Complexity of Propositional Proofs

Alexander A. Razborov

University of Chicago and

Steklov Mathematical Institute

Aisenstadt lecture #2, Montreal, October 13, 2010

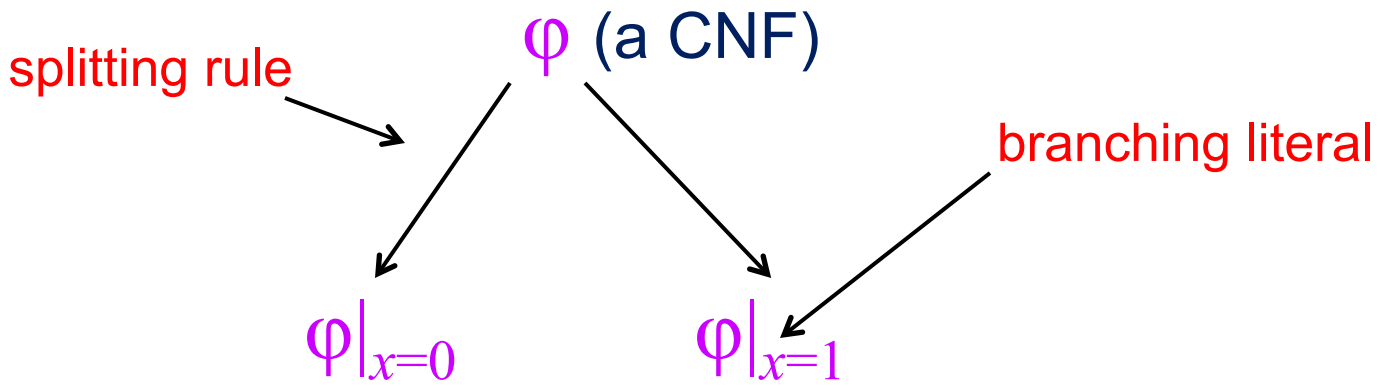
On universal character of propositional logic

- Computer Scientist: basic NP-complete problem, starting point for more interesting problems
- Logician: propositional calculus, basis for more complicated (and more interesting) calculi
- Philosopher: Aristotelian Logic which is the basis for more sophisticated (and, well, more interesting) philosophical systems

Putting it differently, propositional logic is pretty boring and shallow…

…that is, until we bring in complexity issues.

DPLL Algorithms (resolution based)



Proof Complexity:

- restrict attention to unsatisfiable instances
- study theoretical limits of theorem proving procedures

I. Framework

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

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

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.

Definition. [CR73] A propositional proof system P is p-bounded if every tautology has a proof whose length is polynomially bounded in its own length $|\phi|$.

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 membership.

Proof Complexity begins when we are interested in natural proof systems P that have clear logical meaning (proofs in the ordinary, "Aristotelian" sense).

Logical Proof Systems

- Resolution and tree-like resolution
- (bounded-depth) Frege or Extended Frege

Algebraic and Geometric Proof Systems

- Nullstellensatz and Polynomial Calculus
- Cutting Palnes
- Lovász-Schrijver type systems

Some terminology

$x_1, x_2, \ldots, x_n, \ldots$ – Boolean ($= \{0, 1\}$-valued) variables

$x_1, \neg x_1, \ldots, x_n, \neg x_n, \ldots$ – literals

$x_1 \vee \neg x_2 \vee x_5$ – clauses

$x_1 \wedge \neg x_2 \wedge x_5$ – terms

A set of clauses $C_1, \ldots, C_h$ (interpreted as their conjunction) – Conjunctive Normal Form (CNF)

A disjunction of terms $K_1 \vee \ldots \vee K_h$ – Disjunctive Normal Form (DNF).

Resolution and tree-like resolution

Want to prove DNF $\phi = K_1 \vee \ldots \vee K_m \Rightarrow$ refute (infer a contradiction) instead the set of clauses $(\neg K_1), \ldots, (\neg K_m)$.

