Quantum and Classical Coin-Flipping Protocols based on Bit-Commitment and their Point Games

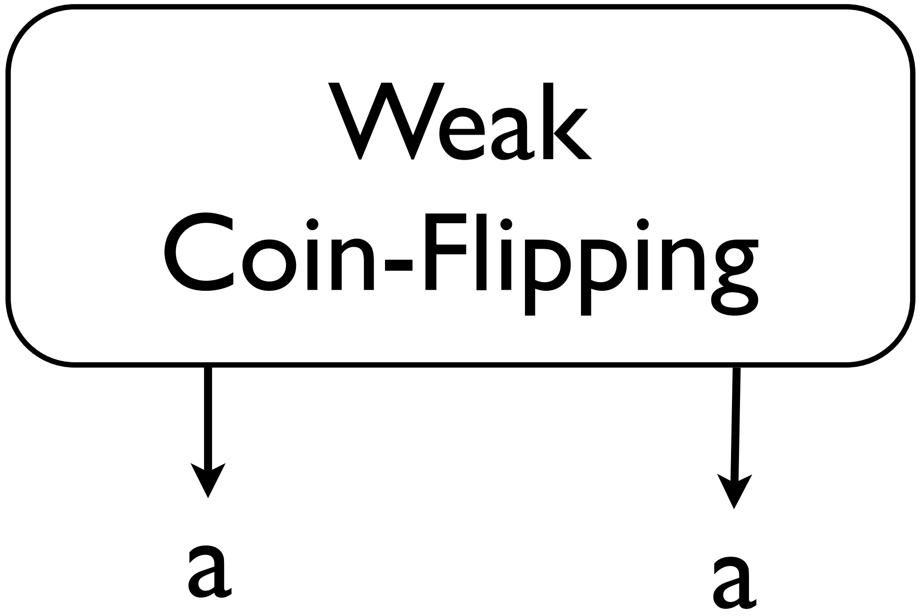
Ashwin Nayak, **Jamie Sikora**, Levent Tunçel

Follow-up work to a paper that will appear on the arXiv on Monday

Berkeley 2014

Fun with Crypto SDPs

(Weak) Coin-Flipping



Weak Coin-Flipping

a

a

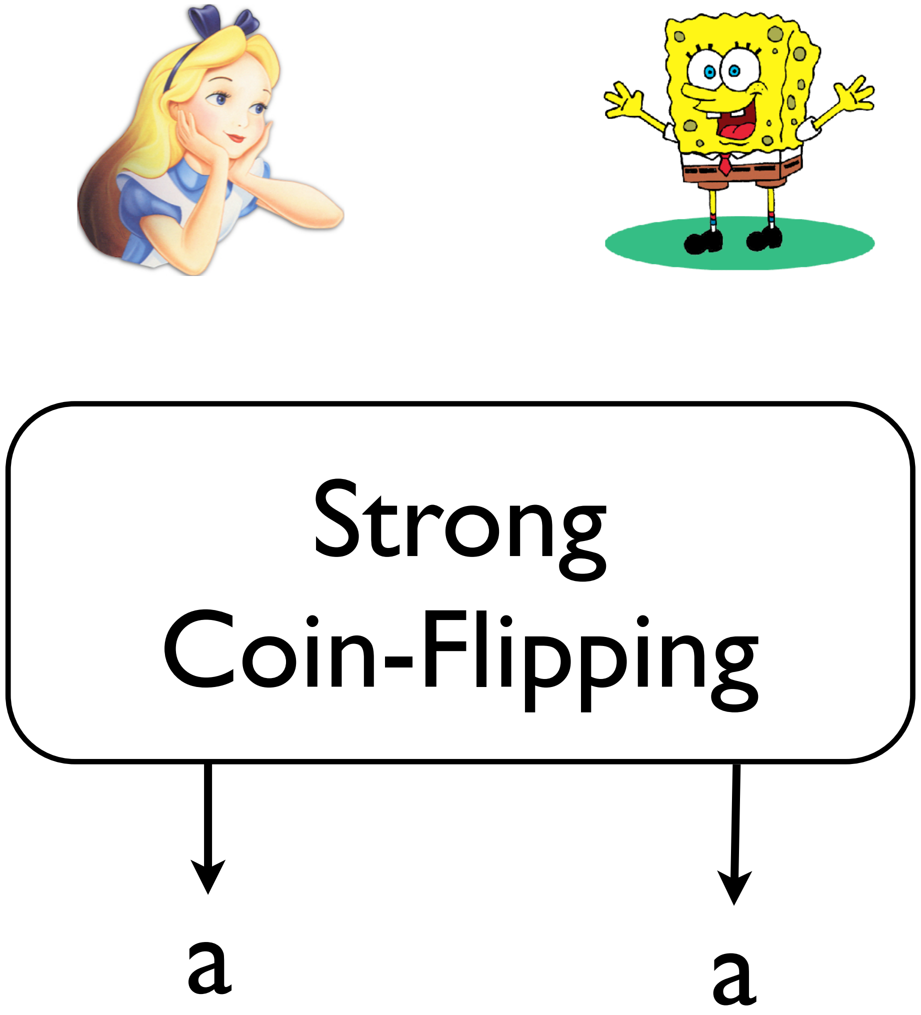
Cheating definitions

$P^*_{A,0} := \max \Pr[\text{Alice can force outcome } 0]$

$P^*_{B,1} := \max \Pr[\text{Bob can force outcome } 1]$

We have good weak coin-flipping protocols (Mochon 2007, Iordanis' talk)

(Strong) Coin-Flipping



Strong Coin-Flipping

a

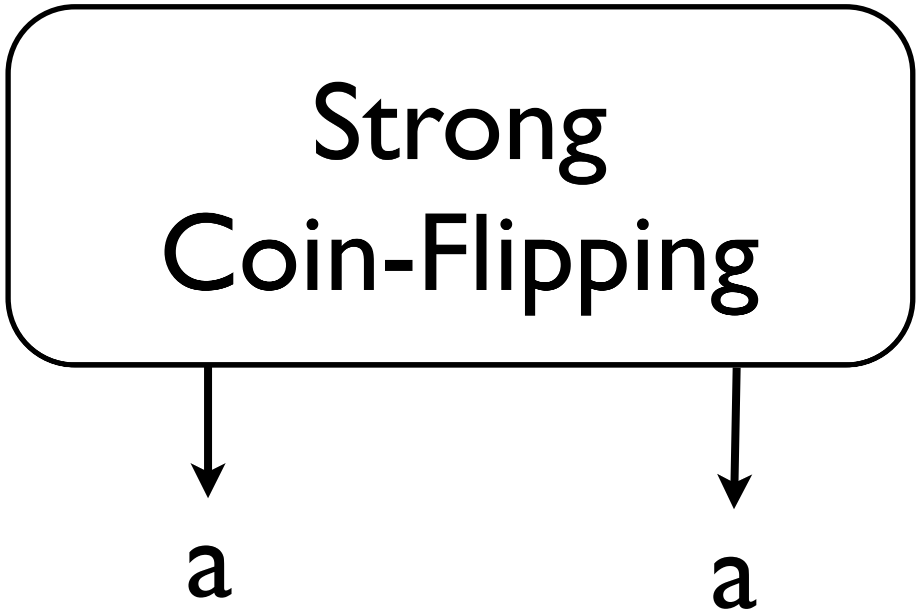
a

Cheating definitions

$$
\begin{aligned}
P^*_{A,0} &:= \max \Pr[\text{Alice can force outcome } 0] \\
P^*_{A,1} &:= \max \Pr[\text{Alice can force outcome } 1] \\
P^*_{B,0} &:= \max \Pr[\text{Bob can force outcome } 0] \\
P^*_{B,1} &:= \max \Pr[\text{Bob can force outcome } 1]
\end{aligned}
$$

Optimal strong coin-flipping protocols?

(Strong) Coin-Flipping



Strong Coin-Flipping

a

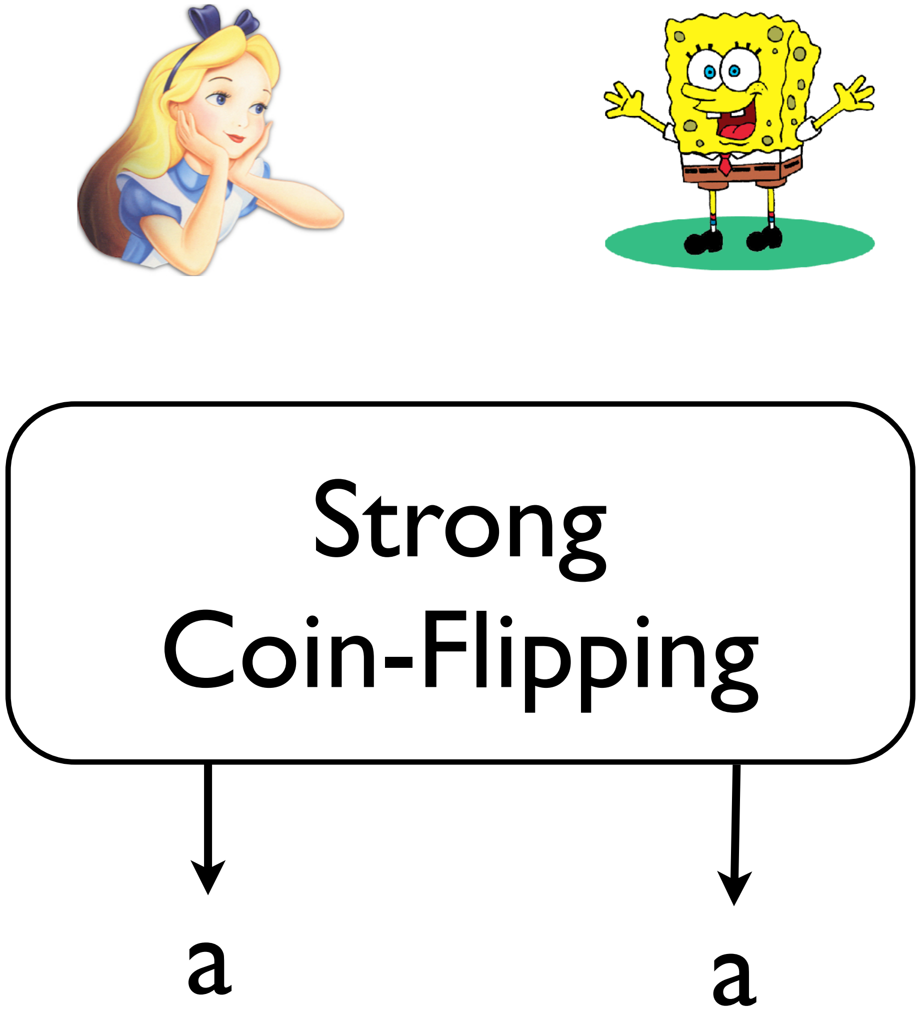
a

Optimal Bounds

$P^*_{A,0}P^*_{B,0} \geq 1/2$ for every protocol [Kitaev 2002]

[Gutoski, Watrous 2007]

(Strong) Coin-Flipping



Strong Coin-Flipping

a

a

<ins>Optimal Bounds</ins>

$P^*_{A,0}P^*_{B,0} \geq 1/2$ for every protocol [Kitaev 2002]

[Gutoski, Watrous 2007]

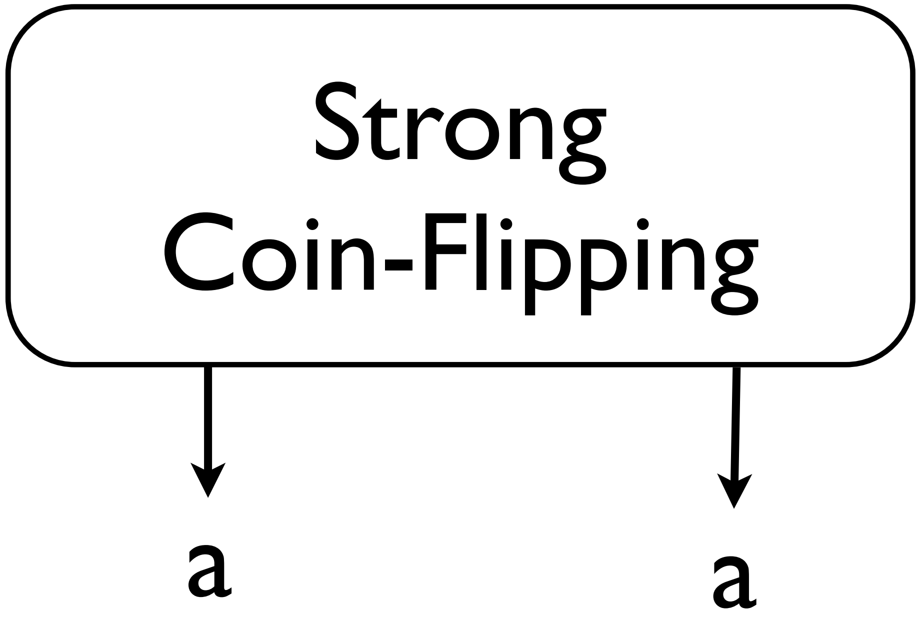
$\max\{P^*_{A,0}, P^*_{A,1}, P^*_{B,0}, P^*_{B,1}\} \leq 1/\sqrt{2} + \epsilon$

is possible for any $\epsilon > 0$

[Chailloux and Kerenidis 2009]

Based on weak coin-flipping!

(Strong) Coin-Flipping



Strong Coin-Flipping

Optimal Bounds

$P^*_{A,0}P^*_{B,0} \geq 1/2$ for every protocol [Kitaev 2002]

[Gutoski, Watrous 2007]

$\max\{P^*_{A,0}, P^*_{A,1}, P^*_{B,0}, P^*_{B,1}\} \leq 1/\sqrt{2} + \epsilon$

is possible for any $\epsilon > 0$

[Chailloux and Kerenidis 2009]

Based on weak coin-flipping!

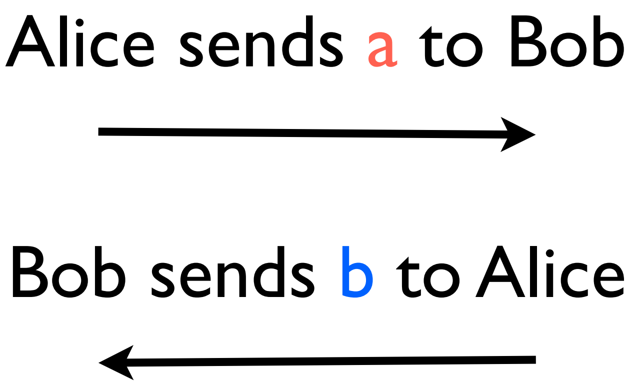
How can we find good and simple coin-flipping protocols?

How do we prove coin-flipping protocol security?

