## Recitation 5

## Randomization

### 5.1 Announcements

- RandomLab has been released, and is due Friday afternoon. It's worth 100 points.
- FingerLab will be released this Friday. However, it will be due in two weeks to allow time to study for Exam I, which is going to be on Friday, Feb 24.


### 5.2 Rock, Paper, Scissors, Shoot!

You and a friend are playing Rock, Paper, Scissors. Despite humans actually being remarkably bad at generating randomness, assume that on each round, both you and your friend will uniformly randomly produce one of Rock, Paper, or Scissors (each has probability $1 / 3$ ).

## Task 5.1. Determine the probability of winning this game.

We make the observation that on any particular round, the probabilities of winning, losing, and tieing are each $1 / 3$. If we tie, we play another round. Since the game only terminates once we either win or lose, and these have equal probability on each round, the probability of us winning overall must be $1 / 2$.

Although this argument is fairly good on its own, here's the formal version. Let $W_{i}$ be the event that we win on round $i$, counting from $i=1$. The event that we win, $W$, is given by

$$
W=\bigcup_{i=1}^{\infty} W_{i}
$$

Notice that these $W_{i}$ 's are disjoint from one another, and therefore

$$
\operatorname{Pr}[W]=\sum_{i=1}^{\infty} \operatorname{Pr}\left[W_{i}\right] .
$$

On any particular round, the probabilities of winning, losing, and tieing are each $1 / 3$. Therefore

$$
\begin{aligned}
\operatorname{Pr}\left[W_{i}\right] & =\mathbf{P r}[\text { tie for } i-1 \text { rounds }] \cdot \mathbf{P r}\left[\text { win on } i^{\text {th }} \text { round }\right] \\
& =(1 / 3)^{i-1} \cdot(1 / 3) \\
& =(1 / 3)^{i}
\end{aligned}
$$

We can now solve for the probability of winning overall:

$$
\operatorname{Pr}[W]=\sum_{i=1}^{\infty} \operatorname{Pr}\left[W_{i}\right]=\sum_{i=1}^{\infty}(1 / 3)^{i}=\frac{1}{2}
$$

Task 5.2. How many rounds do we expect to play before someone wins?

The number of rounds we play is a geometric random variable with probability of success $2 / 3$, where a "successful" round is one where we did not tie. The expected number of rounds, then, is

$$
\frac{1}{(2 / 3)}=\frac{3}{2}
$$

### 5.3 Flipping Coins

Task 5.3. Describe an algorithm which flips a fair coin an expected constant number of times in order to simulate a coin with bias $p$, where $0<p<1$ (that is, we're simulating a coin which flips heads with probability $p$ ). It may be helpful to consider writing $p$ as a binary number $0 . p_{1} p_{2} p_{3} \ldots$, where each $p_{i} \in\{0,1\}$.

Consider the following algorithm: we repeatedly flip our fair coin, interpreting heads as 1 and tails as 0 . On the $i^{\text {th }}$ flip, if this flip does not match $p_{i}$, then we output $p_{i}$. Otherwise, we try again with an $(i+1)^{\text {th }}$ flip.

This algorithm effectively generates a number $x$ between 0 and 1 , returning whether or not $x<p$. We generate this number one bit at a time. Let $x_{i}$ be the bits of the number we're generating. At each round $i$, we have the invariant that $x_{j}=p_{j}$ for every $j<i$, and therefore, as far as we know, $x=p$. If $x_{i} \neq p_{i}$, then certainly $x \neq p$. In this case, if $p_{j}=1$ then $x_{i}=0$ and we know $x<p$, returning heads. Otherwise, we know $p_{j}=0$ and $x_{i}=1$ and therefore $x>p$, returning tails.

Note that both $x$ and $p$ could have an infinite binary representation, but this algorithm avoids an infinite runtime by only generating as far as necessary in order to determine whether or not $x<p$.

How many flips does this algorithm require in expectation? At each step $i, \operatorname{Pr}\left[x_{i}=p_{i}\right]=$ $1 / 2$, since $x_{i}$ is chosenly fairly from $\{0,1\}$. We keep retrying until $x_{i} \neq p_{i}$, and therefore the number of flips required is a geometric random variable with probability of success $1 / 2$. Therefore, in expectation, this algorithm will terminate after $\frac{1}{1 / 2}=2$ fair flips!

