of rational non-decreasing Dyck paths with integer slope, *Graphs and Combinatorics* (2021), doi:10.1007/s00373-021-02392-9.

[18] T.-X. He and R. Sprugnoli, Sequence characterization of Riordan arrays, *Discrete Math.* **309** (2009), 3962–3974, doi:10.1016/j.disc.2008.11.021.

[19] D. Merlini, D. G. Rogers, R. Sprugnoli and M. C. Verri, On some alternative characterizations of Riordan arrays, *Canad. J. Math.* **49** (1997), 301–320, doi:10.4153/cjm-1997-015-x.

[20] H. Prodinger, Words, Dyck paths, trees, and bijections, in: *Words, semigroups, & transductions*, World Sci. Publ., River Edge, NJ, pp. 369–379, 2001, doi:10.1142/9789812810908_0028.

[21] D. G. Rogers, Pascal triangles, Catalan numbers and renewal arrays, *Discrete Math.* **22** (1978), 301–310, doi:10.1016/0012-365x(78)90063-8.

[22] L. W. Shapiro, S. Getu, W. Woan and L. Woodson, The Riordan group, *Discrete Appl. Math.* **34** (1991), 229–239, doi:10.1016/0166-218x(91)90088-e.

[23] N. J. A. Sloane, The on-line encyclopedia of integer sequences, `http://oeis.org/`.

[24] R. P. Stanley, Hipparchus, Plutarch, Schröder, and Hough, *Amer. Math. Monthly* **104** (1997), 344–350, doi:10.1080/00029890.1997.11990645.

A Appendix. Notation tables

	type of peaks			
	symmetric	asymmetric	weakly symmetric	all
number of such peaks in P	$\sigma(P)$	$\overline{\sigma}(P)$	$\tilde{\sigma}(P)$	$\tau(P)$
total number over $\mathcal{D}_n$	s_n	$\overline{s}_n$	$\tilde{s}_n$	t_n
vector of peak weights of P	$\boldsymbol{\omega}(P) = (\omega_1(P), \dots)$			
sum of peak weights of P	$\omega(P)$		$\tilde{\omega}(P)$	
total sum of weights over $\mathcal{D}_n$	w_n		$\tilde{w}_n$	
total sum of heights over $\mathcal{D}_n$	h_n			

Table 1: Summary of notation for peak statistics.

Notation	Page	Notation	Page	Notation	Page
$\mathcal{D}_n, \mathcal{D}$	220	$\iota(P), \nu(P)$	222	$r_{n,k}$	234
$\mathcal{A}_n, \mathcal{B}_n, \mathcal{C}_{n,i}$	221	$S(x)$	223	$q_{n,k}$	239

Table 2: Other notation, along with the page where it is first introduced.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.05 / 243–257
https://doi.org/10.26493/1855-3974.2351.07b
(Also available at http://amc-journal.eu)

Density results for Graovac-Pisanski's distance number

Lowell Abrams

University Writing Program and Department of Mathematics, The George Washington University, Washington, DC 20052, USA

Lindsey-Kay Lauderdale *

Department of Mathematics, Towson University, Towson, MD 21252, USA

Received 2 June 2020, accepted 13 May 2021, published online 30 October 2021

Abstract

The sum of distances between every pair of vertices in a graph G is called the *Wiener index* of G. This graph invariant was initially utilized to predict certain physico-chemical properties of organic compounds. However, the Wiener index of G does not account for any of its symmetries, which are also known to effect these physico-chemical properties. Graovac and Pisanski modified the Wiener index of G to measure the average distance each vertex is displaced under the elements of the symmetry group of G; we call this the *Graovac-Pisanski (GP) distance number* of G. In this article, we prove that the set of all GP distance numbers of graphs with isomorphic symmetry groups is dense in a half-line. Moreover, for each finite group Γ and each rational number q within this half-line, we present a construction for a graph whose GP distance number is q and whose symmetry group is isomorphic to Γ. This construction results in graphs whose vertex orbits are not connected; we also consider an analogous construction which ensures that all vertex orbits are connected.

Keywords: Wiener index, distance number, Graovac-Pisanski index, graph automorphism group, chemical graph theory.

Math. Subj. Class. (2020): 05C12, 05C25, 05C35, 05C92

*Corresponding author. The author is the Jess and Mildred Fisher Endowed Professor of Mathematics in the Fisher College of Science and Mathematics at Towson University and is partially supported by this endowment.

E-mail addresses: labrams@gwu.edu (Lowell Abrams), llauderdale@towson.edu (Lindsey-Kay Lauderdale)

1 Introduction

Throughout this article, all graphs considered are simple and finite, and all groups considered are finite. We let $V(G)$ and $E(G)$ denote the vertex set and edge set of a graph G, respectively. The *Wiener index* of G is the sum of all distances between pairs of vertices in G, namely

$$W(G) := \frac{1}{2}\sum_{u\in V(G)}\sum_{v\in V(G)} d(u,v),$$

where $d(u,v)$ is the length of a shortest path between u and v in G. This graph invariant was original defined by Wiener [14], where he considered graphical representations of molecules. In particular, each vertex in $V(G)$ represents an atom of a molecule and each edge in $E(G)$ represents a bond between atoms. Wiener [14] used this graph invariant to establish an equation that predicts the boiling points of paraffin molecules.

Other physico-chemical properties of organic molecules, including refractive index, heat of isomerization, heat of vaporization, density, surface tension, viscosity, and chromatographic retention time, were later linked to the Wiener index [5]. Consequently, the Wiener index of classes of compounds, including benzenoids [6], chains [13], and trees [2], were calculated; Mohar and Pisanski [11] described numerous algorithms that compute the Wiener index of a graph in general. An interested reader can see [10] and the references within for more results on this graph invariant.

The symmetries of molecules are known to effect certain physico-chemical properties of organic compounds [12]. In this article, we are interested in a modification of $W(G)$ that accounts for these symmetries of G. Recall the set of adjacency-preserving permutations of $V(G)$ is called the *automorphism group* of G and is denoted by $\operatorname{Aut} G$. Graovac and Pisanski [4] defined the *distance number* of G to be the average

$$\delta(G) := \frac{1}{|\operatorname{Aut} G||V(G)|}\sum_{u\in V(G)}\sum_{\sigma\in\operatorname{Aut} G} d\big(u,\sigma(u)\big).$$

We call this invariant the *Graovac and Pisanski (GP) distance number*. Graovac and Pisanski [4] established some basic properties of $\delta(G)$ and computed $\delta(G)$ provided G is a path, cube, cycle graph, complete bipartite graph, or lattice graph. Note that the results in this article only hold for the GP distance number and not what is currently referred to in the literature as the Graovac-Pisanski index, namely $\hat{W}(G) := \frac{1}{2}|V(G)|^2\delta(G)$.

The GP distance number and the GP index were the subject of prior research by a number of authors. For example, Ashrafi and Shabani [1] computed the GP index of graphs that resulted via standard graph operations on trees. The GP index of truncation graphs, Thorn graphs, and caterpillars were calculated by Iranmanesh and Shabani [7]. Additionally, Knor et al. [8] considered the maximum GP index among all graphs of a fixed order. Note that these results on the GP index have direct implications for the GP distance number.

In this article, we consider a dual problem to that of computing the maximum GP distance number among all graphs of a fixed order; this approach better represents how the GP distance numbers of classes of compounds can predict their physico-chemical properties. Specifically, for a given group Γ, we establish the possible values of $\delta(G)$ among all graphs G with $\operatorname{Aut} G \cong \Gamma$. When $\operatorname{Aut} G \cong \Gamma$, we call G a *Γ-graph*. Our main result is stated below.

Theorem 1.1. *Given a group* Γ*, define*

$$D_\Gamma := \{\delta(G) : G \text{ is a } \Gamma\text{-graph}\}.$$

The set D_Γ *is dense in* $(\inf(D_\Gamma), \infty)$*. Moreover, for each rational number* $q \in (\inf(D_\Gamma), \infty)$*, there exists a* Γ*-graph* G *with* $\delta(G) = q$*.*

Our results will establish the exact value of $\inf(D_\Gamma)$, as well as give two infinite families of Γ-graphs whose GP distance numbers equal this infimum.

We prove Theorem 1.1 by constructing a family of Γ-graphs whose vertex orbits under the Γ-action are not necessarily connected. Consideration of Γ-graphs whose vertex orbits are all connected yields a more restricted result, Theorem 6.3, in which the interval of potential GP distance numbers is finite and, moreover, not every rational number in the interval can be obtained as a GP distance number of a graph in the constructed family.

This article is organized as follows. In Section 2, we describe an alternative formula to compute $\delta(G)$ for a given graph G, and then use it to state bounds on this invariant in terms of $W(G)$. Next, for a given group Γ, we construct an infinite family of Γ-graphs in Section 3. The results of Section 4 establish their associated GP distance numbers, and in Section 5, we present a proof of our main result, Theorem 1.1. Finally, we conclude in Section 6 with a discussion leading to Theorem 6.3.

2 Preliminaries

The definition of $\delta(G)$ for a graph G can be reformulated by considering the orbits of $V(G)$ under the action of $\operatorname{Aut} G$. For ease of notation, define

$$d(v, V) := \sum_{u \in V} d(v, u),$$

where $v \in V \subseteq V(G)$. Graovac and Pisanski connected this alternative expression for $\delta(G)$ to the Wiener index of the vertex orbits of G; we state their results below.

Theorem 2.1 (Graovac and Pisanski [4])**.** *If* $V_0, V_1, \ldots, V_{p-1}$ *are the orbits of* $V(G)$ *determined by* $\operatorname{Aut} G$ *and* $v_i \in V_i$ *for each* $i \in \{0, 1, \ldots, p-1\}$*, then*

$$\delta(G) = \frac{1}{|V(G)|} \sum_{i=0}^{p-1} d(v_i, V_i) = \frac{2}{|V(G)|} \sum_{i=0}^{p-1} \frac{W(V_i)}{|V_i|}. \tag{2.1}$$

For the remainder of this article, we will use Equation (2.1) to compute the GP distance number of a given graph. As simple examples, we calculate the GP distance numbers of both complete graphs and paths below.

Example 2.2. Let K_n denote the complete graph with n vertices. If $v \in V(K_n)$, then

$$\delta(K_n) = \frac{1}{n} d\big(v, V(K_n)\big) = \frac{n-1}{n},$$

where the first equality holds because K_n is vertex-transitive (i.e., $p = 1$) and the second equality holds because v is adjacent to all vertices in $V(K_n)$ except itself.

Example 2.3. Let P_n denote the path of order $n \geq 2$, and label this graph so that $u_i u_{i+1} \in E(P_n)$ for each $i \in \{0, 1, \dots, n-2\}$. Since P_n is a $\mathbb{Z}_2$-graph, there are $\lfloor \frac{n+1}{2} \rfloor$ vertex orbits under the action of $\mathrm{Aut}(P_n)$. Set $p = \lfloor \frac{n+1}{2} \rfloor$ and label these orbits by $V_0, V_1, \dots, V_{p-1}$ so that $u_i \in V_i$ for each $i \in \{0, 1, \dots, p-1\}$. Under these assumptions, u_i and u_{n-1-i} comprise the orbit V_i and

$$d(u_i, V_i) = d(u_i, u_i) + d(u_i, u_{n-1-i}) = 0 + (n - 1 - 2i) = n - 1 - 2i$$

for all $i \in \{0, 1, \dots, p-1\}$. Therefore,

$$\delta(P_n) = \frac{1}{n}\sum_{i=0}^{p-1} \underbrace{(n-1-2i)}_{d(u_i,V_i)} = \frac{1}{n}\left[p(n-1) - 2\left(\frac{1}{2}(p-1)p\right)\right] = \begin{cases} \frac{n}{4} & \text{if } n \text{ is even} \\ \frac{n^2-1}{4n} & \text{if } n \text{ is odd,} \end{cases}$$

where the first equality holds by Equation (2.1) and the last equality holds because $p = \lfloor \frac{n+1}{2} \rfloor$.

Paths and complete graphs represent important families of graphs in the context of the Wiener index. In particular, Knor, Škrekovski, and Tepeh [9] observed that if G is a connected graph of order n, then

$$\binom{n}{2} = W(K_n) \leq W(G) \leq W(P_n) = \binom{n+1}{3}. \tag{2.2}$$

For a given graph G, this observation allows us to place simple bounds on $\delta(G)$ in terms of $W(G)$.

Lemma 2.4. *Let G be a graph. If the induced subgraph on each vertex orbit of G under the action of* $\mathrm{Aut}\, G$ *is connected with order k, then*

$$\frac{k-1}{k} \leq \delta(G) \leq \frac{k^2-1}{3k}.$$

Proof. Let $V_0, V_1, \dots, V_{p-1}$ denote the vertex orbits of G under the action of $\mathrm{Aut}\, G$. Because each orbit has size k and $|V(G)| = kp$, Equation (2.1) implies

$$\delta(G) = \frac{2}{k^2 p}\sum_{i=0}^{p-1} W(V_i).$$

Combining the equation above with Equation (2.2), we obtain

$$\frac{k-1}{k} = \frac{2}{k^2 p} \cdot p\binom{k}{2} \leq \delta(G) \leq \frac{2}{k^2 p} \cdot p\binom{k+1}{3} = \frac{k^2-1}{3k},$$

as desired. □

The lower bound stated in Lemma 2.4 is realized by $G = K_n$ (see Example 2.2). As demonstrated by Example 2.3, the upper bound in Lemma 2.4 is not realized by $G = P_n$. Moreover, we conjecture this upper bound is not sharp under the stated assumptions.

For a given group Γ, Theorem 1.1 implies that there is no maximum value of $\delta(G)$ among all Γ-graphs. In fact, the values of GP distance numbers of graphs in general are not bounded; Lemma 2.4 foreshadows how these graphs must be built. To construct a family of graphs with arbitrarily large GP distance numbers, the induced subgraphs on some of the vertex orbits must be disconnected. We continue by constructing such graphs in the next section.

3 Graph construction

To investigate the set D_Γ, we will construct an infinite family of Γ-graphs, parameterized by non-negative integers a and c, from a given Γ-graph G. Specifically, each graph $\varphi_c^a(G)$ in this family will be constructed by appending to G, in a special way, a anti-cliques of order $|V(G)|$ and c cliques of order $|V(G)|$ (see Definition 3.1 below). Every vertex in $\varphi_c^a(G)$ will have two labels; the superscript of a vertex indicates its distance to G and the subscript label represents the vertex in G it is closest to. The parameters a and c are used in Section 5 to increase and decrease the value of $\delta\big(\varphi_c^a(G)\big)$, respectively.

Definition 3.1. Let Γ be a group, and suppose G is a Γ-graph with $V(G) = \{u_0^0, u_1^0, \ldots, u_{n-1}^0\}$. Given $a, c \in \mathbb{N}$, construct a new graph from G, denoted $\varphi_c^a(G)$, with $n(1+a+c)$ vertices and

$$E(G) + an + c\left(n + \frac{1}{2}n(n-1)\right)$$

edges as follows:

1. For each $i \in \{0, 1, \ldots, n-1\}$, attach a path of length a to vertex u_i^0 and sequentially label the vertices on that path by $u_i^0, u_i^1, u_i^2, \ldots, u_i^a$.
2. For each $i \in \{0, 1, \ldots, n-1\}$, attach a path of length c to u_i^0 and sequentially label the vertices $w_i^0, w_i^1, w_i^2, \ldots, w_i^c$, where $w_i^0 := u_i^0$; thereupon, provided $c \neq 0$, include the edges $w_i^k w_j^k$ for all $k \in \{1, 2, \ldots, c\}$ and distinct $i, j \in \{0, 1, \ldots, n-1\}$.

Observe that G and $\varphi_c^a(G)$ are equal when $a = 0 = c$. The graph $\varphi_0^a(C_n)$ is depicted in Figure 1, where C_n denotes the cycle graph of order n. We discuss the structure of the vertex orbits of $\varphi_c^a(G)$ under the action of $\mathrm{Aut}\left(\varphi_c^a(G)\right)$ in the following remark.

Remark 3.2. Let Γ be a group. If G and $\varphi_c^a(G)$ are both Γ-graphs, then the vertex orbits of $\varphi_c^a(G)$ under its Γ-action depend on the vertex orbits of G under its Γ-action. In particular, let $V_0, V_1, \ldots, V_{p-1}$ denote the vertex orbits of G under its Γ-action. By construction, we obtain $a + c$ vertex orbits of $\varphi_c^a(G)$ under its Γ-action for each V_i, so, in total, $\varphi_c^a(G)$ has $(1 + a + c)p$ vertex orbits under its Γ-action.

We continue with an example in which we compute the value of $\delta\big(\varphi_0^a(C_n)\big)$ for all $a, n \in \mathbb{N}$ with $n \geq 3$.

Example 3.3. Let us compute the GP distance number of the graph $\varphi_0^a(C_n)$, which is illustrated in Figure 1. Recall that C_n is vertex-transitive. If A^j is the orbit of u_0^j under the dihedral action of $\mathrm{Aut}\big(\varphi_0^a(C_n)\big) \cong D_{2n}$ for all $j \in \{0, 1, \ldots, a\}$, then $A^0, A^1, \ldots, A^a$ form a partition of $V\left(\varphi_0^a(C_n)\right)$. We claim the value of $d(u_0^j, A^j)$ depends on the parity of n.

Consider the vertices $u_0^j, u_i^j \in A^j$, where $i \in \{1, 2, \ldots, n-1\}$ and $j \in \{0, 1, \ldots, a\}$. A shortest path between these vertices is constructed by concatenating the u_0^j, u_0^0-path of length j, a u_0^0, u_i^0-path of minimum length in C_n, and the u_i^0, u_i^j-path of length j. Therefore, if $n = 2\ell + 1$ is odd, then

$$d(u_0^j, A^j) = \sum_{i=1}^{n-1} d(u_0^j, u_i^j) = 2\sum_{k=1}^{\ell}(2j + k) = 4j\ell + \ell(\ell + 1) = 2(n-1)j + \frac{n^2 - 1}{4},$$

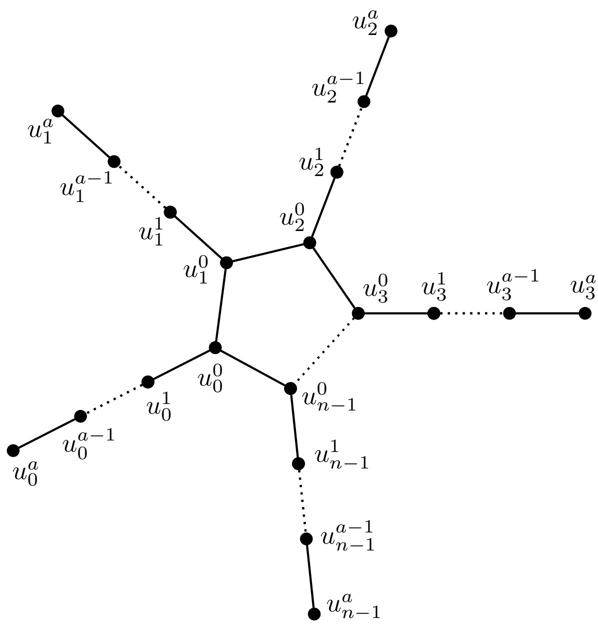


Figure 1: Depiction of the graph $\varphi_0^a(C_n)$.

and, if $n = 2\ell$ is even, then

$$d(u_0^j, A^j) = \sum_{i=1}^{n-1} d(u_0^j, u_i^j) = (2j+\ell) + 2\sum_{k=1}^{\ell-1}(2j+k) = 4j\ell - 2j + \ell^2 = 2(n-1)j + \frac{n^2}{4}.$$

Since $|V(\varphi_0^a(C_n))| = n(1+a)$, we have that

$$\delta(\varphi_0^a(C_n)) = \frac{1}{n(1+a)} \sum_{j=0}^{a} d(u_0^j, A^j) = \begin{cases} \dfrac{4(n-1)a + n^2 - 1}{4n} & \text{if } n = 2\ell+1 \\ \dfrac{4(n-1)a + n^2}{4n} & \text{if } n = 2\ell. \end{cases}$$

The statements in Remark 3.2 are based on the assumption that G and $\varphi_c^a(G)$ have isomorphic automorphism groups. The following proposition proves that this is almost always the case.

Proposition 3.4. *Let Γ be a group. If G is a nontrivial connected Γ-graph and either $a \neq 0$ or G is not a complete graph, then $\varphi_c^a(G)$ is also a Γ-graph.*

Proof. To prove that Γ is isomorphic to a subgroup of $\operatorname{Aut}(\varphi_c^a(G))$, we note that each element of $\operatorname{Aut} G$ induces a (subscript) label-preserving automorphism of $\varphi_c^a(G)$. In particular, if $\sigma \in \operatorname{Aut} G$, then σ induces a permutation on $\{0, 1, \ldots, n-1\}$, denoted ρ_σ, such that $\rho_\sigma(i)$ is the subscript of $\sigma(u_i^0)$ for all $i \in \{0, 1, \ldots, n-1\}$. Define the map $\pi_\sigma : V(\varphi_c^a(G)) \to V(\varphi_c^a(G))$ by $\pi_\sigma(u_i^j) = u_{\rho_\sigma(i)}^j$ and $\pi_\sigma(w_i^k) = w_{\rho_\sigma(i)}^k$ for all $j \in \{0, 1, \ldots, a\}$ and $k \in \{0, 1, \ldots, c\}$. Since π_σ preserves the adjacency relations in $\varphi_c^a(G)$ and $\Gamma \cong \{\pi_\sigma : \sigma \in \operatorname{Aut} G\}$, Γ is isomorphic to a subgroup of $\operatorname{Aut}(\varphi_c^a(G))$.

It remains to prove that any element of $\operatorname{Aut}\big(\varphi_c^a(G)\big)$ is equal to π_σ for some $\sigma \in \operatorname{Aut} G$. Clearly if $a = 0 = c$, then $\varphi_c^a(G) = G$ and the proposition holds. Thus, in what follows we assume that at least one of a or c is nonzero.

Suppose $a \neq 0$, and consider the image of the degree-1 vertex u_i^a under $\psi \in \operatorname{Aut}\big(\varphi_c^a(G)\big)$, where $i \in \{0, 1, \ldots, n-1\}$. Since the only vertices in $\varphi_c^a(G)$ that have degree 1 are of the form u_ℓ^a, it follows that $\psi(u_i^a) = u_\ell^a$ for some $\ell \in \{0, 1, \ldots, n-1\}$. In turn, $\psi\big(u_i^{a-1}\big) = u_\ell^{a-1}$ because u_i^{a-1} and u_ℓ^{a-1} are the only neighbors of u_i^a and u_ℓ^a in $\varphi_c^a(G)$, respectively. Proceeding by induction, assume that $\psi\big(u_i^{j'}\big) = u_\ell^{j'}$ for all $j' \in \{j, j+1, \ldots, a\}$. If $j \geq 1$, then u_i^j has exactly two neighbors, namely u_i^{j+1} and u_i^{j-1}, while u_ℓ^{j+1} and u_ℓ^{j-1} are the only neighbors of vertex u_ℓ^j. In this case, $\psi\big(u_i^{j-1}\big) = u_\ell^{j-1}$ as $\psi\big(u_i^{j+1}\big) = u_\ell^{j+1}$ by induction. Therefore, $\psi\big(u_i^j\big) = u_\ell^j$ for all $j \in \{0, 1, \ldots, a\}$.

Now define $W^k := \{w_0^k, w_1^k, \ldots, w_{n-1}^k\}$ for each $k \in \{0, 1, \ldots, c\}$. If $c \neq 0$, then each vertex in W^c has degree n, and thus $\psi(w_i^c)$ is also a vertex of degree n in $\varphi_c^a(G)$. The only vertices in $\varphi_c^a(G)$ that have degree n are in $W^0 \cup W^c$. However, each element in W^c is adjacent to at least $n-1$ vertices of degree n, and because G is not a complete graph or $a \neq 0$, each vertex in $W^0 = V(G)$ is adjacent to at most $n-2$ vertices of degree n. Consequently, W^c is ψ-invariant; assume that $\psi(w_i^c) = w_m^c$ for some $m \in \{0, 1, \ldots, n-1\}$. Both w_i^c and w_m^c have exactly one neighbor that is not an element of W^c; hence, $\psi\big(w_i^{c-1}\big) = w_m^{c-1}$ and we claim that $\psi\big(w_i^k\big) = w_m^k$ for all $k \in \{0, 1, \ldots, c\}$. Since this claim holds for $k \in \{c-1, c\}$, we again proceed by induction. Assume that $\psi\big(w_i^{k'}\big) = w_m^{k'}$ for all $k' \in \{k, k+1, \ldots, c\}$. When $k \geq 1$, the only neighbors of w_i^k not in W^k are w_i^{k+1} and w_i^{k-1}; moreover, w_m^{k+1} and w_m^{k-1} are the only neighbors of w_m^k not in W^k. Since $\psi\big(w_i^{k+1}\big) = w_m^{k+1}$ by induction, it follows that $\psi\big(w_i^{k-1}\big) = w_m^{k-1}$ and the claim holds.

Our work above proves that $\psi\big(u_i^j\big) = u_\ell^j$ for all $j \in \{0, 1, \ldots, a\}$ and that $\psi\big(w_i^k\big) = w_m^k$ for all $k \in \{0, 1, \ldots, c\}$. Since $u_i^0 = w_i^0$ by definition of $\varphi_c^a(G)$, we have $\ell = m$. Consequently, there exists $\sigma \in \operatorname{Aut}(G)$ such that $\psi = \pi_\sigma$, and $\varphi_c^a(G)$ is also a Γ-graph. □

We are now ready to compute the GP distance number of $\varphi_c^a(G)$ when the graphs G and $\varphi_c^a(G)$ have isomorphic automorphism groups.

4 GP distance number of $\varphi_c^a(G)$

If G and $\varphi_c^a(G)$ have isomorphic automorphism groups, then the value of $\delta\big(\varphi_c^a(G)\big)$ naturally depends on the value $\delta(G)$; however, it also depends on the value of c in a special way. In particular, if $c \neq 0$, then the distance between any two vertices of G is at most 3. Recalling that $V_0, V_1, \ldots, V_{p-1}$ are the vertex orbits of G under the action of $\operatorname{Aut} G$, we define

$$\delta'(c, G) := \begin{cases} \delta(G) & \text{if } c = 0 \\ \delta_3(G) & \text{if } c \neq 0, \end{cases}$$

where

$$\delta_3(G) := \frac{1}{|V(G)|} \sum_{i=0}^{p-1} d_3(u_i, V_i) \quad \text{and} \quad d_3(u_i, V_i) := \sum_{u \in V_i} \min\{d(u_i, u), 3\}.$$

With this notation in hand, we compute the value of $\delta\big(\varphi_c^a(G)\big)$ below.

Proposition 4.1. *Let Γ be a group, and assume that G and $\varphi_c^a(G)$ are both Γ-graphs. If G has order n and p vertex orbits under the action of $\operatorname{Aut} G$, then*

$$\delta\big(\varphi_c^a(G)\big) = \frac{(n-p)(a^2+a+c)+n(a+1)\delta'(c,G)}{n(1+a+c)}.$$

Proof. Let $V_0, V_1, \ldots, V_{p-1}$ denote the p vertex orbits of G under the action of $\operatorname{Aut} G$. After a possible relabelling of $V(G)$, assume that $u_i^0 \in V_i$ for all $i \in \{0, 1, \ldots, p-1\}$. For each V_i, there are $a+c$ associated vertex orbits of $\varphi_c^a(G)$ under the action of $\operatorname{Aut}\big(\varphi_c^a(G)\big)$ by Remark 3.2; label these orbits by $A_i^1, A_i^2, \ldots, A_i^a$ and $C_i^1, C_i^2, \ldots, C_i^c$, where $u_i^j \in A_i^j$ for $j \in \{1, 2, \ldots, a\}$ and $w_i^k \in C_i^k$ for $k \in \{1, 2, \ldots, c\}$. Under these assumptions

$$\delta\big(\varphi_c^a(G)\big) = \frac{1}{\big|V\big(\varphi_c^a(G)\big)\big|}\left(\sum_{j=0}^{a}\sum_{i=0}^{p-1} d(u_i^j, A_i^j) + \sum_{k=1}^{c}\sum_{i=0}^{p-1} d(w_i^k, C_i^k)\right), \tag{4.1}$$

where $A_i^0 = V_i$ for $i \in \{0, 1, \ldots, p-1\}$. We evaluate each of these sums in one of the following cases.

First, observe that $d(w_i^k, C_i^k) = |C_i^k| - 1$ for all $k \in \{1, 2, \ldots, c\}$ as the induced subgraph on C_i^k is a clique. Since

$$\sum_{k=1}^{c} |C_i^k| = c|V_i| \quad \text{and} \quad \sum_{i=0}^{p-1} |V_i| = |V(G)| = n,$$

it follows that

$$\sum_{k=1}^{c}\sum_{i=0}^{p-1} d(w_i^k, C_i^k) = \sum_{i=0}^{p-1}\sum_{k=1}^{c}(|C_i^k| - 1) = \sum_{i=0}^{p-1} c(|V_i| - 1) = c(n-p). \tag{4.2}$$

For the second case, if $u_\ell^0 \in A_i^0$, then a shortest path between vertices $u_i^j \in A_i^j$ and $u_\ell^j \in A_i^j$ is constructed by concatenating the following three paths:

1. the u_i^j, u_i^0-path in $\varphi_c^a(G)$ of length j;
2. a u_i^0, u_ℓ^0-path of minimum length in G if $c = 0$ or in $\varphi_1^0(G)$ provided $c \neq 0$; and
3. the u_ℓ^0, u_ℓ^j-path in $\varphi_c^a(G)$ of length j.

It follows that

$$d(u_i^j, A_i^j) = 2j(|A_i^j| - 1) + d'(c, u_i^0, A_i^0),$$

where

$$d'(c, u_i^0, A_i^0) := \begin{cases} d(u_i^0, A_i^0) & \text{if } c = 0 \\ d_3(u_i^0, A_i^0) & \text{if } c \neq 0. \end{cases}$$

Since $|A_i^j| = |V_i|$ for all $j \in \{0, 1, \ldots, a\}$, we have

$$\begin{aligned} \sum_{j=0}^{a}\sum_{i=0}^{p-1} d(u_i^j, A_i^j) &= \sum_{i=0}^{p-1}\sum_{j=0}^{a}\big(\underbrace{2j(|A_i^j| - 1) + d'(c, u_i^0, A_i^0)}_{d(u_i^j, A_i^j)}\big) \\ &= \sum_{i=0}^{p-1}\left(2\frac{1}{2}a(a+1)(|V_i| - 1) + (a+1)d'(c, u_i^0, A_i^0)\right) \\ &= a(a+1)(n-p) + n(a+1)\delta'(c, G). \end{aligned} \tag{4.3}$$

Since $\left|V\left(\varphi_c^a(G)\right)\right| = n(1+a+c)$, combining Equations (4.2) and (4.3) with Equation (4.1) yields

$$\delta\big(\varphi_c^a(G)\big) = \frac{(n-p)(a^2+a+c)+n(a+1)\delta'(c,G)}{n(1+a+c)},$$

as desired. $\square$

Consider the value of $\delta\big(\varphi_c^a(G)\big)$ given in Proposition 4.1 for a fixed graph G. The parameters a and c can be used to increase and decrease the value of $\delta\big(\varphi_c^a(G)\big)$, respectively; that is,

$$\lim_{a\to\infty} \delta\big(\varphi_c^a(G)\big) = \infty \quad \text{and} \quad \lim_{c\to\infty} \delta\big(\varphi_c^a(G)\big) = \frac{n-p}{n},$$

provided c and a are fixed, respectively. There are several infinite families of order-n graphs whose GP distance numbers are equal to $\frac{n-p}{n}$, where p is the number of vertex orbits under the action of their respective automorphism groups. These families arise when the induced subgraph on every vertex orbit is a clique; Example 2.2 demonstrates that the complete graphs K_n comprise one such family. The following example establishes a second such family of graphs that, in contrast, are not vertex-transitive under the action of their respective automorphism groups.

Example 4.2. Let $\mathbb{Z}_k$ denote the cyclic group of order k, where $k \geq 3$. In this example, we construct an infinite family of $\mathbb{Z}_k$-graphs, denoted by G_n; each graph G_n has order $n = 6k$ and $p = 6$ edge orbits under the action of $\operatorname{Aut}(G_n)$. We will prove that $\delta(G_n) = \frac{n-p}{n}$.

Define the order-7 gadget graph H with edge set

$$E(H) = \big\{h_0h_1, h_1h_2, h_1h_4, h_2h_3, h_2h_5, h_5h_6\big\},$$

which is depicted in Figure 2(A). Let C_k denote the cycle graph of order k, and label its edges so that $v_iv_{i+1} \in E(C_k)$ for all $i \in \{0,1,\ldots,k-2\}$. Replace each edge in C_k with a copy of H, where the vertices v_i and v_{i+1} are identified with h_0 and h_3, respectively; we call the resulting graph $H(k)$. The graph $H(4)$ is illustrated in Figure 2(B). Observe that $H(k)$ is a $\mathbb{Z}_k$-graph with order $n = 6k$, which has six size-k vertex orbits under the action of $\operatorname{Aut}\big(H(k)\big)$.

