Title: Quantum weak coin flipping with arbitrarily small bias

Date: Mar 05, 2008 04:00 PM

URL: http://pirsa.org/08020038

Abstract: Coin flipping by telephone (Blum \'81) is one of the most basic cryptographic tasks of two-party secure computation. In a quantum setting, it is possible to realize (weak) coin flipping with information theoretic security. Quantum coin flipping has been a longstanding open problem, and its solution uses an innovative formalism developed by Alexei Kitaev for mapping quantum games into convex optimization problems. The optimizations are carried out over duals to the cone of operator monotone functions, though the mapped problem can also be described in a very simple language that involves moving points in the plane. Time permitting, I will discuss both Kitaev\'s formalism, and the solution that leads to quantum weak coin flipping with arbitrarily small bias.

Quantum weak coin flipping
(with laughably small bias)

Carlos Mochon

Perimeter Institute for Theoretical Physics
Waterloo, Canada

(includes work/miracles by Alexei Kitaev)

Talk based on arXiv:0711.4114

Outline

1. Coin flipping: What? Why?

2. The Kitaev^{TM} formalism

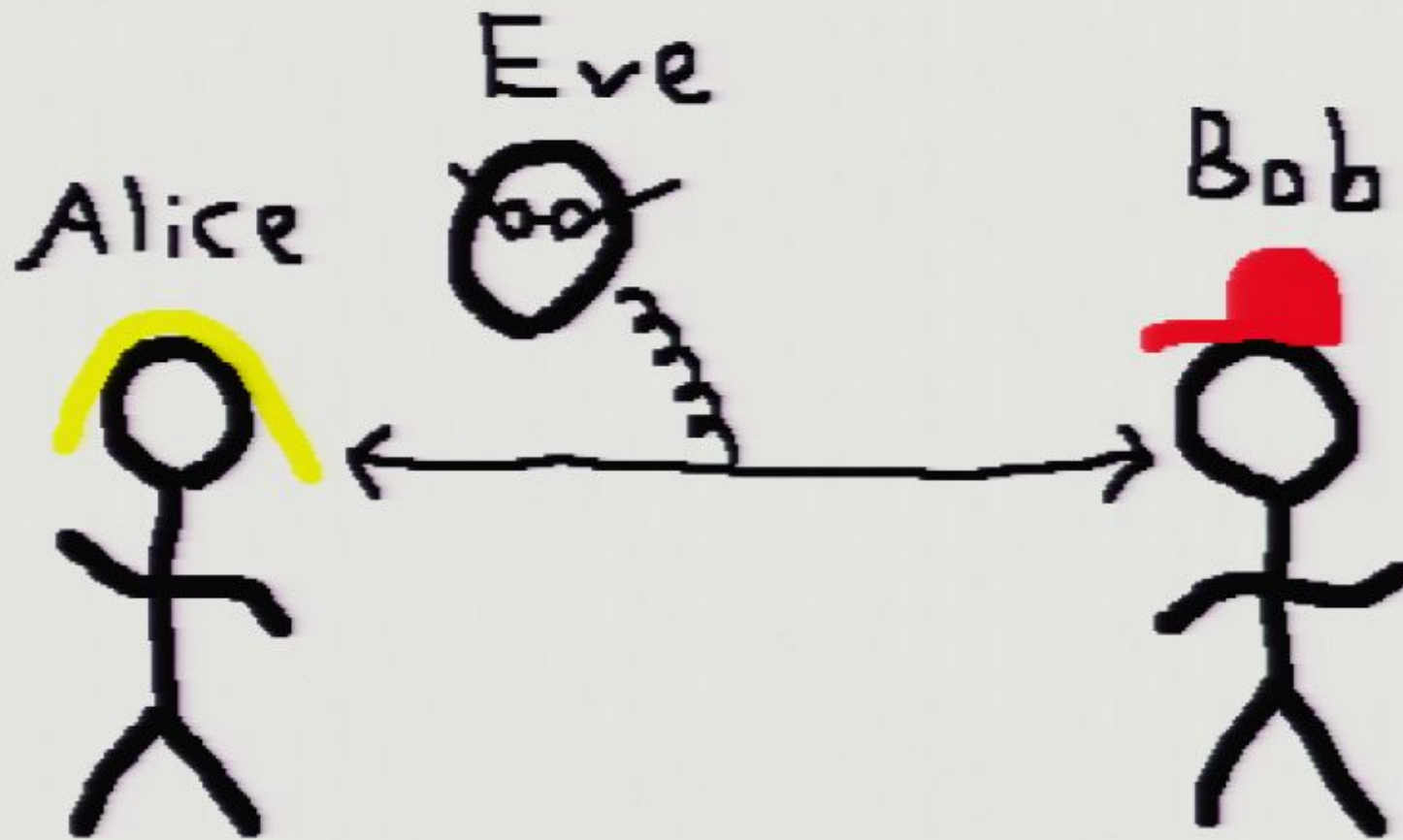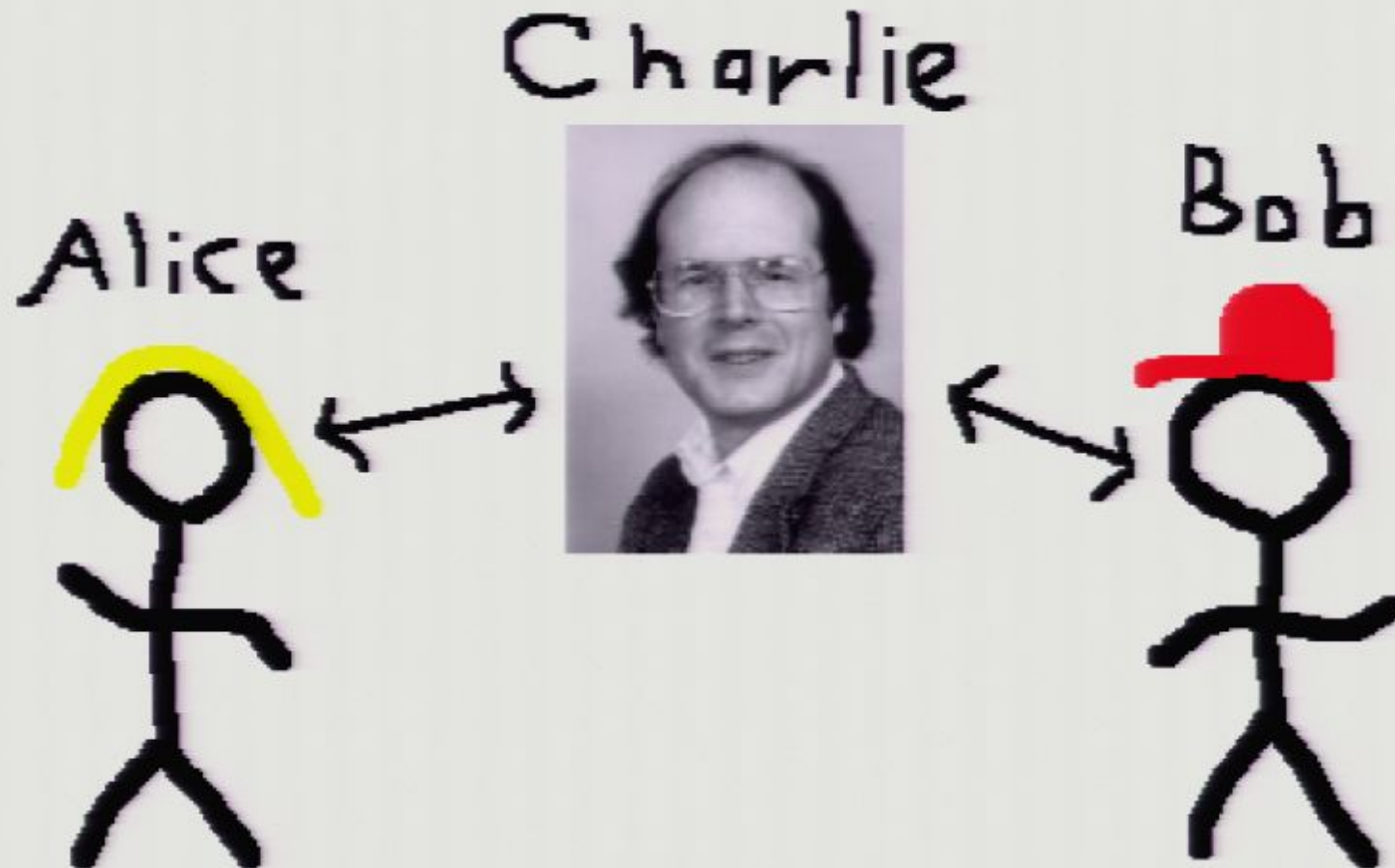3. Lots of pretty pictures

