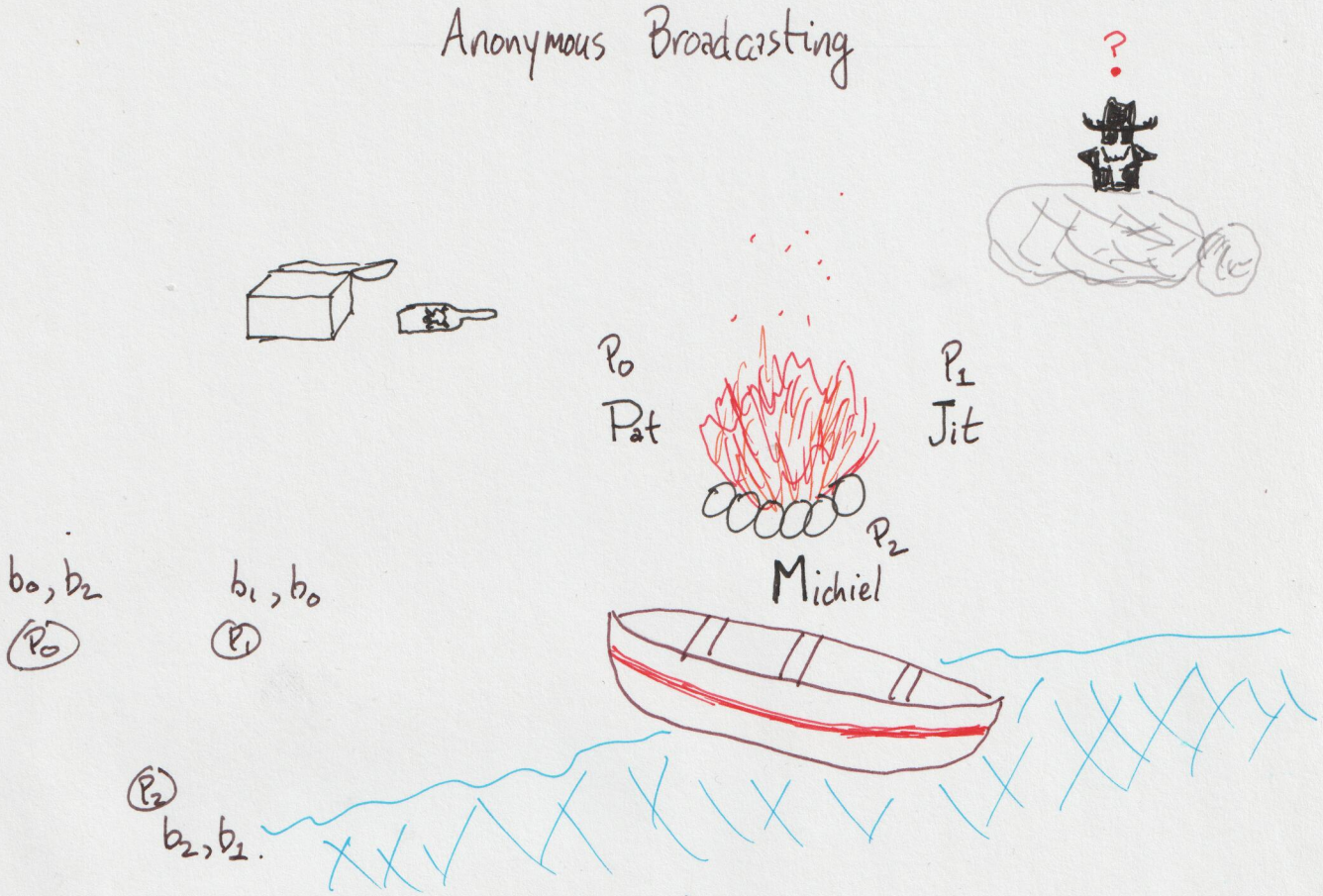
Anonymous Broadcasting



1. Each P_i chooses a random (secret) bit $b_i \in \{0,1\}$.
2. Each P_i whispers the value of b_i to $P_{(i+1) \bmod 3}$.
3. Each P_i computes $t_i = b_i \oplus b_{(i-1) \bmod 3}$.
4. Each P_i computes $\tilde{t}_i$ where.

$$\tilde{t}_i = \begin{cases} t_i & \text{if } P_i \text{ did not drink the whiskey} \\ -t_i \oplus 1 & \text{if } P_i \text{ did drink the whisky.} \end{cases}$$

5. Each P_i announces $\tilde{t}_i$
6. Each player computes $\tilde{t}_0 \oplus \tilde{t}_1 \oplus \tilde{t}_2$

$$0 \oplus 0 = 0$$
$$1 \oplus 0 = 1$$
$$0 \oplus 1 = 1$$
$$1 \oplus 1 = 0.$$

H_0 nobody drank the whisky.

$-\tilde{t}_i = t_i$ for each $i \in \{0,1,2\}$

$\tilde{t}_0 \oplus \tilde{t}_1 \oplus \tilde{t}_2 = b_0 \oplus b_2 \oplus b_1 \oplus b_0 \oplus b_2 \oplus b_1$

$= 0$

H_1 somebody drank whisky:

$\tilde{t}_0 \oplus \tilde{t}_1 \oplus \tilde{t}_2 =$ same $\oplus 1 = 1$

Sample Space: Non-empty countable set (S).

