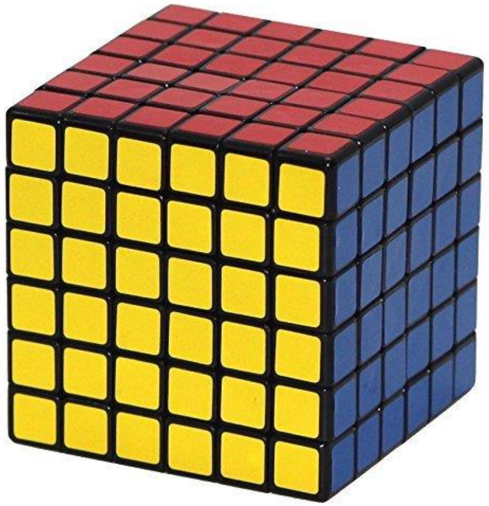
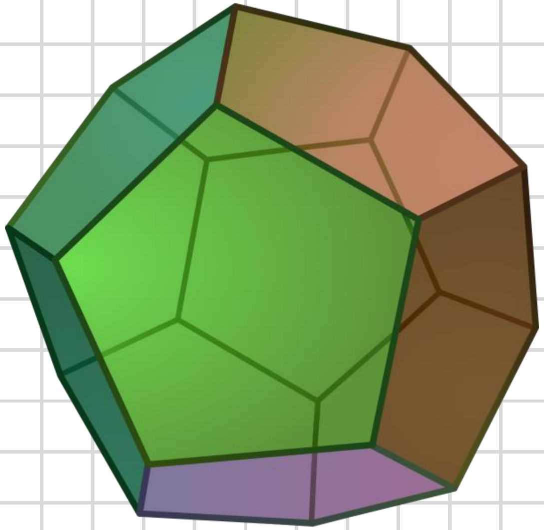
Igor Pak, UCLA

Dec 13 , 2021

How linear algebra proved expansion of graphs and is on the way to rule the world

IPAM Reunion Workshop, UCLA, Lake Arrowhead, CA





Key problem in computational group theory

Input: Finite group G

Output: Random element $h \in G$

More precisely:

Input: Finite group $G = \langle s_1, \ldots, s_k \rangle$, where $s_i \in S_N$ $[\mathrm{GL}(d,\mathbb{R}),\ \mathrm{GL}(d,\mathbb{F}_q)$, etc.$]$, $\varepsilon > 0$

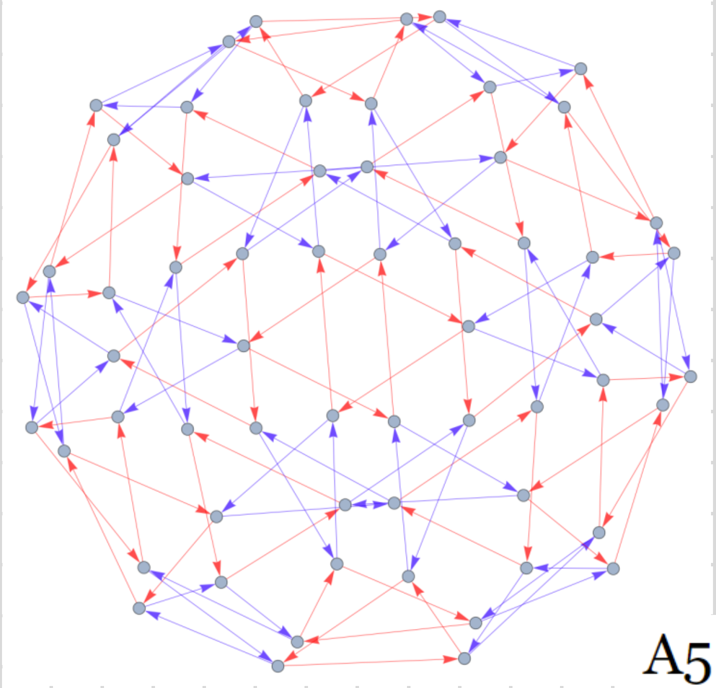
Output: Random element $h \in G$ from an *ε-uniform distribution* on G

ε-uniform distribution: $\frac{1-\varepsilon}{|G|} < \mathbb{P}[h = z] < \frac{1+\varepsilon}{|G|}$ for all $z \in G$

