## Lecture 16

Spring 2023

## CS

## Mathematical Foundations of Computing

CS 13: Mathematical Foundations of Computing

## Probability

Consider the following piece of code:

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

Consider the following piece of code:

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

Does it terminate?

## Some Code

Consider the following piece of code:

```
1 while FlipCoin() # HEADS:
2 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. . .

## Some Code

Consider the following piece of code:

```
1 while FlipCoin() # HEADS:
2 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 today is about!

## Some Code

Consider the following piece of code:

```
1 while FlipCoin() # HEADS:
2 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 today is about!
To drive the point home, we are going to only use probability as a way of analyzing code with randomized components.

We will always assume we have the following random primitives:

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


## Definitions

Suppose we have a piece of random code $\mathcal{R}$. We want to be able to reason about $\mathcal{R}$ formally

## 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)

## 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 $\mathcal{R}$.

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!"
```

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:

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:
(HEADS, 1), (HEADS, 2), (TAILS, 1), (TAILS, 2)

## More 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 $\mathcal{R}$.
Definition (Sample Space)

## More 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 $\mathcal{R}$.
Definition (Sample Space)
The Sample Space of $\mathcal{R}$ is the set of all possible outcomes of running $\mathcal{R}$.

## Definition (Event)

An event is a subset of the sample space.

Definition (Event)
An event is a subset of the sample space. We call these events, because the represent things that can happen.

## Definition (Event)

An event is a subset of the sample space. We call these events, because the 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!"


## Definition (Event)

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

$$
\begin{aligned}
& c=\text { FlipCoin(1/2) } \\
& d=\text { RollDie(2) } \\
& \text { if } c==\text { HEADS : c = } 1 \\
& \text { else: } c=2 \\
& \text { if } c==d: \text { print c } \\
& \text { else: print "Failure!" }
\end{aligned}
$$

Here's some events:

- The code prints "Failure!" $\{($ HEADS, 2$),($ TAILS, 1$)\}$


## Definition (Event)

An event is a subset of the sample space. We call these events, because the represent things that can happen. Consider the code from before:
$\mathrm{c}=\mathrm{FlipCoin}(1 / 2)$
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!" $\{($ HEADS, 2$),($ TAILS, 1$)\}$
- The code halts.


## Definition (Event)

An event is a subset of the sample space. We call these events, because the 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!" $\{($ HEADS, 2$),($ TAILS, 1$)\}$
- The code halts. $\{($ HEADS, 1$),($ HEADS, 2$),($ TAILS, 1$),($ TAILS, 2$)\}$


## Definition (Event)

An event is a subset of the sample space. We call these events, because the represent things that can happen. Consider the code from before:
$c=F l i p C o i n(1 / 2)$
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!" \{(HEADS, 2),(TAILS, 1) \}
- The code halts. $\{($ HEADS, 1$),($ HEADS, 2$),($ TAILS, 1$),($ TAILS, 2$)\}$
- The coin flip gives HEADS.


## Definition (Event)

An event is a subset of the sample space. We call these events, because the represent things that can happen. Consider the code from before:
$c=F l i p C o i n(1 / 2)$
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!" \{(HEADS, 2),(TAILS, 1)\}
- The code halts.
$\{($ HEADS, 1$),($ HEADS, 2$),($ TAILS, 1$),($ TAILS, 2$)\}$
- The coin flip gives HEADS. $\{($ HEADS, 1$),($ HEADS, 2$)\}$

Definition (Probability)
Let $S$ be a sample space and $E \subseteq S$ be an event. Then, we say $\operatorname{Pr}(E)$ is the probability of $E$.

Definition (Probability)
Let $S$ be a sample space and $E \subseteq S$ be an event. Then, we say $\operatorname{Pr}(E)$ is the probability of $E$.
Some facts about $\operatorname{Pr}(E)$ :

## Definition (Probability)

Let $S$ be a sample space and $E \subseteq S$ be an event. Then, we say $\operatorname{Pr}(E)$ is the probability of $E$.
Some facts about $\operatorname{Pr}(E)$ :

- $\operatorname{Pr}(S)=1$


## Definition (Probability)

Let $S$ be a sample space and $E \subseteq S$ be an event. Then, we say $\operatorname{Pr}(E)$ is the probability of $E$.
Some facts about $\operatorname{Pr}(E)$ :

- $\operatorname{Pr}(S)=1$
- $0 \leq \operatorname{Pr}(E) \leq 1$


## Definition (Probability)

Let $S$ be a sample space and $E \subseteq S$ be an event. Then, we say $\operatorname{Pr}(E)$ is the probability of $E$.
Some facts about $\operatorname{Pr}(E)$ :

