Complexity of propositional proofs: Some theory and examples

Sam Buss
Univ. of California, San Diego

Barcelona
April 27, 2015

Frege proofs

Frege proofs are the usual "textbook" proof systems for propositional logic, using modus ponens as their only rule of inference.

Connectives: $\land$, $\lor$, $\neg$, and $\to$.

Modus ponens: $\dfrac{A \quad A \to B}{B}$

Axioms: Finite set of axiom schemes, e.g.: $A \land B \to A$

Defn: Proof *size* is the number of symbols in the proof.

Frege proofs are the usual "textbook" proof systems for propositional logic, using modus ponens as their only rule of inference.

Connectives: $\wedge$, $\vee$, $\neg$, and $\rightarrow$.

Modus ponens: $\dfrac{A \quad A \rightarrow B}{B}$

Axioms: Finite set of axiom schemes, e.g.: $A \wedge B \rightarrow A$

Extended Frege proofs allow also the *extension axiom*, which lets a new variable x abbreviate a formula A:

$$x \leftrightarrow A$$

Defn: Proof *size* is still the number of symbols in the proof.

Soundness and Completeness: A formula A is provable with a Frege (or, extended Frege) proof if and only if A is a tautology. That is, if and only if A is true for all Boolean truth assignments.

Open Question: Is there a polynomial bound on the size of shortest (extended) Frege proofs of A as a function of the size of A?
If yes, then $\mathrm{NP} = \mathrm{coNP}$. [Cook-Reckhow'74].

Open Question: Do Frege systems *polynomially simulate* extended Frege systems?

This is analogous to the open question of whether Boolean circuits can be converted into equivalent polynomial size Boolean formulas.

The pigeonhole principle as a propositional tautology

Let $[n] = \{0, \ldots, n-1\}$.
Let i's range over members of $[n+1]$ and j's range over $[n]$.

$$\mathrm{Tot}_i^n := \bigvee_{j \in [n]} x_{i,j}. \quad \text{“Total at } i\text{”}$$

$$\mathrm{Inj}_j^n := \bigwedge_{0 \le i_1 < i_2 \le n} \neg(x_{i_1,j} \wedge x_{i_2,j}). \quad \text{“Injective at } j\text{”}$$

$$\mathrm{PHP}_n^{n+1} := \neg\Big(\bigwedge_{i \in [n+1]} \mathrm{Tot}_i^n \wedge \bigwedge_{j \in [n]} \mathrm{Inj}_j^n \Big).$$

PHP_n^{n+1} is a tautology.

Cook-Reckhow's $e\mathcal{F}$ proof of PHP_n^{n+1}

Code the graph of $f : [n+1] \to [n]$ with variables $x_{i,j}$ indicating that $f(i) = j$.

$\mathrm{PHP}_n^{n+1}(\vec{x})$: "$f$ is not both total and injective"

Use extension to introduce new variables

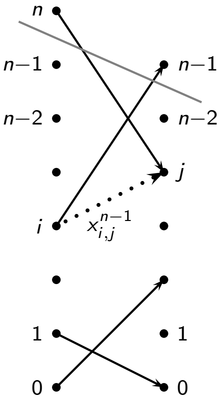
$$x_{i,j}^{\ell-1} \leftrightarrow x_{i,j}^{\ell} \vee (x_{i,\ell-1}^{\ell} \wedge x_{\ell,j}^{\ell}).$$

for $i \le \ell$, $j < \ell$; where $x_{i,j}^{n} \leftrightarrow x_{i,j}$.

Prove, for each ℓ that

$$\neg PHP_{\ell}^{\ell+1}(\vec{x}^{\ell}) \to \neg PHP_{\ell-1}^{\ell}(\vec{x}^{\ell-1}).$$

Finally derive $\mathrm{PHP}_n^{n+1}(\vec{x})$ from $\mathrm{PHP}_1^2(\vec{x}^1)$. □



Theorem (Cook-Reckhow '79)

PHP_n^{n+1} *has polynomial size extended Frege proofs.*

Theorem (B '87)

PHP_n^{n+1} *has polynomial size Frege proofs.*

Theorem (B '15)

PHP_n^{n+1} *has quasipolynomial size Frege proofs.*

Cook-Reckhow's proof of PHP_n^{n+1} as a Frege proof [B'1?]

Let G^ℓ be the directed graph with:
edges $(\langle i,0\rangle,\langle j,1\rangle)$ such that $x_{i,j}$ holds, and
edges $(\langle i,1\rangle,\langle i{+}1,0\rangle)$ such that $i{\ge}\ell$ (blue edges).

