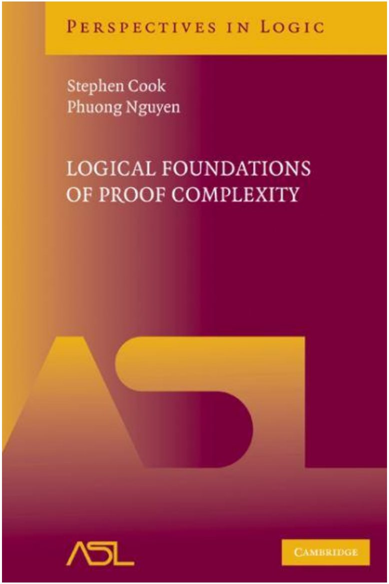
Connecting Complexity Classes, Weak Formal Theories, and Propositional Proof Systems

Stephen Cook

Department of Computer Science
University of Toronto
Canada

CSL 2012

Reference


PERSPECTIVES IN LOGIC
Stephen Cook
Phuong Nguyen
LOGICAL FOUNDATIONS
OF PROOF COMPLEXITY
CAMBRIDGE

Propositional Proof Systems

- A proof system is a polytime map

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

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

- The system is polybounded 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 polybounded proof system.

Conjecture

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

- **Activity:** Try to prove specific proof systems are not super.

Frege Systems for Propositional Calculus (Hilbert Style systems)

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

Example for connectives $\vee, \neg$

- **Axiom scheme:** $\neg A \vee A$
- **Rules:** $\dfrac{A}{B \vee A}$ $\quad \dfrac{A \vee A}{A}$ $\quad \dfrac{(A \vee B) \vee C}{A \vee (B \vee C)}$ $\quad \dfrac{A \vee B \qquad \neg A \vee C}{B \vee C}$

- 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.

Are Frege systems polybounded?

To disprove this, we need a family of hard tautologies.

Possible example:

Pigeonhole Principle:

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

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

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

1. $(p_{i1} \vee \ldots \vee p_{in}), i \in [n+1]$ (pigeon i placed in some hole)
2. $(\neg p_{ik} \vee \neg p_{jk}), i < j \in [n+1], k \in [n]$ (pigeons i, j not both in hole k)

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

Conjecture (C. 1979)

The tautologies $\{\mathrm{PHP}_n^{n+1}\}$ do not have polysize Frege proofs.

Milestone Result:

Theorem (Haken 1985)

$\{\neg\mathrm{PHP}_n^{n+1}\}$ *do not have polysize resolution refutations.*

Theorem (Buss 1987)

$\{\mathrm{PHP}_n^{n+1}\}$ *have polysize Frege proofs*

Theorem (Buss 1987)

$\{\mathrm{PHP}_n^{n+1}\}$ *have polysize Frege proofs*

Proof.

- Counting is in $\mathbf{NC}^1$ (i.e. polynomial formula size).
- Define $Count_{n,k}(p_1, ..., p_n) \leftrightarrow$ Exactly k of $p_1, ..., p_n$ are true.
- Family $\langle Count_{n,k} \rangle$ has poly formula size $(n^{O(1)})$
- Hence there are polysize formulas

  $$A_k(\vec{p_{ij}}) \equiv \text{“Pigeons } 1, ..., k \text{ occupy at least } k \text{ holes”}$$

- Prove if no two pigeons occupy same hole, then

  $$A_1 \rightarrow A_2 \rightarrow ... \rightarrow A_{n+1}$$

  to get a contradiction.

$\square$

- So the tautologies $\{\mathrm{PHP}_n^{n+1}\}$ are not hard for Frege systems.
- The question of whether Frege systems are polybounded remains wide open.
- Later we will give tautology families that might be hard for Frege systems.

Thesis

If a hard tautology family (for Frege systems) comes from a combinatorial principle, then that principle should not be provable using $\mathbf{NC}^1$ concepts.

- This motivates associating a first-order theory **VC** with a complexity class **C**. The theorems of **VC** are those that can be proved using concepts from **C**.
- Associated with **VC** is a propositional proof system **CFrege**.
- Each universal theorem of **VC** can be translated to a tautology family with polysize proofs in **CFrege**.

