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, but we are going to redefine everything from first principles.

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.

Group of people on a network.

We want anyone to be able to broadcast

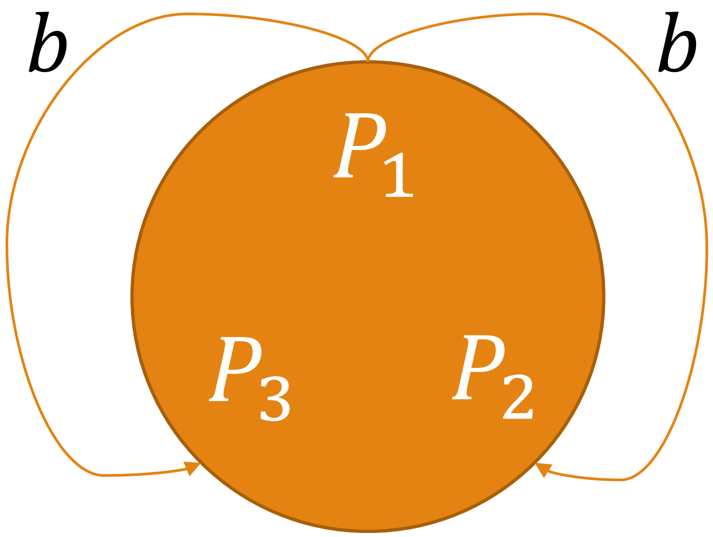
1. One person broadcasts message
2. Everyone receives message
3. No one knows who sent the message

They talk in binary, so they transmit 1 bit at a time (a 0 or a 1).

Three people, P_1, P_2, P_3

One of them broadcasts bit b (0 or 1).

Anonymous Broadcasting



Three people, P_1, P_2, P_3, on a network

1. One person broadcasts message
2. Everyone receives message
3. No one knows who sent the message

They transmit 1 bit at a time.

One of them broadcasts bit b (0 or 1),
and we want to *hide* who sent it

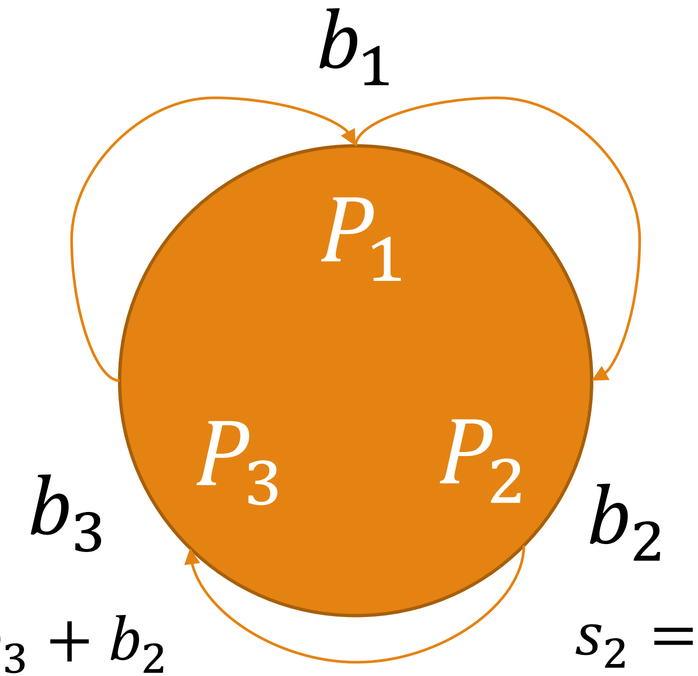
Anonymous Broadcasting

Problem: P_1, P_2, P_3 on a network. One broadcasts bit b (0 or 1). We want to hide who did it.

1. Every person flips a coin – Person P_i has a random bit b_i
2. Each P_i shows b_i to their clockwise neighbour
3. P_1 computes $s_1 = (b_1 + b_3)\ mod\ 2$
   P_2 computes $s_2 = (b_1 + b_2)\ mod\ 2$
   P_3 computes $s_3 = (b_2 + b_3)\ mod\ 2$
4. If P_i is not the broadcaster, $t_i = s_i$
   If P_i is the broadcaster, $t_i = (s_i + b)$ mod 2
5. Each P_i shows t_i to everyone
6. Each P_i computes $(t_1 + t_2 + t_3)\ mod\ 2$
7. $= (s_1 + s_2 + s_3 + b)\ mod\ 2 = (b_1 + b_1 + b_2 + b_2 + b_3 + b_3 + b)\ mod\ 2 = b\ mod\ 2 = b$

$t_1 = s_1$

$s_1 = b_1 + b_3$



$s_3 = b_3 + b_2$

$t_3 = s_3 + b$

$s_2 = b_1 + b_2$

$t_2 = s_2$

Anonymous Broadcasting

Three people, P_1, P_2, P_3.
P_2 is the broadcaster and wants to broadcast $b = 1$.
Each P_i flips a coin, stores result in b_i.

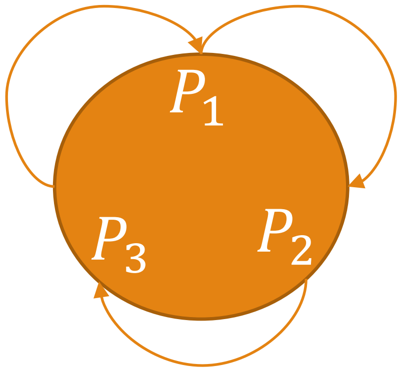
P_1 computes $s_1 = (b_1 + b_3)\ mod\ 2$
P_2 computes $s_2 = (b_1 + b_2)\ mod\ 2$
P_3 computes $s_3 = (b_2 + b_3)\ mod\ 2$

P_1 is not the broadcaster, so $t_1 = s_1$
P_2 is not the broadcaster, so $t_2 = s_2$
P_3 is the broadcaster, so $t_3 = s_3 + b\ mod\ 2$

