Biased coins, blindfold players

Vinícius G. Pereira de Sá

based on the paper "Blind-friendly von Neumann's heads or tails",
to appear in The American Mathematical Monthly,
joint work with Celina M. H. de Figueiredo

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
UFRJ

…back in 2007

Algoritmos Randomizados: Introdução

Celina Figueiredo
Guilherme Fonseca
Manoel Lemos
Vinícius Sá

impa

26º Colóquio Brasileiro de Matemática
IMPA – Rio de Janeiro – Brasil
2007

...back in 2007

Algoritmos Randomizados: Introdução

Celina Figueiredo
Guilherme Fonseca
Manoel Lemos
Vinícius Sá

26º Colóquio Brasileiro de Matemática
IMPA – Rio de Janeiro – Brasil
2007

Guilherme Dias da Fonseca

What's in this talk?

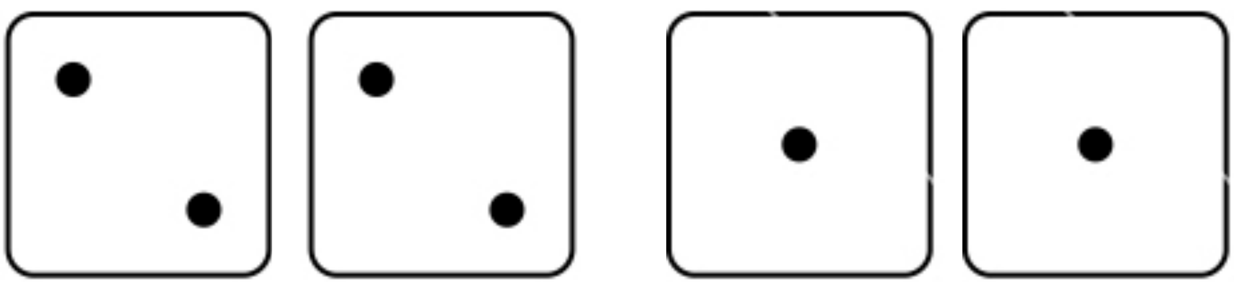
- biased randomness → unbiased randomness
- counterintuitive probabilities
  - a simple 2-player dice game (a triple or two straight doubles?)
  - conditioning on seemingly irrelevant knowledge
  - an interesting lemma
- fair heads or tails with a "concealed" biased coin
  - how *not* to do it
  - how to do it

a triple or two straight doubles?

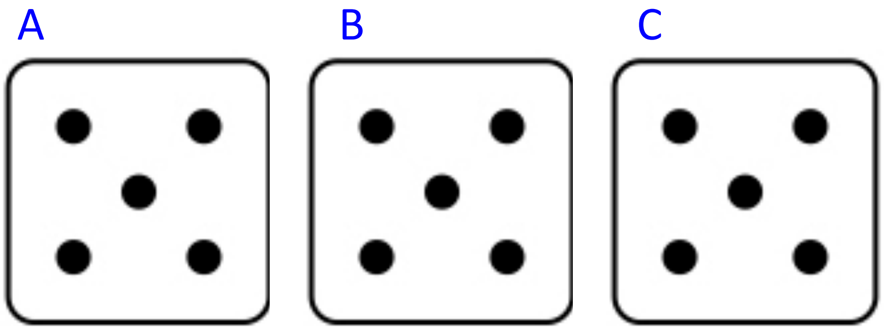
A triple or two straight doubles?

A B C

A B C D

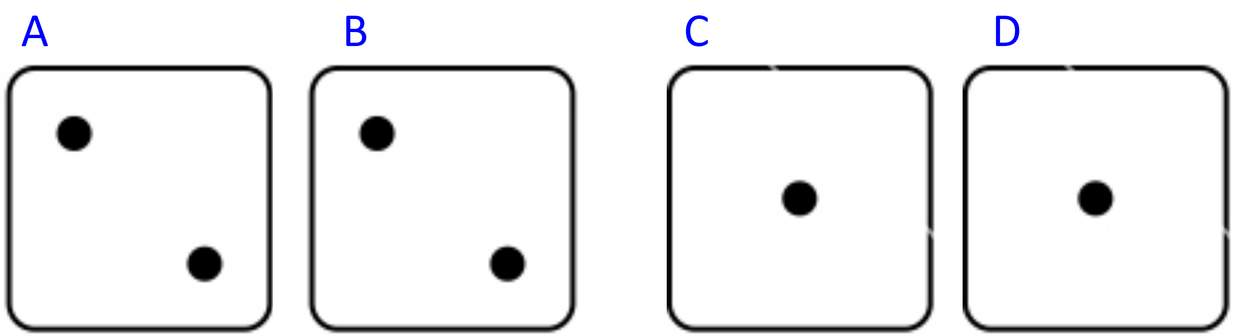


A triple or two straight doubles?



E_3 := A = B = C

$$\Pr\{E_3\} = \sum_{i \in \Omega} p_i^3$$



$E_{2,2}$:= A = B and C = D

$$\Pr\{E_{2,2}\} = \left(\sum_{i \in \Omega} p_i^2 \right)^2$$

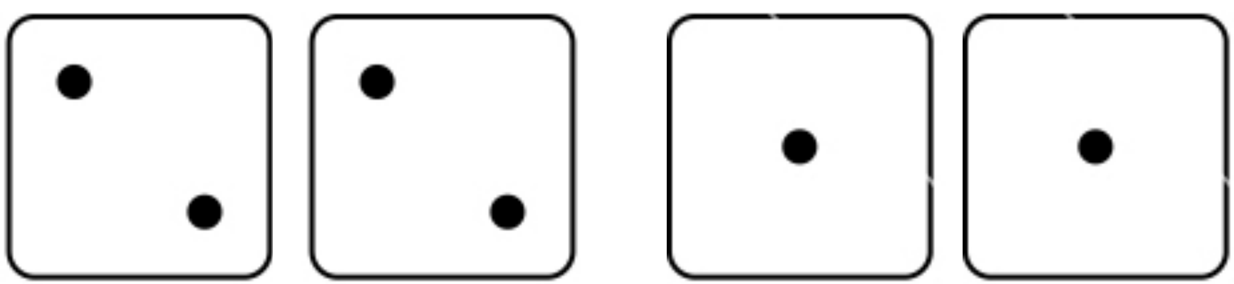
A triple or two straight doubles?