- $\operatorname{Pr}(S)=1$
- $0 \leq \operatorname{Pr}(E) \leq 1$
- If $E_{1}, E_{2}, \ldots, E_{n} \subseteq S$ and are pairwise disjoint, then

$$
\operatorname{Pr}\left(E_{1} \cup E_{2} \cup \cdots \cup E_{n}\right)=\sum_{i=1}^{n} \operatorname{Pr}\left(E_{i}\right)
$$

## Definition (Probability)

Let $S$ be a sample space and $E \subseteq S$ be an event. Then, we say $\operatorname{Pr}(E)$ is the probability of $E$.
Some facts about $\operatorname{Pr}(E)$ :

- $\operatorname{Pr}(S)=1$
- $0 \leq \operatorname{Pr}(E) \leq 1$
- If $E_{1}, E_{2}, \ldots, E_{n} \subseteq S$ and are pairwise disjoint, then

$$
\operatorname{Pr}\left(E_{1} \cup E_{2} \cup \cdots \cup E_{n}\right)=\sum_{i=1}^{n} \operatorname{Pr}\left(E_{i}\right)
$$

Okay, enough of that. Let's do some problems!

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

- I bet a coin will come up HEADS.
- I bet a six-sided die will be even.
- I bet if each of us rolls a four-sided die, the sum will be 4 .
- I bet if I roll a four-sided die, and you roll a die with that many sides, the result will be even.
Which of these bets has a more than $50 \%$ chance of paying off?

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

- I bet a coin will come up HEADS.
- I bet a six-sided die will be even.

I bet if each of us rolls a four-sided die, the sum will be 4 .

- I bet if I roll a four-sided die, and you roll a die with that many sides, the result will be even.
Which of these bets has a more than $50 \%$ chance of paying off?

The first two are relatively easy to analyze:

- I bet a coin will come up HEADS.

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

I bet a coin will come up HEADS.
I bet a six-sided die will be even.

- I bet if each of us rolls a four-sided die, the sum will be 4 .

I bet if I roll a four-sided die, and you roll a die with that many sides, the result will be even.
Which of these bets has a more than $50 \%$ chance of paying off?

The first two are relatively easy to analyze:
I bet a coin will come up HEADS.

$$
\operatorname{Pr}(\text { HEADS })=1 / 2
$$

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

I bet a coin will come up HEADS.
I bet a six-sided die will be even.

- I bet if each of us rolls a four-sided die, the sum will be 4 .

I bet if I roll a four-sided die, and you roll a die with that many sides, the result will be even.
Which of these bets has a more than $50 \%$ chance of paying off?

The first two are relatively easy to analyze:
I bet a coin will come up HEADS.
$\operatorname{Pr}($ HEADS $)=1 / 2$
I bet a six-sided die will be even.

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

I bet a coin will come up HEADS.
I bet a six-sided die will be even.

- I bet if each of us rolls a four-sided die, the sum will be 4.

I bet if I roll a four-sided die, and you roll a die with that many sides, the result will be even.
Which of these bets has a more than $50 \%$ chance of paying off?

The first two are relatively easy to analyze:

- I bet a coin will come up HEADS.
$\operatorname{Pr}($ HEADS $)=1 / 2$
- I bet a six-sided die will be even.
$\operatorname{Pr}($ even roll $)=3 / 6=1 / 2$


## Gambling Problem(s)

"I bet if each of us rolls a four-sided die, the sum will be 4."

## Gambling Problem(s)

"I bet if each of us rolls a four-sided die, the sum will be 4."

```
1 ta_die = RollDie(4)
2 adam_die = RollDie(4)
3 if ta_die + adam_die == 4:
4 print "TA Wins!"
5 else:
6 print "Adam Wins!"
```


## Gambling Problem(s)

"I bet if each of us rolls a four-sided die, the sum will be 4."

```
1 ta_die = RollDie(4)
2 adam_die = RollDie(4)
3 if ta_die + adam_die == 4:
4 print "TA Wins!"
5 else:
6 print "Adam Wins!"
```



## Gambling Problem(s)

"I bet if each of us rolls a four-sided die, the sum will be 4."

```
1 ta_die = RollDie(4)
2 adam_die = RollDie(4)
3 if ta_die + adam_die == 4:
4 print "TA Wins!"
5 else:
6 print "Adam Wins!"
```



$$
\operatorname{Pr}(\text { sum is } 4)=\operatorname{Pr}(\{(1,3),(2,2),(3,1)\})=\frac{3}{16}
$$

## Gambling Problem(s)

"I bet if I roll a four-sided die, and you roll a die with that many sides, the result will be even."