Everyone broadcasts t_i, and everyone computes $t_1 + t_2 + t_3\ mod\ 2$ which reveals the bit $b = 1$

$$b_3 = 1$$
$$s_3 = b_3 + b_2 = 1$$
$$t_3 = s_3 + (b = 1) = 0$$

$$b_1 = 1$$
$$s_1 = b_1 + b_3 = 0$$
$$t_1 = s_1 = 0$$



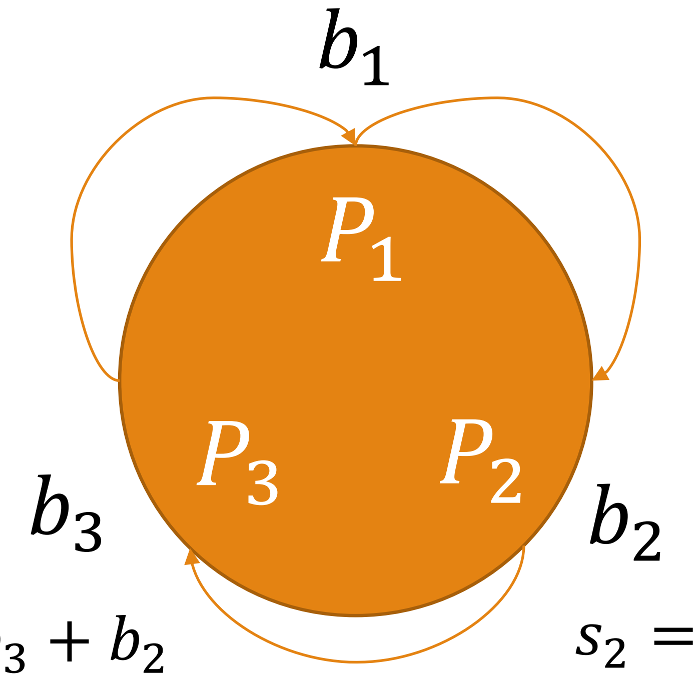
$$t_1 + t_2 + t_3$$
$$= 0 + 1 + 0$$
$$= 1$$
$$= b$$

$$b_2 = 0$$
$$s_2 = b_2 + b_1 = 1$$
$$t_2 = s_2 = 1$$

Anonymous Broadcasting

$t_1 = s_1$

$s_1 = b_1 + b_3$



$s_3 = b_3 + b_2$

$t_3 = s_3 + b$

$s_2 = b_1 + b_2$

$t_2 = s_2$

Each P_i computes

$$(t_1 + t_2 + t_3)\ mod\ 2$$

$$= (s_1 + s_2 + s_3 + b)\ mod\ 2$$

$$= (\underbrace{b_1 + b_1}_{0} + \underbrace{b_2 + b_2}_{0} + \underbrace{b_3 + b_3}_{0} + b)\ mod\ 2$$

$$+b = b$$

$$= b\ mod\ 2 = b$$

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 $1 + 1\ mod\ 2 = 2\ mod\ 2 = 0$

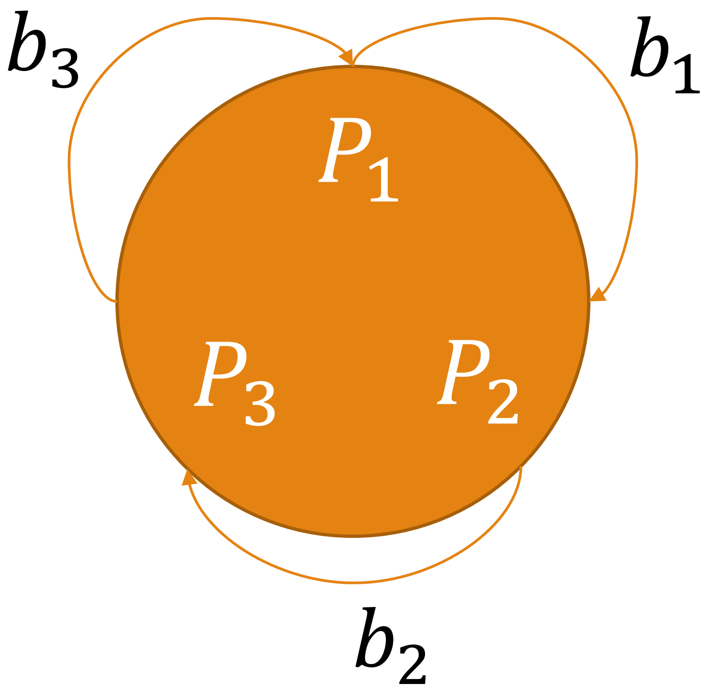
Thus $b_1 + b_1$, $b_2 + b_2$, $and\ b_3 + b_3$ all cancel out, leaving b.

Anonymous Broadcasting

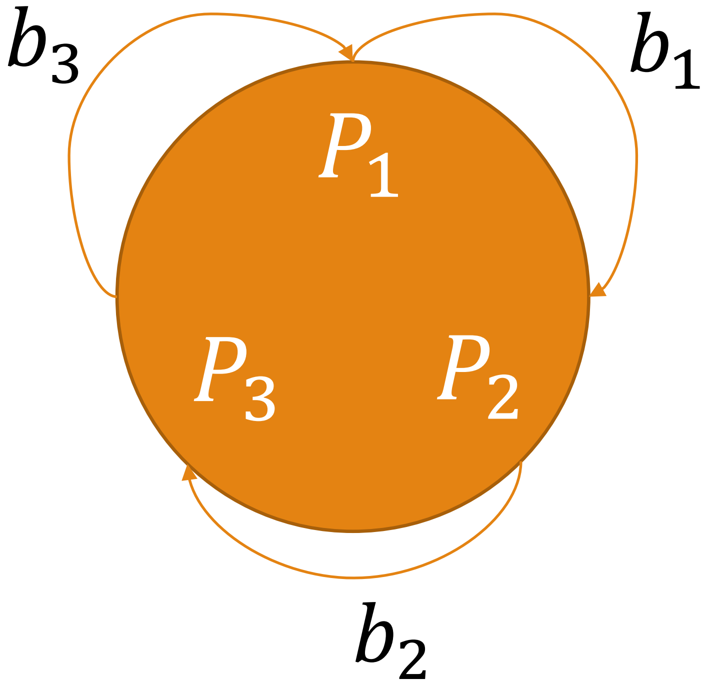
(Hopefully) we are convinced we can broadcast in this way and each person can extract b.