Finally, we construct the graph G_n by including the $3(k-1)k$ edges necessary to turn each vertex orbit of $H(k)$ into a clique. By design G_n is also a $\mathbb{Z}_k$-graph, where each of its six edge orbits under the action of $\operatorname{Aut}(G_n)$ is a clique of order k. Its GP distance number is

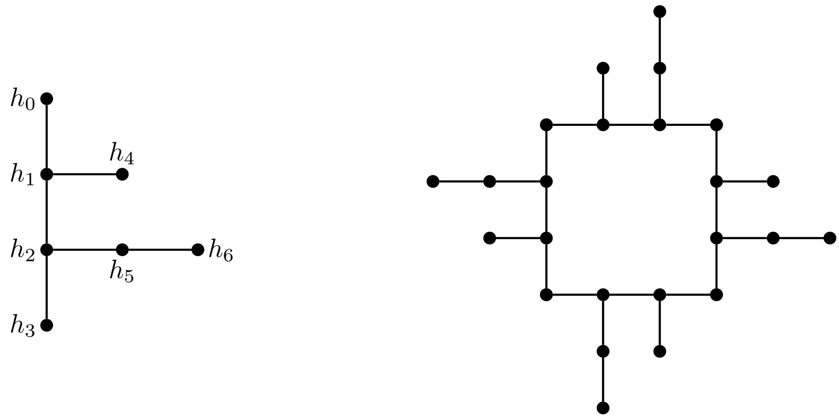
$$\delta(G_n) = \frac{n-6}{n} = \frac{k-1}{k},$$

as desired.

5 Proof of Theorem 1.1

In this section, we will prove our main result, Theorem 1.1. To do so, we make use of the following proposition.

Proposition 5.1. *Let Γ be a group, and suppose G is a nontrivial connected Γ-graph with order n and p vertex orbits under the action of $\operatorname{Aut} G$. For any rational number $q \in (\frac{n-p}{n}, \infty)$, there exist $a, c \in \mathbb{N}$ such that $\delta\big(\varphi_c^a(G)\big) = q$.*



(a) The gadget graph H

(b) The $\mathbb{Z}_4$-graph $H(4)$

Figure 2: Depictions of the graphs H and $H(4)$, which were defined in Example 4.2.

Proof. Choose $r, s \in \mathbb{N}$ such that $q = \frac{r}{s}$, and define

$$b := 2\max\left\{1, \left\lceil \frac{nr - ns\delta_3(G)}{(n-p)s} \right\rceil\right\}.$$

Let

$$a := \big(nr - (n-p)s\big)b - 1, \tag{5.1}$$

and notice that $a \geq 0$ because $\frac{n-p}{n} < q = \frac{r}{s}$. Now define

$$c := -\big(nr - (n-p)as - ns\delta_3(G)\big)b. \tag{5.2}$$

Since G has order n, $n\delta_3(G)$ is an integer, and thus c is as well. In fact, $c \in \mathbb{N}$ because the inequality

$$a = \big(nr - (n-p)s\big)b - 1 \;\geq\; b - 1 \;\geq\; \frac{1}{2}b \;\geq\; \frac{nr - ns\delta_3(G)}{(n-p)s}$$

implies that

$$nr - (n-p)as - ns\delta_3(G)$$

is nonpositive. Consequently, our choices of a and c are valid when considering the graph $\varphi_c^a(G)$, and since $a \neq 0$, $\varphi_c^a(G)$ is also a Γ-graph by Proposition 3.4. Proposition 4.1 then implies that the GP distance number of $\varphi_c^a(G)$ is

$$\delta\big(\varphi_c^a(G)\big) = \frac{(n-p)(a^2 + a + c) + n(a+1)\delta'(c, G)}{n(1 + a + c)}.$$

A tedious algebraic computation shows that combining our choices of a and c $\big($stated in Equations (5.1) and (5.2)$\big)$ with the equation above yields $\delta\big(\varphi_c^a(G)\big) = \frac{r}{s}$, as desired. $\square$

The equation $\delta\big(\varphi_c^a(G)\big) = q$ that appears in Proposition 5.1 does not have a unique solution. In fact, taking any integer value of b greater than the one specified in the proof will also yield a choice of a and c which satisfies the theorem. We now provide an example showing that it is also possible to obtain smaller values of a and c which work.

Example 5.2. Let G be $K_4 - e$ for any edge e of K_4, in which case $\operatorname{Aut} G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\delta(G) = \frac{3}{4}$. Applying the proof of Proposition 5.1 with $q = \frac{4}{5}$, we obtain $b = 2$ and then $a = 11$ and $c = 218$. However, we can in fact take $b = 1$ and still obtain a solution to $\delta\big(\varphi_c^a(G)\big) = q$, namely $a = 5$ and $c = 49$. The solution with the smallest possible values of both a and c, not obtainable through the construction in that proof, is $a = 1$ and $c = 3$.

We conclude this section with a proof of our main result.

Proof of Theorem 1.1. Let the group Γ be given, and recall that

$$D_\Gamma := \{\delta(G) : G \text{ is a } \Gamma\text{-graph}\}.$$

Frucht [3] proved that there exists a graph whose automorphism group is isomorphic to Γ; among all such Γ-graphs G with order n_G and with p_G vertex orbits under the action of $\operatorname{Aut} G$, choose G so that $\frac{n_G - p_G}{n_G}$ is minimal. Under these assumptions, if G has order n and p vertex orbits under the action of $\operatorname{Aut} G$, then

$$\inf(D_\Gamma) = \frac{n-p}{n}.$$

For each rational number $q \in (\inf(D_\Gamma), \infty)$, there exists a Γ-graph with GP distance number equal to q by Proposition 5.1. Consequently, D_Γ is dense in $(\inf(D_\Gamma), \infty)$, as the rational numbers are dense in this interval. The result now follows. □

6 Graphs with connected vertex orbits

For a given group Γ, Theorem 1.1 proved that there was no maximum value of $\delta(G)$ among all Γ-graphs; such arbitrarily large values of $\delta(G)$ were obtained from graphs with disconnected induced subgraphs on the vertex orbits of G under the action of $\operatorname{Aut} G$. If we assume that the induced subgraph on every vertex orbit of G under the action of $\operatorname{Aut} G$ is connected, then we obtain a bounded interval of potential GP distance numbers. While these stricter assumptions preserve density, we no longer can produce a graph with a given GP distance number using a similar construction. We will conclude this article with a result analogous to that of Theorem 1.1 which makes the aforementioned connectedness assumption.

Let the group Γ be given. If a Γ-set V has size n, let $G_{\Gamma,n}$ denote any choice of a connected graph on the Γ-set V which has a Γ-action compatible with the Γ-action on V and has the maximum possible GP distance number among all such graphs. Note that $G_{\Gamma,n}$ need not be a Γ-graph. We use $\delta_\Gamma(G_{\Gamma,n})$ to denote the GP distance number obtained by considering the Γ-action on $G_{\Gamma,n}$ rather than the action of $\operatorname{Aut}(G_{\Gamma,n})$.

Suppose now that G is a Γ-graph with p orbits $V_0, V_1, \dots, V_{p-1}$ of sizes $n_0, n_1, \dots, n_{p-1}$, respectively. Each orbit itself has a Γ-action, so we consider the graphs $G_{\Gamma,n_0}, \dots, G_{\Gamma,n_{p-1}}$; let $\widehat{G}_\Gamma$ denote $G_{\Gamma,n_0} \sqcup \cdots \sqcup G_{\Gamma,n_{p-1}}$, where $\sqcup$ denotes disjoint union. Define

$$\hat{\delta}(G) := \frac{1}{n_0 + \cdots + n_{p-1}} \sum_{i=0}^{p-1} n_i \delta_\Gamma(G_{\Gamma,n_i});$$

$\hat{\delta}(G)$ is the maximum possible GP distance number relative to Γ for all graphs with a Γ-action and vertex set the Γ-set $V(G)$. Note, however, that $\operatorname{Aut}(\widehat{G}_\Gamma)$ may contain an isomorphic copy of Γ as a proper subgroup.

Definition 6.1. Let Γ be a group, and suppose G is a Γ-graph with vertices $u_0^0, u_1^0, \dots, u_{n-1}^0$ and vertex orbits $V_0, V_1, \dots, V_{p-1}$. Without loss of generality, we assume that $u_i^0 \in V_i$ for each $i \in \{0, 1, \dots, p-1\}$. We define a new graph $\hat{\varphi}_c^a(G)$ iteratively with respect to the natural numbers c and a as follows. Given $\hat{\varphi}_c^a(G)$, define $\hat{\varphi}_c^{a+1}(G)$ to be the graph obtained by carrying out the following steps:

1. introduce new vertices $u_0^{a+1}, u_1^{a+1}, \dots, u_{n-1}^{a+1}$; we refer to these vertices as being in "level $a+1$";
2. connect these new vertices with new edges $u_i^a u_i^{a+1}$ for each $i \in \{0, 1, \dots, n-1\}$; and
3. for each orbit V_i, add new edges to build a copy of the Γ-graph $G_{\Gamma,|V_i|}$ on the orbit of vertices in level $a+1$ corresponding to the Γ-set V_i.

Given $\hat{\varphi}_c^a(G)$, let $w_i^0 := u_i^0$ for each $i \in \{0, 1, \dots, n-1\}$. Define $\hat{\varphi}_{c+1}^a(G)$ by connecting an n-clique on new vertices w_i^{c+1} with new edges $w_i^c w_i^{c+1}$ for each $i \in \{0, 1, \dots, n-1\}$.

Note that, under the Γ-action, we have enhanced G with cp orbits whose induced subgraphs are cliques and with ap orbits whose induced subgraphs are disjoint unions of connected GP-distance-number-maximizing graphs.

Let G be a Γ-graph for a given group Γ. The following proposition shows that $\hat{\varphi}_c^a(G)$ is also a Γ-graph in most cases. We omit its proof, which is similar to the proof of Proposition 3.4.

Proposition 6.2. *Let Γ be a group, and suppose G is a nontrivial connected Γ-graph that is not complete. If either $c \neq 0$ or $G \ncong \widehat{G}_\Gamma$, then $\hat{\varphi}_c^a(G)$ is also a Γ-graph.*

We now present our result analogous to Theorem 1.1 that makes an assumption on the connectedness of graphs.

Theorem 6.3. *Let Γ be a group. If G is a connected Γ-graph of order n having p vertex orbits, each of which induces a connected subgraph of G, then*

$$\left\{\delta\big(\hat{\varphi}_c^a(G)\big) \mid a, c \in \mathbb{N} \text{ and } \hat{\varphi}_c^a(G) \text{ is a } \Gamma\text{-graph}\right\}$$

is dense in $\left(\frac{n-p}{n}, \hat{\delta}(G)\right)$.

Proof. Given any $\epsilon > 0$ and any $q \in \left(\frac{n-p}{n}, \hat{\delta}(G)\right)$, it suffices to find $a', c' \in \mathbb{N}$ such that $\left|q - \delta\left(\hat{\varphi}_{c'}^{a'}(G)\right)\right| < \epsilon$. We first determine an expression for $\delta\left(\hat{\varphi}_c^a(G)\right)$, and then explain how to choose a' and c'.

Let $V_0, V_1, \dots, V_{p-1}$ be the Γ-orbits in $V(G)$. For each V_i, there are $a+c$ associated vertex orbits of $\hat{\varphi}_c^a(G)$ under the action of $\mathrm{Aut}\big(\hat{\varphi}_c^a(G)\big)$; for $i \in \{0, 1, \dots, p-1\}$, label these orbits by $A_i^1, A_i^2, \dots, A_i^a$ and $C_i^1, C_i^2, \dots, C_i^c$, where $u_i^j \in A_i^j$ for $j \in \{1, 2, \dots, a\}$ and $w_i^k \in C_i^k$ for $k \in \{1, 2, \dots, c\}$. For $X \in \{G, \widehat{G}_\Gamma\}$, let d_X denote the distance function in X, and let $d_{X,3}$ denote the function given by $\min(d_X(u, v), 3)$ for vertices $u, v \in V(X)$. Write $d'_G = d_G$ for $c = 0$ and $d'_G = d_{G,3}$ for $c \geq 1$.

For each $i \in \{0, 1, \dots, p-1\}$ and any k, any two distinct vertices in C_i^k are at distance 1 from each other. Choosing a representative in each orbit $C_1^k, C_2^k, \dots, C_{p-1}^k$, we find that the total distance over all the orbits in level k is

$$\sum_{i=0}^{p-1}(|C_i^k| - 1) = n - p.$$

For $i \in \{0, 1, \ldots, p-1\}$ and any j, a shortest path between any two vertices u_ℓ^j, u_m^j in A_i^j is either a shortest path in layer j, or is a path obtained by concatenating a shortest u_ℓ^j, u_ℓ^0-path and a shortest u_m^0, u_m^j-path with a shortest u_ℓ^0, u_m^0-path in G if $c = 0$ and with a shortest u_ℓ^0, u_m^0-path in $\hat{\varphi}_1^0(G)$ if $c > 0$. Thus, the length of a shortest u_ℓ^j, u_m^j-path is

$$\min\left\{d_{\widehat{G}_\Gamma}\left(u_\ell^j, u_m^j\right), 2j + d'_G\left(u_\ell^0, u_m^0\right)\right\}.$$

Writing $\mathrm{diam}(X)$ for the length of a longest path in graph X, if $j \geq \mathrm{diam}(\widehat{G}_\Gamma)/2$ then we have

$$\min\left\{d_{\widehat{G}_\Gamma}\left(u_\ell^0, u_m^0\right), 2j + d'_G\left(u_\ell^0, u_m^0\right)\right\} = d_{\widehat{G}_\Gamma}\left(u_\ell^0, u_m^0\right).$$

Note that, to prove the result, it suffices to presume that $a > \mathrm{diam}(\widehat{G}_\Gamma)/2$. Choosing a representative in each orbit, we can calculate the total distance for levels 0 to $\lceil \mathrm{diam}(\widehat{G}_\Gamma)/2 \rceil$; write D for this value. Also, for each $j > \lceil \mathrm{diam}(\widehat{G}_\Gamma)/2 \rceil$, the total distance in level j is $n\hat{\delta}(G)$. Thus, we have

$$\delta\left(\hat{\varphi}_c^a(G)\right) = \frac{(n-p)c + D + \left(a - \lceil \mathrm{diam}(\widehat{G}_\Gamma)/2 \rceil\right) n\hat{\delta}(G)}{(1+a+c)n}.$$

In order to choose appropriate a and c, observe first that, for any positive $a, c \in \mathbb{N}$, we have

$$\begin{aligned}\delta\left(\hat{\varphi}_{c-1}^a(G)\right) - \delta\left(\hat{\varphi}_c^a(G)\right) &= \frac{D + \left(a - \lceil \mathrm{diam}(\widehat{G}_\Gamma)/2 \rceil\right) n\hat{\delta}(G) - (n-p)(a+1)}{(a+c)(1+a+c)n} \\ &< \frac{D + an\hat{\delta}(G)}{(a+c)^2 n}.\end{aligned}$$

Let $\Delta(a, c)$ denote this upper bound, and note that $\Delta(a, c)$ has negative derivative with respect to both a and to c.

We now choose a' and c'. Since

$$\lim_{a \to \infty} \delta(\hat{\varphi}_0^a(G)) = \hat{\delta}(G) > q,$$

we can choose $a' \in \mathbb{N}$ so that $a' > \lceil \mathrm{diam}(\widehat{G}_\Gamma)/2 \rceil$, $\Delta(a', 0) < \epsilon$, and $\delta\left(\hat{\varphi}_0^{a'}(G)\right) > q$. Because

$$\lim_{c \to \infty} \delta\left(\hat{\varphi}_c^{a'}(G)\right) = \frac{n-p}{n} < q$$

we can then choose

$$c' := \min\left\{c \in \mathbb{N} \,\middle|\, \delta\left(\hat{\varphi}_c^{a'}(G)\right) \leq q\right\}.$$

Observe that $c' > 0$ because we have chosen a' to ensure that $\delta\left(\hat{\varphi}_0^{a'}(G)\right) > q$. Since

$$\delta\left(\hat{\varphi}_{c'}^{a'}(G)\right) < q \leq \delta\left(\hat{\varphi}_{c'-1}^{a'}(G)\right),$$

we have

$$q - \delta\left(\hat{\varphi}_{c'}^{a'}(G)\right) < \Delta(a', c') < \Delta(a', 0) < \epsilon,$$

as desired. Furthermore, since $c' > 0$, Proposition 6.2 guarantees that $\hat{\varphi}_{c'}^{a'}(G)$ is a Γ-graph. $\square$

Let Γ be a group, and suppose G is a connected Γ-graph of order n with p vertex orbits under the action of $\operatorname{Aut} G$. If the induced subgraph on each vertex orbit of G is connected, then we claim that there exists infinitely many rational numbers in $\left(\frac{n-p}{n}, \hat{\delta}(G)\right)$ that are not the GP distance numbers of graphs of the form $\hat{\varphi}_c^a(G)$. We demonstrate our claim with the following example.

Example 6.4. Let G be the graph constructed from an 8-cycle on vertices $u_0^0, u_1^0, u_2^0, \ldots, u_7^0$ and a 4-cycle on vertices $u_8^0, u_9^0, u_{10}^0, u_{11}^0$, by including edges

$$u_0^0 u_8^0,\ u_1^0 u_8^0,\ u_2^0 u_9^0,\ u_3^0 u_9^0,\ u_4^0 u_{10}^0,\ u_5^0 u_{10}^0,\ u_6^0 u_{11}^0,\ \text{and } u_7^0 u_{11}^0.$$

The graph G, which is illustrated in Figure 3, is a D_8-graph with two vertex orbits under the action of $\operatorname{Aut} G$ (here D_8 denotes the dihedral group of order 8).

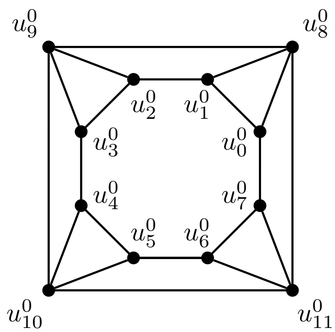


Figure 3: The D_8-graph G constructed in Example 6.4.

Observe that $\widehat{G}_{D_8}$ is equal to $C_8 \sqcup C_4$. Moreover, $\delta(G) = \frac{20}{12} = \hat{\delta}(G)$, and thus Theorem 6.3 established that $\left\{\delta\left(\hat{\varphi}_c^a(G)\right) \mid a, c \in \mathbb{N}\right\}$ is dense in the interval $\left(\frac{5}{6}, \frac{5}{3}\right)$. Observe that

$$\delta\left(\hat{\varphi}_c^a(G)\right) = \begin{cases} \dfrac{20}{12} & \text{if } c = 0 \\ \dfrac{19 + 20a + 10c}{12(1 + a + c)} & \text{if } c \neq 0, \end{cases}$$

and suppose $\delta\left(\hat{\varphi}_c^a(G)\right) = \frac{r}{s}$ for some $\frac{r}{s} \in \left(\frac{5}{6}, \frac{5}{3}\right)$. Solving for c in the case when $c > 0$ we obtain

$$c = \frac{(20s - 12r)a + 19s - 12r}{12r - 10s}.$$

Notice that if s is odd, then the numerator of this expression for c is odd whereas the denominator is even, and thus this value of c is not an integer. It follows that s is even, so no rational number in reduced form with an odd denominator is $\delta\left(\hat{\varphi}_c^a(G)\right)$ for any values of a and c. Finally, the reader may be entertained by the observation that both the set of GP distance numbers and non-GP distance numbers in $\left(\frac{5}{6}, \frac{5}{3}\right)$ are dense.

ORCID iDs

Lowell Abrams https://orcid.org/0000-0002-8174-5957

References

[1] A. R. Ashrafi and H. Shabani, The modified Wiener index of some graph operations, *Ars Math. Contemp.* **11** (2016), 277–284, doi:10.26493/1855-3974.801.968.

[2] D. Bonchev and N. Trinajstić, Information theory, distance matrix, and molecular branching, *J. Chem. Phys.* **67** (1977), 4517–4533, doi:10.1063/1.434593.

[3] R. Frucht, Herstellung von Graphen mit vorgegebener abstrakter Gruppe, *Compositio Math.* **6** (1939), 239–250, `http://www.numdam.org/item?id=CM_1939__6__239_0`.

[4] A. Graovac and T. Pisanski, On the Wiener index of a graph, *J. Math. Chem.* **8** (1991), 53–62, doi:10.1007/bf01166923, mathematical chemistry and computation (Dubrovnik, 1990).

[5] I. Gutman and T. Körtvélyesi, Wiener indices and molecular surfaces, *Z. Naturforsch.* **50** (1995), 669–671, doi:10.1515/zna-1995-0707.

[6] I. Gutman and O. E. Polansky, Wiener numbers of polyacenes and related benzenoid molecules, *Match* **20** (1986), 115–123, `https://match.pmf.kg.ac.rs/content20.htm`.

[7] M. A. Iranmanesh and H. Shabani, The symmetry-moderated Wiener index of truncation graph, Thorn graph and caterpillars, *Discrete Appl. Math.* **269** (2019), 41–51, doi:10.1016/j.dam.2018.05.040.

[8] M. Knor, J. Komorník, R. Škrekovski and A. Tepeh, Unicyclic graphs with the maximal value of Graovac-Pisanski index, *Ars Math. Contemp.* **17** (2019), 455–466, doi:10.26493/1855-3974.1925.57a.

[9] M. Knor, R. Škrekovski and A. Tepeh, Chemical graphs with the minimum value of Wiener index, *Match Commun. Math. Comput. Chem.* **81** (2019), 119–132, `https://match.pmf.kg.ac.rs/content81n1.htm`.

[10] M. Knor, R. Škrekovski and A. Tepeh, Mathematical aspects of Wiener index, *Ars Math. Contemp.* **11** (2016), 327–352, doi:10.26493/1855-3974.795.ebf.

[11] B. Mohar and T. Pisanski, How to compute the Wiener index of a graph, *J. Math. Chem.* **2** (1988), 267–277, doi:10.1007/bf01167206.

[12] R. Pinal, Effect of molecular symmetry on melting temperature and solubility, *Org. Biomol. Chem.* **2** (2004), 2692–2699, doi:10.1039/b407105k.

[13] H. Wiener, Correlation of heats of isomerization, and differences in heats of vaporization of isomers, among the paraffin hydrocarbons, *J. Am. Chem. Soc.* **69** (1947), 2636–2638, doi:10.1021/ja01203a022.

[14] H. Wiener, Structural determination of paraffin boiling points, *J. Am. Chem. Soc.* **69** (1947), 17–20, doi:doi.org/10.1021/ja01193a005.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.06 / 259–269
https://doi.org/10.26493/1855-3974.1926.6ad
(Also available at http://amc-journal.eu)

Decompositions of the automorphism groups of edge-colored graphs into the direct product of permutation groups

Mariusz Grech *

Wrocław University of Science and Technology,
Wybrzeże Wyspiańskiego Str. 27, Wrocław, Poland

Received 31 January 2019, accepted 1 June 2021, published online 11 October 2021

Abstract

In the paper *Graphical complexity of products of permutation groups*, M. Grech, A. Jeż, and A. Kisielewicz have proved that the direct product of automorphism groups of edge-colored graphs is itself the automorphism groups of an edge-colored graph. In this paper, we study the direct product of two permutation groups such that at least one of them fails to be the automorphism group of an edge-colored graph. We find necessary and sufficient conditions for the direct product to be the automorphism group of an edge-colored graph. The same problem is settled for the edge-colored digraphs.

Keywords: Colored graph, automorphism group, permutation group, direct product.

Math. Subj. Class. (2020): 05E18

1 Introduction

For permutation groups (A, V), (B, W), the *direct product* of A and B (with product action) is a permutation group $(A \times B, V \times W)$ with the action given by

$$(a, b)(x, y) = (a(x), b(y)).$$

The study of the direct product of automorphism groups of graphs was initiated by G. Sabidussi [19] in 1960. The problem was taken up in 1971 by M. Watkins [20]. In 1972, L. Nowitz and M. Watkins [21], and independently W. Imrich [13], have described the conditions under which the direct product of *regular* permutation groups that are automorphism groups of graphs is itself the automorphism group of a graph. This result was

*Supported in part by Polish NCN grant UMO-2016/21/B/ST1/03079.
E-mail address: mariusz.grech@pwr.edu.pl (Mariusz Grech)

a contribution to the description of all *regular* automorphism groups of graphs, which has been completed in 1978 by C. Godsil [5] for graphs, and in 1980 by L. Babai [1] for digraphs. The above results in [13, 21] have been extended to arbitrary permutation groups in [6], where the description of the conditions, under which the direct product of automorphism groups of graphs is itself an automorphism group of a graph, is given. In [8], the same is done for digraphs.

All the above results are motivated more or less directly by trying to make a contribution to the solution of the concrete version of König problem asking about a characterization of those permutation groups that are the automorphism groups of graphs (see [14]). There are a number of results (see e.g. [9, 10, 18] and [14]) showing that it is more natural and effective to study the automorphism groups of (edge-)colored graphs (rather than simple graphs), which is essentially the approach suggested by Wielandt [23].

In [14], A. Kisielewicz has introduced the notion of graphical complexity of permutation groups and suggested the study of constructions of permutation groups in this context. By $G(k)$, we denote the class of the automorphism groups of k-edge-colored graphs (those using at most k colors), and by GR, the union of all the classes $G(k)$, which in Wielandt's terminology [23] is the class of 2^*-closed groups. Similarly, by $DG(k)$ we denote the class of the automorphism groups of k-edge-colored digraphs, and by DGR the union of all the classes $DG(k)$ (which in Wielandt's terminology is the class of 2-closed groups). Clearly, $GR \subseteq DGR$, and $G(k) \subseteq DG(k)$, for any k.

The main general problem is to determine which permutation groups are the automorphism groups of edge-colored graphs. Various aspects of this general problem are investigated. For example, it leads to the concept of colored totally symmetric graphs, that was described in [11, 12]. This coincides to a large extent with the research on homogeneous factorization of graphs (c.f., [4, 15, 16]). One direction of research is to consider various constructions of permutation groups and to ask the following question: is it true that if the components of the construction belong to a particular class $G(k)$, then the result belongs to $G(k)$, as well? And if not, how many colors one must add to make sure that the result of the construction belong to $G(k + r)$?

For the direct product the problem has been solved in [9, Theorem 2.2].

Theorem 1.1 (Grech, Jeż, Kisielewicz)**.** If permutation groups $A, B \in GR$, then $A \times B \in GR$. Also, if $A, B \in DGR$, then $A \times B \in DGR$.

Note that the second part of this theorem was also shown in [3, Theorem 5.1]

This result, with some exceptions, is also true for particular classes $G(k)$ and $DG(k)$ (for details see [7]). In this paper we consider the converse of the theorem above. We show that while for DGR the converse also holds (Theorem 3.1), for GR it is not generally true. The main results is Theorem 3.2 characterizing the conditions under which the direct product of two arbitrary permutation groups belongs to GR.

2 Preliminaries

We assume that the reader has basic knowledge in the areas of graphs and permutation groups, so we omit an introduction to standard terminology. If necessary, additional details can be found in [2, 24].

By a *k-edge-colored graph G*, we mean a pair $G = (V, E)$, where V is the set of vertices of G, and E the *edge-color function* from the set $P_2(V)$ of unordered pairs of vertices into the set of colors $\{0, \ldots, k-1\}$ ($E : P_2(V) \to \{0, \ldots, k-1\}$). Thus, G is a complete simple graph with colored edges. Similarly, by a *k-edge-colored digraph* G, we mean a pair (V, E) where E is a color function from the set of ordered pairs of different elements of V to the set of colors $\{0, \ldots, k - 1\}$ ($E : ((V \times V) \setminus \{(v, v); v \in V\}) \to \{0, \ldots, k-1\}$).

An automorphism of an edge-colored graph G is a permutation a of the set V preserving the edge function: $E(\{v, w\}) = E(\{a(v), a(w)\})$, for all $v, w \in V$. The group of automorphisms of G will be denoted by $Aut(G)$, and considered as a permutation group $(Aut(G), V)$ acting on the set of the vertices V. Edge-colored digraphs are defined similarly.

All groups considered in this paper are groups of permutations. They are considered up to permutation group isomorphism. Generally, a permutation group A acting on a set V is denoted (A, V) or just A, if the set V is clear from the context or not important. By S_n we denote the symmetric group on n elements, and by I_n, the one element group acting on n elements (consisting of the identity only, denoted by id).

We shall consider the natural actions of a given permutation group $A = (A, V)$ on the sets of ordered and unordered pairs of V, $V \times V$ and $P_2(V)$, respectively. Let $a \in A$ and $v, w \in V$. Then, the first action of a is given by the formula

$$a((v, w)) = (a(v), a(w)),$$

while the second action is given by

$$a(\{v, w\}) = \{a(v), a(w)\}.$$

The orbits of A in the action on $V \times V$ are called *orbitals* of A. Since in this paper we concider graphs (digraphs) without loops, we exclude trivial orbitals consisting of pairs of the form (v, v). For two orbitals O_1, O_2 we say that O_1 is *paired* with O_2 if and only if $O_2 = \{(w, v) : (v, w) \in O_1\}$. We call an orbital O *self-paired* if it is paired with itself. Moreover, we say that a permutation a *transposes* O_1 and O_2, if $a(O_1) = O_2$.

In addition, the orbits of A in the action on $P_2(V)$ will be called here 2^**-orbitals*. Note that we can think of a 2^*-orbital either as a self paired orbital or as a pair of paired orbitals.

Since $A \times I_1 = I_1 \times A = A$ (up to permutation isomorphism), in this paper, we consider only the direct products $A \times B$ with both the permutation groups A, B different from I_1.

Let $A = (A, V)$ be a permutation group, and let $O_1^*, \ldots O_k^*$ be all the 2^*-orbitals of A. We define an edge-colored graph $G^*(A)$ (called 2^*-*orbital graph*) as follows.

$$G^*(A) = (V, E), \text{ where } E : P_2(V) \to \{0, \ldots k - 1\}.$$

$$E(\{v, w\}) = i \text{ if and only if the edge } \{v, w\} \text{ belongs to the } 2^*\text{-orbital } O_i^*.$$

Now, we define $A^* = Aut(G^*(A))$. Obviously, $A \subseteq A^*$. It should be clear that A^* is the smallest permutation group on V that contains A and belongs to GR. (Indeed, if G' is a colored graph whose automorphism group contains A, then edges in each 2^*-orbital of A have to have the same color. Hence, each permutation in $Aut(G^*(A))$ belongs to $Aut(G')$.) In particular, we have that $A \in GR$ if and only if $A = A^*$.

Similarly we define the *orbital digraph* $G(A)$ replacing 2^*-orbitals by orbitals. In the same way, denoting $\overline{A} = Aut(G(A))$, we have that $\overline{A}$ is the smallest permutation group on X that contains A and belongs to DGR. Moreover, $A \in DGR$ if and only if $A = \overline{A}$. In addition, $A \subseteq \overline{A} \subseteq A^*$.

For direct products of permutation groups we have the following inclusions

Lemma 2.1.

(i) $A \times B \subseteq Aut(G^*(A \times B)) \subseteq A^* \times B^*$,

(ii) $A \times B \subseteq Aut(G(A \times B)) \subseteq \overline{A} \times \overline{B}$,

Proof. The first inclusion holds for all permutation groups, as it was remarked above. We prove the second inclusion.

Consider the edges of the form $\{(v_1, w), (v_2, w)\}$, which we may refer as edges belonging to the rows. Obviously, they form a union of 2^*-orbitals, and therefore the edges $\{(v_1, w_1), (v_2, w_2)\}$ with $w_1 \neq w_2$ in $Aut(G^*(A \times B))$ have different colors than those belonging to the rows. The same is true for columns, i.e. the edges of the form $\{(w, v_1), (w, v_2)\}$. Thus, rows can be mapped only onto rows by automorphisms of $G^*(A \times B)$, and columns can be mapped only onto columns. This implies that $Aut(G^*(A \times B)) \subseteq A_1 \times B_1$, for some A_1 and B_1. Now let $(a, b) \in Aut(G^*(A \times B))$. Then, the edges $(a, b)(\{(v_1, w), (v_2, w)\})$ and $\{(v_1, w), (v_2, w)\}$ have the same color. Therefore, there is $(a_1, b_1) \in A \times B$ such that $(a_1, b_1)(\{(v_1, w), (v_2, w)\}) = \{(v_1, w), (v_2, w)\}$. Hence, $(a_1^{-1}a, b_1^{-1}b) \in Aut(G^*(A \times B))$ preserves the row with the edge $\{(v_1, w), (v_2, w)\}$. Since every row in $Aut(G^*(A \times B))$ is a copy of $G^*(A)$ (up to recoloring), we have that $a_1^{-1}a \in A^*$, which implies that $a \in A^*$. In a similar way, $b \in B^*$, which completes the proof of the first part of the theorem. The second part is proved similarly. □

We observe that if $C = Aut(G^*(A \times B))$, then C^* may be a proper subgroup of $A^* \times B^*$. The smallest example is $I_2 \times I_2$, where $Aut(G^*(I_2 \times I_2)) = I_2 \times I_2$, while ${I_2}^* \times {I_2}^* = S_2 \times S_2$.

We observe also that if $a \in A^*$, then it not only preserves 2^*-orbitals of A (by definition), but it also preserves orbits of A.

Lemma 2.2. Let $A \neq I_2$ be a permutation group. If $a \in A^*$, then a preserves the orbits of A.

