Quantum Weak Coin Flipping

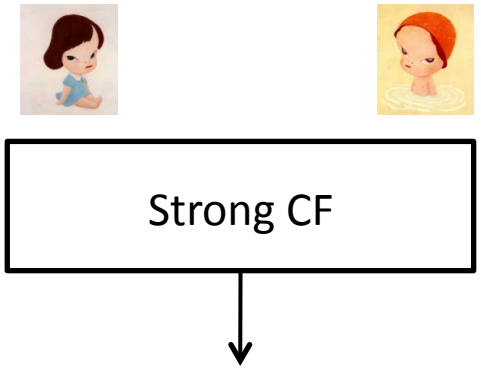
Iordanis Kerenidis
CNRS – Univ Paris Diderot

joint work with: D. Aharonov, A. Chailloux, M. Ganz, L. Magnin,

Secure Computation

- Alice and Bob need to perform a joint operation
  - Identification, Private Information Retrieval, Secure function evaluation
- Goal: protocols with limited cheating possibilities
- Basic cryptographic primitives
  - Bit Commitment, Oblivious Transfer
  - Coin Flipping [Blum81]
    - Alice and Bob need to flip a random coin.
    - No dishonest party should be able to bias the coin

Strong vs Weak Coin Flipping

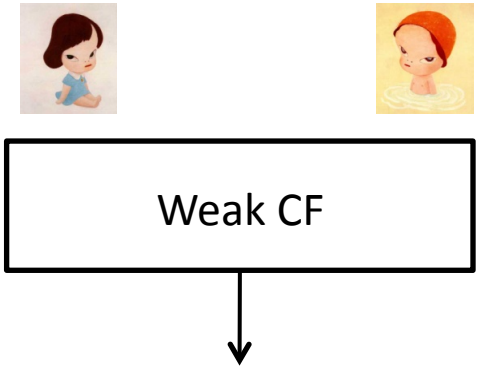


$c \in_R \{0,1\}$

$$P_A^* = \max_{ch.Alice}\{\max\{\Pr[c=0],\Pr[c=1]\}\}$$

$$P_B^* = \max_{ch.Bob}\{\max\{\Pr[c=0],\Pr[c=1]\}\}$$

$$P^* = \max\{P_A^*, P_B^*\}$$



0: Alice wins / 1: Bob wins

$$P_A^* = \max_{ch.Alice}\{\Pr[c=0]\}$$

$$P_B^* = \max_{ch.Bob}\{\Pr[c=1]\}$$

$$P^* = \max\{P_A^*, P_B^*\}$$

Security Conditions

- Computational Security
  - cheating players are computationally bounded (hardness of factoring, Discrete Logarithm)
  - We can achieve any $P^* \approx 1/2$
- Information Theoretic Security
  - Cheating players have unlimited power
  - We can achieve nothing, i.e. $P^* = 1$
- How about quantum protocols?

Quantum Coin Flipping

- Perfect coin flipping is impossible, i.e. $P^* > 1/2$

- Better than classical protocols exist

  (classically always $P^* = 1$)

  For Quantum Strong Coin Flipping

  - $P^* \leq 91\%$ [Aharonov, Ta-Shma, Vazirani, Yao STOC '00]
  - $P^* \geq \frac{1}{\sqrt{2}}$ [Kitaev '03] $P^* \leq \frac{1}{\sqrt{2}} + \varepsilon, \ \forall \varepsilon > 0$ [Chailloux, K. '09]

  For Quantum Weak Coin Flipping

  - Formalism through point games [Kitaev]
  - $P^* = \frac{1}{2} + \varepsilon, \ \forall \varepsilon > 0$ [Mochon '07]

Why care about coin flipping

- Weak coin flipping is one of the few possible crypto primitives
  - There is life beyond QKD
- Beautiful techniques for lower bounds and constructions
- Weak Coin Flipping: Master Primitive
  - Optimal weak coin implies optimal strong coin [Chailloux, K. '09]
  - Optimal weak coin implies optimal bit commitment [Chailloux, K. '11]
- Quantum mechanics from an information point of view
  - Why quantum mechanics allows for these imperfect cryptographic primitives?

Status of weak coin flipping result

- Mochon's paper appeared in 2007
  - Proof of existence, but no simple protocol description
  - Very long (80p) and technical
  - Not peer reviewed

- Initial Goals (back in 2010):
  - Verify the proof
  - Simplify the proof
  - Understand the proof
  - Find a simple protocol

Status of weak coin flipping result

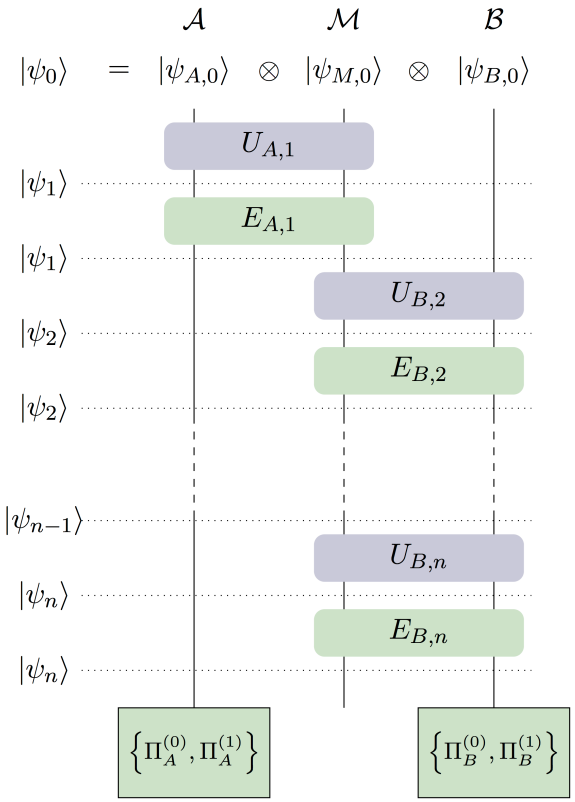
- Mochon's paper appeared in 2007
  - Proof of existence, but no simple protocol description
  - Very long (80p) and technical
  - Not peer reviewed.

- Results (four years later):
  - Verify the proof — YES
  - Simplify the proof — A lot (40p)
  - Understand the proof — A bit
  - Find a simple protocol — Not at all!

- It's only the beginning!

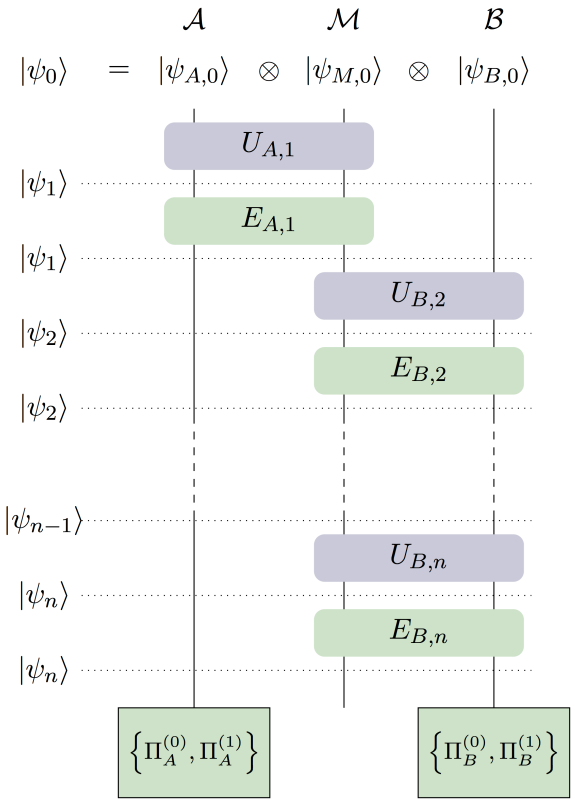
Roadmap

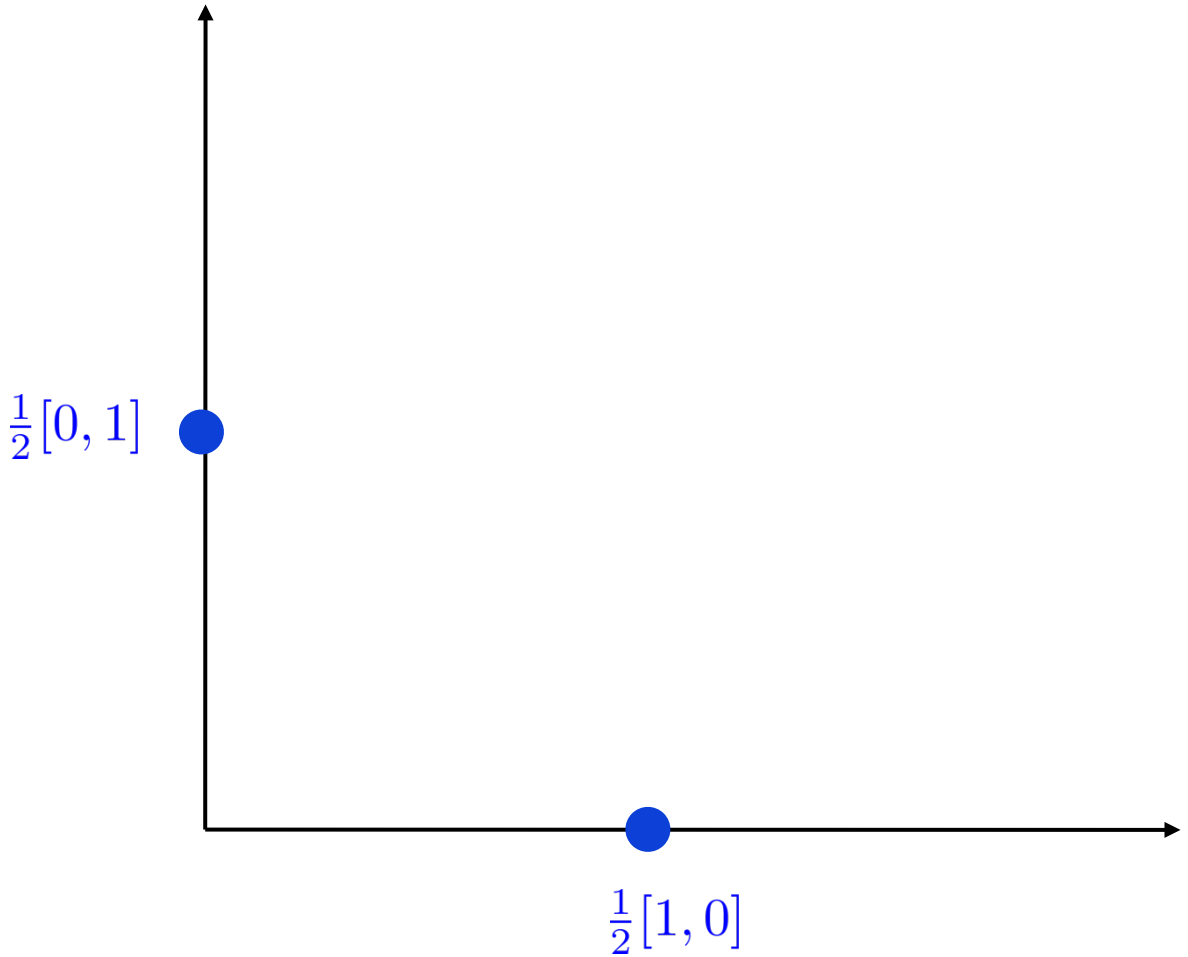
1. Equivalence of protocols and point games



