Computer-Aided Mathematics and Satisfiability

Marijn J.H. Heule

Carnegie Mellon University

Mathematical Foundations for Computer Science
September 20, 2019

40 Years of Successes in Computer-Aided Mathematics

1976 Four-Color Theorem

1998 Kepler conjecture

2010 "God's Number = 20": Optimal Rubik's cube strategy

2012 At least 17 clues for a solvable Sudoku puzzle

2014 Boolean Erdős discrepancy problem

2016 Boolean Pythagorean triples problem

2018 Schur Number Five

40 Years of Successes in Computer-Aided Mathematics

1976 Four-Color Theorem

1998 Kepler conjecture

2010 "God's Number = 20": Optimal Rubik's cube strategy

2012 At least 17 clues for a solvable Sudoku puzzle

2014 Boolean Erdős discrepancy problem (using a SAT solver)

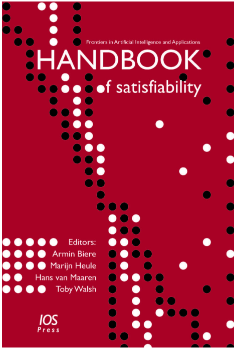
2016 Boolean Pythagorean triples problem (using a SAT solver)

2018 Schur Number Five (using a SAT solver)

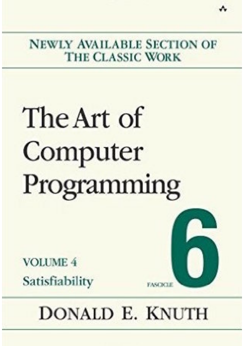
Breakthrough in SAT Solving in the Last 20 Years

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, and Walsh '09]



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

Schur's Theorem [Schur 1916]

Will any coloring of the positive integers with red and blue result in a monochromatic solution of $a + b = c$?

$$
\begin{array}{ccc}
1 + 1 = 2 & 1 + 2 = 3 & 1 + 3 = 4 \\
1 + 4 = 5 & 2 + 2 = 4 & 2 + 3 = 5
\end{array}
$$

Schur's Theorem [Schur 1916]

Will any coloring of the positive integers with red and blue result in a monochromatic solution of $a + b = c$?

$$\begin{array}{ccc} 1 + 1 = 2 & 1 + 2 = 3 & 1 + 3 = 4 \\ 1 + 4 = 5 & 2 + 2 = 4 & 2 + 3 = 5 \end{array}$$

Schur's Theorem [Schur 1916]

Will any coloring of the positive integers with red and blue result in a monochromatic solution of $a + b = c$?

$$1 + 1 = 2 \qquad 1 + 2 = 3 \qquad 1 + 3 = 4$$
$$1 + 4 = 5 \qquad 2 + 2 = 4 \qquad 2 + 3 = 5$$

Schur's Theorem [Schur 1916]

Will any coloring of the positive integers with red and blue result in a monochromatic solution of $a + b = c$?

$$1 + 1 = 2 \qquad 1 + 2 = 3 \qquad 1 + 3 = 4$$
$$1 + 4 = 5 \qquad 2 + 2 = 4 \qquad 2 + 3 = 5$$

Schur's Theorem [Schur 1916]

Will any coloring of the positive integers with red and blue result in a monochromatic solution of $a + b = c$? Yes

$1 + 1 = 2$	$1 + 2 = 3$	$1 + 3 = 4$
$1 + 4 = 5$	$2 + 2 = 4$	$2 + 3 = 5$

Schur's Theorem [Schur 1916]

Will any coloring of the positive integers with red and blue result in a monochromatic solution of $a + b = c$? Yes

$$1 + 1 = 2 \qquad 1 + 2 = 3 \qquad 1 + 3 = 4$$
$$1 + 4 = 5 \qquad 2 + 2 = 4 \qquad 2 + 3 = 5$$

Theorem (Schur's Theorem)

For every positive integer k, there exists a number $S(k)$, such that $[1, S(k)]$ can be colored with k colors while avoiding a monochromatic solution of $a + b = c$ with $a, b, c \leq S(k)$, while this is impossible for $[1, S(k)+1]$.

$S(1) = 1, S(2) = 4, S(3) = 13, S(4) = 44$ [Baumert 1965].

Schur's Theorem [Schur 1916]

Will any coloring of the positive integers with red and blue result in a monochromatic solution of $a + b = c$? Yes

$1 + 1 = 2$	$1 + 2 = 3$	$1 + 3 = 4$
$1 + 4 = 5$	$2 + 2 = 4$	$2 + 3 = 5$

Theorem (Schur's Theorem)

For every positive integer k, there exists a number $S(k)$, such that $[1, S(k)]$ can be colored with k colors while avoiding a monochromatic solution of $a + b = c$ with $a, b, c \leq S(k)$, while this is impossible for $[1, S(k)+1]$.

