ECOLE POLYTECHNIQUE DE BRUXELLES

UNIVERSITÉ LIBRE DE BRUXELLES ULB

Quantum Weak Coin Flipping

Jérémie Roland

Joint work with Atul Singh Arora and Stephan Weis

STOC'19 – arXiv:1811.02984

Overview

- Introduction
  - Motivation
  - Problem statement
- Prior art
  - Protocols
  - Point games (TDPG, TIDPG)
- Contributions
  - Protocol with bias 1/10
  - Obtaining protocols with arbitrarily low bias
- Conclusion and outlook

Motivation

Beyond QKD

Multi-party Computation
(dishonest majority)

$\Updownarrow$

Two-party
Secure Function Evaluation

$\Updownarrow$

Oblivious Transfer

$\Downarrow, \not\Uparrow, \Uparrow$

Bit Commitment

$\Downarrow, \not\Uparrow$

Coin Flipping

Quantumly Impossible [Mayers 97, LoChau 97]

Classically all are impossible.

Problem Statement

Strong CF, Weak CF, correctness and bias

Problem Statement

Coin Flipping (CF): Alice and Bob wish to agree on a random bit remotely without trusting each other.

- **Strong Coin Flipping**: No player knows the preference of the other.
- **Weak Coin Flipping (WCF)**: Each player knows the preference of the other.

Situations

Honest player: A player that follows the protocol exactly as described.

Alice	Bob	Remark
Honest	Honest	Correctness
Cheats	Honest	Alice can bias
Honest	Cheats	Bob can bias
Cheats	Cheats	Independent of the protocol

Bias of a protocol: A protocol that solves the CF problem has bias ε if neither player can force their desired outcome with probability more than ½+ε.

Situations | Weak CF

NB. For WCF the players have opposite preferred outcomes.

Alice	Bob	Pr(A wins)	Pr(B wins)
Honest	Honest	P_A	$P_B = 1 - P_A$
Cheats	Honest	P_A^*	$1 - P_A^*$
Honest	Cheats	$1 - P_B^*$	P_B^*

Bias:

$$\text{smallest } \epsilon \text{ s.t. } P_A^*, P_B^* \leq \frac{1}{2} + \epsilon$$

NB.

$$0 \leq \epsilon \leq \frac{1}{2}$$

Situations | Weak CF | Flip and declare

Protocol: Alice flips a coin and declares the outcome to Bob.

Alice	Bob	Pr(A wins)	Pr(B wins)
Honest	Honest	$P_A = 1/2$	$P_B = 1/2$
Cheats	Honest	$P_A^* = 1$	$1 - P_A^* = 0$
Honest	Cheats	$1 - P_B^* = 1/2$	$P_B^* = 1/2$

Bias: $\text{smallest } \epsilon \text{ s.t. } P_A^*, P_B^* \leq \frac{1}{2} + \epsilon \implies \epsilon = \frac{1}{2}$

Prior Art

Bounds and protocols, Kitaev’s Frameworks, Mochon’s Breakthrough

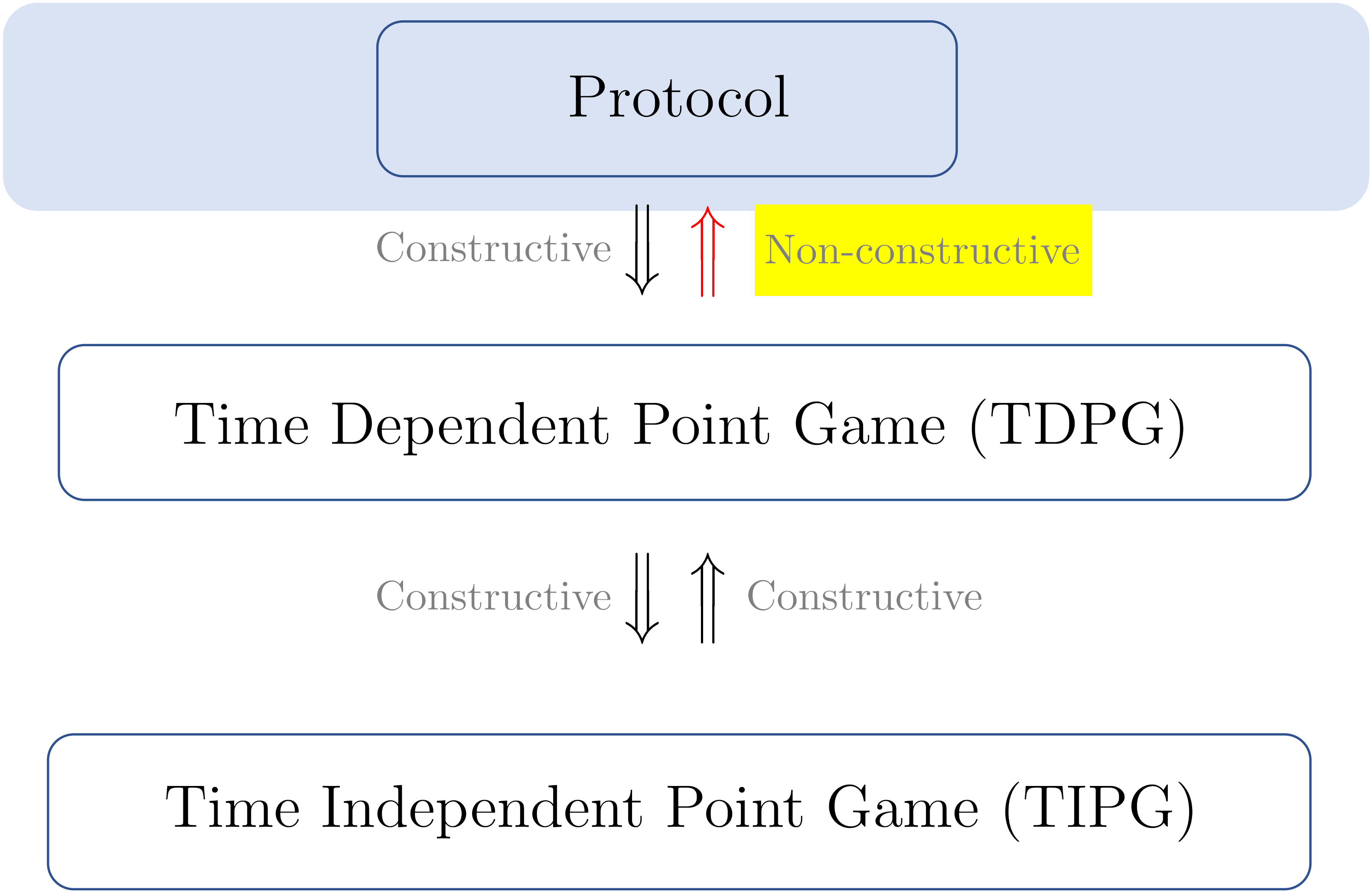
Bounds and Protocols

Classically: $\epsilon = \frac{1}{2}$ viz. at least one player can always cheat and win.

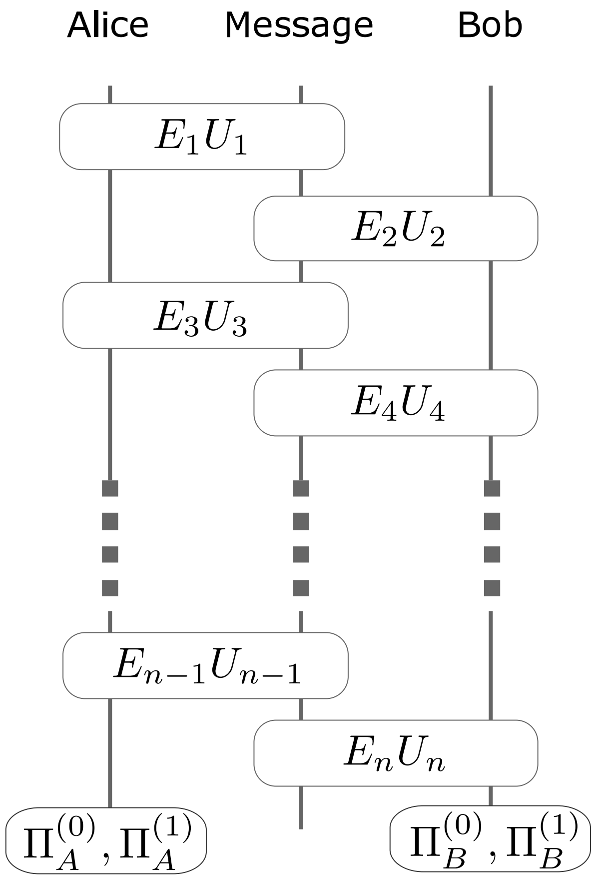
Quantumly:

	Bound	Best protocol known
Strong CF	$\epsilon \geq \frac{1}{\sqrt{2}} - \frac{1}{2}$ [Kitaev 03]	$\epsilon = \frac{1}{4}$ [Ambainis 01] $\epsilon \to \frac{1}{\sqrt{2}} - \frac{1}{2}$ [Chailloux Kerenidis 09]
Weak CF	$\epsilon \to 0$ [Mochon 07] [Aharonov et al 16]	$\epsilon \to \frac{1}{6}$ [Mochon 05]

Kitaev | Three Equivalent Frameworks



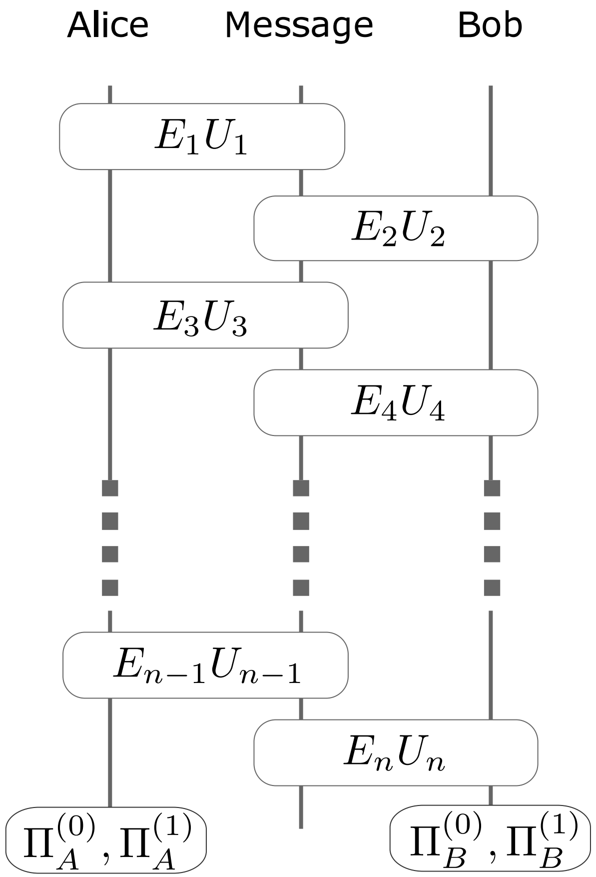
Kitaev | Protocol | Definition



Protocol described by

- Initial (product) state $|\psi_0\rangle_{AMB}$
- Unitaries U_i and projectors E_i alternating between
  - ⋆ Alice for i odd
  - ⋆ Bob for i even
- Final measurements (POVMs)
  - ⋆ $\{\Pi_A^{(0)}, \Pi_A^{(1)}\}$ for Alice
  - ⋆ $\{\Pi_B^{(0)}, \Pi_B^{(1)}\}$ for Bob
- We assume
  - ⋆ 0 means "Alice wins"
  - ⋆ 1 means "Bob wins"

