Counting transversals in group multiplication tables

Rudi Mrazović

University of Zagreb

Joint work with Sean Eberhard and Freddie Manners

24 June 2021

8th European Congress of Mathematics

Supported by HRZZ
UIP-2017-05-4129 (MUNHANAP)

Transversals in Latin squares

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.

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

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:

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

Conjectures about transversals

Conjecture (Ryser, 1967)

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

Conjecture (Brualdi–Stein, 1975)

Every $n \times n$ Latin square has a partial transversal of order $n-1$ (i.e. $n-1$ cells in distinct rows and columns and having different symbols).

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 ($G = \mathbf{Z}_n$, 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':

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

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

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

Heuristic

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

Zeroth approximation

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

First approximation

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

Let $x, y \in \mathbf{Z}_n$ with $x \neq y$. If $\psi_1\colon \mathbf{Z}_n \to \mathbf{Z}_n$ is a random function such that $\sum_{x \in \mathbf{Z}_n} \psi_1(x) = 0$, 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 $\operatorname{coll} f = \#\{x, y \in \mathbf{Z}_n : x \neq y, f(x) = f(y)\}$.

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

Second approximation

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

Let $\psi_2 \sim$ 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 $H = \{f : \sum_{x \in \mathbf{Z}_n} f(x) = 0\}$.

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

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

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

Theorem (Eberhard–Manners–M., 2019)

For n odd we have

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

Nonabelian heuristic

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

Zeroth approximation

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

First approximation

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

Second approximation

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

Nonabelian result

Theorem (Eberhard–Manners–M., 2020)

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

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