## Gambling Problem(s)

"I bet if I roll a four-sided die, and you roll a die with that many sides, the result will be even."

```
1 ta_die = RollDie(4)
2 result = RollDie(ta_die)
3 if result % 2 == 0:
4 print "TA Wins!"
5 else:
6 print "Adam Wins!"
```

"I bet if I roll a four-sided die, and you roll a die with that many sides, the result will be even."

"I bet if I roll a four-sided die, and you roll a die with that many sides, the result will be even."

```
1 ta_die = RollDie(4)
2 result = RollDie(ta_die)
3 if result % 2 == 0:
4 print "TA Wins!"
5 else:
6 print "Adam Wins!"
```


$\operatorname{Pr}($ result is even $)=\operatorname{Pr}(\{(2,2),(3,2),(4,2),(4,4)\})=\frac{1}{8}+\frac{1}{12}+\frac{1}{8}=\frac{1}{3}$

What is the probability that 1313 flips of a fair coin are all HEADS?

What is the probability that 1313 flips of a fair coin are all HEADS?

Answer: Each flip has probability $1 / 2$ of coming up heads;

What is the probability that 1313 flips of a fair coin are all HEADS?

Answer: Each flip has probability $1 / 2$ of coming up heads; so, multiplying them all together, we get $\left(\frac{1}{2}\right)^{1313}$.

What is the probability that 1313 flips of a fair coin are all HEADS?

Answer: Each flip has probability $1 / 2$ of coming up heads; so, multiplying them all together, we get $\left(\frac{1}{2}\right)^{1313}$.

Why did we multiply them together? What allowed us to do that?

What is the probability that 1313 flips of a fair coin are all HEADS?

Answer: Each flip has probability $1 / 2$ of coming up heads; so, multiplying them all together, we get $\left(\frac{1}{2}\right)^{1313}$.

Why did we multiply them together? What allowed us to do that? We will come back to this argument later when we have more powerful machinery.

What is the probability that 1313 flips of a fair coin are all HEADS?

Answer: Each flip has probability $1 / 2$ of coming up heads; so, multiplying them all together, we get $\left(\frac{1}{2}\right)^{1313}$.

Why did we multiply them together? What allowed us to do that? We will come back to this argument later when we have more powerful machinery.

More generally:

What is the probability that 1313 flips of a fair coin are all HEADS?

Answer: Each flip has probability $1 / 2$ of coming up heads; so, multiplying them all together, we get $\left(\frac{1}{2}\right)^{1313}$.

Why did we multiply them together? What allowed us to do that? We will come back to this argument later when we have more powerful machinery.

More generally: The probability of any sequence of 1313 flips of a fair coin is $\left(\frac{1}{2}\right)^{1313}$.

What is the probability that 1313 flips of a fair coin are all HEADS?

Answer: Each flip has probability $1 / 2$ of coming up heads; so, multiplying them all together, we get $\left(\frac{1}{2}\right)^{1313}$.

Why did we multiply them together? What allowed us to do that? We will come back to this argument later when we have more powerful machinery.

More generally: The probability of any sequence of 1313 flips of a fair coin is $\left(\frac{1}{2}\right)^{1313}$. They are all equally likely!

## Dating Service

A dating service has a $1 / 2$ probability of each couple it matches working out. Suppose that the dating service matches 1313 couples.

## Dating Service

A dating service has a $1 / 2$ probability of each couple it matches working out. Suppose that the dating service matches 1313 couples.
What is the probability that exactly 13 couples work out?

A dating service has a $1 / 2$ probability of each couple it matches working out. Suppose that the dating service matches 1313 couples.
What is the probability that exactly 13 couples work out?
First, model it as code:

```
1 good_matches = 0
2 for i=1 to 1313:
3 if FlipCoin(1/2) == HEADS:
4 good_matches++
5 if good_matches == 13:
6 print "Yay!"
```

A dating service has a $1 / 2$ probability of each couple it matches working out. Suppose that the dating service matches 1313 couples.
What is the probability that exactly 13 couples work out?
First, model it as code:

```
1 good_matches = 0
2 for i=1 to 1313:
3 if FlipCoin(1/2) == HEADS:
4 good_matches++
5 if good_matches == 13:
6 print "Yay!"
```

Let $E$ be the event "the program prints "Yay!" ".