Roadmap

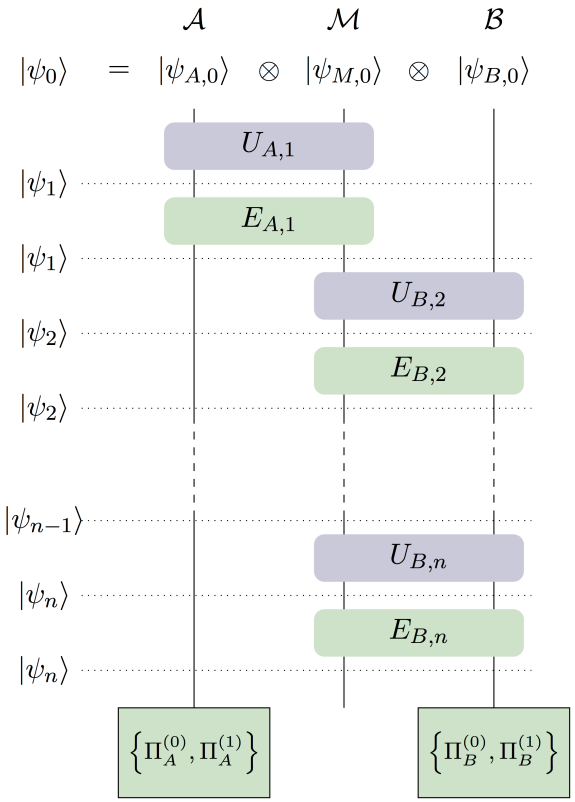
1. Equivalence of protocols and point games

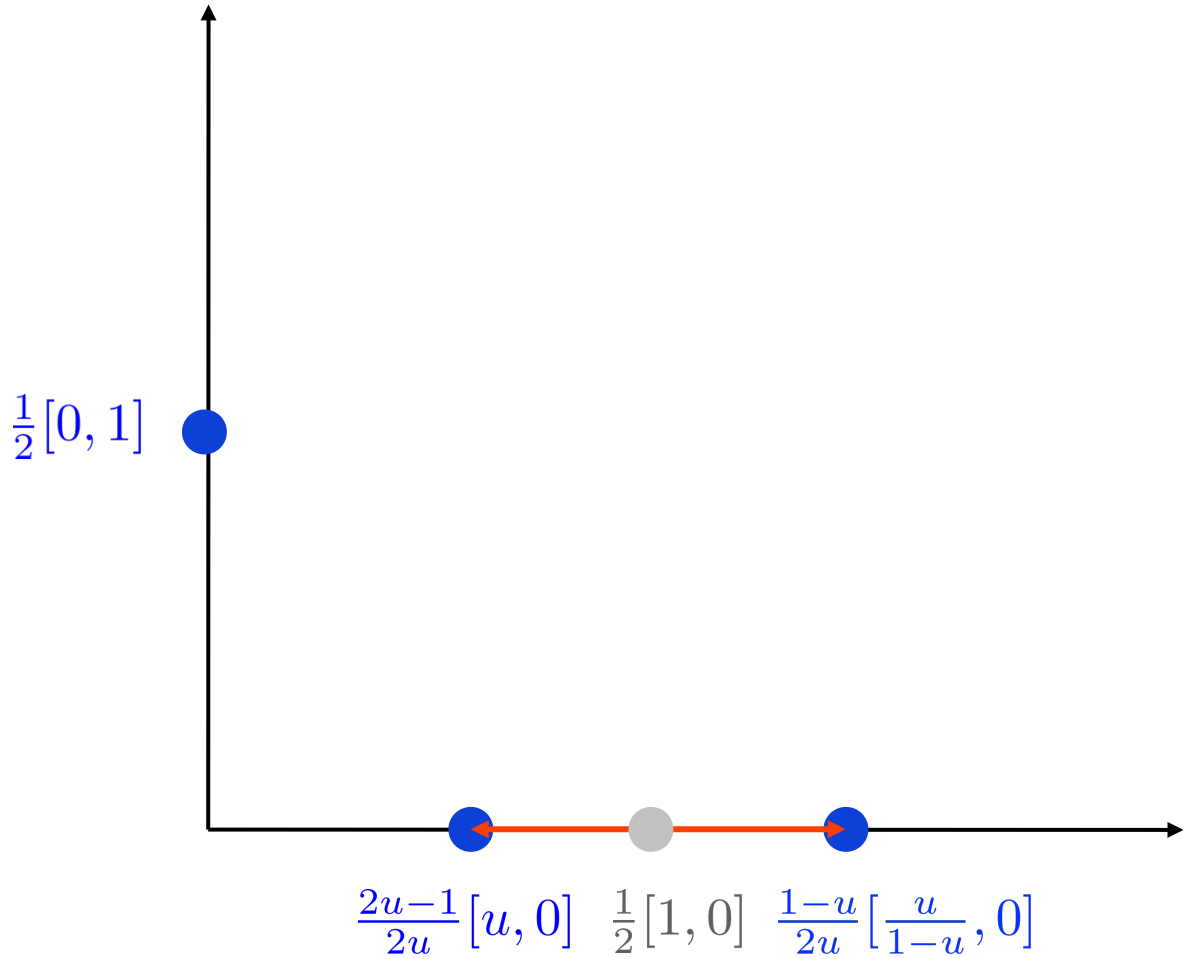




Roadmap

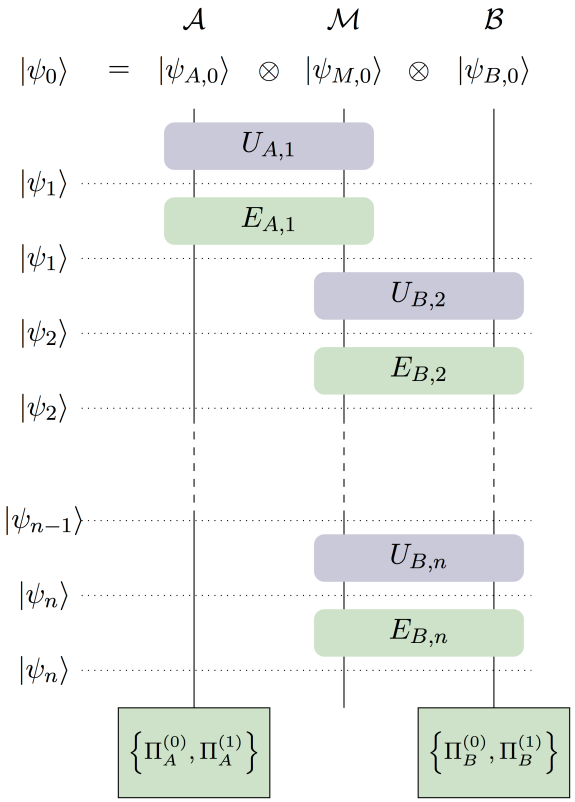
1. Equivalence of protocols and point games

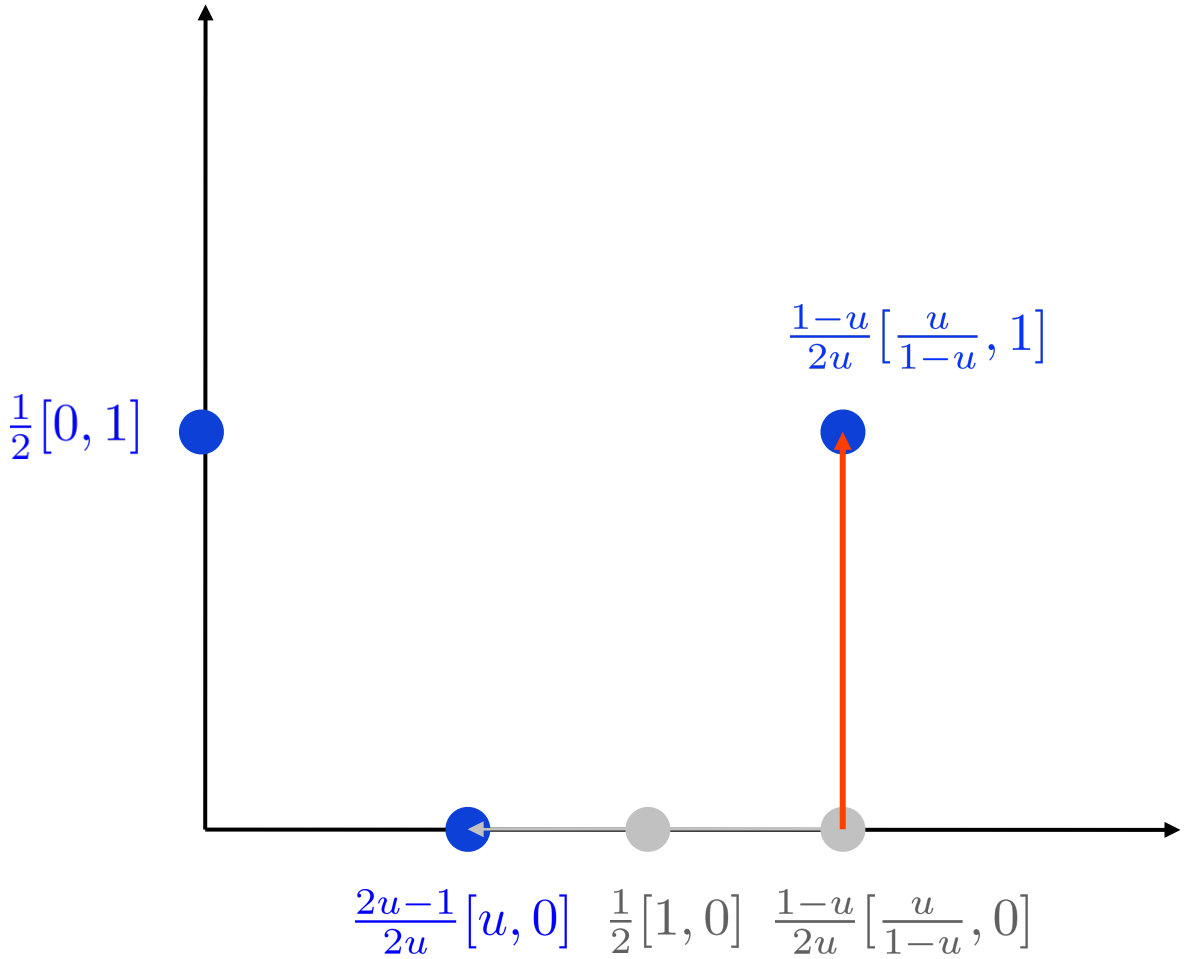




Roadmap

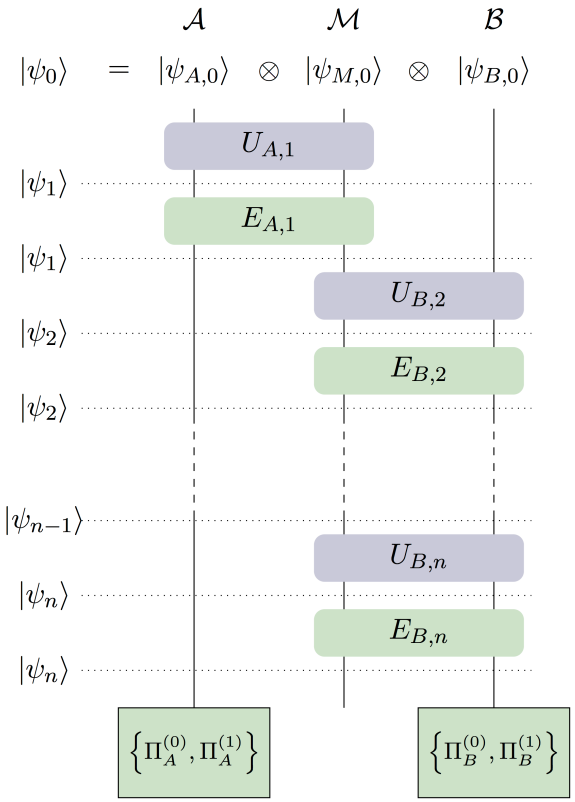
1. Equivalence of protocols and point games

