PROBABILITY

DISCRETE STRUCTURES II

DARRYL HILL

BASED ON THE TEXTBOOK:

DISCRETE STRUCTURES FOR COMPUTER SCIENCE: COUNTING, RECURSION, AND PROBABILITY

BY MICHIEL SMID

Anonymous Broadcasting

You may have seen some probability, and have some intuitions on how to apply it.

We know if you flip a coin it comes up heads with probability 0.50 and it comes up tails with probability 0.50

If I flip a coin and don't show you, you cannot guess with > 0.50 probability whether it is heads or tails.

We intuitively realize that it is unlikely that we will win the lottery.

We intuitively realize that if the weatherman calls for 80% chance of showers, you should bring an umbrella (maybe).

We are going to redefine probability from first principles.

We will start with an example application of probability and random numbers.

Anonymous Broadcasting

A group of 3 cryptographers are dining at a restaurant.

The waiter informs them that someone has paid for their meal.

They respect each other's right to privacy, but also want to find out if the NSA has paid.

They devise a system for someone to announce anonymously if they have paid.

Anonymous Broadcasting

A group of 3 cryptographers are dining at a restaurant.

The waiter informs them that someone has paid for their meal.

They respect each other's right to privacy, but also want to find out if the NSA has paid.

They devise a system for someone to announce anonymously if they have paid.

The person who paid, if they paid, will anonymously transmit a single bit, a 1.

Everyone who did not pay will transmit a 0.

In the end, we will know if a 1 has been transmitted (someone paid), or if everyone transmitted a 0 (NSA paid).

But if there is a 1, we will not know who sent it.

Anonymous Broadcasting

A group of 3 cryptographers are dining at a restaurant.

The waiter informs them that someone has paid for their meal.

They respect each other's right to privacy, but also want to find out if the NSA has paid.

They devise a system for someone to announce anonymously if they have paid.

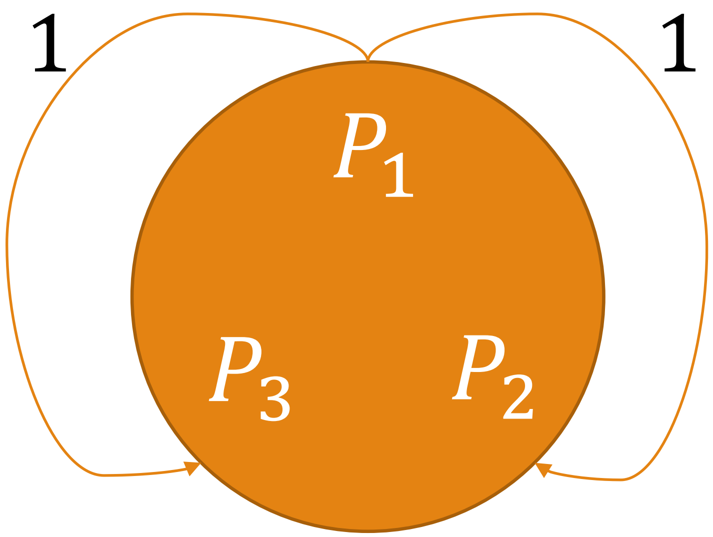
Three people, P_1, P_2, P_3

Either:

1. One person transmits 1 and the rest 0, or
2. They all transmit 0.

Everyone will know if a 1 was transmitted, but not who sent it.

Anonymous Broadcasting



Three people, P_1, P_2, P_3

Either:

1. One person transmits 1, two transmit 0
2. All three transmit 0.

Everyone will know if a 1 was transmitted, but not who sent it.

If someone paid for the meal, they transmit a 1, while everyone else transmits 0.

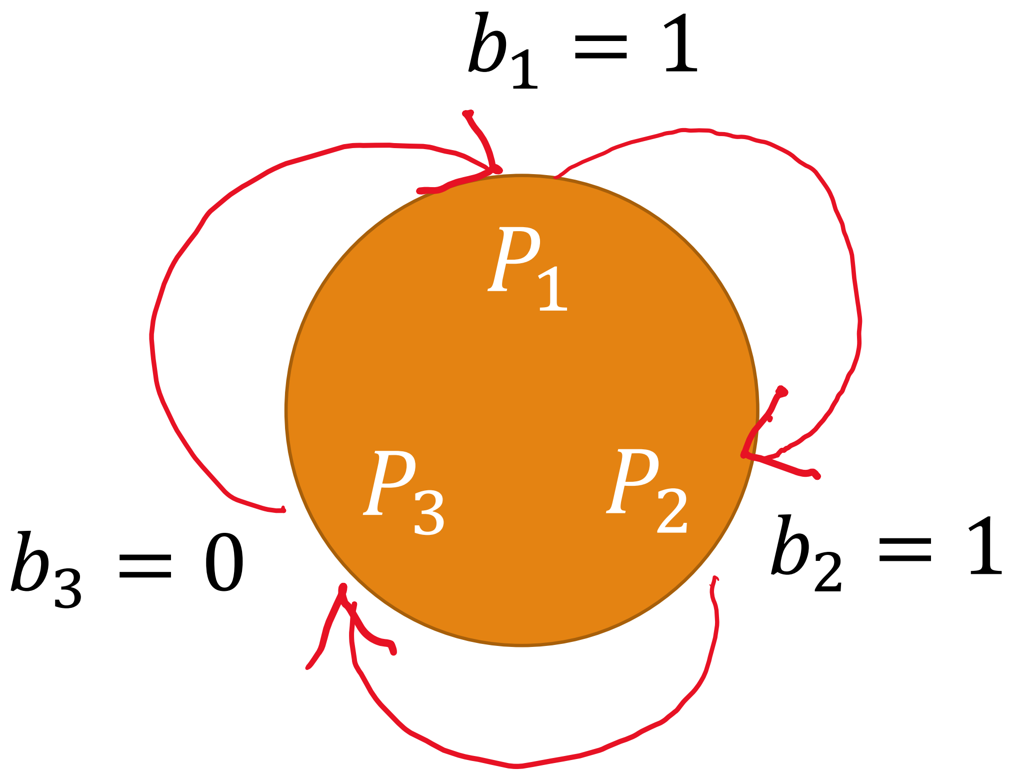
If the transmitted bit is 1, then someone at the table paid.

If the bit is 0, the NSA paid.

We will do an example where P_1 paid.

Algorithm:

1. Every person P_i generates a random bit b_i and shares it with the person to their right.

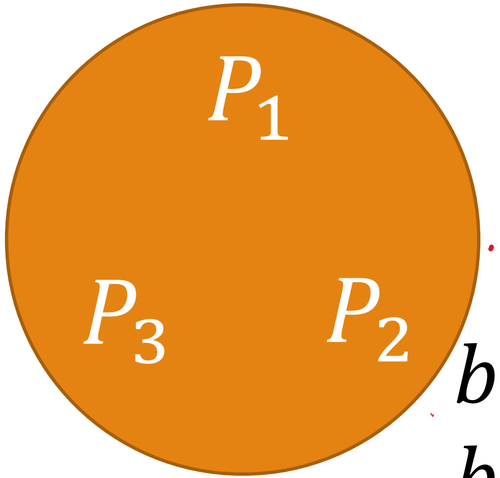


Algorithm:

1. Every person P_i generates a random bit b_i and shares it with the person to their right.
2. Now everyone knows 2 out of the 3 random bits b_i.
3. Everyone adds their known bits together, $mod\ 2$. If someone is sending a 1, they add that as well.
4. $p_1 = b_1 + b_3 + 1\ mod\ 2 = 1 + 0 + 1 = 0$

$\boxed{p_1 = b_1 + b_3 + 1\ mod\ 2 = 0}$

$b_1 = 1,$
$b_3 = 0$



$b_3 = 0,$
$b_2 = 1$

$b_2 = 1,$
$b_1 = 1$

$\boxed{p_3 = b_3 + b_2\ mod\ 2 = 1}$

$\boxed{p_2 = b_1 + b_2\ mod\ 2 = 0}$

Algorithm:

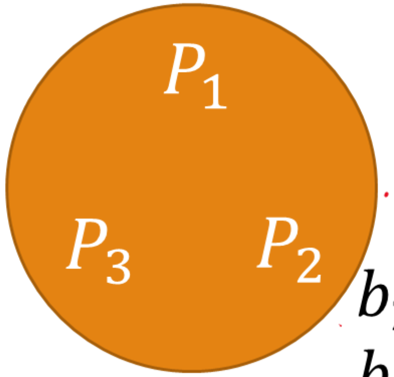
1. Every person P_i generates a random bit b_i and shares it with the person to their right.
2. Now everyone knows 2 out of the 3 random bits b_i.
3. Everyone adds their known bits together, mod 2. If someone is sending a 1, they add that as well.
4. $p_1 = b_1 + b_3 + 1 \; mod \; 2 = 1 + 0 + 1 = 0$
5. All p_i are transmitted to everyone and combined mod 2:

$$a = p_1 + p_2 + p_3 \; mod \; 2$$

6. Claim: $a = 1$ if someone sent a 1, and $a = 0$ otherwise.
7. In other words, the random bits cancel.

$p_1 = b_1 + b_3 + 1 \; mod \; 2 = 0$

$b_1 = 1,$
$b_3 = 0$



$b_3 = 0,$
$b_2 = 1$

$b_2 = 1,$
$b_1 = 1$

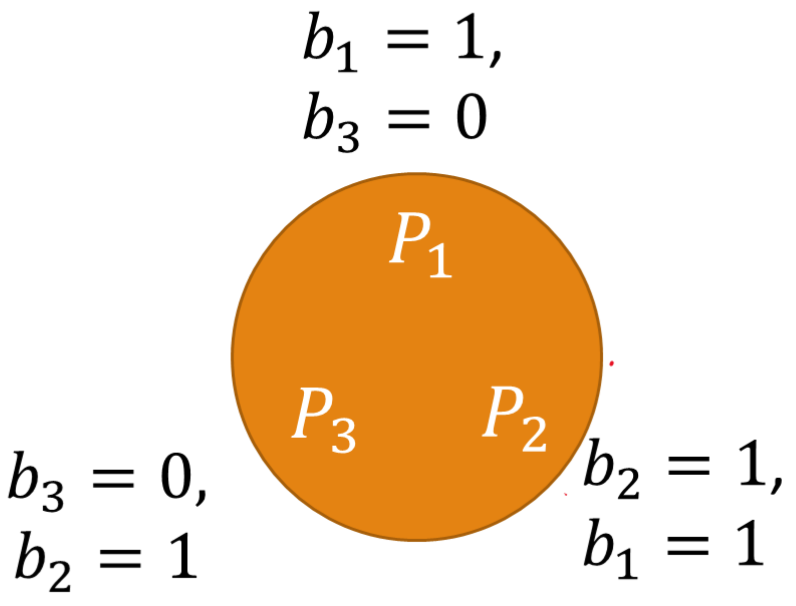
$p_3 = b_3 + b_2 \; mod \; 2 = 1$

$p_2 = b_1 + b_2 \; mod \; 2 = 0$

$a = p_1 + p_2 + p_3$
$a = (b_1 + b_1 + b_2 + b_2 + b_3 + b_3 + 1)$
$a = 1$

Anonymous Broadcasting

$p_1 = b_1 + b_3 + 1 \; mod \; 2 = 0$



$p_3 = b_3 + b_2 \; mod \; 2 = 1$

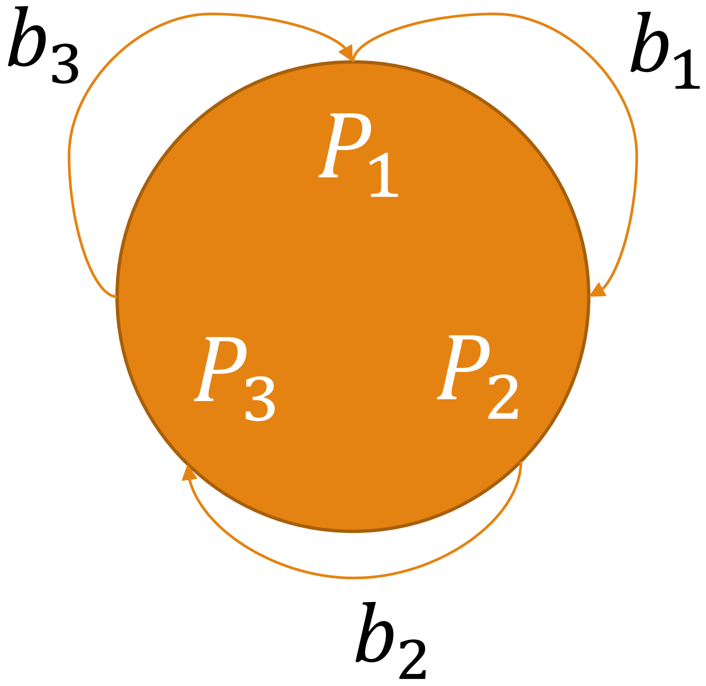
$p_2 = b_1 + b_2 \; mod \; 2 = 0$

$$a = (p_1 + p_2 + p_3) \; mod \; 2$$
$$= (\underbrace{b_1 + b_1}_{0} + \underbrace{b_2 + b_2}_{0} + \underbrace{b_3 + b_3}_{0} + 1) \; mod \; 2 \qquad +1 = 1$$
$$= 1$$

This works because for any bit b_i,
$b_i + b_i \; mod \; 2 = 0$
If $b_i = 0$, then $0 + 0 \; mod \; 2 = 0 \; mod \; 2 = 0$
If $b_i = 1$, then $1 + 1 \; mod \; 2 = 2 \; mod \; 2 = 0$

Thus $b_1 + b_1, \; b_2 + b_2, \; and \; b_3 + b_3$ all cancel out, leaving 1.

Anonymous Broadcasting



(Hopefully) we are convinced we can broadcast in this way and each person can extract b.

The purpose of this exercise is to broadcast $anonymously$. How can we prove that?

Lacking any elegant method, we turn to *brute force*, i.e., case analysis.

But we will just show you one case for the previous example to give you the idea behind all of the cases.

Anonymous Broadcasting

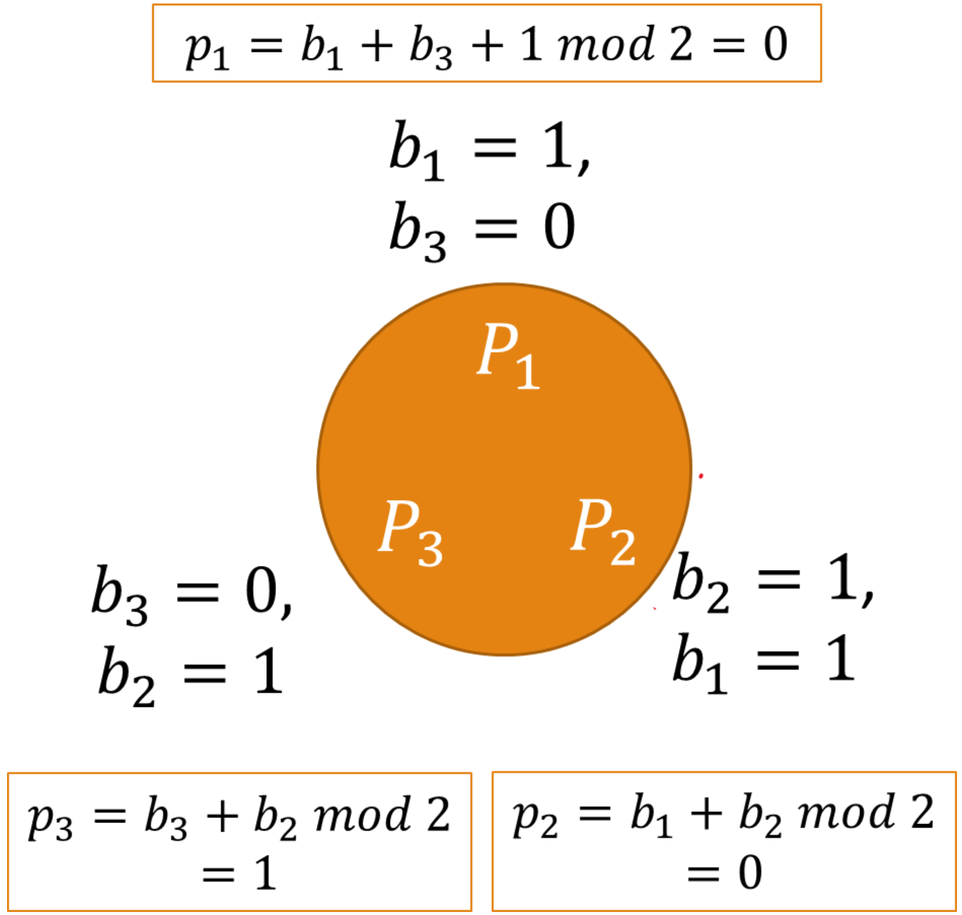
Examine this from P_2's perspective.

