12. Strassen's Lower Bound, Bézout's Inequality

Thursday, September 28, 2023 10:31 PM

Thm 1 (Strassen '73) Let $d > 0$ be an integer coprime to $\mathrm{char}(\mathbb{F})$. (if $\mathrm{char}(\mathbb{F}) = 0$ then any $d > 0$ works)

Let C be a multi-output algebraic circuit in $X_1, \dots, X_n$ that outputs $X_1^d, \dots, X_n^d$. The the size (# gates) of C is $\Omega(n \cdot \log d)$.

Cor Let $f = \sum_{i=1}^{n} X_i^d Y_i \in \mathbb{F}[X_1, \dots, X_n, Y_1, \dots, Y_n]$. Then any circuit computing f has size $\Omega(n \log d)$.

Pf: Suppose f is computed by a circuit of size s.

Then $\frac{\partial f}{\partial Y_1} = X_1^d, \dots, \frac{\partial f}{\partial Y_n} = X_n^d$ are simultaneously computed by a circuit of size $s' = O(s)$ by the Baur-Strassen Theorem (Lecture 3).

By Thm 1, $s' = \Omega(n \log d)$. So $s = \Omega(n \log d)$ □.

This is the best known explicit lower bound for general algebraic circuits!

To prove Thm 1, we need some algebraic geometry.

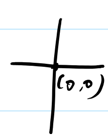
First, a circuit over $\mathbb{F}$ is also a circuit over $\mathbb{K}$ if $\mathbb{K}$ is an extension field of $\mathbb{F}$.

So by replacing $\mathbb{F}$ with its algebraic closure $\overline{\mathbb{F}}$, we may assume $\mathbb{F}$ is algebraically closed (i.e. if a is a root of nonzero $f(x) \in \mathbb{F}[x]$ then $a \in \mathbb{F}$.)

We assume $\mathbb{F}$ is algebraically closed from now on. (e.g., $\mathbb{F} = \mathbb{C}$.)

An (affine) variety $V \subseteq \mathbb{F}^n$ is the set of all common solutions of a set of polynomials in $\mathbb{F}[X_1, \dots, X_n]$.

(Illustration in $\mathbb{R}^2$)

E.g. $X_1^2 + X_2^2 = 1$  $X_1 X_2 = 0$ 

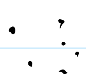
A variety V is irreducible if $V \neq \emptyset$ and V cannot be written as the union

A variety V is *irreducible* if $V \neq \phi$ and V cannot be written as the union of two smaller varieties.

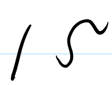
Fact: Every variety V can be uniquely written as a union of finitely many distinct irreducible varieties that are maximal with respect to inclusion.
These irreducible varieties of are called the *irreducible components* of V

The *dimension* of an irreducible variety V is the "degree of freedom" of picking a point in V. (not giving the formal definition), denoted by $\dim V$.

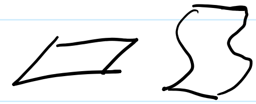
More generally, the dimension of a nonempty variety $V = \max\limits_{\substack{V' \text{ ired} \\ \text{component of } V}} \dim V'$.



dim of finite sets $= 0$.



dim of a line/curve $= 1$.



dim of a plane/surface $= 2$.

The *degree* of an irreducible variety $V \subseteq \mathbb{F}^n$ is

$$\deg V := |V \cap W|$$

where $W \subseteq \mathbb{F}^n$ is an affine subspace of codim $\dim V$ (i.e. $\dim W = n - \dim V$) in "general position". (can be made rigorous)

More generally, we define $\deg V := \sum\limits_{\substack{V' \text{ ired} \\ \text{component of } V}} \deg V'$ for (possibly reducible) varieties.

(Remark: In the reducible case, the definition $|V \cap W|$ only counts the degree of the irreducible components of V of the top dimension (i.e. $\dim V$), which is smaller than $\sum \deg V'$ if the ired components have mixed dimensions.
So we use the definition $\sum \deg V'$, which is better suited as a complexity measure.)

Fact: for a finite set $S \subseteq \mathbb{F}^n$ as a variety, $\deg S = |S|$.

Fact: for a finite set $S \subseteq \mathbb{F}^n$ as a variety, $\deg S = |S|$.

Fact: Let $V(f) \subseteq \mathbb{F}^n$ be the set of common roots of a degree-d nonzero polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$. Then $\deg(V(f)) \le d$ and $\dim(V(f)) = n-1$.

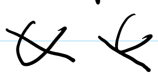
$\deg(V(f)) = d$ if f is square free.

<u>Thm</u> (Bézout's inequality). Let $V, W \subseteq \mathbb{F}^n$ be varieties. Then

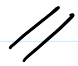
$$\deg(V \cap W) \le \deg V \cdot \deg W.$$

The above version is due to Schnorr '79 and Heintz '79.

Remark: when the intersection is "transverse", and when we count points with multiplicities and count those "at infinity",



multiplicity $=2$.



parallel lines intersect at infinity

then Bézout's inequality is actually an equality, also known as Bézout's Theorem.

However, even ignoring these subtleties, the inequality still holds.

E.g., two plane curves C_1, C_2 of degree 2 in general position satisfies $\deg(C_1 \cap C_2) = 4$.

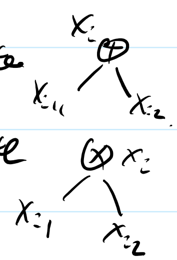
But $\deg(C_1 \cap C_2) = \deg(C_1) = 2 \le 4$ if $C_1 = C_2$.