A B C

E_3 := A = B = C

$$\Pr\{E_3\} = \sum_{i\in\Omega} p_i^3$$

A B C D



$E_{2,2}$:= A = B and C = D

$$\Pr\{E_{2,2}\} = \left(\sum_{i\in\Omega} p_i^2\right)^2$$

A triple or two straight doubles?

$$\Pr\{E_3\} = \sum_{i \in \Omega} p_i^3$$

$$\Pr\{E_{2,2}\} = \left(\sum_{i \in \Omega} p_i^2 \right)^2$$

A triple or two straight doubles?

Cauchy inequality:

$$\left(\sum_{i\in\Omega} x_i y_i\right)^2 \leq \left(\sum_{i\in\Omega} x_i^2\right)\left(\sum_{i\in\Omega} y_i^2\right)$$

$$\Pr\{E_3\} = \sum_{i\in\Omega} p_i^3$$

$$\geq$$

$$\Pr\{E_{2,2}\} = \left(\sum_{i\in\Omega} p_i^2\right)^2$$

A triple or two straight doubles?

Cauchy inequality:

$$\left(\sum_{i\in\Omega} x_i y_i\right)^2 \leq \left(\sum_{i\in\Omega} x_i^2\right)\left(\sum_{i\in\Omega} y_i^2\right)$$

$$x_i = p_i^{3/2} \qquad y_i = p_i^{1/2}$$

$$\Pr\{E_3\} = \sum_{i\in\Omega} p_i^3$$

$$\geq$$

$$\Pr\{E_{2,2}\} = \left(\sum_{i\in\Omega} p_i^2\right)^2$$

A triple or two straight doubles?

Cauchy inequality:

$$\left(\sum_{i\in\Omega} x_i y_i\right)^2 \leq \left(\sum_{i\in\Omega} x_i^2\right)\left(\sum_{i\in\Omega} y_i^2\right)$$

$$x_i = p_i^{3/2} \qquad y_i = p_i^{1/2}$$

$$\left(\sum_{i\in\Omega} p_i^2\right)^2 \leq \left(\sum_{i\in\Omega} p_i^3\right)\cancelto{1}{\left(\sum_{i\in\Omega} p_i\right)} = \sum_{i\in\Omega} p_i^3$$

$$\Pr\{E_3\} = \sum_{i\in\Omega} p_i^3$$

$$\geq$$

$$\Pr\{E_{2,2}\} = \left(\sum_{i\in\Omega} p_i^2\right)^2$$

A triple or two straight doubles?

$$\left(\sum_{i\in\Omega} p_i^2\right)^2 = \boxed{\Pr\{E_{2,2}\} \ \leq \ \Pr\{E_3\}} = \sum_{i\in\Omega} p_i^3$$

- perfectly fair dice
- perfectly unfair (loaded) dice
- coins

A triple or two straight doubles?

$$\left(\sum_{i\in\Omega} p_i^2\right)^2 = \boxed{\Pr\{E_{2,2}\} \ \le \ \Pr\{E_3\}} = \sum_{i\in\Omega} p_i^3$$

- perfectly fair dice

$p_i = 1/n$ for all $i \in \Omega$ $\Rightarrow$ $\Pr\{E_3\} = \Pr\{E_{2,2}\} = \dfrac{1}{n^2}$

$\boxed{n = |\,\Omega\,|}$

- perfectly unfair (loaded) dice

- coins

A triple or two straight doubles?

$$\left(\sum_{i\in\Omega} p_i^2\right)^2 = \boxed{\Pr\{E_{2,2}\} \ \leq \ \Pr\{E_3\}} = \sum_{i\in\Omega} p_i^3$$

- perfectly fair dice

  $p_i = 1/n$ for all $i \in \Omega$ $\Rightarrow$ $\Pr\{E_3\} = \Pr\{E_{2,2}\} = \dfrac{1}{n^2}$

  $\boxed{n = |\,\Omega\,|}$

- perfectly unfair (loaded) dice

  $p_1 = 1$

  $p_i = 0$ for $i \in \{2, \ldots, n\}$ $\Rightarrow$ $\Pr\{E_3\} = \Pr\{E_{2,2}\} = 1$

- coins

A triple or two straight doubles?

$$\left(\sum_{i\in\Omega} p_i^2\right)^2 = \boxed{\Pr\{E_{2,2}\} \ \le \ \Pr\{E_3\}} = \sum_{i\in\Omega} p_i^3$$

- perfectly fair dice

$$p_i = 1/n \text{ for all } i \in \Omega \quad \Rightarrow \quad \Pr\{E_3\} = \Pr\{E_{2,2}\} = \frac{1}{n^2}$$

- perfectly unfair (loaded) dice

$\boxed{n = |\,\Omega\,|}$

$$\begin{aligned} p_1 &= 1 \\ p_i &= 0 \ \text{ for } i \in \{2, \ldots, n\} \end{aligned} \quad \Rightarrow \quad \Pr\{E_3\} = \Pr\{E_{2,2}\} = 1$$

- coins

$$\begin{aligned} p_1 &= p \\ p_2 &= 1 - p \end{aligned} \quad \Rightarrow \quad \Pr\{E_3\} - \Pr\{E_{2,2}\} =$$

$$= \quad \left[p^3 + (1-p)^3\right] - \left[p^2 + (1-p)^2\right]^2 \ =$$

$$= \quad -4p^4 + 8p^3 - 5p^2 + p$$

A triple or two straight doubles?