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.



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 s_1, s_2, s_3 and we know b.

$$s_2 = b_1 + b_2$$
$$s_1 = b_1 + \boxed{b_3 + (\text{perhaps } b)}$$
$$s_3 = b_2 + \boxed{b_3 + (\text{perhaps } b)}$$

unknown

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 $b1 = b_2 = b_3$

Case 1.1.1: if P_1 broadcasts, then

$t_1 = b_1 + b_3 + b = 1$

$t_3 = b_2 + b_3 = 0$

Case 1.1.2: if P_3 broadcasts, then

$t_1 = b_1 + b_3 = 0$

$t_3 = b_2 + b_3 + b = 1$

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

Case 1.2.1: if P_1 broadcasts, then

$t_1 = b_1 + b_3 + b = 0$

$t_3 = b_2 + b_3 = 1$

Case 1.2.2: if P_3 broadcasts, then

$t_1 = b_1 + b_3 = 1$

$t_3 = b_2 + b_3 + b = 0$

Anonymous Broadcasting

For example, we know $t_1 = 0$ and $t_3 = 1$. 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 $b1 = b_2 = b_3$

Case 1.1.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 + b = 1$$
$$t_3 = b_2 + b_3 = 0$$

Case 1.1.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 + b = 1$$

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

Case 1.2.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 + b = 0$$
$$t_3 = b_2 + b_3 = 1$$

Case 1.2.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 + b = 0$$

Anonymous Broadcasting

Or we know $t_1 = 1$ and $t_3 = 0$. 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

$$t_1 = b_1 + b_3 + b = 1$$
$$t_3 = b_2 + b_3 = 0$$

Case 1.1.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 + b = 1$$

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

Case 1.2.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 + b = 0$$
$$t_3 = b_2 + b_3 = 1$$

Case 1.2.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 + b = 0$$

Anonymous Broadcasting

P_2 knows if they are in Case 2, but $s_1 = s_3$ 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 $b1 \neq b_2 = b_3$

Case 2.1.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 + b = 0$$
$$t_3 = b_2 + b_3 = 0$$

Case 2.1.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 + b = 1$$

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

Case 2.2.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 + b = 1$$
$$t_3 = b_2 + b_3 = 1$$

Case 2.2.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 + b = 0$$

Anonymous Broadcasting

We know
$t_1 = 0$ and $t_3 = 0$. 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 $b1 \neq b_2 = b_3$

Case 2.1.1: if P_1 broadcasts, then
$$t_1 = b_1 + b_3 + b = 0$$
$$t_3 = b_2 + b_3 = 0$$

Case 2.1.2: if P_3 broadcasts, then
$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 + b = 1$$

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

Case 2.2.1: if P_1 broadcasts, then
$$t_1 = b_1 + b_3 + b = 1$$
$$t_3 = b_2 + b_3 = 1$$

Case 2.2.2: if P_3 broadcasts, then
$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 + b = 0$$

Anonymous Broadcasting

We know
$t_1 = 1$ and $t_3 = 1$. 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 $b1 \neq b_2 = b_3$

Case 2.1.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 + b = 0$$
$$t_3 = b_2 + b_3 = 0$$

Case 2.1.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 + b = 1$$

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

Case 2.2.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 + b = 1$$
$$t_3 = b_2 + b_3 = 1$$

Case 2.2.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 + b = 0$$

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 $b1 = b_2 = b_3$

Case 1.1.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 = 0$$

Case 1.1.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 = 0$$

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

Case 1.2.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 = 1$$

Case 1.2.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 = 1$$

Anonymous Broadcasting

If t_1 and t_3 are 0, then $b1 = b_2 = b_3$, 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 $b1 = b_2 = b_3$

Case 1.1.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 = 0$$

Case 1.1.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 = 0$$

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

Case 1.2.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 = 1$$

Case 1.2.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 = 1$$

Anonymous Broadcasting

If t_1 and t_3 are 1, then $b1 = b_2 \neq b_3$, but since $b = 0$ we don't know if we are in Case 1.2.1 or 1.2.2

Assume $b = 0$ 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

$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 = 0$$

Case 1.1.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 0$$
$$t_3 = b_2 + b_3 = 0$$

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

Case 1.2.1: if P_1 broadcasts, then

$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 = 1$$

Case 1.2.2: if P_3 broadcasts, then

$$t_1 = b_1 + b_3 = 1$$
$$t_3 = b_2 + b_3 = 1$$

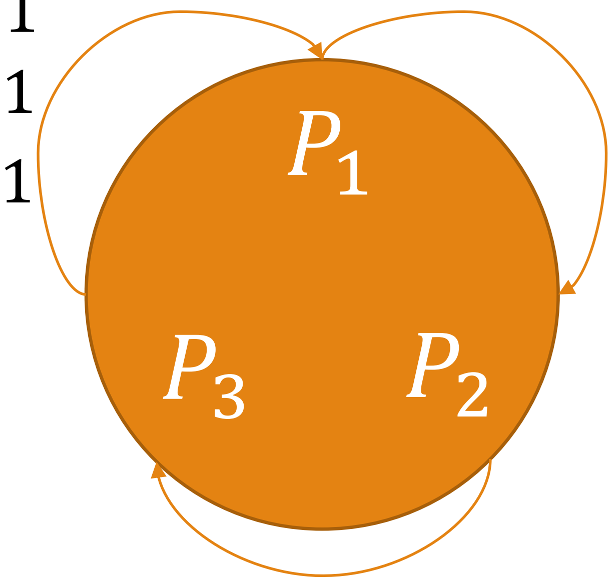
Anonymous Broadcasting

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

$$t_1 + t_2 + t_3$$
$$= 1 + 0 + 0$$
$$= 1$$

$b_3 = 1$
$s_3 = 1$
$t_3 = 1$

$b_1 = 1$
$s_1 = 0$
$t_1 = 0$



$b_2 = 0$
$s_2 = 1$
$t_2 = s_2 + (b = 1) = 0$

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**.

