CSC373S Lecture 14

- Question 5 in the problem set mentions the FFT which I have temporarily skipped. The question can be answered without knowing anything about the FFT except that it enables multiplying two degree n polynomials in $O(n \log n)$ (complex) arithmetic steps. I have skipped it as it is not easy to find a question at the appropriate level but I will (later) discuss the DFT (Discrete Fourier Transform) problem and the FFT (Fast Fourier Transform) algorithm for the FFT.

- The missing probability bounds from the last lecture.

  1. Testing if $C = A * B$. Here we assume that the matrix elements are from a ring R (eg integers) and we let S be an arbitrary subset of R. We will choose a random vector $\vec{x} = (x_1, \ldots, x_n) \in S^n$ meaning that each x_i is uniformly and independently chosen from S.
     Given C, A, B we want to prove that $Prob_{x \in_U S}[(C\vec{x} = (A * B)\vec{x} | C \neq A * B]] = Prob[(C - A * B)\vec{x} = \vec{0} | C \neq A * B] \leq \delta$ for some δ.

     Let $D = C - A * B$ and assume $D \neq 0_{n*n}$, the all zero matrix. By rearranging rows and columns of D, wlg say that the first row $(d_1, ..., d_n) \neq \vec{0}$ and $d_1 \neq 0$.
     If $D\vec{x} = \sum_{i=1}^{n} d_i \cdot x_i = 0$ then $x_1 = -\sum_{i=2,\ldots,n} d_i \cdot x_i / d_1$. Think of choosing x_1 last; then if $-\sum_{i=2,\ldots,n} d_i \cdot x_i / d_1 \notin S$, then $Prob[x_1 = -\sum_{i=2,\ldots,n} d_i \cdot x_i / d_1] = 0$, else $Prob = 1/|S|$.
     Hence $Prob_{\vec{x} \in_U S^n}[C\vec{x} = A * B\vec{x} | C \neq AB] \leq 1/|S|$.
     We can either decrease the error probability by increasing the size of S or we can run this test for several independent trials.

     NOTE: We call this a *one-sided error* algorithm as it can only make an error for the case that $C \neq A * B$ and never makes an error when $C = A * B$.

  2. The symbolic determinant problem. Let $n \times n$ matrix A have entries a_{ij} which are linear polynomials, say $a_{ij} \in R[x_1, \ldots, x_m]$ for some ring R. We are testing if $det(A) = \bar{0}$, the identially zero polynomial. We will again have a one sided error which will always answer correctly when the determinant is the identically zero polynomial and only has some bounded error probability when the determinant is not the identically zero polynomial.

     Recall that $det(A)$ is a degree n polynomial (i.e. total degree n). Let S be a subset of the ring R with $|S| \geq 2n$. (In fact, $|S| \geq n + 1$ will suffice). To prove the desired error probability bound we need to use the Schwartz-Zipple Lemma.

     Let $f \in R[x_1, \ldots x_m]$ be a non zero polynomial of degree $d \geq 0$. Then $Prob_{\vec{r} \in_U S^m}[f(r_1, \ldots, r_m) = 0] \leq \frac{d}{|S|}$.

     Note 1: In the previous example of testing $C = A * B$, we were essentially using this Lemma with $d = 1$.

The proof of the Lemma is by induction on m (i.e. for univariate polynomials) and this base case follows from something well known. Namely, any univariate polynomial of degree d has at most d zeros. Hence the probability is at most $\frac{d}{|S|}$ that we will choose r_1 such that $f(r_1) = 0$. For the induction step, we view f as $\sum_{0 \leq i \leq j} x_1^j f_j(x_2, \ldots, x_m)$ and let j be the largest $j \leq d$ such that f_j is not identically zero. Why must such a j exist? Note that degree of $f_j \leq d - j$. Then by induction, $Prob[f_j(r_2, \ldots, r_m) = 0] \leq \frac{d-j}{|S|}$. If $f_j(r_2, \ldots, r_m) \neq 0)$ then $Prob[f(r_1, r_2, \ldots, r_m] = Prob[\sum_{1 \leq i \leq j} r_1^i f_i = 0] \leq \frac{j}{|S|}$. The probability that $f_(r_1, \ldots, r_m) = 0$ is at most the sum of the probability that f_j is identically zero and the probability $Prob[\sum_{1 \leq i \leq j} r_1 f_i = 0]$ given that f_j is not identically zero. That is, the sum of these two probabilities is at most $\frac{d-j}{|S|} + \frac{j}{|S|} = \frac{d}{|S|}$ which concludes the proof of the Schwartz Zipple Lemma.

Now we apply this to the symbolic determinant problem and we see that the probability of error (when $det(A) = \bar{0}$ is at most $1/2$ if say $|S| \geq 2n$. This error probability can be reduced to $(1/2)^k$ by repeating the algorthm for k independent trials.

- Why did we say that $|S| \geq n + 1$ would suffice in the symbolic determinant algorithm? Here we are saying that the error probability is say only bounded by $n/n + 1 = 1 - 1/(n + 1)$. So as before we can argue that in k repeated trials (of a one sided error algorithm) the error probability is $[1 - \frac{1}{n+1}]^k$. Is this good?

  Fact: $[1 - 1/t]^t \leq \frac{1}{e}$ for all $t \geq 0$ and $lim_{t \to \infty}[1 - 1/t]^t = \frac{1}{e}$. So letting $k = n + 1$, we obtain a constant error probability and can further reduce that by more trials. In general, when we have a one sided error, all we need is a polynomial $\frac{1}{n^s}$ probability of success at the cost of having to run the algorithm n^s times.

  Note: Just having an exponentially small probability of success is not good enough! I refer to algorithms with such small probability of success as being "needle in the haystack algorithms".