The three-way connection

1. **C** is a complexity class.
2. **VC** is a theory whose proofs use concepts from **C**.
3. **CFrege** is a propositional proof system such that the lines in a **CFrege**-proof express concepts from **C**.

Note that $\mathbf{NC}^1$**Frege** is the same as **Frege**.

Example triple: $\{\mathbf{NC}^1, \mathbf{VNC}^1, \mathbf{Frege}\}$

Theories for Polytime reasoning:

- **PV** [C. 75] Equational theory with function symbols for all polytime functions $f : \mathbb{N}^k \to \mathbb{N}$. Inspired by Skolem's Primitive Recursive Arithmetic (1923).

- **PV** functions introduced via Cobham's 1963 characterization of polytime functions:
  - The least class containing initial functions and closed under composition and limited recursion on notation.
  - The axioms and rules include recursive defining equations for eachfunction symbol and
  - **Rule:** Equational Induction on (binary) notation

$$\frac{f(0) = g(0), \qquad \{f(xi) = h_i(x, f(x)), g(xi) = h_i(x, g(x)) : i = 0, 1\}}{f(x) = g(x)}$$

The first-order version of PV

- **PV Nowadays**
  - a first-order theory with polytime function symbols as before, and
  - universal axioms based on Cobham's theorem, but
  - the rule induction on notation is replaced by the axiom scheme induction on notation:
    $$\Big[\varphi(0) \wedge \forall x \Big(\varphi(x) \supset (\varphi(x0) \wedge \varphi(x1))\Big)\Big] \supset \forall y \varphi(y)$$
    where $\varphi(x)$ is a quantifier-free formula.
  - Note that an induction proof of $\varphi(x)$ can be unwound in just $|x|$ steps, where $|x|$ is the binary length of x.
- First-order **PV** is a conservative extension of equational **PV**.

Theorem (Dowd)

PV *proves the induction scheme for open formulas* φ*:*

$$\Big[\varphi(0) \wedge \forall x \Big(\varphi(x) \supset \varphi(x+1)\Big)\Big] \supset \forall y \varphi(y)$$

- But this induction proof of $\varphi(x)$ requires $2^{|x|}$ steps to unwind.
- Dowd's theorem is proved using binary search.

PV Witnessing Theorem

If **PV** $\vdash \forall\vec{x}\exists y\varphi(\vec{x}, y)$, where φ is open (i.e. expresses a polytime predicate) then there is a polytime f such that

$$\mathbf{PV} \vdash \forall\vec{x}\varphi(\vec{x}, f(\vec{x}))$$

Proof.

Since **PV** is a universal theory, this is an easy consequence of the Herbrand Theorem. □

- $\mathbf{S}^1_2$ [Buss 86]: Finitely axiomatizable first-order theory, including induction on notation for **NP** formulas, associated with class **P**.
- **Theorem [Buss 86].** **PV** and $\mathbf{S}^1_2(\mathbf{PV})$ prove the same $\forall\exists\varphi$ theorems, where φ expresses a polytime predicate.
- A function $f(x)$ is *provably total* in a theory T if

$$\mathrm{T} \vdash \forall x\exists y\varphi(x, y)$$

  where $\varphi(x, y)$ is a Σ^b_1 formula expressing $y = f(x)$.
- The provably total functions of **PV** (and of $\mathbf{S}^1_2$) are the polytime functions.

PV is a ROBUST MINIMAL THEORY for **P**.

Observations: ('Polytime proof' means PV proof.)

1. 'Natural' polytime algorithms usually have polytime correctness proofs.
2. Combinatorial theorems of interest in computer science often have polytime proofs.
   - Kuratowski's Theorem
   - Hall's Theorem
   - Menger's Theorem
   - Linear Algebra (Cayley-Hamilton, properties of determinants,...)
   - Extended Euclidean Algorithm

Possible counter-example to 1: Primes in **P**. [AKS 04]

- The correctness statement implies

$$\neg Prime(n) \wedge n \geq 2 \supset \exists d(1 < d < n \wedge d | n)$$

- If **PV** proves this, then by the Witnessing Theorem, the divisor d can be computed from n in polytime, so this implies a polytime integer factoring algorithm.
- (The same reasoning applies to any polytime algorithm for Primes.)

Theses: ('Polytime proof' means PV proof.)