- coins

$$p_1 = p \qquad p_2 = 1 - p$$

$$\Rightarrow \Pr\{E_3\} - \Pr\{E_{2,2}\} =$$

$$= \left[p^3 + (1-p)^3\right] - \left[p^2 + (1-p)^2\right]^2 =$$

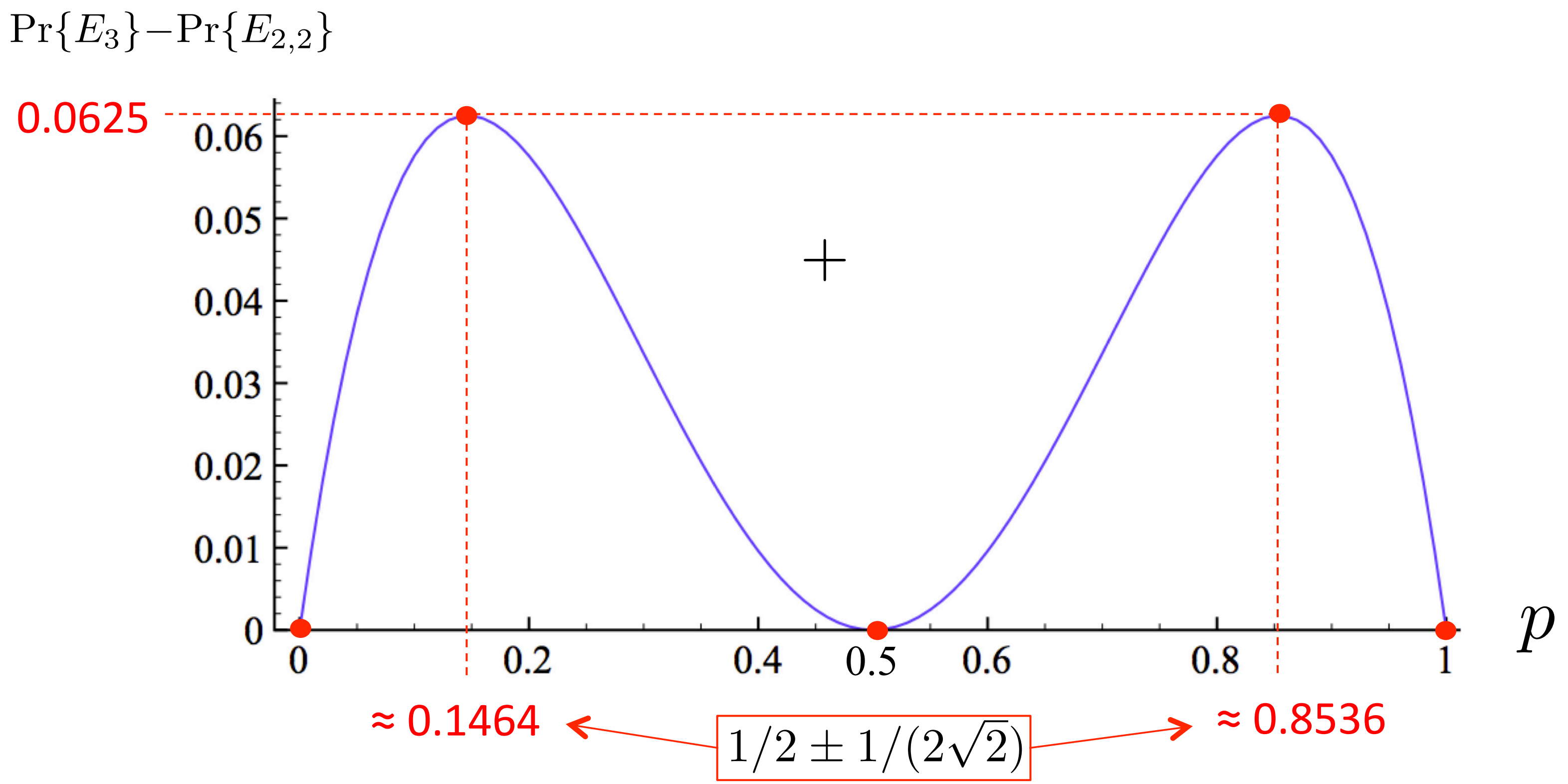
$$= -4p^4 + 8p^3 - 5p^2 + p$$

A triple or two straight doubles?

- coins

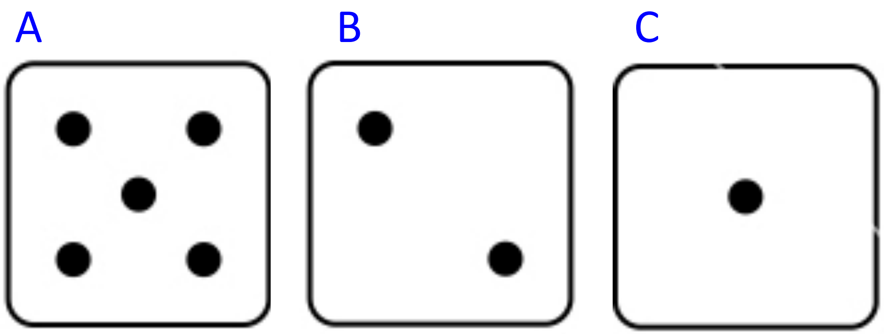
$$p_1 = p$$
$$p_2 = 1 - p$$

$$\Pr\{E_3\} - \Pr\{E_{2,2}\} =$$
$$= \left[p^3 + (1-p)^3\right] - \left[p^2 + (1-p)^2\right]^2 =$$
$$= -4p^4 + 8p^3 - 5p^2 + p$$



seemingly irrelevant knowledge

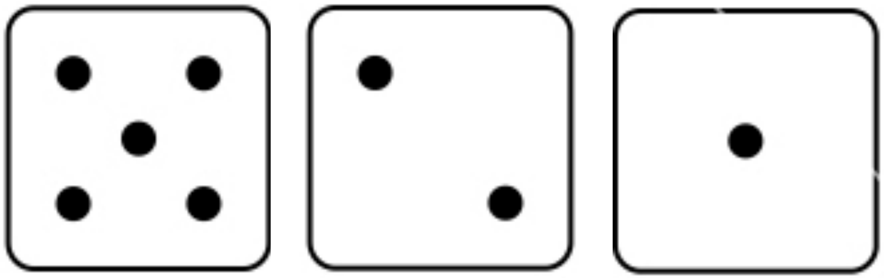
Seemingly irrelevant knowledge



A, B, C **independent** identically distributed (iid) random variables

Seemingly irrelevant knowledge

A B C



A, B, C **independent** identically distributed (iid) random variables

$$\Pr\{ C = B \} \overset{?}{=} \Pr\{ C = B \mid B \neq A \}$$

Seemingly irrelevant knowledge

$$\Pr\{ C = B \} \stackrel{?}{=} \Pr\{ C = B \mid B \neq A \}$$

Seemingly irrelevant knowledge

Pr{ C = B } $\overset{?}{=}$ Pr{ C = B | B ≠ A }

$$\Pr\{C = B\} = \sum_{i \in \Omega} p_i^2$$

$$\Pr\{C = B \mid B \neq A\} = \frac{\Pr\{C = B \neq A\}}{\Pr\{B \neq A\}} = \frac{\sum_{i \in \Omega}[p_i^2(1 - p_i)]}{\sum_{i \in \Omega}[p_i(1 - p_i)]}$$

Seemingly irrelevant knowledge

Pr{ C = B } = Pr{ C = B | B ≠ A }

?

$$\Pr\{C = B\} = \sum_{i \in \Omega} p_i^2$$

$$\neq$$

$$\Pr\{C = B \mid B \neq A\} = \frac{\Pr\{C = B \neq A\}}{\Pr\{B \neq A\}} = \frac{\sum_{i \in \Omega}[p_i^2(1 - p_i)]}{\sum_{i \in \Omega}[p_i(1 - p_i)]}$$

