Proof Complexity of Pigeonhole Principles

Alexander Razborov
Steklov Math Institute and IAS

Workshop in Honour of Anatol Slissenko's 60th birthday, Paris, September 5, 2001

I. Proof Systems

Definition. [Cook, Reckhow 73] TAUT is the set of all propositional tautologies. A propositional proof system is any polynomial time computable function

$$P : \{0,1\}^* \xrightarrow{\text{onto}} \text{TAUT}$$

Intuition. $w \in \{0,1\}^*$ is a P-proof of the tautology $\phi = P(w)$. "Onto" means completeness.

Definition. The complexity of ϕ is the minimal bit size $|w|$ of any P-proof w of ϕ.

Remark. Sometimes other complexity measures are considered like degree of algebraic proofs.

Definition. [CR73] A propositional proof system P is p-bounded if the proof complexity of a tautology ϕ is bounded by a polynomial in $|\phi|$, i.e. every tautology has a proof whose length is comparable with its own length.

Definition. P p-simulates Q if every Q-proof can be efficiently transformed into a P-proof of the same tautology.

Theorem. [CR73] p-bounded propositional proof systems exist if and only if $\mathbf{NP} = co - \mathbf{NP}$.

Proof idea. $\mathbf{NP}$ is the class of all decision problems possessing efficient "proofs" of the membership.

Frege Proof System, denoted by F – any text-book proof system.

Finitely many axiom schemes and inference rules like $A \to (A \vee B),\ A \vee \neg A,$
$((A \to B) \wedge (B \to C)) \to (A \to C)$,

$$\frac{A, \qquad A \to B}{B} \quad \text{(modus ponens)}$$

All Frege systems are polynomially equivalent – [Reckhow 76].

Bounded-depth Frege system F_d: in Frege proofs, we allow the connectives $\wedge, \vee$ to have unbounded fan-in (inference rules are adjusted accordingly) but bound the logical depth of any formula in the proof by an arbitrary but fixed constant d.

Finer classification

Analogous to Hastad Switching Lemma in circuit complexity: $F_{d+0.5}$ – formulas are of logical depth $d+1$ but the fan-in at the bottom level is at most poly-logarithmic.

$$\boxed{F_1 = \text{Resolution}}$$

Resolution proof system R operates with clauses and has one inference Resolution rule (essentially, the cut rule):

$$\frac{C \vee x \qquad D \vee \bar{x}}{C \vee D}$$

$F_{1.5}$ operates with disjunctions of conjunctions that have poly-log fan-in:

$$\boxed{F_{1.5} = R(\text{poly-log})}.$$

We will be also interested in $R(2)$ and $R(\log)$, similarly defined.

Polynomial Calculus
[Clegg, Impagliazzio, Edmonds 96]

Fix a field. A clause $x_{i_1}^{\epsilon_1} \vee \ldots \vee x_{i_k}^{\epsilon_k}$ is satisfied if and only if $(x_{i_1} - \epsilon_1) \cdot \ldots \cdot (x_{i_k} - \epsilon_k) = 0$ (here $x^1 = x$ and $x^0 = (\neg x)$).

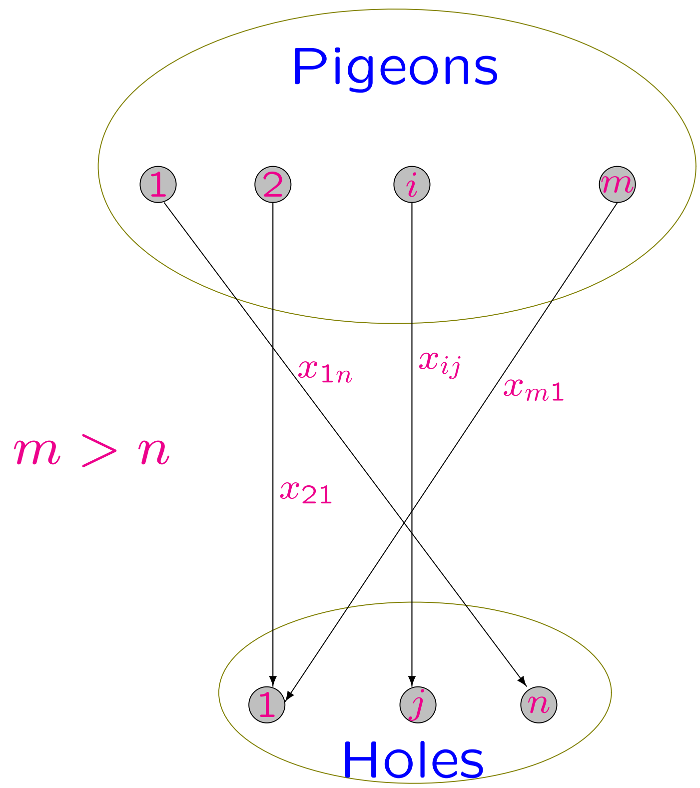
We eventually want to prove that a system of polynomial equations $f_1 = \ldots = f_m = 0$ does not have 0-1 solutions, and this holds if and only if 1 is in the ideal generated by $f_1, \ldots, f_m$ and auxiliary axioms $x_1^2 = \ldots = x_n^2 = 0$.

