SUCCINCT HITTING SETS
AND
BARRIERS TO PROVING ALGEBRAIC CIRCUITS LOWER BOUNDS

Ben Lee Volk

Joint with

Michael A. Forbes
Amir Shpilka

ALTERNATE TITLE:

HOW NOT TO PROVE ALGEBRAIC CIRCUITS LOWER BOUNDS

Ben Lee Volk

Joint with

Michael A. Forbes
Amir Shpilka

WHY IS IT HARD TO PROVE CIRCUIT LOWER BOUNDS?

(One) Answer: natural proofs barrier **[Razborov-Rudich]**:

WHY IS IT HARD TO PROVE CIRCUIT LOWER BOUNDS?

(One) Answer: natural proofs barrier **[Razborov-Rudich]**:

"A computationally-bounded observer cannot distinguish between the truth table of a random function with small circuit and that of a truly random function (assuming some crypto). So every lower bound proof attempt which yields such an algorithm cannot work."

WHY IS IT HARD TO PROVE CIRCUIT LOWER BOUNDS?

(One) Answer: natural proofs barrier **[Razborov-Rudich]**:

“A computationally-bounded observer cannot distinguish between the truth table of a random function with small circuit and that of a truly random function (assuming some crypto). So every lower bound proof attempt which yields such an algorithm cannot work.”

NATURAL PROOFS

Def: A property S of boolean functions is natural if it is:

Natural Proofs

Def: A property S of boolean functions is natural if it is:

1. Useful: if f has S then f doesn't have a small ckt.

NATURAL PROOFS

Def: A property S of boolean functions is natural if it is:

1. Useful: if f has S then f doesn't have a small ckt.
2. Large: random functions have S with large probability.

Natural Proofs

Def: A property S of boolean functions is natural if it is:

1. Useful: if f has S then f doesn't have a small ckt.
2. Large: random functions have S with large probability.
3. Constructive: Given truth table of f of size $N = 2^n$, there is an algorithm for deciding whether $f \in S$ with running time $\mathrm{poly}(N) = 2^{O(n)}$.

NATURAL PROOFS

Def: A property S of boolean functions is natural if it is:

1. Useful: if f has S then f doesn't have a small ckt.
2. Large: random functions have S with large probability.
3. Constructive: Given truth table of f of size $N = 2^n$, there is an algorithm for deciding whether $f \in S$ with running time $\mathrm{poly}(N) = 2^{O(n)}$.

natural proof: a lower bound proof which exhibits a natural property.

NATURAL PROOFS

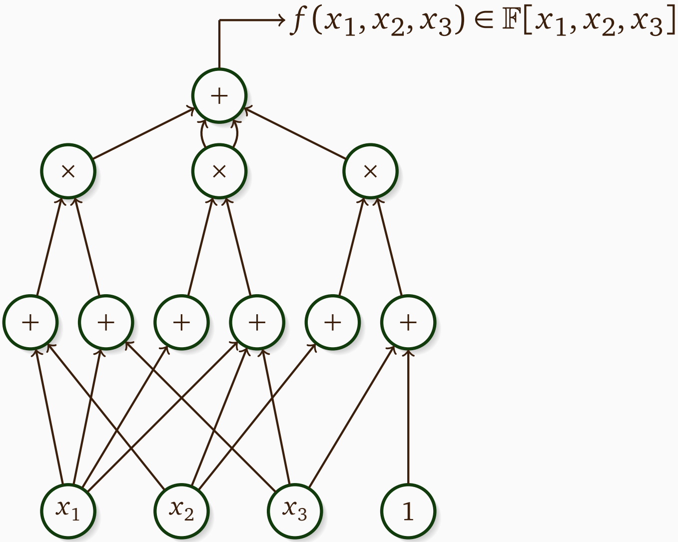
Def: A property S of boolean functions is natural if it is:

1. Useful: if f has S then f doesn't have a small ckt.
2. Large: random functions have S with large probability.
3. Constructive: Given truth table of f of size $N = 2^n$, there is an algorithm for deciding whether $f \in S$ with running time $\mathrm{poly}(N) = 2^{O(n)}$.

natural proof: a lower bound proof which exhibits a natural property.

[Razborov-Rudich]: Most known lower bounds are natural and if there's a pseudorandom function in $\mathscr{C}$ then no natural lower bound against $\mathscr{C}$.

ALGEBRAIC CIRCUITS



Lower Bounds for Algebraic Circuits

...are also pretty hard.

LOWER BOUNDS FOR ALGEBRAIC CIRCUITS

...are also pretty hard.

We can prove lower bounds for restricted models, but all lower bounds eventually also apply to polynomials we think of as “easy”.

LOWER BOUNDS FOR ALGEBRAIC CIRCUITS

...are also pretty hard.

We can prove lower bounds for restricted models, but all lower bounds eventually also apply to polynomials we think of as “easy”.

Most lower bounds seem “natural”, but unclear whether there are pseudorandom functions computed by low-degree algebraic circuits.

LOWER BOUNDS FOR ALGEBRAIC CIRCUITS

...are also pretty hard.

We can prove lower bounds for restricted models, but all lower bounds eventually also apply to polynomials we think of as “easy”.

Most lower bounds seem “natural”, but unclear whether there are pseudorandom functions computed by low-degree algebraic circuits.

(and even if not, maybe there are such functions that are only secure against algebraic circuits?)

LOWER BOUNDS FOR ALGEBRAIC CIRCUITS

...are also pretty hard.

We can prove lower bounds for restricted models, but all lower bounds eventually also apply to polynomials we think of as “easy”.

Most lower bounds seem “natural”, but unclear whether there are pseudorandom functions computed by low-degree algebraic circuits.

(and even if not, maybe there are such functions that are only secure against algebraic circuits?)

