ECOLE POLYTECHNIQUE DE BRUXELLES

UNIVERSITÉ LIBRE DE BRUXELLES ULB

https://atulsingharora.github.io/QIP_19

Coin Flipping

where weakness is a virtue

Joint work with Jérémie Roland and Stephan Weis

Atul Singh Arora

Overview

Acknowledgments

Motivation

Stolen shamelessly from Prof Schaffner's QIP 2018 tutorial talk.

Problem Statement

Strong CF, Weak CF, correctness and bias

Prior Art

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

Contribution

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

Conclusion

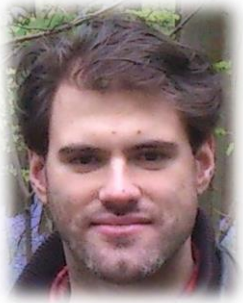
Acknowledgments

Jérémie Roland*

Stephan Weis*

Tobias Fritz

Nicolas Cerf

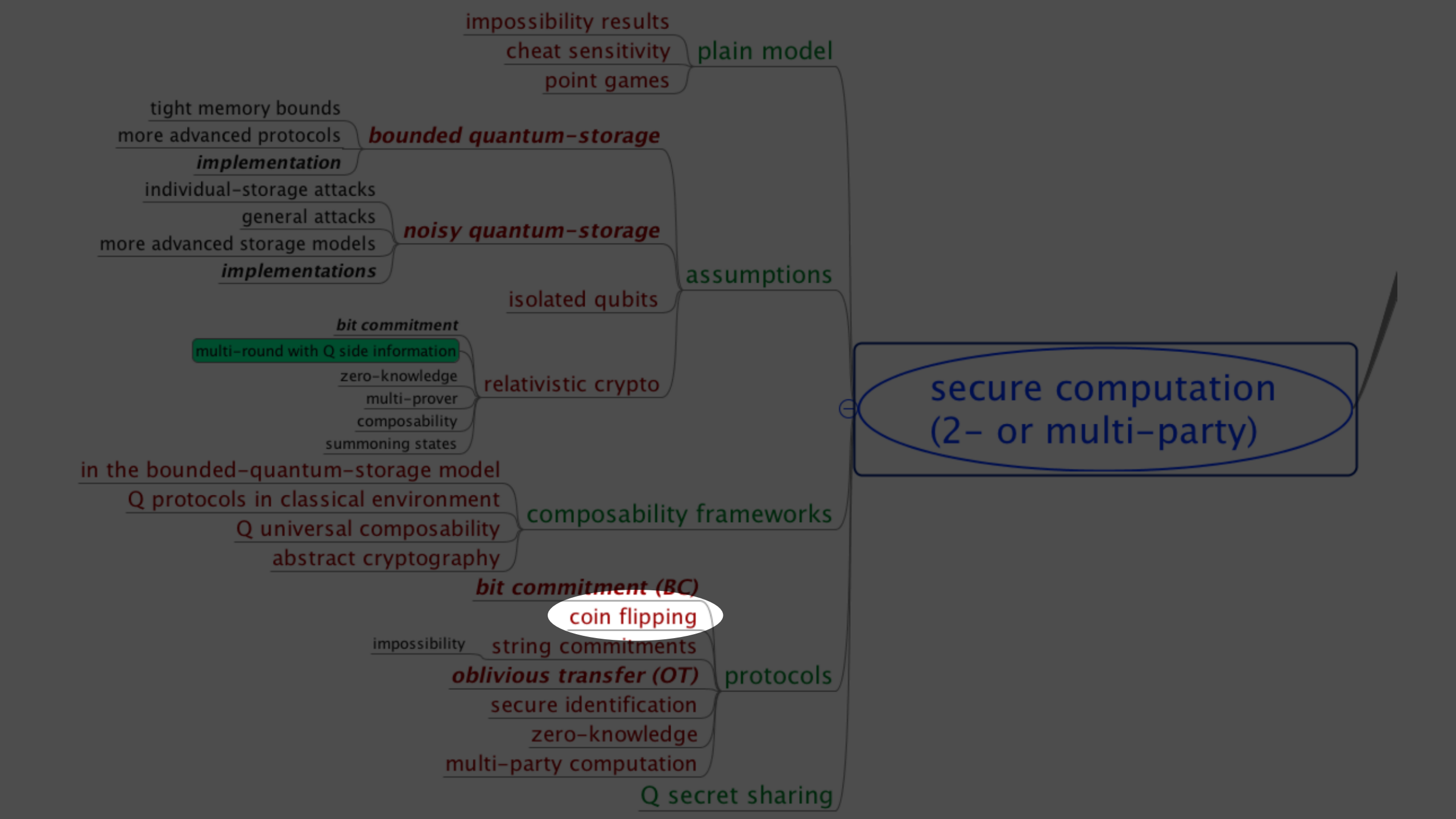


Mathieu Brandeho

* co-authors

Motivation

Stolen shamelessly from Prof Schaffner’s QIP 2018 tutorial talk.


secure computation
(2- or multi-party)
assumptions
plain model
impossibility results
cheat sensitivity
point games
bounded quantum-storage
tight memory bounds
more advanced protocols
implementation
noisy quantum-storage
individual-storage attacks
general attacks
more advanced storage models
implementations
isolated qubits
relativistic crypto
bit commitment
multi-round with Q side information
zero-knowledge
multi-prover
composability
summoning states
composability frameworks
in the bounded-quantum-storage model
Q protocols in classical environment
Q universal composability
abstract cryptography
protocols
bit commitment (BC)
coin flipping
string commitments
impossibility
oblivious transfer (OT)
secure identification
zero-knowledge
multi-party computation
Q secret sharing

Beyond QKD

Multi-party Computation
(dishonest majority)

$\Updownarrow$

Two-party
Secure Function Evaluation

$\Updownarrow$

Oblivious Transfer

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

Quantumly Impossible [Mayers 97, Lo Chau 97]