Bad Coin-Flipping Protocol

Alice chooses a uniformly at random

Bob chooses b uniformly at random



Alice sends a to Bob

Bob sends b to Alice

Alice outputs $a \oplus b$

Bob outputs $a \oplus b$

Bad Coin-Flipping Protocol

Alice chooses a uniformly at random

Bob chooses b uniformly at random

Alice sends a to Bob →

← Bob sends b to Alice

Before sending b, Bob can change it and Alice wouldn't know better

Alice outputs a ⊕ b

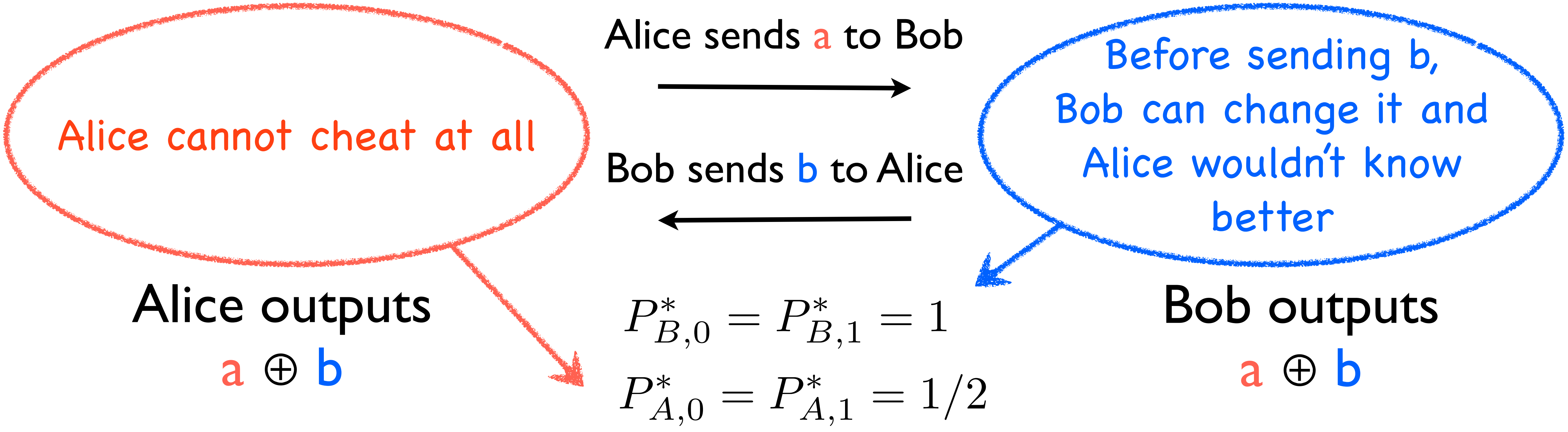
$$P^*_{B,0} = P^*_{B,1} = 1$$

Bob outputs a ⊕ b

Bad Coin-Flipping Protocol

Alice chooses a uniformly at random

Bob chooses b uniformly at random



Alice sends a to Bob

Bob sends b to Alice

Alice cannot cheat at all

Before sending b, Bob can change it and Alice wouldn't know better

Alice outputs a ⊕ b

Bob outputs a ⊕ b

$$P^*_{B,0} = P^*_{B,1} = 1$$

$$P^*_{A,0} = P^*_{A,1} = 1/2$$

Bad Coin-Flippin
Proto

BAD

t random

Alic

efore sending b, Bob can change it and Alice wouldn't know better

to Alice

Ali b

$P^*_{B,0} = P^*_{B,1} = 1$

$P^*_{A,0} = P^*_{A,1} = 1/2$

Bob outputs a ⊕ b

Quantum Coin-Flipping Protocol Construction

Alice creates a in superposition
Controlled on a, she creates

$$|\psi_a\rangle := \sum_x \sqrt{\alpha_{a,x}}|x,x\rangle$$

for some probability vector α_a

Thus, she creates the state below:

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |\underset{\uparrow}{a}, \underset{\uparrow}{a}\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x, \underset{\uparrow}{x}\rangle$$

For Alice For Bob Extra x for cheat detection

Quantum Coin-Flipping Protocol Construction

Bob creates b in superposition
Controlled on b, he creates

$$|\phi_b\rangle := \sum_y \sqrt{\beta_{b,y}}|y, y\rangle$$

for some probability vector β_b

Thus, he creates the state below:

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}}|b, b\rangle \sum_y \sqrt{\beta_{b,y}}\,|y, y\rangle$$

For Bob For Alice Extra y for cheat detection

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}}|a,a\rangle \sum_x \sqrt{\alpha_{a,x}}\,|x,x\rangle$$

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}}|b,b\rangle \sum_y \sqrt{\beta_{b,y}}\,|y,y\rangle$$

For i = 1 to n

Alice sends x_i (from second x register) to Bob →

Bob sends y_i (from second y register) to Alice ←

Alice sends a,x to Bob →

Bob sends b,y to Alice ←

Alice measures to determine:
(1) The value of a ⊕ b
(2) If Bob cheated

Bob measures to determine:
(1) The value of a ⊕ b
(2) If Alice cheated

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a,a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x,x\rangle$$

a a x $x_1 x_2 x_3$

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b,b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y,y\rangle$$

b b y $y_1 y_2 y_3$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a,a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x,x\rangle$$

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b,b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y,y\rangle$$

a a x $x_2 x_3$

b b y $x_1 y_1 y_2 y_3$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a, a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x, x\rangle$$

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b, b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y, y\rangle$$

$a\,a\,x\,y_1x_2x_3$

$b\,b\,y\;\;x_1\,y_2\,y_3$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}}|a,a\rangle \sum_x \sqrt{\alpha_{a,x}}\,|x,x\rangle$$

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}}|b,b\rangle \sum_y \sqrt{\beta_{b,y}}\,|y,y\rangle$$

$a\,a\,x\,y_1\,x_3$

$b\,b\,y\;\;x_1 x_2 y_2\,y_3$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a,a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x,x\rangle$$

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b,b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y,y\rangle$$

a a x $y_1 y_2 x_3$

b b y $x_1 x_2 y_3$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}}|a,a\rangle \sum_x \sqrt{\alpha_{a,x}}\,|x,x\rangle$$

$a\,a\,x\,y_1 y_2$

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}}|b,b\rangle \sum_y \sqrt{\beta_{b,y}}\,|y,y\rangle$$

$b\,b\,y\quad x_1 x_2 x_3 y_3$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a,a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x,x\rangle$$

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b,b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y,y\rangle$$

$a\,a\,x\,y_1 y_2 y_3$

$b\,b\,y\;\;x_1 x_2 x_3$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a, a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x, x\rangle$$

a $y_1 y_2 y_3$

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b, b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y, y\rangle$$

b b y a x $x_1 x_2 x_3$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a,a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x,x\rangle$$

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b,b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y,y\rangle$$

$a\ b\ y\ y_1 y_2 y_3$

$b\ a\ x\ x_1 x_2 x_3$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a, a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x, x\rangle$$

Outcome?

$a\ b\ y\ y_1 y_2 y_3$

Alice “measures” to learn a and b. Depending on b, she measures y, y_1, y_2, y_3 to see if it’s in the state

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b, b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y, y\rangle$$

$b\ a\ x\ x_1 x_2 x_3$

$$|\phi_b\rangle := \sum_y \sqrt{\beta_{b,y}}\, |y, y\rangle$$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a, a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x, x\rangle$$

Bob cheated?

$a\ b\ y\ y_1 y_2 y_3$

Alice "measures" to learn a and b.
Depending on b, she measures y,
y_1, y_2, y_3 to see if it's in the state

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b, b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y, y\rangle$$

$b\ a\ x\ x_1 x_2 x_3$

$$|\phi_b\rangle := \sum_y \sqrt{\beta_{b,y}}\, |y, y\rangle$$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a,a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x,x\rangle$$

$a\ b\ y\ y_1y_2y_3$

Bob "measures" to learn a and b. Depending on a, he measures x, x_1, x_2, x_3 to see if it's in the state

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b,b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y,y\rangle$$

Outcome?

$\boxed{b\ a}\ x\ x_1x_2x_3$

$$|\psi_a\rangle := \sum_x \sqrt{\alpha_{a,x}}\, |x,x\rangle$$

Quantum Coin-Flipping Protocol

Alice creates the quantum state

$$|\psi\rangle := \sum_a \frac{1}{\sqrt{2}} |a,a\rangle \sum_x \sqrt{\alpha_{a,x}}\, |x,x\rangle$$

a b y $y_1y_2y_3$

Bob "measures" to learn a and b. Depending on a, he measures x, x_1, x_2, x_3 to see if it's in the state

Bob creates the quantum state

$$|\phi\rangle := \sum_b \frac{1}{\sqrt{2}} |b,b\rangle \sum_y \sqrt{\beta_{b,y}}\, |y,y\rangle$$

Alice cheated?

b a x $x_1x_2x_3$

$$|\psi_a\rangle := \sum_x \sqrt{\alpha_{a,x}}\, |x,x\rangle$$

Calculating the cheating probabilities as SDPs

Probability Bob outputs "0"

$$\begin{array}{llrcl} P^*_{A,0} = & \sup & \multicolumn{3}{l}{\langle \sigma_F, \Pi_{B,0} \rangle} \\ & \text{s.t.} & \mathrm{Tr}_{X_1}(\sigma_1) & = & |\phi\rangle\langle\phi| \\ & & \mathrm{Tr}_{X_2}(\sigma_2) & = & \mathrm{Tr}_{Y_1}(\sigma_1) \\ & & & \vdots & \\ & & \mathrm{Tr}_{X_n}(\sigma_n) & = & \mathrm{Tr}_{Y_{n-1}}(\sigma_{n-1}) \\ & & \mathrm{Tr}_{X,A}(\sigma_F) & = & \mathrm{Tr}_{Y_n}(\sigma_n) \\ & & \sigma_i & \succeq & 0 \end{array}$$

Variables are Bob's quantum states throughout the protocol

Alice cannot alter all of Bob's state

$$
\begin{array}{rlrcl}
P^*_{A,0} = & \sup & \langle \sigma_F, \Pi_{B,0} \rangle & & \\
& \text{s.t.} & \mathrm{Tr}_{X_1}(\sigma_1) & = & |\phi\rangle\langle\phi| \\
& & \mathrm{Tr}_{X_2}(\sigma_2) & = & \mathrm{Tr}_{Y_1}(\sigma_1) \\
& & & \vdots & \\
& & \mathrm{Tr}_{X_n}(\sigma_n) & = & \mathrm{Tr}_{Y_{n-1}}(\sigma_{n-1}) \\
& & \mathrm{Tr}_{X,A}(\sigma_F) & = & \mathrm{Tr}_{Y_n}(\sigma_n) \\
& & \sigma_i & \succeq & 0
\end{array}
$$

$$
\begin{array}{rlrcl}
P^*_{A,0} = & \sup & \langle \sigma_F, \Pi_{B,0} \rangle & & \\
& \text{s.t.} & \mathrm{Tr}_{X_1}(\sigma_1) & = & |\phi\rangle\langle\phi| \\
& & \mathrm{Tr}_{X_2}(\sigma_2) & = & \mathrm{Tr}_{Y_1}(\sigma_1) \\
& & & \vdots & \\
& & \mathrm{Tr}_{X_n}(\sigma_n) & = & \mathrm{Tr}_{Y_{n-1}}(\sigma_{n-1}) \\
& & \mathrm{Tr}_{X,A}(\sigma_F) & = & \mathrm{Tr}_{Y_n}(\sigma_n) \\
& & \sigma_i & \succeq & 0
\end{array}
$$

$$
\begin{array}{rlrcl}
= & \sup & \frac{1}{2} \sum_a \sum_y \beta_{a,y} F(s^{(a,y)}, \alpha_a) & & \\
& \text{s.t.} & \mathrm{Tr}_{X_1}(s_1) & = & 1 \\
& & \mathrm{Tr}_{X_2}(s_2) & = & s_1 \otimes e_{Y_1} \\
& & & \vdots & \\
& & \mathrm{Tr}_{X_n}(s_n) & = & s_{n-1} \otimes e_{Y_{n-1}} \\
& & \mathrm{Tr}_A(s) & = & s_n \otimes e_{Y_n} \\
& & s, s_i & \geq & 0
\end{array}
$$

$$
\begin{aligned}
P^*_{A,0} = \quad \sup \quad & \langle \sigma_F, \Pi_{B,0} \rangle \\
\text{s.t.} \quad & \begin{aligned}
\mathrm{Tr}_{X_1}(\sigma_1) &= |\phi\rangle\langle\phi| \\
\mathrm{Tr}_{X_2}(\sigma_2) &= \mathrm{Tr}_{Y_1}(\sigma_1) \\
&\vdots \\
\mathrm{Tr}_{X_n}(\sigma_n) &= \mathrm{Tr}_{Y_{n-1}}(\sigma_{n-1}) \\
\mathrm{Tr}_{X,A}(\sigma_F) &= \mathrm{Tr}_{Y_n}(\sigma_n) \\
\sigma_i &\succeq 0
\end{aligned}
\end{aligned}
$$

$$
\begin{aligned}
= \quad \sup \quad & \tfrac{1}{2} \textstyle\sum_a \sum_y \beta_{a,y} F(s^{(a,y)}, \alpha_a) \\
\text{s.t.} \quad & \begin{aligned}
\mathrm{Tr}_{X_1}(s_1) &= 1 \\
\mathrm{Tr}_{X_2}(s_2) &= s_1 \otimes e_{Y_1} \\
&\vdots \\
\mathrm{Tr}_{X_n}(s_n) &= s_{n-1} \otimes e_{Y_{n-1}} \\
\mathrm{Tr}_{A}(s) &= s_n \otimes e_{Y_n} \\
s, s_i &\geq 0
\end{aligned}
\end{aligned}
$$

Polytope!

$$
\begin{array}{rlrcl}
P^*_{A,0} = & \sup & \multicolumn{3}{l}{\langle \sigma_F, \Pi_{B,0} \rangle} \\
& \text{s.t.} & \mathrm{Tr}_{X_1}(\sigma_1) & = & |\phi\rangle\langle\phi| \\
& & \mathrm{Tr}_{X_2}(\sigma_2) & = & \mathrm{Tr}_{Y_1}(\sigma_1) \\
& & & \vdots & \\
& & \mathrm{Tr}_{X_n}(\sigma_n) & = & \mathrm{Tr}_{Y_{n-1}}(\sigma_{n-1}) \\
& & \mathrm{Tr}_{X,A}(\sigma_F) & = & \mathrm{Tr}_{Y_n}(\sigma_n) \\
& & \sigma_i & \succeq & 0
\end{array}
$$

Not a polytope!

$$
\begin{array}{rlrcl}
= & \sup & \multicolumn{3}{l}{\frac{1}{2} \sum_a \sum_y \beta_{a,y} F(s^{(a,y)}, \alpha_a)} \\
& \text{s.t.} & \mathrm{Tr}_{X_1}(s_1) & = & 1 \\
& & \mathrm{Tr}_{X_2}(s_2) & = & s_1 \otimes e_{Y_1} \\
& & & \vdots & \\
& & \mathrm{Tr}_{X_n}(s_n) & = & s_{n-1} \otimes e_{Y_{n-1}} \\
& & \mathrm{Tr}_A(s) & = & s_n \otimes e_{Y_n} \\
& & s, s_i & \geq & 0
\end{array}
$$

Polytope!

$$
\begin{array}{rllcl}
P^*_{A,0} = & \sup & \langle \sigma_F, \Pi_{B,0} \rangle & & \\
& \text{s.t.} & \mathrm{Tr}_{X_1}(\sigma_1) & = & |\phi\rangle\langle\phi| \\
& & \mathrm{Tr}_{X_2}(\sigma_2) & = & \mathrm{Tr}_{Y_1}(\sigma_1) \\
& & & \vdots & \\
& & \mathrm{Tr}_{X_n}(\sigma_n) & = & \mathrm{Tr}_{Y_{n-1}}(\sigma_{n-1}) \\
& & \mathrm{Tr}_{X,A}(\sigma_F) & = & \mathrm{Tr}_{Y_n}(\sigma_n) \\
& & \sigma_i & \succeq & 0
\end{array}
$$

Not a polytope!

$$
\begin{array}{rllcl}
= & \sup & \frac{1}{2} \sum_a \sum_y \beta_{a,y} F(s^{(a,y)}, \alpha_a) & & \\
& \text{s.t.} & \mathrm{Tr}_{X_1}(s_1) & = & 1 \\
& & \mathrm{Tr}_{X_2}(s_2) & = & s_1 \otimes e_{Y_1} \\
& & & \vdots & \\
& & \mathrm{Tr}_{X_n}(s_n) & = & s_{n-1} \otimes e_{Y_{n-1}} \\
& & \mathrm{Tr}_A(s) & = & s_n \otimes e_{Y_n} \\
& & s, s_i & \geq & 0
\end{array}
$$

