UNIVERSITY OF TORONTO

ROYAL INSTITUTE OF TECHNOLOGY

Towards an Understanding of Polynomial Calculus: New Separations and Lower Bounds

Yuval Filmus   Massimo Lauria   **Mladen Mikša**
Jakob Nordström   Marc Vinyals

40th International Colloquium on Automata, Languages and Programming
Riga, Latvia

9 July 2013

Proof Complexity

- **Original motivation:** Program for showing P $\neq$ NP
- **More recently:** Connections to **SAT solving**
- Key concerns in SAT solving: running time and memory
  - Modelled by size and space in proof system

  1. **DPLL (+ clause learning)**
     - Corresponds to **resolution proof system**
     - State of the art
  2. **Algebraic methods (Gröbner bases)**
     - Corresponds to **polynomial calculus**
     - Potentially better than DPLL
- **This talk:** Space complexity in polynomial calculus

The General Set-Up

- **Input:** CNF formula F

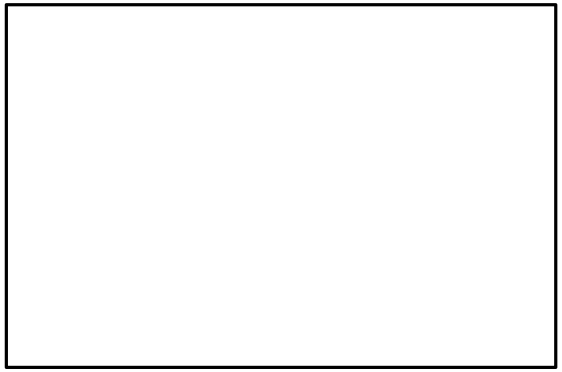
$$(\overline{x} \vee y) \wedge (\overline{x} \vee \overline{y} \vee z) \wedge \overline{z} \wedge (x \vee z)$$

- **Goal:** Proof of unsatisfiability (refutation of F)

- Refer to clauses of formula as **axioms**
- Focus on k-CNF formulas
  (All clauses of size $\leq k = \mathrm{O}(1)$)

Resolution

Think of proof as presented on whiteboard



Resolution

Think of proof as presented on whiteboard

Derivation rules

- Write down axioms

Resolution

Think of proof as presented on whiteboard

$x \vee y$

Derivation rules

- Write down axioms

Resolution

Think of proof as presented on whiteboard

$x \vee y$

$\overline{x} \vee z \vee w$

Derivation rules

- Write down axioms

Resolution

Think of proof as presented on whiteboard

$x \vee y$

$\overline{x} \vee z \vee w$

Derivation rules

- Write down axioms
- Use resolution rule

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

Resolution

Think of proof as presented on whiteboard

$x \lor y$

$\overline{x} \lor z \lor w$

$y \lor z \lor w$

Derivation rules

- Write down axioms
- Use resolution rule

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

Resolution

Think of proof as presented on whiteboard

$x \vee y$

$\overline{x} \vee z \vee w$

$y \vee z \vee w$

Derivation rules

- Write down axioms
- Use resolution rule
  $$\frac{C \vee x \qquad D \vee \overline{x}}{C \vee D}$$
- Erase clause