A dating service has a $1 / 2$ probability of each couple it matches working out. Suppose that the dating service matches 1313 couples.
What is the probability that exactly 13 couples work out?
First, model it as code:

```
1 good_matches = 0
2 for i=1 to 1313:
3 if FlipCoin(1/2) == HEADS:
4 good_matches++
5 if good_matches == 13:
6 print "Yay!"
```

- Let $E$ be the event "the program prints "Yay!" ".
- The sample space, $S=\{\text { HEADS, TAILS }\}^{1313}$.

A dating service has a $1 / 2$ probability of each couple it matches working out. Suppose that the dating service matches 1313 couples.
What is the probability that exactly 13 couples work out?
First, model it as code:

```
1 good_matches = 0
for i=1 to 1313:
    if FlipCoin(1/2) == HEADS:
        good_matches++
if good_matches == 13:
        print "Yay!"
```

- Let $E$ be the event "the program prints "Yay!" ".
- The sample space, $S=\{\text { HEADS, TAILS }\}^{1313}$.
- Every outcome is equally likely, because we showed it above!

A dating service has a $1 / 2$ probability of each couple it matches working out. Suppose that the dating service matches 1313 couples.
What is the probability that exactly 13 couples work out?
First, model it as code:

```
1 good_matches = 0
for i=1 to 1313:
    if FlipCoin(1/2) == HEADS:
        good_matches++
if good_matches == 13:
        print "Yay!"
```

- Let $E$ be the event "the program prints "Yay!" ".
- The sample space, $S=\{\text { HEADS, TAILS }\}^{1313}$.
- Every outcome is equally likely, because we showed it above!
- So, $\operatorname{Pr}(E)=\frac{|E|}{|S|}$.

A dating service has a $1 / 2$ probability of each couple it matches working out. Suppose that the dating service matches 1313 couples. What is the probability that exactly 13 couples work out?
First, model it as code:

```
1 good_matches = 0
```

```
for i=1 to 1313:
```

for i=1 to 1313:
if FlipCoin(1/2) == HEADS:
if FlipCoin(1/2) == HEADS:
good_matches++
good_matches++
if good_matches == 13:
if good_matches == 13:
print "Yay!"

```
        print "Yay!"
```

- Let $E$ be the event "the program prints "Yay!" ".
- The sample space, $S=\{\text { HEADS, TAILS }\}^{1313}$.
- Every outcome is equally likely, because we showed it above!

So, $\operatorname{Pr}(E)=\frac{|E|}{|S|}$. (Take the number of ways to do what we want and divide by the number of outcomes.)

A dating service has a $1 / 2$ probability of each couple it matches working out. Suppose that the dating service matches 1313 couples.
What is the probability that exactly 13 couples work out?
First, model it as code:

```
1 good_matches = 0
for i=1 to 1313:
    if FlipCoin(1/2) == HEADS:
        good_matches++
if good_matches == 13:
    print "Yay!"
```

- Let $E$ be the event "the program prints "Yay!" ".
- The sample space, $S=\{\text { HEADS, TAILS }\}^{1313}$.
- Every outcome is equally likely, because we showed it above!

So, $\operatorname{Pr}(E)=\frac{|E|}{|S|}=\frac{\binom{1313}{13}}{2^{1313}}$.

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space.

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space. We have 23 people each with one of 366 birthdays; so, the outcomes are length 23 strings of birthdays.

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space. We have 23 people each with one of 366 birthdays; so, the outcomes are length 23 strings of birthdays.
Let $E$ be the event that at least two people have the same birthday.

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space. We have 23 people each with one of 366 birthdays; so, the outcomes are length 23 strings of birthdays. Let $E$ be the event that at least two people have the same birthday. If we can calculate $|E|$ and $|S|$, we're done.

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space. We have 23 people each with one of 366 birthdays; so, the outcomes are length 23 strings of birthdays. Let $E$ be the event that at least two people have the same birthday. If we can calculate $|E|$ and $|S|$, we're done.

Since $|E|$ is hard to count, we count $|\bar{E}|$ instead!

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space. We have 23 people each with one of 366 birthdays; so, the outcomes are length 23 strings of birthdays. Let $E$ be the event that at least two people have the same birthday. If we can calculate $|E|$ and $|S|$, we're done.

Since $|E|$ is hard to count, we count $|\bar{E}|$ instead! $\bar{E}$ is the event that no two people share a birthday.

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space. We have 23 people each with one of 366 birthdays; so, the outcomes are length 23 strings of birthdays. Let $E$ be the event that at least two people have the same birthday. If we can calculate $|E|$ and $|S|$, we're done.

Since $|E|$ is hard to count, we count $|\bar{E}|$ instead! $\bar{E}$ is the event that no two people share a birthday. In other words, the event that the string has no duplicate entries.

