ICARM Tutorial

Efficient Search for Combinatorial Objects II

Marijn J.H. Heule and Bernardo Subercaseaux

Institute for Computer-Aided Reasoning in Mathematics

`https://icarm.io/` JMM booth 409

Joint Mathematics Meetings January 6, 2026

`sat4math.com/tutorials/`

50 Years of Successes in Computer-Aided Mathematics

1976 Four-Color Theorem

1998 Kepler Conjecture

2014 Boolean Erdős discrepancy problem (using a SAT solver)

2016 Boolean Pythagorean triples problem (using a SAT solver)

2018 Schur Number Five (using a SAT solver)

2019 Keller's Conjecture (using a SAT solver)

2021 Kaplansky's Unit Conjecture (using a SAT solver)

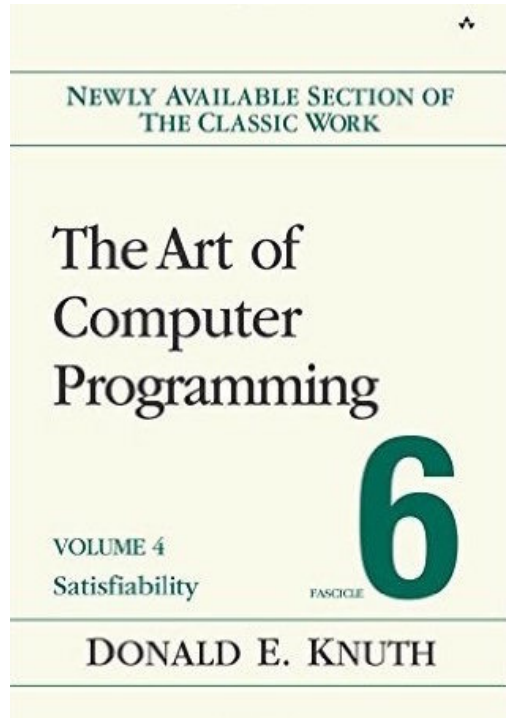
2022 Packing Number of Square Grid (using a SAT solver)

2023 Empty Hexagon in Every 30 Points (using a SAT solver)

Breakthrough in SAT Solving in the Last 30 Years

Satisfiability (SAT) problem: Can a Boolean formula be satisfied?

mid '90s: formulas solvable with thousands of variables and clauses
now: formulas solvable with millions of variables and clauses



Edmund Clarke: *"a key technology of the 21st century"* [Biere, Heule, vanMaaren, Walsh '09/'21]

Donald Knuth: *"evidently a killer app, because it is key to the solution of so many other problems"* [Knuth '15]

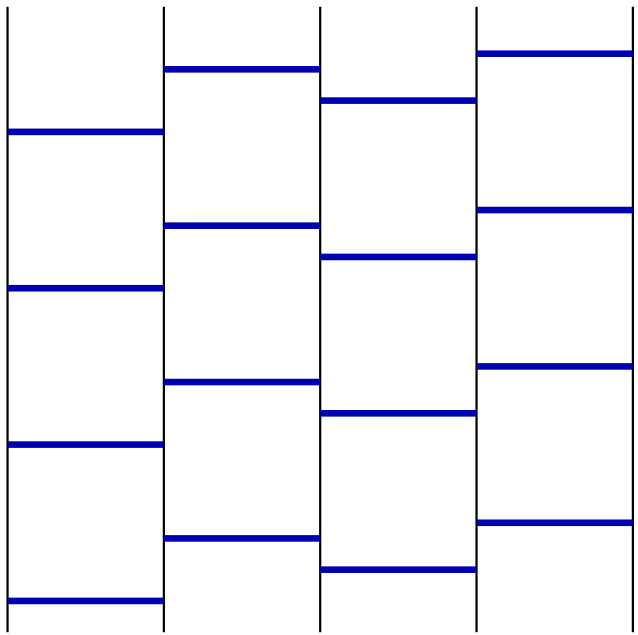
Naive SAT Solving: Truth Table

$$\Gamma := (p \vee \neg q) \wedge (q \vee r) \wedge (\neg r \vee \neg p)$$

p	q	r	falsifies	eval(Γ)
$\bot$	$\bot$	$\bot$	$q \vee r$	$\bot$
$\bot$	$\bot$	$\top$	—	$\top$
$\bot$	$\top$	$\bot$	$p \vee \neg q$	$\bot$
$\bot$	$\top$	$\top$	$p \vee \neg q$	$\bot$
$\top$	$\bot$	$\bot$	$q \vee r$	$\bot$
$\top$	$\bot$	$\top$	$\neg r \vee \neg p$	$\bot$
$\top$	$\top$	$\bot$	—	$\top$
$\top$	$\top$	$\top$	$\neg r \vee \neg p$	$\bot$