Resolution

Think of proof as presented on whiteboard

$\overline{x} \vee z \vee w$

$y \vee z \vee w$

Derivation rules

- Write down axioms
- Use resolution rule

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

- Erase clause

Resolution

Think of proof as presented on whiteboard

$\overline{x} \vee z \vee w$

$y \vee z \vee w$

Derivation rules

- Write down axioms
- Use resolution rule

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

- Erase clause

Resolution — Measures

$x \vee y$

$\overline{x} \vee \overline{y} \vee z \vee w$

$y \vee z \vee w$

Size: # of clauses in proof

Space: # of clauses on board

Resolution — Measures

$x \vee y$
$\overline{x} \vee \overline{y} \vee z \vee w$
$y \vee z \vee w$

Size: # of clauses in proof

Space: # of clauses on board

Width: # variables in largest clause

Resolution — Measures

$x \lor y$

$\overline{x} \lor \overline{y} \lor z \lor w$

$y \lor z \lor w$

Size: # of clauses in proof

Space: # of clauses on board

Width: # variables in largest clause

This board: space $= 3$ & width $= 4$

Resolution — Measures

$x \vee y$

$\overline{x} \vee \overline{y} \vee z \vee w$

$y \vee z \vee w$

Size: # of clauses in proof

Space: # of clauses on board

Width: # variables in largest clause

This board: space $= 3$ & width $= 4$

Size	**Width**	**Space**
$\exp\big(\Theta(n)\big)$	$\Theta(n)$	$\Theta(n)$

Resolution — Measures

$x \vee y$
$\overline{x} \vee \overline{y} \vee z \vee w$
$y \vee z \vee w$

Size: # of clauses in proof

Space: # of clauses on board

Width: # variables in largest clause

This board: space $= 3$ & width $= 4$

$\log($**Size**$)$ $\gtrsim$	**Width**	**Space**
$\exp\big(\Theta(n)\big)$	$\Theta(n)$	$\Theta(n)$

- Small size $\implies$ small width [Ben-Sasson, Wigderson '99]
- Small width $\implies$ small size

Resolution — Measures

$x \vee y$

$\overline{x} \vee \overline{y} \vee z \vee w$

$y \vee z \vee w$

Size: # of clauses in proof

Space: # of clauses on board

Width: # variables in largest clause

This board: space $=$ 3 & width $=$ 4

$\log($**Size**$)$	$\gtrsim$	**Width**	$\leq$	**Space**
$\exp\big(\Theta(n)\big)$		$\Theta(n)$		$\Theta(n)$

- Small size $\Longrightarrow$ small width [Ben-Sasson, Wigderson '99]
- Small width $\Longrightarrow$ small size

- Small space $\Longrightarrow$ small width [Atserias, Dalmau '03]
- Small width $\not\Longrightarrow$ small space [Ben-Sasson, Nordström '08]

Polynomial Calculus [CEI '96, ABRW '00]

- Simulates resolution; can be exponentially stronger
- Proof lines are polynomials over field $\mathbb{F}$
  - Encode axioms: $x \vee \overline{y} \vee z \quad \rightarrow \quad \overline{x} y \overline{z} = 0$
- Use additional axioms: $x^2 - x = 0$ and $x + \overline{x} - 1 = 0$

Polynomial Calculus [CEI '96, ABRW '00]

- Simulates resolution; can be exponentially stronger
- Proof lines are polynomials over field $\mathbb{F}$
  - Encode axioms: $x \vee \overline{y} \vee z \quad \rightarrow \quad \overline{x} y \overline{z} = 0$
- Use additional axioms: $x^2 - x = 0$ and $x + \overline{x} - 1 = 0$

$\overline{x} v - \overline{x} = 0$

Derivation rules

- Write down axioms

Polynomial Calculus [CEI '96, ABRW '00]

- Simulates resolution; can be exponentially stronger
- Proof lines are polynomials over field $\mathbb{F}$
  - Encode axioms: $x \vee \overline{y} \vee z \quad \rightarrow \quad \overline{x}y\overline{z} = 0$
- Use additional axioms: $x^2 - x = 0$ and $x + \overline{x} - 1 = 0$

$\overline{x}v - \overline{x} = 0$

$\overline{x}vz = 0$

Derivation rules

- Write down axioms

Polynomial Calculus [CEI '96, ABRW '00]

- Simulates resolution; can be exponentially stronger
- Proof lines are polynomials over field $\mathbb{F}$
  - Encode axioms: $x \lor \overline{y} \lor z \quad \to \quad \overline{x}y\overline{z} = 0$
- Use additional axioms: $x^2 - x = 0$ and $x + \overline{x} - 1 = 0$

$\overline{x}v - \overline{x} = 0$

$\overline{x}vz = 0$

Derivation rules

- Write down axioms
- Multiplication $\frac{p=0}{xp=0}$

Polynomial Calculus [CEI '96, ABRW '00]

