Towards (Non-)Separations in Propositional Proof Complexity

Sam Buss
Univ. of California, San Diego

Stanford
February 27, 2014

Propositional logic:
Variables: $x, y, z, \ldots$ range over *True*/*False*.
Connectives: $\neg, \wedge, \vee, \rightarrow$ (can vary)

Decision problem: Given a propositional formula φ:
Is φ a tautology? That is, is φ valid?

Complementary decision problem: Is φ satisfiable?

These problems are NP-hard.

Proof systems: Provide proofs of validity.

Examples include: resolution, Frege, extended Frege, cutting planes proofs, nullstellensatz, polynomial calculus, ZF set theory, etc.

The **Frege proof system** $\mathcal{F}$ is a "textbook-style" propositional proof system with Modus Ponens as its only rule of inference.

Modus Ponens:

$$\frac{\varphi \qquad \varphi \to \psi}{\psi}.$$

Axiom Schemes:

$$\varphi \to \psi \to \varphi$$
$$(\varphi \to \psi) \to (\varphi \to \psi \to \chi) \to (\varphi \to \chi)$$

and 8 more axiom schemes.

Thm: $\mathcal{F}$ is (implicationally) sound and (implicationally) complete.

Thus a formula ϕ has an $\mathcal{F}$-proof iff it is valid.

Defn: The **size** of a formula is the number of symbols in the formula.
The **size** of a Frege proof is the number of symbols in the proof.

Open problem: [Reckhow'76; Cook-Reckhow'79]
Is there a polynomial $p(n)$ such that every tautology has an $\mathcal{F}$-proof of size $\le p(n)$?
That is, is $\mathcal{F}$ **polynomially bounded**?

Thm. If $\mathcal{F}$ is polynomially bounded, then NP=coNP.

Proof: To solve the coNP-complete question of whether φ is valid, nondeterministically guess an $\mathcal{F}$-proof of φ.

Defn: An **abstract proof system** is a polynomial time function f mapping $\{0,1\}^*$ *onto* the set of tautologies.
w is an f-**proof** of φ iff $f(w) = \varphi$.
The **size** of w is $|w|$, i.e. the length of w.

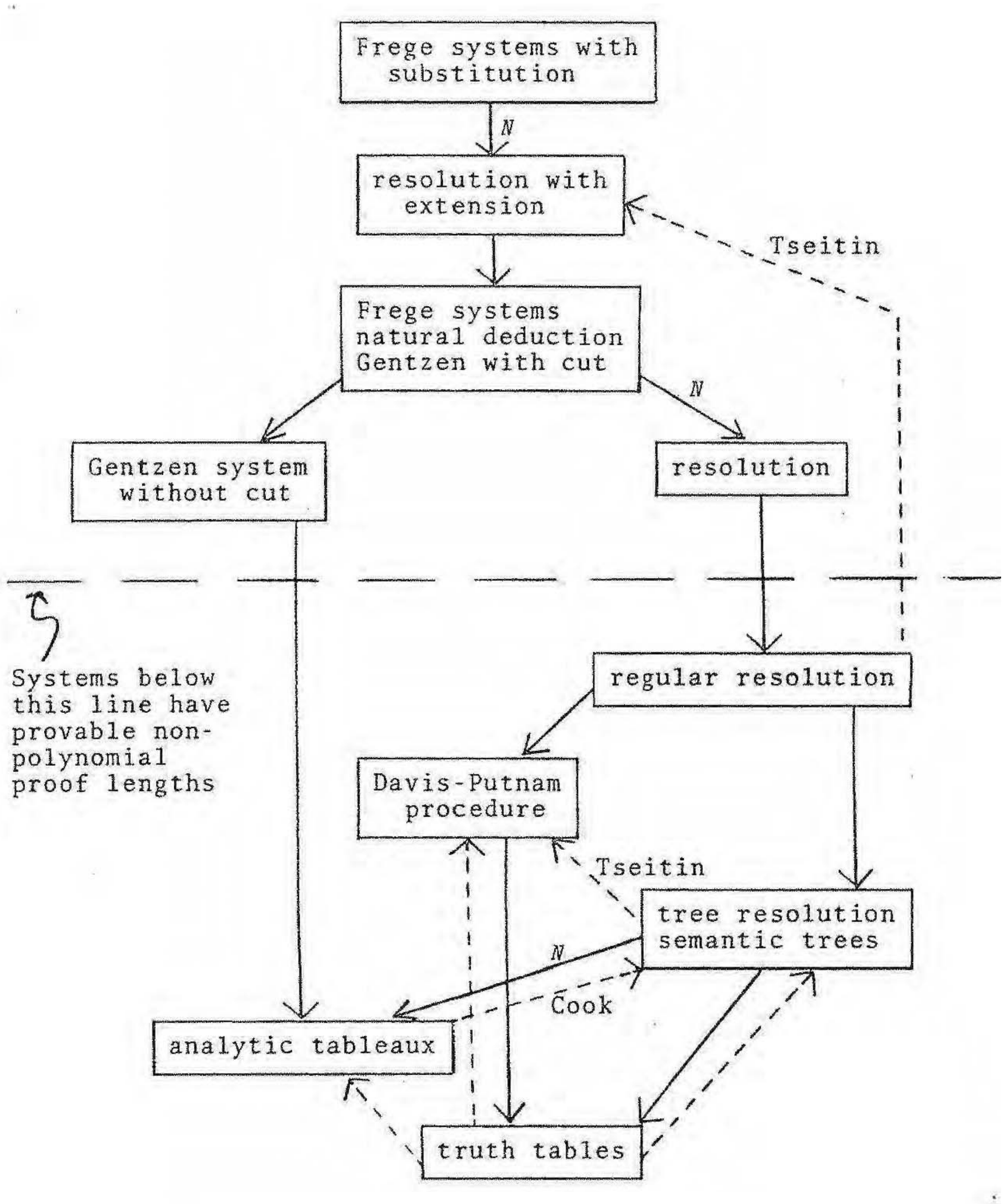
Example: For the Frege system $\mathcal{F}$:

$$f_{\mathcal{F}}(w) = \begin{cases} \text{the last line of } w & \text{if } w \text{ is an } \mathcal{F}\text{-proof} \\ (x \vee \neg x) & \text{otherwise} \end{cases}$$

Similarly very strong systems, e.g. set theory, are abstract proof systems.

Thm. [R'76, CR'79] There is a polynomially bounded abstract proof system iff $\mathrm{NP} = \mathrm{coNP}$.

Cook's Program: Approach $\mathrm{NP} \neq \mathrm{coNP}$ by showing stronger and stronger proof systems are not polynomially bounded.


Frege systems with substitution
N
resolution with extension
Tseitin
Frege systems natural deduction Gentzen with cut
N
Gentzen system without cut
resolution
Systems below this line have provable non-polynomial proof lengths
regular resolution
Davis-Putnam procedure
Tseitin
tree resolution semantic trees
N
Cook
analytic tableaux
truth tables

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.

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

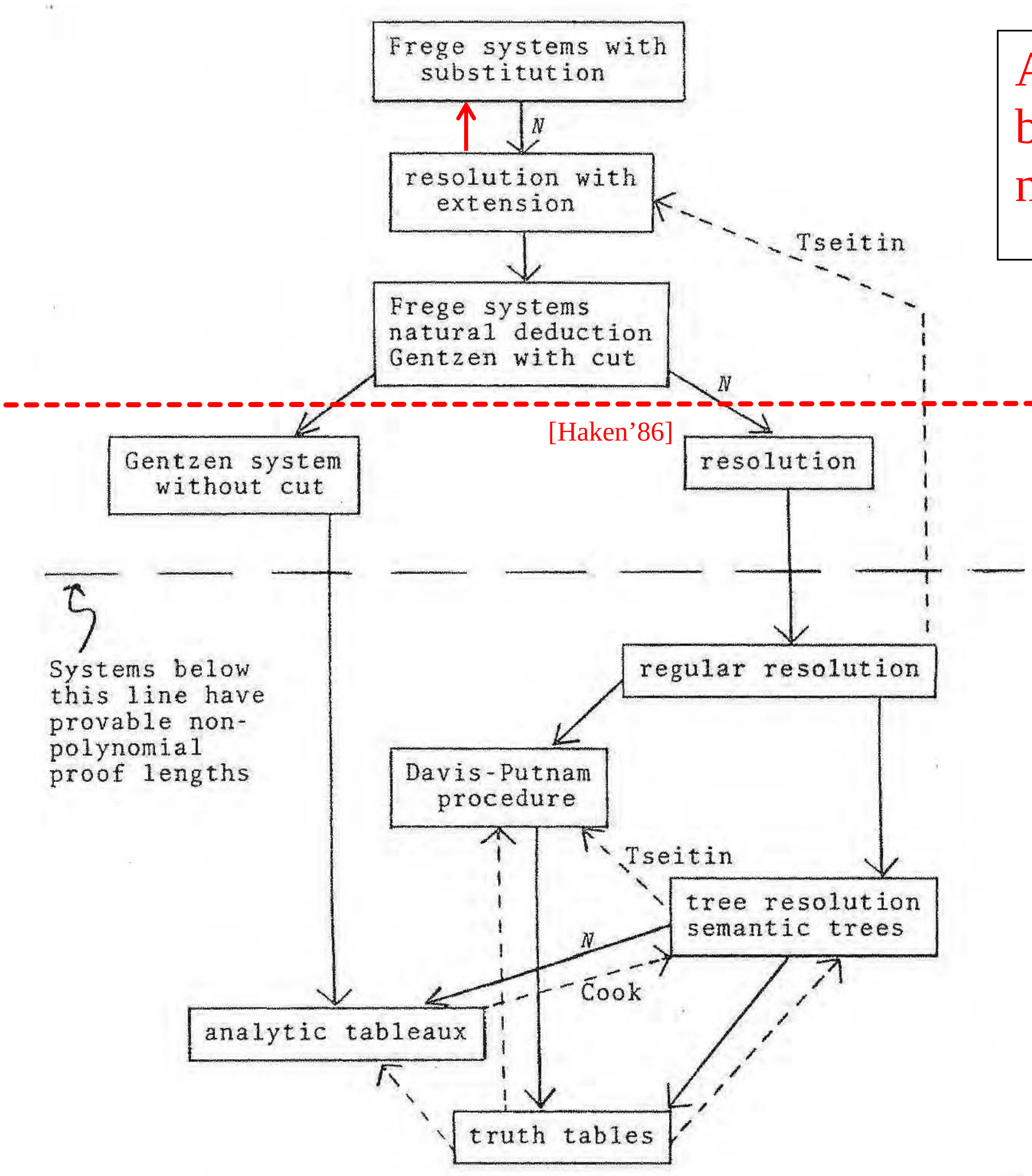
[Pudlak'97]