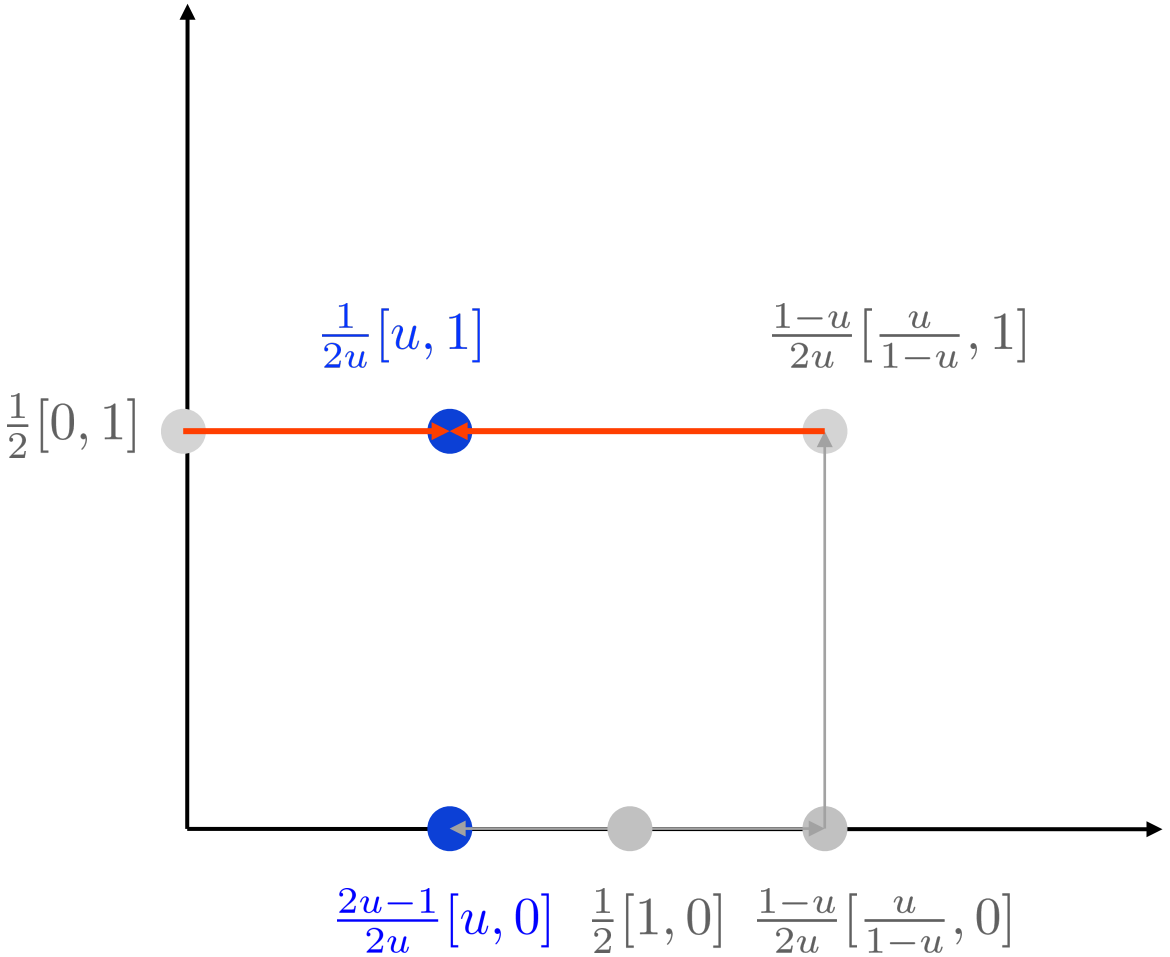




Roadmap

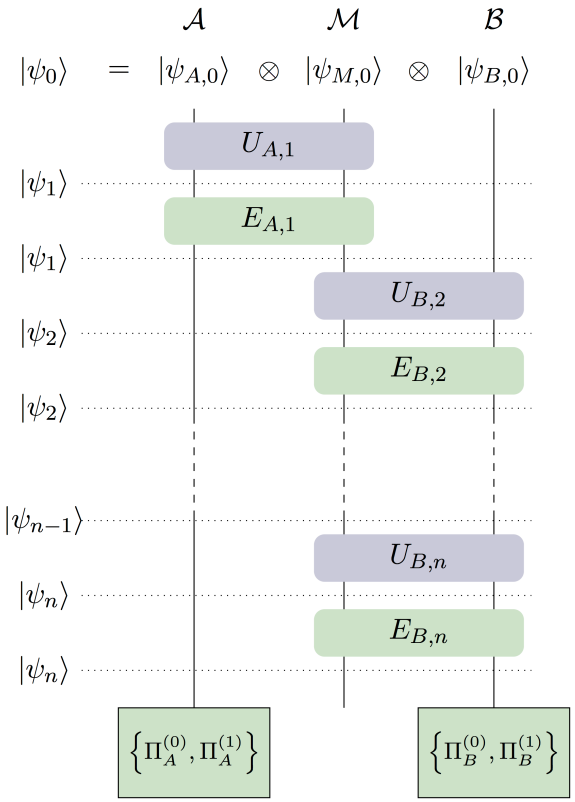
1. Equivalence of protocols and point games

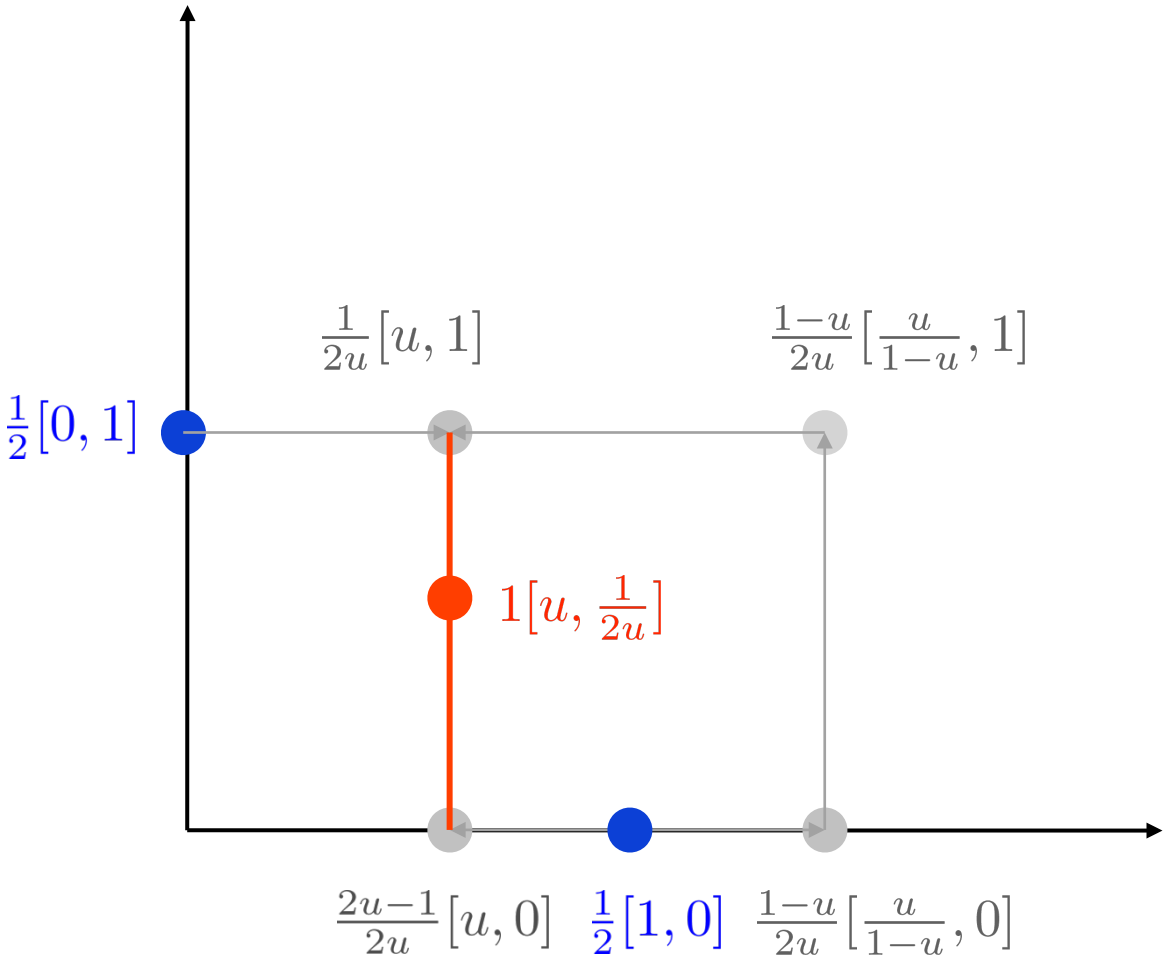




Roadmap

1. Equivalence of protocols and point games





Roadmap

1. Equivalence of protocols and point games

Some tools

- Protocols and cheating strategies
- Semi-definite programs and SDP duality
- Topology of infinite dimensional convex cones
- operator monotone functions
- duality of convex cones
- catalyst points

Beautiful techniques, not yet well understood, waiting to be used! [Kitaev, Mochon]

2. Point game with final point $[1/2+\varepsilon,1/2+\varepsilon]$ [Mochon]

Proof outline

1. Equivalence of different models

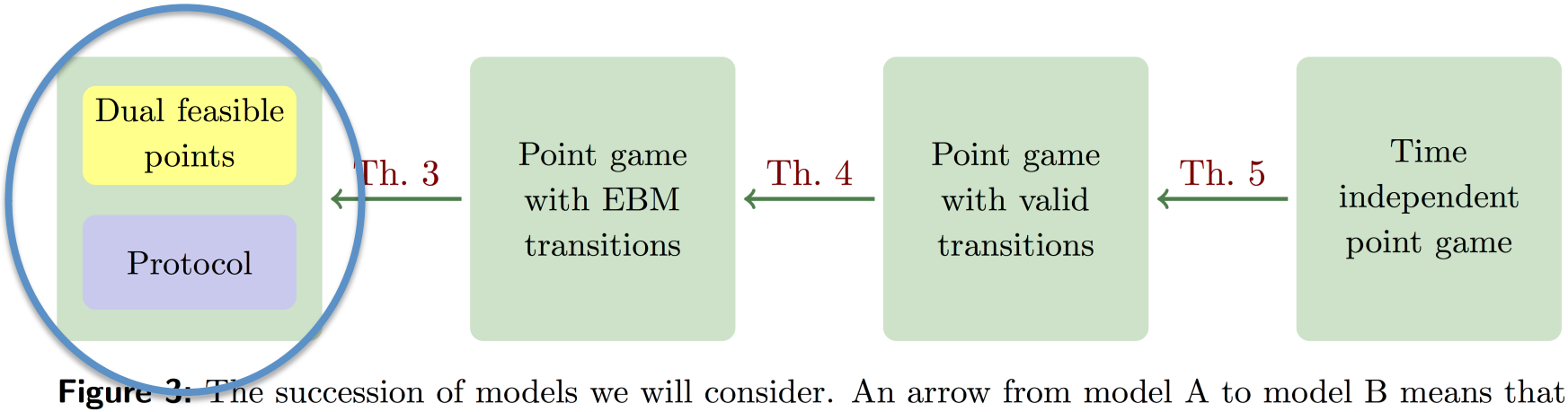


Figure 3: The succession of models we will consider. An arrow from model A to model B means that proving the existence of an ε biased protocol in A implies the existence of an $\varepsilon + \varepsilon'$ biased protocol in B (for all $\varepsilon' > 0$).