Can we identify formal barriers?

LOWER BOUNDS FOR ALGEBRAIC CIRCUITS

...are also pretty hard.

We can prove lower bounds for restricted models, but all lower bounds eventually also apply to polynomials we think of as "easy".

Most lower bounds seem "natural", but unclear whether there are pseudorandom functions computed by low-degree algebraic circuits.

(and even if not, maybe there are such functions that are only secure against algebraic circuits?)

Can we identify formal barriers?

(also asked by **[Aaronson-Drucker]** and **[Grochow]**)

Algebraically Natural Lower Bounds

Many lower bounds for restricted models of algebraic circuits have this form:

Algebraically Natural Lower Bounds

Many lower bounds for restricted models of algebraic circuits have this form:

1. given f, construct some matrix M_f whose entries are coefficients of f.

ALGEBRAICALLY NATURAL LOWER BOUNDS

Many lower bounds for restricted models of algebraic circuits have this form:

1. given f, construct some matrix M_f whose entries are coefficients of f.
2. argue that if f is computed by a small ckt, $\mathrm{rank}(M_f) =$ small.

ALGEBRAICALLY NATURAL LOWER BOUNDS

Many lower bounds for restricted models of algebraic circuits have this form:

1. given f, construct some matrix M_f whose entries are coefficients of f.
2. argue that if f is computed by a small ckt, $\mathrm{rank}(M_f) =$ small.
3. show some explicit f_0 with $\mathrm{rank}(M_{f_0}) =$ large.

ALGEBRAICALLY NATURAL LOWER BOUNDS

Many lower bounds for restricted models of algebraic circuits have this form:

1. given f, construct some matrix M_f whose entries are coefficients of f.
2. argue that if f is computed by a small ckt, $\mathrm{rank}(M_f) =$ small.
3. show some explicit f_0 with $\mathrm{rank}(M_{f_0}) =$ large.

(examples: evaluation dimension, partial derivatives, shifted partial derivatives, ...)

ALGEBRAICALLY NATURAL LOWER BOUNDS

Many lower bounds for restricted models of algebraic circuits have this form:

1. given f, construct some matrix M_f whose entries are coefficients of f.
2. argue that if f is computed by a small ckt, $\mathrm{rank}(M_f) = $ small.
3. show some explicit f_0 with $\mathrm{rank}(M_{f_0}) = $ large.

(examples: evaluation dimension, partial derivatives, shifted partial derivatives, ...)

equivalently: for some $r \times r$ submatrix, $\det(M'_{f_0}) \neq 0$, while $\det(M'_f) = 0$ for all simple f.

ALGEBRAICALLY NATURAL LOWER BOUNDS

Many lower bounds for restricted models of algebraic circuits have this form:

1. given f, construct some matrix M_f whose entries are coefficients of f.
2. argue that if f is computed by a small ckt, $\mathrm{rank}(M_f) =$ small.
3. show some explicit f_0 with $\mathrm{rank}(M_{f_0}) =$ large.

(examples: evaluation dimension, partial derivatives, shifted partial derivatives, ...)

equivalently: for some $r \times r$ submatrix, $\det(M'_{f_0}) \neq 0$, while $\det(M'_f) = 0$ for all simple f.

Thus, the property $\{g : \det(M'_g) \neq 0\}$ is useful, constructive (determinant is efficiently computable) and large.

ALGEBRAICALLY NATURAL LOWER BOUNDS

Def: A (distinguisher) polynomial $D \not\equiv 0$ is an algebraic natural proof against a class $\mathscr{C}$ if

ALGEBRAICALLY NATURAL LOWER BOUNDS

Def: A (distinguisher) polynomial $D \not\equiv 0$ is an algebraic natural proof against a class $\mathscr{C}$ if

1. (Usefulness) $D(\mathrm{coeff}(f)) = 0$ for all $f \in \mathscr{C}$

ALGEBRAICALLY NATURAL LOWER BOUNDS

Def: A (distinguisher) polynomial $D \not\equiv 0$ is an algebraic natural proof against a class $\mathscr{C}$ if

1. (Usefulness) $D(\mathrm{coeff}(f)) = 0$ for all $f \in \mathscr{C}$
2. (Constructiveness) D has a small algebraic circuit

ALGEBRAICALLY NATURAL LOWER BOUNDS

Def: A (distinguisher) polynomial $D \not\equiv 0$ is an algebraic natural proof against a class $\mathscr{C}$ if

1. (Usefulness) $D(\mathrm{coeff}(f)) = 0$ for all $f \in \mathscr{C}$
2. (Constructiveness) D has a small algebraic circuit

(largeness comes for free)

ALGEBRAICALLY NATURAL LOWER BOUNDS

Def: A (distinguisher) polynomial $D \not\equiv 0$ is an algebraic natural proof against a class $\mathscr{C}$ if

1. (Usefulness) $D(\mathrm{coeff}(f)) = 0$ for all $f \in \mathscr{C}$
2. (Constructiveness) D has a small algebraic circuit

(largeness comes for free)

Important: D is an N-variate polynomial for $N = \binom{n+d}{d}$ (if we deal with n-variate degree d polynomials) or $N = 2^n$ (if we deal with multilinear polynomials)

ALGEBRAICALLY NATURAL LOWER BOUNDS

Def: A (distinguisher) polynomial $D \not\equiv 0$ is an algebraic natural proof against a class $\mathscr{C}$ if

1. (Usefulness) $D(\mathrm{coeff}(f)) = 0$ for all $f \in \mathscr{C}$
2. (Constructiveness) D has a small algebraic circuit

(largeness comes for free)

Important: D is an N-variate polynomial for $N = \binom{n+d}{d}$ (if we deal with n-variate degree d polynomials) or $N = 2^n$ (if we deal with multilinear polynomials)

Toy example: $\mathscr{C}$ is the class of perfect squares among polynomials of the form $ax^2 + bx + c$, and $D(a, b, c) = b^2 - 4ac$.

