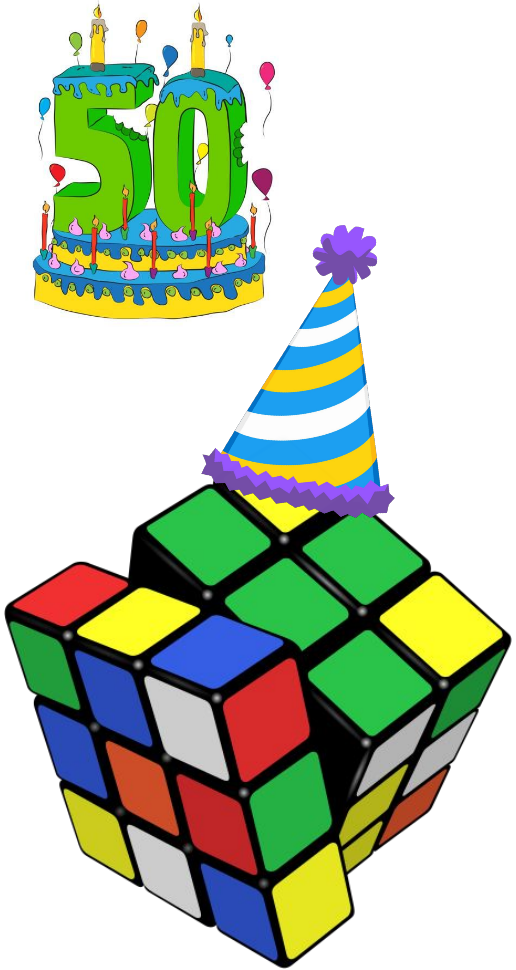


1974 Ernő Rubik invented the cube.
It took him a month to solve it.

1982 Efficient layer-by-layer method,
~20 seconds.

2010 **God’s Number:** 20 moves are
always enough

2024 Single WR: 3.13, Average WR: 4.09

So is everything done now?

"If you find a solution with the Cube, it doesn't mean you find everything. It's only a starting point. You can work on and find something else: you can improve your solution, you can make it shorter, you can go deeper and deeper and collect knowledge and many other things."

- **Ernő Rubik**

God’s Number

Year	Lower bound	Upper bound
1981	**18**	**52**
1990	**18**	**42**
1992	**18**	**39**
1992	**18**	**37**
1995	**18**	**29**
1995	**20**	**29**
2005	**20**	**28**
2006	**20**	**27**
2007	**20**	**26**
2008	**20**	**25**
2008	**20**	**23**
2008	**20**	**22**
2010	**20**	**20**

{Rokicki, Kociemba, Davidson, Dehtridge} proved God’s number to be 20.

Their proof requires **35 CPU years,** and it’s likely never been reproduced

Let's get a better feeling for these numbers!

Easy lower bound of 16

There are 18 basic moves: 6 faces, moves {90°, 180°, 270°}
So in 15 moves at most $18^{15} \approx 6*10^{18}$ positions can be reached.
But the cube has $\approx 4*10^{19}$ positions!

Human's Number

The beginner's method can solve any position in at most 205 moves

God's Number (according to their website)

How We Did It

How did we solve all 43,252,003,274,489,856,000 positions of the Cube?

- We partitioned the positions into 2,217,093,120 sets of 19,508,428,800 positions each.
- We reduced the count of sets we needed to solve to 55,882,296 using symmetry and set covering.
- We did not find optimal solutions to each position, but instead only solutions of length 20 or less.
- We wrote a program that solved a single set in about 20 seconds.
- We used about 35 CPU years to find solutions to all of the positions in each of the 55,882,296 sets.

God's Number = 20: **should you believe?**

God’s Number = 20: **should you believe?**

I personally believe both the result and paper are correct
I’d bet money on it, but not my life!

