How to Associate Propositional Proof Systems and Theories with Complexity Classes

Part III:

Translating Combinatorial Theorems to Propositional Proofs

Stephen Cook

LC2002 Tutorial
August, 2002

Introduction to Propositional Proof Complexity

A *proof system* is a polynomial time map

$$f : \{0,1\}^* \stackrel{\text{onto}}{\longrightarrow} \{\text{tautologies}\}$$

If $f(x) = A$, then x is a *proof* of A.

Def'n: The system is *super* iff for some polynomial $p(n)$, every tautology of length n has a proof of length at most $p(n)$.

Simple Fact: **NP** $=$ **co-NP** iff there exists a super proof system.

Proof: {tautologies} is complete for **co-NP**.
Clearly {tautologies} $\in$ **NP** iff there exists a super proof system. $\square$

Conjecture: **NP** $\neq$ **co-NP**
(i.e. there is no super proof system).

Complexity theorists believe this, but should they??? (Later)
Activity: Try to prove specific proof systems are not super.

Frege Systems (Hilbert Style Systems)

Finitely many axiom schemes and rule schemes. Must be implicationally complete.

Example for connectives $\vee, \neg$ (Shoenfield)

Axiom scheme: $\neg A \vee A$

Rules:

$$\frac{A}{B \vee A} \qquad\qquad \frac{A \vee A}{A}$$

$$\frac{(A \vee B) \vee C}{A \vee (B \vee C)} \qquad\qquad \frac{A \vee B \quad \neg A \vee C}{B \vee C}$$

All Frege systems p-simulate each other.

Definition: Proof system f *p-simulates* proof system g if $\exists$ polytime T such that

$$f(T(x)) = g(x)$$

Gentzen's propositional LK is p-equivalent to every Frege system.

Major Open Question: Are Frege systems super?

Recall $\mathbf{AC^0}$ from Part I

$\mathbf{AC^0}$: uniform bounded depth $\wedge, \vee$ polysize circuit family.

FO Characterization Theorem: [BIS, I]

$$\mathrm{FO} = \mathbf{AC^0} = \mathbf{LH}$$

LH: Log time hierarchy for alternating Turing machines.

Example PAL = set of binary palindromes. $PAL = L(A)$, where A is

$$\forall x \forall y (x + y = max \supset (X(x) \leftrightarrow X(y))$$

Theorem: [Ajtai,FSS 83] $PARITY \notin \mathbf{AC^0}$

($PARITY$ = set of strings with an odd number of 1's.)

Definition: An $\mathbf{AC^0}$-Frege proof is a Frege proof in which all formulas are restricted to some fixed maximum depth d.

Theorem (Ajtai): $\mathbf{AC^0}$-Frege systems are not super.

Proof: We need a family of tautologies with no short $\mathbf{AC^0}$-Frege proofs.

Pigeonhole Principle: If $n+1$ pigeons are placed in n holes, some hole has at least 2 pigeons.

Atoms p_{ij} (pigeon i placed in hole j)
$1 \leq i \leq n+1, \ 1 \leq j \leq n$

$\neg\mathrm{PHP}_n^{n+1}$ is the conjunction of clauses:

$(p_{i1} \vee \ldots \vee p_{in})$ (pigeon i placed in some hole)
$1 \leq i \leq n+1$

$(\neg p_{ik} \vee \neg p_{jk})$ (pigeons i, j not both in hole k)
$1 \leq i < j \leq n+1, \ 1 \leq k \leq n$

$\neg$PHP$_n^{n+1}$ is unsatisfiable: $O(n^3)$ clauses

PHP$_n^{n+1}$ tautology: DNF of negation of $\neg$PHP$_n^{n+1}$

Major Theorem (Ajtai; PBIKPW): The Pigeonhole tautologies $\{PHP_n^{n+1}\}$ require exponential size $\mathbf{AC^0}$-Frege proofs.

(Intuitively, proving the PHP requires counting. $PARITY$ and counting are not in $\mathbf{AC^0}$.)