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]


Frege systems with substitution
N
resolution with extension
Tseitin
Frege systems natural deduction Gentzen with cut
N
[Haken'86]
Gentzen system without cut
resolution
Systems below this line have provable non-polynomial proof lengths
regular resolution
Davis-Putnam procedure
Tseitin
tree resolution semantic trees
N
Cook
analytic tableaux
truth tables

R.A. Reckhow, PhD thesis, 1975

Defn: Let f, g be abstract proof systems.
f **simulates** g if there is a polynomial $q(n)$ s.t., whenever $g(w) = \varphi$, there is a v, $|v| \le q(|w|)$ such that $f(v) = \varphi$.
f **p-simulates** g if there is a polynomial-time computable $h(w)$, such that, whenever $g(w) = \varphi$, we have $f(h(w)) = \varphi$.
f is **polynomially bounded** if, for some polynomial $q(n)$, every tautology φ has an f-proof w of size $\le q(|\varphi|)$.

1. Resolution is not polynomially bounded.
2. Regular resolution does not simulate resolution.
3. Resolution does not simulate $\mathcal{F}$.
4. It is open whether $\mathcal{F}$ is polynomially bounded.
5. It is open whether there is a maximum abstract proof system which (p-)simulates all abstract proof systems.

In most cases: the power of particular proof systems is best understood in terms of what Boolean functions are allowed as lines in the proofs:

Frege, $\mathcal{F}$: Boolean formulas.

extended Frege, $e\mathcal{F}$: Boolean circuits.

constant-depth Frege: AC^0 circuits.

constant-depth $\oplus_m$-Frege: $ACC^0[m]$-circuits.

constant-depth TC^0-Frege: TC^0-circuits.

Cutting planes: Linear inequalities over $\mathbb{N}$.

Polynomial calculus: Polynomials over a finite field.

Resolution: DNF formulas.
(Since a set of clauses is a CNF formula).

Analogy with circuit complexity: If we can separate two Boolean function classes, then we expect to separate the corresponding proof systems. (It is only an analogy: there are no theorems for this!)

Sometimes this analogy works:

Thm: Resolution does not simulate constant-depth Frege.

Thm: Constant-depth Frege does not simulate constant-depth $\oplus_m$-Frege or Frege.

Thm: Constant-depth Frege plus mod-m counting *axioms* does not simulate Frege.

Open: Does Frege (p-)simulate extended Frege?

Sometimes this analogy is unfulfilled, notably:

Open: Does constant-depth $\oplus_p$-Frege (p-)simulate Frege?.

Open: Does depth k Frege quasi-polynomially simulate depth $k+1$ Frege with respect to DNF consequences?

The above are the two most prominent “barrier” problems for propositional proof complexity. The best results to-date include:

Thm: [Impagliazzo-Krajíček'02] Depth k Frege does not polynomially simulate depth $k+1$ Frege w.r.t. DNF consquences.

