University of Tokyo: Advanced Algorithms **Summer 2010**

Lecture 2 — 15 April

Lecturer: François Le Gall *Scribe: Ly Nguyen*

2.1 Verifying matrix multiplication

Let A, B, C be matrices of size $n \times n$ over a field $\mathbb{F}$. We want to check whether $AB = C$. The simplest strategy is to calculate the product of A and B and then compare the result with C. The fastest known algorithm for matrix multiplication, developed by Coppersmith and Winograd, uses $O(n^{2.376})$ field operations, which improves on the obvious $O(n^3)$ algorithm. However the randomized algorithm described below solves this problem with $O(n^2)$ field operations.

Randomized Algorithm

1. Take an element r uniformly at random in $\{0,1\}^n$.
2. Compute $x = Br, y = Ax = ABr$ and $z = Cr$.
3. Check whether $y = z$.

This algorithm uses a *sampling and testing* strategy. Clearly, if $AB = C$ then $y = z$, i.e. $Pr[ABr = Cr] = 1$. We now show that for $AB \neq C$, the probability that $y \neq z$ is at least $1/2$.

Theorem 2.1. *Let A, B, C be matrices of size $n \times n$ over a field $\mathbb{F}$ such that $AB \neq C$. Then for r chosen uniformly at random from $\{0,1\}^n$, $Pr[ABr = Cr] \leq 1/2$.*

Proof: Let $D = AB - C$. Since D is not the all zeroes matrix, let us suppose, without loss of generality, that $D_{11} \neq 0$. To bound the probability of the event $ABr = Cr$, which is equivalent to probability of $Dr = 0$, let us assume that $Dr = 0$. Therefore, we have:

$$\sum_{i=1}^{n} D_{1i} r_i = 0$$

$$\Leftrightarrow r_1 = -\frac{\sum_{i=2}^{n} D_{1i} r_i}{D_{11}}.$$

We can suppose without loss of generality that, when choosing r, the coordinates $r_2, \ldots r_n$ are first chosen. If $r_2, r_3, ..., r_n$ are fixed, there is at most one value of r_1 over a set of size 2 such that $Dr = 0$. Therefore we obtain $Pr[Dr = 0] \leq 1/2$. $\square$

2.2 Verifying polynomial identity

2.2.1 1-variable polynomials

Let $P(x), Q(x)$ be polynomials in $\mathbb{F}$ of degree d. We want to verify that $P(x) \equiv Q(x)$. Two polynomials are said to be equal if they have the same coefficients for corresponding powers of x. Let us first consider about algorithms for verifying the equality of the following two polynomials.

$$P(x) = a_0 + a_1 x + ... + a_d x^d \text{ where } a_0, \ldots, a_d \in \mathbb{F}$$

$$Q(x) = \prod_{i=1}^{d} (x - \alpha_i) \text{ where } \alpha_1, \ldots, \alpha_d \in \mathbb{F}$$

Expanding $Q(x)$ takes $O(d^2)$ field operations. However, we may reduce the number of operations to $O(d)$ by using the randomized algorithm given below.

Randomized Algorithm

1. Let $\mathbb{S} \subseteq \mathbb{F}$ be a fixed set.
2. Take r uniformly at random in $\mathbb{S}$.
3. Verify that $P(r) = Q(r)$.

If $P(x) \equiv Q(x)$ then obviously, $Pr_{r\in\mathbb{S}}[P(r) = Q(r)] = 1$. If $P(x) \not\equiv Q(x)$, then there are at most d values of r such that $P(r) - Q(r) = 0$ because the degree of $P(r) - Q(r)$ is not greater than d. Therefore, we derive:

$$Pr_{r\in\mathbb{S}}[P(r) = Q(r)] \leq \frac{d}{|\mathbb{S}|}.$$

Based on this bound, we have two methods to amplify the success probability. By repeating the above randomized algorithm k times, the success probability will not be smaller than $1 - (\frac{d}{|\mathbb{S}|})^k$. That means if we choose $\mathbb{S}$ such that $|\mathbb{S}| = 2d$ then the success probability will not be smaller than $1 - 1/2^k$. The other method is taking large $\mathbb{S}$.