### 5.4 High Probability

Task 5.4. Umut has a secret algorithm which has $O(\log n)$ span with high probability, and $O(n)$ span in the worst case. Specifically, Umut's algorithm has $O(\log n)$ span with probability at least $1-\frac{1}{n^{3}}$. Prove that Umut's algorithm has $O(\log n)$ span in expectation.

Let "good" be the event that $S(n) \in O(\log n)$, and "bad" be the otherwise event. Using the law of total expectation, we have

$$
\begin{aligned}
\mathbf{E}[S(n)] & =\mathbf{E}[S(n) \mid \text { good }] \operatorname{Pr}[\text { good }]+\mathbf{E}[S(n) \mid \text { bad }] \operatorname{Pr}[\mathrm{bad}] \\
& =\mathbf{E}[S(n) \mid \text { good }](1-\operatorname{Pr}[\mathrm{bad}])+\mathbf{E}[S(n) \mid \text { bad }] \operatorname{Pr}[\mathrm{bad}]
\end{aligned}
$$

Note that we know the following:

- $\mathbf{E}[S(n) \mid$ good $]$ is upper bounded by $O(\log n)$,
- $\mathbf{E}[S(n) \mid$ bad $]$ is upper bounded by $O(n)$, and
- $\operatorname{Pr}[\mathrm{bad}]$ is upper bounded by $\frac{1}{n^{3}}$.

Therefore,

$$
\begin{aligned}
\mathbf{E}[S(n)] & \leq O(\log n) \cdot(1-\operatorname{Pr}[\mathrm{bad}])+O(n) \cdot \mathbf{P r}[\mathrm{bad}] \\
& =O(\log n)+(O(n)-O(\log n)) \cdot \mathbf{P r}[\mathrm{bad}] \\
& \leq O(\log n)+O(n) \cdot \frac{1}{n^{3}} \\
& =O(\log n)+O\left(\frac{1}{n^{2}}\right) \\
& =O(\log n)
\end{aligned}
$$

### 5.5 The Birthday Problem

Task 5.5. Suppose there are $D$ days in the year, and assume that all babies are born uniformly randomly on any one of these days. If there are n people in a room, what is the expected number of them to share a birthday with at least one other person in the same room?

Let $S$ be the number of people to share a birthday with at least one other person, and $B_{i}$ be the birthday of the $i^{\text {th }}$ person. Define

$$
S_{i}= \begin{cases}1, & \text { if } \exists j \cdot j \neq i \wedge B_{i}=B_{j} \\ 0, & \text { otherwise }\end{cases}
$$

Therefore $S=\sum_{i} S_{i}$. By linearity of expectation,

$$
\mathbf{E}[S]=\sum_{i} \mathbf{E}\left[S_{i}\right]=\sum_{i} \operatorname{Pr}\left[\exists j \cdot j \neq i \wedge B_{i}=B_{j}\right] .
$$

We have

$$
\begin{aligned}
& \operatorname{Pr}\left[\exists j \cdot j \neq i \wedge B_{i}=B_{j}\right] \\
& =1-\operatorname{Pr}\left[\forall j \cdot j=i \vee B_{i} \neq B_{j}\right] \\
& =1-\left(\frac{D-1}{D}\right)^{n-1}
\end{aligned}
$$

and therefore

$$
\mathbf{E}[S]=n\left(1-\left(\frac{D-1}{D}\right)^{n-1}\right)
$$

### 5.6 Other Exercises

Exercise 5.6. Prove that the expected value of a geometric random variable $X$ with probability of success $p$ is $1 / p$ in two separate ways:

1. by directly solving using the definition of expected value, and
2. by writing a recurrence and solving it.

In the second approach, use the law of total expectation, i.e.

$$
\mathbf{E}[X]=\sum_{i} \mathbf{E}\left[X \mid Y_{i}\right] \operatorname{Pr}\left[Y_{i}\right]
$$

where the $Y_{i}$ 's form a partition of the sample space.

Exercise 5.7. Suppose you are given a coin with unknown but fixed bias p, where $0<$ $p<1$ (in your analysis, treat $p$ as a constant). Describe an algorithm which flips this mysterious coin an expected constant number of times in order to simulate a fair coin.