Polytope!

$$\begin{array}{rcllcl} P^*_{A,0} & = & \sup & \langle \sigma_F, \Pi_{B,0} \rangle & & \\ & & \text{s.t.} & \mathrm{Tr}_{X_1}(\sigma_1) & = & |\phi\rangle\langle\phi| \\ & & & \mathrm{Tr}_{X_2}(\sigma_2) & = & \mathrm{Tr}_{Y_1}(\sigma_1) \\ & & & & \vdots & \\ & & & \mathrm{Tr}_{X_n}(\sigma_n) & = & \mathrm{Tr}_{Y_{n-1}}(\sigma_{n-1}) \\ & & & \mathrm{Tr}_{X,A}(\sigma_F) & = & \mathrm{Tr}_{Y_n}(\sigma_n) \\ & & & \sigma_i & \succeq & 0 \end{array}$$

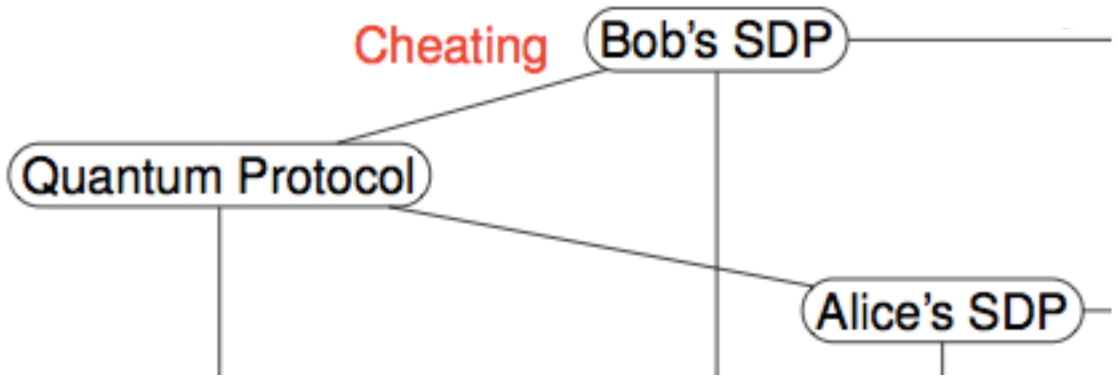
Not a polytope!

$$\begin{array}{rllcl} = & \sup & \frac{1}{2} \sum_a \sum_y \beta_{a,y} F(s^{(a,y)}, \alpha_a) & & \\ & \text{s.t.} & \mathrm{Tr}_{X_1}(s_1) & = & 1 \\ & & \mathrm{Tr}_{X_2}(s_2) & = & s_1 \otimes e_{Y_1} \\ & & & \vdots & \\ & & \mathrm{Tr}_{X_n}(s_n) & = & s_{n-1} \otimes e_{Y_{n-1}} \\ & & \mathrm{Tr}_{A}(s) & = & s_n \otimes e_{Y_n} \\ & & s, s_i & \geq & 0 \end{array}$$

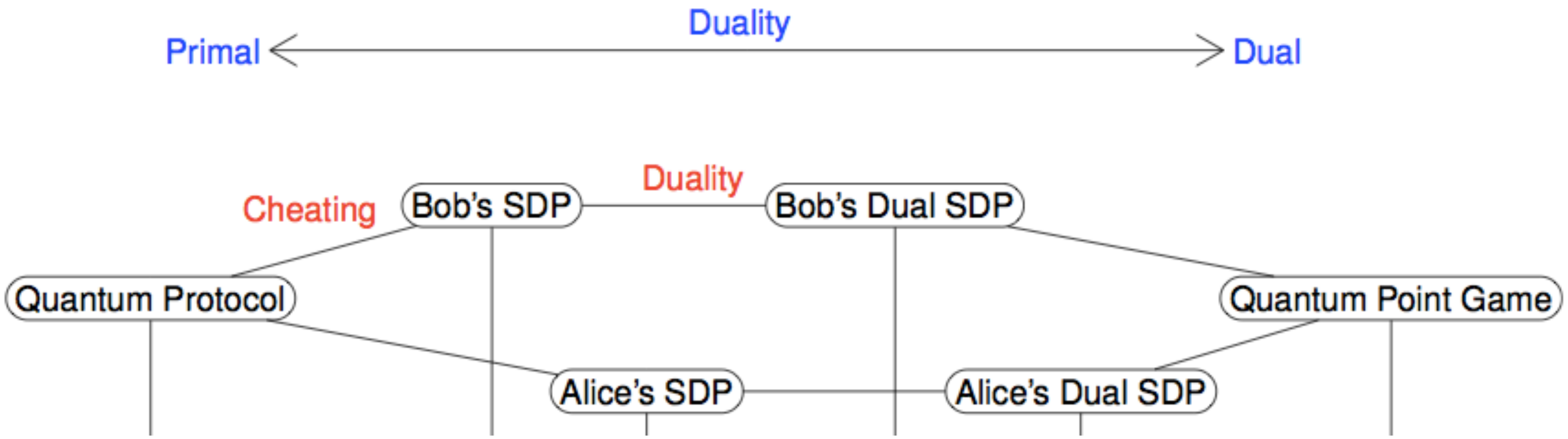
Polytope!

Similar SDPs and reductions for the other cheating probabilities

We have SDP formulations (and their simplifications)



Point Games!


Duality
Primal
Dual
Duality
Cheating
Bob's SDP
Bob's Dual SDP
Quantum Protocol
Quantum Point Game
Alice's SDP
Alice's Dual SDP

Point Game Idea

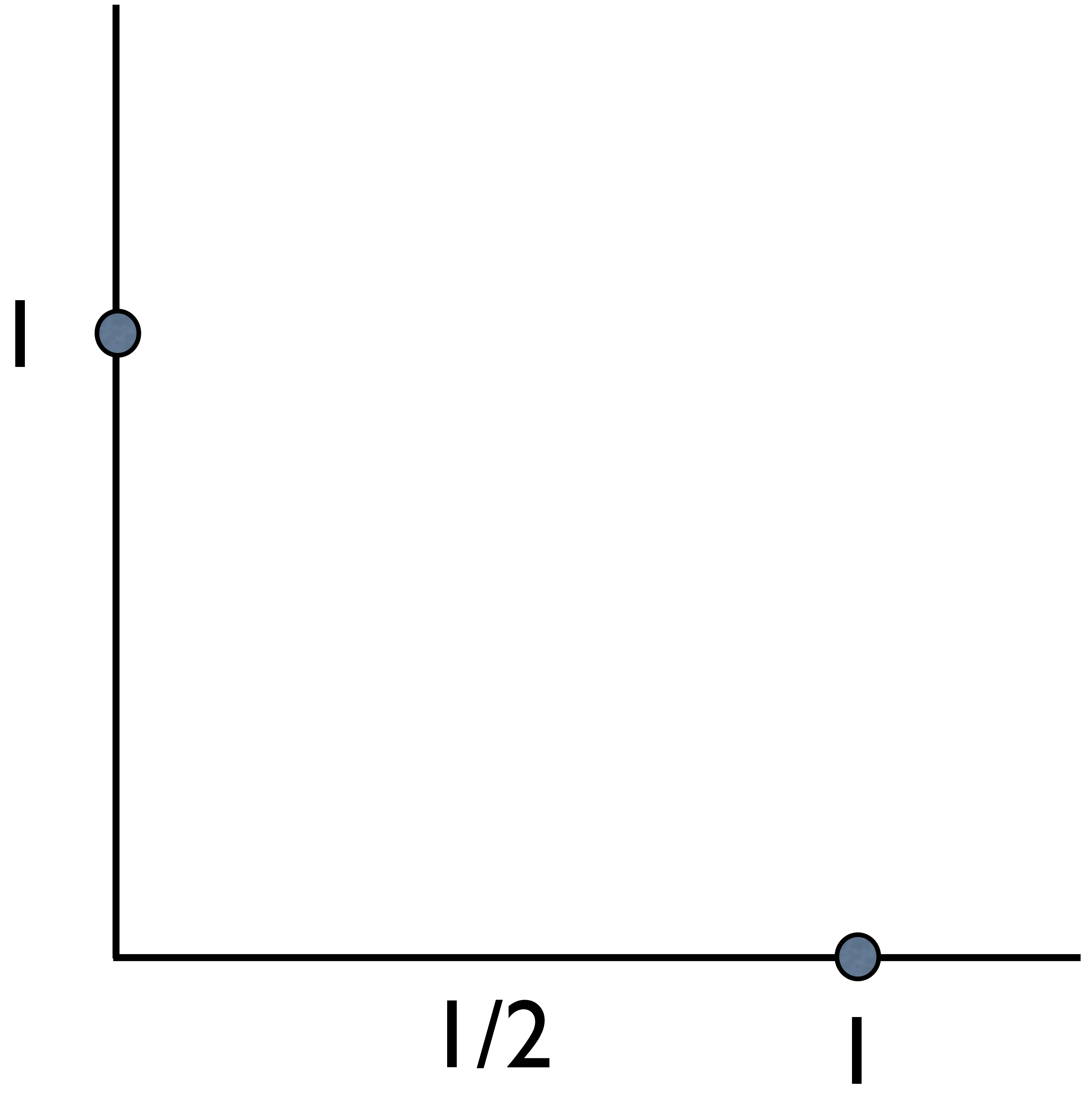
- Start with two points [1,0] and [0,1], each with probability 1/2. The idea is to merge the points/probabilities into a single point
- Points are eigenvalues of dual variables. The idea is to strip away the "messy basis information"
- Notation: "q [x,y]" is point [x,y] with probability q

Basic Point Game Moves

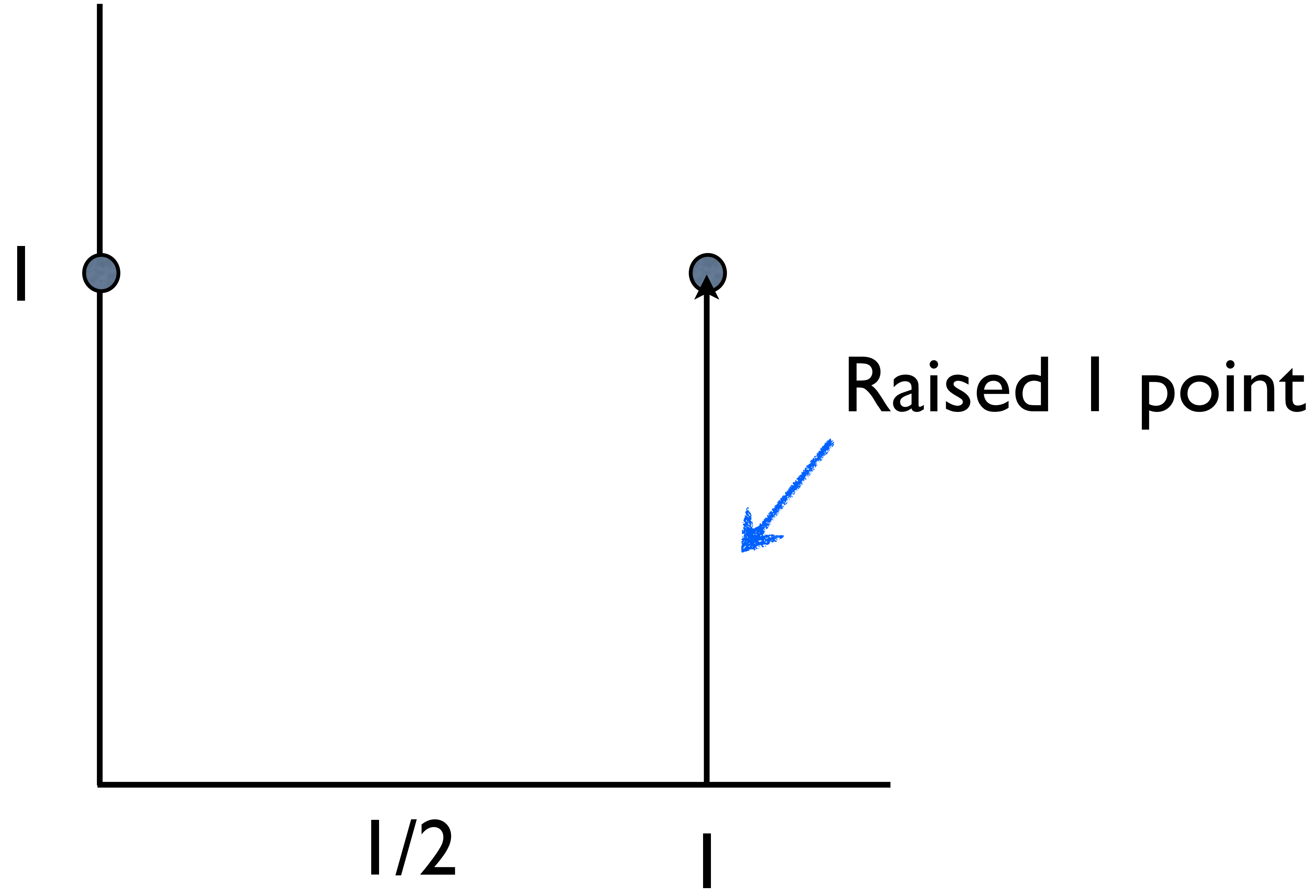
Point Raising: $q[x, y] \to q[x', y] \quad (x' \geq x)$

Point Merging: $\displaystyle\sum_{i=1}^{n} q_i[x_i, y] \to \left(\sum_{i=1}^{n} q_i\right) \left[\frac{\sum_{i=1}^{n} q_i x_i}{\sum_{i=1}^{n} q_i}, y\right]$