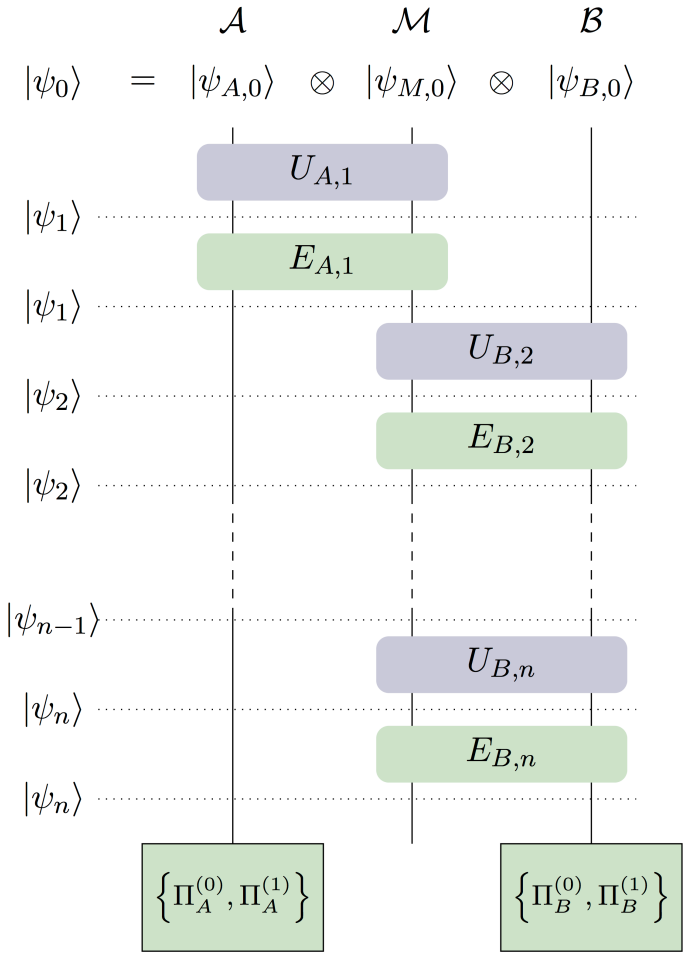
2. Existence of a Time independent point game with final point [1/2+ε,1/2+ε]

Protocol

- Three spaces: A, M, B
- Initial state $|\psi_0\rangle$
- Round i
  - Honest states $|\psi_i\rangle$
  - Unitary $U_{A,i}$ / $U_{B,i}$
  - Projection $E_{A,i}$ / $E_{B,i}$
- Final Projections

$$\langle\psi_n|\Pi_A^{(0)}\otimes I\otimes\Pi_B^{(0)}|\psi_n\rangle = 1/2$$

$$\langle\psi_n|\Pi_A^{(1)}\otimes I\otimes\Pi_B^{(1)}|\psi_n\rangle = 1/2$$

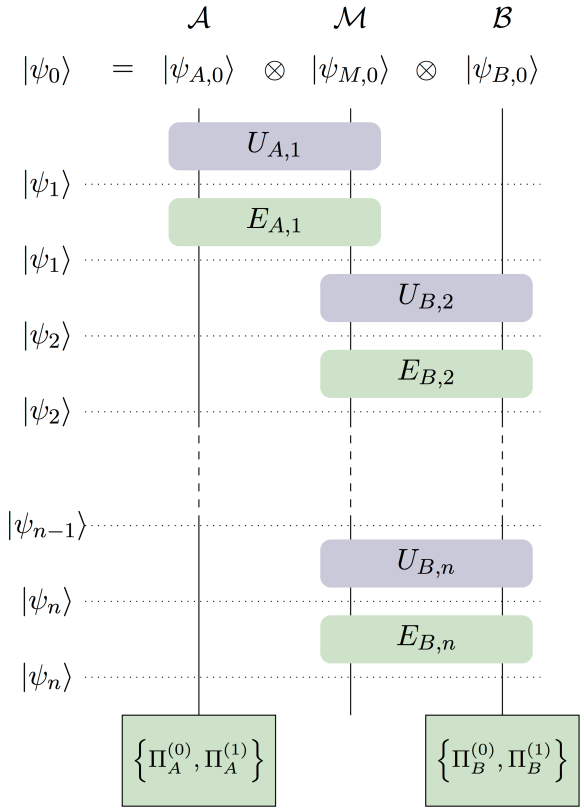


Cheating Probabilities as SDPs

Theorem 1 (Primal)

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

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



Cheating Probabilities as SDPs

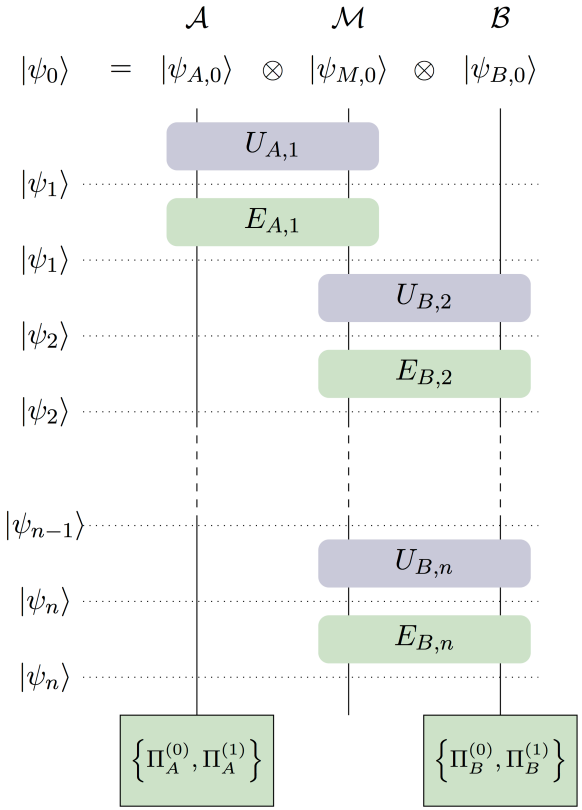
Theorem 1 (Primal)

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

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

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

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



Problem: : it's a maximization so we need to go over all protocols

The dual SDPs

Theorem 1 (Primal)

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

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

Theorem 2 (Dual)

$P_B^* = \min \mathrm{Tr}(Z_{A,0}|\psi_{A,0}\rangle\langle\psi_{A,0}|)$ *over all* $Z_{A,i}$ *under the constraints:*

① $\forall i,\ Z_{A,i} \succeq 0$;

② *for* i *odd,* $Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \succeq U_{A,i}^\dagger E_{A,i}(Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}})E_{A,i}U_{A,i}$;

③ *for* i *even,* $Z_{A,i-1} = Z_{A,i}$;

④ $Z_{A,n} = \Pi_A^{(1)}$.

⑤ $Z_{A,0}|\psi_{A,0}\rangle = \beta|\psi_{A,0}\rangle$ i.e. $|\psi_{A,0}\rangle$ is an eigenvector of $Z_{A,0}$ with eigenvalue $\beta > 0$,

Dual Feasible Points as security witness

Dual feasible point: $\{Z_{A,i}\},\{Z_{B,i}\}$ that are a solution to the dual SDP

Given a dual feasible point, we can bound the cheating probabilities!

$$P_B^* \le \langle\psi_0| Z_{A,0} \otimes I_M \otimes I_B |\psi_0\rangle$$

$$P_A^* \le \langle\psi_0| I_A \otimes I_M \otimes Z_{B,0} |\psi_0\rangle$$

Problem: To write the dual, we need to know the protocol (unitaries and projections)!

Theorem 2 (Dual)

$P_B^* = \min \mathrm{Tr}(Z_{A,0}|\psi_{A,0}\rangle\langle\psi_{A,0}|)$ *over all* $Z_{A,i}$ *under the constraints:*

① $\forall i,\ Z_{A,i} \succeq 0;$

② *for* i *odd,* $Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \succeq U_{A,i}^\dagger E_{A,i}(Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}})E_{A,i}U_{A,i};$

③ *for* i *even,* $Z_{A,i-1} = Z_{A,i};$

④ $Z_{A,n} = \Pi_A^{(1)}.$

⑤ $Z_{A,0}|\psi_{A,0}\rangle = \beta|\psi_{A,0}\rangle$ i.e. $|\psi_{A,0}\rangle$ is an eigenvector of $Z_{A,0}$ with eigenvalue $\beta > 0,$

Roadmap

1. Equivalence of different models

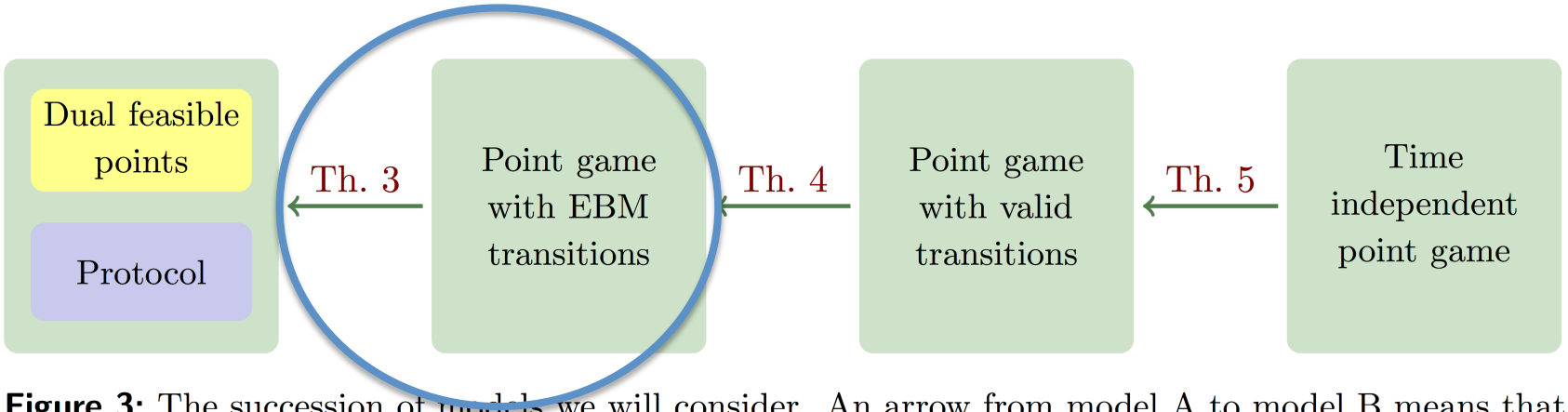


Figure 3: The succession of models we will consider. An arrow from model A to model B means that proving the existence of an ε biased protocol in A implies the existence of an $\varepsilon + \varepsilon'$ biased protocol in B (for all $\varepsilon' > 0$).

2. Existence of a Time independent point game

EBM games

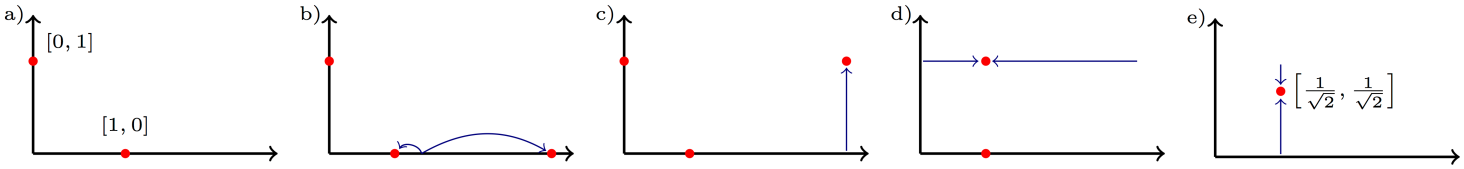


Figure 2: A "simple" point game for the [SR02] protocol with bias $1/\sqrt{2} - 1/2$. The game starts with the uniform distribution over two points. The first transition, between a) and b), is a horizontal transition as the point on the x-axis is split into two points. The second transition, between b) and c) is a vertical transition as one point is raised vertically. The last two transitions are two merges, respectively horizontally and vertically. We omitted the weights of the points in the distributions to simplify the drawings.

Definition: A sequence of n distributions $\{p_0 \to p_1 \to \ldots \to p_n\}$ on points in 2d st.

- Initial condition: $p_0 = 1/2[1,0] + 1/2[0,1]$
- Final condition: $p_n = [\beta, \alpha]$ ($P_B^* \le \beta, P_A^* \le \alpha$)
- ...