Kitaev | Protocol | Honest players



For honest players

- **Honest state:** The global state after step i is given by

$$|\psi_i\rangle = U_i U_{i-1} \dots U_1 |\psi_0\rangle$$

  - ⋆ "Cheat detection" projectors E_i do not affect the "honest" state

- **Correctness:** Final measurements never yield different outcomes

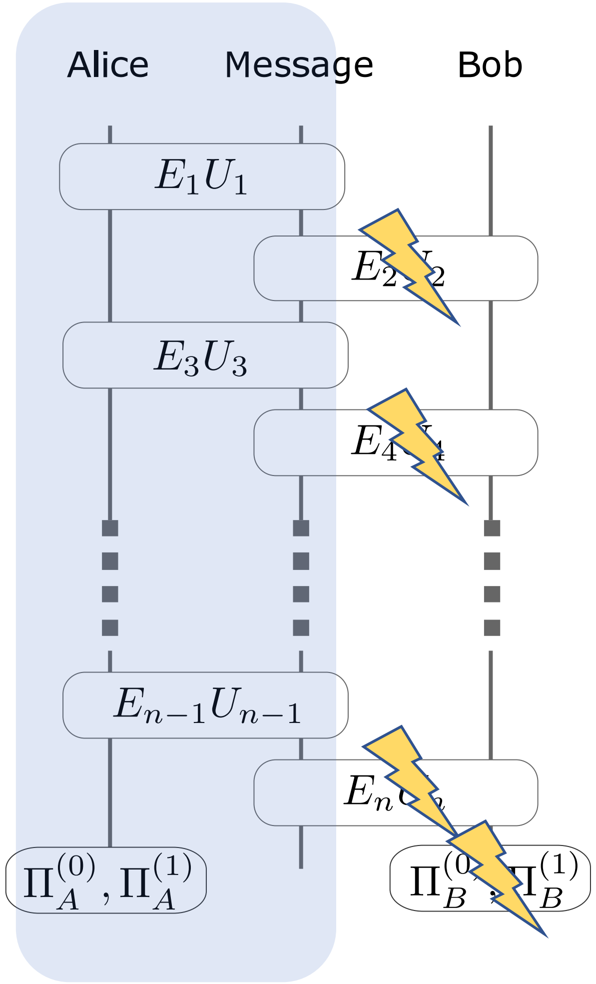
$$\Pi_A^{(0)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(1)} |\psi_n\rangle = \Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(0)} |\psi_n\rangle = 0$$

- **Balanced:** Each player wins with probability 1/2

$$P_A = \|\Pi_A^{(0)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(0)} |\psi_n\rangle \|^2 = \frac{1}{2}$$

$$P_B = \|\Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(1)} |\psi_n\rangle \|^2 = \frac{1}{2}$$

Kitaev | Protocol | Cheating Bob



If Bob is cheating (but Alice remains honest)

- Focus on the Alice-Message reduced state $\rho_{AM,i}$
- Bob cannot affect the initial state

$$\rho_{AM,0} = \mathrm{Tr}_{\mathcal{B}}(|\psi_0\rangle\langle\psi_0|) = |\psi_{AM,0}\rangle\langle\psi_{AM,0}|$$

- For i odd, Alice is honest

$$\rho_{AM,i} = E_i U_i \rho_{AM,i-1} U_i^\dagger E_i$$

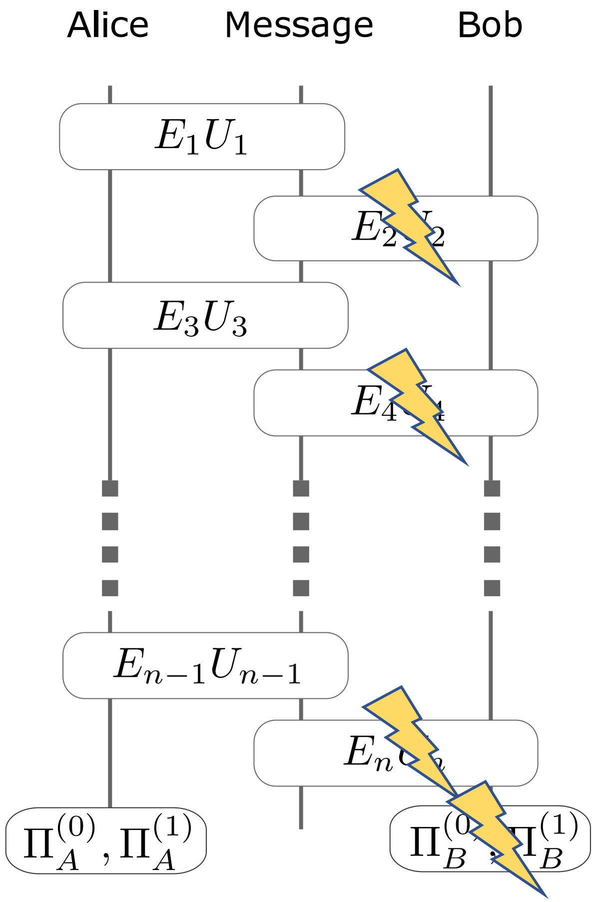
- For i even, Bob can apply any operation on $\mathcal{M}$ but cannot affect $\mathcal{A}$

$$\mathrm{Tr}_{\mathcal{M}}(\rho_{AM,i}) = \mathrm{Tr}_{\mathcal{M}}(\rho_{AM,i-1})$$

- Bob tries to maximise the probability that Alice declares him to be the winner

$$\mathrm{Tr}((\Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}})\rho_{AM,n})$$

Kitaev | Protocol | Cheating Bob



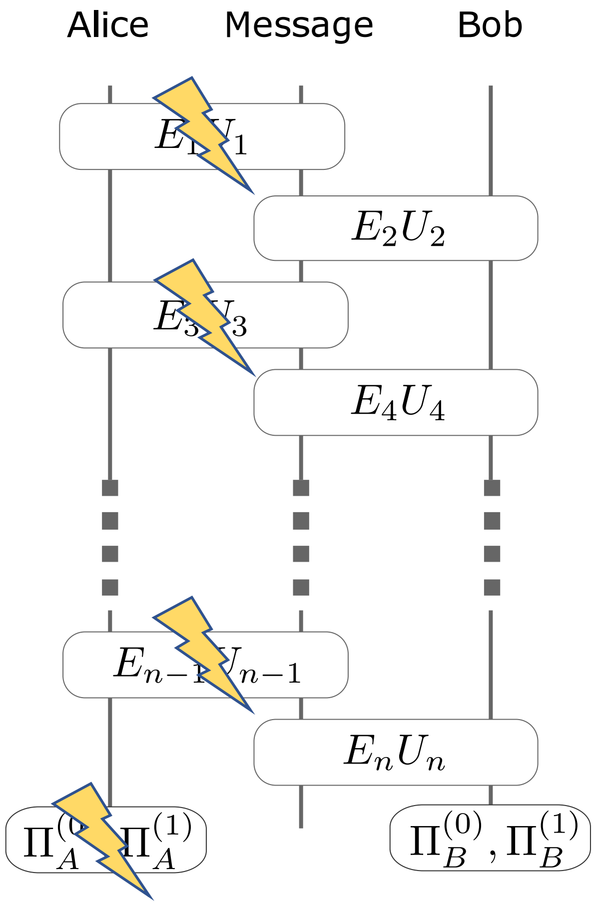
Bob's maximum cheating probability is given by an SDP

$$P_B^* = \max_{\rho_{AM,i}} \mathrm{Tr}((\Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}})\rho_{AM,n})$$

subject to

- $\rho_{AM,0} = \mathrm{Tr}_{\mathcal{B}}(|\psi_0\rangle\langle\psi_0|) = |\psi_{AM,0}\rangle\langle\psi_{AM,0}|$;
- for i odd, $\rho_{AM,i} = E_i U_i \rho_{AM,i-1} U_i^\dagger E_i$;
- for i even, $\mathrm{Tr}_{\mathcal{M}}(\rho_{AM,i}) = \mathrm{Tr}_{\mathcal{M}}(\rho_{AM,i-1})$.

Kitaev | Protocol | Cheating Alice



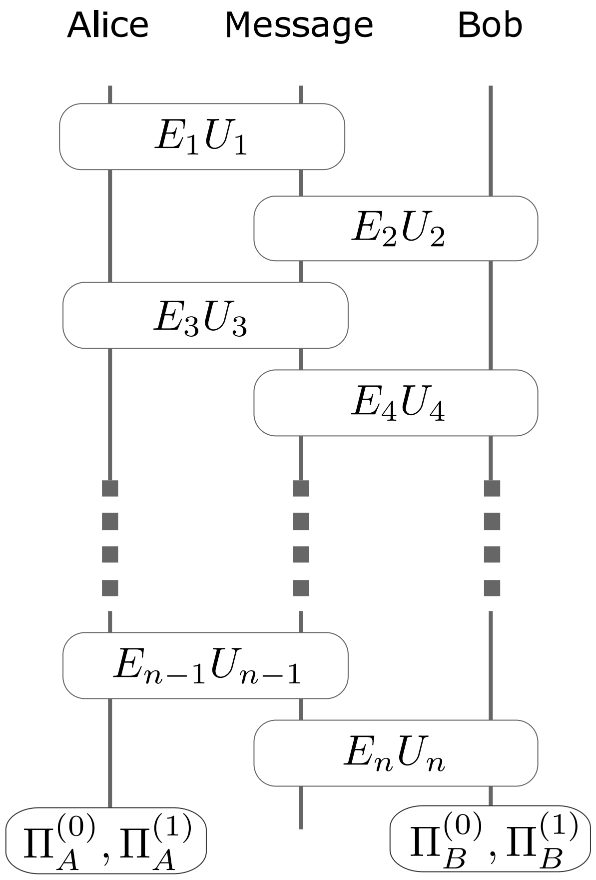
Alice's maximum cheating probability is given by an SDP

$$P_A^* = \max_{\rho_{MB,i}} \mathrm{Tr}((\Pi_B^{(0)} \otimes \mathbb{I}_{\mathcal{M}})\rho_{MB,n})$$

subject to

- $\rho_{MB,0} = \mathrm{Tr}_{\mathcal{A}}(|\psi_0\rangle\langle\psi_0|) = |\psi_{MB,0}\rangle\langle\psi_{MB,0}|$;
- for i odd, $\mathrm{Tr}_{\mathcal{M}}(\rho_{MB,i}) = \mathrm{Tr}_{\mathcal{M}}(\rho_{MB,i-1})$.
- for i even, $\rho_{MB,i} = E_iU_i\rho_{MB,i-1}U_i^\dagger E_i$;