$S(1) = 1, S(2) = 4, S(3) = 13, S(4) = 44$ [Baumert 1965].

We show that $S(5) = 160$ [Heule 2018].

Schur's Theorem [Schur 1916]

Will any coloring of the positive integers with red and blue result in a monochromatic solution of $a + b = c$?

$$1 + 1 = 2 \qquad 1 + 2 = 3 \qquad 1 + 3 = 4$$
$$1 + 4 = 5 \qquad 2 + 2 = 4 \qquad 2 + 3 = 5$$

Theorem (Schur's Theorem)

For every positive integer k, there exists a number $S(k)$, such that $[1, S(k)]$ can be colored with k colors while avoiding a monochromatic solution of $a + b = c$ with $a, b, c \leq S(k)$, while this is impossible for $[1, S(k)+1]$.

$S(1) = 1, S(2) = 4, S(3) = 13, S(4) = 44$ [Baumert 1965].

We show that $S(5) = 160$ [Heule 2018]. Proof: 2 petabytes

Pythagorean Triples Problem (I) [Ronald Graham, early 80's]

Will any coloring of the positive integers with red and blue result in a monochromatic Pythagorean Triple $a^2 + b^2 = c^2$?

$3^2 + 4^2 = 5^2$	$6^2 + 8^2 = 10^2$	$5^2 + 12^2 = 13^2$	$9^2 + 12^2 = 15^2$
$8^2 + 15^2 = 17^2$	$12^2 + 16^2 = 20^2$	$15^2 + 20^2 = 25^2$	$7^2 + 24^2 = 25^2$
$10^2 + 24^2 = 26^2$	$20^2 + 21^2 = 29^2$	$18^2 + 24^2 = 30^2$	$16^2 + 30^2 = 34^2$
$21^2 + 28^2 = 35^2$	$12^2 + 35^2 = 37^2$	$15^2 + 36^2 = 39^2$	$24^2 + 32^2 = 40^2$

Pythagorean Triples Problem (I) [Ronald Graham, early 80's]

Will any coloring of the positive integers with red and blue result in a monochromatic Pythagorean Triple $a^2 + b^2 = c^2$?

$$
\begin{array}{cccc}
3^2 + 4^2 = 5^2 & 6^2 + 8^2 = 10^2 & 5^2 + 12^2 = 13^2 & 9^2 + 12^2 = 15^2 \\
8^2 + 15^2 = 17^2 & 12^2 + 16^2 = 20^2 & 15^2 + 20^2 = 25^2 & 7^2 + 24^2 = 25^2 \\
10^2 + 24^2 = 26^2 & 20^2 + 21^2 = 29^2 & 18^2 + 24^2 = 30^2 & 16^2 + 30^2 = 34^2 \\
21^2 + 28^2 = 35^2 & 12^2 + 35^2 = 37^2 & 15^2 + 36^2 = 39^2 & 24^2 + 32^2 = 40^2
\end{array}
$$

Best lower bound: a bi-coloring of $[1, 7664]$ s.t. there is no monochromatic Pythagorean Triple [Cooper & Overstreet 2015].

Myers conjectures that the answer is No [PhD thesis, 2015].

Pythagorean Triples Problem (II) [Ronald Graham, early 80's]

Will any coloring of the positive integers with red and blue result in a monochromatic Pythagorean Triple $a^2 + b^2 = c^2$?

A bi-coloring of $[1, n]$ is encoded using Boolean variables x_i with $i \in \{1, 2, \ldots, n\}$ such that $x_i = 1$ $(= 0)$ means that i is colored red (blue). For each Pythagorean Triple $a^2 + b^2 = c^2$, two clauses are added: $(x_a \vee x_b \vee x_c)$ and $(\overline{x}_a \vee \overline{x}_b \vee \overline{x}_c)$.

Pythagorean Triples Problem (II) [Ronald Graham, early 80's]

Will any coloring of the positive integers with red and blue result in a monochromatic Pythagorean Triple $a^2 + b^2 = c^2$?

A bi-coloring of $[1, n]$ is encoded using Boolean variables x_i with $i \in \{1, 2, \ldots, n\}$ such that $x_i = 1$ $(= 0)$ means that i is colored red (blue). For each Pythagorean Triple $a^2 + b^2 = c^2$, two clauses are added: $(x_a \vee x_b \vee x_c)$ and $(\overline{x}_a \vee \overline{x}_b \vee \overline{x}_c)$.

