Circle method and counting transversals in group multiplication tables

Rudi Mrazović

University of Zagreb

3 October 2022

joint work with
Sean Eberhard (Cambridge) and Freddie Manners (San Diego)

Representation Theory XVII

Introduction

Transversals in Latin squares

1	0	3	2	4
3	1	0	4	2
4	3	2	1	0
0	2	4	3	1
2	4	1	0	3

Definition

A *transversal* in an $n \times n$ Latin square is a set of n cells in distinct rows and columns and having different symbols.

Does every Latin square have a transversal?

Latin squares with no transversals

n even, L cyclic $n \times n$ Latin square

$$L_{ij} = (i + j) \mod n$$

	0	*1*	*2*	*3*	*4*	*5*
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

If $\{(x, \pi(x)) : x = 0, \ldots, n-1\}$ is a transversal, then modulo n:

$$n/2 \equiv \sum_x L_{x,\pi(x)} = \sum_x (x + \pi(x)) = \sum_x x + \sum_x \pi(x) \equiv 0.$$

Ryser's conjecture

Conjecture (Ryser, 1967)

For n odd, every $n \times n$ Latin square has a transversal.

Group multiplication tables

Group multiplication table

G finite group of order n. Multiplication table of G is the $n \times n$ Latin square $L(G)$ such that $L(G)_{x,y} = xy$.

The necessary condition we've seen for the cyclic Latin square ($G = \mathbf{Z}/n\mathbf{Z}$, n even) can be generalized.

Let G' be the commutator subgroup of G (subgroup generated by all $[x, y]$ where $xy = yx[x, y]$).

If $\{(x, \pi(x)) : x \in G\}$ is a transversal, then modulo G':

$$\prod_{x \in G} x \equiv \prod_{x \in G} L(G)_{x,\pi(x)} = \prod_{x \in G} x\pi(x) \equiv \prod_{x \in G} x \prod_{x \in G} \pi(x) \equiv \Big(\prod_{x \in G} x\Big)^2$$

Hall–Paige condition

A finite group G satisfies Hall-Paige condition if $\prod_{x \in G} x \in G'$.

Hall–Paige conjecture

Conjecture (Hall–Paige, 1955)
Theorem (Wilcox–Evans–Bray, 2009)

If G satisfies the Hall–Paige condition then the multiplication table of G has a transversal.

The proof used the classification of finite simple groups and computer algebra.

Counting transversals in group multiplication tables

Let $\mathrm{tran}(G)$ be the number of transversals in $L(G)$.

Conjecture (Vardi 1991, Wanless 2011)

For n odd

$$\mathrm{tran}(\mathbf{Z}/n\mathbf{Z}) = \big(1/e + o(1)\big)^n n!.$$

Heuristics and main results

Heuristic

Again $G = \mathbf{Z}/n\mathbf{Z}$, n odd. Let $\pi\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ be a random permutation and $\psi(x) = x + \pi(x)$. Hence,

$$\{(x, \pi(x)) : x \in \mathbf{Z}/n\mathbf{Z}\} \text{ is a tranversal } \iff \psi \text{ is a permutation}$$

Zeroth approximation

$$\psi \approx \text{random function} \implies \mathrm{tran}(\mathbf{Z}/n\mathbf{Z}) \approx n! \cdot n!/n^n$$

First approximation

$$\begin{matrix} \psi \approx \text{random function} \\ \sum_{x\in\mathbf{Z}/n\mathbf{Z}} \psi(x) = 0 \end{matrix} \implies \mathrm{tran}(\mathbf{Z}/n\mathbf{Z}) \approx n! \cdot n!/n^n \cdot n$$

Let $x, y \in \mathbf{Z}/n\mathbf{Z}$ with $x \neq y$. If $\psi_1\colon \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ is a random function such that $\sum_{x\in\mathbf{Z}/n\mathbf{Z}} \psi_1(x) = 0$, then $\mathbf{P}(\psi_1(x) = \psi_1(y)) = 1/n$.
However,

$$\mathbf{P}(\psi(x) = \psi(y)) = \mathbf{P}(\pi(x) - \pi(y) = y - x) = 1/(n-1).$$