Proof. Let Q_t, $t \in \{1, \ldots, m\}$ be the orbits of A. The claim is obvious if $A = I_t$ for any $t > 2$, so we may assume that there is an orbit Q_i that has at least two elements. Then, the set $P_2(Q_i)$ is nonempty. Moreover, it is clear that $P_2(Q_i)$ is the union of 2^*-orbitals of A. Hence, the edges of $G^*(A)$ that belong to $P_2(Q_i)$ have different colors than the remaining edges. This implies that a preserves the orbit Q_i.

Now, if there is another orbit Q_t, $t \neq i$, then obviously, the edges $\{v, w\}$ with $v \in Q_i$ and $w \in Q_t$ have different colors than the remaining edges. Consequently, every orbit is preserved by a. □

3 Results

We proceed to the main problem of this paper to describe conditions under which $A \times B$ belongs to GR or DGR. The case of directed graphs is pretty easy.

Theorem 3.1. Let A and B be permutation groups. Then, $A \times B \in DGR$ if and only if both A and B are in DGR.

Proof. In view of the Theorem 1.1 quoted in the introduction we need to prove merely the "only if" part. It is enough to prove, without loss of generality, that if $A \notin DGR$, then

$A \times B \notin DGR$. Let $A = (A, V)$ and $B = (B, W)$. We assume that $A \notin DGR$. Then, $A \neq I_2$ (since $I_2 \in DGR$). Moreover, we may choose $a \in \overline{A} \setminus A$. By definition, it preserves all orbitals of A.

Let id_B be the identity in the permutation group B. We show that the permutation (a, id_B) belongs to $Aut(G(A \times B))$. To this end, we show that for every directed edge $e = ((v_1, w_1), (v_2, w_2))$, where $v_1, v_2 \in V$, $w_1, w_2 \in W$, the image $(a, id_B)(e)$ has the same color as e.

Assume first that $v_1 \neq v_2$. Since a preserves orbitals of A, for every pair (v_1, v_2), there is a permutation $a_2 \in A$ such that $a(v_1) = a_2(v_1)$ and $a(v_2) = a_2(v_2)$. We have $(a, id_B)(e) = (a_2, id_B)(e)$, and therefore the directed edges $(a, id_B)(e)$ and e belong to the same orbital of $A \times B$. So, by the definition of the edge-colored digraph $G(A \times B)$, $(a, id_B)(e)$ and e have the same color in $G(A \times B)$.

If $v_1 = v_2$, then since $A \neq I_2$, we may use Lemma 2.2 and find a permutation $a_1 \in A$ such that $a_1(v_1) = a(v_1)$. We have $(a, id_B)(e) = (a_1, id_B)(e)$, and therefore the directed edges $(a, id_B)(e)$ and e belong to the same orbital of $A \times B$. So, they have the same color.

Thus, in all the cases $(a, id_B) \in Aut(G(A \times B))$, but (a, id_B) does not belong to $A \times B$. Therefore, $A \times B \notin DGR$. □

This settles the problem for the case of edge-colored digraphs. The case of edge-colored graphs is different and more complex.

Theorem 3.2. Let A and B be permutation groups. Then, $A \times B \in GR$, except for the following cases:

(i) $A \times B \notin DGR$, that is, either $A \notin DGR$ or $B \notin DGR$,

(ii) either every orbital of $A \in GR$ is self-paired and $B \notin GR \cup \{I_2\}$ or every orbital of $B \in GR$ is self-paired and $A \notin GR \cup \{I_2\}$,

(iii) $A, B \in DGR \setminus (GR \cup \{I_2\})$, and there exist $a \in A^* \setminus A$ and $b \in B^* \setminus B$, such that a transposes every pair of paired orbitals in A, and b transposes every pair of paired orbitals in B.

Proof. We consider a few cases. An obvious consequence of Theorem 3.1 is the following

Corollary 3.3. Let $A \notin DGR$ and B be an arbitrary permutation group. Then, $A \times B \notin GR$.

Accordingly to this corollary, we will assume further that both the components of $A \times B$ belongs to DGR. The next three lemmas deal with the case when one of the groups belongs to GR or is equal to I_2.

Lemma 3.4. Let $A \in DGR \setminus (GR \cup \{I_2\})$ and $B \in GR$. If every orbital of B is self-paired, then $A \times B \notin GR$.

Proof. Denote $A = (A, V)$ and $B = (B, W)$. Let $a \in A^* \setminus A$, and id_B be the identity in the permutation group B. Let $e = \{(v_1, w_1), (v_2, w_2)\}$, where $v_1, v_2 \in V$, $w_1, w_2 \in W$. We show that the edges e and $(a, id_B)(e)$ have the same color. To this end it is enough to prove that $(a, id_B)(e)$ belongs to the same 2^*-orbital of $A \times B$ as e.

If $w_1 = w_2$, then the statement holds by the fact that a preserves all 2^*-orbitals of A. Assume $v_1 = v_2$. Since $A \neq I_2$, by Lemma 2.2, a preserves all orbits of A (in its action on V). Hence, there is $a_1 \in A$ such that $a(v_1) = a_1(v_1)$. We have,

$$\begin{aligned}(a, id_B)(\{(v_1, w_1), (v_1, w_2)\}) &= \{(a(v_1), w_1), (a(v_1), w_2)\} \\ &= (a_1, id_B)(\{(v_1, w_1), (v_1, w_2)\}).\end{aligned}$$

Thus, e and $(a, id_B)(e)$ belong to the same 2^*-orbital of $A \times B$.

Now let $v_1 \neq v_2$ and $w_1 \neq w_2$. If the pair $a((v_1, v_2))$ belongs to the same orbital of A as the pair (v_1, v_2), then there is $a_1 \in A$ such that $a_1(v_1) = a(v_1)$ and $a_1(v_2) = a(v_2)$. Similarly as above, we have,

$$\begin{aligned}(a, id_B)(\{(v_1, w_1), (v_2, w_2)\}) &= \{(a(v_1), w_1), (a(v_2), w_2)\} \\ &= (a_1, id_B)(\{(v_1, w_1), (v_2, w_2)\}).\end{aligned}$$

Assume, finally, that $v_1 \neq v_2$, $w_1 \neq w_2$ and the pairs $a((v_1, v_2))$, (v_1, v_2) belong to different orbitals of A. Since $a \in A^*$, we know that a preserves all 2^*-orbitals of A. This implies that, the pairs $a((v_1, v_2))$ and (v_2, v_1) belong to the same orbital of A. Hence, there is $a_1 \in A$ such that $a_1((v_2, v_1)) = a((v_1, v_2))$. Moreover, since all orbitals of B are self-paired, there is $b \in B$ such that $b((w_1, w_2)) = (w_2, w_1)$. Consequently,

$$(a, id_B)(e) = \{(a_1(v_2), b(w_2)), (a_1(v_1), b(w_1))\} = (a_1, b)(e).$$

Thus $(a, id_B)(e)$ and e belongs to the same 2^*-orbital of $A \times B$, and consequently, (a, id_B) does not change the color of the edges.

It follows that $(a, id_B) \in Aut(G^*(A \times B)) = (A \times B)^*$. Since $a \in A^* \setminus A$, $(a, id_B) \notin A \times B$, and therefore $A \times B \neq (A \times B)^*$, which completes the proof. □

Lemma 3.5. Let $A \in DGR \setminus (GR \cup \{I_2\})$ and let $B \in GR$ have at least one not-self-paired orbital. Then, $A \times B \in GR$.

Proof. Let $A = (A, V)$ and $B = (B, W)$. We know, by Lemma 2.1(1), that $Aut(G^*(A \times B)) \subseteq A^* \times B$. Therefore, every $c \in Aut(G^*(A \times B))$ has the form (a, b), where $a \in A^*$ and $b \in B$. We show that, in fact, a always belongs to A. Assume, to the contrary, that $a \in A^* \setminus A$. In this case, since $A \in DGR \setminus (GR \cup \{I_2\})$, there is an (ordered) pair $(v_1, v_2), v_1, v_2 \in V$ such that $a((v_1, v_2)) \neq a_1((v_1, v_2))$, for every $a_1 \in A$. Since B has an orbital which is not-self-paired, there are $w_1, w_2 \in W$ such that $b((w_1, w_2)) \neq (w_2, w_1)$ for every $b \in B$. Now, observe that the edges $(a, b)(\{(v_1, w_1), (v_2, w_2)\})$ and $\{(v_1, w_1), (v_2, w_2)\}$ belong to different 2^*-orbitals of $A \times B$. Indeed, if the edges $(a, b)(\{(v_1, w_1), (v_2, w_2)\})$ and $\{(v_1, w_1), (v_2, w_2)\}$ belong to the same 2^*-orbital of $A \times B$, then either there are $a_1 \in A$ and $b_1 \in B$ such that $a((v_1, v_2)) = a_1((v_1, v_2))$ and $b((w_1, w_2)) = b_1((w_1, w_2))$ or there are $a_2 \in A$ and $b_2 \in B$ such that $a((v_1, v_2)) = a_2((v_2, v_1))$ and $b((w_1, w_2)) = b_2((w_2, w_1))$. The first case is impossible by the assumption on a. In the second case, we get $b_2^{-1}b((w_1, w_2)) = (w_2, w_1)$, which contradicts the assumption. This implies that $E((a, b)(\{(v_1, w_1), (v_2, w_2)\})) \neq E(\{(v_1, w_1), (v_2, w_2)\})$, which contradicts the fact that $(a, b) \in Aut(G^*(A \times B))$. Consequently, we have $Aut(G^*(A \times B)) \subseteq A \times B$, which completes the proof. □

We summarize Lemma 3.4 and Lemma 3.5.

Corollary 3.6. Let $A \in DGR \setminus (GR \cup \{I_2\})$ and $B \in GR$. Then, $A \times B \in GR$ if and only if there exists a non-self-paired orbital of B.

The following special case must be considered separately.

Lemma 3.7. Let $B \in GR$. Then, $B \times I_2 \in GR$.

Proof. By Lemma 2.1(1), $Aut(G^*(B \times I_2))$ is equal either to $B \times I_2$ or to $B \times S_2$. By our general assumption $B \neq I_1$, hence, in $G^*(B \times I_2)$, there is at least one edge of the form $\{(v, 0), (w, 0)\}$, and being in different orbitals, it has a different color than $\{(v, 1), (w, 1)\}$. Thus, $Aut(G^*(B \times I_2)) = B \times I_2$. Therefore, $B \times I_2 \in GR$. □

This completes the description in all the cases where at least one of the components belongs to GR.

The remaining case occurs where $A, B \in (DGR \setminus GR)$. We start with the following.

Lemma 3.8. Let $A, B \in (DGR \setminus GR)$. If for every $b \in B^*$ there exists a pair of paired orbitals $O_1 \neq O_2$ of B such that b does not transpose O_1 and O_2, then $A \times B \in GR$.

Proof. Let $A = (A, V)$ and $B = (B, W)$. Assume to the contrary that there exists $(a, b) \in Aut(G^*(A \times B)) \setminus (A \times B)$.

First, assume that $a \in A$; then, $b \notin B$. Since $A \in (DGR \setminus GR)$, there is an (ordered) pair (v_1, v_2), where $v_1, v_2 \in V$, which belongs to a non-self paired orbital of A. Since $B \in DGR$, there is an (ordered) pair (w_1, w_2) where $w_1, w_2 \in W$, for which there is no $b_1 \in B$ such that $b_1((w_1, w_2)) = b((w_1, w_2))$. We prove that the edge $\{(v_1, w_1), (v_2, w_2)\}$ belongs to a different 2^*-orbital than the edge $(a, b)(\{(v_1, w_1), (v_2, w_2)\})$. Indeed, if the edges $(a, b)(\{(v_1, w_1), (v_2, w_2)\})$ and $\{(v_1, w_1), (v_2, w_2)\}$ belong to the same 2^*-orbital, then either there are $a_1 \in A$ and $b_1 \in B$ such that $a((v_1, v_2)) = a_1((v_1, v_2))$ and $b((w_1, w_2)) = b_1((w_1, w_2))$ or there are $a_2 \in A$ and $b_2 \in B$ such that $a((v_1, v_2)) = a_2((v_2, v_1))$ and $b((w_1, w_2)) = b_2((w_2, w_1))$. In the former, by assumption on b and w_1, w_2, this is impossible. In the latter, since $a \in A$ it is also impossible. Hence, the edges $(a, b)(\{(v_1, w_1), (v_2, w_2)\})$ and $\{(v_1, w_1), (v_2, w_2)\}$ have different colors in $G^*(A \times B)$. This contradicts the assumption that $(a, b) \in Aut(G^*(A \times B))$.

Next, consider the case where $a \notin A$. Since $A \in DGR$, there is an ordered pair (v_1, v_2), where $v_1, v_2 \in V$, for which there is no permutation $a_1 \in A$ such that $a_1((v_1, v_2)) = a((v_1, v_2))$. Let O_1, O_2 be orbital from the statement of the lemma. By assumption, there are $w_1, w_2 \in W$ such that $\{w_1, w_2\} \in O_1$ and $b((w_1, w_2)) \in O_1$. Thus, $b((w_1, w_2)) = b_1((w_1, w_2))$ for some $b_1 \in B$. A similar proof as above shows that the edge

$$(a, b)(\{(v_1, w_1), (v_2, w_2)\}) = (a, b_1)(\{(v_1, w_1), (v_2, w_2)\})$$

belongs to a different 2^*-orbital than the edge $\{(v_1, w_1), (v_2, w_2)\}$. Again, this contradicts the assumption that $(a, b) \in Aut(G^*(A \times B))$. □

Now, we consider the case where one of the groups is equal to I_2.

Lemma 3.9. Let $A \in (DGR \setminus GR)$. Then, $A \times I_2 \in GR$.

Proof. Let $A = (A, V)$ and $I_2 = (I_2, \{w_1, w_2\})$. Assume to the contrary that there is $(a, b) \in Aut(G^*(A \times I_2)) \setminus (A \times I_2)$. Since, for any $v_1, v_2, v_3, v_4 \in V$, the edges $\{(v_1, w_1), (v_2, w_1)\}$ and $\{(v_3, w_2), (v_4, w_2)\}$ have different colors, $b = id$. In the same way as in the second case of the proof of the Lemma 3.8, we get a contradiction. □

Now, we consider the last case.

Lemma 3.10. Let $A, B \in DGR \setminus (GR \cup I_2)$. If there exists $a \in A^* \setminus A$ which transposes all the pairs of the paired orbitals of A and there exists $b \in B^* \setminus B$ which transposes all the pairs of the paired orbitals of B, then $A \times B \notin GR$. Moreover, $A \times B$ is transitive.

Proof. Let $A = (A, V)$ and $B = (B, W)$. Since $A \neq I_2$ and $B \neq I_2$, by Lemma 2.2, every permutation $a \in A^* \setminus A$ preserves the orbits of A (in its action on V) and every permutation $b \in B^* \setminus B$ preserves the orbits of B (in its action on W). Hence, we obtain immediately, under the assumptions on A and B, that the permutation groups A and B have to be transitive. Consequently, for every $a \in A^*, b \in B^*$, $v, v_1, v_2 \in V$, and $w, w_1, w_2 \in W$, the edge $(a,b)(\{(v,w_1),(v,w_2)\})$ has the same color in $G^*(A \times B)$ as the edge $\{(v,w_1),(v,w_2)\}$, and moreover, the edge $(a,b)(\{(v_1,w),(v_2,w)\})$ has the same color as the edge $\{(v_1,w),(v_1,w)\}$.

We choose a and b as in the statement of the lemma, and fix the elements $v_1 \neq v_2 \in V$ and $w_1 \neq w_2 \in W$. Since a and b preserves no non-self-paired orbital, the ordered pair $a((v_1,v_2))$ belongs to the orbital of the ordered pair (v_2,v_1) and the ordered pair $b((w_1,w_2))$ belongs to the orbital of the ordered pair (w_2,w_1). Hence, there are $a_1 \in A$ and $b_1 \in B$ such that $a((v_1,v_2)) = a_1((v_2,v_1))$ and $b((w_1,w_2)) = b_1((w_2,w_1))$. Therefore, we have

$$\begin{aligned} E((a,b)(\{(v_1,w_1),(v_2,w_2)\})) &= E(\{(a(v_1),b(w_1)),(a(v_2),b(w_2))\}) \\ &= E(\{(a_1(v_2),b_1(w_2)),(a_1(v_1),b_1(w_1))\}) \\ &= E((a_1,b_1)(\{(v_1,w_1),(v_2,w_2)\})) \\ &= E(\{(v_1,w_1),(v_2,w_2)\}). \end{aligned}$$

The vertices v_1, v_2, w_1, and w_2 are arbitrary. Hence, the permutation (a,b) preserves all colors. Consequently, $(a,b) \in Aut(G^*(A \times B) \setminus (A \times B))$. ☐

This exhausts all cases and ends the proof of the theorem. ☐

4 Corollaries and problems

First, it is worth noting that for some subclasses the result may be stated in a nice simple form. Since all intransitive permutation groups have a non-self-paired orbital, we have the following.

Corollary 4.1. Let $A \in DGR$, and $B \in GR$ be intransitive. Then, $A \times B \in GR$.

Also, it is easy to observe that the only regular groups with all self-paired orbitals are $S_2^n, n \geq 1$. This implies that:

Corollary 4.2. Let $A \in DGR$, and $B \in GR$ be regular. Then, $A \times B \in GR$ if and only if $B \neq S_2^n$, for every n.

Next, we give an alternative proof of the known fact, that was first observed in [22, Example 3.15]

Corollary 4.3. Every regular permutation group belongs to DGR.

Proof. Let U be an nonsolvable regular group. Then, for every regular group A, the group $A \times U$ is nonsolvable. By [5], we have $A \times U \in G(2) \subseteq DGR$. By Theorem 3.1, $A \in DGR$. □

The next fact, it seems, was not recognized so far.

Corollary 4.4. Except for the abelian groups of exponent greater than two and generalized dicyclic groups, all the finite regular permutation groups belong to the class GR.

Proof. Let A be an abelian group of exponent greater than two or a generalized dicyclic group. It is proved in [5], that in such a case $A \notin G(2)$. The proof shows, in fact, that $A \notin GR$. Assume that A is not as those groups mentioned above. Then, it is well known (see [5]) that $A \times S_2^4 \in G(2)$. Since $S_2^4 \in GR$ and it has all orbitals self-paired, then by Theorem 3.2 (ii), $A \in GR$. □

Theorem 3.2 suggests a few open problems.

Problem 4.5. Describe the permutation groups that have all orbitals self-paired.

This does not seem to be an easy problem. Examples of groups whose all orbitals are self-paired are S_n and their transitive products (direct product, wreath product, etc.). In particular, all groups of the form S_2^k (the direct power) belong to this class. Yet, there are other examples, like the automorphism groups of totally symmetric graphs described in [11]. Note that if a permutation group A having all orbitals self-paired is an automorphism group of a colored digraph D, $A = Aut(D)$, then D is, in fact, an undirected colored graph, and so $A \in GR$.

It would be also desirable to have a description of permutation groups with the property given in Theorem 3.2(iii).

Problem 4.6. Describe all transitive permutation groups A having a permutation $\sigma \in A^* \setminus A$ transposing all pairs of paired orbitals.

We note that all regular abelian group of exponent greater than two and regular generalized dicyclic groups have this property. However, there are also many other examples. For instance, the group $A = \langle (0, 1, 2, 3, 4, 5, 6), (1, 2, 4)(3, 6, 5) \rangle$ is one of them. This group is a subgroup of Frobenius group F_7 generated by translations and multiplication by 2 (which is a permutation of order 3). This suggest the following.

Problem 4.7. Let A be a subgroup of the permutation group $AGL_n(p)$ generated by translations and ω^{2k}, where ω is a generator of the the multiplicative group $F_{p^n}^*$, and k divides n. Moreover, let -1 be not quadratic in F_{p^n}. Is it true that for each such group there is an element $a \in A^* \setminus A$ transposing all pairs of paired orbitals?

ORCID iDs

Mariusz Grech https://orcid.org/0000-0002-7328-8792

References

[1] L. Babai, Finite digraphs with given regular automorphism groups, *Period. Math. Hungar.* **11** (1980), 257–270, doi:10.1007/bf02107568.

[2] L. Babai, Automorphism groups, isomorphism, reconstruction, in: *Handbook of combinatorics, Vol. 1, 2*, Elsevier Sci. B. V., Amsterdam, pp. 1447–1540, 1995.

[3] P. J. Cameron, M. Giudici, G. A. Jones, W. M. Kantor, M. H. Klin, D. Marušič and L. A. Nowitz, Transitive permutation groups without semiregular subgroups, *J. London Math. Soc. (2)* **66** (2002), 325–333, doi:10.1112/s0024610702003484.

[4] M. Giudici, C. H. Li, P. Potočnik and C. E. Praeger, Homogeneous factorisations of graphs and digraphs, *European J. Combin.* **27** (2006), 11–37, doi:10.1016/j.ejc.2004.08.003.

[5] C. D. Godsil, GRR's for non solvable groups, in: *Algebraic methods in graph theory*, 1978 pp. 221–239.

[6] M. Grech, Direct products of automorphism groups of graphs, *J. Graph Theory* **62** (2009), 26–36, doi:10.1002/jgt.20385.

[7] M. Grech, The graphical complexity of direct products of permutation groups, *J. Graph Theory* **66** (2011), 303–318, doi:10.1002/jgt.20504.

[8] 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.

[9] M. Grech, A. Jeż and A. Kisielewicz, Graphical complexity of products of permutation groups, *Discrete Math.* **308** (2008), 1142–1152, doi:10.1016/j.disc.2007.04.004.

[10] M. Grech and A. Kisielewicz, Direct product of automorphism groups of colored graphs, *Discrete Math.* **283** (2004), 81–86, doi:10.1016/j.disc.2003.11.008.

[11] M. Grech and A. Kisielewicz, Totally symmetric colored graphs, *J. Graph Theory* **62** (2009), 329–345, doi:10.1002/jgt.20397.

[12] M. Grech and A. Kisielewicz, All totally symmetric colored graphs, *Discrete Math. Theor. Comput. Sci.* **15** (2013), 133–145, doi:10.46298/dmtcs.630.

[13] W. Imrich, On products of graphs and regular groups, *Israel J. Math.* **11** (1972), 258–264, doi:10.1007/bf02789317.

[14] A. Kisielewicz, Supergraphs and graphical complexity of permutation groups, *Ars Combin.* **101** (2011), 193–207.

[15] C. H. Li, T. K. Lim and C. E. Praeger, Homogeneous factorisations of complete graphs with edge-transitive factors, *J. Algebraic Combin.* **29** (2009), 107–132, doi:10.1007/s10801-008-0127-2.

[16] C. H. Li and C. E. Praeger, On partitioning the orbitals of a transitive permutation group, *Trans. Amer. Math. Soc.* **355** (2003), 637–653, doi:10.1090/s0002-9947-02-03110-0.

[17] L. A. Nowitz and M. E. Watkins, Graphical regular representations of non-abelian groups. I, II, *Canadian J. Math.* **24** (1972), 993–1008; ibid. 24 (1972), 1009–1018, doi:10.4153/cjm-1972-101-5.

[18] W. Peisert, Direct product and uniqueness of automorphism groups of graphs, *Discrete Math.* **207** (1999), 189–197, doi:10.1016/s0012-365x(99)00044-8.

[19] G. Sabidussi, raph multiplication, *Math. Z.* **72** (1959), 446–457, doi:10.1007/bf01162967.

[20] M. E. Watkins, On the action of non-Abelian groups on graphs, *J. Combinatorial Theory Ser. B* **11** (1971), 95–104, doi:10.1016/0095-8956(71)90019-0.

[21] M. E. Watkins and L. A. Nowitz, On graphical regular representations of direct products of groups, *Monatsh. Math.* **76** (1972), 168–171, doi:10.1007/bf01298284.

[22] H. Wielandt, Permutation groups through invariant relations and invariant functions [83], in: B. Huppert and H. Schneider (eds.), *Volume 1 Group Theory*, De Gruyter, pp. 237–296, 1969, doi:10.1515/9783110863383.237.

[23] H. Wielandt, Permutation groups through invariant relation and invariant functions, in: B. Huppert and H. Schneider (eds.), *Mathematical works, vol. 1, Group theory*, Walter de Gruyter Co., Berlin, pp. 237–266, 1994.

[24] H. P. Yap, *Some Topics in Graph Theory*, volume 108 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, 1986, doi:10.1017/cbo9780511662065.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.07 / 271–282
https://doi.org/10.26493/1855-3974.2454.892
(Also available at http://amc-journal.eu)

Efficient proper embedding of a daisy cube*

Aleksander Vesel

Faculty of Natural Sciences and Mathematics, University of Maribor, SI-2000 Maribor, Slovenia

Received 4 October 2020, accepted 14 June 2021, published online 25 October 2021

Abstract

For a set X of binary words of length h the daisy cube $Q_h(X)$ is defined as the subgraph of the hypercube Q_h induced by the set of all vertices on shortest paths that connect vertices of X with the vertex 0^h. A vertex in the intersection of all of these paths is a minimal vertex of a daisy cube. A graph G isomorphic to a daisy cube admits several isometric embeddings into a hypercube. We show that an isometric embedding is proper if and only if the label 0^h is assigned to a minimal vertex of G. This result allows us to devise an algorithm which finds a proper embedding of a graph isomorphic to a daisy cube into a hypercube in linear time.

Keywords: Daisy cube, partial cube, isometric embedding, proper embedding.

Math. Subj. Class. (2020): 05C12, 05C85

1 Introduction

Hypercube is one of the most important interconnection scheme for multicomputers. An obstacle to a direct application of a hypercube is the fact that the number of different hypercubes is very small with respect to the wanted (maximum) number of nodes, that is to say, the number of vertices of a hypercube is always equal to a power of two. For that reason, several other interconnection topologies for multicomputers based on hypercubes have been proposed. These graphs have been devised to preserve a hypercube's most essential properties while allowing more variety of resulting specific graphs. The corresponding families of graphs are mostly various subgraphs of a hypercube, of which its isometric subgraphs, i.e. its induced subgraphs that preserve distances, are of particular importance. A crucial problem in this scope is to find an embedding of a graph of this type to a hypercube (see for example [1, 4, 16]).

*This work was supported by the Slovenian Research Agency under the grants P1-0297, J1-2452, J1-9109 and J1-1693.

E-mail address: aleksander.vesel@um.si (Aleksander Vesel)

Quite recently, a new concept which led to the class of graphs called daisy cubes has been proposed in [9]. It has been shown that daisy cubes are isometric subgraphs of a hypercube, moreover, they include several other important classes of graphs, some well-known examples are Fibonacci and Lucas cubes (see, for example [2, 5, 8, 11]) as well as some other families of generalized Fibonacci cubes and generalized Lucas cubes [3, 6, 7, 15]. Daisy cubes play an essential role in showing that specific generalized Fibonacci cubes' cube-complements are isometric subgraphs of a hypercube [13]. It is also proven that a class of graphs, which is of significant importance in chemical graph theory, also belongs to daisy cubes [14].

In [12], daisy cubes are characterized in terms of an expansion procedure. For a given graph G isomorphic to a daisy cube, but without the corresponding embedding into a hypercube, an algorithm which finds a proper embedding of G into a hypercube in $O(mn)$ time is also presented.

Several challenging open problems concerning daisy cubes have been proposed [9, 12]. In this paper, we focus our study to the following one.

Problem 1.1. Is there a faster way of finding the vertex 0^h of a daisy cube $Q_h(X)$ than the one provided in [12]?

It is also noted that a positive answer to Problem 1 would give a linear time algorithm for finding a proper embedding of a graph isomorphic to a daisy cube.

The paper is organized as follows. In the next section some basic definitions, concepts and results needed in the sequel are given. In Section 3, a notion of a minimal vertex of a daisy cube is introduced. Some necessary and sufficient conditions that a minimal vertex has to fulfill are also given. In Section 4, it is shown that an isometric embedding of a graph isomorphic to a daisy cube, but without the corresponding embedding into a hypercube, can be constructed in linear time even if a minimal vertex of a daisy cube is unknown. The last section shows that an isometric embedding devised in the Section 4 can be applied in order to find a proper embedding within the same time bound.

2 Preliminaries

Let $B = \{0, 1\}$. If b is a word of length h over B, that is, $b = (b_1, \dots, b_h) \in B^h$, then we will briefly write b as $b_1 \dots b_h$. If $x, y \in B^h$, then the *Hamming distance* $H(x, y)$ between x and y is the number of positions in which x and y differ.

We will use $[n]$ for the set $\{1, 2, \dots, n\}$.

The *hypercube* of order h or simply h*-cube*, denoted by Q_h, is the graph $G = (V, E)$ where the vertex set $V(G)$ is the set of all binary strings $b = b_1 b_2 \dots b_h$, $b_i \in \{0, 1\}$ for all $i \in [h]$, and two vertices $x, y \in V(G)$ are adjacent in Q_h if and only if the Hamming distance between x and y is equal to one.

For a binary string $b = b_1 b_2 \dots b_n$, let $\overline{b}_i = 1 - b_i$ for $i \in [h]$. The *weight* of $u \in B^h$ is $w(u) = \sum_{i=1}^{h} u_i$, in other words, $w(u)$ is the number of 1s in the word u. For the concatenation of bits the power notation will be used, for instance $0^h = 0 \dots 0 \in B^h$.

If G is a connected graph, then the distance $d_G(u, v)$ (or simply $d(u, v)$) between vertices u and v is the length of a shortest u, v-path (that is, a shortest path between u and v) in G. The set of vertices lying on all shortest u, v-paths is called the *interval* between u and v and denoted by $I_G(u, v)$ [10]. We will also write $I(u, v)$ when G will be clear from the context.

If G is a graph and $X \subseteq V(G)$, then $G[X]$ denotes the subgraph of G induced by X.

If u is a vertex of a graph G, let $N(u)$ denote the set of neighbors of u. Moreover, let $N[u] = N(u) \cup \{u\}$.

Let $G = (V, E)$ be a graph. A mapping $\alpha : V(G) \to V(Q_h)$ is an *isometric embedding* of G into Q_h if $d_{Q_h}(\alpha(u), \alpha(v)) = d_G(u, v)$ for every $u, v \in V(G)$. If $u \in V(G)$, we will denote the i-th coordinate of $\alpha(u)$ as $\alpha_{(i)}(u)$.

Let G be a connected graph. The isometric dimension of G is the smallest integer h such that G admits an isometric embedding into Q_h. Isometric subgraphs of hypercubes are called *partial cubes*.

Let $\leq$ be the partial order on $V(Q_h)$ defined with $u_1 \ldots u_h \leq v_1 \ldots v_h$ if $u_i \leq v_i$ holds for all $i \in [h]$. For $X \subseteq V(Q_h)$ the graph induced by the set $\{v \in V(Q_h) \,|\, v \leq x$ for some $x \in X\}$ is a *daisy cube* of Q_h generated by X and denoted by $Q_h(X)$.

Let also $\vee$, $\wedge$ and $\oplus$ denote the bitwise OR, bitwise AND and bitwise exclusive OR operator, respectively.

By a slight abuse of definition, we will say that a graph G is a daisy cube if it is isomorphic to a daisy cube generated by some $X \subseteq V(Q_h)$. If G is a daisy cube $Q_h(X)$, then G may admit more than one isometric embedding of G into the h-cube. Let $X_G \subseteq B^h$ be the set of labels of the vertices of G assigned by an isometric embedding α, i.e. $X_G = \alpha(V(G))$. We say that α is a *proper embedding* of G if G is isomorphic to $Q_h(X_G)$.

Let G be a graph isomorphic to a daisy cube of G_h and let α denote a proper embedding. Note that every permutation of indices of α yields basically the "same" embedding. We say that proper embeddings α and β are *equivalent* if β can be obtained from α by a permutation of its indices.

For a daisy cube $Q_h(X)$, let $\widehat{X}$ denote the antichain consisting of the maximal elements of the poset $(X, \leq)$. It was shown in [9] that $Q_h(X) = Q_h(\widehat{X})$. Hence, for a given set $X \subseteq B_n$ it is enough to consider the antichain $\widehat{X}$. The vertices of $Q_h(X)$ from $\widehat{X}$ are called the *maximal* vertices of $Q_h(X)$. More generally, if G is a daisy cube of Q_h with a proper embedding α such that $\alpha(v) = 0^h$, then $X \subseteq V(G)$ is the set of *maximal vertices of G with respect to* v if $G \cong Q_h(\alpha(X))$ and $\widehat{\alpha(X)} = \alpha(X)$. Moreover, v is the *minimal vertex of G with respect to* α. We also say that v is a *minimal vertex of G* if there exists a proper embedding α such that $\alpha(v) = 0^h$.

The following result shows that a daisy cube is a subgraph of Q_h induced by the union of intervals between 0^h and the vertices from $\widehat{X}$ [9].

Lemma 2.1. *Let $X \subseteq B^h$. Then $Q_h(X) = Q_h[\cup_{x \in \widehat{X}} I(0^h, x)]$.*

3 Minimal vertices of a daisy cube

If $u \in V(Q_h(X))$, then $I(0^n, u)$ induces a $w(u)$-cube in $Q_h(X)$. Note that if $x \in \widehat{X}$, then the cube induced by $I(0^n, x)$ is maximal in $Q_h(X)$, i.e., it is not contained in any other cube that belongs to $Q_h(X)$.

If $x \in B^h$, let S^x denote the set of indices of v with $x_i = 1$, i.e., $S^x = \{i \,|\, x_i = 1 \text{ and } i \in [h]\}$.

