14. Non-Explicit Lower Bound, PIT, Hitting-Sets

Thursday, October 5, 2023 10:35 AM

Thm 1: Suppose $\mathbb{F}$ is algebraically closed. $\exists$ a degree $\le d$ polynomial $f \in \mathbb{F}[X_1, \dots, X_n]$ that requires circuit of size $\Omega\left(\binom{n+d}{d}\right)$.

Pf sketch: Let W = the space of degree $\le d$ polynomials in $\mathbb{F}[X_1, \dots, X_n]$.

Let V = the "variety of size $\le s$ circuits", where s is determined later.

$$\begin{array}{ccc} V \times W & \xrightarrow{\pi_1} & V \\ {\scriptstyle \pi_2}\downarrow & & \\ W & & \end{array}$$

Let $Z \subseteq V \times W$ be the variety $\{(C, f) : \mathrm{Hom}_{\le d}(C) = f\}$

For fixed $C \in V$, there is a unique $f \in W$ s.t. $(C,f) \in Z$, i.e. $f = \mathrm{Hom}_{\le d}(C)$.

Fact: (dimension of fibers)
For $\phi: X \to Y$, X, Y irred
$\dim \phi^{-1}(p) \ge \dim X - \dim \phi(X)$
for all $p \in \phi(X)$,
and $=$ holds for "general" $p \in \phi(X)$.

$\to$ So $\dim Z \le \dim V$ (actually $=$ holds).

So $\dim(\pi_2(Z)) \le \dim Z \le \dim V \le s$

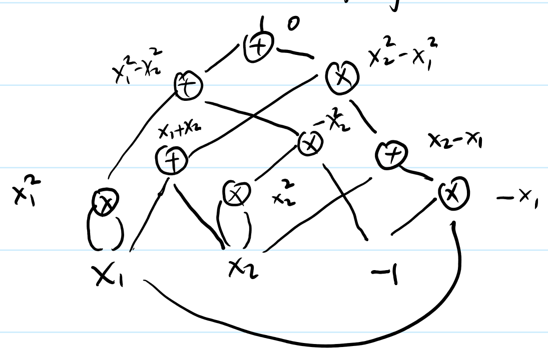
Choose $s = \binom{n+d}{d} - 1 < \dim W$. Then $\exists f \in W \setminus \pi_2(Z)$.

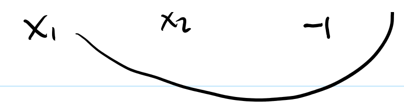
Then f is not computed by any $C \in V$ since $f \ne \mathrm{Hom}_{\le d}(C)$ $\square$

One can even show that the coefficients of f can be chosen from a large enough finite set $S \subseteq \mathbb{F}$. To prove this, first prove a bound $\deg \pi_2(Z) < |S|$. Then use Bézout's inequality to show $\exists f \in S^{\binom{n+d}{d}} \setminus \pi_2(Z)$.

Polynomial identity testing (PIT)

Given a polynomial $f \in \mathbb{F}[X_1, \dots, X_n]$, represented by, e.g., an algebraic circuit of size poly(n), we would like to know if $f = 0$.





In general, a degree $\le d$ polynomial in $x_1, \dots, x_n$ can have $\binom{n+d}{d}$ monomials.

So writing down f can take exponential time if $d = \mathrm{poly}(n)$.

A randomized polynomial-time algorithm.

Assume $\deg(f) \le d$ and f can be evaluated in polynomial time

There is a randomized poly-time algorithm finding if $f = 0$.

It is based on the Schwartz-Zippel Lemma.

Recall: (Schwartz-Zippel) Let $S \subseteq \mathbb{F}$ be a nonempty finite set.

Suppose $f \not\equiv 0$. Then $\Pr_{a \sim_u S^n}[f(a) = 0] \le \frac{\deg(f)}{|S|}$.

The randomized PIT algorithm: Let $S \subseteq \mathbb{F}$ be a finite set of size $\ge d/\varepsilon$. (ε error parameter.)

If $\mathbb{F}$ is too small, replace $\mathbb{F}$ by an extension field and then choose S.

Randomly choose $a \in S^n$.

If $f(a) = 0$, output YES (i.e. "$f = 0$"). Otherwise output NO.

By Schwartz-Zippel: If $f = 0$, always output YES.

If $f \not\equiv 0$, output NO with probability $\ge 1 - \frac{d}{|S|} \ge 1 - \varepsilon$.

Technical remark: Say $\mathbb{F} = \mathbb{Q}$. We may even allow $d = \exp(n)$. We may choose $S = \{0, 1, \dots, d\}$.

It takes $\mathrm{poly}(n)$ bits to represent an element in S.