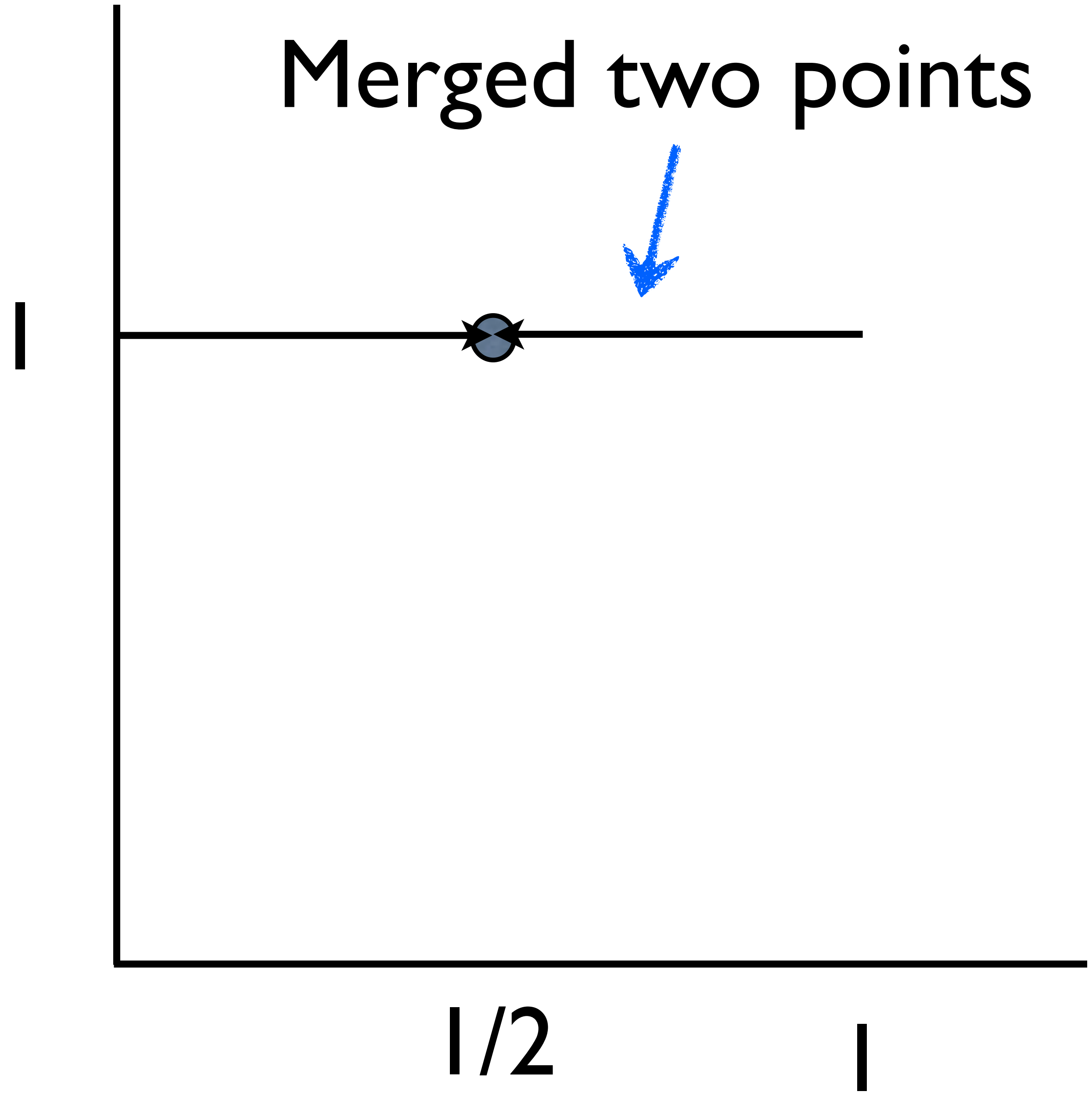
Easy Point Game



Easy Point Game

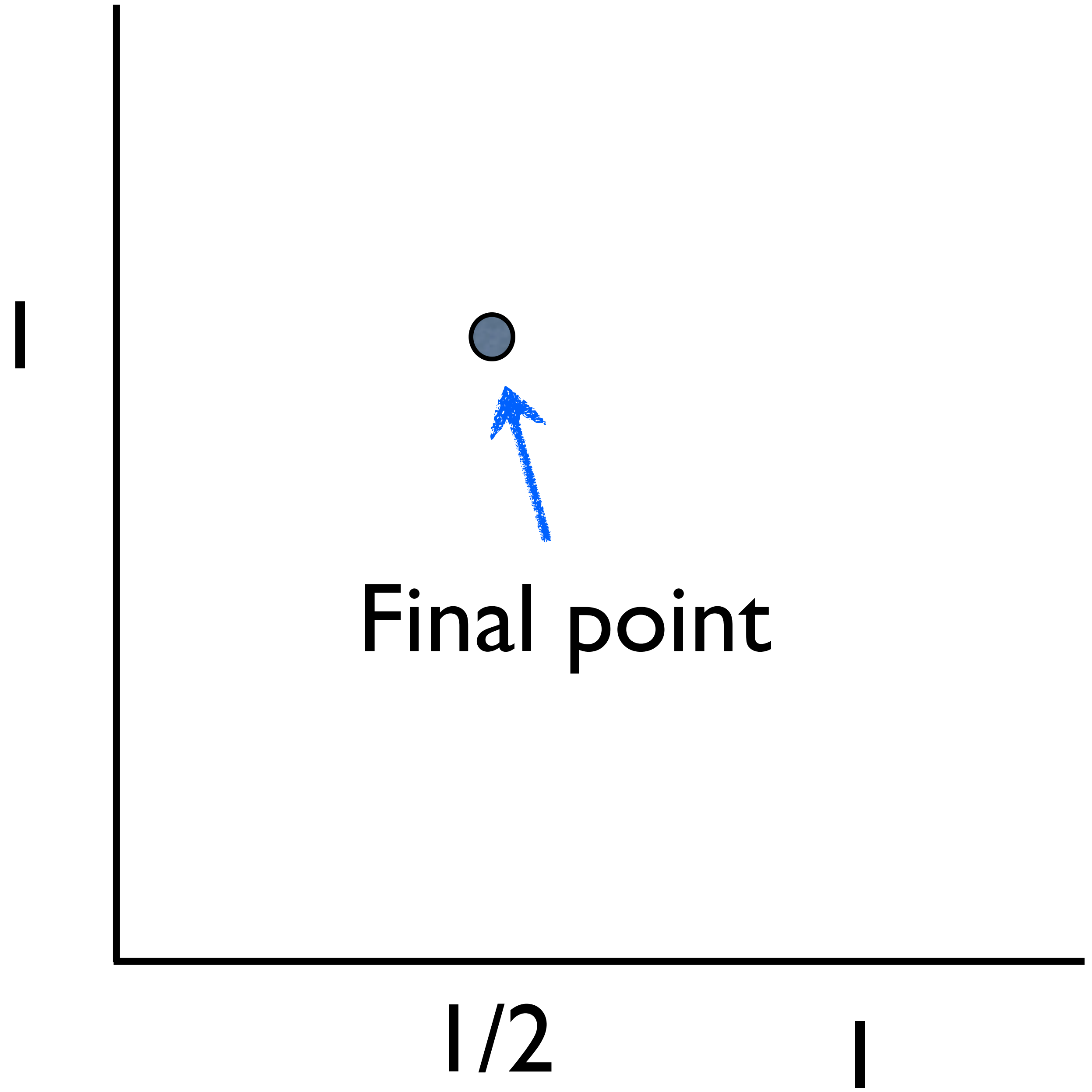


Easy Point Game

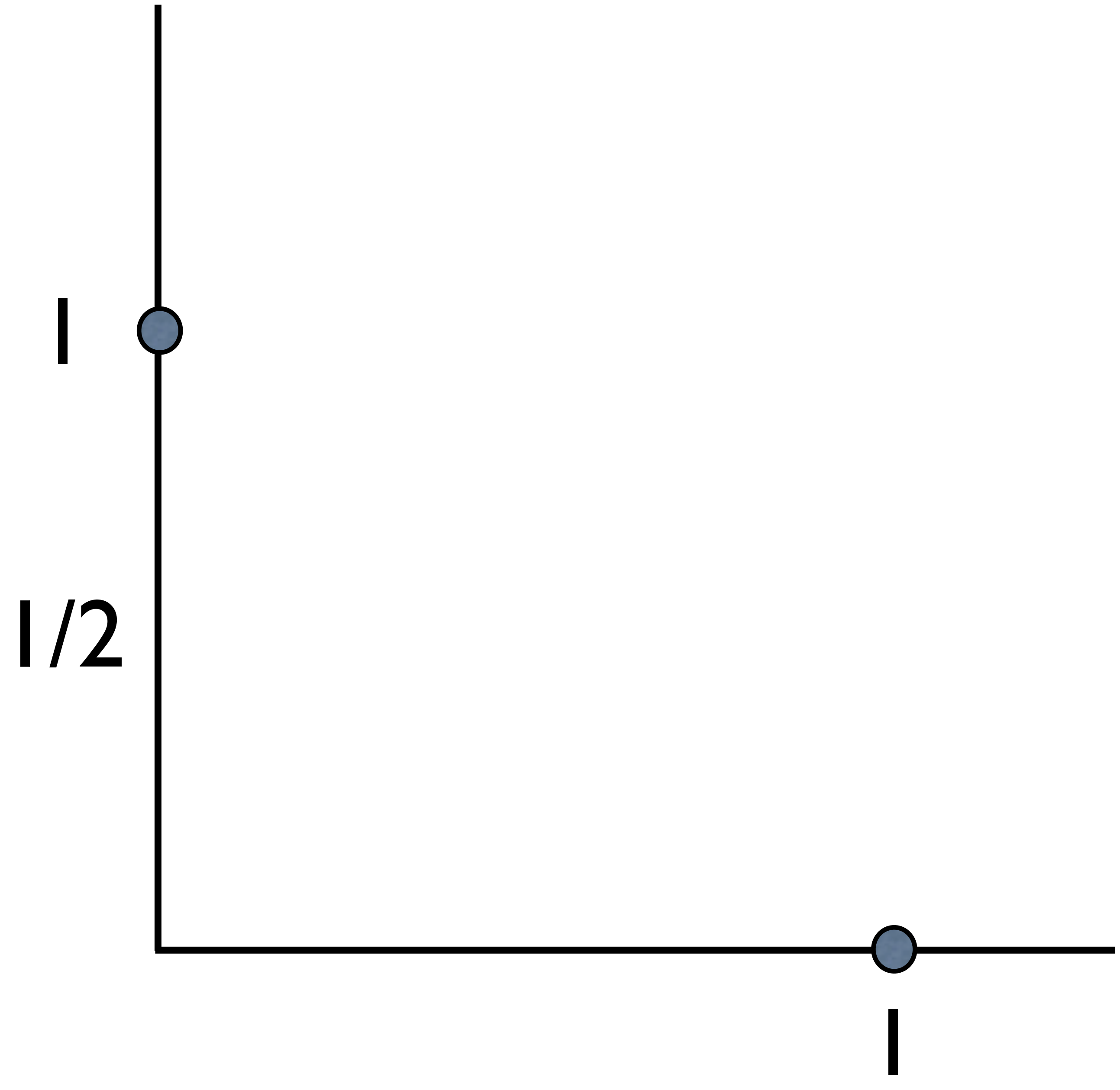


Merged two points

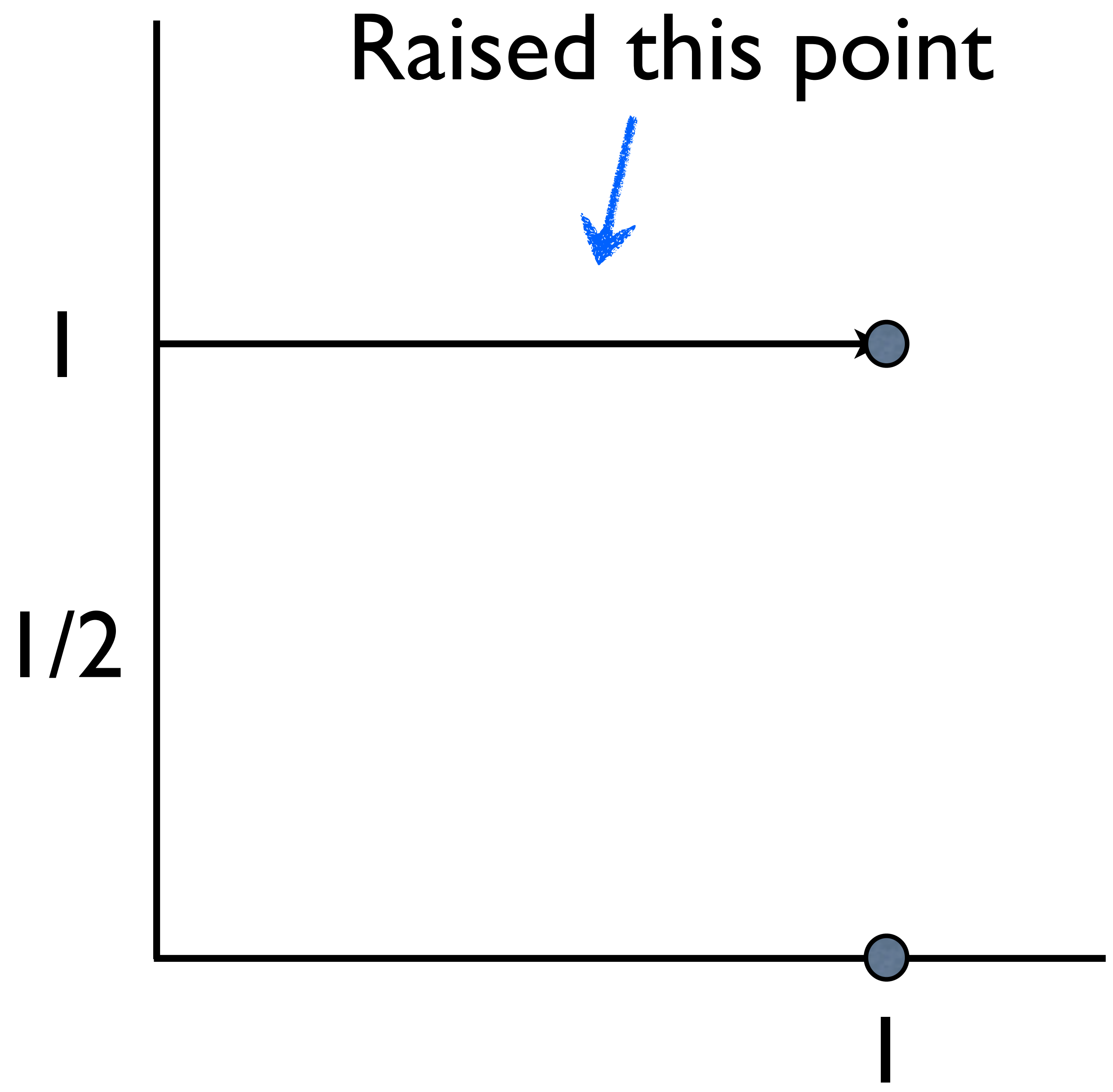
Easy Point Game



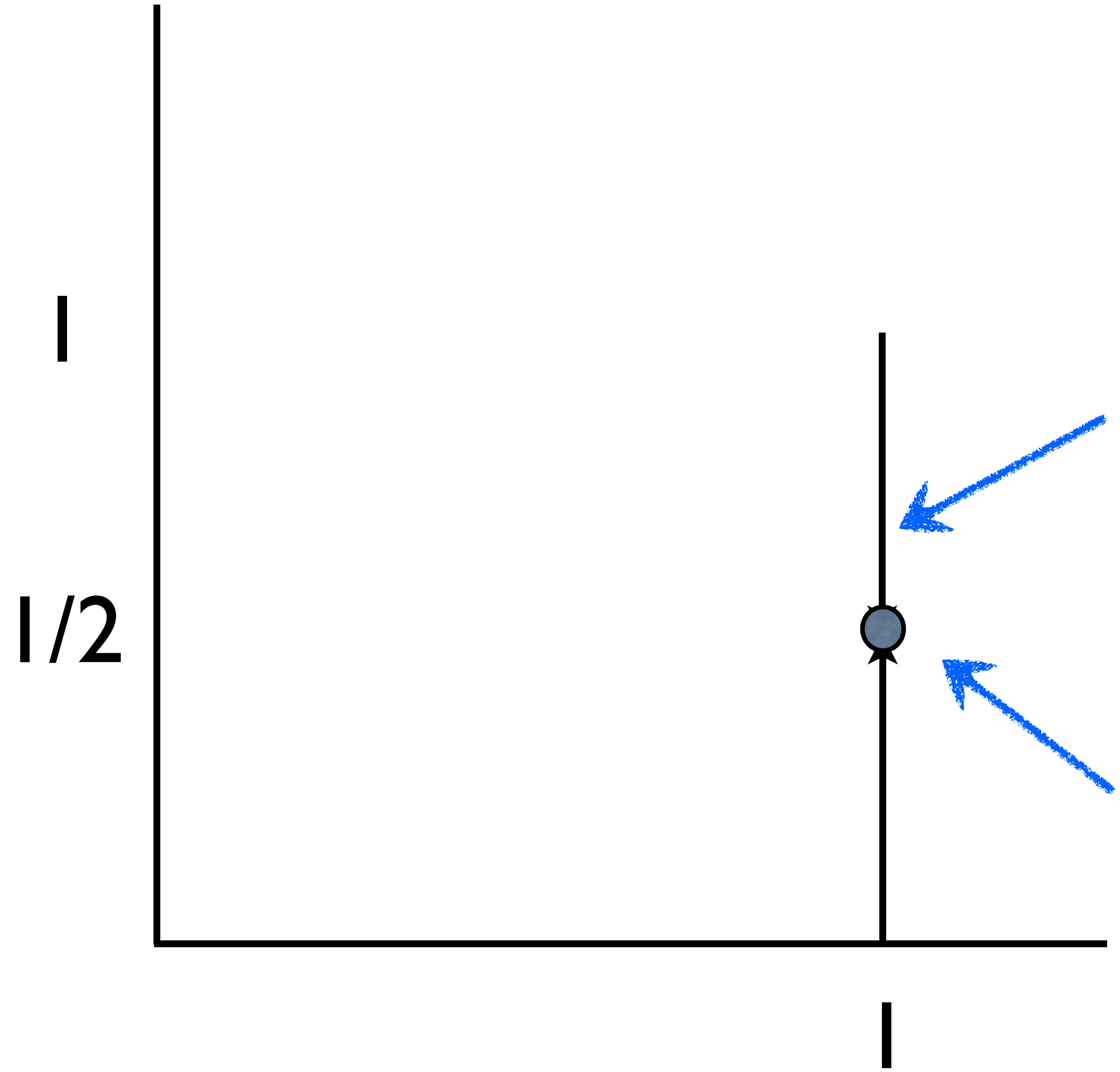
Another Easy Point Game



Another Easy Point Game



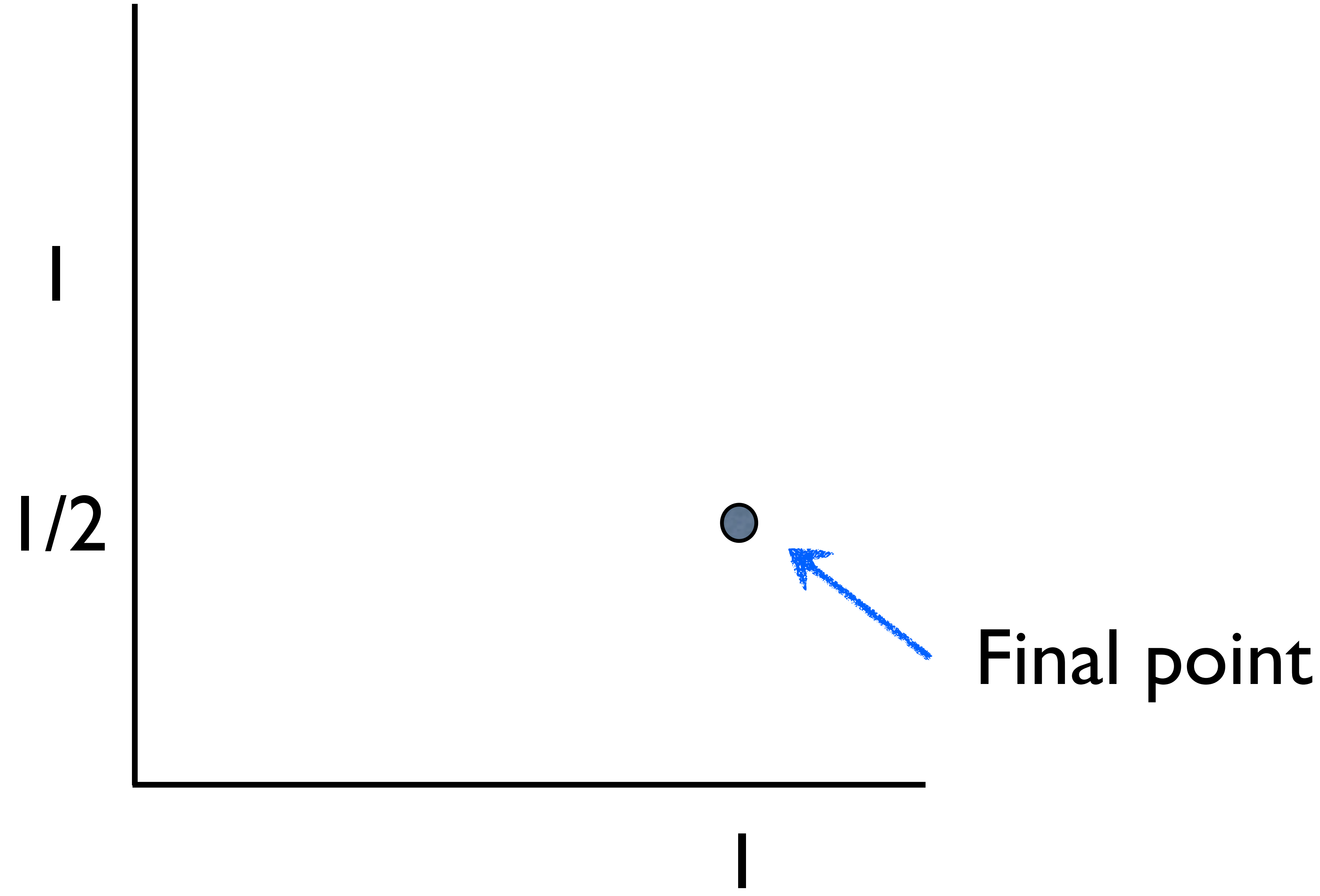
Another Easy Point Game



Merged two points

Final point

Another Easy Point Game



Basic Point Game Moves

Point Raising: $q[x, y] \to q[x', y] \quad (x' \geq x)$

Point Merging: $$\sum_{i=1}^{n} q_i[x_i, y] \to \left(\sum_{i=1}^{n} q_i\right)\left[\frac{\sum_{i=1}^{n} q_i x_i}{\sum_{i=1}^{n} q_i}, y\right]$$

Point Splitting: $$\left(\sum_{i=1}^{n} q_i\right)\left[\frac{\sum_{i=1}^{n} q_i}{\left(\sum_{i=1}^{n} \frac{q_i}{x_i}\right)}, y\right] \to \sum_{i=1}^{n} q_i \, [x_i, y]$$

Bob's Dual

$$
\begin{array}{rrcl}
P^*_{B,1} := \min & \sum_{x_1} (w_1)_{x_1} & & \\
s.t. & (w_1)_{x_1} & \geq & \sum_{x_2} (w_2)_{x_1,y_1,x_2} \\
 & (w_2)_{x_1,y_1,x_2} & \geq & \sum_{x_3} (w_3)_{x_1,y_1,x_2,y_2,x_3} \\
 & & \vdots & \\
 & (w_n)_{x_1,y_1,\ldots,x_n} & \geq & \sum_a \frac{1}{2} \alpha_{a,x} v_{a,y} \\
 & \mathrm{Diag}(v_a) & \succeq & \sqrt{\beta_{\bar{a}}} \sqrt{\beta_{\bar{a}}}^T
\end{array}
$$

Bob’s Dual

$$
\begin{array}{rrcl}
P^*_{B,1} := \min & \sum_{x_1} (w_1)_{x_1} & & \\
s.t. & (w_1)_{x_1} & \geq & \sum_{x_2} (w_2)_{x_1,y_1,x_2} \\
 & (w_2)_{x_1,y_1,x_2} & \geq & \sum_{x_3} (w_3)_{x_1,y_1,x_2,y_2,x_3} \\
 & & \vdots & \\
 & (w_n)_{x_1,y_1,\ldots,x_n} & \geq & \sum_a \frac{1}{2} \alpha_{a,x} v_{a,y} \\