Kitaev | Dual SDPs



We want to upper bound the cheating probabilities
$\Rightarrow$ Better to work with dual SDPs

$$P_B^* = \min_{Z_{A,i} \geq 0} \operatorname{Tr}(Z_{A,0} \left|\psi_{A,0}\right\rangle \left\langle\psi_{A,0}\right|)$$

subject to

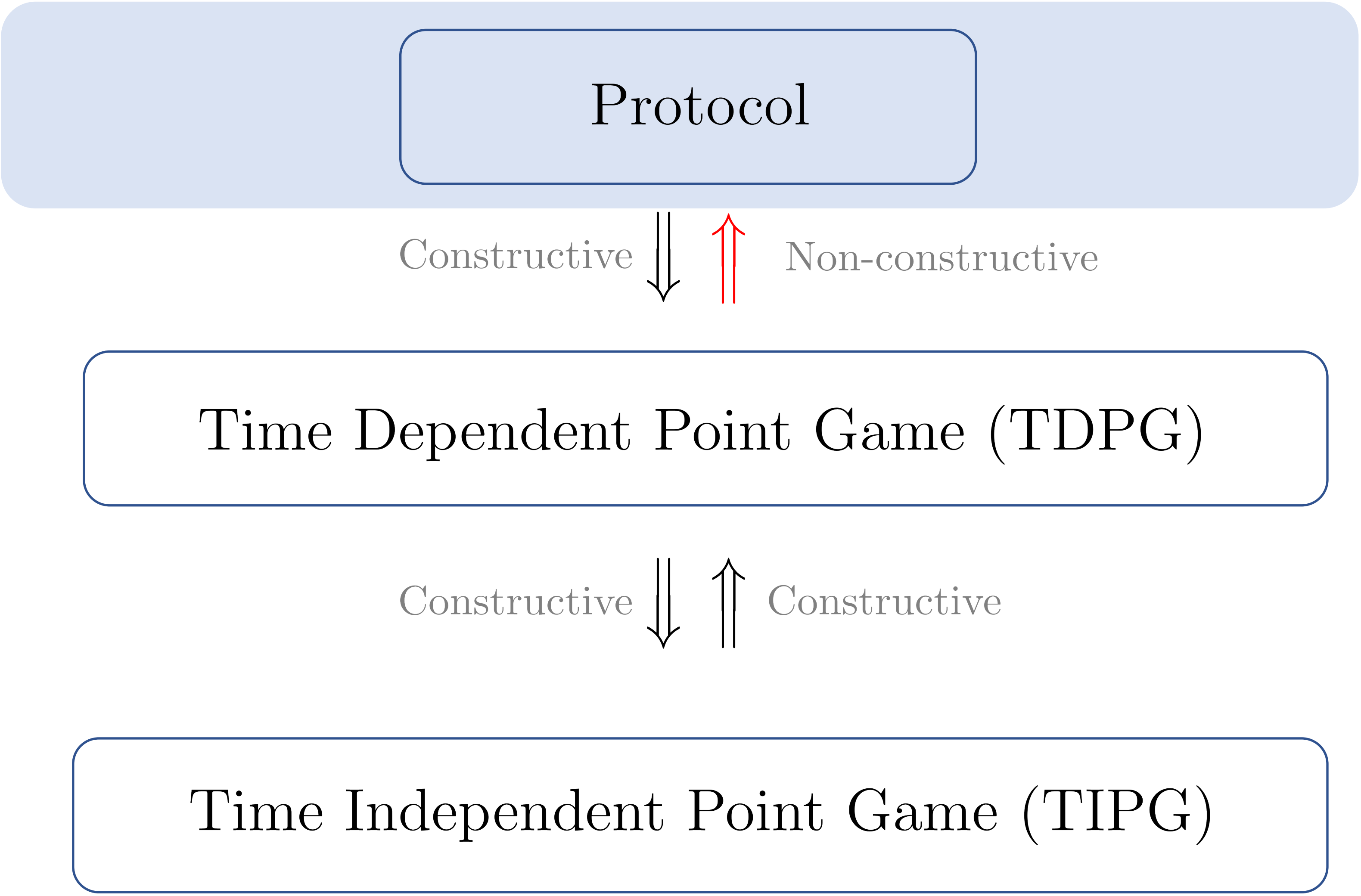
- for i odd, $Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \geq U_{A,i}^{\dagger} E_{A,i} (Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}}) E_{A,i} U_{A,i}$;
- for i even, $Z_{A,i-1} = Z_{A,i}$;
- $Z_{A,n} = \Pi_A^{(1)}$.

$$P_A^* = \min_{Z_{B,i} \geq 0} \operatorname{Tr}(Z_{B,0} \left|\psi_{B,0}\right\rangle \left\langle\psi_{B,0}\right|)$$

subject to

- for i even, $\mathbb{I}_{\mathcal{M}} \otimes Z_{B,i-1} \geq U_{B,i}^{\dagger} E_{B,i} (\mathbb{I}_{\mathcal{M}} \otimes Z_{B,i}) E_{B,i} U_{B,i}$;
- for i odd, $Z_{B,i-1} = Z_{B,i}$;
- $Z_{B,n} = \prod_B^{(0)}$.

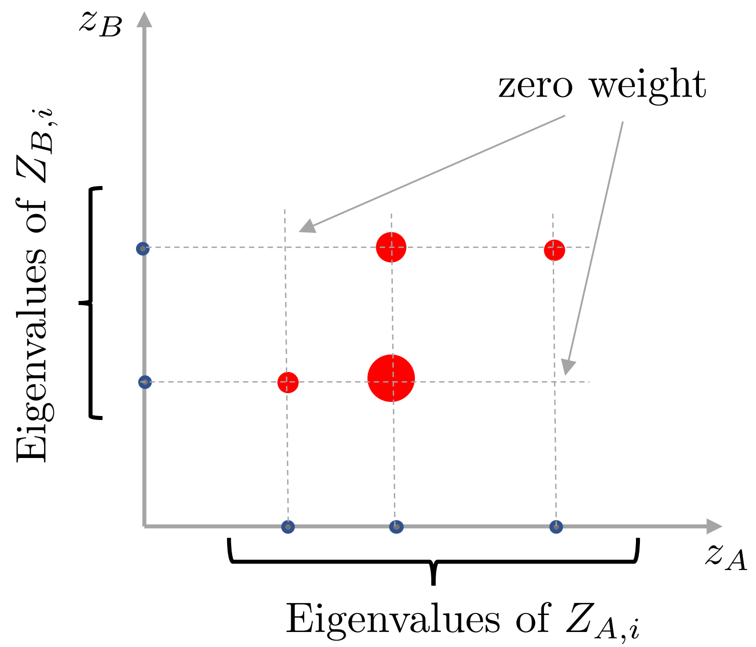
Kitaev | Three Equivalent Frameworks



Kitaev | Time Dependent Point Game

For each $\boldsymbol{i}$, construct the following graphical representation (frame)

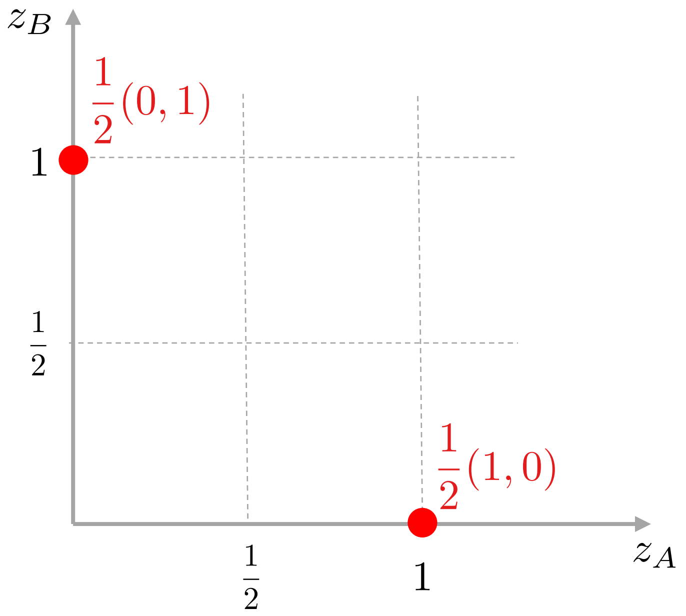
- Set of weighted points on a 2D figure
- Point coordinates: $(\boldsymbol{z_A}, \boldsymbol{z_B})$
  - ⋆ $\boldsymbol{z_A}$ runs over eigenvalues of dual variable $\boldsymbol{Z_{A,i}}$
  - ⋆ $\boldsymbol{z_B}$ runs over eigenvalues of dual variable $\boldsymbol{Z_{B,i}}$
- Point weights: $\boldsymbol{p_{z_A,z_B}} = \langle \boldsymbol{\psi_i} | \boldsymbol{\Pi}^{[\boldsymbol{z_A}]} \otimes \boldsymbol{\Pi}^{[\boldsymbol{z_B}]} | \boldsymbol{\psi_i} \rangle$
  - ⋆ $|\boldsymbol{\psi_i}\rangle$ is the honest state at step $\boldsymbol{i}$
  - ⋆ $\boldsymbol{\Pi}^{[\boldsymbol{z_A}]}$ is the projector on the corresponding eigenspace of $\boldsymbol{Z_{A,i}}$
  - ⋆ $\boldsymbol{\Pi}^{[\boldsymbol{z_B}]}$ is the projector on the corresponding eigenspace of $\boldsymbol{Z_{B,i}}$
- Notation
  - ⋆ $\text{Prob}[\boldsymbol{Z_{A,i}} \otimes \boldsymbol{Z_{B,i}}, |\boldsymbol{\psi_i}\rangle] = \sum_{\boldsymbol{z_A},\boldsymbol{z_B}} \boldsymbol{p_{z_A,z_B}} \cdot (\boldsymbol{z_A}, \boldsymbol{z_B})$



Kitaev | TDPG | SDP constraints

SDP constraints

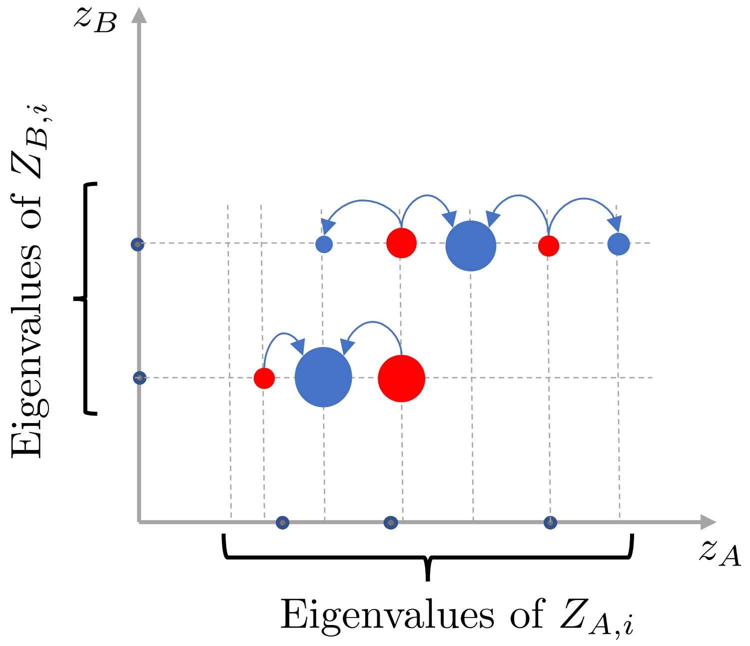
- Initialization
  - ⋆ $\frac{1}{2}(0,1) + \frac{1}{2}(1,0)$
- Point transitions
  - ⋆ i odd $\rightarrow$ Horizontal transition
  - ⋆ i even $\rightarrow$ Vertical transition
- Finalization
  - ⋆ $1 \cdot (\beta, \alpha)$ where
  - ⋆ $\alpha = P_A^*$ (Alice's cheating probability)
  - ⋆ $\beta = P_B^*$ (Bob's cheating probability)