1. 'Natural' polytime algorithms usually have polytime correctness proofs.
2. Combinatorial theorems of interest in computer science often have polytime proofs.

Possible counter-example to 2:

- Fermat's Little Theorem:

$$\mathrm{Prime}(n) \wedge 1 \leq a < n \ \rightarrow \ a^{n-1} \equiv 1 (\bmod n)$$

- Contrapositive:

$$\forall a, n \exists d < n (a^{n-1} \not\equiv 1 (\bmod n) \ \rightarrow \ d \neq 1 \wedge d | n)$$

- Thus if **PV** proves this then by the Witnessing Theorem, d can be found from a, n in time polynomial in $|n|$.
- This leads to a probabilistic polytime algorithm for factoring.

Propositional proof system associated with P?

- Recall: Frege systems are associated with $\mathbf{NC}^1$
- A problem is in $\mathbf{NC}^1$ iff it can be solved by a uniform polysize family of Boolean formulas.
- A Frege proof consists of a sequence of Boolean formulas, where each formula is an axiom or follows from earlier formulas by simple rules.
- NOTE: A problem is in **P** iff it can be solved by a uniform polysize family of Boolean circuits.
- So a proof for a polytime propositional proof system should be a sequence of Boolean circuits, with axioms and rules as for Frege systems.
- A Boolean circuit can be described by a straight line program in which each line defines the value of a gate in terms of previous gate values.
- So we abbreviate circuit outputs by introducing new *extension variables* defined by formulas.

Extended Frege Systems (EFrege systems, or "P-Frege Systems")

- Extend Frege systems by allowing new extension variables and their definitions:

$$p \leftrightarrow A$$

  for 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.

$$p_1 \leftrightarrow A_1,\ \ p_2 \leftrightarrow A_2(p_1), \ldots, p_n \leftrightarrow A_n(p_1, \ldots, p_{n-1})$$

- Lines in an Extended Frege proof are like Boolean circuits. (The new atoms are like gates in the circuit.)

Historical Notes

- Extended Resolution (**ER**) introduced by G.S. Tseitin in 1966.
  - ER extends the resolution proof system by allowing clauses defining new variables.
  - For example, to introduce p so that $p \leftrightarrow (q \vee r)$, add clauses

$$\overline{p} \vee q \vee r, \qquad p \vee \overline{q}, \qquad p \vee \overline{r}$$

- (C. 75) Introduced **PV** and indicated that theorems of **PV** can be translated into polysize families of **ER** proofs.
- (C. 75) also outlined a proof that **PV** proves the soundness of **ER** (reflection principle).
- (C.-Reckhow 74 and 79) Introduced 'Frege Systems' and **EFrege** systems and pointed out the latter are *p*-equivalent to **ER**.

Recall the three-way connection

- **C** is a complexity class.
- **VC** is a theory whose proofs use concepts from **C**.
- **CFrege** is a propositional proof system such that the lines in a **CFrege**-proof express concepts from **C**.

$\mathbf{NC}^1$**Frege** is the same as **Frege**. **PFrege** is the same as **EFrege**.

Example triples

- $\{\mathbf{NC}^1, \mathbf{VNC}^1, \mathbf{Frege}\}$
- $\{\mathbf{P}, \mathbf{PV}, \mathbf{EFrege}\}$

Theorem

- **VC** *proves soundness of* **CFrege**
- *If* **VC** *proves the soundness of proof system* **S**, *then* **CFrege** *p-simulates* **S**.

Recall Historical Notes

- Extended Resolution (**ER**) introduced by G.S. Tseitin in 1966.
- (C. 75) Introduced **PV** and indicated that theorems of **PV** can be translated into polysize families of **ER** proofs.
- (C. 75) also outlined a proof that **PV** proves the soundness of **ER** (reflection principle).
- (C.-Reckhow 74 and 79) Introduced 'Frege Systems' and **EFrege** systems and pointed out the latter are *p*-equivalent to **ER**.
- (Clote 90) 'ALOGTIME and a conjecture of S. A. Cook' introduced first theory **ALV** for $\mathbf{NC}^1$ with translations to Frege systems.
- (Arai 91, 00) 'A bounded arithmetic **AID** for Frege systems' Showed his system **AID** is equivalent to Clote's **ALV**, and proves soundness of Frege using a result of Buss.
- (Krajíček 95) 'Bounded Arithmetic, Propositional Logic, and Complexity Theory' expounded the three way connection.