 & \mathrm{Diag}(v_a) & \succeq & \sqrt{\beta_{\bar{a}}}\sqrt{\beta_{\bar{a}}}^T \quad \Longleftrightarrow \sum_y \frac{\beta_{\bar{a},y}}{v_{a,y}} \leq 1
\end{array}
$$

Bob’s Dual

Upper bound on cheating

Point Merges

$$
\begin{array}{rrcl}
P^*_{B,1} := \min & \sum_{x_1} (w_1)_{x_1} & & \\
s.t. & (w_1)_{x_1} & \geq & \sum_{x_2} (w_2)_{x_1,y_1,x_2} \\
& (w_2)_{x_1,y_1,x_2} & \geq & \sum_{x_3} (w_3)_{x_1,y_1,x_2,y_2,x_3} \\
& & \vdots & \\
& (w_n)_{x_1,y_1,\ldots,x_n} & \geq & \sum_a \frac{1}{2} \alpha_{a,x} v_{a,y} \\
& \mathrm{Diag}(v_a) & \succeq & \sqrt{\beta_{\bar{a}}} \sqrt{\beta_{\bar{a}}}^T \iff \sum_y \frac{\beta_{\bar{a},y}}{v_{a,y}} \leq 1
\end{array}
$$

Point Raises

Point Splits

Alice's Dual

$$
\begin{array}{lrcl}
P^*_{A,0} := \min & z_1 & & \\
s.t. & z_1 & \geq & \sum_{y_1} (z_2)_{x_1,y_1} \\
 & (z_2)_{x_1,y_1} & \geq & \sum_{y_2} (z_3)_{x_1,y_1,x_2,y_2} \\
 & & \vdots & \\
 & (z_n)_{x_1,y_1,\ldots,x_{n-1},y_n} & \geq & (z_{n+1})_{x,y} \\
 & \mathrm{Diag}(z^{(y)}_{n+1}) & \succeq & \frac{1}{2}\beta_{a,y}\sqrt{\alpha_a}\sqrt{\alpha_a}^T
\end{array}
$$

Alice’s Dual

Upper bounds Alice cheating

Point Merges

$$
\begin{array}{rrcl}
P^*_{A,0} := \min & z_1 & & \\
s.t. & z_1 & \geq & \sum_{y_1} (z_2)_{x_1,y_1} \\
& (z_2)_{x_1,y_1} & \geq & \sum_{y_2} (z_3)_{x_1,y_1,x_2,y_2} \\
& & \vdots & \\
& (z_n)_{x_1,y_1,\ldots,x_{n-1},y_n} & \geq & (z_{n+1})_{x,y} \\
& \mathrm{Diag}(z^{(y)}_{n+1}) & \succeq & \frac{1}{2}\beta_{a,y}\sqrt{\alpha_a}\sqrt{\alpha_a}^T \\
& & & \iff \sum_y \frac{\beta_{a,y}\alpha_{a,x}}{2(z_{n+1})_{x,y}} \leq 1
\end{array}
$$

