Caltech

UNIVERSITÉ LIBRE DE BRUXELLES ULB

Quantum Weak Coin Flipping

an analytic solution

Atul Singh Arora

Joint work with Jérémie Roland and Chrysoula Vlachou

A four-slide summary

Motivation

Problem Statement

Take 2

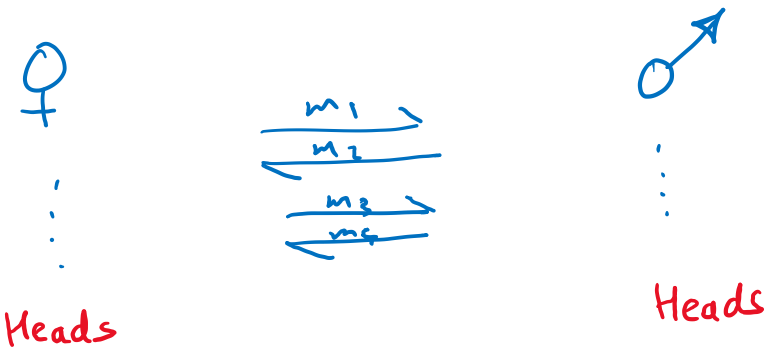
Prior Art

Contribution

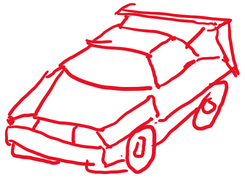
An analytic solution

Conclusion

A four-slide summary



e.g.



Heads = Alice gets the car
Tails = Bob gets the car

(Strong) Coin flipping: **Who gets the car?**: Alice and Bob wish to agree on a random bit, remotely and without trusting each other.

\+

Weak Coin Flipping: **Both want the car**: Alice wants Heads or "0"
Bob wants Tails or "1"

PROBLEM STATEMENT

Not all coin-flipping protocols are born secure.

- Figure of merit of a CF protocol: bias $\doteq \epsilon$

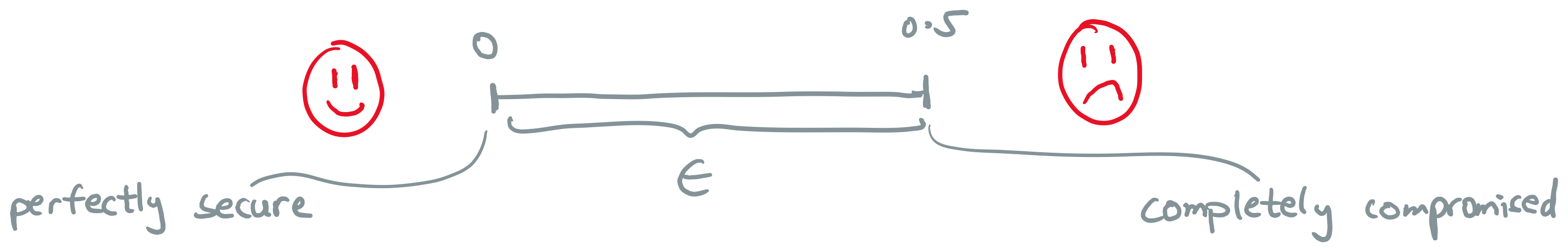
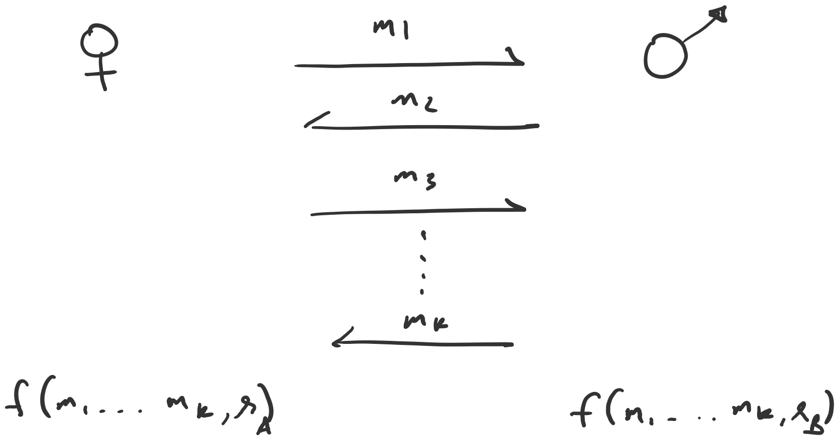
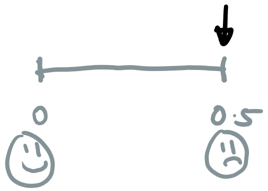


FIGURE OF MERIT

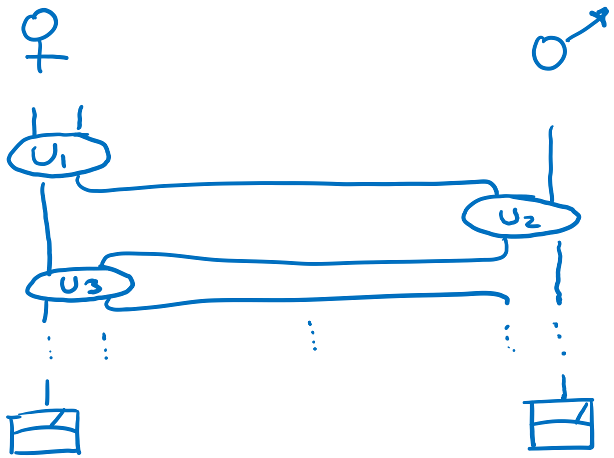
classical



$\epsilon = 0.5$ *



quantum



$\epsilon = \ldots$

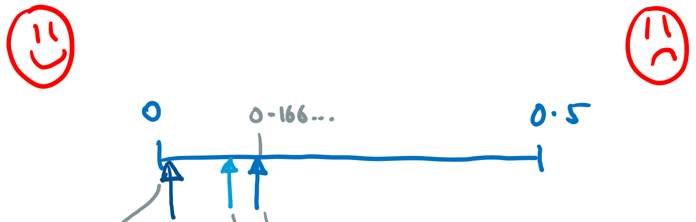
(unless, e.g. computational hardness assumptions are made)

STATE OF THE ART

State of the Art

SCF ϵ is lower bounded by $\frac{1}{\sqrt{2}} - \frac{1}{2}$. [Kitaev '03]

WCF



$\epsilon \to 0$
(existence)