Bit Commitment

$\Downarrow, \not\Uparrow$

Coin Flipping

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

Prior Art

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

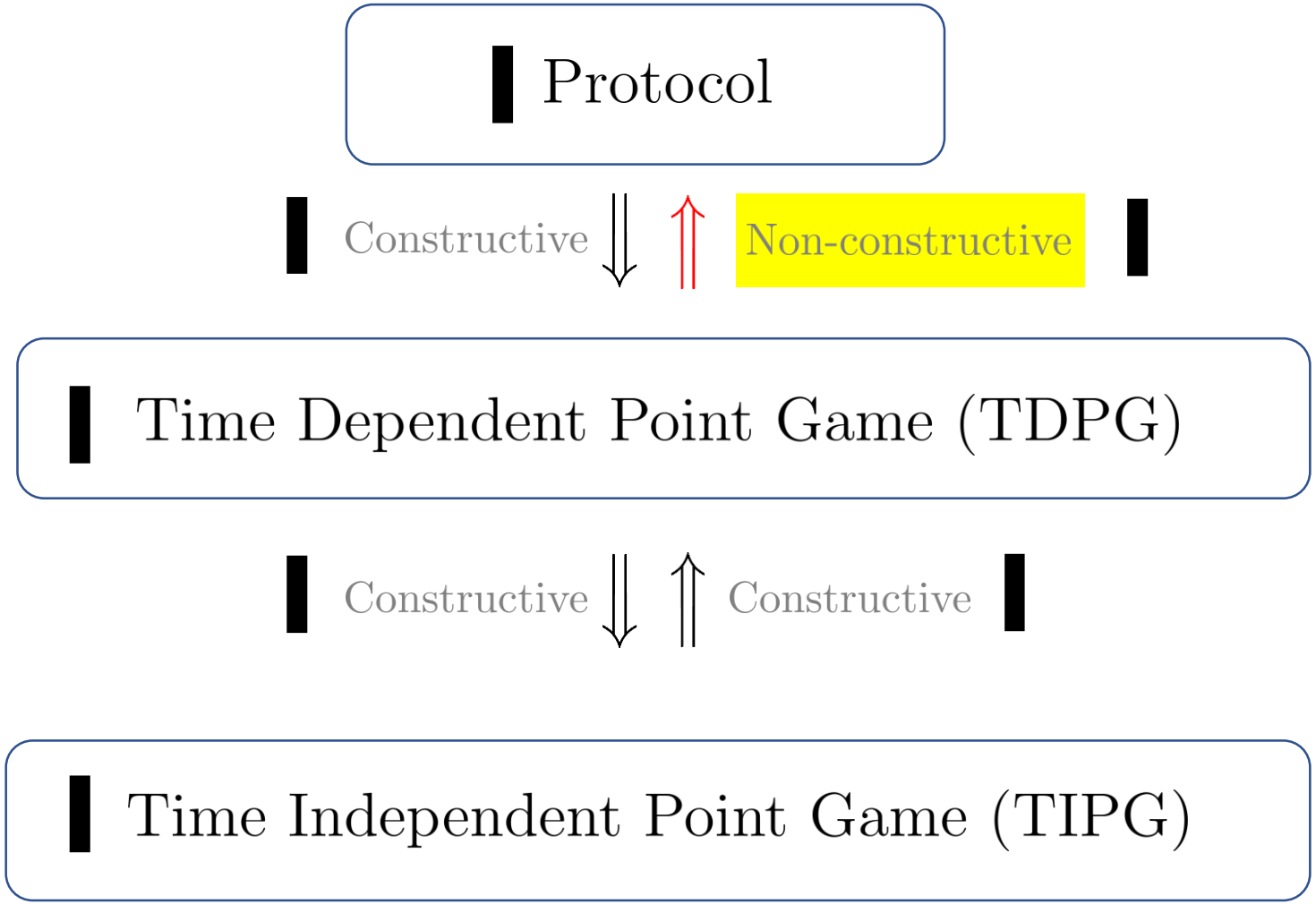
Bounds and Protocols

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

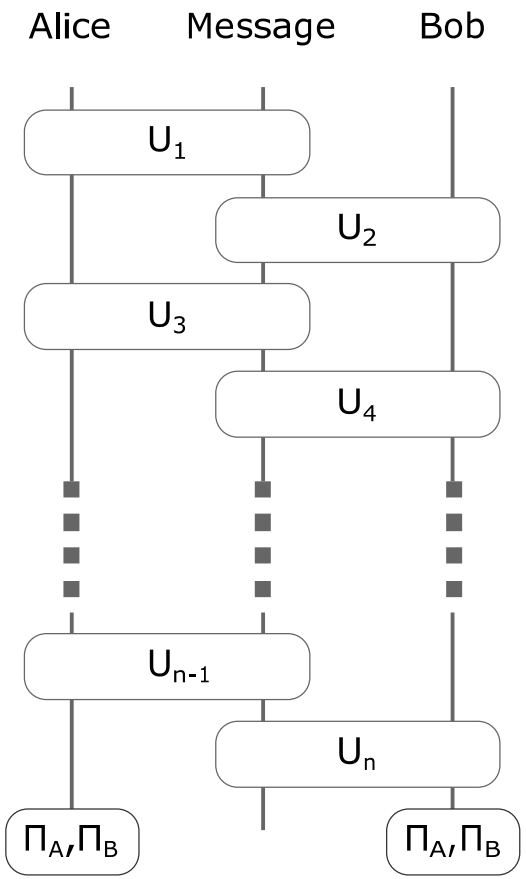
- Quantumly:

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

Kitaev | Three Equivalent Frameworks



Kitaev | Protocol



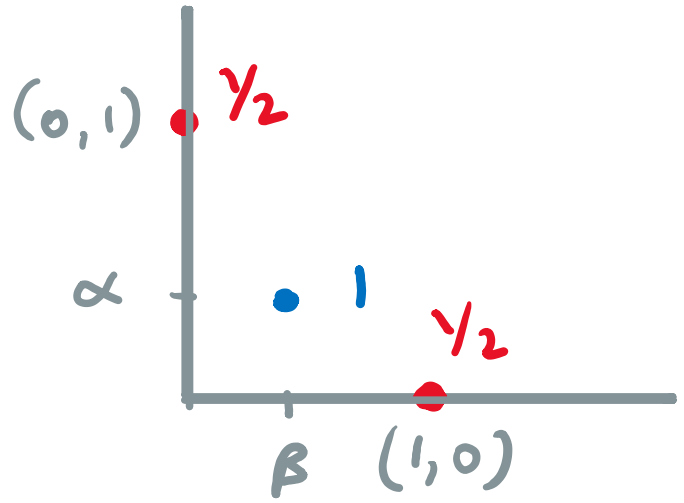
- Variables involved: ρ, U
- Two SDPs
  - P_A^* is an SDP in ρ_B: $P_A^* = \max(\mathrm{tr}(\Pi_A \rho_B))$ s.t. the honest player (Bob) follows the protocol.
  - Similarly for P_B^*.
- Dual: $\rho \leftrightarrow Z$, $\max \leftrightarrow \min$, $P^* = \max \leftrightarrow P^* \leq$ certificate

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 $\lambda \geq 0$

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



- Ends with a single point (β, α).