The coin slide

Queen

Bear

Crypto I: Alice and Bob vs. Eve

Crypto II: A benevolent Charlie helps Alice and Bob

Secure two-party computation

- Alice and Bob:
  - Do not trust each other.
  - Want to work together.

- Example: Find meeting time without revealing schedules.

- Classically impossible with information theoretic security.

Is quantum information useful here?

Quantum secure two-party computation

Bit commitment

- A universal primitive.
- Proven impossible!
  (Mayers, Lo and Chau 1996)

Coin flipping (by telephone)

- Classical problem studied by Manuel Blum (1981).
- Quantum problem...

Bit commitment with cheat detection

- Aharonov et al. (2000) and Hardy and Kent (2003).
- + (your name here) (2008)

Coin flipping (by telephone)

Basic rules

- Starting state: uncorrelated.
- Alice and Bob send messages to each other.
- At the end, each player outputs zero or one.
- Their outputs should agree and be random (when honest).

Cheating players:

- Can output anything they want.
- Want to control the honest player's output.

Parameters

- P_A^* is the maximum probability for Alice to win by cheating.
- The bias is defined as $\max(P_A^*, P_B^*) - \frac{1}{2}$.

Variations on coin flipping

Quantum vs classical

- Information theoretic security.
- No transcript.

Strong vs weak

- Strong: neither player can bias the coin in either direction.
- Weak: Alice wins on 0, Bob wins on 1.
  We don't care if they cheat to lose.

Coin flipping (by telephone)

Basic rules

- Starting state: uncorrelated.
- Alice and Bob send messages to each other.
- At the end, each player outputs zero or one.
- Their outputs should agree and be random (when honest).

Cheating players:

- Can output anything they want.
- Want to control the honest player's output.

Parameters

- P_A^* is the maximum probability for Alice to win by cheating.
- The bias is defined as $\max(P_A^*, P_B^*) - \frac{1}{2}$.

Variations on coin flipping

Quantum vs classical

- Information theoretic security.
- No transcript.

Strong vs weak

- Strong: neither player can bias the coin in either direction.
- Weak: Alice wins on 0, Bob wins on 1.
  We don't care if they cheat to lose.

Why is coin flipping hard?

- Idea 1:
  Start with a shared EPR and measure it.

- Idea 2:
  "I'll prepare an EPR and send you your half."

- Idea 3:
  "You prepare two EPR pairs, I'll choose one as the coin and use the other one for verification."

- Idea 4:
  "Let us have lots of EPRs, we'll check most of them, and one of the remaining ones will be used as the coin."

Impossibility of strong coin flipping

Best lower bound (Kitaev 2003)

For any quantum strong coin flipping protocol:

$$P_A^* P_B^* \geq \frac{1}{2}.$$

Best protocol

$$P_A^* = P_B^* = \frac{3}{4}$$

by Ambainis (2001) and Spekkens and Rudolph (2001) (and now me too using weak CF (2007)).

What about weak coin flipping?

Lower bound on weak coin flipping:

$$\text{\# rounds} >= \Omega\left(\log\log\frac{1}{\epsilon}\right),$$

where ϵ is the bias. Proven by Ambainis (2001).

- Arbitrarily small bias $\Rightarrow$ arbitrarily many rounds.
- It is hard to build protocols that get better with more rounds.

Weak coin flipping protocols

Prior work: Goldenberg, Vaidman, Wiesner, Kerenidis, Nayak, Ambainis, Spekkens, Rudolph, Kitaev and more.

The slow journey towards zero bias

- Spekkens and Rudolph (2002): $P_A^* = P_B^* = \frac{1}{\sqrt{2}} \simeq 0.707$.

- me (2004): $P_A^* = P_B^* \rightarrow \exp\left[-\frac{2}{\sqrt{7}} \arctan \frac{\sqrt{7}}{5}\right] \simeq 0.692$.

- me (2005): $P_A^* = P_B^* \rightarrow \frac{2}{3}$.

- me (2007): $P_A^* = P_B^* \rightarrow \frac{1}{2}$.

Why?

1. Potentially useful.

2. May help bit commitment with cheat detection.

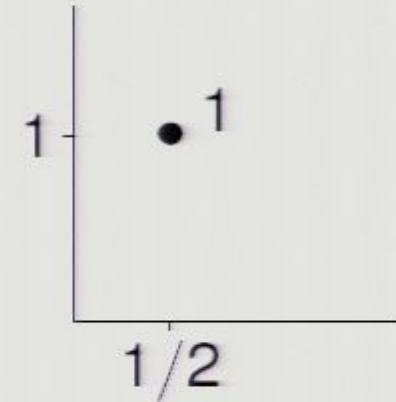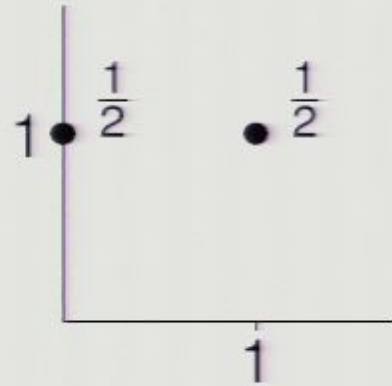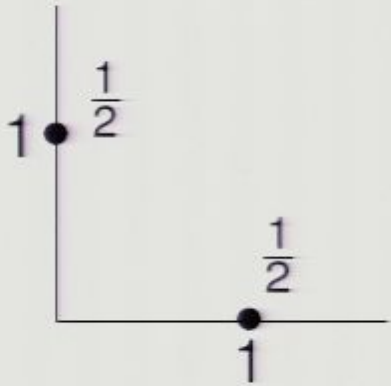3. "My research will help us better understand the mysteries of quantum information."

Outline

1. Coin flipping: What? Why?

2. The Kitaev^{TM} formalism

3. Lots of pretty pictures

The Kitaev$^{\text{TM}}$ formalism

Transition rules

- Probability is conserved.
- $\sum_z \frac{\lambda z}{\lambda + z} p_z \leq \sum_{z'} \frac{\lambda z'}{\lambda + z'} p_{z'}$ for all $\lambda \in (0, \infty)$.

Elements of a coin flipping protocol

Protocol

$\simeq$ Initial states + unitaries + final measurement

Optimization problem for P_A^*

$=$ Semidefinite program (SDP).

Optimization problem for P_B^*

$=$ Semidefinite program (SDP).

Goal:
$$\inf_{\text{protocols}} \left\{ \sup_{\text{SDPs}} \left[\max(P_A^*, P_B^*) \right] \right\}$$

Upper-bounded protocol (UBP)

Protocol

$\simeq$ Initial states $+$ unitaries $+$ final measurement

Certificate of upper bound on P_A^*

Dual SDP: $P_A^* \leq \alpha$.

Certificate of upper bound on P_B^*

Dual SDP: $P_B^* \leq \beta$.