P_2 knows that P_1 transmitted $p_1 = 1$
P_2 knows that P_3 transmitted $p_3 = 1$
P_2 knows b_1 and b_2 but not b_3

$$p_1 = (b_1 + b_3 +?\, 1)\ mod\ 2 = 0$$
$$p_3 = (b_3 + b_2 +?\, 1)\ mod\ 2 = 1$$

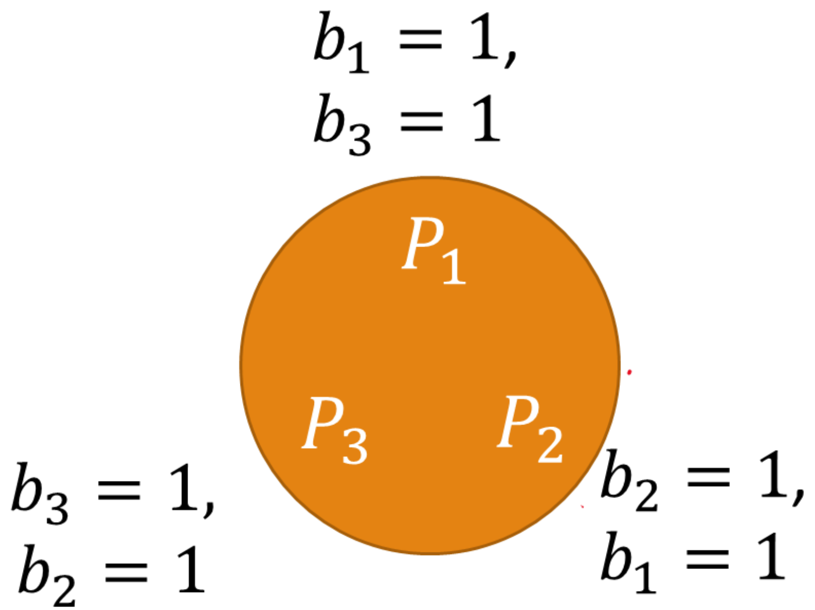
$$p_1 = (1 + b_3 +?\, 1)\ mod\ 2 = 0$$
$$p_3 = (b_3 + 1 +?\, 1)\ mod\ 2 = 1$$

If b_3 is 0, then P_1 sent the bit.
If b_3 is 1, then P_3 sent the bit.



Anonymous Broadcasting

$p_1 = b_1 + b_3 \; mod \; 2 = 0$



$p_3 = b_3 + b_2 + 1 \; mod \; 2 = 1$

$p_2 = b_1 + b_2 \; mod \; 2 = 0$

Examine this from P_2's perspective.

P_2 knows that P_1 transmitted $p_1 = 1$
P_2 knows that P_3 transmitted $p_3 = 1$
P_2 knows b_1 and b_2 but not b_3

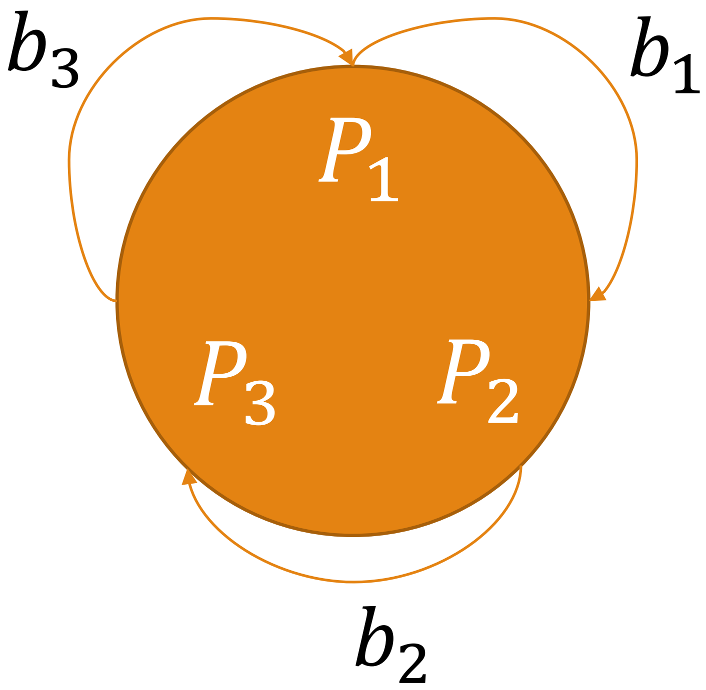
$$p_1 = (b_1 + b_3 +? \, b) \; mod \; 2 = 0$$
$$p_3 = (b_3 + b_2 +? \, b) \; mod \; 2 = 1$$

$$p_1 = (1 + b_3 +? \, 1) \; mod \; 2 = 0$$
$$p_3 = (b_3 + 1 +? \, 1) \; mod \; 2 = 1$$

If b_3 is 0, then P_1 sent the bit.
If b_3 is 1, then P_3 sent the bit.

But P_2 does not know b_3.

Anonymous Broadcasting



Assume $b = 1$ and that P_2 is NOT the broadcaster.
We will take on the role of P_2.
Either P_1 or P_3 is the broadcaster, but we don't know which.

We will see if we can use what we know to determine if P_1 or P_3 is the broadcaster.

We know b_2 and b_1 but do not know b_3.
We also know p_1, p_2, p_3 and we know b.

We don't know b_3 and we don't know who added b.

unknown

$$p_2 = b_1 + b_2$$
$$p_1 = b_1 + \boxed{b_3 + (\text{perhaps } b)}$$
$$p_3 = b_2 + \boxed{b_3 + (\text{perhaps } b)}$$

Anonymous Broadcasting

P_2 knows if they are in Case 1, but does not know if they are in Case 1.1 or Case 1.2 unless they know b_3

Assume $b = 1$ and that P_2 is NOT the broadcaster

Case 1: if $b_1 = b_2$:

Case 1.1: if $b_1 = b_2 = b_3$

Case 1.1.1: if P_1 broadcasts, then
$p_1 = b_1 + b_3 + b = 1$
$p_3 = b_2 + b_3 = 0$

Case 1.1.2: if P_3 broadcasts, then
$p_1 = b_1 + b_3 = 0$
$p_3 = b_2 + b_3 + b = 1$

Case 1.2: if $b_1 = b_2 \neq b_3$

Case 1.2.1: if P_1 broadcasts, then
$p_1 = b_1 + b_3 + b = 0$
$p_3 = b_2 + b_3 = 1$

Case 1.2.2: if P_3 broadcasts, then
$p_1 = b_1 + b_3 = 1$
$p_3 = b_2 + b_3 + b = 0$

Anonymous Broadcasting

For example, we know $p_1 = 0$ and $p_3 = 1$. We are in Case 1.2.1 or 1.1.2. But we don't know which without b_3

Assume $b = 1$ and that P_2 is NOT the broadcaster

Case 1: if $b_1 = b_2$:

Case 1.1: if $b_1 = b_2 = b_3$

Case 1.1.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 1$$
$$p_3 = b_2 + b_3 = 0$$

Case 1.1.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 0$$
$$p_3 = b_2 + b_3 + b = 1$$

Case 1.2: if $b_1 = b_2 \neq b_3$

Case 1.2.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 0$$
$$p_3 = b_2 + b_3 = 1$$

Case 1.2.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 1$$
$$p_3 = b_2 + b_3 + b = 0$$

Anonymous Broadcasting

Or we know $p_1 = 1$ and $p_3 = 0$. We are in Case 1.1.1 or 1.2.2. But we don't know which without b_3

Assume $b = 1$ and that P_2 is NOT the broadcaster

Case 1: if $b_1 = b_2$:

Case 1.1: if $b1 = b_2 = b_3$

Case 1.1.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 1$$
$$p_3 = b_2 + b_3 = 0$$

Case 1.1.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 0$$
$$p_3 = b_2 + b_3 + b = 1$$

Case 1.2: if $b_1 = b_2 \neq b_3$

Case 1.2.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 0$$
$$p_3 = b_2 + b_3 = 1$$

Case 1.2.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 1$$
$$p_3 = b_2 + b_3 + b = 0$$

Anonymous Broadcasting

P_2 knows if they are in Case 2, but $p_1 = p_3$ regardless of who the broadcaster is.