Principle of maximum entropy

Let $\operatorname{coll} f = \#\{x, y \in \mathbf{Z}/n\mathbf{Z} : x \neq y, f(x) = f(y)\}$.

$$\mathbf{E}\operatorname{coll}\psi_1 = \binom{n}{2}\frac{1}{n} = \frac{n-1}{2} \qquad \mathbf{E}\operatorname{coll}\psi = \binom{n}{2}\frac{1}{n-1} = \frac{n}{2}$$

Second approximation

$$\left.\begin{array}{c} \psi \approx \text{random function} \\ \sum_{x\in\mathbf{Z}/n\mathbf{Z}} \psi(x) = 0 \\ \mathbf{E}\operatorname{coll}\psi = n/2 \end{array}\right. \quad \Longrightarrow \quad \operatorname{tran}(\mathbf{Z}/n\mathbf{Z}) \approx n! \cdot n!/n^n \cdot n \cdot \ldots$$

Let $\psi_2 \sim \text{LHS}$. Is there a natural/default choice for the distribution of ψ_2?

Principle of maximum entropy

Principle of maximum entropy

The distribution which best represents our knowledge is the one with the *maximum entropy*.

Let $p_f = \mathbf{P}(\psi_2 = f)$ and $H = \{f : \sum_{x \in \mathbf{Z}/n\mathbf{Z}} f(x) = 0\}$.

$$\begin{aligned} \text{maximize}: \quad & \sum p_f \log(1/p_f) \\ \text{subject to:} \quad & (p_f) \text{ probability distribution} \\ & p_f = 0 \;\text{ if } f \notin H \\ & \sum p_f \operatorname{coll} f = n/2 \end{aligned}$$

Solution is the *Gibbs distribution*:

$$p_f \approx \frac{1_H(f)}{e^{1/2}|H|} e^{\operatorname{coll} f/n}$$

Abelian result

Second approximation

$$\left.\begin{array}{c}\psi \approx \text{random function} \\ \sum_{x\in\mathbf{Z}/n\mathbf{Z}} \psi(x) = 0 \\ \mathbf{E}\,\mathrm{coll}\,\psi = n/2\end{array}\right. \quad \Longrightarrow \quad \mathrm{tran}(\mathbf{Z}/n\mathbf{Z}) \approx n! \cdot n!/n^n \cdot n \cdot e^{-1/2}$$

Theorem (Eberhard–Manners–M., 2019)

For n odd we have

$$\mathrm{tran}(\mathbf{Z}/n\mathbf{Z}) = \left(e^{-1/2} + o(1)\right) n!^2/n^{n-1}.$$

Nonabelian heuristic

G a group of order n satisfying the Hall–Paige condition. Again, $\pi \colon G \to G$ is a random permutation and $\psi(x) = x\pi(x)$.

Zeroth approximation

$$\psi \approx \text{random function} \implies \mathrm{tran}(G) \approx n! \cdot n!/n^n$$

First approximation

$$\begin{array}{c} \psi \approx \text{random function} \\ \prod_{x\in G} \psi(x) \in G' \end{array} \implies \mathrm{tran}(G) \approx n! \cdot n!/n^n \cdot n/|G'|$$

Second approximation

$$\begin{array}{c} \psi \approx \text{random function} \\ \prod_{x\in G} \psi(x) \in G' \\ \mathbf{E}\,\mathrm{coll}\,\psi = n/2 \end{array} \implies \mathrm{tran}(G) \approx n! \cdot n!/n^n \cdot n/|G'| \cdot e^{-1/2}$$

Nonabelian result

Theorem (Eberhard–Manners–M., 2022)

Let G be a group of order n satisfying the Hall–Paige condition. Then

$$\mathrm{tran}(G) = (e^{-1/2} + o(1))\, n!^2 / n^{n-1} |G'|.$$

Corollary

The Hall–Paige conjecture holds for all groups G of order greater than 10^{10}.

Theorem

Let $n = 2^k$. For k sufficiently large

$$\mathrm{tran}(\mathbf{Z}_2^k) > \mathrm{tran}(G) \quad \text{for all other } G \text{ of order } n.$$

Crash course in circle method

Circle method

Let $P_n = \{p \leq n : p \text{ prime}\}$. How can we count the representations $n = p_1 + p_2 + p_3$ for $p_1, p_2, p_3 \in P_n$?