Goal: $\displaystyle \inf_{\text{protocols}} \left\{ \inf_{\text{dual SDPs}} \left[\max(\alpha, \beta) \right] \right\} = \inf_{\text{UBPs}} \max(\alpha, \beta)$

Point games

- To do: eliminate irrelevant information from UBPs (e.g., choices of basis, phases).

- End result: a single convex cone.
  Every feasible quantum game is a point in this cone.

- Is coin flipping in the cone?
  - yes? prove it.
  - no? find separating hyperplane.

The Dual SDP for P_B^*

- Initial state: $\inf \beta \equiv \langle \psi_{A,0} | Z_{A,0} | \psi_{A,0} \rangle$.
- Unitary transitions:

$$Z_{A,i-1} \otimes I_{\mathcal{M}} \geq U_{A,i}^{\dagger} (Z_{A,i} \otimes I_{\mathcal{M}}) U_{A,i} \qquad i \text{ odd}$$
$$Z_{A,i-1} = Z_{A,i} \qquad i \text{ even}$$

- Final measurement: $Z_{A,n} = \Pi_{A,1}$.

Lemma

Given Hermitian operators $Z_{A,0}, \dots, Z_{A,n}$ and a number $\beta > 0$ satisfying the above constraints then

$$P_B^* \leq \beta.$$

Pruning excess information

Combine

- honest state σ (on $\mathcal{A}$ at some time i) and
- dual variable $Z \equiv \sum_z z \Pi^{[z]}$ (on $\mathcal{A}$ at some time i) to get

$$p(z) = \begin{cases} \text{Tr}[\Pi^{[z]}\sigma] & z \in \text{eig}(Z), \\ 0 & \text{otherwise.} \end{cases}$$

Crucial property of p(z)

For every function $f(z)$

$$\sum_z p(z)f(z) = \text{Tr}[\sigma f(Z)].$$

Valid transitions

What is the relation between p_i (constructed from σ_i and Z_i) and p_{i-1} (constructed from σ_{i-1} and Z_{i-1})?

Given a function $f(z)$ such that $X \geq Y \Rightarrow f(X) \geq f(Y)$ then

$$
\begin{aligned}
\sum_z p_{i-1}(z)f(z) &= \mathrm{Tr}[\sigma_{i-1}f(Z_{i-1})] \\
&= \langle \psi_{i-1} | \, f(Z_{i-1} \otimes I) \, | \psi_{i-1} \rangle \\
&\geq \langle \psi_{i-1} | \, f\left(U_i^{-1} (Z_i \otimes I) U_i \right) | \psi_{i-1} \rangle \\
&= \langle \psi_{i-1} | U_i^{-1} \, f(Z_i \otimes I) \, U_i | \psi_{i-1} \rangle \\
&= \langle \psi_i | \, f(Z_i \otimes I) \, | \psi_i \rangle \\
&= \mathrm{Tr}[\sigma_i f(Z_i)] = \sum_z p_i(z)f(z)
\end{aligned}
$$

Pruning excess information

Combine

- honest state σ (on $\mathcal{A}$ at some time i) and
- dual variable $Z \equiv \sum_z z \Pi^{[z]}$ (on $\mathcal{A}$ at some time i) to get

$$p(z) = \begin{cases} \mathrm{Tr}[\Pi^{[z]}\sigma] & z \in \mathrm{eig}(Z), \\ 0 & \text{otherwise.} \end{cases}$$

Crucial property of p(z)

For every function $f(z)$

$$\sum_z p(z)f(z) = \mathrm{Tr}[\sigma f(Z)].$$

Pruning excess information

Combine

- honest state σ (on $\mathcal{A}$ at some time i) and
- dual variable $Z \equiv \sum_z z \Pi^{[z]}$ (on $\mathcal{A}$ at some time i) to get

$$p(z) = \begin{cases} \mathrm{Tr}[\Pi^{[z]}\sigma] & z \in \mathrm{eig}(Z), \\ 0 & \text{otherwise.} \end{cases}$$

Crucial property of p(z)

For every function $f(z)$

$$\sum_z p(z)f(z) = \mathrm{Tr}[\sigma f(Z)].$$

The Dual SDP for P_B^*

- Initial state: $\inf \beta \equiv \langle \psi_{A,0} | Z_{A,0} | \psi_{A,0} \rangle$.
- Unitary transitions:

$$Z_{A,i-1} \otimes I_{\mathcal{M}} \geq U_{A,i}^\dagger (Z_{A,i} \otimes I_{\mathcal{M}}) U_{A,i} \qquad i \text{ odd}$$
$$Z_{A,i-1} = Z_{A,i} \qquad i \text{ even}$$

- Final measurement: $Z_{A,n} = \Pi_{A,1}$.

Lemma

Given Hermitian operators $Z_{A,0}, \ldots, Z_{A,n}$ and a number $\beta > 0$ satisfying the above constraints then

$$P_B^* \leq \beta.$$

The Dual SDP for P_B^*

- Initial state: $\inf \beta \equiv \langle \psi_{A,0} | Z_{A,0} | \psi_{A,0} \rangle$.
- Unitary transitions:

$$Z_{A,i-1} \otimes I_{\mathcal{M}} \geq U_{A,i}^{\dagger} (Z_{A,i} \otimes I_{\mathcal{M}}) U_{A,i} \qquad i \text{ odd}$$
$$Z_{A,i-1} = Z_{A,i} \qquad i \text{ even}$$

- Final measurement: $Z_{A,n} = \Pi_{A,1}$.

Lemma

Given Hermitian operators $Z_{A,0}, \ldots, Z_{A,n}$ and a number $\beta > 0$ satisfying the above constraints then

$$P_B^* \leq \beta.$$

Pruning excess information

Combine

- honest state σ (on $\mathcal{A}$ at some time i) and
- dual variable $Z \equiv \sum_z z \Pi^{[z]}$ (on $\mathcal{A}$ at some time i) to get

$$p(z) = \begin{cases} \text{Tr}[\Pi^{[z]}\sigma] & z \in \text{eig}(Z), \\ 0 & \text{otherwise.} \end{cases}$$

Crucial property of p(z)

For every function $f(z)$

$$\sum_z p(z)f(z) = \text{Tr}[\sigma f(Z)].$$

The Dual SDP for P_B^*

- Initial state: $\inf \beta \equiv \langle \psi_{A,0} | Z_{A,0} | \psi_{A,0} \rangle$.
- Unitary transitions:

$$Z_{A,i-1} \otimes I_{\mathcal{M}} \geq U_{A,i}^{\dagger} (Z_{A,i} \otimes I_{\mathcal{M}}) U_{A,i} \qquad i \text{ odd}$$
$$Z_{A,i-1} = Z_{A,i} \qquad i \text{ even}$$

- Final measurement: $Z_{A,n} = \Pi_{A,1}$.

Lemma

Given Hermitian operators $Z_{A,0}, \ldots, Z_{A,n}$ and a number $\beta > 0$ satisfying the above constraints then

$$P_B^* \leq \beta.$$

Valid transitions

What is the relation between p_i (constructed from σ_i and Z_i) and p_{i-1} (constructed from σ_{i-1} and Z_{i-1})?

