Robust Coin Flipping

Gene Kopp and John Wiltshire-Gordon

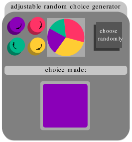
University of Chicago

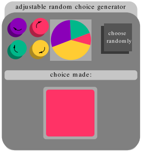
gkopp@uchicago.edu
jwiltshiregordon@uchicago.edu

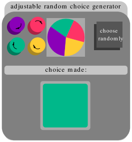
August 16, 2011

The Problem

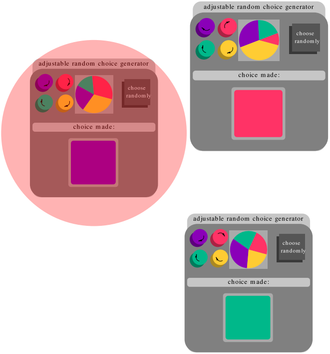
The Problem


adjustable random choice generator
choose randomly
choice made:


adjustable random choice generator
choose randomly
choice made:

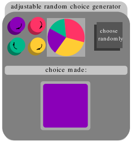

adjustable random choice generator
choose randomly
choice made:

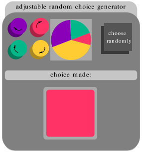
The Problem

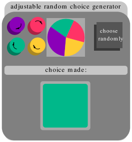

adjustable random choice generator
choose randomly
choice made:
adjustable random choice generator
choose randomly
choice made:
adjustable random choice generator
choose randomly
choice made:

The Problem

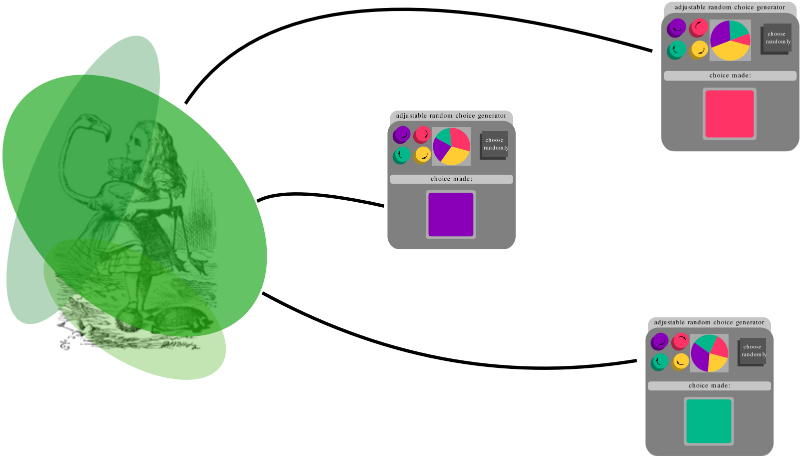
The Problem


adjustable random choice generator
choose randomly
choice made:


adjustable random choice generator
choose randomly
choice made:

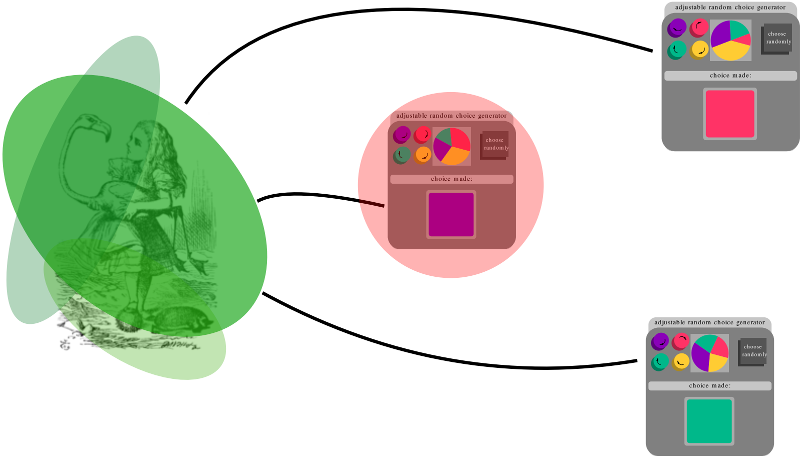

adjustable random choice generator
choose randomly
choice made:

The Problem



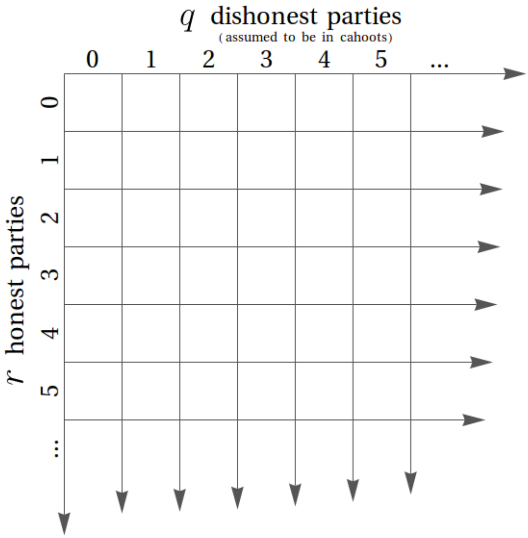
adjustable random choice generator
choose randomly
choice made:
adjustable random choice generator
choose randomly
choice made:
adjustable random choice generator
choose randomly
choice made:

The Problem



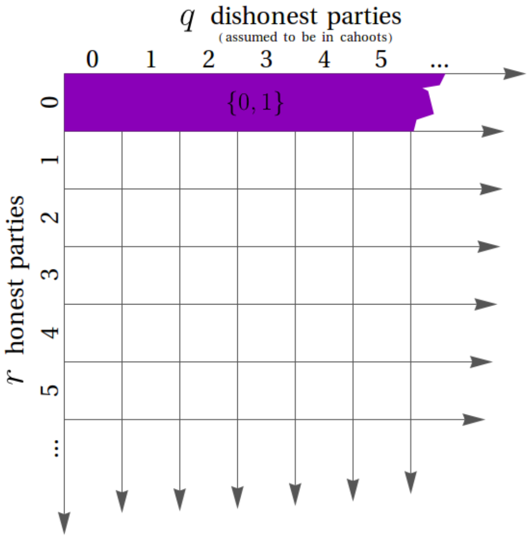
adjustable random choice generator
choose randomly
choice made:
adjustable random choice generator
choose randomly
choice made:
adjustable random choice generator
choose randomly
choice made:

Results



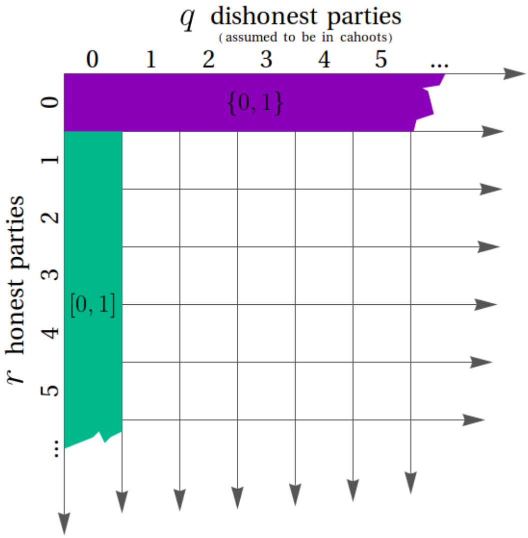
q dishonest parties
(assumed to be in cahoots)
0 1 2 3 4 5 ...
r honest parties
0 1 2 3 4 5 ...

Results



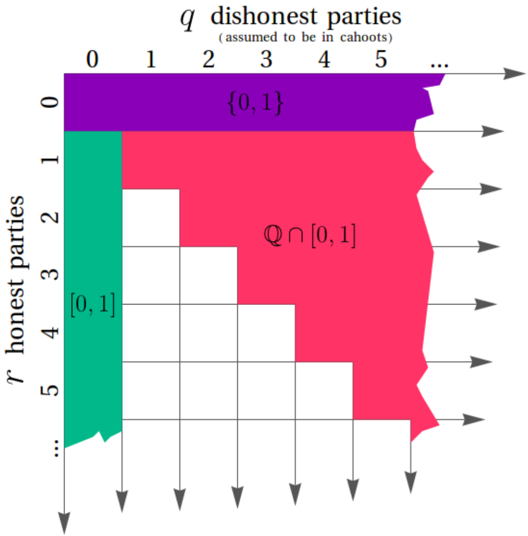
q dishonest parties
(assumed to be in cahoots)
0 1 2 3 4 5 ...
r honest parties
0 1 2 3 4 5 ...
$\{0, 1\}$

