Automated Theorem Proving and the Robbins Conjecture

Prasanna Bramhe & Shashank Pathak

23 December 2020

ISLA 2020

Outline

Caution: More history, less mathematics.

Automated Theorem Proving

Theorem Provers

We know what a formal proof is.

By theorem provers, we mean machines which in collaboration with humans, help to produce a formal proof.

These acts of theorem proving has two blurry divisions:

- Interactive Theorem Proving - User guides the machine to fill gaps in the proofs and formalize it.
- Automated Theorem Proving - Just what needs to be proven is stated, and the machine on its own tries to find a proof.

Some theorem provers: Isabelle, Lean, Coq, Mizar.

Three Early Milestones [1]

- 1954 - M.Davis programs the Presburger algorithm for additive arithmetic into the '**Johniac**' computer at the Institute for Advanced Study. Johniac proves that the sum of two even numbers is even.

- 1956 - The automation of Russell and Whitehead's *Principia Mathematica* begins [2]. By the end of 1959, Wang's procedure had generated proofs of every theorem of the *Principia* in the predicate calculus [3].

- 1968 - N.G. de Bruijn designs the first computer program to check the validity of general mathematical proofs. His program **Automath** eventually checked every proposition in a primer that Landau had written for his daughter on the construction of real numbers as Dedekind cuts.

Recent developments

Year	Theorem	Proof System	Formalizer	Traditional Proof
1986	First Incompleteness	Boyer-Moore	Shankar	Gödel
1990	Quadratic Reciprocity	Boyer-Moore	Rusinoff	Eisenstein
1996	FT of Calculus	HOL Light	Harrison	Henstock
2000	FT of Algebra	Mizar	Milewski	Brynski
2000	FT of Algebra	Coq	Geuvers et al.	Kneser
2004	Four-color	Coq	Gonthier	Robertson et al.
2004	Prime Number	Isabelle	Avigad et al.	Selberg-Erdös
2005	Jordan Curve	HOL Light	Hales	Thomassen
2005	Brouwer Fixed Point	HOL Light	Harrison	Kuhn
2006	Flyspeck I	Isabelle	Bauer-Nipkow	Hales
2007	Cauchy Residue	HOL Light	Harrison	Classical
2008	Prime Number	HOL Light	Harrison	Analytic proof

We will look at one instance where the first proof was an automated one.

The Robbins Conjecture

Boolean Algebra

Boolean algebra was given by George Boole as an algebra for logic.

Boole had the idea that one could use the notation of ordinary algebra, but re-interpret it to express the meanings of symbolic logic while retaining the calculating power of the algebra.

Boolean Algebra (Cont'd)

Standard Axioms for a Boolean Algebra

A Boolean algebra is a set B endowed with a binary operation $+$ and a unary operation $n(\cdot)$, with the following properties.

- $+$ is commutative and associative.
- There is a special element '0' such that $0 + a = a$ for all a in B.
- $n(n(a)) = a$ for all a in B.
- $n(a + n(a)) = 0$ for all a in B.
- $a + n(n(b) + n(c)) = n(n(a + b) + n(a + c))$ for all a, b, c in B.

The Huntington Equation [4]

In 1933, E.V. Huntington presented the following three axioms for Boolean algebra:

$$x + y = y + x, \qquad \text{(commutativity)}$$

$$(x + y) + z = x + (y + z), \qquad \text{(associativity)}$$

$$n(n(x) + y) + n(n(x) + n(y)) = x. \qquad \text{(Huntington equation)}$$

The Robbins Conjecture

Shortly thereafter, Herbert Robbins posed the question whether the Huntington equation can be replaced with the following equation, which has one less occurence of n :

$$n(n(x+y)+n(x+n(y))) = x. \qquad \text{(Robbins equation)}$$

It can be checked that the Robbins equation is valid in Boolean algebras.

Does the Huntington equation follow from commutativity, associativity, and the Robbins equation? Equivalently, **are all Robbin algebras Boolean?**

Some more history

Robbins and Huntington could not find a proof or a counterexample.

Alfred Tarski got interested in the problem and he gave it to many of his colleagues and students.

1979 - Steve Winker, a student visiting Argonne National Laboratory, attempted an automated deduction and was suggested to find sufficient conditions which force Robbins algebras to be Boolean.

A useful sufficient condition?