Point Raises

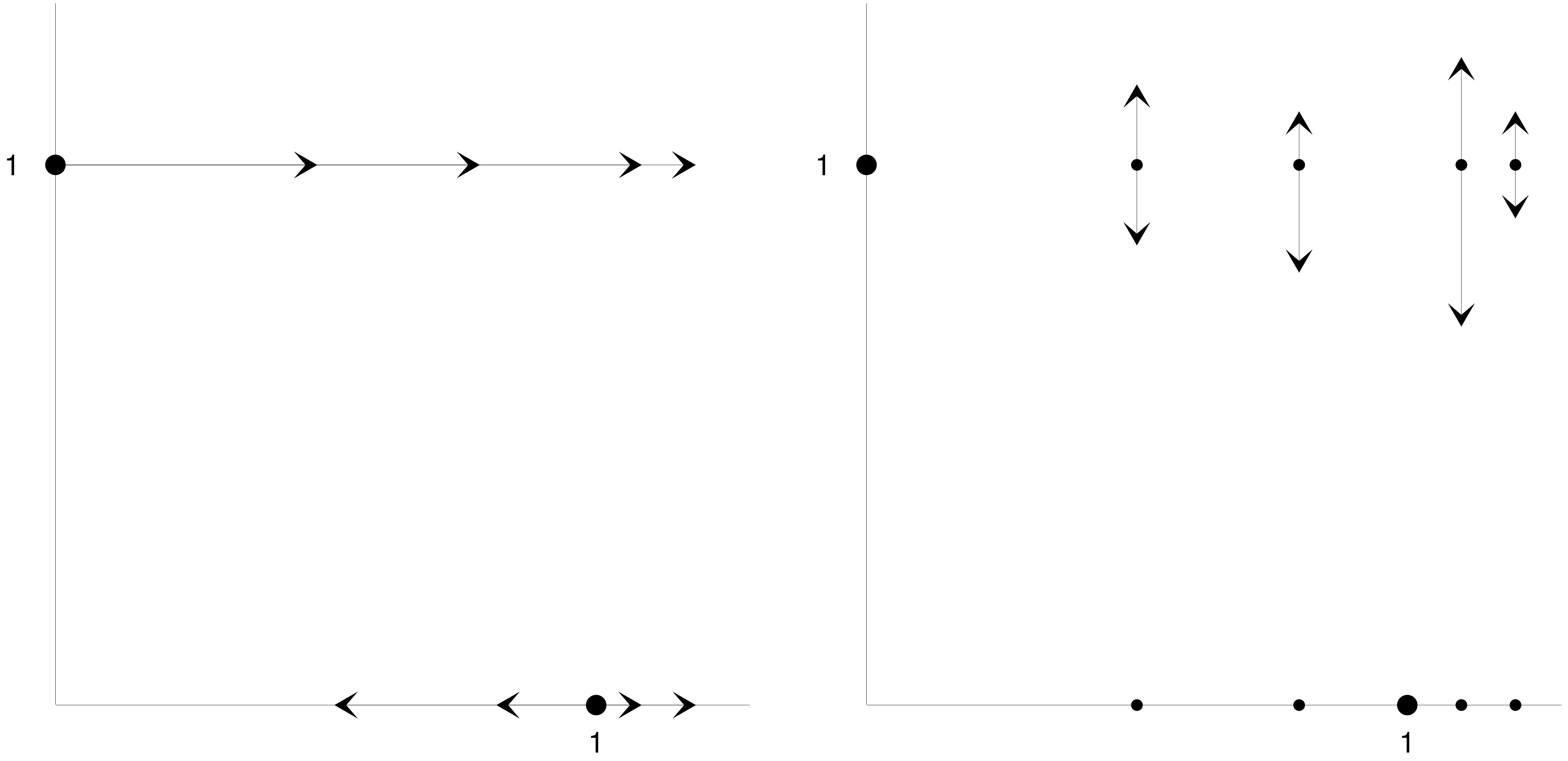
Point Splits

Duals

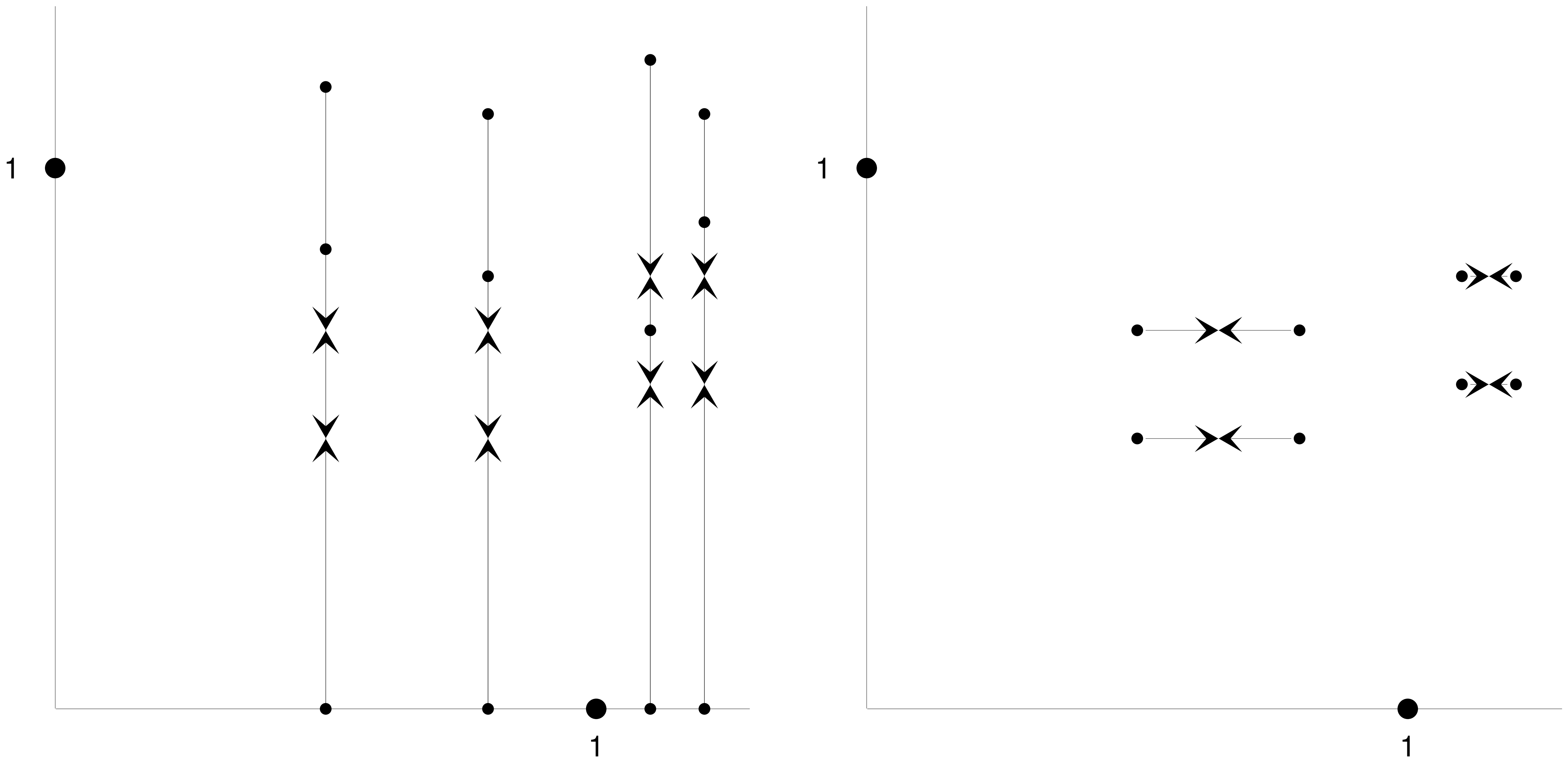
$$\begin{array}{rrcl}
P^*_{B,1} := \min & \sum_{x_1} (w_1)_{x_1} & & \\
s.t. & (w_1)_{x_1} & \geq & \sum_{x_2} (w_2)_{x_1,y_1,x_2} \\
 & (w_2)_{x_1,y_1,x_2} & \geq & \sum_{x_3} (w_3)_{x_1,y_1,x_2,y_2,x_3} \\
 & & \vdots & \\
 & (w_n)_{x_1,y_1,\ldots,x_n} & \geq & \sum_a \frac{1}{2} \alpha_{a,x} v_{a,y} \\
 & \mathrm{Diag}(v_a) & \succeq & \sqrt{\beta_{\bar{a}}}\sqrt{\beta_{\bar{a}}}^T
\end{array}$$

$$\begin{array}{rrcl}
P^*_{A,0} := \min & z_1 & & \\
s.t. & z_1 & \geq & \sum_{y_1} (z_2)_{x_1,y_1} \\
 & (z_2)_{x_1,y_1} & \geq & \sum_{y_2} (z_3)_{x_1,y_1,x_2,y_2} \\
 & & \vdots & \\
 & (z_n)_{x_1,y_1,\ldots,x_{n-1},y_n} & \geq & (z_{n+1})_{x,y} \\
 & \mathrm{Diag}(z^{(y)}_{n+1}) & \succeq & \frac{1}{2} \beta_{a,y} \sqrt{\alpha_a}\sqrt{\alpha_a}^T
\end{array}$$

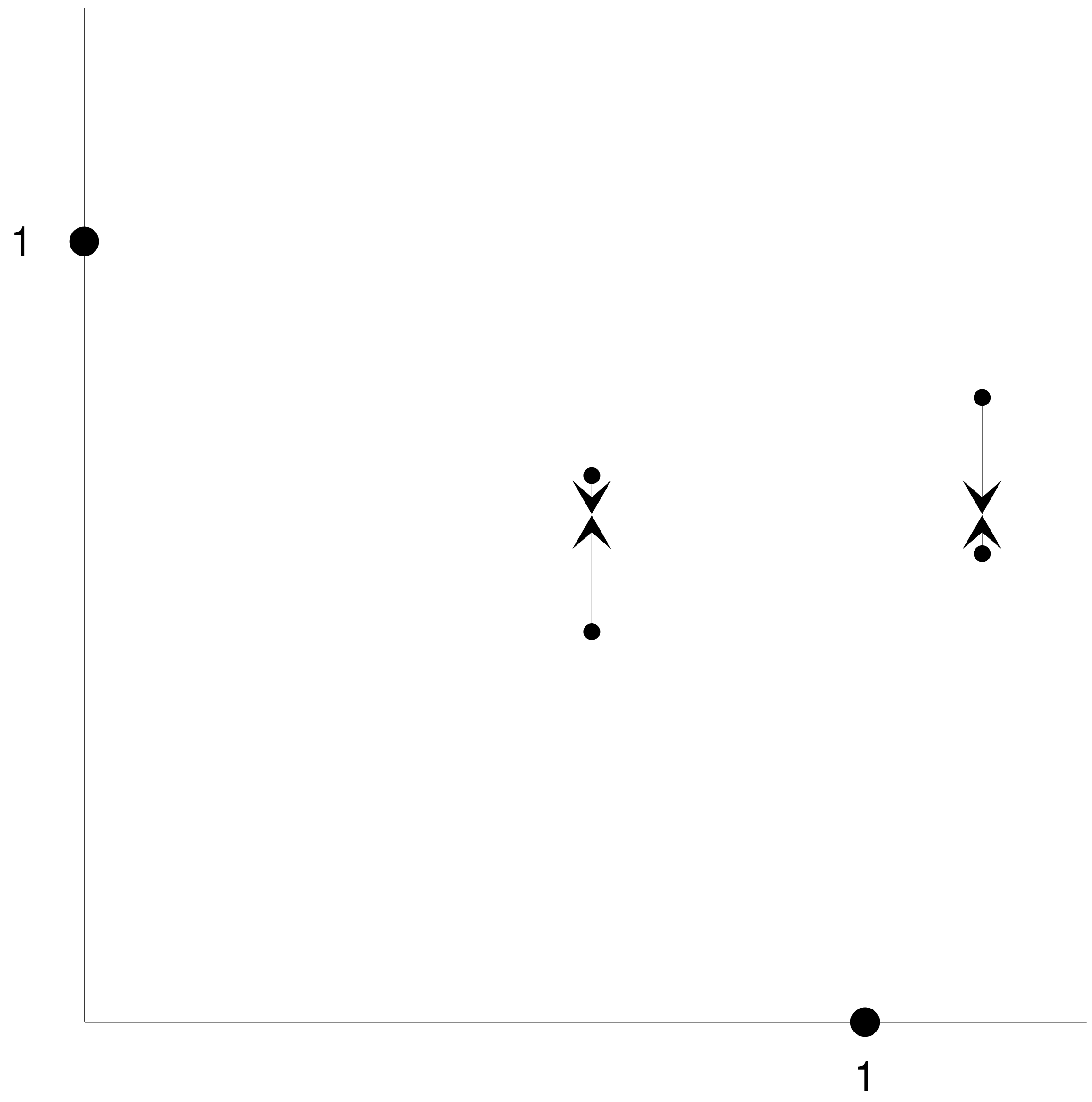
Quantum Point Game (1 of 3)

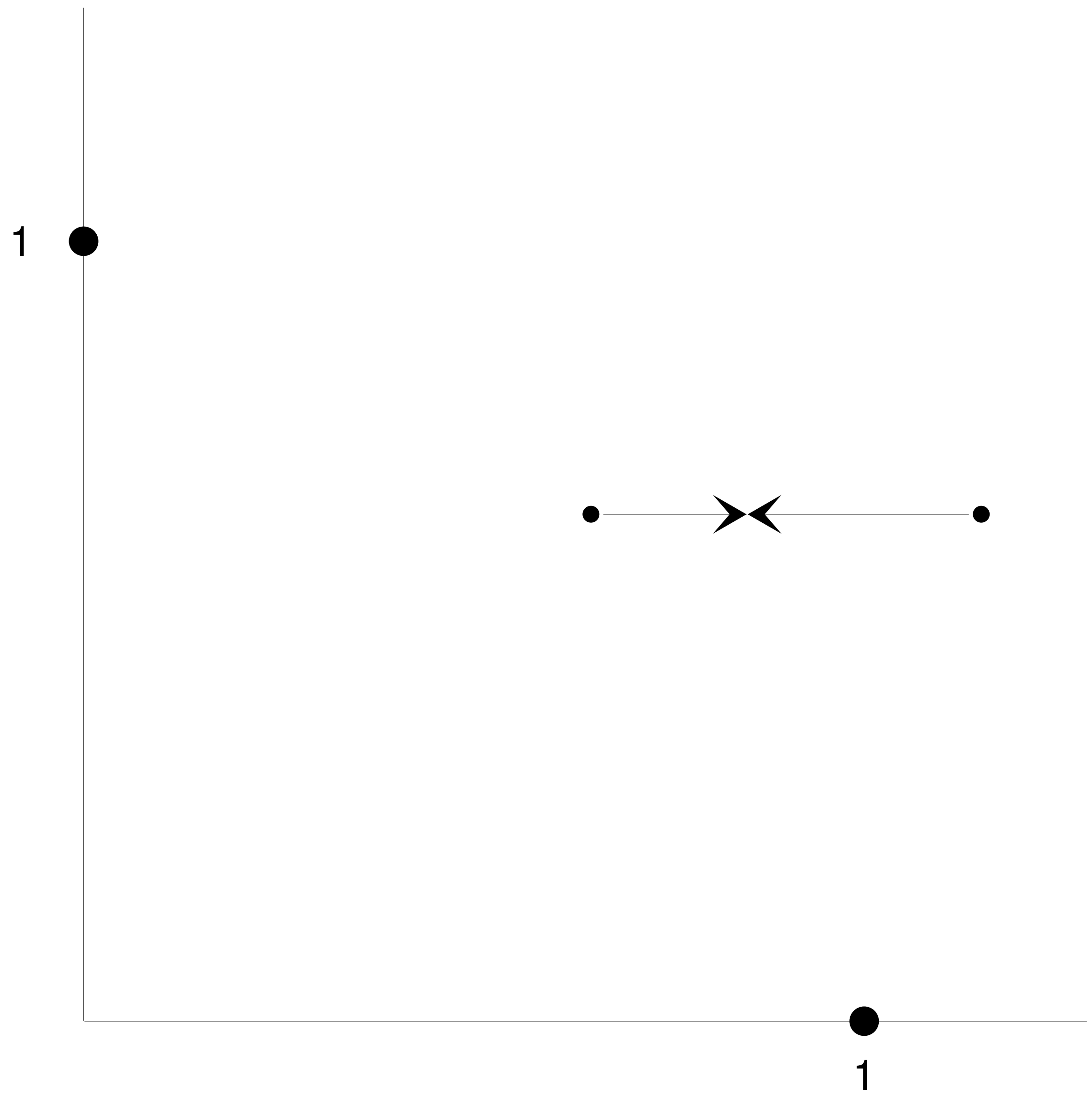


Quantum Point Game (2 of 3)

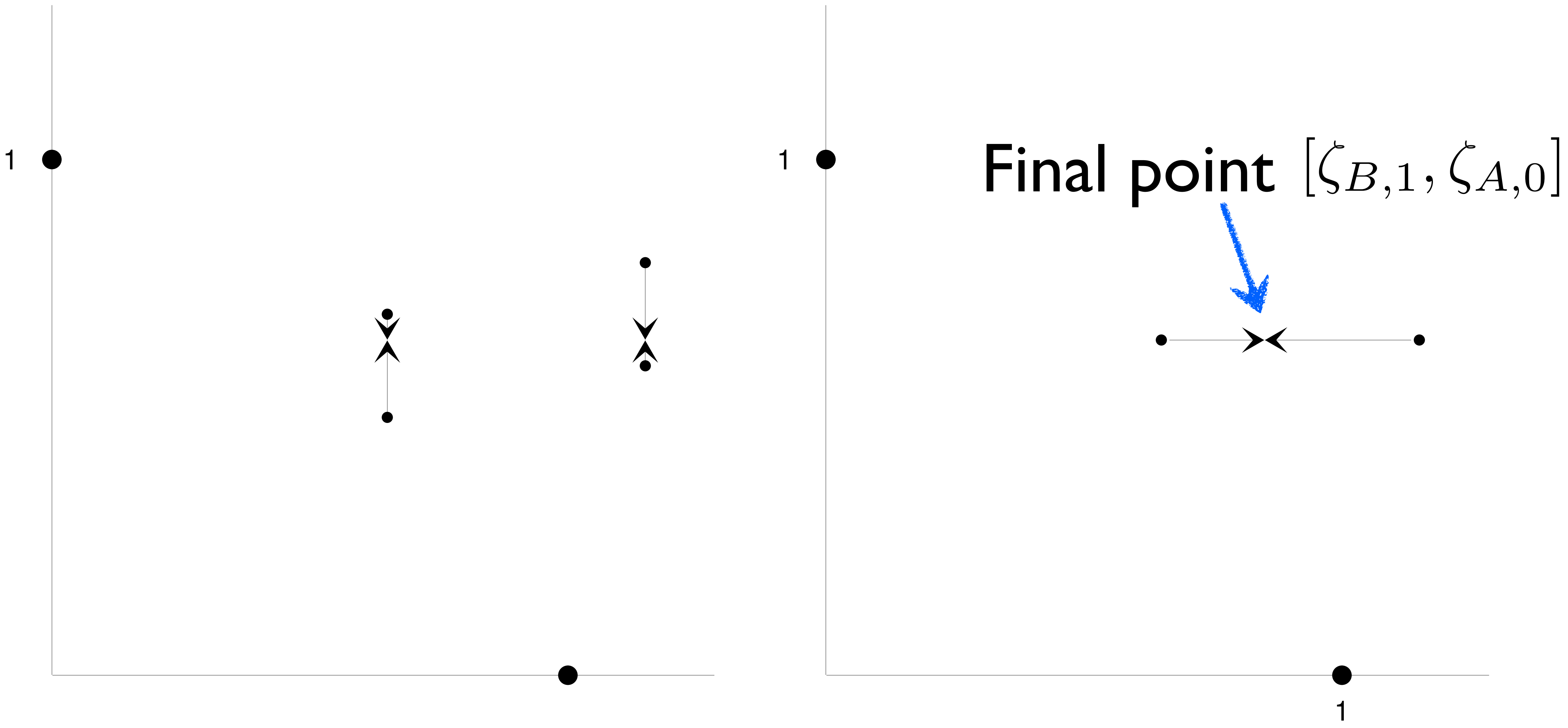


Quantum Point Game (3 of 3)



