VERJETNOST KOMUTIRANJA

URBAN JEZERNIK

Universidad del País Vasco

Math. Subj. Class. (2010): 20P05, 20D60, 20F65

Verjetnost komutiranja je verjetnost, da v dani končni množici, opremljeni z binarno operacijo, dva naključno izbrana elementa komutirata. V članku raziščemo vpliv algebraične strukture na njeno verjetnost komutiranja, pri čemer se osredotočimo predvsem na končne grupe. Razkrijemo nekaj lastnosti množice zavzetih verjetnosti komutiranja končnih grup. Predstavimo tudi sodobnejše posplošitve pojma verjetnosti komutiranja na neskončne grupe.

COMMUTING PROBABILITY

Commuting probability is the probability that in a given finite set equipped with a binary operation, two randomly chosen elements commute. In this paper, we explore the influence of the algebraic structure of this set on its commuting probability, focusing especially on finite groups. Some properties of the set of all commuting probability values of finite groups are revealed. We also present modern generalizations of the concept of commuting probability to infinite groups.

O verjetnosti komutiranja

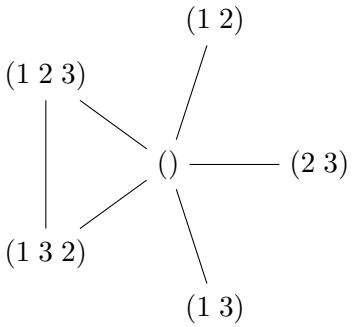
Opazujmo končno množico X, opremljeno z binarno operacijo. Verjetnost komutiranja $\mathrm{vk}(X)$ je verjetnost, da dva naključno in neodvisno izbrana elementa množice X komutirata glede na dano operacijo. Vrednost $\mathrm{vk}(X)$ izračunamo tako, da med vsemi urejenimi pari elementov v X izračunamo delež tistih, ki komutirajo.

Verjetnost komutiranja sta sistematično prvič raziskovala Erdös in Turán med razvijanjem lastne verjetnostne metode [3]. V pričujočem članku si ta koncept ogledamo iz različnih zornih kotov, pri čemer za vodilo vzamemo interakcijo med algebraično strukturo dane množice X in njeno verjetnostjo komutiranja $\mathrm{vk}(X)$.

Vstopimo s primeri.

Primer 1. Za X vzemimo simetrično grupo S_3, najmanjšo nekomutativno grupo. Spomnimo se, da S_3 sestoji iz šestih permutacij na treh točkah, kot je prikazano na naslednji sliki. Dve različni permutaciji sta na sliki povezani

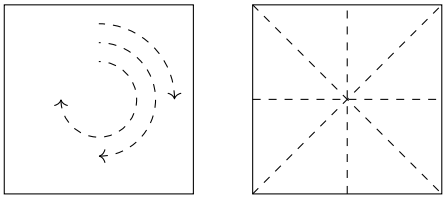
s povezavo, če in samo če komutirata.



Verjetnost komutiranja grupe S_3 izračunamo tako, da med vsemi urejenimi pari elementov izračunamo delež tistih, ki komutirajo. Število vseh urejenih parov elementov v S_3 je $6^2 = 36$. Komutirajoče pare preštejmo tako, da za vsak element posebej premislimo, s katerimi elementi komutira. Enota komutira z vsemi elementi. Dvocikli v S_3 paroma ne komutirajo. Prav tako noben od dvociklov ne komutira z nobenim triciklom. Tricikla (1 2 3) in (1 3 2) komutirata. Hkrati ne pozabimo, da vsak element komutira sam s sabo. Tako je število vseh komutirajočih urejenih parov v S_3 enako $6 + 3 \cdot 2 + 2 \cdot 3 = 18$ in zato je verjetnost, da je naključno izbrani urejeni par komutirajoč, enaka $\mathrm{vk}(S_3) = \frac{18}{36} = \frac{1}{2}$.

V simetričnih grupah višjih redov S_n število urejenih parov elementov raste zelo hitro, komutirajoči pari pa so, razen disjunktnih ciklov, bolj izjemne sorte. Pričakujemo torej, da velja $\lim_{n\to\infty} \mathrm{vk}(S_n) = 0$. Res je tako, utemeljitev podamo v posledici 7.

Primer 2. Za X vzemimo simetrije kvadrata, predstavljene kot diedrska grupa D_4. Spomnimo se, da D_4 sestoji iz štirih rotacij (okrog središča kvadrata za kote $0°$, $90°$, $180°$ in $270°$) in štirih zrcaljenj (dve preko simetral stranic in dve preko diagonal).



Preštejmo komutirajoče pare. Enota grupe, tj. rotacija za $0°$, komutira z vsemi elementi. Vsaka od netrivialnih rotacij komutira z vsako od drugih

rotacij. Rotacija za kot 180° komutira tudi z vsemi zrcaljenji, nobena od drugih dveh netrivialnih rotacij pa ne komutira z nobenim zrcaljenjem. Zrcaljenji komutirata, če in samo če sta istovrstni. Ugotovili smo torej, da enota komutira z 8 elementi, rotacija za 180° prav tako z 8 elementi, rotaciji za 90° in 270° s 4 elementi, ter nazadnje vsako od štirih zrcaljenj s 4 elementi. Tako velja $\mathrm{vk}(D_4) = \frac{8+8+2\cdot 4+4\cdot 4}{64} = \frac{5}{8}$.

Kvadrat lahko zamenjamo s poljubnim pravilnim n-kotnikom. Grupa simetrij pravilnega n-kotnika je diedrska grupa D_n. Ta sestoji iz n rotacij in n zrcaljenj. Število urejenih parov elementov je $(2n)^2$, torej raste kvadratno z n. Vsaj takšno rast pa ima tudi število komutirajočih parov, saj vsaka od n rotacij komutira z vsako drugo. Velja torej $\mathrm{vk}(D_n) > \frac{n\cdot n}{(2n)^2} = \frac{1}{4}$ za vsak n. V posledici 12 premislimo, da velja $\lim_{n\to\infty} \mathrm{vk}(D_n) = \frac{1}{4}$.