But then the circuit may compute integers of bit length $\exp(n)$. E.g. 2^d of bit length $d = \exp(n)$.

To fix this. Choose random $p \in \{2, \dots, N\}$, where $N = \exp(n)$ is large enough.

Repeat until p is prime (tested via primality testing). Then work over $\mathbb{Z}/p = \mathbb{F}_p$

(So it takes $\exp(n)$ time in the Boolean model)

<u>Cor</u> PIT $\in$ coRP. i.e. $\begin{cases} \text{For YES instances, output YES.} \\ \text{For NO instances, output NO w.p. } \ge 1/2. \end{cases}$

Can we find a deterministic poly-time PIT algorithm? (We believe so as we believe coRP = P!)

---

we believe coRP = P !)

We say a PIT algorithm (randomized or deterministic) is white-box if it "knows" the input polynomial f, and black-box if it only uses f as an evaluation oracle, i.e. it only queries the value of f at $a \in \mathbb{F}^n$.

E.g., the Schwartz–Zippel-based PIT algorithm is a black-box algorithm.

Adaptiveness does not help a black-box PIT algorithm. (why?)

Def (Hitting-sets) Let $C \subseteq \mathbb{F}[x_1, \ldots, x_n]$. A finite set $H \subseteq \mathbb{F}^n$ is a hitting-set for C if for every nonzero $f \in C$, there exists $a \in H$ s.t. $f(a) \neq 0$.

H is a δ-hitting-set for C if

$$\Pr_{a \leftarrow H}[f(a) = 0] \leq \delta.$$

Remark: We often allow H to be a multi-set.

Given an explicit hitting set H for C, we have a deterministic black-box PIT algorithm for C: ⟸ "explicit" means "efficiently constructible"

Just enumerate $a \in H$ and evaluate $f(a)$. Output NO iff $\exists\, a \in H$ s.t. $f(a) \neq 0$.

Conversely, given deterministic black-box PIT algorithm for C, the (multi-) set of queries $H \subseteq \mathbb{F}^n$ is a hitting-set for C.

So explicit small hitting sets $\Longleftrightarrow$ fast deterministic black-box PIT algorithms.

Designing efficient deterministic black-box PIT algorithms is equivalent to constructing explicit hitting-sets of polynomial size.

Def A hitting-set generator (HSG) $G: \mathbb{F}^s \to \mathbb{F}^n$ for C is a polynomial map s.t. for every $0 \neq f \in C$, we have $f \circ G \neq 0$. ← $s \ll n$

(suppose G is defined by $g_1, \ldots, g_n \in \mathbb{F}[y_1, \ldots, y_s]$.

Then $f \circ G := f(g_1, \ldots, g_n) \in \mathbb{F}[y_1, \ldots, y_s]$.

From HSGs to hitting-sets:

From HSGs to hitting-sets:

If $H \subseteq \mathbb{F}^s$ is a hitting-set for $C' = \{ f \circ G : f \in C \}$. Then $G(H)$ is a hitting-set for C.

Note if $\deg(f) = d$ & polynomials defining G have degree $\leq d'$, then $\deg(f \circ G) \leq dd'$.
for $f \in C$
$\Downarrow$

Suppose $s=1$. Any set of size $dd'+1$ is a hitting set for $f \circ G$.

Example (Kronecker substitution): $G: \mathbb{F} \to \mathbb{F}^n$ sending $a \in \mathbb{F}$ to $(a, a^d, a^{d^2}, \dots, a^{d^{n-1}})$ is a HSG for individual degree $< d$ polynomials (i.e. $\deg_{X_i}(f) < d$, $i = 1, \dots, n$)

$$\underset{\text{ind. deg of } f < d}{f \neq 0} \Rightarrow f(Y, Y^d, \dots, Y^{d^{n-1}}) \neq 0.$$

However, $\deg(f \circ G)$ is exponentially large.

From hitting-sets to HSGs: Suppose H is a hitting-set for C; $|H| = k$

Using interpolation, we may find $G: \mathbb{F} \to \mathbb{F}^n$ defined by degree $\leq k-1$ polynomials s.t. $H \subseteq G(\mathbb{F})$.

For nonzero $f \in C$, $f|_H \neq 0$. So $f|_{G(\mathbb{F})} \neq 0$. So $f \circ G \neq 0$.

So G is a HSG for C.

Conclusion: Explicit hitting-sets of size $\leq \mathrm{poly}(n) \Leftrightarrow$ Explicit HSG $\mathbb{F}^s \to \mathbb{F}^n$ defined by degree-$\mathrm{poly}(n)$ polynomials. $s = O(1)$.
(Assuming polynomials in C have degree $\leq \mathrm{poly}(n)$).