1. What do the points and the weights represent?
2. What are the legal transitions between distributions?

EBM games: points and weights

Points and weights: from the dual feasible point and the honest states

$$\{Z_{A,i}\},\{Z_{B,i}\} \qquad P_B^* \le \langle\psi_0|Z_{A,0}\otimes I_M\otimes I_B|\psi_0\rangle = \beta \qquad P_A^* \le \langle\psi_0|I_A\otimes I_M\otimes Z_{B,0}|\psi_0\rangle = \alpha$$

The magic quantity $\langle\psi_i|Z_{A,i}\otimes I_M\otimes Z_{B,i}|\psi_i\rangle$

- we need to combine both "cheating" together
- Note $\langle\psi_o|Z_{A,0}\otimes I_M\otimes Z_{B,0}|\psi_0\rangle \ge P_A^*\cdot P_B^*$
- Same as in Kitaev's Strong Coin Flipping lower bound!

Points: $[z_{A,i},z_{B,i}]$, where $z_{A,i},z_{B,i}$ are eigenvalues of the PSD $Z_{A,i},Z_{B,i}$ resp.

Weights: the projection of the honest state onto the corresponding eigenspace

$$\langle\psi_i|\Pi^{[z_{A,i}]}\otimes I_M\otimes\Pi^{[z_{B,i}]}|\psi_i\rangle$$

EBM games

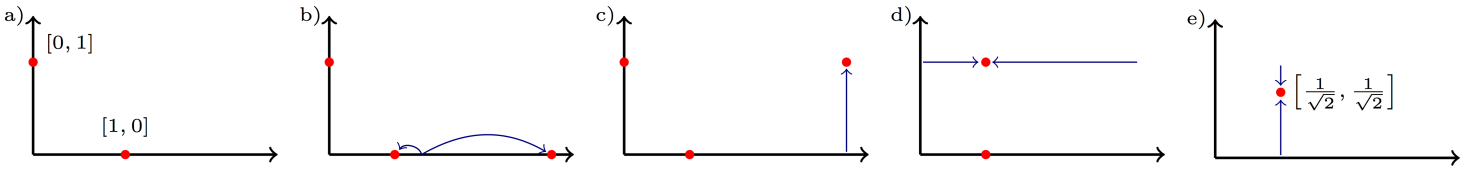


Figure 2: A "simple" point game for the [SR02] protocol with bias $1/\sqrt{2} - 1/2$. The game starts with the uniform distribution over two points. The first transition, between a) and b), is a horizontal transition as the point on the x-axis is split into two points. The second transition, between b) and c) is a vertical transition as one point is raised vertically. The last two transitions are two merges, respectively horizontally and vertically. We omitted the weights of the points in the distributions to simplify the drawings.

1. What do the points and the weights represent? ✓

2. What are the legal transitions between distributions?
   - At every round, either Alice or Bob apply a unitary.
     For i even, $Z_{A,i-1} = Z_{A,i}$ hence, points move horizontally or vertically but not both ways.
   - The Zs fulfill some SDP constraints $Z_{A,i-1} \otimes I_M \succ U_{A,i}^{\perp} E_{A,i} (Z_{A,i} \otimes I_M) E_{A,i} U_{A,i}$

EBM games

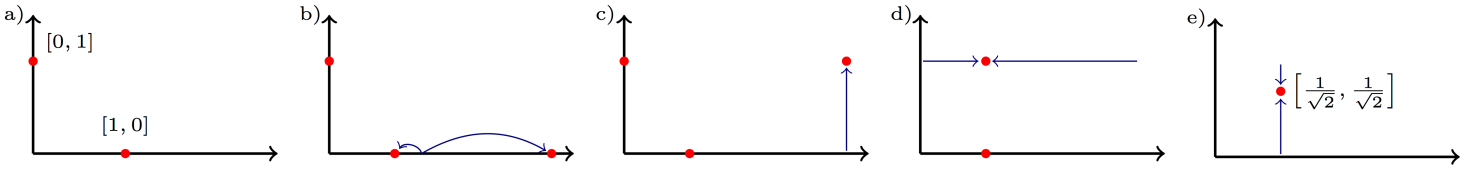


Figure 2: A "simple" point game for the [SR02] protocol with bias $1/\sqrt{2} - 1/2$. The game starts with the uniform distribution over two points. The first transition, between a) and b), is a horizontal transition as the point on the x-axis is split into two points. The second transition, between b) and c) is a vertical transition as one point is raised vertically. The last two transitions are two merges, respectively horizontally and vertically. We omitted the weights of the points in the distributions to simplify the drawings.

Definition: A sequence of n distributions $\{p_0 \to p_1 \to \ldots \to p_n\}$ on points in 2d st.

- Initial condition: $p_0 = 1/2[1,0] + 1/2[0,1]$
- Final condition: $p_n = [\beta, \alpha]$ $\quad (P_B^* \le \beta, P_A^* \le \alpha)$
- for all i: either points move horizontally or vertically
- Let $\{p_i \to p_{i+1}\}$ where points move only horizontally. Then for each height h, we have that

$$p_i = \sum_x \langle\psi|\Pi^{[x]}|\psi\rangle[x,h] \quad p_{i+1} = \sum_y \langle\psi|\Pi^{[y]}|\psi\rangle[y,h]$$

for some $X = \sum_x x\Pi^{[x]}$, $Y = \sum_y y\Pi^{[y]}$, $|\psi\rangle$ and $0 \prec X \prec Y$

Equivalence: X,Y are roughly Z_i, Z_{i-1}, states are the honest states, U's change eigenbases of X and Y

Problem: Hard to find or verify EBM transitions!

Proof outline

1. Equivalence of different models

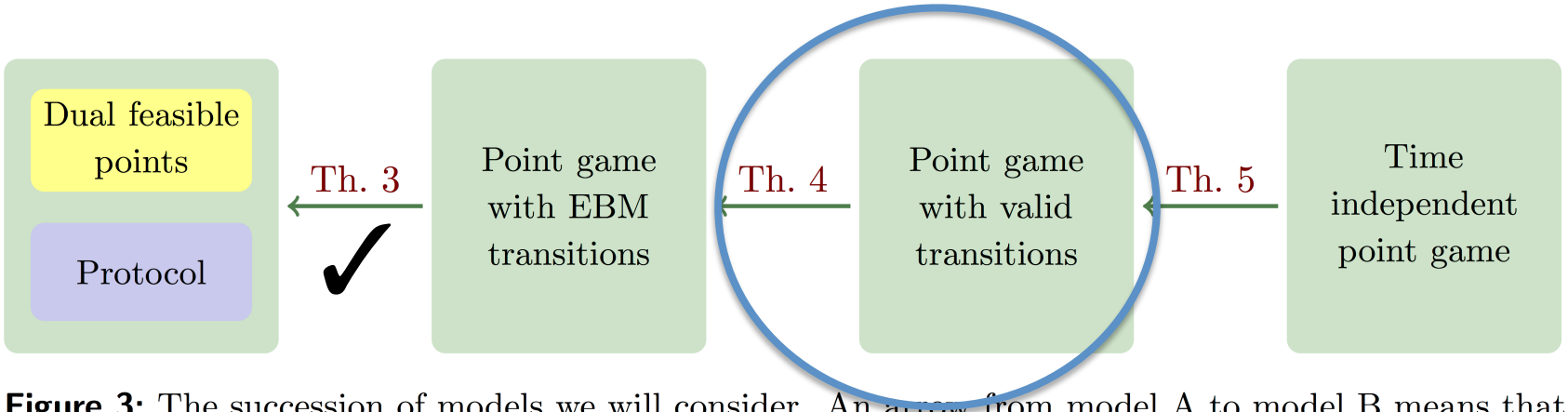


Figure 3: The succession of models we will consider. An arrow from model A to model B means that proving the existence of an ε biased protocol in A implies the existence of an $\varepsilon + \varepsilon'$ biased protocol in B (for all $\varepsilon' > 0$).

2. Existence of a Time independent point game

EBM, operator monotone, valid functions

EBM functions (equivalent to EBM transitions)

$\{p_0 \to p_1 \to \ldots \to p_n\}$ to $\{h_1,\ldots,h_n\}$ where $h = h^+ - h^-$ and $h^- \to h^+$ is EBM

Our space: The set of functions $h_i : [0,\infty] \to R$ with finite support, which is an infinite dimensional normed vector space (Kronecker basis and l_1 norm)

K = set of EBM functions

- convex cone. Fantastic!
- not closed. Hmmm!
- infinite dimensional. S@#%!

Simple but powerful idea: Express K by its bidual

Duals, duals of duals, ...

K = set of EBM functions

- convex cone, not closed, infinite dimensional

K^* = (dual of K) = set of operator monotone functions

- A function $f:[0,\infty)\to R$ is operator monotone if $X \prec Y \Rightarrow f(X) \prec f(Y)$
- [Bhatia]: An operator monotone function can be written as

$$f(t) = c_0 + c_1 t + \int_0^\infty \frac{\lambda t}{\lambda + t} dw(\lambda), \text{ for a measure w satisfying } \int_0^\infty \frac{\lambda}{\lambda + 1} dw(\lambda) < \infty$$

K^{**}= (dual of K^*) = set of valid functions

- A function h is valid if for any operator monotone function f, $\sum_x f(x)h(x) \geq 0$
- A function h is valid if:

  i) $\sum_x h(x) = 0$ ii) $\sum_x xh(x) \geq 0$ iii) $\forall \lambda > 0, \sum_x \frac{\lambda x}{\lambda + x} h(x) \geq 0$

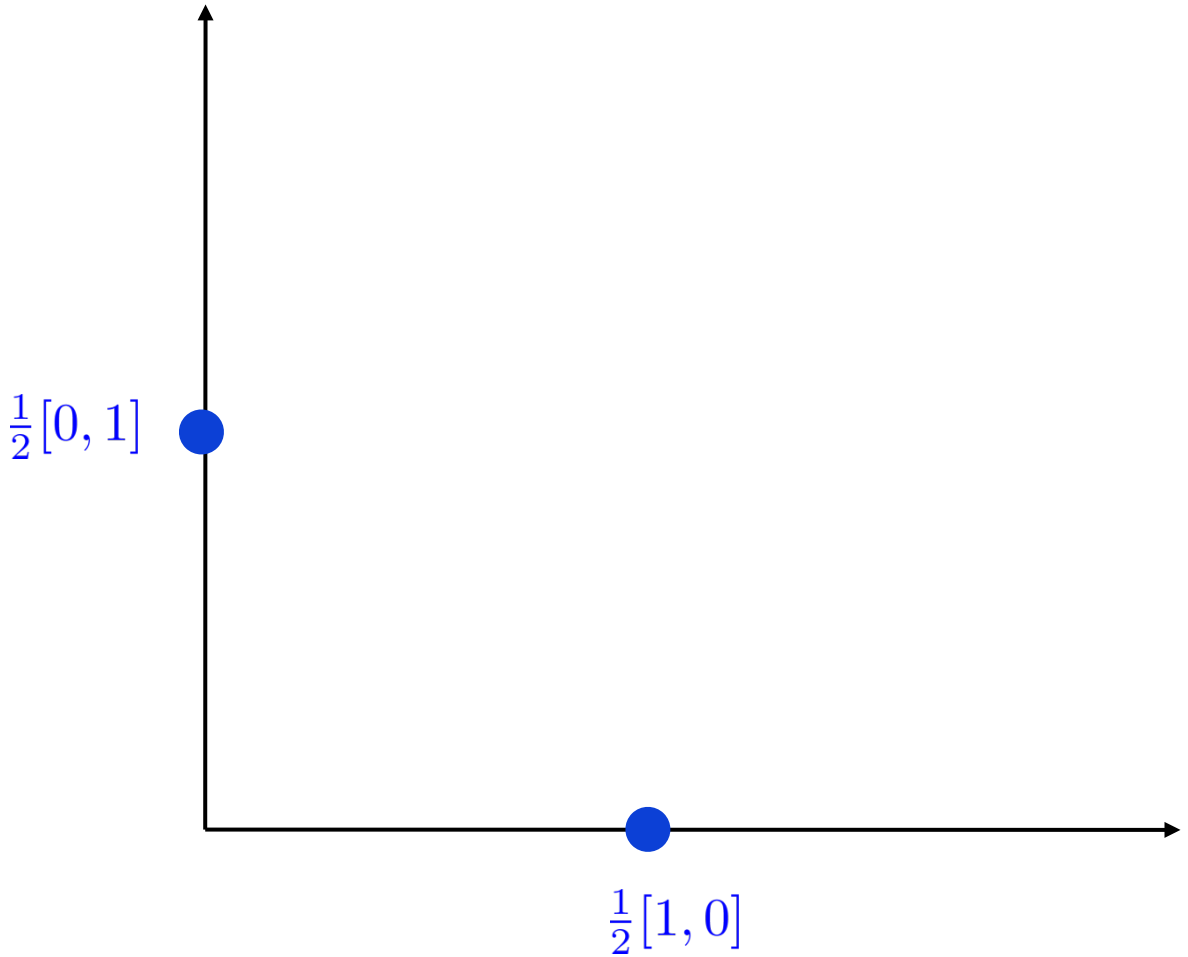
1. But K^{**} is equal to K up to closures, so valid functions "are" EBM functions
2. Valid functions have an easy characterisation!