ALGEBRAICALLY NATURAL LOWER BOUNDS

Def: A (distinguisher) polynomial $D \not\equiv 0$ is an algebraic natural proof against a class $\mathscr{C}$ if

1. (Usefulness) $D(\mathrm{coeff}(f)) = 0$ for all $f \in \mathscr{C}$
2. (Constructiveness) D has a small algebraic circuit

(largeness comes for free)

Important: D is an N-variate polynomial for $N = \binom{n+d}{d}$ (if we deal with n-variate degree d polynomials) or $N = 2^n$ (if we deal with multilinear polynomials)

Toy example: $\mathscr{C}$ is the class of perfect squares among polynomials of the form $ax^2 + bx + c$, and $D(a, b, c) = b^2 - 4ac$.

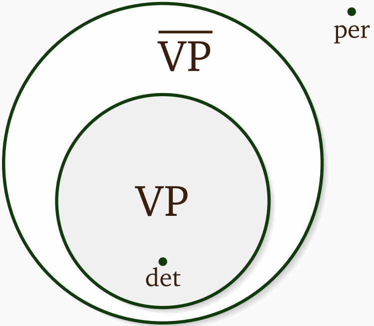
[Grochow]: almost all known lower bounds can be cast in this form.

GEOMETRIC COMPLEXITY THEORY

[Mulmuley-Sohoni]

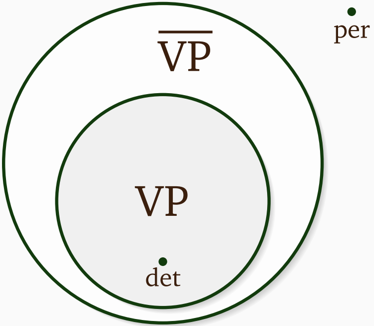
GEOMETRIC COMPLEXITY THEORY

[Mulmuley-Sohoni]



Geometric Complexity Theory

[Mulmuley-Sohoni]



$\overline{\mathrm{VP}}$ is a zero set of a set of polynomials $\mathscr{T}$. What is the complexity of $\mathscr{T}$?

POLYNOMIAL IDENTITY TESTING

Given an algebraic circuit C, decide **deterministically** whether C computes the zero polynomial.

POLYNOMIAL IDENTITY TESTING

Given an algebraic circuit C, decide **deterministically** whether C computes the zero polynomial.

Black-box: compute a hitting set $\mathscr{H}$, i.e., a set such that for every $C \in \mathscr{C}$ there is $\alpha \in \mathscr{H}$ such that $C(\alpha) \neq 0$.

POLYNOMIAL IDENTITY TESTING

Given an algebraic circuit C, decide **deterministically** whether C computes the zero polynomial.

Black-box: compute a hitting set $\mathscr{H}$, i.e., a set such that for every $C \in \mathscr{C}$ there is $\alpha \in \mathscr{H}$ such that $C(\alpha) \neq 0$.

Suppose D is a distinguisher for a class $\mathscr{C}$. Then $D \not\equiv 0$, and yet $D(\mathrm{coeff}(f)) = 0$ for all $f \in \mathscr{C}$.

POLYNOMIAL IDENTITY TESTING

Given an algebraic circuit C, decide **deterministically** whether C computes the zero polynomial.

Black-box: compute a hitting set $\mathscr{H}$, i.e., a set such that for every $C \in \mathscr{C}$ there is $\alpha \in \mathscr{H}$ such that $C(\alpha) \neq 0$.

Suppose D is a distinguisher for a class $\mathscr{C}$. Then $D \not\equiv 0$, and yet $D(\mathrm{coeff}(f)) = 0$ for all $f \in \mathscr{C}$.

$\implies \{\mathrm{coeff}(f) : f \in \mathscr{C}\}$ is **not** a hitting set for D.

POLYNOMIAL IDENTITY TESTING

Given an algebraic circuit C, decide **deterministically** whether C computes the zero polynomial.

Black-box: compute a hitting set $\mathscr{H}$, i.e., a set such that for every $C \in \mathscr{C}$ there is $\alpha \in \mathscr{H}$ such that $C(\alpha) \neq 0$.

Suppose D is a distinguisher for a class $\mathscr{C}$. Then $D \not\equiv 0$, and yet $D(\mathrm{coeff}(f)) = 0$ for all $f \in \mathscr{C}$.

$\implies \{\mathrm{coeff}(f) : f \in \mathscr{C}\}$ is **not** a hitting set for D.

In other words: if $\{\mathrm{coeff}(f) : f \in \mathscr{C}\}$ is a hitting set for a class $\mathscr{D}$, then no natural proof for $\mathscr{C}$ with the distinguisher coming from $\mathscr{D}$.

SUCCINCT HITTING SETS

Def: Let $\mathscr{C} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be a class of degree d polynomials, and $\mathscr{D} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ for $N = \binom{n+d}{d}$. $\mathscr{C}$ is a **succinct hitting set** for $\mathscr{D}$ if $\mathscr{H} := \{\mathrm{coeff}(f) : f \in \mathscr{C}\}$ is a hitting set for $\mathscr{D}$.

SUCCINCT HITTING SETS

Def: Let $\mathscr{C} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be a class of degree d polynomials, and $\mathscr{D} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ for $N = \binom{n+d}{d}$. $\mathscr{C}$ is a **succinct hitting set** for $\mathscr{D}$ if $\mathscr{H} := \{\mathrm{coeff}(f) : f \in \mathscr{C}\}$ is a hitting set for $\mathscr{D}$.

