

Weak Coin Flipping beyond bias 1/6

Atul Singh Arora

Jeremie Roland

Stephan Weis

Problem Statement

QKD: Two trusting parties protect against adversaries.
Two party secure: Two distrustful parties wish to collaborate.
E.g. MS wants to use IBM's QC.

Coin Flipping (CF): Establish a random bit among two mutually distrustful, physically separated players without a trusted third party.

A, B → friends →  → fight → coin flip to decide

Weak CF: Preferences are known. E.g. A and B both want the car.

Strong CF: Preferences are unknown.

Scenarios: Both honest (easy)
One honest other cheats (non-trivial; bias analysis)
Both cheat (independent of the protocol)

Bias: Smallest ϵ s.t. $\text{prob}(\text{heads}), \text{prob}(\text{tails}) \leq \frac{1}{2} + \epsilon$.

NB: $0 \leq \epsilon \leq \frac{1}{2}$.

Prior Art

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

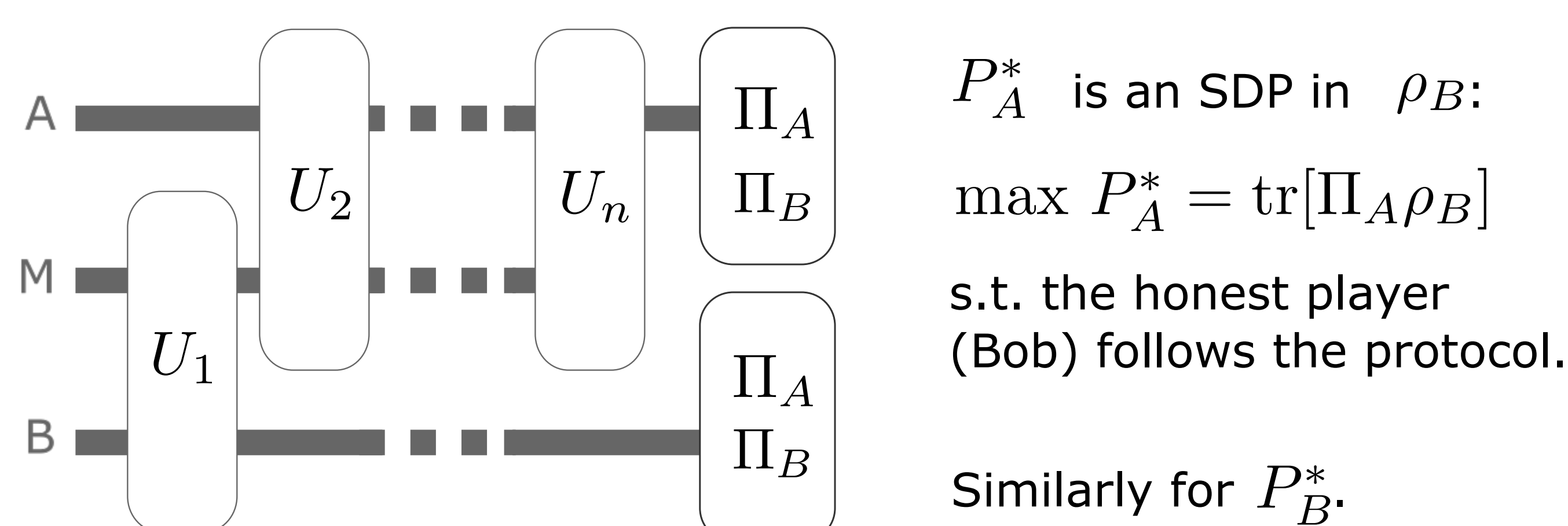
Quantumly: Strong CF: $\epsilon \geq \frac{1}{\sqrt{2}} - \frac{1}{2}$, best known $\epsilon = \frac{1}{4}$.

Weak CF: $\epsilon \rightarrow 0$, best known $\epsilon = \frac{1}{6}$.

Kitaev's Frameworks

e.g. Flip and declare protocol $P_A = P_B = \frac{1}{2}$
 $P_A^* = 1, P_B^* = \frac{1}{2} \implies \epsilon = \frac{1}{2}$.

General Protocol:



Dual: $\rho \leftrightarrow Z$, $\max \leftrightarrow \min$, $P^* = \max \leftrightarrow P^* \leq \text{certificate}$