This theorem is near the limit of our knowledge.

Example: $\mathbf{AC^0}(2)$-Frege proofs allow unbounded fan-in parity connectives $\oplus(p_1, ..., p_n)$.

Open Question: Is $\mathbf{AC^0}(2)$-Frege super??

Propositional translations of formulas of $\mathbf{V}^0$ and $\mathbf{V}^1$

Recall $x, y, z, ...$ range over $\mathbb{N}$
$X, Y, Z, ...$ range over finite subsets of $\mathbb{N}$

A is $\mathbf{\Sigma_0^B}$ if all number variables are bound, no string quantifiers.

Given a $\mathbf{\Sigma_0^B}$ Formula $A(X)$ and given $n \in \mathbb{N}$ associate a propositional formula $A(X)[n]$.
(Assume no free variables besides X in $A(X)$.)

Atoms of $A(X)[n]$ are $p_0^X, p_1^X, ..., p_{n-1}^X$ (bits of X when $|X| = n+1$)

The strings X of length n satisfying $A(X)$ in the standard model represent precisely the truth assignments satisfying $A(X)[n]$.

Ideal due to Paris and Wilkie, 1985, for $\mathbf{I\Delta_0}[R]$

If X does not occur in $A(X)$, then $A(X)[n]$ is simply the constant 1 (TRUE) if $A(X)$ is true in $\mathbb{N}$, and 0 (FALSE) otherwise.

When X occurs in $A(X)$, define $A(X)[n]$ by induction on the logical depth of $A(X)$.

Base Case: $A(X)$ is atomic. If

$$A(X) \equiv \quad t(|X|) = u(|X|)$$

then $A(X)[n]$ is 1 if $val(t(n{+}1)) = val(u(n{+}1))$ and 0 otherwise.

Similarly for $t(|X|) \leq u(|X|)$.

When $A(X) \equiv X(t(|X|)$, then setting $i = val(t(n+1))$

$$A(X)[n] \equiv \begin{cases} p_i & \text{if } i < n \\ 1 & \text{if } i = n \\ 0 & \text{if } i > n \end{cases}$$

Induction Step:

$\{\neg B(X)\}[n] \equiv \neg\{B(X)[n]\}$

$(B(X) \wedge C(X))[n] \equiv (B(X)[n] \wedge C(X)[n])$

$(B(X) \vee C(X))[n] \equiv (B(X)[n] \vee C(X)[n])$

$\{\exists z \leq t(|X|)B(z, X)\}[n] \equiv \bigvee_{i=0}^{m} B(i, X)[n]$
where $m = val(t(n+1))$

$\{\forall z \leq t(|X|)B(z, X)\}[n] \equiv \bigwedge_{i=0}^{m} B(i, X)[n]$
where $m = val(t(n+1))$

Note that for given $A(X)$,
$A(X)[n]$ has size $n^{O(1)}$.

Thus $\{A(X)[n] : n \in \mathbb{N}\}$ is a bounded depth polynomial size family of propositional formulas.

Example: Pigeon Hole Principle

Recall p_{ij} means pigeon $i \longrightarrow$ hole j

Represent the array $\{p_{ij}\}$ by a string X of length $n(n+1)$, where X is the concatenation of the rows of the array.

$A_{\neg PHP}(X)$ asserts X codes one-one map $n+1 \to n$.

$A_{\neg PHP}(X) \equiv$

$$\exists z \leq |X| \left(\begin{array}{l} |X| = z(z+1) \wedge \forall i \leq z \exists j < z X(iz+j) \wedge \\ \forall i \leq z \forall j \leq z \forall k < z (i < j \supset \\ (\neg X(iz+k) \vee \neg X(jz+k)) \end{array} \right)$$

Claim: The propositional formula $\neg\mathrm{PHP}_n^{n+1}$ is essentially isomorphic to $A_{\neg PHP}(X)[n(n+1)]$, where the atom p_{ij} gets renamed $p^X_{(i-1)n+j-1}$.