Thm: If $\mathscr{C}$ is a succinct hitting set for $\mathscr{D}$, no algebraically natural proof against $\mathscr{C}$ with the distinguisher coming from $\mathscr{D}$.

SUCCINCT HITTING SETS

Def: Let $\mathscr{C} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be a class of degree d polynomials, and $\mathscr{D} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ for $N = \binom{n+d}{d}$. $\mathscr{C}$ is a **succinct hitting set** for $\mathscr{D}$ if $\mathscr{H} := \{\mathrm{coeff}(f) : f \in \mathscr{C}\}$ is a hitting set for $\mathscr{D}$.

Thm: If $\mathscr{C}$ is a succinct hitting set for $\mathscr{D}$, no algebraically natural proof against $\mathscr{C}$ with the distinguisher coming from $\mathscr{D}$.

Proof: If $D \in \mathscr{D}$ is non-zero then D does not vanish on $\mathscr{H}$. $\square$

SUCCINCT HITTING SETS

Def: Let $\mathscr{C} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be a class of degree d polynomials, and $\mathscr{D} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ for $N = \binom{n+d}{d}$. $\mathscr{C}$ is a **succinct hitting set** for $\mathscr{D}$ if $\mathscr{H} := \{\mathrm{coeff}(f) : f \in \mathscr{C}\}$ is a hitting set for $\mathscr{D}$.

Thm: If $\mathscr{C}$ is a succinct hitting set for $\mathscr{D}$, no algebraically natural proof against $\mathscr{C}$ with the distinguisher coming from $\mathscr{D}$.

Proof: If $D \in \mathscr{D}$ is non-zero then D does not vanish on $\mathscr{H}$. $\square$

(also observed independently by **[Grochow-Kumar-Saraf-Saks]**)

SUCCINCT HITTING SETS

Def: Let $\mathscr{C} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be a class of degree d polynomials, and $\mathscr{D} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ for $N = \binom{n+d}{d}$. $\mathscr{C}$ is a **succinct hitting set** for $\mathscr{D}$ if $\mathscr{H} := \{\mathrm{coeff}(f) : f \in \mathscr{C}\}$ is a hitting set for $\mathscr{D}$.

Thm: If $\mathscr{C}$ is a succinct hitting set for $\mathscr{D}$, no algebraically natural proof against $\mathscr{C}$ with the distinguisher coming from $\mathscr{D}$.

Proof: If $D \in \mathscr{D}$ is non-zero then D does not vanish on $\mathscr{H}$. $\square$

(also observed independently by **[Grochow-Kumar-Saraf-Saks]**)

Question: are $\mathrm{poly}(n)$ size and $\mathrm{poly}(n)$ degree circuits a hitting sets for $\mathrm{poly}(N)$ size and $\mathrm{poly}(N)$ degree circuits?

("does VP hit VP?")

Algebraic Natural Proofs Barrier

Let $\mathscr{H} = \{\mathrm{coeff}(f) : f \in \mathrm{VP}(n)\}$. If $\mathscr{H}$ is a hitting set for $\mathrm{VP}(N)$ then there are no VP-algebraic natural proofs against VP.

ALGEBRAIC NATURAL PROOFS BARRIER

Let $\mathscr{H} = \{\text{coeff}(f) : f \in \text{VP}(n)\}$. If $\mathscr{H}$ is a hitting set for $\text{VP}(N)$ then there are no VP-algebraic natural proofs against VP.

ALGEBRAIC NATURAL PROOFS BARRIER

Let $\mathscr{H} = \{\mathrm{coeff}(f) : f \in \mathrm{VP}(n)\}$. If $\mathscr{H}$ is a hitting set for $\mathrm{VP}(N)$ then there are no VP-algebraic natural proofs against VP.

(note: $\mathscr{H}$ may a-priori be infinite but we'll soon see that this actually implies there exists some small $\mathscr{H}'$)

GENERATORS

Def: A polynomial map $\mathscr{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{N}$ is a generator for a class $\mathscr{C}$ if for every non-zero $F \in \mathscr{C}$, $F(\mathscr{G}(\mathbf{y})) \not\equiv 0$.

GENERATORS

Def: A polynomial map $\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{N}$ is a generator for a class $\mathscr{C}$ if for every non-zero $F \in \mathscr{C}$, $F(\mathcal{G}(\mathbf{y})) \not\equiv 0$.

(want: deg $\mathbf{poly}(N)$, ℓ as small as possible)

GENERATORS

Def: A polynomial map $\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{N}$ is a generator for a class $\mathscr{C}$ if for every non-zero $F \in \mathscr{C}$, $F(\mathcal{G}(\mathbf{y})) \not\equiv 0$.

(want: deg $\mathbf{poly}(N)$, ℓ as small as possible)

generators $\iff$ hitting sets

Generators

Def: A polynomial map $\mathcal{G} : \mathbb{F}^\ell \to \mathbb{F}^N$ is a generator for a class $\mathcal{C}$ if for every non-zero $F \in \mathcal{C}$, $F(\mathcal{G}(\mathbf{y})) \not\equiv 0$.

(want: deg $\mathbf{poly}(N)$, ℓ as small as possible)

generators $\iff$ hitting sets

($\implies$: evaluate. $\impliedby$: interpolate.)

GENERATORS

Def: A polynomial map $\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{N}$ is a generator for a class $\mathscr{C}$ if for every non-zero $F \in \mathscr{C}$, $F(\mathcal{G}(\mathbf{y})) \not\equiv 0$.

(want: deg $\mathrm{poly}(N)$, ℓ as small as possible)

generators $\iff$ hitting sets

($\implies$: evaluate. $\impliedby$: interpolate.)

succinct hitting sets $\implies$?

