Overview of Succinct Hitting Sets and Barriers for Algebraic Lower Bounds

Abhibhav Garg

April 17, 2019

This is an overview of Forbes, Shpilka and Volk's framework of algebraically natural lower bounds for algebraic circuits (Forbes et al. (2017)).

Contents

1 Introduction

In the 90s, Razborov and Rudich (Razborov and Rudich (1997)) introduced the notion of natural proofs. They showed that a large number of lower bound proofs for boolean circuits are *natural* according to their definition. They also showed that under some cryptographic assumptions, such natural proofs cannot yield super-polynomial lower bounds against many restricted circuit classes. In particular, under the assumption that there are prgs of $\exp\left(n^{\Omega(1)}\right)$ hardness, there is no natural proof for resolving the P vs NP problem.

A natural question then is to ask whether such barriers exist for lower bounds against algebraic circuits. Given that boolean and algebraic circuits are similar in terms of the types of lower bounds proved for them, it seems plausible that there would be barriers to algebraic lower bounds. The missing ingredient in formulating a natural proof type lower bound barrier for algebraic circuits is that there are there is little to no evidence for the existence of algebraic pseudorandom functions. Algebraic circuits are a weaker model than general computation, and thus they might not be able to compute functions that general circuits cannot distinguish from uniform distributions, but it is still feasible that they can compute functions that can fool other algebraic circuits, which is sufficient for applications. Given this lack of algebraic prgs, evidence for algebraic natural proof barriers is given complexity theoretically, following in the steps of Williams (Williams (2013)) in relating the existance of natural proofs with succinct derandomisation.

The next section will provide (informally) some background on natural proofs and its relation to succinct derandomisation. The subsequent sections will set up the algebraic natural proofs framework, and then provide some evidence for barriers.

2 Natural Proofs

We first discuss the original setting of Razborov and Rudich. Ta-Shma and Doron (2016) is a good exposition for this. A property P is a subset of boolean functions,

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

For a complexity class Γ, Property P is called Γ-constructive there is an algorithm in Γ that can test whether $f \in P$ given the truth table for f (which is of size 2^n). Further, P is said to be large if atleast $2^{\mathcal{O}(n)}$ fraction of all boolean functions on n variables have this property. A property satisfying the above two conditions is called natural. Finally, a property is said to be useful against non-uniform class $\mathcal{C}$ if for large enough n, any boolean function f with a circuit from $\mathcal{C}$ does not belong to P.

Razborov and Rudich proved the following: Suppose there is a P-natural proof against P/poly, then there is a distinguisher for a pseudorandom function H that is built upon a prg G. They also showed that a number of known lower bound proofs for restricted circuit classes are actually natural, most of them directly. If these restricted circuit classes are powerful enough to compute prgs, then an argument similar to the above also shows that any natural proofs against these classes also give rise to distinguishers. Given the above, all of the evidence that there are hard prgs (of which there is plenty) is also evidence that natural proofs cannot give lower bounds.

More evidence for the barriers exist, following the framework of Williams. Let ZPE be the complexity class of languages solvable in $2^{\mathcal{O}(n)}$ time with randomness and no error (the machine is allowed to answer *don't know*). Given a language $L \in$ ZPE, a predicate for L is a turing machine $M(x, y)$ that runs in time $2^{\mathcal{O}(|x|)}$ on inputs y of length $2^{\mathcal{O}(|x|^c)}$ such that for every x, y, the following holds: if $x \in L$, then $M(x, y)$ outputs either don't know or 1, and the latter happens with probability atleast $2/3$ over all choices of y. If conversely, $x \neq L$, then the machine outputs either don't know or 0, and again the latter happens with probability $2/3$ over choices of y. Given a complexity class $\mathcal{C}$, we say that ZPE has $\mathcal{C}$ seeds if for every such turing machine M, there is a k such that for every x, there is a circuit $\mathcal{C}_x \in \mathcal{C}$ of size atmost $|x|^k + k$ such that $M(x, tt(\mathcal{C}_x)$ is not don't know. Williams then proved the following: there is no P-natural property useful against $\mathcal{C}$ if and only if ZPE has $\mathcal{C}$ seeds for almost all input lengths. Informally, having $\mathcal{C}$ seeds means that the class ZPE can be derandomised in a strong sense, by just trying out all poly sized circuits from $\mathcal{C}$ as random seeds. In particular, for many restricted classes of circuits, there have been constructions of prgs that fool these classes, and it turns out that the derandomisation that results from these prgs is succinct in the sense of Williams. This also provides evidence for the existance of natural proof barriers.

