Proof Complexity
Part B: Propositional Pigeonhole Principle, Upper and Lower Bounds

Sam Buss

Satisfiability Boot Camp
Simons Institute, Berkeley, California
January–May 2021

Part B. discusses:

- Propositional Pigeonhole Principle
- Polynomial size $e\mathcal{F}$ proofs
- Polynomial size $\mathcal{F}$ proofs
- Exponential lower bounds for resolution

Part C. is independent of Part B.

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 $[n]$.
Intuition: $x_{i,j}$ means "Pigeon i is mapped to hole j.
(i is mapped to j.)

$$\mathbf{Tot}_i^n \; := \; \bigvee_{j \in [n]} x_{i,j}. \quad \text{"Total at } i\text{"}$$

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

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

PHP_n^{n+1} is a tautology. It is a polynomial size DNF.

Thm: PHP_n^{n+1} has polynomial size $e\mathcal{F}$ proofs. [Cook-Reckhow'79]

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"

Identify $x_{i,j}^n$ with $x_{i,j}$.

Use **extension** to introduce new variables

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

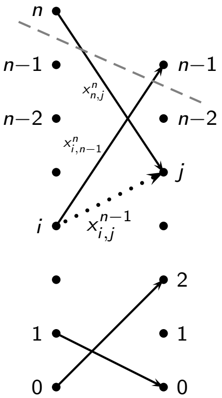
for $i \le \ell$, $j < \ell$; where $x_{i,j}^n \leftrightarrow x_{i,j}$.

Let $\mathrm{PHP}_\ell^{\ell+1}$ be over variables $x_{i,j}^\ell$.

Prove, for each ℓ that

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

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



Theorem (Cook-Reckhow '79)

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

Theorem (Cook-Reckhow '79)

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

Proof: The above proofs are polynomial size $e\mathcal{F}$ proofs.

Expanding the uses of the extension rule, causes an exponential blow up in formula size, $\approx 3^n$. Thus the $e\mathcal{F}$ proofs become exponential size $\mathcal{F}$ proofs.

Open Question: Does extended Frege proofs provide exponential speed up over Frege proofs? And thus, does Frege not p-simulate extended Frege?

Theorem (Cook-Reckhow '79)

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

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 (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.*

Polynomial size $\mathcal{F}$ proofs of PHP_n^{n+1} [B'87]

Proof is based on counting.

- There are polynomial-size formulas for **vector addition.** For $m, n \in \mathbb{N}$, input variables define the n bits of m integers. The $n + \log m$ formulas $\mathrm{CSA}_{m,n}$ define the bits of their sum. Based on carry-save-addition circuits.
- $\mathcal{F}$ can prove elementary facts about sums of vectors of integers as computed with CSA formulas and "2-3" adder trees

Proof sketch: ($\mathcal{F}$) Assume PHP_n^{n+1} is false. Proceed by "brute force induction" on $i' \leq n+1$ to prove that

- The number of $j \leq n$ such that $\bigvee_{i \leq i'} x_{i,j}$ is greater than or equal to i'.

Conclude by obtaining a contradiction $n \geq n+1$. □

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 $i{\geq}\ell$ (blue edges).

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

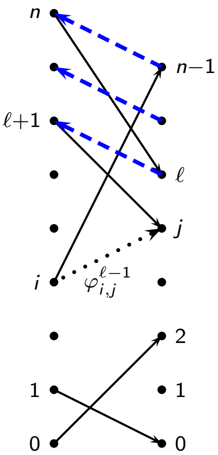
"Range node $\langle j,1\rangle$ is reachable
from domain node $\langle i,0\rangle$ in G^ℓ".

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

For each ℓ, prove that

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

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



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

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

- Cook's $AB = I \Rightarrow BA = I$, Odd-town theorem, etc.
  Now known to have quasipolynomial size $\mathcal{F}$-proofs, by proving matrix determinant properties with NC^2 formulas.
  [Hrubes-Tzameret'15; Tzameret-Cook'21]
- Frankl's Theorem
  Also quasi-polynomial size $\mathcal{F}$ proofs. [Aisenberg-B-Bonet'15]

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

Can the extension rule help resolution?

Yes, extension helps resolution; Since PHP_n^{n+1} has polynomial size $e\mathcal{F}$ proofs and since:

Thm: [Haken'86, Raz'02, Razborov'03, many others]
The pigeonhole principle (PHP) requires resolution proofs of size 2^{n^ϵ} (even PHP_n^m for $m \gg n$).

For PHP_n^{n+1}, a similar bound can be proved for constant-depth Frege proofs.

Thm: [BIKPPW'92]
Depth d Frege proofs of PHP_n^{n+1} require size 2^{n^ϵ} where $\epsilon = \epsilon(d)$.

Def'n Constant depth Frege proofs are formulated using the sequent calculus, with only connectives $\wedge$, $\vee$ applied to literals.

The **depth** of a Boolean formula is the number of alternations of $\wedge$'s and $\vee$'s.

The **depth** of a proof is the max depth of its formulas.

Proof uses two ingredients.

Def'n. Let Γ be an unsatisfiable set of clauses.
$\textsc{ResLen}(\Gamma)$ is the minimum number of steps in a resolution refutation of Γ.
$\textsc{ResWidth}(\Gamma)$ is the minimum width of a resolution refutation of Γ, where "width" is the maximum number of literals in any clause.

Theorem (Ben-Sasson, Wigderson'01)

If Γ is a k-CNF over n variables, then

$$\textsc{ResLen}(\Gamma) \geq exp\left(\Omega\left(\frac{(\textsc{ResWidth}(\Gamma) - k)^2}{n}\right)\right)$$

The $\textsc{ResLen}$ - $\textsc{ResWidth}$ tradeoff cannot be used directly with PHP_n^{n+1} since the Tot_i^n clauses are large and thus force k to be large.

But, **sparse PHP** can be used instead.
For G a bipartite graph on $[n+1] \oplus [n]$, replace Tot_i^n with

$$G\text{-}\mathbf{Tot}_i^n \;:=\; \bigvee_{(i,j)\in G} x_{i,j}. \quad \text{“Total at } i\text{”}$$

For G a constant degree graph with suitable expansion properties, we have $\textsc{ResWidth}(G\text{-}\mathrm{PHP}_n^{n+1})$ is $\Omega(n)$. [B-S,W'01]
Hence

Theorem (Haken'86, Ben-Sasson,Wigderson'01, and others)

G-PHP_n^{n+1} and hence PHP_n^{n+1} requires resolution proofs of size $\exp(\Omega(n))$.

End of part B!