Kitaev | TDPG | SDP constraints

SDP constraints

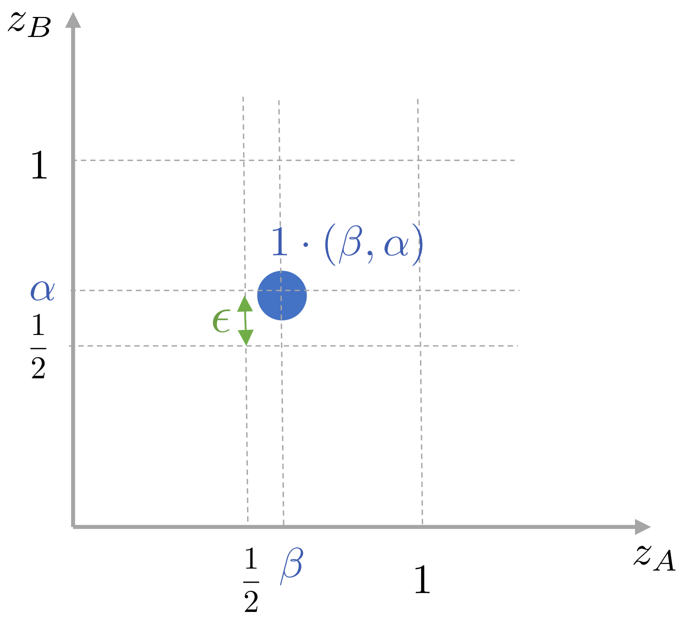
- Initialization
  - ⋆ $\frac{1}{2}(0,1) + \frac{1}{2}(1,0)$
- Point transitions
  - ⋆ i odd $\rightarrow$ Horizontal transition
  - ⋆ i even $\rightarrow$ Vertical transition
- Finalization
  - ⋆ $1 \cdot (\beta, \alpha)$ where
  - ⋆ $\alpha = P_A^*$ (Alice's cheating probability)
  - ⋆ $\beta = P_B^*$ (Bob's cheating probability)



Kitaev | TDPG | SDP constraints

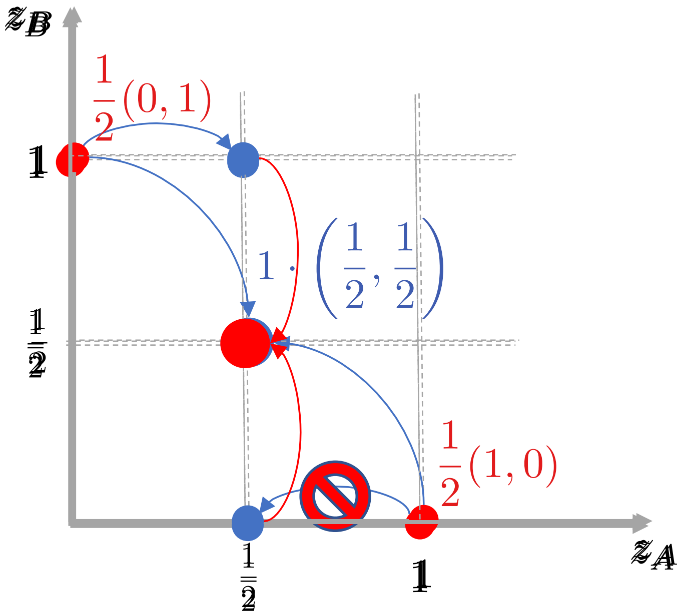
SDP constraints

- Initialization
  - ⋆ $\frac{1}{2}(0,1) + \frac{1}{2}(1,0)$
- Point transitions
  - ⋆ i odd $\rightarrow$ Horizontal transition
  - ⋆ i even $\rightarrow$ Vertical transition
- Finalization
  - ⋆ $1 \cdot (\beta, \alpha)$ where
  - ⋆ $\alpha = P_A^*$ (Alice's cheating probability)
  - ⋆ $\beta = P_B^*$ (Bob's cheating probability)



Kitaev | TDPG | Naïve (wrong) protocol

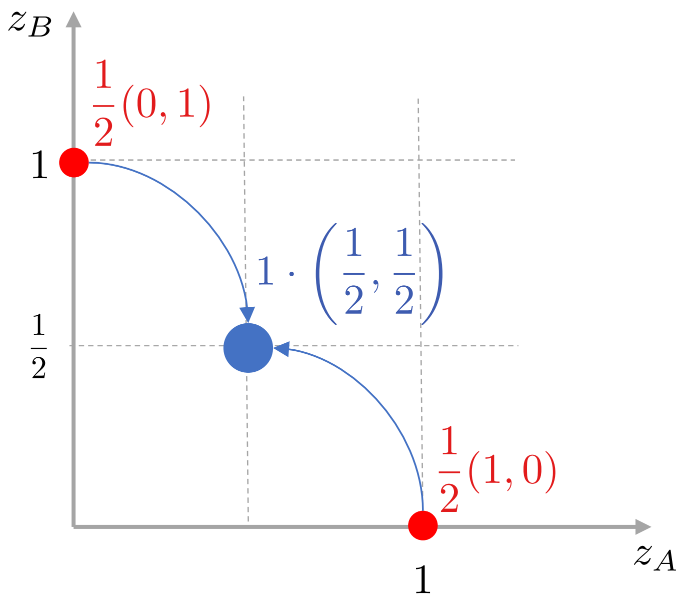
- Ideally
  - ⋆ Zero bias → Final point $(\frac{1}{2}, \frac{1}{2})$
- Naïve (wrong) protocol
  - ⋆ One horizontal transition
  - ⋆ One vertical transition
- Problem
  - ⋆ This transition is not valid
  - ⋆ For each line, coordinates of the center of mass can only increase



$$Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \geq U^{\dagger}_{A,i} E_{A,i} (Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}}) E_{A,i} U_{A,i}$$

Kitaev | TDPG | Naïve (wrong) protocol

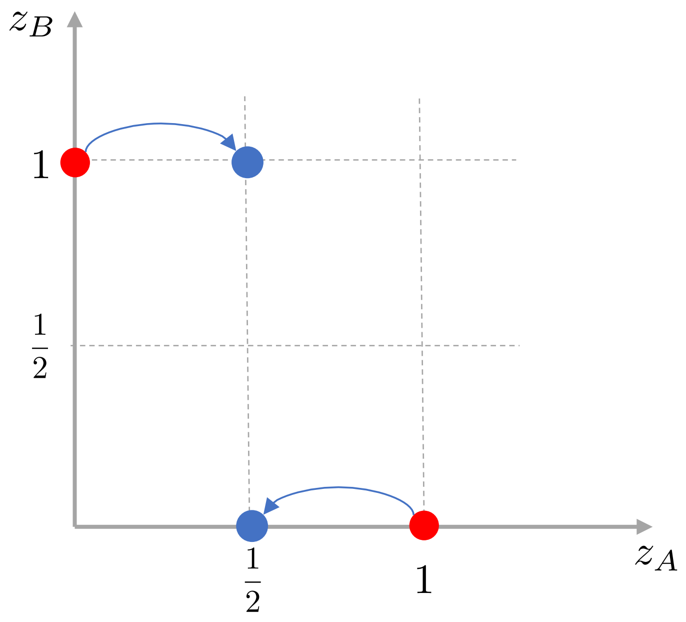
- Ideally
  - ⋆ Zero bias → Final point $(\frac{1}{2}, \frac{1}{2})$
- Naïve (wrong) protocol
  - ⋆ One horizontal transition
  - ⋆ One vertical transition
- Problem
  - ⋆ This transition is not valid
  - ⋆ For each line, coordinates of the center of mass can only increase



$$Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \geq U^{\dagger}_{A,i} E_{A,i} (Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}}) E_{A,i} U_{A,i}$$

Kitaev | TDPG | Naïve (wrong) protocol

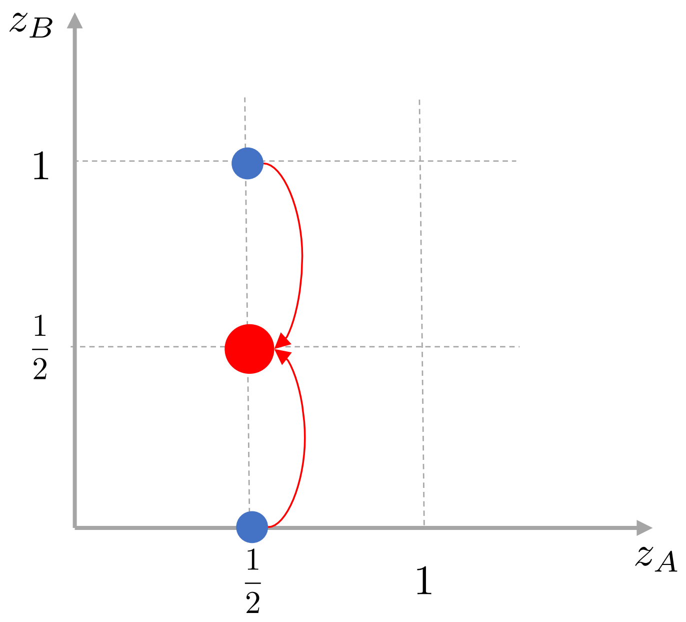
- Ideally
  - ⋆ Zero bias $\rightarrow$ Final point $(\frac{1}{2}, \frac{1}{2})$
- Naïve (wrong) protocol
  - ⋆ One horizontal transition
  - ⋆ One vertical transition
- Problem
  - ⋆ This transition is not valid
  - ⋆ For each line, coordinates of the center of mass can only increase



$$Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \geq U_{A,i}^{\dagger} E_{A,i} (Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}}) E_{A,i} U_{A,i}$$

Kitaev | TDPG | Naïve (wrong) protocol

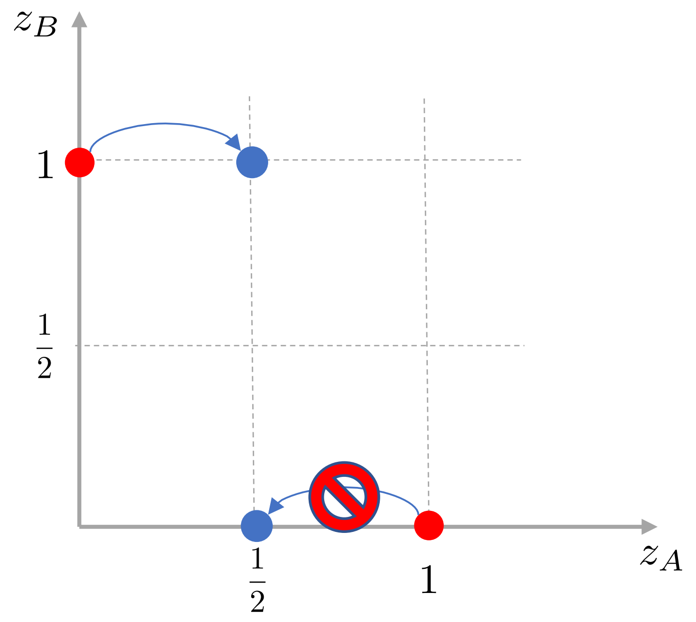
- Ideally
  - ⋆ Zero bias → Final point $(\frac{1}{2}, \frac{1}{2})$
- Naïve (wrong) protocol
  - ⋆ One horizontal transition
  - ⋆ One vertical transition
- Problem
  - ⋆ This transition is not valid
  - ⋆ For each line, coordinates of the center of mass can only increase



$$Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \geq U^{\dagger}_{A,i} E_{A,i} (Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}}) E_{A,i} U_{A,i}$$