Results



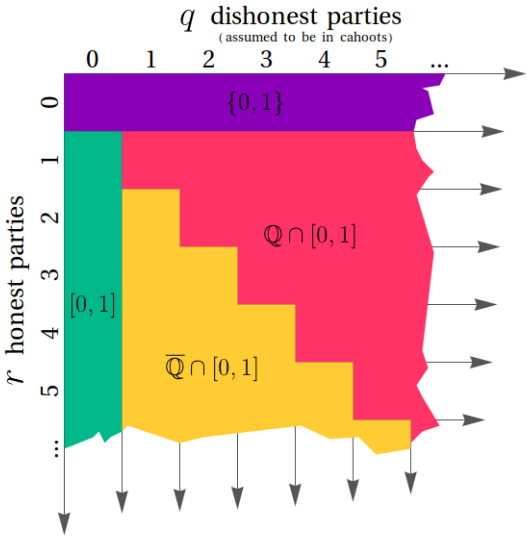
q dishonest parties
(assumed to be in cahoots)
0 1 2 3 4 5 ...
{0, 1}
r honest parties
0 1 2 3 4 5 ...
[0, 1]

Results



q dishonest parties
(assumed to be in cahoots)
0 1 2 3 4 5 ...
r honest parties
0 1 2 3 4 5 ...
$\{0,1\}$
$\mathbb{Q} \cap [0,1]$
$[0,1]$

Results



q dishonest parties
(assumed to be in cahoots)
0 1 2 3 4 5 ...
r honest parties
0 1 2 3 4 5 ...
$\{0,1\}$
$[0,1]$
$\mathbb{Q} \cap [0,1]$
$\overline{\mathbb{Q}} \cap [0,1]$

Results

Theorem (KW)

Alice has access to $p = q + r$ indistinguishable random oracles, q unreliable and r reliable.

- *For $r = 0$, Alice can simulate only an always-heads or always-tails coin.*
- *For $0 < q \leq r$, any rational bias α is possible, and nothing else.*
- *For $q > r > 0$, any algebraic probability α is possible, and nothing else.*
- *For $q = 0$ and $r > 0$, any bias is possible.*

Algebraic α?

Q: Why would anyone want to choose anything with irrational probabilities?

Algebraic α?

Q: Why would anyone want to choose anything with irrational probabilities?

A: Shows up in applications (e.g. Nash equilibria).

Algebraic α?

Q: Why would anyone want to choose anything with irrational probabilities?

A: Shows up in applications (e.g. Nash equilibria).

Q: Why don't we just approximate by rationals?

Algebraic α?

Q: Why would anyone want to choose anything with irrational probabilities?

A: Shows up in applications (e.g. Nash equilibria).

Q: Why don't we just approximate by rationals?

A: If Alice simulates an (a/b)-biased bit, her communication with the oracles and her computation of the bit will both be linear in $\log b$.

Algebraic α?

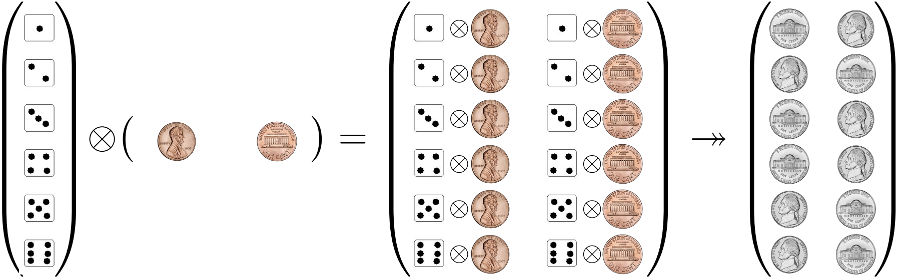
Q: Why would anyone want to choose anything with irrational probabilities?

A: Shows up in applications (e.g. Nash equilibria).

