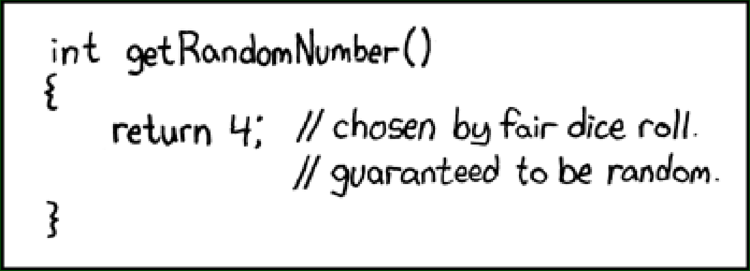
CSE 312

Foundations of Computing II

Probability Axioms & Equally-Likely Outcomes



Consider the following piece of code:

```
while FlipCoin(1/2) ≠ HEADS:
    print "Hello!"
```

Does it terminate?

Despite the answer seeming like an **obvious** “almost certainly”, we don’t really have the tools to give a real answer...

That’s what pretty much the rest of the course is about!

To drive the point home, we will use probability as a way of **analyzing code with randomized components**.

Probability Primitives

For now, assume we have two random generators:

- **FlipCoin**(p) returns `HEADS` with probability p and `TAILS` otherwise.
- **RollDie**(N) returns $x \in [N]$ with probability $1/N$.

(We will do better later, but for now…)

Definitions

Suppose we have a piece of random code $\mathcal{R}$. We want to be able to reason about $\mathcal{R}$ formally; so, we use the following definitions:

Definition (Outcome)

An **outcome** for $\mathcal{R}$ is a sequence of values for all random calls in $\mathcal{R}$. For example, if our code is

```
c = FlipCoin(1/2)
d = RollDie(2)

if c == HEADS: c = 1
else: c = 2

if c == d: print c
else: print "Failure!"
```

The possible outcomes are:

$$(\mathtt{HEADS}, 1), (\mathtt{HEADS}, 2), (\mathtt{TAILS}, 1), (\mathtt{TAILS}, 2)$$

Suppose we have a piece of random code $\mathcal{R}$. We want to be able to reason about $\mathcal{R}$ formally; so, we use the following definitions:

Definition (Outcome)

An **outcome** for $\mathcal{R}$ is a sequence of values for all random calls in $\mathcal{R}$.

Definition (Sample Space)

The **Sample Space** of $\mathcal{R}$ is the set of all possible outcomes of running $\mathcal{R}$.

Even More Definitions

Definition (Event)

An **event** is a subset of the sample space. We call these events, because they represent things that can happen. Consider the code from before:

```
c = FlipCoin(1/2)
d = RollDie(2)

if c == HEADS: c = 1
else: c = 2

if c == d: print c
else: print "Failure!"
```

Here's some events:

- The code prints "Failure!"
  $\{(\mathtt{HEADS}, 2), (\mathtt{TAILS}, 1)\}$
- The code halts.
  $\{(\mathtt{HEADS}, 1), (\mathtt{HEADS}, 2), (\mathtt{TAILS}, 1), (\mathtt{TAILS}, 2)\}$
- The coin flip gives HEADS.
  $\{(\mathtt{HEADS}, 1), (\mathtt{HEADS}, 2)\}$

Definition (Probability)

Let Ω be a sample space and $E \subseteq \Omega$ be an event. Then, we say $\Pr(E)$ is the probability of E.
All probability functions must satisfy the following three axioms:

- $0 \leq \Pr(E)$
- $\Pr(\Omega) = 1$
- If $E_1, E_2, \ldots, E_n \subseteq \Omega$ and are pairwise disjoint events, then

$$\Pr(E_1 \cup E_2 \cup \cdots \cup E_n) = \sum_{i=1}^{n} \Pr(E_i)$$

Claim

$\Pr(\overline{E}) = 1 - \Pr(E)$

Proof.