Unfortunately, **you can’t reproduce the computation**, and the result is **“brittle”**, a single position missed could break the result

In this talk

Super basic group theory

Basic graph theory

Basic Rubik ideas

Basic probabilities

You hopefully leave convinced that any position of the Rubik's cube can be solved in at most 36 moves,
(More precisely, convinced that you can finish convincing yourself at home)

Summary

- Consider the graph **G** whose vertices are positions of the cube, and edges between any two positions that are one move away
- We want to bound its diameter **diam(G)**.
- **G** is vertex-transitive (highly symmetric), we show **diam(G) ≤ 2 avgDist(G)**
- We don't know **avgDist(G)**, but we can estimate it by sampling random states
- Is a random sample going to be representative? What if there's a few rare positions that require a gazillion moves?
- **Human's Number: diam(G) ≤ 205**
- Our method takes a Human's number, and leverages it into a bound that is half as good as the best, so a **Demigod's number**

Prime Testing Analogy

Suppose you wanna prove some number theory conjecture **T**,

and you manage to prove that if **N** $= 2^{382{,}589{,}959}-1$ is prime, then **T** holds.

Checking that deterministically is currently too hard. But you can use a <u>Probabilistic Primality Test</u>!

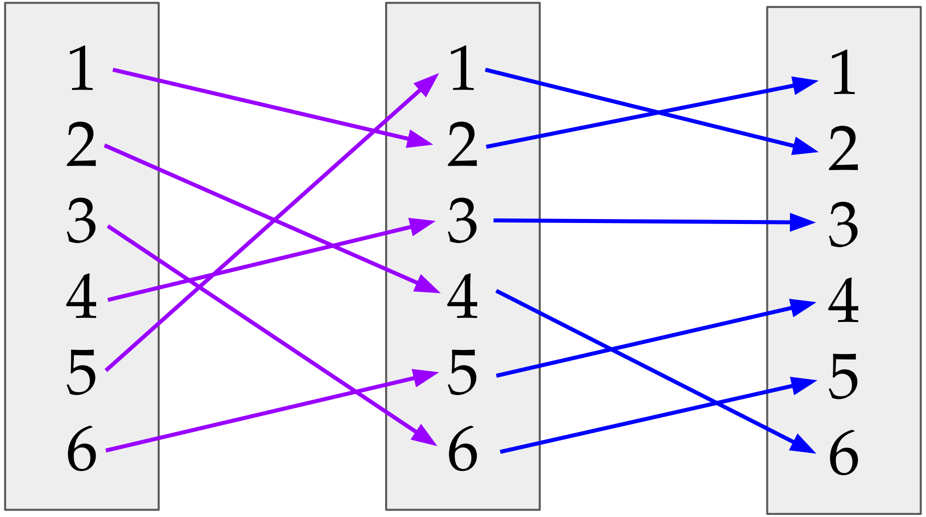
The test said *"prime"*, and the probability of that happening when provided a composite is $< 10^{-10}$.

Question: what can we say about **T**?

A Demigod's Number for the Rubik's Cube

Bernardo Subercaseaux (bersub@cmu.edu)
Joint work with Arturo Merino

What is the Rubik's cube? What's a move?



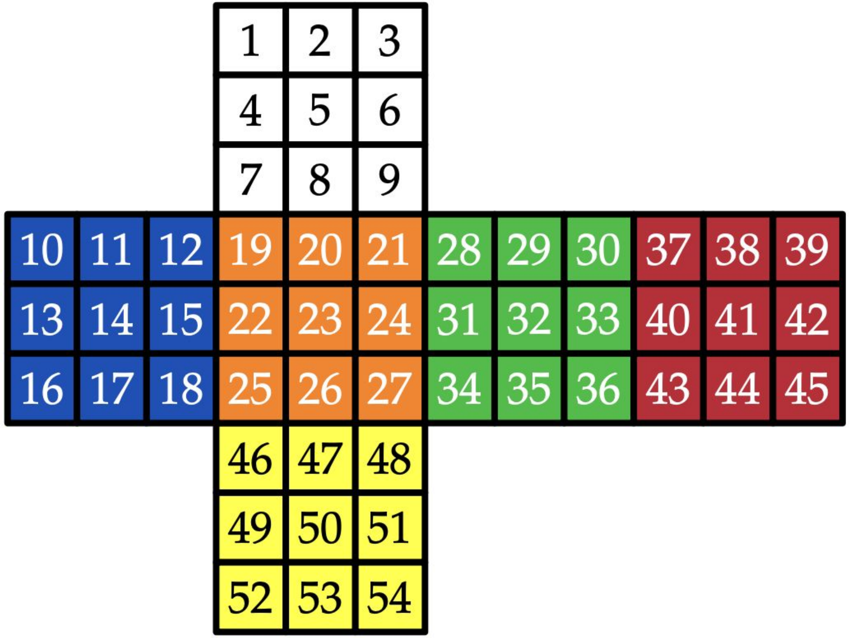
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 2 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 3 & 1 & 5 \end{pmatrix} \star \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \end{pmatrix}$$