Resolution proof system R operates with clauses and has one inference Resolution rule:

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

(Bounded-Depth) Frege Proof System

Any textbook proof system. Finitely many axiom schemes and inference rules like $A \rightarrow (A \vee B)$, $A \vee \neg A$,
$((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$,

$$\frac{A, \qquad A \rightarrow B}{B}$$ (modus ponens)

Theorem. *[Reckhow 76] Every two Frege proof systems p-simulate each other.*

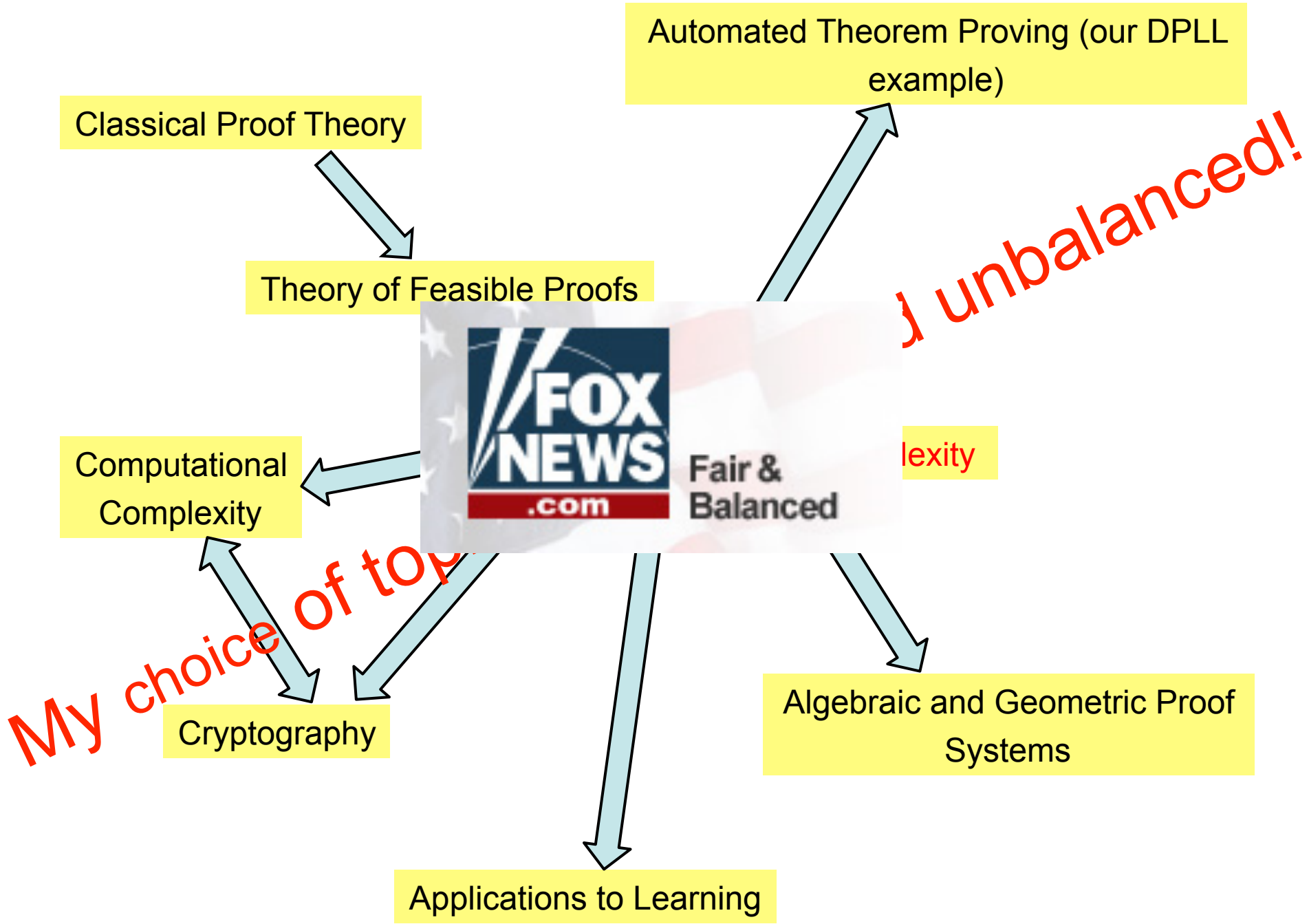
Extended Frege Proof System

Extend a Frege proof system with the following extension axioms (essentially, allow abbreviations):

$$(p_A \equiv A),$$

where p_A is a new propositional variable.