Notice that, more generally, this technique works whenever the polynomials P and Q can be evaluated efficiently.

2.2.2 Multivariate polynomials

Let $P(x_1, x_2, ..., x_n)$ and $Q(x_1, x_2, ..., x_n)$ be multivariate polynomials in $\mathbb{F}[x_1, x_2, ..., x_n]$ of degree d. In a multivariate polynomial $R(x_1, x_2, ..., x_n)$, the degree of any term is the sum of the exponents of the variables, and the total degree of R is the maximum of the degrees of its terms. For example:

$$R(x_1, x_2, ..., x_n) = x_1^2 x_2 x_3^3 + x_1 x_2^3 + x_2^2 x_3.$$

The degrees of first term, second term, third term are 6, 4, 3 respectively. The maximum degree is 6 therefore the degree of R is 6.

Our goal is verifying that $P(x_1, x_2, ..., x_n) \equiv Q(x_1, x_2, ..., x_n)$. We suppose that both P and Q can be evaluated efficiently at a specific point. Let us write $R(x_1, x_2, ..., x_n) = P(x_1, x_2, ..., x_n) - Q(x_1, x_2, ..., x_n)$. We have thus to check whether $R \equiv 0$.

We now describe a very general randomized algorithm for this task that uses only one evaluation of the polynomial R.

Randomized Algorithm

1. Fix a set $\mathbb{S} \subseteq \mathbb{F}$
2. Take an element $(r_1, r_2, ..., r_n)$ uniformly at random in $\mathbb{S}^n$
3. Check whether $R(r_1, r_2, ..., r_n) = 0$

Clearly, if $R \equiv 0$ then $Pr[R(r_1, r_2, ..., r_n) = 0] = 1$. If $R \not\equiv 0$ we can bound the success probability by using Schwartz-Zippel Theorem described below.

Theorem 2.2 (Schwartz-Zippel Theorem). *Let $R(x_1, x_2, ..., x_n) \in \mathbb{F}(x_1, x_2, ..., x_n)$ be a nonzero multivariate polynomial of total degree d. Fix any finite set $\mathbb{S} \in \mathbb{F}$, and let $r_1, r_2, ..., r_n$ be chosen independently and uniformly at random from $\mathbb{S}$. Then*

$$Pr[R(r_1, r_2, ..., r_n) = 0] \leq \frac{d}{|\mathbb{S}|}.$$

Proof: (by induction on n)

1. If $n = 1$: This case involves a 1-variable polynomial of degree d and, by the preceding discussion, we know that the theorem is true.
2. If $n > 1$: We assume that the theorem is always true when the number of variables is at most $n - 1$.

   $R(x_1, x_2, ..., x_n)$ can be written $R(x_1, x_2, ..., x_n) = \sum_{i=1}^{d} x_1^i R_i(x_2, ..., x_n)$. For example, if $R(x_1, x_2, x_3) = x_1^2 x_2 x_3^3 + x_1 x_2^2 + x_2^2 x_3$, then

   $$R_0 = x_2^2 x_3$$

   $$R_1 = x_2^2$$

   $$R_2 = x_2 x_3^3.$$

   Consider that k is the largest exponent of x_1 such that $R_k(x_2, ..., x_n) \not\equiv 0$. Then $R(x_1, x_2, ..., x_n) = \sum_{i=1}^{k} x_1^i R_i(x_2, ..., x_n)$. Obviously, $0 \leq k \leq d$, and R_k has at most $n - 1$ variables and degree at most $d - k$.

   We can easily obtain the following two inequalities:

$$Pr[R_k(r_2, ..., r_n) = 0] \leq \frac{d-k}{|\mathbb{S}|}$$

$$Pr[R(r_1, r_2, ..., r_n) = 0 | R_k(r_2, ..., r_n) \neq 0] \leq \frac{k}{|\mathbb{S}|}.$$

The first inequality follows from the fact the $R_k(x_2, ..., x_n)$ is a nonzero polynomial of at most $n-1$ variables (so we can use the induction hypothesis), and the second inequality follows from the fact that, once $(r_2, \ldots, r_n)$ are fixed and satisfy $R_k(r_2, ..., r_n) \neq 0$, then $R(x_1, r_2, ..., r_n)$ is a nonzero polynomial of one variable (so we can use again the induction hypothesis). Invoking the lemma described below, we find that the probability that $R(r_1, r_2, ..., r_n) = 0$ is no more than the sum of these two probabilities, which is $d/|\mathbb{S}|$.