Given a function $f(z)$ such that $X \geq Y \Rightarrow f(X) \geq f(Y)$ then

$$\sum_z p_{i-1}(z)f(z) = \mathrm{Tr}[\sigma_{i-1}f(Z_{i-1})]$$

$$= \langle\psi_{i-1}|\, f(Z_{i-1} \otimes I)\, |\psi_{i-1}\rangle$$
$$\geq \langle\psi_{i-1}|\, f\left(U_i^{-1}\,(Z_i \otimes I)\, U_i\right)\, |\psi_{i-1}\rangle$$
$$= \langle\psi_{i-1}|U_i^{-1}\, f\,(Z_i \otimes I)\; U_i|\psi_{i-1}\rangle$$
$$= \langle\psi_i|\, f\,(Z_i \otimes I)\, |\psi_i\rangle$$
$$= \mathrm{Tr}[\sigma_i f(Z_i)] = \sum_z p_i(z)f(z)$$

Operator monotone functions

Definition

A function $f(z) : [0, \infty) \to [0, \infty)$ is operator monotone if for all positive semidefinite operators X and Y

$$X \geq Y \Rightarrow f(X) \geq f(Y).$$

- $f(z) = 1$ and $f(z) = z$ are operator monotone.
- $f(z) = z^2$ is not operator monotone.
- The operator monotone functions form a convex cone.
- The extremal rays of the cone are generated by $f(z) = 1$ and $f(z) = z$ and

$$f(z) = \frac{\lambda z}{\lambda + z} \qquad \text{for all } \lambda \in (0, \infty).$$

Validity defined

Definition

$p \to p'$ is valid if for all operator monotone functions f

$$\sum_z p(z)f(z) \leq \sum_z p'(z)f(z).$$

Equivalently, $p \to p'$ is valid if probability is conserved and

$$\sum_z p(z)\frac{\lambda z}{\lambda + z} \leq \sum_z p'(z)\frac{\lambda z}{\lambda + z}$$

for all $\lambda \in (0, \infty)$.

The bipartite case

At some fixed time

- Let $|\psi\rangle$ be the honest state on $\mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$
- Let Z_A be the dual SDP variable on $\mathcal{A}$.
- Let Z_B be the dual SDP variable on $\mathcal{B}$.

$$p(x,y) = \begin{cases} \langle\psi|\Pi_A^{[x]} \otimes I_{\mathcal{M}} \otimes \Pi_B^{[y]}|\psi\rangle & x \in \mathrm{eig}(Z_A), y \in \mathrm{eig}(Z_B) \\ 0 & \text{otherwise,} \end{cases}$$

Reverse time convention: p_{n-i} constructed from $|\psi_i\rangle$, $Z_{A,i}$, $Z_{B,i}$

Bipartite validity

Definition

$p_i(x, y) \rightarrow p_{i+1}(x, y)$ is valid if either

- for all $c \in [0, \infty)$ the transition $p_i(z, \underline{c}) \rightarrow p_{i+1}(z, \underline{c})$ is valid, or
- for all $c \in [0, \infty)$ the transition $p_i(\underline{c}, z) \rightarrow p_{i+1}(\underline{c}, z)$ is valid,

where $p_i(z, \underline{c})$ is the one-variable function obtained by fixing the second input.

Putting it all together

Definition

A point game is a sequence $p_0 \to p_1 \to \cdots \to p_{n-1} \to p_n$ of valid transitions such that

$$p_0 = \frac{1}{2}[1, 0] + \frac{1}{2}[0, 1], \qquad\qquad p_n = 1[\beta, \alpha].$$

- Point games are equivalent to protocols + upper bounds.
- The mapping is constructive in both directions.
- There are excellent tools for proving lower bounds.
- The optimal point game produces the optimal protocol.

The bipartite case

At some fixed time

- Let $|\psi\rangle$ be the honest state on $\mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$
- Let Z_A be the dual SDP variable on $\mathcal{A}$.
- Let Z_B be the dual SDP variable on $\mathcal{B}$.

$$p(x,y) = \begin{cases} \langle\psi|\Pi_A^{[x]} \otimes I_{\mathcal{M}} \otimes \Pi_B^{[y]}|\psi\rangle & x \in \text{eig}(Z_A), y \in \text{eig}(Z_B) \\ 0 & \text{otherwise,} \end{cases}$$

Reverse time convention: p_{n-i} constructed from $|\psi_i\rangle$, $Z_{A,i}$, $Z_{B,i}$

Bipartite validity

Definition

$p_i(x, y) \to p_{i+1}(x, y)$ is valid if either

- for all $c \in [0, \infty)$ the transition $p_i(z, \underline{c}) \to p_{i+1}(z, \underline{c})$ is valid, or

- for all $c \in [0, \infty)$ the transition $p_i(\underline{c}, z) \to p_{i+1}(\underline{c}, z)$ is valid,

where $p_i(z, \underline{c})$ is the one-variable function obtained by fixing the second input.

Putting it all together

Definition

A point game is a sequence $p_0 \to p_1 \to \cdots \to p_{n-1} \to p_n$ of valid transitions such that

$$p_0 = \frac{1}{2}[1, 0] + \frac{1}{2}[0, 1], \qquad\qquad p_n = 1[\beta, \alpha].$$

- Point games are equivalent to protocols + upper bounds.
- The mapping is constructive in both directions.
- There are excellent tools for proving lower bounds.
- The optimal point game produces the optimal protocol.

From point games back to protocols

- Hilbert spaces

$$\mathcal{A} = \text{span}\{|x\rangle : x \geq 0\}, \qquad \mathcal{B} = \text{span}\{|y\rangle : y \geq 0\},$$
$$\mathcal{M} = \text{span}\{|x, y\rangle : x \geq 0, y \geq 0\}.$$

- SDP dual operators

$$Z_A = \sum_{x \geq 0} x|x\rangle\langle x|, \qquad Z_B = \sum_{y \geq 0} y|y\rangle\langle y|.$$

- States

$$|\psi_i\rangle = \sum_{x,y} \sqrt{p_{n-i}(x, y)}|x\rangle \otimes |x, y\rangle \otimes |y\rangle.$$

Outline

1. Coin flipping: What? Why?

2. The Kitaev^{TM} formalism

3. **Lots of pretty pictures**

Trivial protocol 1 (Alice flips the coin)
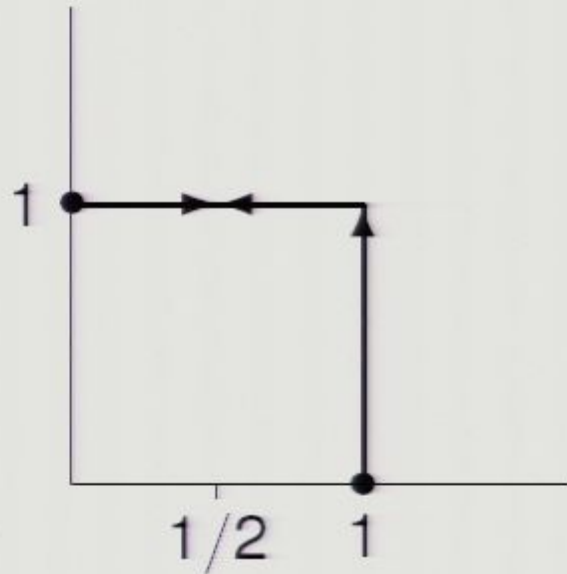
$$\frac{1}{2}[1,0] + \frac{1}{2}[0,1] \quad \rightarrow \quad \frac{1}{2}[1,1] + \frac{1}{2}[0,1] \quad \rightarrow \quad 1\left[\frac{1}{2},1\right]$$