The set of permutations over **n** elements forms a group under composition: $\mathbf{S_n}$

What is the Rubik's cube? What's a move?

$$\mathbf{R} = \begin{pmatrix} 3 & 6 & 9 & 21 & 24 & 27 & 28 & 29 & 30 & 31 & 33 & 34 & 35 & 36 & 48 & 51 & 54 \\ 48 & 51 & 54 & 3 & 6 & 9 & 30 & 33 & 36 & 29 & 35 & 28 & 31 & 34 & 21 & 24 & 27 \end{pmatrix}$$



We will think of states/moves as permutations!

What is the Rubik's cube? What's a move?

$$\mathbf{R} = \begin{pmatrix} 3 & 6 & 9 & 21 & 24 & 27 & 28 & 29 & 30 & 31 & 33 & 34 & 35 & 36 & 48 & 51 & 54 \\ 48 & 51 & 54 & 3 & 6 & 9 & 30 & 33 & 36 & 29 & 35 & 28 & 31 & 34 & 21 & 24 & 27 \end{pmatrix}$$

$$\mathbf{L} = \begin{pmatrix} 1 & 4 & 7 & 10 & 11 & 12 & 13 & 15 & 16 & 17 & 18 & 19 & 22 & 25 & 46 & 49 & 52 \\ 19 & 22 & 25 & 12 & 15 & 18 & 11 & 17 & 10 & 13 & 16 & 46 & 49 & 52 & 1 & 4 & 7 \end{pmatrix}$$

$$\mathbf{U} = \begin{pmatrix} 1 & 2 & 3 & 4 & 6 & 7 & 8 & 9 & 19 & 20 & 21 & 28 & 29 & 30 & 37 & 38 & 39 \\ 3 & 6 & 9 & 2 & 8 & 1 & 4 & 7 & 10 & 11 & 12 & 19 & 20 & 21 & 28 & 29 & 30 \end{pmatrix}$$

What is the Rubik's cube? What's a move?

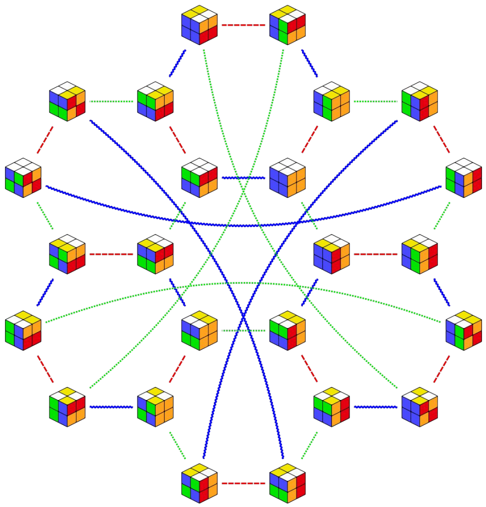
$$\mathcal{R} = \langle \mathbf{R}, \mathbf{L}, \mathbf{U}, \mathbf{D}, \mathbf{F}, \mathbf{B} \rangle < S_{54}$$

Well defined, since $\mathbf{M}^3 = \mathbf{M}^{-1}$

Actually isomorphic to a subgroup of $\mathbf{S}_{48}$
since centers don't move

Cayley Graphs

Given a group $\mathbf{G} = (\mathbf{A}, \star)$ and a set of generators $\mathbf{S} \subseteq \mathbf{A}$, the Cayley graph $\mathbf{G_S}$ is the graph with vertex set $\mathbf{A}$ and where two vertices $\mathbf{u}, \mathbf{v}$ have an edge iff there is some $\mathbf{s} \in \mathbf{S}$ such that $\mathbf{u} \star \mathbf{s} = \mathbf{v}$