$\mathbf{V}^0$ Translation Theorem:
Let $A(X)$ be a $\mathbf{\Sigma_0^B}$ formula such that

$$\mathbf{V^0} \vdash A(X)$$

Then the family $\{A(X)[n]\}$ has polynomial size $\mathbf{AC^0}$-Frege proofs.

Corollary: The true $\mathbf{\Sigma_0^B}$ formula $\neg A_{\neg PHP}(X)$ is not a theorem of $\mathbf{V^0}$.

Proof: By Ajtai, the family PHP_n^{n+1} does not have polynomial size $\mathbf{AC^0}$-Frege proofs.

Surprise: The problem, given the map X, of finding two pigeons mapped to the same hole, can be solved by a $\mathbf{AC^0}$ function. But correctness of the algorithm cannot be proved with $\mathbf{AC^0}$ concepts (need to count?)

Note: $\mathbf{V^1} \vdash A_{PHP}(X)$

Proof of $\mathbf{V}^0$ Translation Theorem

Generalize the transformation from

$$A(X) \longrightarrow \{A(X)[n] : n \in \mathbb{N}\} \text{ to}$$

$$A(X_1, ..., X_k) \longrightarrow \{A(X_1, ..., X_k)[n_1, ..., n_k] : n_i \in \mathbb{N}\}$$

Here $n_i + 1 = |X_i|$, $i = 1, ..., k$.

Note: If $X_i = \emptyset$ then $|X_i| = 0$ so $n_i = -1$.

If $A(\vec{x}, \vec{Y})$ has free number variables $\vec{x}$, use the transformation

$$A(\vec{x}, \vec{Y}) \longrightarrow \{A(\vec{r}, \vec{Y})[\vec{n}] : r_i, n_j \in \mathbb{N}\}$$

Notice that for each $\mathbf{\Sigma_0^B}$ formula $A(\vec{x}, \vec{Y})$, the corresponding family of propositional formulas has bounded depth, and size bounded by a polynomial in $\max\{\vec{r}, \vec{n}\}$.

Recall axioms for $\mathbf{V^0}$:

Number axioms: Like Robinson's system Q

Length axioms:
L1: $X(y) \supset y < |X|$
L2: $y + 1 = |X| \supset X(y)$

$\mathbf{\Sigma_0^B}$-Comprehension
$\exists X \leq y \forall z < y [X(z) \leftrightarrow A(z, \vec{w}, \vec{Y})]$ where $A(z)$ is a $\mathbf{\Sigma_0^B}$ formula not containing X.

Let $\tilde{\mathrm{V}}^{\mathbf{0}}$ be $\mathbf{V^0}$ except replace $\mathbf{\Sigma_0^B}$ comprehension with $\mathbf{\Sigma_0^B}$ induction scheme.

Lemma: $\tilde{\mathrm{V}}^{\mathbf{0}}$ has the same $\mathbf{\Sigma_0^B}$ theorems as $\mathbf{V^0}$.

Proof: We know $\mathbf{V^0}$ proves $\mathbf{\Sigma_0^B}$-induction. Conversely, A model for $\tilde{\mathrm{V}}^{\mathbf{0}}$ can be extended to satisfy $\mathbf{\Sigma_0^B}$ comprehension by adding the $\mathbf{\Sigma_0^B}$ definable sets.

Sequent system for $\tilde{\mathrm{V}}^{\mathbf{0}}$: No comprehension or induction axioms.
Incorporates the $\mathbf{\Sigma_0^B}$ IND rule. All axioms for $\tilde{\mathrm{V}}^{\mathbf{0}}$ are quantifier-free (or $\mathbf{\Sigma_0^B}$)

Suppose $\tilde{\mathrm{V}}^{\mathbf{0}} \vdash A(X)$, where $A(X)$ is $\mathbf{\Sigma_0^B}$. Let π be an anchored proof of $\longrightarrow A(X)$. All formulas in π are $\mathbf{\Sigma_0^B}$. Typical sequent

$$D_1(\vec{x},\vec{Y}),...,D_p(\vec{x},\vec{Y}) \longrightarrow E_1(\vec{x},\vec{Y}),...,E_q(\vec{x},\vec{Y})$$