Theorem ([Heule, Kullmann, and Marek (2016)])

$[1, 7824]$ *can be bi-colored s.t. there is no monochromatic Pythagorean Triple. This is impossible for* $[1, 7825]$.

Pythagorean Triples Problem (II) [Ronald Graham, early 80's]

Will any coloring of the positive integers with red and blue result in a monochromatic Pythagorean Triple $a^2 + b^2 = c^2$?

A bi-coloring of $[1, n]$ is encoded using Boolean variables x_i with $i \in \{1, 2, \ldots, n\}$ such that $x_i = 1$ $(= 0)$ means that i is colored red (blue). For each Pythagorean Triple $a^2 + b^2 = c^2$, two clauses are added: $(x_a \vee x_b \vee x_c)$ and $(\overline{x}_a \vee \overline{x}_b \vee \overline{x}_c)$.

Theorem ([Heule, Kullmann, and Marek (2016)])

$[1, 7824]$ *can be bi-colored s.t. there is no monochromatic Pythagorean Triple. This is impossible for* $[1, 7825]$.

4 CPU years computation, but 2 days on cluster (800 cores)

Pythagorean Triples Problem (II) [Ronald Graham, early 80's]

Will any coloring of the positive integers with red and blue result in a monochromatic Pythagorean Triple $a^2 + b^2 = c^2$?

A bi-coloring of $[1, n]$ is encoded using Boolean variables x_i with $i \in \{1, 2, \ldots, n\}$ such that $x_i = 1$ $(= 0)$ means that i is colored red (blue). For each Pythagorean Triple $a^2 + b^2 = c^2$, two clauses are added: $(x_a \vee x_b \vee x_c)$ and $(\overline{x}_a \vee \overline{x}_b \vee \overline{x}_c)$.

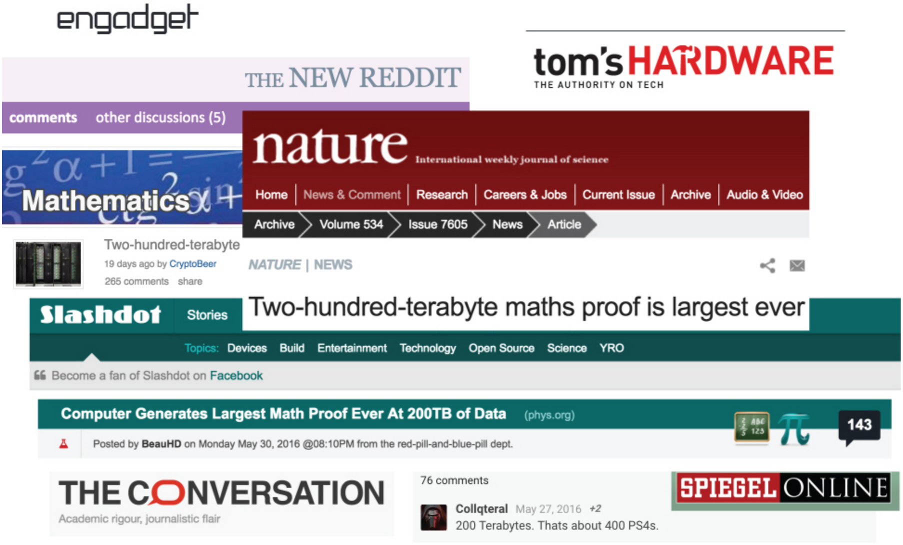
Theorem ([Heule, Kullmann, and Marek (2016)])

$[1, 7824]$ *can be bi-colored s.t. there is no monochromatic Pythagorean Triple. This is impossible for* $[1, 7825]$.

4 CPU years computation, but 2 days on cluster (800 cores)

200 terabytes proof, but validated with verified checker

Media: “The Largest Math Proof Ever”



Future of Computer-Aided Mathematics

Fields Medalist Timothy Gowers stated that mathematicians would like to use three kinds of technology [Big Proof 2017]:

- Proof Assistant Technology
  - Prove any lemma that a graduate student can work out
- Proof Search Technology
  - Automatically determine whether a conjecture holds
  - Recent improvement: Linear speedups on thousands of cores
- Proof Checking Technology
  - Mechanized validation of all details
  - Recent improvement: Formally verified checking of huge proofs

Classic problems ready for mechanization:

- Chromatic number of the plane
- The most wanted Folkman graph
- Ramsey number five