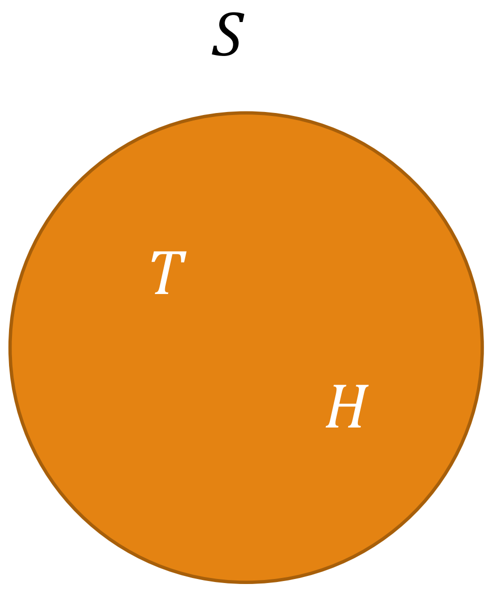
A **Probability function** $\Pr: S \rightarrow \mathbb{R}$

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



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

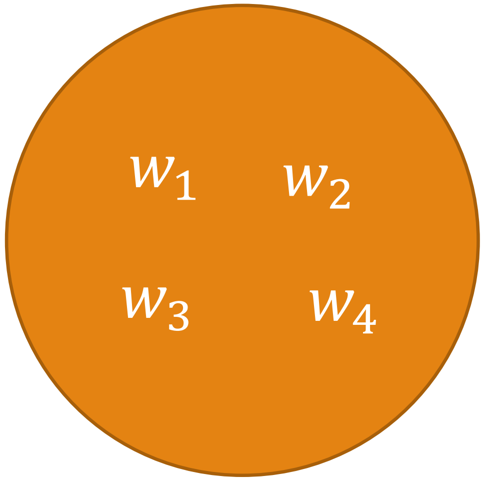
probability that outcome is w

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

S

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



Probability

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

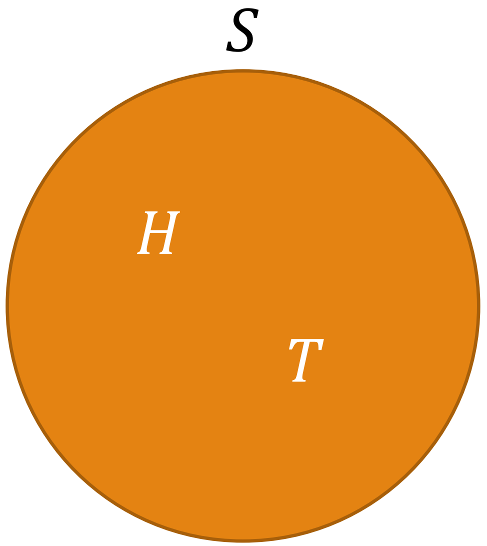
If the coin is fair:

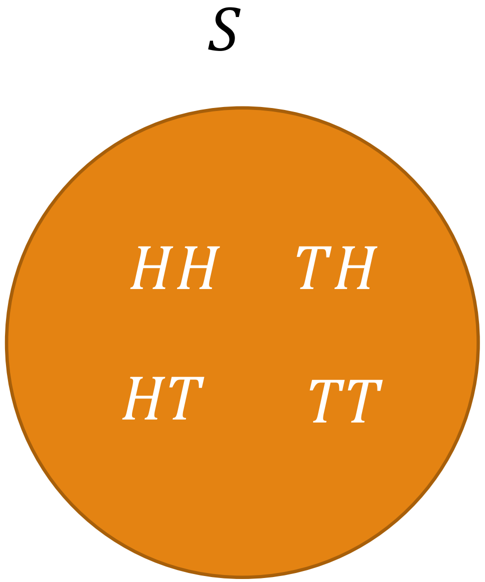
$$\left.\begin{aligned} \Pr(H) &= \frac{1}{2} \\ \Pr(T) &= \frac{1}{2} \end{aligned}\right\} \quad \Pr(H) + \Pr(T) = 1$$