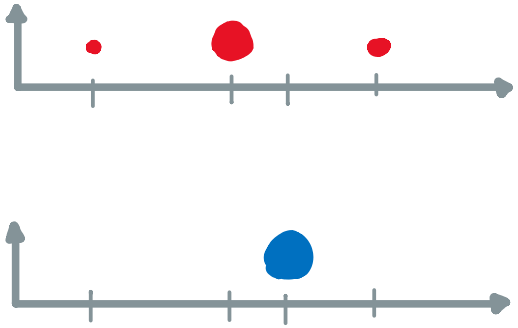
Mathemagic: For a valid TDPG there is a protocol with $P_A^* \leq \alpha$, $P_B^* \leq \beta$.

Charm: Operator monotone functions.

Kitaev's Framework #2 | TDPG | Rule

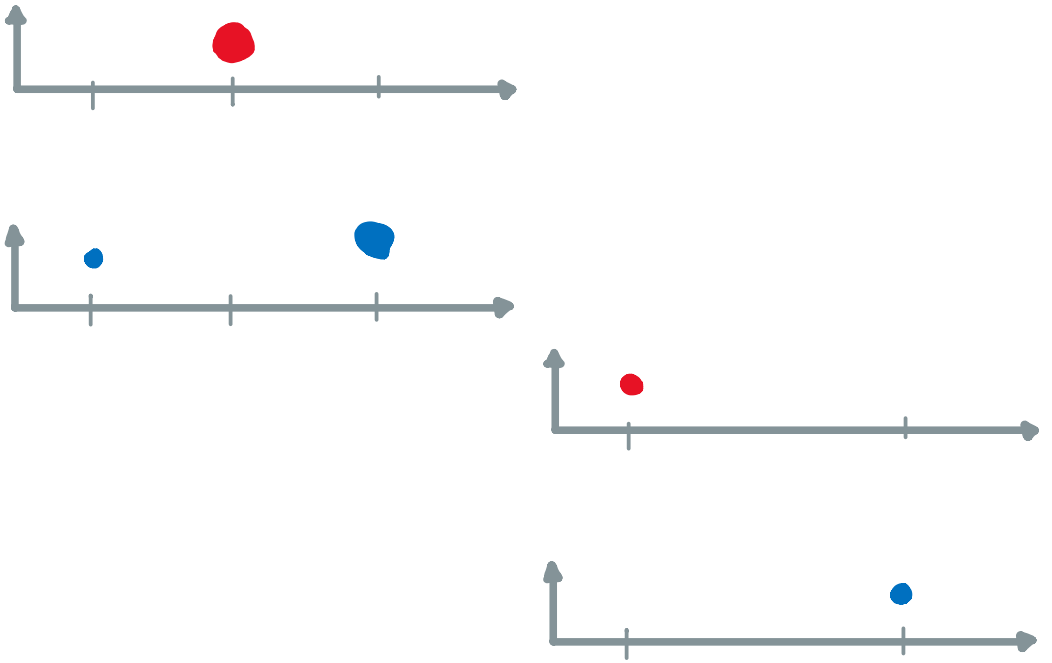
Merge $(n_g \to 1)$:

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



Split $(1 \to n_h)$:

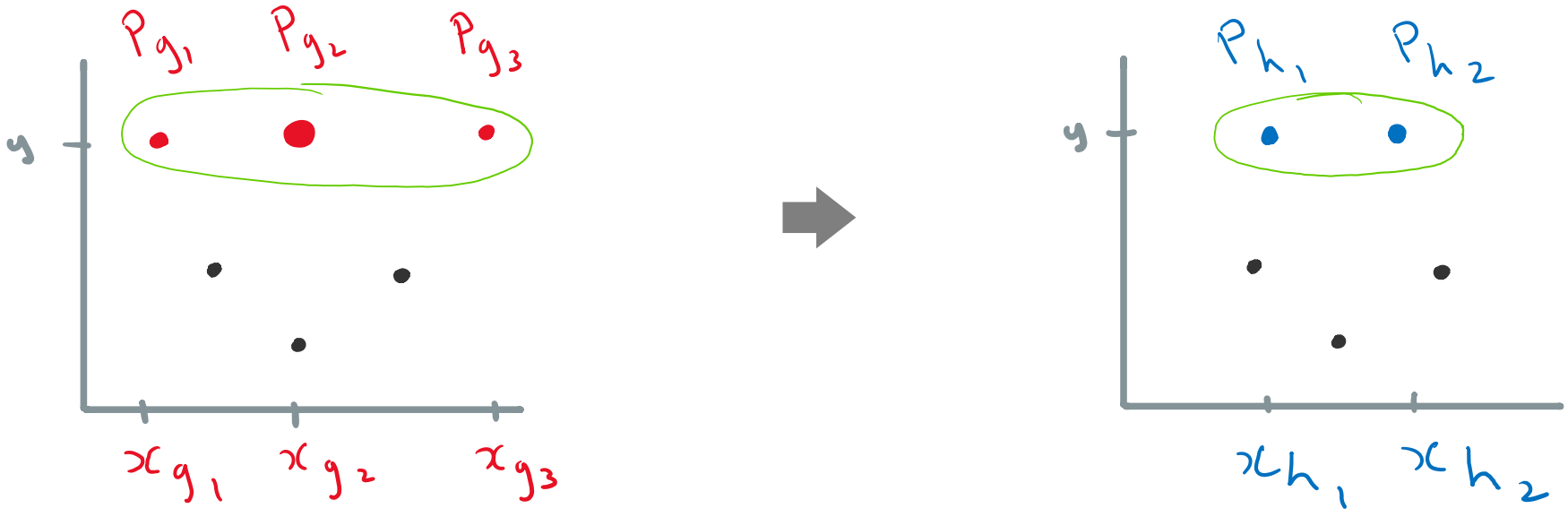
$$\frac{1}{x_g} \geq \left\langle \frac{1}{x_h} \right\rangle$$



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

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

Kitaev's Frameworks | TDPG | Rule



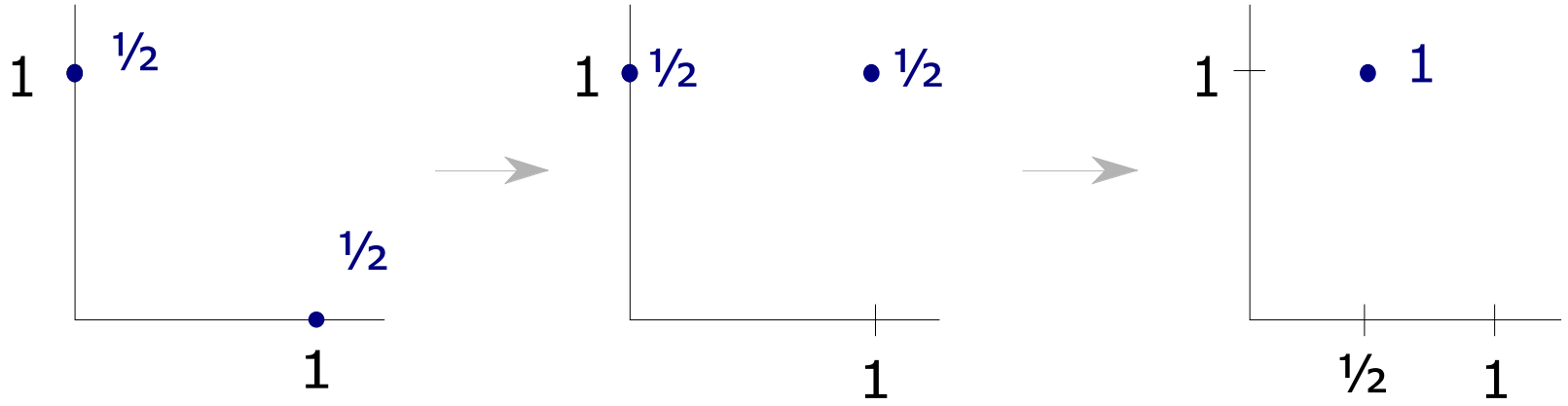
Consecutive frames: along a line, for all $\lambda \geq 0$