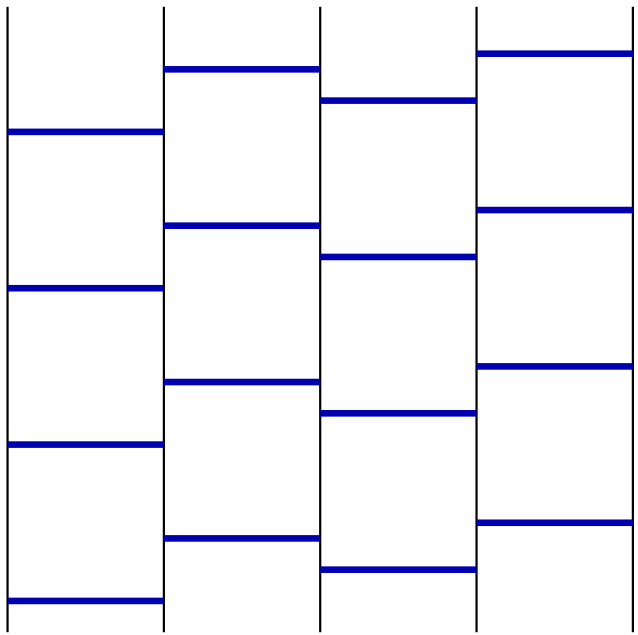
Keller's Conjecture: A Tiling Problem

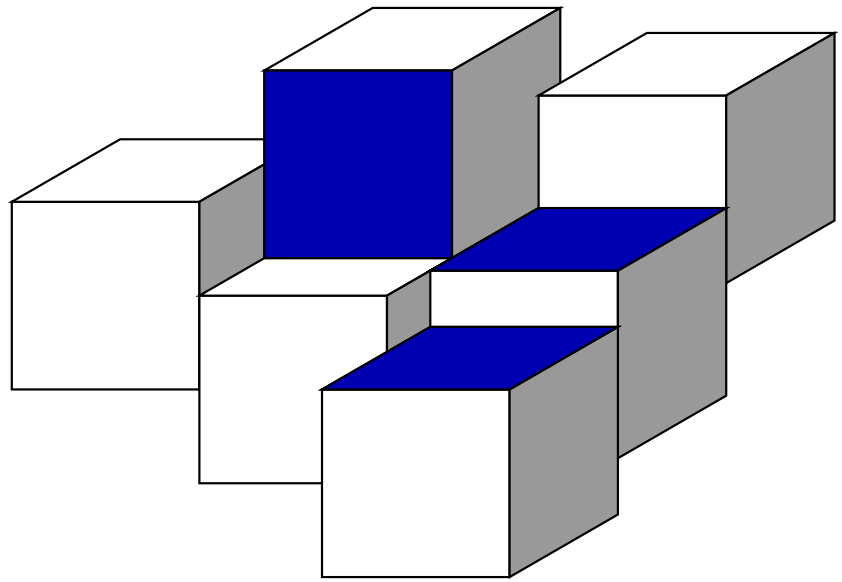
Consider tiling a floor with square tiles, all of the same size. Is it the case that any gap-free tiling results in at least two fully connected tiles, i.e., tiles that have an entire edge in common?



Keller's Conjecture: A Tiling Problem

Consider tiling a floor with square tiles, all of the same size. Is it the case that any gap-free tiling results in at least two fully connected tiles, i.e., tiles that have an entire edge in common?





Keller's Conjecture: Resolved

[Brakensiek, Heule, Mackey, & Narvaez 2019]

In 1930, Ott-Heinrich Keller conjectured that this phenomenon holds in every dimension.

Keller's Conjecture.
For all $n \geq 1$, every tiling of the n-dimensional space with unit cubes has two which fully share a face.

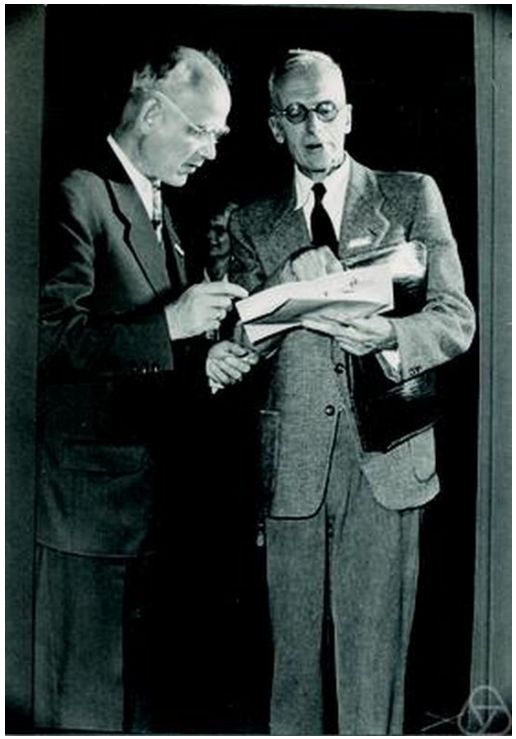
Keller's Conjecture: Resolved

[Brakensiek, Heule, Mackey, & Narvaez 2019]

In 1930, Ott-Heinrich Keller conjectured that this phenomenon holds in every dimension.

