CS-E4500 Problem Set 6

Jaan Tollander de Balsch - 452056

February 28, 2019

Problem 1

Let F be a field with at least q elements.

(a)

Let $f, \tilde{f} \in F[x]$ be polynomials of degree at most d. Show that if $f \neq \tilde{f}$ then a uniform random $\xi \in F$ satisfies $f(\xi) \neq \tilde{f}(\xi)$ with probability at least $1 - d/q$.

By assuming that the polynomials are not equal $f \neq \tilde{f}$ the polynomial $g = f - \tilde{f}$ is nonzero. The roots ξ of the polynomial g satisfy $f(\xi) = \tilde{f}(\xi)$. Since g is nonzero it has at most d distinct roots $\xi \in F$. Therefore there is at most a probability d/q of picking a uniform random value ξ in F such that it satisfies $f(\xi) = \tilde{f}(\xi)$. Equivalently, there is at least $1 - d/q$ probability that ξ satisfies $f(\xi) \neq \tilde{f}(\xi)$.

(b)

Let $a, b, c \in F[x]$ be three polynomials, each of degree at most d and each given as a sequence of coefficients. Present a randomized test that verified $c = ab$ and uses $O(d)$ operations in F. If $c = ab$ the test must accept with probability 1; if $c = ab$ the test must reject with probability at least $1 - d/q$.

The probability is quaranteed by results from (a).

Evaluate the polynomials a, b, c at uniform random $\xi \in F$ using the Horner's rule. Horner's rule uses $O(d)$ operations in F and assumes constant $O(1)$ complexity for addition and multiplication in F. Then compute $b(\xi)c(\xi)$ and do the comparison $a(\xi) = b(\xi)c(\xi)$ which reduces to addition $a(\xi) - b(\xi)c(\xi) = 0$. Therefore the total number of operations required in for the test is $O(d) + O(1) + (1) = O(d)$.

Problem 2

Let A, B, C be three $n \times n$ matrices with entries in a field F. Present a randomized algorithm that tests whether $C = AB$ using $O(n^2)$ operations in F. When $C = AB$, your algorithm must always assert that $C = AB$. When $C \neq AB$, your algorithm must assert that $C \neq AB$ with probability at least $1/2$.

We have the following equality

$$\begin{aligned} C &= AB \\ Cx &= (AB)x \\ Cx &= A(Bx) \end{aligned}$$

where $x \in F^n$ is a vector. Using this form of the equality, the equality testing will only require $O(n^2)$ operations since the product of $F^{n \times n}$ matric and F^n vector has dimension of F^n and uses $O(n^2)$ operations in F (unlinke naive matrix multiplication, which uses $O(n^3)$).

By assuming $C \neq AB$ we have nonzero matrix $D = (C - AB) \neq \mathbf{0}$. Let $x \in \Omega = \{0, 1\}^n \subseteq F^n$ be a binary vector. Then the probability that we choose a uniform random x such that $Dx \neq 0$ is the same as the probability that $Dx = 0$ due to a symmetry.

Proof: Let the star $\star$ represent an element that is either 0 or 1. Let $x \in \Omega$ be a vector such that $Dx \neq 0$. Then x consists of elements 1 and $\star$. Then we can construct a vector $y \in \Omega$ such that $Dy = 0$ by substituting all 1 with 0, but keeping stars $\star$ as stars. As an example:

$$Dx = \begin{bmatrix} \varepsilon & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ \star \end{bmatrix} \neq \mathbf{0} \text{ then } Dy = \begin{bmatrix} \varepsilon & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ \star \end{bmatrix} = \mathbf{0}$$

where $\varepsilon \neq 0$.

Because there is a vector y for every vector x this means that the probabilities are equal

$$P(Dx = 0) = P(Dx \neq 0).$$

Also, probability theory gives us

$$P(Dx = 0) + P(Dx \neq 0) = 1.$$

Therefore the probability

$$P(Dx \neq 0) = \frac{1}{2}.$$

Problem 3

Problem 4

References