Working with Toni in Algebraic Proof Complexity

[ToniCS: Celebrating the Contributions & Influence of Toniann Pitassi]
March 2023

Joshua A. Grochow

University of Colorado **Boulder**

Proof Complexity

Something I like about proof complexity: gives a way of measuring the complexity of individual instances of SAT

Proof Complexity

Something I like about proof complexity: gives a way of measuring the complexity of individual instances of SAT

Unsaid: but actually, coming from computational/circuit complexity, I had a really hard time understanding and getting into proof complexity!

Why I Find
Proof Complexity Too Hard

Too finicky about proofs:

What do you mean the Pigeonhole Principle and the *Onto*-Pigeonhole Principle aren't just *obviously* equivalent?

Why should it matter whether I encode the pigeonhole principle using $\sum_j x_{ij} \geq 1$ or $\prod_j (x_{ij} - 1) = 0$? *It's the same principle!*

Why I Find
Proof Complexity Too Hard

Too syntactic:

"AC^0-Frege"? Where every line is an AC^0 formula?
But as a function, every line is just "1".

$$\cfrac{\cfrac{\neg x \vee (x \wedge \neg y) \vee y}{\neg y \vee y}}{1} \qquad\qquad \cfrac{\cfrac{1}{1}}{1}$$

Enter Toni

2012-2014: I did a postdoc at U. Toronto.

Toni Built This Community!

Toni's Grad Students
Ian Mertz
Noah Fleming
David Madras
Elliot Creager
Morgan Shirley
Alex Emonds
Yasaman Mahdaviyeh
Robert Robere
Venkatesh Medabalimi
Mika Göös
Nick Spooner
David Liu
Wu Yu
Yuval Filmus
Lila Fontes
Siavosh Benabbas
Frank Vanderzwet
Konstantinos Georgiou
Natan Dubitski
Lei Huang
Matei David
Siu Man Chan
Philipp Hertel
Alex Hertel
Paul McCabe
Daniel Zabwawa
Frank Pok Man Chu
Dennis Kao
Daniel Ivan
Alan Skelley
Josh Buresh-Oppenheim
Tsuyoshi Morioka
Stephanie Horn
Shannon Dalmao
Barbara Kauffmann

Toni's Postdocs
Rafael Oliveira
Denis Pankratov
Siu Man Chan
Thomas Watson
Josh Grochow
Rotem Oshman
Per Austrin
Arkadev Chattopadhyay
Rahul Santhanam
Iannis Tourlakis
Klaus Aehlig
Philipp Woelfel
Evangelos Markakis
Emil Jerabek
Marcus Latte
Neil Thapen
Shlomo Hoory
Avner Magen
Tasos Viglas
Nicola Galesi
Alexis Maciel

Enter Toni

2012-2014: I did a postdoc at U. Toronto.

Technically under Allan Borodin. But Toni met with me (almost) every week, often for 2 hours

Enter Toni

2012-2014: I did a postdoc at U. Toronto.

Technically under Allan Borodin. But Toni met with me (almost) every week, often for 2 hours

She tricked me! “Let’s just talk; you teach me something about algebraic circuits, I’ll teach you something about proof complexity, and we’ll see if we can come up with something to work on”

A Very Toni View On Frege Systems

Bounded depth Frege = Frege where there's a constant d s.t. proofs only ever uses the cut rule on formulas of depth d.

Similarly for C-Frege for any syntactically-defined circuit class C.

Okay, that made some sense to me!

Algebraic Proof Complexity

Lines are of the form “f=0” (f a polynomial)

Various complexity measures:

- Max degree per line
- Total number of monomials
- Number of lines

Coming from algebraic circuit complexity: how to prove a lower bound on this? What polynomial even to prove bounds on (every proof has lots of lines)? It looks like a mess!

