On Extended Frege Proofs

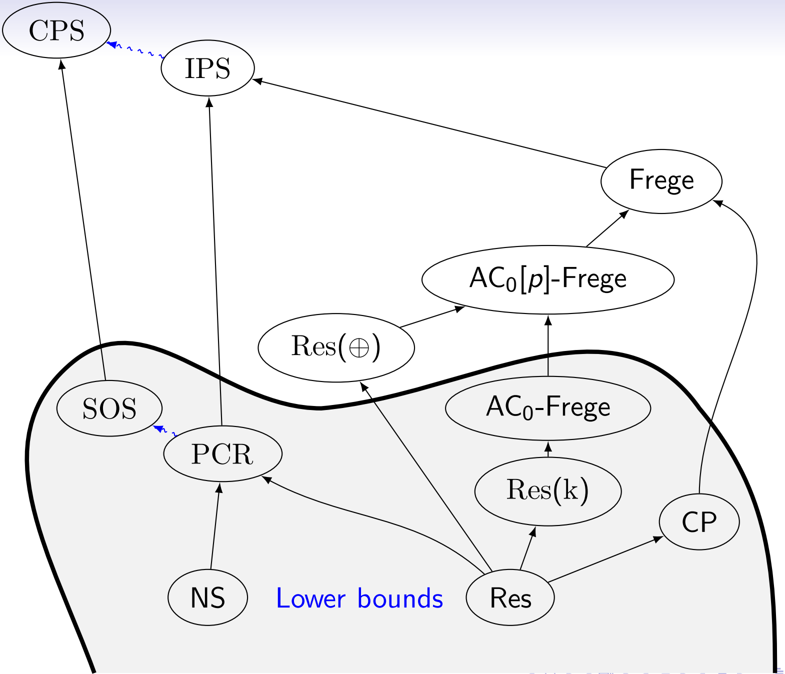
–

On the Occasion of Toni Pitassi's 60^{th} Birthday

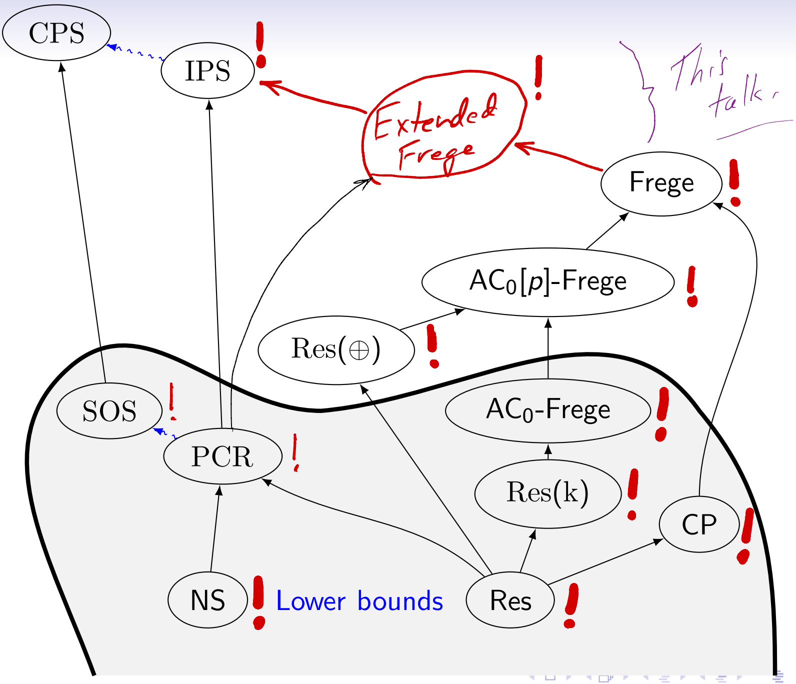
Sam Buss

ToniCS 2023

Simons Institute for the Theory of Computing
March 28, 2023



CPS
IPS
Frege
$AC_0[p]$-Frege
Res(⊕)
SOS
AC_0-Frege
PCR
Res(k)
CP
NS
Lower bounds
Res



CPS
IPS
Extended Frege
This talk.
Frege
AC0[p]-Frege
Res(⊕)
SOS
AC0-Frege
PCR
Res(k)
CP
NS
Lower bounds
Res

Frege proofs - Lines are Boolean formulas, using propositional connectives, $\wedge, \vee, \rightarrow, \neg, \ldots$.

Modus Ponens

$$\frac{A \quad A \rightarrow B}{B}$$

only rule of inference

Extended Frege Proofs - Add the extension rule

$p \leftrightarrow A$ for p a <u>new</u> variable.

Lines in an extended Frege proof can be viewed as Boolean <u>circuits</u>.

in: Automation of Reasoning 2, J. Siekmann + G. Wrightson
Springer-Verlag 1983

On the Complexity of Derivation in Propositional Calculus

G. S. Tseitin

Tseitin [1966]: Introduced extended Frege (eF) proofs.

Rules: Resolution rule ("annihilation" rule)
& Extension rule.

Exponential lower bounds on tree-like resolution & regular resolution, using the "Tseitin principle" for grid graphs.