□

Lemma 2.3. *For any events A and B, the following inequality is always true*

$$Pr[A] \leq Pr[A|\bar{B}] + Pr[B]$$

Proof:

$$Pr[A] = Pr[A \cap \bar{B}] + Pr[A \cap B] = Pr[A|\bar{B}] \times Pr[\bar{B}] + Pr[A \cap B] \leq Pr[A|\bar{B}] + Pr[B].$$

□

2.3 Application: Perfect Matchings in Graphs

In this section, we illustrate the power of the techniques of last section by giving an application. Let $G = (U, V, E)$ be a bipartite graph, in which $U = \{u_1, u_2, ..., u_n\}$, $V = \{v_1, v_2, ..., v_n\}$, and E describes the set of edges of G. A *matching* is a collection of edges $M \subseteq E$ such that each vertex occurs at most once in M. A *perfect matching* is a matching of size n. The perfect matchings in G can be put into a one-to-one correspondence with the permutations in S_n, where the matching corresponding to a permutation $\pi \in S_n$ is given by the pairs $(u_i, v_{\pi(i)})$, for $1 \leq i \leq n$.

Theorem 2.4 (Edmonds' Theorem). *Let A be the $n \times n$ symbolic matrix obtained from $G(U, V, E)$ as follows.*

$$A_{ij} = \begin{cases} x_{ij} & (u_i, v_j) \in E \\ 0 & (u_i, v_j) \notin E \end{cases}$$

A is called the Edmonds' matrix of G. Then G has perfect matching if and only if $det(A) \not\equiv 0$ (as a multivariate polynomial of the $x'_{ij}s$).

Proof:

$$det(A) = \sum_{\pi \in S_n} A_{1,\pi(1)} A_{2,\pi(2)} ... A_{n,\pi(n)}$$

Since each indeterminate x_{ij} occurs at most once in A, there can be no cancellation of the terms in the sum. Therefore $det(A)$ is not zero if and only if there is a permutation π for which the corresponding term in the sum is nonzero. It happens if and only if each of the entries $A_{i,\pi(i)}$, for $1 \leq i \leq n$, is nonzero. This is equivalent to having a perfect matching in G. $\square$

Remark. Computing the polynomial $det(A)$ is hard. However, we can easily compute $det(A)$ for specific values of x_{ij} in $O(n^3)$ time. Therefore, by using the randomized algorithm described in last section, we can detect the existence of a perfect matching with high probability efficiently.

Example:

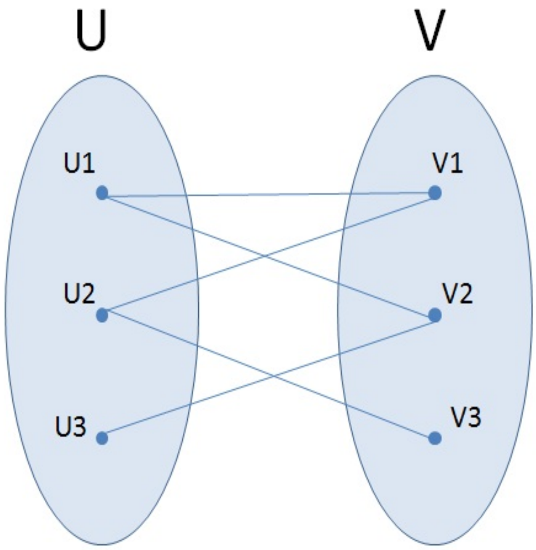

Figure 2.1. example of a graph containing a perfect matching

Edmonds' matrix corresponding to fig 2.1 is given by A.

$$A = \begin{pmatrix} x_{11} & x_{12} & 0 \\ x_{21} & 0 & x_{23} \\ 0 & x_{32} & 0 \end{pmatrix}$$

Since $det(A) = -x_{11}x_{23}x_{32}$, G has one unique perfect matching $\{(u_1, v_1), (u_2, v_3), (u_3, v_2)\}$.