Complexity Classes

(Google: Complexity Zoo)

$$\mathbf{AC^0} \subset \mathbf{AC^0}(m) \subseteq \mathbf{TC^0} \subseteq \mathbf{NC}^1 \subseteq \mathbf{NC}^2 \subseteq \mathbf{P}$$

Defined by uniform polysize Boolean circuit families

- $\mathbf{AC^0}$ – bounded-depth circuits with unbounded fanin $\wedge, \vee$ (Immerman's **FO**)
- $\mathbf{AC^0}(m)$ – Allow mod m gates $(p_1 + p_2 + \ldots + p_k)$ mod m in above circuits.
- $\mathbf{TC^0}$ – Allow threshold gates (counting class)
- $\mathbf{NC}^1$ – polynomial formula size
- $\mathbf{NC}^2$ – polysize $\log^2$ depth families of Boolean circuits (contains matrix inverse, determinant, etc)
- $\mathbf{P}$ – polysize families of Boolean circuits

Complexity Classes

$$\mathbf{AC^0} \subset \mathbf{AC^0}(m) \subseteq \mathbf{TC^0} \subseteq \mathbf{NC}^1 \subseteq \mathbf{NC}^2 \subseteq \mathbf{P}$$

- **Open question:** $\mathbf{P} = \mathbf{NP}$?
- **Also open:** $\mathbf{AC^0}(6) = \mathbf{NP}$?

Theorem (Razborov-Smolensky 87)

$\mathbf{AC^0}(p^k) \subsetneq \mathbf{TC^0}$, *for every* $k \geq 1$ *and prime* p.

$\mathbf{AC^0} \subset \mathbf{AC^0}(m) \subseteq \mathbf{TC^0} \subseteq \mathbf{NC}^1 \subseteq \mathbf{NC}^2 \subseteq \mathbf{P}$

[C.-Nguyen 2010] presents a unified way to define a first-order theory **VC** (over a two-sorted language) corresponding to a complexity class **C**, including all of the above classes.

In particular:

- $\mathbf{VNC}^1$ is a simplified version of Clote's **ALV** and Arai's **AID**.
- **VP** is a finitely axiomatized theory for polynomial time.
- **VPV** is the two-sorted version **PV**, with function symbols for all polytime functions.
- **VPV** is a conservative extension of **VP**.

Also the book describes propositional translations of the theories to the corresponding proof systems.

Two-sorted theories cont'd

- The base theory $\mathbf{V^0}$ ($= \mathbf{VAC}^0$) corresponds to $\mathbf{AC^0}$.
- The pigeonhole principle $\mathrm{PHP}(n, X)$ is expressed by the following two-sorted formula where X is a bit-array, and $X(i,j)$ means that pigeon i is mapped to hole j:

$$\forall i \leq n \exists j < n X(i,j) \rightarrow \exists i, k \leq n \exists j < n (i < k \wedge X(i,j) \wedge X(k,j))$$

- For each constant n, This translates into a propositional formula equivalent to PHP_n^{n+1}
- Each bit $X(i,j)$ translates to a Boolean variable p_{ij}^X.
- Bounded quantifiers $\exists i \leq n$ and $\forall i \leq n$ translate to

$$\bigvee_{i=1}^{n} \qquad \bigwedge_{i=1}^{n}$$

respectively.
- Does $\mathbf{V^0}$ prove $\mathrm{PHP}(n, X)$?

What is the proof system AC^0-Frege?

- Answer: Restrict formulas in a Frege proof to have depth $\leq d$, for some constant d.

Theorem (Ajtai 88)

There are no polysize $\mathbf{AC^0}$*-Frege proofs of* $\{\mathrm{PHP}_n^{n+1}\}$

- Since Σ_0^B theorems of $\mathbf{V^0}$ translate to polysize families of $\mathbf{AC^0}$-Frege proofs, we answer our earlier question:

Corollary

$\mathbf{V^0}$ *does not prove* $\mathrm{PHP}(n, X)$.