If $f * g(n) = \sum_m f(m)g(n-m)$, then the count is

$$c(n) := 1_{P_n} * 1_{P_n} * 1_{P_n}(n).$$

Let $\widehat{f}(\theta) = \sum_m f(m)e^{2\pi i\theta m}$. Basic Fourier analysis gives

$$\begin{aligned} c(n) = 1_{P_n} * 1_{P_n} * 1_{P_n}(n) &= \int_0^1 (1_{P_n} * 1_{P_n} * 1_{P_n})\widehat{\ }(\theta) e^{-2\pi i\theta n}\, d\theta \\ &= \int_0^1 \widehat{1_{P_n}}(\theta)^3 e^{-2\pi i\theta n}\, d\theta \end{aligned}$$

Major and minor arcs

$$c(n) = \int_0^1 \widehat{1_{P_n}}(\theta)^3 e^{-2\pi i\theta n}\, d\theta$$

$|\widehat{1_{P_n}}(\theta)| = \left|\sum_{m\in P_n} e^{2\pi i\theta m}\right| \le |P_n|$ for every $\theta \in [0,1]$ (triangle inequality).

However, for most θ, $|\widehat{1_{P_n}}(\theta)|$ is much smaller (e.g. $|\widehat{1_{P_n}}(\theta)| \approx |P_n|^{1/2}$ on average).

For some θ, $|\widehat{1_{P_n}}(\theta)|$ is large. Let $\mathcal{M}$ be the set of all such θ ("major arcs"). E.g. $1/3 \in \mathcal{M}$:

$$\widehat{1_{P_n}}(1/3) = \sum_{m\in P_n} e^{2\pi i m/3} \approx \frac{|P_n|}{2} e^{2\pi i/3} + \frac{|P_n|}{2} e^{4\pi i/3} = -\frac{|P_n|}{2}$$

Let $\mathfrak{m} = [0,1] \setminus \mathcal{M}$ ("minor arcs"). For $\theta \in \mathfrak{m}$, $|\widehat{1_{P_n}}(\theta)|$ is small.

Major and minor arcs

$$c(n) = \underbrace{\int_{\mathcal{M}} \widehat{1_{P_n}}(\theta)^3 e^{-2\pi i\theta n}\, d\theta}_{\text{main term}} + \underbrace{\int_{\mathfrak{m}} \widehat{1_{P_n}}(\theta)^3 e^{-2\pi i\theta n}\, d\theta}_{\text{error term}=o(\text{main term})}$$

Aim: calculate the main term (i.e. major arcs) precisely, and bound the error term (i.e. minor arcs).

Proof idea (cyclic groups)

Fourier analysis on $(\mathbf{Z}/n\mathbf{Z})^n$

Let $S = \{\text{bijections } \{1,\dots,n\} \to \mathbf{Z}/n\mathbf{Z}\} \subset (\mathbf{Z}/n\mathbf{Z})^n$. Then

$$n! \cdot \mathrm{tran}(\mathbf{Z}/n\mathbf{Z}) = \#\{\pi_1,\pi_2,\pi_3 \in S^3 : \pi_1+\pi_2+\pi_3 = 0\}.$$

For $f, g\colon (\mathbf{Z}/n\mathbf{Z})^n \to \mathbf{R}$ and $a_1,\dots,a_n \in \mathbf{Z}/n\mathbf{Z}$:

$$f * g(x) = \sum_{y \in (\mathbf{Z}/n\mathbf{Z})^n} f(y) g(x-y)$$

$$\widehat{f}(a_1,\dots,a_n) = \sum_{x \in (\mathbf{Z}/n\mathbf{Z})^n} f(x) e^{2\pi i (a_1x_1+\cdots+a_nx_n)/n}$$