- Simulates resolution; can be exponentially stronger
- Proof lines are polynomials over field $\mathbb{F}$
  - Encode axioms: $x \vee \overline{y} \vee z \quad \rightarrow \quad \overline{x}y\overline{z} = 0$
- Use additional axioms: $x^2 - x = 0$ and $x + \overline{x} - 1 = 0$

$\overline{x}v - \overline{x} = 0$

$\overline{x}vz = 0$

$\overline{x}vz - \overline{x}z = 0$

Derivation rules

- Write down axioms
- Multiplication $\frac{p=0}{xp=0}$

Polynomial Calculus [CEI '96, ABRW '00]

- Simulates resolution; can be exponentially stronger
- Proof lines are polynomials over field $\mathbb{F}$
  - Encode axioms: $x \vee \overline{y} \vee z \quad \rightarrow \quad \overline{x}y\overline{z} = 0$
- Use additional axioms: $x^2 - x = 0$ and $x + \overline{x} - 1 = 0$

$\overline{x}v - \overline{x} = 0$

$\overline{x}vz = 0$

$\overline{x}vz - \overline{x}z = 0$

Derivation rules

- Write down axioms
- Multiplication $\frac{p=0}{xp=0}$
- Linear combination $\frac{p=0 \quad q=0}{\alpha p+\beta q=0}$

Polynomial Calculus [CEI '96, ABRW '00]

- Simulates resolution; can be exponentially stronger
- Proof lines are polynomials over field $\mathbb{F}$
  - Encode axioms: $x \vee \overline{y} \vee z \quad \rightarrow \quad \overline{x}y\overline{z} = 0$
- Use additional axioms: $x^2 - x = 0$ and $x + \overline{x} - 1 = 0$

$\overline{x}v - \overline{x} = 0$

$\overline{x}vz = 0$

$\overline{x}vz - \overline{x}z = 0$

$\overline{x}z = 0$

Derivation rules

- Write down axioms
- Multiplication $\frac{p=0}{xp=0}$
- Linear combination $\frac{p=0 \quad q=0}{\alpha p + \beta q = 0}$

Polynomial Calculus [CEI '96, ABRW '00]

- Simulates resolution; can be exponentially stronger
- Proof lines are polynomials over field $\mathbb{F}$
  - Encode axioms: $x \vee \overline{y} \vee z \quad \rightarrow \quad \overline{x}y\overline{z} = 0$
- Use additional axioms: $x^2 - x = 0$ and $x + \overline{x} - 1 = 0$

$$\boxed{\begin{array}{l} \overline{x}v - \overline{x} = 0 \\ \overline{x}vz = 0 \\ \overline{x}vz - \overline{x}z = 0 \\ \overline{x}z = 0 \end{array}}$$

Derivation rules

- Write down axioms
- Multiplication $\frac{p=0}{xp=0}$
- Linear combination $\frac{p=0 \quad q=0}{\alpha p + \beta q = 0}$
- Erase polynomial

Polynomial Calculus [CEI '96, ABRW '00]

- Simulates resolution; can be exponentially stronger
- Proof lines are polynomials over field $\mathbb{F}$
  - Encode axioms: $x \vee \overline{y} \vee z \quad \rightarrow \quad \overline{x}y\overline{z} = 0$
- Use additional axioms: $x^2 - x = 0$ and $x + \overline{x} - 1 = 0$

$\overline{x}vz = 0$

$\overline{x}vz - \overline{x}z = 0$

$\overline{x}z = 0$

Derivation rules

- Write down axioms
- Multiplication $\frac{p=0}{xp=0}$
- Linear combination $\frac{p=0 \qquad q=0}{\alpha p + \beta q = 0}$
- Erase polynomial

Polynomial Calculus [CEI '96, ABRW '00]

- Simulates resolution; can be exponentially stronger
- Proof lines are polynomials over field $\mathbb{F}$
  - Encode axioms: $x \vee \overline{y} \vee z \quad \rightarrow \quad \overline{x}y\overline{z} = 0$
- Use additional axioms: $x^2 - x = 0$ and $x + \overline{x} - 1 = 0$