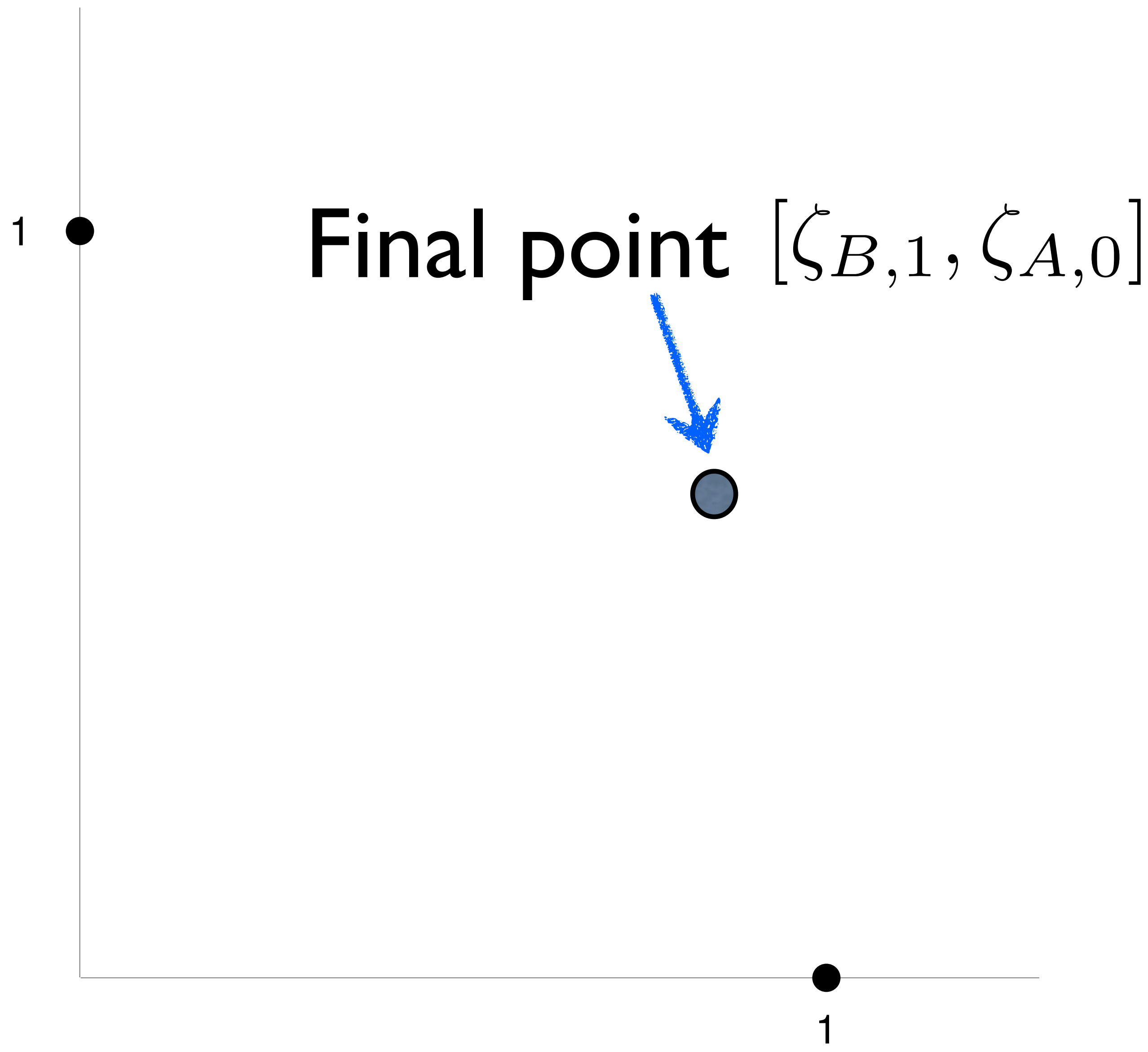


Quantum Point Game (3 of 3)



Final point $[\zeta_{B,1}, \zeta_{A,0}]$

Point Game Usefulness

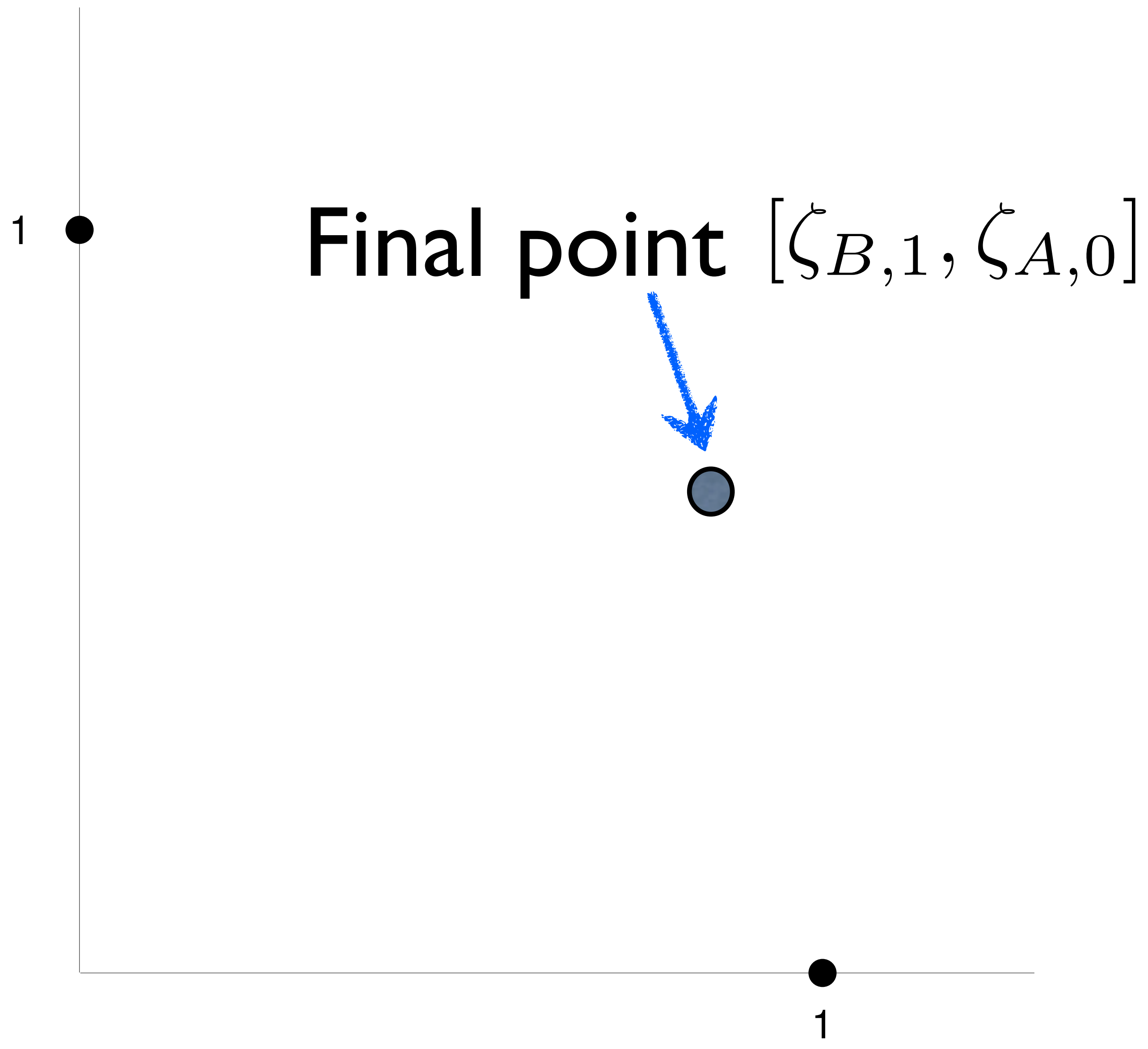


Final point $[\zeta_{B,1}, \zeta_{A,0}]$

Point Game Usefulness

Weak Duality: $P^*_{B,1} \le \zeta_{B,1}$
$P^*_{A,0} \le \zeta_{A,0}$

Strong Duality: $P^*_{B,1} = \zeta_{B,1}$
$P^*_{A,0} = \zeta_{A,0}$
is possible



Point Game Usef ess

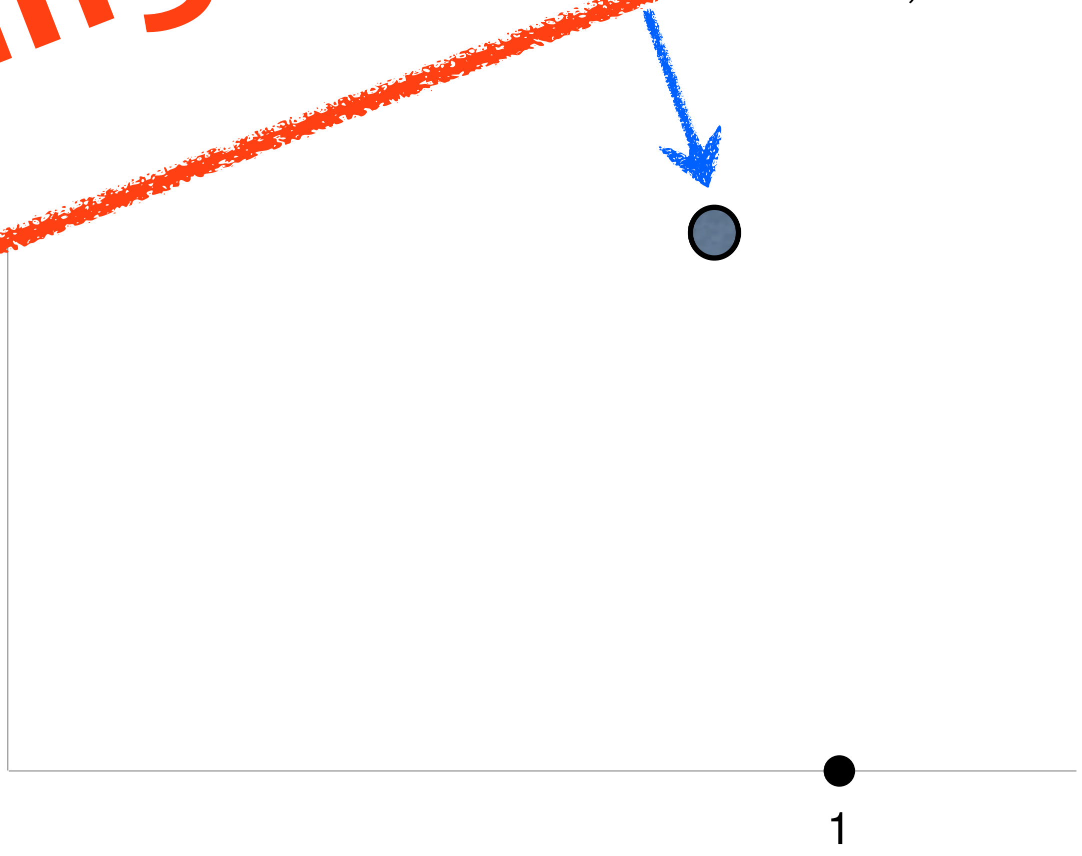
Weak Duality: I

Strong Du

ble

Bounds weak coin-flipping only!