In the algerbaic setting, in the absense of algebraic prgs, evidence of the second type will be provided for the existance of barriers.

3 Algebraic Natural Proofs

3.1 Framework

We now discuss the framework of algebraic natural proofs. It will be advantageous to slighly change the definition of a property P. In particular, we will define a property to be useful against $\mathcal{C}$ if all functions in $\mathcal{C}$ do have this property, and we will call this property large if most functions do not have this property. A property in the new sense is exactly the complement of a property defined in the previous section.

We now motivate the definition of an algebraic natural proof before defining it. Consider the matrix rank. The full-rankness of a matrix M is captured by the non-zeroness of a polynomial, namely the determinant. Many lower bound proofs, such as partial derivatives and its variations, evaluation dimension, etc essentially do the following: given a polynomial f, they form a large matrix M_f using the coefficients of f. By then showing that simple polynomials, say those computed by circuits from $\mathcal{C}$ are such that M_f has rank $< r$, and showing that some explicit polynomial h has rank $\geq r$, a lower bound is obtained. The key observation is that low-rankness is a property that is natural in the sense described above (after the modification): Indeed that M_f has rank atmost r and that M_h has high rank is captured by identifying some $r \times r$ minor M'_f, M'_h of M_f, M_h (potentially after a linear transform) such that the determinant of M'_f is zero, and that of M'_h is non-zero. More formally, if we define property P as

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

it is easy to see that P is natural and useful against $\mathcal{C}$. That it is constructive follows from the fact that checking whether a determinant is zero is easy. That it is large follows from the fact that the determinant is a polynomial, and thus cannot have many roots. Finally, that it is useful follows from the fact that for all $\mathcal{C} \in f$, the rank of M_f is atmost r.

We can now define the notion of algebraic natural proofs.

Definition 3.1 (Algebraic Natural Proofs)**.** *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 $D(\operatorname{coeff}_{\mathcal{M}}(f)) = 0$.*

This can be compared to the Razborov Rudich framework, in the exact same way as the motivating example. Let property P be defined as

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

The defining property of D, namely that it vanishes on the coefficients of polynomials from $\mathcal{C}$ is the usefulness property. The non-zeroness of D implies that it does not have too many roots, which implies that the property is large. The constructivity property follows from the fact that D belongs to some restricted class $\mathcal{D}$.

In this framework, questions of the following type can now be asked: For the space of total degree d polynomials, is there an algebraic $\text{poly}(N, d)$ sized natural proof for lower bounds against $\text{poly}(n, d)$ sized circuits, where $N = \binom{n+d}{d}$. More succinctly, are there VP-natural proofs against VP.

3.2 Succinct Derandomisation

Similar to the equivalence proved by Willians, there is an equivalence between succinct derandomisation and algebraic proof barriers. Given that natural proofs are defined using vanishing of polynomials, the derandomisation in this case is the derandomisation of PIT. This equivalence will follow straight from definitions, unlike the one for boolean circuits. We first define the notion of a succinct hitting set.