[Mochon '07
Aharonov, '16
Chailloux,
Ganz, Kerenidis, Magnin]

$\epsilon \to \frac{1}{6} = 0.166\ldots$ [Mochon '05]

$\epsilon \to \frac{1}{10} = 0.1$ [ARW '19]

$\epsilon \to 0$ (numerical algorithm)

$\epsilon \to 0$ [*] Analytic Sol^n

(protocols)

Motivation

Cryptography / Secure Two-Party Computation

Secure Two-Party Computation
(Secure Function Evaluation)

⇕

Oblivious Transfer

⇓ ⇑ ~ Quantumly

if BC has "extraction" & "equivocation" [Damgard, Fehr, Lunemann, Salvail, Schaffner '09]

Bit Commitment — Impossible Quantumly [Meyers '97, Lo Chau '97]

⇓

(Strong) Coin Flipping — Impossible ($\epsilon \geq \frac{1}{\sqrt{2}} - \frac{1}{2}$) [Kitaev '03]

[Kerenidis Chailloux '09, '11]
optimal but necessarily imperfect

⇓

Weak Coin Flipping — Possible but protocol missing

impossible classically
(without further assumptions)

- Simple to state
- Distribution of entanglement + randomness

Both honest

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

One honest, other cheats

$$\frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2}$$

Problem Statement

Take 2

Situations

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

Alice	Bob	Feature
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 $\frac{1}{2} + \epsilon$.

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

Prior Art

Kitaev | Three Equivalent Formalisms

Protocol + Certificate (SDP Duality)

(constructive) ⇓ ⇑ (non-constructive)   (numerical algorithm: EMA) [ARW '19]

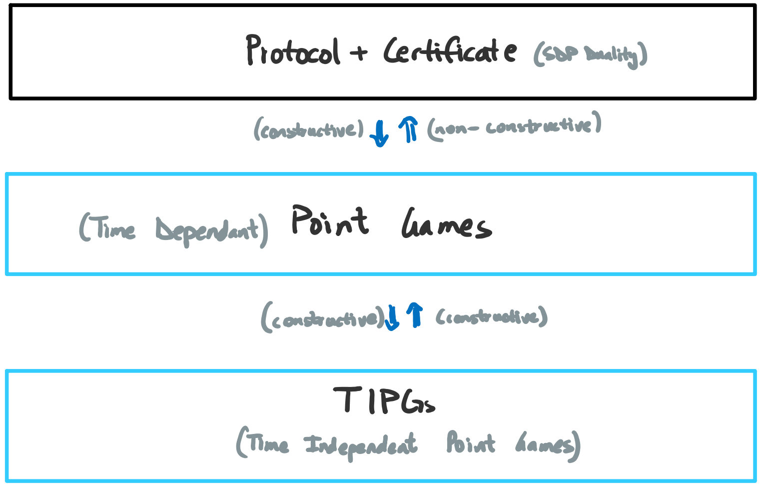
(Time Dependant) Point Games

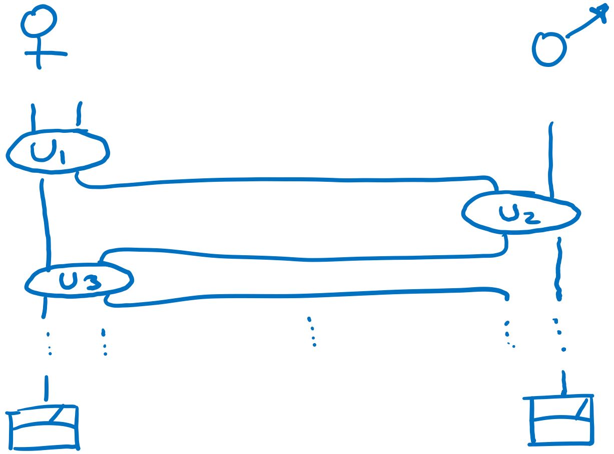
(constructive) ⇓ ⇑ (constructive)

TIPGs
(Time Independent Point Games)

REVIEW OF MOCHON/KITAEV/ACGKM
'06 '03 '16

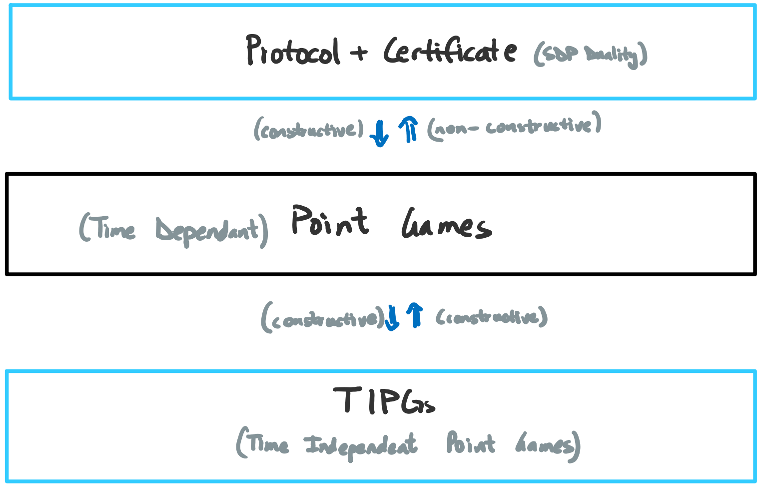
Kitaev | Protocol





- Variables involved: ρ, U
- Two SDPs
  - P_A^* is an SDP in ρ_B: $P_A^* = \max(\mathrm{tr}(\Pi_A \rho_B))$ s.t. the honest player (Bob) follows the protocol.
  - Similarly for P_B^*.
- Dual: $\rho \leftrightarrow Z$, $\max \leftrightarrow \min$, $P^* = \max \leftrightarrow P^* \leq$ certificate

Kitaev | TDPG

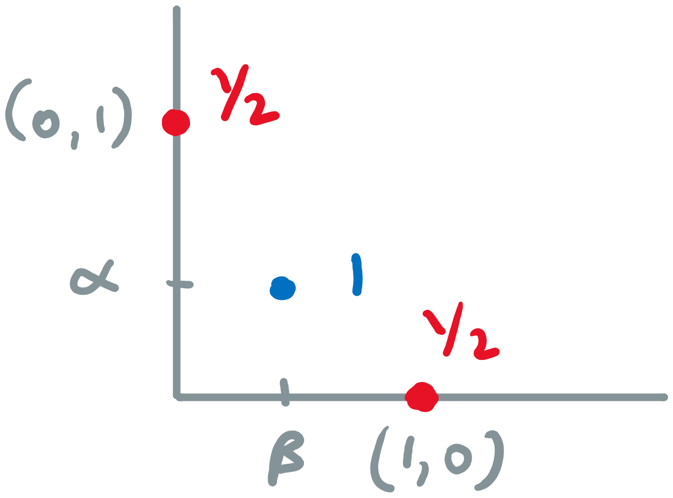


Time Dependent Point Game (TDPG):
A sequence of frames (frames = points on a plane) such that

- Starts with points at $(0,1)$ and $(1,0)$ with weight $1/2$.
- Consecutive frames: along a line, for all $\lambda \geq 0$

"Valid Moves"
$$\sum_z \frac{\lambda z}{\lambda + z} p_z \leq \sum_{z'} \frac{\lambda z'}{\lambda + z'} p'_{z'}.$$

- Ends with a single point (β, α).