SUCCINCT GENERATOR

Def: A polynomial $G(\mathbf{x}, \mathbf{y})$ is a $\mathscr{C}$-succinct generator for $\mathscr{D}$ if:

Succinct Generator

Def: A polynomial $G(\mathbf{x}, \mathbf{y})$ is a $\mathscr{C}$-succinct generator for $\mathscr{D}$ if:

1. For every α, $G(\mathbf{x}, \alpha) \in \mathscr{C}$.

SUCCINCT GENERATOR

Def: A polynomial $G(\mathbf{x}, \mathbf{y})$ is a $\mathscr{C}$-succinct generator for $\mathscr{D}$ if:

1. For every α, $G(\mathbf{x}, \alpha) \in \mathscr{C}$.
2. The polynomial map $\mathscr{G} = \mathrm{coeff}_{\mathbf{x}}(G(\mathbf{x}, \mathbf{y}))$ is a generator for $\mathscr{D}$.

Succinct Generator

Def: A polynomial $G(\mathbf{x},\mathbf{y})$ is a $\mathscr{C}$-succinct generator for $\mathscr{D}$ if:

1. For every α, $G(\mathbf{x},\alpha) \in \mathscr{C}$.
2. The polynomial map $\mathscr{G} = \mathrm{coeff}_{\mathbf{x}}(G(\mathbf{x},\mathbf{y}))$ is a generator for $\mathscr{D}$.

$$G(x,y) = 1\cdot(y_1+y_2) + x_1\cdot(y_1y_2^3) + x_2\cdot(y_1^2+y_2) + x_1x_2\cdot 1$$

$$\mathscr{G}(\mathbf{y}) = (y_1+y_2\,,\; y_1y_2^3\,,\; y_1^2+y_2\,,\; 1)$$

Succinct Generator

Def: A polynomial $G(\mathbf{x}, \mathbf{y})$ is a $\mathscr{C}$-succinct generator for $\mathscr{D}$ if:

1. For every α, $G(\mathbf{x}, \alpha) \in \mathscr{C}$.
2. The polynomial map $\mathscr{G} = \mathrm{coeff}_{\mathbf{x}}(G(\mathbf{x}, \mathbf{y}))$ is a generator for $\mathscr{D}$.

$$G(x, y) = 1 \cdot (y_1 + y_2) + x_1 \cdot (y_1 y_2^3) + x_2 \cdot (y_1^2 + y_2) + x_1 x_2 \cdot 1$$
$$\mathscr{G}(\mathbf{y}) = (y_1 + y_2\,,\ y_1 y_2^3\,,\ y_1^2 + y_2\,,\ 1)$$

$\{G(\mathbf{x}, \alpha) : \alpha \in \mathbb{F}^\ell\}$ is a $\mathscr{C}$-succinct hitting set against $\mathscr{D}$.

So succinct generator $\implies$ succinct hitting set (and even a "uniform" one).

SUCCINCT GENERATOR

Def: A polynomial $G(\mathbf{x}, \mathbf{y})$ is a $\mathscr{C}$-succinct generator for $\mathscr{D}$ if:

1. For every α, $G(\mathbf{x}, \alpha) \in \mathscr{C}$.
2. The polynomial map $\mathscr{G} = \mathrm{coeff}_{\mathbf{x}}(G(\mathbf{x}, \mathbf{y}))$ is a generator for $\mathscr{D}$.

Aside: why not just require $G(\mathbf{x}, \mathbf{y}) \in \mathscr{C}$?

Succinct Generator

Def: A polynomial $G(\mathbf{x},\mathbf{y})$ is a $\mathscr{C}$-succinct generator for $\mathscr{D}$ if:

1. For every α, $G(\mathbf{x},\alpha) \in \mathscr{C}$.
2. The polynomial map $\mathscr{G} = \mathrm{coeff}_{\mathbf{x}}(G(\mathbf{x},\mathbf{y}))$ is a generator for $\mathscr{D}$.

Aside: why not just require $G(\mathbf{x},\mathbf{y}) \in \mathscr{C}$?

We can, but

1. unnecessary for succinct hitting sets which imply barriers
2. $G(\mathbf{x},\alpha)$ might be in even smaller class (e.g., if $\mathbf{y}$ has high deg)

SUCCINCT GENERATORS AND HITTING SETS

Recall: succinct generator $\implies$ succinct hitting sets.

SUCCINCT GENERATORS AND HITTING SETS

Recall: succinct generator $\implies$ succinct hitting sets.

Other direction?

Succinct generators and hitting sets

Recall: succinct generator $\implies$ succinct hitting sets.

Other direction?

Interpolating has complexity $\mathbf{poly}(|\mathscr{H}|)$ which is not succinct.

Succinct generators and hitting sets

Recall: succinct generator $\implies$ succinct hitting sets.

Other direction?

Interpolating has complexity $\mathbf{poly}(|\mathscr{H}|)$ which is not succinct.

But still true because of the existence of universal circuits.

SUCCINCT GENERATORS AND HITTING SETS

Recall: succinct generator $\implies$ succinct hitting sets.

Other direction?

Interpolating has complexity $\mathrm{poly}(|\mathscr{H}|)$ which is not succinct.

But still true because of the existence of universal circuits.

In particular, if $\mathscr{H} := \{\mathrm{coeff}(f) : f \in \mathrm{VP}(n)\}$ is an (infinite) hitting set for $\mathrm{VP}(N)$, there is a $N^{\mathrm{poly}\log(N)}$ size hitting set ($\mathscr{H}$ is in the image of a universal circuit).

EVIDENCE?

Conjecture: VP hits VP.

EVIDENCE?

Conjecture: VP hits VP.

How to obtain evidence to support this conjecture?

Evidence?