Assume $b = 1$ and that P_2 is NOT the broadcaster

Case 2: if $b_1 \neq b_2$:

Case 2.1: if $b_1 \neq b_2 = b_3$

Case 2.1.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 0$$
$$p_3 = b_2 + b_3 = 0$$

Case 2.1.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 1$$
$$p_3 = b_2 + b_3 + b = 1$$

Case 2.2: if $b_1 = b_3 \neq b_2$

Case 2.2.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 1$$
$$p_3 = b_2 + b_3 = 1$$

Case 2.2.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 0$$
$$p_3 = b_2 + b_3 + b = 0$$

Anonymous Broadcasting

We know $p_1 = 0$ and $p_3 = 0$. We are in Case 2.1.1 or 2.2.2. But we don't know which without b_3

Assume $b = 1$ and that P_2 is NOT the broadcaster

Case 2: if $b_1 \neq b_2$:

Case 2.1: if $b_1 \neq b_2 = b_3$

Case 2.1.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 0$$
$$p_3 = b_2 + b_3 = 0$$

Case 2.1.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 1$$
$$p_3 = b_2 + b_3 + b = 1$$

Case 2.2: if $b_1 = b_3 \neq b_2$

Case 2.2.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 1$$
$$p_3 = b_2 + b_3 = 1$$

Case 2.2.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 0$$
$$p_3 = b_2 + b_3 + b = 0$$

Anonymous Broadcasting

We know $p_1 = 1$ and $p_3 = 1$. We are in Case 2.1.2 or 2.2.1. But we don't know which without b_3

Assume $b = 1$ and that P_2 is NOT the broadcaster

Case 2: if $b_1 \neq b_2$:

Case 2.1: if $b_1 \neq b_2 = b_3$

Case 2.1.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 0$$
$$p_3 = b_2 + b_3 = 0$$

Case 2.1.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 1$$
$$p_3 = b_2 + b_3 + b = 1$$

Case 2.2: if $b_1 = b_3 \neq b_2$

Case 2.2.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 1$$
$$p_3 = b_2 + b_3 = 1$$

Case 2.2.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 0$$
$$p_3 = b_2 + b_3 + b = 0$$

Anonymous Broadcasting

If we are in Case 1.1 or Case 2.2 then we can determine b_3 but we cannot determine who broadcasted.

Assume $b = 0$ and that P_2 is NOT the broadcaster

Case 1: if $b_1 = b_2$:

Case 1.1: if $b_1 = b_2 = b_3$

Case 1.1.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 = 0$$
$$p_3 = b_2 + b_3 = 0$$

Case 1.1.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 0$$
$$p_3 = b_2 + b_3 = 0$$

Case 1.2: if $b1 = b_2 \neq b_3$

Case 1.2.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 = 1$$
$$p_3 = b_2 + b_3 = 1$$

Case 1.2.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 1$$
$$p_3 = b_2 + b_3 = 1$$

Anonymous Broadcasting

If p_1 and p_3 are 0, then $b_1 = b_2 = b_3$, but since $b = 0$ we don't know if we are in Case 1.1.1 or 1.1.2

Assume $b = 0$ and that P_2 is NOT the broadcaster

Case 1: if $b_1 = b_2$:

Case 1.1: if $b_1 = b_2 = b_3$

Case 1.1.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 0$$
$$p_3 = b_2 + b_3 = 0$$

Case 1.1.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 0$$
$$p_3 = b_2 + b_3 + b = 0$$

Case 1.2: if $b1 = b_2 \neq b_3$

Case 1.2.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 = 1$$
$$p_3 = b_2 + b_3 = 1$$

Case 1.2.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 1$$
$$p_3 = b_2 + b_3 = 1$$

Anonymous Broadcasting

Assume $b = 0$ and that P_2 is NOT the broadcaster

Case 1: if $b_1 = b_2$:

Case 1.1: if $b_1 = b_2 = b_3$

Case 1.1.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 = 0$$
$$p_3 = b_2 + b_3 = 0$$

Case 1.1.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 0$$
$$p_3 = b_2 + b_3 = 0$$

If p_1 and p_3 are 1, then $b_1 = b_2 \neq b_3$, but since $b = 0$ we don't know if we are in Case 1.2.1 or 1.2.2

Case 1.2: if $b1 = b_2 \neq b_3$

Case 1.2.1: if P_1 broadcasts, then

$$p_1 = b_1 + b_3 + b = 1$$
$$p_3 = b_2 + b_3 = 1$$

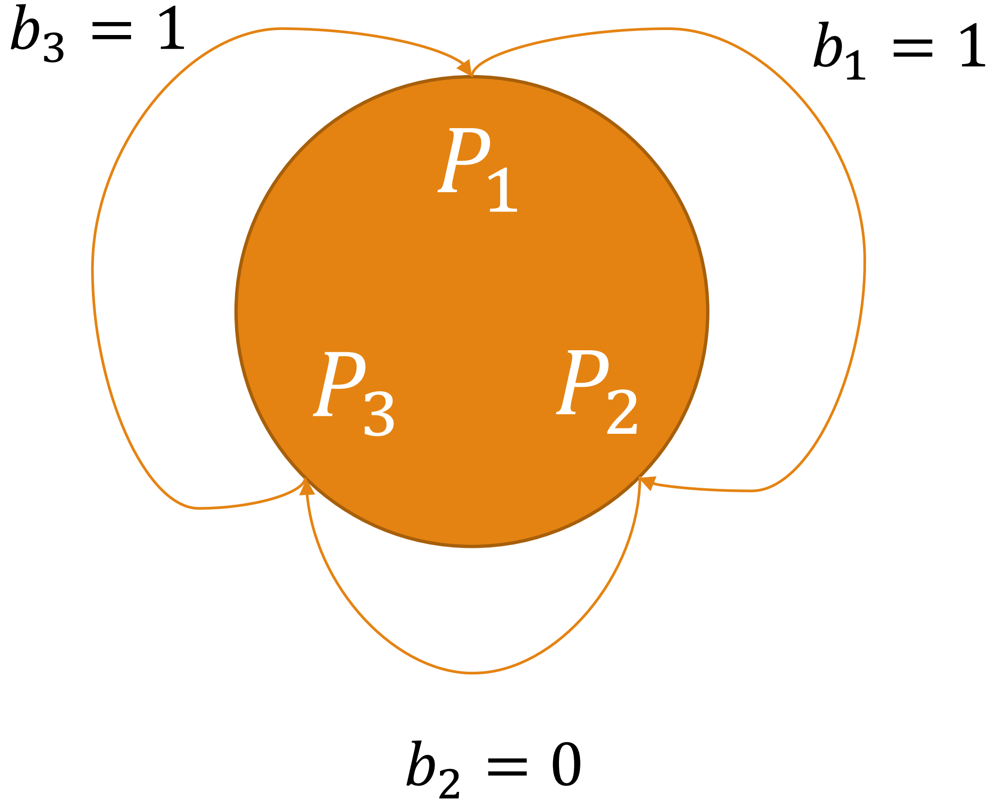
Case 1.2.2: if P_3 broadcasts, then

$$p_1 = b_1 + b_3 = 1$$
$$p_3 = b_2 + b_3 + b = 1$$

Anonymous Broadcasting

$$p_1 + p_2 + p_3 + b$$
$$= 0 + 1 + 1 + 1$$
$$= 1$$

This process must be repeated for every bit in order to transmit a longer string.



Probability

Sample space S is a non-empty set.

Outcome: an element of S.

Ex. Flip a coin, $S = \{H, T\}$ is the **Sample space.**

H and T are **Outcomes**.