Claim: For a valid TDPG there is a protocol with $P_A^* \leq \alpha$, $P_B^* \leq \beta$.

Technique: Operator monotone functions.

Kitaev | TDPG | Valid Moves

Merge $(n_g \to 1)$:

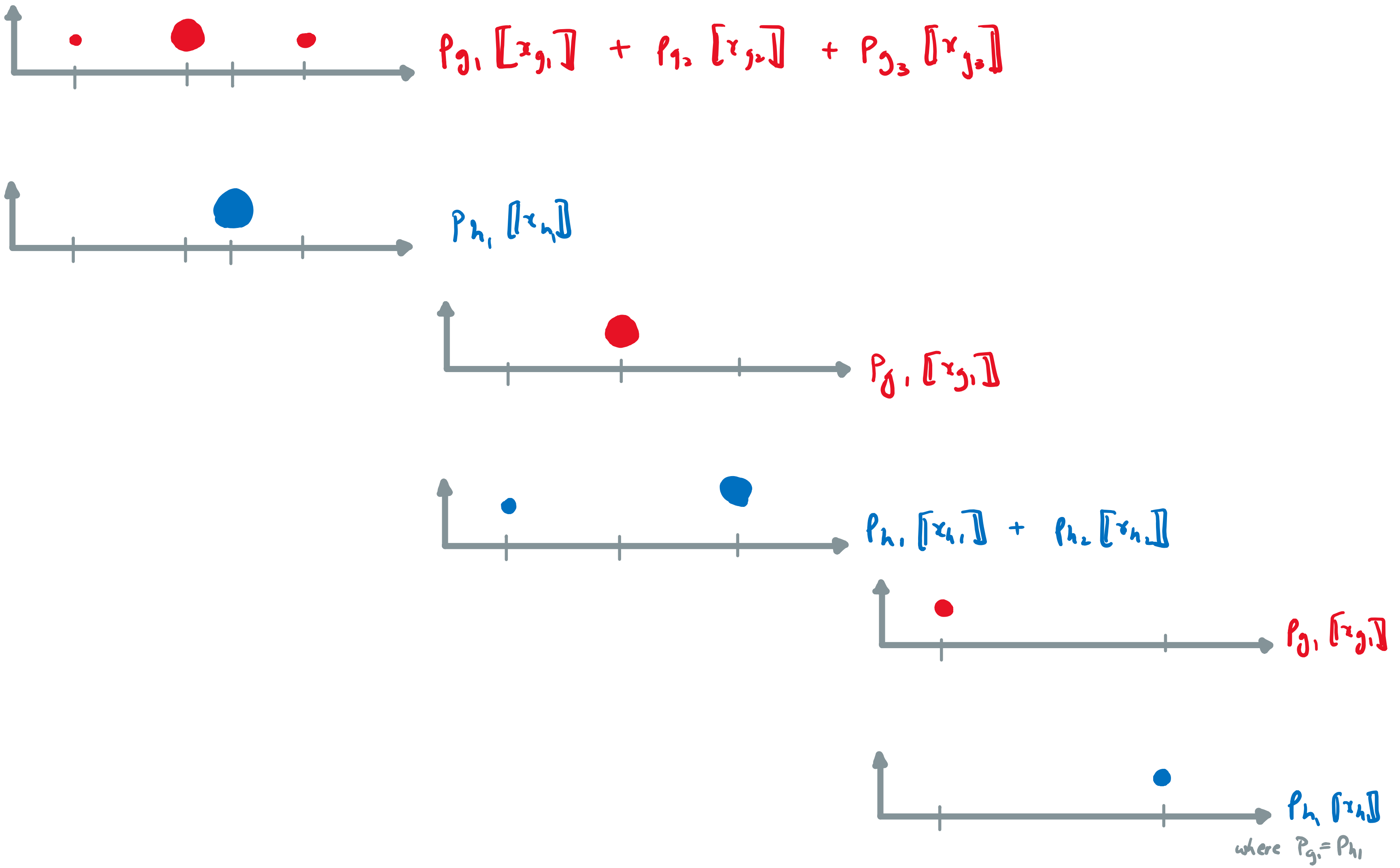
$$\langle x_g \rangle \leq x_h$$

Split $(1 \to n_h)$:

