Quantum weak coin flipping with arbitrarily small bias[1]

"where weakness is a virtue", or

"how to reduce instead of abort"

Portugal Crypto Day
13/12/2024

[1]Atul S. Arora, Jérémie Roland and Chrysoula Vlachou, ACM SIAM SODA 2021, pp. 919-938. See also https://ia.cr/2022/1101.

Coin flipping (over the telephone)[3]

Two distrustful parties, Alice and Bob, wish to remotely generate an unbiased random bit.

- **Strong Coin Flipping** (SCF)
  The parties do not know a priori each other's preferred outcome

- **Weak Coin Flipping** (WCF)
  The parties have a priori known opposite preferred outcomes

Security: neither player can force their desired outcome with $P \geq \frac{1}{2} + \epsilon$.

Quantum WCF is the strongest known S2PC primitive with unconditional security

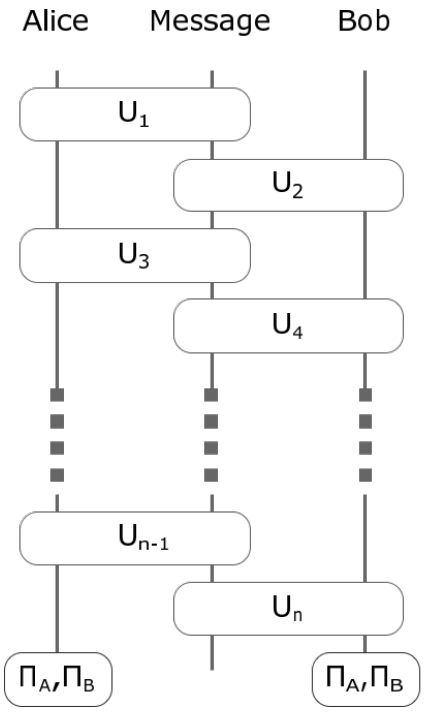
*Optimal protocols for SCF, BC and OT[2]

[2]A. Chailloux and I. Kerenidis, IEEE FOCS 2009, pp. 527-533 and IEEE FOCS 2011, pp. 354-362, A. Chailloux, G. Gutoski and J. Sikora, CJTCS 2016, no 13.

[3]M. Blum, SIGACT News 15.1, 23-27 (1983).

Quantum WCF protocols

Creation of quantum correlations towards an honest state



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

A *new framework* is needed permitting us to find *both* the protocol and its bias.

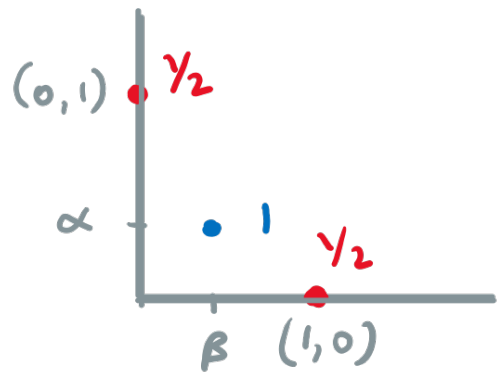
Time-dependent point games (TDPG)[4]

Sequence of frames including points on $x - y$ plane with probability weights

- Initial points: $(0, 1)$ and $(1, 0)$ with $p = 1/2$.
- Transitions between frames:

$$\sum_z p_z = \sum_{z'} p_{z'} \text{ probability conservation}$$

$$\sum_z \frac{\lambda z}{\lambda + z} p_z \leq \sum_{z'} \frac{\lambda z'}{\lambda + z'} p_{z'}, \forall \lambda \geq 0 \text{ monotonicity}$$



- Final point (β, α) with $p = 1$.

Theorem. **TDPG[!!!] $\Leftrightarrow$ WCF protocol with $P_A^* \leq \alpha, P_B^* \leq \beta$.**

[4]Mochon in arXiv:0711.4114 attributes the formalism to A. Y. Kitaev.