Remark. Reckhow's theorem becomes trivial for Extended Frege proof systems. Moreover, we get an equivalent system of Extended Resolution (or, for that matter, of Extended 4-Resolution).


Automated Theorem Proving (our DPLL example)
Classical Proof Theory
Theory of Feasible Proofs
unbalanced!
lexity
Computational Complexity
My choice of top
Cryptography
Algebraic and Geometric Proof Systems
Applications to Learning
FOX NEWS .com
Fair & Balanced

II. Bounded Arithmetic

- Bounded Arithmetic is a generic name for a collection of weak (well below $I\Delta_1$) arithmetical theories capturing feasible arguments
- customary look: open axioms describing non-logical symbols + schemes of limited induction (+ comprehension, collection etc. in the second-order case)
- main characteristic feature: focus on bounded quantifiers $(\exists x \le t), (\forall x \le t)$, as opposed to unbounded.

The most famous member of the family [Buss 86]

Language of S^1_2: Peano Arithmetic plus $\lfloor x/2 \rfloor$, $|x|$, $x\#y$ (smash function $2^{|x|\cdot|y|}$)

The hierarchy Σ^b_i of bounded formulae: forbid unbounded quantifiers, count bounded quantifiers $(\exists x \leq t)A(x)$, $(\forall x \leq t)A(x)$ and ignore sharply bounded quantifiers $(\exists x \leq |t|)A(x)$, $(\forall x \leq |t|)A(x)$

Axioms of S_2^1:

A set of open axioms BASIC (like Robinson's arithmetic);

$\Sigma_1^b - PIND$ induction principle:

$$A(0) \wedge (\forall x)(A(\lfloor x/2 \rfloor) \rightarrow A(x)) \rightarrow A(a),$$

where $A \in \Sigma_1^b$.

Main Witnessing Theorem [Buss 86] *If* $S^1_2 \vdash (\forall x)(\exists y)A(x,y)$, *where* $A \in \Sigma^b_1$ *then there exists a poly-time computable function* $f(x)$ *on integers such that for every* n, $\models A(n, f(n))$. *The converse is also true.*

The class of functions Σ^b_1-definable in S^1_2 =
The class of poly-time computable functions

Feasible proofs = proofs in S_2^1

Mathematical corollary: If FACTORING is hard then Fermat's little theorem is not provable in S_2^1

Fun corollary: two ways to destroy the world economy: build a Quantum Computer or prove Fermat's little theorem in S_2^1

Informal corollary: S_2^1 is precisely what you can prove in the world in which all intermediate constructions are also feasible

What about Σ_0^b-formulas?

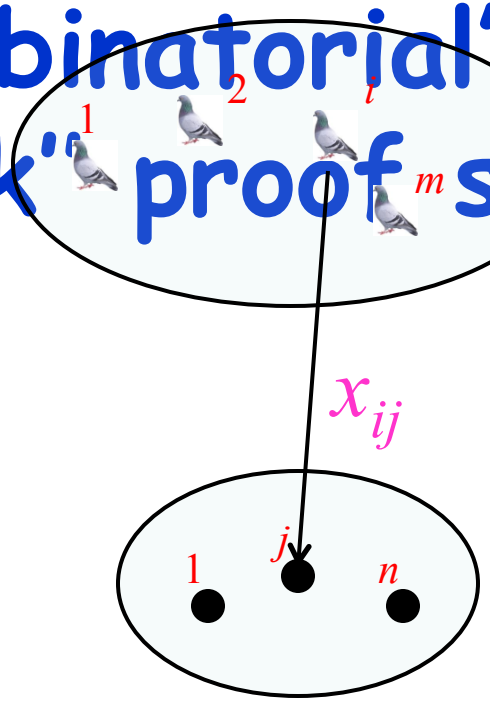
Gödel Incompleteness Theorem [Buss 86]: different versions depending on what kind of cuts is allowed.

No quantifiers to play with… very disappointing.

But this is where propositional proof complexity enters the stage.

In the nutshell: feasible (first-order) proofs $\approx$ short propositional proofs in the companion propositional system.

