Quantum Weak Coin Flipping

Atul Singh Arora
atul.singh.arora@ulb.ac.be
Université libre de Bruxelles
Brussels, Belgium

Jérémie Roland
jroland@ulb.ac.be
Université libre de Bruxelles
Brussels, Belgium

Stephan Weis
maths@weis-stephan.de
Université libre de Bruxelles
Brussels, Belgium

ABSTRACT

We investigate weak coin flipping, a fundamental cryptographic primitive where two distrustful parties need to remotely establish a shared random bit. A cheating player can try to bias the output bit towards a preferred value. For weak coin flipping the players have known opposite preferred values. A weak coin-flipping protocol has a bias ϵ if neither player can force the outcome towards their preferred value with probability more than $\frac{1}{2} + \epsilon$. While it is known that all classical protocols have $\epsilon = \frac{1}{2}$, Mochon showed in 2007 that quantumly weak coin flipping can be achieved with arbitrarily small bias (near perfect) but the former best known explicit protocol has bias 1/6 (also due to Mochon, 2005). We propose a framework to construct new explicit protocols achieving biases below 1/6. In particular, we construct explicit unitaries for protocols with bias down to 1/10. To go lower, we introduce what we call the Elliptic Monotone Align (EMA) algorithm which, together with the framework, allows us to construct protocols with arbitrarily small biases.

CCS CONCEPTS

• **Theory of computation → Cryptographic primitives**; **Cryptographic protocols**; *Quantum information theory*;

KEYWORDS

cryptographic primitive, two party secure, quantum cryptography, quantum information

ACM Reference Format:
Atul Singh Arora, Jérémie Roland, and Stephan Weis. 2019. Quantum Weak Coin Flipping. In *Proceedings of the 51st Annual ACM SIGACT Symposium on the Theory of Computing (STOC '19), June 23–26, 2019, Phoenix, AZ, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3313276.3316306

1 INTRODUCTION

Coin flipping is a fundamental cryptographic primitive wherein two distrustful and remote players wish to generate a shared unbiased random bit through an exchange of messages, without involving a third party. The primitive must prevent the outcome from being biased towards any specific value when an honest player plays against a cheating adversary. For weak coin flipping (WCF), the players have known opposite preferences. A WCF protocol has bias ϵ if it is the smallest number such that neither player can force their desired outcome with probability more than $\frac{1}{2} + \epsilon$. For strong coin-flipping there are no a priori preferred values and the bias is defined similarly. Restricting to classical resources, neither weak nor strong coin flipping is possible under information-theoretic security, as there always exists a player [7] who can force any outcome with probability 1. However, in a quantum world, strong coin flipping protocols with bias strictly less than $\frac{1}{2}$ have been found and the best known explicit protocol has bias $\frac{1}{4}$ [3]. Nevertheless, Kitaev showed a lower bound of $\frac{1}{\sqrt{2}} - \frac{1}{2}$ for the bias of any quantum strong coin flipping, so an unbiased protocol is not possible.

As for weak coin flipping, the former best known explicit protocol—the Dip Dip Boom protocol—is due to Mochon [11] and has bias 1/6. In a breakthrough result, he even proved the existence of a quantum weak coin-flipping protocol with arbitrarily low bias $\epsilon > 0$, hence showing that near-perfect weak coin flipping is theoretically possible [12]. This fundamental result for quantum cryptography, unfortunately, was proved non-constructively, by elaborate successive reductions (80 pages) of the protocol to different versions of so-called point games, a formalism introduced by Kitaev [10] in order to study coin flipping. Consequently, the description of the protocol whose existence is proved is lost. A systematic verification of this by independent researchers recently led to a simplified proof [2] (*only* 50 pages) but eleven years later, an explicit weak coin-flipping protocol is still unknown, despite various expert approaches ranging from the distillation of a protocol using the proof of existence to numerical search [14, 15]. Further, weak coin flipping provides, via black-box reductions, optimal protocols for strong coin flipping [5], bit commitment [6] and a variant of oblivious transfer [4] (fundamental cryptographic primitives). It is also used to implement other cryptographic tasks such as leader election [8] and dice rolling [1].

We construct a framework that allows us to convert simple point games (i.e. corresponding to known protocols) into explicit quantum protocols defined in terms of unitaries and projectors. We use the said framework to convert Mochon's bias 1/10 point game into its corresponding explicit protocol finally improving upon Mochon's Dip Dip Boom protocol (bias 1/6; see [11]).

Our second contribution, the Elliptic Monotone Align (EMA) algorithm, can provably find the unitaries required for implementing protocols with arbitrary biases, including the ones with $\epsilon \to 0$.

Many proofs have been omitted from this extended abstract and can be found in the full version of the paper.

STOC '19, June 23–26, 2019, Phoenix, AZ, USA

ACM ISBN 978-1-4503-6705-9/19/06…$15.00
https://doi.org/10.1145/3313276.3316306

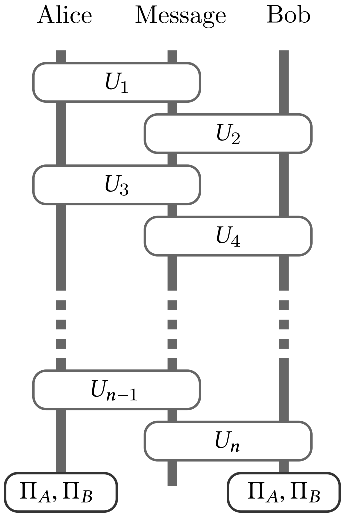

Figure 1: Every Weak Coin Flipping protocol can be expressed in this general form.

2 KITAEV'S FORMALISMS AND MOCHON'S GAMES | STATE OF THE ART

Let us start with noting two features of weak coin flipping. First, we say a player wins if they get their preferred value. This makes sense, as the players have opposite preferred values. Second, we note that there are four situations which can arise in a weak coin flipping scenario of which three are of interest. Let us denote by HH the situation where both Alice and Bob are honest, i.e. follow the protocol. In this situation we want the protocol to be such that both Alice and Bob (a) win with equal probability and (b) are in agreement with each other. In the situation HC where Alice is honest and Bob is cheating, the protocol must protect Alice from a cheating Bob. In this situation, a cheating Bob tries to convince an honest Alice that he has won. The probability that Bob wins using his best cheating strategy is denoted by P_B^* where the subscript identifies the cheating player, Bob in this case. The CH situation where Bob is honest and Alice is cheating naturally points us to the corresponding definition of P_A^*. The situation CC where both players are cheating will not be of interest to us as nothing can be said which depends on the protocol. This is because nobody is following the protocol.

A trivial example of a weak coin flipping protocol is where Alice flips a coin and reveals the outcome to Bob over the phone. A cheating Alice can simply lie and always win against an honest Bob which means $P_A^* = 1$. On the other hand, a cheating Bob can not do anything to convince Alice that he has won, unless it happens by random chance on the coin flip. This corresponds to $P_B^* = \frac{1}{2}$. The bias of the protocol is $\max[P_A^*, P_B^*] - \frac{1}{2}$ which for this naïve protocol amounts to $\frac{1}{2}$, the worst possible. Manifestly, constructing protocols where one player is protected is nearly trivial. Constructing protocols where neither player is able to cheat (against an honest player) is the real challenge.

Given a WCF protocol it is not a priori clear how the best success probability of a cheating player, denoted by $P_{A/B}^*$, should be computed as the strategy space can be dauntingly large. It turns out that all quantum WCF protocols can be defined using the exchange of a message register interleaved with the players applying the unitaries U_i locally (see Figure 1) until a final measurement, say Π_A denoting Alice won and Π_B denoting Bob won, is made in the end. The state at each step is called the *honest state*, and is denoted by $|\psi_i\rangle$, when both players follow the protocol. Hence, every WCF protocol is specified by the initial state $|\psi_0\rangle$ and the operators $\{U_i\}, \Pi_A, \Pi_B$. Computing the cheating probability P_A^* reduces to the semi-definite program (SDP) of maximizing the objective functional $\mathrm{tr}(\Pi_A \rho)$ over the final state ρ of Bob's system, subject to the constraint that Bob is honest (follows the protocol). An analogous SDP can be written for computing P_B^*. Using SDP duality one can turn this maximization problem over cheating strategies into a minimization problem over dual variables $Z_{A/B}$. Any dual feasible assignment then provides an upper bound on the cheating probabilities $P_{A/B}^*$. SDPs are usually easy to handle but in this case, there are two SDPs, and we must optimise both simultaneously (see Section 1 of [2]). Note that here we assume the protocol is known and we are trying to find bounds on P_A^* and P_B^*. However, our goal was to find good protocols. So what we would like is a formalism which allows us to do both, construct protocols and find the associated P_A^* and P_B^*. Kitaev and Mochon defined a formalism, which distils out the relevant mathematical structure and can be used to prove the *existence* of protocols together with upper bounds on P_A^* and P_B^*, bringing us significantly closer to the final goal of constructing good protocols.