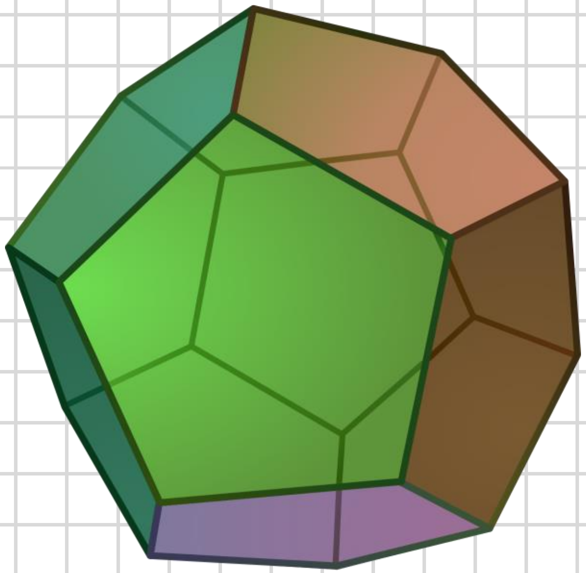
Think $k = 10,\ N = 10^4,\ d = 100,\ q = 49$

Why bother?

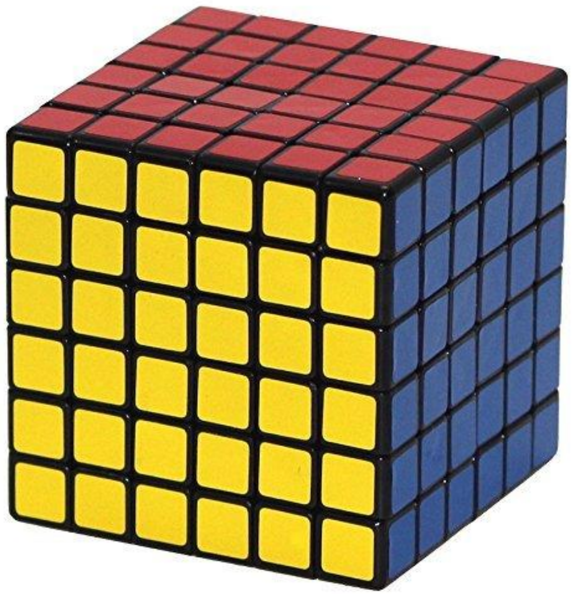
Groups appear: symmetries of combinatorial objects, graphs or general data
scientific computing (physics, chemistry, genomics, etc.)



A5



$A_5 \times Z_2$



$$|G| = \frac{8! \times 3^7 \times 24!^6}{24^{25}} \approx 1.57 \times 10^{116}$$

Why bother?

Search The Guardian For 200 years US edition

Australia sport

'The popularity has just completely exploded': Rubik's Cube's second coming

Fri 10 Dec 2021

Red Bull RUBIK'S CUBE WORLD CUP

03 – 04 Dec

H. A 6-year-old girl who set a world record in Rubik's Cube game!!

india herald .com epass

Alberta teen solves Rubik's cube 300 times while riding unicycle, beats Guinness World Record

CBC NEWS

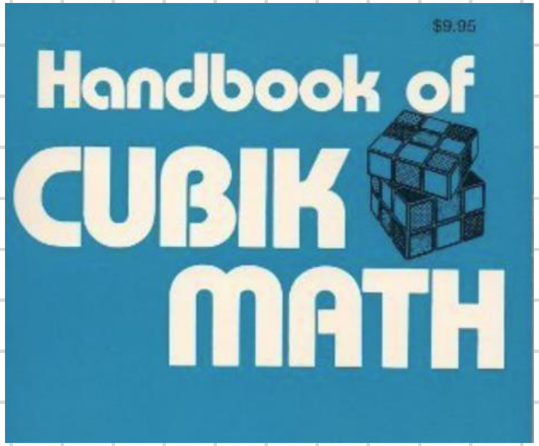
WSJ

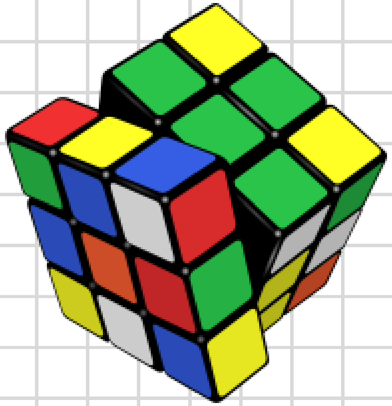
HOW TO TEACH PROFESSORS HUMILITY? HAND THEM A RUBIK'S CUBE.

Feb. 26, 2021

Why bother?