Time-Independent Point Games (TIPG)[6]

Simplifying the formalism[7]

Instead of the entire sequence of frames we can only consider suitably$^{!!!}$ constructed initial and final frame.

***Theorem*. TIPG$^{!!!}$ $\Leftrightarrow$ TDPG$^{!!!}$ with the same final frame.**

Family of TIPG approaching bias[5]

$$\epsilon(k) = \frac{1}{4k+2}, k \in \mathbb{N}$$

Existence of WCF protocols with $\epsilon \to 0$

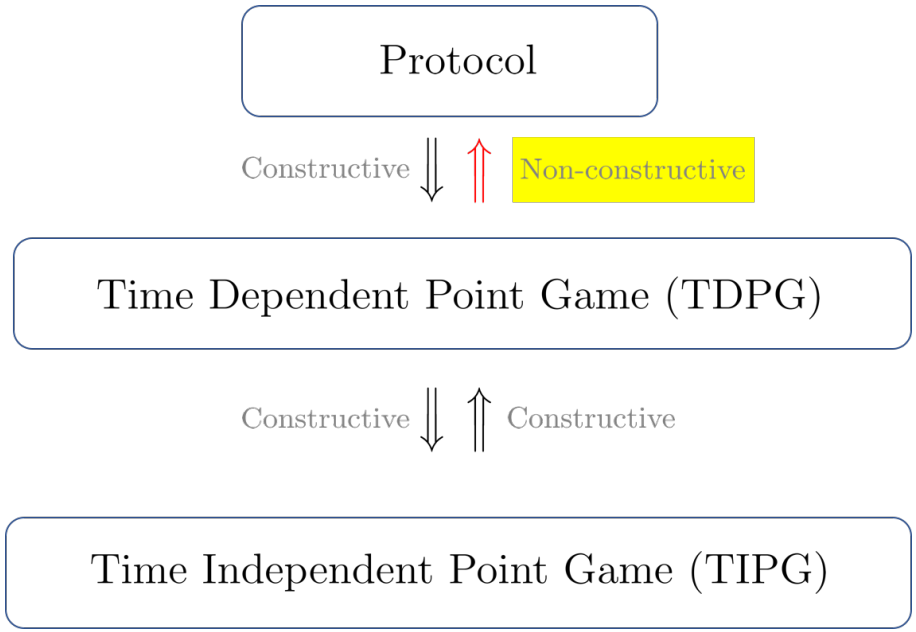
---

[5] $2k$: number of points involved in the main move of the point game.

[6] C. Mochon, arXiv:0711.4114 (2007)

[7] Trading matrix for real number constraints; verifying matrix inequalities for all transitions is hard.

