

17. Suppose that we flip a fair coin,  $n$  times to obtain  $n$  random bits. Consider all  $m = \binom{n}{2}$  pairs of these bits in some order. Let  $Y_i$  be the **exclusive-or**  $\oplus$  of the  $i$ -th pair of bits, and let  $Y = \sum_{i=1}^m Y_i$  be the number of  $Y_i$  that equal 1.

(a) Show that each  $Y_i = 0$  with prob  $= \frac{1}{2}$  (therefore,  $Y_i = 1$  with probability also  $\frac{1}{2}$ )

(b) Show that  $Y_i$  are not mutually independent.

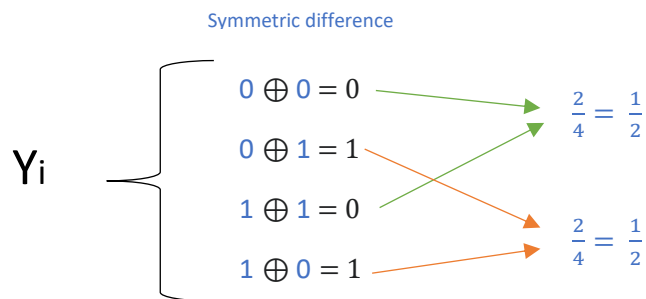
(c) Show that  $E[Y_i Y_j] = E[Y_i]E[Y_j]$ .

(d) Find  $\text{Var}[Y]$ .

(e) Use Chebyshev to bound  $\Pr[|Y - E[Y]| \geq n]$ .

---

(a)



$$P(Y_i = 1) = \frac{2 \times 2^{n-2}}{2^n} = \frac{1}{2}$$

$$P(Y_i = 0) = 1 - P(Y_i = 1) = \frac{1}{2}$$


---

(b)

To investigate their independence, let's consider  $P(Y_i = 1; Y_j = 1; Y_k = 1)$ .

$Y_i = 1 \Rightarrow$  The **first** and the **second** variable

$Y_j = 1 \Rightarrow$  The **second** and the **third** variable

$Y_k = 1 \Rightarrow$  The **first** and the **third** variable

If they are mutually independent, we should have:

$$P(Y_i = 1) = \frac{2 \times 2^{n-2}}{2^n} = \frac{1}{2} \quad \text{The same for } Y_j \text{ and } Y_k$$

$$P(Y_i = 1; Y_j = 1; Y_k = 1) = P(Y_i = 1) \times P(Y_j = 1) \times P(Y_k = 1) = \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{8}$$

**Nevertheless, these events cannot be happened at the same time. Therefore  $P(Y_i = 1; Y_j = 1; Y_k = 1) = 0$**

$$P(Y_i = 1; Y_j = 1; Y_k = 1) = 0 \Rightarrow 0 \neq \frac{1}{8}$$

Let's assume:

000  
001  
011  
010  
110  
111  
101  
100

---

(c)

First, we will show, that  $Y_i$  are pairwise independent. Consider 2 possibilities.

1.)  $Y_i$  and  $Y_j$  do not share a bit position. They are obviously independent.

2.)  $Y_i$  and  $Y_j$  share a bit position. Consider all 3-bit strings to confirm the independence.

$Y_i$	=>	The Sth and the Rth variable
$Y_j$	=>	The Kth and the Rth variable

...	R	...	K	...	S	...
...	0	...	0	...	0	...
Or						
...	R	...	K	...	S	...
...	1	...	1	...	1	...

$$P(Y_i = 0, Y_j = 0) = \frac{2 \times 2^{n-3}}{2^n} = \frac{1}{4}$$

$$P(Y_i = 0) = \frac{2 \times 2^{n-2}}{2^n} = \frac{1}{2}$$

$$P(Y_i = 0; Y_j = 0) = P(Y_i = 0) \times P(Y_j = 0) = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$$

---

(d)

When our variables are independent:

$$Var(Y) = \sum_{i=1}^m Var(Y_i)$$

$$\sum_{i=1}^m E(Y_i^2) - E(Y_i)^2 = \sum_{i=1}^m \left( 0^2 \frac{1}{2} + 1^2 \frac{1}{2} \right) - \left( 0 \frac{1}{2} + 1 \frac{1}{2} \right)^2 = \sum_{i=1}^m \frac{1}{4} = m \times \frac{1}{4} = \frac{m}{4}$$

---

(e)

*From the previous part we have*  $\text{Var}(Y) = \frac{m}{4}$

$$P[|Y - E(Y)| \geq n] \leq \frac{\text{Var}(Y)}{n^2} = \frac{1}{8} \frac{n(n-1)}{n^2} \leq \frac{1}{8}$$