III. "Combinatorial" results for "weak" proof systems



Benchmark: Pigeonhole Principle PHP_n^m is the following unsatisfiable ($m > n$) 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).

m=n+1

Theorem. [Haken 85] *Every Resolution proof of* PHP_n^{n+1} *must have size* $\exp(\Omega(n))$.

Theorem. [Beame, Impagliazzio, Krajiček, Pitassi, Pudlák, Woods 92] *Every bounded-depth Frege proof of* PHP_n^{n+1} *must have size* $\exp(\Omega(n))$.

Theorem. [Buss 87] *The Frege proof system proves* PHP_n^{n+1} *within polynomial size.*

m way larger than n

Theorem. [Paris, Wilkie, Woods 88; Maciel, Pitassi, Woods 00] *Depth-2 Frege operating with* $(\log n)^{O(1)}$*-CNFs proves* PHP_n^{2n} *within quasi-polynomial* ($n^{(\log n)^{O(1)}}$) *size.*

Theorem. [Atserias, Bonet, Esteban 00; Segerlind, Buss, Impagliazzio 02; Razborov 03] The previous bound is tight.

Theorem. [Raz 01; Razborov 02] *Every Resolution proof of* PHP_n^{∞} *must have size* $\exp(\Omega(n^{1/3}))$.

Feasible Provability of P≠NP

IV. Algebraic Proof Systems (Vladimir's homework turned in)

0,1 can not only stand for FALSE and TRUTH but also can be interpreted as elements of a field!

The clause $x_1 \vee \bar{x}_2 \vee x_3$ translates to $(1 - x_1)x_2(1 - x_3) = 0$. A CNF translates into a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0,$$

and we want to prove that it does not have 0-1 solutions.

The ring

$$\Lambda_n \stackrel{\text{def}}{=} K[x_1, \ldots, x_n]/(x_i^2 - x_i | 1 \leq i \leq n)$$

of multilinear polynomials is well-known in Complexity Theory. $\text{Hom}(\Lambda_n, K)$ is precisely the set of 0-1 asignments!

By Hilbert's Nullstellensatz, the system is unsolvable if and only if there exist polynomials $Q_1, \ldots, Q_m$ such that

$$f_1 Q_1 + f_2 Q_2 + \ldots + f_m Q_m = 1 \text{ in } \Lambda_n.$$

Nullstellensatz Proof System

Just described: a proof is the set of polynomials $Q_1, \ldots, Q_m$.

An important twist: the complexity is usually mesaured by the maximal degree of $Q_1, \ldots, Q_m$.

PHP_n^m: to say that the ith pigeon flies somewhere, we say $\sum_{j=1}^{n} x_{ij} - 1 = 0$ instead of $\bigvee_{j=1}^{n} x_{ij}$.

Benchmark: Pigeonhole Principle PHP_n^m 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).

Theorem. [Beame Cook Edmonds Impagliazzo Pitassi 95] Every Nullstellensatz refutation of PHP_n^∞ must have degree $\Omega(\sqrt{n})$.

Polynomial Calculus: a dynamical version

We generate elements in the ideal $(f_1, \ldots, f_m)$ using obvious rules:

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

and keep track of the maximal degree of all polynomials occurring in the proof.

Polynomial Calculus is stronger than both Nullstellensatz and Resolution!

Theorem. [Razborov 98] Every Polynomial Calculus refutation of PHP_n^∞ must have degree $\Omega(n)$.

V. Geometric Proof Systems

The clause $x_1 \vee \bar{x}_2 \vee x_3$ translates to $x_1 + (1 - x_2) + x_3 \geq 1$. A CNF translates into a system of linear inequalities

$$f_1(x_1, \ldots, x_n) \geq 0, \ldots, f_m(x_1, \ldots, x_n) \geq 0,$$

and we want to prove that it does not have 0-1 solutions.

The clause $x_1 \vee \bar{x}_2 \vee x_3$ translates to $(1 - x_1)x_2(1 - x_3) = 0$. A CNF translates into a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0,$$

and we want to prove that it does not have 0-1 solutions.

