Beginning of 04/04/2025 — more algebraic techniques

Polynomial Identity Testing

Let $x_1, \cdots, x_n$ be the variables. Let $p = p(x_1, \cdots, x_n)$ be a polynomial. We ask if $p \equiv 0$. For example, this can be used to check if two polynomials written in different forms are identical.

Theorem: Schwarz-Zipper Theorem

Let S be any finite set of integers. If $a_1, \cdots, a_n$ are drawn u.a.r. (uniformly at random) from S, and $p \not\equiv 0$, then

$$\mathbb{P}(p(a_1, \cdots, a_n) = 0) \leqslant \frac{d(p)}{|S|}.$$

That is, with high probability we can efficiently evaluate our unknown polynomial at random values and correctly conclude whether $p \equiv 0$.

Proof. We induct on n, the number of variables. The base case is trivial: a univariate polynomial p of degree d can have at most d roots, so if $p \not\equiv 0$ we immediately have $\mathbb{P}(p(a) = 0) \leqslant d/|S|$.
Now given a generic polynomial $p(x_1, \cdots, x_n)$, we decompose it based on powers of x_1. Let the highest exponent of x_1 be k. Then

$$p(x_1, \cdots, x_n) = x_1^k Q_1(x_2, \cdots, x_n) + x^{k-1} Q_2(x_2, \cdots, x_n) + \cdots.$$

Assume that p and all Q_i's are not identically equal to 0 (for we can easily remove those trivial terms). Since p has degree d, Q_1 has degree $\leqslant d - k$, so by IH

$$\mathbb{P}(Q_1(a_2, \cdots, a_n) \mid Q_1 \not\equiv 0) \leqslant \frac{d-k}{|S|}.$$

Now we look at the univariate polynomial $p(x_1, a_2, \cdots, a_n) = R(x_1)$, with degree $\leqslant k$. Base case implies

$$\mathbb{P}(R(a_1) \neq 0 \mid Q_1(a_2, \cdots, a_n) \neq 0) \leqslant \frac{k}{|S|}.$$

Let

$$E_1 = \{p(a_1, \cdots, a_n) = 0\} \qquad \text{and} \qquad E_2 = \{Q_1(a_2, \cdots, a_n) \neq 0\}.$$

By definition of conditional, $\mathbb{P}(E_1) = \mathbb{P}(E_1 \mid E_2)\mathbb{P}(E_2) + \mathbb{P}(E_1 \mid \overline{E}_2)\mathbb{P}(\overline{E}_2) \leqslant \mathbb{P}(E_1 \mid E_2) + \mathbb{P}(\overline{E}_2)$. But this is precisely $(d-k)/|S| + k/|S| = d/|S|$, so the proof is complete. □

Application: Perfecting Matchings in Bipartite Graphs

Consider a bipartite graph $L \cup R$. For a given graph, we consider a polynomial that is identically zero iff there exists a perfect matching on the graph.
Consider a matrix A where $A_{i,j} = 1$ if $i \in L$ has an edge to $j \in R$ (note this matrix is NOT symmetric). Observe a perfect matching exists if we can choose n ones in the matrix such that each row and column is chosen precisely once. Recall the determinant of A via cofactor expansion can be viewed as a sum over all permutations $\sigma \in S_n$

weighted by their permutation signs. A term does not vanish if and only if there exists a permutation of all-nonzero entries, and this precisely corresponds to a perfect matching.
To ensure uniqueness (so that nonzero terms don't cancel each other), we replace ones with monomials. Specifically, we define a new matrix B such that for each entry $A[i][j] = 1$, we define a new variable $x_{i,j}$ corresponding to $B[i][j]$. Then $\det(B)$ as a function of all edges in $L \cup R$ will identically equal to 0 if and only if the graph has no perfect matching.
And to use the Theorem?

- Choose a set of integers of size n^2
- Choose $a_1, \cdots, a_{n^2}$ uniformly at randomly from S
- Valuate $\det(B[a_1, \cdots, a_{n^2}])$ where all other entries of B are filled by 0.
- The Theorem states that

$$\mathbb{P}(\det B([a_1, \cdots, a_{n^2}] = 0 \mid G \text{ has a perfect matching}) \leqslant \frac{n}{n^2} = \frac{1}{n}.$$

The computation bottleneck of this application is the determinant which takes $\mathcal{O}(n^3)$. To prevent exponentially large multiplication, one trick is to perform everything modulo a large prime P so that we work in a finite field.