Let $v \in B^h$ and let ${}^v\beta : B^h \to B^h$ be the function defined as

$${}^v\beta_{(i)}(u) = \begin{cases} u_i, & v_i = 0 \\ \bar{u}_i, & v_i = 1 \end{cases}$$

Lemma 3.1. *Let G be a graph isomorphic to a daisy cube of Q_h with a proper embedding α such that $\alpha(v^0) = 0^h$ and $\widehat{X} \subseteq V(G)$ is its corresponding maximal set. If $v \in \cap_{x\in\widehat{X}} I(v^0, x)$, then*

(i) *${}^v\beta$ restricted to $\alpha(V(G))$ is a bijection that maps to $\alpha(V(G))$,*

(ii) *${}^v\beta \circ \alpha$ is a proper embedding of G with the minimal vertex v and the maximal vertex set $Y = \{y \,|\, {}^v\beta(\alpha(y)) = \alpha(x) \text{ and } x \in \widehat{X}\}$.*

Proof. (i) We have to show that if $v \in \cap_{x\in\widehat{X}} I(v^0, x)$, then for every $u \in \alpha(V(G)))$ there is exactly one ${}^v\beta(u) \in \alpha(V(G))$. Note that $\alpha^{-1}(u) \in I(v^0, x)$ and $v \in I(v^0, x)$ for some $x \in \widehat{X}$. Thus, $S^u \subseteq S^{\alpha(x)}$ and $S^{\alpha(v)} \subseteq S^{\alpha(x)}$. It follows that $S^{{}^v\beta(u)} \subseteq S^{\alpha(x)}$. Since α is proper, $\alpha(V(G)) = \cup_{x\in\widehat{X}} I(0^h, \alpha(x))$ by Lemma 2.1 and we obtain ${}^v\beta(u) \in V(\alpha(G))$.

In order to see that ${}^v\beta$ is injective, note that ${}^v\beta({}^v\beta(u)) = u$ for every $u \in \alpha(V(G))$. Suppose to the contrary that there exist $u, z \in \alpha(V(G))$, $u \neq z$, such that ${}^v\beta(u) ={}^v \beta(z)$. It follows that ${}^v\beta({}^v\beta(u)) ={}^v\beta({}^v\beta(z))$ and thus $u = z$, which yields a contradiction.

(ii) By (i), ${}^v\beta$ maps from $\alpha(V(G))$ to $\alpha(V(G))$. Let $x \in \widehat{X}$ and recall that ${}^v\beta({}^v\beta(\alpha(x))) = \alpha(x)$. Thus, if $y \in V(G)$ such that $\alpha(y) = {}^v\beta(\alpha(x))$, we have ${}^v\beta(\alpha(y)) = \alpha(x)$. Moreover, ${}^v\beta(v) = 0^h$. It follows that $Y = \{y \,|\, {}^v\beta(\alpha(y)) = \alpha(x) \text{ and } x \in \widehat{X}\}$ is the maximal vertex set of G with respect to ${}^v\beta \circ \alpha$, while v is the corresponding minimal vertex. □

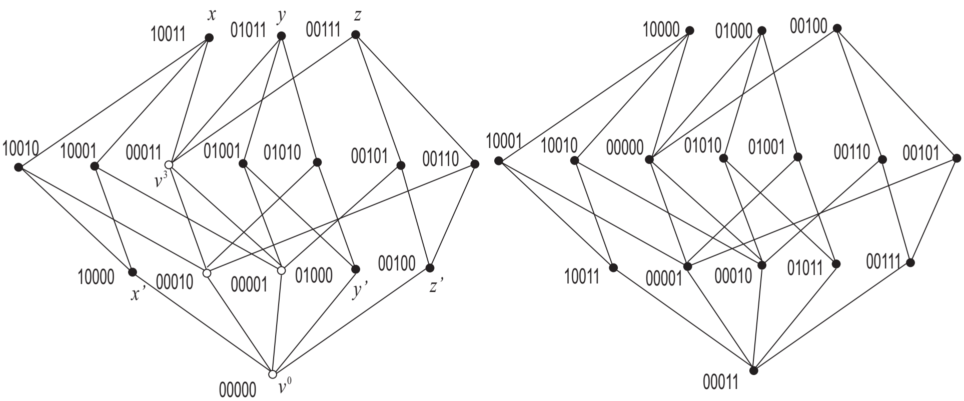


Figure 1: Two proper embeddings of a daisy cube.

Figure 1 shows two proper embeddings of a daisy cube G. The embedding on the left hand side, say α, admits the set of maximal vertices $\widehat{X} = \{x, y, z\}$ with labels $\alpha(x) = 10011$, $\alpha(y) = 01011$ and $\alpha(z) = 00111$. Let $v^0 \in V(G)$ such that $v^0 = \alpha^{-1}(00000)$. Then $I(v^0, x) \cap I(v^0, y) \cap I(v^0, z) = \{v^0, v^1, v^2, v^3\}$, where $\alpha(v^3) = 00011$. The embedding on the right hand side of Figure 1 is ${}^{v^3}\beta \circ \alpha$ with the set of maximal vertices $Y = \{x', y', z'\}$, where the corresponding labels are $\alpha(x') = 10000$, $\alpha(y') = 01000$ and $\alpha(z') = 00100$. Note also that ${}^{v^3}\beta(\alpha(x')) = 10011$, ${}^{v^3}\beta(\alpha(y')) = 01011$ and ${}^{v^3}\beta(\alpha(z')) = 00111$.

Let $u \in V(G)$ where $G = Q_h(X)$ and let X^u be the maximal subset of $\widehat{X}$ with the property $u \in \cap_{x\in X^u} I(0^h, x)$. Let G^u be the graph induced by the set $\cup_{x\in X^u} I(0^h, x)$, i.e. $G^u = G[\cup_{x\in X^u} I(0^h, x)]$. Note that by Lemma 3.1 and Lemma 2.1, G^u is a daisy cube of

Q_h and u is its minimal vertex. Observe for example the graph $Q_4(0111, 1011, 1101, 1110)$ on the right hand side of Figure 2: if $u = 1100$, then $X^u = \{1110, 1101\}$.

As noted in [12], an efficient way of finding a minimal vertex of a daisy cube G would give a linear time algorithm for finding a proper embedding of G. It was also shown that if G is a daisy cube of Q_h, then a minimal vertex of G is of degree h. It is not difficult to see that a vertex of degree h need not to be a minimal vertex of G. Note for example that Q_h^- (that is a vertex deleted Q_h) admits $2^h - h - 1$ vertices of degree h and exactly one minimal vertex (see also Figure 2, where Q_4^- is depicted).

Proposition 3.2. *Let $u \in V(G)$, where $G = Q_h(X)$ and $d(u) = h$. Moreover, let X^u be the maximal subset of $\widehat{X}$ such that $u \in \cap_{x\in X^u} I(0^h, x)$. Then for every proper embedding α, the minimal vertex of G with respect to α belongs to $\cap_{x\in X^u} I(0^h, x)$.*

Proof. Let v be the minimal vertex of G with respect to some proper embedding. Note that for every $x \in \widehat{X}$ and every $u \in I(0^h, x)$ we have $d(v, u) \leq |S^x|$. Suppose to the contrary that $v \notin \cap_{x\in X^u} I(0^h, x)$. It follows that there exists $x \in X^u$ such that $v \notin I(0^h, x)$. Since $u \in I(0^h, x)$, it follows that $S^u \subseteq S^x$. Moreover, since $v \notin I(0^h, x)$, there exists an index $j \notin S^x$ such that $v_j = 1$. It follows that the string u defined by

$$u_i = \begin{cases} \bar{v}_i, \ i \in S^x \\ 0, \ \text{otherwise} \end{cases}$$

is a vertex of $I(0^h, x)$ with $d(v, u) > |S^x|$ and we obtain a contradiction. □

Theorem 3.3. *If $G = Q_h(X)$ and $\hat{x} = \wedge_{x\in\widehat{X}} x$, then for every proper embedding α, v is the minimal vertex of G with respect to α if and only if $v \in \cap_{x\in\widehat{X}} I(0^h, x) = I(0^h, \hat{x})$.*

Proof. By Lemma 3.1 and Proposition 3.2, v is a minimal vertex of G, if and only if $v \in \cap_{x\in\widehat{X}} I(0^h, x)$. Note that $v \in \cap_{x\in\widehat{X}} I(0^h, x)$ if and only if $S^v \subseteq \cap_{x\in X} S^x$. Since $S^{\hat{x}} = \cap_{x\in X} S^x$, for every $v \in V(G)$ we have $v \in \cap_{x\in\widehat{X}} I(0^h, x)$ if and only if $v \leq \hat{x}$. It follows that $\cap_{x\in X} I(0^h, x) = I(0^h, \hat{x})$ and the assertion follows. □

4 Isometric embedding

If v is a vertex of a partial cube G, then $N_G^v(u)$ (or simply $N^v(u)$) is the set of neighbors of u which are closer to v than u, more formally $N_G^v(u) := \{z \mid z \in N(u) \text{ and } d(v, z) = d(v, u) - 1\}$,

If G is a graph isomorphic to a hypercube (but without an embedding), then its isometric embedding is easy to obtain as shown in the next result.

Proposition 4.1. *Let G be a graph isomorphic to a h-cube, v an arbitrary vertex of G and $\alpha : V(G) \to V(Q_h)$ a function such that $\alpha(v) = 0^d$, the vertices of $N(v)$ obtain pairwise different labels of the form $0^{i-1}10^{h-i}$, $i \in [h]$, while for the other vertices $u \in V(G)$ ordered by an increasing distance from v, we set $\alpha(u) = \vee_{z\in N^v(u)} \alpha(z)$. Then α is an isometric embedding of G into Q_h. Moreover, when a labeling of vertices in $N[v]$ is chosen, α is unique.*

Proof. Since a hypercube is vertex-transitive, we may choose an arbitrary vertex v of G and set $\alpha(v) = 0^h$. Moreover, for every $u \in V(G)$ with $d(v, u) = s$, $s \geq 1$, we must have $N^v(u) = \{z \mid \alpha_{(i)}(z) = \alpha_{(i)}(u) = 1$ for exactly one $i \in [h]$ and $\alpha_{(j)}(z) = \alpha_{(j)}(u)$ for every $j \in [h] \setminus \{i\}\}$. Thus, $\alpha(u) = \vee_{z \in N^v(u)} \alpha(z)$. It follows that for chosen labeling of vertices in $N[v]$, α is unique. $\square$

Lemma 4.2. *Let G be partial cube of isometric dimension h, u a vertex of degree h in G and let for every $v \in V(G) \setminus N[u]$ it holds that $|N^u(v)| \geq 2$. Define the function $\alpha : V(G) \to V(Q_h)$ such that $\alpha(u) = 0^h$, the vertices of $N(u)$ obtain pairwise different labels of the form $0^{i-1}10^{h-i}$, $i \in [h]$, while for the other vertices $v \in V(G)$ ordered by an increasing distance from u, we set $\alpha(v) = \vee_{z \in N^u(v)} \alpha(z)$. Moreover,*

(i) *α is an isometric embedding of G into Q_h,*

(ii) *when a fixed embedding of vertices in $N[v]$ is chosen, α is unique.*

Proof. Since G is a partial cube of dimension h, we may assume that G is an isometric subgraph of an (unlabeled) h-cube H. Let β be an embedding of H with respect to v as defined in Proposition 4.1 and let α be an embedding of G such that for every $z \in N[u]$ we set $\alpha(z) = \beta(z)$. Since $|N^u_G(v)| \geq 2$ and $N^u_G(v) \subseteq N^u_H(v)$ for every $v \in V(G) \setminus N[u]$, it follows that $\alpha(v) = \beta(v)$ for every vertex $v \in V(G)$. By Proposition 4.1, β is an isometric embedding of H into Q_h. Thus, α is an isometric embedding of H into Q_h. Moreover, by Proposition 4.1, α is unique for a fixed embedding of vertices in $N[v]$. $\square$

Corollary 4.3. *Let G be a graph isomorphic to a daisy cube of order h. If v is a minimal vertex of G and α an isometric embedding with $\alpha(v) = 0^h$, then α is proper.*

Proof. Since v is a minimal vertex of G, there exist a proper embedding, say β, such that $\beta(v) = 0^h$. We may also assume w.l.o.g. that for every $u \in N(v)$ we have $\beta(u) = \alpha(u)$. From Lemma 4.2 then it follows that $\beta(u) = \alpha(u)$ for every $v \in V(G)$. $\square$

Remark 4.4. If G is isomorphic to a daisy cube and α a proper embedding of G, then different selections of labels for vertices of $N(u)$ yield different but equivalent proper embeddings.

If G is a partial cube and α its isometric embedding to Q_h, let $W_i(G)$ denote the set of vertices of G with weight i, i.e. $W_i(G) = \{v \mid w(\alpha(v)) = i\}$.

We will also need the following result.

Proposition 4.5. *If G is a partial cube, α its isometric embedding to Q_h and $v \in V(G)$ such that $w(\alpha(v)) = i$, then $|N(v) \cap W_{i-1}(G)| \leq i$.*

Proof. Since α is isometric embedding of G to Q_h, for every $v \in V(G)$ with $w(\alpha(v)) = i$, we have $N_G(v) \subseteq N_{Q_h}(v)$. Moreover, $|N(v) \cap W_{i-1}(Q_h)| = i$ and therefore $|N(v) \cap W_{i-1}(G)| \leq i$. $\square$

Proposition 4.6. *Let $G = Q_h(X)$, $x, y \in \widehat{X}$ and $x \neq y$. If $u \in I(0^h, x)$ and $v \in I(0^n, y)$ such that $u, v \notin I(0^n, x) \cap I(0^h, y)$ then $uv \notin E(G)$.*

Proof. Suppose to the contrary that there exist $u \in I(0^h, x)$ and $v \in I(0^h, y)$ such that $u, v \notin I(0^h, x) \cap I(0^h, y)$ and $d(u, v) = 1$. Since $\widehat{X}$ is maximal, there exist at least two indices $i, j \in [h]$, such that $x_i \neq y_i$ and $x_j \neq y_j$ (otherwise we have either $x \leq y$ or $y \leq x$). Suppose w.l.o.g. $x_i = 1$, $y_j = 1$ and $u_k = v_k$ for every $k \in [h] \setminus \{i, j\}$. If $u_i = 0$ (resp. $v_j = 0$), then $u \in I(0^h, y)$ (resp. $v \in I(0^h, x)$). It follows that $u_i = v_j = 1$. But then $u = v$ and we obtain a contradiction. $\square$

Proposition 4.7. *Let $G = Q_h(X)$, X^u be the maximal subset of $\widehat{X}$ such that $u \in \cap_{x\in X^u} I(0^h, x)$ and $G^u = G[\cup_{x\in X^u} I(0^h, x)]$. If $u \in V(G)$ and $d(u) = h$, then $N(u) \subseteq V(G^u)$.*

Proof. Suppose to the contrary that there exists $v \in N(u)$ such that $v \notin \cup_{x\in X^u} I(0^h, x)$. It follows that there exists $y \in \widehat{X} - X^u$ such that $v \in I(0^h, y)$. Since $u \in I(0^h, x)$ for some $x \in \widehat{X}$ and $x \neq y$, Proposition 4.6 yields a contradiction. □

Proposition 4.8. *Let $G = Q_h(X)$, $u \in V(G)$ and X^u be the maximal subset of $\widehat{X}$ such that $u \in \cap_{x\in X^u} I(0^h, x)$. If $d(u) = h$, then $| \cup_{x\in X^u} S^x| = h$.*

Proof. Suppose $| \cup_{x\in X^u} S^x| < h$. It follows that there exist $j \in [h]$ such that for all $v \in \cup_{x\in X^u} I(0^h, x)$ we have $v_j = 0$. Since $d(u) = h$, there exists $z \in N(u)$ such that $z_j = 1$. It follows that $z \notin \cup_{x\in X^u} I(0^h, x)$. Thus, there exists $y \in \widehat{X} - X^u$ such that $v \in I(0^h, y)$. Proposition 4.7 yields a contradiction. □

Lemma 4.9. *Let $G = Q_h(X)$ and $u \in V(G)$ such that $d(u) = h$. Then $|N^u(v)| \geq 2$ for every $v \in V(G) \setminus N[u]$.*

Proof. Let X^u be the maximal subset of $\widehat{X}$ with the property $u \in \cap_{x\in X^u} I(0^h, x)$ and $G^u = G[\cup_{x\in X^u} I(0^h, x)]$. By Lemma 3.1 and Lemma 2.1, G^u is a daisy cube and u its minimal vertex. It follows that the lemma holds for every $v \in V(G^u)$. Suppose then that $v \notin \cup_{x\in X^u} I(0^h, x)$. Thus, there exists $y \in \widehat{X} - X^u$, such that $v \in I(0^h, y)$. Note that $S^u \subseteq \cap_{x\in X^u} S^x$.

Let $S^{u+} = \{i \,|\, u_i = 1 \text{ and } v_i = 0\}$ and $S^{u-} = \{i \,|\, v_i = 1 \text{ and } u_i = 0\}$.

We first show that $|S^{u-}| \neq 1$. Suppose to the contrary that there exists exactly one index $i \in [h] \setminus S^{u+}$, such that $v_i = 1$ and $u_i = 0$. Since $d(u) = h$, by Proposition 4.8, there exists $x \in X^u$ such that $x_i = 1$. Note also that $S^u \subseteq S^x$ and since $x_i = 1$, we have $S^v \subseteq S^x$. It follows that $v \leq x$ and we obtain a contradiction.

If $|S^{u+}| = 0$, then vertices of $I(u, v)$ induce a $|S^{u-}|$-cube in G. Thus, v admits $|S^{u-}|$ neighbors at distance $d(u, v) - 1$ from u. Clearly, $|S^{u+}| = 0$ implies $|S^{u-}| > 0$. Moreover, since we show above that $|S^{u-}| \neq 1$, we have $|S^{u-}| \geq 2$ and the case is settled.

If $|S^{u+}| > 0$, we may find $i, j \in S^{u-}$ such that $i \neq j$. Let z and z' be vertices obtained from v by setting the i-th and j-th coordinate to zero, respectively. Obviously, $z, z' \in N^u(v)$.

Since we show that we obtain $|N^u(v)| \geq 2$ for every value of $|S^{u+}|$, the lemma holds for every $v \in V(G) \setminus N[u]$. This assertion concludes the proof. □

Lemma 4.9 is the basis for the next algorithm which finds an isometric embedding for an unlabeled graph isomorphic to a daisy cube of dimension h.

Procedure Embedding(G, h, β, u);
1. u is a vertex of degree h in G;
2. $\beta(u) := 0^h$;
3. $i := 1$;
4. $Q := \emptyset$; $\{Q$ is an empty queue$\}$
5. **for all** $v \in V(G)$ **do** $p(v) := 0$;
6. **for all** $v \in N(u)$ **do begin**
   $\beta(v) := 0^{i-1}10^{h-i}$;

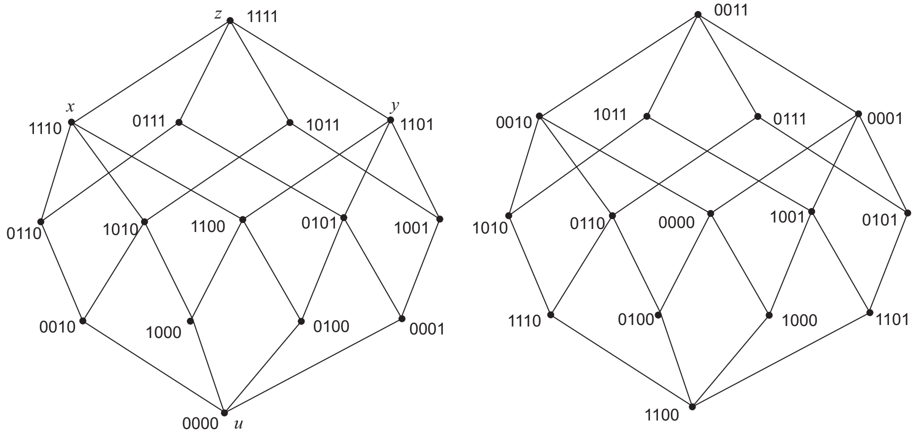


Figure 2: An isometric (left) and proper (right) embedding of a daisy cube isomorphic to Q_4^-.

$i := i + 1$;
$p(v) := u$;
Insert v in the end of Q;
end;
7. **while** $Q \neq \emptyset$ **do begin**
7.1 Remove the first vertex v from Q;
7.2. **for all** $z \in N(v)$ **do**
if $p(z) = 0$ **then begin**
$p(z) := v$;
Append z to the end of Q;
end
else $\beta(z) := \beta(v) \vee \beta(p(z))$;
end.

Theorem 4.10. *If G is a daisy cube, then an isometric embedding of G can be found in linear time.*

Proof. Note first that Lemma 4.2 defines the procedure to construct an isometric embedding of G into Q_h. Let α and β be isometric embeddings as defined in Lemma 4.2 and algorithm Embedding, respectively. Suppose that u is the vertex being labeled 0^h both by the algorithm and by the construction of Lemma 4.2. Clearly, for every v in $N[u]$ we could have $\alpha(v) = \beta(v)$. Note also that in the essence the algorithm performs a BFS search in G (see for example [4, Section 17.3]). Thus, for every $z \in N(v)$ of Step 7.2 we have $d(u, z) = d(u, p(z)) + 1 = d(u, v) + 1$. It follows that $v, p(z) \in N^u(z)$. By Lemma 4.9, since $d(u) = h$, for every $v \in V(G) \setminus N[u]$ we have $|N_G^u(v)| \geq 2$. Therefore, $\alpha(z) = \beta(z)$ for every $z \in V(G) \setminus N[u]$.

For the time complexity of the algorithm, note that the number of the executions of the body of the loop in Step 7.2 is bounded by the number of edges of a graph. Since the time complexity of the body of the loop is constant, the overall number of step of the algorithm is linear in the number of the edges of the graph. $\square$

5 Proper embedding

Lemma 5.1. *Let G be a daisy cube of Q_h, v a minimal vertex of G and u a vertex of degree h of G. If β is an isometric embedding of G such that $\beta(u) = 0^h$, then ${}^v\beta \circ \beta$ is a proper embedding of G.*

Proof. Note that ${}^v\beta(\beta(v)) = 0^h$. Since β is isometric, it is easy to see that ${}^v\beta \circ \beta$ is also isometric. Corollary 4.3 now yields the assertion. □

Let u be a vertex of degree h of $G = Q_h(X)$. Let X^u be the maximal subset of $\widehat{X}$ with the property $u \in \cap_{x \in X^u} I(0^h, x)$ and $G^u = G[\cup_{x \in X^u} I(0^h, x)]$. Recall that G^u is a daisy cube of Q_h and u its minimal vertex. If β is an isometric embedding of G such that $\beta(u) = 0^h$, let Y^u be the set of maximal vertices of G^u with respect to u and let Z^u be the set of vertices z of $V(G) \setminus V(G^u)$ with the property $N^u(z) = N(z)$.

Proposition 5.2. *Let u be a vertex of degree h of $G = Q_h(X)$. If β is an isometric embedding of G such that $\beta(u) = 0^h$, then $Y^u = \{y \mid \beta(y) = x \text{ and } x \in X^u\}$.*

Proof. As noted above, G^u is a daisy cube of Q_h and u its minimal vertex. Since u is of degree h and $\beta(u) = 0^h$, the restriction of β to $V(G^u)$ is a proper embedding of G^u. Moreover, since every permutation of indices of a proper embedding yields an equivalent embedding, we may assume w.l.o.g. that for every $z \in N(u)$ we have $\beta(z) = 0^{i-1}10^{h-i}$ if and only if $u_i \neq z_i$. It follows that for every $w \in N(0^h)$ we have ${}^u\beta(\beta(w)) = w$. By Lemma 3.1, ${}^u\beta \circ \beta$ is proper. Moreover, by Lemma 4.2, ${}^u\beta(\beta(v)) = v$ for every $v \in V(G^u)$. From Lemma 3.1 then follows that $Y^u = \{y \mid \beta(y) = x \text{ and } x \in X^u\}$. □

Proposition 5.3. *Let u be a vertex of degree h of $G = Q_h(X)$ and $z \in Z^u$. If β is an isometric embedding of G and $\beta(u) = 0^h$, then there exists $y \in \widehat{X} - X^u$ such that $z \in I(0^h, y)$. Moreover,*

$$\beta_{(i)}(z) = \begin{cases} 0, & i \in S^u \\ y_i, & i \notin S^u \end{cases}$$

Proof. Let X^u be the maximal subset of $\widehat{X}$ with the property $u \in \cap_{x \in X^u} I(0^h, x)$. By Lemma 2.1, since $z \notin \cup_{x \in X^u} I(0^h, x)$, there must be $y \in \widehat{X} - X^u$ such that $z \in I(0^h, y)$. By $N^u(z) = N(z)$, we have $d(u, z) \geq d(u, v)$ for every $v \in I(0^h, y)$. If $v_i = 1$ for some $i \in S^u$, then let v' be the vertex of G such that $v'_j = v_j$ for every $j \neq i$ and $v'_i = 0$. Obviously, $v' \leq y$, thus $v' \in I(0^h, y)$. Moreover, since $\beta_{(i)}(v') = 1$, we have $d(u, v') > d(u, v)$ and we obtain a contradiction. It follows that the assertion holds for every $i \in S^u$. If $i \notin S^u$, then $\beta_{(i)}(v) = v_i$ for every $v \in I(0^h, y)$. Since y is maximal in $I(0^h, y)$, the assertion follows. □

Theorem 5.4. *Let u be a vertex of degree h of $G = Q_h(X)$. If β is an isometric embedding of G such that $\beta(u) = 0^h$, $\hat{y} = \wedge_{y \in Y^u} \beta(y)$, $\hat{z} = \wedge_{z \in Z^u} \beta(z)(\wedge 1^h)$ and $v = \beta^{-1}(\hat{y} \wedge \hat{z})$, then v is the minimal vertex of G with respect to ${}^v\beta \circ \beta$.*

Proof. Note first that $\beta = \beta^{-1}$, thus, for every $b \in B^h$ and every $i \in [h]$ it holds

$$\beta_{(i)}(b) = \beta^{-1}_{(i)}(b) = \begin{cases} \bar{b}_i, & i \in S^u \\ b_i, & i \notin S^u \end{cases} \tag{5.1}$$

Let $\hat{x} = \wedge_{x \in X^u} x$. By Proposition 5.2, we have $Y^u = \{y \mid \beta(y) = x \text{ and } x \in X^u\}$. Thus, $\hat{x} = \hat{y}$. Note that by Proposition 3.2, every minimal vertex of G belongs to $I(0^h, \hat{x})$.

If $X^u = \widehat{X}$, then $Z^u = \emptyset$ and we get $\beta^{-1}(\hat{y} \wedge \hat{z}) = \beta^{-1}(\hat{y}) = \beta^{-1}(\hat{x})$. By equation (5.1), we have $\beta^{-1}(\hat{x}) \leq x$. It follows that $\beta^{-1}(\hat{x}) \in I(0^h, \hat{x})$ and we are done.

Otherwise, let $z \in Z^u$ be such that $z \in I(0^h, y)$ for some $y \in \widehat{X} - X^u$. We have to show that $\beta^{-1}(\hat{x} \wedge \beta(z))$ is a minimal vertex of $\cup_{x \in X^u} I(0^h, x) \cup I(0^h, y)$, i.e. $S^{\beta^{-1}(\hat{x} \wedge \beta(z))} \subseteq S^{\hat{x} \wedge y}$.

By Proposition 5.3, we have

$$\beta_{(i)}(z) = \begin{cases} 0, \ i \in S^u \\ y_i, \ i \notin S^u \end{cases}$$

Since $S^u \subseteq S^{\hat{x}}$, we have

$$(\hat{x} \wedge \beta(z))_i = \begin{cases} y_i, \ i \notin S^{\hat{x}} \setminus S^u \\ 0, \ \text{otherwise} \end{cases}$$

By equation (5.1), we have $\beta_i^{-1}(\hat{x} \wedge \beta(z)) = 0$ for every $i \in [h] \setminus S^{\hat{x} \wedge y}$. Since we can repeat the above discussion for every $z \in Z^u$, we showed that $\beta^{-1}(\hat{x} \wedge \hat{z}) = \beta^{-1}(\hat{y} \wedge \hat{z})$ is a minimal vertex of G. Moreover, since by Lemma 5.1 it follows that ${}^{\beta^{-1}(\hat{y} \wedge \hat{z})}\beta \circ \beta$ is a proper embedding of G, the proof is complete. □

Figure 2 shows two embeddings of a daisy cube G isomorphic to Q_4^-. The embedding β on the left hand side is determined such that $\beta(u) = 0000$ (note that $d(u) = 4$). Since u is not minimal in G, the embedding β is isometric but not proper. From $X^u = Y^u = \{x, y\}$ and $Z^u = \{z\}$ we get $\hat{y} = 1110 \wedge 1101 = 1100$, $\hat{z} = 1111$ and $\hat{y} \wedge \hat{z} = 1100 \wedge 1111 = 1100$. Moreover, the minimal vertex of G is $v = \beta^{-1}(1100)$ and ${}^v\beta \circ \beta$ is the proper embedding of G as described in Lemma 5.1. That is to say, we obtain the proper embedding of G by assigning $\beta(w) \oplus 1100$ to every $w \in V(G)$.

Theorem 5.4 is the basis for the next algorithm, which finds a proper embedding of a graph isomorphic to a daisy cube of dimension h.

Procedure Proper(G, h, α);
1. Embedding(G, h, β, u);
2. **for** $i := 1$ **to** $h + 1$ **do** $W_i := \emptyset$;
3. **for all** $v \in V(G)$ **do** $W_{w(\beta(v))} := W_{w(\beta(v))} \cup \{v\}$;
4. **for all** $v \in V(G)$ **do** $q(v) := 0$;
5. **for** $i := 1$ **to** h **do begin**
   5.1. **for all** $x \in W_i$ **do**
      5.1.1 **if** $\sum_{y \in N(x) \cap W_{i-1}} q(y) = i(i-1)$ **then begin**
         $q(x) := i$;
         for all $y \in N(x) \cap W_{i-1}$ **do** $q(y) := 0$;
      end
      5.1.2 **else if** $N(x) \cap W_{i+1} = \emptyset$ **then** $q(x) := i$
6. $s := 1^h$;
7. **for all** $v \in V(G)$ **do**
   7.1. **if** $q(v) \neq 0$ **then** $s := s \wedge \beta(v)$;
8. **for all** $v \in V(G)$ **do** $\alpha(v) := s \oplus \beta(v)$;

end.

Theorem 5.5. *A proper embedding of an unlabeled graph isomorphic to a daisy cube can be found in linear time.*

Proof. We first show that the algorithm Proper finds a proper embedding of G. As shown in Theorem 4.10, embedding β provided by the algorithm Embedding is isometric. With respect to Theorem 5.4 and Step 7, we have to show that if $q(v) \neq 0$, then either $v \in Y^u$ or $v \in Z^u$. Clearly, in Step 3, all vertices at distance i from u are inserted in W_i, while in Step 4, $q(v)$ is set to 0 for every $v \in V(G)$. The value of $q(v)$ is altered either in Step 5.1.1 or in Step 5.1.2.

Let $w(x) = i$. We show that $q(x) = i$ in the i-th iteration of for loop if and only if either $I(u,x)$ induces an i-cube or $x \in Z^u$. Note that $I(u,x)$ induces an i-cube, if and only $|N(x) \cap W_{i-1}| = i$ and for every $y \in N(x) \cap W_{i-1}$ the set $I(u,y)$ induces a $(i-1)$-cube. Moreover, if $x \in Y^u$, then $I(u,x)$ induces a maximal i-cube in G^u.

In the first iteration of Step 5, for every vertex of W_1 the value of q is set to 1. In the next iteration, when a vertex x of W_2 is considered, these values for two vertices of W_1, say y and y', are set to zero if $\{u, y, y', x\}$ induce a 2-cube. Thus, for every $x, y \in W_1 \cup W_2$ we have

- $q(y) = 1$ if and only if $x \in N(u)$ and there is no vertex $y \in W_2$ such that $I(u,y) \subseteq I(u,x)$ and $I(u,x)$ induces Q_2.

- $q(x) = 2$ if and only $I(u,x)$ induces Q_2.

Suppose now that for $i \geq 3$ and $y \in W_{i-1}$ it holds that $q(y) = i-1$ if and only if $I(u,y)$ induces a maximal cube in $G[W_1 \cup W_2 \ldots \cup W_{i-1}]$ or $N^u(y) = N(y)$; otherwise, $q(y) = 0$. Let $w(x) = i$. Note that $|N(x) \cap W_{i-1}| \leq i$ by Proposition 4.5. Thus, the condition of the if statement in Step 5.1.1 is fulfilled if and only if for every $y \in N(x) \cap W_{i-1}$ we have $q(y) = i - 1$, i.e. for every $y \in N(x) \cap W_{i-1}$ the set $I(u,y)$ induces an $(i-1)$-cube. If the condition of the if statement returns true, then $q(x)$ obtains the value i while for every $y \in N(x) \cap W_{i-1}$ the value of $q(y)$ is set to 0. If the condition of the if statement returns false, then $q(x)$ is set to i if and only if $N(x) \cap W_{i+1} = \emptyset$, i.e. $x \in Z^u$. Thus, we showed that in the i-th iteration of the for loop $q(x) = i$ if and only if either $I(u,x)$ induces an i-cube or $x \in Z^u$. Since the claim holds for every i, we showed that if $q(v) \neq 0$, $v \in V(G)$, then either $v \in Y^u$ or $v \in Z^u$. From Theorem 5.4 then it follows that the string s computed in Step 7 is equal to $\hat{y} \wedge \hat{z}$, where $\hat{y} = \wedge_{y \in Y^u} \beta(y)$ and $\hat{z} = \wedge_{z \in Z^u} \beta(z)$. By Theorem 5.4, $\beta^{-1}(s) = v$ is a minimal vertex of G while the embedding α obtained in Step 8 is equal to ${}^v\beta \circ \beta$. Moreover, α is proper by Lemma 5.1.