Note that $\Pr(\Omega) = 1$ by the second axiom. Furthermore, $E \cup \overline{E} = \Omega$ for all events E; so, $1 = \Pr(\Omega) = \Pr(E \cup \overline{E}) = \Pr(E) + \Pr(\overline{E})$ by the above and axiom 3. Then, $\Pr(\overline{E}) = 1 - \Pr(E)$. $\square$

Definitions Recap

Code

```
coin1 = FlipCoin(1/2)
coin2 = FlipCoin(1/2)
```

Sample Space (All potential outcomes of the random calls)

$$\Omega = \{(\texttt{HEADS},\texttt{HEADS}),(\texttt{HEADS},\texttt{TAILS}),(\texttt{TAILS},\texttt{HEADS}),(\texttt{TAILS},\texttt{TAILS})\}$$

Example Events ($E \subseteq \Omega$)

- $\varnothing$
- $\{(\texttt{HEADS},\texttt{HEADS})\}$
- $\texttt{coin1} = \texttt{HEADS}$

Equally-Likely Outcomes


```
flip = FlipCoin(1/2)
```

$\Omega = \{\mathtt{HEADS}, \mathtt{TAILS}\}$

```
flip1 = FlipCoin(1/2)
flip2 = FlipCoin(1/2)
```

$\Omega = \{(\mathtt{HEADS}, \mathtt{HEADS}), (\mathtt{HEADS}, \mathtt{TAILS}), (\mathtt{TAILS}, \mathtt{HEADS}), (\mathtt{TAILS}, \mathtt{TAILS})\}$

```
roll = RollDie(6)
```

$\Omega = \{1, 2, 3, 4, 5, 6\}$

```
flip = FlipCoin(1/3)
```

$$\Omega = \{\mathtt{HEADS}, \mathtt{TAILS}\}$$

$$\Pr(\mathtt{HEADS}) = \left(\frac{1}{3}\right) \qquad \Pr(\mathtt{TAILS}) = \left(\frac{2}{3}\right)$$

```
flip = FlipCoin(1/2)
if flip == HEADS:
   flip2 = RollDie(2)
else:
   flip2 = RollDie(3)
```

$$\Omega = \{(\mathtt{HEADS},1),(\mathtt{HEADS},2),(\mathtt{TAILS},1),(\mathtt{TAILS},2),(\mathtt{TAILS},3)\}$$

$$\Pr((\mathtt{HEADS},1)) = \left(\frac{1}{2}\right)^2 \qquad \Pr((\mathtt{TAILS},1)) = \left(\frac{1}{2}\right)\left(\frac{1}{3}\right)$$

We'll stick with equally-likely outcomes for now.

If we have a sample space, Ω, and all the outcomes are equally-likely, then the $\Pr(\{x\}) = \frac{1}{|\Omega|}$. So, $\Pr(\{x_1, x_2, \ldots, x_n\}) = \frac{n}{|\Omega|}$. So, $\Pr(E) = \frac{|E|}{|\Omega|}$.

A's Gambling Problem(s)

One of the TAs has a gambling problem. They make all of the following bets with Adam:

- I bet a fair coin will come up `HEADS`.
- I bet a six-sided die will be even.
- I bet if each of us rolls a six-sided die, the sum will be 7.

Let's model each of these with code, determine the events and sample space, and evaluate the probabilities of each.

```
coin = FlipCoin(1/2)
```

$$\Omega = \{\mathtt{HEADS}, \mathtt{TAILS}\}$$
$$E = \{\mathtt{HEADS}\}$$
$$\Pr(E) = \frac{|E|}{|\Omega|} = \frac{1}{2}$$

I bet a six-sided die will be even


```
roll = RollDie(6)
```

$$\Omega = \{1, 2, 3, 4, 5, 6\}$$
$$E = \{2, 4, 6\}$$
$$\mathsf{Pr}(E) = \frac{|E|}{|\Omega|} = \frac{3}{6} = \frac{1}{2}$$

```
adamRoll = RollDie(6)
taRoll = RollDie(6)
```

What is $\Pr(\texttt{adamRoll} + \texttt{taRoll} = 7)$?