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

Kitaev's Frameworks | 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's Frameworks | TDPG | Example

Merge $(n_g \to 1)$:

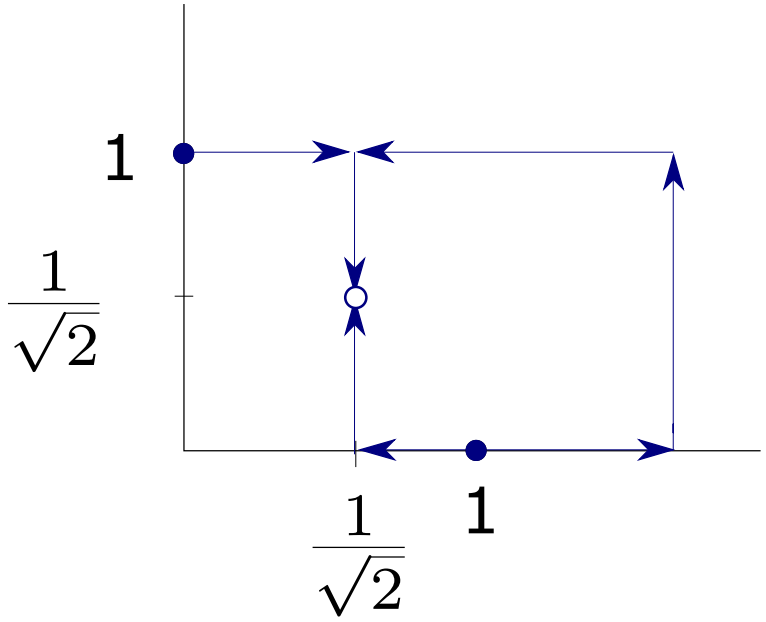
$$\langle x_g \rangle \leq x_h$$

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's Frameworks | TDPG | Example

Merge $(n_g \to 1)$:

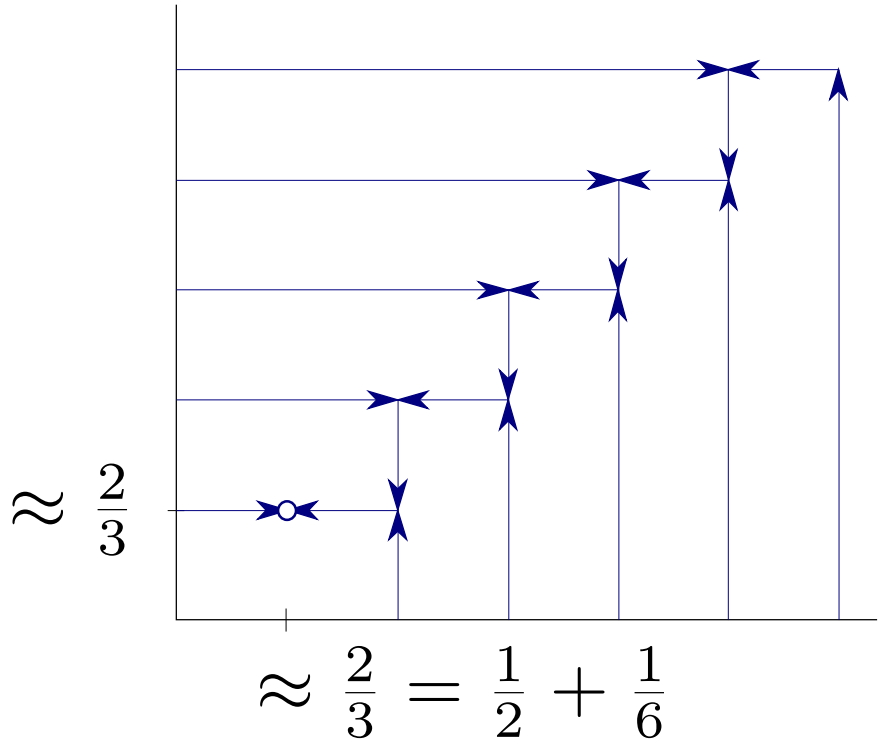
$$\langle x_g \rangle \leq x_h$$

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:
Dip Dip Boom (Mochon, PRA 2005)

Kitaev's Frameworks | 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.

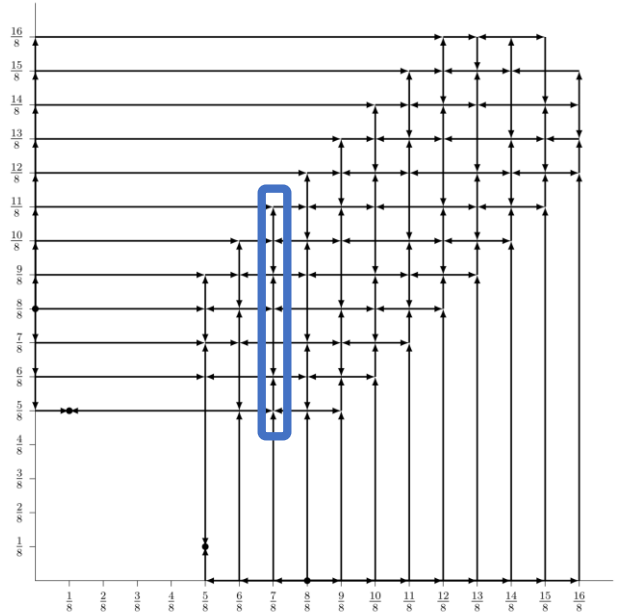


Image taken from E. Pelchat's Master Thesis

Contribution

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

TEF

TDPG to Explicit protocol Framework (TEF):

A TDPG $\rightarrow$ 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.