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

Each outcome may happen with equal probability

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





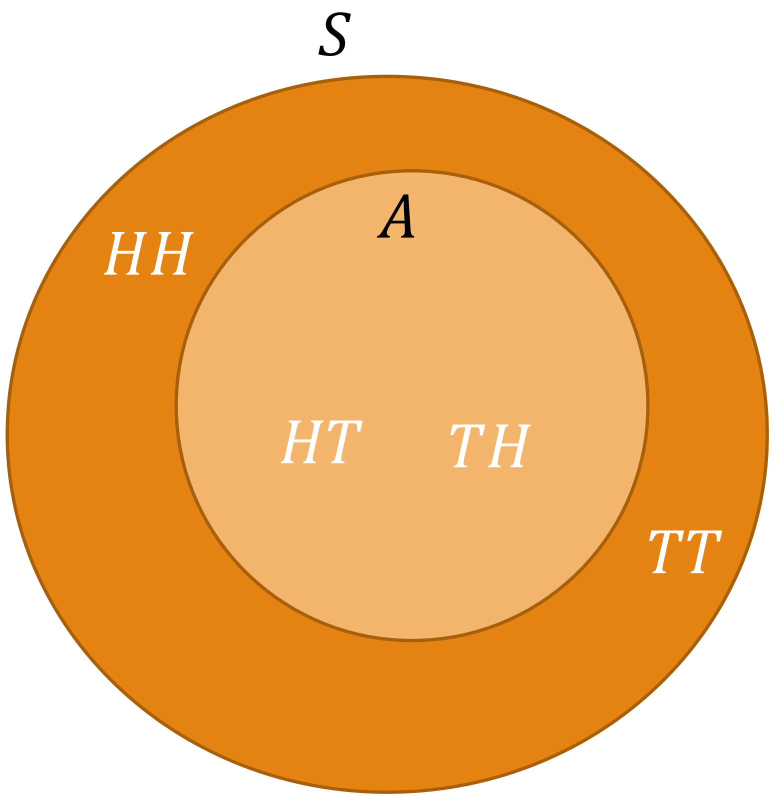
Events

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

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

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** $A, A \subseteq S$

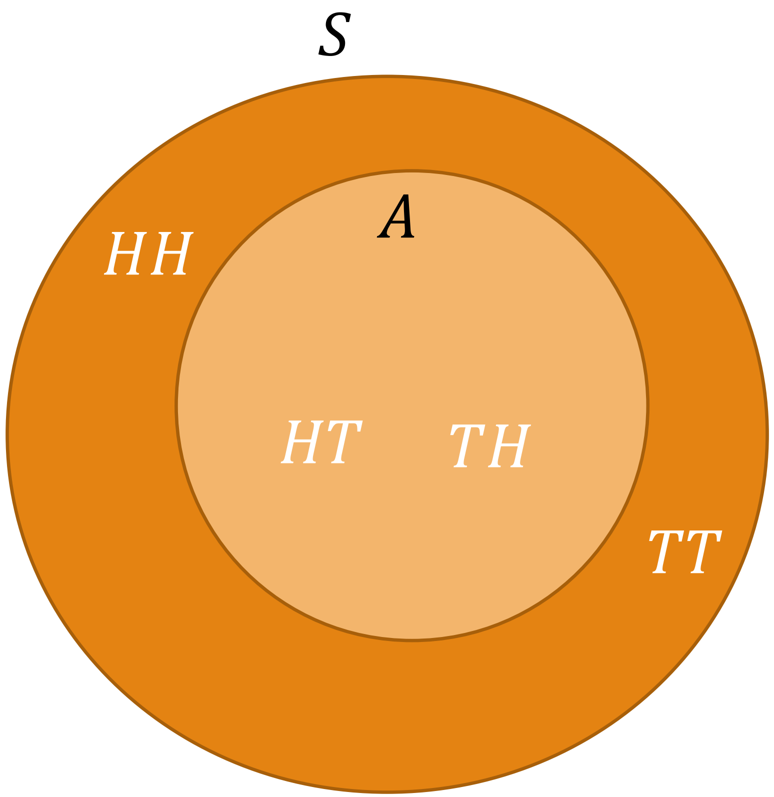
$$\Pr(A) = \sum_{w \in A} \Pr(w)$$

Flip a fair coin twice

$A =$ "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

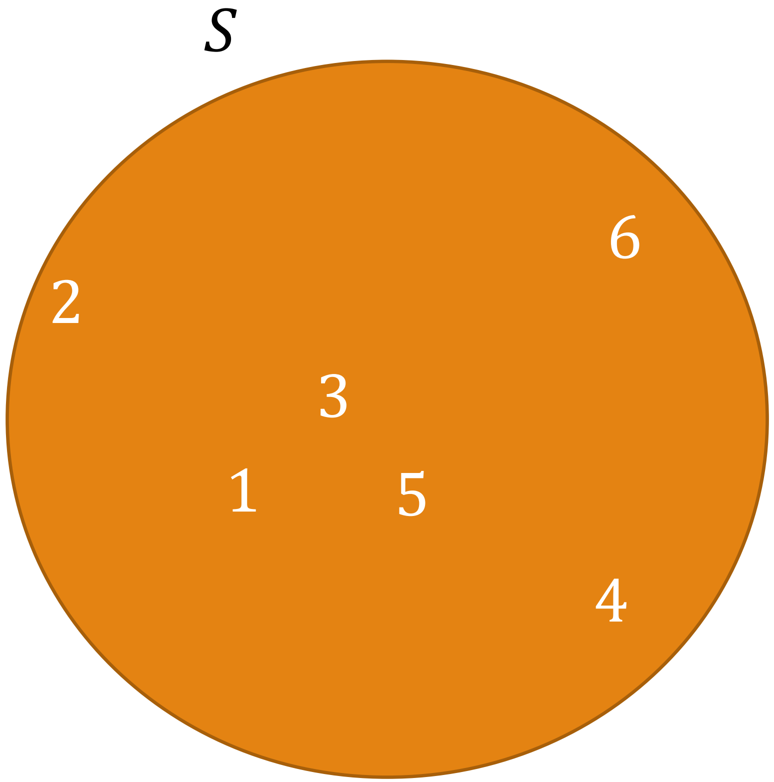
Roll a fair die:

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

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

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

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



Probability

Roll a fair die

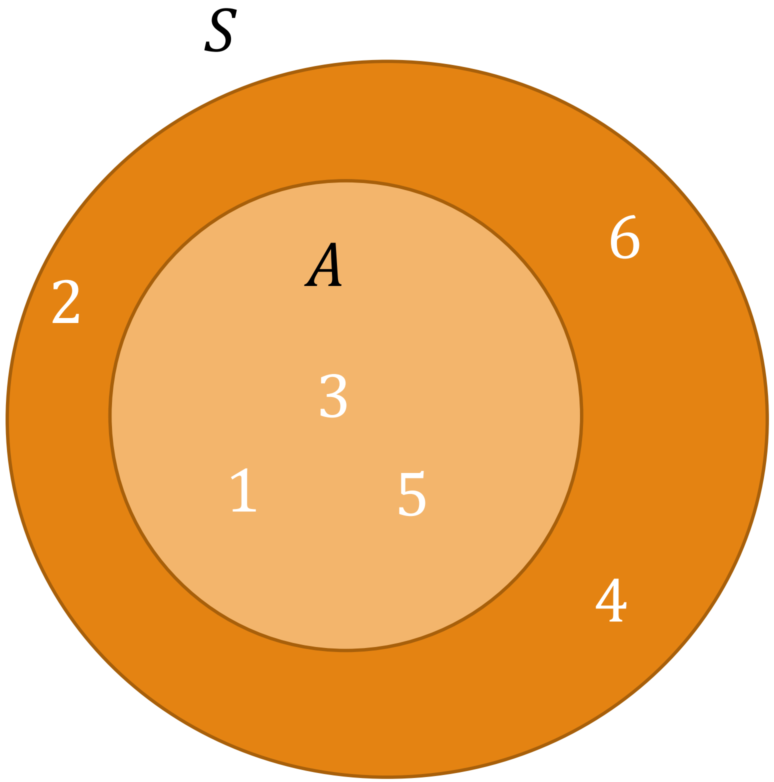
$$S = \{1, 2, 3, 4, 5, 6\}$$

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

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

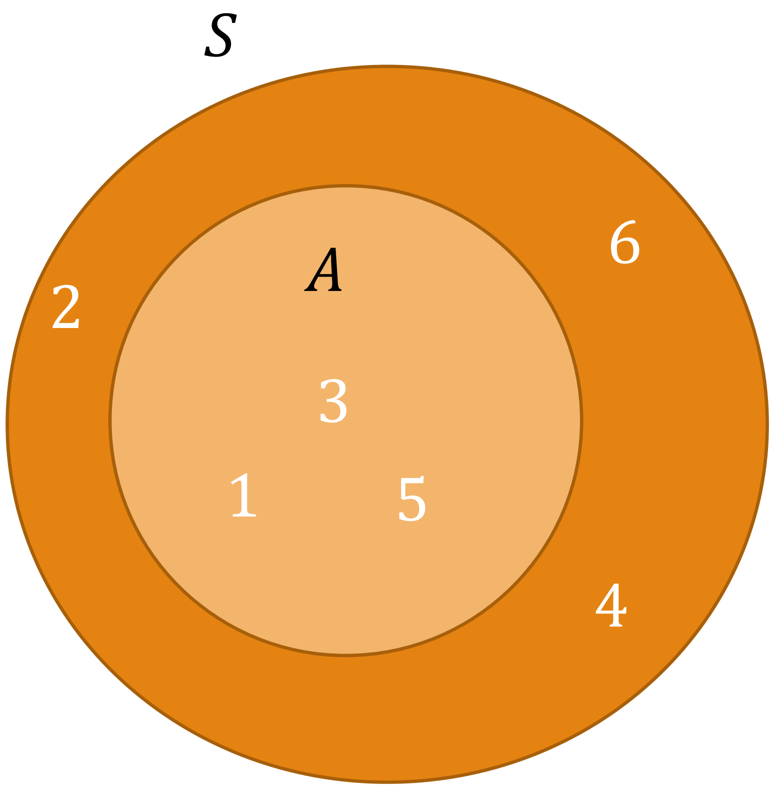
$$S = \{1, 2, 3, 4, 5, 6\}$$

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

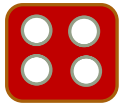
Define an **Event** A = “We rolled an odd number"

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

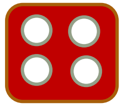
$$\Pr(A) = \Pr(1) + \Pr(3) + \Pr(5)$$
$$= \frac{1}{6} + \frac{1}{6} + \frac{1}{6}$$
$$= \frac{1}{2}$$



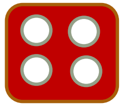
Probability

Roll a red die and a blue die.  

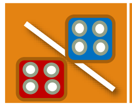
$$S = \{\ (i, j) \mid 1 \le i \le 6, 1 \le j \le 6\ \}$$

i = red die , j = blue die  

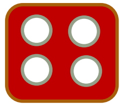
What is the size of the sample space?
(Hint: Product rule)

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

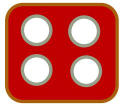
$$\Pr(i, j) = \frac{1}{36}$$

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

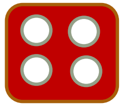
Probability

Roll a red die and a blue die.  

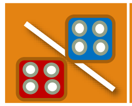
$$S = \{ (i, j) \mid 1 \leq i \leq 6, 1 \leq j \leq 6 \}$$

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?

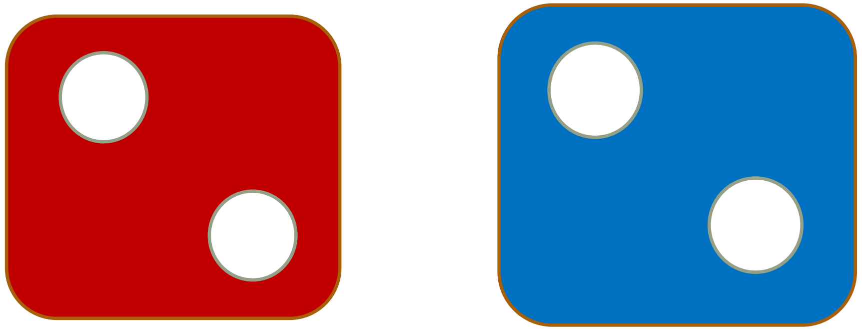
$$\Pr(i, j) = \frac{1}{36}$$

	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

Probability

Event A = "sum of a 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	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

Probability

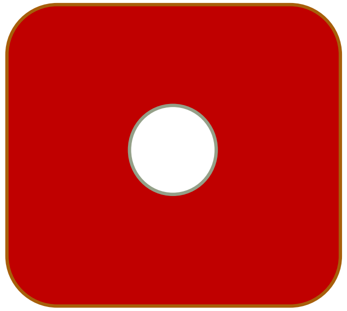
Event A = "sum of a red and blue is 4"

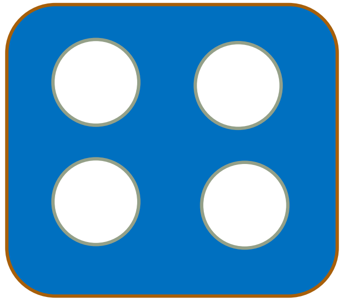
$$= \{\ (1{,}3), (2{,}2), (3{,}1)\ \}$$
$$\Pr(A) = \Pr(1{,}3) + \Pr(2{,}2) = \Pr(3{,}1)$$
$$= \frac{3}{36} = \frac{1}{12}$$

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	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