Claim: $\exists d, \ell$ s.t. every translation of this into a propositional sequent

$$D_1(\vec{r},\vec{Y})[\vec{n}],...,D_p(\vec{r},\vec{Y})[\vec{n}] \longrightarrow$$
$$E_1(\vec{r},\vec{Y})[\vec{n}],...,E_q(\vec{r},\vec{Y})[\vec{n}]$$

has an **LK** proof of size $\leq (\max(\vec{r},\vec{n})+2)^{\ell}$ in which every formula has depth at most d.
(Hence $\mathbf{AC^0}$-Frege proof)

Proof of Claim: Induction on position of sequent in π.

Base Case: Trivial (All axioms translate to 1 (TRUE).)

Ind Step: One case for each sequent rule for $\tilde{\mathbf{V}}^{\mathbf{0}}$.

- The propositional rules are all easy: we can apply the same rules to get the propositional **LK** proof.
- The induction rule is handled by unwinding the induction and applying a sequence of cuts.
- The string quantifier rules are never applied, because there are no string quantifiers in π.
- We illustrate the case of the number quantifier rules by $\forall$ **right**.

$\forall$ **right:**

$$\frac{... \to b \le t(\vec{a}, |\vec{Y}|) \supset E(b, \vec{a}, \vec{Y}), ...}{... \to \forall z \le t(\vec{a}, |\vec{Y}|)E(z, \vec{a}, \vec{Y}), ...}$$

where b does not occur in the bottom sequent. By the induction hypothesis there are bounded depth polynomial size **LK** proofs of the propositional sequents

$$... \to i \le t(\vec{r}, \vec{n}) \supset E(i, \vec{r}, \vec{Y})[\vec{n}], ...$$

For fixed $\vec{r}, \vec{n}$ we combine these proofs for $i = 0, 1, ..., m = val(t(\vec{r}, \vec{n}))$ to obtain an **LK** proof of

$$... \to \bigwedge_{i=0}^{m} E(i, \vec{r}, \vec{Y})[\vec{n}], ...$$

($\wedge$-introduction, right)

$\Box$ ($\mathbf{V^0}$ Translation Theorem)

Extended Frege Systems (EFrege systems)

Allow definitions

$$p \leftrightarrow A$$

any atom p and formula A, provided p does not occur in A, or earlier in the proof, or in the conclusion.

p may occur in a later formula A'.
This allows *lines* in a Frege proof to be massively abbreviated.

$p_1 \leftrightarrow A_1,\ p_2 \leftrightarrow A_2(p_1), ..., p_n \leftrightarrow A_n(p_1, ..., p_{n-1})$
Lines in an Extended Frege proof are like Boolean circuits. (The new atoms are like gates in the circuit.)

The number of *lines* in a Frege proof is p-equivalent to the total length of an EFrege proof.

EFrege systems might be called "**P**-Frege systems"

OPEN QUESTION: Do Frege systems p-simulate EFrege systems? (vs $\mathbf{NC}^1 = P/poly$)?

Quantified Propositional Calculus [KP,BK]

A Σ_1^q formula has the form

$$\exists x_1 ... \exists x_n A(\vec{x}, \vec{p})$$

where $A(\vec{x}, \vec{p})$ is a propositional formula.

The problem of witnessing quantifiers given a Σ_1^q formula is **NP**-complete.

Definition [KP]: System G_1 is Gentzen style where lines are sequents

$$A_1, ..., A_k \rightarrow B_1, ..., B_m$$

where the A's and B's are Σ_1^q or quantifier-free.

G_1^* (treelike G_1) is p-equivalent to EFrege.

G_1 is associated with the complexity class **PLS** (Polynomial Local Search) [JPY].