The Ideal Proof System [P96, P98, GP14]

Input: An unsatisfiable system of polynomial equations

$$F_1(\vec{x}) = F_2(\vec{x}) = \cdots = F_k(\vec{x}) = 0$$

Hilbert's Nullstellensatz: $F_1 = F_2 = \cdots = F_k = 0$ has no solutions if and only if there are polynomials $G_1, \ldots, G_k$ such that

$$F_1 G_1 + F_2 G_2 + \cdots + F_k G_k = 1.$$

Introduce new place-holder variables $y_1, \ldots, y_k$, get a new polynomial

$$C(y_1, \ldots, y_k, \vec{x}) = y_1 G_1(\vec{x}) + \cdots + y_k G_k(\vec{x})$$

The Ideal Proof System [P96, P98, GP14]

Definition [GP14]: $C(\vec{y}, \vec{x})$ is an IPS **certificate** if

1. $C\left(\overrightarrow{F(\vec{x})}, \vec{x}\right) = 1$
2. $C(\vec{y}, \vec{x}) \in \langle y_1, \ldots, y_k \rangle$ (ideal in $F[y_1, \ldots, y_k, x_1, \ldots, x_n]$)

Definition: The **IPS complexity** of an unsatisfiable system of equations is the optimum function complexity of any certificate.

E.g. algebraic circuit size, formula size, VNP, …

Default: algebraic circuit size *(no degree bound!)*

Our First Work Together

July 2013: earliest email I could find with a draft of our Ideal Proof System paper

Our First Work Together

- July 2013: earliest email I could find with a draft of our Ideal Proof System paper
- Feb , 2014: Gave a talk at Rutgers on it. Called it "our algebraic proof system", listed "find a better name" as the most important open question.

Our First Work Together

July 2013: earliest email I could find with a draft of our Ideal Proof System paper

Feb , 2014: Gave a talk at Rutgers on it. Called it "our algebraic proof system", listed "find a better name" as the most important open question.

Eric Allender:

(1) Suggests the name "Ideal Proof System" (thanks Eric!)

(2) Asks "If PIT is EF-provably easy, *then* does EF p-simulate IPS?" (Also Andy Drucker.) Turns out yes!

Our First Work Together

July 2013: earliest email I could find with a draft of our Ideal Proof System paper

Feb **19**, 2014: Gave a talk at Rutgers on it. Called it “our algebraic proof system”, listed “find a better name” as the most important open question.

Eric Allender:

(1) Suggests the name “Ideal Proof System” (thanks Eric!)

(2) Asks “If PIT is EF-provably easy, *then* does EF p-simulate IPS?” (Also Andy Drucker.) Turns out yes!

Our First Work Together

July 2013: earliest email I could find with a draft of our Ideal Proof System paper

Feb 19, 2014: Gave a talk at Rutgers on it. Called it "our algebraic proof system", listed "find a better name" as the most important open question.

Eric Allender:

(1) Suggests the name "Ideal Proof System" (thanks Eric!)

(2) Asks "If PIT is EF-provably easy, *then* does EF p-simulate IPS?" (Also Andy Drucker.) Turns out yes!

April 2, 2014 : submitted to FOCS

Our First Work Together

July 2013: earliest email I could find with a draft of our Ideal Proof System paper

Feb 19, 2014: Gave a talk at Rutgers on it. Called it “our algebraic proof system”, listed “find a better name” as the most important open question.

Eric Allender:

(1) Suggests the name “Ideal Proof System” (thanks Eric!)

(2) Asks “If PIT is EF-provably easy, *then* does EF p-simulate IPS?” (Also Andy Drucker.) Turns out yes!

April 2, 2014 **4:29pm**: submitted to FOCS

Our First Work Together

July 2013: earliest email I could find with a draft of our Ideal Proof System paper

Feb 19, 2014: Gave a talk at Rutgers on it. Called it “our algebraic proof system”, listed “find a better name” as the most important open question.

Eric Allender:

(1) Suggests the name “Ideal Proof System” (thanks Eric!)

(2) Asks if “PIT is EF-provably easy, *then* does EF p-simulate IPS?” Turns out yes!