Probability

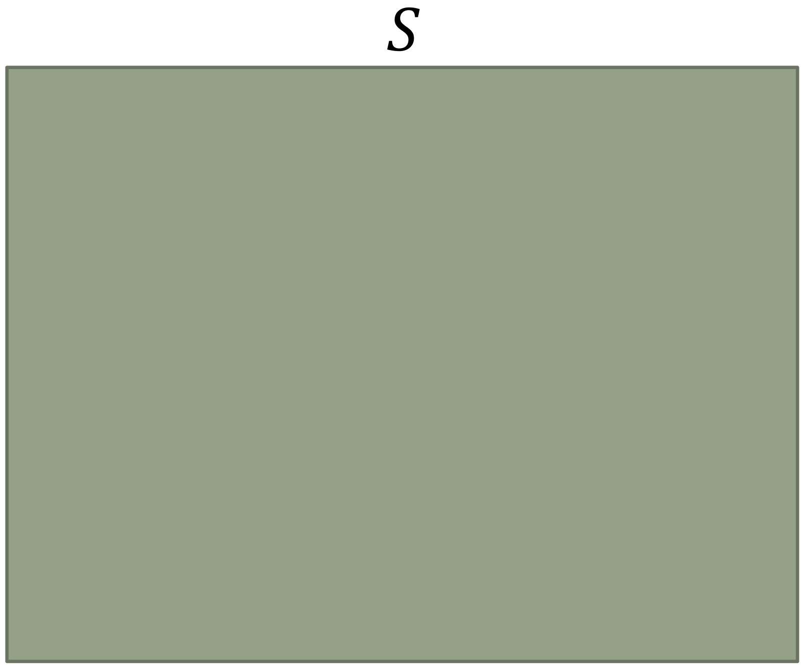
Event $A, A \subseteq S$

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

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 happens?"



Probability

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

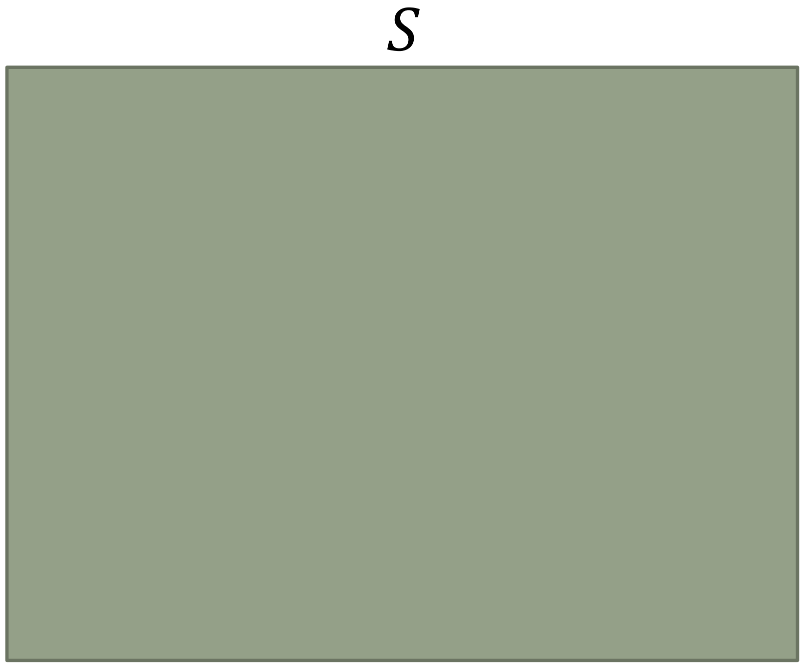
Event $A, A \subseteq S$

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

Also $\emptyset$ is an event

And $\Pr(\emptyset) = 0$

"What is the probability of an impossible outcome?“



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.

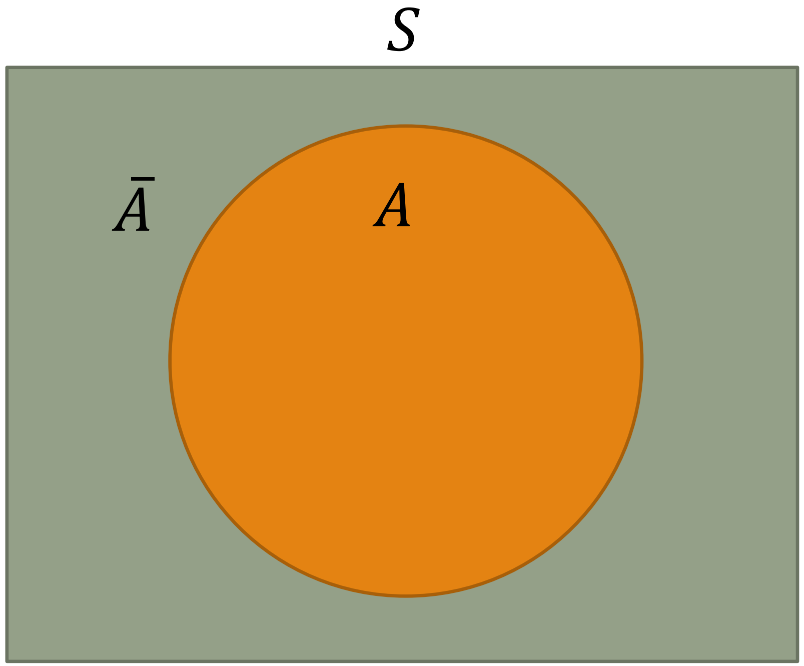
We can use what we know of A to determine it.
Since $A \cup \bar{A} = S$,

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

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

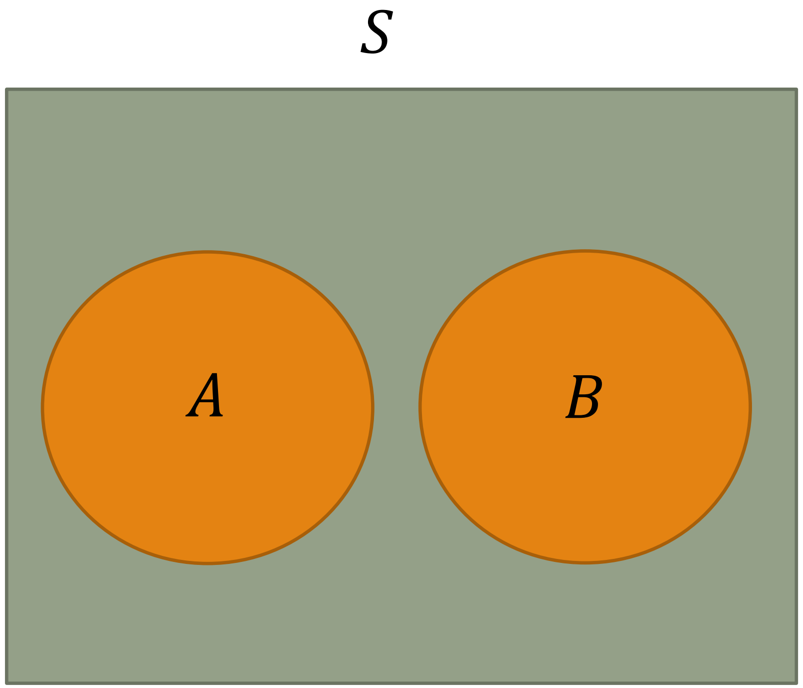
Event A, B **disjoint** sets.