For $i \le \ell$, $j < \ell$, let $\varphi^\ell_{i,j}$ express

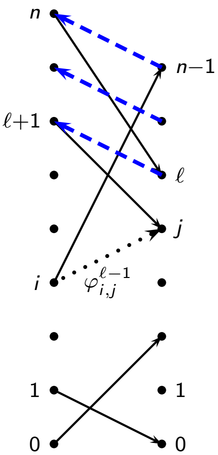
"Range node $\langle j,1\rangle$ is reachable
from domain node $\langle i,0\rangle$ in G^ℓ".

$\varphi^\ell_{i,j}$ is a quasi-polynomial size formula via an NC^2 definition of reachability.

For each ℓ, prove that

$$\neg PHP^{\ell+1}_{\ell}(\vec{\varphi}^{\ell}) \to \neg PHP^{\ell}_{\ell-1}(\vec{\varphi}^{\ell-1}).$$

Finally derive $\mathrm{PHP}_n^{n+1}(\vec{x})$ from $\mathrm{PHP}_1^2(\vec{\varphi}^1)$. □



Thus, PHP_n^{n+1} no longer provides evidence for Frege not p-simulating $e\mathcal{F}$.

[Bonet-B-Pitassi'94] "Are there hard examples for Frege?": examined candidates for separating Frege and $e\mathcal{F}$. We found very few:

- Cook's $AB = I \Rightarrow BA = I$, Odd-town theorem, etc. [Hrubes-Tzameret'15]
- Frankl's Theorem [Aisenberg-B-Bonet'15]

[Kołodziejczyk-Nguyen-Thapen'11]: Local improvement principles, mostly settled by [Beckmann-B'14], RLI_2 still open.

[Crãciun-Istrate'14] suggested the Kneser-Lovász theorem as hard for $e\mathcal{F}$. (!)

Kneser graph on n.

Def'n: Fix $n > 1$ and $1 \leq k < n$. The (n, k)-Kneser graph has $\binom{n}{k}$ vertices: the k-subsets of $[n]$. The edges are the pairs

$$\{S, T\} \text{ s.t. } S \cap T = \emptyset,\ S, T \subset [n],\ |S| = |T| = k.$$

Kneser-Lovász Theorem: [Lovász'78] There is no coloring of the (n, k)-Kneser graph with $\leq n - 2k + 1$ colors.

Usual proof involves the octahedral Tucker lemma, or other principles from topology. There is no known way to formalize these topology-based arguments with short propositional proofs, even in extended Frege systems.

Definition (Kneser-Lovász tautologies)

Let $n \geq 2k > 1$, and let $m = n - 2k + 1$ be the number of colors. For $S \in \binom{n}{k}$ and $i \in [m]$, the propositional variable $p_{S,i}$ has the intended meaning that vertex S of the Kneser graph is assigned the color i. The Kneser-Lovász principle is expressed propositionally by

$$\bigwedge_{S \in \binom{n}{k}} \bigvee_{i \in [m]} p_{S,i} \rightarrow \bigvee_{\substack{S,T \in \binom{n}{k} \\ S \cap T = \emptyset}} \bigvee_{i \in [m]} (p_{S,i} \wedge p_{T,i}) \, .$$

Theorem [ABBCI'15]: Fix a value for k. The Kneser-Lovász Theorem has polynomial size extended Frege proofs, and quasipolynomial size Frege proofs.

J. Aisenberg, M.L. Bonet, B., A. Crãciun, G. Istrate; ICALP '15

The Frege proof is based on a new counting proof.

Proof sketch. Assume there is a coloring with $n - 2k + 1$ colors. Let ℓ be a color, and P_ℓ the set of k-subsets of n with color ℓ.

P_ℓ is *star-shaped* if the intersection of its members is non-empty.

Claim: If P_ℓ is *not* star-shaped, then $|P_\ell| < k^2\binom{n-2}{k-2}$.

Pf: on next slide ... □

For n large enough ($n > k^4$), there are $\binom{n}{k} > (n - 2k + 1) \cdot k^2\binom{n-2}{k-2}$ k-subsets of n. Thus, some color P_ℓ is star-shaped.

Remove this color ℓ and the central element of P_ℓ. This gives a $(n - 1) - 2k + 1$ coloring of the $(n{-}1, k)$-Kneser graph.
Proceed by induction on n until $n < k^4$. Now there are only finitely colorings to consider; this final case can be proved by exhaustive enumeration by a constant size Frege proof.