Seemingly irrelevant knowledge

$$\Pr\{C = B \mid B \neq A\} \;\leq\; \Pr\{C = B\}$$

$$\Pr\{C = B\}$$

$$\rotatebox{-90}{$\geq$}$$

$$\Pr\{C = B \mid B \neq A\}$$

Seemingly irrelevant knowledge

$$\Pr\{C = B \mid B \neq A\} \ \leq \ \Pr\{C = B\}$$

$$\frac{\Pr\{C = B \neq A\}}{1 - \Pr\{B = A\}} \ \leq \ \Pr\{C = B\}$$

$$\Pr\{C = B\}$$

$$\Pr\{C = B \mid B \neq A\}$$

Seemingly irrelevant knowledge

$$\Pr\{C = B \mid B \neq A\} \;\leq\; \Pr\{C = B\}$$

$$\frac{\Pr\{C = B \neq A\}}{1 - \Pr\{B = A\}} \;\leq\; \Pr\{C = B\}$$

$$\begin{aligned} \Pr\{C = B \neq A\} \;\leq\;& \Pr\{C = B\} \\ & - \Pr\{C = B\}\ \Pr\{B = A\} \end{aligned}$$

$$\boxed{\begin{array}{c} \Pr\{C = B\} \\ \geq \\ \Pr\{C = B \mid B \neq A\} \end{array}}$$

Seemingly irrelevant knowledge

$$\Pr\{C = B \mid B \neq A\} \;\leq\; \Pr\{C = B\}$$

$$\frac{\Pr\{C = B \neq A\}}{1 - \Pr\{B = A\}} \;\leq\; \Pr\{C = B\}$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B\} - \Pr\{C = B\}\ \Pr\{B = A\}$$

A, B, C iid

$$\Pr\{B = A\} = \Pr\{C = B\}$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B\} - \Pr\{C = B\}^2$$

$$\Pr\{C = B\}$$

$$\geq$$

$$\Pr\{C = B \mid B \neq A\}$$

Seemingly irrelevant knowledge

$$\Pr\{C = B \mid B \neq A\} \;\leq\; \Pr\{C = B\}$$

$$\frac{\Pr\{C = B \neq A\}}{1 - \Pr\{B = A\}} \;\leq\; \Pr\{C = B\}$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B\} - \Pr\{C = B\}\,\Pr\{B = A\}$$

A, B, C iid

$$\Pr\{B = A\} = \Pr\{C = B\}$$

$$\Pr\{C = B\}$$

$$\Pr\{C = B \mid B \neq A\}$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B\} - \Pr\{C = B\}^2$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B \neq A\} + \Pr\{C = B = A\} - \Pr\{C = B\}^2$$

Seemingly irrelevant knowledge

$$\Pr\{C = B \mid B \neq A\} \;\leq\; \Pr\{C = B\}$$

$$\frac{\Pr\{C = B \neq A\}}{1 - \Pr\{B = A\}} \;\leq\; \Pr\{C = B\}$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B\} - \Pr\{C = B\}\,\Pr\{B = A\}$$

A, B, C iid

$$\Pr\{B = A\} = \Pr\{C = B\}$$

$$\Pr\{C = B\}$$

$$\geq$$

$$\Pr\{C = B \mid B \neq A\}$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B\} - \Pr\{C = B\}^2$$

$$\cancel{\Pr\{C = B \neq A\}} \;\leq\; \cancel{\Pr\{C = B \neq A\}} + \Pr\{C = B = A\} - \Pr\{C = B\}^2$$

$$\Pr\{C = B\}^2 \leq \Pr\{C = B = A\}$$

Seemingly irrelevant knowledge

$$\Pr\{C = B \mid B \neq A\} \;\leq\; \Pr\{C = B\}$$

$$\frac{\Pr\{C = B \neq A\}}{1 - \Pr\{B = A\}} \;\leq\; \Pr\{C = B\}$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B\} - \Pr\{C = B\}\,\Pr\{B = A\}$$

A, B, C iid

$$\Pr\{B = A\} = \Pr\{C = B\}$$

$$\Pr\{C = B\}$$

$$\Pr\{C = B\} \geq \Pr\{C = B \mid B \neq A\}$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B\} - \Pr\{C = B\}^2$$

$$\cancel{\Pr\{C = B \neq A\}} \;\leq\; \cancel{\Pr\{C = B \neq A\}} + \Pr\{C = B = A\} - \Pr\{C = B\}^2$$

$$\Pr\{C = B\}^2 \leq \Pr\{C = B = A\}$$

$$\Pr\{C = B\}^2 = \left(\sum_{i \in \Omega} p_i^2\right)^2 \qquad \Pr\{C = B = A\} = \sum_{i \in \Omega} p_i^3$$

Seemingly irrelevant knowledge

$$\Pr\{C = B \mid B \neq A\} \;\leq\; \Pr\{C = B\}$$

$$\frac{\Pr\{C = B \neq A\}}{1 - \Pr\{B = A\}} \;\leq\; \Pr\{C = B\}$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B\} - \Pr\{C = B\}\;\Pr\{B = A\}$$

A, B, C iid

$$\Pr\{B = A\} \;=\; \Pr\{C = B\}$$

$$\Pr\{C = B\}$$

$$\geq$$

$$\Pr\{C = B \mid B \neq A\}$$

$$\Pr\{C = B \neq A\} \;\leq\; \Pr\{C = B\} - \Pr\{C = B\}^2$$

$$\cancel{\Pr\{C = B \neq A\}} \;\leq\; \cancel{\Pr\{C = B \neq A\}} + \Pr\{C = B = A\} - \Pr\{C = B\}^2$$

$$\Pr\{C = B\}^2 \leq \Pr\{C = B = A\}$$

$$\left(\sum_{i\in\Omega} p_i^2\right)^2 \;\leq\; \sum_{i\in\Omega} p_i^3$$

Seemingly irrelevant knowledge

$$\frac{\sum_{i\in\Omega}[p_i^2(1-p_i)]}{\sum_{i\in\Omega}[p_i(1-p_i)]} = \boxed{\Pr\{C=B \mid B\neq A\} \leq \Pr\{C=B\}} = \sum_{i\in\Omega} p_i^2$$

Example:

$$\Omega = \{1,2,3\}$$

$$p_1 = 0.8$$

$$p_2 = p_3 = 0.1$$

Seemingly irrelevant knowledge

$$\frac{\sum_{i\in\Omega}[p_i^2(1-p_i)]}{\sum_{i\in\Omega}[p_i(1-p_i)]} = \boxed{\Pr\{C=B \mid B\neq A\} \leq \Pr\{C=B\}} = \sum_{i\in\Omega} p_i^2$$