Theorem: (a) The problem: Given a G_1^* proof P of a Σ_1^q formula $\exists\vec{x}A(\vec{x}, \vec{p})$ and values for $\vec{p}$, find a witness for $\vec{x}$, is complete for polytime. (b) The same problem when P is a G_1 proof is complete for **PLS**.

Quantified Propositional Translations of $\mathbf{\Sigma_1^B}$ formulas

Translate

$$A(\vec{x}, \vec{Y}) \equiv \quad \exists Z \leq t(\vec{x}, |\vec{Y}|)\ B(\vec{x}, \vec{Y}, Z)$$

(where B is $\mathbf{\Sigma_0^B}$) to the $\mathbf{\Sigma}_1^q$ formula

$$A(\vec{x}, \vec{Y})[\vec{r}, \vec{n}] \equiv \ \exists p_0^Z ... \exists p_{m-2}^Z \bigvee_{k=-1}^{m-1} B(\vec{r}, \vec{Y}, Z)[\vec{n}, k]$$

where $m = val(t(\vec{r}, \vec{n} + 1))$.

$\mathbf{V}^1 - \mathbf{G}_1^*$ Translation Theorem;
Let A(X) be a strict $\mathbf{\Sigma_1^B}$ formula such that

$$\mathbf{V}^1 \vdash A(X)$$

Then the family $\{A(X)[n]\}$ has polynomial size $\mathbf{G}_1^*$ proofs.

Proof: Similar to $\mathbf{V}^0$ case, and $\mathbf{V}^1$ witnessing.

Corollary: If $A(X)$ above is $\mathbf{\Sigma_0^B}$, then $\{A(X)[n]\}$ has polysize EFrege proofs.

Which combinatorial principles might translate to tautology families with no polysize EF proofs?

Godel: NOT $\mathbf{V}^1 \vdash consis_{\mathbf{V}^1}(X)$

Conjecture: $\{consis_{\mathbf{V}^1}(X)[n]\}$ do not have polysize EF proofs.

(Can substitute **ZF** for $\mathbf{V}^1$)

Fact [C75]: $\mathbf{V}^1$ proves soundness of EF, so $\{\text{soundness}_{EF}[n]\}$ has polysize EF proofs.

Fact [Buss91] $\{\text{soundness}_{Frege}[n]\}$ has polysize Frege proofs, and Frege P-simulates EF iff $\{\text{soundness}_{EF}[n]\}$ has polysize Frege proofs.

Also, linear algebra may distinguish Frege and EF:

$AB = I \Longleftrightarrow BA = I$, where A, B matrices over GF(2).

(Determinants are polytime computable, but maybe not in $\mathbf{NC}^1$).

Examples of Triples $\langle C, S, T \rangle$

Class	**Proof System**	**Theory**
AC^0	AC^0-Frege	$I\Delta_0(R), \mathbf{V^0}, TAC^0$
$AC^0[2]$	$AC^0[2]$-Frege	$TAC^0(2)$
TC^0	TC^0-Frege	TTC^0
NC^1	Frege	AID, T_1, TNC^1
L	L-Frege	Σ_0^p-rec, TLS
DET		$\forall LAP$
NC	NC-Frege	U_1^1, R_2^1, TNC
P	EFrege	$QPV, S_2^1, \mathbf{V}^1$
PLS	G_1	T_2^1
PSPACE	G, BoolPr	U_2^1, PSA

Each class has a uniform and a nonuniform version.

Conclusion

Separating the $\forall\Sigma_0^B$ fragments of the logical theories is as interesting (and maybe easier) than separating the corresponding proof systems.

This is like separating the uniform versions of the complexity classes (e.g. P $\neq$ NP), as opposed to separating the non-uniform classes (e.g. circuit size lower bounds).

If theory T corresponds to proof system S, then T proves "S is sound", but this is probably not provable by the weaker theories. PROBLEM: Find natural equivalent combinatorial statements.

Example: Avigad's combinatorial DAG principle separates the $\forall\Sigma_0^b$ fragments of S_2^1 and AID, if anything does.

Final Thought: Proving propositional proof lower bounds is difficult.

Maybe Frege systems are super???