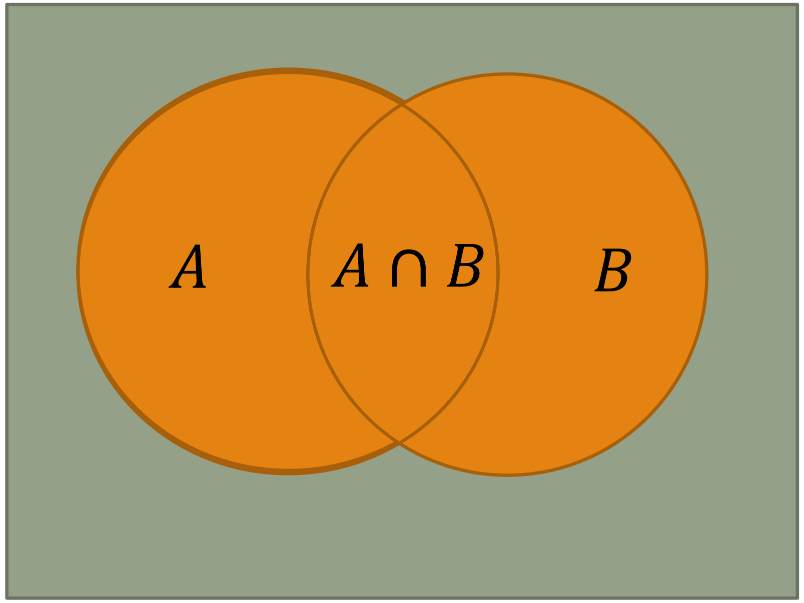
$$\Pr(A) = \sum_{w \in A} \Pr(w)$$
$$\Pr(B) = \sum_{w \in B} \Pr(w)$$

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.

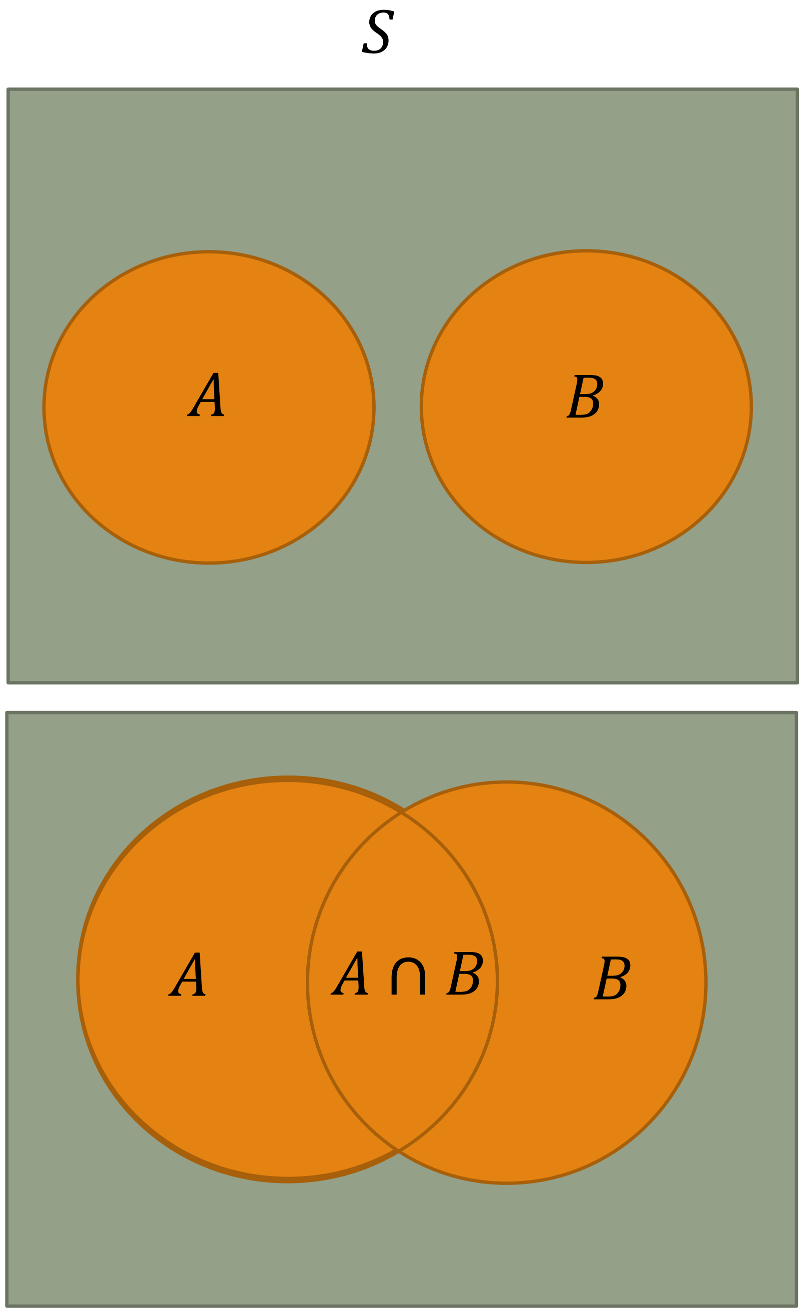
To count the elements:

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

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

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

Choose a random element x in S.

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

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

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

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

$$= \frac{500}{1000} + \frac{333}{1000} - \frac{166}{1000} = \frac{667}{1000}$$