Example:

$$\Omega = \{1,2,3\}$$
$$p_1 = 0.8$$
$$p_2 = p_3 = 0.1$$

$$\Pr\{C=B\} = 0.66$$

$$\Pr\{C=B \mid B\neq A\} \approx 0.429$$

Seemingly irrelevant knowledge

$$\frac{\sum_{i\in\Omega}[p_i^2(1-p_i)]}{\sum_{i\in\Omega}[p_i(1-p_i)]} = \boxed{\Pr\{C = B \mid B \neq A\} \leq \Pr\{C = B\}} = \sum_{i\in\Omega} p_i^2$$

Example:

$$\Omega = \{1, 2, 3\}$$

$$p_1 = 0.8$$

$$p_2 = p_3 = 0.1$$

$$\Pr\{C = B\} = 0.66$$

$$\geq$$

$$\Pr\{C = B \mid B \neq A\} \approx 0.429$$

Seemingly irrelevant knowledge

$$\frac{\sum_{i\in\Omega}[p_i^2(1-p_i)]}{\sum_{i\in\Omega}[p_i(1-p_i)]} = \boxed{\Pr\{C=B \mid B \neq A\} \leq \Pr\{C=B\}} = \sum_{i\in\Omega} p_i^2$$

- perfectly fair dice
- perfectly unfair (loaded) dice
- coins

Seemingly irrelevant knowledge

$$\frac{\sum_{i\in\Omega}[p_i^2(1-p_i)]}{\sum_{i\in\Omega}[p_i(1-p_i)]} = \boxed{\Pr\{C=B \mid B\neq A\} \leq \Pr\{C=B\}} = \sum_{i\in\Omega} p_i^2$$

- perfectly fair dice

$p_i = 1/n \text{ for all } i \in \Omega$ ⇒ $\Pr\{C=B \mid B\neq A\} =$

$= \Pr\{C=B\} = 1/n$

$\boxed{n = |\Omega|}$

- perfectly unfair (loaded) dice
- coins

Seemingly irrelevant knowledge

$$\frac{\sum_{i\in\Omega}[p_i^2(1-p_i)]}{\sum_{i\in\Omega}[p_i(1-p_i)]} = \boxed{\Pr\{C = B \mid B \neq A\} \;\leq\; \Pr\{C = B\}} = \sum_{i\in\Omega} p_i^2$$

- perfectly fair dice

  $p_i = 1/n$ for all $i \in \Omega$ ⇨ $\Pr\{C = B \mid B \neq A\} =$
  $= \Pr\{C = B\} = 1/n$

  $\boxed{n = |\,\Omega\,|}$

- perfectly unfair (loaded) dice

  $p_1 = 1$
  $p_i = 0$ for $i \in \{2, \ldots, n\}$ ⇨ $B \neq A$
  impossible event

- coins

Seemingly irrelevant knowledge

$$\frac{\sum_{i\in\Omega}[p_i^2(1-p_i)]}{\sum_{i\in\Omega}[p_i(1-p_i)]} = \boxed{\Pr\{C=B \mid B\neq A\} \leq \Pr\{C=B\}} = \sum_{i\in\Omega} p_i^2$$

- perfectly fair dice

  $p_i = 1/n \text{ for all } i \in \Omega \Rightarrow \Pr\{C=B \mid B\neq A\} = = \Pr\{C=B\} = 1/n$

  $\boxed{n = |\Omega|}$

- perfectly unfair (loaded) dice

  $p_1 = 1$
  $p_i = 0 \text{ for } i \in \{2,\ldots,n\} \Rightarrow B \neq A$

  impossible event

- coins

  $\Pr\{C=B\} = p_1^2 + p_2^2 = p^2 + (1-p)^2 = 2p^2 - 2p + 1$ minimum at (0.5, 0.5)

Seemingly irrelevant knowledge

$$\frac{\sum_{i\in\Omega}[p_i^2(1-p_i)]}{\sum_{i\in\Omega}[p_i(1-p_i)]} = \boxed{\Pr\{C=B \mid B\neq A\} \leq \Pr\{C=B\}} = \sum_{i\in\Omega} p_i^2$$

- perfectly fair dice

  $p_i = 1/n \text{ for all } i \in \Omega$ $\Rightarrow$ $\Pr\{C=B \mid B\neq A\} = \Pr\{C=B\} = 1/n$

  $\boxed{n = |\Omega|}$

- perfectly unfair (loaded) dice

  $p_1 = 1$

  $p_i = 0 \text{ for } i \in \{2,\ldots,n\}$ $\Rightarrow$ $B \neq A$

  impossible event

- coins

  $\Pr\{C=B\} = p_1^2 + p_2^2 = p^2 + (1-p)^2 = 2p^2 - 2p + 1$ minimum at (0.5, 0.5)

  $$\Pr\{C=B \mid B\neq A\} = \frac{p^2(1-p)+(1-p)^2p}{2p-2p^2} = \frac{p-p^2}{2p-2p^2}$$

Seemingly irrelevant knowledge

$$\frac{\sum_{i\in\Omega}[p_i^2(1-p_i)]}{\sum_{i\in\Omega}[p_i(1-p_i)]} = \boxed{\Pr\{C=B \mid B\neq A\} \leq \Pr\{C=B\}} = \sum_{i\in\Omega} p_i^2$$

- perfectly fair dice

  $p_i = 1/n$ for all $i \in \Omega$ $\Rightarrow$ $\Pr\{C=B \mid B\neq A\} =$
  $= \Pr\{C=B\} = 1/n$

  $\boxed{n = |\Omega|}$

- perfectly unfair (loaded) dice

  $p_1 = 1$
  $p_i = 0$ for $i \in \{2,\ldots,n\}$ $\Rightarrow$ $B \neq A$

  impossible event

- coins

  $\Pr\{C=B\} = p_1^2 + p_2^2 = p^2 + (1-p)^2 = 2p^2 - 2p + 1$ minimum at (0.5, 0.5)

  $$\Pr\{C=B \mid B\neq A\} = \frac{p^2(1-p)+(1-p)^2p}{2p-2p^2} = \frac{p-p^2}{2p-2p^2} = \mathbf{0.5}$$

Seemingly irrelevant knowledge

$$\Pr\{C = B \mid B \neq A\} \quad = \quad \frac{p^2(1-p) + (1-p)^2 p}{2p - 2p^2} \quad = \quad \frac{p - p^2}{2p - 2p^2} \quad = \quad \mathbf{0.5}$$