$$
\begin{array}{lccccccl}
\Omega = \{ & (1,1), & (1,2), & (1,3), & (1,4), & (1,5), & (1,6), & \\
 & (2,1), & (2,2) & (2,3), & (2,4), & (2,5), & (2,6), & \\
 & (3,1), & (3,2) & (3,3), & (3,4), & (3,5), & (3,6), & \\
 & (4,1), & (4,2), & (4,3), & (4,4), & (4,5), & (4,6), & \\
 & (5,1), & (5,2), & (5,3) & (5,4), & (5,5), & (5,6), & \\
 & (6,1), & (6,2), & (6,3) & (6,4), & (6,5), & (6,6) & \}
\end{array}
$$

$$
\begin{array}{lccccccl}
E = \{ & (6,1), & (5,2), & (4,3), & (3,4), & (2,5) & (1,6) & \}
\end{array}
$$

So, $\Pr(\texttt{adamRoll} + \texttt{taRoll} = 7) = \dfrac{|E|}{|S|} = \dfrac{6}{36} = \dfrac{1}{6}$

Birthdays

What is the probability that none of n people share the same birthday?

```
person1 = RollDie(1/365)
person2 = RollDie(1/365)
...
person365 = RollDie(1/365)
```

What assumptions have we implicitly made with this code?

- Birthdays are equally likely (not actually true. . . but close enough)

What is the sample space?

$|\Omega| = |\{(x_1, x_2, \ldots, x_n) : 0 < x_i \leq 365\}| = 365^n$

Let E be the event that all people have different birthdays.

What is E?

$|E| = 365 \times 364 \times \cdots \times (365 - n + 1)$

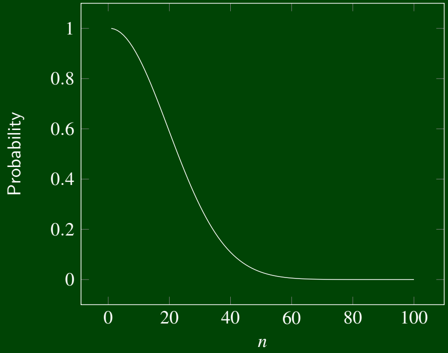
What is the probability that none of n people share the same birthday?

Let E be the event that all people have different birthdays.

$|\Omega| = 365^n$

$|E| = 365 \times 364 \times \cdots \times (365 - n + 1)$

So, $\Pr(\text{no shared birthdays}) = \dfrac{|E|}{|\Omega|} = \dfrac{365 \times 364 \cdots \times (365 - n + 1)}{365^n}$.



Notice that as low as $n = 23$, the probability is already less than 0.5.

The Situation

- n chips manufactured
- k chips randomly selected for testing
- **one** chip defective

What is Pr(defective chip in k selected chips)?

- $|\Omega| = \binom{n}{k}$
- $|E| = \binom{1}{1}\binom{n-1}{k-1}$ (choose defective chip; pick remaining chips to test)
- Pr(defective chip in k selected chips) $= \dfrac{|E|}{|\Omega|} = \dfrac{\binom{1}{1}\binom{n-1}{k-1}}{\binom{n}{k}}$

What is Pr(the ith selected chip is defective)?

It is equally likely that each of the n chips is the defective one.

So, Pr(the ith selected chip is defective) $= \Pr(E_i) = \dfrac{1}{n}$

Pr(defective chip in k selected chips) $= \Pr(E_1) + \Pr(E_2) + \cdots + \Pr(E_k) = \dfrac{k}{n}$.

Chips

The Situation

- n chips manufactured
- k chips randomly selected for testing
- d chips defective

What is Pr(at least one defective chip in k selected chips)?

Consider Pr(no chip defective in k selected chips) instead.

- $|\Omega| = \binom{n}{k}$
- $|E| = \binom{n-d}{k}$ (choose from non-defective chips)
- Pr(at least one defective in k) $= 1 - \frac{|E|}{|\Omega|} = 1 - \frac{\binom{n-d}{k}}{\binom{n}{k}}$