Let P_ℓ be a non-star-shaped color:

Fix some $S = \{a_1, \ldots, a_k\} \in P_\ell$.

For each a_i, pick some $S_i \in P_\ell$ s.t. $a_i \notin S_i$.
(The S_i's exist, since P_ℓ is not star-shaped.)

Can specify arbitrary $T \in P_\ell$, by:

- Specifying an $a_i \in T$, (since $S \cap T \neq \emptyset$.)
- Specifying an $a' \in S_i \cap T$.
- Specifying the remaining $k-2$ elements of T.

There are $\leq k \cdot k \cdot \binom{n-2}{k-2} = k^2\binom{n-2}{k-2}$ possible specifications.

Thus $|P_\ell| \leq k^2\binom{n-2}{k-2}$.

The above argument can be straightforwardly formulated as polynomial-size extended Frege proofs by:

- Straightforward counting (possible with poly size Frege proofs [B'87]),
- Defining the $(n-1, k)$-Kneser graph from the (n, k)-Kneser graph using the extension rule,
- Showing that the coloring for the (n, k)-Kneser graph induces a coloring for the $(n-1, k)$-Kneser graph. (No further uses of the extension rule needed.)

There are $O(n)$ rounds of extension.
So this is only an extended Frege proof: The extension axioms cannot be "unwound" without causing exponential blowup in formula size.

To get quasipolynomial size Frege proofs, need to have only $O(\log n)$ rounds of extension rules.

Proof idea: 1. Non-star-shaped P_ℓ's have size $< k^2\binom{n-2}{k-2}$.

2. Star-shaped P_ℓ's have size $\le \binom{n-1}{k-1}$.

Lemma: Let $n > 2k^3(k-1/2)$. Any coloring of the (n,k)-Kneser graph has at least $\frac{1}{2k}n$ star-shaped colors.

Proof is simple counting.

Eliminate, fraction $1/(2k)$ of the colors in a single step — i.e., star-shaped colors. (One round of extension axioms.)

After $O(\log n)$ many rounds, have reduced n to a constant, $n < 2k^3(k-1/2)$.

Unwinding the extension axioms gives quasipolynomial size Frege proofs. QED

The Octahedral Tucker Lemma

Definition (Octahedral ball $\mathcal{B}^n$)

$\mathcal{B}^n \ := \ \{(A, B) : A, B \subseteq [n] \text{ and } A \cap B = \emptyset\}.$

Definition (Antipodal)

A mapping $\lambda : \mathcal{B}^n \to \{1, \pm 2, \ldots, \pm n\}$ is *antipodal* if $\lambda(\emptyset, \emptyset) = 1$, and for all other $(A, B) \in \mathcal{B}^n$, $\lambda(A, B) = -\lambda(B, A)$.

Definition (Complementary)

(A_1, B_1) and (A_2, B_2) in $\mathcal{B}^n$ are *complementary* w.r.t. λ iff $A_1 \subseteq A_2$, $B_1 \subseteq B_2$ and $\lambda(A_1, B_1) = -\lambda(A_2, B_2)$.

Theorem (Tucker lemma)

If $\lambda : \mathcal{B}^n \to \{1, \pm 2, \ldots, \pm n\}$ is antipodal, then there are two elements in $\mathcal{B}^n$ that are complementary.

Truncated Tucker Lemma

Definition (Truncated octahedral ball $\mathcal{B}^n_k$)