Seemingly irrelevant knowledge

$$\Pr\{C = B \mid B \neq A\} \qquad = \mathbf{0.5}$$

Lemma:

Given three independent Bernoulli random variables A, B, and C with success probability $0 < p < 1$, we have

$$\Pr\{C = B \mid B \neq A\} \;=\; \mathbf{0.5} \qquad \text{regardless of } p.$$

Lemma:

Given three independent Bernoulli random variables A, B, and C with success probability $0 < p < 1$, we have

$$\Pr\{C = B \mid B \neq A\} = \mathbf{0.5} \quad \text{regardless of } p.$$

fair heads or tails
with a concealed biased coin

von Neumann's idea

take a biased coin, flip it twice

(H)eads-(T)ails, Player 1 wins

T-H, Player 2 wins

H-H or T-T, start over

$\boxed{p = \Pr\{\mathrm{H}\}}$

$$\Pr\{\text{H-T}\} = \Pr\{\text{T-H}\} = p\,(1-p)$$

von Neumann's idea

$\Pr\{\text{H-T}\} = \Pr\{\text{T-H}\} = p\,(1 - p)$

$\Pr\{\text{someone wins at a given turn}\} = \Pr\{\text{T-H}\} + \Pr\{\text{H-T}\} = 2\,p\,(1 - p)$

$$\text{expected \# flips until someone wins} = 2 \times \frac{1}{2\,p\,(1-p)} = \frac{1}{p\,(1-p)}$$

von Neumann's idea

$\Pr\{\text{H-T}\} = \Pr\{\text{T-H}\} = p\,(1-p)$

$\Pr\{\text{someone wins at a given turn}\} = \Pr\{\text{T-H}\} + \Pr\{\text{H-T}\} = 2\,p\,(1-p)$

$$\text{expected \# flips until someone wins} = 2 \times \frac{1}{2\,p\,(1-p)} = \frac{1}{p\,(1-p)}$$

many variations/improvements ever since, e.g.

P. Elias, The efficient construction of an unbiased random sequence, *The Annals of Mathematical Statistics* **43** (1972) 865–870.

Q. F. Stout, B. Warren, Tree algorithms for unbiased coin tossing with a biased coin, *The Annals of Probability* **12** (1984) 212–222.

S. Vembu, S. Verdú, Generating random bits from an arbitrary source: fundamental limits, *IEEE Transactions on Information Theory* **41** (1995) 1322–1332.

A. Srinivasan, D. Zuckerman, Computing with very weak random sources, *SIAM Journal on Computing* **28** (1999) 1433–1459.

Concealed biased coins

- a coin that is possibly biased (the exact bias is unknown)
- the players are not able to know whether the coin flip resulted H or T
- it is possible to infer a (mis)match between the two latest results

Concealed biased coins

- a coin that is possibly biased (the exact bias is unknown)
- the players are not able to know whether the coin flip resulted H or T
- it is possible to infer a (mis)match between the two latest results

a hand clap (Cl)

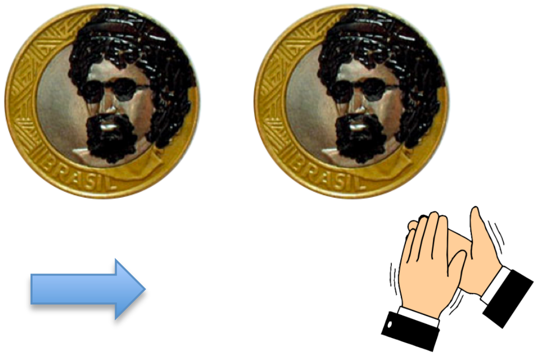
the latest result is **the same** as the previous

a whistle (W)