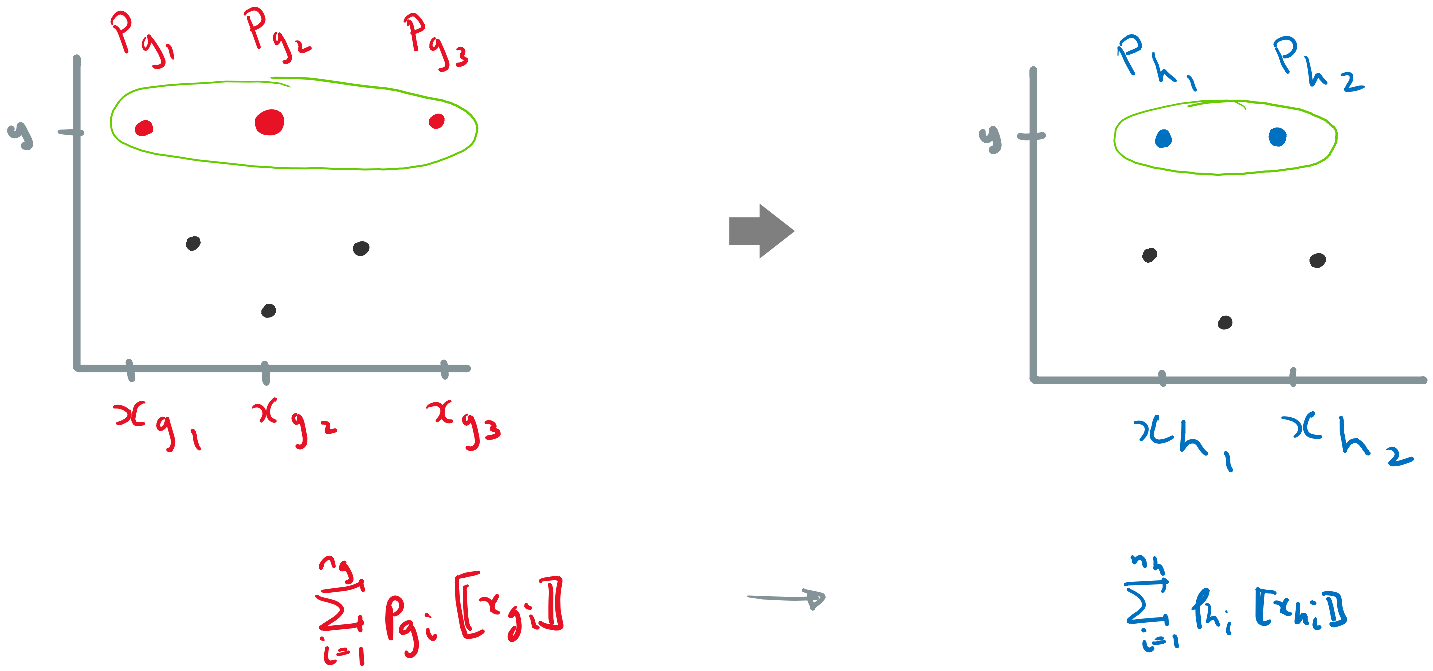
$$\frac{1}{x_g} \geq \left\langle \frac{1}{x_h} \right\rangle$$

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

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



Kitaev | TDPG | Valid Moves



Consecutive frames: along a line, for all $\lambda \geq 0$

$$\sum_i \frac{\lambda x_{g_i}}{\lambda + x_{g_i}} p_{g_i} \leq \sum_i \frac{\lambda x_{h_i}}{\lambda + x_{h_i}} p_{h_i}.$$

Kitaev | TDPG | Example

Merge ($n_g \to 1$):

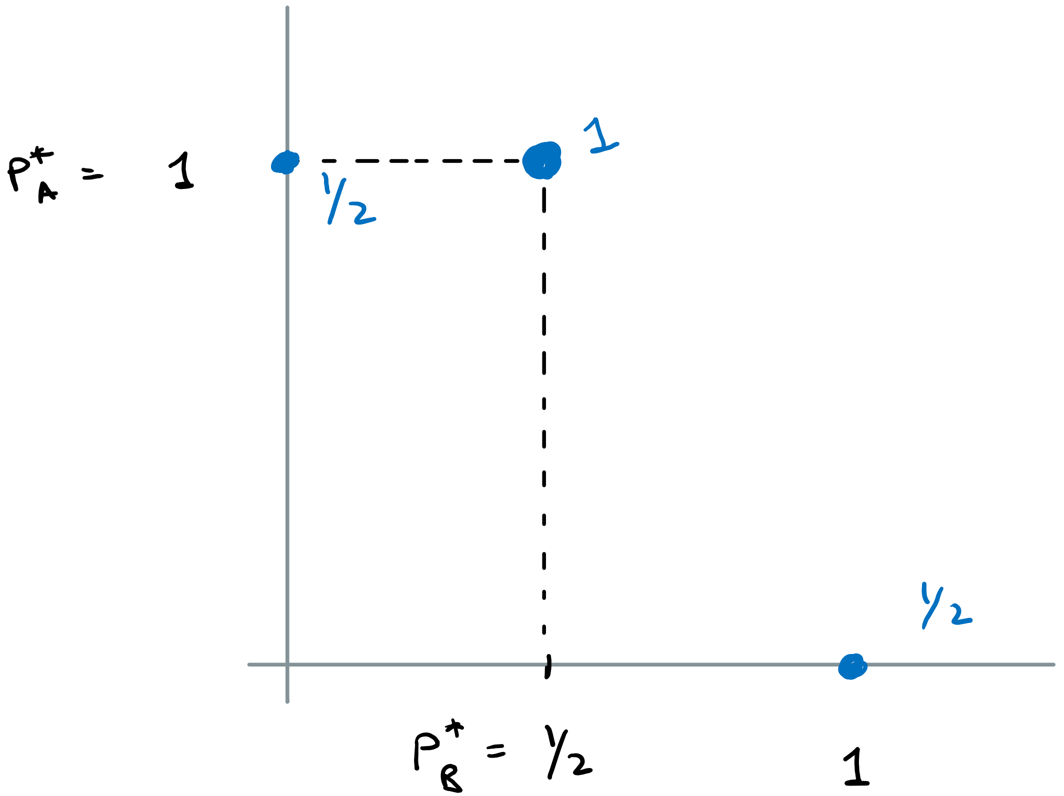
$$\langle x_g \rangle \leq x_h$$

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

Merge ($n_g \to 1$):

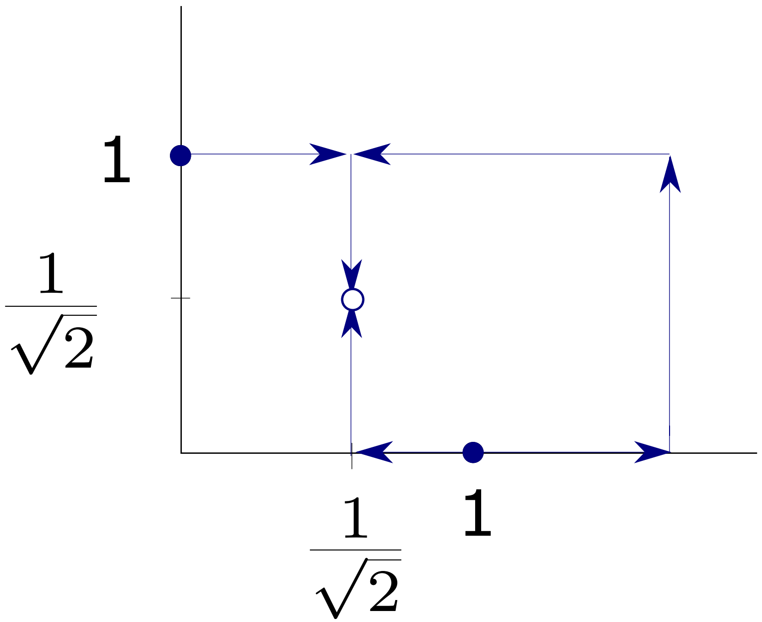
$$\langle x_g \rangle \leq x_h$$

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

Merge ($n_g \to 1$):