Kitaev converted this problem about matrices (Zs, ρs and Us) into a problem about points on a plane, which Mochon called Kitaev's Time Dependent Point Game (TDPG) formalism.

Definition 1 (TDPG)**.** A *frame* is a probability distribution on the non-negative quadrant of the plane supported at finitely many points. A *Time Dependent Point Game (TDPG)* is a sequence of frames of which the first frame is the uniform distribution on the points $[0, 1]$ and $[1, 0]$ and the last frame consists of a single point $[\beta, \alpha]$ (with weight 1). All pairs of consecutive frames, *transitions*, obey the following rules.

Only points along a line (either horizontal or vertical) can change. Consider a given frame and focus on a set of points that fall on this vertical (or horizontal) line. Let the y coordinate (or x coordinate) of the ith point be given by z_{g_i} and the weight be given by p_{g_i}. Let z_{h_i} and p_{h_i} denote the corresponding quantity in the subsequent frame. Then, the following conditions must hold

(1) the probabilities are conserved, viz. $\sum_i p_{g_i} = \sum_i p_{h_i}$
(2) for all $\lambda > 0$

$$\sum_i \frac{\lambda z_{g_i}}{\lambda + z_{g_i}} p_{g_i} \leq \sum_i \frac{\lambda z_{h_i}}{\lambda + z_{h_i}} p_{h_i}. \tag{1}$$

More precisely, Kitaev showed that for all $\alpha, \beta > 0$ the existence of a WCF protocol together with its dual variables $\{Z_i\}$ certifying $P_A^* \leq \alpha, P_B^* \leq \beta$ is equivalent to the existence of a TDPG with final point $[\beta, \alpha]$ (see Theorem 4 and 5 of [2]). The objective of the protocol designer therefore is to get this end point as close to the origin as possible by transitioning through intermediate frames (see Figure 2) while obeying the aforementioned rules. These rule and

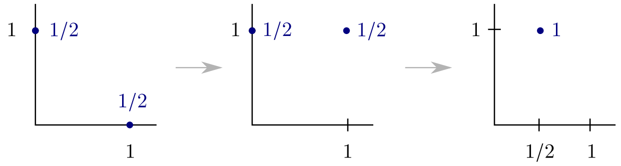

Figure 2: Point game corresponding to the Weak Coin Flipping over the phone protocol.

the points in the frames, in fact, arise from the dual SDP variables $Z_{A/B}$. Just as the state ρ evolves through the protocol, so do the dual variables $Z_{A/B}$. The points and their weights in the TDPG are exactly the eigenvalue pairs of $Z_{A/B}$ with the probability weight assigned to them by the honest state $|\psi\rangle$ at a given point in the protocol. Given an explicit WCF protocol and a feasible assignment for the dual variables witnessing a given bias, it is straightforward to construct the TDPG. However, going backwards, constructing the WCF dual from a TDPG is non-trivial and no general construction was known.

Our main contribution is precisely to this part. We construct a framework which allows for a ready conversion of simple TDPGs into explicit protocols, and once supplemented with the EMA algorithm, it can convert any TDPG into its corresponding protocol. Mochon's breakthrough result was to define a family of games[1] with bias $\epsilon = \frac{1}{4k+2}$ (see Section 5 of either [2, 12]). Here k encodes the number of points that are involved in the non-trivial step (for $k = 1$ it reduces to a version of the Dip Dip Boom (bias 1/6) protocol). Combining this family of point games with the our results—the framework and the EMA algorithm—one can (algorithmically) construct quantum weak coin flipping protocols with arbitrarily small biases.

As this point game formalism is the cornerstone of the analysis, we simplify the rules further and then apply them to construct a simple example game. Later, we convert this example game into an explicit protocol using our framework. If we restrict ourselves to transitions involving only one initial and one final point, the second condition reduces to $z_g \leq z_h$ (we suppressed the subscript). This is called a *raise*. It means that we can always increase the coordinate of a single point. What about going from one initial point to many final points (note that the points before and after must lie along either a horizontal or a vertical line)? The second condition in this case becomes $1/z_g \geq \langle 1/z_h \rangle$, that is the harmonic mean of the final points must be greater than or equal to that of the initial point, where $\langle f(z_h) \rangle := \left(\sum_i f(z_{h_i}) p_{h_i}\right) / \left(\sum_j p_{h_j}\right)$. This is called a *split*. Finally, we can ask: What happens upon merging many points into a single point? The second condition becomes $\left\langle z_g \right\rangle \leq z_h$, that is the final position must not be smaller than the average initial position (where $\left\langle f(z_g) \right\rangle$ is analogously defined). This is called a *merge*. While these three transitions/moves do not exhaust the set of moves, they are enough to construct games that almost achieve the bias 1/6. Let us construct a simple game as an example. We start with the initial frame and raise the point [1, 0] along the vertical to [1, 1] (see Figure 2). We know this move is allowed as it is just a raise. Next we merge the points [0, 1] with [1, 1] using a horizontal merge. The x-coordinate of the resulting point can at best be $\frac{1}{2}.0 + \frac{1}{2}.1 = \frac{1}{2}$ where we used the fact that both points have weight 1/2. Thus we end up with a single point at $[\frac{1}{2}, 1]$ with all the weight. Kitaev's formalism tells us that there must exist a protocol which yields $P_A^* = 1$ while $P_B^* = \frac{1}{2}$. This, however, is the phone protocol that we started our discussion with! It is a neat consistency check but it yields a trivial bias. This is because we did not use the split. If we use a split once, we can already obtain a game with $P_A^* = P_B^* = \frac{1}{\sqrt{2}}$ by appropriately matching the weights (see Section 3.2.1 of [12]). Protocols corresponding to this bias were found by various researchers [9, 13, 18] long before this formalism was known. In fact, the bias of the said weak coin flipping protocols, $\epsilon = \frac{1}{\sqrt{2}} - \frac{1}{2}$, is exactly the lower bound for *strong* coin flipping. The technique used to bound strong coin flipping fails for weak coin flipping and the matter was not resolved for a while. These protocols held the record for being the best known weak coin flipping protocols until Mochon progressively showed that if we use multiple splits wisely at the beginning followed by a raise, one simply needs to use merges thereafter to obtain a game with bias approaching 1/6, which corresponds to his Dip Dip Boom protocol. The Dip Dip Boom protocol is actually a family of protocols which in the limit of infinite rounds of communication yields bias 1/6. Going lower, therefore, is not a straight forward extension and we need to use moves which can not be decomposed into the three basic ones: splits, merges and raises.

3 A FRAMEWORK | FIRST CONTRIBUTION

We first describe our framework for converting a TDPG into an explicit protocol. We start by defining a 'canonical form' for any given frame of a TDPG. This allows one to write the WCF dual variables, Zs, and the honest state $|\psi\rangle$ associated with each frame of the TDPG (see Definition 4). We define a sequence of quantum operations, unitaries and projections, which allow Alice and Bob to transition from the initial frame to the final frame. It turns out that there is only one non-trivial quantum operation in the sequence which we leave partially specified for the moment. This means that we know that the unitary should send the honest initial state to the honest final state. However the action of the unitary on the orthogonal space, which intuitively is what would bestow on it the cheating prevention/detection capability, is obtained as a non-trivial constraint. Using the SDP formalism we write the constraints at each step of the sequence on the Zs and show that they are indeed satisfied (see Subsection A.1 for details).

Theorem 2 (TEF constraint (simplified)). *If a unitary matrix U acting on the space span$\{|g_1\rangle, |g_2\rangle \ldots, |h_1\rangle, |h_2\rangle \ldots\}$ satisfying the constraints*

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

$$\sum_i x_{h_i} |h_i\rangle \langle h_i| - \sum_i x_{g_i} E_h U |g_i\rangle \langle g_i| U^\dagger E_h \geq 0 \qquad (2)$$

can be found for every move/transition of a TDPG then an explicit protocol with the corresponding bias can be obtained using the

[1] Mochon describes his games in Kitaev's *Time Independent Point Game (TIPG)* formalism but it is straightforward to go back from a TIPG to a TDPG.