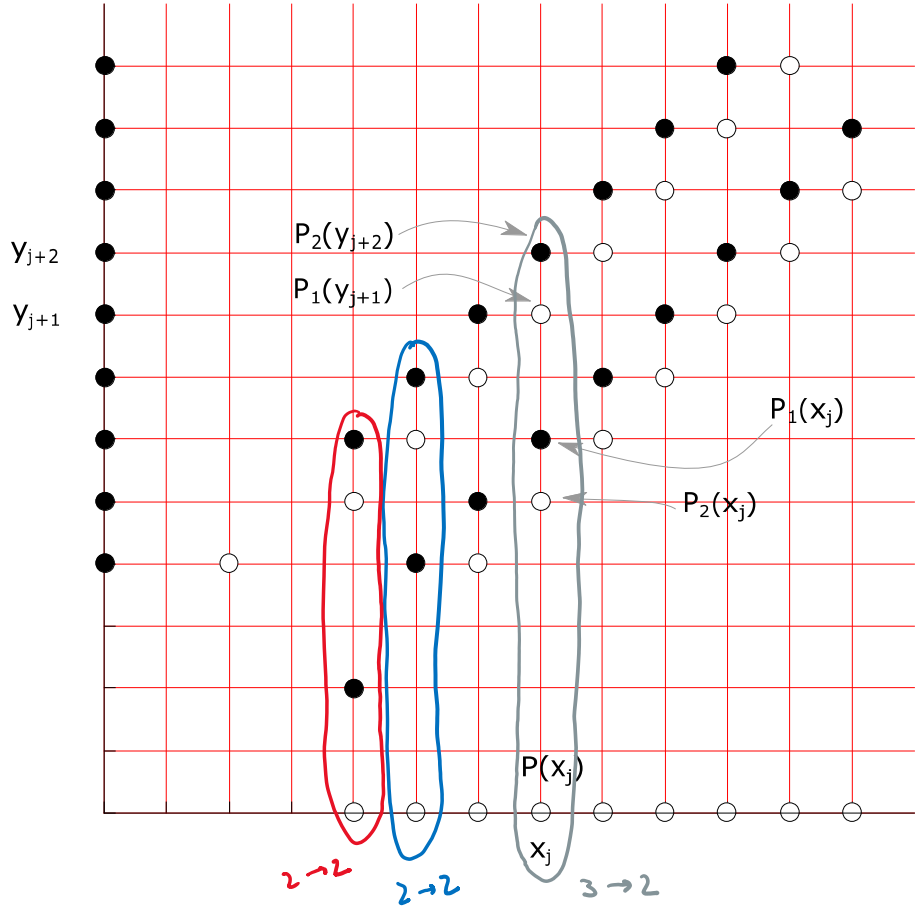
TEF | 1/10 Explicit

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.

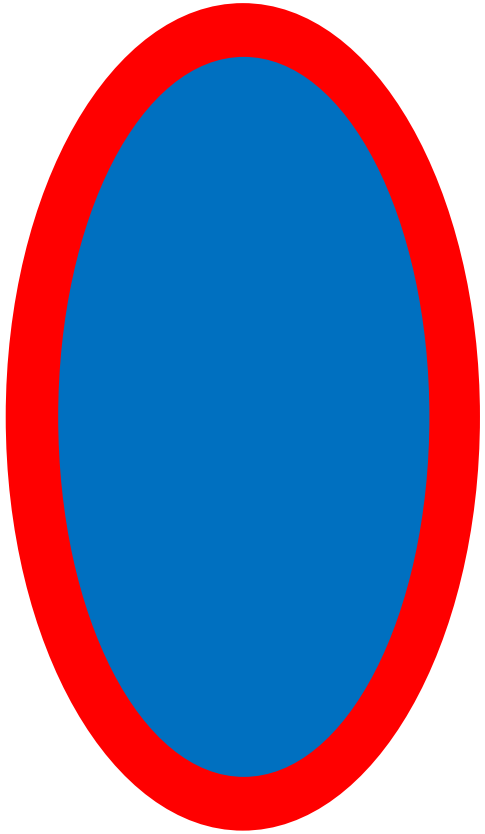
$$X_h \geq U X_g U^\dagger$$

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



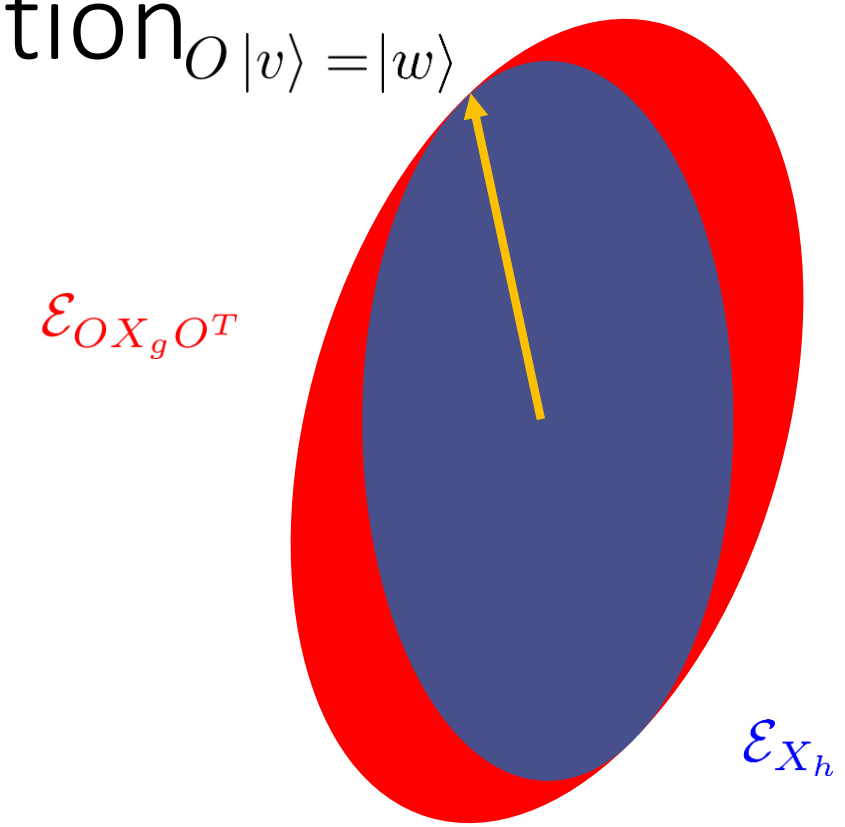
- Restrict to reals: $U \to O$.
- For X diagonal

$$\mathcal{E}_X = \{|u\rangle \,|\, \langle u| X |u\rangle = 1\}$$

  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).

