Advanced Proof-Systems ; Problem Set 1

Yosef Goren

November 15, 2022

1 Chernoff Bound and Sequential Repetition

1.1 Markov's Inequality

$$\mu = \sum_{r} Pr[x = r] \cdot r = \sum_{r \leq \alpha\mu} Pr[x = r] \cdot r + \sum_{r > \alpha\mu} Pr[x = r] \cdot r$$

$$\geq \sum_{r > \alpha\mu} Pr[x = r] \cdot r > \sum_{r > \alpha\mu} Pr[x = r] \cdot \alpha\mu = \alpha\mu \sum_{r > \alpha\mu} Pr[x = r] = \alpha\mu \cdot Pr[x > \alpha\mu]$$

$$\Rightarrow 1 > \alpha Pr[x > \alpha\mu] \Rightarrow Pr[x > \alpha\mu] < \frac{1}{\alpha}$$

1.2 Chernoff Bound

2

3

4 Matrix Multiplication

4.1 Naive Algorithm

We can deduce an algorithm from the definition of matrix multiplication. Since $\forall i, j : (A \cdot B)_{i,j} = \langle A_{i,:}, B_{:,j} \rangle = \sum_{k=1}^{n} A_{i,k} \cdot B_{k,j}$, we can write the following algorithm:

```
C = zeros(n,n)
for i=1 to n:
for j=1 to n:
    for k=1 to n:
        C[i,j] += A[i,k] * B[k,j]
```

4.2 Random Subset Sum Principle

Lemma:
For any $x \in \mathbb{F}^n \neq 0$ and uniformly sampled $\in \mathbb{F}^n$, $\langle x, y\rangle$ is uniformly distributed over $\mathbb{F}^n$.
Proof of lemma: Since $x \neq 0$, it must have at least one non-zero entry - denote it with x_i. We can see that:

$$\langle x, y\rangle = \sum_{j=1}^{n} x_j y_j = x_i y_i + \sum_{j \neq i} x_j y_j := x_i y_i + \alpha \qquad (*)$$

Note how α is just a constant (with respect to i) value in $\mathbb{F}^n$.
We have also seen in the lecture that for any non-zero $a \in \mathbb{F}^n$, and uniformly sampled $b \in \mathbb{F}^n$ - $a \cdot b$ is distributed uniformly - meaning so is $x_i \cdot y_i$ in (*).
Moreover, for any non-zero $a \in \mathbb{F}^n$, and uniformly sampled $b \in \mathbb{F}^n$ - $a + b$ is also uniformly distributed.
Meaning that in (*), $x_i \cdot y_i + \alpha$ is uniformly distributed, hence - so is $\langle x, y\rangle$.

Proof of claim:
Let $x \in \mathbb{F}^n \setminus \{0\}$. From the lemma, we know that $\langle x, y\rangle$ is uniformly distributed over $\mathbb{F}^n$, thus the probability that $\langle x, y\rangle = 0$ is $\frac{|\{0\}|}{|\mathbb{F}^n|} = \frac{1}{|\mathbb{F}^n|}$.

4.3 Randomized Verification of Matrix Multiplication

Algorithm P:

```
1 On input A,B,C
2 sample x uniformly from F^n
3 d := B*x
4 e := A*d
5 c := C*x
6 return e=c
```

Now it is easy to see how the complexity of this algorithm is $O(n^2)$, since in lines 3,4,5 we have operations of $O(n^2)$ complexity, and the rest of the operations seen can be done in linear complexity.

As for the correctness:

- Completness - If $A \cdot B = C$, then $Pr[P(A, B, C) = 1] = 1$:
  When indeed $A \cdot B = C$, then multipling both sides by x will yield the same value, meaning $e = c$ and $P(A, B, C) = 1$.

- Soundness - If $A \cdot B \neq C$, then $Pr[P(A, B, C) = 1] \leq \frac{1}{2}$:
  The conditions for the algorithm to accept are:

  $$(AB)x = Cx \Leftrightarrow \forall i \in [n] : (AB)_{i,:} x_i = C_{i,:} x_i \Leftrightarrow \forall i \in [n] : ((AB)_{i,:} - C_{i,:}) x_i = 0$$

Now since $A \cdot B \neq C$, there must be at least one k such that:

$$(AB)_{k,:} - C_{k,:} \neq 0 \Rightarrow Pr[(AB)_{k,:} - C_{k,:} \cdot x_k] \leq \frac{1}{|\mathbb{F}^n|}$$

So we can see:

$$Pr[\forall i \in [n] : ((AB)_{i,:} - C_{i,:})x_i = 0] \leq Pr[((AB)_{i,:} - C_{i,:})x_i] \leq \frac{1}{|\mathbb{F}^n|}$$

It seems fair to assume $|\mathbb{F}^n| \geq 2$, but just in case, we can handle $\mathbb{F} = \{e\}$ by checking for this case spesifically.