TDPG–to–Explicit–protocol Framework (TEF), where $\{|g_i\rangle\}$, $\{|h_i\rangle\}$ are orthonormal vectors and if the transition is horizontal

- *the initial points have x_{g_i} as their x-coordinate and p_{g_i} as their corresponding probability weight,*
- *the final points have, similarly, x_{h_i} as their x-coordinate and p_{h_i} as their corresponding probability weight*
- *E_h is a projection onto the span $\{|h_i\rangle\}$ space,*
- *$|v\rangle = \sum_i \sqrt{p_{g_i}}\,|g_i\rangle \,/\sqrt{\sum_j p_{g_j}}$, $|w\rangle = \sum_i \sqrt{p_{h_i}}\,|h_i\rangle\,/\sqrt{\sum_j p_{h_j}}$*

and if the transition is vertical, the x_{g_i} and x_{h_i} become the y-coordinates y_{g_i} and y_{h_i} with everything else unchanged.

Note that the TDPG already specifies the coordinates x_{h_i}, x_{g_i} and the probabilities p_{h_i}, p_{g_i} which satisfy, Equation (1), the scalar condition. Our task therefore reduces to finding the correct U which satisfies the aforesaid matrix constraints. It is this general problem that is solved by our EMA algorithm which we describe later.

Given such a unitary U acting on the space span$\{|g_1\rangle, |g_2\rangle \dots |h_1\rangle, |h_2\rangle \dots\}$ one can construct a unitary, $U^{(2)}_{AM}$, acting non-trivially on the space span$\{|g_1g_1\rangle_{AM}, |g_2g_2\rangle_{AM} \dots, |h_1h_1\rangle_{AM}, |h_2h_2\rangle_{AM}, \dots\}$ by mapping $|g_i\rangle \to |g_ig_i\rangle_{AM}$, $|h_i\rangle \to |h_ih_i\rangle_{AM}$ and as identity otherwise. We now informally describe how to convert a TDPG into an explicit protocol. It suffices to show what a transition from a given frame to the next frame corresponds to in terms of the protocol. In this discussion, we refer to them as the initial frame and the final frame. Assume that the corresponding non-trivial $U^{(2)}_{AM}$ is known. As we saw, a given transition would either be horizontal or vertical. We assume it is horizontal without loss of generality[2]. We label the points that do not participate in this horizontal transition, i.e. remain unchanged in both frames, by $k_1, k_2 \dots$ in both frames. The points in the initial frame involved in this transition are labelled $g_1, g_2 \dots$ and the ones in the final frame are labelled $h_1, h_2 \dots$. All the points are now labelled. We denote the coordinates of the final points by $x_{h_1}, x_{h_2} \dots$ and the probability weights by $p_{h_1}, p_{h_2} \dots$. We similarly define x_{g_i}, p_{g_i} and x_{k_i}, p_{k_i}. The Hilbert space of interest is given by $\mathcal{H} :=$ span$\{|k_1\rangle, |k_2\rangle \dots, |g_1\rangle, |g_2\rangle \dots, |h_1\rangle, |h_2\rangle \dots, |m\rangle\}$ where each vector is assumed orthonormal ($|m\rangle$ is just an idle state in which the message register is assumed to be initially and returned to finally). We assume that Alice's register, Bob's register and the message register each have dimension at least as large as $\dim(\mathcal{H})$. The state (by state in this discussion, we mean the honest state) corresponding to the initial frame is assumed to have the form

$$\left|\psi_{(1)}\right\rangle = \left(\sum_i \sqrt{p_{g_i}}\,|g_ig_i\rangle_{AB} + \sum_i \sqrt{p_{k_i}}\,|k_ik_i\rangle_{AB}\right) \otimes |m\rangle_M .$$

Bob: Assume Bob has the message register. He applies the conditional swap $U^{\mathrm{SWP}\{\vec{g},m\}}_{BM}$ where $U^{\mathrm{SWP}\{\vec{g},m\}}_{BM}$ swaps conditionally on both registers being in the subspace span$\{|g_1\rangle, |g_2\rangle \dots, |m\rangle\}$. The state after this operation is

$$\left|\psi_{(2)}\right\rangle = \sum_i \sqrt{p_{g_i}}\,|g_ig_i\rangle_{AM} \otimes |m\rangle_B + \sum_i \sqrt{p_{k_i}}\,|k_ik_i\rangle_{AB} \otimes |m\rangle_M .$$

He then sends the message register to Alice.

Alice: Alice applies the non-trivial unitary $U^{(2)}_{AM}$ on her local register and the message register. She then measures $\{E^{(2)}, \mathbb{I} - E^{(2)}\}$ where $E^{(2)} := (\sum |h_i\rangle\langle h_i| + \sum |k_i\rangle\langle k_i|)_A \otimes \mathbb{I}_M$. The state at this point is

$$\left|\psi_{(3)}\right\rangle = \sum_i \sqrt{p_{h_i}}\,|h_ih_i\rangle_{AM} \otimes |m\rangle_B + \sum_i \sqrt{p_{k_i}}\,|k_ik_i\rangle_{AB} \otimes |m\rangle_M .$$

If the outcome corresponds to the latter, she declares herself to be the winner. Otherwise she sends the message register back to Bob.

Bob: Bob again applies a conditional swap $U^{\mathrm{SWP}\{\vec{h},m\}}_{BM}$ followed by a measurement corresponding to $\{E^{(3)}, \mathbb{I} - E^{(3)}\}$ where $E^{(3)} := (\sum_i |h_i\rangle\langle h_i| + \sum_i |k_i\rangle\langle k_i|)_B \otimes \mathbb{I}_M$. The final state is

$$\left|\psi_{(4)}\right\rangle = \left(\sum_i \sqrt{p_{h_i}}\,|h_ih_i\rangle_{AB} + \sum_i \sqrt{p_{k_i}}\,|k_ik_i\rangle_{AB}\right) \otimes |m\rangle_M .$$

If the outcome corresponds to $\mathbb{I} - E^{(3)}$, Bob declares himself the winner.

As the final state is in the same form as the initial state, one can progressively build the sequence corresponding to the complete protocol. Once the entire sequence is known, one must reverse the order of all the operations to obtain the final protocol. Note that the message register is initially decoupled, it then gets entangled, and finally it emerges decoupled again. This simplifies the analysis (and also entails that one need not keep the message register coherent for the duration of the protocol; keeping it coherent for each round individually is sufficient).

Let us try to apply this procedure to our example game (see Figure 2). We label the points in the first frame as g_1 and g_2. The state is given by $\frac{1}{\sqrt{2}}\left(|g_1g_1\rangle_{AB} + |g_2g_2\rangle_{AB}\right) \otimes |m\rangle_M$. (This should make it clear that the order is reversed here because we want to end with an EPR like state so that when Alice and Bob make a measurement, they agree on a random bit.) We simply claim for the moment that raising does not require Alice and Bob to do anything. This means that we can consider the second frame with the same labels. We now apply the merge transition by using the aforesaid recipe, where Bob applies a swap, sends the message register to Alice, she applies $U^{(2)}_{AM}$ and the projector, returns the message register to Bob and he applies the final swap and measurement. We continue to assume we are given the correct $U^{(2)}_{AM}$ that implements the merge step. The state one obtains after the application of these unitaries turns out to be $|h_1h_2\rangle_{AB} \otimes |m\rangle_M$. (This looks like the state we should start with, completely unentangled. This is intuitively why the actual protocol is a reversed version of what we have.) Our procedure can be applied to any point game, granted the non-trivial unitary $U^{(2)}$ can be found. The central issue was that there was no general recipe known for constructing $U^{(2)}$s.

To address this we can prove that what we call the Blinkered Unitary satisfies the required constraints for both the split and merge moves (see Subsection A.2). It is defined as

$$U_{\text{blink}} = |w\rangle\langle v| + |v\rangle\langle w| + \sum_i |v_i\rangle\langle v_i| + \sum_i |w_i\rangle\langle w_i| \qquad (3)$$

where $|v\rangle$, $\{|v_i\rangle\}$ and $|w\rangle$, $\{|w_i\rangle\}$ are orthonormal vectors spanning the $\{|g_i\rangle\}$ and $\{|h_i\rangle\}$ space respectively. With these the former

[2] Mochon's point games have a repeating structure he calls a "ladder". Corresponding to each k he constructs a family of point games parametrised by the number of points in this ladder. The game approaches the bias $\epsilon = (4k+2)^{-1}$ as the number of points is increased (the value is reached in the limit of infinite points). Consequently, we consider a finite set of points in the transition.