Primer 3. Za X vzemimo direktni produkt množic $\{0,1\} \times \{1,2,\ldots,n\}$. Na X definirajmo binarno operacijo $\star$ na naslednji način:

$$(i,j) \star (k,l) = \begin{cases} (i,j) & \text{če je } j \leq l; \\ (k,l) & \text{sicer.} \end{cases}$$

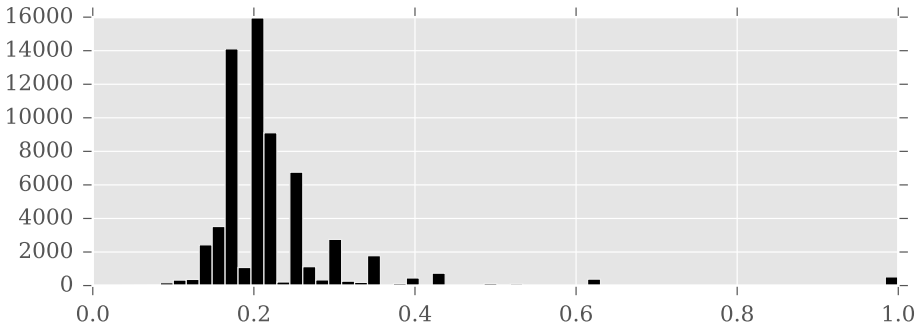
Operacija $\star$ torej vrne element, katerega druga komponenta je manjša, če pa sta drugi komponenti enaki, vrne prvi element. Hitro lahko preverimo, da je ta operacija asociativna, torej je $(X,\star)$ polgrupa. Vsaka dva elementa z različnima drugima komponentama komutirata, elementa z enako drugo komponento pa komutirata le, če sta enaka. Komutirajočih parov je veliko, zato verjetnost komutiranja v X lažje izrazimo kot nasprotni dogodek nekomutiranja. Tako velja $\mathrm{vk}(X) = 1 - \frac{2n}{(2n)^2} = 1 - \frac{1}{2n}$. Z naraščajočim n na ta način najdemo nekomutativne polgrupe z verjetnostjo komutiranja poljubno blizu 1.

Z modifikacijo tega primera sta Ponomarenko in Selinski pokazala, da je lahko verjetnost komutiranja končne polgrupe poljubno pozitivno racionalno število med 0 in 1.

Izrek 4 ([13] – Ponomarenko in Selinski 2012). *Za vsako racionalno število $r \in (0,1]$ obstaja končna polgrupa S, za katero velja* $\mathrm{vk}(S) = r$.

Nekoliko bolj pestro je z množicami, v katerih je več algebraične strukture. Slika 1 prikazuje histogram verjetnosti komutiranja, ki jih dobimo, če opazujemo le grupe moči največ 256. Število takšnih grup je 63 104, le 516 od teh je komutativnih. Najmanjša možna verjetnost komutiranja je

tukaj $1/28 \approx 3{,}6\,\%$. Verjetnosti komutiranja so sicer skoncentrirane okoli $22\,\%$. Ne spreglejmo tudi presenetljivih praznin: na histogramu je videti cele intervale verjetnosti brez zavzetih vrednosti.



Slika 1. Histogram verjetnosti komutiranja grup moči kvečjemu 256.

Ko na množico X dodamo še več algebraične strukture, recimo z dodatno operacijo, s katero X postane kolobar, so rezultati glede verjetnosti komutiranja sorodni tistim za grupe [10], čeravno se jih v literaturi najde manj. V nadaljevanju se zato osredotočimo na verjetnosti komutiranja grup. V naslednjih razdelkih podamo nekaj osnovnih lastnosti verjetnosti komutiranja končnih grup, dokažemo obstoj verjetnostnih lukenj in dosedanja opažanja še izostrimo, nazadnje pa pokažemo, kako lahko pojem verjetnosti komutiranja posplošimo na neskončne grupe.

O strukturnem vplivu

Osredotočeni smo na končne grupe in na razumevanje vpliva grupne strukture na verjetnost komutiranja. Zabeležimo najprej povezavo med verjetnostjo komutiranja grupe in njenih podgrup ter kvocientov.

Trditev 5. *Naj bo G končna grupa in H njena podgrupa. Tedaj velja* $\mathrm{vk}(G) \leq \mathrm{vk}(H)$. *Če je H podgrupa edinka v G, velja* $\mathrm{vk}(G) \leq \mathrm{vk}(G/H)$.

Dokaz. Verjetnost komutiranja izrazimo eksplicitno kot delež komutirajočih parov med vsemi urejenimi pari v grupi G:

$$\mathrm{vk}(G) = \frac{|\{(x,y) \in G \times G : xy = yx\}|}{|G|^2}.$$

Slednje zapišimo kot

$$\mathrm{vk}(G) = \frac{\sum_{x\in G} |\{y \in G : xy = yx\}|}{|G|^2}$$

in prepoznajmo centralizator $C_G(x) = \{y \in G : xy = yx\} \leq G$. Da lahko primerjamo vrednost $\mathrm{vk}(G)$ z $\mathrm{vk}(H)$, bo torej dovolj primerjati velikost $C_G(x)$ z velikostjo $C_H(x) = \{y \in H : xy = yx\}$ za vsak izbran $x \in G$.

Očitno je $C_H(x)$ podgrupa grupe $C_G(x)$ in tako je $C_G(x)$ unija odsekov $\{aC_H(x) : a \in C_G(x)\}$. Vsakemu takemu odseku $aC_H(x)$ lahko na naraven način priredimo odsek grupe G po podgrupi H, in sicer aH. Hitro preverimo, da je to prirejanje dobro definirano in celo injektivno. Za $a, b \in C_G(x)$ namreč drži $aH = bH$ natanko tedaj, ko je $a^{-1}b \in H$, kar je ekvivalentno pogoju $a^{-1}b \in C_G(x) \cap H = C_H(x)$, slednje pa je enako kot $aC_H(x) = bC_H(x)$. Tako smo izpeljali neenakost $|C_G(x) : C_H(x)| \leq |G : H|$ med števili odsekov.