<u>Proof of Thm 1.</u> Suppose C computes $x_1^d, \dots, x_n^d$ simultaneously.

For every non-input gate, associate a new variable.

Then we get $x_1, \dots, x_m$ where $m = \#$gates.

Let S be the set of polynomials
$$\begin{cases} x_i = a, & x_i \text{ is associate with a constant input gate } a \\ x_i = x_{i_1} + x_{i_2} & x_i \cdots + \text{gate} \\ x_i = x_{i_1} \cdot x_{i_2} & x_i \cdots \times \text{gate} \end{cases}$$



$i = 1, \dots, m$

together with the polynomials $x_{i_j} = 1$, $1 \le j \le n$

together with the polynomials $x_{i_j} = 1$, $1 \le j \le n$

where $x_{i_1}, \dots, x_{i_n}$ are associated with the n output gates

Let $V(S) \subseteq \mathbb{F}^m$ be the variety defined by S.

By Bézout's inequality, $\deg(V(S)) \le 2^{\mathrm{size}(C)}$.

Let $\omega \in \mathbb{F} = \overline{\mathbb{F}}$ be a primitive d-th root of unity, i.e. d is the smallest positive integer such that $\omega^d = 1$.

Then for every $e = (e_1, \dots, e_n) \in \{0, \dots, d-1\}^n$, there is a unique solution to S with $\underbrace{x_1 = \omega^{e_1}, \dots, x_n = \omega^{e_n}}$.

these determines other x_i's via $x_i = x_{i_1} + x_{i_2}$ and $x_i = x_{i_1} \cdot x_{i_2}$.

moreover, the outputs are $(x_1^d, \dots, x_n^d) = (1, \dots, 1)$

These are the only points in $V(S)$ due to $x_1^d = \dots = x_n^d = 1$.

So $\dim V(S) = 0$ and $\deg V(S) = |V(S)| = d^n$.

So we have $d^n = \deg V(S) \le 2^{\mathrm{size}(C)} \Rightarrow \mathrm{size}(C) = \Omega(n \log d)$. □

Remark: The proof actually shows # multiplication gates $\ge n \cdot \log_2 d$.

Smolensky '96 gave an elementary proof of Thm 1.

Another application:

(Schwartz-Zippel Lemma, aka DeMillo-Lipton-Schwartz-Zippel Lemma).

Suppose $0 \ne f \in \mathbb{F}[x_1, \dots x_n]$ and $\deg(f) = d$. Let $\phi \ne S \subseteq \mathbb{F}$ be a finite set. Then

$$\Pr_{a \leftarrow_u S^n} [f(a) = 0] \le \frac{d}{|S|}.$$

<u>Lemma</u> Let $V \subseteq \mathbb{F}^n$ be a variety of dimension k. Let $f_1, \dots, f_m \in \mathbb{F}[x_1, \dots, x_n]$ be nonzero polynomials such that $\deg(f_1) \ge \dots \ge \deg(f_m)$.

Then $\deg(V \cap V(f_1) \cap \dots \cap V(f_m)) \le \deg(V) \cdot \prod_{i}^{\min\{m,k\}} \deg(f_i)$.

Then $\deg(V \cap V(f_1) \cap \dots \cap V(f_m)) \le \deg(V) \cdot \prod_{i=1}^{\min\{m,k\}} \deg(f_i)$.

Pf: We need the following fact in algebraic geometry:

Fact: If f does not vanish on V and V is irreducible, then $\dim(V \cap V(f)) \le \dim(V) - 1$. (In fact, equality holds if $V \cap V(f) \ne \phi$)

The lemma is proved by induction on $\dim V$.

Base case: $\dim V = 0$ or $V = \phi$. Easy to verify.

Induction: By decomposing into irred components, we may assume V is irreducible.

If $V(f_1) \supseteq V$. We may skip f_1.

So assume $V(f_1) \not\supseteq V$. Then $\dim(V \cap V(f_1)) \le \dim(V) - 1$

and $\deg(V \cap V(f_1)) \le \deg V \cdot \deg(V(f_1))$ by Bézout's Theorem. $\le \deg V \cdot \deg(f_1)$

By the induction hypothesis on $V' := V \cap V(f_1)$

$$\deg(V \cap V(f_1) \cap \dots \cap V(f_m)) = \deg(V' \cap V(f_2) \cap \dots \cap V(f_m))$$

$$\le \deg V' \cdot \prod_{i=1}^{\min\{m-1,k-1\}} \deg(f_{i+1}) \le \deg V \cdot \prod_{i=1}^{\min\{m,k\}} \deg(f_i)$$

$\square$.

Proof of Schwartz-Zippel: We know $\deg(V(f)) = d$ and $\dim(V(f)) = n-1$.

Let $f_i = \prod_{a \in S} (X_i - a)$ for $i = 1, \dots, n$.

Then $\deg(f_i) = |S|$.

Let $V = V(f) \cap V(f_1) \cap \dots \cap V(f_n)$.

Then $\deg(V) \le d \cdot |S|^{n-1}$ by the above lemma.

And $V = \{a \in S^n : f(a) = 0\}$. As V is finite, $|V| = \deg(V)$.

So $\Pr_{a \sim_u S^n}[f(a) = 0] = \frac{|V|}{|S^n|} \le \frac{d \cdot |S|^{n-1}}{|S|^n} = \frac{d}{|S|}$. $\square$.