(CS602) Applied Algorithms 10 Jan, 2014

Lecture 0: Mathematical Preliminaries

Lecturer: Nutan Limaye *Scribe: Nutan Limaye*

In this note we will cover some basics of probability theory and algebra which will be used during the course.

0.1 Some useful inequalities

We will use capital letters to denote random variables. The notations $\mathbb{E}(X)$ and $\mathbb{V}ar(X)$ stand for expectation and variance of the random variable X, respectively.

Lemma 0.1.1 (Markov's inequality)**.** *Let X be any non-negative random variable. Then,*

$$\Pr[X \geq \alpha] \leq \frac{\mathbb{E}(X)}{\alpha}$$

Lemma 0.1.2 (Chebyshev's inequality)**.** *Let X be any random variable and $\alpha > 0$. Then,*

$$\Pr[|X - \mathbb{E}(X)| \geq \alpha] \leq \frac{\mathbb{V}ar(X)}{\alpha^2}$$

Markov's inequality can be used to prove Chebyshev's inequality. From Markov's inequality, one can also obtain the following strong tail bound for independent random variables.

Lemma 0.1.3 (Chernoff bound)**.** *Let $X_1, X_2, \ldots, X_n$ be i.i.d random variables and $\forall i$ $X_i \in \{0,1\}$. Let $X = \sum_{i=1}^{n} X_i$. Then,*

$$\Pr[|X - \mathbb{E}(X)| \geq \alpha\mathbb{E}(X)] \leq 2e^{-\alpha^2\mathbb{E}(X)}$$

Exercise 1. *You are given a fair unbiased coin. The coin is tossed n times independently. Use all the above inequalities and compute the probability of the following events.*

1. *More than $3n/4$ heads are observed.*
2. *More than $n/2 + 2\sqrt{n}$ heads are observed.*

Comment on which inequalities are applicable and comment on which inequality gives the best bounds.

Exercise 2. *You are given n independent random variables $X_1, X_2, \ldots, X_k$. For every $i \in [n]$, $\Pr[X_i = 1] \geq 3/4$ and $\Pr[X_i = 0] \leq 1/4$. Let $X = \sum_i X_i$. In terms of k compute the probability of the event $X \leq k/4$.*

Exercise 3. *Let $b\{0,1\}$ be a fixed bit. We generate bits $X_1, X_2, \ldots, X_k$ from b by tossing independent coins. Each coin comes up HEAD with probability $3/4$ and TAIL with probability $1/4$. If the ith coin toss comes out to be HEAD then $X_i = b$ else $X_i = 1 - b$. Let $X = majority_i(X_i)$, that is $X = 1$ iff $\sum_i X_i \geq k/2$. What is the probability that $X \neq b$?*

0.2 Abstract algebra

A field $\mathbb{F} = (S, +, *)$ is a set S with two binary operators, $+$ and $*$ with the following properties:

- Closure: For all $a, b \in S$, $a + b \in S$ and $a * b \in S$.
- Associativity: For all $a, b, c \in S$ $a + (b + c) = (a + b) + c$ and $a * (b * c) = (a * b) * c$.
- Identity: There exist two special elements $i_0, i_1 \in S$ such that for all $a \in S$ $a + i_0 = i_0 + a = a$ and $a * i_1 = i_1 * a = a$. Here, i_0 is called the additive identity and i_1 is called the multiplicative identity.
- Inverses: For each element $a \in S$ there exist $a', a'' \in S$ such that $a + a' = a' + a = i_0$ and $a * a'' = a'' * a = i_1$.
- Distributivity: For all $a, b, c \in S$, $a * (b + c) = a * b + a * c$.

A field is called a finite field if $|S|$ is finite.

Exercise 4. *Let p be a prime and let $\mathbb{F}_p$ denote $(\{0, 1, \ldots, p-1\}, + \pmod p, \times \pmod p)$. Prove that $\mathbb{F}_p$ is a finite field. Here, $+$(mod p) and $\times$(mod p) represent addition and multiplication modulo p.*

Is $\mathbb{F}_6$ a finite field? Justify your answer.

