Algebraic Techniques

Wafi AlBalawi and Yan Liu
Department of Computer Science and Electrical Engineering,
West Virginia University,
Morgantown, WV
wafi,yanliu@csee.wvu.edu

1 Introduction

In this chapter we describe some basic randomization techniques with an underlying algebraic flavor. We begin by describing Freivalds' technique for the verification of identities involving matrices, polynomials, and integers. We describe how this generalizes to the Schwartz-Zippel technique for identities involving multivariate polynomials, and we illustrate this technique by applying it to the problem of detecting the existence of perfect matchings in graphs.

Most of these techniques and their applications involve a `fingerprinting` mechanism, which can be described as follows. Consider the problem of deciding the equality of two elements x and y drawn from a large universe U. Under any "reasonable" model of computation, testing the equality of x and y then has a deterministic complexity of at least $\log |U|$. An alternative approach is to pick a random mapping from U into a significantly smaller universe V in such a way that there is a good chance that x and y are identical if and only if their images are identical. The images of x and y are their fingerprints, and their equality can be verified in $\log |V|$ time by comparing the `fingerprints`.

2 Fingerprinting and Freivalds' Technique

We illustrate fingerprinting by describing a technique for verifying matrix multiplication. The fastest known algorithm for matrix multiplication runs in time $O(n^{2.376})$, which improves significantly on the obvious $O(n^3)$ time algorithm but has the disadvantage of being extremely complicated. Suppose we are given an implementation of this algorithm and would like to verify its correctness. Since program verification is a difficult task, a reasonable goal might be to verify the correctness of the output produced on specific executions of the algorithm.

Given $n \times n$ matrices A, B, we can calculate matrix $C = AB$ in $O(n^{2.376})$. The problem: if you are given A, B, and C over the field $\mathbf{F}$, we would like to verify if indeed $AB = C$. We would like to use the fact that we do not have to compute C. The following technique, known as Freivalds' technique 2.1, provides an elegant solution which takes $O(n^2)$ time with bounded error probability.

1: Choose a random vector $\vec{\mathbf{r}} \in \{0,1\}^n$; each component of r is chosen independently and uniformly at random from 0 and 1, the additive and multiplicative identities of the field F.
2: Compute $x = Br$, $y = Ax = ABr$, $z = Cr$ in $O(n^2)$ time.
3: If $AB = C$ then $y = z$
4: We show that $\Pr(y \neq z | AB \neq C) \geq \frac{1}{2}$, algorithem errs only if $AB \neq C$ BUT $y = z$

Algorithm 2.1: Freivalds' Algorithm

Theorem: 2.1 *Let A, B and C be $n \times n$ matrices over $\boldsymbol{F}$ such that $AB \neq C$. Then for r chosen uniformly at random from $\{0,1\}^n$:*

$$Pr[ABr = Cr | AB \neq C] \leq \frac{1}{2}$$

Proof:
Let $D = AB - C$, $D \neq Z$ where Z is the 0-matrix. Permute D so that the first row has non-zero entries and all non-zero occur before zeros.
Let d be the first row in D, the first entry in Dr is $d^T r$.
$Pr[d^T r] \neq 0$ is a lower bound on $Pr[Dr]$=[0].
Now the inner product, $d^T r = 0$ if and only if $r_1 = \frac{-\sum_{i=2}^{k} d_i r_i}{d_1}$.
By the principle of deferred decision, the right hand side of the above expression has a predetermined value v, which is 0 or 1 with uniform probability.
Then $Pr[r_1 = v] \leq \frac{1}{2}$.
□

3 Verifying Polynomial Identities

In this section we show that Freivalds' technique applies to the verification of identities involving polynomials. Two polynomials $P(x)$ and $Q(x)$ are said to be equal if they have the same coefficients for corresponding powers of x. Verifying identities of integers, or, in general, strings over any fixed alphabet, is a special case since we can represent any string of length n as a polynomial of degree n. This is achieved by treating the k^{th} element in the string as the coefficient of the k^{th} power of a symbolic variable.

3.1 Verifing Polynomial Identities (Univariate)

We first consider the `polynomial product verification` problem: given polynomials $P_1(x), P_2(x), P_3(x) \in \mathbf{F}[X]$ where $\mathbf{F}$ is a field, verify that $P_1(x) \times P_2(x) = P_3(x)$. Assume that the polynomials $P_1(x)$ and $P_2(x)$ are of degree at most n; then $P_3(x)$ cannot have degree exceeding $2n$. Polynomials of degree n can be multiplied in $O(n \log n)$ time using *Fast Fourier Transforms*, whereas the evaluation of a polynomial at a fixed point requires $O(n)$ time.

Let $\mathbf{S} \subseteq \mathbf{F}$ be a set of size at least $2n + 1$ pick $r \in \mathbf{S}$ uniformly at random. if $P_1(r) \times P_2(r) = P_3(r)$, then with high probability $P_1(x) \times P_2(x) = P_3(x)$ if $P_1(r) \times P_2(r) \neq P_3(r)$, then we `know` $P_1(x) \times P_2(x) \neq P_3(x)$ we err `only` if we say `YES` where it is not.