Conjecture: VP hits VP.

How to obtain evidence to support this conjecture?

Can we construct algebraic pseudorandom functions?

EVIDENCE?

Conjecture: VP hits VP.

How to obtain evidence to support this conjecture?

Can we construct algebraic pseudorandom functions?

[Aaronson-Drucker]'s candidate:

$$\det\left(\qquad \ell_{i,j}(\mathbf{x}) \qquad \right)$$

where $\ell_{i,j}$'s are random linear functions.

EVIDENCE?

Conjecture: VP hits VP.

How to obtain evidence to support this conjecture?

Can we construct algebraic pseudorandom functions?

[Aaronson-Drucker]'s candidate:

$$\det\left(\quad \ell_{i,j}(\mathbf{x}) \quad \right)$$

where $\ell_{i,j}$'s are random linear functions.

Conjecture: this is pseudorandom (maybe only against alg ckts?)

EVIDENCE?

Conjecture: VP hits VP.

How to obtain evidence to support this conjecture?

Can we construct algebraic pseudorandom functions?

[Aaronson-Drucker]'s candidate:

$$\det\begin{pmatrix} & & \\ & \ell_{i,j}(\mathbf{x}) & \\ & & \end{pmatrix}$$

where $\ell_{i,j}$'s are random linear functions.

Conjecture: this is pseudorandom (maybe only against alg ckts?)

Challange: establish this under some crypto hardness assumption.

Provable evidence?

This work: nearly all the hitting sets we know for restricted models can be made succinct.

Provable evidence?

This work: nearly all the hitting sets we know for restricted models can be made succinct.

Thm: coefficient vectors of $\mathrm{poly}(\log s, n)$ size multilinear formulas are hitting sets for $N = 2^n$ variate size s:

PROVABLE EVIDENCE?

This work: nearly all the hitting sets we know for restricted models can be made succinct.

Thm: coefficient vectors of $\mathrm{poly}(\log s, n)$ size multilinear formulas are hitting sets for $N = 2^n$ variate size s:

- $\Sigma^k \Pi \Sigma$ formulas,

Provable Evidence?

This work: nearly all the hitting sets we know for restricted models can be made succinct.

Thm: coefficient vectors of $\mathrm{poly}(\log s, n)$ size multilinear formulas are hitting sets for $N = 2^n$ variate size s:

- $\Sigma^k\Pi\Sigma$ formulas,
- $\Sigma\Pi\Sigma$ formulas of constant transcendence degree,

PROVABLE EVIDENCE?

This work: nearly all the hitting sets we know for restricted models can be made succinct.

Thm: coefficient vectors of $\mathrm{poly}(\log s, n)$ size multilinear formulas are hitting sets for $N = 2^n$ variate size s:

- $\Sigma^k\Pi\Sigma$ formulas,
- $\Sigma\Pi\Sigma$ formulas of constant transcendence degree,
- sparse polynomials,

PROVABLE EVIDENCE?

This work: nearly all the hitting sets we know for restricted models can be made succinct.

Thm: coefficient vectors of $\mathrm{poly}(\log s, n)$ size multilinear formulas are hitting sets for $N = 2^n$ variate size s:

- $\Sigma^k \Pi \Sigma$ formulas,
- $\Sigma\Pi\Sigma$ formulas of constant transcendence degree,
- sparse polynomials,
- $\Sigma \mathrm{m} \wedge \Sigma\Pi^{O(1)}$ formulas,

PROVABLE EVIDENCE?

This work: nearly all the hitting sets we know for restricted models can be made succinct.

Thm: coefficient vectors of $\mathrm{poly}(\log s, n)$ size multilinear formulas are hitting sets for $N = 2^n$ variate size s:

- $\Sigma^k\Pi\Sigma$ formulas,
- $\Sigma\Pi\Sigma$ formulas of constant transcendence degree,
- sparse polynomials,
- $\Sigma\mathrm{m}\wedge\Sigma\Pi^{O(1)}$ formulas,
- commutative roABPs,

PROVABLE EVIDENCE?

This work: nearly all the hitting sets we know for restricted models can be made succinct.

Thm: coefficient vectors of $\mathrm{poly}(\log s, n)$ size multilinear formulas are hitting sets for $N = 2^n$ variate size s:

- $\Sigma^k \Pi \Sigma$ formulas,
- $\Sigma\Pi\Sigma$ formulas of constant transcendence degree,
- sparse polynomials,
- $\Sigma \mathrm{m} \wedge \Sigma \Pi^{O(1)}$ formulas,
- commutative roABPs,
- depth-$O(1)$ Occur-$O(1)$ formulas

PROVABLE EVIDENCE?

This work: nearly all the hitting sets we know for restricted models can be made succinct.

Thm: coefficient vectors of $\mathrm{poly}(\log s, n)$ size multilinear formulas are hitting sets for $N = 2^n$ variate size s:

- $\Sigma^k \Pi \Sigma$ formulas,
- $\Sigma \Pi \Sigma$ formulas of constant transcendence degree,
- sparse polynomials,
- $\Sigma \mathrm{m} \wedge \Sigma \Pi^{O(1)}$ formulas,
- commutative roABPs,
- depth-$O(1)$ Occur-$O(1)$ formulas
- circuits composed with sparse polynomials of transcendence degree $O(1)$.

YET MORE:

Not as succinct but still worth mentioning:

YET MORE:

Not as succinct but still worth mentioning:

width w^2 length-n roABPs are hitting set for width-w length-N roABPs (in certain variable orders).

YET MORE:

Not as succinct but still worth mentioning:

width w^2 length-n roABPs are hitting set for width-w length-N roABPs (in certain variable orders).

