Is Your Combinatorial Search Algorithm Telling the Truth?

Ciaran McCreesh

University of Glasgow

Royal Academy of Engineering

The Algorithms I Work On

Constraint Programming

Worst-Case Complexity vs Practice

The Slight Problem…

How We Fix This

What Is A Proof?

COUNTEREXAMPLE TO EULER'S CONJECTURE ON SUMS OF LIKE POWERS

BY L. J. LANDER AND T. R. PARKIN

Communicated by J. D. Swift, June 27, 1966

A direct search on the CDC 6600 yielded

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

as the smallest instance in which four fifth powers sum to a fifth power. This is a counterexample to a conjecture by Euler [1] that at least n nth powers are required to sum to an nth power, $n > 2$.

REFERENCE

1. L. E. Dickson, *History of the theory of numbers*, Vol. 2, Chelsea, New York, 1952, p. 648.

Constraints and Satisfiability

Resolution Proofs

Model axioms From the input

Resolution

$$\frac{x_1 \vee x_2 \vee \ldots \vee x_i \vee c \qquad \overline{c} \vee y_1 \vee y_2 \vee \ldots y_j}{x_1 \vee x_2 \vee \ldots \vee x_i \vee y_1 \vee y_2 \vee \ldots \vee y_j}$$

- To prove unsatisfiability: resolve until you reach the empty clause.

Resolution Proofs

$x \vee y \vee z$	(1)
$\overline{x} \vee \overline{y} \vee \overline{z}$	(2)
$\overline{x} \vee y$	(3)
$\overline{x} \vee z$	(4)
$x \vee \overline{y}$	(5)
$x \vee \overline{z}$	(6)

1, 5 on y	$x \vee z$	(7)
6, 7 on z	x	(8)
3, 8 on x	y	(9)
4, 8 on x	z	(10)
2, 8 on x	$\overline{y} \vee \overline{z}$	(11)
9, 11 on y	$\overline{z}$	(12)
10, 12 on z	$\emptyset$	(13)

Equisatisfiability and Completeness

- Start with the constraints we're given.
- At each step in a proof, add a new constraint which obviously doesn't affect satisfiability.
- If we can derive contradiction, there were no solutions to the original problem.
- Using resolution, we can always do this for any unsatisfiable SAT problem.

Reverse Unit Propagation Proofs

- Unit propagation:
  - Look for a clause containing just one literal ℓ.
  - Delete $\overline{\ell}$ from every other clause.
  - Repeat until you can't do anything.
- Reverse unit propagation:
  - Add the negation of a constraint C, and unit propagate.
  - If contradiction is reached, derive C.
- Can rewrite to resolution in polynomial time.

Backtracking Search as RUP

- Every time you backtrack, output a RUP step for the sequence of guesses you just made.

Backtracking Search as RUP

$$x \vee y \vee z \quad (1)$$

$$\overline{x} \vee \overline{y} \vee \overline{z} \quad (2)$$

$$\overline{x} \vee y \quad (3)$$

$$\overline{x} \vee z \quad (4)$$

$$x \vee \overline{y} \quad (5)$$

$$x \vee \overline{z} \quad (6)$$

Backtracking Search as RUP

$x \vee y \vee z$	(1)	RUP x	(7)
$\overline{x} \vee \overline{y} \vee \overline{z}$	(2)		
$\overline{x} \vee y$	(3)		
$\overline{x} \vee z$	(4)		
$x \vee \overline{y}$	(5)		
$x \vee \overline{z}$	(6)		

Backtracking Search as RUP

$x \vee y \vee z$	(1)	RUP x		(7)
$\overline{x} \vee \overline{y} \vee \overline{z}$	(2)		$\overline{x}$ assumed	
$\overline{x} \vee y$	(3)		$\overline{y}$ from 5	
$\overline{x} \vee z$	(4)		$\overline{z}$ from 6	
$x \vee \overline{y}$	(5)		x from 1	
$x \vee \overline{z}$	(6)			

Backtracking Search as RUP

$x \vee y \vee z$	(1)	RUP x	(7)
$\overline{x} \vee \overline{y} \vee \overline{z}$	(2)	RUP $\overline{x}$	(8)
$\overline{x} \vee y$	(3)		
$\overline{x} \vee z$	(4)		
$x \vee \overline{y}$	(5)		
$x \vee \overline{z}$	(6)		

Backtracking Search as RUP

$x \vee y \vee z$	(1)	RUP x		(7)
$\overline{x} \vee \overline{y} \vee \overline{z}$	(2)	RUP $\overline{x}$		(8)
$\overline{x} \vee y$	(3)		x assumed	
$\overline{x} \vee z$	(4)		y from 3	
$x \vee \overline{y}$	(5)		z from 4	
$x \vee \overline{z}$	(6)		$\overline{x}$ from 2	

Backtracking Search as RUP

$x \vee y \vee z$	(1)	RUP x	(7)
$\overline{x} \vee \overline{y} \vee \overline{z}$	(2)	RUP $\overline{x}$	(8)
$\overline{x} \vee y$	(3)	RUP $\emptyset$	(9)
$\overline{x} \vee z$	(4)		
$x \vee \overline{y}$	(5)		
$x \vee \overline{z}$	(6)		

Backtracking Search as RUP

$x \vee y \vee z$	(1)	RUP x		(7)
$\overline{x} \vee \overline{y} \vee \overline{z}$	(2)	RUP $\overline{x}$		(8)
$\overline{x} \vee y$	(3)	RUP $\emptyset$		(9)
$\overline{x} \vee z$	(4)		x from 7	
$x \vee \overline{y}$	(5)		$\overline{x}$ from 8	
$x \vee \overline{z}$	(6)			

Resolution Can't Count

Cutting Planes

Bounds

Degree Reasoning

Cardinality Reasoning

Reformulation

Non-Implicational Proofs

What Reasoning Can We Justify?

Verifed Encodings

Proof Trimming

Counting and Sampling without Enumerating

Going the Other Way

Getting Involved

https://ciaranm.github.io/

ciaran.mccreesh@glasgow.ac.uk

University of Glasgow

Royal Academy of Engineering