Theorem: 3.1 *Let $Q(x)$ be a polynomial of degree d over field $\boldsymbol{F}$. Let $\boldsymbol{S} \subseteq \boldsymbol{F}$ be a finite subset of $\boldsymbol{F}$. Let $r \in \boldsymbol{S}$ be chosen uniformly at random, then*

$$Pr[Q(r) = 0 \mid Q(x) \neq 0] \leq \frac{d}{|\boldsymbol{S}|}$$

Proof: *The degree of $Q(x)$ is d, so it can be 0, at most, d points.*
Any two non-zero degree d polynomials can touch at, at most d points. □

3.2 Schwartz-Zippel Theorem

Theorem: 3.2 *Let $Q(x_1, ..., x_n) \in \boldsymbol{F}[x_1, ..., x_n]$ be a multivariate of total degree d.*
Fix any finite set $\boldsymbol{S} \subseteq \boldsymbol{F}$, and let $r_1, ..., r_n$ be chosen independently and uniformly at random form $\boldsymbol{S}$. Then

$$Pr[Q(r_1, ..., r_n) = 0 \mid Q(x_1, ..., x_n) \neq 0] \leq \frac{d}{|\boldsymbol{S}|}$$

Proof: *Proof by induction:*
The Base Case: $Q(x_1)$ *of degree d. (As before). Assume that the induction hypothesis is true for a multivariate polynomial with* $n-1$ *variable.*
Consider $Q(x_1,..,x_n) = \sum_{i=0}^{k} X_1^i Q_i(x_2,...,x_n)$, *Consider* $Q(x_(2),...,x_n \neq 0)$ *by choice of k.*
$Pr[Q_k(r_2,...,r_n) = 0 \mid Q_k(x_2,...,x_n) \neq 0] \leq \frac{d-k}{|\boldsymbol{S}|}$ *by the hypothesis.*
Now Assume that $Q_k(r_2, r_3, ..., r_n) \neq 0$.
Consider $q(x_1) = Q(x_1, r_2, r_3, ..., r_n) = \sum_{i=0}^{k} X_1^i Q_i(r_2,...,r_n)$, $q(x_1)$ *has degree k and it is NOT identically 0.*

The base case implies that:

$$Pr[q(r_1 = 0) \mid q(x_1 \neq 0) \leq \frac{k}{\boldsymbol{S}}]$$

Now we have these two facts:

1. $Pr[Q_k(r_2, r_3, ..., r_n) = 0] \leq \frac{(d-k)}{\boldsymbol{S}}$.
2. $Pr[Q_k(r_1, r_2, ..., r_n) = 0 \mid Q_k(r_2, ..., r_n) \neq 0] \leq \frac{(k)}{\boldsymbol{S}}$.

Then $Pr[Q_k(r_1, r_2, ..., r_n) = 0 \mid Q(x_1, x_2, ..., x_n) \neq 0)] \leq \frac{(d-k)}{\boldsymbol{S}}$.
Invoking the result in Exercise 3.1, we find that the probability that $Q(r_1, r_2, ..., r_n) = 0$ *is no more than the sum of these two probabilities, which is* $\frac{d}{\boldsymbol{S}}$. □

Exercise 3.1: Show that for any two events E_1 and E_2,

$$Pr[E_1] \leq Pr[E_1|\bar{E_2}] + Pr[E_2]$$

Solution: look at the lecture notes "A Probabilistic Identity" which posted on the class website.

4 Perfect Matchings in Graphs

Consider a bipartite graph $G(U, V, E)$ with the independent sets of vertices $U = u_1, ..., u_n$ and $V = v_1, ..., v_n$. 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. Each perfect matching M in G can be viewed as a permutation from U into V. More precisely, 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 $1 \leq i \leq n$.

Edmonds' Theorem

Theorem: 4.1 *Let A be the* $n \times n$ *matrix obtained from* $G(U, V, E)$ *as follows:*

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

Define the multivariate polynomial $Q(x_1, x_2, ..., x_n)$ *as being equal to* $det(A)$. *Then, G has a perfect matching if and only if* $Q \neq 0$.

Proof: *The determinant of A is given by*

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

Since each indeterminate x_{ij} *occurs at most once in A, there can be no cancellation of the terms in the summation. Therefore the determinant is not identically zero if and only if there is a permutation* π *for which the corresponding term in the summation is non-zero. The latter happens if and only if each of the entries* $A_i, \pi_(i)$, *for* $1 \leq i \leq n$, *is non-zero. This is equivalent to having a perfect matching in G.* □

References

[1] Rajeev Motawani, and Prabhakar Raghavan. *Randomized Algorithms.* Cambridge University Press, 1995.