Simple hard instances for low-depth algebraic proofs

Tuomas Hakoniemi

Imperial College London

July 7th 2022, ICMS, Edinburgh

Joint work with Nashlen Govindasamy and Iddo Tzameret

The proof system

We consider NS refutations of $q_1 = 0, \ldots, q_\ell = 0$ the form

$$1 = \sum_{k \in [\ell]} t_\ell q_\ell \mod \bar{x}^2 - \bar{x}.$$

The proof system

We consider NS refutations of $q_1 = 0, \ldots, q_\ell = 0$ the form

$$1 = \sum_{k \in [\ell]} t_\ell q_\ell \mod \bar{x}^2 - \bar{x}.$$

Complexity measure: the algebraic circuit size of t_k's.

The proof system

We consider NS refutations of $q_1 = 0, \ldots, q_\ell = 0$ the form

$$1 = \sum_{k \in [\ell]} t_\ell q_\ell \mod \bar{x}^2 - \bar{x}.$$

Complexity measure: the algebraic circuit size of t_k's.

A very strong proof system.

The proof system

We consider NS refutations of $q_1 = 0, \ldots, q_\ell = 0$ the form

$$1 = \sum_{k \in [\ell]} t_\ell q_\ell \mod \bar{x}^2 - \bar{x}.$$

Complexity measure: the algebraic circuit size of t_k's.

A very strong proof system.

Essentially Hilbert-style IPS of [GP'14] or $\mathrm{IPS}_{\mathrm{Lin}'}$ of [FSTW'16].

The hard instance

Consider a variant of knapsack (or subset sum)

$$\sum_{i,j,k,\ell \in [n]} z_{ijk\ell} x_i x_j x_k x_\ell = \beta$$

unsatisfiable over the Boolean hypercube.

The hard instance

Consider a variant of knapsack (or subset sum)

$$\sum_{i,j,k,\ell \in [n]} z_{ijk\ell} x_i x_j x_k x_\ell = \beta$$

unsatisfiable over the Boolean hypercube.

Theorem (Informal)

*Any low-depth **multilinear** refutation of the knapsack variant requires superpolynomial algebraic circuit size.*

Smörgåsbord of previous work

Lower bounds for subsystems of IPS based on roABPs and multilinear formulas [FSTW '16]

Smörgåsbord of previous work

Lower bounds for subsystems of IPS based on roABPs and multilinear formulas [FSTW '16]

Conditional IPS lower bounds for Binary Value Principle [AGHT'20] and refutation formulas [ST'21]

Smörgåsbord of previous work

Lower bounds for subsystems of IPS based on roABPs and multilinear formulas [FSTW '16]

Conditional IPS lower bounds for Binary Value Principle [AGHT'20] and refutation formulas [ST'21]

Unconditional low-depth IPS lower bounds [AF'21]

Smörgåsbord of previous work

Lower bounds for subsystems of IPS based on roABPs and multilinear formulas [FSTW '16]

Conditional IPS lower bounds for Binary Value Principle [AGHT'20] and refutation formulas [ST'21]

Unconditional low-depth IPS lower bounds [AF'21]

Bit-complexity lower bounds for Extended Polynomial Calculus over rationals for Binary Value Principle [A'21]

Smörgåsbord of previous work

Lower bounds for subsystems of IPS based on roABPs and multilinear formulas [FSTW '16]

Conditional IPS lower bounds for Binary Value Principle [AGHT'20] and refutation formulas [ST'21]

Unconditional low-depth IPS lower bounds [AF'21]

Bit-complexity lower bounds for Extended Polynomial Calculus over rationals for Binary Value Principle [A'21]

Size lower bounds for Extended Polynomial Calculus over finite fields with restricted use of extension variables. [IMP'22]

Our result

Theorem

Assume $\mathrm{char}(\mathbb{F}) = 0$ *and let* $n, \Delta \in \mathbb{N}_+$ *with* $\Delta \leq \frac{1}{4} \log \log \log n$. *Let* f *be the unique multilinear polynomial so that*

$$f = \frac{1}{\sum_{ijk\ell} z_{ijk\ell} x_i x_j x_k x_\ell - \beta} \quad \textit{over Boolean valuations.}$$