best protocol (bias 1/6) can already be derived from its TDPG, in a manner analogous to the one used for the example game. This was not known (to the best of our knowledge), even though the protocol itself was separately known and analysed. We next study the family of bias 1/10 TDPGs and isolate the precise moves required to implement it (see Subsection A.3). Let $n_g \longrightarrow n_h$ denote a move from n_g initial points to n_h final points. While the bias 1/6 games used a $2 \longrightarrow 1$ merge as its key move, the bias 1/10 games use a combination of $3 \longrightarrow 2$ and $2 \longrightarrow 2$ moves (these can not be produced by a combination of merges and splits, as was pointed out earlier). We give analytic expressions for these unitaries and show that they satisfy the required constraints (see Subsection A.3). In particular, we show that for $3 \longrightarrow 2$ moves with $x_{g_1} < x_{g_2} < x_{g_3}$ and $x_{h_1} < x_{h_2}$

$$U_{3\to 2} = |w\rangle\langle v| + |w_1\rangle\langle v_1'| + |v_2'\rangle\langle v_2'| + |v_1'\rangle\langle w_1| + |v\rangle\langle w| \quad (4)$$

satisfies the required constraints (under some further technical conditions which are satisfied by the 1/10 games of interest), where

$$|v\rangle = \frac{\sqrt{p_{g_1}}\,|g_1\rangle + \sqrt{p_{g_2}}\,|g_2\rangle + \sqrt{p_{g_3}}\,|g_3\rangle}{N_g},$$

$$|v_1\rangle = \frac{\sqrt{p_{g_3}}\,|g_2\rangle - \sqrt{p_{g_2}}\,|g_3\rangle}{N_{v_1}},$$

$$|v_2\rangle = \frac{-\frac{(p_{g_2}+p_{g_3})}{\sqrt{p_{g_1}}}\,|g_1\rangle + \sqrt{p_{g_2}}\,|g_2\rangle + \sqrt{p_{g_3}}\,|g_3\rangle}{N_{v_2}}$$

and

$$|w\rangle = \frac{\sqrt{p_{h_1}}\,|h_1\rangle + \sqrt{p_{h_2}}\,|h_2\rangle}{N_h}, |w_1\rangle = \frac{\sqrt{p_{h_2}}\,|h_1\rangle - \sqrt{p_{h_1}}\,|h_2\rangle}{N_h}$$

are normalised vectors (this fixes the normalisation factors) which we use to define

$$|v_1'\rangle = \cos\theta\,|v_1\rangle + \sin\theta\,|v_2\rangle\,, |v_2'\rangle = \sin\theta\,|v_1\rangle - \cos\theta\,|v_2\rangle$$

where $\cos\theta$ is obtained by solving

$$\frac{\sqrt{p_{h_1}p_{h_2}}}{N_h^2}\left(x_{h_1} - x_{h_2}\right) - \cos\theta\frac{\sqrt{p_{g_2}p_{g_3}}}{N_g N_{v_1}}\left(x_{g_2} - x_{g_3}\right) - \sin\theta\left\langle x_g\right\rangle\frac{N_g}{N_{v_2}} = 0$$

and choosing the solution which is closer to 1. Similarly we give an explicit unitary corresponding to the second move, i.e. the $2 \longrightarrow 2$ move. For the second move, i.e. the $2 \longrightarrow 2$ move with $x_{g_1} < x_{g_2}$ and $x_{h_1} < x_{h_2}$, we show that

$$U_{2\to 2} = |w\rangle\langle v| + (\alpha\,|v\rangle + \beta\,|w_1\rangle)\langle v_1| + |v\rangle\langle w| + (\beta\,|v\rangle - \alpha\,|w_1\rangle)\langle w_1|$$

satisfies the required constraints (again, under further technical conditions which are satisfied by the 1/10 games of interest) where

$$|v\rangle = \frac{1}{N_g}\left(\sqrt{p_{g_1}}\,|g_1\rangle + \sqrt{p_{g_2}}\,|g_2\rangle\right),$$

$$|v_1\rangle = \frac{1}{N_g}\left(\sqrt{p_{g_2}}\,|g_1\rangle - \sqrt{p_{g_1}}\,|g_2\rangle\right)$$

and

$$|w\rangle = \frac{1}{N_h}\left(\sqrt{p_{h_1}}\,|h_1\rangle + \sqrt{p_{h_2}}\,|h_2\rangle\right)$$

$$|w_1\rangle = \frac{1}{N_h}\left(\sqrt{p_{h_2}}\,|h_1\rangle - \sqrt{p_{h_1}}\,|h_2\rangle\right).$$

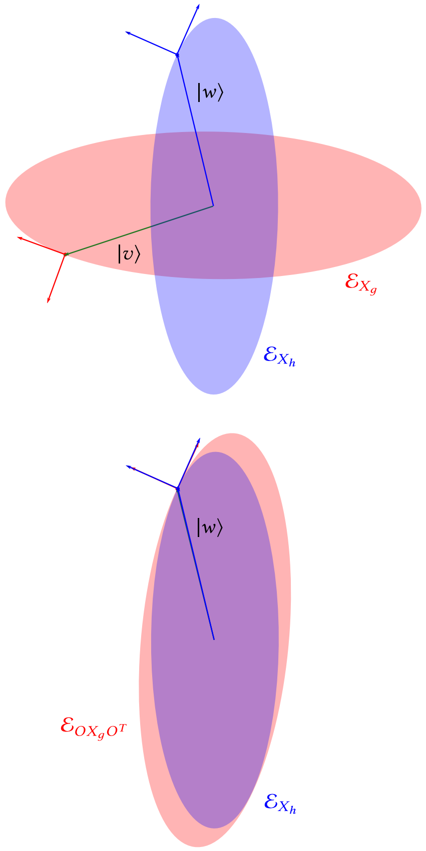

Figure 3:
Top: The ellipsoids correspond to the diagonal matrices X_g and X_h. The vectors $|w\rangle$ and $|v\rangle$ indicate only the direction. Bottom: The larger ellipsoid is now rotated to correspond to OX_gO^T. The point of contact is along the vector $|w\rangle = O\,|v\rangle$.

Further, $\alpha, \beta \in \mathbb{R}$ are such that $\alpha^2 + \beta^2 = 1$ and

$$\beta = \sqrt{\frac{p_{h_1}p_{h_2}}{p_{g_1}p_{g_2}}\frac{(x_{h_1} - x_{h_2})}{(x_{g_1} - x_{g_2})}}.$$

This lets us, in effect, convert Mochon's family of bias 1/10 games into explicit protocols, finally breaking the 1/6 barrier. Mochon's games achieving lower biases correspond to larger unitary matrices. Consequently, this approach based on guessing the correct form of the solution becomes untenable.

4 EMA ALGORITHM | SECOND CONTRIBUTION

To go lower than 1/10 we use our Elliptic Monotone Align (EMA) algorithm which we now describe. Note that if we neglect the projector in Equation (2), we can express it as $X_h \geq UX_gU^\dagger$ where X_h, X_g are diagonal matrices with positive entries. One can restrict to orthogonal matrices without loss of generality (see Subsection B.1). Once we restrict to real numbers, the set of vectors $\mathcal{E}_{X_h} := \{|u\rangle \mid \langle u| X_h |u\rangle = 1\}$ describe the boundary of an ellipsoid as $\sum_i u_i^2/(x_{h_i}^{-1}) = 1$ (note x_{h_i} is fixed here and u_i is the variable). Similarly $\mathcal{E}_{OX_gO^T}$ represents a rotated ellipsoid where O is orthogonal (see Figure 3). Geometrically, the aforesaid inequality means that $\mathcal{E}_{X_h}$ ellipsoid is contained in the $\mathcal{E}_{OX_gO^T}$ ellipsoid (the order gets reversed; see Subsection B.2).

Recall from Theorem 2 that the orthogonal matrix also has the property $O\left|v\right\rangle = \left|w\right\rangle$. Imagine that in addition, we have $\left\langle w\right| X_h \left|w\right\rangle = \left\langle v\right| X_g \left|v\right\rangle$ which in terms of the point game means that the average is preserved (as was the case for merge). In terms of the ellipsoids, it means that the ellipsoids touch along the $\left|w\right\rangle$ direction. More precisely, the point $\left|c\right\rangle := \left|w\right\rangle / \sqrt{\left\langle w\right| X_h \left|w\right\rangle}$ belongs to both $\mathcal{E}_{X_h}$ and $\mathcal{E}_{OX_gO^T}$. Since the inequality tells us the smaller h ellipsoid is contained inside the larger g ellipsoid, and we now know that they touch at the point $\left|c\right\rangle$, we conclude that their normals evaluated at $\left|c\right\rangle$ must be equal. Further, we can conclude that the inner ellipsoid must be more curved than the outer ellipsoid.