Izpeljano neenakost uporabimo v gornjem zapisu verjetnosti komutiranja:

$$\mathrm{vk}(G) = \frac{\sum_{x\in G} |C_G(x)|}{|G|^2} \leq \frac{|G : H| \sum_{x\in G} |C_H(x)|}{|G|^2}.$$

V zadnji vsoti gremo po elementih grupe G in preštejemo število elementov v H, ki z vsakim od njih komutirajo. S tem torej preštejemo komutirajoče pare v $G \times H$. Te lahko preštejemo tudi tako, da gremo po elementih podgrupe H in preštejemo elemente v G, ki z njimi komutirajo. Tako dobimo

$$\mathrm{vk}(G) \leq \frac{|G : H| \sum_{x\in H} |C_G(x)|}{|G|^2}.$$

Še enkrat uporabimo neenakost med števili odsekov in zaključimo

$$\mathrm{vk}(G) \leq \frac{|G : H|^2 \sum_{x\in H} |C_H(x)|}{|G|^2} = \frac{\sum_{x\in H} |C_H(x)|}{|H|^2} = \mathrm{vk}(H).$$

Tako je dokazan prvi del trditve.

Za dokaz drugega dela najprej razpišemo

$$\mathrm{vk}(G/H) = \frac{|\{(xH, yH) \in G/H \times G/H : xyH = yxH\}|}{|G/H|^2}.$$

Ob elementih $x, y \in G$ je pogoj $xyH = yxH$ ekvivalenten pogoju $x^{-1}y^{-1}xy \in H$. Veljavnost tega pogoja je neodvisna od menjave elementa x ali y s kakšnim drugim predstavnikom istega odseka xH ali yH. Tako lahko izrazimo

$$\mathrm{vk}(G/H) = \frac{|\{(x, y) \in G \times G : x^{-1}y^{-1}xy \in H\}|}{|G/H|^2 \cdot |H|^2}.$$

Parov $(x, y) \in G \times G$ z lastnostjo $x^{-1}y^{-1}xy \in H$ je vsaj toliko, kolikor je parov z lastnostjo $x^{-1}y^{-1}xy = 1$, se pravi $xy = yx$. S tem lahko omejimo verjetnost komutiranja v kvocientu,

$$\mathrm{vk}(G/H) \geq \frac{|\{(x, y) \in G \times G : xy = yx\}|}{|G|^2} = \mathrm{vk}(G),$$

s čimer je tudi dokaz drugega dela zaključen. ∎

Iz dveh grup G_1 in G_2 lahko napravimo novo grupo. To storimo najlažje kar tako, da ju zložimo v direktni produkt grup $G_1 \times G_2$. Spomnimo se, da je kot množica to običajen kartezični produkt množic G_1 in G_2, grupna operacija pa je definirana po komponentah, se pravi $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ za $g_i \in G_1$, $h_i \in G_2$. Preverimo, da je verjetnost komutiranja v tem smislu multiplikativna.

Trditev 6. *Za končni grupi G_1 in G_2 velja* $\mathrm{vk}(G_1 \times G_2) = \mathrm{vk}(G_1) \cdot \mathrm{vk}(G_2)$.

Dokaz. Res, najprej zapišimo

$$\mathrm{vk}(G_1 \times G_2) = \frac{\sum_{x \in G_1 \times G_2} |C_{G_1 \times G_2}(x)|}{|G_1 \times G_2|^2} = \frac{\sum_{a \in G_1} \sum_{b \in G_2} |C_{G_1 \times G_2}((a, b))|}{|G_1 \times G_2|^2}.$$

Ker v kartezičnem produktu $G_1 \times G_2$ množimo po komponentah, lahko centralizator izrazimo kot $C_{G_1 \times G_2}((a, b)) = C_{G_1}(a) \times C_{G_2}(b) \leq G_1 \times G_2$. Sledi

$$\mathrm{vk}(G_1 \times G_2) = \frac{\sum_{a \in G_1} \sum_{b \in G_2} |C_{G_1}(a)||C_{G_2}(b)|}{|G_1|^2|G_2|^2}.$$

Zadnjo vsoto prepoznamo kot produkt

$$\frac{\sum_{a \in G_1} |C_{G_1}(a)|}{|G_1|^2} \cdot \frac{\sum_{b \in G_2} |C_{G_2}(b)|}{|G_2|^2} = \mathrm{vk}(G_1) \cdot \mathrm{vk}(G_2)$$

in dokaz je zaključen. ∎

Z zabeleženima trditvama nam že uspe utemeljiti, da je v dovolj velikih simetričnih grupah komutirajočih parov zanemarljivo malo.

Posledica 7. *Velja* $\lim_{n \to \infty} \mathrm{vk}(S_n) = 0$.

Dokaz. Simetrična grupa nižje stopnje se naravno vloži v simetrično grupo višje stopnje, zato je po trditvi 5 zaporedje verjetnosti komutiranja simetričnih grup $(\mathrm{vk}(S_n))_{n=1}^{\infty}$ padajoče. Pokažimo, da konvergira proti 0. V ta

namen za vsako naravno število k opazujmo grupo $G_k = S_3 \times \cdots \times S_3$, ki je produkt k kopij simetrične grupe S_3. Po trditvi 6 velja $\mathrm{vk}(G_k) = \left(\frac{1}{2}\right)^k$. Po Cayleyjevem izreku lahko vsako končno grupo vložimo v dovolj veliko simetrično grupo. Torej za vsak k obstaja n, da velja $G_k \leq S_n$, in zato za vsak $m \geq n$ velja $\mathrm{vk}(S_m) \leq \mathrm{vk}(S_n) \leq \mathrm{vk}(G_k) = \left(\frac{1}{2}\right)^k$. Tako je $\lim_{n\to\infty} \mathrm{vk}(S_n) = 0$. ∎

Verjetnost komutiranja simetričnih grup $\mathrm{vk}(S_n)$ je mogoče izračunati eksplicitno in tako podati tudi asimptotično obnašanje tega zaporedja, ko gre n proti neskončno. Ta in splošnejši opis za vse končne grupe sta našla že Erdös in Turán, gre pa takole. Elementa x, y abstraktne grupe G sta konjugirana, če obstaja tak $g \in G$, da velja $x = g^{-1}yg$. Lahko je preveriti, da je relacija konjugiranosti ekvivalenčna relacija na množici G. Ekvivalenčni razred elementa x je enak $x^G = \{g^{-1}xg : g \in G\}$, imenujemo ga razred konjugiranosti. Grupa G tako razpade na disjunktno unijo razredov konjugiranosti. Število teh razredov označimo s $\mathrm{k}(G)$. Za elementa $g, h \in G$ velja $g^{-1}xg = h^{-1}xh$, če in samo če je $(gh^{-1})^{-1}x(gh^{-1}) = x$. Slednje je enako kot $gh^{-1} \in C_G(x)$, kar preberemo kot enakost desnih odsekov $C_G(x)g = C_G(x)h$. Na ta način se vzpostavi bijekcija $g^{-1}xg \mapsto C_G(x)g$ med elementi razreda x^G in odseki grupe G po podgrupi $C_G(x)$. V posebnem drži enakost $|G : C_G(x)| = |x^G|$. Na vsem povedanem temelji naslednji izrek, ki razkrije povezavo med verjetnostjo komutiranja in $\mathrm{k}(G)$.