Then any algebraic circuit of product-depth at most Δ *computing* f *requires size*

$$n^{(log n)^{\exp(-O(\Delta))}}$$

Proof ingredients

Our proof combines

Proof ingredients

Our proof combines

the methods to prove superpolynomial lower bounds for constant-depth algebraic circuits from [LST '21]:

Proof ingredients

Our proof combines

the methods to prove superpolynomial lower bounds for constant-depth algebraic circuits from [LST '21]:

- lower bounds for low-depth **lopsided** set-multilinear circuits from suitable rank lower bounds;

Proof ingredients

Our proof combines

the methods to prove superpolynomial lower bounds for constant-depth algebraic circuits from [LST '21]:

- lower bounds for low-depth **lopsided** set-multilinear circuits from suitable rank lower bounds;
- a depth-preserving reduction from general circuits to set-multilinear ones;

Proof ingredients

Our proof combines

the methods to prove superpolynomial lower bounds for constant-depth algebraic circuits from [LST '21]:

- lower bounds for low-depth **lopsided** set-multilinear circuits from suitable rank lower bounds;
- a depth-preserving reduction from general circuits to set-multilinear ones;

the methods to prove IPS lower bounds via functional lower bounds from [FSTW '16]:

Proof ingredients

Our proof combines

the methods to prove superpolynomial lower bounds for constant-depth algebraic circuits from [LST '21]:

- lower bounds for low-depth **lopsided** set-multilinear circuits from suitable rank lower bounds;
- a depth-preserving reduction from general circuits to set-multilinear ones;

the methods to prove IPS lower bounds via functional lower bounds from [FSTW '16]:

- rank lower bounds using partial valuations.

Proof outline

Step 1: restrict to another variant of knapsack ks_w by setting the z-variables and some of the x-variables.

Proof outline

Step 1: restrict to another variant of knapsack ks_w by setting the z-variables and some of the x-variables.

Step 2: find a suitable lopsided set-multilinear polynomial within the multilinear refutation f of ks_w.

Proof outline

Step 1: restrict to another variant of knapsack ks_w by setting the z-variables and some of the x-variables.

Step 2: find a suitable lopsided set-multilinear polynomial within the multilinear refutation f of ks_w.

Step 3: project f to the space of these lopsided set-multilinear polynomials and prove a rank lower bound for the projection.

Proof outline

Step 1: restrict to another variant of knapsack ks_w by setting the z-variables and some of the x-variables.

Step 2: find a suitable lopsided set-multilinear polynomial within the multilinear refutation f of ks_w.

Step 3: project f to the space of these lopsided set-multilinear polynomials and prove a rank lower bound for the projection.

Step 4: obtain the circuit lower bounds from the rank lower bounds using [LST'21].

Constructing ks_w

Setup: let $w \in \mathbb{Z}^d$ be a word, and fix for any $i \in [d]$ a set of variables of size $2^{|w_i|}$.

Constructing ks_w

Setup: let $w \in \mathbb{Z}^d$ be a word, and fix for any $i \in [d]$ a set of variables of size $2^{|w_i|}$.

Consider **positive** variables $x_\sigma^{(i)}$ and **negative** variables $y_\sigma^{(j)}$.

Constructing ks_w

Setup: let $w \in \mathbb{Z}^d$ be a word, and fix for any $i \in [d]$ a set of variables of size $2^{|w_i|}$.

Consider **positive** variables $x_\sigma^{(i)}$ and **negative** variables $y_\sigma^{(j)}$.

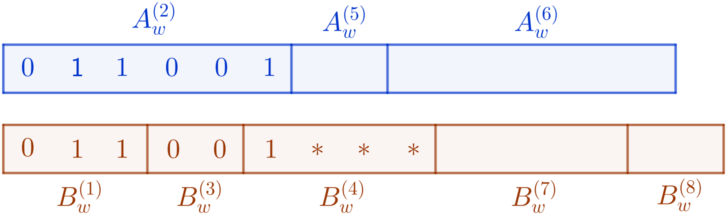
We define a variant of the Knapsack of the form

$$\mathsf{ks}_w := \sum x_\sigma^{(i)} f_\sigma^{(i)} - \beta,$$

where $f_\sigma^{(i)}$ is a polynomial in the negative variables.