Mark the point $\left|c\right\rangle$ on the $\mathcal{E}_{OX_gO^T}$ ellipsoid. Now imagine that the $\mathcal{E}_{X_g}$ ellipsoid is rotated to the $\mathcal{E}_{OX_gO^T}$ ellipsoid (see Figure 3). The normal at the marked point must be mapped to the normal of $\mathcal{E}_{X_h}$ at $\left|c\right\rangle$. To evaluate the normals[3] $\left|n_h\right\rangle$ on $\mathcal{E}_{X_h}$ at $\left|c\right\rangle$ and $\left|n_g\right\rangle$ on $\mathcal{E}_{X_g}$ at the marked point, one only needs to know $X_h, X_g, \left|v\right\rangle$ and $\left|w\right\rangle$. Complete knowledge of O is not required and yet we can be sure that $O\left|n_g\right\rangle = \left|n_h\right\rangle$ which means O must have a term $\left|n_h\right\rangle\left\langle n_g\right|$. In fact, one can even evaluate the curvature from the aforesaid quantities (see Subsection B.3). It so turns out that when this condition is expressed precisely, it becomes an instance of the same problem we started with one less dimension (see Subsection B.4). This allows us to iteratively find O, which so far we had only assumed to exist. An easy method for evaluating the curvatures—the reverse Weingarten map—is key to the said simplification. This, however, only works under our assumption that $\left\langle w\right| X_h \left|w\right\rangle = \left\langle v\right| X_g \left|v\right\rangle$. This is not always the case which we address next.

A monotone function f is defined to be a function which has the property "$x \geq y \implies f(x) \geq f(y)$". An operator monotone function[4] is obtained from a generalisation of the aforesaid property to matrices, which in our notation can be expressed as "$X_h \geq OX_gO^T \implies f(X_h) \geq Of(X_g)O^T$". An important class of operator monotone functions is characterised by the parameter λ as $f_\lambda(x) = -(\lambda + x)^{-1}$.

The tuple $\underline{X} := (X_h, X_g, \left|w\right\rangle, \left|v\right\rangle)$ is defined to be a *matrix instance*. A matrix instance $\underline{X}$ is said to have a solution if there exists an orthogonal matrix O such that $O\left|v\right\rangle = \left|w\right\rangle$ and $X_h \geq OX_gO^T$. The matrix instance is said to have a *tight* solution if, in addition, every solution O satisfies $X_h \ngtr OX_gO^T$. Building on the results of Kitaev, Mochon [12] Aharonov, Chailloux, Ganz, Kerenidis and Magnin [2], one can use the aforesaid operator monotone functions to check if a given matrix instance has a (tight) solution (see Subsection B.5). This can be used to find a $\gamma \in [1, 0)$ such that the matrix instance $(\gamma X_h, X_g, \left|w\right\rangle, \left|v\right\rangle)$ has a tight solution. The same method also yields a λ such that $\left\langle w\right| f_\lambda(\gamma X_h) \left|w\right\rangle = \left\langle v\right| f_\lambda(X_g) \left|v\right\rangle$. It is not too hard to see that $f_\lambda^{-1}(x)$ is also an operator monotone function. Therefore, one can conclude that $\gamma X_h \geq OX_gO^T$ is equivalent to $f_\lambda(\gamma X_h) \geq Of_\lambda(X_g)O^T$. Let $\chi - 1$ be the smallest value in the spectrum of $f_\lambda(\gamma X_h)$ and $f_\lambda(X_g)$. Now observe that $\gamma X_h \geq OX_gO^T$ is, using the aforesaid, also equivalent to $X'_h \geq OX'_gO^T$ where $X'_h = f_\lambda(\gamma X_h) - \chi\mathbb{I}$ and $X'_g = f_\lambda(X_g) - \chi\mathbb{I}$. Further, $X'_h, X'_g > 0$ and $\left\langle w\right| X'_h \left|w\right\rangle = \left\langle v\right| X'_g \left|v\right\rangle$ which entails we have reduced our problem to the form we started our discussion with. Since the orthogonal matrix which solves the various matrix instances remains the same, we can use our technique on the final one to proceed. This outlines how and why the EMA algorithm works. Let us summarise the algorithm into an informal statement.

Definition (EMA Algorithm (informal)). Given a transition from a TDPG the algorithm proceeds in three phases.

(1) Initialise
- Tightening: Bring the final points close to zero until the corresponding ellipsoids start to touch.
- Spectral domain, matrices: Find the spectrum of the matrices which represent the ellipsoid. Evaluate the smallest matrix size n needed to represent the problem using ellipsoids.
- Bootstrapping: Using the aforesaid, define $\left(X_h^{(n)}, X_g^{(n)}, \left|w^{(n)}\right\rangle, \left|v^{(n)}\right\rangle\right) := \underline{X}^{(n)}$ where the superscript denotes the size of the matrix and vectors.

(2) Iterate (neglecting special cases)
Input: $\underline{X}^{(k)}$
Output: $\underline{X}^{(k-1)}$, the vector $\left|n_h^{(k)}\right\rangle$ and the orthogonal matrices $\bar{O}_g^{(k)}, \bar{O}_h^{(k)}$
Procedure:
- Tightening: Similar to the one above, stretch the inner ellipsoid until it touches the outer ellipsoid.
- Honest align: Use operator monotone functions to make the ellipsoids touch along the $\left|w^{(k)}\right\rangle$ direction.
- Evaluate the Reverse Weingarten Map: Evaluate the curvatures and the normal (which fixes $\left|n_h^{(k)}\right\rangle$) along the $\left|w^{(k)}\right\rangle$ direction.
- Finite Method: Use the curvatures to specify $\underline{X}^{(k-1)}$ and find the orthogonal matrices $\bar{O}_g^{(k)}, \bar{O}_h^{(k)}$.

(3) Reconstruction
Evaluate $O^{(n)}$ recursively using
$O^{(k)} = \bar{O}_g^{(k)}\left(\left|n_h^{(k)}\right\rangle\left\langle n_h^{(k)}\right| + O^{(k-1)}\right)\bar{O}_h^{(k)}$.

Theorem 3 (Correctness of the EMA Algorithm (informal)). *Given a transition of a TDPG, the EMA Algorithm always finds a real unitary U such that the constraints in Theorem 2 are satisfied.*

The complete algorithm and the proof of its correctness have been omitted from this extended abstract and can be found in the full version of the paper.

Despite the apparent simplicity of the main argument there are many difficulties one must address in order to prove the aforesaid statement. The results about operator monotone functions must be extended to make them applicable to the tightening step as indicated and for being certain that the solution unitary/orthogonal

[3] The vector $\left|n_h\right\rangle$ is not related to the number of initial points n_h; similarly $\left|n_g\right\rangle$ and n_g are unrelated.

[4] Note that the monotone function $f(x) = x^2$ is not an operator monotone. To see this, use $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \geq \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$.

matrix stays unchanged under these transformations. Some results related to different representations of the aforesaid transitions must be extended as these situations arise in the tightening procedure. A critical aspect of the algorithm is the handling of the cases where one of the tangent directions of an ellipsoid has an infinite curvature. For concreteness, imagine an ellipse which under an operator monotone gets mapped to a line segment. The tip of the line segment, if viewed as a limit of an ellipse, has an infinite curvature. In these cases, our finite analysis breaks down as the normal is no longer well defined. This situation arises, for instance, if one tries to solve the split move using this algorithm. This is handled by considering the sequence leading to the infinite curvature and expressing the troublesome component of the normal in terms of known quantities which stay well defined even when the curvature becomes infinite. Notably, for the moves used by Mochon in his 1/18 game that we numerically solved using this algorithm, this infinite case did not appear.

The implication is that we can now convert known games with arbitrarily small bias into complete protocols. One remaining question is the effect of noise. In the current analysis two idealising assumptions have been made. First, the EMA algorithm assumes one can exactly solve certain problems classically, namely finding the roots of polynomials and diagonalising matrices. Second, in Mochon/Kitaev’s point game formalisms, one assumes that the unitaries are known and applied exactly. Neither of these will hold practically, therefore, the effect of noise on the bias of the protocol must be quantified, which we leave as an open problem for further work.

A FRAMEWORK

A.1 TEF

We now discuss the key ingredients of the proof of Theorem 2. These show how the dual SDP (see Section 1 of [2]) can be constructed. The dual SDP formulation itself encodes within it the protocol (the unitaries and the projectors) which can be trivially extracted.

Definition 4 (Canonical Form). Consider a frame of the TDPG where the ith point has weight $p_i > 0$ and coordinates $[x_i, y_i]$. The tuple $(|\psi\rangle, Z^A, Z^B)$ is said to be in the Canonical Form with respect to this frame if $|\psi\rangle = \sum_i \sqrt{p_i}\,|ii\rangle_{AB} \otimes |.\rangle_M$, $Z^A = (\sum x_i\,|i\rangle\langle i|_A)$ and $Z^B = (\sum y_i\,|i\rangle\langle i|_B)$ where $|.\rangle_M$ is any arbitrary state.

As stated, we start with the Canonical Form for the initial frame, transition through intermediate frames and show that the final frame is again in the Canonical Form.