the latest result is **different** from the previous

Hand claps and whistles

Hand claps and whistles



Hand claps and whistles

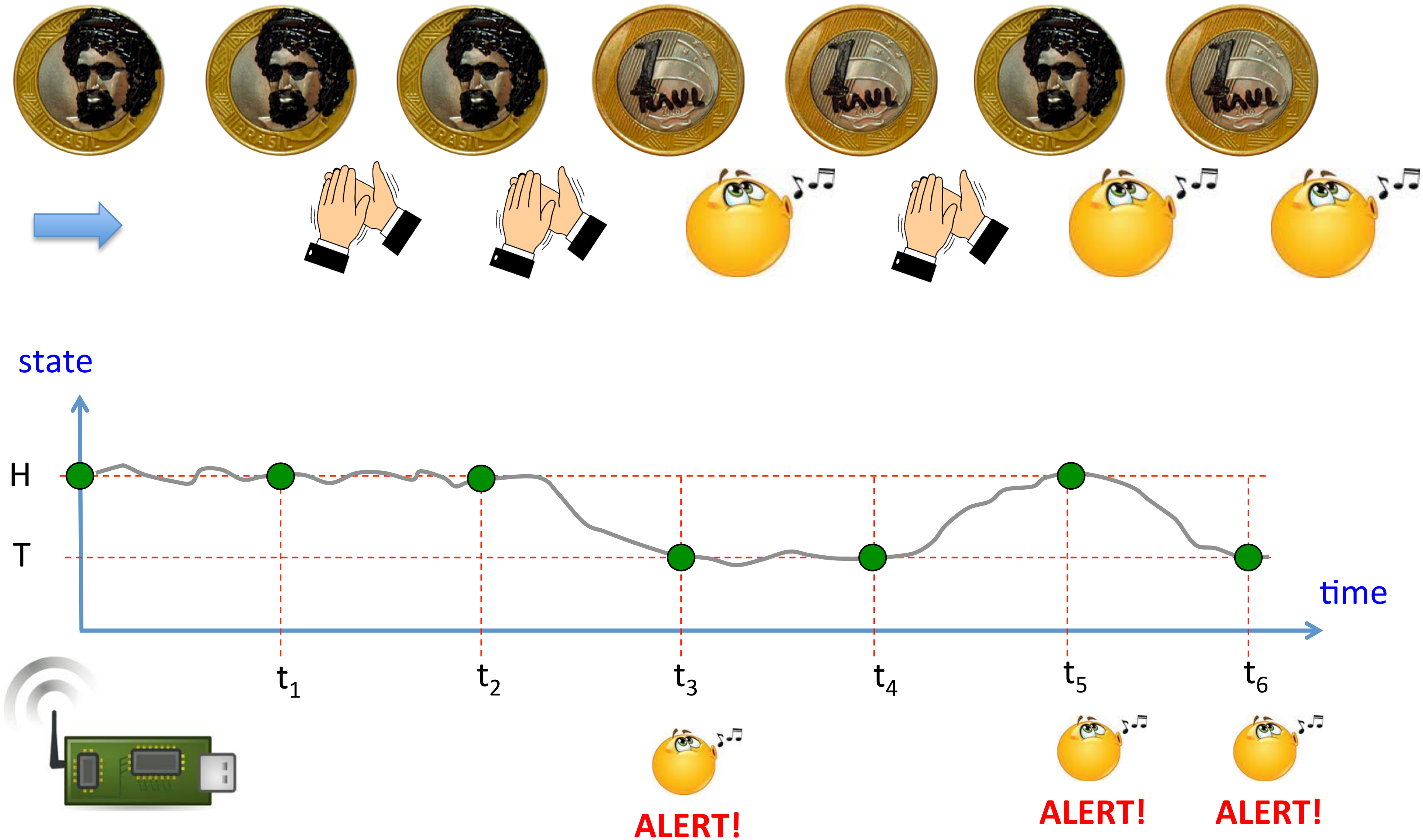
Hand claps and whistles

Hand claps and whistles

Hand claps and whistles

Hand claps and whistles

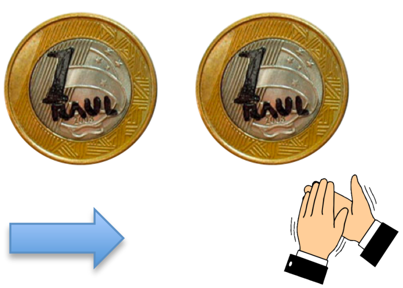
Hand claps and whistles



First attempt: Cl vs. W (2 flips)

Player 1: Cl

or



Player 2: W

or

$\boxed{p = \Pr\{\mathrm{H}\}}$

$$P_1 \;=\; \Pr\{\text{Player 1 wins}\} \;=\; p^2 + (1-p)^2 \;=\; 2p^2 - 2p + 1$$

First attempt: Cl vs. W (2 flips)

Player 1: Cl

Player 2: W

$$\boxed{p = \Pr\{\mathrm{H}\}}$$

$$P_1 \;=\; \Pr\{\text{Player 1 wins}\} \;=\; p^2 + (1-p)^2 \;=\; 2p^2 - 2p + 1$$

Second attempt: Cl-W vs. W-Cl (initial + 2 flips per turn)

Player 1: Cl-W

…………H | H | T

Cl W

or

…………T | T | H

Cl W

Player 2: W-Cl

…………T | H | H

W Cl

or

…………H | T | T

W Cl

From now on…

H

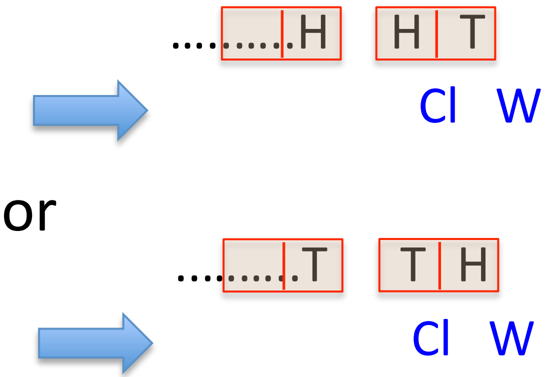
T

Cl

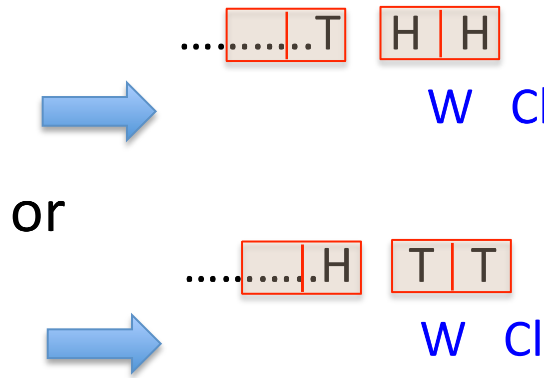
W

Second attempt: Cl-W vs. W-Cl (initial + 2 flips per turn)

Player 1: Cl-W



Player 2: W-Cl



P_1^H := probability that Player 1 wins the game provided the first coin flip yields a H

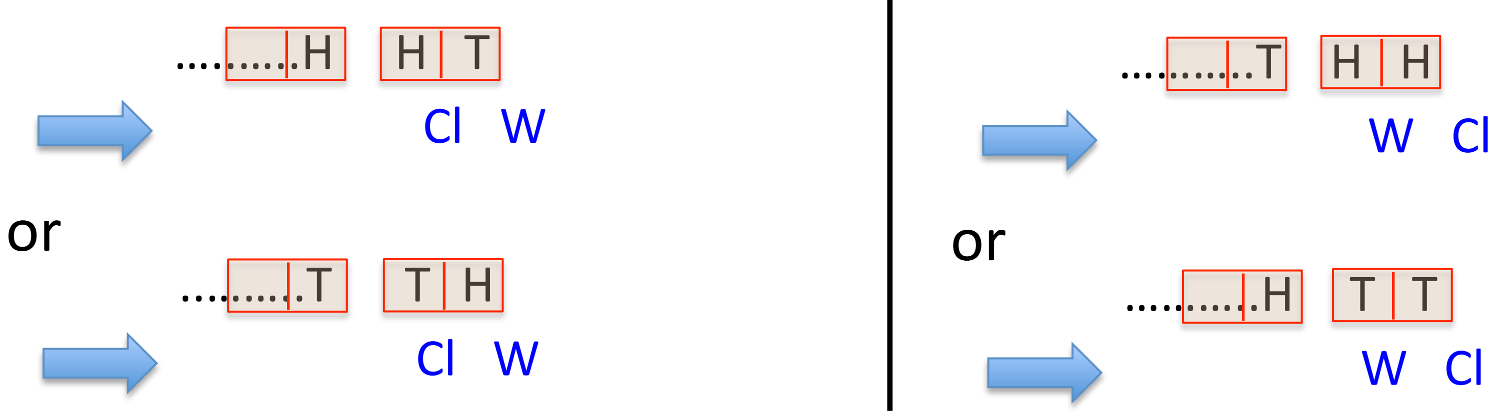
$$P_1 = P_1^H \cdot p + P_1^T \cdot (1-p)$$

$$\boxed{\mathcal{S} = \{\text{H-H, H-T, T-H, T-T}\}}$$

$$\begin{aligned} P_1^H &= \sum_{S \in \mathcal{S}} \Pr\{P_1^H \mid S\} \cdot \Pr\{S\} \\ &= P_1^H \cdot p^2 + 1 \cdot p(1-p) + P_1^H \cdot (1-p)p + 0 \cdot (1-p)^2 = p \end{aligned}$$