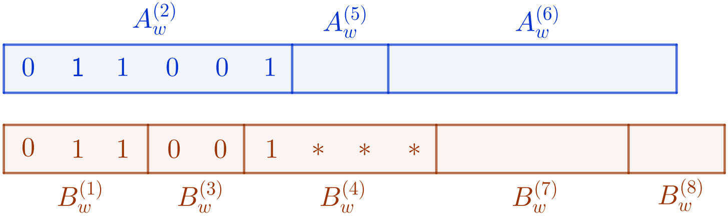
Defining $f_\sigma^{(i)}$

Definition by example:



Defining $f_\sigma^{(i)}$

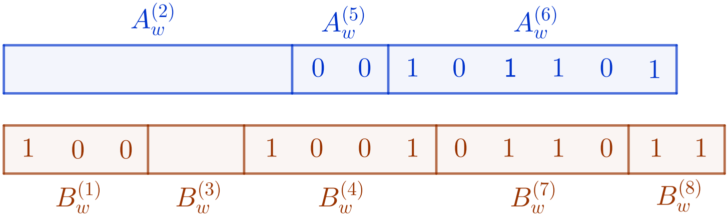
Definition by example:



Here $f_{011001}^{(2)} = y_{011}^{(1)} \cdot y_{00}^{(3)} \cdot (y_{1000}^{(4)} + y_{1001}^{(4)} + \cdots + y_{1111}^{(4)})$

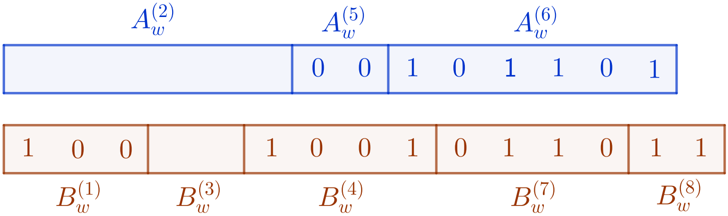
Knapsacks all the way down

What's the point?



Knapsacks all the way down

What's the point?



A partial valuation corresponding to the monomial

$$y^{(1)}_{100}y^{(4)}_{1001}y^{(7)}_{0110}y^{(8)}_{11}$$

simplifies ks_w to

$$x^{(5)}_{00} + x^{(6)}_{101101} - \beta.$$

Multilinear refutations of vanilla Knapsack

From [FSTW'16] we know exactly the structure of the multilinear f such that

$$f = \frac{1}{\sum_{i \in [n]} x_i - \beta} \quad \text{over Boolean valuations.}$$

Multilinear refutations of vanilla Knapsack

From [FSTW'16] we know exactly the structure of the multilinear f such that

$$f = \frac{1}{\sum_{i \in [n]} x_i - \beta} \quad \text{over Boolean valuations.}$$

In particular, the leading monomial of f is $\prod_{i \in [n]} x_i$.

Rank lower bound

Lemma

Let $w \in \mathbb{Z}$ be a balanced word, and let f be the multilinear polynomial so that

$$f = \frac{1}{\mathsf{ks}_w} \quad \textit{over Boolean valuations.}$$

Then $M_w(f)$ is full-rank.

Rank lower bound

Lemma

Let $w \in \mathbb{Z}$ be a balanced word, and let f be the multilinear polynomial so that

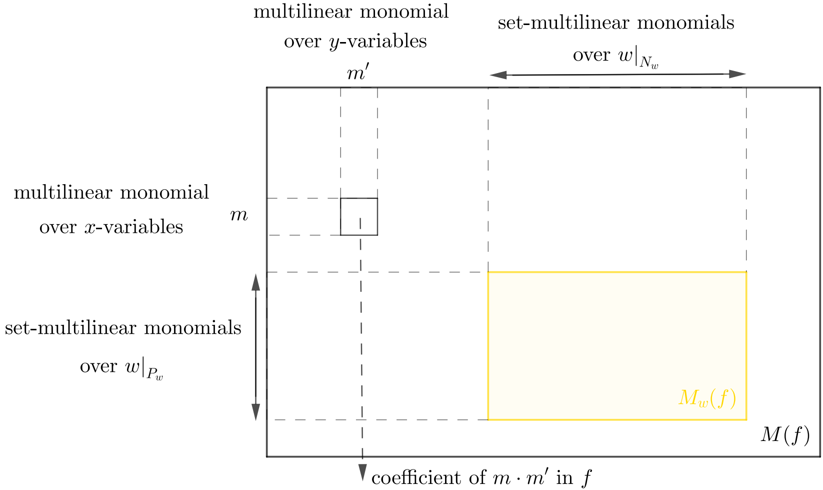
$$f = \frac{1}{\mathsf{ks}_w} \quad \textit{over Boolean valuations.}$$