Exercise 5. *Let p be a prime and let $\mathbb{F}_p[x] = (S(x), \oplus_p, \otimes_p)$ be a structure defined so that $S = \{$polynomials over the indeterminate x with coefficients from $\{0, 1, \ldots, p-1\}\}$, for two polynomials $r(x), q(x) \in S$, $r(x) \oplus_p q(x)$ defined as addition of two polynomials with coefficients modulo p and $r(x) \otimes_p q(x)$ defined as multiplication of two polynomials with coefficients modulo p. Prove that $\mathbb{F}_p[x]$ is not a field.*

The above is a very useful structure and we may encounter it many times during the course.

Exercise 6. *Let us consider the following structure: $(\{1, 0, x, 1+x\}, + \pmod 2, \times \pmod{x^2 + x + 1})$. Prove that this is a finite field. This finite field is often denoted as $\mathbb{F}_{2^2}$, as this is a finite field with 4 elements.*

In the Exercise 6 we have constructed a field of size 2^2 by performing additions modulo 2 and multiplications modulo a certain fixed polynomial of degree 2. In the same way, if we were to create fields of size 2^k, we can do this by performing additions modulo 2 and multiplications modulo a certain fixed polynomial of degree k.

0.3 Linear algebra

Exercise 7. *Let Q be a $2 \times n$ 0-1 matrix. Suppose the rank of Q is 2, then*

$$\Pr_{\alpha \in \{0,1\}^n}\left[Q\alpha = \begin{bmatrix} 0 \\ 0 \end{bmatrix}\right] = \Pr_{\alpha \in \{0,1\}^n}\left[Q\alpha = \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right] = \Pr_{\alpha \in \{0,1\}^n}\left[Q\alpha = \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right] = \Pr_{\alpha \in \{0,1\}^n}\left[Q\alpha = \begin{bmatrix} 1 \\ 1 \end{bmatrix}\right]$$

0.4 Pairwise independence

Let us define a set of functions $\mathcal{H} = \{h : \{0,1\}^m \to \{0,1\}^n\}$. The number of functions in this set is $(2^n)^{2^m}$. The number of bits required to pick a random function from this family is $\log((2^n)^{2^m})$, i.e. $O(2^m n)$.

Definition 0.4.1. *We call a set of functions $\mathcal{F} \subseteq \mathcal{H}$ a pairwise independent family of functions if $\forall x \neq y \in \{0,1\}^m$ and for any fixed $u, v \in \{0,1\}^n$we have*

$$\Pr_{f \in \mathcal{F}}[f(x) = u \wedge f(y) = v] = \frac{1}{2^{2n}}$$

In class we will often design an algorithm which picks a *purely* random function from a set of *all* functions, i.e. from $\mathcal{H}$. We will then analyze the algorithm and observe that we only need to pick a purely random function from a set of pairwise independent family of functions. We will first give a construction of such a family and then observe some useful properties of such families.

Exercise 8 (Pairwise independent hash functions)**.** *Let $A \in \{0,1\}^{m \times n}$ and $b \in \{0,1\}^n$. Let us define a function $f_{A,b} : \{0,1\}^m \to \{0,1\}^n$ as $f_{A,b}(x) = Ax + b$, where all additions and multiplications are defined modulo 2. Let $\mathcal{F} = \{f_{A,b} \mid A \in \{0,1\}^{n \times m}, b \in \{0,1\}^n\}$. Prove that $\mathcal{F}$ is a family of pairwise independent hash functions. Formally, prove that $\forall x \neq y \in \{0,1\}^m$ and for any fixed $u, v \in \{0,1\}^n$we have*

$$\Pr_{A \in \{0,1\}^{m \times n}, b \in \{0,1\}^n}[f_{A,b}(x) = u \wedge f_{A,b}(y) = v] = \frac{1}{2^{2n}}$$

Proof. Let $x \neq y \in \{0,1\}^m$ be any two fixed vectors and let $u, v \in \{0,1\}^n$ also be two fixed vectors. For an $n \times m$ matrix A, let the ith row of the matrix be denoted as $\tilde{a}_i$. For a vector b let b_i denote its ith bit. Then the condition $Ax + b = u$ can be written as $\wedge_{i=1}^n(\langle \tilde{a}_i, x\rangle + b_i = u_i)$. Therefore,

$$\Pr[f_{A,b}(x) = u \wedge f_{A,b}(y) = v] = \Pr[\wedge_{i=1}^n (\langle \tilde{a}_i, x\rangle + b_i = u_i \wedge \langle \tilde{a}_i, y\rangle + b_i = v_i)]$$