$\overline{x}vz = 0$

$\overline{x}vz - \overline{x}z = 0$

$\overline{x}z = 0$

Derivation rules

- Write down axioms
- Multiplication $\frac{p=0}{xp=0}$
- Linear combination $\frac{p=0 \quad q=0}{\alpha p+\beta q=0}$
- Erase polynomial

Polynomial Calculus — Measures

$$\overline{x}v - \overline{x} = 0$$

$$\overline{x}vz = 0$$

$$\overline{x}vz - \overline{x}z = 0$$

Size: # of monomials in proof

Space: # of monomials on board

Polynomial Calculus — Measures

$$\boxed{\begin{array}{l} \overline{x}v - \overline{x} = 0 \\ \overline{x}vz = 0 \\ \overline{x}vz - \overline{x}z = 0 \end{array}}$$

Size: # of monomials in proof

Space: # of monomials on board

Degree: # variables in largest monomial

Polynomial Calculus — Measures

$$\overline{x}v - \overline{x} = 0$$

$$\overline{x}vz = 0$$

$$\overline{x}vz - \overline{x}z = 0$$

Size: # of monomials in proof

Space: # of monomials on board

Degree: # variables in largest monomial

This board: space = 5 & degree = 3

Polynomial Calculus — Measures

$$\overline{x}v - \overline{x} = 0$$

$$\overline{x}vz = 0$$

$$\overline{x}vz - \overline{x}z = 0$$

Size: # of monomials in proof

Space: # of monomials on board

Degree: # variables in largest monomial

This board: space = 5 & degree = 3

Size	**Degree**	**Space**
$\exp\big(\Theta(n)\big)$	$\Theta(n)$	$\Theta(n)$

Polynomial Calculus — Measures

$\overline{x}v - \overline{x} = 0$

$\overline{x}vz = 0$

$\overline{x}vz - \overline{x}z = 0$

Size: # of monomials in proof

Space: # of monomials on board

Degree: # variables in largest monomial

This board: space = 5 & degree = 3

$\log(\textbf{Size})$ $\gtrsim$	**Degree**	**Space**
$\exp\big(\Theta(n)\big)$	$\Theta(n)$	$\Theta(n)$

- Small size $\Longrightarrow$ small degree [Impagliazzo, Pudlák, Sgall '99]
- Small degree $\Longrightarrow$ small size [Clegg, Edmonds, Impagliazzo '96]

Polynomial Calculus — Measures

$$\overline{x}v - \overline{x} = 0$$
$$\overline{x}vz = 0$$
$$\overline{x}vz - \overline{x}z = 0$$

Size: # of monomials in proof

Space: # of monomials on board

Degree: # variables in largest monomial

This board: space = 5 & degree = 3

$\log($**Size**$)$	$\gtrsim$	**Degree**	???	**Space**
$\exp(\Theta(n))$		$\Theta(n)$		$\Theta(n)$

- Small size $\Longrightarrow$ small degree [Impagliazzo, Pudlák, Sgall '99]
- Small degree $\Longrightarrow$ small size [Clegg, Edmonds, Impagliazzo '96]

- Small space $\Longrightarrow$ small degree**?**
- Small degree $\Longrightarrow$ small space**?**

Our Results

- Small space (sort of) implies small degree

Theorem 1

If F requires degree w, then **XORified** version of F requires polynomial calculus space $\Omega(w)$

Our Results

- Small space (sort of) implies small degree

Theorem 1

If F requires **resolution width** w, then **XORified** version of F requires polynomial calculus space $\Omega(w)$

Our Results

- Small space (sort of) implies small degree

Theorem 1

If F requires **resolution width** w, then **XORified** version of F requires polynomial calculus space $\Omega(w)$

  - **Stronger:** Holds for **resolution width**
  - **Weaker:** Requires **XORification**

Our Results

- Small space (sort of) implies small degree

Theorem 1

If F requires **resolution width** w, then **XORified** version of F requires polynomial calculus space $\Omega(w)$

  - **Stronger:** Holds for **resolution width**
  - **Weaker:** Requires **XORification**

- Small degree does not imply small space

Theorem 2

Exist formulas refutable in constant degree but requiring linear space

Our Results

- Small space (sort of) implies small degree

Theorem 1

If F requires **resolution width** w, then **XORified** version of F requires polynomial calculus space $\Omega(w)$