(open: make the w^2 closer to $\mathbf{poly}\log(w)$ and remove the restriction on ordering)

YET MORE:

Not as succinct but still worth mentioning:

width w^2 length-n roABPs are hitting set for width-w length-N roABPs (in certain variable orders).

(open: make the w^2 closer to $\operatorname{poly}\log(w)$ and remove the restriction on ordering)

We can’t make all known hitting sets succinct but we have some excuses (more on that later).

HOW TO CONSTRUCT A SUCCINCT HITTING SET

Toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials with monomials of support $\leq \operatorname{poly}\log(N)$.

How to construct a succinct hitting set

Toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials with monomials of support $\leq \operatorname{poly}\log(N)$.

Hitting set for $\mathscr{C}$: $\{\mathbf{v} : \operatorname{supp}(\mathbf{v}) \leq \operatorname{poly}\log(N) = \operatorname{poly}(n)\}$.

HOW TO CONSTRUCT A SUCCINCT HITTING SET

Toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials with monomials of support $\leq \operatorname{poly}\log(N)$.

Hitting set for $\mathscr{C}$: $\{\mathbf{v} : \operatorname{supp}(\mathbf{v}) \leq \operatorname{poly}\log(N) = \operatorname{poly}(n)\}$.

("guess" vars in small support monomials, brute-force over them)

HOW TO CONSTRUCT A SUCCINCT HITTING SET

Toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials with monomials of support $\leq \operatorname{poly}\log(N)$.

Hitting set for $\mathscr{C}$: $\{\mathbf{v} : \operatorname{supp}(\mathbf{v}) \leq \operatorname{poly}\log(N) = \operatorname{poly}(n)\}$.

("guess" vars in small support monomials, brute-force over them)

Q: Is this succinct?

How to Construct a Succinct Hitting Set

Toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials with monomials of support $\leq \mathrm{poly}\log(N)$.

Hitting set for $\mathscr{C}$: $\{\mathbf{v} : \mathrm{supp}(\mathbf{v}) \leq \mathrm{poly}\log(N) = \mathrm{poly}(n)\}$.

("guess" vars in small support monomials, brute-force over them)

Q: Is this succinct?

A: Yes. Each $\mathbf{v}$ is a coefficient vector of a $\mathrm{poly}(n)$ $\Sigma\Pi$ circuit in $x_1, \ldots, x_n$ (only $\mathrm{poly}(n)$ monomials with non-zero coefficient). $\square$

SPARSE POLYNOMIALS

Less-of-a-toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials of sparsity at most s.

SPARSE POLYNOMIALS

Less-of-a-toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials of sparsity at most s.

$F \in \mathscr{C}$ doesn't necessarily contain small support monomials.

SPARSE POLYNOMIALS

Less-of-a-toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials of sparsity at most s.

$F \in \mathscr{C}$ doesn't necessarily contain small support monomials.

Exercise: if $F(\mathbf{X})$ has sparsity $\leq s$, $F(\mathbf{X} + \mathbf{1})$ has non-zero monomial of support $\leq \log s$.

[Forbes15, Gurjar-Korwar-Saxena-Theirauf16]

SPARSE POLYNOMIALS

Less-of-a-toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials of sparsity at most s.

$F \in \mathscr{C}$ doesn't necessarily contain small support monomials.

Exercise: if $F(\mathbf{X})$ has sparsity $\leq s$, $F(\mathbf{X} + \mathbf{1})$ has non-zero monomial of support $\leq \log s$.

[Forbes15, Gurjar-Korwar-Saxena-Theirauf16]

Cor: $\{\mathbf{v} + \mathbf{1} : \mathrm{supp}(\mathbf{v}) \leq \mathrm{poly}\log(s)\}$ hitting set for $\mathscr{C}$.

SPARSE POLYNOMIALS

Less-of-a-toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials of sparsity at most s.

$F \in \mathscr{C}$ doesn't necessarily contain small support monomials.

Exercise: if $F(\mathbf{X})$ has sparsity $\leq s$, $F(\mathbf{X}+\mathbf{1})$ has non-zero monomial of support $\leq \log s$.

[Forbes15, Gurjar-Korwar-Saxena-Theirauf16]

Cor: $\{\mathbf{v}+\mathbf{1} : \mathrm{supp}(\mathbf{v}) \leq \mathrm{poly}\log(s)\}$ hitting set for $\mathscr{C}$.

Q: Is **this** succinct?

SPARSE POLYNOMIALS

Less-of-a-toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials of sparsity at most s.

$F \in \mathscr{C}$ doesn't necessarily contain small support monomials.

Exercise: if $F(\mathbf{X})$ has sparsity $\leq s$, $F(\mathbf{X} + \mathbf{1})$ has non-zero monomial of support $\leq \log s$.
[Forbes15, Gurjar-Korwar-Saxena-Theirauf16]

Cor: $\{\mathbf{v} + \mathbf{1} : \mathrm{supp}(\mathbf{v}) \leq \mathrm{poly}\log(s)\}$ hitting set for $\mathscr{C}$.

Q: Is **this** succinct?

A: Yes. $\mathbf{1}$ is coeff vector of $\prod_{i=1}^{n}(x_i + 1)$. Now take the sum of this and the circuit from previous slide. $\square$

SPARSE POLYNOMIALS

Less-of-a-toy example: $\mathscr{C} \subseteq \mathbb{F}[X_1, \ldots, X_N]$ is the class of polynomials of sparsity at most s.

$F \in \mathscr{C}$ doesn't necessarily contain small support monomials.

Exercise: if $F(\mathbf{X})$ has sparsity $\leq s$, $F(\mathbf{X}+\mathbf{1})$ has non-zero monomial of support $\leq \log s$.
[Forbes15, Gurjar-Korwar-Saxena-Theirauf16]

Cor: $\{\mathbf{v}+\mathbf{1} : \mathrm{supp}(\mathbf{v}) \leq \mathrm{poly}\log(s)\}$ hitting set for $\mathscr{C}$.

