Solution to HW 3, Problem 1

Al-Naji, Nader

Consider a program that runs a loop n times, updating variable X in a randomized fashion. In the ith iteration of the loop, with probability $1/i$, X is set to i. Compute $P[X = i]$ at the end of n iterations.

Let S_i be the event that X is set to i at the ith iteration of the loop. So the probability that $X = i$ at the end of n iterations is the probability that at iteration i, X is set to i, and at every iteration k such that $i < k \leq n$, X is not set to k. Written formally, this quantity is:

$P[S_i \cap \bar{S}_{i+1} \cap ... \cap \bar{S}_{n-1} \cap \bar{S}_n]) = P[S_i] \times P[\bar{S}_{i+1}] \times ... \times P[\bar{S}_{n-1}] \times P[\bar{S}_n]$
Note that whether or not X is set to i at any given iteration is mutually independent of all other iterations and so it is safe to say that this intersection is equal to this product.

If we write out these lines, we begin to notice a pattern:

$P[S_i] \times P[\bar{S}_{i+1}] \times ... \times P[\bar{S}_{n-1}] \times P[\bar{S}_n] = \frac{1}{i} \times (1 - \frac{1}{i+1}) \times ... \times (1 - \frac{1}{n-1}) \times (1 - \frac{1}{n})$
$= \frac{1}{\cancel{i}} \times \frac{\cancel{i}}{\cancel{i+1}} \times \frac{\cancel{i+1}}{\cancel{i+2}} \times ... \times \frac{\cancel{n-3}}{\cancel{n-2}} \times \frac{\cancel{n-2}}{\cancel{n-1}} \times \frac{\cancel{n-1}}{n} = \frac{1}{n}.$

All the terms in between cancel leaving n in the denominator and thus, $P[X = i] = \frac{1}{n}$ $\forall\ i \in [1, n]$ and $P[X = i] = 0$ otherwise.

Solution to HW 3, Problem 2

Al-Naji, Nader

The goal of this problem is to show that given n independent random bits (fair coin flips) $x_1, x_2, ..., x_n$ one can generate a much larger number (m) of bits which are pairwise independent.

1. Consider the following construction: Given $S \subseteq x_1, ..., x_n$, let y_S be the random variable whose value is the sum (mod 2) of all the elements in S. Show that for any two (distinct) sets S and T, y_S and y_T are independent random variables. Conclude that from a set of n random independent bits, one can generate 2^n pairwise independent random bits.

First, let us show that for any set $S \subseteq x_1, ..., x_n$ of random bits, $P(y_S = 1) = P(y_S = 0) = 1/2$. We will do this using induction:

Let $P(x)$ = "for a set $S \subseteq x_1, ..., x_n$ of x independent random bits (fair coin flips), $P(y_S = 1) = P(y_S = 0) = 1/2$".
Base: $x = 1$
Clearly if the set S contains a single random bit, then the probabilities will be $1/2$ by construction.
Step: assuming $P(x)$ for $x = n$ is true, show it is true for $n + 1$.
So we have $P(y_{S,n} = 1) = P(y_{S,n} = 0) = 1/2$. Now we want to show that adding a random bit preserves this.
$P(y_{S,n+1} = z) = P(y_{S,n} \oplus x_{n+1} = z) = P(x_{n+1} = z \oplus y_{S,n}) = 1/2$.
Because x_{n+1} is a random bit with probability $1/2$ of taking on a value of 0 or 1. Note that this is true regardless of whether z is zero or one.
Thus, $P(y_S = 0) = P(y_S = 1) = 1/2$ for all $S \subseteq x_1, ..., x_n$.

Now we want to show that for two distinct sets S and T of bits, that $P(y_S, y_T) = P(y_T)P(y_S)$ for all choices of S and T. To do this we will consider three possibilities for S and T and show that $P(y_T|y_S) = P(y_T)$ and vice versa for all three cases. First, that S and T are disjoint, second that $S \subset T$, and third that S and T are distinct non-disjoint sets such that neither is a subset of the other.

a) If S and T are disjoint, then $P(y_S, y_T) = P(y_T)P(y_S)$, the definition of independence.

This is trivially true since if S and T are disjoint, then the value of y_S says nothing about y_T and vice versa because they have no bits in common. Thus, if S and T are disjoint, then $P(y_T|y_S) = P(y_T)$ and vice versa. So we have:

$P(y_T, y_S) = P(y_S)P(y_T|y_S) = P(y_S)P(y_T)$, the definition of independence using the chain rule.

b) If $S \subset T$, then $P(y_S, y_T) = P(y_S)P(y_T)$.

First, note that because $T - S$ is a mutually independent set of bits, we can apply the results of the theorem proved at the beginning and get:
$P(y_T = z|y_S = x) = P(x \oplus y_{T-S} = z) = P(y_{T-S} = x \oplus z) = 1/2 = P(y_T = z)$.
Note that this applies to all valid values of x and z in general and so we have $P(y_T|y_S) = P(y_T)$. To show that this is sufficient for independence, we again combine the chain rule with this result:
$P(y_T, y_S) = P(y_S)P(y_T|y_S) = P(y_S)P(y_T)$, the definition of independence.

c) If $S \not\subseteq T$ and $T \not\subseteq S$ and S and T are not disjoint and not equal, then $P(y_S, y_T) = P(y_T)P(y_S)$.