Fourier analysis on $(\mathbf{Z}/n\mathbf{Z})^n$ gives

$$\begin{aligned} n! \cdot \mathrm{tran}(\mathbf{Z}/n\mathbf{Z}) &= \#\{\pi_1,\pi_2,\pi_3 \in S^3 : \pi_1+\pi_2+\pi_3 = 0\} \\ &= 1_S * 1_S * 1_S(0) = n^{-n} \sum_{a_1,\dots,a_n \in \mathbf{Z}/n\mathbf{Z}} \widehat{1_S}(a_1,\dots,a_n)^3. \end{aligned}$$

Major arcs (cyclic group case)

$$n! \cdot \mathrm{tran}(\mathbf{Z}/n\mathbf{Z}) = n^{-n} \sum_{a_1,\dots,a_n \in \mathbf{Z}/n\mathbf{Z}} \widehat{1_S}(a_1,\dots,a_n)^3$$

$\widehat{1_S}(0,\dots,0) = n!$ (maximal value)

Major arcs: $(a_1,\dots,a_n) \in (\mathbf{Z}/n\mathbf{Z})^n$ with almost all a_is equal to some common element of $\mathbf{Z}/n\mathbf{Z}$ (*low entropy*). E.g.:

$$\begin{aligned}\widehat{1_S}(a_1,a_2,0,\dots,0) &= \sum_{x\in S} e^{2\pi i(a_1x_1+a_2x_2)/n} \\ &= (n-2)! \sum_{x_1\neq x_2} e^{2\pi i(a_1x_1+a_2x_2)/n} \\ &= -(n-2)! \sum_{x_1} e^{2\pi i(a_1x_1+a_2x_1)/n} \\ &= \begin{cases} -n(n-2)! & \text{if } a_1+a_2=0 \\ 0 & \text{else} \end{cases}\end{aligned}$$

Minor arcs (cyclic group case)

Minor arcs: $(a_1, \ldots, a_n) \in (\mathbf{Z}/n\mathbf{Z})^n$ with lots of different coordinates (*high entropy*). E.g. if all a_is are distinct, then (invariance under permutations + Parseval):

$$n!|\widehat{1_S}(a_1, \ldots, a_n)|^2 \leq \sum_{b_1,\ldots,b_n \in (\mathbf{Z}/n\mathbf{Z})^n} |\widehat{1_S}(b_1, \ldots, b_n)|^2 = n^n n!$$

$$|\widehat{1_S}(a_1, \ldots, a_n)| \leq n^{n/2}$$

Proof idea (general case)

Fourier analysis on G^n

Instead of the usual abelian discrete Fourier analysis, we use a variant which utilizes group representations.

G group, $|G| = n$

Let $S = \{\text{bijections } \{1, \ldots, n\} \to G\} \subset G^n$. Then

$$n! \cdot \mathrm{tran}(G) = \#\{\pi_1, \pi_2, \pi_3 \in S^3 : \pi_1\pi_2\pi_3 = 1\}.$$

Irreducible representations of G^n

$$\mathrm{Irr}(G^n) = \{\rho_1 \otimes \cdots \otimes \rho_n : \rho_1, \ldots, \rho_n \in \mathrm{Irr}(G)\}.$$

For $f\colon G^n \to \mathbf{R}$ and $\rho_1, \ldots, \rho_n \in \mathrm{Irr}(G)$:

$$\widehat{f}(\rho_1 \otimes \cdots \otimes \rho_n) = \sum_{x \in G^n} f(x) \cdot \rho_1(x_1) \otimes \cdots \otimes \rho_n(x_n).$$

Fourier analysis on G^n gives

$$n! \cdot \mathrm{tran}(G) = n^{-n} \sum_{\rho \in \mathrm{Irr}(G^n)} \left\langle \widehat{1_S}(\rho)^3, \rho(1) \right\rangle_{\mathrm{HS}} \dim \rho.$$

Major and minor arcs

$$n! \cdot \mathrm{tran}(G) = n^{-n} \sum_{\rho \in \mathrm{Irr}(G^n)} \left\langle \widehat{1_S}(\rho)^3, \rho(1) \right\rangle_{\mathrm{HS}} \dim \rho.$$

Major arcs: $\rho = (\rho_1, \ldots, \rho_n)$ with almost all ρ_is equal to some common one-dimensional representation $\rho_0 \in \mathrm{Irr}(G)$.

Minor arcs: the rest.