Succinct Hitting Sets and Algebraic Circuit Lower Bound Barriers[1]

[1] Forbes et al. (2017)

Outline

Introductin

Natural Proofs

Algebraic Natural Proofs
- Framework
- Succinct Derandomisation
- Succinct Generators

Evidence for Barriers

References

Boolean Natural Proofs

- Razborov and Rudich (1997) introduced the notion of natural proofs. Showed that many proofs are natural.

Boolean Natural Proofs

- Razborov and Rudich (1997) introduced the notion of natural proofs. Showed that many proofs are natural.
- Also showed that assuming crypto, natural proofs cannot give superpoly lower bounds.

Boolean Natural Proofs

- Razborov and Rudich (1997) introduced the notion of natural proofs. Showed that many proofs are natural.
- Also showed that assuming crypto, natural proofs cannot give superpoly lower bounds.
- In particular, existance of $\exp\left(n^{\Omega(1)}\right)$ prg.

Algebraic Natural Proofs?

- Natural question, are there barriers for algebraic proofs.

Algebraic Natural Proofs?

- Natural question, are there barriers for algebraic proofs.
- Missing key ingredient - crypto.

Algebraic Natural Proofs?

- Natural question, are there barriers for algebraic proofs.
- Missing key ingredient - crypto.
- Fix: reduce to derandomisation problem, like Williams (2013).

Razborov and Rudich: Useful Properties, Natural Proofs

- Property P is a subset of boolean functions,

$$P \subseteq \bigcup_{n \geq 1} \{f \mid f : \{0,1\}^n \to \{0,1\}\}.$$

Razborov and Rudich: Useful Properties, Natural Proofs

- Property P is a subset of boolean functions,

$$P \subseteq \bigcup_{n \geq 1} \{f \mid f : \{0,1\}^n \to \{0,1\}\}.$$

- Γ-constructive: If we can check $f \in P$ in Γ, given truth table.
- Large if atleast $2^{\mathcal{O}(n)}$ fraction of f in P.

Such a property is called Γ-natural.

Razborov and Rudich: Useful Properties, Natural Proofs

- Property P is a subset of boolean functions,

$$P \subseteq \bigcup_{n \geq 1} \{f \mid f : \{0,1\}^n \to \{0,1\}\}.$$

- Γ-constructive: If we can check $f \in P$ in Γ, given truth table.
- Large if atleast $2^{\mathcal{O}(n)}$ fraction of f in P.

Such a property is called Γ-natural.

- Useful against $\mathcal{C}$ if $f \in \mathcal{C} \Rightarrow f \notin P$.

Razborov and Rudich: Useful Properties, Natural Proofs

- Property P is a subset of boolean functions,

$$P \subseteq \bigcup_{n \geq 1} \{f \mid f : \{0,1\}^n \to \{0,1\}\}.$$

- Γ-constructive: If we can check $f \in P$ in Γ, given truth table.
- Large if atleast $2^{\mathcal{O}(n)}$ fraction of f in P.

Such a property is called Γ-natural.

- Useful against $\mathcal{C}$ if $f \in \mathcal{C} \Rightarrow f \notin P$.
- A proof is natural against $\mathcal{C}$ if it contains the definition of a natural P.

Razborov and Rudich: Quote

Quoting the original paper:
... consider a commonly envisioned proof strategy for showing $P \neq NP$.

- Formulate some mathematical notion of "discrepency" ... (... formalised as a combinatorial property P ...).
- Show that poly sized circuits can only compute "low discrepency" functions ... (... P is useful ...).
- SAT has "high discrepency" ... (... SAT has P ...).

Razborov and Rudich: Quote

Quoting the original paper:
... consider a commonly envisioned proof strategy for showing $P \neq NP$.

- Formulate some mathematical notion of "discrepency" ... (... formalised as a combinatorial property P ...).
- Show that poly sized circuits can only compute "low discrepency" functions ... (... P is useful ...).
- SAT has "high discrepency" ... (... SAT has P ...).

Their main result: no such strategy can succeed.