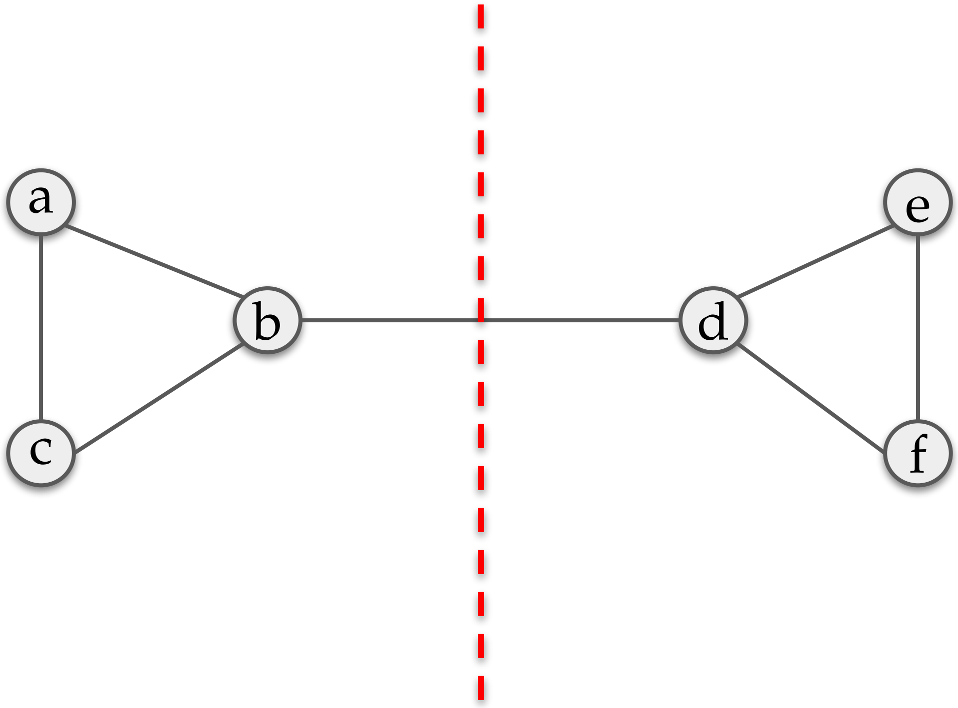
God’s Number = Diameter of Cayley Graph

$$S_{\mathcal{R}} := \{\mathbf{R}, \mathbf{R'}, \mathbf{R2}, \mathbf{L}, \mathbf{L'}, \mathbf{L2}, \mathbf{U}, \mathbf{U'}, \mathbf{U2}, \mathbf{D}, \mathbf{D'}, \mathbf{D2}, \mathbf{F}, \mathbf{F'}, \mathbf{F2}, \mathbf{B}, \mathbf{B'}, \mathbf{B2}\}$$

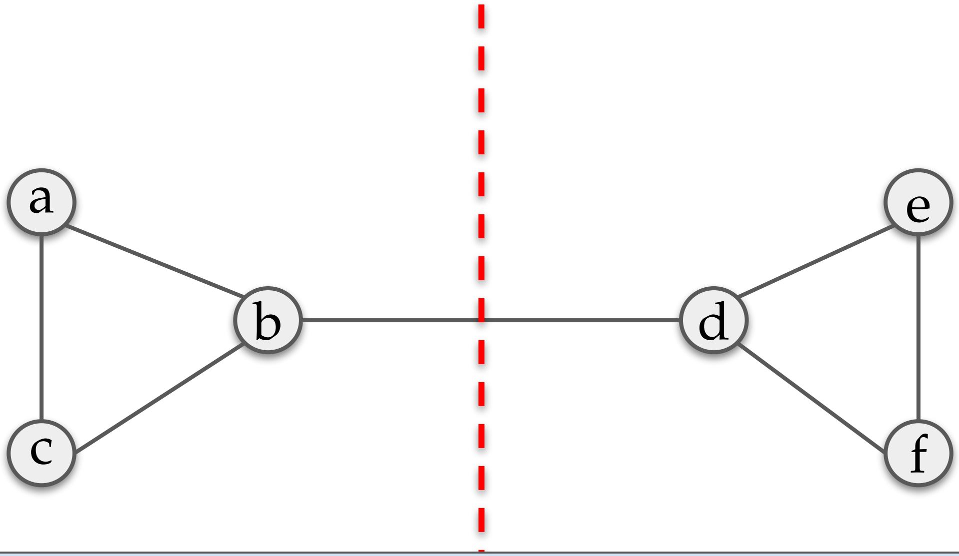
We want to count all face turns as a single move (“half turn metric”)
God’s number is actually 26 in the “quarter turn” metric