Trivial protocol 2 (Bob flips the coin)
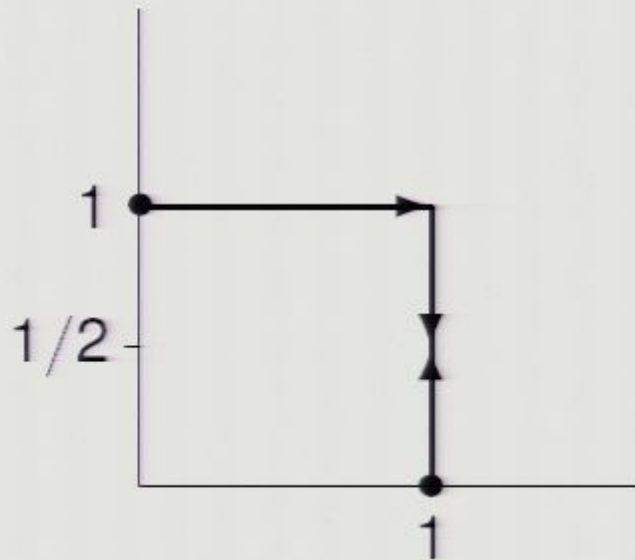
$$\frac{1}{2}[1,0] + \frac{1}{2}[0,1] \quad \rightarrow \quad \frac{1}{2}[1,0] + \frac{1}{2}[1,1] \quad \rightarrow \quad 1\left[1,\frac{1}{2}\right]$$
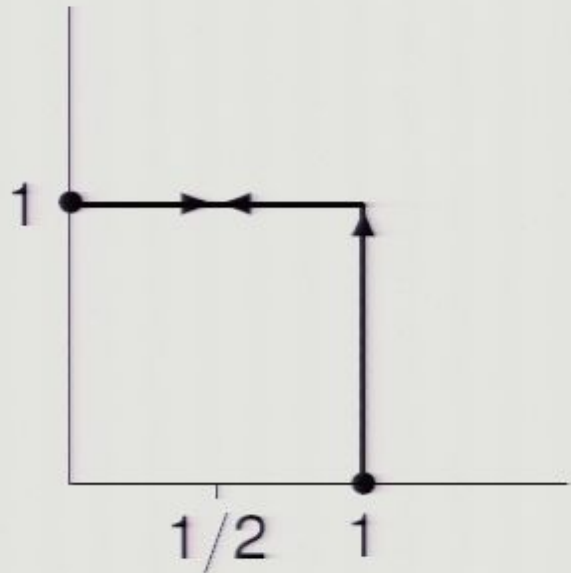
Alice flips the coin
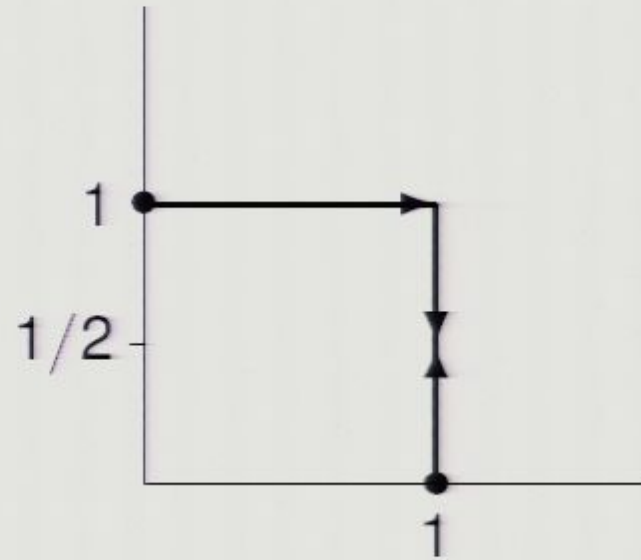
Bob flips the coin

Some simple valid transitions
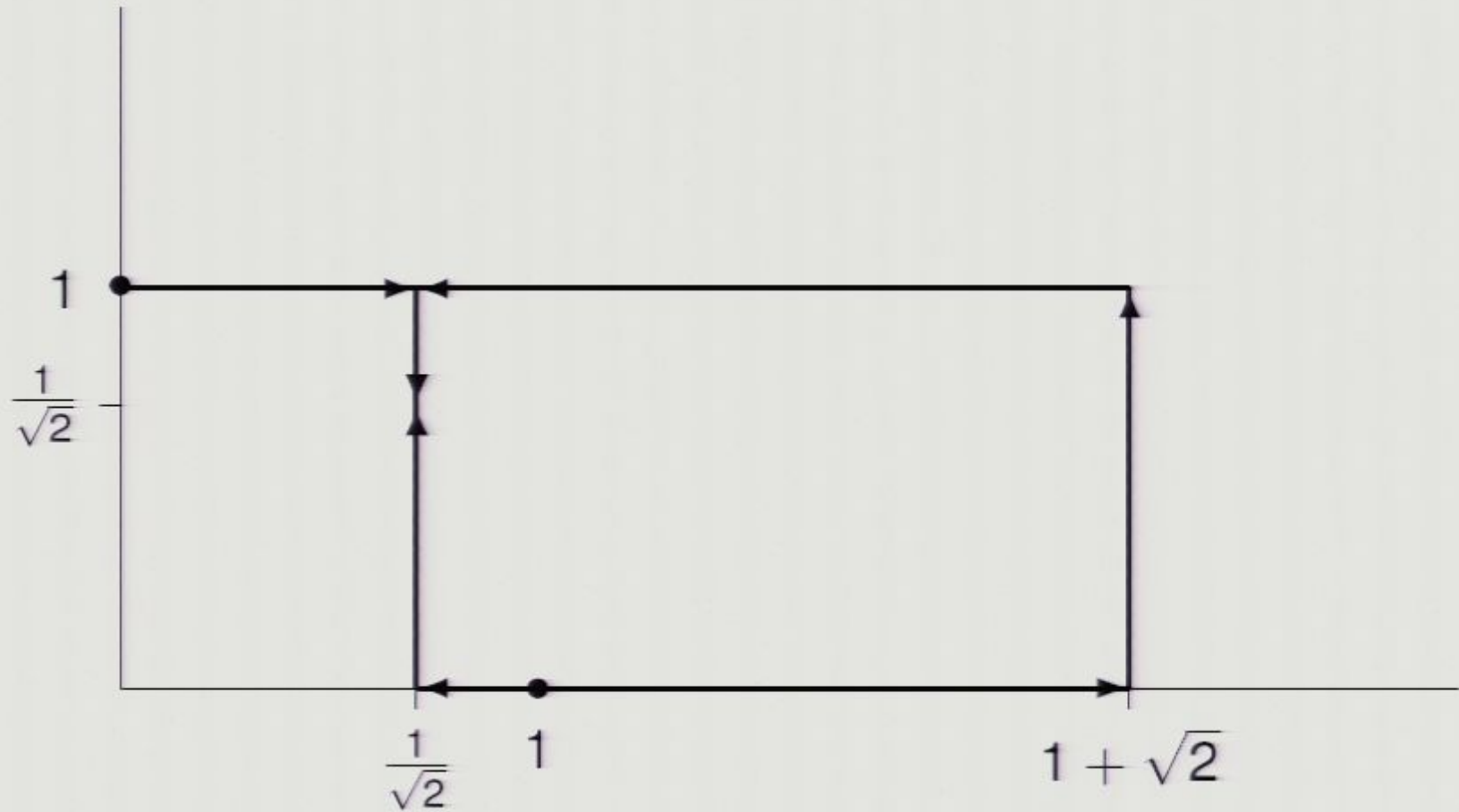
- Point raising

$$p[z] \to p[z'] \qquad \text{(for } z \le z').$$

- Point merging

$$p_1[z_1] + p_2[z_2] \to (p_1 + p_2) \left[\frac{p_1 z_1 + p_2 z_2}{p_1 + p_2} \right].$$

- Point splitting

$$(p_1 + p_2) \left[\frac{p_1 + p_2}{p_1 w_1' + p_2 w_2'} \right] \to p_1 \left[\frac{1}{w_1'} \right] + p_2 \left[\frac{1}{w_2'} \right].$$