Examples of valid functions

Definition: A function h is valid if $\sum_x h(x) = 0$ $\sum_x xh(x) \geq 0$ $\forall \lambda > 0, \sum_x \frac{\lambda x}{\lambda + x} h(x) \geq 0$

Examples

- Raise
- Merge
- Split



Examples of valid transitions

Definition: A function h is valid if $\sum_x h(x) = 0 \quad \sum_x xh(x) \geq 0 \quad \forall \lambda > 0, \sum_x \frac{\lambda x}{\lambda + x} h(x) \geq 0$

Examples

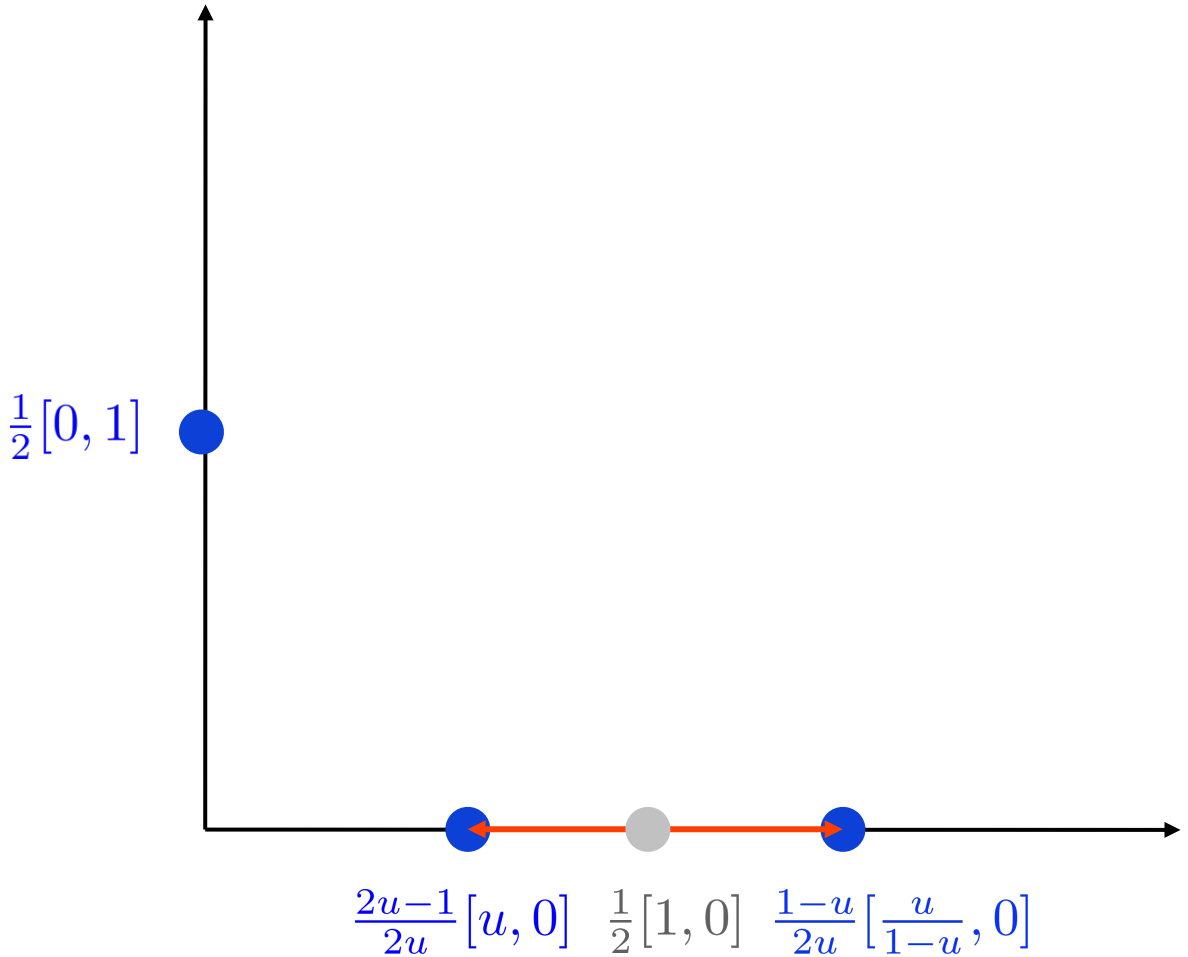
- Raise

- Merge

- Split

$(w_1 + w_2)[x] \rightarrow w_1[x_1] + w_2[x_2],$

$\frac{w_1 + w_2}{x} \geq \frac{w_1}{x_1} + \frac{w_2}{x_2}$



Examples of valid transitions

Definition: A function h is valid if $\sum_x h(x) = 0 \quad \sum_x xh(x) \geq 0 \quad \forall \lambda > 0, \sum_x \frac{\lambda x}{\lambda + x} h(x) \geq 0$

Examples

- Raise

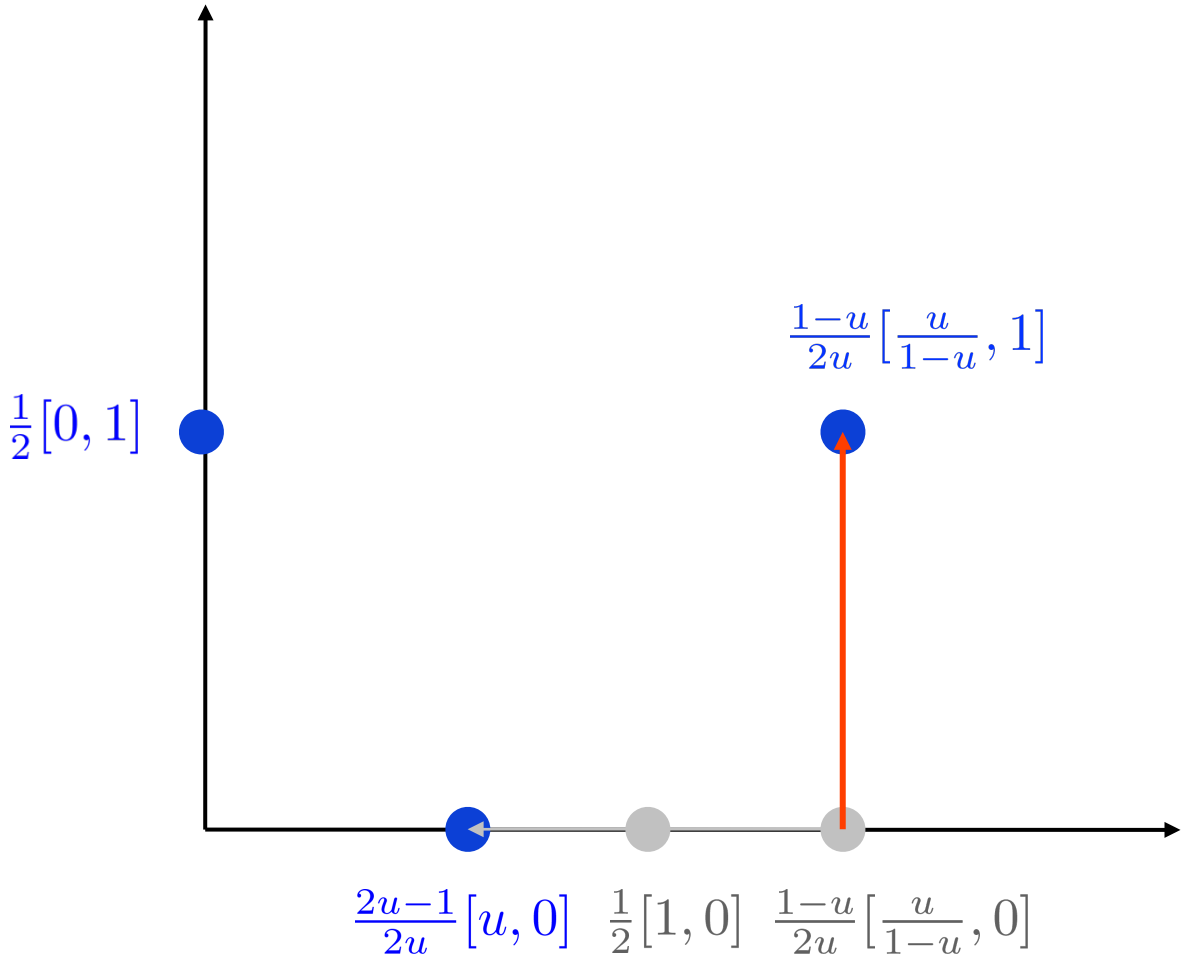
$w[x] \rightarrow w[x'], \quad x' \geq x$

- Merge

- Split

$(w_1 + w_2)[x] \rightarrow w_1[x_1] + w_2[x_2],$

$\frac{w_1 + w_2}{x} \geq \frac{w_1}{x_1} + \frac{w_2}{x_2}$



Examples of valid transitions

Definition: A function h is valid if $\sum_x h(x) = 0 \quad \sum_x xh(x) \geq 0 \quad \forall \lambda > 0, \sum_x \frac{\lambda x}{\lambda + x} h(x) \geq 0$