Q: Is **this** succinct?

A: Yes. $\mathbf{1}$ is coeff vector of $\prod_{i=1}^{n}(x_i+1)$. Now take the sum of this and the circuit from previous slide. $\square$

Cor: $\mathrm{poly}(\log s, n)$-$\Sigma\Pi\Sigma$ succinct hitting set for sparse polynomials.

MORE SUCCINCT HITTING SETS

In the paper: many other succinct generators, most of them follow from various combinations of basic constructs such as **Shpilka-Volkovich generator** and Gabizon-Raz's **rank condenser**, which we make succinct.

MORE SUCCINCT HITTING SETS

In the paper: many other succinct generators, most of them follow from various combinations of basic constructs such as **Shpilka-Volkovich generator** and Gabizon-Raz's **rank condenser**, which we make succinct.

Builds on a lot of previous work: **[Dvir-Shpilka, Karnin-Shpilka, Kayal-Saraf, Saxena-Seshadhri, Shpilka-Volkovich, Forbes-Shpilka, Forbes-Shpilka-Saptharishi, Beecken-Mittmann-Saxena, Agrawal-Saha-Saxena-Saptharishi,...]**.

MORE SUCCINCT HITTING SETS

In the paper: many other succinct generators, most of them follow from various combinations of basic constructs such as **Shpilka-Volkovich generator** and Gabizon-Raz's **rank condenser**, which we make succinct.

Builds on a lot of previous work: **[Dvir-Shpilka, Karnin-Shpilka, Kayal-Saraf, Saxena-Seshadhri, Shpilka-Volkovich, Forbes-Shpilka, Forbes-Shpilka-Saptharishi, Beecken-Mittmann-Saxena, Agrawal-Saha-Saxena-Saptharishi,...]**.

Cor: Super-polynomial lower bounds on defining equations of $\overline{\mathrm{VP}}$ in many models.

What we can't do

conspicuously missing: **Klivans-Spielman** (Kronecker) generator.

WHAT WE CAN'T DO

conspicuously missing: **Klivans-Spielman** (Kronecker) generator.

$$X_i \mapsto y^{k^i} \mod p$$

y new var, k integer and p prime chosen from sufficiently large set.

WHAT WE CAN'T DO

conspicuously missing: **Klivans-Spielman** (Kronecker) generator.

$$X_i \mapsto y^{k^i} \mod p$$

y new var, k integer and p prime chosen from sufficiently large set.

Hits sparse polynomials and very useful in other constructions.

What we can't do

conspicuously missing: **Klivans-Spielman** (Kronecker) generator.

$$X_i \mapsto y^{k^i \mod p}$$

y new var, k integer and p prime chosen from sufficiently large set.

Hits sparse polynomials and very useful in other constructions.

Challenge: make it succinct, i.e., find a small circuit in $\{x_1, \ldots, x_n, y\}$ such that the coefficient of $\mathbf{x}_S$ is $y^{k^{\mathrm{bin}(S)} \mod p}$, $\mathrm{bin}(S) =$ integer whose binary expansion is the characteristic vector of S.

USEFULNESS OF KS

The generator $X_i \mapsto y_1^{k^i \mod p_1} \cdots y_m^{k^i \mod p_m}$ for $m = O(\log n)$ hits roABPs (in any order) and read-once determinants

(polys of the form $\det(M)$ where each entry in M contains a var or a constant and each var appears at most once)

[Agrawal-Gurjar-Korwar-Saxena, Fenner-Gurjar-Thierauf, Gurjar-Thierauf]

USEFULNESS OF KS

The generator $X_i \mapsto y_1^{k^i \mod p_1} \cdots y_m^{k^i \mod p_m}$ for $m = O(\log n)$ hits roABPs (in any order) and read-once determinants

(polys of the form $\det(M)$ where each entry in M contains a var or a constant and each var appears at most once)

[Agrawal-Gurjar-Korwar-Saxena, Fenner-Gurjar-Thierauf, Gurjar-Thierauf]

[Raz] and **[Raz-Yehudayoff]** showed: small multilinear formulas are not a hitting set for read-once determinants.

USEFULNESS OF KS

The generator $X_i \mapsto y_1^{k^i \bmod p_1} \cdots y_m^{k^i \bmod p_m}$ for $m = O(\log n)$ hits roABPs (in any order) and read-once determinants

(polys of the form $\det(M)$ where each entry in M contains a var or a constant and each var appears at most once)

[Agrawal-Gurjar-Korwar-Saxena, Fenner-Gurjar-Thierauf, Gurjar-Thierauf]

[Raz] and **[Raz-Yehudayoff]** showed: small multilinear formulas are not a hitting set for read-once determinants.

Our constructions are all small multilinear formulas, so we might need new ideas.

More Open Problems

More models for which we know of hitting sets but not succinct ones:

More Open Problems

More models for which we know of hitting sets but not succinct ones:

- roABPs in any order
- read-k oblivious ABPs
- bounded-depth multilinear formulas

More Open Problems

More models for which we know of hitting sets but not succinct ones:

- roABPs in any order
- read-k oblivious ABPs
- bounded-depth multilinear formulas

Also: pseudorandom polynomials?
Is **[Aaronson-Drucker]**'s construction pseudorandom?

MORE OPEN PROBLEMS

More models for which we know of hitting sets but not succinct ones:

- roABPs in any order
- read-k oblivious ABPs
- bounded-depth multilinear formulas

Also: pseudorandom polynomials?
Is **[Aaronson-Drucker]**'s construction pseudorandom?

THANK YOU