Izrek 8 ([3] – Erdös in Turán 1968). *Naj bo G končna grupa. Tedaj je*

$$\mathrm{vk}(G) = \frac{\mathrm{k}(G)}{|G|}.$$

Dokaz. Kot običajno razpišemo

$$\mathrm{vk}(G) = \frac{\sum_{x\in G} |C_G(x)|}{|G|^2}.$$

Velikost centralizatorja s pomočjo enakosti $|G : C_G(x)| = |x^G|$ zamenjamo z velikostjo razreda konjugiranosti in dobimo

$$\mathrm{vk}(G) = \frac{\sum_{x\in G} \frac{1}{|x^G|}}{|G|}.$$

Vsoto v številcu razdelimo po razredih konjugiranosti in iz vsakega izberimo predstavnika x_i za $1 \leq i \leq \mathrm{k}(G)$. Razredi konjugiranosti x_i^G so med sabo

disjunktni in pokrijejo ves G, za vsak element $x \in x_i^G$ pa velja $x^G = x_i^G$. Sledi

$$\mathrm{vk}(G) = \frac{\sum_{i=1}^{\mathrm{k}(G)} |x_i^G| \frac{1}{|x_i^G|}}{|G|} = \frac{\mathrm{k}(G)}{|G|}$$

in dokaz je zaključen. ∎

Število razredov konjugiranosti dane grupe lahko izračunamo hitreje kot število vseh komutirajočih parov. Premislimo, kakšni so razredi konjugiranosti v primeru simetrične grupe S_n. Naj bo σ izbrana permutacija. Če zanjo velja $\sigma(i) = j$, potem za konjugirano permutacijo $\alpha^{-1}\sigma\alpha$ ob poljubni $\alpha \in S_n$ velja

$$(\alpha^{-1}\sigma\alpha)(\alpha^{-1}(i)) = (\alpha^{-1}\sigma)(i) = \alpha^{-1}(j).$$

Konjugirani element $\alpha^{-1}\sigma\alpha$ torej preslika $\alpha^{-1}(i)$ v $\alpha^{-1}(j)$ in tako permutira na enak način kot σ, le da je treba vsako od števil $1 \leq i \leq n$ zamenjati z $\alpha^{-1}(i)$. Ko α preteče vse elemente grupe S_n, v razredu za konjugiranost σ^{S_n} najdemo ravno vse permutacije z enako ciklično strukturo kot σ. Število razredov konjugiranosti v S_n je zato enako številu vseh možnih razčlenitev naravnega števila n. Elementarna eksplicitna formula za to število ne obstaja, že dolgo pa je poznana njena dobra asimptotska ocena [7]. Z njo velja

$$\mathrm{vk}(S_n) \sim \frac{\exp\left(\pi\sqrt{\frac{2n}{3}}\right)}{4n\sqrt{3}\cdot n!},$$

zato je logaritem $\log(\mathrm{vk}(S_n))$ po Stirlingovi aproksimaciji proporcionalen $-n\log n$ za velike vrednosti n.

Število $\mathrm{k}(G)$ je povezano z mnogimi drugimi aspekti teorije grup, tudi bržkone naslavnejšim – teorijo upodobitev. Brez strahu se lahko s tem dejstvom okoristimo! Teorija upodobitev je del matematične folklore, potrebno znanje pa lahko osvežimo že z zapiski [11].

Opazovano grupo G s homomorfizmom $\rho\colon G \to GL(V)$ upodobimo na končnorazsežnem kompleksnem vektorskem prostoru V. Kadar je $\dim V = n$, grupo $\mathrm{GL}(V)$ enačimo z $\mathrm{GL}_n(\mathbb{C})$. Kadar lahko vektorski prostor V zapišemo kot direktno vsoto $V = U \oplus W$, pri čemer grupa G preko preslikave ρ deluje na vsaki komponenti te vsote posebej, rečemo, da je upodobitev razcepna. V nasprotnem imamo opravka z nerazcepno upodobitvijo. Prav tako kot cepimo naravna števila na prafaktorje, lahko upodobitev ρ razcepimo na nerazcepne upodobitve. Število vseh različnih nerazcepnih upodobitev (do izomorfizma natančno) grupe G je ravno $\mathrm{k}(G)$ [11, posledica 1.2.5]. Vse

najdemo v univerzalnem primeru upodobitve; to je regularna upodobitev, pri kateri elemente grupe G upodobimo kot leva množenja na grupni algebri $\mathbb{C}G$. Finejši pogled na slednjo upodobitev poda naslednji izrek, ki ga najdemo v [11, izrek 1.2.3].

Izrek 9 (Wedderburn). *Naj bo G končna grupa. Tedaj je njena regularna upodobitev izomorfna direktni vsoti*

$$\mathbb{C}G \cong \bigoplus_{i=1}^{\mathrm{k}(G)} \underbrace{V_i \oplus \cdots \oplus V_i}_{\dim V_i},$$

kjer so $V_1, V_2, \ldots, V_{\mathrm{k}(G)}$ ravno vse različne nerazcepne upodobitve (do izomorfizma natančno) grupe G. V posebnem sta kompleksni dimenziji leve in desne strani enaki, zato velja

$$|G| = \sum_{i=1}^{\mathrm{k}(G)} (\dim V_i)^2 . \tag{1}$$

Primer 10. Opazujmo kvaternionsko grupo $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Spomnimo se, da v njej množimo z zakoni $i^2 = j^2 = k^2 = -1$ in $ij = k$, $jk = i$, $ki = j$. Da grupo Q_8 upodobimo na enorazsežnem kompleksnem prostoru, je treba podati homomorfizem $\chi\colon Q_8 \to \mathbb{C}^\times$. Ta je natanko določen s sliko generatorjev i in j. Za vsakega od njiju smemo izbrati enega od dveh kompleksnih korenov števila -1. Enostavno je preveriti, da vsaka taka izbira porodi homomorfizem χ. Skupaj imamo torej štiri enorazsežne upodobitve grupe Q_8. Po Wedderburnovem izreku velja $8 = 1^2 + 1^2 + 1^2 + 1^2 + \sum_i d_i^2$, kjer so d_i stopnje višjerazsežnih nerazcepnih upodobitev. Edina možnost je, da obstaja natanko ena taka upodobitev stopnje 2. Tako velja $\mathrm{k}(Q_8) = 5$ in zato $\mathrm{vk}(Q_8) = \frac{5}{8}$.