April 2, 2014 **4:29pm**: submitted to FOCS

Follow-up work on the Ideal Proof System

[Forbes-Shpilka-Tzameret-Wigderson ’16]: Lower bounds on C-IPS for small circuit classes C, by “powering up” algebraic circuit lower bounds

[Li-Tzameret-Wang ‘15]: Characterize ordinary Frege (up to quasipoly) by noncommutative formula IPS (follows our/Allender’s suggestion to show that PIT for this class is Frege-provable)

[Alekseev-Grigoriev-Hirsch-Tzameret ‘19]: “Cone proof system”, analogue of IPS for semi-algebraic proofs, connection w/ τ Conjecture

Additional works: [ST21], [AF21], [GHT22], [G**P**??]

Back to Pitassi ’96/’98

[P96]: Introduced considering algebraic circuit size of the Nullstellensatz certificates. (“Hilbert-like IPS” or “IPS_{LIN}”, proved equivalent to IPS [FSTW16])

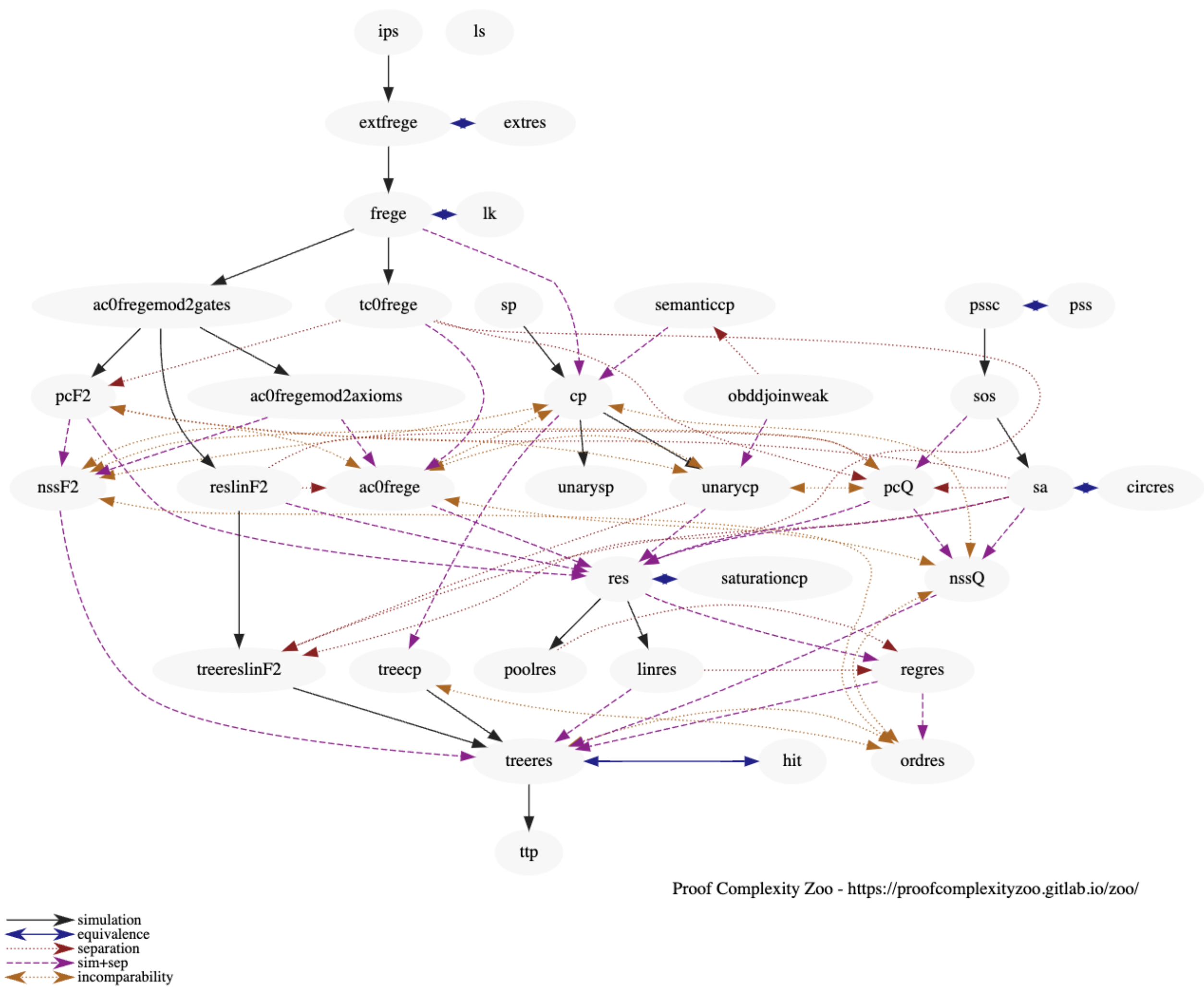
[P98]: Number of lines in PC, represent each line however* you want. (Proved equivalent to det-IPS [GP14].)