Under these conditions, there must at least one element that is in S and not in T and vice versa and at least one element that is in $S \cap T$ so the intersection is non-empty. Basically this says that $S \cap T$ is a strict subset of S and T. So we have:
$P(y_T|y_S) = P(y_T|y_{S-T} \oplus y_{T \cap S}) = P(y_T|y_{S \cap T})$ using (a) since $T - S$ and T are disjoint.
But, as stated, $T \cap S$ is a strict subset of T. So, by (b) we have: $P(y_T|y_{S \cap T}) = P(y_T) \rightarrow P(y_T|y_S) = P(y_T) \rightarrow P(y_S, y_T) = P(y_T)P(y_S)$ from above and so y_T and y_S are independent.

Because these three cases cover all possibilities for S and T to overlap, showing that all three of them result in independence of S and T is sufficient and we have $P(y_S, y_T) = P(y_T)P(y_S)$ in general and so y_S and y_T are independent.

For the last part, there are 2^n distinct subsets of a set of n elements. Thus, because we have shown that any two distinct subsets of n random bits are pairwise independent, and there are 2^n such subsets, given n random bits, we can generate 2^n pairwise random bits using these distinct subsets.

2. Are the bits y_S constructed above 3-wise independent? Prove your answer.

No. Consider $S = \{x_1\}, T = \{x_2\}$, and $U = \{x_1, x_2\}$. Then given y_S and y_T, we can deduce that $y_S = x_1$ and $y_T = x_2$ and know that $y_U = x_1 \oplus x_2 = y_S \oplus y_T$ with probability 1. So, we have as a counterexample:
$P(y_U = z|y_S = z, y_T = 0) = P(z = z \oplus 0) = P(z = z) = 1 \neq 1/2 = P(y_U = z)$.

Thus, we have $P(y_U = z, y_S = z, y_T = 0) = P(y_S = z)P(y_T = 0|y_S = z)P(y_U = z|y_S = z, y_T = 0) = 1/2 \times 1/2 \times 1 = 1/4 \neq P(y_S = z)P(y_T = 0)P(y_U = z) = 1/8$ by the chain rule, a violation of the definition of three-wise independence.

Solution to HW 3, Problem 3

Al-Naji, Nader

Let $X_1, ..., X_k$ be iid random variables where each X_i is uniform in 1, ..., n. Let $Y = maxX_1, ..., X_k$.

1. Compute $P[Y > i]$ for $0 \leq i \leq n$.

This quantity is equal to $1 - P[X_j \leq i]$ for every value of j between one and k inclusive. Thus, because all the X_i are independent and identically distributed, we have:

$$P[Y > i] = 1 - P[X_1 \leq i] \times ... \times P[X_k \leq i] = 1 - P[X_1 \leq i]^k = 1 - (\tfrac{i}{n})^k = \tfrac{n^k - i^k}{n^k}.$$

2. Compute $E[Y]$.

$$E[Y] = \sum_{i=0}^{n} P[Y > i] = \sum_{i=0}^{n} 1 - (\tfrac{i}{n})^k = \sum_{i=0}^{n} 1 - \sum_{i=0}^{n} (\tfrac{i}{n})^k = n + 1 - \sum_{i=0}^{n} (\tfrac{i}{n})^k$$

3. Find $\lim_{n\to\infty} \frac{E[Y]}{n}$

$$\lim_{n\to\infty} \tfrac{E[Y]}{n} = 1 + \tfrac{1}{n} - \tfrac{1}{n^{k+1}} \sum_{i=0}^{n} i^k$$

Using a basic result from calculus, we know that, because i^k is an increasing function of i for positive i, it can be bound between two integrals as such:

$$\int_{a-1}^{b} i^k \, di \leq \sum_{i=a}^{b} i^k \leq \int_{a}^{b+1} i^k \, di.$$

However, because we are taking the limit as n goes to infinity, we care only about the high order terms and so we have:

$$\lim_{n\to\infty} \sum_{i=0}^{n} i^k \to \lim_{n\to\infty} \int_{0}^{n} i^k \, di = \tfrac{n^{k+1}}{k+1}.$$

Finally, subbing this result into our original equation, we can evaluate the limit and get the answer:

$$\lim_{n\to\infty} \tfrac{E[Y]}{n} = 1 + \tfrac{1}{n} - \tfrac{1}{n^{k+1}} \sum_{i=0}^{n} i^k = \lim_{n\to\infty} 1 + \tfrac{1}{n} - \tfrac{1}{n^{k+1}} \times \tfrac{n^{k+1}}{k+1} = \lim_{n\to\infty} 1 + \tfrac{1}{n} - \tfrac{1}{k+1} = \tfrac{k}{k+1}.$$

Solution to HW 3, Problem 4

Al-Naji, Nader

A fair coin is tossed $2n$ times.