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space. We have 23 people each with one of 366 birthdays; so, the outcomes are length 23 strings of birthdays. Let $E$ be the event that at least two people have the same birthday. If we can calculate $|E|$ and $|S|$, we're done.

Since $|E|$ is hard to count, we count $|\bar{E}|$ instead! $\bar{E}$ is the event that no two people share a birthday. In other words, the event that the string has no duplicate entries. Using the Rule of Product, we see that

$$
|\bar{E}|=(366)(365) \cdots(344)
$$

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space. We have 23 people each with one of 366 birthdays; so, the outcomes are length 23 strings of birthdays. Let $E$ be the event that at least two people have the same birthday. If we can calculate $|E|$ and $|S|$, we're done.

Since $|E|$ is hard to count, we count $|\bar{E}|$ instead! $\bar{E}$ is the event that no two people share a birthday. In other words, the event that the string has no duplicate entries. Using the Rule of Product, we see that

$$
|\bar{E}|=(366)(365) \cdots(344)
$$

We also know that $|S|=366^{23}$ (also by the Rule of Product).

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space. We have 23 people each with one of 366 birthdays; so, the outcomes are length 23 strings of birthdays. Let $E$ be the event that at least two people have the same birthday. If we can calculate $|E|$ and $|S|$, we're done.

Since $|E|$ is hard to count, we count $|\bar{E}|$ instead! $\bar{E}$ is the event that no two people share a birthday. In other words, the event that the string has no duplicate entries. Using the Rule of Product, we see that

$$
|\bar{E}|=(366)(365) \cdots(344)
$$

We also know that $|S|=366^{23}$ (also by the Rule of Product). Then, $\frac{|\overline{\bar{E}}|}{|S|}=0.494$

How many people do we need before there's a $50 \%$ chance that two of them share a birthday?

It's actually only 23! Let's prove it:
Let $S$ be the sample space. We have 23 people each with one of 366 birthdays; so, the outcomes are length 23 strings of birthdays. Let $E$ be the event that at least two people have the same birthday. If we can calculate $|E|$ and $|S|$, we're done.

Since $|E|$ is hard to count, we count $|\bar{E}|$ instead! $\bar{E}$ is the event that no two people share a birthday. In other words, the event that the string has no duplicate entries. Using the Rule of Product, we see that

$$
|\bar{E}|=(366)(365) \cdots(344)
$$

We also know that $|S|=366^{23}$ (also by the Rule of Product). Then, $\frac{|\bar{E}|}{|S|}=0.494$ So,

$$
\frac{|E|}{|S|}=0.506
$$

It is sometimes useful to discuss how often an event $A$ occurs assuming that another event $B$ has already occurred.

It is sometimes useful to discuss how often an event $A$ occurs assuming that another event $B$ has already occurred.

Definition (Conditional Probability)
$\operatorname{Pr}(A \mid B)$ is pronounced "the probability of $A$ given $B$ ", and it's defined as:

It is sometimes useful to discuss how often an event $A$ occurs assuming that another event $B$ has already occurred.

Definition (Conditional Probability)
$\operatorname{Pr}(A \mid B)$ is pronounced "the probability of $A$ given $B$ ", and it's defined as:

$$
\operatorname{Pr}(A \mid B)=\frac{\operatorname{Pr}(A \cap B)}{\operatorname{Pr}(B)}
$$

It is sometimes useful to discuss how often an event $A$ occurs assuming that another event $B$ has already occurred.

Definition (Conditional Probability)
$\operatorname{Pr}(A \mid B)$ is pronounced "the probability of $A$ given $B$ ", and it's defined as:

$$
\operatorname{Pr}(A \mid B)=\frac{\operatorname{Pr}(A \cap B)}{\operatorname{Pr}(B)}
$$



Think of $\operatorname{Pr}(A \mid B)$ as restricting the sample space to $B$ and considering how often $A$ occurs.

Suppose we roll a black die and a white die. What is the probability that the white die is 1 given that the sum is 7 ?