S. Cook & R. Reckhow: - [1974, 1975, 1976, 1979]

R. Statman - [1976]

⓪ The "Cook" program for $NP \neq coNP$

① Reformulation of extended Resolution as extended Frege

② Choice of propositional language makes only polynomial difference to length of eF-proofs.

③ The PV-provable formulas have poly-size extended Frege proofs

④ $e\mathcal{F}$ is the strongest propositional proof system for which PV can prove consistency.

⑤ $e\mathcal{F}$-proof size $\approx_p$ $\mathcal{F}$-proof # of lines

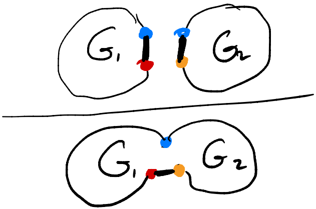
⑥ Polynomial size proofs of the pigeonhole principle (PHP)

and more....

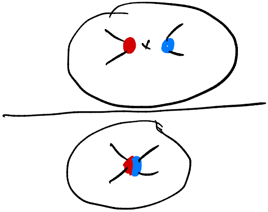
Hajós Calculus — T. Pitassi & A. Urquhart [1992, 1995]

- Hajós Calculus (HC) - a non-deterministic procedure for generating graphs which are not 3-colorable.
- Generation Rules. (1) K_4 is not 3-colorable.

(2) Join rule



(3) Contraction Rule



(4) Weakening rule - add vertices & edges.

- Def'n $HC^- := HC \setminus (3)$ is implicationally sound & implicationally complete (HC is not implicationally sound)

Theorem [Pitassi-Urquhart]. The Hajos calculus HC is polynomially equivalent to extended Frege (eF).
- This is for formulas expressing 3-colorability.

Theorem [Pitassi-Urquhart]. The $HC^- := HC \setminus (3)$ is implicationally complete and is p-simulated by the depth 5 Frege system.

Corollary HC^- requires exponential size derivations

Proof: uses the superpolynomial/exponential lower bounds for constant-depth Frege proofs of Ajtai [1988], Pitassi-Beame-Impagliazzo [1991] Krajicek-Pudlák-Woods [1991].

Theorem [Iwama-Pitassi, 1995]: Tree-like Hajos calculus requires exponential size proofs.

The Hajos Calculus proofs used the fact that

Frege + 0/1 substitution rule $\equiv_p$ extended Frege.

Substitution Rule

$$\frac{\varphi(\cdots x \cdots)}{\varphi(\cdots \psi \cdots)}$$

(Substitute formula ψ for variable x).

Known results include

(1) $e\mathcal{F} \equiv_p s\mathcal{F}$ [Cook-Reckhow, Dowd, Krajíček-Pudlák]

(2) $e\mathcal{F} \equiv_p \mathcal{F}$ + 0/1-substitution [B]

(3) $e\mathcal{F} \equiv_p \mathcal{F}$ + variable-substitution ["]

Open Does $\mathcal{F}$ + variable permutation p-simulate $e\mathcal{F}$?

Actually: Does the Frege proof system ($\mathcal{F}$) simulate extended Frege ($e\mathcal{F}$)???

Bonet-B-Pitassi [1995] examined the lack of plausible separating examples:

It is known that $\mathcal{F}$ simulates $e\mathcal{F}$ iff

$$\mathcal{F} \vdash^{poly} Con_n(e\mathcal{F}) \qquad [Cook]$$

where $Con_n(e\mathcal{F})$ are the partial (finitary) propositional formulations of "$e\mathcal{F}$ is consistent".

But what about combinatorial examples?

Bonet - B - Pitassi - candidates -

Already known:

- PHP - poly size proofs in $\mathcal{F}$ and $e\mathcal{F}$. [Cook-Reckhow, B]
- Ramsey - poly size proofs in $\mathcal{F}$ and $e\mathcal{F}$ [Pudlák]

New suggestions

- Odd-Town Theorem
- Graham-Pollack Theorem
- Fisher Inequality
- Ray-Chauduri-Wilson
- Boolean: $AB = I \Rightarrow BA = I$ [Cook]

Poly size $e\mathcal{F}$ proofs

Linear algebra proofs and $DET \in NC^2$: conjectured they have quasipoly size $\mathcal{F}$-proofs

- Frankl's Theorem

- Poly size $e\mathcal{F}$-proofs, no poly-size $\mathcal{F}$-proof known at that time

- Bondy's Theorem
- Kruskal-Katona Theorem

Examples shown to have poly-size $\mathcal{F}$-proofs.

Subsequent suggestions

- Boolean: $AB = I \Rightarrow BA = I$ [Cook]
- Kneser-Lovasz [Istrate-Craciun]
- Truncated Tucker Lemma
- Local Improvement Principles [Kołodziejczyk-Nguyen-Thapen]

Disappointing (?) Outcomes

- All of the linear algebra based examples have quasi-poly size $\mathcal{F}$-proofs [Hrubes-Tzameret; Cook-Tzameret]
- Frankl's theorem - poly size $\mathcal{F}$-proofs [Aisenberg-Bonet-B]
- Kneser-Lovasz, Tucker also. [Aisenberg-B-Gracian-Istrate]
- Many Local Improvement principles - have poly-size $\mathcal{F}$-proofs [Beckmann-B]

A few cases of the Tucker lemma & RLI_1 remain that have poly-size $e\mathcal{F}$-proof and are not known to have (quasi-)poly size Frege proofs.