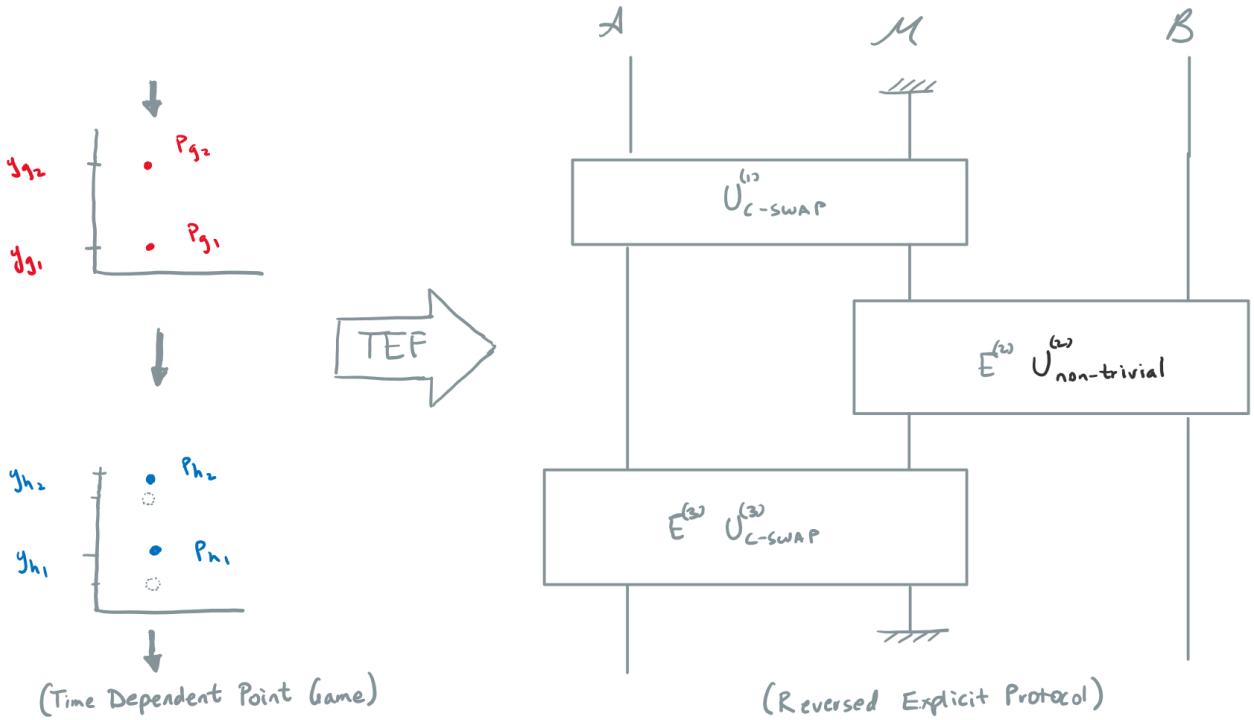
Equivalent frameworks and the proof of existence[8]



[8]C. Mochon, arXiv:0711.4114 (2007) and D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis and L. Magnin, SIAM J Comp 45.3, 633-679 (2016).

TDPG-to-Explicit-Protocol Framework (TEF)[9]

TDPG$^{!!!}$ $\rightarrow$ WCF protocol given that for every transition, a unitary U satisfying certain constraints can be found.



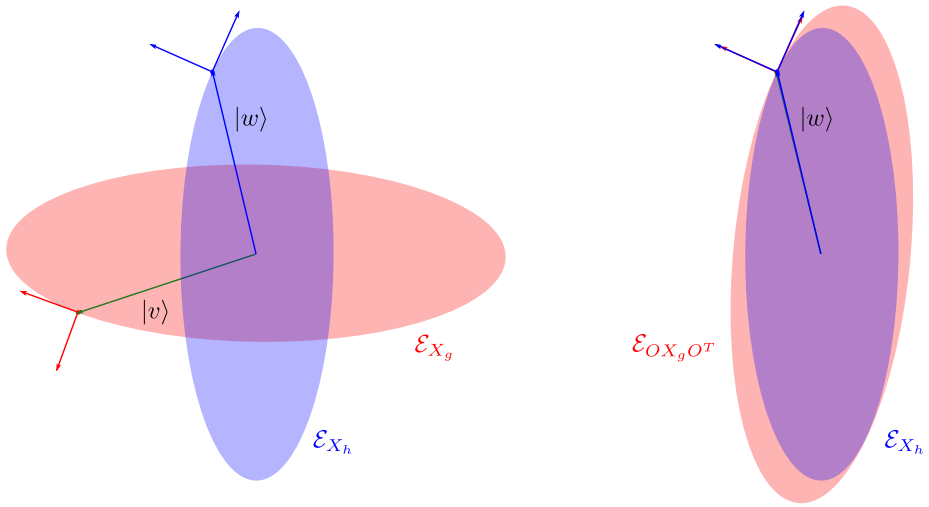
Explicit protocol with $\epsilon = \frac{1}{10}$

[9] A. S. Arora, J. Roland and S. Weis, ACM SIGACT STOC 2019, pp. 205-216.

