

CME 305: Discrete Mathematics and Algorithms

Instructor: Professor Amin Saberi (saberi@stanford.edu)

February 10, 2009

Lecture 10: Randomized Algorithms

Randomization plays a central role in the design and analysis of algorithms. It is still an open question whether the ability to make random choices allows some problems to be solved in polynomial time that cannot be solved without this ability. Nevertheless, in many situations, it is possible to come up with randomized algorithms that are faster, or easier to implement.

Polynomial Identity

Say that we are given two polynomials and want to determine whether or not they are identical. For example,

$$(x - 1)(x + 1) \equiv x^2 - 1.$$

One way would be to expand each polynomial and compare coefficients. A simpler method is to 'plug in' a few numbers and see if both sides are equal. If they are not, we now have a proof of their inequality, otherwise with good confidence we can say they are equal. This idea is the basis of a randomized algorithm.

We can formulate the polynomial equality verification of two given polynomials F and G as:

$$H(x) \equiv F(x) - G(x) \stackrel{?}{=} 0.$$

Denote the maximum degree of F and G as n . Assuming that $F(x) \not\equiv G(x)$, $H(x)$ will be a polynomial of degree at most n and therefore it can have at most n roots. Choose an integer x uniformly at random from $[1, n^2]$. $H(x)$ will be zero with probability at most $1/n$.

After a small number of samples, we will be able to determine with high probability whether the two polynomials are identical.

The following lemma by Schwartz, generalizes the above observation to polynomials on a number of variables:

Lemma 1 *Suppose that f is a polynomial in the variables x_1, x_2, \dots, x_n , and that f is not identically zero. For $1 \leq i \leq n$, let d_i be the degree of f in x_i . Also, for $1 \leq i \leq n$, let I_i be any set of elements in the domain or field of F . Then in the set $I_1 \times \dots \times I_n$, f has at most*

$$\left(\frac{d_1}{|I_1|} + \frac{d_2}{|I_2|} + \dots + \frac{d_n}{|I_n|} \right) (|I_1||I_2|\dots|I_n|)$$

zeros.

Proof: The case $n = 1$ is obvious since a nonzero polynomial of degree d can have at most d zeros, and we proceed by induction on n . Let f' be the polynomial that is the coefficient $x_1^{d_1}$. f' is a polynomial on at most $n - 1$ variables. If (y_2, \dots, y_n) is not a zero of f' , $f(x_1, y_2, \dots, y_n)$ has at most d_1 zeros in I_1 . Thus the total number of zeros of f in $I_1 \times \dots \times I_n$ is bounded by

$$|I_1| \left(\frac{d_2}{|I_2|} + \dots + \frac{d_n}{|I_n|} \right) (|I_2| \cdots |I_n|) + d_1 (|I_2| \cdots |I_n|)$$

which gives the desired bound. ■

Perfect matchings

Given a bipartite graph $G(U, V, E)$ s.t. $|U| = |V|$, define the matrix A such that

$$a_{ij} = \begin{cases} 1 & \text{if } i \sim j, i \in U, j \in V \\ 0 & \text{otherwise} \end{cases}$$

Lemma 2 *If $\det(A) \neq 0$ then G has a perfect matching.*

Proof: Recall the definition of determinant:

$$\det(A) = \sum_{\pi} \text{sign}(\pi) \prod_{i=1}^n a_{i, \pi(i)}$$

where the sign of a permutation is 1 if it is even or -1 if it is odd. Recall that a permutation of size n is just a bijection from $\{1, \dots, n\} \mapsto \{1, \dots, n\}$. One can also see a permutation π as describing a perfect matching in a complete bipartite graph; for each vertex $i \in U$, we match it to vertex $\pi(i) \in V$.

For a bipartite graph G with adjacency matrix A , $\prod_{i=1}^n a_{i, \pi(i)}$ will be non-zero if and only if all terms $a_{i, \pi(i)} \neq 0$; i.e. each $(i, \pi(i))$ is an edge G , so π describes a perfect matching in G . Since the determinant is the sum of these terms, it follows that if $\det(A)$ is nonzero there must be at least one perfect matching in G . ■

Since computing the determinant of a matrix is easy, this gives us a simple test for determining if G has a perfect matching. However, this only gives us a sufficient condition, not a necessary one. It may very well be possible that G has many perfect matchings, but has equal numbers of ones with odd and even permutations, leaving $\det(A) = 0$. So how can we modify this so that it's also a necessary condition?

Define the matrix B such that

$$b_{i,j} = \begin{cases} x_{i,j} & \text{if } i \sim j, i \in U, j \in V \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 3 $\det(B) \neq 0$ iff G has a perfect matching.

Proof:

\Rightarrow : choose the permutation that gives a non-zero value.

\Leftarrow : set all $x_{i,j}$ corresponding to perfect matching to 1 and the rest to 0. ■

So in order to determine if G has a perfect matching, we just need to see if a multivariate polynomial of degree at most n is equivalent to 0. There can be up to $n!$ terms of the determinant of B , but we can apply the randomized polynomial equality testing given in the first section to design an efficient algorithm.

Algorithm 1 Randomized algorithm to detect perfect matching

set $x_{i,j} = \text{UAR}\{1, \dots, n^2\}$ for all i, j

compute $\det(B)$.

if $\det(B) = 0$ repeat until confidence above desired threshold

The determinant of B may be exponentially large, but this still only requires $n \log n$ bits. We can also get around this by performing determinant calculation modulo some prime $p > n^2$ and the lemma will still hold.

1. Extension to general graphs

For a given graph $G(V, E)$, define the 'Tutte' matrix T as follows:

$$t_{i,j} = \begin{cases} x_{i,j} & \text{if } i \sim j, i > j \\ -x_{i,j} & \text{if } i \sim j, i < j \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 4 $\det(T) \neq 0$ iff G has a perfect matching.

Proof:

\Leftarrow : Let $x_{i,j} = 1$ for every edge in the perfect matching and set the other variables to zero.

\Rightarrow : Every permutation in the matrix corresponds to a collection of cycles that cover all vertices of the graph.

The permutations having odd cycles cancel each other. To see this, take the edges in an odd cycle in the opposite direction. This doesn't change the sign of the permutation, but the value of each term is negated. Since there are an odd number of terms being negated, the contribution to the determinant by the reversed cycle is negative that of the forward cycle.

Therefore, $\det(T) \neq 0$ iff T has a permutation such that its corresponding cycle representation consists of even cycles. This can only happen if G has a perfect matching. ■