1. First frame.

$$\begin{aligned}
\left|\psi_{(1)}\right\rangle &= \left(\sum_i \sqrt{p_{g_i}}\,|g_i g_i\rangle_{AB} + \sum_i \sqrt{p_{k_i}}\,|k_i k_i\rangle_{AB}\right) \otimes |m\rangle_M \\
Z^A_{(1)} &= \sum_i x_{g_i}\,|g_i\rangle\langle g_i|_A + \sum_i x_{k_i}\,|k_i\rangle\langle k_i|_A \\
Z^B_{(1)} &= \sum_i y_{g_i}\,|g_i\rangle\langle g_i|_B + \sum_i y_{k_i}\,|k_i\rangle\langle k_i|_B\,.
\end{aligned}$$

Proof. Follows from the assumption of starting with a Canonical Form. □

2. Bob sends to Alice. With $y \geq \max\{y_{g_i}\}$ the following is a valid choice

$$\begin{aligned}
\left|\psi_{(2)}\right\rangle &= \sum_i \sqrt{p_{g_i}}\,|g_i g_i\rangle_{AM} \otimes |m\rangle_B + \sum_i \sqrt{p_{k_i}}\,|k_i k_i\rangle_{AB} \otimes |m\rangle_M \\
U^{(1)} &= U^{\mathrm{SWP}\{\vec{g},m\}}_{BM} \\
Z^A_{(2)} &= Z^A_{(1)} \\
Z^B_{(2)} &= y\mathbb{I}^{\{\vec{g},m\}}_B + \sum_i y_{k_i}\,|k_i\rangle\langle k_i|_B\,.
\end{aligned}$$

Proof. We have to prove:
(1) $\left|\psi_{(2)}\right\rangle = U^{(1)}\left|\psi_{(1)}\right\rangle$ and
(2) $U^{(1)\dagger}\left(Z^B_{(2)} \otimes \mathbb{I}_M\right)U^{(1)} \geq \left(Z^B_{(1)} \otimes \mathbb{I}_M\right)$.
The demonstration is as follows.
(1) It follows trivially from the defining action of $U^{(1)}$.
(2) For convenience, let momentarily $U = U^{(1)}$ and note that $U^\dagger = U$ so that we can write

$$\begin{aligned}
&U\left(Z^B_{(2)} \otimes \mathbb{I}_M\right)U \\
=&y\left(U\left(\mathbb{I}^{\{\vec{g},m\}}_B \otimes \mathbb{I}^{\{\vec{g},m\}}_M\right)U + U\underbrace{\left(\mathbb{I}^{\{\vec{g},m\}}_B \otimes \mathbb{I}^{\{\vec{k},\vec{h}\}}_M\right)}_{\text{outside } U\text{'s action space}}U\right) \\
&+ U\underbrace{\left(\sum y_{k_i}\,|k_i\rangle\langle k_i|_B \otimes \mathbb{I}_M\right)}_{\text{outside } U\text{'s action space}}U \\
=&Z^B_{(2)} \otimes \mathbb{I}_M \geq Z^B_{(1)} \otimes \mathbb{I}_M
\end{aligned}$$

so long as $y \geq y_{g_i}$ which is guaranteed by the choice of y. □

3. Alice’s non-trivial step. We claim that the following is a valid choice,

$$\begin{aligned}
\left|\psi_{(3)}\right\rangle &= \sum_i \sqrt{p_{h_i}}\,|h_i h_i\rangle_{AM} \otimes |m\rangle_B + \sum_i \sqrt{p_{k_i}}\,|k_i k_i\rangle_{AB} \otimes |m\rangle_M \\
&U^{(2)} \text{ s.t. } U^{(2)}\,|v\rangle = |w\rangle \\
Z^A_{(3)} &= \sum_i x_{h_i}\,|h_i\rangle\langle h_i|_A + \sum_i x_{k_i}\,|k_i\rangle\langle k_i|_A \\
Z^B_{(3)} &= Z^B_{(2)}
\end{aligned}$$

where

$$|v\rangle = \frac{\sum_i \sqrt{p_{g_i}}\,|g_i g_i\rangle_{AM}}{\sqrt{\sum_j p_{g_j}}},\ |w\rangle = \frac{\sum_i \sqrt{p_{h_i}}\,|h_i h_i\rangle_{AM}}{\sqrt{\sum_j p_{h_j}}},$$

$$E^{(2)} = \left(\sum_i |h_i\rangle\langle h_i|_A + \sum_i |k_i\rangle\langle k_i|_A\right) \otimes \mathbb{I}_M$$

subject to the condition

$$\sum_i x_{h_i}\,|h_i h_i\rangle\langle h_i h_i|_{AM} \geq \sum_i x_{g_i} E^{(2)} U^{(2)}\,|g_i g_i\rangle\langle g_i g_i|_{AM}\,U^{(2)\dagger} E^{(2)}$$

and of course the conservation of probability, viz. $\sum_i p_{g_i} = \sum_i p_{h_i}$.

Proof. We must show that
(1) $E^{(2)}\left|\psi_{(3)}\right\rangle = U^{(2)}\left|\psi_{(2)}\right\rangle$ and
(2) $Z^A_{(3)} \otimes \mathbb{I}_M \geq E^{(2)}U^{(2)}\left(Z^A_{(2)} \otimes \mathbb{I}_M\right)U^{(2)\dagger}E^{(2)}$.
The demonstration is as follows.
(1) Observing $E^{(2)}\left|\psi_{(3)}\right\rangle = \left|\psi_{(3)}\right\rangle$ the statement holds almost trivially by construction of $U^{(2)}$.
(2) Consider the space

$$\mathcal{H} = \text{span}\left\{|g_1g_1\rangle, |g_2g_2\rangle \ldots, |h_1h_1\rangle, |h_2, h_2\rangle \ldots\right\}.$$

We will separate all expressions (they are nearly diagonal) into the $\mathcal{H}$ space (which gets non-diagonal) and the rest. We start with the LHS,

$$\begin{aligned} Z^A_{(3)} \otimes \mathbb{I}_M = & \underbrace{\sum_i x_{h_i}|h_ih_i\rangle\langle h_ih_i|_{AM}}_{\text{I}} \\ & + \sum_i x_{h_i}|h_i\rangle\langle h_i|_A \otimes (\mathbb{I} - |h_i\rangle\langle h_i|)_M \\ & + \sum x_{k_i}|k_i\rangle\langle k_i|_A \otimes \mathbb{I}_M, \end{aligned}$$

where only term I is in the operator space spanned by $\mathcal{H}$. Note that all the terms are still diagonal. Next consider the RHS, without the EU (defined to be $E^{(2)}U^{(2)}$),

$$\begin{aligned} Z^A_{(2)} \otimes \mathbb{I}_M = & \underbrace{\sum x_{g_i}|g_ig_i\rangle\langle g_ig_i|_{AM}}_{\text{I}} \\ & + \sum x_{g_i}|g_i\rangle\langle g_i|_A \otimes (\mathbb{I} - |g_i\rangle\langle g_i|)_M \\ & + \sum x_{k_i}|k_i\rangle\langle k_i|_A \otimes \mathbb{I}_M, \end{aligned}$$

which also has only term I in the $\mathcal{H}$ operator space. Consequently, only on these will U have a non-trivial action. Let us first evaluate the non-$\mathcal{H}$ part where we only need to apply the projector. The result after separating equations where possible is

$$\begin{aligned} \sum x_{h_i}|h_i\rangle\langle h_i|_A \otimes (\mathbb{I} - |h_i\rangle\langle h_i|)_M \geq 0 \\ \sum (x_{k_i} - x_{k_i})|k_i\rangle\langle k_i|_A \otimes \mathbb{I}_M \geq 0 \end{aligned}$$

which essentially only implies $x_{h_i} \geq 0$. Finally the non-trivial part yields

$$\sum x_{h_i}|h_ih_i\rangle\langle h_ih_i|_{AM} \geq \sum x_{g_i}EU|g_ig_i\rangle\langle g_ig_i|_{AM}U^\dagger E$$

which completes the proof. □

4. Bob accepts Alice's change. The following is valid.

$$\begin{aligned} \left|\psi_{(4)}\right\rangle &= \left(\sum_i \sqrt{p_{h_i}}|h_ih_i\rangle_{AB} + \sum_i \sqrt{p_{k_i}}|k_ik_i\rangle_{AB}\right) \otimes |m\rangle_M \\ E^{(3)}U^{(3)} &= E^{(3)}U^{\text{SWP}\{\vec{h},m\}}_{BM} \\ Z^A_{(4)} &= Z^A_{(3)} \\ Z^B_{(4)} &= y\sum_i |h_i\rangle\langle h_i|_B + \sum_i y_{k_i}|k_i\rangle\langle k_i|_B \end{aligned}$$

where $E^{(3)} = (\sum_i |h_i\rangle\langle h_i| + \sum_i |k_i\rangle\langle k_i|)_B \otimes \mathbb{I}_M$.