We have defined the problem!
Now let’s try to say something about it

Symmetries in Graphs



Symmetries in Graphs

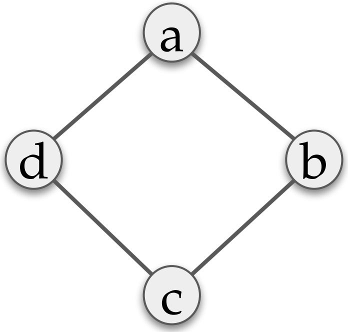


The function **φ** mapping vertices across the symmetry
(e.g., **φ(a) = e, φ(b) = d, φ(e) = a, φ(f) = c**)
respects the graph structure:
(u, v) is edge iff (**φ(u), φ(v)**) is edge

Symmetries in Graphs

Given a graph **G = (V, E)**,
a
<u>graph automorphism</u> of **G** is a bijection $\boldsymbol{\varphi}$**:** $\mathbf{V \rightarrow V}$ such that

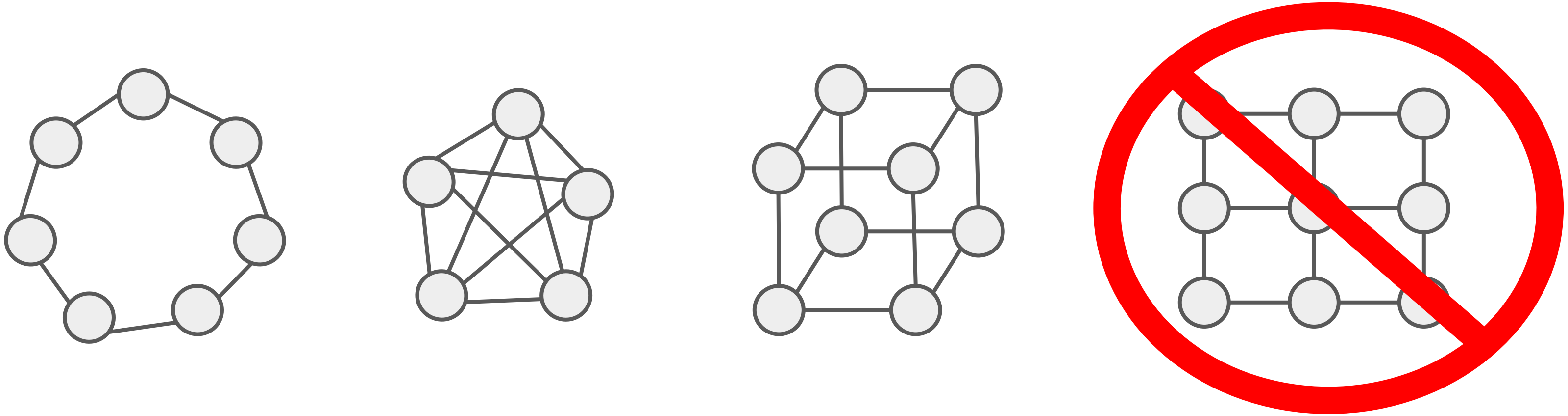
$$(\mathbf{u}, \mathbf{v}) \in \mathbf{E} \Leftrightarrow (\varphi(\mathbf{u}), \varphi(\mathbf{v})) \in \mathbf{E}$$



How many automorphisms?

Vertex-transitive graphs: full symmetry

A graph **G = (V, E)** is vertex-transitive if for every pair of vertices u, v there exists an automorphism **φ** such that **φ(u) = v**



All Cayley's are vertex-transitive!

- Let $\mathbf{G} = (\mathbf{A}, \star)$ be a group, and $\mathbf{S} \subseteq \mathbf{A}$ a set of generators. Let $\mathbf{u}, \mathbf{v}$ be any vertices of $\mathbf{G_S}$; our goal is to build an automorphism $\boldsymbol{\varphi}$ such that $\boldsymbol{\varphi}(\mathbf{u}) = \mathbf{v}$.