Thm: [B-Kołodziejczyk-Zdanowski'??]. Constant depth k $\oplus_p$-Frege collapses (with quasipolynomial size increase) to constant depth 3 $\oplus_p$-Frege.

The theorems are proved via Bounded Arithmetic!

Extended Frege $e\mathcal{F}$ — aka Extended Resolution

Extended Frege ($e\mathcal{F}$) has modus ponens and the axioms of Frege ($\mathcal{F}$).

There are several equivalent definitions for extended Frege systems:

A. The lines in an $e\mathcal{F}$ proof are Boolean circuits (dags).

B. The lines are formulas, but proof size is measured in terms of number of lines, not number of symbols.

C. Lines are formulas, but variables may be introduced by the **extension rule**:

$$x \leftrightarrow \phi,$$

where x is a new variable, and ϕ does not involve x.

The extension rule can be used with resolution too, and **extended resolution** is equivalent to extended Frege.

[Cook-Reckhow'79] proposed the pigeonhole principle as a principle separating Frege and extended Frege:
PHP_n^{n+1} states there is no injective mapping from $[n+1]$ into $[n]$.

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

(Proof sketch on next slide.)

Thm. [Haken'86, BIKPPW'92; Raz'02; Razborov'03, & others]
PHP_n^{n+1} requires exponential size refutations.

But, with a very different proof than [CR'79] using counting:

Thm. [B'86] PHP_n^{n+1} has polynomial size Frege proofs.

Thm. [B'??] The [CR'79] $e\mathcal{F}$-proof of PHP_n^{n+1} can be formalized in $\mathcal{F}$ with a quasipolynomial size proof.

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

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

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

Use extension to introduce new variables

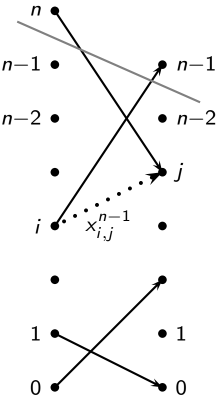
$$x_{i,j}^{\ell-1} \leftrightarrow x_{i,j}^{\ell} \vee (x_{i,\ell-1}^{\ell} \wedge x_{\ell,j}^{\ell}).$$

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 $\textsc{Php}_n^{n+1}(\vec{x})$ from $\textsc{Php}_1^2(\vec{x}^1)$. □



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

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

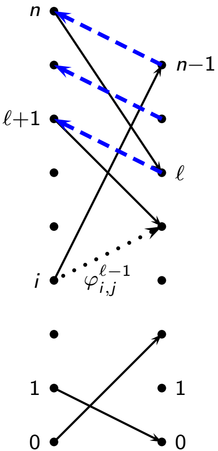
"Range node $\langle j,1\rangle$ is reachable
from domain node $\langle i,0\rangle$ in G^ℓ".

$\varphi^\ell_{i,j}$ 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 $\mathrm{PHP}_1^2(\vec{\varphi}^1)$. □



[Bonet-B-Pitassi'95] Suggested several other tautologies for separating Frege and extended Frege systems. However, these all now have been shown to have quasi-polynomial size Frege proofs:

Thm: [Hrubes-Tzameret'12] The matrix identity over $\mathbb{Z}_2$, $AB = I \Rightarrow BA = I$ (c.f. [BBP'95]) has quasi-polynomial size Frege proofs.

Proof uses an NC^2 definition of determinants, and power series approximations.

Thm. [Aisenberg-Bonet-B'??] There are quasipolynomial size Frege proofs of Frankl's Theorem (c.f. [BBP'95]): "If A is an $m \times n$ 0/1-matrix with distinct rows and $m \leq n\frac{2^t-1}{t}$, then there is some column which when deleted identifies $< t$ pairs of rows".

Proof uses an explicit (complicated) reduction to PHP.
For constant t, the proofs are polynomial size AC^0-Frege reductions to PHP.

The $t = 2, 3$ cases were proved by [BBP'95] and [Nozaki-Arai-Arai'08].

Thus, we have no concrete tautologies conjectured to super-quasipolynomially separate Frege and extended Frege, except for partial consistency statements for $e\mathcal{F}$.

In contrast, we have many decision problems conjectured to separate Boolean formulas and Boolean circuits.

Is it reasonable to conjecture a quasipolynomial simulation?

Resolution is a refutation system for sets of clauses (CNF formulas). The only rule is **resolution**:

$$\frac{C, x \qquad D, \overline{x}}{C, D}$$

A refutation is **regular** if no variable is resolved on twice on any path through the resolution dag. [Tseitin'68].