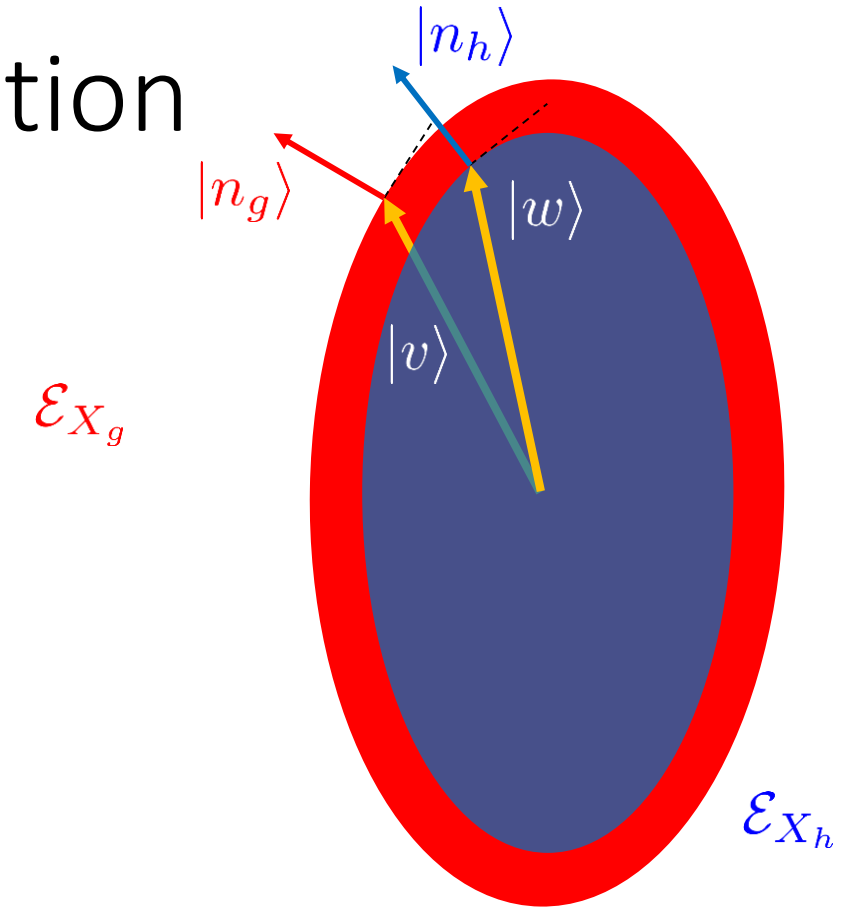
EMA | Elliptic Representation

- Imagine: Solution O is known, viz.
  - $O\,|v\rangle = |w\rangle\,.$
  - $X_h \geq O X_g O^T.$
- 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.
  - $O\,|v\rangle = |w\rangle\,.$
  - $X_h \geq O X_g O^T.$
- 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]	$\epsilon \to \frac{1}{\sqrt{2}} - \frac{1}{2}$ [Chailloux Kerenidis 09]
Weak CF	$\epsilon \to 0$ [Mochon 07] [Aharonov et al 16]	$\epsilon \to \frac{1}{10}$ (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

https://the-dots.com/projects/stephan-schmitz-207570

?

arXiv:1811.02984

Thank you

The work was funded by 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 ε. 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†

EMA | Big Picture

Best Strategy (SDP) $\xrightarrow{\text{Dual}}$ **(SDP)** $\xrightarrow{\text{Kitaev}^\dagger}$ **TDPG**

Constraint: Honest player follows the protocol

$$\rho_f = \mathrm{tr}(U\rho_i U^\dagger)$$

Constraint: Matrix inequality

$$\underbrace{Z_f}_{H} \geq \underbrace{(UZ_iU^\dagger)}_{G}$$

frame

=Measurement outcome of $Z_A \otimes Z_B$ with prob. given by $|\psi\rangle$

$= \mathrm{Prob}[Z_A \otimes Z_B, |\psi\rangle]$

Constraint: (*)

† Combine the dual SDP with the "honest state" or primal variable to get rid of the extra basis information.

Same idea behind his bound on Strong CF.

EMA | Big Picture (cont.)

(*) Expressible By Matrices (EBM)

$H \geq G, |\psi\rangle$ s.t.

$\text{Prob}[G, |\psi\rangle] \rightarrow \text{Prob}[H, |\psi\rangle]$

Operator monotone function

f s.t.

$\forall\ H \geq G, f(H) \geq f(G)$

Valid functions

$\sum_{\text{final}} \frac{\lambda z}{\lambda + z} p_z \geq \sum_{\text{init}} \frac{\lambda z}{\lambda + z} p_z$

K : cone of EBM

$\overset{\text{Dual}}{\rightarrow}$

K^* : cone of Operator Monotones

$\overset{\text{Dual}}{\rightarrow}$

K^{**} : cone of valid functions

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

EMA | EBRM=EBM

Expressible By Real Matrices (EBRM)

$H \geq G, |\psi\rangle$ s.t.

$\text{Prob}[G, |\psi\rangle] \to \text{Prob}[H, |\psi\rangle]$

Operator monotone function

f s.t.

$\forall\ H \geq G, f(H) \geq f(G)$

Valid functions

$\sum_{\text{final}} \frac{\lambda z}{\lambda + z} p_z \geq \sum_{\text{init}} \frac{\lambda z}{\lambda + z} p_z$

K' : cone of EBRM

$\xrightarrow{\text{Dual}}$

K^* : cone of Operator Monotones

$\xrightarrow{\text{Dual}}$

K^{**} : cone of valid functions

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

$$\implies \boxed{K' = K}$$

i.e. we don't need complex numbers for quantum weak coin flipping.