Keller's Conjecture.
For all $n \geq 1$, every tiling of the n-dimensional space with unit cubes has two which fully share a face.

- Only true for $n \leq 7$



[Wikipedia, CC BY-SA]

GEOMETRY

Computer Search Settles 90-Year-Old Math Problem

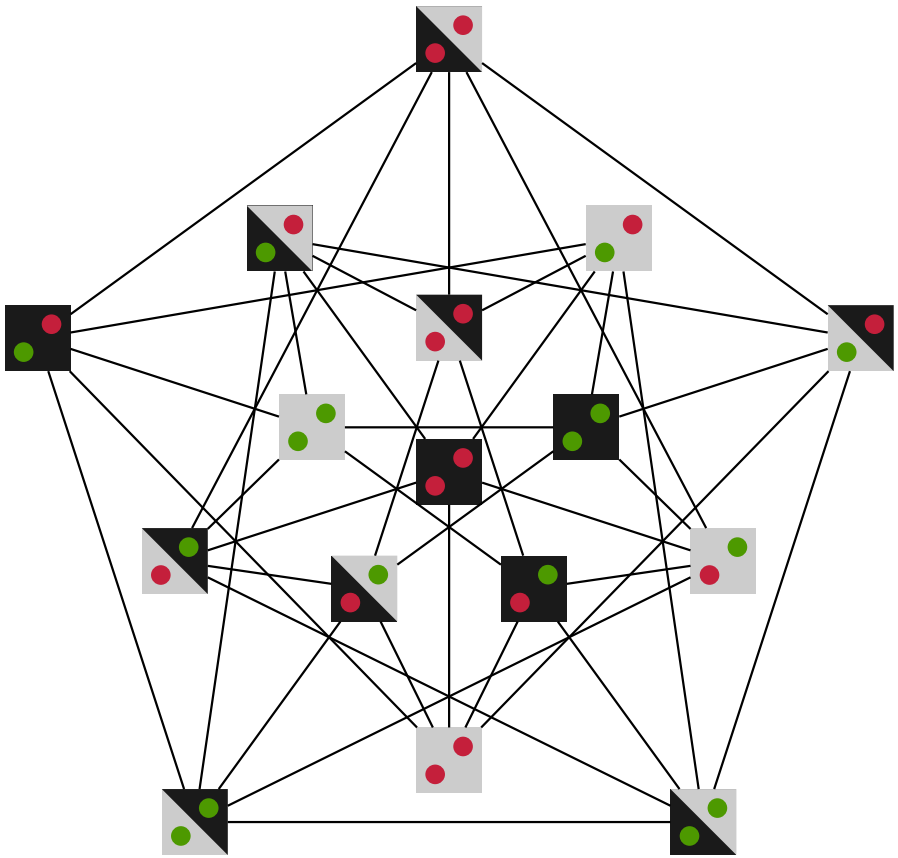
10 |

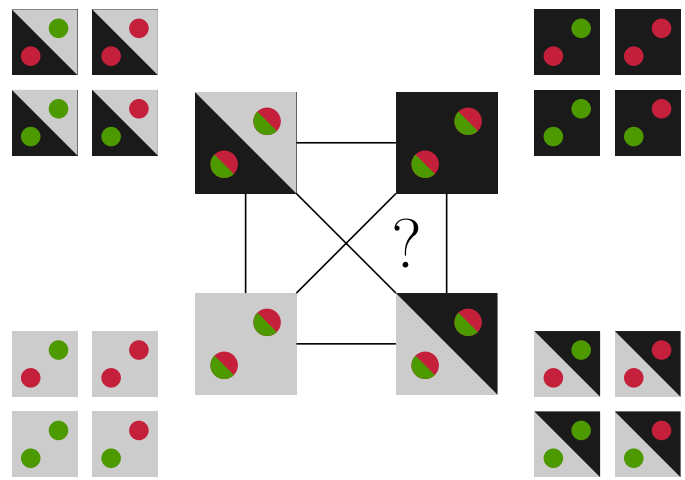
By translating Keller's conjecture into a computer-friendly search for a type of graph, researchers have finally resolved a problem about covering spaces with tiles.