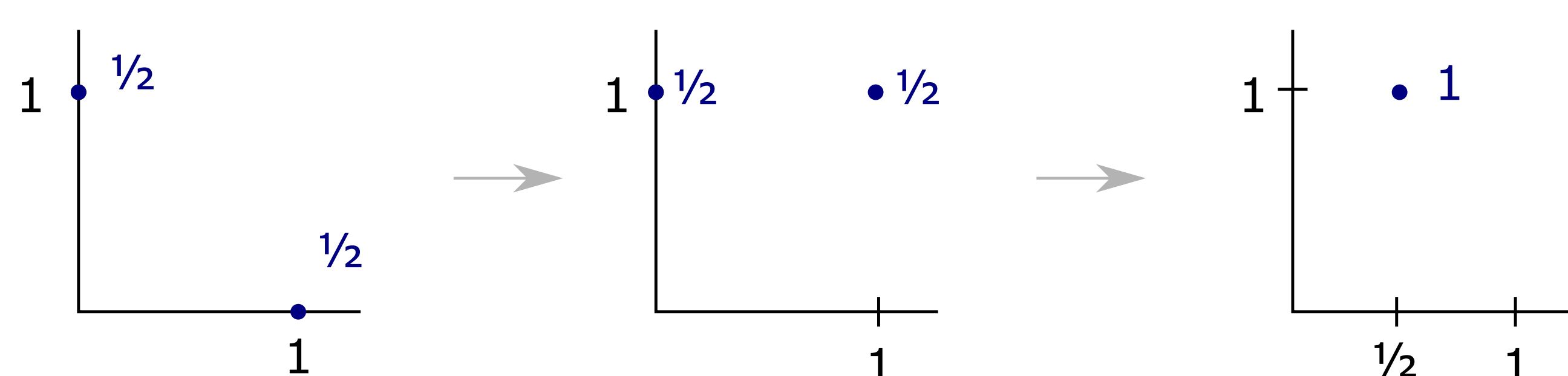
Time Dependent Point Game (TDPG):

Sequence of frames (frame = points on a plane) s.t.

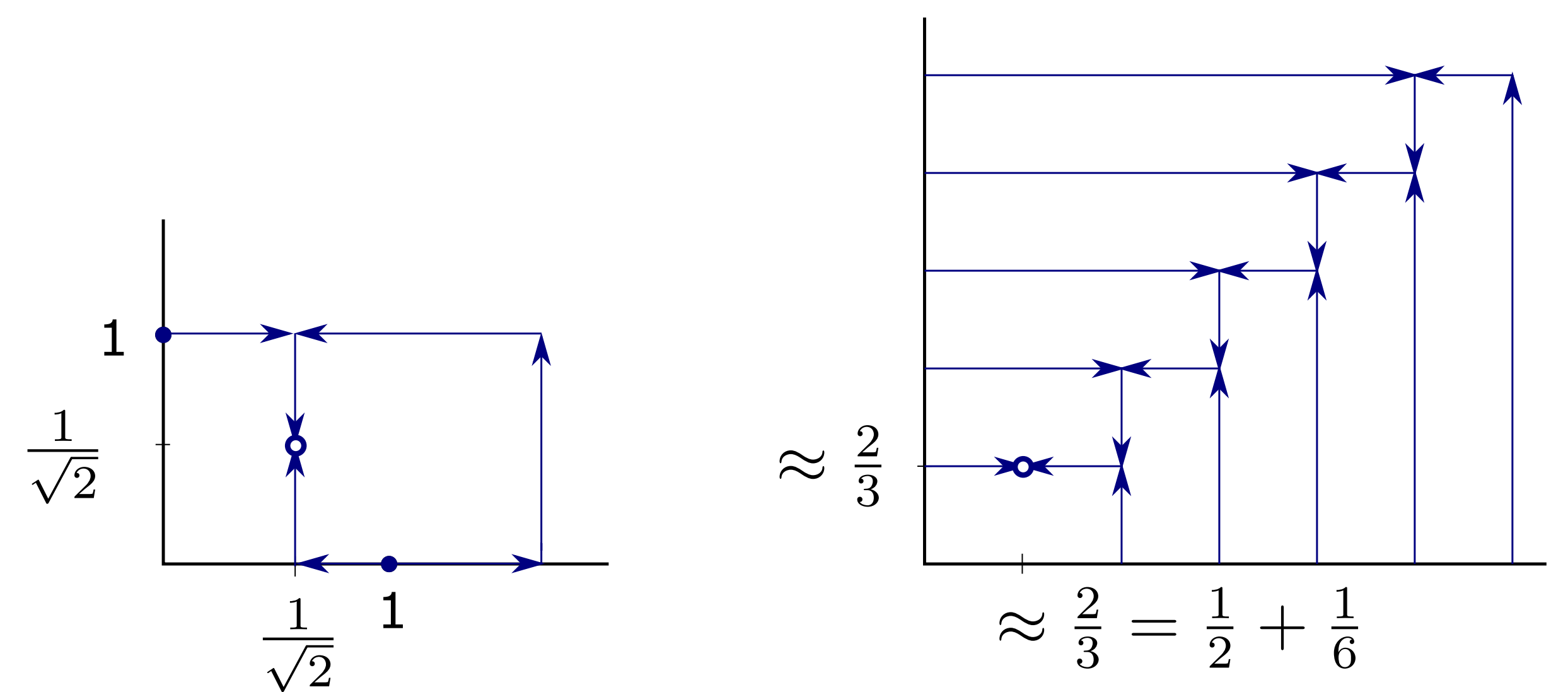
1. Start and end frames are fixed.