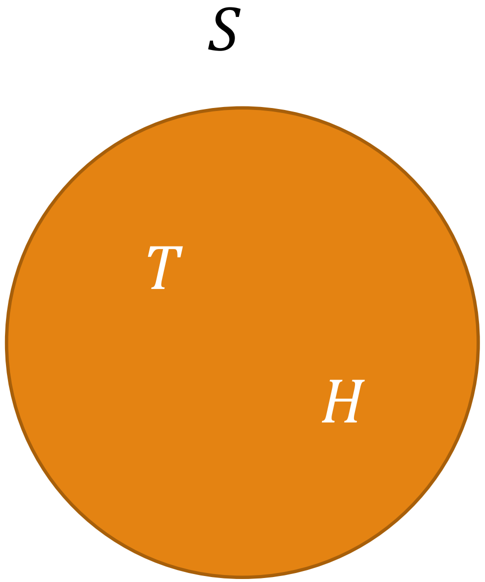
A **Probability function** $\mathrm{Pr}: S \rightarrow \mathbb{R}$

1. $\forall\, w \in S: 0 \leq \mathrm{Pr}(w) \leq 1$
2. $\sum_{w \in S} \mathrm{Pr}(w) = 1$

probability that outcome is w

The **Probability Function** assigns a real number to each element of S. All of these numbers summed must equal 1.

If we select an element (outcome) “at random”, we do so with the probability defined by Pr



Probability

Sample space S is a non-empty set.

Outcome: an element of S.

Ex. Flip a coin, $S = \{H, T\}$ is the **Sample space.**

H and T are **Outcomes**.

A **Probability function** $\Pr: S \rightarrow \mathbb{R}$

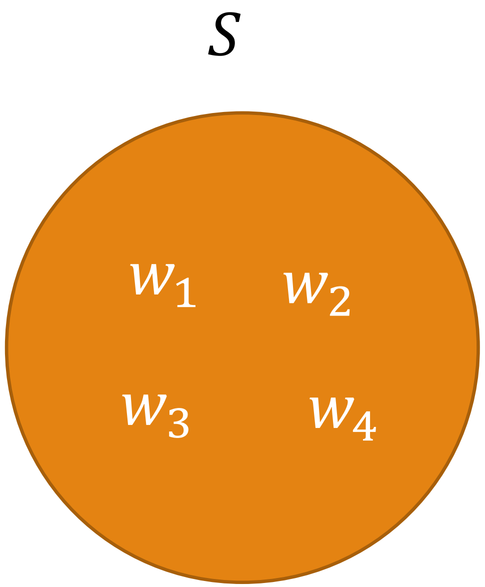
1. $\forall\, w \in S: 0 \leq \Pr(w) \leq 1$
2. $\sum_{w \in S} \Pr(w) = 1$

probability that outcome is w

The **Probability Function** assigns a real number to each element of S. All of these numbers summed must equal 1.

If we select an element (outcome) "at random", we do so with the probability defined by Pr

$$\Pr(w_1) = 0.3$$
$$\Pr(w_2) = 0.25$$
$$\Pr(w_3) = 0.2$$
$$\Pr(w_4) = 0.25$$
$$\overline{}$$
$$1$$



Probability

Flip a coin, $S = \{H, T\}$.

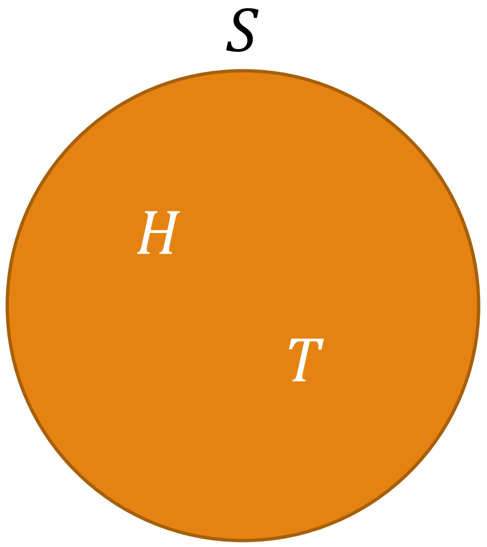
If the coin is fair:

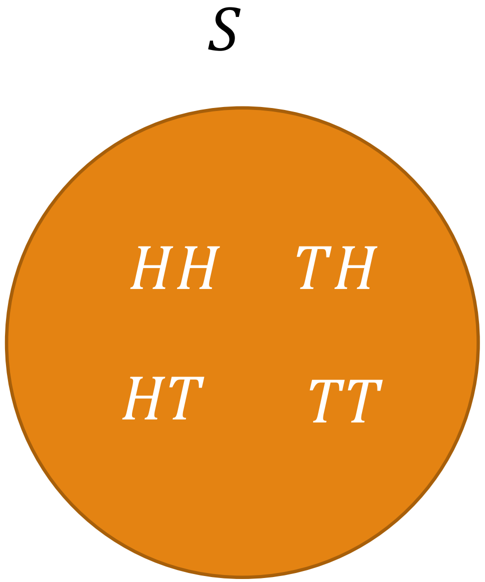
$$\left.\begin{array}{l} \Pr(H) = \frac{1}{2} \\ \Pr(T) = \frac{1}{2} \end{array}\right\} \quad \Pr(H) + \Pr(T) = 1$$

Flip a fair coin twice:
$S = \{HH, HT, TH, TT\}$

Each outcome may happen with equal probability

$\Pr(HH) = \Pr(HT) = \Pr(TH) = \Pr(TT) = 1/4$





Events

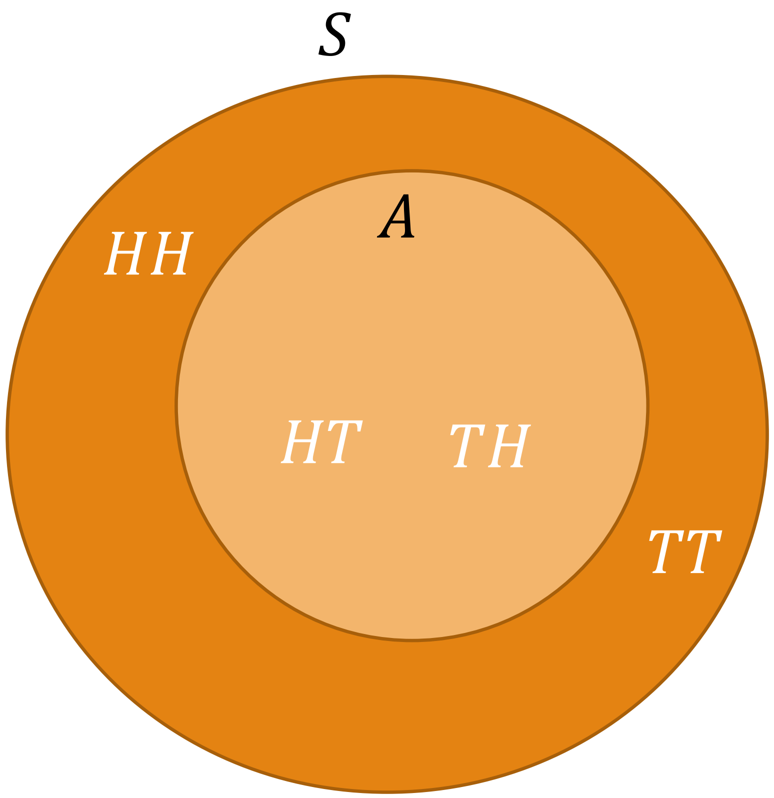
An **Event** $A, A \subseteq S$

An **Event** is a **subset** of the **sample space.**

$A =$ "One head, one tail"