Na splošno je število enorazsežnih upodobitev dane grupe G ravno število odsekov po njeni izpeljani podgrupi $G' = \langle \{x^{-1}y^{-1}xy : x, y \in G\} \rangle$. Dokaz tega dejstva najdemo v [11, izrek 2.8.4]. Wedderburnovo formulo (1) zato lahko zapišemo kot

$$|G| = |G : G'| + \sum_i d_i^2,$$

kjer so d_i stopnje višjerazsežnih nerazcepnih upodobitev grupe G. Od tod je mogoče izpeljati zgornjo mejo za verjetnost komutiranja poljubne grupe.

Trditev 11 ([14] – Rusin 1979). *Naj bo G končna grupa. Tedaj velja*

$$\mathrm{vk}(G) \leq \frac{1}{4}\left(1 + \frac{3}{|G'|}\right).$$

Dokaz. V Wedderburnovi formuli upoštevajmo $d_i \geq 2$, pa velja

$$|G| = |G : G'| + \sum_{i=|G:G'|+1}^{\mathrm{k}(G)} d_i^2 \geq |G : G'| + (\mathrm{k}(G) - \left|G : G'\right|) \cdot 4.$$

Neenakost delimo z $|G|$, izrazimo $\mathrm{vk}(G) = \mathrm{k}(G)/|G|$ in trditev sledi. ∎

O zavzetih vrednostih

Množico zavzetih verjetnosti komutiranja vseh končnih grup označimo z $\mathcal{V}$. S strukturnimi rezultati iz prejšnjega razdelka lahko dokažemo dve zanimivi lastnosti množice $\mathcal{V}$. Najprej se prepričajmo, da $\mathcal{V}$ ni diskretna podmnožica intervala $[0, 1]$.

Posledica 12. *Velja* $\lim_{n\to\infty}\mathrm{vk}(D_n) = \frac{1}{4}$.

Dokaz. Naj bosta ρ in τ rotacija in zrcaljenje v D_n. Velja $\rho^{-1}\tau^{-1}\rho\tau = \rho^{-2}$. Izpeljana podgrupa D_n' torej vsebuje kvadrate vseh rotacij. Teh je vsaj $\frac{n}{2}$ in tako gre $|D_n'|$ proti neskončno, ko gre n proti neskončno. Že iz uvodnega razdelka vemo, da je $\mathrm{vk}(D_n) > \frac{1}{4}$, zato iz trditve 11 sledi $\lim_{n\to\infty}\mathrm{vk}(D_n) = \frac{1}{4}$. ∎

Vrednost $\frac{1}{4}$ je torej limitna točka množice $\mathcal{V}$. Hkrati je po trditvi 6 verjetnost komutiranja grupe $S_3 \times S_3$ ravno $\frac{1}{4}$, torej je limitna vrednost tudi zavzeta in množica $\mathcal{V}$ ni diskretna. Iz strukturnih ocen izpeljimo še drugo lastnost, in sicer obstoj intervalov nezavzetih vrednosti.

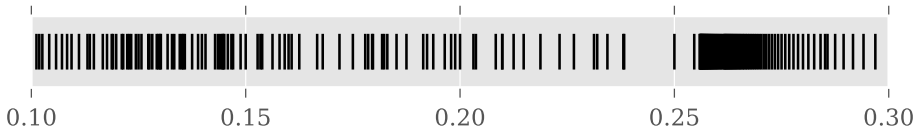
Posledica 13 ([6] – Gustafson 1973). *Interval* $(\frac{5}{8}, 1)$ *ne vsebuje verjetnosti komutiranja nobene končne grupe.*

Dokaz. Naj bo G končna grupa z $\mathrm{vk}(G) > \frac{5}{8}$. Iz predpostavke in trditve 11 sledi neenakost

$$\frac{5}{8} < \mathrm{vk}(G) \leq \frac{1}{4}\left(1 + \frac{3}{|G'|}\right),$$

ki se poenostavi do $|G'| < 2$. Sledi $G' = 1$, torej je G komutativna in zato $\mathrm{vk}(G) = 1$. ∎

Oglejmo si verjetnosti komutiranja grup moči največ 256 še enkrat, tokrat bolj podrobno. Omejimo se na verjetnosti z intervala [0,1, 0,3]. Slika 2 prikazuje zalogo vrednosti funkcije verjetnosti komutiranja, zožene na množico grup moči kvečjemu 256. Vemo že, da se verjetnosti komutiranja diedrskih grup z zgornje strani stekajo k vrednosti $\frac{1}{4}$, na sliki je razločen začetek te konvergence. Tik pod limitno točko $\frac{1}{4}$ je moč zaznati verjetnostno luknjo. Opazimo tudi, da je limitnih točk množice $\mathcal{V}$ najbrž več. Zanimivo bi jih bilo opisati.



Slika 2. Zavzete verjetnosti komutiranja grup moči kvečjemu 256.

O teh in splošnejših lastnostih množice zavzetih verjetnosti komutiranja je razmišljal že Joseph in postavil naslednje domneve.

Domneva 14 ([9] – Joseph 1977). Množica $\mathcal{V}$ ima naslednje lastnosti:

1. Limitne točke množice $\mathcal{V}$ so racionalne.
2. K limitnim točkam množice $\mathcal{V}$ se zavzete verjetnosti komutiranja lahko stekajo le z zgornje strani.
3. Množica $\mathcal{V} \cup \{0\}$ je zaprta.

Po prvi domnevi naj bi okoli vsakega iracionalnega števila na intervalu $[0, 1]$ našli okolico, ki ne seka množice $\mathcal{V}$. Tretja domneva pravi, da za vsako zaporedje $v_n \in \mathcal{V}$ s pozitivno limito $\lim_{n\to\infty} v_n = v$ obstaja končna grupa z verjetnostjo komutiranja v. Nazadnje druga domneva trdi, da za vsako limitno točko v obstaja $\delta > 0$, da velja $(v - \delta, v) \cap \mathcal{V} = \emptyset$. Slednje pomeni, da je množica $\mathcal{V}$ dobro urejena glede na relacijo $>$.