My favorite real world application: search under symmetry





$|G| = 43{,}252{,}003{,}274{,}489{,}856{,}000$

"No one knows how many moves would be needed for 'God's Algorithm' assuming he always used the fewest moves required to restore the cube. Experienced group theorists have conjectured that the smallest number of moves which would be in the low twenties." [Frey, Singmaster, 1982]

Why bother?

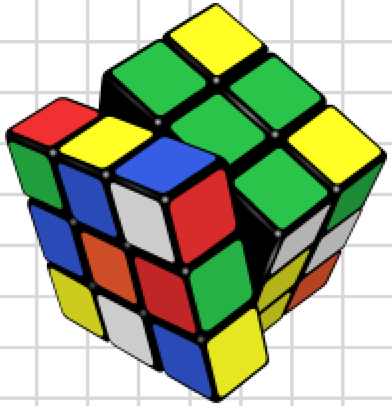
My favorite real world application: search under symmetry

ISSAC '07

Twenty-Six Moves Suffice for Rubik's Cube

Daniel Kunkle* Gene Cooperman*

8000 CPU hours ≈ 1 year



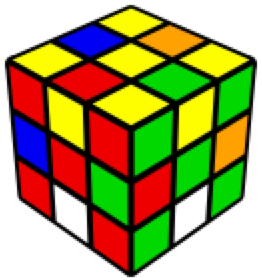
$$|G| = 43{,}252{,}003{,}274{,}489{,}856{,}000$$

SIAM Rev., 56(4), 645–670. (26 pages) © 2014

The Diameter of the Rubik's Cube Group Is Twenty

Tomas Rokicki, Herbert Kociemba, Morley Davidson, and John Dethridge

Superflip



one billion sec. CPU time
≈ 32 years (donated by Google)

Why bother?

In mathematics: Classification of Finite Simple Groups

Higman–Sims group (1968), Lyons–Sims group (1973), etc.

Random group elements: Testing group properties (nilpotent, solvable, etc.)

Group isomorphism, maximal subgroups, computing the whole lower central series, etc.

Example: $g, h \leftarrow$ random elements in G

- If $\mathbb{P}[gh = hg] > \frac{5}{8}$ then G is abelian [MacHale, 1974]
- If $\mathbb{P}\big[\langle g, h\rangle \text{ is solvable}\big] > \frac{11}{30}$ then G is solvable [Guralnick, Wilson, 2000]

Proof uses CFSG

In theory it's all easy

Theorem [Babai, 1991]
Random group elements can be generated in $O(\mu \cdot \log^5 |G|)$ time, where μ is the cost of group multiplication and inversion.

Minor problem: The real world $(k = 10,\ N = 10^4,\ d = 100,\ q = 49$, etc.)

Theorem [Cooperman'02, Dixon'08]
Random group elements can be generated in $O(\mu \cdot \log^2 |G|)$ time.

Minor problem: Still there...

Want: Random group elements in $O(\mu \cdot \log |G|)$ time.

Product Replacement Algorithm

Input: Finite group $G = \langle s_1, \ldots, s_k \rangle$

Output: Random element $h \in G$

Generating random elements of a finite group

Frank Celler , Charles R. Leedham-Green , Scott H. Murray , Alice C. Niemeyer & E.A. O'brien

COMMUNICATIONS IN ALGEBRA, 23(13), 4931–4948 (1995)

Set: $(g_1, \ldots, g_k) \leftarrow (s_1, \ldots, s_k)$

Repeat: *product replacement* t times

$$R^{\pm}_{i,j} : (g_1, \ldots, g_i, \ldots, g_k) \longrightarrow (g_1, \ldots, g_i \cdot g_j^{\pm 1}, \ldots, g_k), \text{ or}$$

$$L^{\pm}_{i,j} : (g_1, \ldots, g_i, \ldots, g_k) \longrightarrow (g_1, \ldots, g_j^{\pm 1} \cdot g_i, \ldots, g_k),$$

where L/R, sign $\pm$, and $i \neq j$ are chosen at random

Output: random component g_i

Group	Order	t
J_2	604800	51
$PSp(6,2)$	1451520	48
$U_5(2)$	13685760	56
A_{11}	19958400	71
HS	44352000	49
M_{24}	244823040	57
S_{12}	479001600	53

Experimental evidence: for $k = 10$, $t < 100$ seems to suffice even for very large groups.

Product Replacement Algorithm

GAP (Groups, Algorithms and Programming)

Magma (computer algebra system)

From Wikipedia, the free encyclopedia

Product Replacement in the Monster

Petra E. Holmes, Stephen A. Linton, Scott H. Murray

Experiment. Math. 12(1): 123-126 (2003).

Product Replacement Algorithm

Experimental Claim: PRA generates random elements in $O\big(\mu \cdot \log |G|\big)$ time.