In order to consider the time complexity of the algorithm, note first that all steps of the algorithm except Step 5 can be executed in $O(m)$ time, where m is the number of edges of G. For the time complexity of Step 5 it is convenient to store the weights of vertices in a vector, which allows that the weight of a vertex and therefore its inclusion in a set W_i can be determined in constant time. Thus, the time complexity of Steps 5.1.1 and 5.1.2 is linear in the number of edges incident with the vertex x. Since Step 5 is performed for every vertex of the graph, the total number of steps is bounded by the number of edges of G. This assertion concludes the proof. □

ORCID iDs

Aleksander Vesel https://orcid.org/0000-0003-3705-0071

References

[1] M. Aïder, S. Gravier and K. Meslem, Isometric embeddings of subdivided connected graphs into hypercubes, *Discrete Math.* **309** (2009), 6402–6407, doi:10.1016/j.disc.2008.10.030.

[2] J. Azarija, S. Klavžar, Y. Rho and S. Sim, On domination-type invariants of Fibonacci cubes and hypercubes, *Ars Math. Contemp.* **14** (2018), 387–395, doi:10.26493/1855-3974.1172.bae.

[3] P. Codara and O. M. D'Antona, Generalized Fibonacci and Lucas cubes arising from powers of paths and cycles, *Discrete Math.* **339** (2016), 270–282, doi:10.1016/j.disc.2015.08.012.

[4] R. Hammack, W. Imrich and S. Klavžar, *Handbook of product graphs*, Discrete Mathematics and its Applications (Boca Raton), CRC Press, Boca Raton, FL, 2nd edition, 2011, with a foreword by Peter Winkler.

[5] W.-J. Hsu, Fibonacci cubes-a new interconnection topology, *IEEE Trans. Parallel Distr. Systems* **4** (1993), 3–12, doi:10.1109/71.205649.

[6] W. J. Hsu and M. J. Chung, Generalized fibonacci cubes, in: *1993 International Conference on Parallel Processing - ICPP'93*, volume 1, 1993 pp. 299–302, doi:10.1109/icpp.1993.95.

[7] A. Ilić, S. Klavžar and Y. Rho, Generalized Fibonacci cubes, *Discrete Math.* **312** (2012), 2–11, doi:10.1016/j.disc.2011.02.015.

[8] A. Ilić and M. Milošević, The parameters of Fibonacci and Lucas cubes, *Ars Math. Contemp.* **12** (2017), 25–29, doi:10.26493/1855-3974.915.f48.

[9] S. Klavžar and M. Mollard, Daisy cubes and distance cube polynomial, *European J. Combin.* **80** (2019), 214–223, doi:10.1016/j.ejc.2018.02.019.

[10] H. M. Mulder, *The interval function of a graph*, volume 132 of *Mathematical Centre Tracts*, Mathematisch Centrum, Amsterdam, 1980.

[11] E. Saygı, On the domination number and the total domination number of Fibonacci cubes, *Ars Math. Contemp.* **16** (2019), 245–255, doi:10.26493/1855-3974.1591.92e.

[12] A. Taranenko, Daisy cubes: a characterization and a generalization, *European J. Combin.* **85** (2020), 103058, 10, doi:10.1016/j.ejc.2019.103058.

[13] A. Vesel, Cube-complements of generalized Fibonacci cubes, *Discrete Math.* **342** (2019), 1139–1146, doi:10.1016/j.disc.2019.01.008.

[14] P. Žigert Pleteršek, Resonance graphs of kinky benzenoid systems are daisy cubes, *MATCH Commun. Math. Comput. Chem.* **80** (2018), 207–214.

[15] J. Wei, Y. Yang and G. Wang, Circular embeddability of isometric words, *Discrete Math.* **343** (2020), 112024, 11, doi:10.1016/j.disc.2020.112024.

[16] P. M. Winkler, Isometric embedding in products of complete graphs, *Discrete Appl. Math.* **7** (1984), 221–225, doi:10.1016/0166-218x(84)90069-6.

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.08 / 283–299
https://doi.org/10.26493/1855-3974.2398.7d5
(Also available at http://amc-journal.eu)

The polynomial method for list-colouring extendability of outerplanar graphs

Przemysław Gordinowicz *, Paweł Twardowski

Institute of Mathematics, Lodz University of Technology, Al. Politechniki 10, Łódź, Poland

Received 3 August 2020, accepted 28 June 2021, published online 25 October 2021

Abstract

We restate theorems of Hutchinson [4] on list-colouring extendability for outerplanar graphs in terms of non-vanishing monomials in a graph polynomial, which yields an Alon-Tarsi equivalent for her work. This allows to simplify her proofs as well as obtain more general results.

Keywords: Outerplanar graph, list colouring, paintability, Alon-Tarsi number.

Math. Subj. Class. (2020): 05C10, 05C15, 05C31

1 Introduction

In his famous paper [8] Thomassen proved that every planar graph is 5-choosable. Actually, to proceed with an inductive argument, he proved the following stronger result.

Theorem 1.1 ([8]). *Let G be any plane near-triangulation (every face except the outer one is a triangle) with outer cycle C. Let x, y be two consecutive vertices on C. Then G can be coloured from any list of colours such that the length of lists assigned to x, y, any other vertex on C and any inner vertex is 1, 2, 3, and 5, respectively.*

In other words vertices x and y can be precoloured in different colours. Basically, this theorem implies that any outerplanar graph is 3-choosable. Moreover, lists of any two neighbouring vertices can have a deficiency. To formalise this fact we say that a triple (G, x, y), where G is outerplanar graph, $x, y \in V(G)$ are neighbouring vertices is $(1, 2)$-*extendable* in the sense that G is colourable from any lists whose length is 1, 2 and 3 for vertex x, y and any other vertex, respectively.

*Corresponding author.
E-mail addresses: pgordin@p.lodz.pl (Przemysław Gordinowicz), pawel.twardowski@dokt.p.lodz.pl (Paweł Twardowski)

Hutchinson [4] analysed extendability of outerplanar graphs, in the case when the selected vertices are not adjacent, showing that for any two vertices x, y of outerplanar graph G a triple (G, x, y) is $(2, 2)$-extendable. Of course, it is enough to prove this for outerplane 2-connected near-triangulation only, as each outerplane graph can be extended to such a graph just by adding some edges. The main theorem was the following.

Theorem 1.2 ([4]). *Let G be outerplane 2-connected near-triangulation and $x, y \in V(G)$, $x \neq y$. Let $C\colon V(G) \to \{1, 2, 3\}$ be any proper 3-colouring of G. Then*

(i) (G, x, y) *is not* $(1, 1)$*-extendable;*

(ii) (G, x, y) *is* $(1, 2)$*-extendable if and only if* $C(x) \neq C(y)$*;*

(iii) (G, x, y) *is* $(2, 2)$*-extendable.*

Indeed, it is enough to prove the above theorem for near-triangulations with exactly 2 vertices of degree 2 and to let x and y be these degree 2 vertices. Hutchinson called such configurations *fundamental subgraphs*. Such a configuration can be obtained by successively shrinking the outerplane near-triangulation along some chord (inner edge) that separates the component of the graph not containing vertices x and y (in case when $xy \in E(G)$ this reduces to an edge xy). The general result follows now by succesive colouring of shrank parts using Theorem 1.1 — the chord is an outer edge of the shrank component and its endpoins (already coloured) are these 2 precoloured vertices. The details are in [4]. Also in [4], Hutchinson provided further results about extendability of general outerplanar graphs, for which the conditions are more relaxed than those of Theorem 1.2, allowing for $(1, 1)$-extendability.

One important thing is that the proper 3-colouring C mentioned in the theorem above is not in any way connected to possible list colouring of G, but is rather an inherent property of the graph. This is due to the fact that every 2-connected outerplane near triangulation has an unique (up to permutation) 3-colouring, i.e the vertices graph can be uniquely partitioned into 3 groups so that in every proper 3-colouring of the graph the vertices in the same group will always have the same colour (the groups in this partition are called *colour classes*, as the partition defines an equivalence relation). The reason for this is that the graph consists entirely of triangles, and every vertex of a given triangle needs to be of different colour.

The situation of particular importance is when two vertices are in the same colour class. This can be forced in two ways. One, mentioned in [4], is the so called *chain of diamonds*, where the diamond is understood as K_4 minus an edge. It is obviously a 2-connected outerplane near triangulation, and the two non-neighbouring vertices are always of the same colour. Therefore is we link diamonds together glueing them by the vertices of degree 2, each of the linking vertices will have the same colour. The second way is to attach a diamond to diamond along the common edge (cf. [6]). Both of those ways can be seen on Figure 1.

Recently, Zhu [10] strengthened the theorem of Thomassen in the language of graph polynomials showing that Alon-Tarsi number of any planar graph G satisfies $AT(G) \leq 5$. His approach utilizes a certain polynomial arising directly from the structure of the graph. This *graph polynomial* is defined as:

$$P(G) = \prod_{uv \in E(G), u<v} (u - v),$$

where the relation $<$ fixes an arbitrary orientation of graph G. Here we understand u and v both as the vertices of G and variables of $P(G)$, depending on the context. Notice that the orientation affects the sign of the polynomial only. Therefore individual monomials and the powers of the variables in each monomials are orientation-invariant. We refer the reader to [1, 2, 7] for the connection between list colourings and graph polynomials. The approach of Zhu may be described in the following form, analogous to Theorem 1.1.

Theorem 1.3 ([10]). *Let G be any plane near-triangulation, let $e = xy$ be a boundary edge of G. Denote other boundary vertices by $v_1, \ldots, v_k$ and inner vertices by $u_1, \ldots, u_m$. Then the graph polynomial of $G - e$ contains a non-vanishing monomial of the form $\eta x^0 y^0 v_1^{\alpha_1} \ldots v_k^{\alpha_k} u_1^{\beta_1} \ldots u_m^{\beta_m}$ with $\alpha_i \leq 2, \beta_j \leq 4$ for $i \leq k$, $j \leq m$.*

The main tool connecting graph polynomials with list colourings is Combinatorial Nullstellensatz [1]. It implies that for every non-vanishing monomial of $P(G)$, if we assign to each vertex of G a list of length greater than the exponent of corresponding variable in that monomial, then such list assignment admits a proper colouring.

We note that this approach can be continued, allowing one to obtain stronger equivalents of already known results for list-colouring. Moreover, in [3] where it is proven that every planar graph G contains a matching M such that $AT(G-M) \leq 4$, one can find an example that with this approach it is possible to get results that are not known (or hard to prove) for ordinary list colouring.

In this paper we provide a graph polynomial analogue to the result of Hutchinson, obtaining a characterisation of polynomial extendability for outerplanar graphs, which may be presented in the form of the following theorem.

Theorem 1.4. *Let G be any outerplanar graph with $V(G) = \{x, y, v_1, \ldots, v_n\}$. Then in $P(G)$ there is a non-vanishing monomial of the form $\eta x^\beta y^\gamma \prod_{i=1}^n v_i^{\alpha_i}$ with $\alpha_i \leq 2$, $\beta, \gamma \leq 1$ satisfying:*

(i) $\beta = \gamma = 1$ *when every proper* 3*-colouring C of G forces $C(x) = C(y)$;*

(ii) $\beta + \gamma = 1$ *when every proper* 3*-colouring C of G forces $C(x) \neq C(y)$;*

(iii) $\beta = \gamma = 0$ *otherwise.*

We note that our proofs are simpler than the ones of Hutchinson, which show the strength of the graph polynomial method for graph colouring problems. All considered graphs are simple, undirected, and finite. For background in graph theory see [9].

2 Outerplane near-triangulations

In this section we provide a graph polynomial analogue to Theorem 1.2. The main tool is the following theorem.

Theorem 2.1. *Let G be a triangle or any* 2*-connected, outerplane near-triangulation with exactly two vertices of degree 2. Let $z \in V(G)$ be any neighbour of a degree 2 vertex. Denote $V(G) = \{x, y, z, v_1, \ldots, v_n\}$, where $deg(x) = deg(y) = 2$, $yz \in E(G)$, $y, z \neq x$. Then*

$$P(G) = Q(G) + \eta_1 x v_1^2 \ldots v_n^2 y^0 z^2 + \eta_2 x v_1^2 \ldots v_n^2 y^1 z^1 + \eta_3 x v_1^2 \ldots v_n^2 y^2 z^0,$$

where $\{\eta_1, \eta_2, \eta_3\} = \{-1, 0, 1\}$, while $Q(G)$ is a sum of monomials of the form $\eta x^{\alpha_x} v_1^{\alpha_1} \ldots v_n^{\alpha_n} y^{\alpha_y} z^{\alpha_z}$, $\eta \neq 0$, with $(\alpha_x, \alpha_1, \ldots, \alpha_n) \neq (1, 2, \ldots, 2)$.

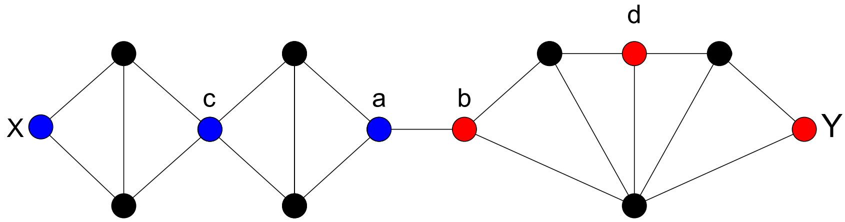


Figure 1: An example of a graph satisfying conditions of point $ii)$ of Theorem 1.4. When 3-colouring the graph, vertices a and b need to be in different colours. Vertices x and c are in the same colour class as a (an example of the chain of diamonds), while y and d are in the same colour class as b (the diamonds are linked along an edge). Therefore x and y have different colours in every proper 3-colouring of the graph. The black vertices are yet to be coloured.

Proof. The proof is done by induction on n. For the base step $(n = 0)$, let G be a triangle on vertices $\{x, y, z\}$. It is easy to check, that:

$$\begin{aligned} P(G) &= (x-y)(y-z)(x-z) \\ &= x^2y^1z^0 - x^2y^0z^1 + x^1y^0z^2 - x^1y^2z^0 + x^0y^2z^1 - x^0y^1z^2 \\ &= Q(G) + x^1y^0z^2 - x^1y^2z^0, \end{aligned}$$

hence we have $\eta_2 = 0$ and $\{\eta_1, \eta_3\} = \{1, -1\}$, and with $Q(G)$ having necessary form, G is concordant with the assertion.

We now proceed with the induction. Let $n \in \mathbb{N}$ and suppose the theorem holds for graphs on at most $n + 3$ vertices. Let G' be any 2-connected, outerplane near-triangulation on $n + 4$ vertices and $x, y \in V(G')$ be the only two vertices of degree 2. Notice that x and y cannot be adjacent (their common neighbour would then be a cutvertex, thus violating 2-connectivity). Let z and v_{n+1} be the neighbours of y. There is $deg(z), deg(v_{n+1}) \geq 3$ and (because G' is triangulated) $zv_{n+1} \in E(G')$. Now consider $G = G' - y$. Note that G remains 2-connected outerplane near-triangulation. As outerplanar graph should have at least 2 vertices of degree at most 2, one of neighbours of y has now degree 2. Let us name it $\tilde{\mathrm{y}}$, while the second one — $\tilde{\mathrm{z}}$. Notice that due to triangularity and 2-connectiveness, we have $deg(\tilde{\mathrm{z}}) > 2$ (with an exception when G is a triangle), as $\tilde{\mathrm{y}}$ and $\tilde{\mathrm{z}}$ have a common neighbour. Now, we may consider $P(G)$ using the inductive assumption. There are three possible cases:

1. $\tilde{\eta}_1 = 0$. As $\tilde{\eta}_1 = 0$ and $\{\tilde{\eta}_2, \tilde{\eta}_3\} = \{-1, 1\}$, we know that:

$$\begin{aligned} P(G) &= Q(G) + \tilde{\eta}_2 x v_1^2 \ldots v_n^2 \tilde{\mathrm{y}}^1 \tilde{\mathrm{z}}^1 + \tilde{\eta}_3 x v_1^2 \ldots v_n^2 \tilde{\mathrm{y}}^2 \tilde{\mathrm{z}}^0 \\ &= Q(G) + \tilde{\eta}_2 x v_1^2 \ldots v_n^2 \tilde{\mathrm{y}}^1 \tilde{\mathrm{z}}^1 - \tilde{\eta}_2 x v_1^2 \ldots v_n^2 \tilde{\mathrm{y}}^2 \tilde{\mathrm{z}}^0 \\ &= Q(G) + \tilde{\eta}_2 x v_1^2 \ldots v_n^2 (\tilde{\mathrm{y}}^1 \tilde{\mathrm{z}}^1 - \tilde{\mathrm{y}}^2 \tilde{\mathrm{z}}^0). \end{aligned}$$

Now, $P(G') = P(G)(\tilde{y} - y)(\tilde{z} - y) = P(G)(\tilde{y}\tilde{z} - \tilde{y}y - \tilde{z}y + y^2)$, thus:

$$\begin{aligned} P(G') &= (Q(G) + \tilde{\eta}_2 x v_1^2 \dots v_n^2(\tilde{y}^1\tilde{z}^1 - \tilde{y}^2\tilde{z}^0))(\tilde{y}\tilde{z} - \tilde{y}y - \tilde{z}y + y^2) \\ &= Q(G)(\tilde{y}\tilde{z} - \tilde{y}y - \tilde{z}y + y^2) + \tilde{\eta}_2 x v_1^2 \dots v_n^2(\tilde{y}^2\tilde{z}^2 y^0 - \tilde{y}^2\tilde{z}^1 y^1 - \\ &\qquad - \tilde{y}^1\tilde{z}^2 y^1 + \tilde{y}^1\tilde{z}^1 y^2 - \tilde{y}^3\tilde{z}^1 + \tilde{y}^3 y^1 + \tilde{y}^2\tilde{z}^1 y^1 - \tilde{y}^2\tilde{z}^0 y^2) \\ &= Q'(G') + \tilde{\eta}_2 x v_1^2 \dots v_n^2(\tilde{y}^2\tilde{z}^2 y^0 - \tilde{y}^1\tilde{z}^2 y^1 - \tilde{y}^2\tilde{z}^0 y^2) \end{aligned}$$

Now either $z = \tilde{y}$ and $v_{n+1} = \tilde{z}$, respectively, or the inverse may occur. In the first case, we have:

$$P(G') = Q'(G') + \tilde{\eta}_2 x v_1^2 \dots v_n^2(v_{n+1}^2 y^0 z^2 - v_{n+1}^2 y^1 z^1 - v_{n+1}^0 y^2 z^2),$$

thus $\{\eta_1, \eta_2\} = \{-1, 1\}$ and $\eta_3 = 0$, with the last monomial going into $Q'(G')$. With analogous calculations, in the second case we have $\{\eta_1, \eta_3\} = \{-1, 1\}$ and $\eta_2 = 0$. As $Q'(G')$ obviously contains only monomials of the form $\eta x^{\alpha_x} v_1^{\alpha_1} \dots v_{n+1}^{\alpha_{n+1}} y^{\alpha_y} z^{\alpha_z}$, $\eta \neq 0$, $(\alpha_x, \alpha_1, \dots, \alpha_{n+1}) \neq (1, 2, \dots, 2)$, it can assume the role of $Q(G)$, and the case is finished.
2. $\tilde{\eta}_2 = 0$. As $\tilde{\eta}_2 = 0$ and $\{\tilde{\eta}_1, \tilde{\eta}_3\} = \{-1, 1\}$, we know that:

$$\begin{aligned} P(G) &= Q(G) + \tilde{\eta}_1 x v_1^2 \dots v_n^2 \tilde{y}^0\tilde{z}^2 + \tilde{\eta}_3 x v_1^2 \dots v_n^2 \tilde{y}^2\tilde{z}^0 \\ &= Q(G) + \tilde{\eta}_1 x v_1^2 \dots v_n^2 \tilde{y}^0\tilde{z}^2 - \tilde{\eta}_1 x v_1^2 \dots v_n^2 \tilde{y}^2\tilde{z}^0 \\ &= Q(G) + \tilde{\eta}_1 x v_1^2 \dots v_n^2(\tilde{y}^0\tilde{z}^2 - \tilde{y}^2\tilde{z}^0). \end{aligned}$$

And then:

$$\begin{aligned} P(G') &= (Q(G) + \tilde{\eta}_1 x v_1^2 \dots v_n^2(\tilde{y}^0\tilde{z}^2 - \tilde{y}^2\tilde{z}^0))(\tilde{y}\tilde{z} - \tilde{y}y - \tilde{z}y + y^2) \\ &= Q(G)(\tilde{y}\tilde{z} - \tilde{y}y - \tilde{z}y + y^2) + \tilde{\eta}_1 x v_1^2 \dots v_n^2(\tilde{y}^1\tilde{z}^3 y^0 - \tilde{y}^1\tilde{z}^2 y^1 - \tilde{y}^0\tilde{z}^3 y^1 + \\ &\qquad + \tilde{y}^0\tilde{z}^2 y^2 - \tilde{y}^3\tilde{z}^1 y^0 + \tilde{y}^3\tilde{z}^0 y^1 + \tilde{y}^2\tilde{z}^1 y^1 - \tilde{y}^2\tilde{z}^0 y^2) \\ &= Q'(G') + \tilde{\eta}_1 x v_1^2 \dots v_n^2(\tilde{y}^0\tilde{z}^2 y^2 - \tilde{y}^1\tilde{z}^2 y^1 - \tilde{y}^2\tilde{z}^0 y^2 + \tilde{y}^2\tilde{z}^1 y^1) \end{aligned}$$

Continuing as in case 1, when $z = \tilde{y}$ and $v_{n+1} = \tilde{z}$, respectively, we have $\{\eta_2, \eta_3\} = \{-1, 1\}$ and $\eta_1 = 0$. In the inverse case, when $v_{n+1} = \tilde{y}$ and $z = \tilde{z}$, there is $\{\eta_2, \eta_3\} = \{1, -1\}$ and $\eta_1 = 0$. $Q'(G')$ can again assume the role of $Q(G)$, and this case is also done.
3. $\tilde{\eta}_3 = 0$. This case is handled analogously as $\tilde{\eta}_1 = 0$, interchanging the roles of $\tilde{y}$ and $\tilde{z}$. Here we have:

$$\begin{aligned} P(G) &= Q(G) + \tilde{\eta}_1 x v_1^2 \dots v_n^2 \tilde{y}^0\tilde{z}^2 + \tilde{\eta}_2 x v_1^2 \dots v_n^2 \tilde{y}^1\tilde{z}^1 \\ &= Q(G) + \tilde{\eta}_2 x v_1^2 \dots v_n^2 \tilde{y}^1\tilde{z}^1 - \tilde{\eta}_2 x v_1^2 \dots v_n^2 \tilde{y}^0\tilde{z}^2 \\ &= Q(G) + \tilde{\eta}_2 x v_1^2 \dots v_n^2(\tilde{y}^1\tilde{z}^1 - \tilde{y}^0\tilde{z}^2). \end{aligned}$$

And then:

$$\begin{aligned} P(G') &= (Q(G) + \tilde{\eta}_2 x v_1^2 \dots v_n^2(\tilde{y}^1\tilde{z}^1 - \tilde{y}^0\tilde{z}^2))(\tilde{y}\tilde{z} - \tilde{y}y - \tilde{z}y + y^2) \\ &= Q(G)(\tilde{y}\tilde{z} - \tilde{y}y - \tilde{z}y + y^2) + \tilde{\eta}_2 x v_1^2 \dots v_n^2(\tilde{y}^2\tilde{z}^2 y^0 - \tilde{y}^2\tilde{z}^1 y^1 - \tilde{y}^1\tilde{z}^2 y^1 + \\ &\qquad + \tilde{y}^1\tilde{z}^1 y^2 - \tilde{y}^1\tilde{z}^3 + \tilde{y}^1\tilde{z}^2 y^1 + \tilde{z}^3 y^1 - \tilde{y}^0\tilde{z}^2 y^2) \\ &= Q'(G') + \tilde{\eta}_2 x v_1^2 \dots v_n^2(\tilde{y}^2\tilde{z}^2 y^0 - \tilde{y}^2\tilde{z}^1 y^1 - \tilde{y}^0\tilde{z}^2 y^2) \end{aligned}$$

Finally, when $z = \tilde{y}$ and $v_{n+1} = \tilde{z}$, respectively, we have $\{\eta_1, \eta_3\} = \{-1, 1\}$ and $\eta_2 = 0$. In the inverse case, when $v_{n+1} = \tilde{y}$ and $z = \tilde{z}$, there is $\{\eta_1, \eta_2\} = \{-1, 1\}$ and $\eta_3 = 0$.

Therefore, in each case we have the desired form of the polynomial, thus completing the inductive argument. □

Recall that by Combinatorial Nullstellensatz, (i, j)-extendability of (G, x, y) can be expressed as the fact that there is a non-vanishing monomial in $P(G)$ where exponents of x and y are $i-1$ and $j-1$, respectively, and every other exponent is less than 3. We obtain an analogue to Theorem 1.2 as the following

Corollary 2.2. *Let G be any 2-connected, outerplane near-triangulation with $V(G) = \{x, y, v_1, \ldots, v_n\}$. Let $C\colon V(G) \to \{1, 2, 3\}$ be any proper 3-colouring of G. Then in the graph polynomial $P(G)$*

(i) *there is no monomial of the form $\eta x^0 y^0 \prod_{i=1}^n v_i^{\alpha_i}$ with $\alpha_i \leq 2$;*

(ii) *the monomial of the form $\eta x^1 y^0 \prod_{i=1}^n v_i^{\alpha_i}$ with $\alpha_i \leq 2$ does not vanish if and only if $C(x) \neq C(y)$;*

(iii) *there is non-vanishing monomial of the form $\eta x^\beta y^\gamma \prod_{i=1}^n v_i^{\alpha_i}$ with $\alpha_i \leq 2$, $\beta, \gamma \leq 1$.*

Proof. For the first point, simply note that outerplane near-triangulation on $n+2$ vertices has $2n+1$ edges, while the sum of the exponents of the given monomial is at most $2n$.

For the second point and for the third one: when x and y are adjacent one may apply Theorem 1.3 directly; otherwise, by the Hutchinson's shrinking argument it is enough to verify an existence of a suitable monomial for G having exactly 2 vertices of degree 2, when x and y are these vertices.

Indeed, suppose otherwise and consider any chord (inner edge) ab of G that separates the component H of the graph not containing vertices x and y. Such a chord exists, unless x and y are the only degree 2 vertices of G. Let $G_1 = G[V(G) \setminus V(H)]$ and $G_2 = G[V(H) \cup \{a, b\}]$. By Theorem 1.3 $P(G_2 - ab)$ contains non-vanishing monomial of the form $s_2 = \eta a^0 b^0 v_1^{\alpha_1} \ldots v_k^{\alpha^k}$ with $\alpha_i \leq 2$. Note, that common variables in $P(G_1)$ and $P(G_2 - ab)$ are a and b only and that the sum of the exponents in any monomial in $P(G_2 - ab)$ is fixed. Hence, any other monomial in $P(G_2 - ab)$ has different exponents for some of $v_1, \ldots v_k$. Therefore, as there is $P(G) = P(G_1)P(G_2 - ab)$, G with x and y satisfies the second (or the third one, respectively) point of the corollary if and only if G_1 with x and y does. Actually, the existence of desired monomials s in $P(G)$ and s_1 in $P(G_1)$, respectively, is equivalent by identity $s = s_1 s_2$.

Repeating the above argument until there is no separating chord one can shrink G to the claimed form. By Theorem 2.1 this finishes the proof of the third point as then one has either $\eta_1 \neq 0$ or $\eta_2 \neq 0$. For the second point it is enough to notice that under the assumption of Theorem 2.1 there is $\eta_1 = 0$ if and only if $C(x) = C(y)$. Note that there is also $\eta_3 = 0$ if and only if $C(z) = C(x)$ and then $\eta_2 = 0$ if and only if x, y and z have 3 different colours. One may prove this fact by a simple analysis of the inductive step in the proof of Theorem 2.1.

Indeed, in the base case (a triangle xyz) we have $\eta_2 = 0$. Further, when G is extended to G' by a triangle $\tilde{y}\tilde{z}y$ then

1. $\tilde{\eta}_1 = 0$ ($C(\tilde{y}) = C(x)$) forces $\eta_3 = 0$ (when $z = \tilde{y}$) or $\eta_2 = 0$ (when $z = \tilde{z}$),

2. $\tilde{\eta}_2 = 0$ forces $\eta_1 = 0$ ($C(x) = C(y)$),
3. $\tilde{\eta}_3 = 0$ ($C(\tilde{z}) = C(x)$) forces $\eta_3 = 0$ (when $z = \tilde{z}$) or $\eta_2 = 0$ (when $z = \tilde{y}$). □

3 Poly-extendability of general outerplanar graphs

The results of the previous section can be of course applied to any outerplanar graph, not necessarily triangulated. This, however, leads to loss of information, as usually there is more than one way to triangulate the graph, and different triangulations may lead to different types of extendability. Moreover, in the case of non-triangulated graphs, as well as those that are not 2-connected, the counting argument behind point (i) of Corollary 2.2 does not work any more. Hence, it is possible for a general outerplanar graph to be $(1, 1)$-extendable. At first, a formal definition of fundamental subgraphs is provided, followed by three instrumental lemmas.

Definition 3.1. Let G be a 2-connected outerplane graph, $x, y \in V(G)$ and let $T(G)$ be the weak dual of G. The *fundamental* $x - y$ *subgraph of* G is the subgraph of G induced by the vertices belonging to faces that have vertices representing them in $T(G)$ lying on the shortest path between vertices representing faces on which x and y lie. If $xy \in E(G)$, then the fundamental subgraph reduces to an edge xy.

Here, the assumption that the graph is outerplane is needed, as the construction of weak dual requires a particular embedding to be chosen. Notice however that in case of 2-connected outerplanar graphs there is, up to isomorphism, just one outerplane embedding, hence every 2-connected outerplanar graphs has essentially a single weak dual. Therefore in the rest of the paper we will assume the graphs to be outerplanar, as the choice of an embedding is irrelevant for our purpose.

Definition 3.2. Let G be a connected outerplanar graph with cutvertices, and let $BC(G)$ be the block-cutvertex graph of G. Let $x, y \in V(G)$ be vertices lying in two different blocks of G. The fundamental $x - y$ subgraph of G consists of all blocks that have vertices representing them in $BC(G)$ lying on the shortest path between vertices representing blocks containing x and y, and each of those blocks is restricted to the fundamental $a - b$ subgraph, where $a, b \in V(G)$ are the two cutvertices belonging to the given block and to the shortest path between blocks containing x and y in $BC(G)$.

Definition 3.3. An outerplanar graph G with $x, y \in V(G)$ is *xy-fundamental* if its fundamental $x - y$ subgraph is equal to G. An outerplanar graph G is *fundamental* if it is xy-fundamental for some $x, y \in V(G)$.

Lemma 3.4. *Let G be a 2-connected xy-fundamental near-triangulation, such that $C(x) = C(y)$, where $C\colon V(G) \to \{1, 2, 3\}$ is any proper 3-colouring of G. Let v_0 be the vertex of G that has degree 2 in $G - y$, and $v_1, \dots, v_n$ be the remaining vertices. Then in $P(G)$ there is a non-vanishing monomial of the form $\eta x^0 y^2 v_0^1 v_1^2 \dots v_n^2$, with $\eta \in \{-1, 1\}$.*

Proof. As $C(x) = C(y)$, then $C(x) \neq C(v_0)$. Hence by the second case of Corollary 2.2, there is a non-vanishing monomial $\eta x^0 v_0^1 v_1^2 \dots v_n^2$, with $\eta \in \{-1, 1\}$ in $P(G - y)$. Adding y back, thus multiplying $P(G - y)$ by $(y - v_0)(y - v_n) = y^2 - yv_0 - yv_n + v_0 v_n$, we get the monomial specified in the statement, and as it is the only way to obtain it, it is non-vanishing. □

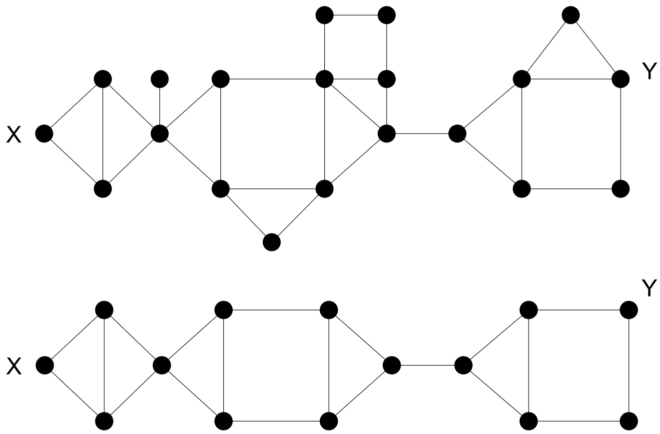


Figure 2: Top: a connected, outerplanar graph G; Bottom: a fundamental $x - y$ subgraph of G.