Suppose we roll a black die and a white die. What is the probability that the white die is 1 given that the sum is 7 ?

| $(1,1)$ | $(1,2)$ | $(1,3)$ | $(1,4)$ | $(1,5)$ |  |
| :--- | :--- | :--- | :--- | :--- | :--- |
| $(2,1)$ | $(2,2)$ | $(2,3)$ | $(2,4)$ | $(2,5)$ | $(2,6)$ |
| $(3,1)$ | $(3,2)$ | $(3,3)$ | $(3,4)$ | $(3,5)$ | $(3,6)$ |
| $(4,1)$ | $(4,2)$ | $(4,3)$ | $(4,4)$ | $(4,5)$ | $(4,6)$ |
| $(5,1)$ | $(5,2)$ | $(5,3)$ | $(5,4)$ | $(5,5)$ | $(5,6)$ |
| $(6,1)$ | $(6,2)$ | $(6,3)$ | $(6,4)$ | $(6,5)$ | $(6,6)$ |

We can calculate this two ways:

Suppose we roll a black die and a white die. What is the probability that the white die is 1 given that the sum is 7 ?

| $(1,1)$ | $(1,2)$ | $(1,3)$ | $(1,4)$ | $(1,5)$ |  |
| :--- | :--- | :--- | :--- | :--- | :--- |
| $(2,1)$ | $(2,2)$ | $(2,3)$ | $(2,4)$ | $(2,5)$ | $(2,6)$ |
| $(3,1)$ | $(3,2)$ | $(3,3)$ | $(3,4)$ | $(3,5)$ | $(3,6)$ |
| $(4,1)$ | $(4,2)$ | $(4,3)$ | $(4,4)$ | $(4,5)$ | $(4,6)$ |
| $(5,1)$ | $(5,2)$ | $(5,3)$ | $(5,4)$ | $(5,5)$ | $(5,6)$ |
| $(6,1)$ | $(6,2)$ | $(6,3)$ | $(6,4)$ | $(6,5)$ | $(6,6)$ |

We can calculate this two ways:
Way 1: Let $W$ be the event that the white die is 1 and $S$ be the event that the sum is 7 . We see that $\operatorname{Pr}(S)=\frac{6}{36}$ and $\operatorname{Pr}(S \cap W)=\frac{1}{36}$. Using the formula for conditional probability, we get $\operatorname{Pr}(W \mid S)=\frac{\frac{1}{36}}{\frac{6}{6}}=\frac{1}{6}$.

Suppose we roll a black die and a white die. What is the probability that the white die is 1 given that the sum is 7 ?

| $(1,1)$ | $(1,2)$ | $(1,3)$ | $(1,4)$ | $(1,5)$ |  |
| :--- | :--- | :--- | :--- | :--- | :--- |
| $(2,1)$ | $(2,2)$ | $(2,3)$ | $(2,4)$ | $(2,5)$ | $(2,6)$ |
| $(3,1)$ | $(3,2)$ | $(3,3)$ | $(3,4)$ | $(3,5)$ | $(3,6)$ |
| $(4,1)$ | $(4,2)$ | $(4,3)$ | $(4,4)$ | $(4,5)$ | $(4,6)$ |
| $(5,1)$ | $(5,2)$ | $(5,3)$ | $(5,4)$ | $(5,5)$ | $(5,6)$ |
| $(6,1)$ | $(6,2)$ | $(6,3)$ | $(6,4)$ | $(6,5)$ | $(6,6)$ |

We can calculate this two ways:
Way 1: Let $W$ be the event that the white die is 1 and $S$ be the event that the sum is 7 . We see that $\operatorname{Pr}(S)=\frac{6}{36}$ and $\operatorname{Pr}(S \cap W)=\frac{1}{36}$. Using the formula for conditional probability, we get $\operatorname{Pr}(W \mid S)=\frac{\frac{1}{36}}{\frac{6}{36}}=\frac{1}{6}$.

Way 2: If we restrict our sample space to the six outcomes where the sum is 7 , only one of them has the white die as 1 . So, the probability we're looking for is $\frac{1}{6}$.

## Golden Coins

We have three bags with coins: one has two gold coins, one has two silver coins, and the third has one gold coin and one silver coin.


We randomly choose one of the bags, and we randomly select a coin from the bag. It turns out to be gold.
What is the probability that the other coin in that bag is gold?

## Golden Coins

We have three bags with coins: one has two gold coins, one has two silver coins, and the third has one gold coin and one silver coin.


We randomly choose one of the bags, and we randomly select a coin from the bag. It turns out to be gold.
What is the probability that the other coin in that bag is gold?
Let $G_{1}$ be the event that the coin we chose first is gold.

## Golden Coins

We have three bags with coins: one has two gold coins, one has two silver coins, and the third has one gold coin and one silver coin.


We randomly choose one of the bags, and we randomly select a coin from the bag. It turns out to be gold.
What is the probability that the other coin in that bag is gold?
Let $G_{1}$ be the event that the coin we chose first is gold. Let $G_{2}$ be the event that the second chosen coin is gold.

We have three bags with coins: one has two gold coins, one has two silver coins, and the third has one gold coin and one silver coin.