Razborov and Rudich: Key Idea

- If there are prgs, we can get pseudorandom functions indistinguishable from uniform.
- But constructivity will give us an advantage in distinguishing the prf.

Razborov and Rudich: Key Idea

- If there are prgs, we can get pseudorandom functions indistinguishable from uniform.
- But constructivity will give us an advantage in distinguishing the prf.
- This works for any class powerful enough to have one-way functions.
- Under standard assumptions, includes classes like TC^0.

Williams: Succinct Derandomisation

- ZPE: solvable in randomised $2^{\mathcal{O}(n)}$ time, no error, allowed to answer don't know.
- Predicate for $L \in$ ZPE: Machine $M(x, y)$ such that for all x, for all y of length $2^{c|x|}$, in $2^{\mathcal{O}(|x|)}$, if $x \in L$ then $M(x, y)$ is 1 wp atleast $2/3$, and if $x \notin L$ then 0 wp atleast $2/3$.
- Given $\mathcal{C}$, ZPE has $\mathcal{C}$ seeds if for all $x, \exists \mathcal{C}_x \in \mathcal{C}$ of size $|x|^k + k$ such that $M(x, tt(C_x))$ is not don't know.

Williams: Succinct Derandomisation

- ZPE: solvable in randomised $2^{\mathcal{O}(n)}$ time, no error, allowed to answer don't know.
- Predicate for $L \in$ ZPE: Machine $M(x, y)$ such that for all x, for all y of length $2^{c|x|}$, in $2^{\mathcal{O}(|x|)}$, if $x \in L$ then $M(x, y)$ is 1 wp atleast $2/3$, and if $x \notin L$ then 0 wp atleast $2/3$.
- Given $\mathcal{C}$, ZPE has $\mathcal{C}$ seeds if for all $x, \exists \mathcal{C}_x \in \mathcal{C}$ of size $|x|^k + k$ such that $M(x, tt(C_x))$ is not don't know.
- There is no natural P-natural property useful against $\mathcal{C}$ iff ZPE has $\mathcal{C}$ seeds for almost all lengths.

Redefine Properties

- We slighly change the definition of a property.
- P is useful against $\mathcal{C}$ if all $f \in \mathcal{C}$ are in P.
- P is large if most f are NOT in P.

Redefine Properties

- We slighly change the definition of a property.
- P is useful against $\mathcal{C}$ if all $f \in \mathcal{C}$ are in P.
- P is large if most f are NOT in P.
- The complement of properties defined earlier, do not matter in boolean setting, do matter in algebraic.

Motivation - Rank Based Lower Bound Proofs

- Many lower bound proofs use matrix rank, for eg partial derivatives, shifted pds, etc.

Motivation - Rank Based Lower Bound Proofs

- Many lower bound proofs use matrix rank, for eg partial derivatives, shifted pds, etc.
- Given f, find a matrix M_f, entries polynomials in coefficients of f.
- Usually M_f is exponentially big.
- Show, that $\text{rank} M_f < r$ if $f \in \mathcal{C}$.
- For explicit h, show that $\text{rank} M_h \geq r$.

Motivation - Small rank is natural

- The above rank bounds are shown by identifying minor M' and showing $\det M'_f = 0$ and $\det M'_h \neq 0$.

Motivation - Small rank is natural

- The above rank bounds are shown by identifying minor M' and showing $\det M'_f = 0$ and $\det M'_h \neq 0$.
- This gives a natural property:

$$P := \left\{ f \mid \det(M'_f) = 0 \right\}.$$

- It is useful by definition, constructive since det is easy, and large by SZ.

Algebraic Natural Proof: Definition

Definition

Let $\mathcal{M}$ be a set of monomials. Given a polynomial $f \in \operatorname{span}(\mathcal{M})$, let $\operatorname{coeff}_{\mathcal{M}}(f)$ denote its coefficient vector, indexed by elements of $\mathcal{M}$.

Algebraic Natural Proof: Definition

Definition

Let $\mathcal{M}$ be a set of monomials. Given a polynomial $f \in \text{span}\,(\mathcal{M})$, let $\text{coeff}_{\mathcal{M}}(f)$ denote its coefficient vector, indexed by elements of $\mathcal{M}$. Let $\mathcal{C} \subseteq \text{span}\,(\mathcal{M})$ denote some complexity class.