- $\mathbf{VTC}^0$ corresponds to $\mathbf{TC^0}$ (the counting class), so it is easy to see that
$$\mathbf{VTC}^0 \vdash \mathrm{PHP}(n, X)$$
- Since $\mathbf{VTC}^0 \subseteq \mathbf{VNC}^1$, if follows that $\mathbf{VNC}^1 \vdash \mathrm{PHP}(n, X)$, so we obtain Buss's Theorem that $\{\mathrm{PHP}_n^{n+1}\}$ has polysize Frege proofs as a corollary.
- (Recall that $\mathbf{NC}^1$-Frege = Frege.)

We can associate propositional systems with other classes

- $\mathbf{AC^0}(m)$-Frege
- $\mathbf{TC^0}$-Frege Has polysize proofs of $\{\mathrm{PHP}_n^{n+1}\}$
- $\mathbf{NC}^1$-Frege = Frege
- $\mathbf{NC}^2$-Frege
- **PFrege** = **EFrege** (Extended Frege):
  - Allows introduction of new variables by definition, corresponding to gates in a circuit

Surprising open question

Is $\mathbf{AC^0}(2)$**Frege** polybounded?

This is open, despite the [Razborov-Smolensky 87] proof that $\mathbf{AC^0}(p) \not\subseteq \mathbf{TC^0}$ for any prime p.

Conjecture

PHP_n^{n+1} do not have polysize $\mathbf{AC^0}(2)$**Frege** proofs.

A weaker conjecture:

$$\mathbf{VAC}^0(2) \nvdash \mathrm{PHP}(n, X)$$

but this is also open.

Hard tautology families for Frege systems?

Consider the 'hard matrix identity'

$$AB = I \to BA = I$$

where A, B are $n \times n$ matrices.

- If the entries are in $GF(2)$ (or even in $\mathbb{Z}$ or $\mathbb{Q}$) this translates into a polysize family $\{\varphi_n\}$ of tautologies.
- Proofs of these identities seem to require tools from linear algebra, such as Gaussian Elimination, or the Cayley-Hamilton Theorem.
- Note that computing matrix inverses (over finite fields or $\mathbb{Z}$ or $\mathbb{Q}$) can be done in $\mathbf{NC}^2$, but apparently not in $\mathbf{NC}^1$.

Conjecture (e.g. [Soltys-C. 04])

$\{\varphi_n\}$ do not have polysize Frege proofs.

- This conjecture remains open.

Hard matrix tautologies cont'd

$$AB = I \rightarrow BA = I$$

where A, B are $n \times n$ matrices.

- In [Solys-C. 04] we develop formal theories for linear algebra. Although the standard linear algebra operators are in $\mathbf{NC}^2$, proving their properties seems to require **VP** rather than $\mathbf{VNC}^2$.
- **Question:** Do these matrix identies have polysize $\mathbf{NC}^2$-Frege proofs? **Answer:** [Hrubeš -Tzameret 2011]: Yes, and they have quasi-polysize Frege proofs.
- But [Hrubeš -Tzameret] leave open the question of whether the theory $\mathbf{VNC}^2$ proves the identities.

What about hard tautologies for EFrege systems?

- It's difficult to think of interesting universal combinatorial theorems involving polytime functions, which cannot be proved in **VPV**.
- However mathematical logic suggests consistency statements.
- We know [Gödel 31] **con**(**VPV**) is universal sentence not provable in **VPV**.
- It seems plausible to conjecture that the corresponding tautology family does not have polysize **EFrege** proofs.
- For that matter what about **con**(**PA**), or **con**(**ZF**)?
- Let $[\mathbf{con}(\mathbf{ZF})]_n$ be a propositional tautology asserting **ZF** has no proof of $0 \neq 0$ of length n or less.
- It's hard to imagine how the family $\left\{[\mathbf{con}(\mathbf{ZF})]_n\right\}$ could have polysize **EFrege** proofs, unless **EFrege** is polybounded.

Concluding thought

- Given the extreme difficulty of proving lower bounds even for simple proof systems (such as $\mathbf{AC^0}(2)\mathbf{Frege}$), perhaps we should contemplate the possibility

$$\mathbf{NP} = \mathbf{coNP}$$

- This might surprise complexity-theorists, but would not otherwise have the potentially earth-shaking consequences of

$$\mathbf{P} = \mathbf{NP}$$