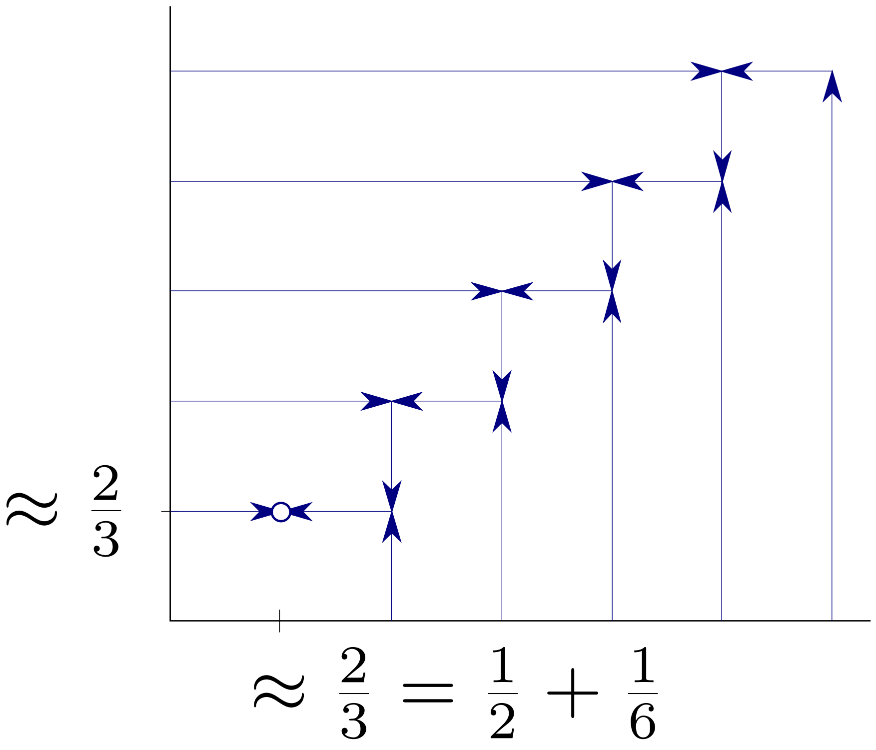
$$\langle x_g \rangle \leq x_h$$

Split ($1 \to n_h$):

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

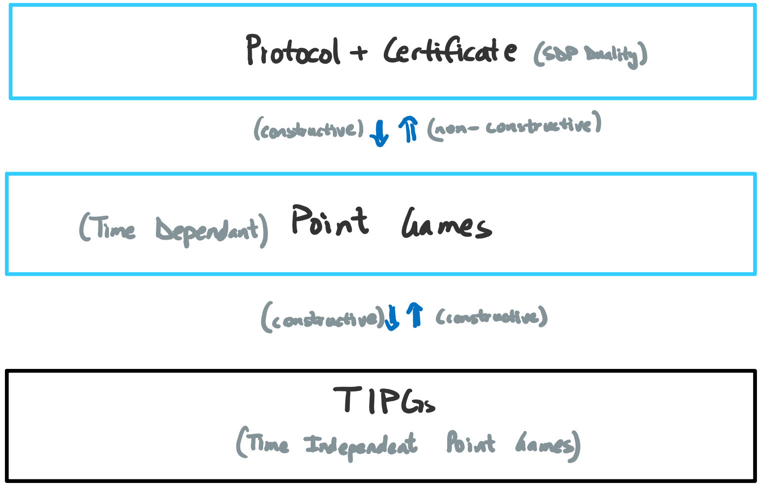
Raise ($n_g = n_h \to n_h$):

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



Best known explicit protocol until '18:
Dip Dip Boom (Mochon, PRA '05)

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.

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

Technique: Catalyst state.

Mochon | Near-perfect WCF is possible

- Result: 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.
- Technique: Polynomials.

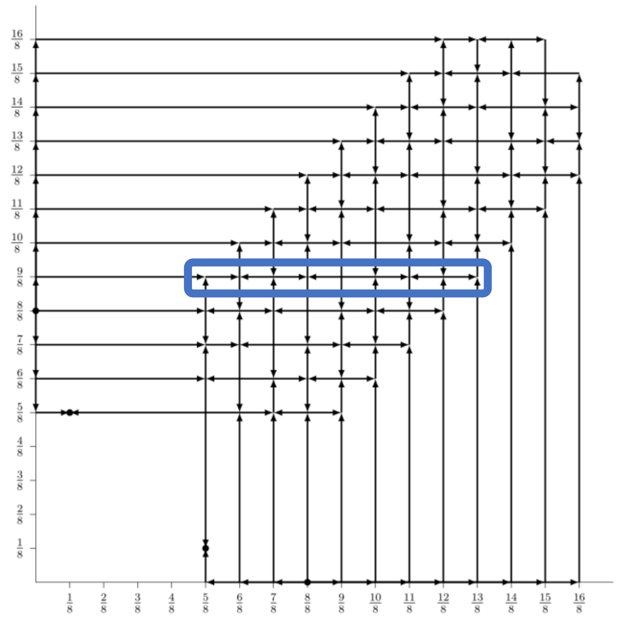


Image taken from E. Pelchat's Master Thesis

Mochon | Valid moves and valid functions

Def^n: $[\![x]\!](a) := \delta_{x,a}$ ~ Kronecker Delta.

NB: $\underbrace{\sum_{i=1}^{n_g} p_{g_i} [\![x_{g_i}]\!]}_{g} \to \underbrace{\sum_{i=1}^{n_h} p_{h_i} [\![x_{h_i}]\!]}_{h}$. Then g & h are finitely supported functions.