Algebraic Natural Proof: Definition

Definition

Let $\mathcal{M}$ be a set of monomials. Given a polynomial $f \in \operatorname{span}(\mathcal{M})$, let $\operatorname{coeff}_{\mathcal{M}}(f)$ denote its coefficient vector, indexed by elements of $\mathcal{M}$. Let $\mathcal{C} \subseteq \operatorname{span}(\mathcal{M})$ denote some complexity class. Let $\mathcal{D} \subseteq \mathbb{F}\left[\{y_\alpha\}_{x^\alpha \in \mathcal{M}}\right]$ denote a class of polynomials in $|\mathcal{M}|$ many variables.

Algebraic Natural Proof: Definition

Definition

Let $\mathcal{M}$ be a set of monomials. Given a polynomial $f \in \operatorname{span}(\mathcal{M})$, let $\operatorname{coeff}_{\mathcal{M}}(f)$ denote its coefficient vector, indexed by elements of $\mathcal{M}$. Let $\mathcal{C} \subseteq \operatorname{span}(\mathcal{M})$ denote some complexity class. Let $\mathcal{D} \subseteq \mathbb{F}\left[\{y_\alpha\}_{x^\alpha \in \mathcal{M}}\right]$ denote a class of polynomials in $|\mathcal{M}|$ many variables. A non-zero polynomial $D \in \mathcal{D}$ is said to be a $\mathcal{D}$-natural proof against $\mathcal{C}$ if the following holds: for all $f \in \mathcal{C}$, the polynomial D vanishes on $\operatorname{coeff}_{\mathcal{M}}(f)$, that is $D(\operatorname{coeff}_{\mathcal{M}}(f)) = 0$.

Comparing to Razborov Rudich

- As in the motivating example, we get a property P, defined as

$$P := \{f \mid D(\mathrm{coeff}_{\mathcal{M}}(f) = 0\}\,.$$

Comparing to Razborov Rudich

- As in the motivating example, we get a property P, defined as

$$P := \{f \mid D(\mathrm{coeff}_{\mathcal{M}}(f) = 0\}\,.$$

- Constructive since $D \in \mathcal{D}$, large due to SZ, useful since D vanishes on coefficients.

Instantiation

- Let $\mathcal{M}$ be the set of monomials in n variables of total degree atmost d, and let $N = |\mathcal{M}| = \binom{n+d}{d}$.
- Let $\mathcal{C}$ be the set of polynomials poly (n, d)-sized circuits.

Instantiation

- Let $\mathcal{M}$ be the set of monomials in n variables of total degree atmost d, and let $N = |\mathcal{M}| = \binom{n+d}{d}$.
- Let $\mathcal{C}$ be the set of polynomials poly (n, d)-sized circuits.
- Is there an algebraic poly (N) sized natural proof for $\mathcal{C}$.

Instantiation

- Let $\mathcal{M}$ be the set of monomials in n variables of total degree atmost d, and let $N = |\mathcal{M}| = \binom{n+d}{d}$.
- Let $\mathcal{C}$ be the set of polynomials poly(n, d)-sized circuits.
- Is there an algebraic poly(N) sized natural proof for $\mathcal{C}$.
- In other words, are there VP natural proofs against VP.

PIT

- Given that algebraic natural proofs are based on vanishing of polynomials, derandomisation will be that of the PIT problem.

PIT

- Given that algebraic natural proofs are based on vanishing of polynomials, derandomisation will be that of the PIT problem.
- The equivalence here will follow from definitions, unlike the boolean setting.

Succinct Hitting Sets

Definition

Let $\mathcal{M}, \mathcal{C}, \mathcal{D}$ be defined as in the definition of algebraic natural proofs. We say that $\mathcal{C}$ is a $\mathcal{C}$-succinct hitting set for $\mathcal{D}$ if $\mathcal{H} := \{\mathrm{coeff}(f) \mid f \in \mathcal{C}\}$ is a hitting set for $\mathcal{D}$. In other words, $D \in \mathcal{D}$ is non-zero if and only if there is some $f \in \mathcal{C}$ such that $D(\mathrm{coeff}(f)) \neq 0$.