Then $M_w(f)$ is full-rank.

Corollary

For a balanced word with $|w_i| \leq b$, $\mathsf{relrk}_w(f) \geq 2^{-b/2}$.

Rank lower bound



Lower bounds for set-multilinear circuits

Take a balanced word $w \in \{-k, \lfloor k/\sqrt{2} \rfloor\}^d$ with $k \geq 10d$. By [LTS'21] any set-ml formula C over w of size s and product-depth Δ satisfies

$$\mathrm{relrk}_w(C) \leq s \cdot 2^{-\frac{kd^{1/(2^\Delta - 1)}}{20}}.$$

Lower bounds for set-multilinear circuits

Take a balanced word $w \in \{-k, \lfloor k/\sqrt{2} \rfloor\}^d$ with $k \geq 10d$. By [LTS'21] any set-ml formula C over w of size s and product-depth Δ satisfies

$$\mathrm{relrk}_w(C) \leq s \cdot 2^{-\frac{kd^{1/(2^{\Delta}-1)}}{20}}.$$

Corollary

Let k, d and w be as above, and let f be the multilinear polynomial that equals $1/\mathrm{ks}_w$ over Boolean valuations. Then any set-ml circuit of product-depth at most Δ computing $\Pi_w(f)$, requires size

$$2^{k\left(\frac{d^{1/(2^{\Delta}-1)}-20}{40\Delta}\right)}.$$

Final reduction

Also from [LST'21] we have that for any word $w \in \mathbb{Z}^d$ and any polynomial f:

Final reduction

Also from [LST'21] we have that for any word $w \in \mathbb{Z}^d$ and any polynomial f:

$\exists$ a circuit of size s and product-depth Δ computing f

Final reduction

Also from [LST'21] we have that for any word $w \in \mathbb{Z}^d$ and any polynomial f:

$\exists$ a circuit of size s and product-depth Δ computing f

$$\implies$$

$\exists$ a set-ml circuit of size $d^{O(d)}\text{poly}(s)$ and product-depth 2Δ computing $\Pi_w(f)$.

Final touches

Finally take $k = \lfloor \log n/2 \rfloor$ and $d = \lfloor \log n/30 \rfloor$.

Final touches

Finally take $k = \lfloor \log n/2 \rfloor$ and $d = \lfloor \log n/30 \rfloor$.

Now $d2^k < n$, and the polynomials $f_\sigma^{(i)}$ are of degree at most 3.

Final touches

Finally take $k = \lfloor \log n/2 \rfloor$ and $d = \lfloor \log n/30 \rfloor$.

Now $d2^k < n$, and the polynomials $f_\sigma^{(i)}$ are of degree at most 3.

Hence there is a restriction that maps

$$\sum_{i,j,k,\ell \in [n]} z_{ijk\ell} x_i x_j x_k x_\ell - \beta$$

to ks_w (up to renaming variables).

Open questions

- Upper bounds for low-depth multilinear refutations.

Open questions

- Upper bounds for low-depth multilinear refutations.
- Can we get around the multilinearity restriction? Bounded individual degree?

Open questions

- Upper bounds for low-depth multilinear refutations.
- Can we get around the multilinearity restriction? Bounded individual degree?
- Lower bounds for CNFs?

Open questions

- Upper bounds for low-depth multilinear refutations.
- Can we get around the multilinearity restriction? Bounded individual degree?
- Lower bounds for CNFs?
- Lower bounds over finite fields?

Thank you!