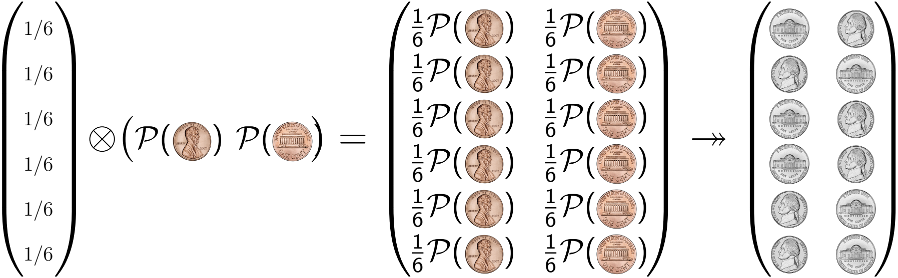
Q: Why don't we just approximate by rationals?

A: If Alice simulates an (a/b)-biased bit, her communication with the oracles and her computation of the bit will both be linear in $\log b$. In our solution (without rational approximation), Alice's communication and computation stay constant even as her desired accuracy increases.

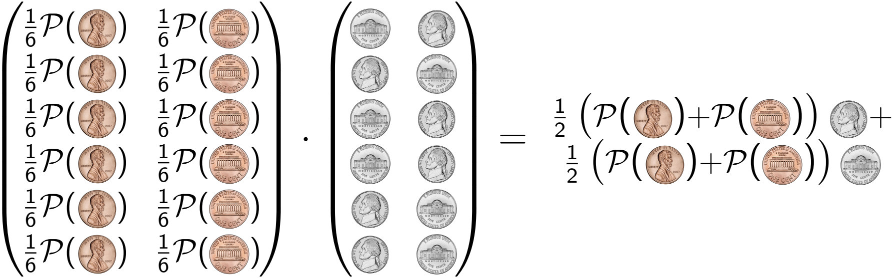
A Basic Example



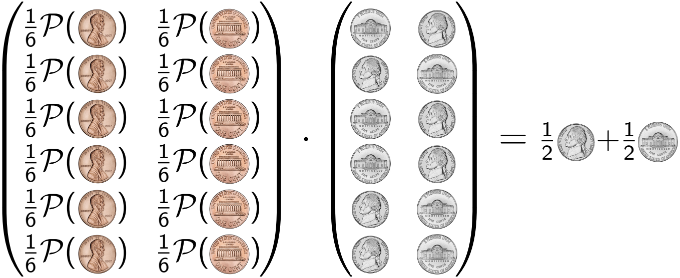
A Basic Example



A Basic Example



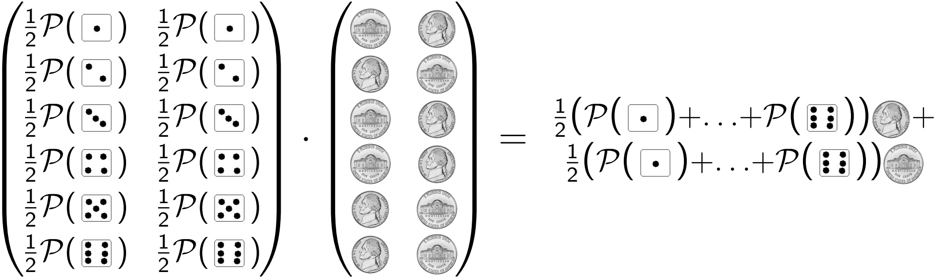
A Basic Example



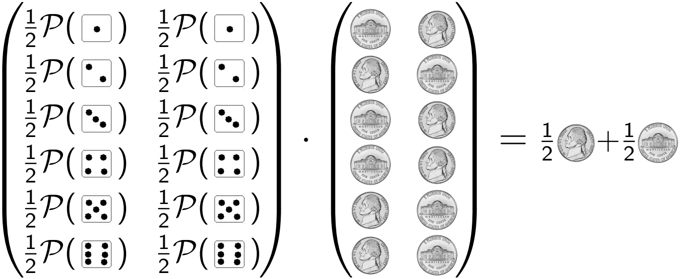
A Basic Example

$$\begin{pmatrix} \mathcal{P}(\text{⚀}) \\ \mathcal{P}(\text{⚁}) \\ \mathcal{P}(\text{⚂}) \\ \mathcal{P}(\text{⚃}) \\ \mathcal{P}(\text{⚄}) \\ \mathcal{P}(\text{⚅}) \end{pmatrix} \otimes \begin{pmatrix} 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2}\mathcal{P}(\text{⚀}) & \frac{1}{2}\mathcal{P}(\text{⚀}) \\ \frac{1}{2}\mathcal{P}(\text{⚁}) & \frac{1}{2}\mathcal{P}(\text{⚁}) \\ \frac{1}{2}\mathcal{P}(\text{⚂}) & \frac{1}{2}\mathcal{P}(\text{⚂}) \\ \frac{1}{2}\mathcal{P}(\text{⚃}) & \frac{1}{2}\mathcal{P}(\text{⚃}) \\ \frac{1}{2}\mathcal{P}(\text{⚄}) & \frac{1}{2}\mathcal{P}(\text{⚄}) \\ \frac{1}{2}\mathcal{P}(\text{⚅}) & \frac{1}{2}\mathcal{P}(\text{⚅}) \end{pmatrix} \twoheadrightarrow$$

A Basic Example



A Basic Example



Rational α Is Easy

- Say $\alpha = \frac{a}{b}$.

Rational α Is Easy

- Say $\alpha = \frac{a}{b}$.
- Alice asks party i to pick uniformly a random $x_i \in \mathbb{Z}/b\mathbb{Z}$.

Rational α Is Easy

- Say $\alpha = \frac{a}{b}$.
- Alice asks party i to pick uniformly a random $x_i \in \mathbb{Z}/b\mathbb{Z}$.