Theorem [Diaconis and Saloff-Coste, 1998]

PRA works in $O\big(\mu \cdot |G|^{2k+3} \log |G| (\log\log |G|)^{2k}\big)$ time for $k = \Omega(\log |G|)$

Invent. math. 134, 251–299 (1998)

Walks on generating sets of groups

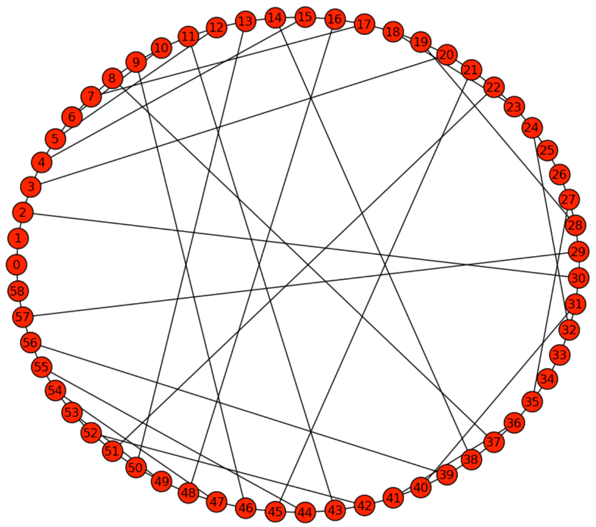
P. Diaconis[1], L. Saloff-Coste[2]

Theorem [P., 2000]

PRA works in $O\big(\mu \cdot \log^9 |G| \cdot (\log\log |G|)^5\big)$ time for $k = \Theta\big(\log |G| \log\log |G|\big)$

FOCS 2000

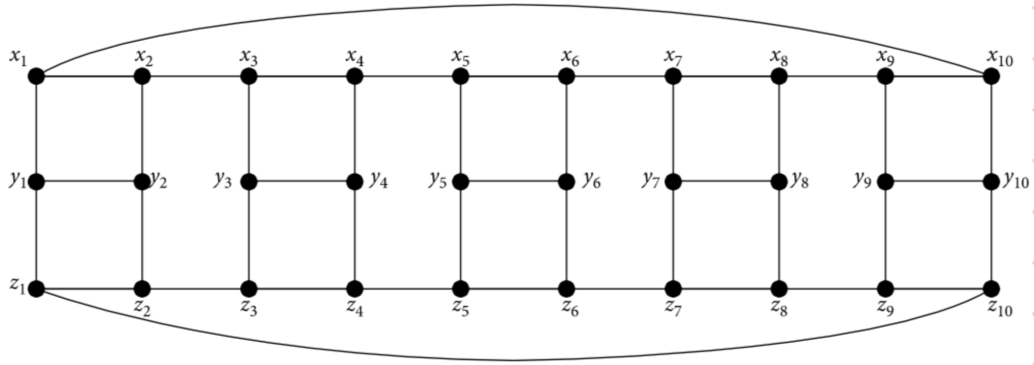
Expander graphs



Definition: (d, ε)-*expander* is a d-regular graph $H = (V, E)$

s.t. $\phi(H) > \varepsilon > 0$, where $\phi(H) := \min_{A \subset V,\ 1 \leq |A| \leq |V|/2} \dfrac{|E(A, V \smallsetminus A)|}{d \cdot |A|}$

Note: Random 3-regular graphs are expanders,
but explicit constructions are hard to find.



Proposition: For d, ε fixed and $|V| \to \infty$,
we have $\operatorname{mix}(\Gamma) = O\big(\log |V|\big)$.

Proof: Easy linear algebra.

Now we want: Product replacement graphs $\mathrm{PR}(G, k)$ are expanders.

Proving expansion: first steps

Theorem [Nielsen, 1924]
Let $G = F_k$ be free group with k generators.
Then $L^{\pm}_{i,j}$, $R^{\pm}_{i,j}$ are generators of $\mathrm{Aut}(F_k)$.

Corollary: $\mathrm{PR}(G,k)$ are *Schreier graphs* of $\mathrm{Aut}(F_k)$
[i.e. graphs of the action of $\mathrm{Aut}(F_k)$ on generating k-tuples of G]

Definition: Group $\Gamma = \langle S \rangle$ has *Kazhdan's property* (T) if *all* Schreier graphs H of $\Gamma = \langle S \rangle$ (finite and infinite), have expansion $\phi(H) > \varepsilon(S) > 0$.

