Conjectures, Proofs and Consensus

Chad E. Brown

Czech Technical University in Prague

June 2020

Introduction

- Conjecture: Is φ a theorem?
- Positive answer: Proof of φ.
- Negative answer? If lucky, proof of $\neg\varphi$.
  - In complete theories, we're always lucky.
  - If "almost" complete, then "almost" always lucky.
- Where do conjectures come from?
- Where do proofs come from?

An "Almost" Complete Theory: HOHF

- Start with simply typed lambda calculus with a base type o of propositions and another base type ι.
- Add axioms so that o is 2 valued (true and false).
- Add axioms so that ι contains the hereditarily finite sets (and only those sets, assuming standard semantics).
- Conjectures are closed propositions (sentences).

A Simple HOHF Conjecture

- Simple "Conjecture":
  $\forall p : \iota \to o. \forall AB : \iota. pA \to p(A \cup B)$
- Negation of this formula:

$$(\forall p : \iota \to o. \forall AB : \iota. pA \to p(A \cup B)) \to \bot$$

- Idea: Assume the conjecture, then:
  - Choose p to be $\lambda x : \iota. x = \emptyset$.
  - Choose A to be $\emptyset$.
  - Choose B to be $\{\emptyset\}$.
  - Prove a contradiction by proving pA and $\neg(p(A \cup B))$.

Expressiveness of HOHF

- There are many families containing "hard" conjectures.
- Diophantine: Can $X \uplus Y \uplus 1$ and $2 \times X \times X \times Y$ have the same cardinality?
- AIM Related: If Q is a (finite) set and $\cdot, \backslash, /$ are loop operators with identity e, then does equation E follow from equations $E_1, \ldots, E_n$.
- Higher-order unification: Is there a function $F : (\iota \to \iota) \to \iota \to \iota$ such that $\forall xy.Fxy = x(xy)$?
- QBF: $\forall p : o.\exists q : o.p \leftrightarrow q$.

Pseudorandom Conjectures

- Diophantine: Generate two polynomials p and q, each with monomials of the form $X^k Y^m Z^n$ with $k, m, n \in \{0, 1, 2, 3\}$. Then form conjectures like "there are no X, Y, Z such that p and q have the same cardinality."
- AIM Related: Randomly construct inner mappings by composing some basic inner mappings, and add assumptions that pairs of these inner mappings commute (AIM) and possibly that some inner mappings have a small order (not AIM). Under these conditions, conjecture an equation equivalent to part of the AIM conjecture.
- QBF: A prefix of at least 50 quantifiers followed by $lhs \leftrightarrow rhs$ where both sides use all quantified variables.

Theorem Proving as Proof-of-Work?

- PoW: Proof-of-work (e.g., Bitcoin, Litecoin, etc.):
  - Every 10 minutes or so someone (a "miner") solves a puzzle and creates a block.
  - The miner is rewarded with X bitcoins in the block.
  - The block records data about who owns what.
  - Difficulty of puzzles adjust smoothly with mining power.
- Theorem proving as proof-of-work?
  - Where would the conjectures come from?
  - How could they be ensured to be not-too-easy and not-too-hard?
  - How could difficulty smoothly adjust?

Other Consensus Methods

- PoS: Proof-of-stake (e.g., Peercoin):
  - For each block, someone who owns a certain amount of the cryptocurrency is "randomly" chosen to create a new block.
- Proof-of-burn (e.g., Slimcoin):
  - Burning one kind of coin allows users to create new blocks for another coin.
  - The burning is a proxy for PoW.

Integrating Theorem Proving into Consensus

- Proofgold (proofgold.org) combines proof-of-burn, proof-of-stake and theorem proving as proof-of-work.
- Burning litecoins, possibly combined with staking proofgold bars, allows users to create new Proofgold blocks.
- Each new Proofgold block creates 50 new bars.
  - 25 new bars go to the block creator (burner/staker).
  - 25 new bars go to a bounty on a conjecture.
  - The conjecture (in HOHF) is determined by Litecoin information.
  - Litecoin is being used to secure the Proofgold chain and as a pseudorandom number generator for conjectures.

Integrating Theorem Proving into Consensus

- Proving bounty conjectures (or their negations) gives users more stake to participate in creating blocks.
- In addition to pseudorandom conjectures, users can publish their own conjectures (in HOHF or another theory) and place bounties on them.
- *Proofgold rewards the best theorem provers.*
- Where do proofs come from?
  - Megalodon (Interactive Prover for Set Theory)
  - Use ATPs for suggestions
  - (Partial?) Ivy to Proofgold Translator
  - To do: Translators from other ATPs and ITPs.