Examples

- Raise

$w[x] \rightarrow w[x'], \quad x' \geq x$

- Merge

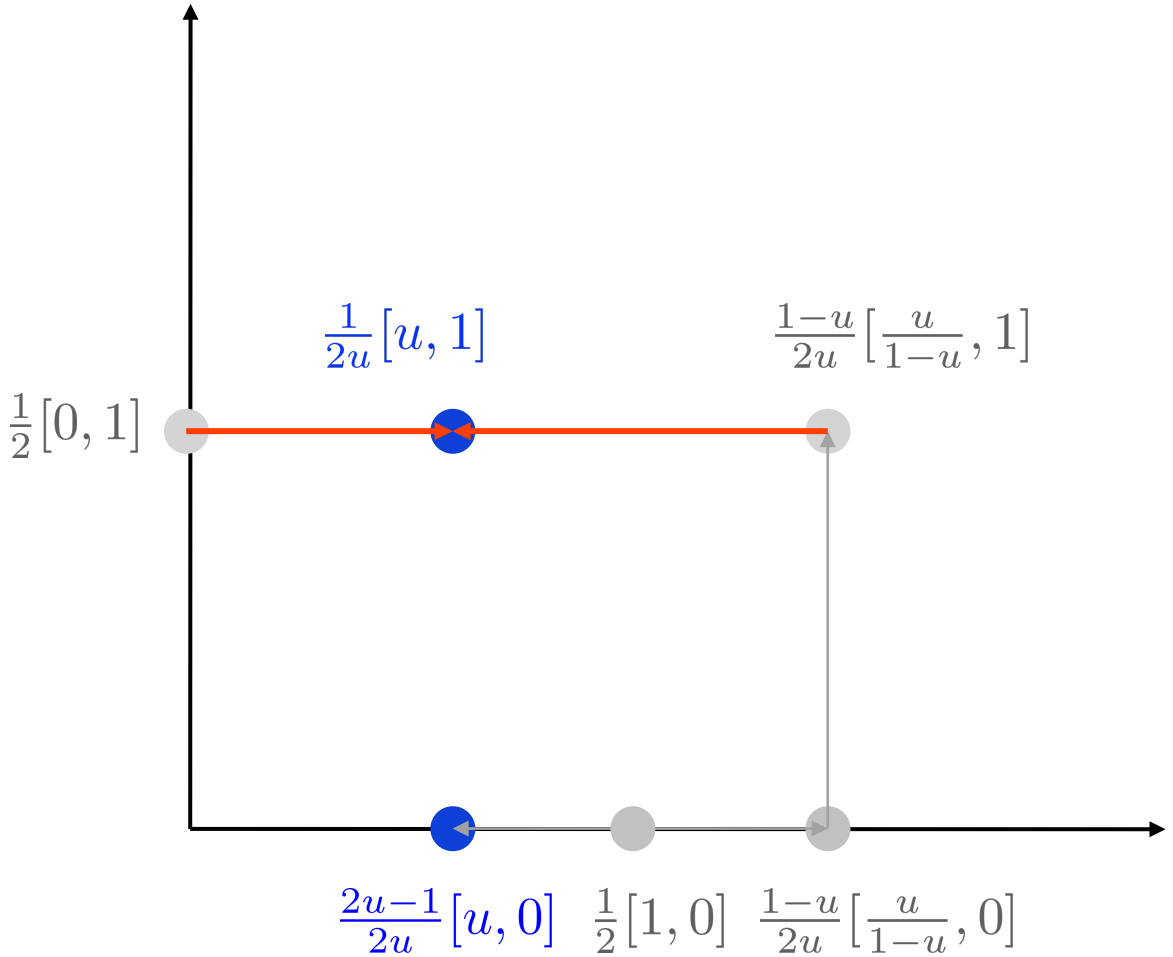
$w_1[x_1] + w_2[x_2] \rightarrow (w_1 + w_2)[x_3],$

$x_3 \geq \frac{w_1 x_1 + w_2 x_2}{w_1 + w_2}$

- Split

$(w_1 + w_2)[x] \rightarrow w_1[x_1] + w_2[x_2],$

$\frac{w_1 + w_2}{x} \geq \frac{w_1}{x_1} + \frac{w_2}{x_2}$



Examples of valid transitions

Definition: A function h is valid if $\sum_x h(x) = 0 \quad \sum_x xh(x) \geq 0 \quad \forall \lambda > 0, \sum_x \frac{\lambda x}{\lambda + x} h(x) \geq 0$

Examples

- Raise

$w[x] \rightarrow w[x'], \quad x' \geq x$

- Merge

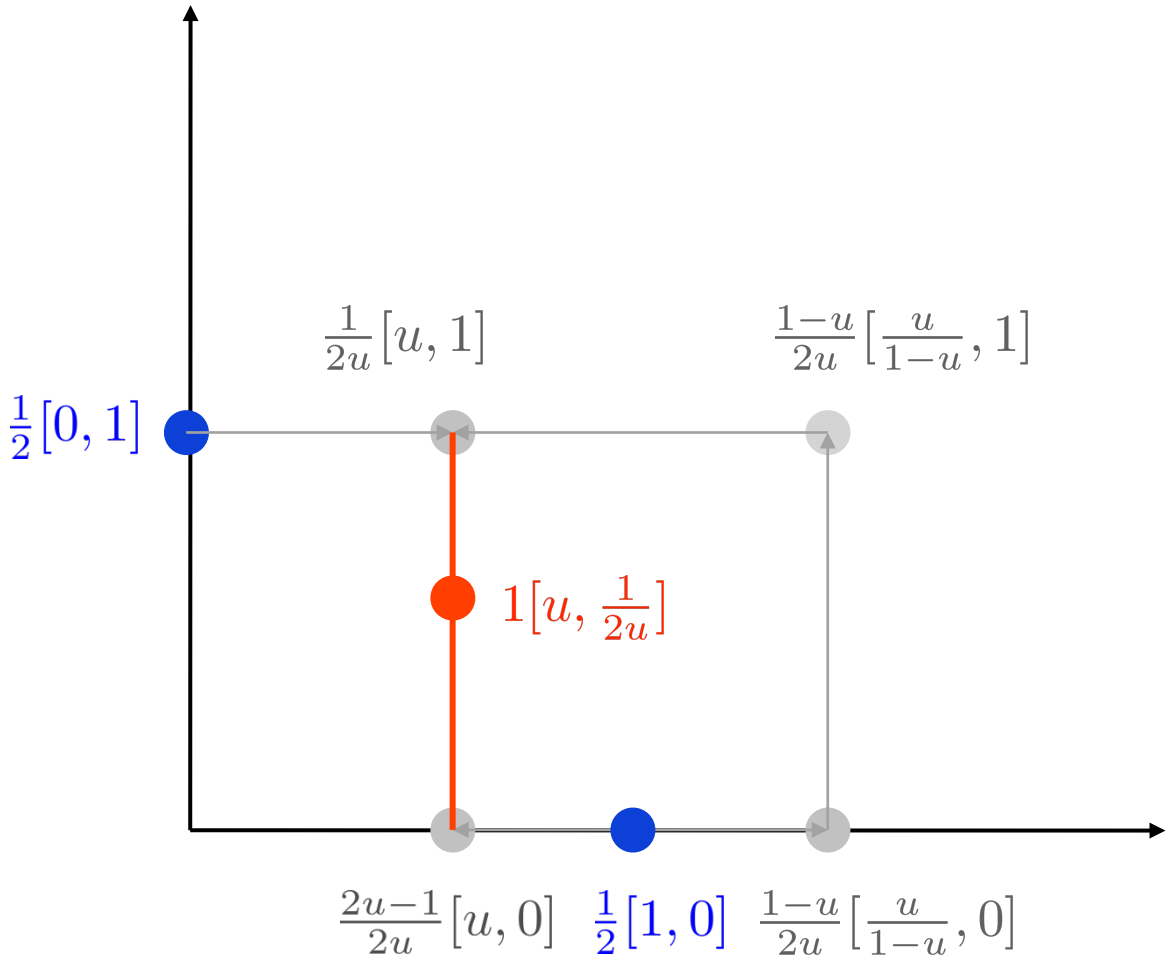
$w_1[x_1] + w_2[x_2] \rightarrow (w_1 + w_2)[x_3],$

$x_3 \geq \frac{w_1 x_1 + w_2 x_2}{w_1 + w_2}$

- Split

$(w_1 + w_2)[x] \rightarrow w_1[x_1] + w_2[x_2],$

$\frac{w_1 + w_2}{x} \geq \frac{w_1}{x_1} + \frac{w_2}{x_2}$



"Equivalence" of EBM and Valid functions

K = set of EBM functions (convex cone, not closed, infinite dimensional)

K^{**} = set of valid functions (A function h is valid if for any OMF, $\sum_x f(x)h(x) \geq 0$)

- Imagine K was closed
  - Then K^{**} = closure(K) = K, and we are done, Valid functions are EBM functions!
- Imagine K was finite dimension
  - Then K^{**}=closure(K)
  - Define the "strict dual" of K^*
    - A function h is strictly valid if for any operator monotone f, $\sum f(x)h(x) > 0$
    - In finite dimension "strict dual" = Interior(K^{**})=Interior(K) < K

      and we are done, Strictly valid functions are EBM functions!

Problem: We are in infinite dimensions

- K and K^{**} have empty interiors!

Solution:

- Consider closed subsets of K, K_L, for L > 0. Any strictly valid function is in some K_L
- Strictly valid functions can be approximated by valid functions

Proof outline

1. Equivalence of different models

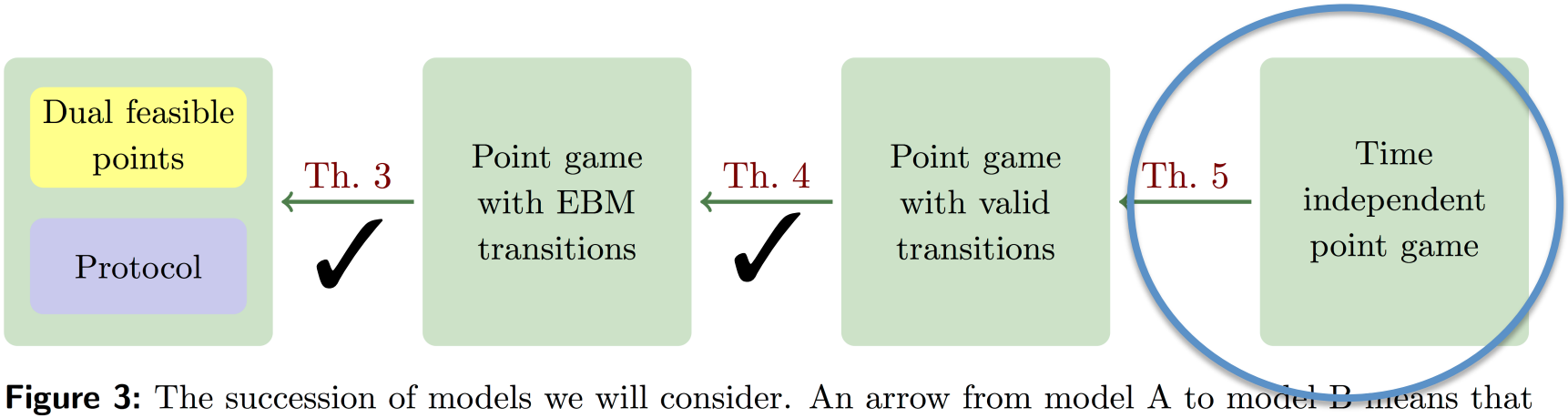


Figure 3: The succession of models we will consider. An arrow from model A to model B means that proving the existence of an ε biased protocol in A implies the existence of an $\varepsilon + \varepsilon'$ biased protocol in B (for all $\varepsilon' > 0$).

2. Existence of a Time independent point game

Time independent point game

Definition (valid game): an ordered sequence of valid functions $\{h_1,\dots,h_n\}$

Definition (TIPG): A Time independent point game is two valid functions h and v st.

$$h+v=[\beta,\alpha]-1/2[1,0]-1/2[0,1] \qquad h=\sum_{horizontal} h_i \qquad v=\sum_{vertical} h_i$$

From TIPG to valid

From a TIPG with final point $[\beta,\alpha]$ and largest point at coordinate Γ,
we can construct a valid point game with final point $[\beta+\varepsilon,\alpha+\varepsilon]$, rounds $O\left(\frac{\|h\|\Gamma}{\varepsilon^2}\right)$

- we use extra points as catalysts
- we move the points little by little

Proof outline

1. Equivalence of different models

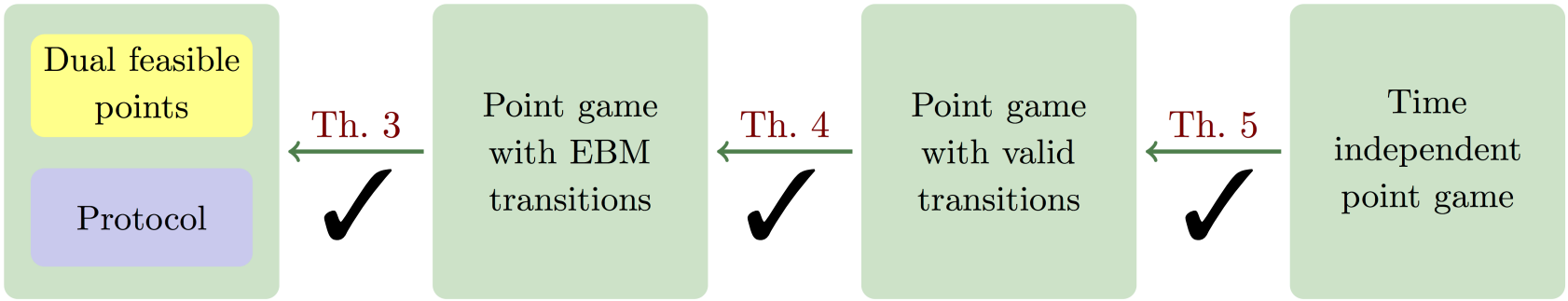


Figure 3: The succession of models we will consider. An arrow from model A to model B means that proving the existence of an ε biased protocol in A implies the existence of an $\varepsilon + \varepsilon'$ biased protocol in B (for all $\varepsilon' > 0$).