Second attempt: Cl-W vs. W-Cl (initial + 2 flips per turn)

Player 1: Cl-W | **Player 2: W-Cl**



P_1^H := probability that Player 1 wins the game provided the first coin flip yields a H

$$P_1 = P_1^H \cdot p + P_1^T \cdot (1-p)$$

$$\boxed{\mathcal{S} = \{\text{H-H, H-T, T-H, T-T}\}}$$

$$\boxed{P_1 = p^2 + (1-p)^2 = 2p^2 - 2p + 1}$$

$$\begin{aligned} P_1^H &= \sum_{S \in \mathcal{S}} \Pr\{P_1^H \mid S\} \cdot \Pr\{S\} \\ &= P_1^H \cdot p^2 + 1 \cdot p(1-p) + P_1^H \cdot (1-p)p + 0 \cdot (1-p)^2 = p \end{aligned}$$

Second attempt: Cl-W vs. W-Cl (initial + 2 flips per turn)

Player 1: Cl-W

….......H H | T

Cl W

or

….......T T | H

Player 2: W-Cl

….......T H | H

W Cl

W Cl

Not fair!

P_1^H := probabil… first coin flip yields a H

$P_1 = P_1^H \cdot p + P_1^T \cdot (1 - \ldots$

$$\boxed{\mathcal{S} = \{\text{H-H, H-T, T-H, T-T}\}}$$

$$\boxed{P_1 = p^2 + (1-p)^2 = 2p^2 - 2p + 1}$$

$$P_1^H = \sum_{S \in \mathcal{S}} \Pr\{P_1^H \mid S\} \cdot \Pr\{S\}$$

$$= P_1^H \cdot p^2 + 1 \cdot p(1-p) + P_1^H \cdot (1-p)p + 0 \cdot (1-p)^2 = p$$

Third attempt: Cl-W vs. W-Cl (4 flips per turn)

Player 1: Cl-W

| H | H | T | H |

→ • Cl • W

or

| H | H | H | T |

→ • Cl • W

or

| T | T | T | H |

→ • Cl • W

or

| T | T | H | T |

→ • Cl • W

Player 2: W-Cl

| H | T | H | H |

→ • W • Cl

or

| T | H | H | H |

→ • W • Cl

or

| H | T | T | T |

→ • W • Cl

or

| T | H | T | T |

→ • W • Cl

Third attempt: Cl-W vs. W-Cl (4 flips per turn)

Player 1: Cl-W

H	H	T	H

• Cl • W

or

H	H	H	T

• Cl • W

or

T	T	T	H

• Cl • W

or

T	T	H	T

• Cl • W

Player 2: W-Cl

H	T	H	H

• W • Cl

or

T	H	H	H

• W • Cl

or

H	T	T	T

• W • Cl

or

T	H	T	T

• W • Cl

$$\text{expected \# flips until someone wins} = \frac{1}{-2p^4 + 4p^3 - 3p^2 + p}$$

Third attempt: Cl-W vs. W-Cl (4 flips per turn)

$$\text{expected \# flips until someone wins} = \frac{1}{-2p^4 + 4p^3 - 3p^2 + p}$$

Third attempt: Cl-W vs. W-Cl (4 flips per turn)

$$\text{expected \# flips until someone wins} = \frac{1}{-2p^4 + 4p^3 - 3p^2 + p}$$

$$\text{expected \# flips (regular von Neumann's)} = \frac{1}{p\,(1 - p)}$$

Third attempt: Cl-W vs. W-Cl (4 flips per turn)

expected # flips until someone wins $= \dfrac{1}{-2p^4 + 4p^3 - 3p^2 + p}$

$\div$

expected # flips (regular von Neumann's) $= \dfrac{1}{p\,(1-p)}$

$= \dfrac{1}{2p^2 - 2p + 1}$

for $0 < p < 1$, this means up to twice the number of flips!!

Our method: W*-Cl vs. W*-W (2 flips per turn + final)

Player 1: W*-Cl

..........H H

- W* Cl

or

..........T T

- W* Cl

Player 2: W*-W

..........H T

- W* W

or

..........T H

- W* W

W* := a whistle of even parity

Our method: W*-Cl vs. W*-W (2 flips per turn + final)

Player 1: W*-Cl

..........H H

• W* Cl

or

..........T T

• W* Cl

Player 2: W*-W

..........H T

• W* W

or

..........T H

• W* W

W* := a whistle of even parity

the three last flips

.... A | B C

W*

Our method: W*-Cl vs. W*-W (2 flips per turn + final)

Player 1: W*-Cl

.........H H

• W* Cl

or

.........T T

• W* Cl

Player 2: W*-W

.........H T

• W* W

or

.........T H

• W* W

W* := a whistle of even parity

the three last flips

.... A B C

W*

$$\Pr\{C \neq B \mid B \neq A\} = \Pr\{C = B \mid B \neq A\} = 0.5$$

Perfectly fair!

Our method: W*-Cl vs. W*-W (2 flips per turn + final)

Player 1: W*-Cl

.........H H

• W* Cl

or

.........T T

• W* Cl

Player 2: W*-W

.........H T

• W* W

or

.........T H

• W* W

W* := a whistle of even parity

W* occurs by the end of a "H-T" or a "T-H" turn

$\Pr\{W^*\} = 2\,p\,(1-p)$

expected # flips until someone wins $= 2 \times \dfrac{1}{2\,p\,(1-p)} + 1 = \boxed{\dfrac{1}{p\,(1-p)} + 1}$

Our method: W*-Cl vs. W*-W (2 flips per turn + final)

Player 1: W*-Cl

………H H

• W* Cl

or

………T T

• W* Cl

Player 2: W*-W

………H T

• W* W

or

………T H

• W* W

W* := a whistle of even parity

W* occurs by the end of a "H-T" or a "T-H" turn

$\Pr\{W^*\} = 2\,p\,(1-p)$

expected # flips until someone wins $= 2 \times \dfrac{1}{2\,p\,(1-p)} + 1 =$  $+ 1$



Thank you!


Biased coins, blindfold players

Vinícius G. Pereira de Sá

based on the paper "Blind-friendly von Neumann's heads or tails",
to appear in The American Mathematical Monthly,
joint work with Celina M. H. de Figueiredo

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
UFRJ