Discrete Structures EPFL, Fall 2014

Solution to Problem Set 13

Date: 12.12.2014 Not graded

Problem 1.

(a) Since the bet is doubled every time, the first loss is of 1 franc, the second loss in a row is of 2 francs, and, in general, the i-th loss in a row is of 2^{i-1} francs. As $255 = \sum_{i=0}^{7} 2^i$, you walk away broke if you lose exactly 8 times in a row. This happens with probability $p_{\text{lose}} = 2^{-8}$, since the coin flips are independent. Therefore, with probability p_{lose}, you lose 255 francs.

At the i-th turn, you bet 2^{i-1} francs and you have already lost $\sum_{j=0}^{i-2} 2^j = 2^{i-1} - 1$ francs. Hence, whenever you win, you win exactly 1 franc. Since the probability of winning is $1 - p_{\text{lose}}$, the expected value won is $p_{\text{lose}} \cdot (-255) + (1 - p_{\text{lose}}) \cdot 1 = 0$.

(b) If you have an infinite supply of money, it is not possible to become broke, so $p_{\text{lose}} = 0$.

The computation of the expected value is a bit subtle and it depends on what we exactly mean with "infinite supply of money".

Indeed, for any finite amount of money, we have that the expected value won is 0 by using the same argument of part (a). Hence, if we take the limit in which the amount of money at disposal tends to infinity, we have that the expected value won is 0.

On the other hand, if we have an infinite amount of money, we cannot lose. In addition, no matter at what point we win, we always win 1 franc. Hence, the expected value won is 1 franc.

Problem 2.

(a) The probability of picking the very easy question is clearly $\frac{1}{3}$.

(b) Suppose that the very easy question was picked initially. Then, it is in the student's box and this happens with probability $\frac{1}{3}$. Otherwise, if a very hard question was picked initially, then the easy question is in the remaining box, and this happens with probability $\frac{2}{3}$. Hence, you should exchange the original box, because the probability that the very easy question is in the unpicked box is equal to $\frac{2}{3}$. The reason why the probabilities change is that revealing a box with a very hard question gives the student some extra information about the other boxes.

Another way to see the same result is the following. Suppose without loss of generality that box 1 is chosen at the beginning. Then, the ETA opens box 2. Denote by A_i the event that the very easy question is in box i, with $i \in \{1, 2, 3\}$, and by B the event that the ETA opens box 2. The probability that the very easy question is in the unpicked box can be computed as follows,

$$\mathbb{P}(A_3|B) = \frac{\mathbb{P}(B|A_3)\mathbb{P}(A_3)}{\mathbb{P}(B|A_3)\mathbb{P}(A_3) + \mathbb{P}(B|A_1)\mathbb{P}(A_1) + \mathbb{P}(B|A_2)\mathbb{P}(A_2)}.$$

Clearly, $\mathbb{P}(A_1) = \mathbb{P}(A_2) = \mathbb{P}(A_3) = \frac{1}{3}$. Since box 1 is chosen at the beginning, if the very easy question is in box 3, the ETA must open box 2. Then, $\mathbb{P}(B|A_3) = 1$. If the very easy question is in box 1, the ETA can open either box 2 or box 3. Hence, $\mathbb{P}(B|A_2) = \frac{1}{2}$. If the very easy question were in box 2, then the ETA would not have opened that box! Therefore, $\mathbb{P}(B|A_2) = 0$. As a result, we obtain $\mathbb{P}(A_3|B) = \frac{2}{3}$.

This problem is a form of the well-known Monty Hall problem.

Problem 3.

(a) Note that $\mathbb{P}(X=0)=\mathbb{P}(X=1)=1/2$, because the coin whose outcome is encoded by X is fair. Then,

$$\begin{aligned}\mathbb{P}(Z=0) &\overset{(a)}{=} \mathbb{P}(X=0,Y=0)+\mathbb{P}(X=1,Y=1)\\ &\overset{(b)}{=} \mathbb{P}(X=0)\cdot\mathbb{P}(Y=0)+\mathbb{P}(X=1)\cdot\mathbb{P}(Y=1)\\ &\overset{(c)}{=} \frac{1}{2}\cdot\mathbb{P}(Y=0)+\frac{1}{2}\cdot\mathbb{P}(Y=1)\\ &= \frac{1}{2}\left(\mathbb{P}(Y=0)+\mathbb{P}(Y=1)\right)=\frac{1}{2},\end{aligned}$$

where (a) uses that Z is 0 if and only if $X=Y$ and that the events $\{X=0,Y=0\}$ and $\{X=1,Y=1\}$ are clearly disjoint, (b) uses the independence of X and Y, and (c) uses that $\mathbb{P}(X=0)=\mathbb{P}(X=1)=1/2$, $\mathbb{P}(Y=0)=p$, and $\mathbb{P}(Y=1)=1-p$.