Delno razrešitev Josephovih domnev najdemo v nedavno objavljenem članku [2]. Avtor prikaže presenetljivo in čudovito povezavo med verjetnostjo komutiranja in egipčansko kompleksnostjo racionalnih števil. Vsako racionalno število $q > 0$ lahko zapišemo kot vsoto $q = 1/n_1 + \cdots + 1/n_m$ za neka naravna števila n_i in m. To lahko storimo na več načinov, na primer $\frac{5}{6} = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2} + \frac{1}{3}$. Najmanjše število uporabljenih sumandov m, za katerega obstaja tak zapis, je (egipčanska) kompleksnost $\mathcal{E}(q)$ števila q. Eberhard dokaže, da so verjetnosti komutiranja končnih grup tesno povezane z ulomki omejene kompleksnosti.

Izrek 15 ([2] – Eberhard 2015). *Za vsako padajočo funkcijo* $\eta\colon \mathbb{N} \to (0,1)$ *obstaja konstanta* $M = M(\eta) \in \mathbb{N}$*, tako da je verjetnost komutiranja poljubne končne grupe oblike* $q + \epsilon$*, kjer je* $\mathcal{E}(q) \leq M$ *in* $0 \leq \epsilon \leq \eta(\mathcal{E}(q))$*.*

Od tod lahko hitro izpeljemo veljavnost prvih dveh zgornjih domnev.

Dokaz prvih dveh Josephovih domnev. Naj bo $v > 0$ limitna točka množice $\mathcal{V}$. Številu v se približajmo kar se da dobro z ulomki omejene kompleksnosti; naj bo

$$Q(m) = \sup\{q < v : \mathcal{E}(q) \leq m\}$$

za vsako naravno število m. Definirajmo funkcijo $\eta\colon \mathbb{N} \to (0,1)$ s predpisom $\eta(m) = (v - Q(m))/2$. Po izreku obstaja konstanta M, da vsako vrednost $p \in \mathcal{V}$ lahko zapišemo kot $p = q + \epsilon$, kjer je $\mathcal{E}(q) \leq M$ in $0 \leq \epsilon \leq \eta(\mathcal{E}(q))$. Če slučajno drži še neenakost $q < v$, sledi $q \leq Q(\mathcal{E}(q))$ in zato velja najprej neenakost

$$\epsilon \leq \eta(\mathcal{E}(q)) = \frac{v - Q(\mathcal{E}(q))}{2} \leq \frac{v - q}{2},$$

s tem pa še

$$p = q + \epsilon \leq \frac{v + q}{2} \leq \frac{v + Q(M)}{2} = v - \eta(M).$$

V tem primeru je torej število p oddaljeno vsaj $\eta(M)$ od števila v.

Vzemimo zaporedje $v_n = q_n + \epsilon_n \in \mathcal{V}$ z limito v. Iz zgornjega premisleka sledi, da lahko le za končno mnogo indeksov velja $q_n < v$. S tem je dokazana druga domneva. Ker je zato $v_n \geq q_n \geq v$ za skoraj vse indekse, tudi zaporedje q_n konvergira k v. Množica vseh ulomkov kompleksnosti največ M je zaprta (ko ji dodamo 0), saj jo lahko predstavimo kot sliko zvezne preslikave

$$\left(\left\{\frac{1}{n} : n \in \mathbb{N}\right\} \cup \{0\}\right)^M \to [0, M],$$

ki sešteje M-terico števil na levi. Od tod sledi $\mathcal{E}(v) \leq M$. Tako je v racionalno število in tudi prva domneva je dokazana. ∎

Tretja Josephova domneva je še vedno odprta.

O neskončnih grupah

Pojem verjetnosti komutiranja ima smisel za poljubne grupe, opremljene z verjetnostno mero. V posebnem to naravno velja za kompaktne (Hausdorffove) topološke grupe. Ponovimo, da je topološka grupa G množica, ki je hkrati opremljena s strukturo grupe in topološkega prostora, oboje pa je uglašeno z zahtevo, da sta množenje in invertiranje v G zvezni preslikavi. Vsaka kompaktna topološka grupa G je naravno opremljena s Haarovo mero; to je verjetnostna Borelova mera μ, za katero med drugim velja $\mu(x \cdot E) = \mu(E)$ pri vsakem $x \in G$ in Borelovi množici $E \subseteq G$. Bralec lahko več o Haarovi meri prebere v [8, razdelek I.2].

Primer 16. Opazujmo končno grupo G, opremljeno z diskretno topologijo. Njena Haarova mera μ sovpada z normalizirano mero štetja točk. Torej za podmnožico $A \subseteq G$ velja $\mu(A) = |A|/|G|$.

Primer 17. Opazujmo multiplikativno grupo S^1 kompleksnih števil absolutne vrednosti 1. Tukaj je Haarova mera merljive množice $A \subseteq S^1$ enaka vrednosti $\lambda(\{t \in [0,1] : e^{2\pi i t} \in A\})$, kjer je λ običajna Lebesgueova mera na intervalu $[0,1]$.

Pare elementov iz grupe G slučajno izbiramo iz produktnega prostora $G \times G$, opremljenega z verjetnostno produktno mero $\mu \times \mu$. Komutiranje v G izrazimo z zvezno preslikavo $k\colon G \times G \to G,\ k(x,y) = x^{-1}y^{-1}xy$. Komutirajoči pari so natanko množica $k^{-1}(\{1\})$. Verjetnost komutiranja v grupi G je tako enaka

$$\mathrm{vk}(G) = (\mu \times \mu)(k^{-1}(\{1\})) = \int_{k^{-1}(\{1\})} \mathrm{d}(\mu \times \mu).$$

Ni se težko prepričati, da tudi za kompaktne grupe velja izrek o verjetnostni luknji. Tokrat predstavimo elementarnejši dokaz, ki se izogne teoriji upodobitev.