Keller Graphs

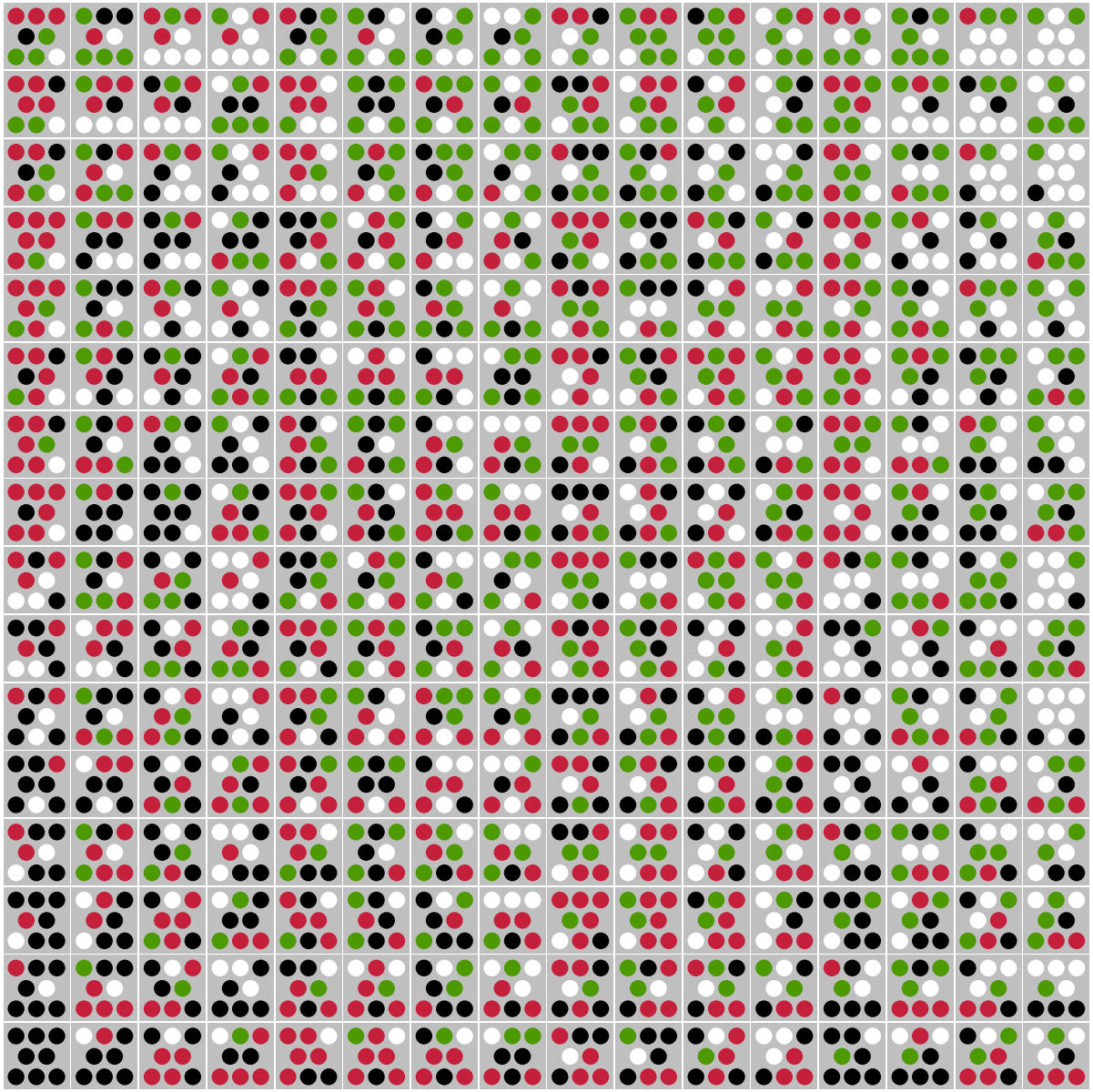
Keller's conjecture for dimension n holds if and only if the Keller graph doesn't contain a clique of size 2^n

- Graph can be partitioned into 2^n independent sets





A Counterexample to Keller's Conjecture (Dimension 8)



A Counterexample to the Unit Conjecture

Theorem ([Gardam 2021])
Let $P = \langle a, b \mid b^{-1}a^2b = a^{-2}, a^{-1}b^2a = b^{-2} \rangle$ *be a torsion-free group. Set*

$$\begin{aligned} u \;=\; & a(a+b+b^{-1}) + a^{-1}(a^{-1}+b+b^{-1}) + \\ & b(b+a+a^{-1}) + b^{-1}(b^{-1}+a+a^{-1}) + \\ & ab(a+b) + a(ab^{-1}+b^{-1}a) + ba(b+a) + b(ba^{-1}+a^{-1}b). \end{aligned}$$

Then $(u+abab)(u+baba) = 1$ *in the ring* $\mathbb{F}_2[P]$.