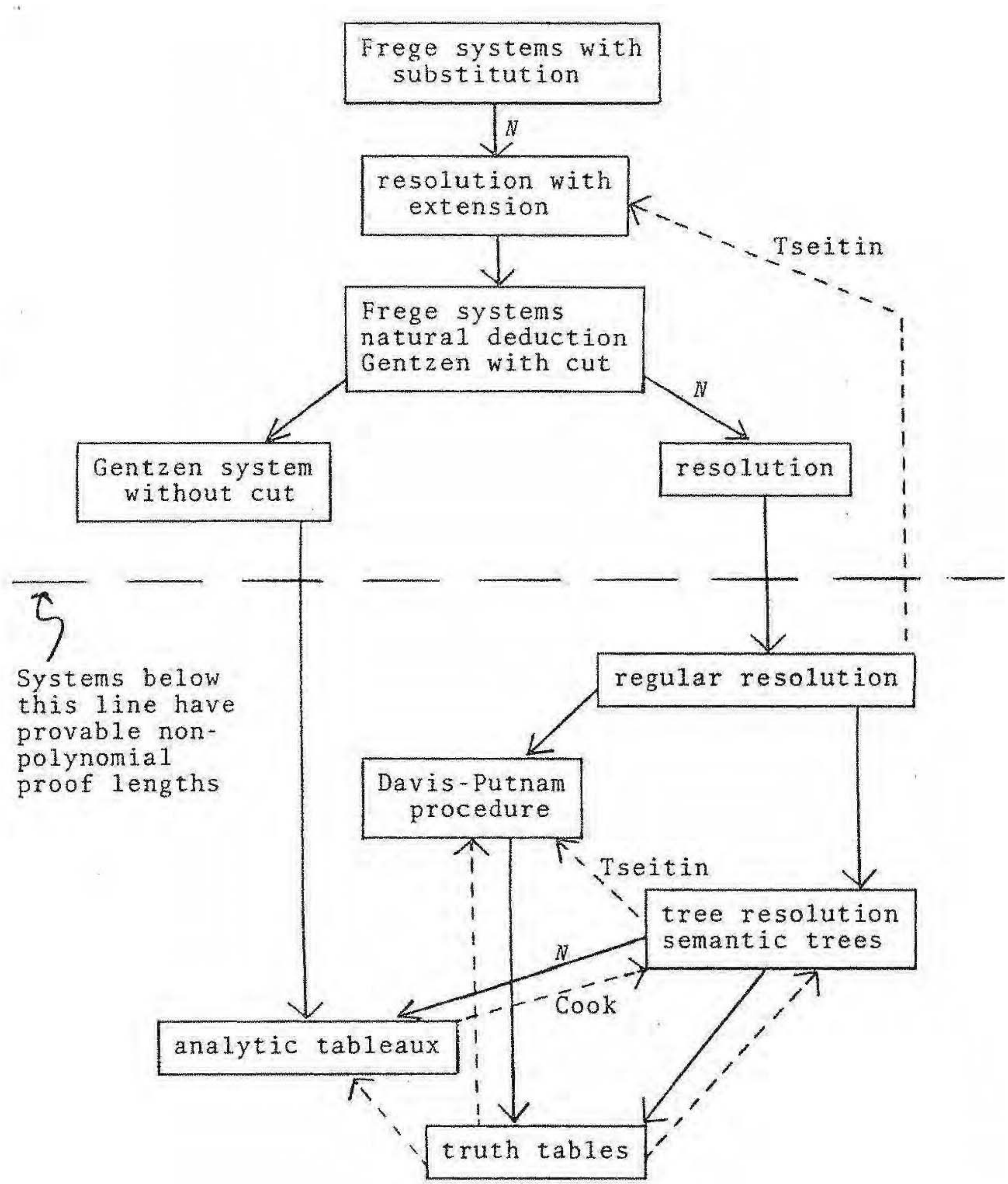
$$\mathcal{B}^n_k := \left\{(A,B) : A,B \in \binom{n}{k} \cup \{\emptyset\},\ A \cap B = \emptyset \ \&\ (A,B) \neq (\emptyset,\emptyset)\right\}.$$

Definition ($\preceq$ and k-Complementary)

- $A_1 \preceq A_2$ iff $(A_1 \cup A_2)_{\leq k} = A_2$.
- $(A_1,B_1) \preceq (A_2,B_2)$ iff $A_1 \preceq A_2$, $B_1 \preceq B_2$, & $A_i \cap B_j = \emptyset$, $\forall i,j$.
- (A_1,B_1) and (A_2,B_2) are *k-complementary* w.r.t. λ if $(A_1,B_1) \preceq (A_2,B_2)$ and $\lambda(A_1,B_1) = -\lambda(A_2,B_2)$.

Theorem (Truncated Tucker)