For example, any Robbins algebra with $n(n(x)) = x$ is a Boolean algebra, as

$$\begin{aligned}
& n(n(x+y)+n(x+n(y))) = x && \text{(Robbins equation)}\\
\Rightarrow\ & n(n(n(x)+y)+n(n(x)+n(y)))) = n(x) && \text{(Substituting } n(x) \text{ for } x)\\
\Rightarrow\ & n(n(n(n(x)+y)+n(n(x)+n(y))))) = n(n(x)) && \text{(Applying } n(\cdot) \text{ both sides)}\\
\Rightarrow\ & n(n(x)+y)+n(n(x)+n(y)) = x && \text{(Using } n(n(z)) = z)
\end{aligned}$$

The last equation is the Huntington equation.

Even more history

Some conditions that were shown to be sufficient by Argonne's theorem provers are

1. $\forall x(x + x = x)$,
2. $\exists c \forall x(c + x = x)$ and
3. $\exists c \forall x(c + x = c)$.

Winker proved (by hand) several weaker conditions sufficient.

Lemma

(S. Winker [5, 6]) A robbins algebra satisfying $\exists c \exists d(c + d = c)$ is a Boolean algebra.

The proof

Lemma

All Robbins algebras satisfy $\exists c \exists d (c + d = c)$.

The following proof was found by W. McCune's **EQP**. It took 8 days and 30 megabytes of memory for EQP to find this proof [4]. It was verified by another prover called **OTTER**.

7	$n(n(n(x)+y)+n(x+y)) = y$	[Robbins equation*]
10	$n(n(n(x+y)+n(x)+y)+y) = n(x+y)$	[$7 \to 7$]
11	$n(n(n(n(x)+y)+x+y)+y) = n(n(x)+y)$	[$7 \to 7$]
29	$n(n(n(n(x)+y)+x+2y)+n(n(x)+y)) = y$	[$11 \to 7$]
54	$n(n(n(n(n(x)+y)+x+2y)+n(n(x)+y)+z)+n(y+z)) = z$	[$29 \to 7$]
217	$n(n(n(n(n(x)+y)+x+2y)+n(n(x)+y)+$ $n(y+z)+z)+z) = n(y+z)$	[$54 \to 7$]
674	$n(n(n(n(n(n(x)+y)+x+2y)+n(n(x)+y)+$ $n(y+z)+z)+z+u)+n(n(y+z)+u)) = u$	[$217 \to 7$]
6736	$n(n(n(n(3x)+x)+n(3x))+n(n(n(3x)+x)+5x)) = n(n(3x)+x)$	[$10 \to 674$]
8855	$n(n(n(3x)+x)+5x) = n(3x)$	[$6736 \to 7$,simp:54,flip]
8865	$n(n(n(n(3x)+x)+n(3x)+2x)+n(3x)) = n(n(3x)+x)+2x$	[$8855 \to 7$]
8866	$n(n(n(3x)+x)+n(3x)) = x$	[$8855 \to 7$,simp:11]
8870	$n(n(n(n(3x)+x)+n(3x)+y)+n(x+y)) = y$	[$8866 \to 7$]
8871	$n(n(3x)+x)+2x = 2x$	[8865,simp:8870,flip]

Equation 8871 asserts the existence of an object c, namely $2x$, and an object d, namely $n(n(3x)+x)$, such that $c + d = c$. □

The methods used in the proof, the search algorithm and a more detailed version of the same proof can be found in [4].

References

[1] http://www.ams.org/notices/200811/tx081101370p.pdf

[2] A. Newell, J. C. Shaw and H. A. Simon, 1956, Empirical explorations of the Logic Theory Machine: A case study in heuristics, Proc. Western Joint Computer Conf., 15, pp. 218–239.

[3] H. Wang, Computer Theorem Proving and Artificial Intelligence, in W. W. Bledsoe and D. W. Loveland (eds.), Automated Theorem Proving: After 25 Years, Contemporary Mathematics, Vol. 29, AMS, Providence, RI, 1984, 49-70.

[4] William McCune, Solutins of the Robbins Problem, Journal of Automated Reasoning 19:263-276, 1997.

[5] Winker, S.: Robbins algebra: Conditions that make a near-Boolean algebra Boolean, J. Automated Reasoning 6(4) (1990), 465–489.

[6] Winker, S.: Absorption and idempotency criteria for a problem in near-Boolean algebras, J. Algebra 153(2) (1992), 414–423.

Thank you!