Proof. We have to prove:
(1) $E^{(3)}\left|\psi_{(4)}\right\rangle = U^{(3)}\left|\psi_{(3)}\right\rangle$ and
(2) $Z^B_{(4)} \otimes \mathbb{I}_M \geq E^{(3)}U^{(3)}\left(Z^B_{(3)} \otimes \mathbb{I}_M\right)U^{(3)\dagger}E^{(3)}$.
The demonstration is as follows.
(1) This can be proven again, by a direct application of EU (defined to be $E^{(3)}U^{(3)}$ for the proof).
(2) Note that

$$\begin{aligned} EU\left(\mathbb{I}^{\{\vec{g},m\}}_B \otimes \mathbb{I}^{\{\vec{h},\vec{g},\vec{k},m\}}_M\right)U^\dagger E &= EU\left(\mathbb{I}^{\{m\}}_B \otimes \mathbb{I}^{\{\vec{h},\vec{g},\vec{k},m\}}_M\right)U^\dagger E \\ &\quad + E\left(\mathbb{I}^{\{\vec{g}\}}_B \otimes \mathbb{I}^{\{\vec{h},\vec{g},\vec{k},m\}}_M\right)E \\ &= EU\left(\mathbb{I}^{\{m\}}_B \otimes \mathbb{I}^{\{\vec{h},m\}}_M\right)U^\dagger E \\ &= \sum_i |h_i\rangle\langle h_i|_B \otimes \mathbb{I}^{\{m\}}_M. \end{aligned}$$

Since the other term in $Z^B_3 \otimes \mathbb{I}_M$ is anyway in the non-action space of U it follows that

$$EU(Z^B_3 \otimes \mathbb{I}_M)U^\dagger E = y\sum_i |h_i\rangle\langle h_i|_B \otimes \mathbb{I}^{\{m\}}_M + \sum_i y_{k_i}|k_i\rangle\langle k_i|_B \otimes \mathbb{I}_M.$$

It only remains to show that

$$Z^B_{(4)} \otimes \mathbb{I}_M \geq E^{(3)}U^{(3)}\left(Z^B_{(3)} \otimes \mathbb{I}_M\right)U^{(3)\dagger}E^{(3)}$$

which it obviously is because $y\sum_i |h_i\rangle\langle h_i|_B \otimes \mathbb{I}_M \geq y\sum_i |h_i\rangle\langle h_i|_B \otimes \mathbb{I}^{\{m\}}_M$ and the y_{k_i} term is common. □

A.2 Blinkered Unitaries

The blinkered unitary can be used to implement the two non-trivial operations of the set of basic moves.

Merge: $g_1, g_2 \longrightarrow h_1$
We can construct from the definitions

$$\begin{aligned} |v\rangle &= \frac{\sqrt{p_{g_1}}|g_1\rangle + \sqrt{p_{g_2}}|g_2\rangle}{N}, \\ |v_1\rangle &= \frac{\sqrt{p_{g_2}}|g_1\rangle - \sqrt{p_{g_1}}|g_2\rangle}{N}, \\ |w\rangle &= |h_1\rangle \end{aligned}$$

with $N = \sqrt{p_{g_1} + p_{g_2}}$ and

$$U = |w\rangle\langle v| + |v\rangle\langle w| + |v_1\rangle\langle v_1| \,(= U^\dagger).$$

Using

$$EU|g_1\rangle = \frac{\sqrt{p_{g_1}}|w\rangle}{N}, \; EU|g_2\rangle = \frac{\sqrt{p_{g_2}}|w\rangle}{N}$$

and the aforesaid, Equation (2) becomes

$$x_h|h_1\rangle\langle h_1| \geq \sum_{i=1}^{2} x_{g_i}EU|g_i\rangle\langle g_i|U^\dagger E$$

which is equivalent to

$$x_h \geq \frac{p_{g_1}x_{g_1} + p_{g_2}x_{g_2}}{N^2}.$$

This readily generalises to an $m \longrightarrow 1$ point merge and matches the merge condition $x_h \geq \langle x_g\rangle$.

Split: $g_1 \longrightarrow h_1, h_2$
Again from the definitions, one can write

$$\begin{aligned} |v\rangle &= |g_1 g_1\rangle, \\ |w\rangle &= \frac{\sqrt{p_{h_1}}\,|h_1\rangle + \sqrt{p_{h_2}}\,|h_2\rangle}{N}, \\ |w_1\rangle &= \frac{\sqrt{p_{h_2}}\,|h_1\rangle - \sqrt{p_{h_1}}\,|h_2\rangle}{N} \end{aligned}$$

with $N = \sqrt{p_{h_1} + p_{h_2}}$ and

$$U = |v\rangle\langle w| + |w\rangle\langle v| + |w_1\rangle\langle w_1| = U^\dagger.$$

We evaluate $EU\,|g_1\rangle = |w\rangle$ and insert into the constraints to get

$$x_{h_1}\,|h_1\rangle\langle h_1| + x_{h_2}\,|h_2\rangle\langle h_2| - x_g\,|w\rangle\langle w| \geq 0.$$

This yields the matrix equation

$$\begin{aligned} \begin{bmatrix} x_{h_1} & \\ & x_{h_2} \end{bmatrix} - \frac{x_g}{N^2}\begin{bmatrix} p_{h_1} & \sqrt{p_{h_1}p_{h_2}} \\ \sqrt{p_{h_1}p_{h_2}} & p_{h_2} \end{bmatrix} &\geq 0 \\ \Longleftrightarrow \quad \mathbb{I} - \frac{x_g}{N^2}\begin{bmatrix} \frac{p_{h_1}}{x_{h_1}} & \sqrt{\frac{p_{h_1}}{x_{h_1}}\frac{p_{h_2}}{x_{h_2}}} \\ \sqrt{\frac{p_{h_1}}{x_{h_1}}\frac{p_{h_2}}{x_{h_2}}} & \frac{p_{h_2}}{x_{h_2}} \end{bmatrix} &\geq 0 \\ \Longleftrightarrow \quad \frac{x_g}{N^2}\left(\frac{p_{h_1}}{x_{h_1}} + \frac{p_{h_2}}{x_{h_2}}\right) &\leq 1 \end{aligned}$$

where in the second step we used the fact that $F - M \geq 0$ is equivalent to $\mathbb{I} - \sqrt{F}^{-1} M \sqrt{F}^{-1} \geq 0$ (if $F > 0$) and the last step is obtained by writing the matrix in the previous step as $|\psi\rangle\langle\psi|$ followed by demanding $1 \geq \langle\psi|\psi\rangle$. This also readily generalises to a $1 \longrightarrow m$ point split and matches the split condition $\langle 1/x_h\rangle \leq 1/x_g$.

A.3 Bias 1/10

Mochon's family of games with bias $1/(4k+2)$ for $k \in \{1, 2 \ldots\}$ only use a special kind of transition based on the following assignment.

Definition (Mochon's assignment). Given a set of n points $0 \leq x_1 < x_2 \cdots < x_n$, a polynomial $f(x)$ with order k at most $n-2$ and $f(-\lambda) \geq 0$ for all $\lambda \geq 0$, let the weight corresponding to the point x_l be given by $p(x_l) = -\frac{f(x_l)}{\prod_{j \neq l}(x_j - x_l)}$.