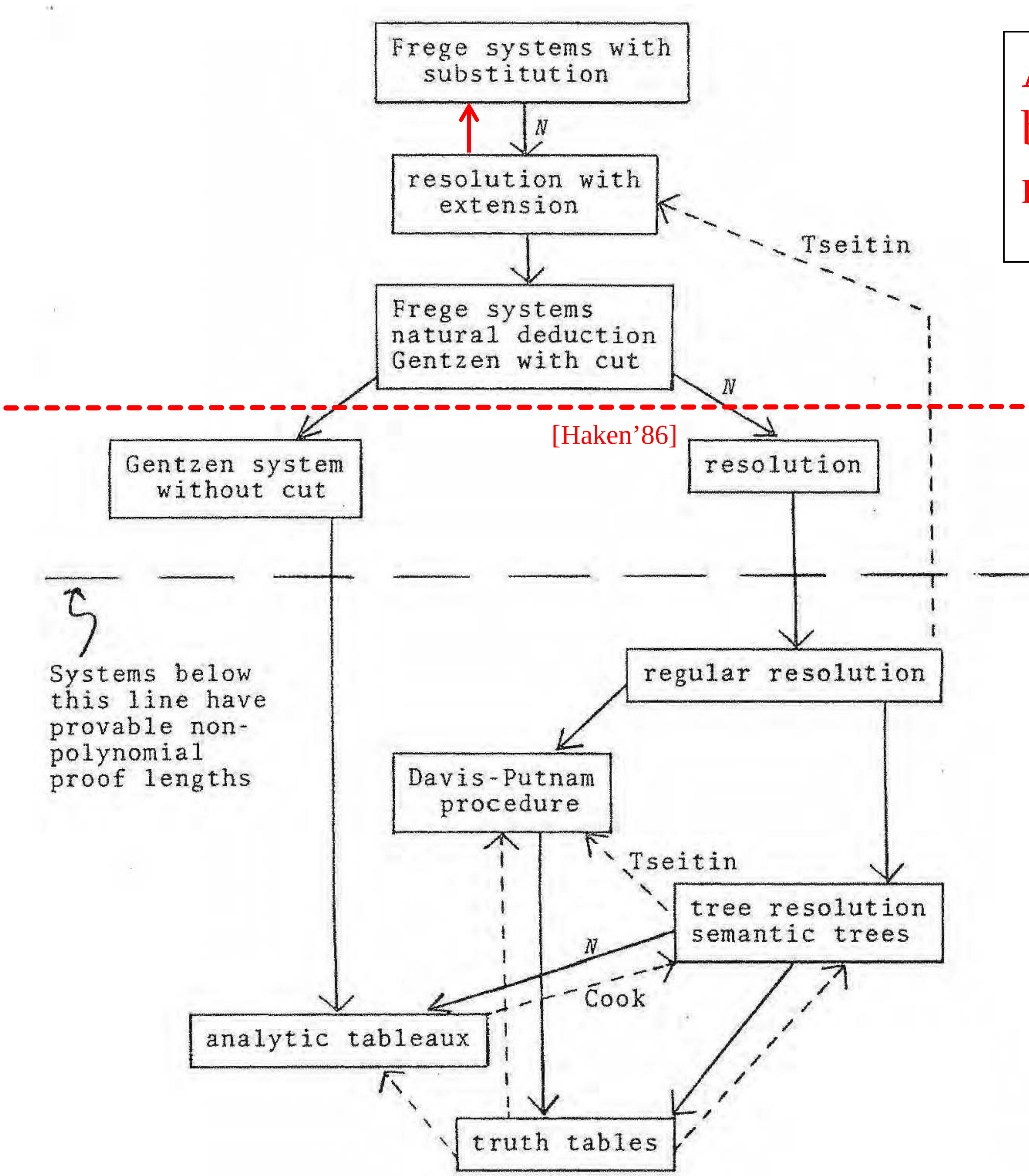
Let $n \geq 2k > 1$. If $\lambda : \mathcal{B}^n_k \to \{\pm 2k \ldots, \pm n\}$ is antipodal, then there are two elements in $\mathcal{B}^n_k$ that are k-complementary.



R.A. Reckhow, PhD thesis, 1975

Cook's Program: Prove NP≠coNP by proving there is no polynomially bounded propositional proof system.

As of 1975: Systems above the line were not known to not be polynomially bounded.



R.A. Reckhow, PhD thesis, 1975

As of 2014, proof systems below the line are known to not be polynomially bounded:

Constant-depth (AC^0) Frege
[Ajtai'88; Pitassi-Beame-Impagliazzo'93; Krajicek-Pudlak-Woods'95]

Constant-depth Frege with counting mod *m* axioms
[Ajtai'94; Beame-Impagliazzo-Krajicek-Pitassi-Pudlak'96; B-Impagliazzo-Krajicek-Pudlak-Razborov-Sgall'96; Grigoriev'98]

Cutting Planes
[Pudlak'97]

Nullstellensatz
[B-Impagliazzo-Krajicek-Pudlak-Razborov-Sgall'96; Grigoriev'98]

Polynomial calculus
[Razborov'98; Impagliazzo-Pudlak-Sgall'99; Ben-Sasson-Impagliazzo'99; B-Grigoriev-Impagliazzo-Pitassi'96; B-Impagliazzo-Krajicek-Pudlak-Razborov-Sgall'96; Alekhnovich-Razborov'01]

Thank You!