Trditev 18 ([6] – Gustafson 1973). *Interval* $(\frac{5}{8}, 1)$ *ne vsebuje verjetnosti komutiranja nobene kompaktne grupe.*

Dokaz. Verjetnost komutiranja kompaktne grupe G izrazimo kot

$$\int_{k^{-1}(\{1\})} \mathrm{d}(\mu \times \mu) = \int_G \int_{C_G(x)} \mathrm{d}\mu(y)\mathrm{d}\mu(x) = \int_G \mu(C_G(x))\,\mathrm{d}\mu(x),$$

kjer prva enakost sledi po Fubinijevem izreku. Razdelimo verjetnost komutiranja na dva dela,

$$\mathrm{vk}(G) = \int_{Z(G)} \mu(C_G(x))\,\mathrm{d}\mu(x) + \int_{G-Z(G)} \mu(C_G(x))\,\mathrm{d}\mu(x).$$

Predpostavimo, da G ni komutativna. Tedaj kvocientna grupa $G/Z(G)$ grupe G po svojem centru ni ciklična, zato je $|G : Z(G)| \geq 4$. Ker je G disjunktna unija odsekov po centru, sledi $\mu(Z(G)) \leq \frac{1}{4}$. Za tiste elemente $x \in G$, ki ne pripadajo centru, velja neenakost $|G : C_G(x)| \geq 2$ in zato $\mu(C_G(x)) \leq \frac{1}{2}$. Zdaj velja

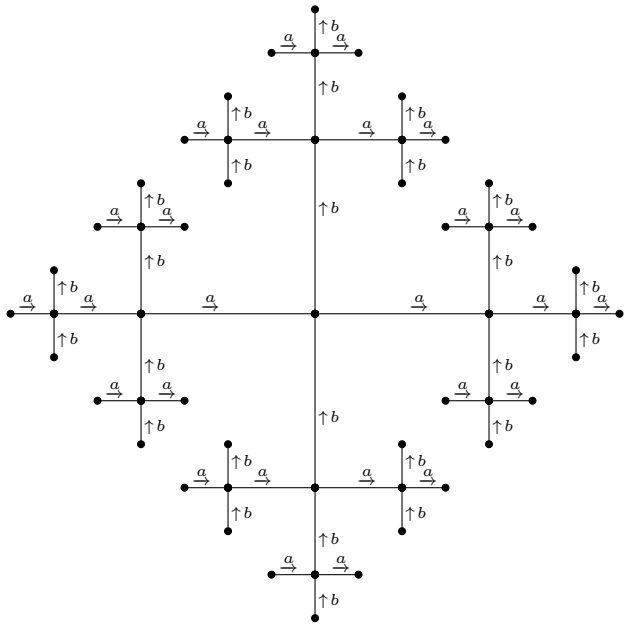
$$\mathrm{vk}(G) \leq \mu(Z(G)) \cdot 1 + \mu(G - Z(G)) \cdot \frac{1}{2} \leq \frac{\mu(Z(G))}{2} + \frac{1}{2} \leq \frac{5}{8},$$

s čimer je dokaz zaključen. ∎

Nekoliko bolj izvirna definicija verjetnosti komutiranja je potrebna za neskončne grupe, ki same po sebi niso opremljene z verjetnostno mero. Avtorji [1] k temu problemu pristopijo s stališča geometrijske teorije grup. Vsaki končno generirani grupi G, generirani s simetrično množico $X = X^{-1}$, lahko priredimo njen Cayleyjev graf $\mathrm{Cay}(G, X)$. Vozlišča tega grafa so elementi grupe G, med elementoma $x, y \in G$ pa obstaja povezava, če in samo če je $x^{-1}y \in X$.

Primer 19. Naj bo F prosta grupa na dveh generatorjih a, b. Njeni elementi so okrajšane besede s črkami iz množice $X = \{a, a^{-1}, b, b^{-1}\}$. Cayleyjev graf $\mathrm{Cay}(F, X)$ dobimo tako, da vsako besedo povežemo z njenim nadaljevanjem z vsako od črk iz množice X. Ta graf je neskončen in je delno prikazan na sliki 3. V središču je enota 1 grupe F. Ko jo podaljšamo z vsakim elementom množice X, dobimo njene sosede a, a^{-1}, b, b^{-1}. Vsakega od teh lahko zopet podaljšamo. Pri tem upoštevamo še krajšanje besed, na primer $aa^{-1} = 1$. Če se torej v grafu sprehodimo od enote 1 v smeri »desno-gor-levo«, prispemo do elementa aba^{-1}.

Cayleyjev graf lahko opremimo z naravno metriko: za razdaljo $d_X(x, y)$ med vozliščema x in y razglasimo število povezav na najkrajši poti med x in y. Namesto algebraičnega objekta G tako lahko opazujemo metrični prostor $\mathrm{Cay}(G, X)$. Verjetnost komutiranja lahko izmerimo v vsakem končnem kosu tega metričnega prostora, cel prostor pa lahko izčrpamo s končnimi množicami, najbolj naravno kar s kroglami okoli enote



Slika 3. Del Cayleyjevega grafa proste grupe z generatorjema a, b.

$\mathbb{B}_X(n) = \{x \in G : d_X(x, 1) \leq n\}$. V tem jeziku slika 3 prikazuje kroglo $\mathbb{B}_X(3)$ Cayleyjevega grafa proste grupe. Stopnja komutiranja (v tej splošnosti ne moremo govoriti več o verjetnosti) v grupi G je

$$\mathrm{sk}(G, X) = \limsup_{n\to\infty} \frac{|\{(x, y) \in \mathbb{B}_X(n) \times \mathbb{B}_X(n) : xy = yx\}|}{|\mathbb{B}_X(n)|^2}.$$

Antolín, Martino in Ventura dokažejo, da za grupe G polinomske besedne rasti (to pomeni, da velikosti krogel $\mathbb{B}_X(n)$ rastejo kvečjemu polinomsko z n) v zgornji definiciji obstaja celo limita ter da je ta neodvisna od izbire končne generirajoče množice X. Poleg tega avtorji premislijo, da je v takih grupah stopnja komutiranja pozitivna le v izjemnih primerih.

Trditev 20 ([1] – Antolín, Martino in Ventura 2017). *Naj bo G grupa, generirana s končno množico X. Predpostavimo, da je G polinomske rasti. Tedaj je* $\mathrm{sk}(G, X) > 0$ *natanko tedaj, ko ima G komutativno podgrupo končnega indeksa.*

Predpostavka o polinomski rasti je precej omejujoča. Grupe s to lastnostjo so natanko grupe, ki imajo nilpotentno podgrupo končnega indeksa [4]. Ko nasprotno opazujemo grupe s hitro, eksponentno rastjo, so te daleč stran

od komutativnih in avtorji pričakujejo, da je njihova stopnja komutiranja ničelna.