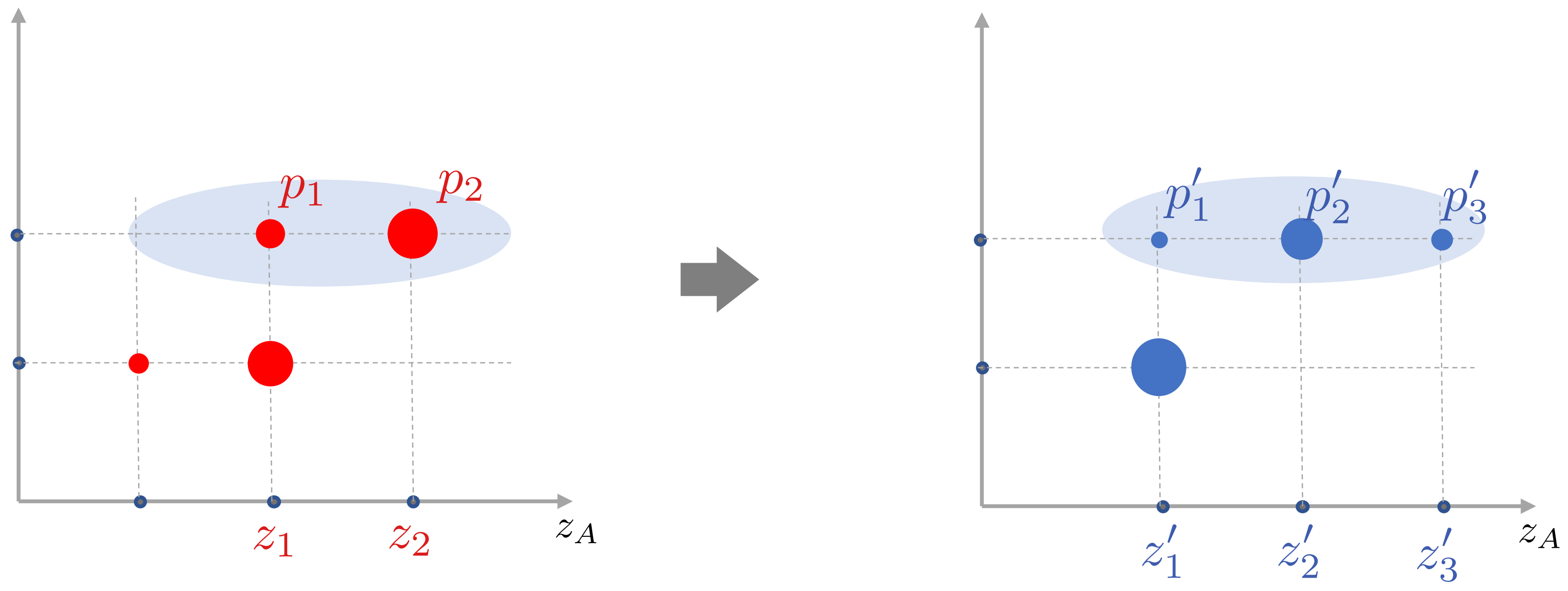
Kitaev | TDPG | Naïve (wrong) protocol

- Ideally
  - ⋆ Zero bias → Final point $(\frac{1}{2}, \frac{1}{2})$
- Naïve (wrong) protocol
  - ⋆ One horizontal transition
  - ⋆ One vertical transition
- Problem
  - ⋆ This transition is not valid
  - ⋆ For each line, coordinates of the center of mass can only increase



$$Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \geq U^{\dagger}_{A,i} E_{A,i} (Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}}) E_{A,i} U_{A,i}$$

Kitaev | TDPG | EBM transitions

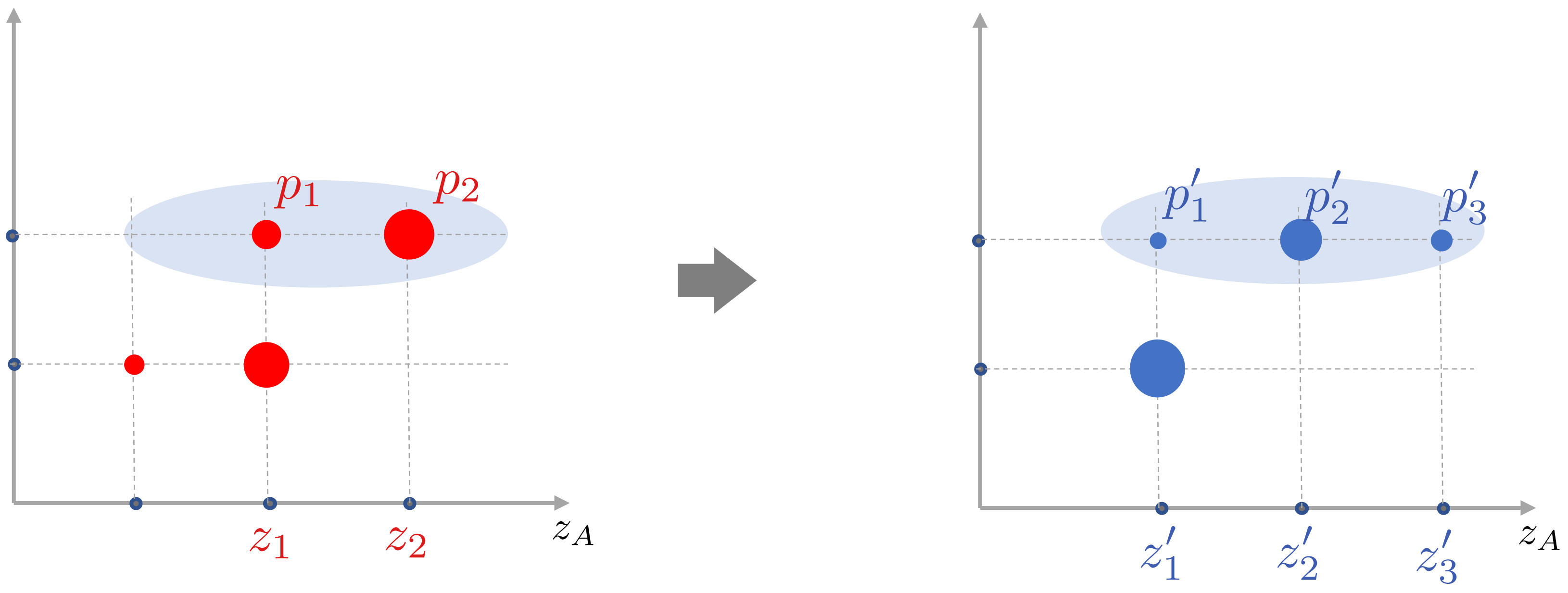


Validity condition: Expressible by matrices (EBM):

- There exists $\boldsymbol{G} \leq \boldsymbol{H}$ and $|\psi\rangle$ such that the transition can be written

$$\mathrm{Prob}[\boldsymbol{G}, |\psi\rangle] \mapsto \mathrm{Prob}[\boldsymbol{H}, |\psi\rangle]$$

Kitaev | TDPG | Valid transitions



Validity condition: Valid transition:

- For all $\boldsymbol{\lambda} \geq \mathbf{0}$

$$\sum_i p_i \frac{\lambda z_i}{\lambda + z_i} \leq \sum_i p'_i \frac{\lambda z'_i}{\lambda + z'_i}$$

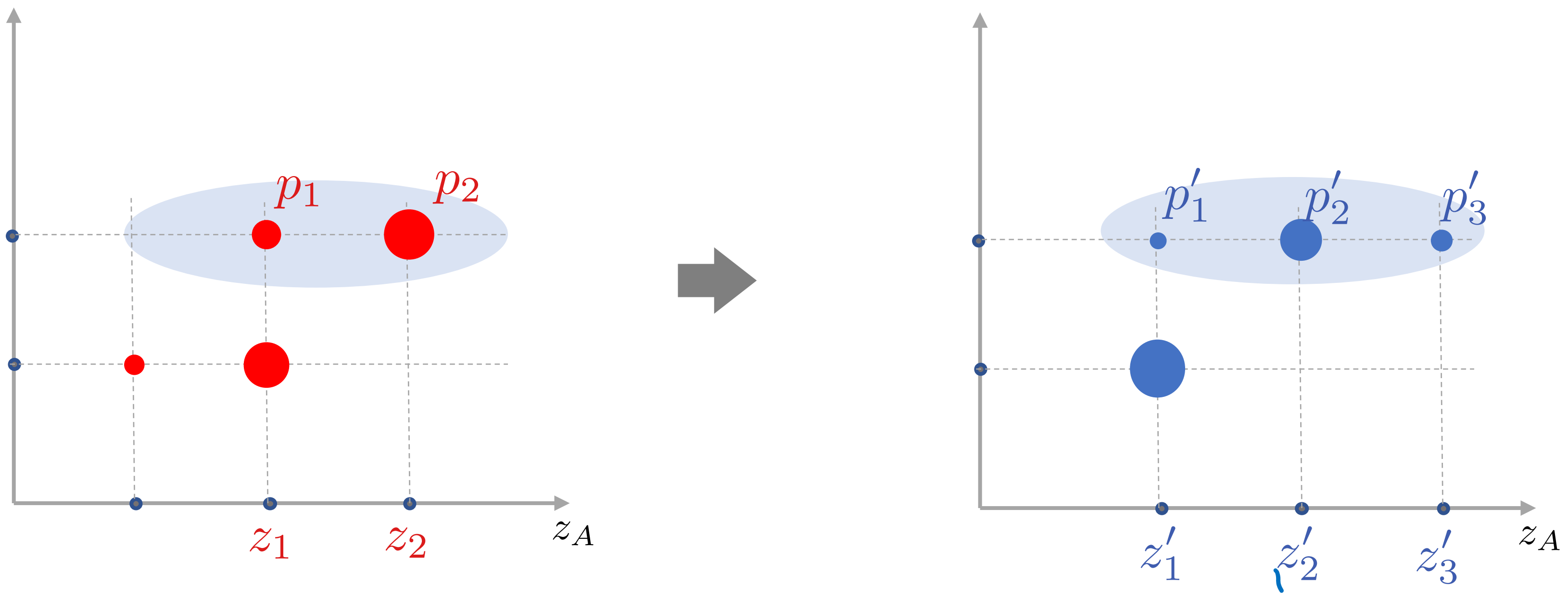
Kitaev | TDPG | EBM and valid transitions

(*) Expressible By Matrices (EBM)	Operator monotone function	Valid functions
$H \geq G, \lvert\psi\rangle$ s.t.	f s.t.	$\sum_{\text{final}} \frac{\lambda z}{\lambda+z} p_z \geq \sum_{\text{init}} \frac{\lambda z}{\lambda+z} p_z$
$\text{Prob}[G, \lvert\psi\rangle] \to \text{Prob}[H, \lvert\psi\rangle]$	$\forall\ H \geq G, f(H) \geq f(G)$	

K : cone of EBM $\overset{\text{Dual}}{\to}$ K^* : cone of Operator Monotones $\overset{\text{Dual}}{\to}$ K^{**} : cone of valid functions

Lemma: $K = K^{**}$

Kitaev | TDPG | Valid transitions



Validity condition: Valid transition:

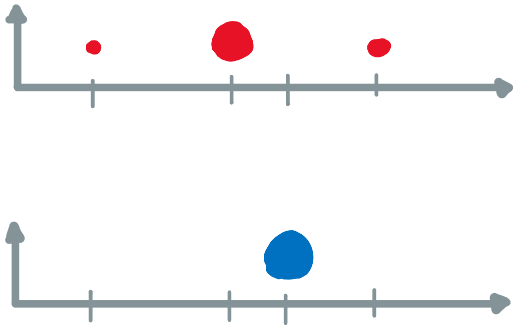
- For all $\boldsymbol{\lambda} \geq \mathbf{0}$

$$\sum_i p_i \frac{\lambda z_i}{\lambda + z_i} \leq \sum_i p_i' \frac{\lambda z_i'}{\lambda + z_i'}$$

Kitaev | TDPG | Basic transitions

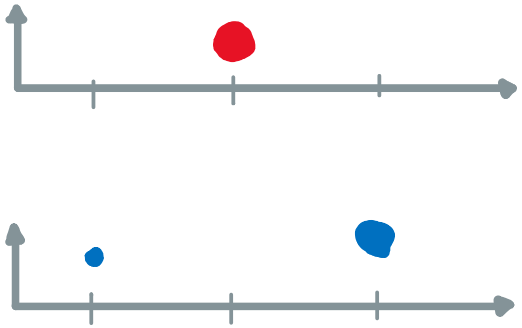
Merge ($n_g \to 1$):

$$\langle x_g \rangle \leq x_h$$



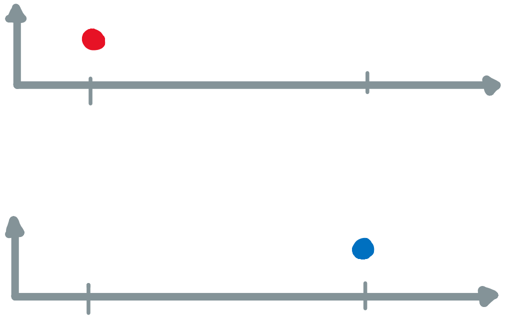
Split ($1 \to n_h$):

$$\frac{1}{x_g} \geq \left\langle \frac{1}{x_h} \right\rangle$$



Raise ($n_g = n_h \to n_h$):

$$x_{g_i} \leq x_{h_i}$$



Kitaev | TDPG | Example

Merge ($n_g \to 1$):

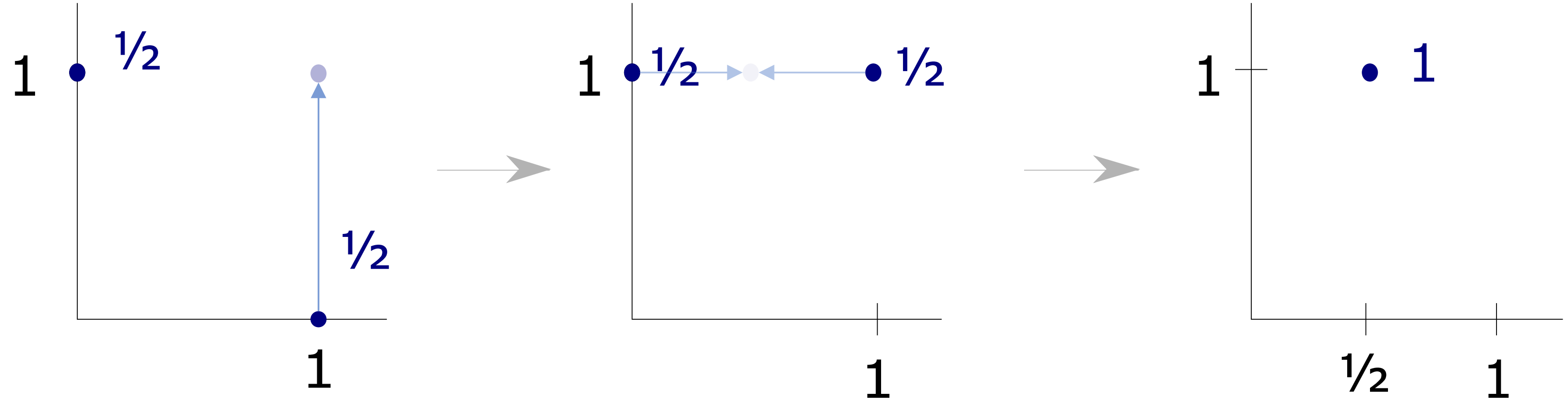
$$\langle x_g \rangle \leq x_h$$

Split ($1 \to n_h$):

$$\frac{1}{x_g} \geq \left\langle \frac{1}{x_h} \right\rangle$$

Raise ($n_g = n_h \to n_h$):

$$x_{g_i} \leq x_{h_i}$$



The flip and declare protocol!

Kitaev | TDPG | Example (2)

Merge ($n_g \to 1$):

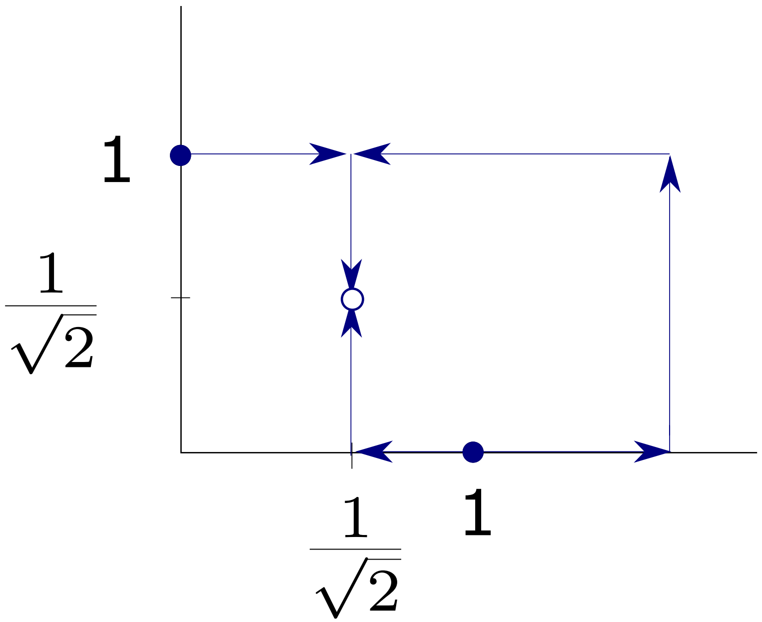
$$\langle x_g \rangle \leq x_h$$

Split ($1 \to n_h$):

$$\frac{1}{x_g} \geq \left\langle \frac{1}{x_h} \right\rangle$$

Raise ($n_g = n_h \to n_h$):

$$x_{g_i} \leq x_{h_i}$$



Spekkens Rudolph protocol (PRL, 2002)

Kitaev | TDPG | Example (3)

Merge ($n_g \to 1$):

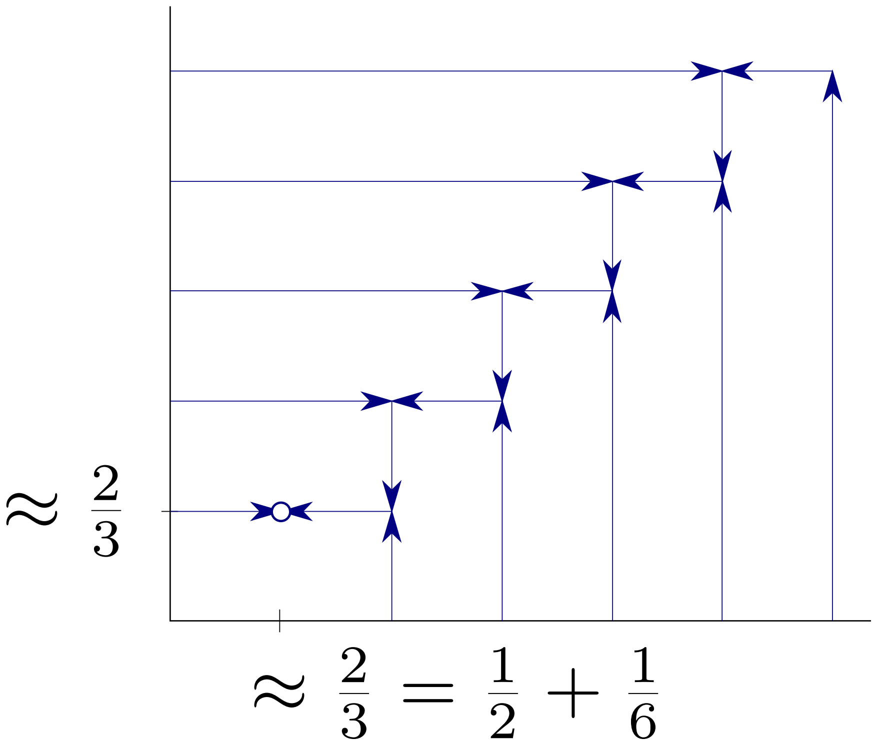
$$\langle x_g \rangle \leq x_h$$

Split ($1 \to n_h$):

$$\frac{1}{x_g} \geq \left\langle \frac{1}{x_h} \right\rangle$$

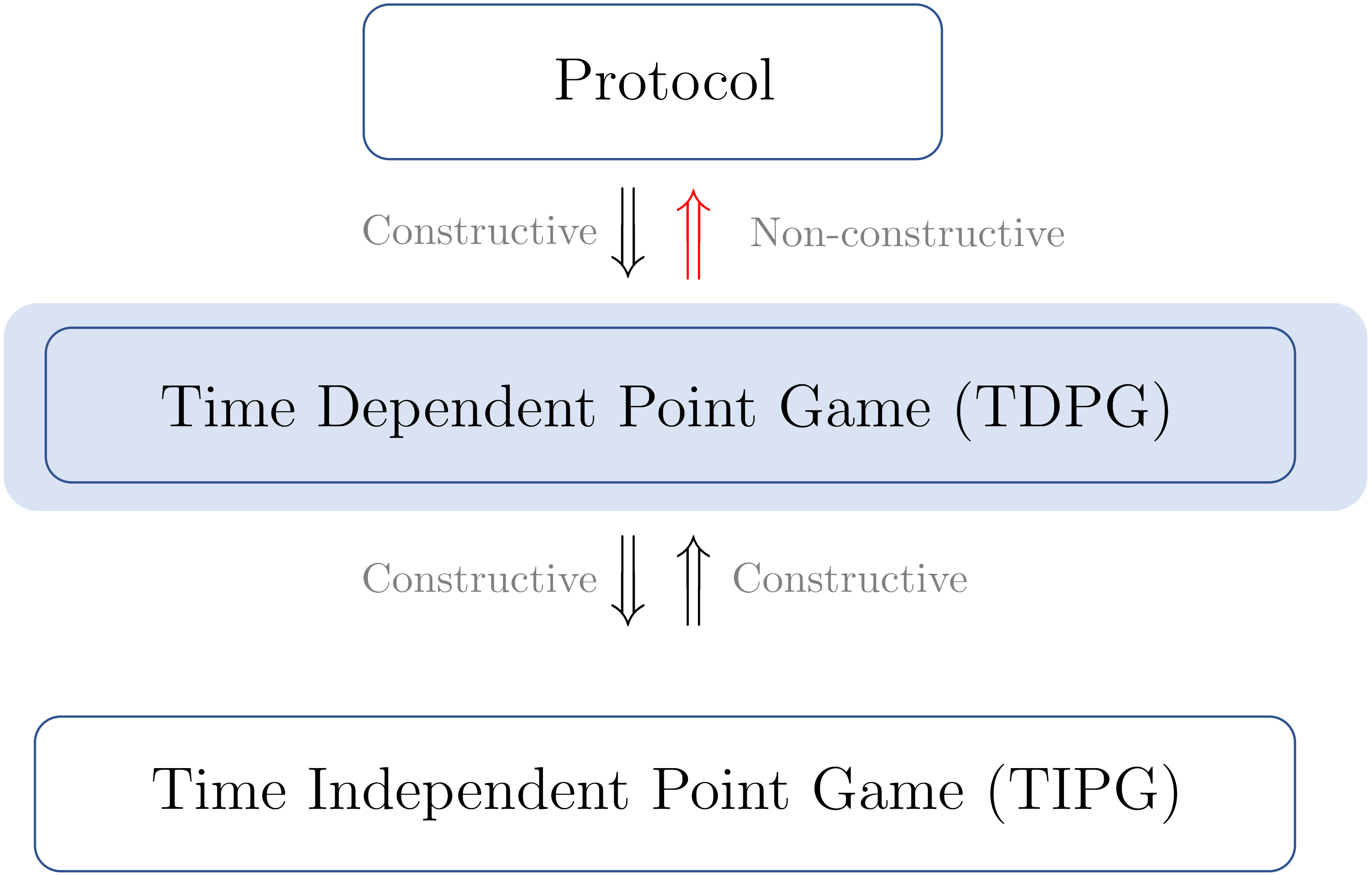
Raise ($n_g = n_h \to n_h$):

