Algebraic Techniques

Basic question: $\forall x : f(x) = 0$?

Idea: evaluate at random points.

Use algebraic properties to obtain a Monte Carlo Algorithm.

Verifying Matrix Multiplication

Consider $n \times n$ matrices A, B, C and a random vector $\mathbf{r} \in \mathbb{F}^n$.

Theorem 1. *If* $\mathsf{D} = AB - C \neq 0$ *then* $\mathbb{P}[\mathsf{D}r = 0] \leq \frac{1}{|\mathbb{F}|}$

Proof. Wlog assume the first row d of D has the form $(d_1, \ldots, d_k, 0, \ldots, 0)^T, d_j \neq 0$ for $1 \leq j \leq k$.

$d \cdot r$ is the first entry of Dr.

We show that the claim is true for any fixed choice of $r_2, \ldots, r_k$.

$d \cdot r = 0$ iff $d_1 r_1 = \sum_{j=2}^{k} d_j r_j$.

There is at most one $r_1 \in \mathbb{F}$ that satisfies this equality.

$$\mathbb{P}[\mathsf{D}r = 0 \mid r2, \ldots, r_k] \leq \mathbb{P}[d \cdot r = 0 \mid r2, \ldots, r_k] \leq 1/|\mathbb{F}|$$

□

Verifying Matrix Multiplication II

Evaluating $\mathsf{D}r$ takes time $\mathcal{O}(n^2)$.

Actual multiplication takes time $\mathcal{O}(n^3)$ (or $\mathcal{O}(n^{2.376})$ ...).

Verifying Polynomial Identities

$\mathbb{F}$: any field (German "Körper")

$\mathbb{F}[x_1, \ldots, x_n]$: multivariate polynomials over $\mathbb{F}$.

Theorem 2.

$\forall Q(x) \not\equiv 0 \in \mathbb{F}[x] : \mathbb{P}[Q(r) = 0] \leq \frac{d}{|\mathbb{S}|}$ *for degree* d *random* $r \subseteq \mathbb{S}$.

Proof. Nonzero polynomials have at most d zeroes. □

Application: A Checker for Sorting

Let $\langle b_0, \ldots, b_n \rangle = \text{sort}(\langle a_0, \ldots, a_n \rangle)$.

Its easy to check whether the output of `sort` is sorted.

Oops. But is it a permutation of the input?

Iff $(x - b_0) \cdots (x - b_n) - (x - a_0) \cdots (x - a_n) \equiv 0$

where the bits defining a_i and b_i are reinterpreted as elements of some field.

This can be checked in linear time whp.

The Multivariate Case

Lemma 3. *For any two events $\mathcal{E}_1$ and $\mathcal{E}_2$,*

$$\mathbb{P}[\mathcal{E}_1] \leq \mathbb{P}\left[\mathcal{E}_1 \mid \bar{\mathcal{E}}_2\right] + \mathbb{P}[\mathcal{E}_2]$$

Proof.

$$\begin{aligned}\mathbb{P}[\mathcal{E}_1] =& \mathbb{P}\left[\mathcal{E}_1 \cap \bar{\mathcal{E}}_2\right] + \mathbb{P}[\mathcal{E}_1 \cap \mathcal{E}_2] \\ =& \mathbb{P}\left[\mathcal{E}_1 \mid \bar{\mathcal{E}}_2\right] \mathbb{P}\left[\bar{\mathcal{E}}_2\right] + \mathbb{P}[\mathcal{E}_1 \cap \mathcal{E}_2] \\ \leq& \mathbb{P}\left[\mathcal{E}_1 \mid \bar{\mathcal{E}}_2\right] + \mathbb{P}[\mathcal{E}_2]\end{aligned}$$

□

Theorem 4. *Consider $Q(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$:*

$\mathbb{P}[Q(r_1, \ldots, r_n) = 0 \mid Q \not\equiv 0] \leq \frac{d}{|\mathbb{S}|}$ *for random $r_i \subseteq \mathbb{S}$, total degree d.*

Proof. By induction on n.

$n = 1$: see Theorem 2

$n - 1 \rightsquigarrow n$: write $Q = \sum_{i=0}^{k} x_1^i Q_i(x_2, \ldots, x_n)$ s.t. $Q_k \not\equiv 0$

Fix $r_2, \ldots, r_n$

Q_k has total degree at most $d - k$, i.e., by the induction hypothesis,

$$\mathbb{P}[Q_k(r_2, \ldots, r_n) = 0] \leq \frac{d - k}{|\mathbb{S}|}$$

Since $\sum_{i=0}^{k} x_1^i Q_i(r_2, \ldots, r_n)$ is univariate, Theorem 2 implies

$$\mathbb{P}[Q(r_1, \ldots, r_n) \mid Q_k(r_2, \ldots, r_n) \neq 0] \leq \frac{k}{|\mathbb{S}|}$$

Now Lemma 3 implies the desired relation. □

Black Boxes

We can check exponentially large polynomials if we can evaluate them in polynomial time.

For example, $\det(\mathsf{A})$ can have exponentially many coefficients if the entries in A involve variables.