Succinct Hitting Sets

- If D is an algebraic natural proof for $\mathcal{C}$, then D must vanish on coefficient vectors $\mathcal{H}$.
- Thus, $\mathcal{H}$ is NOT a hitting set for $\mathcal{D}$.

Succinct Hitting Sets

- If D is an algebraic natural proof for $\mathcal{C}$, then D must vanish on coefficient vectors $\mathcal{H}$.
- Thus, $\mathcal{H}$ is NOT a hitting set for $\mathcal{D}$.
- There are algebraic natural proofs if and only if coefficient vectors of simple polynomials are not hitting sets.

Succinct Hitting Sets

- If D is an algebraic natural proof for $\mathcal{C}$, then D must vanish on coefficient vectors $\mathcal{H}$.
- Thus, $\mathcal{H}$ is NOT a hitting set for $\mathcal{D}$.
- There are algebraic natural proofs if and only if coefficient vectors of simple polynomials are not hitting sets.
- The existance of barriers is equivalent to whether PIT can be derandomised using succinct pseudorandomness.

Equivalence of Barriers and Derandomisation

Theorem

Let $\mathcal{M}, \mathcal{C}, \mathcal{D}$ be defined as in the definition of algebraic natural proofs. Then there is an algebraic $\mathcal{D}$-natural proof against $\mathcal{C}$ if and only if $\mathcal{C}$ is not a $\mathcal{C}$-succinct hitting set for $\mathcal{D}$.

Instantiating

Corollary

Let $\mathcal{C}$ be the class of $\operatorname{poly}(n, d)$*-sized circuits of total degree atmost d. Then there is an algebraic* $\operatorname{poly}(N)$*-natural proof against $\mathcal{C}$ if and only if $\mathcal{C}$ is not a* $\operatorname{poly}(n, d)$*-succinct hitting set for* $\operatorname{poly}(N)$*-sized circuits in N variables.*

Instantiating

Corollary

Let $\mathcal{C}$ be the class of $\operatorname{poly}(n, d)$*-sized circuits of total degree atmost d. Then there is an algebraic* $\operatorname{poly}(N)$*-natural proof against $\mathcal{C}$ if and only if $\mathcal{C}$ is not a* $\operatorname{poly}(n, d)$*-succinct hitting set for* $\operatorname{poly}(N)$*-sized circuits in N variables.*

If $d = \operatorname{poly}(n)$, then existence of barrier is equivalent to saying that coefficient vectors of polylog sized circuits are a hitting set for circuits of polynomial size.

Succinct Generators

Definition (Succinct Generators)

Let $\mathcal{C}, \mathcal{M}, \mathcal{D}$ be as in the earlier definitions. Let $\mathcal{C}' \subseteq \mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_l]$ be another class of polynomials. A polynomial map $\mathcal{G} : \mathbb{F}^l \to \mathbb{F}^{|\mathcal{M}|}$ is a $\mathcal{C}$-succinct generator for $\mathcal{D}$ computable in $\mathcal{C}'$ if the following conditions hold:

- The polynomial $G(\mathbf{x}, \mathbf{y}) := \sum_{\mathbf{x}^\alpha \in \mathcal{M}} \mathcal{G}_{\mathbf{x}^\alpha}(\mathbf{y})\mathbf{x}^\alpha$ is in $\mathcal{C}'$, where $\mathcal{G}_{\mathbf{x}^\alpha}$ is the coordinate of $\mathcal{G}$ corresponding to α.
- For every $\alpha \in \mathbb{F}^l$, the polynomial $G(\mathbf{x}, \alpha)$ is in $\mathcal{C}$.
- $\mathcal{G}$ is a generator for $\mathcal{D}$, that is $D(\text{coeff}_{\mathcal{M}}(\mathcal{G})) \neq 0$ as a polynomial if and only if D is non-zero. For this, we define $\text{coeff}_{\mathcal{M}}(\mathcal{G})$ by treating $\mathcal{G}$ as a polynomial in the variables $\mathbf{x}$ over the ring $\mathbb{F}[\mathbf{y}]$.