Some simple valid transitions

- Point raising

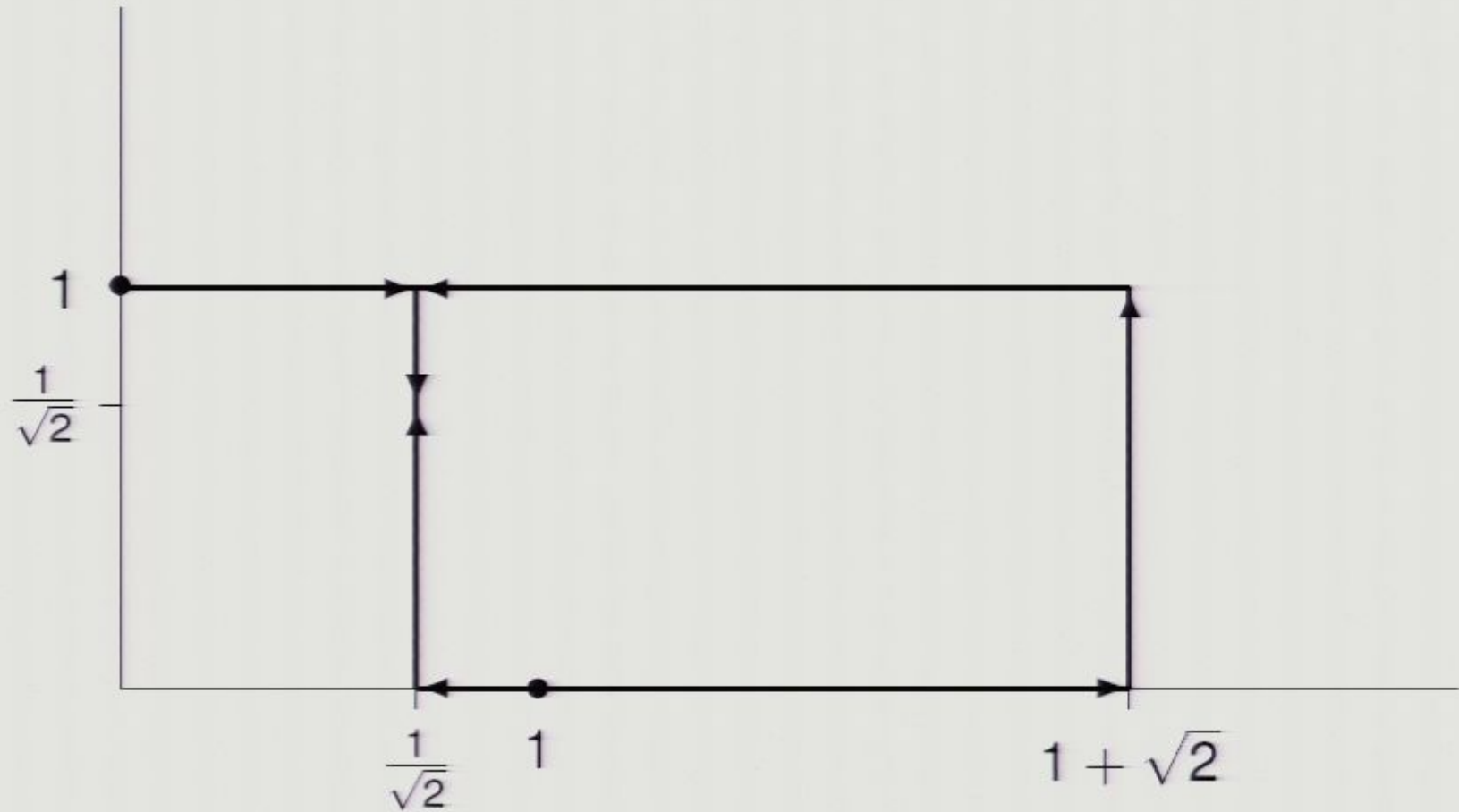$$p[z] \rightarrow p[z'] \qquad \text{(for } z \leq z').$$

- Point merging

$$p_1[z_1] + p_2[z_2] \rightarrow (p_1 + p_2) \left[\frac{p_1 z_1 + p_2 z_2}{p_1 + p_2} \right].$$

- Point splitting

$$(p_1 + p_2) \left[\frac{p_1 + p_2}{p_1 w_1' + p_2 w_2'} \right] \rightarrow p_1 \left[\frac{1}{w_1'} \right] + p_2 \left[\frac{1}{w_2'} \right].$$

Some simple valid transitions

- Point raising

$$p[z] \rightarrow p[z'] \qquad \text{(for } z \leq z').$$

- Point merging

$$p_1[z_1] + p_2[z_2] \rightarrow (p_1 + p_2) \left[\frac{p_1 z_1 + p_2 z_2}{p_1 + p_2} \right].$$

- Point splitting

$$(p_1 + p_2) \left[\frac{p_1 + p_2}{p_1 w_1' + p_2 w_2'} \right] \rightarrow p_1 \left[\frac{1}{w_1'} \right] + p_2 \left[\frac{1}{w_2'} \right].$$