Lemma 3.5. *Let G, G' be any two graphs, such that $V(G) = \{x, v_1, \dots, v_n\}$, $V(G') = \{x', u_1, \dots, u_m\}$. Let G'' be the graph obtained from G and G' by identifying x with x', thus creating vertex x'', and carrying neighbouring relations from G, G'. Suppose there are non-vanishing monomials $\eta x^{\alpha} \Pi v_i^{\alpha_i}$ and $\eta' x'^{\beta} \Pi u_j^{\beta_j}$ in $P(G)$ and $P(G')$ respectively. Then in $P(G'')$ there is a non-vanishing monomial $A(G'') = \eta\eta' x''^{\alpha+\beta} \Pi v_i^{\alpha_i} \Pi u_j^{\beta_j}$.*

Proof. As both η and η' are non-zero, then the only way $A(G'')$ would vanish is that there were a monomial $A'(G'') = \nu\nu' x''^{\alpha'+\beta'} \Pi v_i^{\alpha_i} \Pi u_j^{\beta_j}$, where $\nu\nu' = -\eta\eta'$ and $\alpha' + \beta' = \alpha + \beta$. But then in $P(G)$ and $P(G')$ there would have to be respective non-vanishing monomials $\nu x^{\alpha'} \Pi v_i^{\alpha_i}$ and $\nu' x'^{\beta'} \Pi u_j^{\beta_j}$, and as the sum of exponents in every monomial in a polynomial of given graph is fixed, we have that $\alpha = \alpha'$ and $\beta = \beta'$, a contradiction. Thus $A(G'')$ is non-vanishing. $\square$

Lemma 3.6. *Let G be a path of length n, $n \geq 2$, where x, y are the endpoints and $v_1, \dots, v_{n-1}$ are the internal vertices of G. Then in $P(G)$ there is a non-vanishing monomial of the form $\eta x^0 y^0 v_1^2 v_2^1 \dots v_{n-1}^1$, where $\eta \in \{-1, 1\}$.*

Proof. Suppose at first that $n = 2$. Then $P(G) = (x - v_1)(y - v_1) = xy - xv_1 - yv_1 + v_1^2$, and the last monomial is the one fulfilling the assertion. Now suppose that the lemma holds for $n = k - 1$. Then in $P(G)$, where G is a path $xv_1 \dots v_{k-1}$, there is a monomial $\eta x^0 v_1^2 v_2^1 \dots v_{k-2}^1 v_{k-1}^0$. Now adjoining v_k to v_{k-1}, thus multiplying $P(G)$ by $(v_{k-1} - v_k)$ we obtain a monomial $\eta x^0 v_1^2 v_2^1 \dots v_{k-2}^1 v_{k-1}^1 v_k^0$ for path of length k, hence completing the induction. $\square$

3.1 Near-triangulations with cutvertices

The following theorem is a polynomial analogue of [4, Theorem 5.3] that characterizes extendability of outerplanar near-triangulations with cutvertices.

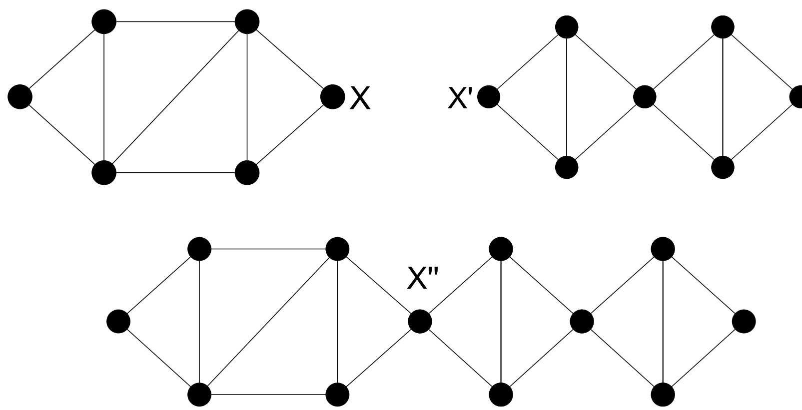


Figure 3: Illustration for Lemma 3.5. Top: graphs G (left) and G' (right); Bottom: graph G''.

Theorem 3.7. *Let G be a fundamental $x - y$ subgraph with cutvertices $\{v_1, \ldots, v_{j-1}\}$, $CV(G) = (x, v_1, \ldots, v_{j-1}, y)$ be the sequence consisting of x, y and the cutvertices of G in order that they occur on any of the paths from x to y, and $u_{i,k}$ being the remaining vertices in the i-th block. Then in $P(G)$:*

(i) *there is a non-vanishing monomial of the form $\eta_1 x^1 y^1 \Pi v_m^{\alpha_m} \Pi u_{i,k}^{\beta_{i,k}}, \alpha_m, \beta_{i,k} \le 2$ if every vertex from $CV(G)$ is in the same colour class;*

(ii) *there is a non-vanishing monomial of the form $\eta_2 x^0 y^1 \Pi v_m^{\alpha_m} \Pi u_{i,k}^{\beta_{i,k}}, \alpha_m, \beta_{i,k} \le 2$ if there is a single pair of successive vertices in $CV(G)$ that are in different colour classes;*

(iii) *there is a non-vanishing monomial of the form $\eta_3 x^0 y^0 \Pi v_m^{\alpha_m} \Pi u_{i,k}^{\beta_{i,k}}, \alpha_m, \beta_{i,k} \le 2$ if there are at least two pairs of successive vertices in $CV(G)$ that are in different colour classes;*

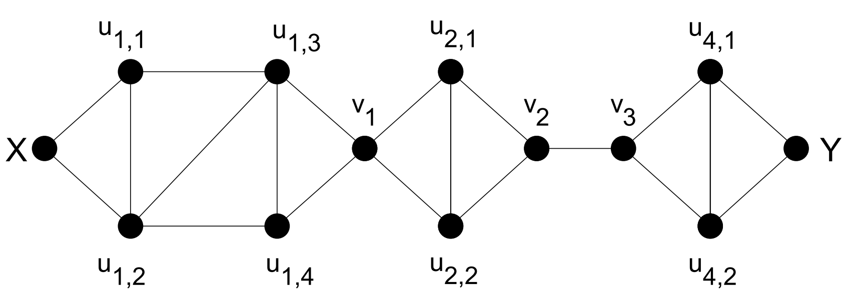


Figure 4: An example of labelling described in Theorem 3.7.

Proof. Start with partitioning G by its cutvertices into separate, 2-connected, $v_{i-1}v_i$-fundamental outerplanar near-triangulations $B_1, \dots, B_j$. To each of these graphs, Theorem 2.1 applies, and $P(G) = P(B_1) \dots P(B_j)$. If in each of those blocks the colour class of degree 2 vertices is the same, then in each of their polynomials there is a non-vanishing monomial such that exponents of degree 2 vertices are equal to 1, with other exponents no larger than 2. Thus case 1 is just a repeated use of Lemma 3.5.

In the second case, let B_i be the block with degree 2 vertices in different colour classes. If $i = 1$, then in $P(B_1)$ there is a non-vanishing monomial of the form $\eta_0 x^0 v_1^1 \Pi u_{1,k}^2$. Hence again by Lemma 3.5 we get the desired monomial. If $i > 1$, then we apply Lemma 3.4 to each block B_1 to B_{i-1}, thus by Lemma 3.5 obtaining monomial with x^0 and v_{i-1}^2. As v_{i-1} and v_i are in different colour classes, $P(B_i)$ contains a non-vanishing monomial $\eta_i v_{i-1}^0 v_i^1 \Pi u_{i,k}^2$, hence through Lemma 3.5 we finish the case.

The last case is starts analogously to the second one, with $B_i, B_l, i < l$ being two blocks with endpoints in different colour classes. Let G' be the $v_{i-1}v_l$-fundamental subgraph of G. By Theorem 2.1 there is a non-vanishing monomial in $P(B_i)$ with v_{i-1}^0 and v_i^1 and a monomial in $P(B_l)$ with v_{l-1}^1 and v_l^0. As every block between B_i and B_l has a monomial with endpoints in power 1, by Lemmas 3.4 and 3.5 there is a monomial in $P(G')$ with both v_{i-1} and v_l in power 0. Again by Lemmas 3.4 and 3.5 we can now adjoin remaining parts of G to G', with their suitable monomials creating a desired monomial in $P(G)$. □

3.2 2-connected outerplanar graphs with non-triangular faces

The following three theorems are jointly analogous to [4, Theorem 4.3].

Theorem 3.8. *Let G be a 2-connected xy-fundamental graph with exactly one non-triangular interior face, and that face contains x and does not contain y. Let $V(G) = \{x, y, a, b, v_1, \dots, v_n\}$, where a, b are the two vertices of non-triangular face belonging to the neighbouring interior face. Let $C(v)$ be the colour class of vertex v in the 3-colouring of the graph induced by all of the triangular faces. Then in $P(G)$:*

- (i) *there is a non-vanishing monomial of the form $\eta_1 x^0 y^1 a^{\alpha_a} b^{\alpha_b} \Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$ if $d(x, a) = 1$ and $C(a) = C(y)$ OR $d(x, b) = 1$ and $C(b) = C(y)$;*
- (ii) *there is a non-vanishing monomial of the form $\eta_2 x^0 y^0 a^{\alpha_a} b^{\alpha_b} \Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$ otherwise.*

Proof. Suppose that $d(x, a) = 1$ and $C(a) = C(y)$. Let G' be the subgraph of G created by deleting all the vertices on the non-triangular face except for a and b. As G' is an outerplanar near-triangulation Theorem 2.1 applies, and as $C(a) = C(y)$, then in $P(G')$ there is a non-vanishing monomial with a^1 and y^1. If we now adjoin vertex x to a, creating graph G'', then it $P(G'')$ there is a non-vanishing monomial with x^0, a^2 and y^1. Now adding a path between x and b, thus reconstructing G (notice that the length of this path is at least 2, as the face is not a triangle), by Lemma 3.6 we obtain a desired monomial. The case when $d(x, b)$ and $C(b) = C(y)$ is handled analogously.

If this is not the case, then either $d(x, a) > 1$ and $d(x, b) > 1$, or $d(x, a) = 1$ and $C(a) \neq C(y)$ (or analogously $d(x, b) = 1$ and $C(b) \neq C(y)$). In the first case, then by Theorem 2.1 and Lemma 3.4 in $P(G')$ (with G' defined as previously) there is a non-vanishing monomial with y^0 and all other powers less than 3. Now as we join x with a and b with previously deleted paths, Lemma 3.6 gives us a monomial with x^0, y^0 and all other

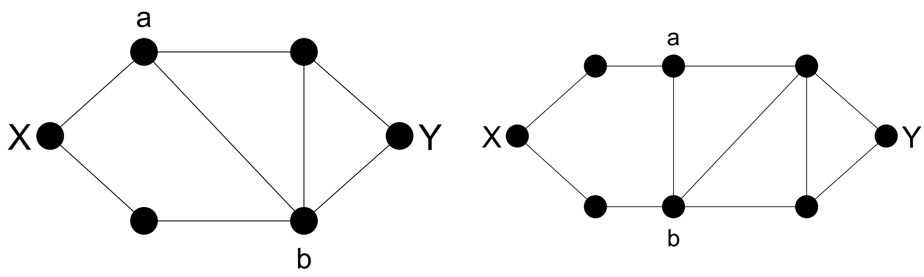


Figure 5: Examples of labelling as in Theorem 3.8. Left: example to point (i); Right: example to point (ii).

powers less than 3. In the second case, as $C(a) \neq C(y)$, by 2.1 there is a monomial in $P(G')$ where y has power 0 and a has power 1. Adjoining x to a, we obtain a monomial with x^0, y^0 and a^2, and as we join x with b by a path, Lemma 3.6 gives us a desired monomial. Case when $d(x,b) = 1$ and $C(b) \neq C(y)$ is again analogous to the last one. □

Theorem 3.9. *Let G be a 2-connected xy-fundamental graph with exactly one non-triangular interior face, and that face does not contain x nor y. Let $V(G) = \{x, y, a, b, c, v_1, \ldots, v_n\}$, where a, b and a, c are the two pairs of vertices of non-triangular face belonging to the neighbouring interior faces, and let $C(v)$ be the colour class of vertex v in the 3-colouring of the subgraph of G created by deleting the path connecting b and c. Then in $P(G)$:*

(i) *there is a non-vanishing monomial of the form $\eta_1 x^1 y^1 a^{\alpha_a} b^{\alpha_b} c^{\alpha_c} \Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$, if $C(x) = C(a) = C(y)$;*

(ii) *there is a non-vanishing monomial of the form $\eta_2 x^0 y^1 a^{\alpha_a} b^{\alpha_b} c^{\alpha_c} \Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$, if $C(x) \neq C(a) = C(y)$ or $C(x) = C(a) \neq C(y)$;*

(iii) *there is a non-vanishing monomial of the form $\eta_3 x^0 y^0 a^{\alpha_a} b^{\alpha_b} c^{\alpha_c} \Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$, if $C(x) \neq C(a) \neq C(y)$;*

Proof. Let G' be the subgraph of G obtained by deleting path connecting b and c from G. Obviously G' is an outerplanar near-triangulation with a single cutvertex a, hence Theorem 3.7 applies to it. Notice moreover, that the first case of the above theorem leads to the first case of Theorem 3.7, and the second and third case also relate similarly. As Theorem 3.7 gives us suitable monomials, when we add back the path we previously deleted, an application of Lemma 3.6 finishes the proof. □

Theorem 3.10. *Let G be a 2-connected xy-fundamental graph with exactly one non-triangular interior face, and that face does not contain x nor y. Let $V(G) = \{x, y, a, b, c, d, v_1, \ldots, v_n\}$, where a, b and c, d are the two pairs of vertices of the non-triangular face belonging to the neighbouring interior faces with $ab \in E(G)$ and $cd \in E(G)$, and let $C(v)$ be the colour class of vertex v in the 3-colouring of the subgraphs of G created by deleting the paths connecting a with c and b with d. Then in $P(G)$:*

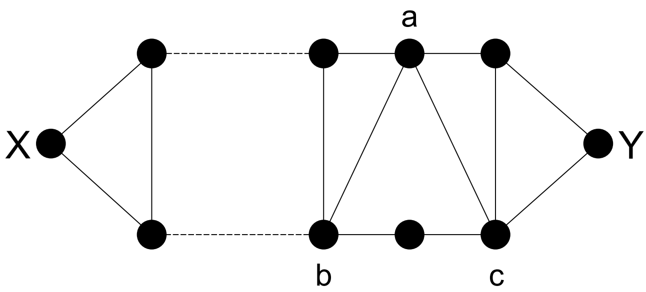


Figure 6: An example of labelling described in Theorem 3.9.

(i) *there is a non-vanishing monomial of the form* $\eta_1 x^0 y^1 a^{\alpha_a} b^{\alpha_b} c^{\alpha_c} d^{\alpha_d} \Pi v_i^{\alpha_i}$*,* $\alpha_k \leq 2$*, if* $d(a, c) = 1$*,* $C(x) = C(a)$ *and* $C(y) = C(c)$ *OR* $d(b, d) = 1$*,* $C(x) = C(b)$ *and* $C(y) = C(d)$*;*

(ii) *there is a non-vanishing monomial of the form* $\eta_2 x^0 y^0 a^{\alpha_a} b^{\alpha_b} c^{\alpha_c} d^{\alpha_d} \Pi v_i^{\alpha_i}$*,* $\alpha_k \leq 2$ *otherwise;*

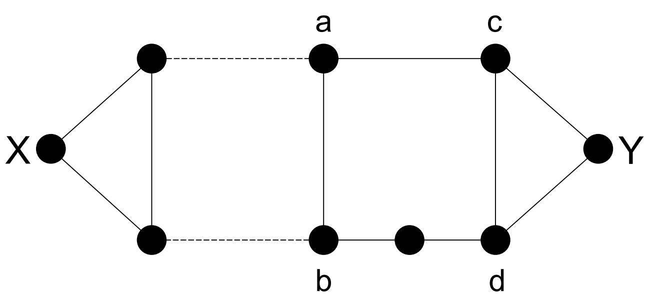


Figure 7: An example of labelling described in Theorem 3.10.

Proof. Suppose at first that $C(x) = C(a)$ and $C(y) = C(c)$. We can connect vertex a with d, and if $d(b, d) > 1$, also with every interior vertex on the path connecting b with d, thus obtaining an xy-fundamental 2-connected near triangulation G'. If $d(a, c) = 1$, then $C(a) \neq C(c)$, thus $C(x) \neq C(y)$, and by Corollary 2.2 $P(G')$ contains a non-vanishing monomial with x^0, y^1 and every other exponent equals 2. As neither x nor y were affected by addition of edges to G, $P(G)$ contains a non-vanishing monomial of the form $\eta_1 x^0 y^1 a^{\alpha_a} b^{\alpha_b} c^{\alpha_c} d^{\alpha_d} \Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$. If $d(a, c) > 1$, then G' fulfils the conditions of Theorem 3.9, with d serving as vertex a in the statement of that theorem. Moreover, as $C(x) = C(a)$ and $C(y) = C(c)$, and d neighbours both a and c in G', then in colouring of G' $C(x) \neq C(d)$ and $C(y) \neq C(d)$. Hence by Theorem 3.9 $P(G')$ contains a non-vanishing monomial with x^0, y^0 and every other exponent no larger than 2, and this again implies that there is a non-vanishing monomial of the form $\eta_2 x^0 y^0 a^{\alpha_a} b^{\alpha_b} c^{\alpha_c} d^{\alpha_d} \Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$ in $P(G)$. The case when $C(x) = C(b)$ and $C(y) = C(d)$ is analogous.

Suppose now that $C(x) \neq C(a)$ and $C(y) = C(c)$. Start by removing the paths from a to c and b to d from G. This leaves us with two separate, 2-connected near triangulations G' and G'' with $\{x, a, b\} \in V(G')$ and $\{y, c, d\} \in V(G'')$. As $C(y) = C(c)$, then $C(y) \neq C(d)$, and by Corollary 2.2 in $P(G'')$ there is a non-vanishing monomial of the form $\eta_1 y^0 d^1 c^2 \Pi v_i^2$. Now as $C(x) \neq C(a)$, there exists a non-vanishing monomial $\eta_1 x^0 a^1 b^2 \Pi u_i^2$ in $P(G')$, as the polynomial of xa-fundamental subgraph of G' contains a non-vanishing monomial with x^0 and a^1, and as G' is a 2-connected near triangulation, every other exponent must be equal to 2. Now add back the previously removed paths. Each of them contains in its graph polynomial a non-vanishing monomial with every exponent equal to 1, except for one of its endpoints, which has power 0. We will call that monomial *oriented towards* the endpoint with non-zero exponent. Add paths connecting a with c and b with d to G' and G'', and by multiplication of the monomials described above we obtain a monomial of the form $\eta_2 x^0 y^0 a^{\alpha_a} b^{\alpha_b} c^{\alpha_c} d^{\alpha_d} \Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$ in $P(G)$, where exponent of each of the vertices a, b, c, d is equal to 2. This monomial does not vanish, as the only other way to get this monomial would require us to orient both of the paths in the opposite direction, but this would imply that there were a non-vanishing monomial $\eta_1 y^0 d^2 c^1 \Pi v_i^2$ in $P(G'')$, which is not the case as $C(y) = C(c)$. Cases where $C(x) = C(a)$ and $C(y) \neq C(c)$, $C(x) \neq C(b)$ and $C(y) = C(d)$ or $C(x) = C(b)$ and $C(y) \neq C(d)$ are sorted out in the same manner.

The last case is when $C(x) \neq C(a)$ and $C(y) \neq C(c)$. Observe at first, that we can also assume that $C(x) \neq C(b)$ and $C(y) \neq C(d)$, as all the other cases were already solved in previous arguments due to symmetries. Let G' and G'' be as in previous case. As $C(b) \neq C(x) \neq C(a)$, then in $P(G')$ there are non-vanishing monomials $\eta_1 x^0 a^1 b^2 \Pi v_i^2$ and $-\eta_1 x^0 a^2 b^1 \Pi v_i^2$. Similarly, there are non-vanishing monomials $\eta_2 y^0 c^1 d^2 \Pi u_i^2$ and $-\eta_2 y^0 c^2 d^1 \Pi u_i^2$ in $P(G'')$. Now reconstruct G as previously, orienting path connecting a and c towards a and path connecting b and d towards d. To comply with requirements of the assertion, we have to use the first and fourth monomial from those specified above, thus in $P(G)$ we have a monomial $-\eta_1 \eta_2 x^0 y^0 a^2 b^2 c^2 d^2 \Pi v_i^2$. The only other way to reach this set of exponents is to use the second and third monomial, and orient paths in opposite directions, but as a simultaneous switch of orientations preserves sign, we again obtain $-\eta_1 \eta_2 x^0 y^0 a^2 b^2 c^2 d^2 \Pi v_i^2$, so those monomials do not annihilate each other, but rather double the coefficient. As all cases are now addressed, the proof is complete. □

3.3 General outerplanar graphs

The three theorems above can be combined with Theorem 3.7 to obtain a general characterisation of (i, j)-extendability of outerplanar graphs. We will start with some technicalities.

Definition 3.11. Let G be an outerplanar graph. A non-triangular inner face of G will be called *type 0* if it is as defined in Theorem 3.8 (with possibly y belonging to that face instead of x), *type 1* if it is as defined in Theorem 3.9 and *type 2* if it is as defined in Theorem 3.10. In case of type 1 faces, the vertex belonging to the two neighbouring faces will be called an *apex* of that face.

Lemma 3.12. *Let G be a connected outerplanar graph with $V(G) = \{x, y, v_1, \ldots, v_i\}$ and let G' be a supergraph of G obtained by adding a path of the length 2 to G in a way that preserves outerplanarity. Then the monomial $x^{\alpha_x} y^{\alpha_y} \Pi v_i^{\alpha_i}$ does not vanish in $P(G)$ if* *and only if the monomial $x^{\alpha_x}y^{\alpha_y}\Pi v_i^{\alpha_i}z^2$ does not vanish in $P(G')$, where z is the middle vertex of the added path.*

Proof. The implication from $P(G)$ to $P(G')$ is obvious and was shown to be true and utilized multiple times in this paper. Suppose there is a non-vanishing monomial $x^{\alpha_x}y^{\alpha_y}\Pi v_i^{\alpha_i}z^2$ in $P(G')$. As $P(G') = P(G)(ab - az - bz + z^2)$, where a, b are the endpoints of the added path, and none of the monomials from $P(G)$ contains z due to the fact that $z \notin V(G)$, then the only way to obtain the monomial above is by multiplying $x^{\alpha_x}y^{\alpha_y}\Pi v_i^{\alpha_i}$ by z^2, thus the former must occur in $P(G)$. □

Definition 3.13. Let G be a 1-connected fundamental outerplanar graph. For every cutvertex of G that is not an endpoint of any bridge add a path of length 2, connecting the pair of some neighbours of that cutvertex without disrupting outerplanarity, thus creating a non-triangular face of type 0. Then for every bridge or chain of bridges of G add a path of the length 2 connected to the pair of the neighbours of the endpoints of that bridge or chain of bridges (or to the neighbour and the endpoint if it has degree 1) in a way that preserves outerplanarity, creating a face of type 2 (or type 0). Finally, if G is a path, connect endpoints of that path with a path of length 2. The resulting supergraph of G will be called a *2-connection* of G. The 2-connection of A 2-connected graph would be the graph itself.

Notice, that the 2-connection of a 1-connected graph is not unique — for example, the graph on Figure 8 has 8 different 2-connections. However, each of the 2-connections has the same relevant properties — namely the color classes of the cutvertices and types of the newly created non-triangular faces.

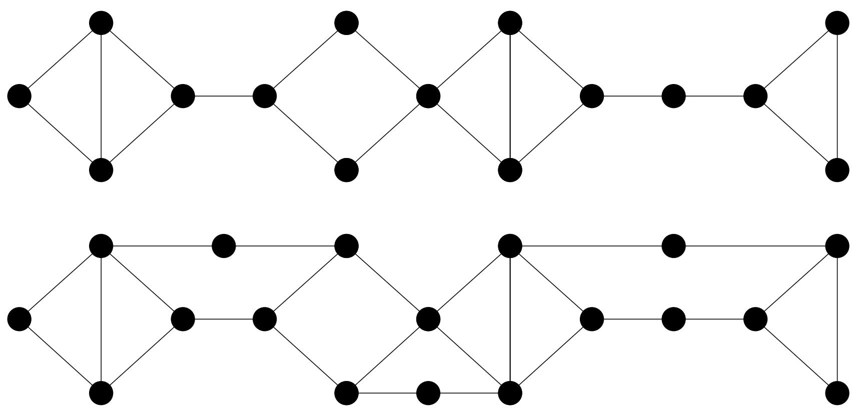


Figure 8: Top: a connected, outerplanar graph G; Bottom: a possible 2-connection of G.

The following remark is a direct consequence of Lemma 3.12.

Remark 3.14. Let G be a connected xy-fundamental outerplanar graph, $V(G) = \{x, y, v_1, \dots, v_m\}$ and let G' be its 2-connection, $V(G') = \{x, y, v_1, \dots, v_m, u_1, \dots, u_n\}$. There is a non-vanishing monomial $x^{\alpha_x}y^{\alpha_y}\Pi v_i^{\alpha_i}$ in $P(G)$ if and only if there is a non-vanishing monomial $x^{\alpha_x}y^{\alpha_y}\Pi v_i^{\alpha_i}\Pi u_j^2$ in $P(G')$.

The following theorem presents a full characterisation of the polynomial extendability of connected fundamental outerplanar graphs.

Theorem 3.15. *Let G be a connected xy-fundamental outerplanar graph, $V(G) = \{x, y, v_1, \dots, v_i\}$, and let G' be a 2-connection of G. Then in $P(G)$:*

(i) *there is a non-vanishing monomial of the form $x^1y^1\Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$ if G is a 2-connected near-triangulation with $C(x) = C(y)$ OR G is as in point 1 of Theorem 3.7 OR every non-triangular face of G' is of type 1 and every apex, x and y have the same colour in every 3-colouring of G.*

(ii) *there is a non-vanishing monomial of the form $x^0y^1\Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$ if G is a 2-connected near-triangulation with $C(x) \neq C(y)$ OR G is as in point 2 of Theorem 3.7 OR G' is as in point 1 of Theorem 3.8 OR G' is as in point 1 of Theorem 3.10 OR every non-triangular face of G' is of type 1 and in every 3-colouring of G' there is exactly one pair of consecutive apexes (or either x or y with the closest apex) with different colours OR only one of the non-triangular faces of G' is not of the type 1 and conditions of point 1 of Theorem 3.10 are fulfilled on that face.*

(iii) *there is a non-vanishing monomial of the form $x^0y^0\Pi v_i^{\alpha_i}$, $\alpha_k \leq 2$ otherwise.*

Proof. We will omit every case that is covered already by previous theorems, leaving us only with the cases when there are multiple non-triangular faces. Suppose all of those are of type 1. It is easy to see (with some help of Lemma 3.6) that for every such face removal of all vertices belonging only to this (and outer) face produces a cutvertex, simultaneously changing nothing in terms of extendability-relevant monomials. Hence apply Theorem 3.7, with each apex acting as a cutvertex.

Suppose now there is a face of type either 0 or 2 in G'. Theorems 3.8 and 3.10 show that the only cases where there is no monomial in $P(G')$ (and thus in $P(G)$) with both x and y in power 0 is when 3-colouring G' we cannot avoid a situation described in point 1 of either of these theorems on any of such faces, and in those cases there is a non-vanishing monomial with x^0 and y^1. Observe that this is not the case when there are at least two faces of type 0 or 2, as we can avoid this situation by either permuting the colours, or by changing them on vertices of degree 2 (as in case of type 0 faces at least one such vertex other than x and y definitely exists). So there are only two cases when we cannot avoid that. The first is when in G' there is only one face of type 2, no faces of type 0, there is a pair of neighbouring vertices belonging to this face such that the only other face of G' they belong to simultaneously is the outer face, and in any 3-colouring of G (and thus also G') each of those vertices has the same colour as x or y, depending on which of those vertices lies on the same "side" of that face. Label the vertex from this pair lying closer to x as v_x, and the one being closer to y as v_y. The case of $C(x) = C(v_x)$ can occur either when on one side there are only triangular faces between x and v_x, with the structure of that triangulation forcing the same colour of those vertices, or when for every type 1 face between those vertices, the triangular structure between neighbouring faces or between x (or v_x) and the nearest such face forces the same colour on each of those vertices. The same is true for y and v_y, with the restriction that the former situation cannot occur for both of those pairs. The second case is when there is exactly one face of type 0 in G' (without loss of generality we can assume that x lies on that face), no faces of type 2, x has a neighbour (v_0) that lies also on adjacent inner face, and the colour of that vertex is the same as colour of y in every 3-colouring of G'. This can be only caused by the fact that the apex of every type 1 face is forced to have the same colour as the others, as well as y and v_0. □

Finally, we prove that Theorem 3.15 can be restated as Theorem 1.4.

Proof of Theorem 1.4. Neither the graph polynomial nor the colouring depends on a particular graph embedding. Therefore, let G be any outerplanar graph with $V(G) = \{x, y, v_1, \ldots, v_n\}$. At first notice, that if G is not connected and x and y are in different connected components, one may use Theorem 1.3 directly to obtain a monomial with $\beta = \gamma = 0$, so then obviously the third case occurs.

For x and y in one component observe that by the Hutchinson's shrinking argument it is enough to prove theorem for G being xy-fundamental graph. See the proof of Corollary 2.2 for details. Now consider consequences of each of the situations described in the statement of Theorem 3.15 in terms of 3-colourings. In every case of point (i) we obviously have that $C(x) = C(y)$. Moving to the second point, the first condition again directly states that $C(x) \neq C(y)$. If G is as in point 2 of Theorem 3.7 or every non-triangular face of G' is of type 1 and in every 3-colouring of G' there is exactly one pair of consecutive apexes (or either x or y with the closest apex) with different colours, as the colour class changes only once on the cutvertices/apexes, then obviously classes of terminal vertices x and y have to be different. If G' is as in point 1 of Theorem 3.8, then it is directly stated that the colour of one of terminal vertices is the same as the colour of one of the neighbours of the other terminal vertex, thus the colours of terminal vertices have to be different. Finally, if G' is as in point 1 of Theorem 3.10 or only one of the non-triangular faces of G' is not of the type 1 and the conditions of point 1 of Theorem 3.10 are fulfilled on that face, the vertices x and y are in the same colour class as vertices a and c (or b and d), respectively, and those vertices are adjacent, hence their colours cannot possibly be the same.

Finally, observe that in any other case the colour classes of x and y are independent — the structure of the graph permits the colours to be rearranged in some parts without changing the colours in the other parts, therefore the graph can be properly 3-coloured with both $C(x) = C(y)$ and $C(x) \neq C(y)$. As an example consider point (ii) of Theorem 3.8, other cases are analogous. Starting with the triangulated part of the graph (i.e. the graph minus internal vertices of the path between a and b containing x) already coloured, analyse possible proper 3-colourings of the path from a to b. If $\min(d(x, a), d(x, b)) > 1$, then we can colour x with any of the 3 colours. Otherwise, suppose without loss of generality that $d(x, a) = 1$ and hence $d(x, b) > 1$. Then x can be coloured with any colour except $C(a)$, but there is $C(a) \neq C(y)$. Therefore, again x can get colour of y or some different one. □

4 Further work

Extendability is naturally transformed into plane graphs by allowing interior vertices to have a list of colours of length 5. In [5] and [6] Postle and Thomas provided results that may be summarized in the following theorem.

Theorem 4.1. *Let $G = (V, E)$ be any plane graph, let $C \subseteq V$ be the set of vertices on the outer face, $x, y \in C$, $x \neq y$. Then*

(i) *(G, x, y) is $(1, 2)$-extendable if and only if there exists a proper colouring $c\colon C \to \{1, 2, 3\}$ such that $c(x) \neq c(y)$;*

(ii) (G, x, y) *is* $(2, 2)$*-extendable.*

One may ask, whether is it possible to restate the above theorem in the terms of a graph polynomial, i.e. to extend, at least partially Theorem 1.4 to planar graphs. Our partial results suggest that it is possible.

ORCID iDs

Przemysław Gordinowicz https://orcid.org/0000-0001-9843-3928
Paweł Twardowski https://orcid.org/0000-0003-1259-4830

References

[1] N. Alon, Combinatorial Nullstellensatz, *Combin. Probab. Comput.* **8** (1999), 7–29, doi:10.1017/s0963548398003411, recent trends in combinatorics (Mátraháza, 1995).

[2] N. Alon and M. Tarsi, Colorings and orientations of graphs, *Combinatorica* **12** (1992), 125–134, doi:10.1007/bf01204715.

[3] J. Grytczuk and X. Zhu, The Alon-Tarsi number of a planar graph minus a matching, *J. Combin. Theory Ser. B* **145** (2020), 511–520, doi:10.1016/j.jctb.2020.02.005.

[4] J. P. Hutchinson, On list-coloring extendable outerplanar graphs, *Ars Math. Contemp.* **5** (2012), 171–184, doi:10.26493/1855-3974.179.189.