Definition 3.2 (Succinct Hitting Set). *Let $\mathcal{M}, \mathcal{C}, \mathcal{D}$ be defined as in the definition of algebraic natural proofs (3.1). We say that $\mathcal{C}$ is a $\mathcal{C}$-succinct hitting set for $\mathcal{D}$ if $\mathcal{H} := \{\text{coeff}(f) \mid f \in \mathcal{C}\}$ 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 $D(\text{coeff}(f)) \neq 0$.*

Notice that if D is an algebraic natural proof against $\mathcal{C}$, then D must vanish on the set of coefficient vectors $\mathcal{H}$. In particular, this says that $\mathcal{H}$ is NOT a hitting set for D. We thus get the following: there are algebraic natural proofs if and only if coefficient vectors of simple polynomials are not hitting sets. In other words, the existance of algebraic natural proof barriers is equivalent to whether PIT can be derandomised using succinct pseudorandomness. We formalise this as a theorem.

Theorem 3.3. *Let $\mathcal{M}, \mathcal{C}, \mathcal{D}$ be defined as in the definition of algebraic natural proofs (3.1). 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 $\mathcal{D}$.*

The following corollary is an instantiation of the above. Let $N_{n,d} := \binom{n+d}{d}$.

Corollary 3.4. *Let $\mathcal{C}$ be the class of $\text{poly}(n, d)$-sized circuits of total degree atmost d. Then there is an algebraic $\text{poly}(N_{n,d})$-natural proof against $\mathcal{C}$ if and only if $\mathcal{C}$ is not a $\text{poly}(n, d)$-succinct hitting set for $\text{poly}(N_{n,d})$-sized circuits in $N_{n,d}$ variables.*

If we have $d = \text{poly}(n)$, then the corollary says that the existence of an algebraic natural proof barrier is equivalent to saying that coefficient vectors of polylog sized circuits are a hitting set for circuits of polynomial size.

3.3 Succinct Generators

Given a notion of succinct hitting sets, a natural question is to ask whether there it gives rise to a notion of succinct generators. A generator in the usual sense $\mathcal{G}$ is a map $\mathbb{F}^l \to \mathbb{F}^N$ such that $D \in \mathcal{D}$ is non-zero if and only if $D \circ \mathcal{G}$ is non-zero as a polynomial. A succinct generator should be a polynomial map that is the coefficient vector of a polynomial computable by small circuits. We have the following formal definition.

Definition 3.5 (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 $D(\mathrm{coeff}_{\mathcal{M}}(\mathcal{G})) \neq 0$ as a polynomial if and only if D is non-zero. For this, we define $\mathrm{coeff}_{\mathcal{M}}(\mathcal{G})$ by treating $\mathcal{G}$ as a polynomial in the variables $\mathbf{x}$ over the ring $\mathbb{F}[\mathbf{y}]$.*

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.

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.

4 Evidence for Barriers

As discussed above, succinct derandomisation for PIT for restricted classes gives barriers for algebraic proofs. While known derandomisation results are usually not succinct, they can be made so by slight modification. First, a simple example is presented.

Consider a linear form over N variables, $\sum \alpha_i x_i$. We can do a change of variables by setting $x_i \hookleftarrow y^i$, and this preserves the zeroness/non-zeroness of the original linear form. This new univariate in y has degree N, and thus has a hitting set H of size $N+1$. Therefore, we get a hitting set $\left(c, c^2, c^3, \ldots, c^N\right), c \in H$ for the original linear form. If N is a power of two, say $N = 2^n$, we get that such vectors are coefficient vectors of the multilinear polynomials

$$c\left(1 + z_0 c^{2^0}\right)\left(1 + z_1 c^{2^1}\right)\ldots\left(1 + z_{n-1} c^{2^{n-1}}\right).$$

By introducing new variables w_i, we can get a VP-succinct generator that embeds the previous construction, namely polynomials of the form

$$c\left(1 + z_0 w_0\right)\left(1 + z_1 w_1\right)\ldots\left(1 + z_{n-1} w_{n-1}\right).$$

Now we prove one of the main results. We will use a number of statements without proofs.

Theorem 4.1. *In the space of multilinear polynomials in n variables, 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 $\sum\prod\sum$ circuits of constant transcendence degree.*

We will now prove this.