We randomly choose one of the bags, and we randomly select a coin from the bag. It turns out to be gold.
What is the probability that the other coin in that bag is gold?
Let $G_{1}$ be the event that the coin we chose first is gold. Let $G_{2}$ be the event that the second chosen coin is gold. The problem is asking us to find $\operatorname{Pr}\left(G_{2} \mid G_{1}\right)$ :

- $\operatorname{Pr}\left(G_{1}\right)=3 / 6=1 / 2$ (three of the six coins are gold)
$\square \operatorname{Pr}\left(G_{1} \cap G_{2}\right)=1 / 3$ (the coins must be in the gold-gold bag)
- $\operatorname{Pr}\left(G_{2} \mid G_{1}\right)=\frac{\operatorname{Pr}\left(G_{1} \cap G_{2}\right)}{\operatorname{Pr}\left(G_{1}\right)}=\frac{2}{3}$


## Independence

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

## Independence

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:

## Independence

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class.

## Independence

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class. Let $C_{S}$ be the event that Sandy comes to $98-000$ class.

## Independence

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class. Let $C_{S}$ be the event that Sandy comes to $98-000$ class. Empirically, we know that:

- $\operatorname{Pr}\left(C_{P}\right)=1$


## Independence

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class. Let $C_{S}$ be the event that Sandy comes to $98-000$ class. Empirically, we know that:
$-\operatorname{Pr}\left(C_{P}\right)=1$

- $\operatorname{Pr}\left(C_{S}\right)=\frac{1}{8}$


## Independence

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class. Let $C_{S}$ be the event that Sandy comes to $98-000$ class. Empirically, we know that:

- $\operatorname{Pr}\left(C_{P}\right)=1$
- $\operatorname{Pr}\left(C_{S}\right)=\frac{1}{8}$
- $\operatorname{Pr}\left(C_{P} \cap C_{S}\right)=\frac{1}{8}$

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class. Let $C_{S}$ be the event that Sandy comes to $98-000$ class. Empirically, we know that:

- $\operatorname{Pr}\left(C_{P}\right)=1$
- $\operatorname{Pr}\left(C_{S}\right)=\frac{1}{8}$
- $\operatorname{Pr}\left(C_{P} \cap C_{S}\right)=\frac{1}{8}$

Since $\frac{1}{8}=\frac{1}{8}, \operatorname{Pr}\left(C_{P}\right)$ and $\operatorname{Pr}\left(C_{S}\right)$ are independent!

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class. Let $C_{S}$ be the event that Sandy comes to $98-000$ class. Empirically, we know that:

- $\operatorname{Pr}\left(C_{P}\right)=1$
- $\operatorname{Pr}\left(C_{S}\right)=\frac{1}{8}$
- $\operatorname{Pr}\left(C_{P} \cap C_{S}\right)=\frac{1}{8}$

Since $\frac{1}{8}=\frac{1}{8}, \operatorname{Pr}\left(C_{P}\right)$ and $\operatorname{Pr}\left(C_{S}\right)$ are independent! What does this mean?

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class. Let $C_{S}$ be the event that Sandy comes to $98-000$ class. Empirically, we know that:

- $\operatorname{Pr}\left(C_{P}\right)=1$
- $\operatorname{Pr}\left(C_{S}\right)=\frac{1}{8}$
- $\operatorname{Pr}\left(C_{P} \cap C_{S}\right)=\frac{1}{8}$

Since $\frac{1}{8}=\frac{1}{8}, \operatorname{Pr}\left(C_{P}\right)$ and $\operatorname{Pr}\left(C_{S}\right)$ are independent! What does this mean?
Tempting Answer: Pete and Sandy's decisions to go to class aren't reliant on each other.

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class. Let $C_{S}$ be the event that Sandy comes to $98-000$ class. Empirically, we know that:

- $\operatorname{Pr}\left(C_{P}\right)=1$
- $\operatorname{Pr}\left(C_{S}\right)=\frac{1}{8}$
- $\operatorname{Pr}\left(C_{P} \cap C_{S}\right)=\frac{1}{8}$

Since $\frac{1}{8}=\frac{1}{8}, \operatorname{Pr}\left(C_{P}\right)$ and $\operatorname{Pr}\left(C_{S}\right)$ are independent! What does this mean?
Tempting Answer: Pete and Sandy's decisions to go to class aren't reliant on each other.
In Actuality: There are a total of 8 sessions of 98-000.

