ECE 471/571 pseudorandom numbers

- Randomness: uniform distribution

  e.g. 01 0101010101010101 .. X

- unpredictability.

  (independence of bits). X 1111111 000000

  ✓ 0100001010010100001

Entropy.

Coin toss: head – 0, tail – 1

$Pr[X=0] = 0.5$ fair coin

0.1 unfair coin

0 deterministic

$\log_2 \frac{1}{p}$ (bits)

$p=1$. for tails. $\log_2 1 = 0$

$p=0.5$. $\log_2 2 = 1$. (bits)

$p=0.25$. $\log_2 4 = 2$ (bits).

⋮

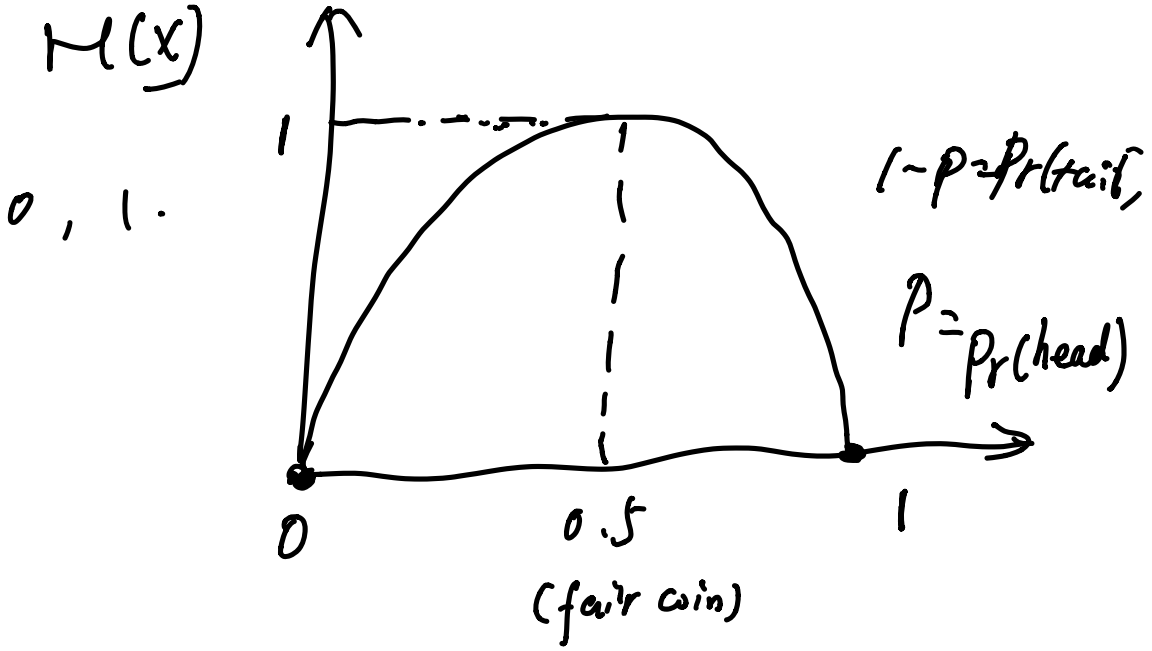
random variable.

$X \sim \{x_1, x_2, \ldots x_n\}$.

$$H(X) = \sum_{x_i \in X} p_i \cdot \log_2 \frac{1}{p_i}$$

$$= -\sum_{x \in X} p(x) \cdot \log_2 p(x) \quad \text{(bits)}$$

coin.



$$H(X) = -p \cdot \log_2 p - (1-p) \log_2 (1-p)$$

if $p=0$ $H(X)=0$

$p=1$ $H(X)=0$

$p=0.5$ $H(X)=1$.

0 1 0 0 1 0 0 0 1 1 1 ... n length

$$\Pr[\text{each sequence of len } n.] = \frac{1}{2^n}$$

$n-1$	$\frac{1}{2^{n-1}} \times 2^n = 2$
$n-2$	$\frac{1}{2^{n-2}} \times 2^n = 4.$
	⋮

$n = 10.$

Length 1. 2^8 ..

2 : 2^8.

⋮

n ⋮