The probability of an **Event** is the sum of the probabilities of each of the **outcomes** in the **Event.**

$$\Pr(A) = \sum_{w \in A} \Pr(w)$$



Events

An **Event** $A, A \subseteq S$

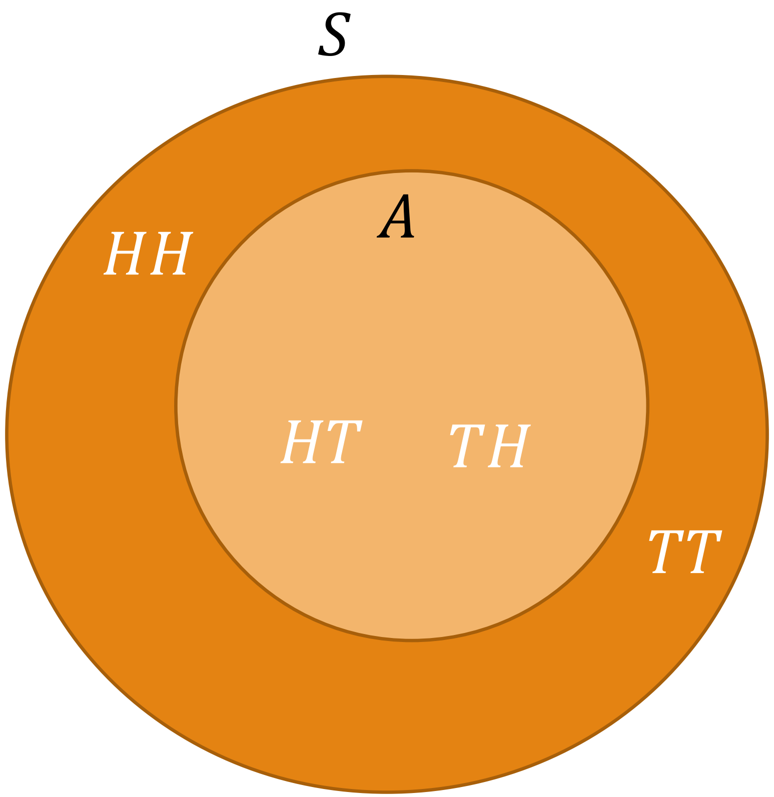
$$\Pr(A) = \sum_{w \in A} \Pr(w)$$

Experiment: Flip a fair coin twice

The **Event** $A =$ "One head, one tail"

$S = \{HH, HT, TH, TT\}$
$A = \{HT, TH\}$

$$\Pr(A) = \Pr(HT) + \Pr(TH) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$



Probability

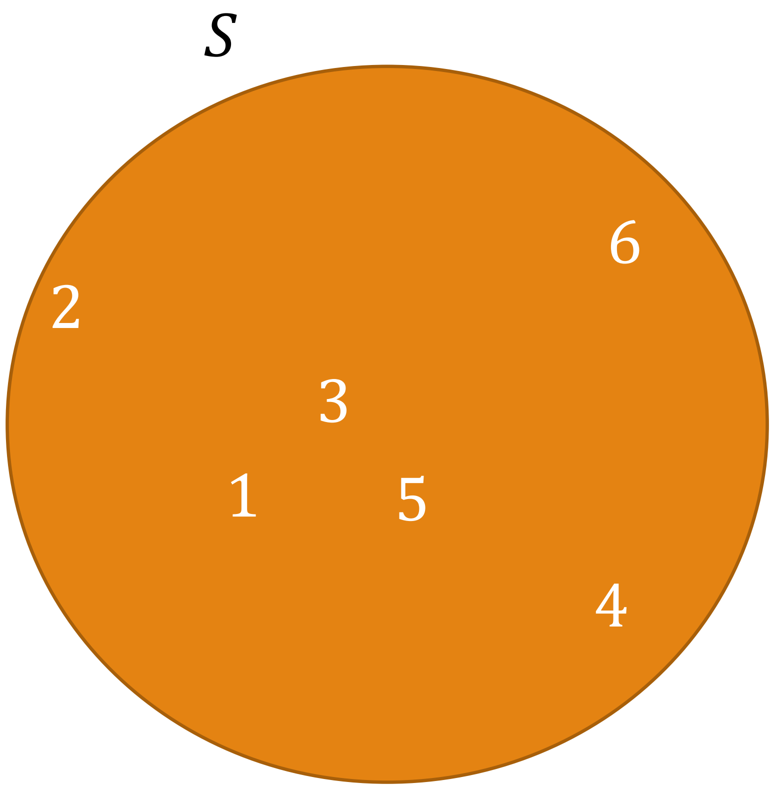
Roll a fair die:

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

$$\Pr(1) = \Pr(2) = \cdots = \Pr(6) = \frac{1}{6}$$

$$\frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = 1$$

$$\sum_{i \in \{1..6\}} \Pr(i) = 1$$



Probability

Roll a fair die

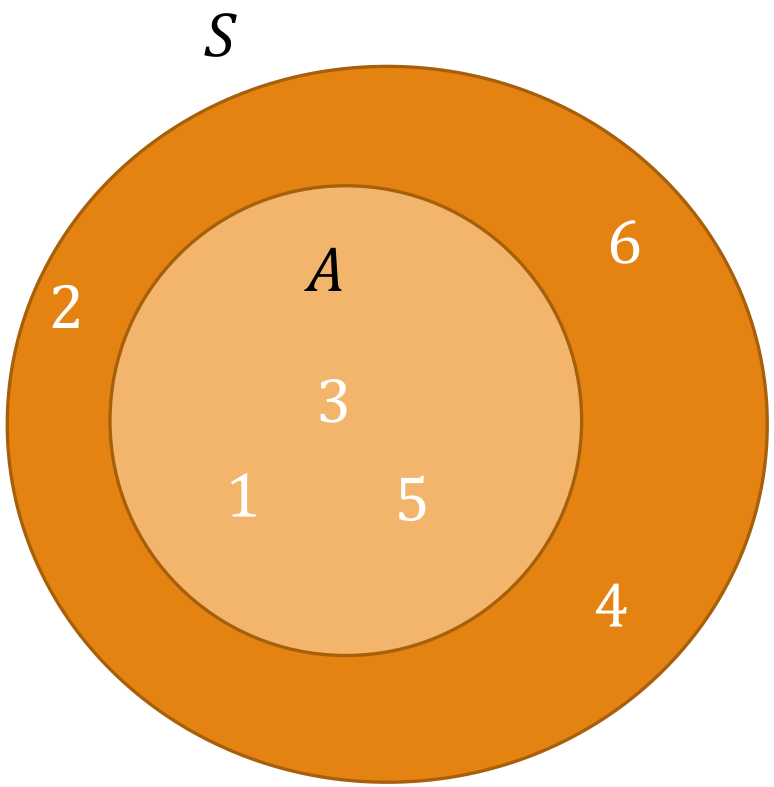
$$S = \{1, 2, 3, 4, 5, 6\}$$

$$\Pr(1) = \Pr(2) = \cdots = \Pr(6) = \frac{1}{6}$$

Define an **Event** $A =$ “We rolled an odd number"

Event $A =$ "Odd number" $= \{1, 3, 5\}$

The probability of an **Event** A is the sum of the probabilities of the individual **Outcomes** in A



Probability

Roll a fair die

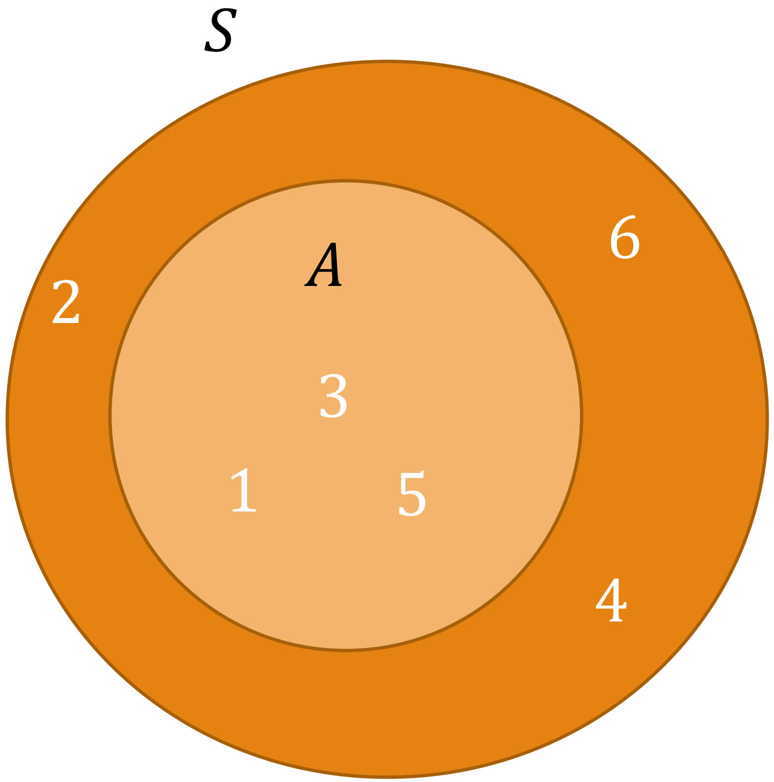
$$S = \{1, 2, 3, 4, 5, 6\}$$

$$\Pr(1) = \Pr(2) = \cdots = \Pr(6) = \frac{1}{6}$$

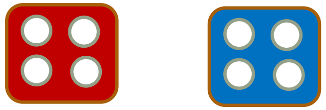
Define an **Event** A = "We rolled an odd number"