Resolution is known to be weak, in that it does not p-simulate Frege, but it supports efficient proof search and (fragments of) resolution have proved to be very powerful for SAT solvers which use *Conflict Driven Clause Learning (CDCL)* (also known as "DPLL with clause learning").

Remarkably, SAT solvers are able to routinely solve industrial instances of SAT with 100,000's variables or more!

CDCL / DPLL with clause learning (and no restarts)

CDCL: implements a depth first search:
Input: A set Γ of clauses.

Loop: (maintaining a partial truth assignment τ)

1. Use unit propagation to set variables until either
   - · some clause is falsified (a "conflict"), or
   - · no unit clauses remain in $\Gamma{\upharpoonright}\tau$.

   If a conflict is found, *learn one or more clauses* using resolution based on the unit propagations leading to the conflict.
   Then backtrack (unset variables) until no conflict remains.

3. Choose an unset literal x, and set $\tau(x) = \mathit{True}$.

Learned clauses are always falsified by the current assignment τ.

Implementations of CDCL benefit greatly from restarts, but in this talk we mostly do not allow restarts.

A proof system for CDCL

Def'n: A **pool resolution** proof is a resolution proof that (a) has a depth-first, regular traversal, and (b) admits a degenerate resolution rule that combines resolution and weakening.

Thm. [Van Gelder'05] CDCL refutations (without restarts) can be simulated by pool resolution.

Proof idea: A CDCL refutation corresponds directly to a depth-first traversal of a refutation. The traversal is regular since variables do not switch values except after backtracks. Clauses are learned as they are traversed. □

(Remark: A sharpened system RegWRTI with more restrictions on learning exactly characterizes non-greedy CDCL without restarts [B-Hoffmann-Johannsen'08].)

Open question: Is there a superpolynomial, or exponential, separation of pool resolution (or RegWRTI) and resolution.

Does CDCL without restarts polynomially simulate resolution?

Thm: [Beame-Kautz-Sabharwal'04; Atserias-Fichte-Thurley'11; Pipatsrisawat-Darwiche'11]
CDCL with restarts simulates resolution.

Thm: [Goerdt'92; Alekhnovich-Johannsen-Pitassi-Urquhart'07; Urquhart'11] Regular resolution does not simulate resolution.

[AJPU'07,U'11] proved the separation using modified ("guarded") graph tautologies and pebbling principles, and using a "Stone" principle. All three principles are based on well-foundedness conditions in directed acyclic graphs.

For several years, it was conjectured that these tautologies may also separate CDCL with restarts from resolution....

CDCL versus resolution

Thm: [Bonet-B'12, Bonet-B-Johannsen'14,B-Kołodziejczyk'??]
The guarded pebbling tautologies, the guarded graph tautologies, and the Stone principles of [AJPU'07,U'11] all have polynomial size refutations in pool resolution (and RegWRTI).

[BBJ'14] also give explicit greedy CDCL refutations (without restarts) for the guarded graph tautologies.

Thus, we have no conjectured examples for separating resolution from CDCL without restarts, or from RegWRTI.

On the other hand, no subexponential size simulation of resolution by CDCL without restarts has been found.

Conjecture: (?) No such simulation is possible.

Open problems / Challenges

- Resolve the “barrier” questions.
- Candidates for separating $\mathcal{F}$ and $e\mathcal{F}$.
- Better linkage of theory and practice of SAT solvers.
- Augment CDCL to incorporate extension. (Advantageously!)

Thank you!

Some survey articles:

- S. Buss, “Towards NP-P via Proof Complexity and Search”, Annals of Pure and Applied Logic 163, 7 (2012) 906-917.
- S. Buss, “Propositional Proof Complexity: An Introduction”, In Computational Logic, edited by U. Berger and H. Schwichtenberg, Springer-Verlag, Berlin, 1999, pp. 127-178.
- P. Beame and T. Pitassi, “Propositional Proof Complexity: Past, Present and Future”, In Current Trends in Theoretical Computer Science Entering the 21st Century, World Scientific, 2001, pp. 42-70.
- P. Beame with A. Sabharwal, “Propositional Proof Complexity”, In Computational Complexity Theory, IAS/Park City Clay Mathematics Series 10, 2000, pp. 199-246.
- P. Pudlák, “Twelve problems in proof complexity”, In Proc. 3rd International Computer Science Symposium in Russia, CSR 2008, pp.13-27
- N.Segerlind, “The Complexity of Propositional Proofs”, Bulletin of Symbolic Logic 13 (2007) 417-481.