- Heads if $\sum_{i=1}^{p} x_i \in \{0, ..., a-1\}$; tails otherwise.

Rational α Is Easy

- Say $\alpha = \frac{a}{b}$.
- Alice asks party i to pick uniformly a random $x_i \in \mathbb{Z}/b\mathbb{Z}$.
- Heads if $\sum_{i=1}^{p} x_i \in \{0, ..., a-1\}$; tails otherwise.

Works as long as $q < p$.

Multilinear Algebra

For $p = 3$, $q = 1$, we want to find a $\{0, 1\}$-hypermatrix A and probability vectors $\beta^{(i)}$ such that, for all probability vectors $x^{(i)}$,

$$A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) = A(\beta^{(1)}, x^{(2)}, \beta^{(3)}) = A(\beta^{(1)}, \beta^{(2)}, x^{(3)}) = \alpha.$$

Multilinear Algebra

For $p = 3$, $q = 1$, we want to find a $\{0,1\}$-hypermatrix A and probability vectors $\beta^{(i)}$ such that, for all probability vectors $x^{(i)}$,

$$A(x^{(1)}, \beta^{(2)}, \beta^{(3)}) = A(\beta^{(1)}, x^{(2)}, \beta^{(3)}) = A(\beta^{(1)}, \beta^{(2)}, x^{(3)}) = \alpha.$$

So, $\alpha J - A$ is degenerate in the sense of Gelfand, Kapranov, and Zelevinsky, and the theory of complex projective duality and stratification shows that α lies on a zero-dimensional variety defined over $\mathbb{Q}$. But positive results are more fun...

Multilinear Algebra

$$A = \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{array} \right)$$

$$\beta^{(1)} = \left(\begin{array}{c|c} \frac{1}{2}(-1+\sqrt{5}) & \frac{1}{2}(3-\sqrt{5}) \end{array} \right)$$

$$\beta^{(2)} = \begin{pmatrix} \frac{1}{2}(3-\sqrt{5}) \\ \frac{1}{2}(-1+\sqrt{5}) \end{pmatrix}$$

$$\beta^{(3)} = \begin{pmatrix} \frac{1}{10}(5-\sqrt{5}) & \frac{1}{10}(5-\sqrt{5}) & \frac{1}{5}\sqrt{5} \end{pmatrix}$$

$$\alpha = ?$$

- Read our paper!
- Play around with our code!
- arxiv.org/abs/1009.4188