- Define $\boldsymbol{\varphi}(\mathbf{x}) = \mathbf{v} \star \mathbf{u}^{-1} \star \mathbf{x}$. Note that indeed $\boldsymbol{\varphi}(\mathbf{u}) = \mathbf{v}$.
  Bijective since $\mathbf{x} \rightarrow \mathbf{u} \star \mathbf{v}^{-1} \star \mathbf{x}$ is an inverse.

- Recall that $(\mathbf{x}, \mathbf{y})$ **in** $\mathbf{E}(\mathbf{G_S})$ **iff** $\mathbf{x} \star \mathbf{s} = \mathbf{y}$ for some $\mathbf{s}$ **in** $\mathbf{S}$. Equivalently, $\mathbf{x}^{-1} \star \mathbf{y}$ **in** $\mathbf{S}$.

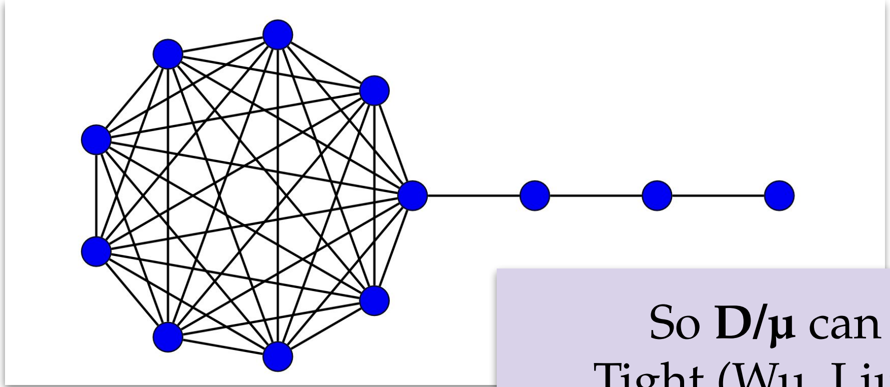
- $$\begin{aligned}\boldsymbol{\varphi}(\mathbf{x})^{-1} \star \boldsymbol{\varphi}(\mathbf{y}) &= (\mathbf{v} \star \mathbf{u}^{-1} \star \mathbf{x})^{-1} \star (\mathbf{v} \star \mathbf{u}^{-1} \star \mathbf{y}) \\ &= (\mathbf{x}^{-1} \star \mathbf{u} \star \mathbf{v}^{-1}) \star (\mathbf{v} \star \mathbf{u}^{-1} \star \mathbf{y}) = \mathbf{x}^{-1} \star \mathbf{y}\end{aligned}$$
- So $(\mathbf{x}, \mathbf{y})$ **in** $\mathbf{E}(\mathbf{G_S}) \Leftrightarrow \mathbf{x}^{-1} \star \mathbf{y}$ **in** $\mathbf{S} \Leftrightarrow \boldsymbol{\varphi}(\mathbf{x})^{-1} \star \boldsymbol{\varphi}(\mathbf{y})$ **in** $\mathbf{S} \Leftrightarrow (\boldsymbol{\varphi}(\mathbf{x}), \boldsymbol{\varphi}(\mathbf{y}))$ **in** $\mathbf{E}(\mathbf{G_S})$

The **Mean** and the **Max**

Average Wage: $36

Question: can the diameter of a graph be arbitrarily larger than its average distance?

The **Mean** and the **Max:** General Case



Clique on **N** vertices + Path on $\mathbf{N^{1/2}}$ vertices

Diameter = $\mathbf{N^{1/2} + 1}$

So **D/μ** can be up to $\mathbf{N^{1/2}}$
Tight (Wu, Liu, An , Yan, Liu)

$$
\begin{aligned}
\mu &= \frac{1}{\binom{|V(G)|}{2}} \sum_{u,v \in \binom{V(G)}{2}} d(u,v) \\
&= \frac{1}{\Omega(n^2)} \Bigg(\underbrace{1 \cdot O(n^2)}_{\text{between clique vertices}} + \underbrace{O(n^{1/2}) \cdot O(n)}_{\text{between path vertices}} + \underbrace{O(n^{1/2}) \cdot n \cdot n^{1/2}}_{\text{clique-to-path}} \Bigg) \\
&= O(1).
\end{aligned}
$$