- The non-trivial units differ from published one, but similar
- Giles Gardam guessed P (the Promislow group)
- The SAT solver found $(u+abab)$ and $(u+baba)$

Group Ring Arithmetic Example

Example

In $\mathbb{F}_2[\mathbb{Z}/5]$, so $t^5 = 1$, we have $(1 + t + t^4)(1 + t^2 + t^3) = 1$

Group Ring Arithmetic Example

Example

In $\mathbb{F}_2[\mathbb{Z}/5]$, so $t^5 = 1$, we have $(1 + t + t^4)(1 + t^2 + t^3) = 1$

	1	t	t^2	t^3	t^4
1	1	t	t^2	t^3	t^4
t	t	t^2	t^3	t^4	1
t^2	t^2	t^3	t^4	1	t
t^3	t^3	t^4	1	t	t^2
t^4	t^4	1	t	t^2	t^3

Group Ring Arithmetic Example

Example

In $\mathbb{F}_2[\mathbb{Z}/5]$, so $t^5 = 1$, we have $(1 + t + t^4)(1 + t^2 + t^3) = 1$

	1	t	t^2	t^3	t^4
1	1	t	t^2	t^3	t^4
t	t	t^2	t^3	t^4	1
t^2	t^2	t^3	t^4	1	t
t^3	t^3	t^4	1	t	t^2
t^4	t^4	1	t	t^2	t^3

	1	t^2	t^3
1	1	t^2	t^3
t	t	t^3	t^4
t^4	t^4	t	t^2

Group Ring Arithmetic Example

Example

In $\mathbb{F}_2[\mathbb{Z}/5]$, so $t^5 = 1$, we have $(1 + t + t^4)(1 + t^2 + t^3) = 1$

	1	t	t^2	t^3	t^4
1	1	t	t^2	t^3	t^4
t	t	t^2	t^3	t^4	1
t^2	t^2	t^3	t^4	1	t
t^3	t^3	t^4	1	t	t^2
t^4	t^4	1	t	t^2	t^3

	1	t^2	t^3
1	1	t^2	t^3
t	t	t^3	t^4
t^4	t^4	t	t^2

$$1 + 2t + 2t^2 + 2t^3 + 2t^4 = 1 \quad \text{in } \mathbb{F}_2$$

Group Ring Arithmetic Example

Example

In $\mathbb{F}_2[\mathbb{Z}/5]$, so $t^5 = 1$, we have $(1 + t + t^4)(1 + t^2 + t^3) = 1$

	1	t	t^2	t^3	t^4
1	1	t	t^2	t^3	t^4
t	t	t^2	t^3	t^4	1
t^2	t^2	t^3	t^4	1	t
t^3	t^3	t^4	1	t	t^2
t^4	t^4	1	t	t^2	t^3

	1	t^2	t^3
1	1	t^2	t^3
t	t	t^3	t^4
t^4	t^4	t	t^2

$$1 + 2t + 2t^2 + 2t^3 + 2t^4 = 1 \quad \text{in } \mathbb{F}_2$$

Conjecture: Non-trivial units only occur when group is torsion

Group Ring Arithmetic of the Promislow Group

Recall $P = \langle a, b \mid b^{-1}a^2b = a^{-2}, a^{-1}b^2a = b^{-2} \rangle$

	1	a	a^{-1}	b	b^{-1}	a^2	ab	ab^{-1}	a^{-2}	$\cdots$
1	1	a	a^{-1}	b	b^{-1}	a^2	ab	ab^{-1}	a^{-2}	$\cdots$
a	a	a^2	a	ab	ab^{-1}	a^3	a^2b	a^2b^{-1}	a^{-1}	$\cdots$
a^{-1}	a^{-1}	1	a^{-2}	$a^{-1}b$	$a^{-1}b^{-1}$	a	b	b^{-1}	a^{-3}	$\cdots$
b	b	ba	ba^{-1}	b^2	1	ba^2	bab	bab^{-1}	a^2b	$\cdots$
b^{-1}	b^{-1}	$b^{-1}a$	$b^{-1}a^{-1}$	1	b^{-2}	$b^{-1}a^2$	$b^{-1}ab$	$b^{-1}ab^{-1}$	a^2b^{-1}	$\cdots$
a^2	a^2	a^3	a	a^2b	a^2b^{-1}	a^4	a^3b	a^3b^{-1}	1	$\cdots$
ab	ab	aba	aba^{-1}	ab^2	a	$a^{-1}b$	$(ab)^2$	$abab^{-1}$	a^3b	$\cdots$
ab^{-1}	ab^{-1}	$ab^{-1}a$	$ab^{-1}a^{-1}$	a	ab^{-2}	$a^{-1}b^{-1}$	$ab^{-1}ab$	$(ab)^{-2}$	a^3b^{-1}	$\cdots$
a^{-2}	a^{-2}	a	a^{-3}	ba^2	$b^{-1}a^2$	1	$a^{-1}b$	$a^{-1}b^{-1}$	a^{-4}	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