[5] L. Postle and R. Thomas, Five-list-coloring graphs on surfaces I. Two lists of size two in planar graphs, *J. Combin. Theory Ser. B* **111** (2015), 234–241, doi:10.1016/j.jctb.2014.08.003.

[6] L. Postle and R. Thomas, Five-list-coloring graphs on surfaces III. one list of size one and one list of size two, *J. Combin. Theory Ser. B* **128** (2018), 1–16, doi:10.1016/j.jctb.2017.06.004.

[7] U. Schauz, Mr. Paint and Mrs. Correct, *Electron. J. Combin.* **16** (2009), Research Paper 77, 18, doi:10.37236/166.

[8] C. Thomassen, Every planar graph is 5-choosable, *J. Combin. Theory Ser. B* **62** (1994), 180–181, doi:10.1006/jctb.1994.1062.

[9] D. B. West, *Introduction to Graph Theory, 2nd edition*, Prentice Hall, Inc., Upper Saddle River, NJ, 2001, `https://faculty.math.illinois.edu/~west/igt/`.

[10] X. Zhu, The Alon-Tarsi number of planar graphs, *J. Combin. Theory Ser. B* **134** (2019), 354–358, doi:10.1016/j.jctb.2018.06.004.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.09 / 301–307
https://doi.org/10.26493/1855-3974.2388.928
(Also available at http://amc-journal.eu)

On generalized strong complete mappings and mutually orthogonal Latin squares*

Amela Muratović-Ribić †

University of Sarajevo, Faculty of Science, Zmaja od Bosne 33-35, Sarajevo, Bosnia and Herzegovina

Received 20 July 2020, accepted 1 April 2021, published online 2 November 2021

Abstract

We present an application of generalized strong complete mappings to construction of a family of mutually orthogonal Latin squares. We also determine a cycle structure of such mapping which form a complete family of MOLS. Many constructions of generalized strong complete mappings over an extension of finite field are provided.

Keywords: Strong complete mapping, group, finite field, mutually orthogonal Latin squares (MOLS).

Math. Subj. Class. (2020): 11T06, 12Y05

1 Introduction

Let G be an additive group. A mapping $\theta : G \to G$ is called a complete mapping if both $\theta(x)$ and $\theta(x)+x$ are 1-to-1 and onto. If both $\theta(x)$ and $\theta(x)-x$ are 1-to-1 and onto, $\theta(x)$ is called an orthomorphism. A strong complete mapping is a complete mapping which is also an orthomorphism. These mappings are used for a construction of Knut Vic designs and they exist only for the groups of order n where $\gcd(n, 6) = 1$. An Abelian group admits strong complete mappings if and only if its Sylow 2-subgroup is trivial or noncyclic, and also, its Sylow 3-group is trivial or noncyclic (see [2]).

Let p be a prime, m be a positive integer and $q = p^m$. Let $\mathbb{F}_q$ be a finite field of order q. We consider complete and strong complete mappings (and orthomorphisms) over $(\mathbb{F}_q(x), +)$. Polynomials induced by these mappings are called complete and strong complete polynomials, respectively. In [1], strong complete mappings over finite fields are called very complete mappings. Many results have been established on this topic. In the

*Results in this article were partially presented on the Carleton Finite Fields Workshop, May 21 – 24, 2019.

†The author gratefully thanks the anonymous referee for the constructive comments and recommendations which definitely helped to improve the quality of the paper.

E-mail address: amela@pmf.unsa.ba (Amela Muratović-Ribić)

sequel, $f^0(x) = x$, $f^2(x) = f \circ f(x)$, $f^k(x) = f \circ f^{k-1}(x)$ for $k > 0$. Generalized complete polynomials were introduced in [6] with applications to the check digit systems. There were considered polynomials over finite fields with a property that $f(x), f(x) \pm x$ and $f^2(x) \pm x$ are all permutation polynomials. Note that there exist monomials of the form $x^{\ell \frac{q-1}{m}}$ where $m \mid q-1$ with this property (see [5]).

We turn our attention to mappings $\theta(x)$ such that $\theta^k(x)$ are strong complete mappings for all $k = 1, 2, ..., t$. Here, t is a positive integer. Our point of interest is an application of these mappings to construction of mutually orthogonal Latin squares (MOLS). Many constructions of such mappings over finite fields will be presented.

2 Construction of MOLS

Theorem 2.1. *Let G be an additive finite Abelian group of order n, where n is odd. Assume that $\theta : G \to G$ is such that $\theta^k(x)$ are strong complete mappings for $k = 1, 2, \ldots, t$ where t is a positive integer. For $1 \leq k \leq t$ and $i, j \in G$ define*

$$a^k_{i,j} = i + \theta^k(j)$$

$$a^{-k}_{i,j} = i - \theta^k(j)$$

$$a^{0^+}_{i,j} = i + j; \quad a^{0^-}_{i,j} = i - j.$$

A family of Latin squares $L_k = (a^k_{i,j})$ where $k = -t, \ldots, -1, 0^-, 0^+, 1 \ldots t$ is a family of pairwise mutually orthogonal Latin squares. Therefore, a family of $2(t+1)$ MOLS is obtained.

Proof. We use the following convention $\theta^{0^\pm}(x) = x$. Assume $(a^k_{i,j}, a^s_{i,j}) = (a^k_{u,v}, a^s_{u,v})$ for $k \neq s$ and consider the following cases:

- If $(0 < s < k)$ or $(s = 0^+$ and $0 < k)$ we have that

$$i + \theta^k(j) = u + \theta^k(v) \tag{2.1}$$

  and

$$i + \theta^s(j) = u + \theta^s(v).$$

  Subtracting these equalities we obtain

$$\theta^k(j) - \theta^s(j) = \theta^k(v) - \theta^s(v).$$

  Thus

$$\theta^{k-s}(\theta^s(j)) - \theta^s(j) = \theta^{k-s}(\theta^s(v)) - \theta^s(v).$$

  By assumption, $\theta^{k-s}(y) - y$ is a permutation. Hence, $\theta^s(j) = \theta^s(v)$ and $j = v$. Inserting this in (2.1) we obtain $i = u$.

- If $(k < s < 0)$ or $(k < 0$ and $s = 0^-)$ then we have

$$i - \theta^{|k|}(j) = u - \theta^{|k|}(v) \tag{2.2}$$

  and

$$i - \theta^{|s|}(j) = u - \theta^{|s|}(v).$$

Subtracting these equalities, we obtain

$$\theta^{|k|}(j) - \theta^{|s|}(j) = \theta^{|k|}(v) - \theta^{|s|}(v).$$

Thus

$$\theta^{|k|-|s|}(\theta^{|s|}(j)) - \theta^{|s|}(j) = \theta^{|k|-|s|}(\theta^{|s|}(v)) - \theta^{|s|}(v).$$

Reasoning as above, we get $j = v$ and $i = u$.

- If $(-s < 0 < k)$, $(s = 0^-$ and $k > 0)$ or $(s < 0$ and $k = 0^+)$ then we have that

$$i + \theta^k(j) = u + \theta^k(v) \tag{2.3}$$

and

$$i - \theta^{|s|}(j) = u - \theta^{|s|}(v)$$

which implies

$$\theta^k(j) + \theta^{|s|}(j) = \theta^k(v) + \theta^{|s|}(v).$$

Assume first $k > |s|$. Then $\theta^{k-|s|}(\theta^{|s|}(j)) + \theta^{|s|}(j) = \theta^{k-|s|}(\theta^{|s|}(v)) + \theta^{|s|}(v)$. As $\theta^{k-|s|}(y) + y$ is a permutation, it follows that $\theta^{|s|}(j) = \theta^{|s|}(v)$. Thus $j = v$. Using this in (2.3), we obtain $i = u$. If $k \leq |s|$ then $\theta^{|s|-k}(\theta^k(j)) + \theta^k(j) = \theta^{|s|-k}(\theta^k(v)) + \theta^k(v)$ similarly implies $j = v$ and $i = u$.

- If $k = 0^+$ and $s = 0^-$ then $i + j = u + v$ and $i - j = u - v$ which implies $2i = 2u$. Then $2ki = 2ku$ for all integers k. By assumption, the order of the group G is an odd integer. Then $n + 1$ is even and thus $(n + 1)i = (n + 1)u$. However, $ni = nu$ by Lagrange's theorem. Hence, $i = u$ and further $j = v$.

□

Lemma 2.2. *Let G be a group of order n. Assume that $\theta : G \to G$ is such that all $\theta^k(x)$ are strong complete mappings for $k = 1, 2, \ldots, t$. Then the permutation θ has exactly one fixed element and lengths of all other cycles are greater than t.*

Proof. Assume that ℓ is the length of a cycle $(a_1, a_2, \ldots, a_\ell)$ of the permutation θ, where $1 < \ell \leq t$. Then $\theta^\ell(a_1) = a_1$ and $\theta^\ell(a_2) = a_2$. Therefore $\theta^\ell(a_1) - a_1 = \theta^\ell(a_2) - a_2 = 0$. It follows that $\theta^\ell(x) - x$ is not a permutation which is a contradiction. Therefore, there is no cycle of the length $1 < \ell \leq t$. Since $\theta(x) - x$ is a permutation, there is exactly one solution of the equation $\theta(x) - x = 0$ and thus exactly one fixed element of θ. □

Theorem 2.3. *If θ generates a complete set of MOLS over a finite Abelian group of order n as in the* Theorem 2.1*, then θ has either one fixed element and one cycle of the length $n - 1$ or one fixed element and two cycles of the length $\frac{n-1}{2}$.*

Proof. In this case all $\theta^k(x)$ are strong complete mappings for $k = 1, 2, \ldots, \frac{n-1}{2} - 1$. By the Lemma 2.2, there is one fixed element in the permutation θ and the lengths of nontrivial cycles are greater than $\frac{n-1}{2} - 1$. It follows that there can either one such cycle with the length $n - 1$ or two cycles of the length $\frac{n-1}{2}$. □

Remark 2.4. Let $\mathbb{Z}_p$ be a field of order p, where $p > 2$ is a prime. Let d be a generator of $\mathbb{Z}_p^*$. Then $\theta^k(s) = d^k s$ is a strong complete mapping for $k = 1, 2, \ldots, \frac{p-3}{2}$. The mapping $\theta(s)$ has a fixed element $s = 0$ and one full cycle $(1, d, d^2, ..., d^{p-2})$ of the length $p - 1$. On the other hand, $\theta^2(s) = d^2 s$ has a property that $\theta^{2k}(s) = d^{2k} s$ is also a strong complete mapping for all $k = 1, 2, \ldots, \frac{p-3}{2}$ since $\frac{p-1}{2}$ is odd. This mapping has a fixed element $s = 0$ and two cycles of the length $\frac{p-1}{2}$.

Proposition 2.5. *Assume that $\Psi : G \to G$, is a permutation such that $\Psi(x \pm y) = \Psi(x) \pm \Psi(y)$ for all $x, y \in G$. If $\theta(x)$ generates a complete set of MOLS as in* Theorem 2.1, *then $\eta(x) = \Psi \circ \theta \circ \Psi^{-1}(x)$ also generates a complete set of MOLS.*

Note: An example of the mapping is $\Psi(x) = kx$ where k is an integer, which prove its existence.

Proof. Since $\eta^k(x) = \Psi \circ \theta^k \circ \Psi^{-1}(x)$ is a permutation we need to show that $\eta^k(x) + x$ and $\eta^k(x) - x$ are permutations for all $k = 1, 2, \ldots \frac{|G|-1}{2}$. Using substitution $y = \psi^{-1}(x)$ we get

$$\eta^k(x) \pm x = \Psi[\theta^k(\Psi^{-1}(x))] \pm \Psi(\Psi^{-1}(x)) = \Psi[\theta^k(\Psi^{-1}(x)) \pm \Psi^{-1}(x)] = \Psi(\theta^k(y) \pm y).$$

This is a permutation since $\Psi(x)$ and $\theta^k(x) \pm x$ are permutations. Therefore, $\eta(x)$ generates a complete set of MOLS. □

Let $\mathbb{F}_q$ be a field with a prime subfield $\mathbb{Z}_p$. Linearized polynomials over $\mathbb{F}_q$ are of the form $L(x) = \sum_{k=0}^{m} a_k x^{p^k}$ and these polynomials have property that $L(ax) = aL(x)$ for all $a \in \mathbb{Z}_p$ and $L(x + y) = L(x) + L(y)$ for all $x, y \in \mathbb{F}_q$. Thus, if we consider $\mathbb{F}_q$ as a vector space over $\mathbb{Z}_p$, then $L(x)$ is a linear operator on $\mathbb{F}_q$.

Corollary 2.6. *Let $\mathbb{F}_q$ be a finite field of order $q = p^n$ where p is a prime. Let d be a primitive element of $\mathbb{F}_q$ and $L(x)$ be a linearized permutation polynomial of $\mathbb{F}_q$. Then the polynomial $f(x) = L(dL^{-1}(x))$ generates a complete set of MOLS as in* Theorem 2.1.

Proof. It is easy to see that sx is strong complete polynomial for $s \in \mathbb{F}_q \setminus \{0, \pm 1\}$. Therefore, for $g(x) = dx$, $g^k(x) = d^k x$ are strong complete mappings for all $k \neq \frac{q-1}{2}, q-1$. Since, $L(x \pm y) = L(x) \pm L(y)$ we have that $f(x) = L \circ g \circ L^{-1}(x) = L(dL^{-1}(x))$ generates a complete set of MOLS as in Theorem 2.1. □

Remark 2.7. Consider a family of strong complete polynomials over finite field $\mathbb{F}_q$ which generate a complete set of MOLS as in Theorem 2.1 and which have one fixed element and one cycle of the length $q - 1$. Let d be a generator of $\mathbb{F}_q^*$. Then $f(x) = dx$ is in this family and considering the cycle structure, all other polynomials are conjugate with $f(x)$. Therefore, all polynomials in this family are of the form $\Psi(d\Psi^{-1}(x))$ for some permutation polynomial $\Psi(x)$ over $\mathbb{F}_q$.

If $\frac{q-1}{2}$ is odd, then $g(x) = d^2 x$ is a strong polynomial which generate a complete family of MOLS as in Theorem 2.1 and which have one fixed element and two cycles of the length $\frac{q-1}{2}$. Similarly, all other strong complete mappings with a same cycle structure induce a polynomial of the form $\Psi(d^2\Psi^{-1}(x))$ for some permutation polynomial $\Psi(x)$ over $\mathbb{F}_q$.

3 Construction of the strong complete mappings over extension fields

Let n be a positive integer and $\mathbb{F}_{q^n}$ be an extension field of $\mathbb{F}_q$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of the vector space $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We shall use similar technique as in the proof of Theorem 2.1 in [3] to obtain the following recursive constructions of many strong complete polynomials over the extension field.

Theorem 3.1. *Let $f_i(x)$ be strong complete polynomials over $\mathbb{F}_q$ for $i = 1, 2, \ldots, n$. Let $\psi_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be arbitrary functions for $i = 1, 2, \ldots, n-1$. Denote $X = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$. Then the function*

$$F(X) = f_1(x_1)\alpha_1 + [f_2(x_2) + \psi_1(x_1)]\alpha_2 + \cdots + [f_n(x) + \psi_{n-1}(x_1, x_2, \ldots, x_{n-1})]\alpha_n$$

is a strong complete polynomial over $\mathbb{F}_{q^n}$.

Proof. In the proof of Theorem 1 in [3], it was shown that $F(X)$ is a complete polynomial. To show that it is a strong complete polynomial, lets check that $F(X) - X$ is $1 - to - 1$. Assume that $F(X) - X = F(Y) - Y$ for $X = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$ and $Y = y_1\alpha_1 + y_2\alpha_2 + \cdots + y_n\alpha_n$. Then the coefficients with the basis elements on the two sides of equation are identical.

Looking at the coefficient with α_1 we see that $f_1(x_1) - x_1 = f_1(y_1) - y_1$. As $f_1(x)$ is orthomorphism it follows that $x_1 = y_1$.

Now, equating the coefficients with α_2 we get $f_2(x_2) + \psi_1(x_1) - x_2 = f_2(y_2) + \psi_1(y_1) - y_2$. Taking into account $x_1 = y_1$, this implies $f_2(x_2) - x_2 = f_2(y_2) - y_2$. Hence, $x_2 = y_2$ since $f_2(x)$ is an orthomorphism. We proceed by induction. Assume that $x_1 = y_1, x_2 = y_2, \ldots, x_{i-1} = y_{i-1}$ which imply $\psi_{i-1}(x_1, x_2, \ldots, x_{i-1}) = \psi_{i-1}(y_1, y_2, \ldots, y_{i-1})$. Comparing the coefficients with α_i, we obtain

$$f_i(x_i) + \psi_{i-1}(x_1, x_2, \ldots, x_{i-1}) - x_i = f_i(y_i) + \psi_{i-1}(y_1, y_2, \ldots, y_{i-1}) - y_i.$$

Thus $f_i(x_i) - x_i = f_i(y_i) - y_i$. So, $x_i = y_i$ since $f_i(x)$ is an orthomorphism. Therefore, $x_i = y_i$ for all $i = 1, 2, \ldots, n$ and $X = Y$. Now, $F(X) - X$ being $1 - to - 1$ on the finite set $\mathbb{F}_{q^n}$ it is a bijection, i.e. a permutation. □

In the case of linearized polynomials, we extend the same technique to the compositions of mappings. The proofs of the next theorems are similar to the proof of the Theorem 3.1. So, we may omit a number of details.

Theorem 3.2. *Let $f_i(x)$, $i = 1, 2, \ldots, n$, be linearized strong complete polynomials over $\mathbb{F}_q$ such that $f_i^k(x)$ are also strong complete polynomials for $k = 1, 2, ..., t$. Let $\psi_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be arbitrary functions for $i = 1, 2, \ldots, n-1$. Denote $X = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$. Then function*

$$F(X) = f_1(x_1)\alpha_1 + [f_2(x_2) + \psi_1(x_1)]\alpha_2 + \cdots + [f_n(x) + \psi_{n-1}(x_1, x_2, \ldots, x_{n-1})]\alpha_n$$

is a strong complete polynomial over $\mathbb{F}_{q^n}$ such that $F^{(k)}(X)$ are also strong complete mappings for all $k = 2, 3, ..., t$.

Proof. By Theorem 3.1, $F(X)$ is a strong complete polynomial. Since $F(X)$ is permutation, it follows that $F^{(k)}(X)$ are permutations for all $k = 2, \cdots, t$. Assume now that $F^{(2)}(X) + X = F^{(2)}(Y) + Y$ (or $F^{(2)}(X) - X = F^{(2)}(Y) - Y$).

Equating the coefficients with α_1 on the both sides, we get $f_1^{(2)}(x_1) + x_1 = f_2^{(2)}(y_1) + y_1$ (or $f_1^{(2)}(x_1) - x_1 = f_2^{(2)}(y_1) - y_1$). This implies $x_1 = y_1$ because $f_1^{(2)}(x)$ is a strong complete polynomial. With α_2 we have

$$f_2[f_2(x_2) + \psi_1(x_1)] + \psi_1(f_1(x_1)) \pm x_2 = f_2[f_2(y_2) + \psi_1(y_1)] + \psi_1(f_1(y_1)) \pm y_2.$$

Since f_2 is linearized, we obtain

$$f_2(f_2(x_2))+f_2(\psi_1(x_1))+\psi_1(f_1(x_1))\pm x_2 = f_2(f_2(y_2))+f_2(\psi_1(y_1))+\psi_1(f_1(y_1))\pm y_2.$$

Taking into account that $x_1 = y_1$, we get $f_2(f_2(x_2)) \pm x_2 = f_2(f_2(y_2)) \pm y_2$.This yields $x_2 = y_2$ since $f_2^{(2)}(x_2)$ is a strong complete polynomial. Proceeding by induction, we can prove that $x_3 = y_3, ..., x_n = y_n$ and thus $X = Y$. Therefore, $F^{(2)}(X)$ is strong complete. We can also prove by induction that $F^{(k)}(X)$ are strong complete for all $k = 2, 3, ..., t$. □

Proposition 3.3. *Assume that $f(x)$ is a permutation and that $f(dx) + f(x)$, $f(dx) - f(x)$ are also permutations where $d \in \mathbb{F}_q$, $d \neq 0$, $d \neq \pm 1$. Then the polynomial $g_d(x) = f(df^{-1}(x))$ is strong complete.*

Proof. Assume that $f(x)$, $f(dx) + f(x)$ and $f(dx) - f(x)$ are permutations. Let $x = f^{-1}(y)$. Then $f(df^{-1}(y))$, $f(df^{-1}(y)) + y$ and $f(df^{-1}(y)) - y$ are permutations. Therefore, $g_d(x) = f(df^{-1}(x))$ is a strong complete polynomial. □

Note that $g_d^{(2)}(x) = g_d(f(df^{-1}(x)) = f(df^{-1}(fdf^{-1}(x))) = f(d^2f^{-1}(x)) = g_{d^2}(x)$ and, by induction $g_d^{(k)}(x) = g_{d^k}(x)$.

A permutation polynomial $f(x)$ such that $f(dx) - f(x)$ is also a permutation for all $d \in \mathbb{F}_q$, $d \neq 1$, is called a Costas polynomial. The only Costas polynomial over a field of the prime order p is x^s where $\gcd(s, p-1) = 1$. The only known Costas polynomial over $\mathbb{F}_q$ is $L(x^s)$ where $\gcd(s, q-1) = 1$ and L is a linearized permutation polynomial (see [4]). The polynomial $L(x^s)$ satisfies the conditions of Proposition 2.5. Indeed, $L(dx^s) \pm L(x^s) = L((d \pm 1)x^s)$ is permutation polynomial whenever $d \pm 1 \neq 0$ and $d \neq 0$. Thus, $g_d(x) = L(d^sL^{-1}(x))$ is strong complete polynomial for all $d^s \notin \{0, 1, -1\}$. Then, $g_d^{(k)}(x) = g_{d^k}(x)$ is the strong complete polynomial whenever $d^{ks} \notin \{0, 1, -1\}$. If $d^{sk_1} + d^{sk_2} + \cdots + d^{sk_t} \notin \{0, 1, -1\}$ for a set of positive integers $\mathcal{K} = \{k_1, k_2, ..., k_t\}$ then

$$\sum_{i=1}^{t} g_d^{k_i}(x) \pm x = \sum_{i=1}^{t} L(d^{sk_i}L^{-1}(x)) \pm x = L((\sum_{i=1}^{t} d^{sk_i})L^{-1}(x)) \pm x$$

is also a permutation. It follows that $g_d(x)$ is the $\mathcal{K}$-strong complete mapping (see [6]). This class of $\mathcal{K}$-strong complete polynomials is linearized. Now, we will present one more construction of the nonlinearized generalized strong complete polynomials over extension fields.

Theorem 3.4. *Let $f_i(x)$ be permutation polynomials over $\mathbb{F}_q$ such that $f_i(d^kx) \pm f_i(x)$ are permutation polynomials for $d \in \mathbb{F}_q^*$, $k = 1, 2, ..., t < q-1$ and $i = 1, 2, ..., n$. Let $\psi_i : \mathbb{F}_q^i \to \mathbb{F}_q$ be arbitrary functions for $i = 1, 2, \ldots, n-1$. Denote $X = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$. Then the mapping*

$$F(X) = f_1(x_1)\alpha_1 + [f_2(x_2) + \psi_1(x_1)]\alpha_2 + \cdots + [f_n(x) + \psi_{n-1}(x_1, x_2, \ldots, x_{n-1})]\alpha_n$$

is a permutation polynomial such that $F(d^kX) \pm F(X)$ are permutation polynomials for all $k = 1, 2, ..., t$.

Note: For functions $f_i(x)$ we can take $L(x^s)$ as discussed above.

Proof. As $d^k \in \mathbb{F}_q^*$ we have that $d^k X = d^k x_1\alpha_1 + d^k x_2\alpha_2 + ... + d^k x_n\alpha_n$. Assume $F(d^k X) \pm F(X) = F(d^k Y) \pm F(Y)$. Then, equating the coefficients with the basis elements, we get $f_1(d^k x_1) \pm f_1(x_1) = f_1(d^k y_1) \pm f_1(y_1)$. Thus $x_1 = y_1$. Further, $f_2(d^k x_2) + \psi_1(d^k x_1) \pm (f_2(x_2) + \psi_1(x_1)) = f_2(d^k y_2) + \psi_1(d^k y_1) \pm (f_2(y_2) + \psi_1(y_1))$. Since $x_1 = y_1$, we have $f_2(d^k x_2) \pm f_2(x_2) = f_2(d^k y_2) \pm f_2(y_2)$. It follows that $x_2 = y_2$. By induction, $x_3 = y_3, ..., x_n = y_n$. Hence, $X = Y$. Therefore, $F(d^k X) \pm F(X)$ are permutations for all $k = 1, 2, ..., t$. □

Corollary 3.5. *For a function $F(X)$ defined in* Theorem 3.4*, the function $G_d(X) = F(dF^{-1}(X))$ is strong complete mapping with a property that $G_d^{(k)}(X)$ are strong complete mappings for all $d = 1, 2, ..., t$.*

Proof. The result follows from Proposition 3.3 and $G_d^{(k)}(X) = G_{d^k}(X)$. □

Note: If we put $x_1 = x_2 = \ldots = x_{n-1} = 0$ and $x_n = 1$, then in all constructions presented in Section 3 we will form a cycle whose elements are of the form $(0, 0, \ldots, 0, s)$. The length of this cycle is less or equals to q. Using Lemma 2.2, we obtain $t < q$. Therefore, by means of Theorem 2.1 we can not obtain more than $2q$ of MOLS over $\mathbb{F}_{q^n}$ using constructions in the Section 3.

ORCID iDs

Amela Muratović-Ribić https://orcid.org/0000-0001-7903-4884

References

[1] W.-S. Chou, *Permutation polynomials on finite fields and their combinatorial applications*, Ph.D. thesis, Penn State Universit, 1990, `https://www.proquest.com/openview/24d2ca00f8f48ffe88a97a7c431a2096/1?pq-origsite=gscholar&cbl=18750&diss=y`.

[2] A. B. Evans, The existence of strong complete mappings of finite groups: a survey, *Discrete Math.* **313** (2013), 1191–1196, doi:10.1016/j.disc.2011.11.040.

[3] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in cryptography, *Finite Fields Appl.* **25** (2014), 306–315, doi:10.1016/j.ffa.2013.10.008.

[4] A. Muratović-Ribić, A. Pott, D. Thomson and Q. Wang, On the characterization of a semi-multiplicative analogue of planar functions over finite fields, in: *Topics in finite fields*, Amer. Math. Soc., Providence, RI, volume 632 of *Contemp. Math.*, pp. 317–325, 2015, doi:10.1090/conm/632/12635.

[5] A. Muratović-Ribić and S. Surdulli, On strong complete monomials and its multiplicative analogue over finite fields, *Sarajevo J. Math.* **16(29)** (2020), 137–144, doi:10.5644/sjm.

[6] A. Winterhof, Generalizations of complete mappings of finite fields and some applications, *J. Symbolic Comput.* **64** (2014), 42–52, doi:10.1016/j.jsc.2013.12.006.

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.10 / 309–317
https://doi.org/10.26493/1855-3974.2049.3db
(Also available at http://amc-journal.eu)

Point-primitive generalised hexagons and octagons and projective linear groups*

Stephen P. Glasby †, Emilio Pierro ‡, Cheryl E. Praeger

Centre for the Mathematics of Symmetry and Computation, Department of Mathematics and Statistics, The University of Western Australia

Received 16 July 2019, accepted 8 April 2021, published online 11 November 2021

Abstract

We discuss recent progress on the problem of classifying point-primitive generalised polygons. In the case of generalised hexagons and generalised octagons, this has reduced the problem to primitive actions of almost simple groups of Lie type. To illustrate how the natural geometry of these groups may be used in this study, we show that if $\mathcal{S}$ is a finite thick generalised hexagon or octagon with $\mathcal{G} \leqslant \mathrm{Aut}(\mathcal{S})$ acting point-primitively and the socle of $\mathcal{G}$ isomorphic to $\mathrm{PSL}_n(q)$ where $n \geqslant 2$, then the stabiliser of a point acts irreducibly on the natural module. We describe a strategy to prove that such a generalised hexagon or octagon $\mathcal{S}$ does not exist.

Keywords: Generalised hexagon, generalised octagon, generalised polygon, primitive permutation group.

Math. Subj. Class. (2020): 51E12, 20B15, 05B25

1 Introduction

We show in this paper that the Aschbacher–Dynkin [2] classification of maximal subgroups of classical groups is a potentially useful tool to investigate whether or not a finite thick

*This work was supported by the Australian Research Council. Discovery Project Grants DP140100416 and DP190100450. The research reported in the paper forms part of the Australian Research Council (ARC) Discovery Project Grant DP140100416 of the first and third authors. The authors gratefully acknowledge support from the Australian Research Council Discovery Project Grants DP140100416 and DP190100450; and also advice from an anonymous referee on exposition. This research was conducted at the University of Western Australia whose campus we acknowledge is located on the traditional lands of the Whadjuk people of the Noongar Nation. We pay our respects to Noongar Elders past, present and emerging.

†Corresponding author.

‡Author gratefully acknowledges the support of the ARC Discovery Project Grant DP140100416.

E-mail addresses: stephen.glasby@uwa.edu.au (Stephen P. Glasby), e.pierro@mail.bbk.ac.uk (Emilio Pierro), cheryl.praeger@uwa.edu.au (Cheryl E. Praeger)

generalised hexagon or octagon admits a large rank classical group as an automorphism group with a point-primitive action.

The notion of a generalised polygon arose from the investigations of Tits [12] and is connected with the groups of Lie type having twisted Lie rank 2. They belong to a wider class of geometric objects known as buildings, which were also introduced by Tits, whose motivation was to find natural geometric objects on which the finite groups of Lie type act, in order to work towards a proof of the classification of finite simple groups. Indeed, all families of simple groups of Lie type having twisted Lie rank 2 arise as automorphism groups of generalised polygons.

An *incidence geometry* $\mathcal{S} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ *of rank 2* consists of a point set $\mathcal{P}$, a line set $\mathcal{L}$ and an incidence relation $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$ such that $\mathcal{P}$ and $\mathcal{L}$ are disjoint non-empty sets. We say that $\mathcal{S}$ is finite if $|\mathcal{P} \cup \mathcal{L}|$ is finite. The *dual* of $\mathcal{S}$ is $\mathcal{S}^D = (\mathcal{L}, \mathcal{P}, \mathcal{I}^D)$, where $(p, \ell) \in \mathcal{I}$ if and only if $(\ell, p) \in \mathcal{I}^D$. We say that $\mathcal{S}$ is *thick* if each point is incident with at least three lines and each line is incident with at least three points. A *flag* of $\mathcal{S}$ is a set $\{p, \ell\}$ with $p \in \mathcal{P}$, $\ell \in \mathcal{L}$ and $(p, \ell) \in \mathcal{I}$. The *incidence graph* of $\mathcal{S}$ is the bipartite graph whose vertices are $\mathcal{P} \cup \mathcal{L}$ and whose edges are the flags of $\mathcal{S}$. A *generalised n-gon* is, then, a thick incidence geometry of rank 2 whose incidence graph is connected of diameter n and girth $2n$ such that each vertex lies on at least three edges [13, Lemma 1.3.6]. It is not immediate, but if $\mathcal{S}$ is a thick generalised n-gon, then there exist constants $s, t \geqslant 2$ such that each point is incident with $t + 1$ lines and each line is incident with $s + 1$ points [13, Corollary 1.5.3]. We then say that the *order* of $\mathcal{S}$ is (s, t). A *collineation* of $\mathcal{S}$ is a pair $(\alpha, \beta) \in \mathrm{Sym}(\mathcal{P}) \times \mathrm{Sym}(\mathcal{L})$ that preserves the subset $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$. The subset of all collineations of $\mathrm{Sym}(\mathcal{P}) \times \mathrm{Sym}(\mathcal{L})$ is a subgroup denoted $\mathrm{Aut}(\mathcal{S})$. A celebrated result of Feit and Higman [8] states that if $\mathcal{S}$ is a finite thick generalised n-gon, then $n \in \{2, 3, 4, 6, 8\}$. We refer the reader to Van Maldeghem's book [13] both for further details about classical generalised polygons, and for a full introduction to the theory of generalised polygons.

In this paper we shall only be concerned in the case that $\mathcal{S}$ is a finite thick generalised hexagon or octagon. At present the only known examples of these are the split Cayley hexagon $H(q)$, the twisted triality hexagon $T(q, q^3)$, the Ree–Tits octagon $O(2^{2m+1})$ and their duals. These correspond to the groups $G_2(q)$, ${}^3D_4(q)$ and ${}^2F_4(2^{2m+1})$ and complete descriptions of these can be found in [13].

The *point graph* of a generalised polygon $\mathcal{S}$ is the graph with points as vertices and with two points adjacent if they are collinear. The classification of (not necessarily thick) generalised polygons admitting an automorphism group which acts distance-transitively on the point graph of $\mathcal{S}$ is due to Buekenhout and Van Maldeghem [6]. In addition, they show that distance-transitivity implies that $\mathcal{G}$ acts primitively on $\mathcal{P}$. If $\mathcal{S}$ is also thick, then Buekenhout and Van Maldeghem show that the socle of $\mathcal{G}$ is a finite simple group of Lie type having twisted Lie rank 2. The assumption of distance-transitivity for this graph is strong, and in recent years there has been work by a number of authors to show that the assumption of distance-transitivity can be relaxed.