"Notation": $t = h - g$ is a valid function

$\Updownarrow$ (assuming no overlapping points)

$h \to g$ is a valid move

Mochon | f-assignments

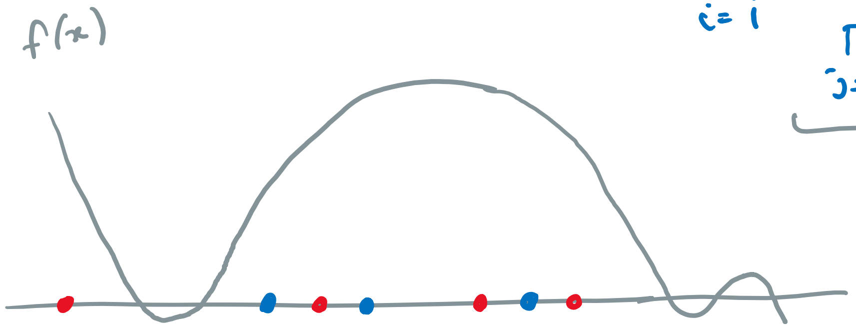
Def^n: f-assignment. Given

- coordinates $0 \le x_1 < x_2 \dots < x_n$
- a polynomial $f(x)$ of degree at most $n-2$ satisfying $f(-\lambda) \geq 0 \;\; \forall \; \lambda \geq 0$,

an f-assignment is the function

$$t = \sum_{i=1}^{n} \underbrace{\frac{-f(x_i)}{\prod_{j \neq i} (x_j - x_i)}}_{=: p_i} [\![x_i]\!] = h - g \quad \text{where} \quad h = \sum_{i:\, p_i > 0} p_i [\![x_i]\!], \quad g = \sum_{i:\, p_i < 0} p_i [\![x_i]\!].$$

E.g.



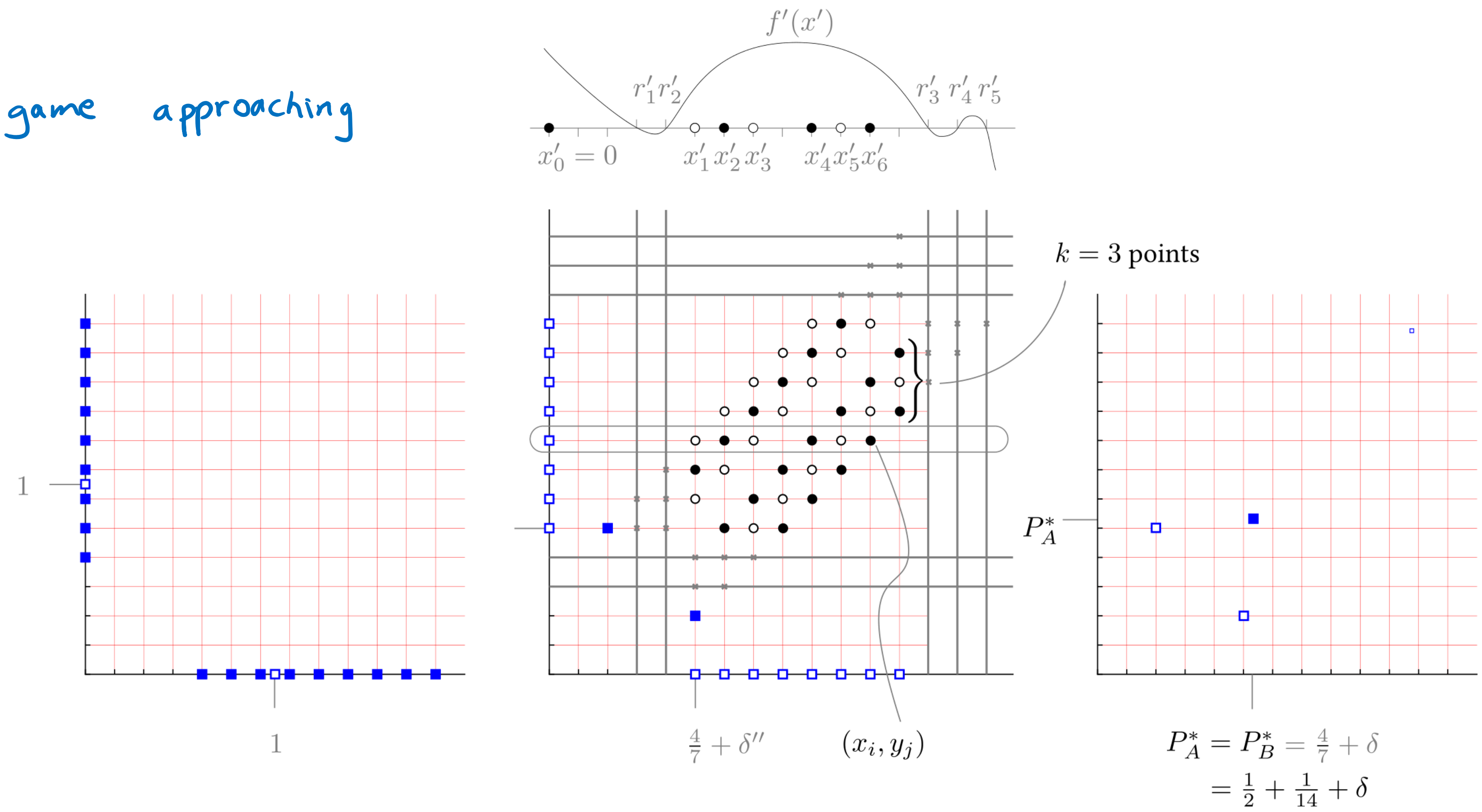
7 points ; $n=7$

5 roots ; $n-2=5$

Mochon | *f*-assignments (cont.)

Lemma: All *f*-assignments are valid functions.

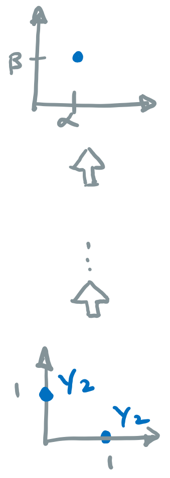
Illustration: Mochon's point game approaching bias 1/14.