$[\zeta_{B,1}, \zeta_{A,0}]$

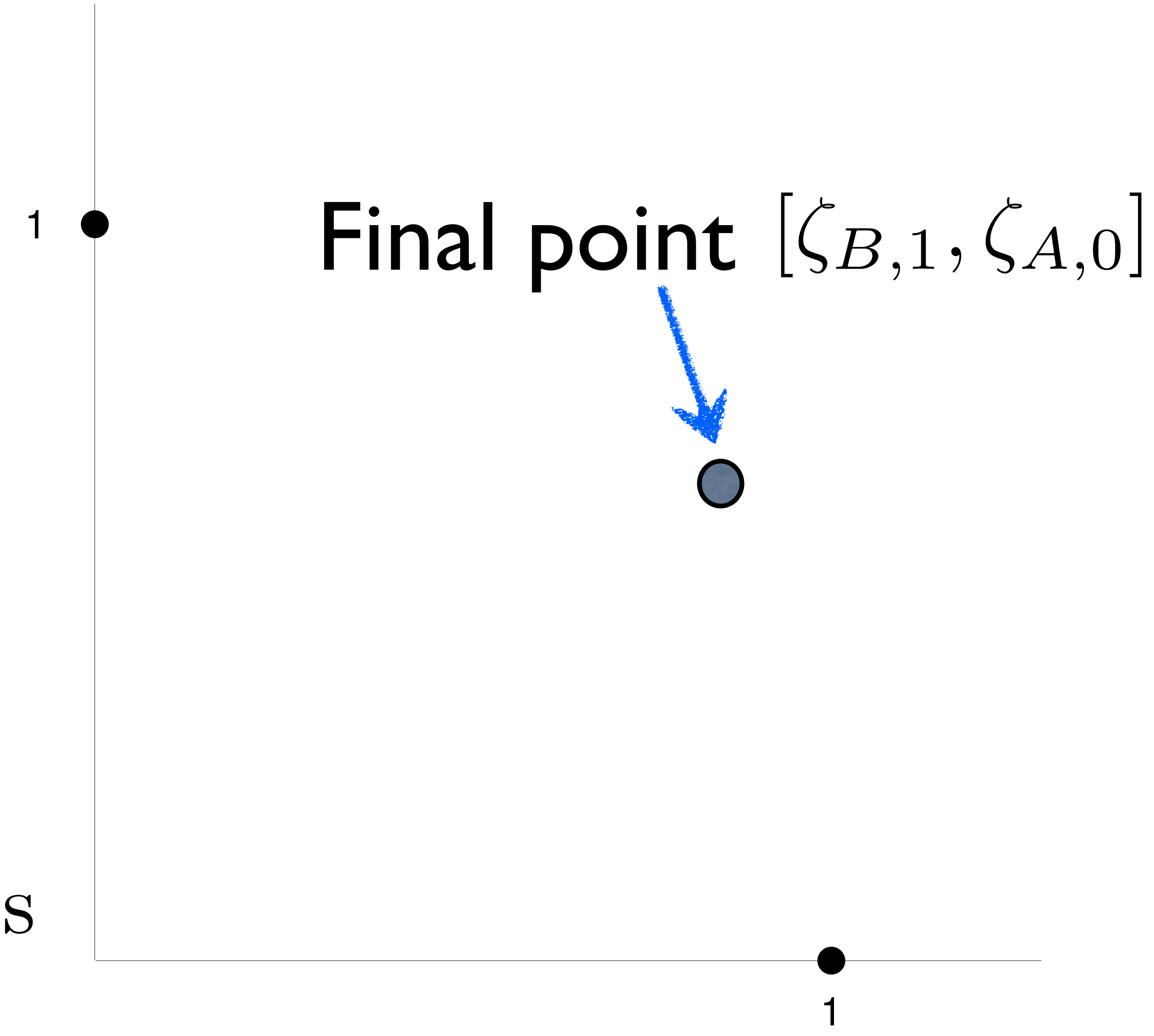


Point Game Usefulness

Weak Duality: $P^*_{B,1} \leq \zeta_{B,1}$
$P^*_{A,0} \leq \zeta_{A,0}$

Strong Duality: $P^*_{B,1} = \zeta_{B,1}$
$P^*_{A,0} = \zeta_{A,0}$
is possible

Can be *paired* to bound the other two cheating probabilities as well



Point Game Usefulness

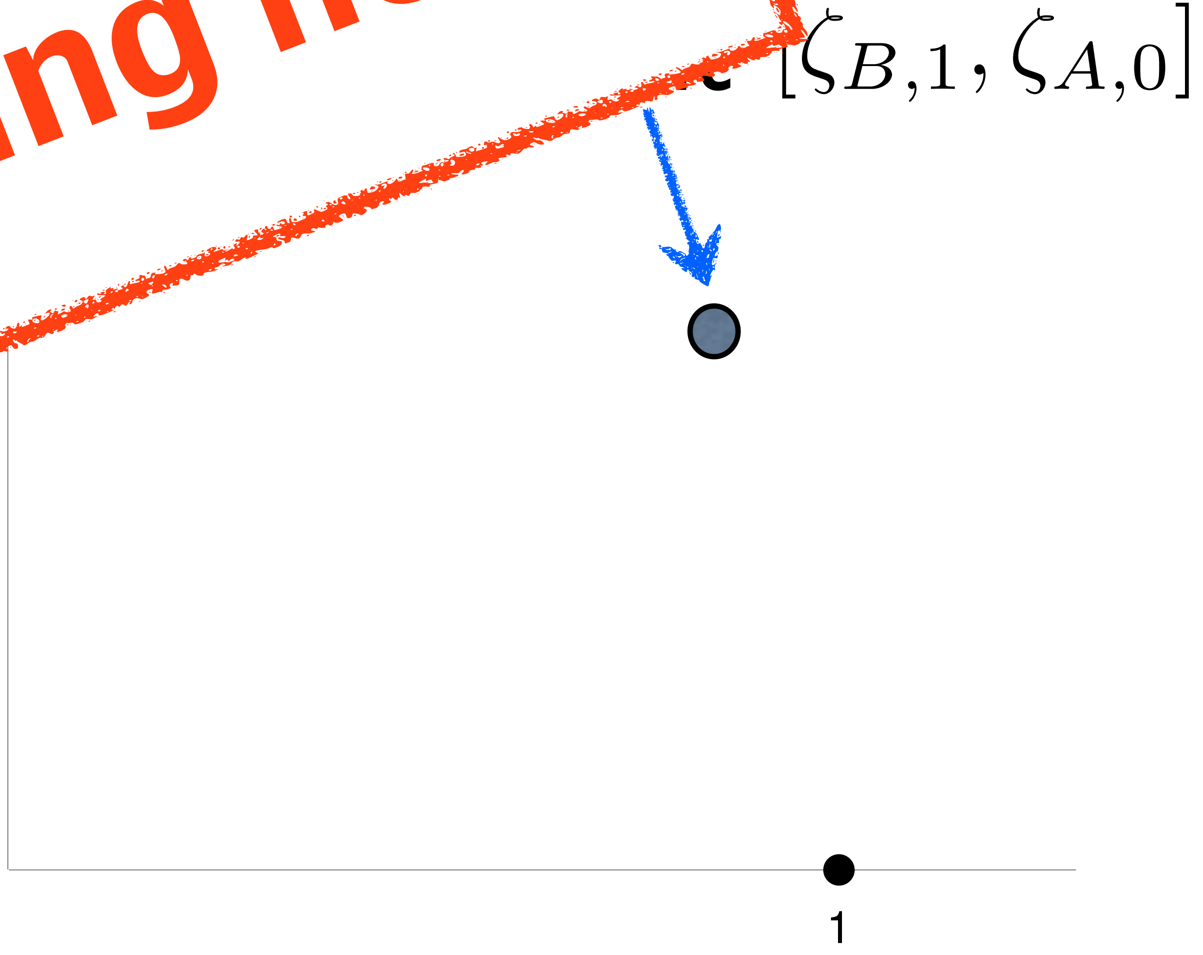
Bounds strong coin-flipping now!

Weak Duality:

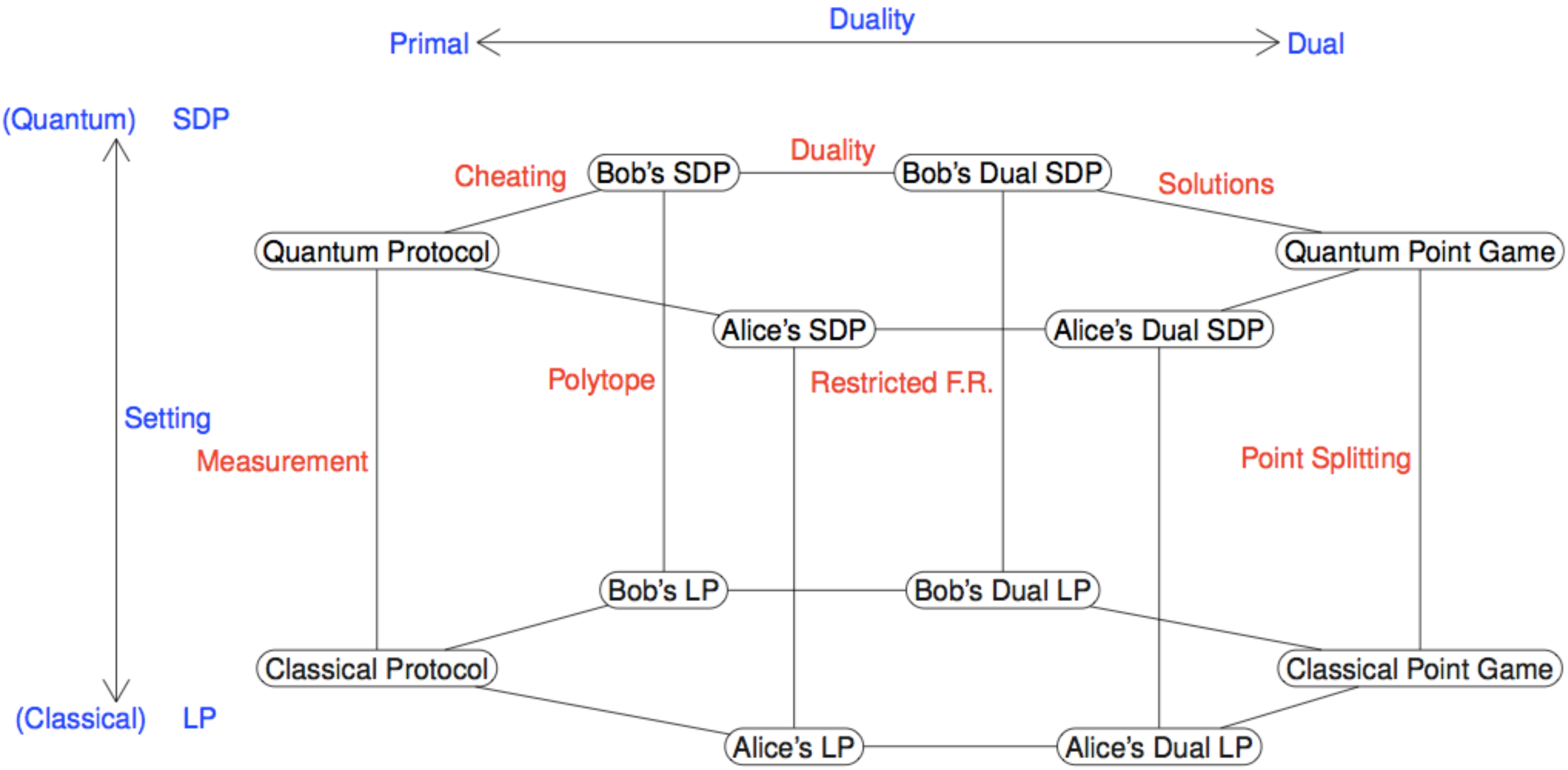
Strong Du

ble

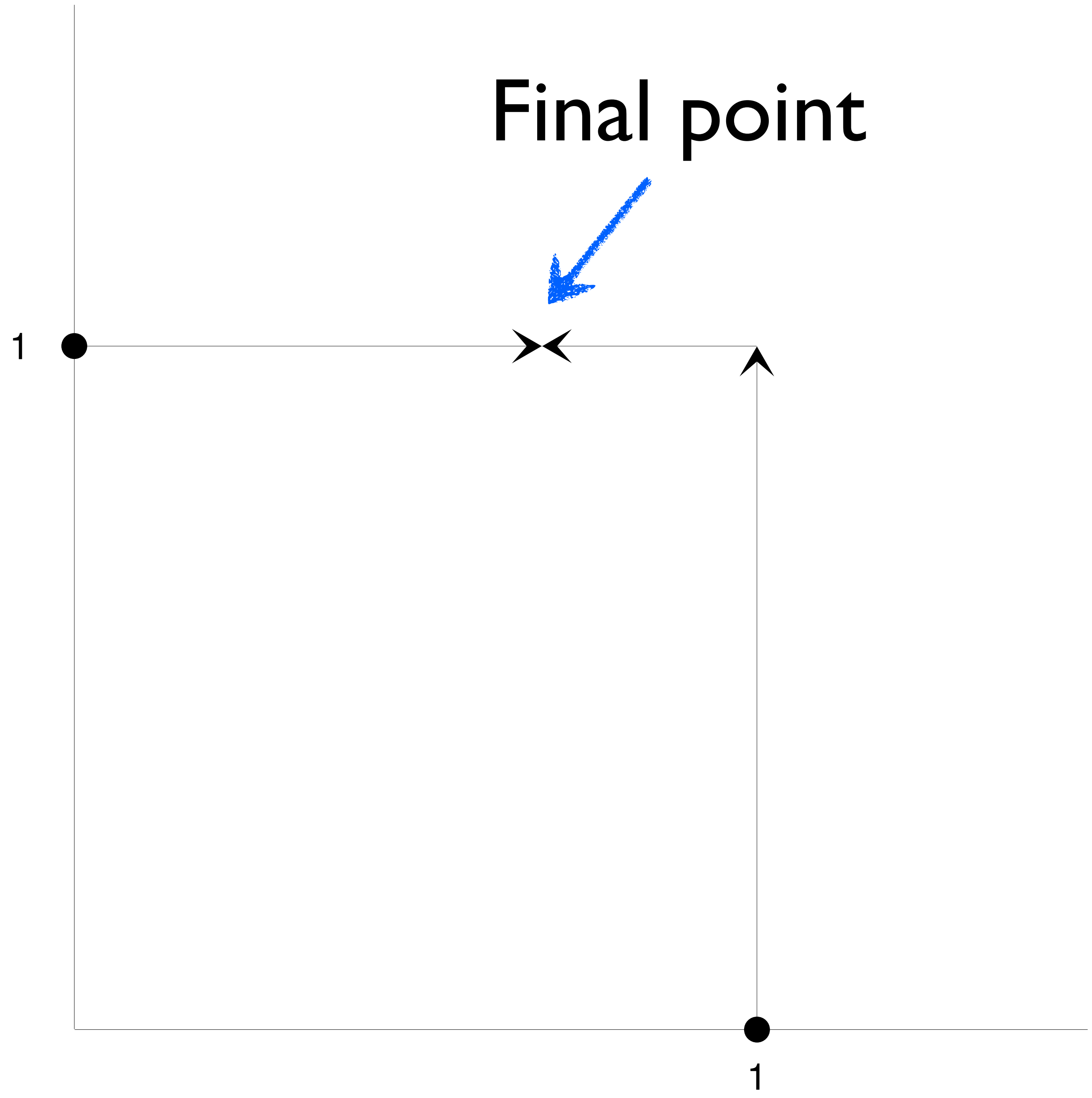
Can be *paired* to bound the other two cheating probabilities as well



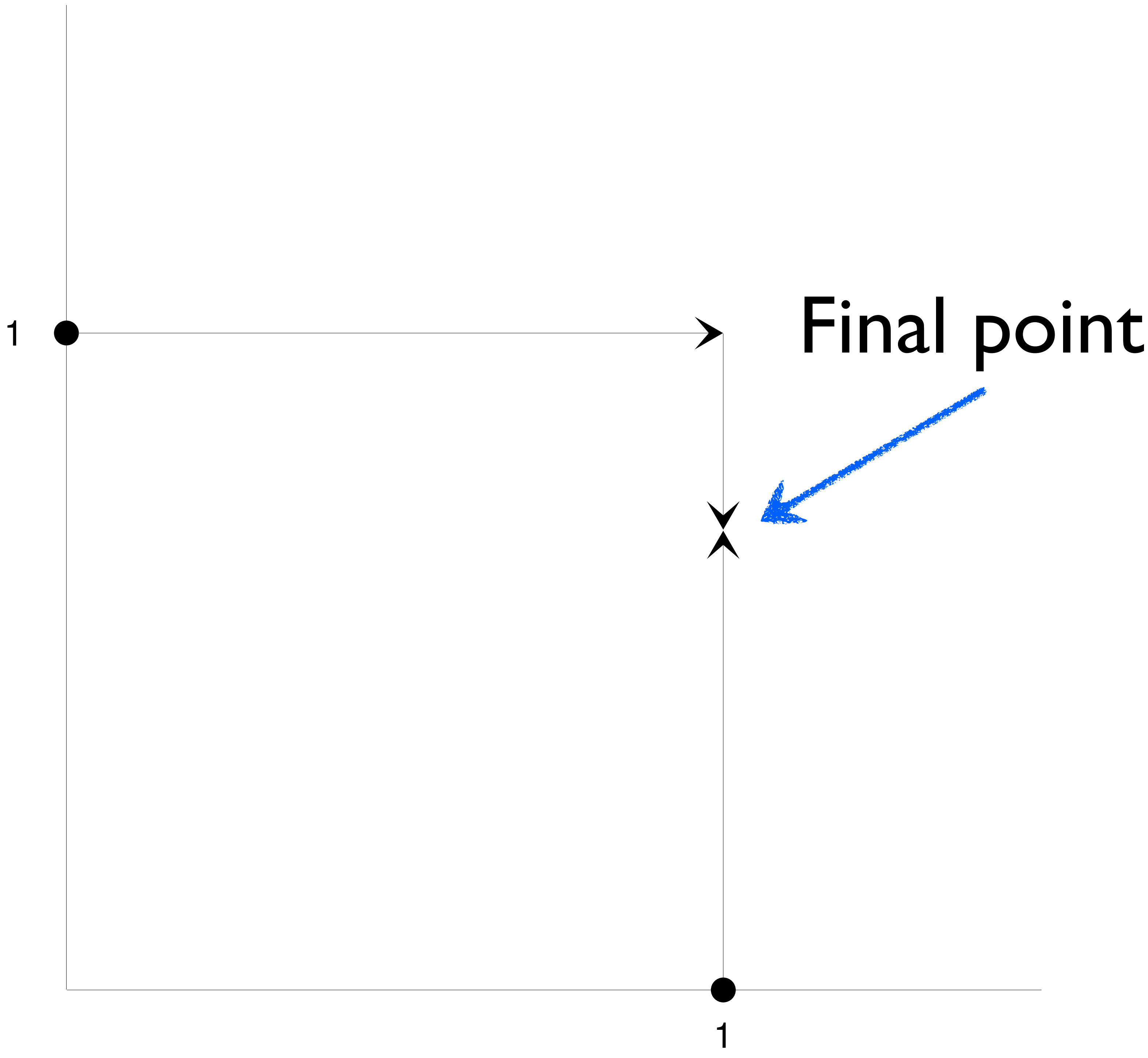
Classical Point Games!



Classical Point Game (Favouring Cheating Alice)



Classical Point Game (Favouring Cheating Bob)



Quantum security from studying classical protocols...

- We have a classical equivalence as well
- Classical point games have large final points
- Classical coin-flipping protocols are insecure
- At most one party can cheat perfectly (holds in the classical and quantum case)
- Quantum protocols (of this form) cannot saturate Kitaev's lower bound

Open questions

- Can we find optimal protocols within this family? (We conjecture 3/4 is optimal from numerical tests)
- Can time-independent point games (TIPGs) be used to simplify things?
- Can we find point games for strong coin-flipping?
- What are the optimal solutions to the SDPs?

Open questions

- Can we find optimal protocols within this family? (We conjecture 3/4 is optimal from numerical tests)
- Can time-independent point games (TIPGs) be used to simplify things?
- Can we find point games for strong coin-flipping?
- What are the optimal solutions to the SDPs?

Thank you!