The Combinatorics of Propositional Provability

Jeremy Avigad

Department of Philosophy

Carnegie Mellon University

avigad@cmu.edu

with thanks to DIMACS

(Center for Discrete Mathematics and

Theoretical Computer Science)

A Modern Look at Propositional Provability

Traditional Logic: Given a first-order theory T find statements φ such that

$$T \not\vdash \varphi.$$

Proof Complexity: Given a propositional proof system P find a sequence of tautologies φ_n such that

$$P \not\vdash_{p(|\varphi_n|)} \varphi_n$$

for any polynomial p.

Motivation: if $NP \neq co{-}NP$, then no proof system has polynomial-size proofs of every tautology.

Frege Systems

Definition: A *Frege system* is an implicationally complete propositional proof system, axiomatized by finitely many schemata.

For example, in the *Principia Mathematica*, one finds

1. $\neg(p \vee p) \vee p$
2. $\neg[p \vee (q \vee r)] \vee q \vee (p \vee r)$
3. $\neg q \vee p \vee q$
4. $\neg(\neg q \vee r) \vee \neg(p \vee q) \vee p \vee r$
5. $\neg(p \vee q) \vee q \vee p$

combined with the single rule of modus ponens: from $\neg p \vee q$ and p conclude q.

Fact: Any two Frege systems p-simulate each other.

Proving Lower Bounds

Goal: Given a proof system P, show that P does not have polynomial-size proofs of every tautology.

A natural approach:

1. Define an explicit sequence of tautologies φ_n
2. Show that P can't prove these tautologies efficiently.

Example (Ajtai, et al.): if P is a fixed-depth Frege-system, and φ_n is a propositional form of the pigeonhole principle, then the shortest proofs of φ_n in P are $O(2^{cn})$.

Adding an Extension Rule

Definition: An **extended Frege system** allows one to introduce new propositional constants, with axioms

$$C_\varphi \equiv \varphi.$$

Conjecture: Extended Frege systems are exponentially more efficient than Frege systems.

Problem: Find tautologies expressing a natural combinatorial principle that (1) have short extended Frege proofs, but (2) don't seem to have short Frege proofs.

Bonet, Buss, and Pitassi (1995) consider a wide range of combinatorial theorems that have polynomial extended-Frege proofs, and conclude that in most cases there seem to be Frege proofs whose lengths are at most quasipolynomial.

Plausibly Hard Tautologies

Definition: The tautologies $Con_{EF}(n)$ express the assertion "the variables x_1 to x_n do not code a proof of a contradiction in a (fixed) extended Frege system."

Theorem (Cook): Any extended Frege-system has polynomial-size proofs of the assertions $Con_{EF}(n)$.

Theorem (Buss): Let F be any Frege-system. Then

$$F + \{Con_{EF}(n)\}_{n \in \omega}$$

polynomially simulates any extended Frege system.

As a result, if there is any separation between Frege systems and extended Frege systems, it is witnessed by the tautologies $Con_{EF}(n)$.

"... But, this is not what we mean by a natural combinatorial assertion."

An Analogy

Theorem (Gödel): Peano Arithmetic doesn't prove Con_{PA}.

Paris and Harrington construct a natural combinatorial statement PH.

Theorem (Paris and Harrington): Peano Arithmetic doesn't prove PH.

Proof: PH implies Con_{PA}.

Idea: Find a more "combinatorial" version of $Con_{EF}(n)$.

A Multi-ary connective

Let $NAND(\varphi_1, \ldots, \varphi_k)$ denote the assertion that at least one of the φ_i is false.

$NAND()$ can be interpreted as falsehood, and $NAND(\varphi)$ is equivalent to $\neg\varphi$.

Build formulas from variables x_i and $NAND$'s.

Formulas of the following form are always true:

$$NAND(\varphi_1, \ldots, \varphi_k, \psi_1, \ldots, \psi_l, NAND(\psi_1, \ldots, \psi_l)).$$

The following rule is sound: from

$$NAND(\psi_1, \ldots, \psi_k, \varphi_1, \ldots, \varphi_l)$$

and

$$NAND(\psi_1, \ldots, \psi_k, NAND(\varphi_1, \ldots, \varphi_l))$$

conclude

$$NAND(\psi_1, \ldots, \psi_k).$$

A Surprising Fact

Theorem: The axiom and rule taken together are complete, and p-simulate any Frege system.