$$x_{g_i} \leq x_{h_i}$$



Best known explicit protocol:
Dip Dip Boom (Mochon, PRA 2005)

Kitaev | Three Equivalent Frameworks



Kitaev | TIPG

Time Independent Point Game (TIPG):

- Key idea: Allow negative weights
- $h(x, y), v(x, y)$ s.t.

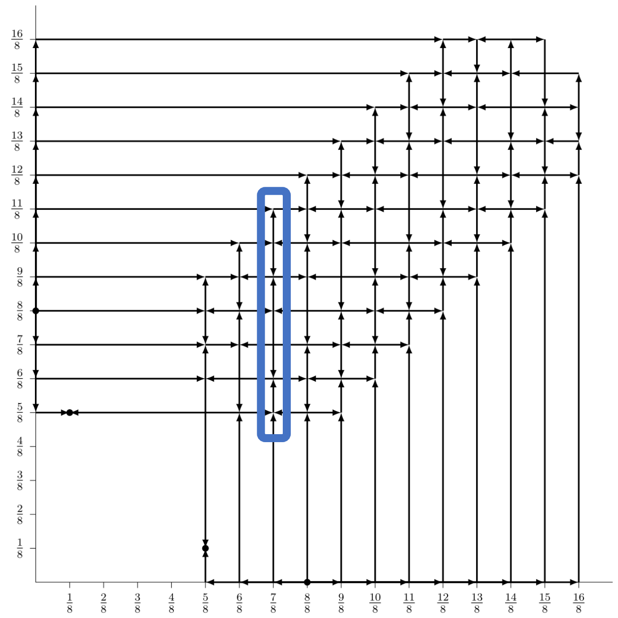
  $h + v =$ final frame - initial frame

  h, v satisfy a similar equation.

Mathemagic: For a valid TIPG there is TDPG with the same last frame.

Charm: Catalyst state.

Mochon | Near-perfect WCF is possible



- Mathemagic: Family of TIPGs that yield

$$\epsilon = \frac{1}{4k+2}$$

  where $2k$ = number of points involved in the non-trivial step.

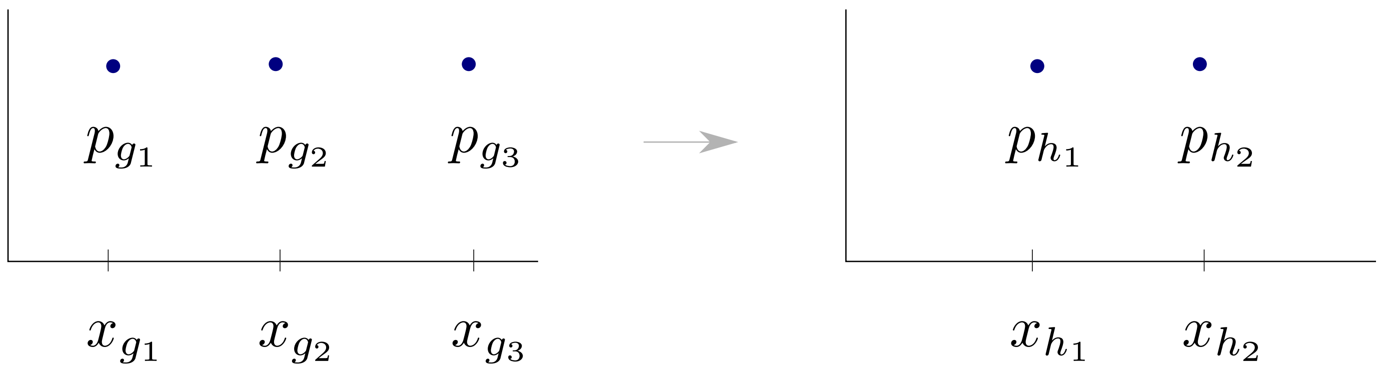
- $k = 1$ yields the Dip Dip Boom protocol ($\epsilon = 1/6$) protocol.
- Charm: Polynomials.

Image taken from E. Pelchat's Master Thesis

Contributions

TEF, Blinkered Unitaries, 1/10 explicit, Elliptic-Monotone-Align Algorithm

TEF



TDPG to Explicit protocol Framework (TEF):

A TDPG → Protocol if
for each consecutive frame of a TDPG one can construct a U s.t.

$$\sum x_{h_i} |h_i\rangle \langle h_i| - \sum x_{g_i} E_h U |g_i\rangle \langle g_i| U^\dagger E_h \geq 0$$

and

$$U(\underbrace{\sum \sqrt{p_{g_i}} |g_i\rangle}_{|v\rangle}) = \underbrace{\sum \sqrt{p_{h_i}} |h_i\rangle}_{|w\rangle}.$$

TEF | Blinkered Unitaries

For the Dip Dip Boom ($\epsilon = 1/6$) protocol, we need a U that implements

- Split: $1 \to n_h$
- Merge: $n_g \to 1$

Claim: $U_{\text{blink}} = |w\rangle\langle v| + |v\rangle\langle w| + \mathbb{I}_{\text{else}}$ can perform both.

Significance: Current best protocol from its point game directly.

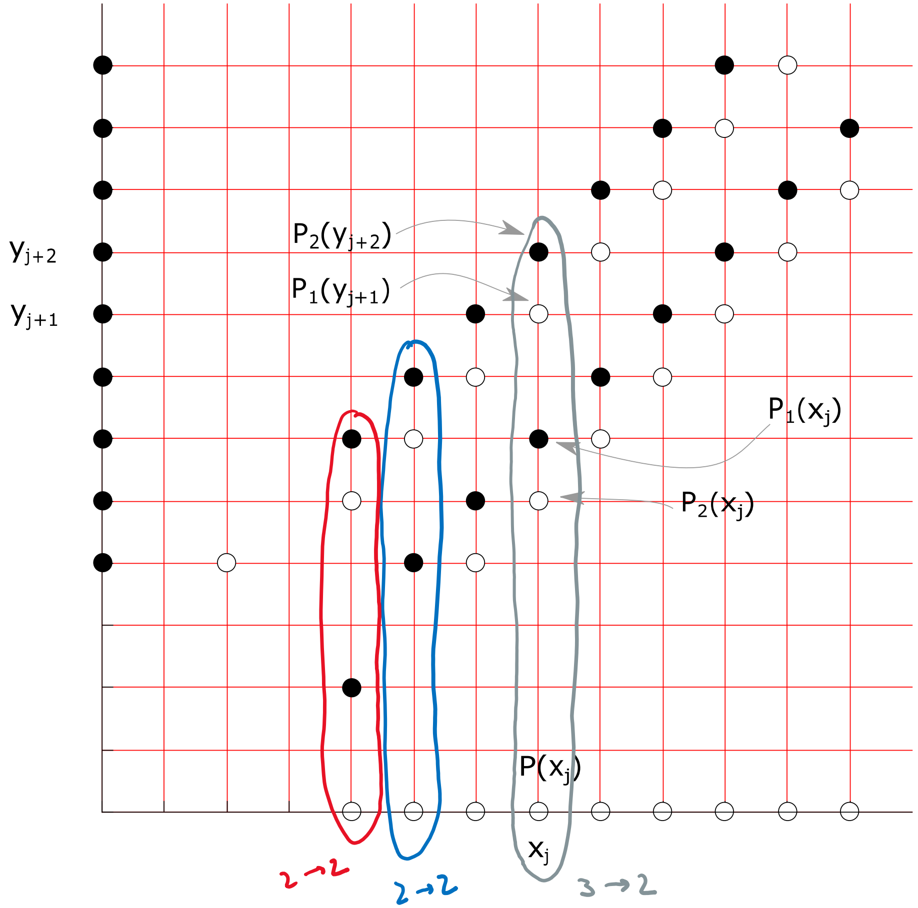
TEF | 1/10 Explicit

For initialising and the catalyst state we need

- Merge
- Split

and to climb down the ladder we need a special class

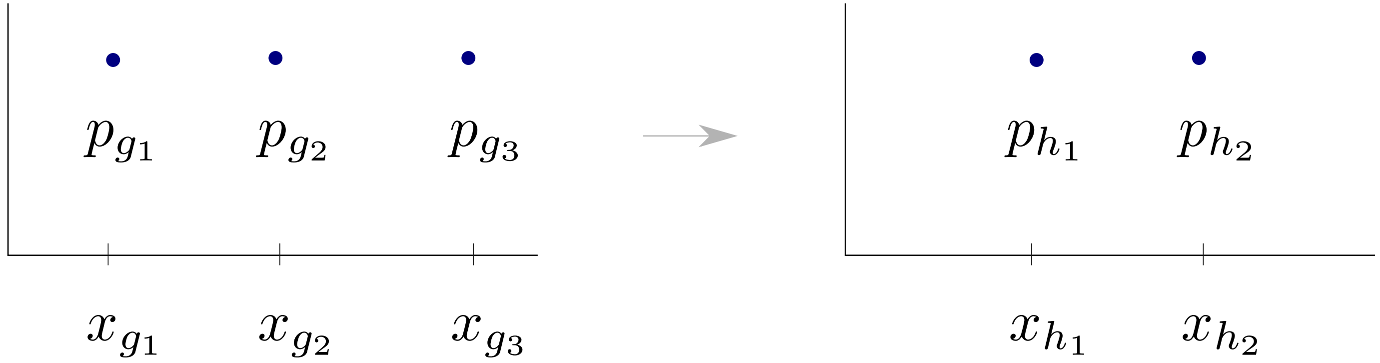
- $3 \to 2$
- $2 \to 2$.



$$U_{3\to 2} = |w_1\rangle\langle v_1| + (|v_2'\rangle + |w_2\rangle)\langle v_2'| + |v_0'\rangle\langle v_0'| + (|v_2'\rangle - |w_2\rangle)\langle w_2| + |v_1\rangle\langle w_1|$$

$$U_{2\to 2} = |w_1\rangle\langle v_1| + (\alpha|v_1\rangle + \beta|w_2\rangle)\langle v_2| + |v_1\rangle\langle w_1| + (\beta|v_1\rangle - \alpha|w_2\rangle)\langle w_2|$$

Elliptic Monotone Align (EMA) Algorithm



Find a U s.t.