PHP - Original proof of Cook-Reckhow can be carried out with quasi-poly size $\mathcal{F}$-proofs. [B, 2015]

Summary: We believe $e\mathcal{F}$ to be stronger than $\mathcal{F}$, but lack candidate separating principles!

More Results on $e\mathcal{F}$

Theorem [Krajíček] - Tree-like $e\mathcal{F}$ is polynomially equivalent to (non-tree-like) $e\mathcal{F}$.

Theorem [Krajíček-Pudlák, 1990]

Extended Frege ($e\mathcal{F}$) is equivalent to Tree-Like G_1

G_1 - Propositional Sequent Calculus for quantified propositional logic, restricted to purely existential quantified propositional logic.

(Also: Close connection to bounded arithmetic S_2^1)

Theorem [Avigad 1997]

Gives a family of "plausibly hard" combinatorial tautologies $T(n)$ which are equivalent to $\mathrm{Con}_n(e\mathcal{F})$.

So
$$\mathcal{F} + \{T(n)\} \equiv e\mathcal{F}.$$

Two Conditional Hardness Results

(A) Theorem [Krajíček-Pudlák, 1995].

If RSA is cryptographically secure, extended Frege does not have feasible interpolation.

Theorem [Bonet-Pitassi-Raz, 2000]

If integer factorization is hard (for Blum integers), then (extended) Frege and TC^0-Frege do not have feasible interpolation.

These results block some of our known lower bounds methods.

(B) <u>Theorem</u> [Alekhnovich - B - Moran - Pitassi, 2001]

If $P \neq NP$, then there is no poly time algorithm that approximates the length of the shortest Q-proof within a factor of $2^{(\log n)^{1-\varepsilon}}$.

For $Q :=$ extended Frege or Frege, resolution, Horn resolution, polynomial calculus, etc.

(Reduction to Minimum Monotone Satisfying Assignment. [Dinur]

CDCL Proof Logging Proof Systems

CDCL solvers use non-implicational ("without loss of generality") reasoning.

Several proof systems can be used for proof logging to verify the correctness of "UNSAT" answers.

This includes proof systems such as

BC, RAT, PR, SPR, SR & the clause deletion versions DBC, DRAT, ...

Theorem: [Kullman; Kiesl-RebardoPardo-Huele; also B-Thapen; & Biere, Hunt, Wetzler..]

The above proof systems are polynomially equivalent to extended Frege.

The Ideal Proof System (IPS) - [Grochow-Pitassi 2018]

A static algebraic proof system. An IPS proof is an algebraic circuit C such that

$$C(x_1, \ldots x_n, 0, \ldots, 0) = 0$$

$$C(x_1, \ldots x_n, F_1(\vec{x}), \ldots, F_m(\vec{x})) = 1$$

with a randomized polytime verification algorithm (based on PIT)

PIT := "Polynomial Identity Testing"

Theorem: IPS polynomially simulates eF.

Theorem: If $e\mathcal{F}$ proves the Grochow-Pitassi PIT axioms for (some) poly-size Boolean circuits K, then $e\mathcal{F}$ is polynomially equivalent to IPS.

PIT axioms for a Boolean circuit $K(z_1, .. z_n)$

Let $z_1 .. z_n$ encode an algebraic circuit C.

The PIT axioms state some simple properties about $K(\underline{C})$. Intent is $K(C)$ holds if C evaluates to the zero polynomial

PIT axioms, loosely speaking:

- Substitution into 0: $K(\underline{C}(x)) \Rightarrow K(\underline{C(p)})$
- $\neg K(\underline{C}) \vee \neg K(\underline{1-C})$ i.e. $1-0 \neq 0$
- Substituting 0 for 0: $K(\underline{C(\vec{x},0)}) \wedge K(\underline{G}) \Rightarrow K(\underline{C(\vec{x},G)})$
- Permuting variables: $K(\underline{C(\vec{x})}) \Rightarrow K(\underline{C(\pi(\vec{x}))})$

Theorem If IPS is not polynomially bounded then $VP \neq VNP$. I.e., the permanent does not poly-size algebraic circuits.

Defn VP :: polysize polynomials
VNP :: exponential sum of polysize polynomials

Corollary: Suppose $e\mathcal{F}$ has polysize proofs of the PIT axioms for (some) polysize Boolean circuits K. If $e\mathcal{F}$ is not polynomially bounded, then $VP \neq VNP$.

(Similar results apply to Frege & other systems.)

Grochow-Pitassi: This may explain why lower bounds for $e\mathcal{F}$ are hard to obtain.

Namely, under plausible PIT-axiom assumptions, lower bounds on $e\mathcal{F}$ would resolve the VP/VNP/permanent problem.

Happy 60th!

Toni!

By Ed G2s - own work - CC-by-SA 3.0, 3 Feb 2005