To domnevo znajo potrditi za precej širok razred grup s takšno rastjo, in sicer hiperbolične grupe [5]. To so grupe, katerih Cayleyjev graf je videti kot hiperbolični prostor v naslednjem smislu:

obstaja $\delta > 0$, pri katerem je vsak trikotnik v $\mathrm{Cay}(G, X)$ δ-ozek.

Tukaj s pojmom trikotnik mislimo izbiro treh točk v grafu in geodetskih poti med njimi, izraz δ-ozek pa pomeni, da je vsaka točka na kateremkoli robu trikotnika oddaljena za največ δ od vsaj ene točke na uniji drugih dveh robov trikotnika. V takem metričnem prostoru so torej trikotniki negativno ukrivljeni, podobno kot v hiperboličnem prostoru.

Primer 21. Proste grupe so hiperbolične. Kot smo videli v primeru 19, so njihovi Cayleyjevi grafi neskončna drevesa in trikotniki v njih so zelo ozki.

Primer 22. Lep primer hiperbolične grupe je modularna grupa transformacij hiperbolične ravnine $\{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Ta sestoji iz preslikav oblike

$$z \mapsto \frac{az + b}{cz + d},$$

kjer so a, b, c, d cela števila, za katera velja $ad - bc = 1$. Opremljena je z operacijo komponiranja preslikav. Ni težko preveriti, da preslikavi $S\colon z \mapsto -1/z$ in $T\colon z \mapsto z + 1$ generirata to grupo. Preslikava S je kompozicija inverzije preko enotske krožnice in zrcaljenja preko imaginarne osi, preslikava T pa enotska translacija. Generatorja zadoščata relacijama $S^2 = (ST)^3 = 1$. S tema dvema relacijama je modularna grupa enolično določena in jo v tem smislu lahko podamo kot končno prezentirano grupo $\langle S, T \mid S^2, (ST)^3 \rangle$. Ko postavimo $X = \{S, S^{-1}, ST, (ST)^{-1}\}$, si lahko Cayleyjev graf te grupe glede na X predstavljamo sorodno kot graf na sliki 3, le da moramo v slednjem mnogo vozlišč identificirati. V Cayleyjevem grafu modularne grupe obstajajo dvocikli zaradi enakosti $S^2 = 1$ in tricikli zaradi enakosti $(ST)^3 = 1$.

Ko prosti grupi dodajamo naključne dolge relacije, skoraj vedno dobimo hiperbolično grupo.

Izrek 23 ([5] – Gromov 1987, [12] – Ol'shanskiĭ 1992). *Ob danih naravnih številih $n \geq 2$ in $k \geq 1$ enakomerno in neodvisno iz proste grupe z n generatorji $a_1, a_2, \ldots, a_n$ izberimo besede $r_1, r_2, \ldots, r_k$ dolžine največ ℓ. Naj bo $G = \langle a_1, \ldots, a_n \mid r_1, \ldots, r_k \rangle$ kvocient proste grupe po teh relacijah. Tedaj verjetnost, da je G hiperbolična grupa, konvergira proti 1, ko gre ℓ proti neskončno.*

Vsako končno generirano grupo lahko predstavimo kot kvocient proste grupe. Kadar za to potrebujemo le končno mnogo relacij, je torej grupa v smislu izreka 23 skoraj zagotovo hiperbolična. Če izključimo tiste, ki vsebujejo ciklično podgrupo končnega indeksa, zanje velja naslednji rezultat.

Trditev 24 ([1] – Antolín, Martino in Ventura 2017). *Naj bo G hiperbolična grupa, generirana s končno množico X. Predpostavimo, da G ne vsebuje ciklične podgrupe končnega indeksa. Tedaj je* $\mathrm{sk}(G, X) = 0$.

Nazadnje imajo torej skoraj vse (končno prezentirane) grupe ničelno stopnjo komutiranja. Temu primerno naš izlet po verjetnosti komutiranja končajmo z enim Šalamunom –

nič nič nič nič

fiuuuuu še ena gobica

LITERATURA

[1] Y. Antolín, A. Martino in E. Ventura, *Degree of commutativity of infinite groups*, Proc. Am. Math. Soc. **145** (2017), 479–485.

[2] S. Eberhard, *Commuting probabilities of finite groups*, Bull. Lond. Math. Soc. **47** (2015), 796–808.

[3] P. Erdös in P. Turán, *On some problems of a statistical group-theory. IV*, Acta Math. Acad. Sci. Hungar **19** (1968), 413–435.

[4] M. Gromov, *Groups of polynomial growth and expanding maps*, Inst. Hautes Études Sci. Publ. Math. **53** (1981), 53–73.

[5] M. Gromov, *Hyperbolic groups*, Essays in group theory **8** (1987), 75–263.

[6] W. H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.

[7] G. H. Hardy in S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. Lond. Math. Soc. **2** (1918), 75–115.

[8] M. Hladnik, *Uvod v harmonično analizo na lokalno kompaktnih grupah*, zapiski predavanj, Ljubljana, 2006, dostopno na `www.fmf.uni-lj.si/~hladnik/3st/HA.pdf`, ogled 21. 12. 2018.

[9] K. Joseph, *Several conjectures on commutativity in algebraic structures*, Amer. Math. Monthly **84** (1977), 550–551.

[10] D. MacHale, *Commutativity in finite rings*, Amer. Math. Monthly **83** (1976), 30–32.

[11] P. Moravec, *Osnove upodobitev končnih grup*, Samozal., Ljubljana, 2018, dostopno na `www.fmf.uni-lj.si/~moravec/Papers/upodob_moravec.pdf`, ogled 21. 12. 2018.

[12] A. Yu. Ol'shanskiĭ, *Almost every group is hyperbolic*, Internat. J. Algebra Comput. **2** (1992), 1–17.

[13] V. Ponomarenko in N. Selinski, *Two semigroup elements can commute with any positive rational probability*, College Math. J. **43** (2012), 334–336.

[14] D. J. Rusin, *What is the probability that two elements of a finite group commute?*, Pacific J. Math. **82** (1979), 237–247.