- Elements of S are called "outcomes" (elementary events).
- Subsets of S are called "events"

Probability Function: $Pr: S \to [0,1]$ such that $\sum_{\omega \in S} Pr(\omega) = 1$. (Probability function over S).

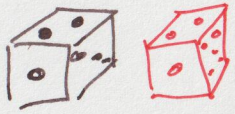
(S, Pr): Probability space.

For any event A, $Pr(A) = \sum_{\omega \in A} Pr(\omega)$.

Example: Coin toss $S = \{H, T\}$. $Pr(H) = Pr(T) = 1/2$.

Example: Toss 2 coins: $S = \{HH, HT, TH, TT\}$ $Pr(HH) = Pr(HT) = Pr(TH) = Pr(TT) = 1/4$.

Example: Roll a 6-sided die $S = \{1,2,3,4,5,6\}$ $Pr(1) = Pr(2) = \cdots = Pr(6) = 1/6$.



Uniform Probability Space: $Pr(\omega) = \frac{1}{|S|}$ for each $\omega \in S$.

Example: Roll 2 6-sided dice:

$S = \{(i,j) : i,j \in \{1,2,3,4,5,6\}\}$. $Pr(\omega) = \frac{1}{|S|} = \frac{1}{36}$ for any $\omega \in S$.

For each $K \in \{2,3,4,5,6,7,8,9,10,11,12\}$. let A_K = "the sum of the two dice is K".

$A_4 = \{(1,3), (2,2), (3,1)\}$. $Pr(A_4) = Pr((1,3)) + Pr((2,2)) + Pr((3,1)) = \frac{1}{36} + \frac{1}{36} + \frac{1}{36} = \frac{3}{36} = \frac{1}{12}$.

red die.

black die.	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.

$Pr(A_2) = \frac{1}{36}$

$Pr(A_3) = \frac{2}{36} = \frac{1}{18}.$

$Pr(A_4) = \frac{3}{36} = \frac{1}{12}$

$Pr(A_5) = \frac{4}{36} = \frac{1}{9}$

$Pr(A_6) = \frac{5}{36}$

$Pr(A_7) = \frac{6}{36} = \frac{1}{6}.$

$Pr(A_8) = \frac{5}{36}$

$Pr(A_9) = 4/36.$

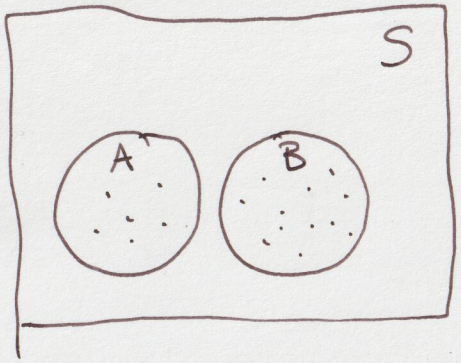
$Pr(A_{10}) = 3/36$

$Pr(A_{11}) = 2/36$

$Pr(A_{12}) = \frac{1}{36}$

If $A, B \subseteq S$ and A and B are disjoint

then $\Pr(A \cup B) = \sum_{\omega \in A \cup B} \Pr(\omega) = \sum_{\omega \in A} \Pr(\omega) + \sum_{\omega \in B} \Pr(\omega) = \Pr(A) + \Pr(B)$.



If $A_1, \ldots A_n$ are pairwise disjoint events then

$$\Pr(A_1 \cup A_2 \cup \ldots \cup A_n) = \sum_{i=1}^{n} \Pr(A_i)$$

(Sum Rule).

$$\begin{aligned}
\Pr(\text{sum of two dice is even}) &= \Pr(A_2 \cup A_4 \cup A_6 \cup A_8 \cup A_{10} \cup A_{12}) \\
&= \Pr(A_2) + \Pr(A_4) + \Pr(A_6) + \Pr(A_8) + \Pr(A_{10}) + \Pr(A_{12}). \\
&= \frac{1}{36} + \frac{3}{36} + \frac{5}{36} + \frac{5}{36} + \frac{3}{36} + \frac{1}{36}. \\
&= \frac{18}{36} = \frac{1}{2}.
\end{aligned}$$

$S = \{(i,j) : i,j \in \{1,\ldots,6\}\}$.

$A =$ "$i+j$ is even"

$A_0 =$ "i and j are both even" $\quad |A_0| = |\{(i,j) : i,j \in \{2,4,6\}\}| = 9$.

$A_1 =$ "i and j are both odd" $\quad |A_1| = |\{(i,j) : i,j \in \{1,3,5\}\}| = 9$

$$\begin{aligned}
\Pr(A) &= \Pr(A_0 \cup A_1) \\
&= \Pr(A_0) + \Pr(A_1). \\
&= \frac{|A_0|}{36} + \frac{|A_1|}{36} = \frac{9}{36} + \frac{9}{36} = \frac{18}{36} = \frac{1}{2}.
\end{aligned}$$