- Select at least one row and at least two columns

Group Ring Arithmetic of the Promislow Group

Recall $P = \langle a, b \mid b^{-1}a^2b = a^{-2}, a^{-1}b^2a = b^{-2} \rangle$

	1	a	a^{-1}	b	b^{-1}	a^2	ab	ab^{-1}	a^{-2}	$\cdots$
1	1	a	a^{-1}	b	b^{-1}	a^2	ab	ab^{-1}	a^{-2}	$\cdots$
a	a	a^2	a	ab	ab^{-1}	a^3	a^2b	a^2b^{-1}	a^{-1}	$\cdots$
a^{-1}	a^{-1}	1	a^{-2}	$a^{-1}b$	$a^{-1}b^{-1}$	a	b	b^{-1}	a^{-3}	$\cdots$
b	b	ba	ba^{-1}	b^2	1	ba^2	bab	bab^{-1}	a^2b	$\cdots$
b^{-1}	b^{-1}	$b^{-1}a$	$b^{-1}a^{-1}$	1	b^{-2}	$b^{-1}a^2$	$b^{-1}ab$	$b^{-1}ab^{-1}$	a^2b^{-1}	$\cdots$
a^2	a^2	a^3	a	a^2b	a^2b^{-1}	a^4	a^3b	a^3b^{-1}	1	$\cdots$
ab	ab	aba	aba^{-1}	ab^2	a	$a^{-1}b$	$(ab)^2$	$abab^{-1}$	a^3b	$\cdots$
ab^{-1}	ab^{-1}	$ab^{-1}a$	$ab^{-1}a^{-1}$	a	ab^{-2}	$a^{-1}b^{-1}$	$ab^{-1}ab$	$(ab)^{-2}$	a^3b^{-1}	$\cdots$
a^{-2}	a^{-2}	a	a^{-3}	ba^2	$b^{-1}a^2$	1	$a^{-1}b$	$a^{-1}b^{-1}$	a^{-4}	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

- Select at least one row and at least two columns
- The number of ones should be odd

Group Ring Arithmetic of the Promislow Group

Recall $P = \langle a, b \mid b^{-1}a^2b = a^{-2}, a^{-1}b^2a = b^{-2} \rangle$

	1	a	a^{-1}	b	b^{-1}	a^2	ab	ab^{-1}	a^{-2}	$\cdots$
1	1	a	a^{-1}	b	b^{-1}	a^2	ab	ab^{-1}	a^{-2}	$\cdots$
a	a	a^2	a	ab	ab^{-1}	a^3	a^2b	a^2b^{-1}	a^{-1}	$\cdots$
a^{-1}	a^{-1}	1	a^{-2}	$a^{-1}b$	$a^{-1}b^{-1}$	a	b	b^{-1}	a^{-3}	$\cdots$
b	b	ba	ba^{-1}	b^2	1	ba^2	bab	bab^{-1}	a^2b	$\cdots$
b^{-1}	b^{-1}	$b^{-1}a$	$b^{-1}a^{-1}$	1	b^{-2}	$b^{-1}a^2$	$b^{-1}ab$	$b^{-1}ab^{-1}$	a^2b^{-1}	$\cdots$
a^2	a^2	a^3	a	a^2b	a^2b^{-1}	a^4	a^3b	a^3b^{-1}	1	$\cdots$
ab	ab	aba	aba^{-1}	ab^2	a	$a^{-1}b$	$(ab)^2$	$abab^{-1}$	a^3b	$\cdots$
ab^{-1}	ab^{-1}	$ab^{-1}a$	$ab^{-1}a^{-1}$	a	ab^{-2}	$a^{-1}b^{-1}$	$ab^{-1}ab$	$(ab)^{-2}$	a^3b^{-1}	$\cdots$
a^{-2}	a^{-2}	a	a^{-3}	ba^2	$b^{-1}a^2$	1	$a^{-1}b$	$a^{-1}b^{-1}$	a^{-4}	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

- Select at least one row and at least two columns
- The number of ones should be odd
- Each other element should occur an even number of times

Encoding Exclusive OR

Given a set of Boolean variables $x_1, \ldots, x_n$, how to encode

$$\mathrm{XOR}(x_1, \ldots, x_n)$$

into SAT using a linear number of binary clauses?

The direct encoding requires 2^{n-1} clauses of length n:

$$\bigwedge_{\text{even } \#\neg} (\neg x_1 \vee \neg x_2 \vee \cdots \vee \neg x_n)$$

Encoding Exclusive OR

Given a set of Boolean variables $x_1, \ldots, x_n$, how to encode

$$\mathrm{XOR}(x_1, \ldots, x_n)$$

into SAT using a linear number of binary clauses?