The Elliptic Monotone Align (EMA) Algorithm[10]

Numerical solution

TEF constraint for each transition as a containment of ellipsoids



The curvature condition at the point of contact is an instance of the same problem with one less dimension, allowing us to iteratively find U.

[10] A. S. Arora, J. Roland and S. Weis, ACM SIGACT STOC 2019, pp. 205-216.

Geometric analytic solution[11]

- Consider isometries instead of unitaries
- Restrict to Mochon's family of TIPGs
- Contact and component conditions must hold at all iterations
- Expressed in terms of the initial value
- Proof by induction

Solution by Iteration:

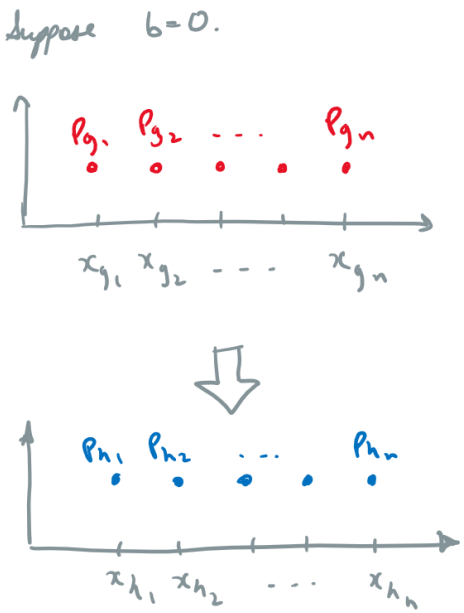
$$Q^{\overline{k}} = |u_h^{\overline{k}}\rangle \langle u_g^{\overline{k}}| + Q^{\overline{k-1}}$$

[11] A. S. Arora, J. Roland and CV, see https://ia.cr/2022/1101.

Algebraic solution[12]

Translating the geometric properties to the algebraic properties of Mochon's assignment

If we find O satisfying the TEF constraints we have a protocol.



O s.t.

$$|v\rangle \longmapsto |w\rangle$$
$$\Pi_{g_1} X_g |v\rangle \longmapsto \Pi_{h_1} X_h |w\rangle$$
$$\Pi_{g_2} X_g^2 |v\rangle \longmapsto \Pi_{h_2} X_h^2 |w\rangle + \text{h.c.}$$
$$\vdots$$
$$\Pi_{g_n} X_g^n |v\rangle \longmapsto \Pi_{h_n} X_h^n |w\rangle$$

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

[12] A. S. Arora, J. Roland and CV, ACM SIAM SODA 2021, pp. 919-938.

Geometric vs Algebraic

- G: intuitive, "constructive" and pedagogical
- G: cumbersome and very technical[13]
- A: Neat and much less technical (albeit not intuitive)
- A: Significant simplification of the formalism
  - TEF and $O \rightarrow$ Protocol
  - TEF=TIPG$^{!!!}$=TDPG$^{!!!}$ $\rightarrow$ bypassing part of the non-constructive part

Elegance vs Intuition

[13] infinite curvatures, ill-defined vectors, etc.

Open questions

...well, some of them (the "classical" ones)

- Protocols for other families of TIPGs[14]?
- Given the bound $\Omega(1/\sqrt{\epsilon})$ on the rounds of communication[15], can we find protocols matching on resources?
- Optimization of our constructions (number of points, memory and register's size)
- Composability of WCF[16].
- A fundamental connection: does optimal SCF imply WCF with $\epsilon \to 0$?

---

[14] P. Høyer and E. Pelchat, MA thesis, University of Calgary (2013).

[15] C. A. Miller, 52nd ACM SIGACT STOC, pp. 916-929 (2020).

[16] J. Wu, Y. Hu, A. Bansal, M. Tomamichel, arXiv:2402.15233 (2024).