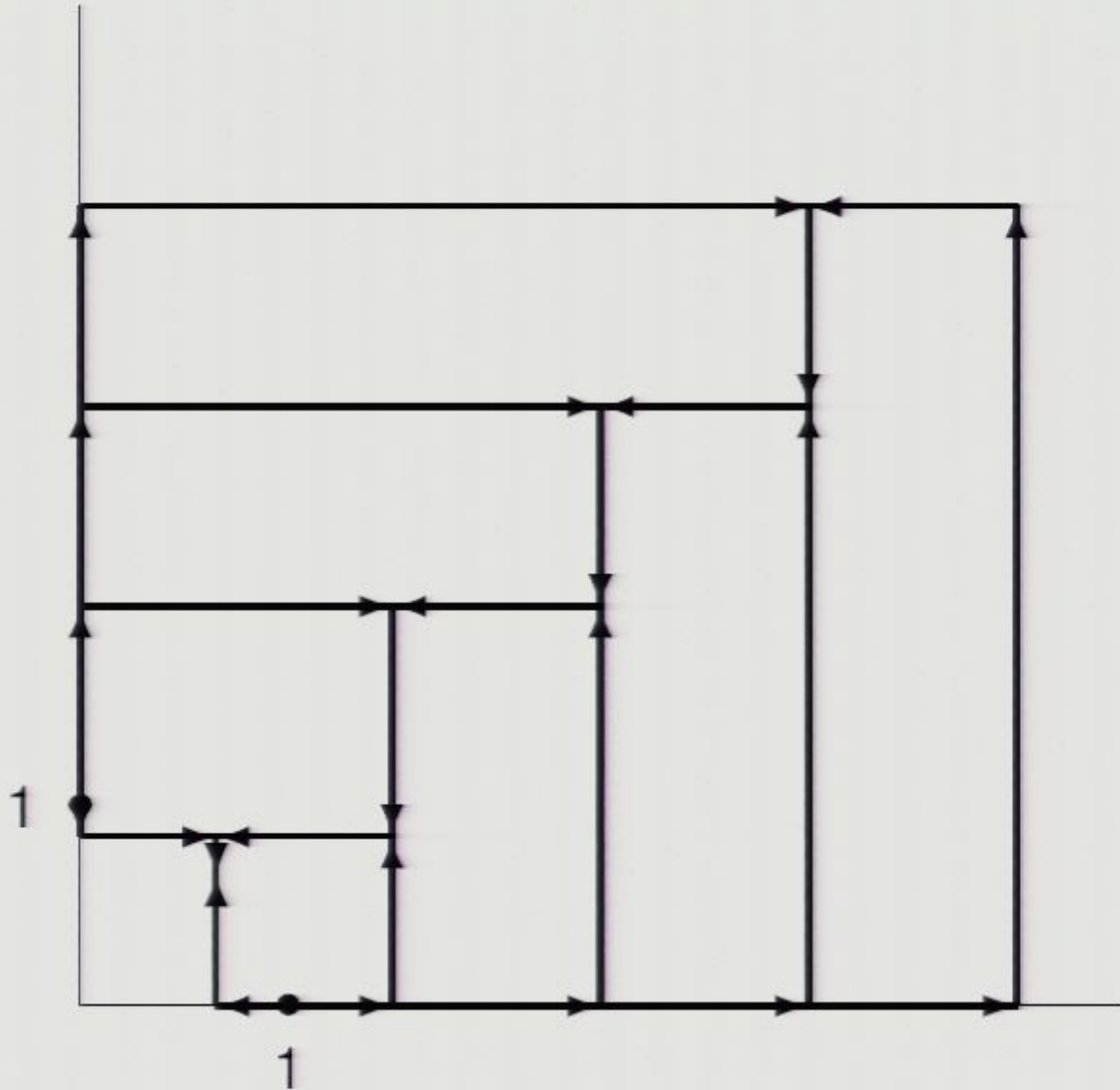# The Spekkens and Rudolph protocol
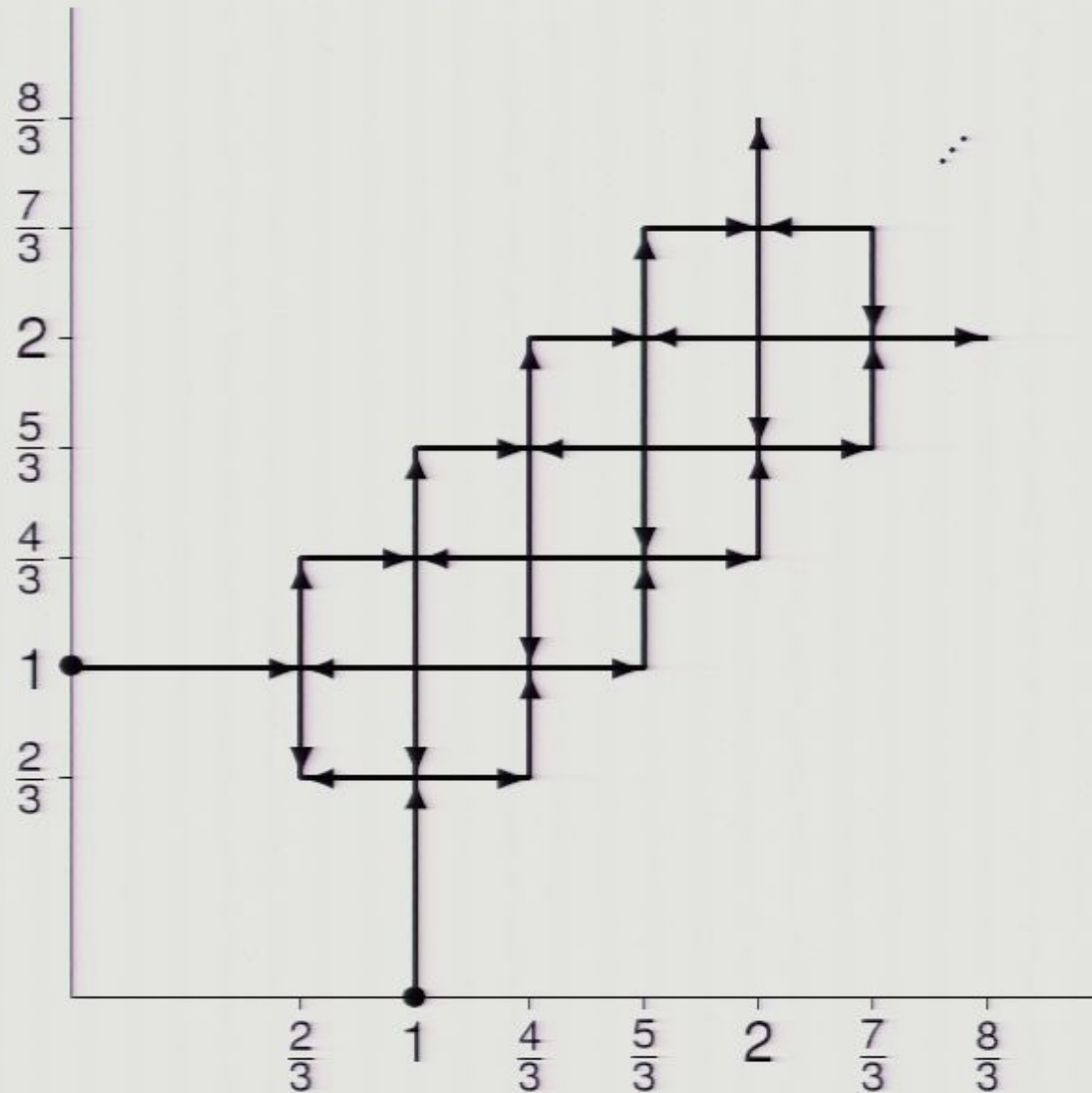
$$\frac{1}{2}[1, 0] + \frac{1}{2}[0, 1] \rightarrow \frac{2x - 1}{2x}\left[x, 0\right] + \frac{1 - x}{2x}\left[\frac{x}{1 - x}, 0\right] + \frac{1}{2}[0, 1]$$

$$\rightarrow \frac{2x - 1}{2x}\left[x, 0\right] + \frac{1 - x}{2x}\left[\frac{x}{1 - x}, 1\right] + \frac{1}{2}[0, 1]$$

$$\rightarrow \frac{2x - 1}{2x}\left[x, 0\right] + \frac{1}{2x}\left[x, 1\right]$$

$$\rightarrow 1\left[x, \frac{1}{2x}\right]$$
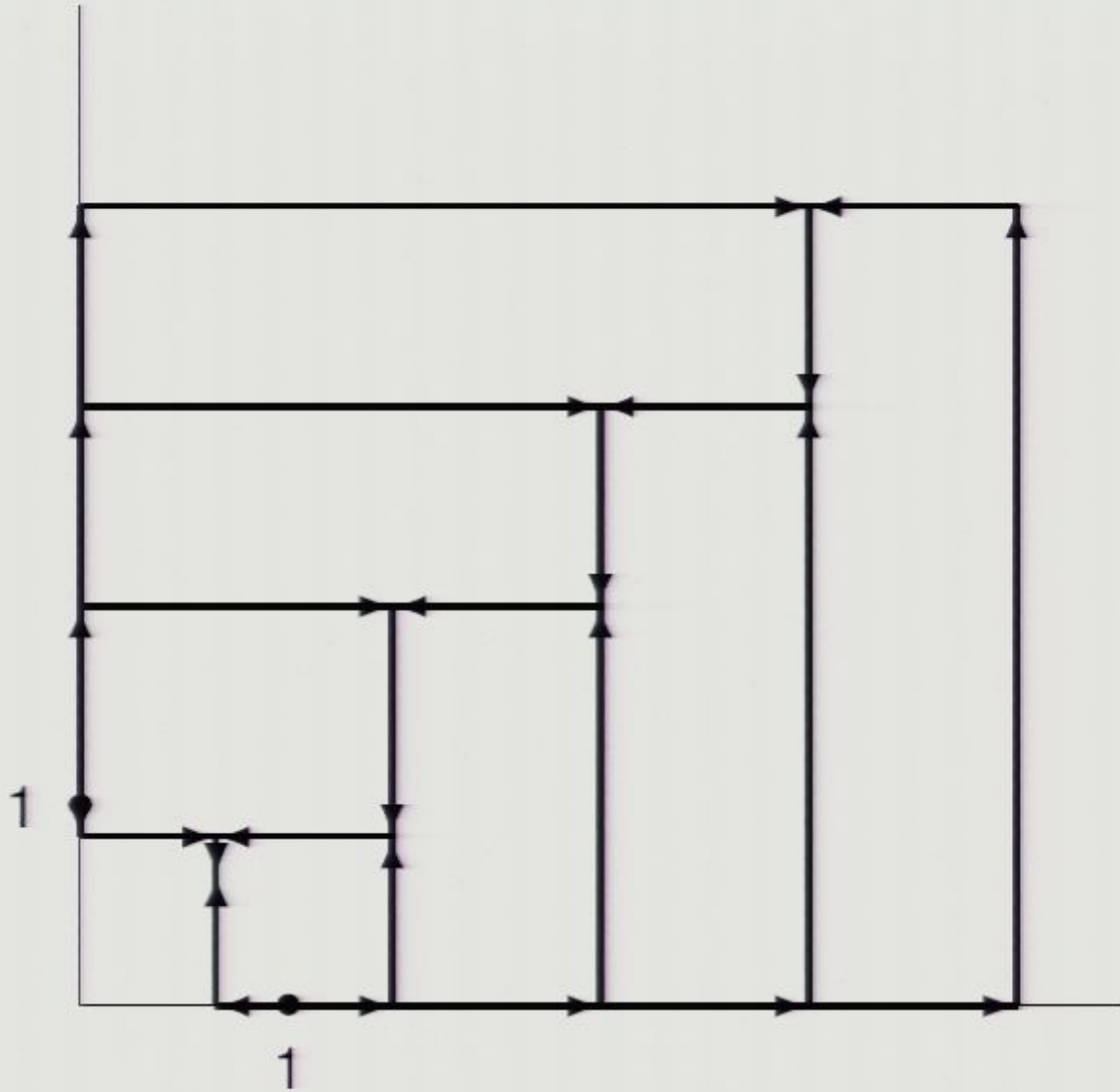
for $x \in (1/2, 1)$. Last slide used $x = 1/\sqrt{2}$.