The direct encoding requires 2^{n-1} clauses of length n:

$$\bigwedge_{\text{even } \#\neg} (\neg x_1 \vee \neg x_2 \vee \cdots \vee \neg x_n)$$

Make it compact: $\mathrm{XOR}\,(x_1, x_2, x_3, \neg y) \wedge \mathrm{XOR}\,(x_4, \ldots, x_n, y)$

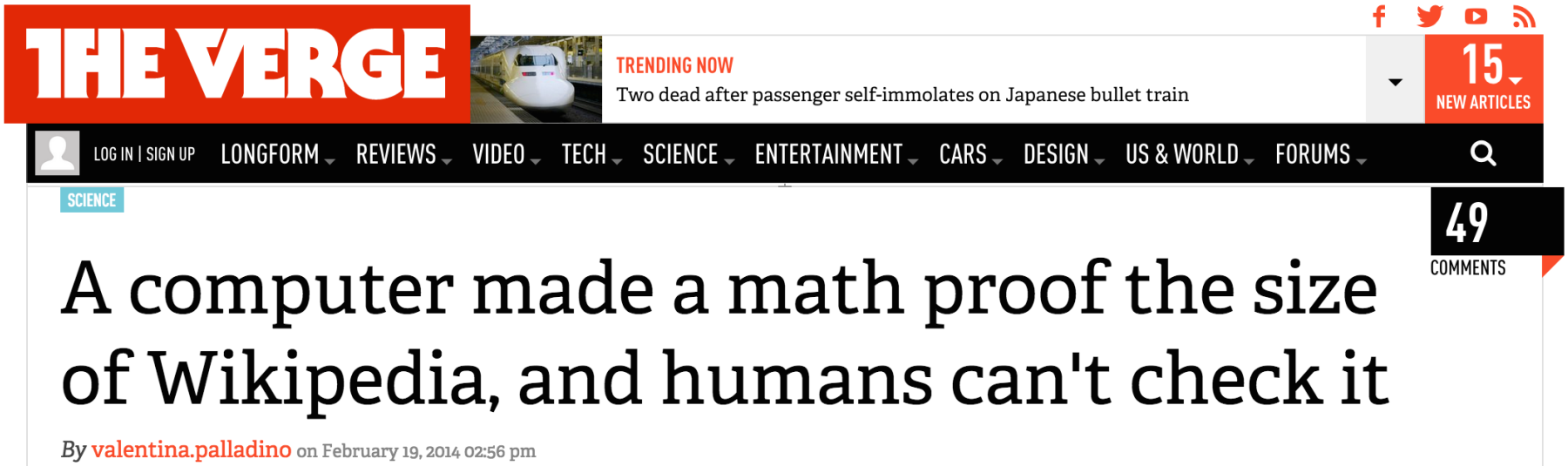
Note: $\mathrm{XOR}\,(x_1, x_2, x_3, \neg y) \equiv y \leftrightarrow \mathrm{XOR}\,(x_1, x_2, x_3)$

Tradeoff: more variables but fewer clauses!

sat4math.com/tutorials/

Unit Conjecture Tutorial

Erdős Discrepancy Problem



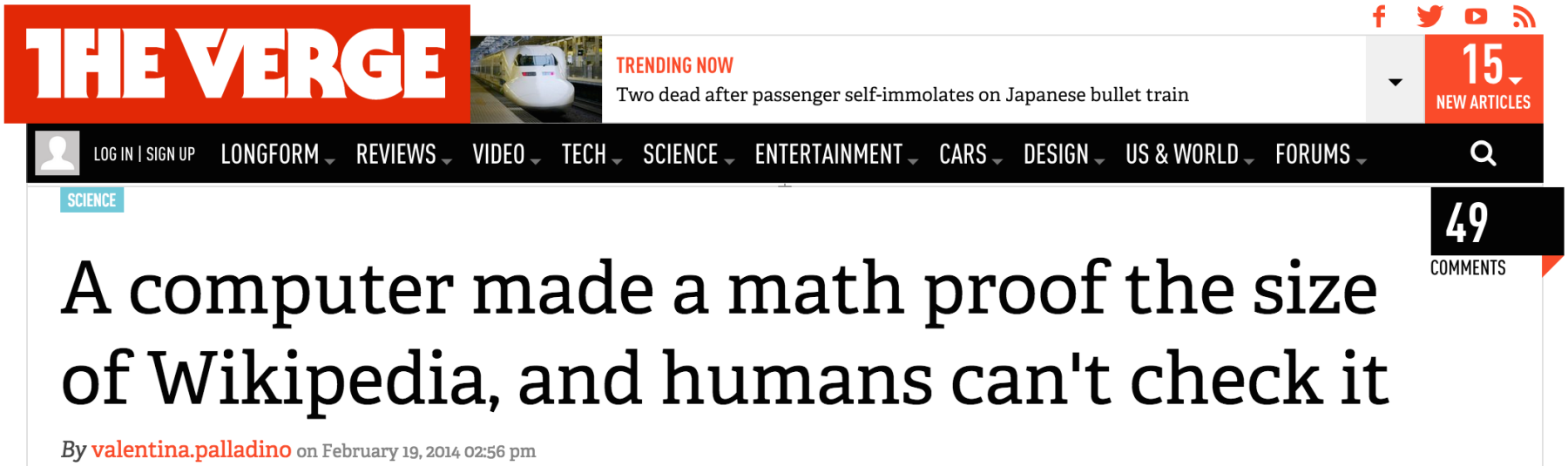
Erdős discrepancy problem with $d = 2$ solved with SAT (2014)