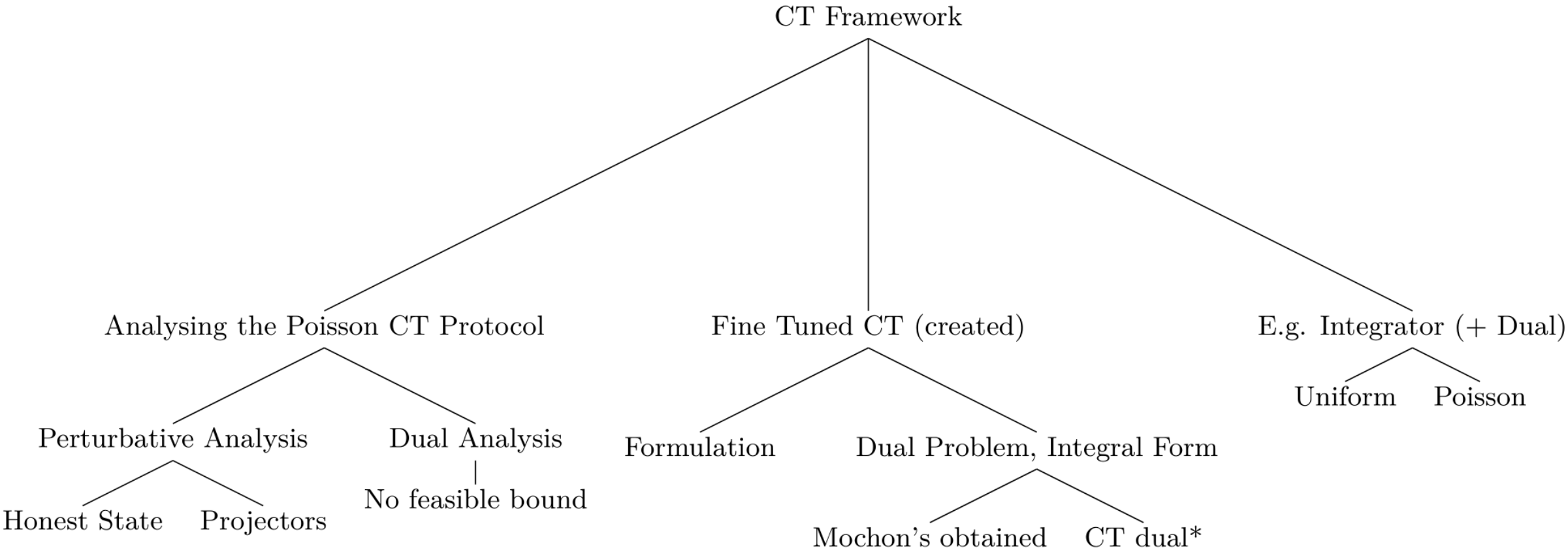


Figure 1: Attempting calculation of bias (performance parameter of the WCF protocols) using the CT framework