The **Mean** and the **Max:** Vertex Transitive Case

Lemma

In any vertex transitive graph $G = (V, E)$, the average distance between vertices $\mu := \sum_{u,v \in V} d(u,v)/\binom{|V|}{2}$ coincides with the average distance to any fixed vertex u. That is,

$$\mu = \frac{\sum_{v \in V} d(u,v)}{|V| - 1}.$$

Theorem

For any vertex-transitive graph G we have

$$D < 2\mu.$$

The **Mean** and the **Max:** Vertex Transitive Case

Theorem

For any vertex-transitive graph G we have

$$D < 2\mu.$$

Let **u** and **v** be "antipodal", **d(u, v) = D.**

$$\mu = \frac{\sum_{x\in V} d(u,x)}{|V|-1} = \frac{\sum_{x\in V} d(v,x)}{|V|-1}$$

$$\begin{aligned} 2\mu &= \frac{\sum_{x\in V} d(u,x)}{|V|-1} + \frac{\sum_{x\in V} d(v,x)}{|V|-1} \\ &\geq \frac{\sum_{x\in V} d(u,v)}{|V|-1} \\ &= \frac{|V|\cdot D}{|V|-1} > D. \end{aligned}$$

Getting a good estimate of the mean

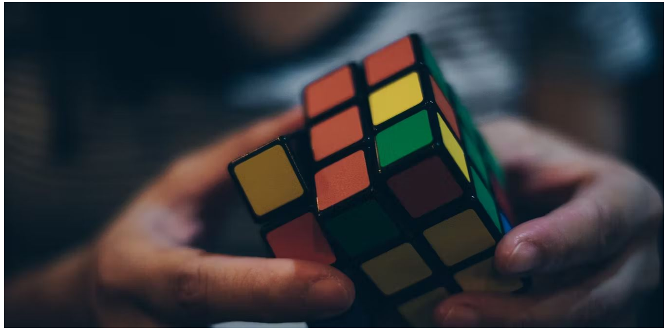
Lemma 1 (Hoeffding's inequality). *Let $X_1, X_2, \ldots, X_s$ be identical independent random variables such that $X_i \in [0, C]$. Let $\hat{\mu} = (\sum_{i=1}^{s} X_i)/s$ be their average, and $\mu = \mathbb{E}[X_1] = \ldots = \mathbb{E}[X_s]$ their expectation. Then,*

$$\Pr\left(\left|\mu - \hat{\mu}\right| \geq t\right) \leq 2\exp\left(\frac{-2t^2}{C^2 \cdot s}\right).$$

In our case **C = 205 (Human's number; beginner's method)**

How can we sample uniformly random states of the cube **efficiently**?

When solving the cube we think that



This is the **legit** way

This is **lame**

For scrambling into a uniformly random position
it's the opposite!
A random permutation of the pieces has a 1/12 chance of being a valid state of the cube

Putting things together

Theorem 1. *Given a state s of the Rubik's Cube, let $d(s)$ be the distance from s to the solved state. Let S be a set of states of the Rubik's cube sampled uniformly at random, and let $\widehat{\mu}_S = \frac{1}{|S|} \sum_{s \in S} d(s)$ be the random variable corresponding to the average distance between states in S and the solved state. Then, if D denotes the diameter of the Rubik's Cube, we have*

$$\Pr_S \left[D \geq 2\widehat{\mu}_S + 0.36\right] < 2 \exp\left(-\frac{|S|}{1\,541\,939}\right).$$

Proof is just combining **μ < 2D** with Hoeffding and the Human's number.

The empirical average we got in 500.000 samples was of 18.318

We haven't exactly "proved" that **D ≤ 36**

We have designed an experiment E, such that:

1. $D > 36$ implies E being very unlikely ($< 10^{-10}$) to have a certain outcome O_E.
2. We can observe outcome O_E consistently, and running E takes only a few hours!

Hope you find this compelling evidence :)

A Demigod's Number for the Rubik's Cube

Bernardo Subercaseaux (bersub@cmu.edu)

Joint work with Arturo Merino

Permanent address: https://bsubercaseaux.github.io/assets/pdf/rubik.pdf

https://shorturl.at/JianH