2. Consecutive: $\sum_z \frac{\lambda z}{\lambda + z} p_z \leq \sum_z \frac{\lambda z'}{\lambda + z'} p'_z$ along a line.

e.g. merge: weighted average; raise
split: harmonic average $(\forall \lambda \geq 0)$



Protocols Re-expressed



Time Independent Point Game (TIPG):

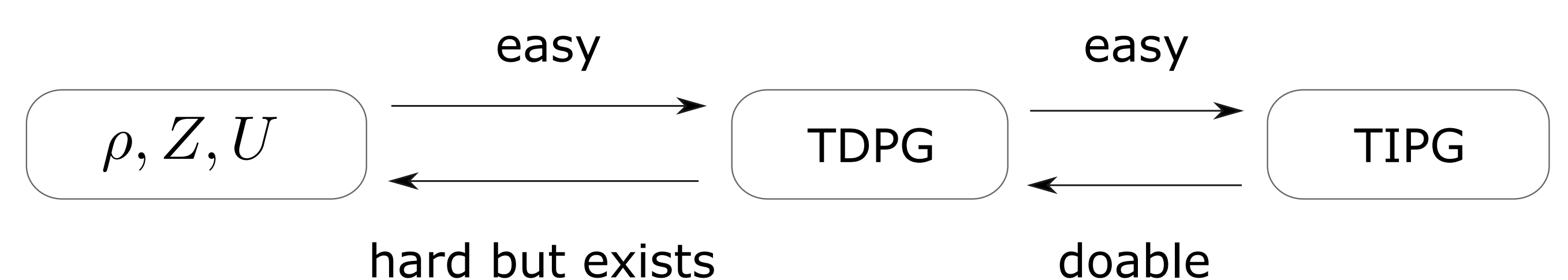
Weight can be negative; $h(x, y), v(x, y)$ s.t.

$h + v = \text{final} - \text{initial frame}$; h, v satisfy a similar eqn.

Mochon's Breakthrough

Family of TIPGs yield $\epsilon = \frac{1}{4k+2}$

$2k = \# \text{ points (non-trivial step)}$.



Contribution

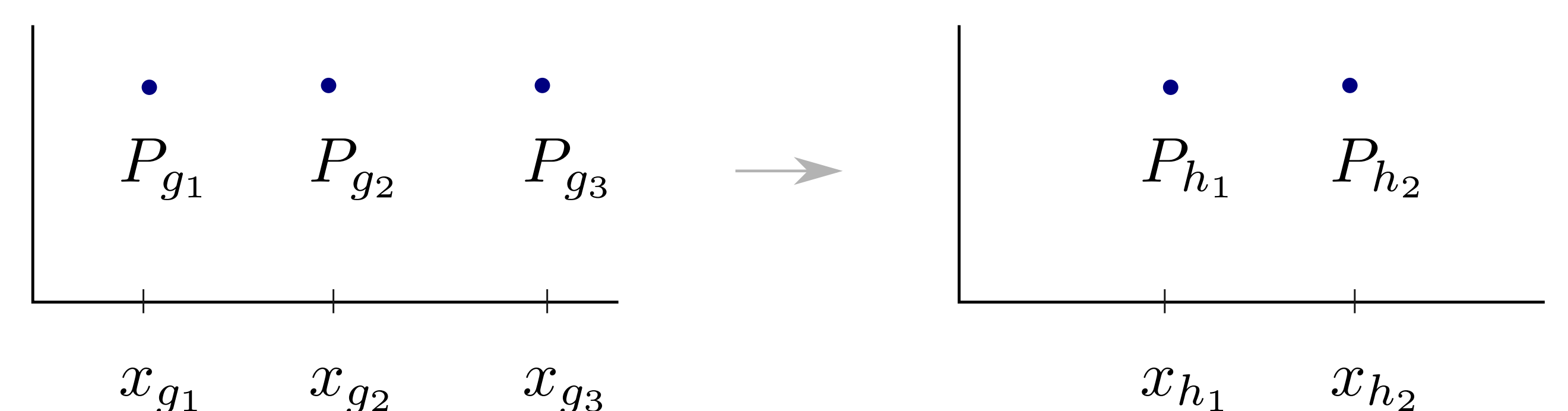
Framework: A TDPG $\rightarrow \rho, Z, U$ if

for each "TDPG move" 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

$$U \sum_{|v\rangle} \sqrt{P_{g_i}} |g_i\rangle = \sum_{|w\rangle} \sqrt{P_{h_i}} |h_i\rangle.$$



E.g.: For the 1/6 protocol, U to implement the following are needed:

(a) split: $1 \rightarrow n$ (b) merge: $n \rightarrow 1$

Claim: $U_{\text{blink}} = |w\rangle \langle v| + |v\rangle \langle w| + 1_{\text{else}}$ can perform both.

E.g.: For the 1/10 protocol, U to implement the following are needed in addition to the split and merge:

(a) $3 \rightarrow 2$ (b) $2 \rightarrow 2$

Claim: $U_{3 \rightarrow 2}$ and $U_{2 \rightarrow 2}$ constructed (not pretty).

NB: Better than the current best.

Future: Construct a systematic scheme for constructing U s.

[References, Affiliation, PDF and related | QR](#)