Major Conjecture: $\mathrm{Aut}(F_k)$ has Kazhdan's property (T)

Theorem/Observation [Lubotzky, P., 2001]
Major Conjecture implies that graphs $\mathrm{PR}(G,k)$ are expanders.

Proving expansion: brief history

1) Kazhdan (1967): $\mathrm{SL}(k,\mathbb{Z})$ has (T) for $k \geq 3$

2) Margulis (1973): Cayley graphs of $\mathrm{SL}(3,\mathbb{F}_q)$ are expanders

More recently and more to the point:

3) Shalom (1999): (T) for $\mathrm{SL}(3,\mathbb{Z})$ implies Kazhdan's thm

4) P. and Zuk (2001): (T) implies rapid mixing for symmetric generating sets S

5) Silberman (2011): (T) is *semidecidable*

6) Ozawa (2016): (T) is a statement in *semidefinite optimization*

7) Netzer and Thom (2015): Ozawa's approach works to prove (T) for $\mathrm{SL}(3,\mathbb{Z})$

8) Fujiwara and Kabaya (2017), Kaluba and Nowak (2018): *computer assisted proofs* for more groups

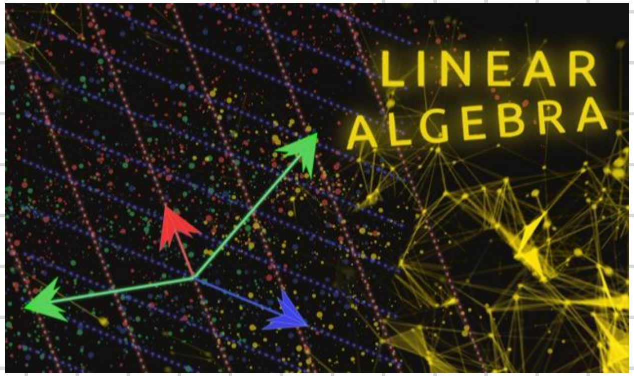
Problem solved!

1) McCool (1988): $\mathrm{Aut}(F_3)$ does not have (T)

2) Kaluba, Nowak and Ozawa (2019): $\mathrm{Aut}(F_5)$ has (T) [800 hours CPU time]

3) Kaluba, Kielak and Nowak (2021): $\mathrm{Aut}(F_k)$ has (T) for all $k \geq 5$ (only minor calculations)

4) Nitsche (2020+): $\mathrm{Aut}(F_4)$ has (T) [20 min CPU time]



Proof: Quantitative Linear Algebra and Semidefinite Programming

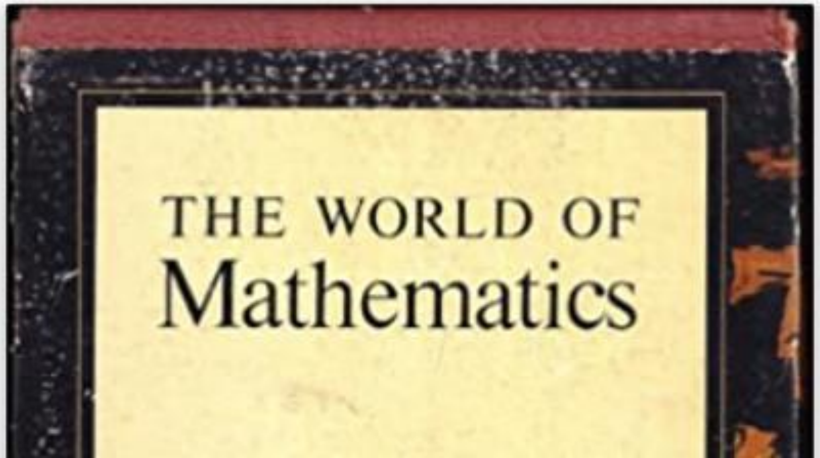
"Can a special element of the group ring $\mathbb{Z}\mathrm{Aut}(F_5)$ be written as a sum of Hermitian squares?"

Iter | pri res | dua res | rel gap | pri obj | dua obj | kap/tau | time (s)
429400| 2.31e-08 7.59e-10 4.22e-08 7.07e-08 1.13e-07 5.66e-16
3.48e+04

Conclusions:

- *Major Conjecture* is completely resolved, i.e. $\mathrm{Aut}(F_k)$ have (T) for all $k \geq 4$
- *Product replacement graphs* $\mathrm{PR}(G, k)$ are *expanders* for all finite G and all $k \geq 4$
- *Experimental Claim* confirmed, i.e. Product Replacement Algorithm works well for small k

- ***Linear Algebra is on its way to rule the world!***



Thank you!