1. Calculate P_t, the probability that it turns up heads exactly t times.

This is similar to problem four in homework 2. Here $p = 1/2$ so the probability of a specific sequence of t heads and $2n - t$ tails is $(1/2)^{2n}$. Since there are $\binom{2n}{t}$ ways to get t heads in $2n$ flips, the total probability is simply:

$P_t = \binom{2n}{t}(\frac{1}{2})^{2n}$.

2. Find a number α such that $P_n = \Theta(n^\alpha)$.

We will use Stirling's approximation and simplify the following:

$P_n = \binom{2n}{n}(\frac{1}{2})^{2n} = \frac{(2n)!}{n!n!2^{2n}} = \Theta(\frac{\sqrt{2n}(2n)^{2n}e^n e^n}{e^{2n}\sqrt{n}\sqrt{n}n^n n^n 2^{2n}}) = \Theta(\frac{\sqrt{2n}2^{2n}n^{2n}e^{2n}}{n2^{2n}n^{2n}e^{2n}}) = \Theta(\frac{2^{1/2}}{n^{1/2}}) = \Theta(n^{-1/2})$.

So $\alpha = -1/2$.

3. Prove that for any integer $t \in [n - \sqrt{n}, n + \sqrt{n}]$, $P_t = \Theta(P_n)$

First, we will show that $\lim_{n\to\infty} \frac{P_t}{P_n} \leq 1$. This will establish that P_t is at least $O(P_n)$. Then, to achieve the tight bound, we will establish a lower bound of $P_t = \Omega(P_n)$ for all $t \in [n - \sqrt{n}, n + \sqrt{n}]$ and conclude that, because $P_t = O(P_n)$ and $P_t = \Omega(P_n)$, that $P_t = \Theta(P_n)$ for all $t \in [n - \sqrt{n}, n + \sqrt{n}]$.

$\lim_{n\to\infty} \frac{P_t}{P_n} = \lim_{n\to\infty} \frac{\binom{2n}{t}2^{2n}}{\binom{2n}{n}2^{2n}} = \lim_{n\to\infty} \frac{\binom{2n}{t}}{\binom{2n}{n}}$.

To see that the value of this limit never exceeds one, simply consider that the choose function is at a maximum at $\binom{2n}{n}$. Because this maximum occurs at $\binom{2n}{n}$, it follows that $\binom{2n}{t}$ can be at most $\binom{2n}{n}$ (when $t = n$) and so the ratio $\frac{\binom{2n}{t}}{\binom{2n}{n}}$ cannot exceed one. This is enough to provide us with an upper bound on P_t. Namely, $P_t = O(P_n)$.

Now we want to show that $P_t = \Omega(P_n)$ for $t = n + c\sqrt{n}$ with $-1 \leq c \leq 1$.

$P_n = \binom{2n}{n}(\frac{1}{2})^{2n} = \frac{(2n)!}{t!(2n-t)!2^{2n}} = \Theta(\frac{e^{2n}(2n)^{2n}\sqrt{2n}}{e^{2n}\sqrt{n-c\sqrt{n}}\sqrt{n+c\sqrt{n}}(n-c\sqrt{n})^{n-c\sqrt{n}}(n+c\sqrt{n})^{n+c\sqrt{n}}})$
$= \Theta(\frac{n^{2n}\sqrt{n}}{n\sqrt{1-c/\sqrt{n}}\sqrt{1+c/\sqrt{n}}(n-c\sqrt{n})^{-c\sqrt{n}}(n+c\sqrt{n})^{c\sqrt{n}}((n-c\sqrt{n})(n+c\sqrt{n}))^{n}})$
$= \Theta(\frac{n^{2n}}{\sqrt{n}\sqrt{1-c^2/n}(n-c\sqrt{n})^{-c\sqrt{n}}(n+c\sqrt{n})^{c\sqrt{n}}(n^2-c^2n)^{n}})$
$= \Theta(\frac{1}{\sqrt{n}\sqrt{1-c^2/n}(n-c\sqrt{n})^{-c\sqrt{n}}(n+c\sqrt{n})^{c\sqrt{n}}(1-c^2/n)^{n}})$
$= \Theta(\frac{1}{\sqrt{n}\sqrt{1-c^2/n}(1-c/\sqrt{n})^{-c\sqrt{n}}(1+c/\sqrt{n})^{c\sqrt{n}}(1-c^2/n)^{n}}).$

Now, note that $1 + x \leq e^x \rightarrow \frac{1}{1+x} \geq e^x$. Because this term will appear in the denominator, we now switch to Ω to indicate that this is a lower bound. Note that $e^{c^2/2n}$ goes to one as n grows.

$= \Omega(\frac{1}{\sqrt{n}e^{c^2/2n}e^{c^2}e^{c^2}e^{-c^2}}) = \Omega(\frac{1}{\sqrt{n}}) = \Omega(P_n).$

Thus, we have established that $P_t = O(P_n) = \Omega(P_n) \rightarrow P_t = \Theta(P_n)$ for all $t \in [n - \sqrt{n}, n + \sqrt{n}]$.