Event A = "Odd number" $= \{1, 3, 5\}$

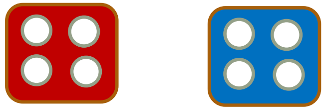
$$\Pr(A) = \Pr(1) + \Pr(3) + \Pr(5)$$
$$= \frac{1}{6} + \frac{1}{6} + \frac{1}{6}$$
$$= \frac{1}{2}$$



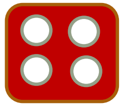
Probability

Roll a red die and a blue die. 

$$S = \{\ (i,j) \mid 1 \le i \le 6, 1 \le j \le 6\ \}$$

i = red die , j = blue die 

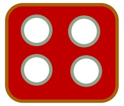
What is the size of the sample space?
(Hint: Product rule)

6 choices for  , 6 choices for  ,
$6 \cdot 6 = 36$ numbers. What is the Pr of each outcome?

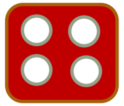
$$\Pr(i,j) = \frac{1}{36}$$

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

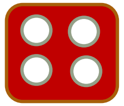
Probability

Roll a red die and a blue die.  

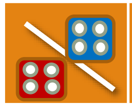
$$S = \{\, (i, j) \mid 1 \le i \le 6, 1 \le j \le 6 \,\}$$

i = red die , j = blue die  

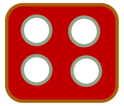
What is the size of the sample space?
(Hint: Product rule)

6 choices for  , 6 choices for  ,
$6 \cdot 6 = 36$ numbers. What is the Pr of each outcome?

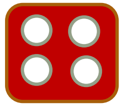
$$\Pr(i, j) = \frac{1}{36}$$

	**1**	**2**	**3**	**4**	**5**	**6**
1	1,1	1,2	1,3	1,4	1,5	1,6
2	2,1	2,2	2,3	2,4	2,5	2,6
3	3,1	3,2	3,3	3,4	3,5	3,6
4	4,1	4,2	4,3	4,4	4,5	4,6
5	5,1	5,2	5,3	5,4	5,5	5,6
6	6,1	6,2	6,3	6,4	6,5	6,6

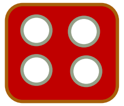
Probability

Roll a red die and a blue die.  

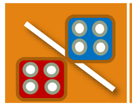
$$S = \{\ (i, j)\ |\ 1 \le i \le 6, 1 \le j \le 6\ \}$$

i = red die , j = blue die  

What is the size of the sample space?
(Hint: Product rule)

6 choices for  , 6 choices for  ,
$6 \cdot 6 = 36$ numbers. What is the Pr of each outcome?

$$\Pr(i, j) = \frac{1}{36}$$

	1	2	3	4	5	6
1	1,1	1,2	1,3	1,4	1,5	1,6
2	2,1	2,2	2,3	2,4	2,5	2,6
3	3,1	3,2	3,3	3,4	3,5	3,6
4	4,1	4,2	4,3	4,4	4,5	4,6
5	5,1	5,2	5,3	5,4	5,5	5,6
6	6,1	6,2	6,3	6,4	6,5	6,6

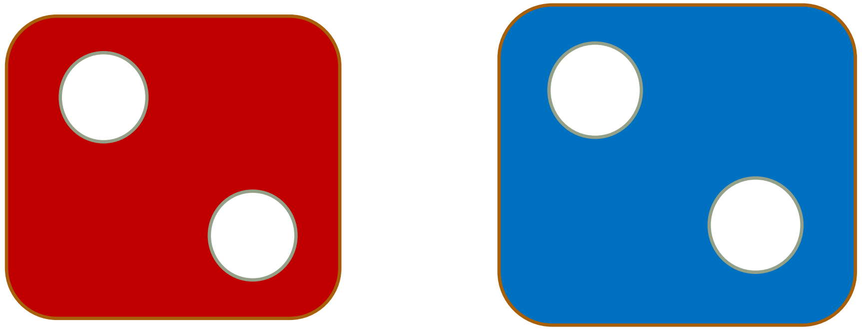
Probability

Event A $=$ "sum of red and blue is 4"

$$= \{\ (1{,}3), (2{,}2), (3{,}1)\ \}$$

$$\Pr(A) = \Pr(1{,}3) + \Pr(2{,}2) + \Pr(3{,}1)$$

$$= \frac{3}{36} = \frac{1}{12}$$



	1	2	3	4	5	6
1	1,1	1,2	1,3	1,4	1,5	1,6
2	2,1	2,2	2,3	2,4	2,5	2,6
3	3,1	3,2	3,3	3,4	3,5	3,6
4	4,1	4,2	4,3	4,4	4,5	4,6
5	5,1	5,2	5,3	5,4	5,5	5,6
6	6,1	6,2	6,3	6,4	6,5	6,6

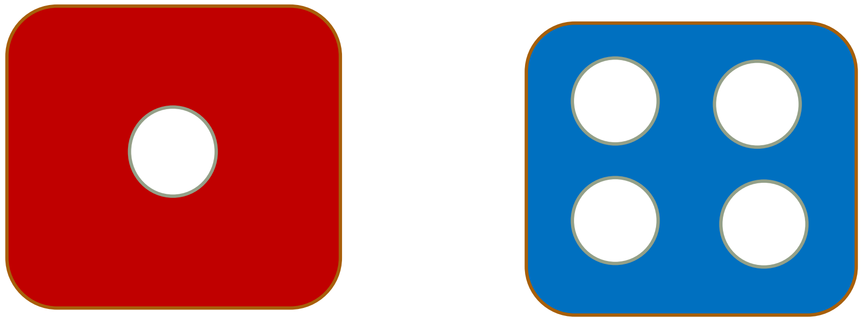
Probability

Event A = "sum of red and blue is 4"

$= \{ (1,3), (2,2), (3,1) \}$
$\Pr(A) = \Pr(1,3) + \Pr(2,2) + \Pr(3,1)$
$= \frac{3}{36} = \frac{1}{12}$

Event B = "sum is 5"
$= \{(1,4), (2,3), (3,2), (4,1)\}$

$\Pr(B)$
$= \Pr(1,4) + \Pr(2,3) + \Pr(3,2) + \Pr(4,1)$
$= \frac{4}{36} = \frac{1}{9}$



	1	2	3	4	5	6
1	1,1	1,2	1,3	1,4	1,5	1,6
2	2,1	2,2	2,3	2,4	2,5	2,6
3	3,1	3,2	3,3	3,4	3,5	3,6
4	4,1	4,2	4,3	4,4	4,5	4,6
5	5,1	5,2	5,3	5,4	5,5	5,6
6	6,1	6,2	6,3	6,4	6,5	6,6

Probability

Event $A, A \subseteq S$

$$\Pr(A) = \sum_{w \in A} \Pr(w)$$

We know that $S \subseteq S$,
Thus S is an event and

$$\Pr(S) = \sum_{w \in S} \Pr(w) = 1$$

"What is the probability that something (anything) happens?"

S

Probability

We have to select something because of how we defined “outcome”.

Event $A, A \subseteq S$

$$\Pr(A) = \sum_{w \in A} \Pr(w)$$

Also $\emptyset$ is an event

And $\Pr(\emptyset) = 0$

"What is the probability of an impossible outcome?“

S

Probability

Event $A, A \subseteq S$

$$\Pr(A) = \sum_{w \in A} \Pr(w)$$

What is $\Pr(\bar{A})$?

$\bar{A} \subseteq S$ is a subset of S and thus an event.

