Lecture - 8

Wednesday, 10 August 2016 (14:25- 15:15)

Matrix Multiplication Verification

1 One sided errors in randomized algorithms

In this section we will study the notion of one-sided error in randomized algorithms. Please note that the meaning of one-sided error in approximation algorithms is very different from what we will be discussing in the case of randomized algorithms.

1.1 One sided error in polynomial evaluation

In the previous lecture, we studied a randomized algorithm (let us represent it by $\mathcal{A}$) which checks if $p(x)$ equals $q(x)r(x)$ very efficiently, where p, q and r are polynomials. Whenever the algorithm $\mathcal{A}$ outputs "unequal", then we are sure that the input polynomials are not the same, since there exists some α such that $p(\alpha) \neq q(\alpha)r(\alpha)$. Whereas, if the algorithm $\mathcal{A}$ outputs "equal", we cannot say with 100% confidence that the polynomial $p(x)$ equals $q(x)r(x)$. This is what is meant by a one-sided error in a randomized algorithm. A randomized algorithm with one-sided error can be of two types: true-biased and false-biased. A true-biased algorithm is the one which is correct whenever it outputs "yes", whereas it may be wrong when it outputs "no", on the other hand a false-biased algorithm is the one which is correct whenever it outputs "no", whereas it may be wrong when "yes" is its output.

1.2 Another example to illustrate one-sided error

Consider the following program:

Check if a number is prime

---

i/p: n, where n is any number greater than 4
o/p: yes/no

If ($n\%6 == 1$ or $n\%6 == 5$):
    return "yes"
else
return "no"

If the above algorithm outputs "no", then the input number n is without doubt composite (it must be a multiple of 2 or 3), whereas if the output is "yes", we cannot say for sure if the input number is prime. Few numbers on which the algorithm gives a false positive include 25, 47 and 65. This is an example of an algorithm that is false-biased.

2 Pre-requisites for the next randomized algorithm

Before studying the next randomized algorithm (which is matrix multiplication verification) you will need to brush up some basic linear algebra and modular arithmetic. All the pre-requisites are summarized in the following four points:

1. Let $A, B \subseteq S$, where S is a finite set, such that $A \cap B = \phi$ i.e. A and B are disjoint sets. Show that if there exist a bijection $f : A \to B$, then $|A| = |B| \leq \frac{1}{2}|S|$.

   Proof. First we observe that $|A| = |B|$, since there exist a bijection between the two finite sets A and B. Further, we have

   $$\begin{aligned} |S| &\geq |A \cup B| \\ &= |A| + |B| - |A \cap B| && \text{(from the inclusion-exclusion principle)} \\ &= |A| + |B| && \text{(since } A \text{ and } B \text{ are disjoint sets)} \\ &= 2|A| \end{aligned}$$

   □

2. The application of an $n \times n$ matrix M on an $n \times 1$ column vector v is a linear combination of the columns of M, where the scalar constants are the entries of the vector v. In other words,

   $$Mv = v_1C_1 + v_2C_2 + \cdots + v_nC_n$$

   where C_i and v_i represents the i^{th} column of M and the i^{th} entry of the column vector v respectively.
   As an example, let

   $$M = \begin{pmatrix} 1 & 4 & 5 \\ 7 & 2 & 4 \\ 6 & 7 & 0 \end{pmatrix} \text{ and } v = \begin{pmatrix} 4 \\ 8 \\ 3 \end{pmatrix}$$

   then

   $$Mv = 4\begin{pmatrix} 1 \\ 7 \\ 6 \end{pmatrix} + 8\begin{pmatrix} 4 \\ 2 \\ 7 \end{pmatrix} + 3\begin{pmatrix} 5 \\ 4 \\ 0 \end{pmatrix}$$

3. Let $\mathbb{R}$ represent the set of all real numbers, then $\mathbb{R}^2$ represents the set $\{(a, b)|a, b \in \mathbb{R}\}$. Given $\mathbb{Z}_2 = \{0, 1\}$, we can define $\mathbb{Z}_2^n$ as the set of all n length binary vectors i.e.

   $$\mathbb{Z}_2^n = \{(v_1, v_2, \ldots, v_n)_{n\times 1} | \text{ where } v_i \in \mathbb{Z}_2 \ \forall 1 \leq i \leq n\}$$

   Further we can define the addition operation $+^n$ over $\mathbb{Z}_2^n$ as the component wise xor operation. For example, $(0, 1, 0) +^3 (1, 0, 0) = (1, 1, 0)$.

4. A simple yet very useful result for our next expedition is the following:

   Lemma 1. *An $n \times n$ matrix M is non-zero if and only if there exist a vector $v \in \mathbb{Z}_2^n$ such that Mv is a non-zero vector.*

   Proof. First we will prove (LHS $\implies$ RHS). Since M is a non-zero matrix, it has a non-zero column as well, let say it is the i^{th} column C_i for some $1 \leq i \leq n$. Consider the non-zero vector $v = (0, 0, \ldots, 0, 1, 0, \ldots, 0)_{n\times 1}$, where only the i^{th} entry of v is 1 while others are 0. The RHS follows since, $Mv = v$ and v is a non-zero vector. The proof for (RHS $\implies$ LHS) is trivial. □

3 A randomized algorithm for verifying matrix multiplication

Let say you wish to compute the product of two $n \times n$ matrices A and B (where n is a very large). Since the naive old school algorithm for multiplication (which runs in $\mathcal{O}(n^3)$) is too time consuming to be run on your laptop, you pass on this computation to a high performance computing (HPC) facility in your institute. Let say the output of the algorithm is a matrix C. The computation performed by the HPC facility is prone to bugs, hence you are now given the task of verifying if $A * B$ equals C. Can we verify the product of two matrices faster than just multiplying them? And the answer is: Yes, we can! Further we will go through Freivalds' algorithm for matrix multiplication verification proposed in 1977.

Matrix multiplication verification

---

i/p: A, B and C, where all these three are $n \times n$ matrices
o/p: yes/no depending on whether or not AB equals C

for $i = 1$ to 100:
    Pick $v \in_R \mathbb{Z}_2^n$
    if $A(Bv) \neq C(v)$
        return "no"
return "yes"

Please note that $\in_R$ signifies that the element is randomly picked. For example, $r \in_R \{1, 2, 3\}$ implies that r can be 1 with probability 1/3, 2 with probability 1/3 and 3 with probability 1/3.

Few observations about the above algorithm:

- The algorithm runs in $\mathcal{O}(n^2)$.
- The algorithm has one-sided error and is false-biased.

The one-sided error of this randomized algorithm will be quatified in the next lecture.