Prior Art

Summarised

$\epsilon = \max\{\alpha, \beta\} - \frac{1}{2}$



Protocol + Certificate (SDP Duality)

(constructive) ⇓ ⇑ (non-constructive)] our focus

(numerical algorithm: EMA) [ARW '19]

(Time Dependant) Point Games

(constructive) ⇓ ⇑ (constructive)

TIPGs

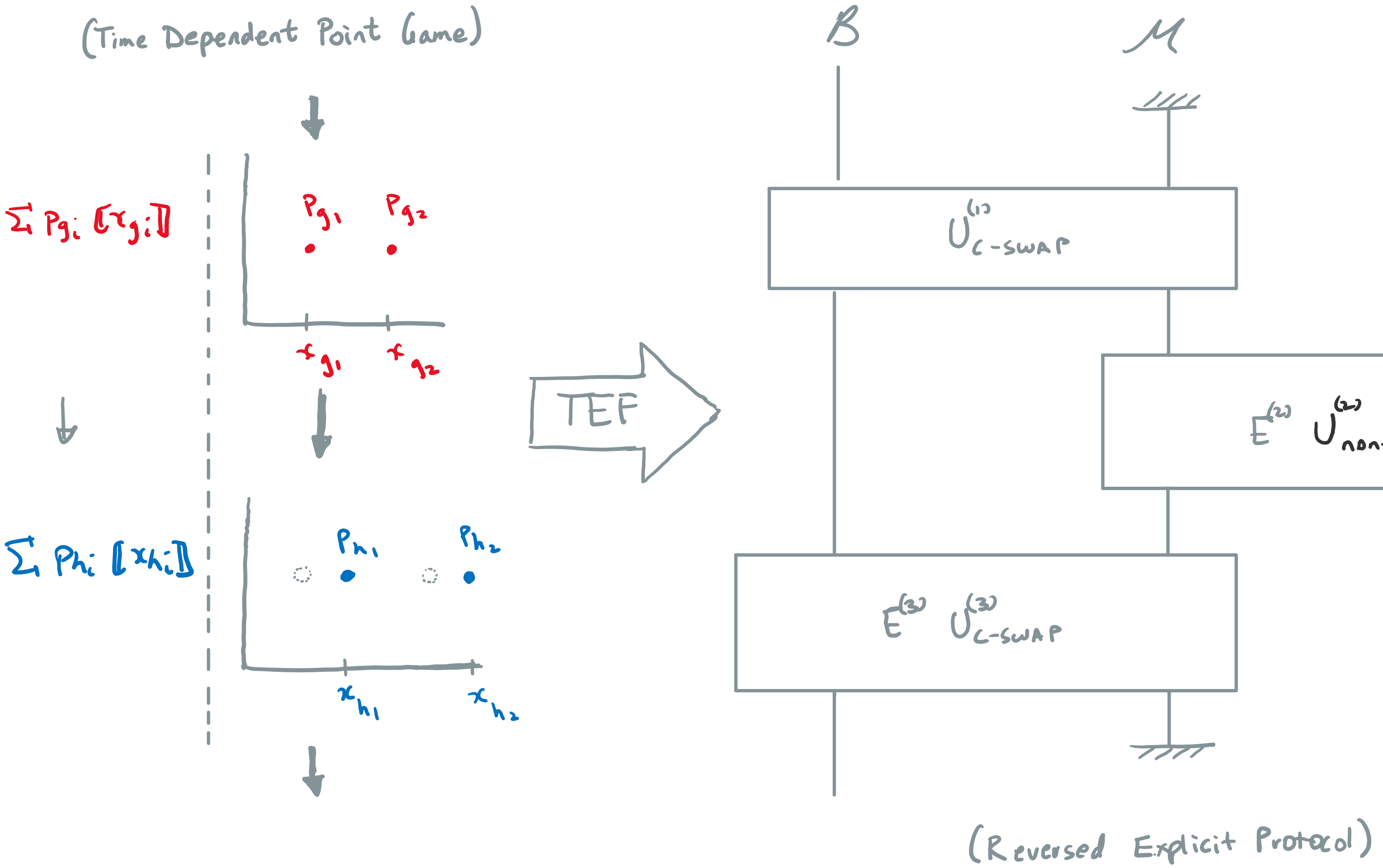
(Time Independent Point Games)

Mochon gave a family of TIPGs with bias approaching

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

REVIEW OF MOCHON / KITAEV / ACGKM

'06 '03 '16



Simplified Constraint on $U_{\text{non-trivial}}$

$\{|g_1\rangle, |g_2\rangle, \dots |h_1\rangle, |h_2\rangle, \dots\}$

$X_h := \sum_i x_{h_i} |h_i\rangle\langle h_i|$

$X_g := \sum_i x_{g_i} |g_i\rangle\langle g_i|$

$|v\rangle := \sum_i \sqrt{p_{g_i}} |g_i\rangle$

$|w\rangle := \sum_i \sqrt{p_{h_i}} |h_i\rangle$

U s.t.

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

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

where $E_h := \sum_i |h_i\rangle\langle h_i|$

TEF TDPG-to-Explicit-Protocol Framework [ARW '19]

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: Mochon's $\epsilon = 1/6$ protocol from its point game directly.

Contribution

An analytic solution

Analytic Solution | Special cases of f-assignments

Recall: f-assignment: $t = \sum_{i=1}^{\hat{n}} \frac{-f(x_i)}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!]$

where f was a polynomial of deg $\leq n-2$

& $f(-\lambda) \geq 0 \quad \forall \lambda \geq 0$.

Aim: "Solve" f-assignments i.e.

find U s.t. $X_h \succeq E_h U X_g U^T E_h$

Special Cases:

- monomial assignment: $f(x) = (-x)^q$
  - balanced monomial: # points with +ve weight = # points with −ve weight | unbalanced
  - aligned: $\deg(f) = q$ is an even # | misaligned

Analytic Solution | Effective Solutions

(Inf) Def^n: Suppose $t = \sum_i t_i$ where $t, t_1, t_2, \ldots$ are valid functions.

We say t has an effective solution if each t_i has a sol^n.

(Inf) Lemma: A TIPG can be converted into an explicit protocol if each valid function it uses, admits an effective solution.

Analytic Solution | Sum of Monomial Assgnmnt

Idea: Break an f-assignment, t, into a sum of monomial assignments, $\{t_i\}$
(almost trivial)

$$t = \sum_i t_i,$$

and solve the monomial assignments.

Significance: Mochon's TIPG approaching $\epsilon = \frac{1}{4k+2}$ use only f-assignments (+ splits but those we already handled using blinkered unitaries)
so the aforesaid yields exact WCF protocols approaching zero bias.

Non-trivial: Solving monomial assignments.