Proof: Derive some additional rules; then show that from a given a tautology one can "work backwards" to axioms.

The Hereditarily Finite Sets

Definition: The hereditarily finite sets are defined inductively as follows:

- $\emptyset$ is a hereditarily finite set.
- If $a_1, a_2, \ldots, a_n$ are hereditarily finite sets, so is
$$\{a_1, a_2, \ldots, a_k\}.$$

By making the association

$$NAND(\varphi_1, \ldots, \varphi_k) \rightsquigarrow \{\varphi_1, \ldots, \varphi_k\}$$

we can identify closed formulas with hereditarily finite sets.

Definition: Call a hereditarily finite set a *good* if there is some $b \subset a$ such that $b \in a$.

For example,

$$\{a, b, c, d, \{a, b\}\}$$

is good.

A Somewhat Combinatorial Theorem

Theorem. Let C be a hereditarily finite set, such that for every a in C, either

1. a is good, or

2. for some hereditarily finite b not contained in a, $a \cup b$ and $a \cup \{b\}$ are both in C.

Then the empty set is not in C.

Proof. From a counterexample we could find a proof of a contradiction in the simple Frege-system.

Formulas and Directed Acyclic Graphs

Idea. Code formulas based on $NAND$ as nodes in a directed acyclic graph. Identify nodes v with the $NAND$ of the neighborhood of v.

Note. By explicitly "naming" every formula in sight, we can think of an extended Frege system as reasoning about such nodes.

A Somewhat Combinatorial Theorem About DAGS

Theorem. Let G be a directed acyclic graph, and suppose C is a subset of the vertices of G such that for every a in C, one of the following two conditions holds:

1. Either there is a vertex b in $N(a)$ such that $N(b) \subseteq N(a)$, or
2. there are vertices d and e in C, and a nonterminal vertex b of G, such that
   (a) $N(d) = N(a) \cup \{b\}$,
   (b) $N(e) = N(a) \cup N(b)$, and
   (c) $N(e) \neq N(a)$.

Then every element of C is nonterminal.

Proof. Once again, a counterexample would correspond to a Frege-proof of a contradiction.

Thanks to the correspondence between DAGs and formulas, this more or less expresses the consistency of an extended Frege-system.

Extracting a Propositional Tautlogy

Variables p_{ij}, where $i < j \leq n$, express the assertion that there is an edge from i to j. Variables q_i asssert that $i \in C$.

The hypothesis is of the form:

$$\bigwedge_i (q_i \to \varphi_1(i) \vee \varphi_2(i))$$

where $\varphi_1(i)$ is the assertion

$$\bigvee_j \left(p_{ij} \wedge \bigwedge_k (p_{jk} \to p_{ik}) \right)$$

and $\varphi_2(i)$ is the assertion

$$\bigvee_{j,k,l} \left(q_k \wedge q_l \wedge p_{kj} \wedge \bigwedge_{m \neq j} (p_{km} \leftrightarrow p_{im}) \wedge \bigwedge_m (p_{lm} \leftrightarrow (p_{im} \vee p_{jm})) \right).$$

The conclusion is of the form:

$$\bigwedge_i (q_i \to \bigvee_j p_{ij}).$$

Call the resulting tautology $T(n)$.

The Net Result

Theorem. EF has polynomial-size proofs of the tautologies $T(n)$.

Proof. Similar to the proof that EF has polynomial-size proofs of the tautologies $Con_{EF}(n)$.

Theorem. $F + \{T(n)\}$ p-simulates any extended Frege-system.

Proof. Similar to the proof that $F + \{Con_{EF}(n)\}$ p-simulates any extended Frege-system.

A Historical Note

In 1913, Sheffer showed that the binary $NAND$ is a complete connective.

In 1917, Jean Nicod presented a Frege-system based on the Sheffer stroke, with the single axiom

$$\{[p \mid (q \mid r)] \mid [t \mid (t \mid t)]\} \mid \{[s \mid q] \mid [(p \mid s) \mid (p \mid s)]\}$$

and rule

$$\frac{p \mid (r \mid q) \quad p}{q}.$$

In 1925, in the introduction to the second edition of the *Principia Mathematica*, Russell calls Sheffer's reduction "the most definite improvement resulting from work in mathematical logic during the past fourteen years."

Can This Be Put To Good Use?

Notice that now we know exactly what Frege proofs look like:

Can this fact be used to prove lower bounds?