Cutting Planes Proof System

Cutting Planes operates with statements expressible as $f(x_1, \ldots, x_n) \geq 0$, where f is a linear polynomial with integer coefficients and has obvious axioms and the following inference rules:

$$\frac{f \geq 0 \quad g \geq 0}{\alpha f + \beta g \geq 0} \qquad (\alpha, \beta \geq 0)$$

$$\frac{r \cdot f \geq a}{f \geq \lceil a/r \rceil}.$$

Sound and complete, stronger than Resolution.

Homework #2, same due date. PHP_n^m is no longer with us – it has linear (in n) size refutation in Cutting Planes.

No direct combinatorial proofs of lower bounds are known for this system.

[Bonet Pitassi Raz 95; Pudlák 97] Exponential lower bounds $\exp(n^{\Omega(1)})$ based on the material from the skipped part (and lower bounds for monotone circuits).

Lovász-Schrijver type Proof Systems

LS proof system operates with statements expressible as $f(x_1, \ldots, x_n) \geq 0$, where f is a multi-linear quadratic polynomial and has obvious axioms and the following inference rules:

$$\frac{f \geq 0 \quad g \geq 0}{\alpha f + \beta g \geq 0} \qquad (\alpha, \beta \geq 0)$$

$$\frac{f \geq 0}{f x_i \geq 0} \qquad \frac{f \geq 0}{f(1 - x_i) \geq 0}$$

as long as f is linear.

For simplicity: consider only primal feasibility problem for 0-1 programs.

$$\frac{f \geq 0 \quad g \geq 0}{\alpha f + \beta g \geq 0} \quad (\alpha, \beta \geq 0)$$

P_0 is the polytope generated by original linear constraints.

$$\frac{f \geq 0}{f x_i \geq 0} \qquad \frac{f \geq 0}{f(1 - x_i) \geq 0}$$

Lift: P_1^+ is the polytope made by all quadratic polynomials generated by these rules.

Project: P_1 is the intersection of P_1^+ with the subspace of linear polynomials.

Etc. until $P_r = \emptyset$. The minimal r is the Lovász-Schrijver rank of the original system.

Lovász-Schrijver rank = minimal proof depth in LS

Other geometric proof systems/relaxation procedures: LS_+, Sherali-Adams, Lassere… all operating with low-degree polynomial inequalities. Many upper/lower bounds are proven for depth = rank.

All these procedures are highly uneconomical and, unlike DPLL, do not try to separate ``useful'' constraints from stupid.

Size lower bounds for all these systems in the DAG model are at the moment completely out of reach.

$TH(k)$ – the proof system operating with arbitrary inequalities expressible by degree k polynomials; k is a constant.

[Beame Pitassi Segerlind 07] – exponential lower bounds for tree-like $TH(k)$ proofs modulo lower bounds for the communication complexity of the DISJOINTNESS function in the Number-on-Forehead model.

The necessary lower bounds for DISJOINTNESS were recently supplied in the breakthrough development [Lee, Shraibman 08; Chattopadhyay Ada 08].

[Beame Huynh Pitassi 10]: industrial way to construct hard tautologies (for $TH(k)$), hardness escalation.

Group-Theoretical Proof Systems??? (speculative)

What we are looking for: ways to convert a Boolean formula $\phi(x_1, \ldots, x_n)$ into a group-theoretic statement which is true iff it is satisfiable.

Attempt # 1. [Barrington Straubing Thérien McKenzie et. all] programs over finite groups and monoids. $\phi \rightarrow P_\phi$, and ϕ is unsatisfiable iff P identically computes the unit element.

Good news: locality. Bad News: not clear what is the proof system.

Attempt # 2. [Birget Olshanskii Rips Sapir 02; Krajiček 03] Dehn functions. $\phi \to w_\phi$ in a specially designed group, and ϕ is unsatisfiable iff $w_\phi = 1$.

Good news: proof system is very clean. Bad news: neither the mapping is local in any reasonable sense nor the group is quite natural.

Attempt # 3??? $\phi \to G_\phi$ such that ϕ is not satisfiable iff $G_\phi \approx 1$. Need some algebraic geometry like $\mathrm{Hom}(G, ???) \approx \{0,1\}^n$ (G is a mother group like Λ_n).

Thank you