Alternative protocol with bias 1/6
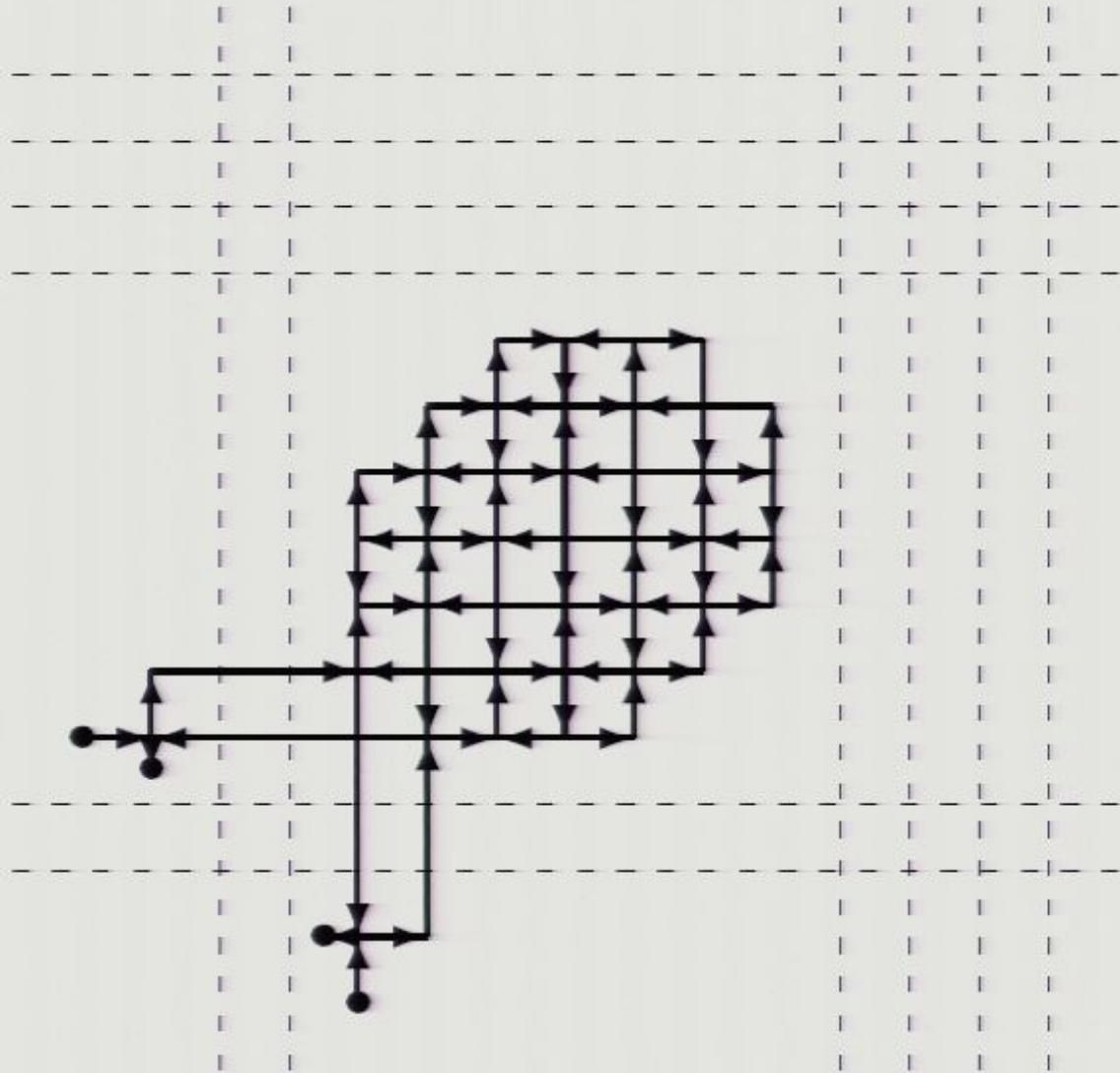
Catalyzed transitions

$$\frac{1}{2}[1, 0] + \frac{1}{2}[0, 1] + \sum_i w_i[x_i, y_i] \rightarrow 1[\beta, \alpha] + \sum_i w_i[x_i, y_i]$$

- Catalysis allows "negative probability."
- Catalysis allows point games with no explicit time ordering.

Lemma (Also proven by Kitaev)

Coin flipping without catalysis is possible given coin flipping with catalysis.

Results and Conclusions

- For every integer $k \geq 0$ there is a family of protocols that converges to

$$P_A^* = P_B^* = \frac{k+1}{2k+1}.$$

- Quantum weak coin flipping with arbitrarily small bias is possible.

- Kitaev's formalism is awesome!

Open problems!

- How practical is coin flipping?

- Find more applications of Kitaev's formalism.

  Beyond coin flipping it can trivially be extended to deal with:
  - Multiple parties.
  - Cheat detection.
  - General quantum games.

- Find protocols for secure computation with cheat detection. What is the best that quantum information has to offer to this important field?

Results and Conclusions

- For every integer $k \geq 0$ there is a family of protocols that converges to

$$P_A^* = P_B^* = \frac{k+1}{2k+1}.$$

- Quantum weak coin flipping with arbitrarily small bias is possible.

- Kitaev's formalism is awesome!

Open problems!

- How practical is coin flipping?

- Find more applications of Kitaev's formalism.

  Beyond coin flipping it can trivially be extended to deal with:
  - Multiple parties.
  - Cheat detection.
  - General quantum games.

- Find protocols for secure computation with cheat detection. What is the best that quantum information has to offer to this important field?

Catalyzed transitions

$$\frac{1}{2}[1,0] + \frac{1}{2}[0,1] + \sum_i w_i[x_i, y_i] \;\rightarrow\; 1[\beta, \alpha] + \sum_i w_i[x_i, y_i]$$

- Catalysis allows "negative probability."
- Catalysis allows point games with no explicit time ordering.

Lemma (Also proven by Kitaev)

Coin flipping without catalysis is possible given coin flipping with catalysis.

Catalyzed transitions

$$\frac{1}{2}[1,0] + \frac{1}{2}[0,1] + \sum_i w_i[x_i, y_i] \;\rightarrow\; 1[\beta, \alpha] + \sum_i w_i[x_i, y_i]$$

- Catalysis allows "negative probability."
- Catalysis allows point games with no explicit time ordering.

Lemma (Also proven by Kitaev)

Coin flipping without catalysis is possible given coin flipping with catalysis.