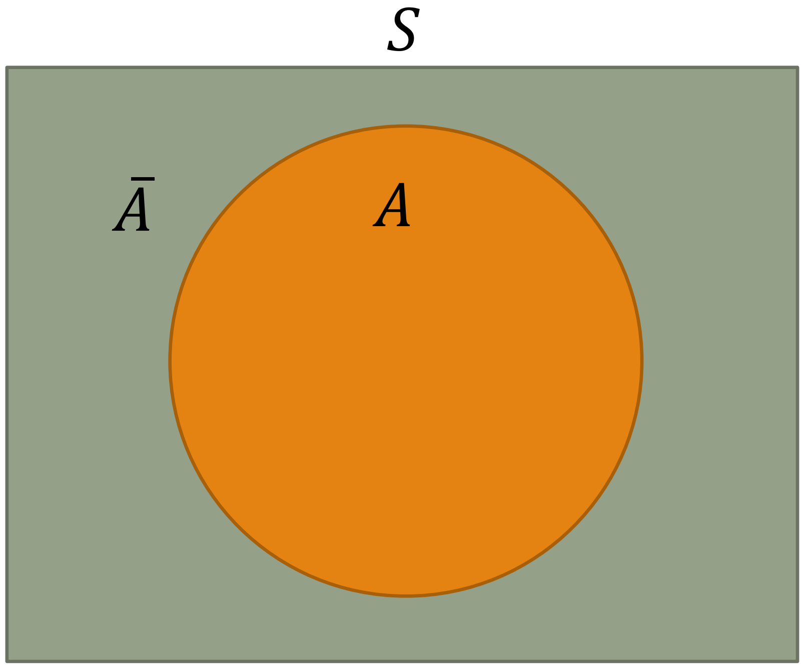
We can use what we know of A to determine it.
Since $A \cup \bar{A} = S$,

$$\Pr(A) + \Pr(\bar{A}) = \Pr(S) = 1$$

Thus $\Pr(\bar{A}) = 1 - \Pr(\mathrm{A})$

Complement Rule: $\Pr(A) = 1 - \Pr(\bar{A})$

As with counting, sometimes it is easier to compute the $\Pr$ of the complement



Probability

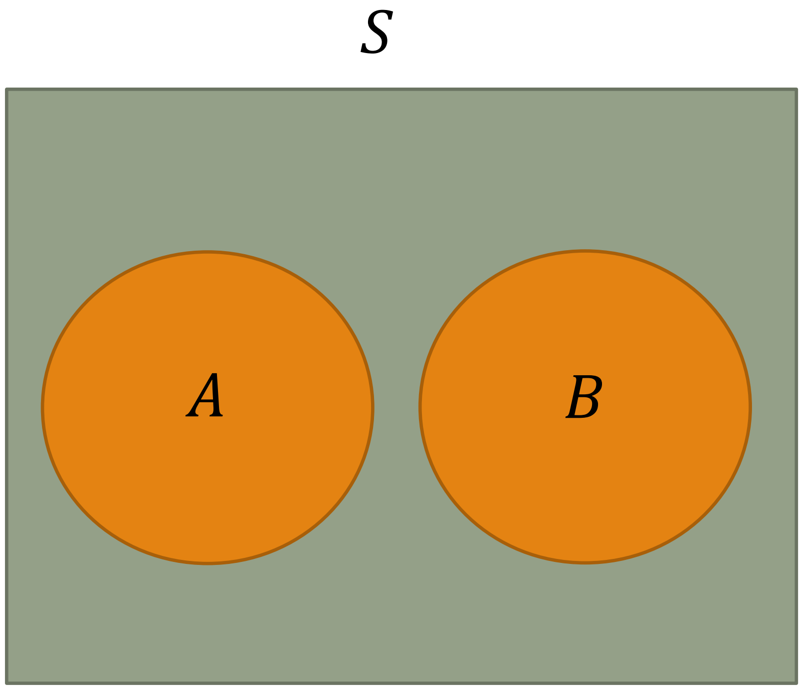
Event A, B **disjoint** sets.

$\Pr(A) = \sum_{w \in A} \Pr(w)$
$\Pr(B) = \sum_{w \in B} \Pr(w)$

We can define an event $A \cup B$, and thus:

$$\Pr(A \cup B) = \Pr(A) + \Pr(B)$$

Equivalent of sum rule of counting, but now each element has a value ($\Pr$) associated with it.



Probability

Events A, B **NOT disjoint** sets.

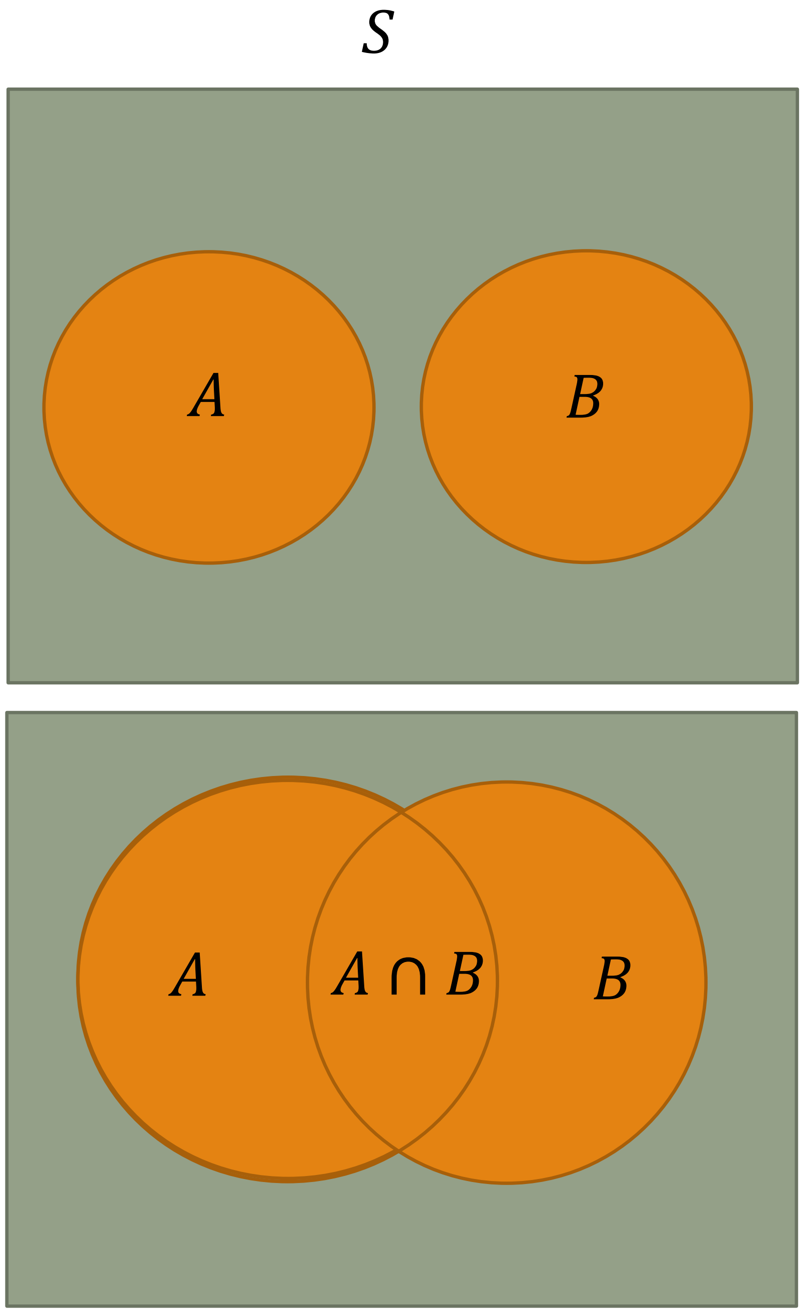
To count the elements:

$$|A \cup B| = |A| + |B| - |A \cap \mathrm{B}|$$

Instead of counting elements, we are counting the probabilities, and thus:

$$\Pr(A \cup B) = \Pr(A) + \Pr(B) - \Pr(A \cap B)$$

Similar to inclusion / exclusion



Example

$S = \{1,2,\ldots,1000\}$, $\Pr(i) = \frac{1}{1000}$

Choose a random element x in S.

What is $\Pr(x$ is divisible by 2 or 3)?

$A =$ "div by 2", $B =$ "div by 3"

$\Pr(A) + \Pr(B) - \Pr(A \cap B)$

$$= \frac{500}{1000} + \frac{333}{1000} - \Pr(div\ by\ 6)$$
$$= \frac{500}{1000} + \frac{333}{1000} - \frac{166}{1000} = \frac{667}{1000}$$