  - **Stronger:** Holds for **resolution width**
  - **Weaker:** Requires **XORification**

- Small degree does not imply small space

Theorem 2

Exist formulas refutable in constant degree but requiring linear space

- Also some other results (won't have time to cover):
  - Space lower bounds for so-called Tseitin contradictions
  - Provable limitations of current lower-bound techniques

Theorem 2 — Brief Overview

Theorem 2

Exist formulas refutable in constant degree but requiring linear space

Theorem 2 — Brief Overview

Theorem 2

Exist formulas refutable in constant degree but requiring linear space

- Focus on $\mathbb{F}_2$ case
- Find formulas with:
  - Large resolution width
  - Small polynomial calculus degree
- Use **full strength** of Theorem 1 to get:
  - Large polynomial calculus space
  - While keeping degree small

Theorem 1 and XORification

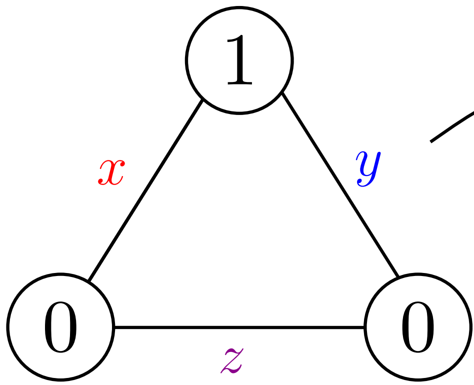
Theorem 1

If F requires **resolution width** w, then **XORified** version of F requires polynomial calculus space $\Omega(w)$

- **XORification:** Substitute variables with XOR ($\oplus$)
- Expand to CNF formula

$$\overline{x} \vee y \longrightarrow (\overline{x_1 \oplus x_2}) \vee (y_1 \oplus y_2) \longrightarrow \begin{array}{l} (\overline{x_1} \vee x_2 \vee y_1 \vee y_2) \wedge \\ (\overline{x_1} \vee x_2 \vee \overline{y_1} \vee \overline{y_2}) \wedge \\ (x_1 \vee \overline{x_2} \vee y_1 \vee y_2) \wedge \\ (x_1 \vee \overline{x_2} \vee \overline{y_1} \vee \overline{y_2}) \end{array}$$

Tseitin Contradictions



$$x + y = 1$$
$$x + z = 0$$
$$y + z = 0$$

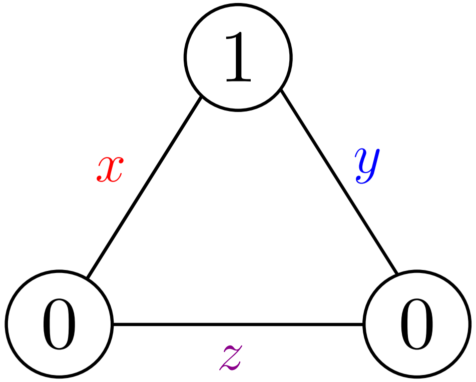
$$(x \vee y) \wedge$$
$$(\overline{x} \vee \overline{y}) \wedge$$
$$(\overline{x} \vee z) \wedge$$
$$(x \vee \overline{z}) \wedge$$
$$(\overline{y} \vee z) \wedge$$
$$(y \vee \overline{z})$$

- Linear equations on graph encoded as CNF formula

- Easy for polynomial calculus
  - Add equations together using constant degree

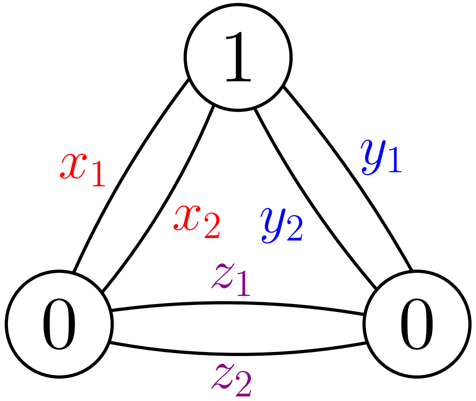
- Tseitin on expander graphs $\Longrightarrow$ large resolution width [Ben-Sasson, Wigderson '99]