Hence, $\mathbb{P}(Z=0)=\mathbb{P}(Z=1)=1/2$, and the proof of the first part is complete.

(b) Let $i\in\{0,1,\cdots,q-1\}$. Then,

$$\begin{aligned}\mathbb{P}(Z=i) &\overset{(a)}{=} \sum_{j=0}^{i}\mathbb{P}(X=i-j,Y=j)+\sum_{j=i+1}^{q-1}\mathbb{P}(X=q+i-j,Y=j)\\ &\overset{(b)}{=} \sum_{j=0}^{i}\mathbb{P}(X=i-j)\mathbb{P}(Y=j)+\sum_{j=i+1}^{q-1}\mathbb{P}(X=q+i-j)\mathbb{P}(Y=j)\\ &\overset{(c)}{=} \frac{1}{q}\cdot\sum_{j=0}^{q-1}\mathbb{P}(Y=j)\\ &= \frac{1}{q},\end{aligned}$$

where (a) uses that $Z=i$ if and only if $X+Y=i \pmod q$, (b) uses the independence of X and Y, (c) uses that X takes the values in $\{0,1,\ldots,q-1\}$ with equal probability of $\frac{1}{q}$.

This suffices to prove the claim.

(c) Since q is a prime number, for any $i\in\{1,\cdots,q-1\}$, there exists $m_i\in\{1,\cdots,q-1\}$ s.t. $i\cdot m_i\equiv 1 \pmod q$. In words, for any i, m_i is the multiplicative inverse of i modulo q. Then, for any $i\in\{1,\cdots,q-1\}$,

$$\begin{aligned}\mathbb{P}(Z=i) &\overset{(a)}{=} \sum_{j=0}^{q-1}\mathbb{P}(X=j,Y=m_j)\\ &\overset{(b)}{=} \sum_{j=0}^{q-1}\mathbb{P}(X=j)\mathbb{P}(Y=m_j)\\ &\overset{(c)}{=} \frac{1}{q}\cdot\sum_{j=0}^{q-1}\mathbb{P}(Y=m_j)\\ &= \frac{1}{q},\end{aligned}$$

where (a) uses that $Z=i$ if and only if $X\cdot Y=i \pmod q$ and the fact that, for any $j\in\{0,1,\cdots,q-1\}$, m_j is the unique integer in $\{0,1,\cdots,q-1\}$ s.t. $j\cdot m_j\equiv 1 \pmod q$,

(b) uses the independence of X and Y, (c) uses that X takes the values in $\{0, 1, \ldots, q-1\}$ with equal probability of $\frac{1}{q}$. In addition,

$$\mathbb{P}(Z = 0) = 1 - \sum_{i=1}^{q-1} \mathbb{P}(Z = i) = \frac{1}{q}.$$

As a result, Z still has uniform distribution in $\{0, 1, \cdots, q-1\}$.

Problem 4.

(a) Let x be the unique integer in $\{0, 1, \cdots, q-1\}$ s.t. $x \equiv c - b \pmod q$. Then,

$$\begin{aligned}\mathbb{P}(Y = b, Z = c) &= \mathbb{P}(Z = c \mid Y = b) \cdot \mathbb{P}(Y = b)\\ &\overset{(a)}{=} \mathbb{P}(X + Y = c \mid Y = b) \cdot \mathbb{P}(Y = b)\\ &\overset{(b)}{=} \mathbb{P}(X = x \mid Y = b) \cdot \mathbb{P}(Y = b)\\ &\overset{(c)}{=} \mathbb{P}(X = x) \cdot \mathbb{P}(Y = b)\\ &\overset{(d)}{=} \frac{1}{q} \cdot \mathbb{P}(Y = b)\\ &\overset{(e)}{=} \mathbb{P}(Z = c) \cdot \mathbb{P}(Y = b),\end{aligned}$$

where (a) uses the definition of Z, (b) uses the definition of x, (c) uses the independence of X and Y, (d) uses that X takes values in $\{0, 1, \cdots, q-1\}$ with equal probability, and (e) uses that Z takes values in $\{0, 1, \cdots, q-1\}$ with equal probability (which has been proved in Problem 3, part (b)).

As a result, for any $b, c \in \{0, 1, \ldots, q-1\}$ the events $\{Y = b\}$ and $\{Z = c\}$ are independent.