Interpretation

- The second and third conditions (when the field is large enough) are equivalent to the fact that the output $\mathcal{G}(\mathbf{x}, \mathbb{F}^l) = \left\{ G(\mathbf{x}, \alpha) \mid \alpha \in \mathbb{F}^l \right\}$ is a $\mathcal{C}$-succinct hitting set for $\mathcal{D}$ in the above sense.
- The first condition adds a succinct indexing condition on the generator.

Interpretation

- The second and third conditions (when the field is large enough) are equivalent to the fact that the output $\mathcal{G}(\mathbf{x}, \mathbb{F}^l) = \{ G(\mathbf{x}, \alpha) \mid \alpha \in \mathbb{F}^l \}$ is a $\mathcal{C}$-succinct hitting set for $\mathcal{D}$ in the above sense.
- The first condition adds a succinct indexing condition on the generator.
- It is clear that succinct generators give rise to succinct hitting sets. The converse also holds in some sense: if there are succinct hitting set, then the universal circuit is a succinct generator.

Example 1

- Let $\mathcal{D}$ be the set of polynomials with monomials of support size $\operatorname{poly}(\log N)$.
- A hitting set is $\{\mathbf{v} \mid \operatorname{supp}(v) \leq \operatorname{poly}(\log N) = \operatorname{poly}(n)\}$.

Example 1

- Let $\mathcal{D}$ be the set of polynomials with monomials of support size $\text{poly}(\log N)$.
- A hitting set is $\{\mathbf{v} \mid \text{supp}(v) \leq \text{poly}(\log N) = \text{poly}(n)\}$.
- These are coefficient vectors of $\sum \prod$ circuits of size $\text{poly}(n)$.

Example 2

- Let $\mathcal{D}$ be the class of polynomials of sparsity atmost s.
- We will use the following result: if $f(\mathbf{x})$ has sparsity $\leq s$ then $f(\mathbf{x}+\mathbf{1})$ has a monomial of support $\leq \log s$.
- A hitting set is $\{\mathbf{1}+\mathbf{v} \mid \text{supp}(v) \leq \text{poly}(\log N) = \text{poly}(n)\}$.

Example 2

- Let $\mathcal{D}$ be the class of polynomials of sparsity atmost s.
- We will use the following result: if $f(\mathbf{x})$ has sparsity $\leq s$ then $f(\mathbf{x} + \mathbf{1})$ has a monomial of support $\leq \log s$.
- A hitting set is $\{\mathbf{1} + \mathbf{v} \mid \mathrm{supp}(v) \leq \mathrm{poly}(\log N) = \mathrm{poly}(n)\}$.
- Since $\mathbf{1} = \mathrm{coeff}(g)$ where $g = \prod (x_i + 1)$, this is succinct.

Main Theorem

Theorem

The set of $\mathrm{poly}(\log s, n)$*-sized multilinear* $\sum\prod\sum$ *formulas is a succinct hitting set for* $N = 2^n$ *variate size* s *computations of the form*

- $\sum^{\mathcal{O}(1)}\prod\sum$ *formulas*
- $\sum\prod\sum$ *formulas of constant trdeg.*
- *Sparse polynomials*
- *Commutative roABPs*

References

Michael A. Forbes, Amir Shpilka, and Ben Lee Volk. Succinct hitting sets and barriers to proving algebraic circuits lower bounds. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 653–664, New York, NY, USA, 2017. ACM. ISBN 978-1-4503-4528-6. doi: 10.1145/3055399.3055496. URL `http://doi.acm.org/10.1145/3055399.3055496`.

Alexander A Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24 – 35, 1997. ISSN 0022-0000. doi: https://doi.org/10.1006/jcss.1997.1494. URL `http://www.sciencedirect.com/science/article/pii/S002200009791494X`.

Ryan Williams. Natural proofs versus derandomization. In *Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing*, STOC '13, pages 21–30, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-2029-0. doi: 10.1145/2488608.2488612. URL `http://doi.acm.org/10.1145/2488608.2488612`.