Back to Pitassi '96/'98

Toni's questions [P96] eventually resolved:

1. Close the $O(n)$ vs $\Omega(\sqrt{n})$ gap for PC degree for PHP. **[R98]**
2. Is $\Theta(\sqrt{n})$ the right bound for PHP_n^m with m large? **No. [R98]**
3. Nullstellensatz degree lower bound on random 3CNF? **[BI99]**
4. Does Extended Frege p-simulate IPS? **Implies PIT in NP [G '23]**
5. Tighten degree bound on simulation of Resolution by PC. **?**
6. Is Cutting Planes p-simulated by PC in sublinear degree? **Incomparable.**

Proof Complexity Zoo [Vinyals]



Proof Complexity Zoo [Vinyals]

All about Cutting Planes

Proof Systems

- Cutting Planes stronger than Resolution
  - Source: cp → unarycp → res
  - Source: cp → unarycp → php → pcQ_ → res_
- Cutting Planes stronger than Truth table
  - Source: cp → treecp → treeres → ttp
  - Source: cp → unarycp → php → treereslinF2_ → treeres_ → ttp_
- Cutting Planes stronger than Tree-like resolution
  - Source: cp → treecp → treeres
  - Source: cp → unarycp → php → treereslinF2_ → treeres_
- Cutting Planes stronger than Regular resolution
  - Source: cp → unarycp → res → regres
  - Source: cp → unarycp → php → pcQ_ → res_ → regres_
- Cutting Planes stronger than Ordered resolution
  - Source: cp → unarycp → res → regres → ordres
  - Source: cp → unarycp → res → regres → pearl → ordres_
- Cutting Planes stronger than Pool resolution
  - Source: cp → unarycp → res → poolres
  - Source: cp → unarycp → php → pcQ_ → res_ → poolres_
- Cutting Planes stronger than Linear resolution
  - Source: cp → unarycp → res → linres
  - Source: cp → unarycp → php → pcQ_ → res_ → linres_
- Cutting Planes stronger than Tree-like Cutting Planes
  - Source: [subsystem]
  - Source: cp → unarycp → res → regres → ordres → peb+ind → treecp_
- Cutting Planes simulates Cutting Planes with Unary Coefficients
  - Source: [subsystem]
- Cutting Planes weaker than Semantic Cutting Planes
  - Source: [subsystem]
  - Source: semanticcp → cliquecolouringeq → cp_
- Cutting Planes stronger than Cutting Planes with Saturation
  - Source: cp → unarycp → res → saturationcp
  - Source: cp → unarycp → php → pcQ_ → res_ → saturationcp_
- Cutting Planes simulated by Stabbing Planes
  - Source: [citation needed]
- Cutting Planes simulates Stabbing Planes with Unary Coefficients
  - Source: FGIPRTW21 On the Power and Limitations of Branch and Cut.
- Cutting Planes incomparable wrt Polynomial Calculus over $\mathbb{F}_2$
  - Source: cp → unarycp → php → pcF2_
  - Source: pcF2 → nssF2 → ts+ind → cp_
- Cutting Planes incomparable wrt Nullstellensatz over $\mathbb{F}_2$
  - Source: cp → unarycp → php → pcF2_ → nssF2_
  - Source: nssF2 → ts+ind → cp_
- Cutting Planes [missing?] ResLin over $\mathbb{F}$

Back to Pitassi ’96/’98

Toni’s questions eventually resolved:

1. Close the $O(n)$ vs $\Omega(\sqrt{n})$ gap for PC degree for PHP. **[R98]**
2. Is $\Theta(\sqrt{n})$ the right bound for PHP_n^m with m large? **No. [R98]**
3. Nullstellensatz degree lower bound on random 3CNF? **[BI99]**
4. Does Extended Frege p-simulate IPS? **Implies PIT in NP [G ‘23]**
5. Tighten degree bound on simulation of Resolution by PC. **?**
6. Is Cutting Planes p-simulated by PC in sublinear degree? **Incomparable.**
7. [P98] Relationship between degree and number of monomials? **[Impagliazzo-Pudlák-Sgall ‘99, …, Lagarde-Nordström-Sokolov-Swernofsky ‘20]**

Back to Pitassi ’96/’98

Toni’s questions from P96 still open:

1. Does poly-degree IPS p-simulate Extended Frege? (Probably not. Prove it!)
2. Get PC to work well for SAT in practice (though, see Noriko Arai’s talk yesterday)
3. $AC^0[2]$-Frege lower bounds? Maciel-Pitassi ‘97 proved quasi-poly reduction to depth 3 (proof complexity version of Biegel-Tarui/Yao). Toni suggested looking at PC proofs over probabilistic polynomials.

Back to Pitassi '96/'98

Toni's questions from P98 still open:

4. Ajtai/Krajicek representation-theoretic approach to uniform lower bounds deserves further study.
5. Conjecture: For a prime p, if IPS over GF(p) is p-bounded, then NP=coNP. (Can prove directly, avoiding PIT?)
6. Natural proofs-like barrier for proof complexity?

Algebraic Proof Complexity Of Tensor Isomorphism

Joint w/ Toni, Nicola Galesi, Adrian She (to appear on arXiv momentarily)

Tensor Isomorphism:

- Verbose version a bottleneck to improving Graph Isomorphism
- Succinct version is GI-hard
- Many natural algebraic problems are TI-complete, eg Ring Isomorphism or local equivalence of quantum states

Algebraic Proof Complexity Of Tensor Isomorphism

How hard, really, could TI be?

Are these tensors isomorphic?

$\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ $\qquad$ $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$

Psst: Proof complexity?

From my talk at Banff (2019)

Tricks
Returning the Favor

How hard, really, could TI be?

Are these tensors isomorphic?

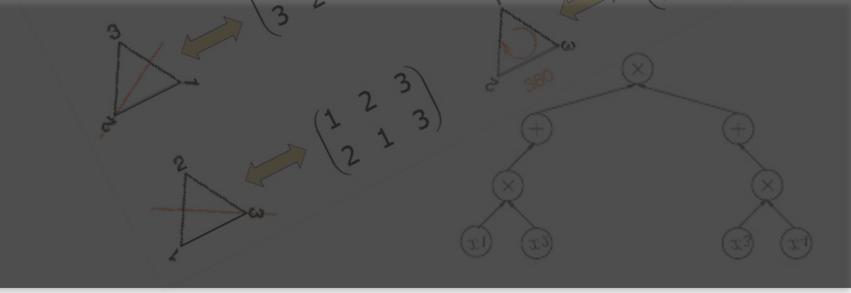
$$\begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}, \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \qquad \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}$$

Psst: Proof complexity?

Aimed at Toni

From my talk at Banff (2019)

Algebraic Proof Complexity Of Tensor Isomorphism



Main Results [Galesi-G.-Pitassi-She '23]:

1. $\Omega(n)$ lower bound on PC degree for Tensor Iso
2. O(1)-degree PC proofs for non-isomorphism of *bounded-rank* tensors
3. PC can't decide matrix rank, nor derive AB=I from BA=I in sub-linear degree

Inv

4. **Conjecture:** PC+Inv can't solve Tensor Iso either

Open:

Stronger lower bound? Note: no Boolean axioms here (obv. upper bound is $2^{O(n^2)}$).

Highlights

Go back and look at Toni’s open questions from 1996/98!

Toni: still at the forefront of proof complexity

Highlights

Go back and look at Toni's open questions from 1996/98!

Toni: still at the forefront of proof complexity

What great things will Toni trick us into next?

Highlights

Go back and look at Toni’s open questions from 1996/98!

Toni: still at the forefront of proof complexity

What great things will Toni trick us into next?

Happy Birthday Toni!