

# UNPREDICTABILITY

whether or not a sequence is generated randomly.

\* References:

- Paper of Merkle, et al.
- Book - Downey, Hirschfeld

Def. A (monotonic) stake function:

$$q: \{0,1\}^* \rightarrow [0,2]$$

interpreted as: if  $q(\sigma) < 1$ , bet that the next bit is 1  
 $q(\sigma) > 1$ , bet 0  
 $q(\sigma) = 1$ , agnostic.

Def. A payoff function,  $C_q: \{0,1\}^* \rightarrow [0,2]$ , defined by

$$C_q(\sigma 0) = q(\sigma)$$

$$C_q(\sigma 1) = 2 - q(\sigma)$$

Def. The capital function,  $d_q: \{0,1\}^* \rightarrow \mathbb{R}^{\geq 0}$ , defined by

$$d_q(\sigma_0, \sigma_1, \dots, \sigma_n) = C_q(\sigma_0) C_q(\sigma_0 \sigma_1) \dots C_q(\sigma_0 \dots \sigma_n)$$

★ Convention: initial capital,  $d(\epsilon) = 1$

Def. Martingales,  $d: \{0,1\}^* \rightarrow \mathbb{R}^{\geq 0}$  s.t.  $\forall \sigma \in \{0,1\}^*$ ,

$$d(\sigma) = \frac{d(\sigma 0) + d(\sigma 1)}{2}$$

where  $d(\sigma)$  is capital

These represent a fair game.

Comment. Martingales  $\stackrel{*}{=}$  capital fcn of monotonic stake function,  
i.e., <sup>(i)</sup> given a Martingale  $d$ ,  $\exists q$  s.t.  $d_q = d$ , and given  $q$ ,  $d_q$  is a Martingale. <sup>(ii)</sup>

Proof of (ii): (Given  $q$ , check  $d_q(\sigma) = \frac{d_q(\sigma_0) + d_q(\sigma_1)}{2}$ )

$$d_q(\sigma_0) = C_q(\sigma_0) C_q(\sigma_0 \sigma_1) \dots C_q(\sigma) C_q(\sigma_0)$$

$$= d_q C_q(\sigma_0) = d_q(\sigma) q(\sigma)$$

$$d_q(\sigma_1) = d_q C_q(\sigma_1) = d_q(\sigma) (2 - q(\sigma))$$

$$\text{so, } \frac{d_q(\sigma_0) + d_q(\sigma_1)}{2} = \frac{d_q(\sigma) q(\sigma) + d_q(\sigma) (2 - q(\sigma))}{2} = d_q(\sigma) \checkmark$$

(i): Define  $q(\sigma) = \frac{d(\sigma_0)}{d(\sigma)}$

Can check  $q(\sigma) = 2 - \frac{d(\sigma_1)}{d(\sigma)}$  b/c Martingale

Def. Let  $X \in \{0,1\}^{\omega}$ ,  $q: \{0,1\}^* \rightarrow [0,2]$ , then the payoff while playing on  $X$  is defined to be  $C_q^X: \mathbb{Z}^+ \rightarrow [0,2]$ ,

$$C_q^X(n+1) = \begin{cases} q(X \uparrow^{n+1}) & \text{if } X(n+1) = 0 \\ 2 - q(X \uparrow^{n+1}) & \text{if } X(n+1) = 1 \end{cases}$$

where  $X \uparrow^{n+1} = X(0) X(1) \dots X(n)$

And the capital function for this game becomes  $d_q^X: \mathbb{Z}^+ \rightarrow \mathbb{R}^{\geq 0}$ ,

$$d_q^X(n) = \prod_{i=1}^n C_q^X(i)$$

Def. The Capital fcn / Martingale succeeds on  $X$  if

$$\limsup_{n \rightarrow \infty} d_q^X(n) = \infty$$

## Sanity Check

$$\limsup_{n \rightarrow \infty} d_q^x(n) = \infty \Rightarrow \exists^\infty n, C_q^x(n) > 1$$

i.e.,  $\exists^\infty n$  ( $q(x/n) > 1$  and  $x(n+1) = 0$   
or  $q(x/n) < 1$  and  $x(n+1) = 1$ )

Fact.  $\forall x \in \mathbb{Z}^\omega$ ,  $\exists$  a Martingale that succeeds on it.

The gist: If there is a Martingale that succeeds on  $X$ , and is effective then  $X$  is not "random."