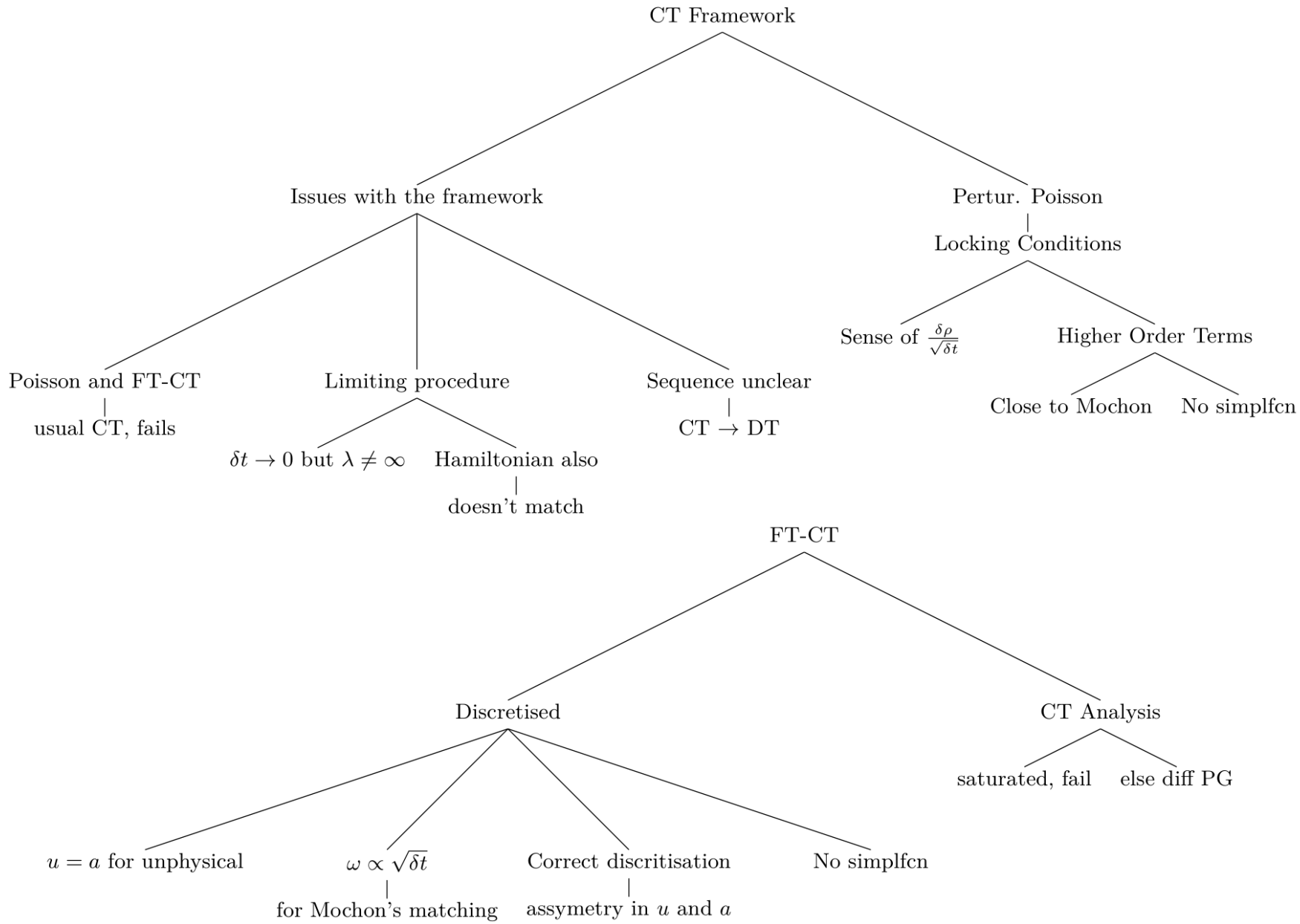


Figure 2: Comparing the difference in approach

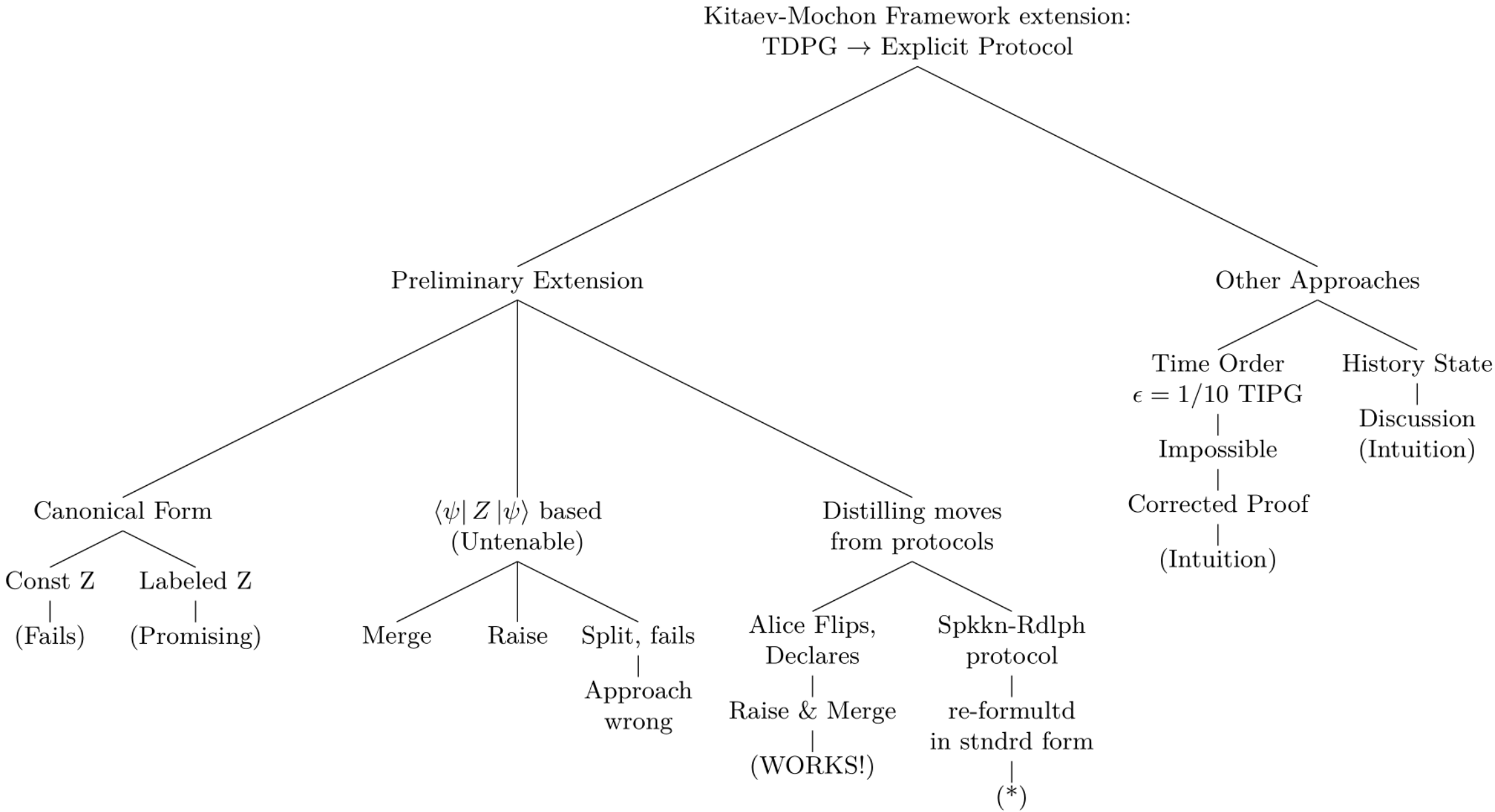


Figure 3: Extending the Kitaev-Mochon Framework to allow TDPG→Explicit Protocol construction

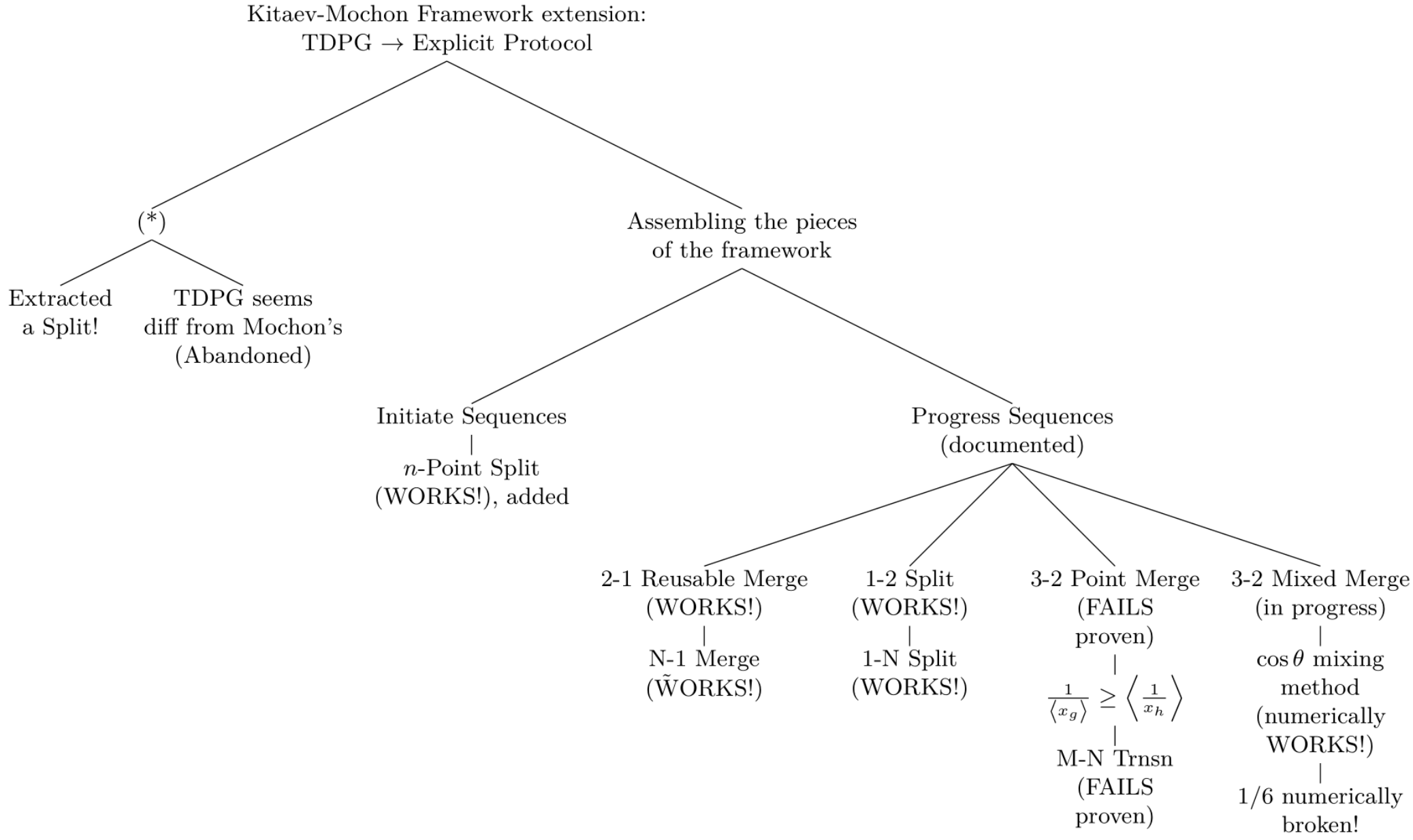


Figure 4: Adding moves to the framework for TDPG→Explicit Protocol construction