Exercises to Complexity Theory and Cryptography

Mihai Prunescu

Definition: Let Ω be a finite set, $Pr : \Omega \to [0,1]$ a probability (meaning that $\sum_{\omega\in\Omega} Pr(\omega) = 1$) and $X : \Omega \to \mathbb{R}$ a random variable. We define here the mean (expectation) $E(X)$, the variance $Var(X)$ and the standard deviation σ:

$$E(X) = \sum_{\omega\in\Omega} X(\omega)Pr(\omega),$$

$$Var(X) = E[(X - E(X))^2],$$

$$\sigma = \sqrt{Var(X)}.$$

Exercise 1: *Let $X \geq 0$ be a random variable and $a, b > 0$. Prove Markov's inequalities:*

$$Pr[\ X \geq a\ ] \leq \frac{E(X)}{a},$$

$$Pr[\ X \geq bE(X)\ ] \leq \frac{1}{b}.$$

Recall that for some probability space Ω and some $B \subseteq \Omega$ such that $Pr[B]$ is defined, B is itself a probability space with the new probability:

$$Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]}.$$

This is called conditional probability.

Observe that:

$$E(X) = Pr[X < a] \cdot E(X|X < a) + Pr[X \geq a] \cdot E(X|X \geq a).$$

But $E(X|X < a) \geq 0$ because $X \geq 0$ and $E(X|X \geq a) \geq a$ because there all values of X are $\geq a$. It follows:

$$E(X) \geq Pr[\ X \geq a\ ] \cdot E(X|X \geq a) \geq aP[\ X \geq a\ ],$$

$$Pr[\ X \geq a\ ] \leq \frac{E(X)}{a}.$$

For the second inequality, replace a with $bE(X)$.

Exercise 2: *No more than $1/5$ of population can earn more than 5 times the average income.*

Follows directly from the second inequality of Markov for $b = 5$.

Exercise 3: *Let $a, b > 0$ and X be any random variable, not necessarily positive. Prove Chebychev's inequalities:*

$$Pr[\ |X - E(X)| \geq a\ ] \leq \frac{Var(X)}{a^2},$$

$$Pr[\ |X - E(X)| \geq b\sigma\ ] \leq \frac{1}{b^2}.$$

We consider the nonnegative random variable $Y := (X - E(X))^2$ and we write down Markov's inequality for $a^2 > 0$:

$$Pr[\ Y \geq a^2\ ] \leq \frac{E(Y)}{a^2},$$

and this means by definition:

$$Pr[\ (X - E(X))^2 \geq a^2\ ] \leq \frac{Var(X)}{a^2}.$$

But $(X - E(X))^2 \geq a^2$ if and only if $|X - E(X)| \geq a$, so:

$$Pr[\ |X - E(X)| \geq a\ ] \leq \frac{Var(X)}{a^2}.$$

But $\sigma^2 = Var(X)$. We put $a = b\sigma$ and get:

$$Pr[\ |X - E(X)| \geq b\sigma\ ] \leq \frac{1}{b^2}.$$

Exercise 4: *Show that:*

$$Var(X) = E(X^2) - E(X)^2.$$

Indeed: $Var(X) = E((X - E(X))^2) = E(X^2 - 2XE(X) + E(X)^2) = E(X^2) - E(2XE(X)) + E(E(X)^2) = E(X^2) - 2E(X)E(X) + E(X)^2 = E(X^2) - E(X)^2$.

Exercise 5: *Compute the mean (expectation), the variance and the standard deviation for a fair coin with values a and b. Also for $a = 0$ and $b = 1$.*

$E(C) = (a + b)/2$, $Var(C) = E(C^2) - E(C)^2 = (a^2 + b^2)/2 - (a + b)^2/4 = a^2/4 - ab/2 + b^2/4$, so $Var(C) = (a - b)^2/4$ and $\sigma = |a - b|/2$. For the 0 - 1 coin, $E(C) = 1/2$, $Var(C) = 1/4$ and $\sigma = 1/2$.

Exercise 6: *Compute the mean (expectation), the variance and the standard deviation for a fair die with values* $1, 2, 3, 4, 5, 6$.

$E(Z) = (1 + 2 + 3 + 4 + 5 + 6)/6 = 21/6 = 7/2 = 3.5$

$Var(Z) = (1 + 4 + 9 + 16 + 25 + 36)/6 - 49/4 = 91/6 - 49/4 = 182/12 - 147/12 = 35/12$

$\sigma = \sqrt{105}/6 = 1.707$

Exercise 7: *The random variables X_1 and X_2 are independent if $Pr[\ X_1 = a \wedge X_2 = b\ ] = Pr[\ X_1 = a\ ] \cdot Pr[\ X_2 = b\ ]$ for all values of a and b. Show that for independent variables the following are true:*

$$E(X_1X_2) = E(X_1)E(X_2),$$

$$Var(X_1 + X_2) = Var(X_1) + Var(X_2).$$

Indeed:

$$E(X_1X_2) = \sum_{a,b\in\mathbb{R}} abPr[\ X_1 = a \wedge X_2 = b\ ] = \sum_{a,b\in\mathbb{R}} abPr[\ X_1 = a\ ] \cdot Pr[\ X_2 = b\ ] =$$

$$= \Big(\sum_{a\in\mathbb{R}} aPr[\ X_1 = a\ ]\Big)\Big(\sum_{b\in\mathbb{R}} bPr[\ X_2 = b\ ]\Big) = E(X_1)E(X_2).$$

$$Var(X_1 + X_2) = E((X_1 + X_2)^2) - E(X_1 + X_2)^2 =$$
$$= E(X_1^2) + 2E(X_1X_2) + E(X_2^2) - E(X_1)^2 - 2E(X_1)E(X_2) - E(X_2)^2 =$$
$$= E(X_1^2) - E(X_1)^2 + E(X_2^2) - E(X_2)^2 = Var(X_1) + Var(X_2).$$