Schneider and Van Maldeghem [11, Theorem 2.1] showed that if $\mathcal{G} \leqslant \mathrm{Aut}(\mathcal{S})$ acts flag-transitively, point-primitively and line-primitively, then $\mathcal{G}$ is an almost simple group of Lie type. The following theorem, which significantly strengthened this result, provided motivation for the present paper.

Theorem 1.1 ([3, Theorem 1.2]). *Let $\mathcal{S}$ be a finite thick generalised hexagon or octagon. If a subgroup $\mathcal{G}$ of* $\mathrm{Aut}(\mathcal{S})$ *acts point-primitively, then $\mathcal{G}$ is an almost simple group of Lie type.*

The proof of Theorem 1.1 relies on the classification of finite simple groups. In order to rule out certain possibilities for $\mathrm{soc}(G)$, it is sufficient to consider the primitive actions of the almost simple groups of Lie type, or equivalently, their maximal subgroups. For an exceptional Lie type group that has a faithful projective representation in defining characteristic of degree at most 12, a complete classification of its maximal subgroups is summarised in [4, Chapter 7]. Using this classification it was proved by Morgan and Popiel in [9] that under the hypothesis of the above theorem, if in addition it is assumed that the socle of $\mathcal{G}$ is isomorphic to one of the Suzuki–Ree groups, ${}^2B_2(2^{2m+1})'$, ${}^2G_2(3^{2m+1})'$ or ${}^2F_4(2^{2m+1})'$, where $m \geqslant 0$, then up to point-line duality, $\mathcal{S}$ is the Ree–Tits octagon $O(2^{2m+1})$. For a general classical group $\mathcal{G}$, however, we appeal to the Aschbacher–Dynkin classification [2] of its maximal subgroups. The maximal subgroups of $\mathcal{G}$ fall into eight families of "geometric" subgroups, those which preserve a natural geometric structure, and a ninth class of exceptions. These classes are denoted $\mathscr{C}_i$ for $1 \leqslant i \leqslant 9$, and some authors denote $\mathscr{C}_9$ as $\mathscr{S}$. The class $\mathscr{C}_1$ consists of stabilisers of subspaces and includes the maximal parabolic subgroups of $\mathcal{G}$. Our main result is as follows.

Theorem 1.2. *Let $\mathcal{S}$ be a finite thick generalised hexagon or octagon. If $\mathcal{G} \leqslant \mathrm{Aut}(\mathcal{S})$ acts point-primitively on $\mathcal{S}$ and the socle of $\mathcal{G}$ is isomorphic to $\mathrm{PSL}_n(q)$ where $n \geqslant 2$, then the stabiliser of a point of $\mathcal{S}$ is not the stabiliser in $\mathcal{G}$ of a subspace of the natural module $V = (\mathbb{F}_q)^n$.*

The subspace stabilisers considered in Theorem 1.2 are all maximal parabolic subgroups. Given this result, and in the light of the result of Morgan and Popiel [9] mentioned above, it would in the first instance be good to handle all primitive coset actions of Lie type groups on maximal parabolic subgroups.

Problem 1.3. Extend Theorem 1.2 to show that, if $\mathcal{S}$ is a finite thick generalised hexagon or octagon and $\mathcal{G} \leqslant \mathrm{Aut}(\mathcal{S})$ is an almost simple group of Lie type such that the stabiliser $\mathcal{G}_x$ of a point x is a maximal parabolic subgroup, then $(\mathcal{S}, \mathcal{G})$ is one of the known classical examples.

Problem 1.3 has been solved for the Suzuki–Ree groups in [9], and it has also been solved by Popiel and the second author [10] for the groups $G_2(q)'$. It would be especially interesting to have a solution to Problem 1.3 for the groups of (twisted or untwisted) Lie rank 2, and in particular for the family ${}^3D_4(q)'$ which is the only untreated case where the groups are known to act on a generalised hexagon or octagon. Moreover, it would be even more interesting to have a characterisation of all point-primitive actions of groups with socle $G_2(q)'$ or ${}^3D_4(q)'$ on a thick generalised hexagon or octagon (not just the coset actions on maximal parabolic subgroups). This, however, seems to be a substantially harder problem.

Maximal parabolic subgroups mentioned in Problem 1.3 are examples of large subgroups, a notion introduced by Alavi and Burness in [1], namely a subgroup H of a finite group G is *large* if $|H|^3 > |G|$. In [1] all large subgroups of all finite simple groups are determined. In our view the next level of attack on the general classification problem would be to handle actions on cosets of large subgroups.

Problem 1.4. Extend Theorem 1.2 to show that, if $\mathcal{S}$ is a finite thick generalised hexagon or octagon and $\mathcal{G} \leqslant \mathrm{Aut}(\mathcal{S})$ is an almost simple group of Lie type such that the stabiliser $\mathcal{G}_x$ of a point is a large maximal subgroup, then $(\mathcal{S}, \mathcal{G})$ is one of the known classical examples.

Popiel and the second author [10] have almost solved Problem 1.4 for groups $\mathcal{G}$ with socle $G_2(q)'$. The only unresolved point-primitive action is on a generalised hexagon with stabiliser satisfying $\mathcal{G}_x \cap \operatorname{soc}(G) \cong G_2(q^{1/2})$.

The result of Alavi and Burness [1, Theorem 4] for groups $\mathcal{G} \cong \mathrm{PSL}_n(q)$, taking into account Theorem 1.2 for parabolic actions and using properties of the parameters of a generalised n-gon, shows that a solution to Problem 1.4 for these groups involves consideration of just four kinds of point actions. We follow Alavi and Burness in using *type* to denote a rough approximation of the structure of a subgroup.

Proposition 1.5. *Let $\mathcal{S}$ be a finite thick generalised hexagon or octagon of order (s,t). Suppose that $\mathcal{G} \leqslant \mathrm{Aut}(\mathcal{S})$ with $\mathcal{G} \cong \mathrm{PSL}_n(q)$, and $\mathcal{G}$ acts point-primitively on $\mathcal{S}$ such that the stabiliser $\mathcal{G}_x$ of a point x is a large subgroup. Then one of the following holds:*

(a) $\mathcal{G}_x$ is a $\mathscr{C}_2$-subgroup of type $\mathrm{GL}_{n/k}(q) \wr S_k$, where $k = 2$ or $k = 3$;

(b) $\mathcal{G}_x$ is a $\mathscr{C}_3$-subgroup of type $\mathrm{GL}_{n/k}(q^k)$, where $k = 2$ or $k = 3$;

(c) $\mathcal{G}_x$ is a $\mathscr{C}_5$-subgroup of type $\mathrm{GL}_n(q_0)$ with $q = q_0^k$, and either $k = 2$ or $k = 3$, or;

(d) $\mathcal{G}_x \in \mathscr{C}_8$ of type $\mathrm{Sp}_n(q)$ (n even), $\mathrm{SU}_n(q_0)$ ($q = q_0^2$), $\mathrm{SO}_n(q)$ (nq odd), or $\mathrm{SO}_n^{\epsilon}(q)$ (n even, $\epsilon = \pm$).

Proof of Proposition 1.5. In addition to the classes asserted in the statement of the proposition, Alavi and Burness show that either $\mathcal{G}_x \in \mathscr{C}_1$, which is excluded by Theorem 1.2, or $\mathcal{G}_x$ is one of finitely many cases belonging to classes $\mathscr{C}_6$ or $\mathscr{C}_9$ [1, Proposition 4.7 and Theorem 4(ii)]. Of these, the cases where $\mathcal{G}$ is a group appearing in the Atlas [7] are excluded by [5, Theorems 1.1 and 1.2]. The remaining possibilities for $(\mathcal{G}, \mathcal{G}_x)$ are:

$\mathcal{G}$	$\mathrm{PSL}_5(3)$	$\mathrm{PSL}_4(5)$	$\mathrm{PSL}_4(7)$	$\mathrm{PSL}_2(q)$ $q \in \{41, 49, 59, 61, 71\}$
$\mathcal{G}_x$	M_{11}	$2^4 . A_6$	$\mathrm{PSU}_4(2)$	A_5

The number $|\mathcal{P}|$ of points is the polynomial $f(s,t) = (s+1)(s^2t^2 + st + 1)$ if $\mathcal{S}$ is a generalised hexagon, and $f(s,t) = (s+1)(s^3t^3 + s^2t^2 + st + 1)$ if $\mathcal{S}$ is a generalised octagon. Running through the possibilities for $|\mathcal{P}| = |\mathcal{G} : \mathcal{G}_x|$ from the table above, we find that there are no solutions to the equation $|\mathcal{P}| = f(s,t)$ with $s, t \geqslant 2$. This completes the proof. □

Extending Theorem 1.2 to include the large subgroups in class $\mathscr{C}_2$ has also proven to be unexpectedly challenging to the authors.

2 The proof of Theorem 1.2

To prove Theorem 1.2, we assume for a contradiction that $\mathcal{S}$ is a thick generalised hexagon or octagon and $\mathcal{G} \leqslant \mathrm{Aut}(\mathcal{S})$, with $\operatorname{soc}(\mathcal{G}) = \mathrm{PSL}_n(q)$, is such that a point stabiliser is maximal in $\mathcal{G}$ and is the stabiliser of a k-subspace of the natural module $V = (\mathbb{F}_q)^n$, where $0 < k < n$. Hence we may identify the point set $\mathcal{P}$ of $\mathcal{S}$ with the set of k-subspaces of V, which we denote by $\binom{V}{k}$. If $\mathcal{G}$ contains a graph automorphism then $k = n/2$ and, for its index 2 subgroup $\mathcal{H} = \mathcal{G} \cap \mathrm{P\Gamma L}_n(q)$, the stabiliser $\mathcal{H}_U$ is maximal in $\mathcal{H}$. Thus we may assume that $\mathrm{PSL}_n(q) \trianglelefteqslant \mathcal{G} \leqslant \mathrm{P\Gamma L}_n(q)$. It is convenient in the proofs to work with a group G such that $\mathrm{SL}_n(q) \trianglelefteq G \leqslant \Gamma\mathrm{L}_n(q)$ acting linearly on V, with the scalar matrices acting trivially on $\binom{V}{k}$, so $\mathcal{G} = G/Z$ where Z is the subgroup of scalars. Since a graph automorphism of G maps $\binom{V}{k}$ to $\binom{V}{n-k}$, and hence maps $\mathcal{S}$ to an isomorphic generalised polygon with point set identified with $\binom{V}{n-k}$, we may assume further that $1 \leqslant k \leqslant n/2$, and so the following hypotheses hold.

Hypothesis 2.1. *Let $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ be a finite thick generalised hexagon or octagon of order (s,t), such that $\mathcal{P}$ is identified with the set $\binom{V}{k}$ of k-subspaces of $V = (\mathbb{F}_q)^n$, where $1 \leqslant k \leqslant n/2$. Suppose that $\mathrm{SL}_n(q) \trianglelefteq G \leqslant \Gamma\mathrm{L}_n(q)$ and that G induces a group of automorphisms of $\mathcal{S}$ acting naturally on $\mathcal{P}$, (so that a point stabiliser belongs to class $\mathscr{C}_1$).*

Our proof of Theorem 1.2 uses the following three lemmas. The first is from [3].

Lemma 2.2 ([3, Lemma 2.1(iv)])**.** *Let $\mathcal{S}$ be a finite thick generalised hexagon or octagon of order (s,t), and let $\mathcal{P}$ denote the set of points of $\mathcal{S}$. Let $x, y_1, y_2 \in \mathcal{P}$ such that $x \sim y_1$ and $x \sim y_2$, and let $g \in \mathrm{Aut}(\mathcal{S})$ such that $xg \neq x$. If g fixes y_1 and y_2, then x, y_1, y_2, xg all lie on a common line.*

The second lemma is not difficult to prove, and its proof is left to the reader.

Lemma 2.3. *Suppose $\mathrm{SL}_n(q) \trianglelefteq G \leqslant \Gamma\mathrm{L}_n(q)$, $V = (\mathbb{F}_q)^n$ and $k \leqslant n/2$. Then, if $\dim(V) = n$ and $k \leqslant n/2$, then the orbits of G on $\binom{V}{k} \times \binom{V}{k}$ are*

$$\Gamma_i = \left\{(x,y) \in \binom{V}{k} \times \binom{V}{k} \mid \dim(x \cap y) = i\right\} \quad \text{where } 0 \leqslant i \leqslant k. \tag{2.1}$$

Moreover, for $x \in \binom{V}{k}$ the orbits of G_x, are

$$\Gamma_i(x) = \left\{y \in \binom{V}{k} \mid \dim(x \cap y) = i\right\} \quad \text{where } 0 \leqslant i \leqslant k.$$

The third lemma allows us to characterise adjacency in $\mathcal{S}$.

Lemma 2.4. *Assume Hypothesis 2.1 and let $x, y \in \mathcal{P}$. Then the following properties hold.*

(F1) *For every $i \in \{0, \ldots, k\}$, if x, y are collinear and $\dim(x \cap y) = i$, then any $x', y' \in \mathcal{P}$ with $\dim(x' \cap y') = i$ are also collinear.*

(F2) *For every $i \in \{0, \ldots, k-1\}$, if x, y are collinear and $\dim(x \cap y) = i$, then there exists $y' \in \mathcal{P}$ such that $\dim(x \cap y') = i$ and $y' \not\sim y$.*

Proof. Property (F1) follows from Lemma 2.3. For (F2), suppose towards a contradiction that every point y' with $\dim(x \cap y') = i$ is collinear with y. By (F1), every such point y' is also collinear with x, and hence lies on the line ℓ through x and y (because otherwise $\{x, y, y'\}$ would form a triangle and $\mathcal{S}$ contains no triangles). Let $J = J(n,k)_i$ denote the generalised Johnson graph with vertex set $V(J) = \binom{V}{k}$ and two vertices adjacent if and only if they intersect in an i-subspace. Since G acts primitively on $\binom{V}{k}$, and since the connected components are G-invariant, J is a connected graph. Note that Property (F1) implies that adjacency in J implies collinearity, but the converse is not necessarily true. By definition of J, $y, y' \in J_1(x)$, the set of vertices adjacent to x in J. By the above argument, $\{x\} \cup J_1(x)$ is contained in the line ℓ. Since G acts transitively on J and since adjacency is preserved by this action, it is true for all $u \in \mathcal{P}$ that $\{u\} \cup J_1(u)$ is contained in a line of $\mathcal{S}$. Since $\mathcal{S}$ has more than one line, the diameter of J is at least 2.

We now prove by induction on the distance d, where $2 \leqslant d \leqslant \mathrm{diam}(J)$, that, for any vertices u, v of J, if the distance $d = \delta(u, v)$ and $(u_0, u_1, \ldots, u_d)$ is a path of length d in J from $u = u_0$ to $v = u_d$, then $\{u_0, \ldots, u_d\}$ is contained in the line ℓ containing $\{u\} \cup J_1(u)$. First we prove this for $d = 2$. Suppose that $\delta(u, v) = 2$ and let (u, w, v) be a path of length 2 in J from u to v. Note that $w \in J_1(u) \subseteq \ell$. Also u, v both lie in $\{w\} \cup J_1(w)$ which, as we have shown, is contained in some line ℓ' of $\mathcal{S}$. Then u, w are contained in both ℓ and ℓ', and since two points lie in at most one line of $\mathcal{S}$ it follows that $\ell' = \ell$, and so u, w, v all lie in ℓ and the inductive assertion is proved for $d = 2$. Now suppose inductively that $3 \leqslant d \leqslant \mathrm{diam}(J)$ and that the assertion is true for all integers from 2 to $d - 1$. Suppose that $\delta(u, v) = d$ and that $(u_0, u_1, \ldots, u_d)$ is a path in J from $u = u_0$ to $v = u_d$. Then $\delta(u, u_{d-1}) = d - 1$, so by induction $\{u_0, \ldots, u_{d-1}\} \subseteq \ell$. Also $u_{d-2}, v \in \{u_{d-1}\} \cup J(u_{d-1})$, which we have shown to be contained in some line ℓ'; since u_{d-2}, u_{d-1} are contained in both ℓ and ℓ', it follows that $\ell' = \ell$, and the inductive assertion is proved for d. Hence by induction the assertion holds for all $d \leqslant \mathrm{diam}(J)$. However, this is a contradiction because the points of $\mathcal{S}$ do not all lie on a single line. □

We are now in a position to prove Theorem 1.2.

Proof of Theorem 1.2. As discussed at the beginning of this section we may assume that Hypothesis 2.1 holds. Thus $\mathcal{P} = \binom{V}{k}$ and $k \leqslant n/2$.

CLAIM 1: $k \geqslant 4$. Consider the action of G on $\mathcal{P} \times \mathcal{P}$. For each i with $0 \leqslant i \leqslant k - 1$, G acts transitively on the set Γ_i defined in (2.1) by Lemma 2.3. It is a standard result in the theory of permutation groups that the orbits of G on $\mathcal{P} \times \mathcal{P}$ are in one-to-one correspondence with the orbits of G_x on $\mathcal{P}$, and there must be at least one G_x-orbit for each possible distance from x in the point graph of $\mathcal{S}$. If $k < 3$, then the number of orbits of G_x is less than four, so no point of $\mathcal{P} \setminus \{x\}$ is at distance 3 from x in $\mathcal{S}$, contradicting the assumption that $\mathcal{S}$ is either a generalised hexagon or a generalised octagon. If $k = 3$, then for the same reason $\mathcal{S}$ is not a generalised octagon, and so $\mathcal{S}$ is a generalised hexagon and G acts distance transitively on the point graph. By the main result of Buekenhout and Van Maldeghem in [6], $\mathcal{S}$ is a classical generalised hexagon and its distance transitive group has socle $G_2(r^f)$ for some prime power r^f, which is a contradiction. Hence $k \geqslant 4$ as claimed.

Now let $\{e_1, \ldots, e_n\}$ be a basis of V and take $x = \langle e_1, \ldots, e_k\rangle$. Let $k_1 < k$ be maximal such that there exists a point $y \sim x$ with $(x, y) \in \Gamma_{k_1}$ (as defined in (2.1)). Note that, by Claim 1, $n \geqslant 2k \geqslant 8$.

CLAIM 2: $k_1 < k - 1$. For a contradiction, assume that $k_1 = k - 1$ and without loss of generality that $y = \langle e_1, \ldots, e_{k-1}, e_{k+1}\rangle$. By (F2) there exists a point $y' \in \mathcal{P}$ such that $(x, y') \in \Gamma_{k-1}$ and $y \nsim y'$ and by (F1) we have $x \sim y'$ and so $\dim(x \cap y') = k - 1$ and $\dim(y \cap y') \leqslant k - 2$. Now $\dim(x \cap y) = \dim(x \cap y') = k - 1$ implies that $\dim(x \cap y \cap y') \geqslant k - 2$, and hence $\dim(y \cap y') = \dim(x \cap y \cap y') = k - 2$. We may assume without loss of generality that $y' = \langle e_2, \ldots, e_k, e_{k+2}\rangle$. But now the permutation matrix corresponding to $(1, k+1)(k, k+2)$ leaves y and y' fixed, but not x. By Lemma 2.2, this implies that $y \sim y'$, a contradiction. Hence $k_1 < k - 1$, as required.

CLAIM 3: $k_1 = 0$. Assume to the contrary that $k_1 > 0$. Recall that $k_1 < k$ is maximal such that there exists a point $y \sim x$ with $y \in \Gamma_{k_1}$. Thus we may assume that

$$y = \langle e_1, \ldots, e_{k_1}, e_{k+1}, \ldots, e_{2k-k_1}\rangle.$$

If $2k - k_1 + 1 \leqslant n$, let

$$z = \langle e_1, \dots, e_{k_1}, e_{k+2}, \dots, e_{2k-k_1+1} \rangle$$

so that $\dim(x \cap z) = k_1$ and $\dim(y \cap z) = k - 1 > k_1$. It then follows from (F1) that $x \sim z$ and from Claim 2 and the maximality of k_1 that $y \nsim z$. Since $1 \leqslant k_1 \leqslant k-2$, we have $k + 2 \leqslant 2k - k_1$ and hence the permutation matrix corresponding to $(1, k+2)(k, k-1)$ fixes y and z but not x. But once again Lemma 2.2 implies that $y \sim z$, a contradiction. Therefore $k_1 = 0$ as claimed.

An immediate corollary of Claim 3 and (F1) is that G acts flag-transitively on $\mathcal{S}$.

CLAIM 4: $n = 2k$ or $2k+1$. For a contradiction, suppose that $2k+1 < n$ and recall $k \leqslant n/2$. Let $y = \langle e_{k+1}, \dots, e_{2k} \rangle$ and $z = \langle e_{k+2}, \dots, e_{2k+1} \rangle$. Observe that $x \sim y$, $x \sim z$ by $(F1)$; furthermore $\dim(y \cap z) = k - 2 > 0$, so $y \nsim z$ by the maximality of k_1. Since $k \geqslant 4$ by Claim 1, the permutation matrix corresponding to $(1, 2k+2)(2,3)$ fixes y and z but not x, contradicting Lemma 2.2.

CLAIM 5: $n = 2k$. Assume $n = 2k+1$. Let y be as in Claim 4 and let $z = \langle e_{k+1}, \dots, e_{2k-1}, e_1 + e_{2k+1} \rangle$. Then $x \sim y$ and $x \sim z$ by Claim 3 and since $\dim(y \cap z) = k - 1 > 0$, we see that $y \nsim z$ by Claim 3. Once again we apply Lemma 2.2 by noting that since $k \geqslant 4$, the permutation matrix for $(1, 2k+1)(k+1, k+2)$ leaves y and z fixed but not x, contradicting Lemma 2.2. Hence $n = 2k$ and Claim 5 is true.

To complete the proof let

$$\begin{aligned} x = \langle e_1, \dots, e_k \rangle, \qquad & y = \langle e_{k+1}, \dots, e_{2k} \rangle, \\ z = \langle e_1 + e_{k+1}, \dots, e_i & + e_{i+k}, \dots, e_k + e_{2k} \rangle. \end{aligned} \tag{2.2}$$

Then $\dim(x \cap y) = \dim(x \cap z) = \dim(y \cap z) = 0$, and so x, y and z are pairwise collinear by Claim 3. Then, since $\mathcal{S}$ does not contain any triangles, x, y and z lie on a line of $\mathcal{S}$, say ℓ. Consider the stabiliser G_ℓ. Note that ℓ is the unique line containing any pair of the elements x, y or z and so in particular, $G_\ell \geqslant \langle G_{xy}, G_{xz}, G_{yz} \rangle$. Writing vectors in V as n-dimensional row vectors over $\mathbb{F}_q$ relative to the basis $e_1, \dots, e_n$, and writing matrices relative to this basis, we see that x consists of all vectors of the form $(X, 0)$, where $X, 0$ denote k-dimensional row vectors, and the stabiliser G_x consists of all matrices $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in G$ for which $(I \mid 0)M$ has the form $(X \mid 0)$ where $X \in \mathrm{GL}_k(\mathbb{F}_q)$. Our aim is to show that $\langle G_{xy}, G_{xz}, G_{yz} \rangle$ contains $\mathrm{SL}_n(q)$. Let $H = \mathrm{SL}_n(q)$ and let $H_x = H \cap G_x$ and define H_y, H_z, H_{xy}, H_{xz}, H_{yz} and H_ℓ analogously. Let $M_k(q)$ denote the ring of all $k \times k$ matrices over $\mathbb{F}_q$, and recall that $k = n/2$. Then

$$H_x = \langle \left(\begin{smallmatrix} A & 0 \\ C & D \end{smallmatrix}\right) \in \mathrm{SL}_n(q) \mid A, D \in \mathrm{GL}_k(q), C \in M_k(q) \rangle.$$

Similarly,

$$H_y = \langle \left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right) \in \mathrm{SL}_n(q) \mid A, D \in \mathrm{GL}_k(q), B \in M_k(q) \rangle$$

and

$$H_z = \langle \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{SL}_n(q) \mid A + C = B + D \rangle.$$

From this we see that

$$H_{xy} = \langle \left(\begin{smallmatrix} A & 0 \\ 0 & D \end{smallmatrix}\right) \in \mathrm{GL}_n(q) \mid A, D \in \mathrm{GL}_k(q), \det(AD) = 1 \rangle.$$

Similarly,

$$H_{xz} = \langle \left(\begin{smallmatrix} A & 0 \\ D-A & D \end{smallmatrix}\right) \in \mathrm{GL}_n(q) \mid A, D \in \mathrm{GL}_k(q), \det(AD) = 1 \rangle$$

and

$$H_{yz} = \langle \left(\begin{smallmatrix} A & A-D \\ 0 & D \end{smallmatrix}\right) \in \mathrm{GL}_n(q) \mid A, D \in \mathrm{GL}_k(q), \det(AD) = 1 \rangle.$$

Our aim is now to show that $H_\ell := \langle H_{xy}, H_{xz}, H_{yz} \rangle$ is equal to H. We interrupt our proof of Theorem 1.2 to prove this in the following lemma.

Lemma 2.5. *The group generated by all matrices of the form* $\left(\begin{smallmatrix} A & 0 \\ 0 & D \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} A & A-D \\ 0 & D \end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix} A & 0 \\ D-A & D \end{smallmatrix}\right)$ *where* $A, D \in \mathrm{GL}_k(q)$ *and* $\det(AD) = 1$ *equals* $H := \mathrm{SL}_{2k}(q)$.

Proof. Let $L = \langle \left(\begin{smallmatrix} A & 0 \\ 0 & D \end{smallmatrix}\right), \left(\begin{smallmatrix} A & A-D \\ 0 & D \end{smallmatrix}\right), \left(\begin{smallmatrix} A & 0 \\ D-A & D \end{smallmatrix}\right) \mid A, D \in \mathrm{GL}_k(q), \det(AD) = 1 \rangle$ and let $x, y, z \in \binom{V}{k}$ be as in (2.2). Then, L contains the matrix $\left(\begin{smallmatrix} A & 0 \\ D-A & D \end{smallmatrix}\right)\left(\begin{smallmatrix} A^{-1} & 0 \\ 0 & D^{-1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} I & 0 \\ DA^{-1}-I & I \end{smallmatrix}\right)$. In particular, choosing $A = I$ and $D = I + E_{1,2}$ we have $DA^{-1} = I + E_{1,2}$ so that L contains the matrix $M = \left(\begin{smallmatrix} I & 0 \\ E_{1,2} & I \end{smallmatrix}\right)$. An element $h = h_{A,D} = \left(\begin{smallmatrix} A & 0 \\ 0 & D \end{smallmatrix}\right)$ conjugates $M = \left(\begin{smallmatrix} I & 0 \\ E_{1,2} & I \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} I & 0 \\ D^{-1}E_{1,2}A & I \end{smallmatrix}\right)$. Since L contains $\left(\begin{smallmatrix} A & 0 \\ 0 & A \end{smallmatrix}\right)$ for each permutation matrix A, it follows that L contains $\left(\begin{smallmatrix} I & 0 \\ E_{i,j} & I \end{smallmatrix}\right)$ for each i, j. Hence L contains H_x. Similarly, L contains H_y. Since H_x is maximal in H and $H_x \neq H_y$, we conclude that $L = H$. □

Resuming our proof: Lemma 2.5 implies that G_ℓ contains $\mathrm{SL}_n(q)$ and since G is primitive on points it follows that $\mathrm{SL}_n(q)$ and hence also G_ℓ, is transitive on points. This implies that ℓ is incident with all points, which is a contradiction. This completes the proof of Theorem 1.2. □

ORCID iDs

Stephen P. Glasby https://orcid.org/0000-0002-0326-1455
Emilio Pierro https://orcid.org/0000-0003-1300-7984
Cheryl E. Praeger https://orcid.org/0000-0002-0881-7336

References

[1] S. H. Alavi and T. C. Burness, Large subgroups of simple groups, *J. Algebra* **421** (2015), 187–233, doi:10.1016/j.jalgebra.2014.08.026.

[2] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469–514, doi:10.1007/bf01388470.

[3] J. Bamberg, S. P. Glasby, T. Popiel, C. E. Praeger and C. Schneider, Point-primitive generalised hexagons and octagons, *J. Comb. Theory Ser. A* **147** (2017), 186–204, doi:10.1016/j.jcta.2016.11.008.

[4] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, volume 407 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, 2013, doi:10.1017/cbo9781139192576.

[5] F. Buekenhout and H. Van Maldeghem, Remarks on finite generalized hexagons and octagons with a point-transitive automorphism group, in: A. Beutelspacher, F. Buekenhout, J. Doyen, F. De Clerck, J. A. Thas and J. W. P. Hirschfeld (eds.), *Finite Geometry and Combinatorics*, Cambridge University Press, Cambridge, volume 191 of *London Mathematical Society Lecture Note Series*, pp. 89–102, 1993, doi:10.1017/cbo9780511526336.011, Proceedings of the Second International Conference held in Deinze, May 31 – June 6, 1992.

[6] F. Buekenhout and H. Van Maldeghem, Finite distance-transitive generalized polygons, *Geom. Dedicata* **52** (1994), 41–51, doi:10.1007/bf01263523.

[7] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *An Atlas of Finite Groups*, Oxford University Press, Eynsham, 1985.

[8] W. Feit and G. Higman, The nonexistence of certain generalized polygons, *J. Algebra* **1** (1964), 114–131, doi:10.1016/0021-8693(64)90028-6.

[9] L. Morgan and T. Popiel, Generalised polygons admitting a point-primitive almost simple group of Suzuki or Ree type, *Electron. J. Combin.* **23** (2016), #P1.34 (12 pages), doi:10.37236/5510.

[10] E. Pierro and T. Popiel, On the action of $G_2(q)$ on generalised hexagons and octagons, preprint.

[11] C. Schneider and H. Van Maldeghem, Primitive flag-transitive generalized hexagons and octagons, *J. Comb. Theory Ser. A* **115** (2008), 1436–1455, doi:10.1016/j.jcta.2008.02.004.

[12] J. Tits, Sur la trialité et certains groupes qui s'en déduisent, *Inst. Hautes Études Sci. Publ. Math.* **2** (1959), 13–60, `http://www.numdam.org/item/PMIHES_1959__2__13_0/`.

[13] H. Van Maldeghem, *Generalized Polygons*, volume 93 of *Monographs in Mathematics*, Birkhäuser, 1998, doi:10.1007/978-3-0348-8827-1.

Author Guidelines

Before submission

Papers should be written in English, prepared in LaTeX, and must be submitted as a PDF file. The title page of the submissions must contain:

- *Title*. The title must be concise and informative.
- *Author names and affiliations*. For each author add his/her affiliation which should include the full postal address and the country name. If avilable, specify the e-mail address of each author. Clearly indicate who is the corresponding author of the paper.
- *Abstract*. A concise abstract is required. The abstract should state the problem studied and the principal results proven.
- *Keywords*. Please specify 2 to 6 keywords separated by commas.
- *Mathematics Subject Classification*. Include one or more Math. Subj. Class. (2020) codes – see https://mathscinet.ams.org/mathscinet/msc/msc2020.html.

After acceptance

Articles which are accepted for publication must be prepared in LaTeX using class file amcjoucc.cls and the bst file amcjoucc.bst (if you use BibTeX). If you don't use BibTeX, please make sure that all your references are carefully formatted following the examples provided in the sample file. All files can be found on-line at:

https://amc-journal.eu/index.php/amc/about/submissions/#authorGuidelines

Abstracts: Be concise. As much as possible, please use plain text in your abstract and avoid complicated formulas. Do not include citations in your abstract. All abstracts will be posted on the website in fairly basic HTML, and HTML can't handle complicated formulas. It can barely handle subscripts and greek letters.
Cross-referencing: All numbering of theorems, sections, figures etc. that are referenced later in the paper should be generated using standard LaTeX \label{...} and \ref{...} commands. See the sample file for examples.
Theorems and proofs: The class file has pre-defined environments for theorem-like statements; please use them rather than coding your own. Please use the standard \begin{proof} ... \end{proof} environment for your proofs.
Spacing and page formatting: Please do not modify the page formatting and do not use \medbreak, \bigbreak, \pagebreak etc. commands to force spacing. In general, please let LaTeX do all of the space formatting via the class file. The layout editors will modify the formatting and spacing as needed for publication.
Figures: Any illustrations included in the paper must be provided in PDF format, or via LaTeX packages which produce embedded graphics, such as TikZ, that compile with PdfLaTeX. (Note, however, that PSTricks is problematic.) Make sure that you use uniform lettering and sizing of the text. If you use other methods to generate your graphics, please provide .pdf versions of the images (or negotiate with the layout editor assigned to your article).

Subscription

Yearly subscription: 150 EUR

Any author or editor that subscribes to the printed edition will receive a complimentary copy of *Ars Mathematica Contemporanea*.

Subscription Order Form

Name: ....
E-mail: ....
Postal Address: ....
....
....
....

I would like to subscribe to receive ...... copies of each issue of
Ars Mathematica Contemporanea in the year 2021.

I want to renew the order for each subsequent year if not cancelled by e-mail:

☐ Yes ☐ No

Signature: ....

Please send the order by mail, by fax or by e-mail.

By mail: Ars Mathematica Contemporanea
UP FAMNIT
Glagoljaška 8
SI-6000 Koper
Slovenia

By fax: +386 5 611 75 71

By e-mail: info@famnit.upr.si

Printed in Slovenia by *IME TISKARNE*