We try to do that according to the definition:

$$\frac{f{=}0 \qquad g{=}0}{\alpha f + \beta g{=}0} \qquad\qquad \frac{f{=}0}{f \cdot g{=}0}$$

Complexity= the maximal degree among all polynomials participating in the proof

II. Pigeonhole Principle



Definition. Pigeonhole Principle PHP^m_n is the following unsatisfiable set of clauses:

- $x_{i1} \vee \ldots \vee x_{in}$, for all pigeons i (ith pigeon flies somewhere);

- $\bar{x}_{ij} \vee \bar{x}_{i'j}$, for different pigeons i, i' and every hole j (no two pigeons fly to the same hole).

Pigeon Spectrum

m increases $\longrightarrow$ propositional proofs can use more pigeons and become more capable (principle becomes weaker) $\longrightarrow$ it is easier to prove upper bounds (construct proofs) and harder to prove lower bounds.

All results in this talk give a trade-off between the number of pigeons m and complexity... but we will stop only at the "critical" points in the spectrum

$$m = n + 1,\ 2n,\ n^2,\ \infty$$

Weak traditionally refers to the fact $m \geq 2n$.

Variations

Functional Pigeonhole Principle $fun-PHP^m_n$ – one pigeon may not split between several holes. Additional axioms: $\bar{x}_{ij} \vee \bar{x}_{ij'}$ for any pigeon i and two different holes j, j'.

Onto Pigeonhole Principle $onto-PHP^m_n$ – pigeons and holes are completely symmetric. Additional axioms: $x_{1j} \vee \ldots \vee x_{mj}$, for all holes j.

Same remark as above: the more axioms we add, the weaker is the principle, proving lower bounds is harder, and proving upper bounds is easier.

III. Results

Classical Case: $m = n + 1$

Upper Bound. [Buss 87] Frege proof system proves PHP_n^{n+1} within polynomial size.

Lower Bound. [Haken 85; Ajtai88; Beame, Impagliazzo, Krajíček, Pitassi, Pudlák, Woods 92] Every F_d-proof of $onto - PHP_n^{n+1}$ must have size $\exp(\epsilon_d \cdot n)$.

Lower Bound. [Razborov 96; Impagliazzo, Pudlák, Sgall 97] Every Polynomial Calculus proof of $fun - PHP_n^{\infty}$ must have degree $\Omega(n)$.

Upper Bound. By summing up, it is easy to see that $onto - PHP_n^{n+1}$ is easy for Polynomial Calculus.

Moderately Weak PHP: $m = 2n$ (Mystery Begins)

Upper bound. [Paris, Wilkie, Woods 88; Krajíček 00; Maciel, Pitassi, Woods 00] $F_{1.5} = R(\text{poly-log})$ proves PHP_n^{2n} within quasi-polynomial size.

Lower bound. [Buss, Turan 88] Every resolution proof of $onto - PHP_n^{2n}$ still must have size $\exp(\Omega(n))$.

Lower bound. [Atserias, Bonet, Esteban 00] Every $R(2)$-proof of $onto - PHP_n^{2n}$ must have size $\exp(n/(\log n)^{O(1)})$.

Surprising corollary. Exponential separation between $R(2)$ and $R(\text{poly-log})$.

Weak PHP: $m = \infty$

No new upper bounds.

Lower bound. [Razborov, Wigderson, Yao 97; Pitassi, Raz 00; Raz 01; Razborov 01] Every resolution proof of $fun{-}PHP_n^{n^2}$ must have size $\exp(\Omega(n/(\log n)^2))$.

Very weak PHP: $m = n^2$

Upper bound. [Buss, Pitassi 96] PHP_n^{∞} is provable in Resolution by a proof of size $\exp(O(n \log n)^{1/2})$.

Lower bound. [Raz 01; Razborov 01] Every resolution proof of $fun{-}PHP_n^{\infty}$ must have size $\exp(\Omega(n^{1/3}))$.

There still remains the gap between $1/2$ and $1/3$.

IV. Proof ideas

Why it was hard to prove this result before 2001 or Width-Size tradeoff

Let us denote by $S_R(\phi)$ the minimal number of clauses in a resolution refutation of ϕ (equivalent to the ordinary bit size).

Another complexity measure. The width $w(C)$ of a clause C is the number of literals in it. The width of a resolution proof is the maximal width of all clauses occurring in the proof. $w_R(\phi)$ – the width complexity measure.

$n(\phi)$ – the number of variables in ϕ.

Theorem. [Ben-Sasson, Wigderson 99]

$$w_R(\phi) \leq O\left(\sqrt{n(\phi) \cdot \log S_R(\phi)}\right)$$

(imprecise since the term corresponding to the width of initial clauses in ϕ is left out).

Empirical observation: all size resolution lower bounds known at that moment followed from this relation and width lower bounds (perhaps, with a little bit of extra work).

For pigeonhole principle PHP_n^m, width is equal to n and the number of variables can not be reduced below m.

For weak pigeonhole principle ($m \geq n^2$) Ben-Sasson-Wigderson relation completely fails.