Exercise 8: *Let* $C_1, \ldots, C_n$ *be* n *independent fair coins with faces marked* 0 *and* 1. *Consider the random variable* $C = C_1 + \cdots + C_n$. *Find* $E(C^2)$.

We observe that:

$$E(C) = \frac{1}{2^n}\Big[\binom{n}{1} + \binom{n}{2}2 + \cdots + \binom{n}{n}n\Big]$$

Further we introduce a real variable x and observe that:

$$\binom{n}{1} + \binom{n}{2}2x + \cdots + \binom{n}{n}nx^{n-1} = D_x\Big[1 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n\Big] =$$
$$= D_x(1+x)^n = n(1+x)^{n-1}.$$

With $x = 1$ we get $E(C) = n/2$. This could have been derived also from $E(C) = \sum E(C_i) = n/2$, but it was a good point to recall the binomial distribution. Now, as the coins are independent,

$$Var(C) = \sum Var(C_i) = \frac{n}{4}.$$

But as $Var(C) = E(C^2) - E(C)^2$, we get the equation:

$$\frac{n}{4} = E(C^2) - \frac{n^2}{4},$$
$$E(C^2) = \frac{n^2 + n}{4}.$$

Exercise 9: *Let* $Z_1, \ldots, Z_n$ *be* n *independent fair dice with faces marked* $1, 2, \ldots, 6$. *Consider the random variable* $Z = Z_1 + \cdots + Z_n$. *Find* $E(Z^2)$.

$$E(Z) = \sum E(Z_i) = \frac{7n}{2},$$
$$Var(Z) = \sum Var(Z_i) = \frac{35n}{12},$$
$$\frac{35n}{12} = E(Z^2) - \frac{49n^2}{4},$$
$$E(Z^2) = \frac{35n}{12} + \frac{49n^2}{4} = \frac{35n}{12} + \frac{147n^2}{12} = \frac{147n^2 + 35n}{12}.$$
$$E(Z^2) = \frac{7}{12}n(21n + 5).$$

Exercise 10: *Four fair dice have following faces:*

$$A = \{4, 4, 4, 4, 0, 0\}$$

$$B = \{3, 3, 3, 3, 3, 3\}$$
$$C = \{6, 6, 2, 2, 2, 2\}$$
$$D = \{5, 5, 5, 1, 1, 1\}$$

(a) Compute the means and the variances.

(b) Show that:

$$Pr[\ A > B\ ] = Pr[\ B > C\ ] = Pr[\ C > D\ ] = Pr[\ D > A\ ] = \frac{2}{3}.$$

(a)

$E(A) = 16/6 = 8/3$, $Var(A) = E(A^2) - E(A)^2 = 1/6 \cdot 4 \cdot 16 - 64/9 = 96/9 - 64/9 = 32/9$,

$E(B) = 18/6 = 3$, $Var(B) = E(B^2) - E(B)^2 = 9 - 9 = 0$,

$E(C) = 20/6 = 5/3$, $Var(C) = E(C^2) - E(C)^2 = (2 \cdot 36 + 3 \cdot 4)/6 - 25/9 = 14 - 25/9 = 101/9$,

$E(D) = 18/6 = 3$, $Var(D) = E(D^2) - E(D)^2 = (3 \cdot 25 + 3)/6 - 9 = 13 - 9 = 4$.

(b)

$Pr[\ A > B\ ] = 2/3$:

We look at the possible values of A versus B. 24 of 36 pairs are $(4, 3)$ and are won by A.

$Pr[\ B > C\ ] = 2/3$:

We make again pairs of values. For exactly 24 pairs of values we get $(B, D) = (3, 2)$ and B wins.

$Pr[\ C > D\ ] = 2/3$:

C wins in the following situations: $(C, D) = (6, x)$ and $(C, D) = (2, 1)$. There are $12 + 12 = 24$ such pairs.

$Pr[\ D > A\ ] = 2/3$:

D wins in the following situations: $(D, A) = (5, x)$ and $(D, A) = (1, 0)$. There are $18 + 6 = 24$ such pairs.

Exercise 11: *You are in a TV show to winn* 10^6 *\$. The prize can be found in one room of three and all three doors are closed. You choose a door of three but you are not allowed to open it. The show-master opens the door to an empty room, show it to the public, and then asks you again. You still change you mind and open the other closed door or you can insist to open your first choice.*

Strategy A: Open the door you have chosen first.

Strategy B: Make a random choice between the two doors which are still closed.

Stragegy C: Open the other closed door, not the door you have chosen first.

Compute the winn probabilities P_A, P_B, P_C.

$P_A = 1/3$, $P_B = 1/2$, $P_C = 2/3$.