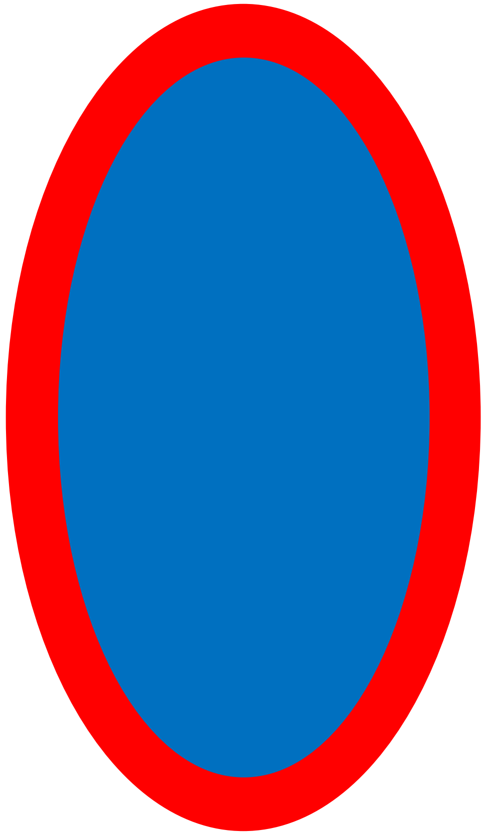
$$X_h \geq U X_g U^\dagger$$

and

$$U |v\rangle = |w\rangle$$

where $X_h = \mathrm{diag}(x_{h_1}, x_{h_2} \dots)$, $|w\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \dots)^T$.
X_g and $|v\rangle$ are similarly defined.

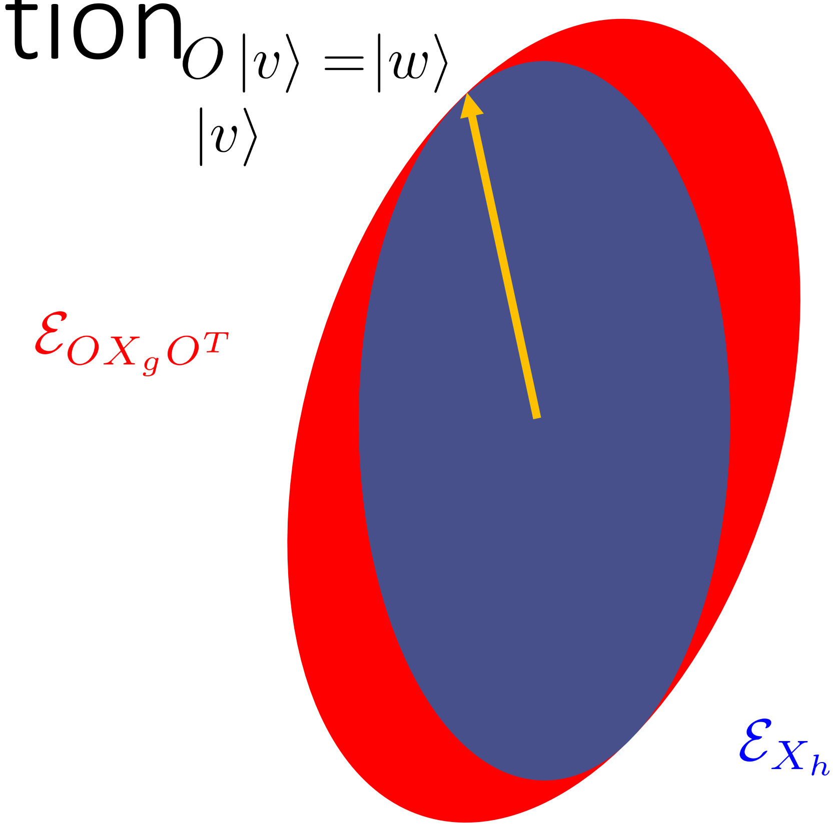
EMA | Elliptic Representation



- Restrict to reals: $U \to O$.
- For X diagonal
$$\mathcal{E}_X = \{|u\rangle \mid \langle u| X |u\rangle = 1\}$$
is $\vec{u}$ which satisfy $\sum x_i u_i^2 = 1$, viz. an ellipsoid.
- Generalises to all $X > 0$.
- $\underbrace{X_h}_{H} \geq \underbrace{O X_g O^T}_{G}$ means $\mathcal{E}_H$ is contained in $\mathcal{E}_G$ (containment is reversed).

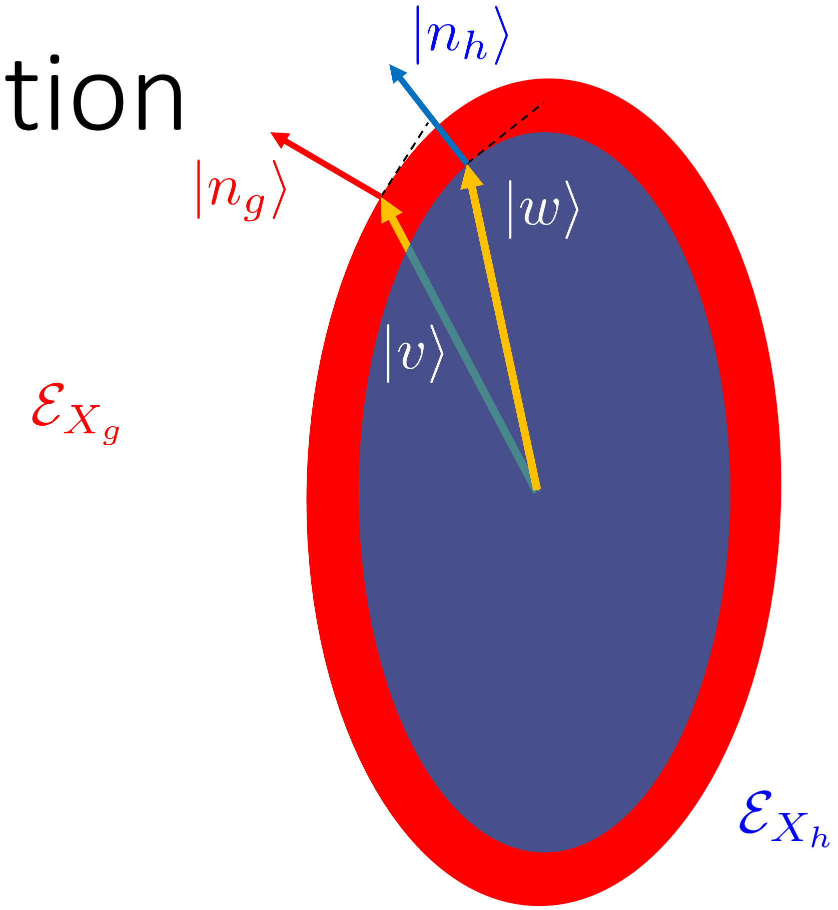
EMA | Elliptic Representation

- Imagine: Solution O is known, viz.
  - $O\,|v\rangle = |w\rangle\,.$
  - $X_h \geq OX_gO^T.$
- Suppose: Point of contact is $|w\rangle$.
- Observation:
  - $O\,|n_g\rangle = |n_h\rangle.$
  - Inner ellipsoid more curved.



EMA | Elliptic Representation

- Imagine: Solution O is known, viz.
  - $O|v\rangle = |w\rangle$.
  - $X_h \geq OX_gO^T$.
- Suppose: Point of contact is $|w\rangle$.
- Observation:
  - $O|n_g\rangle = |n_h\rangle$.
  - Inner ellipsoid more curved.



EMA | Elliptic Monotone-Align Algorithm

- EBRM=EBM
- Elliptic Representation
- Weingarten Maps
  (to evaluate curvatures)

Given a k dimension problem:

- Tighten;
- Normals must coincide at the point of contact;
- The inner ellipsoid must be more curved
  than the outer ellipsoid,

which yields a $k-1$ dimension problem.

Apply iteratively and combine to get U.

Significance: Explicit protocol for Weak CF with $\epsilon \to 0$.

Conclusion

Summary

- Framework for finding protocols from point games.
    - Split and Merge, basic moves in these games, exactly converted to unitaries
        - Bias 1/6 protocol
        - Catalyst State
    - Bias 1/10 protocol moves exactly determined
- Elliptic Monotone Align (EMA) Algorithm.
    - A systematic way of finding unitaries for any valid move
    - Protocol for WCF with $\varepsilon \to 0$.

Summary

Classically: $\epsilon = \frac{1}{2}$ viz. at least one player can always cheat and win.

Quantumly:

	Bound	**Best protocol known**
Strong CF	$\epsilon \geq \frac{1}{\sqrt{2}} - \frac{1}{2}$ [Kitaev 03]	$\epsilon = \frac{1}{4}$ [Ambainis 01]
Weak CF	$\epsilon \to 0$ [Mochon 07] [Aharonov et al 16]	$\epsilon \to \frac{1}{6}$ [Mochon 05] $\epsilon \to \frac{1}{10}$ (analytic) $\epsilon \to 0$ (algorithmic)

Outlook

- *Resources*. Compile the 1/10 game into a neater protocol
- *Structure*. Relation between Mochon’s polynomial assignment and the EMA solution
- *Simpler*. Study the Pelchat-Høyer point games and its moves
- *Robust*. Account for noise in the unitaries
  - EMA will run with finite precision; quantify its effect on the bias
- *Bounds*. Prove lower bounds on number of points needed for achieving a certain bias

arXiv:1811.02984

Thank you

The work was funded by EU H2020, FRIA, FNRS; FNRS grant QUICTIME; FNRS grant QuantAlgo.

Resource Requirements

COROLLARY 4.6. *Assume there exists a TIPG with a valid horizontal function* $h = h^+ - h^-$ *and a valid vertical function* $v = v^+ - v^-$ *such that* $h + v = 1[\beta, \alpha] - \frac{1}{2}[0,1] - \frac{1}{2}[1,0]$. *Let* Γ *be the largest coordinate of all the points that appear in the TIPG game. Then, for all* $\varepsilon > 0$, *we can construct a point game with* $O(\frac{\|h\|\Gamma^2}{\varepsilon^2})$ *valid transitions and final point* $[\beta + \varepsilon, \alpha + \varepsilon]$.

5. Construction of a TIPG achieving bias $\boldsymbol{\varepsilon}$**.** In this section we construct for every $\varepsilon > 0$ a game with final point $[1/2 + \varepsilon, 1/2 + \varepsilon]$. Moreover, the number of qubits used in the protocol will be $O(\log \frac{1}{\varepsilon})$ and the number of rounds $(\frac{1}{\varepsilon})^{O(\frac{1}{\varepsilon})}$.

DORIT AHARONOV†, ANDRÉ CHAILLOUX‡, MAOR GANZ†, IORDANIS KERENIDIS§, AND LOÏCK MAGNIN†