- The general case was solved by Terry Tao in 2015

The conjecture states that there exists no infinite sequence of $-1, +1$ such that for all k, s holds that $(x_i \in \{-1, +1\})$:

$$\left| \sum_{i=1}^{s} x_{ik} \right| \leq 2$$

Erdős Discrepancy Problem


THE VERGE

TRENDING NOW
Two dead after passenger self-immolates on Japanese bullet train

15 NEW ARTICLES

LOG IN | SIGN UP LONGFORM REVIEWS VIDEO TECH SCIENCE ENTERTAINMENT CARS DESIGN US & WORLD FORUMS

SCIENCE

49 COMMENTS

A computer made a math proof the size of Wikipedia, and humans can't check it

By valentina.palladino on February 19, 2014 02:56 pm

Erdős discrepancy problem with $d = 2$ solved with SAT (2014)

- The general case was solved by Terry Tao in 2015

The conjecture states that there exists no infinite sequence of $-1, +1$ such that for all k, s holds that $(x_i \in \{-1, +1\})$:

$$\left| \sum_{i=1}^{s} x_{ik} \right| \leq 2$$

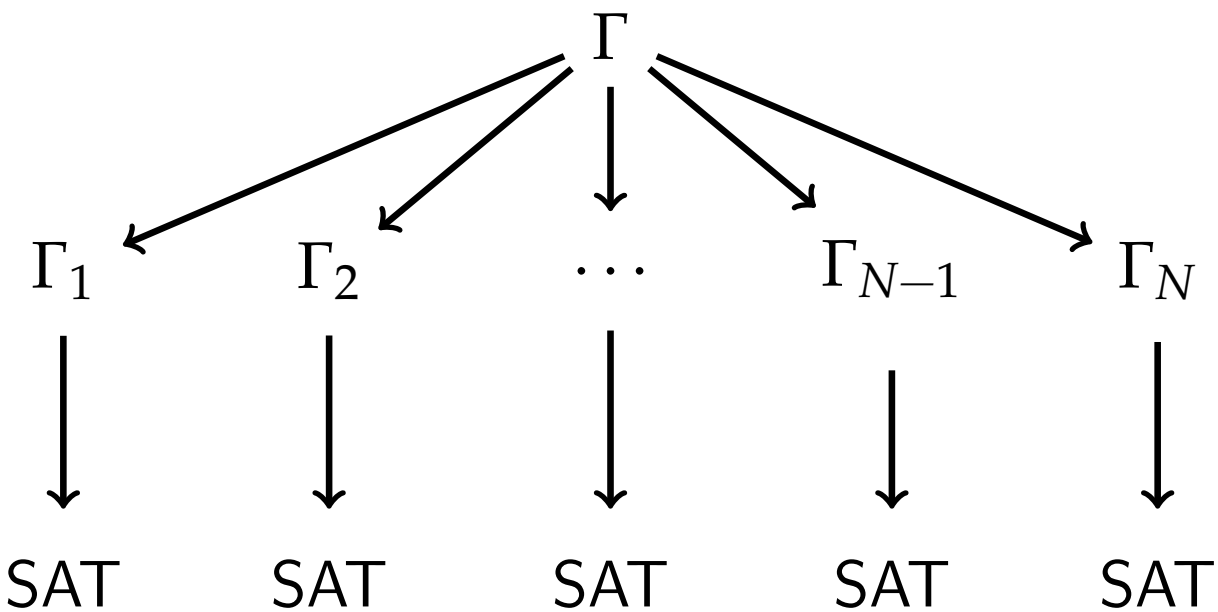
The DRAT proof was 13Gb and checked with the tool DRAT-trim [SAT14]

Cube-and-Conquer [Heule, Kullmann, Wieringa, and Biere 2011]

The Cube-and-Conquer paradigm has two phases:

Cube First a look-ahead solver is employed to split the problem — the splitting tree is cut off appropriately.

Conquer At the leaves of the tree, SAT solvers are employed.



Cube-and-Conquer achieves a good equal splitting and the sub-problems are scheduled independently (easy parallel SAT).

sat4math.com/tutorials/

Erdős Discrepancy Tutorial