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class. Let $C_{S}$ be the event that Sandy comes to $98-000$ class. Empirically, we know that:

- $\operatorname{Pr}\left(C_{P}\right)=1$
- $\operatorname{Pr}\left(C_{S}\right)=\frac{1}{8}$
- $\operatorname{Pr}\left(C_{P} \cap C_{S}\right)=\frac{1}{8}$

Since $\frac{1}{8}=\frac{1}{8}, \operatorname{Pr}\left(C_{P}\right)$ and $\operatorname{Pr}\left(C_{S}\right)$ are independent!
What does this mean?
Tempting Answer: Pete and Sandy's decisions to go to class aren't reliant on each other.
In Actuality: There are a total of 8 sessions of 98-000. Sandy met Pete at the first class which they both attended.

Definition (Independence)
We say that two events $A$ and $B$ are independent iff

$$
\operatorname{Pr}(A \cap B)=\operatorname{Pr}(A) \operatorname{Pr}(B)
$$

Here's an example:
Let $C_{P}$ be the event that Pete comes to $98-000$ class. Let $C_{S}$ be the event that Sandy comes to $98-000$ class. Empirically, we know that:

- $\operatorname{Pr}\left(C_{P}\right)=1$
- $\operatorname{Pr}\left(C_{S}\right)=\frac{1}{8}$
- $\operatorname{Pr}\left(C_{P} \cap C_{S}\right)=\frac{1}{8}$

Since $\frac{1}{8}=\frac{1}{8}, \operatorname{Pr}\left(C_{P}\right)$ and $\operatorname{Pr}\left(C_{S}\right)$ are independent!
What does this mean?
Tempting Answer: Pete and Sandy's decisions to go to class aren't reliant on each other.
In Actuality: There are a total of 8 sessions of $98-000$. Sandy met Pete at the first class which they both attended. For all future sessions, Pete took notes for Sandy, and she never showed up again.

What is the probability that 1313 flips of a fair coin are all HEADS?

What is the probability that 1313 flips of a fair coin are all HEADS?

```
1 num_heads = 0
2 for i=1 to 1313:
3 if FlipCoin(1/2) == HEADS:
4 num_heads++
5 if num_heads == 1313:
6 print "Yay!"
```

What is the probability that 1313 flips of a fair coin are all HEADS?

```
1 num_heads = 0
2 for i=1 to 1313:
3 if FlipCoin(1/2) == HEADS:
4 num_heads++
5 if num_heads == 1313:
6 print "Yay!"
```

Let $C_{i}$ (for $1 \leq i \leq 1313$ ) be the event that the $i$ th coin flip is HEADS.

What is the probability that 1313 flips of a fair coin are all HEADS?

```
1 num_heads = 0
2 for i=1 to 1313:
3 if FlipCoin(1/2) == HEADS:
4 num_heads++
5 if num_heads == 1313:
6 print "Yay!"
```

Let $C_{i}$ (for $1 \leq i \leq 1313$ ) be the event that the $i$ th coin flip is HEADS. We see that none of the results of the coin flips in the procedure interact with each other; so, each of them is independent.

What is the probability that 1313 flips of a fair coin are all HEADS?

```
    num_heads = 0
    for i=1 to 1313:
        if FlipCoin(1/2) == HEADS:
            num_heads++
    if num_heads == 1313:
        print "Yay!"
```

Let $C_{i}$ (for $1 \leq i \leq 1313$ ) be the event that the $i$ th coin flip is HEADS.
We see that none of the results of the coin flips in the procedure interact with each other; so, each of them is independent. It follows that

$$
\operatorname{Pr}\left(\bigcap_{i=1}^{1313} C_{i}\right)=\prod_{i=1}^{1313} \operatorname{Pr}\left(C_{i}\right)=\left(\frac{1}{2}\right)^{1313}
$$

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

Does this code terminate?
Let $E$ be the event that the code terminates.

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

Does this code terminate?
Let $E$ be the event that the code terminates. Note that if $E_{i}$ is the event that the code terminates on the $i$ th run through the loop, we have:

$$
E=\bigcup_{i=0}^{\infty} E_{i}
$$

Then, we know $\operatorname{Pr}(E)=\operatorname{Pr}\left(\bigcup_{i=0}^{\infty} E_{i}\right)=\sum_{i=1}^{\infty} \operatorname{Pr}\left(E_{i}\right)$. Note that $\operatorname{Pr}\left(E_{i}\right)$ is the probability that the code does not terminate on the first $i-1$ iterations and does on the $i$ th iteration. Then, $\operatorname{Pr}\left(E_{i}\right)=\left(\frac{1}{2}\right)^{i}$. So,

$$
\operatorname{Pr}(E)=\sum_{i=1}^{\infty}\left(\frac{1}{2}\right)^{i}=\frac{1}{1-\frac{1}{2}}-1=1
$$