The first step is to obtain a succinct rank condensor. A rank condensor is a collection of linear maps $\mathcal{E} = \{E \mid \mathbb{F}^n \to \mathbb{F}^r\}$ such that given any vector space $V \subseteq \mathbb{F}^n$ of dimension atleast r, there is atleast one map $E \in \mathcal{E}$ such that $\dim E(V) = \dim V = r$. We will use the following construction, from Gabizon and Raz (2008). Let E be a linear map defined by $E_{ij} = t^{ij}$ for formal variable t. If we evaluate E at sufficiently many points, we get $\mathcal{E}$. We just need a generator, so we keep t formal. We now construct the succinct rank condensor.

Let $n \geq r \geq 1$. Define polynomial $P^{RC}_{n,r}$, in variables $x_1, \ldots, x_n, y_1, \ldots, y_r, t_0, \ldots, t_n$ as

$$P^{RC}_{n,r}(\mathbf{x}, \mathbf{y}, \mathbf{t}) := \sum_{j=1}^{r} y_j t_0^j \prod_{k=1}^{n} \left(1 + x_k t_k^j\right).$$

Notice that this polynomial is multilinear in $\mathbf{x}$, and thus the coefficient vector, with entries in $\mathbb{F}[\mathbf{y}, \mathbf{t}]$ has length $N = 2^n$. It is easy to see that this polynomial is computable by depth-4 circuits. Further, for every $\boldsymbol{\alpha}, \boldsymbol{\beta}$, $P^{RC}_{n,r}(\mathbf{x}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ is computed by a $\sum\prod\sum$ circuit. The claim is that this embeds the rank condensor described earlier. In particular, if i indexed $[N]$, then for all i, the i^{th} element in the polynomial map is $\sum_{j=1}^{r} y_j t^{ij}$. The proof is fairly straightforward and is skipped here.

We will now use the following result by Agrawal, Saha, Saptharishi and Saxena. In the following, each T_i will be a product of linear polynomials in variables X_i.

Lemma 4.2 (Generators for circuits of constant trdeg, Agrawal et al. (2011))**.** *Suppose $\mathbb{F}$ is a field of large enough characteristic. Then the map $\Psi : \mathbb{F}[\mathbf{X}] \to \mathbb{F}[y_1, \ldots, y_k, t, z_1, \ldots, z_k, s]$ given by*

$$X_i \to \sum_{j=1}^{k+1} z_j s^{ij} + \sum_{j=1}^{k} y_j t^{ij}$$

is a generator for the class of polynomials expressible as circuits in $T_1, \ldots, T_M$ where the set of T_i have transcendence degree atmost k.

In order to show that this generator is succinct, we just have to notice that

$$P(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{s}, \mathbf{t}) = P^{RC}_{n,k+1}(\mathbf{x}, \mathbf{z}, \mathbf{s}) + P^{RC}_{n,k}(\mathbf{x}, \mathbf{y}, \mathbf{t})$$

is such that $\text{coeff}_{\mathbf{x}}(P) = \Psi$, and that P is succinct.

5 Bibliography

Manindra Agrawal, Chandan Saha, Ramprasad Saptharishi, and Nitin Saxena. Jacobian hits circuits: Hitting-sets, lower bounds for depth-d occur-k formulas and depth-3 transcendence degree-k circuits. *Proceedings of the 44th Annual Symposium on Theory of Computing, ACM, New York*, 11 2011. doi: 10.1145/2213977.2214033.

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`.

Ariel Gabizon and Ran Raz. Deterministic extractors for affine sources over large fields. *Combinatorica*, 28(4):415–440, Jul 2008. ISSN 1439-6912. doi: 10.1007/s00493-008-2259-3. URL `https://doi.org/10.1007/s00493-008-2259-3`.

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`.

Amnon Ta-Shma and Dean Doron. Natural proofs, 2016. URL `http://www.cs.tau.ac.il/~amnon/Classes/2017-BPP/Lectures/Lecture10.pdf`.

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`.