Analytic Solution | Balanced Aligned Monomial

(Inf) Prop^n: Let
- $m = 2b$ $(b \geq 0 ;\ b \in \mathbb{Z})$
- $t = \sum_{i=1}^{n} x_{h_i}^m p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} x_{g_i}^m p_{g_i} [\![x_{g_i}]\!]$ be a monomial assignment over $0 < x_1 < x_2 \ldots < x_{2n}$
- $\{|h_1\rangle, |h_2\rangle, \ldots |h_n\rangle, |g_1\rangle, |g_2\rangle \ldots |g_n\rangle\}$ be an orthonormal basis
- $X_h := \sum_i x_{h_i} |h_i\rangle\langle h_i|$; $X_g := \sum_i x_{g_i} |g_i\rangle\langle g_i|$ $\quad |w'\rangle := \sum_i \sqrt{p_{h_i}}\, |h_i\rangle$; $|v'\rangle := \sum_i \sqrt{p_{g_i}}\, |g_i\rangle$
  $|w\rangle := (X_h)^b |w'\rangle$; $|v\rangle := (X_g)^b |v'\rangle$.

Then U solves t where

$$U = \sum_{i=-b}^{n-b-1} \left(\frac{\overbrace{\Pi_{h_i}^{\perp} (X_h)^i |w\rangle\langle v| (X_g)^i \Pi_{g_i}^{\perp}}}{\sqrt{c_{h_i} c_{g_i}}} + h.c. \right)$$

"monomial"

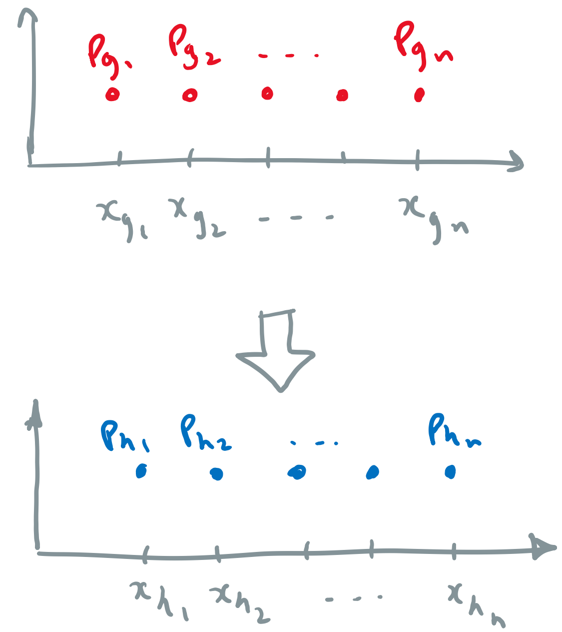
normalization of the braced term

where

$$\Pi_{h_i}^{\perp} := \begin{cases} \text{projector orthogonal to } \operatorname{span}\{(X_h)^{-|i|+1}|w\rangle, (X_h)^{-|i|+2}|w\rangle \ldots, |w\rangle\} & i < 0 \\ \text{projector orthogonal to } \operatorname{span}\{(X_h)^{-b}|w'\rangle, (X_h)^{-b+1}|w\rangle, \ldots (X_h)^{i-1}|w\rangle\} & i > 0 \\ \mathbb{1} & i = 0 \end{cases}$$

Analytic Solution | Zeroth Assignment

Suppose $b=0$. i.e. $t = \sum_{i=1}^{2n} \frac{-1}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!] =: \sum_{i=1}^{n} p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} p_{g_i} [\![x_{g_i}]\!]$



U s.t.

$$|v\rangle \longmapsto |w\rangle$$

$$\Pi_{g_1} X_g |v\rangle \longmapsto \Pi_{h_1} X_h |w\rangle$$

$$\Pi_{g_2} X_g^2 |v\rangle \longmapsto \Pi_{h_2} X_h^2 |w\rangle \qquad + \text{h.c.}$$

$$\vdots$$

$$\Pi_{g_n} X_g^n |v\rangle \longmapsto \Pi_{h_n} X_h^n |w\rangle$$

Analytic Solution | Intuition behind the proof

Recall: U had to be s.t. $X_h \geq E_h U X_g U^\dagger E_h$

(and $U|v\rangle = |w\rangle$ but this is by construction for us).

Def^n: $D := X_h - E_h U X_g U^\dagger E_h$

Claim: $\langle x^k \rangle = 0 \quad \forall\, k \in \{0, 1, 2 \ldots 2n-2\}$ & where $\langle x^\ell \rangle := \sum_i x_{h_i}^\ell p_{h_i} - \sum_i x_{g_i}^\ell p_{g_i}$

(due to Mochon) + ARW

$\langle x^{2n-1} \rangle > 0$

Assertion:

$$D \doteq \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \langle w'_{n-1} | D | w'_{n-1} \rangle \end{bmatrix}$$

$$\langle w'_{n-1} | D | w'_{n-1} \rangle \overset{\text{claim}}{=} \frac{1}{c_{h_{n-1}}} \langle w | (X_h)^{2n-2+1} | w \rangle - \frac{1}{c_{g_{n-1}}} \langle v | X_g^{2n-2+1} | v \rangle$$

recall $|w\rangle := \sum_i \sqrt{p_{h_i}} |h_i\rangle$, recall $|v\rangle := \sum_i \sqrt{p_{g_i}} |g_i\rangle$

$$= \frac{\langle x^{2n-1} \rangle}{c_{n-1}} > 0$$

Conclusion

Conclusion

- Found exact and relatively simple unitaries which constitute WCF protocols with vanishing bias.

- It circumvents the conic-duality argument (a technical reduction) which was crucially used in ARW'19 & in Mochon's proof of existence (simplified further in ACGKM '14).

Outlook

- Resource requirements
  - Use of effective solutions increases the dimension
  - [Miller20] # rounds for WCF with bias $\epsilon \geq e^{\Omega\left(\frac{1}{\sqrt{\epsilon}}\right)}$.
  - # qubits — b/w 1/6 & 1/10 currently there's a large gap.
- Noise Robustness — [Vlachou, Roland, *] Quantum strategies / Quantum combs; general bounds?
- Device Independence — [Sikora, Van Himbeeck, *] — lower bound?
  - protocol $P_A^* = 3/4$, $P_B^* = \cos^2\left(\frac{\pi}{8}\right)$
  - [SCAKPM 11] $\epsilon \simeq 0.336$
  - [In preperation] $\epsilon \simeq 0.317$
  - no-signalling
  - avoiding NPA
    - ↳ self-testing
    - ↳ restricted boxes
    - ↳ iterative improvements.

Thank You

arXiv:1911.13288 v2

https://doi.org/10.1137/1.9781611976465.58 ← SODA '21