Tseitin Contradictions — XORification



$$x + y = 1$$
$$x + z = 0$$
$$y + z = 0$$

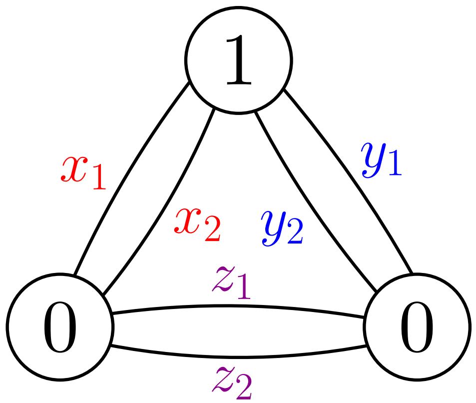
Tseitin Contradictions — XORification



$$x_1 + x_2 + y_1 + y_2 = 1$$
$$x_1 + x_2 + z_1 + z_2 = 0$$
$$y_1 + y_2 + z_1 + z_2 = 0$$

- XOR substitution = edge doubling
- Still linear equations $\implies$ still easy in polynomial calculus
- Expander graph $\implies$ space lower bound
  - Width lower bound + XORification + Theorem 1

Tseitin Contradictions — XORification



$$\color{red}{x_1 + x_2} + \color{blue}{y_1 + y_2} = 1$$
$$\color{red}{x_1 + x_2} + \color{purple}{z_1 + z_2} = 0$$
$$\color{blue}{y_1 + y_2} + \color{purple}{z_1 + z_2} = 0$$

Theorem 2

Exist formulas refutable in constant degree but requiring linear space

- XO
- Still linear equations $\implies$ still easy in polynomial calculus
- Expander graph $\implies$ space lower bound
  - Width lower bound + XORification + Theorem 1

Theorem 1 — Brief Overview

Theorem 1

If F requires **resolution width** w, then **XORified** version of F requires polynomial calculus space $\Omega(w)$

Theorem 1 — Brief Overview

Theorem 1

If F requires **resolution width** w, then **XORified** version of F requires polynomial calculus space $\Omega(w)$

- Characterization of resolution width by combinatorial game [Atserias, Dalmau '03]
- PC space lower bounds via (other) combinatorial game [Bonacina, Galesi '13]
- XORification of formulas

Run [AD '03] game on original formula as subroutine of [BG '13] game on XORified formula

Some Open Problems

Open Problem 1

Prove space lower bounds for 3-CNF formulas

- Nothing is known — only k-CNF lower bounds for $k \geq 4$

Some Open Problems

Open Problem 1

Prove space lower bounds for 3-CNF formulas

- Nothing is known — only k-CNF lower bounds for $k \geq 4$

Open Problem 2

Extend techniques for lower bounding space

- Exist formulas that:
  - Likely hard (e.g., functional pigeonhole principle)
  - But [BG '13] provably doesn't work

Some Open Problems

Open Problem 1

Prove space lower bounds for 3-CNF formulas

- Nothing is known — only k-CNF lower bounds for $k \geq 4$

Open Problem 2

Extend techniques for lower bounding space

- Exist formulas that:
  - Likely hard (e.g., functional pigeonhole principle)
  - But [BG '13] provably doesn't work

Open Problem 3

Does degree lower bound space?

- Might be helpful to characterize degree à la [AD '03]

Concluding Remarks

- Key concerns in SAT solving: running time and memory
- Modelled by size and space in proof complexity
- Resolution well understood — key measure: width
- **Polynomial calculus** less clear — role of degree?
- **This work:** Sheds some light on space-degree relation
  (Short version: picture seems very similar to resolution)
- Still many **open problems** in polynomial calculus

Concluding Remarks

- Key concerns in SAT solving: running time and memory
- Modelled by size and space in proof co
- Resolution well understood — re: width
- **Polynomial calculus** – role of degree?
- **This work:** S ight on space-degree relation
  (Short v ture seems very similar to resolution)
- Still m **open problems** in polynomial calculus

Thank you for your attention!