As A, b are chosen independently and uniformly at random, we get that

$$\Pr[\wedge_{i=1}^n (\langle \tilde{a}_i, x\rangle + b_i = u_i \wedge \langle \tilde{a}_i, y\rangle + b_i = v_i))] = \prod_{i=1}^n \Pr_{\tilde{a}_i, b_i}[\langle \tilde{a}_i, x\rangle + b_i = u_i \wedge \langle \tilde{a}_i, y\rangle + b_i = v_i]$$

Suppose we are able to prove that for every i, $\Pr_{\tilde{a}_i \in \{0,1\}^n, b_i\{0,1\}}[\langle \tilde{a}_i, x\rangle + b_i = u_i] = \frac{1}{4}$ then we will be done. To prove that consider the following:

$$\begin{bmatrix} x_1, x_2, ..., x_n, & 1 \\ y_1, y_2, ..., y_n, & 1 \end{bmatrix} \begin{bmatrix} \tilde{a}_{i1}, \tilde{a}_{i2}, \ldots, \tilde{a}_{in}, b_i \end{bmatrix}^T = \begin{bmatrix} u_i \\ v_i \end{bmatrix}$$

As $x \neq y$, there exists $j \in [n]$ such that $x_j \neq y_j$. Therefore the matrix $\begin{bmatrix} x_1, x_2, ..., x_n, & 1 \\ y_1, y_2, ..., y_n, & 1 \end{bmatrix}$ has full row rank.

Therefore, using Exercise 7, we get $\Pr_{\tilde{a}_i \in \{0,1\}^n, b_i \in \{0,1\}}[\langle \tilde{a}_i, x\rangle + b_i = u_i] = \frac{1}{4}$. □

Note that $|\mathcal{F}|$ is $2^{mn}+2^n$. Therefore, the number of bits required for pick a random function from $\mathcal{F}$ is $O(mn)$.

Here is one useful property of pairwise independent 0-1 random variables.

Exercise 9. *Let $X_1, X_2, \ldots, X_n$ be pairwise independent 0-1 random variables. Let $X = \sum_{i=1}^n X_i$. Then $\mathbb{V}ar(X) \leq E(X)$.*

Proof.

$$\begin{aligned}
\mathbb{E}(X^2) &= \mathbb{E}\left((\sum_{i=1}^n X_i)^2\right) \\
&= \mathbb{E}\left(\sum_{i=1}^n X_i^2 + \sum_{i\neq j} X_i X_j\right) \\
&= \mathbb{E}\left(\sum_{i=1}^n X_i + \sum_{i\neq j} X_i X_j\right) && \text{(As } X_i\text{s are 0-1 valued)} \\
&= \mathbb{E}(X) + \sum_{i\neq j} \mathbb{E}(X_i X_j) && \text{(By linearity of expectation)} \\
&= \mathbb{E}(X) + \sum_{i\neq j} 1.\Pr\left[X_i = 1 \wedge X_j = 1\right] && \text{(By the definition of expectation)} \\
&= \mathbb{E}(X) + \sum_{i\neq j} \Pr\left[X_i = 1\right]\Pr\left[X_j = 1\right] && \text{(By pairwise independence of } X_i\text{s)} \\
&= \mathbb{E}(X) + \sum_{i\neq j} \mathbb{E}(X_i)\mathbb{E}(X_j) && \text{(By the definition of expectation)}
\end{aligned}$$

Similarly, we can evaluate $(\mathbb{E}(X))^2$ as follows:

$$\begin{aligned}
(\mathbb{E}(X))^2 &= \left(\mathbb{E}(\sum_{i=1}^n X_i)\right)^2 \\
&= \left(\sum_{i=1}^n \mathbb{E}(X_i)\right)^2 && \text{(By linearity of expectation)} \\
&= \sum_{i=1}^n \mathbb{E}(X_i)^2 + \sum_{i\neq j} \mathbb{E}(X_i)\mathbb{E}(X_j)
\end{aligned}$$

Therefore, $\mathbb{V}ar(X) = \mathbb{E}(X^2) - (\mathbb{E}(X))^2 = \mathbb{E}(X) - \sum_{i=1}^n \mathbb{E}(X_i)^2 \leq \mathbb{E}(X)$. $\square$