2. Existence of a Time independent point game

TIPG with arbitrarily small bias

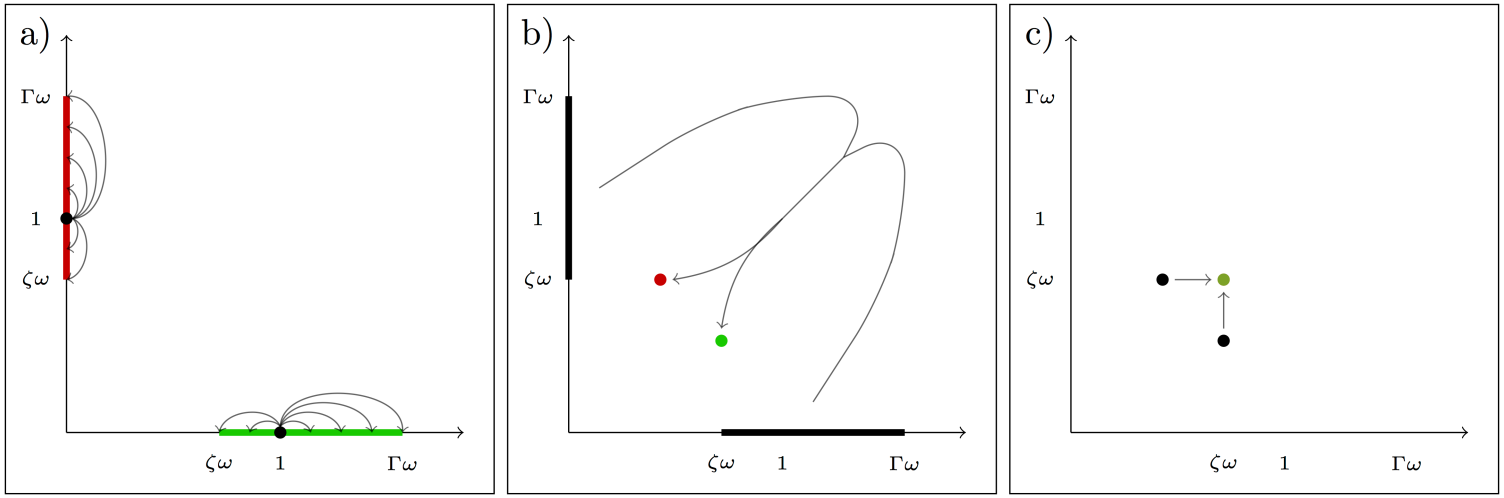


Figure 4: Schematic representation of the game. The initial points are in black, the final points are colored in red if they are part of the horizontal ladder and in green of the vertical ladder. The arrows represents the idea of the movements of the points. a) Each point is split into many points (represented by a line) on their axes. b) The ladder combines the points on the axes into 2 points. c) The raises create the final point of the game.

$$\frac{1}{2}[1,0]+\frac{1}{2}[0,1]\rightarrow\sum_{j=\xi}^{\Gamma} split(j)\left([0,j\omega]+[j\omega,0]\right)$$

$$\rightarrow\frac{1}{2}[\alpha-k\omega,\alpha]+\frac{1}{2}[\alpha,\alpha-k\omega]$$

$$\rightarrow[\alpha,\alpha]$$

ω: grid step, Γ: max coordinate

k: width of the ladder

To Show

1. split is valid
2. ladder is a TIPG

TIPG with arbitrarily small bias

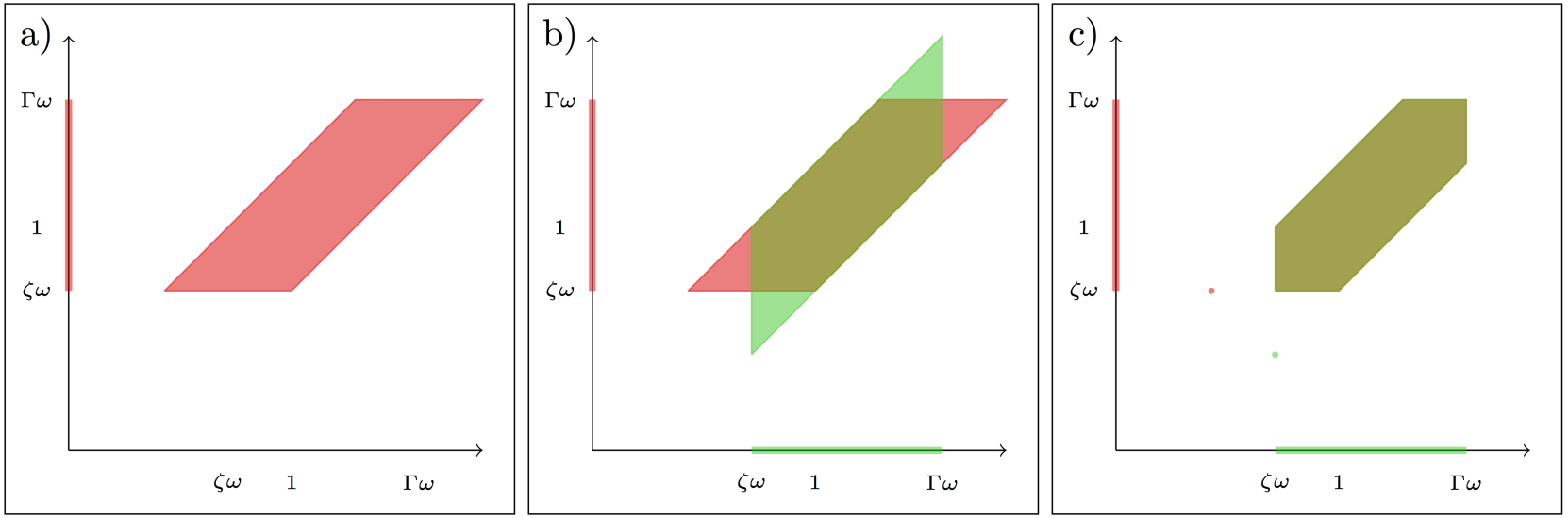


Figure 5: Schematic construction of the ladder. a) The horizontal part of the ladder. b) Superposition of the horizontal part and the vertical part of the ladder. By symmetry, the sum of the weights of the point in the overlap is 0. Except the final points, the weights of the points in the 4 "triangles" with no overlap will be set to 0 by truncation. c) All the points actually involved in the ladder transition.

The ladder of width k

Find valid functions h_{lad} and v_{lad} such that

$$h_{lad} + v_{lad} = \frac{1}{2}[\alpha - k\omega, \alpha] + \frac{1}{2}[\alpha, \alpha - k\omega] - \sum_{j=\zeta}^{\Gamma} split(j)([0, j\omega] + [j\omega, 0])$$

TIPG with arbitrarily small bias

- And the magic continues...

$$h_{\text{lad}} = \sum_{j=\zeta}^{\Gamma} \left(\frac{-C \cdot f(0, j\omega)}{\prod_{l=-k}^{k}((j+l)\omega)} [0, j\omega] + \sum_{\substack{i=-k \\ i\neq 0}}^{k} \frac{C \cdot f((j+i)\,\omega,\ j\omega)}{((j+i)\omega)(j\omega)\prod_{\substack{l\neq i \\ l\neq 0}}((l-i)\omega)} [(j+i)\omega,\ j\omega] \right)$$

$$f(x,y) = (-1)^{k+1} \prod_{i=1}^{k-1} (\alpha - i\omega - x)\,(\alpha - i\omega - y) \prod_{i=1}^{k} (\Gamma\omega + i\omega - x)\,(\Gamma\omega + i\omega - y)$$

Lemma: If the weights follow a polynomial with certain properties, the function is valid.

Thm[Mochon]: For any k, taking $\omega \to 0, \Gamma \to \infty$ makes the above function valid for a final point $[\frac{k+1}{2k+1}, \frac{k+1}{2k+1}]$

Resources of the protocol

Thm[Mochon]: Parameters are $\omega \to 0, \Gamma \to \infty$ (grid step, maximum point)

New Thm: For any k, $\omega = k^{-4}, \Gamma = 2k^8, [\frac{1}{2} + O\left(\frac{1}{k}\right), \frac{1}{2} + O\left(\frac{1}{k}\right)]$

Hence for bias epsilon, take $k = O\left(\frac{1}{\varepsilon}\right)$

Number of qubits: log(number of points)=$\log(poly(k)) = O\left(\log\frac{1}{\varepsilon}\right)$

Number of rounds: $O\left(\frac{\|h\|\Gamma}{\varepsilon^2}\right) = \left(\frac{1}{\varepsilon}\right)^{O\left(\frac{1}{\varepsilon}\right)}$ (after a few more pages of calculations)

- seems to be tight, but maybe not

Proof outline

1. Equivalence of different models

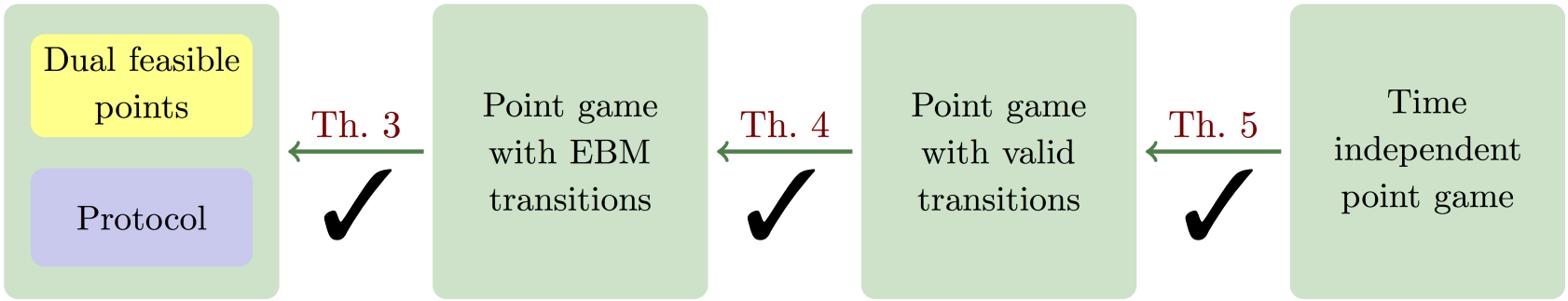


Figure 3: The succession of models we will consider. An arrow from model A to model B means that proving the existence of an ε biased protocol in A implies the existence of an $\varepsilon + \varepsilon'$ biased protocol in B (for all $\varepsilon' > 0$).

2. Existence of a Time independent point game ✓

Conclusions

1. There exists a WCF protocol with arbitrarily small bias
   - simpler, more intuitive proof, resource analysis

2. Can we really understand the equivalence WCF vs point games?

3. Can we find explicit / more efficient / implementable protocols?

4. Can we use the techniques for other protocols?