(b) The proof is identical to the one of part (a). Let y be the unique integer in $\{0, 1, \cdots, q-1\}$ s.t. $y \equiv c - a \pmod q$. Then,

$$\begin{aligned}\mathbb{P}(X = a, Z = c) &= \mathbb{P}(Z = c \mid X = a) \cdot \mathbb{P}(X = a)\\ &\overset{(a)}{=} \mathbb{P}(X + Y = c \mid X = a) \cdot \mathbb{P}(X = a)\\ &\overset{(b)}{=} \mathbb{P}(Y = y \mid X = a) \cdot \mathbb{P}(X = a)\\ &\overset{(c)}{=} \mathbb{P}(Y = y) \cdot \mathbb{P}(X = a)\\ &\overset{(d)}{=} \frac{1}{q} \cdot \mathbb{P}(X = a)\\ &\overset{(e)}{=} \mathbb{P}(Z = c) \cdot \mathbb{P}(X = a),\end{aligned}$$

where (a) uses the definition of Z, (b) uses the definition of y, (c) uses the independence of X and Y, (d) uses that Y takes values in $\{0, 1, \cdots, q-1\}$ with equal probability, and (e) uses that Z takes values in $\{0, 1, \cdots, q-1\}$ with equal probability.

(c) It is clearly not possible that the events $\{X = a\} \cap \{Y = b\}$ and $\{Z = c\}$ are independent. Indeed, given X and Y, the value of Z is uniquely determined. More formally, pick b s.t. $\mathbb{P}(Y = b) \neq 0$. Set $a = 0$ and $c \in \{0, 1, \cdots, q-1\}$ s.t. $c \equiv b - 1 \pmod q$. Then, since X and Z take values in $\{0, 1, \cdots, q-1\}$ with equal probability, we have that

$$\mathbb{P}(X = a) \cdot \mathbb{P}(Y = b) \cdot \mathbb{P}(Z = c) \neq 0,$$

while, since $Z = X + Y \pmod q$, we also have that

$$\mathbb{P}(X = a, Y = b, Z = c) = 0.$$

Therefore, $\mathbb{P}(X = a) \cdot \mathbb{P}(Y = b) \cdot \mathbb{P}(Z = c) \neq \mathbb{P}(X = a, Y = b, Z = c)$ and the events $\{X = a\} \cap \{Y = b\}$ and $\{Z = c\}$ are *not* independent.

Problem 5. Let us denote by A the event that urn 1 is chosen and by B the event that the token is blue. Then, we are required to compute the conditional probability $\mathbb{P}(A|B)$. By Bayes theorem we obtain that

$$\mathbb{P}(A|B) = \frac{\mathbb{P}(B|A)\mathbb{P}(A)}{\mathbb{P}(B|A)\mathbb{P}(A) + \mathbb{P}(B|\overline{A})\mathbb{P}(\overline{A})},$$

where $\overline{A}$ denotes the complementary event to A, i.e., the event that urn 2 is chosen. Now, all the probabilities in the previous formula can be easily computed: $\mathbb{P}(A) = \frac{1}{3}$, $\mathbb{P}(\overline{A}) = \frac{2}{3}$, $\mathbb{P}(B|A) = \frac{1}{5}$, and $\mathbb{P}(B|\overline{A}) = \frac{4}{5}$. Hence, we conclude that $\mathbb{P}(A|B) = \frac{1}{9}$.

Problem 6.

(a) Let F be the event of getting the flu and V be the event of being vaccinated. Given any event A, let $\bar{A}$ denote the complement event of A. Then, from the text of the problem we deduce that

$$\begin{aligned}
\mathbb{P}(V) &= 0.17, \\
\mathbb{P}(F \mid \bar{V}) &= 0.12, \\
\mathbb{P}(F \mid V) &= 0.02.
\end{aligned}$$

Consequently, the probability of getting the flu is given by

$$\begin{aligned}
\mathbb{P}(F) &= \mathbb{P}(F \mid \bar{V}) \cdot \mathbb{P}(\bar{V}) + \mathbb{P}(F \mid V) \cdot \mathbb{P}(V) \\
&= \mathbb{P}(F \mid \bar{V}) \cdot (1 - \mathbb{P}(V)) + \mathbb{P}(F \mid V) \cdot \mathbb{P}(V) \\
&= 0.12 \cdot 0.83 + 0.02 \cdot 0.17 = 0.103.
\end{aligned}$$

(b) In order to evaluate the probability that a person that has the flu was vaccinated, we use Bayes law:

$$\mathbb{P}(V \mid F) = \frac{\mathbb{P}(F \mid V) \cdot \mathbb{P}(V)}{\mathbb{P}(F)} = \frac{0.02 \cdot 0.17}{0.103} \approx 0.033.$$