Let $\{i\}$ be the set of indices for which $p(x_i) < 0$ and $\{k\}$ be the remaining indices with respect to $\{1, 2, \ldots n\}$. Mochon's assignment is given by (component-wise)

$$\begin{aligned} \{x_{g_1}, x_{g_2} \ldots\} &= \{x_i\} \\ \{p_{g_1}, p_{g_2} \ldots\} &= \{-p(x_i)\} \\ \{x_{h_1}, x_{h_2} \ldots\} &= \{x_k\} \\ \{p_{h_1}, p_{h_2} \ldots\} &= \{p(x_k)\}. \end{aligned}$$

Mochon showed that this assignment always satisfies Equation (2), the scalar condition (see Lemma 5.1 of [2]; or Lemma 31 of [12]). The games corresponding to $k = 2$ approach bias 1/10 and are defined by points on a grid as indicated in Figure 4. Using Mochon's assignment, for the vertical transition highlighted in the figure, with $f(y_i) = (y_{-1} - y_i)(\Gamma_1 - y_i)(\Gamma_2 - y_i)$, the weight of the point at $[x_j, y_j]$ is given by

$$\frac{f(y_j)c(x_j)}{\prod_{k \neq j}(y_k - y_j)}$$

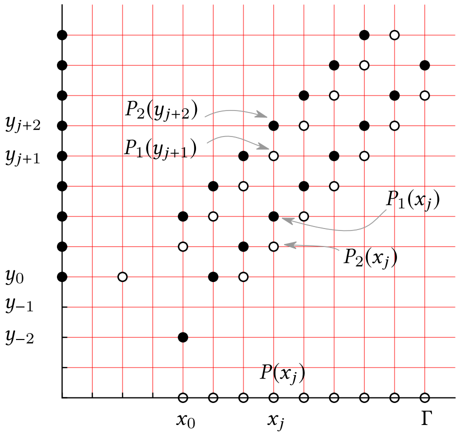

Figure 4: An illustration of Mochon's bias 1/10 game. The $3 \longrightarrow 2$ transition, the key move, has been highlighted. For concreteness, let $x_j = x_0 + j\Delta$ and let similarly $y_j = y_0 + j\Delta$ for some lattice spacing $\Delta =: \delta x =: \delta y$; $y_0 = x_0$. For vertical transitions, the unfilled dots represent initial points and the filled dots represent final points. For horizontal transitions, it is the other way. See Section 4.1 of [12] or Section 4 of [2] for an explanation. It is related to the well-understood connection between TIPGs and TDPGs.

where $\Gamma_l = \Gamma + l$, Γ is large compared to 1 and c is a constant (wrt y-coordinate) normalisation factor. Applying Mochon's assignment we get

$$\begin{aligned} P_2(y_{j+2}) &= \frac{-f(y_{j+2})c(x_j)}{4.3(\delta y)^2 y_{j+2}} =: p_{h_2} \\ P_1(y_{j+1}) &= \frac{-f(y_{j+1})c(x_j)}{3.2(\delta y)^2 y_{j+1}} =: p_{g_3} \\ P_1(x_j) &= \frac{-f(y_{j-1})c(x_j)}{3.2(\delta y)^2 y_{j-1}} =: p_{h_1} \\ P_2(x_j) &= \frac{-f(y_{j-2})c(x_j)}{4.3(\delta y)^2 y_{j-2}} =: p_{g_2} \\ P(x_j) &= \frac{f(0)c(x_j)\delta y}{y_{j+2}y_{j+1}y_{j-1}y_{j-2}} =: p_{g_1} \end{aligned}$$

where we added the minus sign to account for the fact that f will be negative for coordinates between y_{-1} and Γ_1. Mochon's game is symmetric under the exchange of axes, viz. $x \leftrightarrow y$, unto signs (filled and unfilled points get flipped). This means the game satisfies the symmetry constraints $P_1(y_j) = P_1(x_j)$ which yields

$$\frac{f(y_j)c(x_{j-1})}{\cancel{3.2(\delta y)^2} y_j} = \frac{f(y_{j-1})c(x_j)}{\cancel{3.2(\delta y)^2} y_{j-1}}$$

which means $c(x_j) = c_0 f(x_j)/x_j$ where c_0 is a constant. This also entails that $P_2(y_j) = P_2(x_j)$, viz. it satisfies the second symmetry constraint. Finally we can evaluate

$$P(x_j) = \frac{f(0)f(x_j)\delta x}{x_{j+2}x_{j+1}x_j x_{j-1}x_{j-2}} = \frac{c_0 x_0(x_0 - x_j)}{x_j^5}\delta x + O(\delta x^2).$$

In all of Mochon's games, the weight on each axis sums to 1/2. This is because each of his games start with splitting all the weight at [0, 1] and [1, 0] along the axis. The remaining weight, i.e. the weight on the ladder as Mochon calls it, gets cancelled finally; all the weight except that on the two isolated points near the origin. Imposing this normalisation condition and that the split is valid, we get

$$\sum_j P(x_j) = \frac{1}{2} = \sum_j \frac{P(x_j)}{x_j} \approx \int_{x_0}^{\Gamma} \frac{(x_0 - x)dx}{x^5} = \int_{x_0}^{\Gamma} \frac{(x_0 - x)dx}{x^6}.$$

The approximation assumes Δ is small and the number of points large. Since we can merge the two isolated points to the point $[x_0, x_0]$, this quantity yields the bias[5] and can be computed using the aforesaid, in the large Γ limit, as

$$\begin{aligned} x_0 \int_{x_0}^{\Gamma} \left(\frac{1}{x^5} - \frac{1}{x^6}\right) dx &= \int_{x_0}^{\Gamma} \left(\frac{1}{x^4} - \frac{1}{x^5}\right) dx \\ \left[\frac{1}{4} - \frac{1}{3}\right] &\approx \left[\frac{1}{5} - \frac{1}{4}\right]\frac{1}{x_0} \\ x_0 \approx \frac{3}{5} &\implies \epsilon \approx \frac{3}{5} - \frac{1}{2} = \frac{1}{10}. \end{aligned}$$

We now outline the proof of the claim that $U_{3\to 2}$ (see Equation (4)) satisfies the required constraint (see Equation (2)). We will need terms of the form $EU|g_i\rangle$ with $E = \mathbb{I}^{\{h_i\}}$. This entails that on the $\{|g_i\rangle\}$ space ($U_{3\to 2}$ is referred to as U in the following discussion)

$$\begin{aligned} E_h U E_g &= |w\rangle\langle v| + |w_1\rangle\langle v_1'| \\ &= |w\rangle\langle v| + |w_1\rangle(\cos\theta\langle v_1| + \sin\theta\langle v_2|). \end{aligned}$$

Consequently we have

$$\begin{aligned} E_h U|g_1\rangle &= \frac{\sqrt{p_{g_1}}}{N_g}|w\rangle + \left[\cos\theta.0 - \sin\theta\frac{p_{g_2} + p_{g_3}}{\sqrt{p_{g_1}}N_{v_2}}\right]|w_1\rangle \\ E_h U|g_2\rangle &= \frac{\sqrt{p_{g_2}}}{N_g}|w\rangle + \left[\cos\theta\frac{\sqrt{p_{g_3}}}{N_{v_1}} + \sin\theta\frac{\sqrt{p_{g_2}}}{N_{v_2}}\right]|w_1\rangle \\ E_h U|g_3\rangle &= \frac{\sqrt{p_{g_3}}}{N_g}|w\rangle + \left[-\cos\theta\frac{\sqrt{p_{g_2}}}{N_{v_1}} + \sin\theta\frac{\sqrt{p_{g_3}}}{N_{v_2}}\right]|w_1\rangle. \end{aligned}$$

The first sum of the constraint inequality becomes

$$\begin{bmatrix} \langle x_h\rangle & \frac{\sqrt{p_{h_1}p_{h_2}}}{N_h^2}(x_{h_1} - x_{h_2}) \\ \text{h.c.} & \frac{p_{h_2}x_{h_1} + p_{h_1}x_{h_2}}{N_h^2} \end{bmatrix}$$

in the $|w\rangle, |w_1\rangle$ basis (as defined after Equation (4)). Since Mochon's game uses the 3 ⟶ 2 move with one point on the axis, we take $x_{g_1} = 0$. Consequently we need only evaluate

$$x_{g_2}E_h U|g_2\rangle\langle g_2|U^\dagger E_h \doteq$$
$$x_{g_2}\begin{bmatrix} \frac{p_{g_2}}{N_g^2} & \left(\cos\theta\frac{\sqrt{p_{g_3}p_{g_2}}}{N_g N_{v_1}} + \sin\theta\frac{p_{g_2}}{N_g N_{v_2}}\right) \\ \text{h.c.} & \left(\cos\frac{\sqrt{p_{g_3}}}{N_{v_1}} + \sin\theta\frac{\sqrt{p_{g_2}}}{N_{v_2}}\right)^2 \end{bmatrix},$$

$$x_{g_3}E_h U|g_3\rangle\langle g_3|U^\dagger E_h \doteq$$
$$x_{g_3}\begin{bmatrix} \frac{p_{g_3}}{N_g^2} & \left(-\cos\theta\frac{\sqrt{p_{g_2}p_{g_3}}}{N_g N_{v_1}} + \sin\theta\frac{p_{g_3}}{N_g N_{v_2}}\right) \\ \text{h.c.} & \left(-\cos\frac{\sqrt{p_{g_2}}}{N_{v_1}} + \sin\frac{\sqrt{p_{g_3}}}{N_{v_2}}\right)^2 \end{bmatrix}$$

which means that the constraint yields the 2 × 2 matrix inequality

$$\left[\begin{array}{c|c} \langle x_h\rangle - \langle x_g\rangle & \begin{array}{c}\frac{\sqrt{p_{h_1}p_{h_2}}}{N_h^2}(x_{h_1} - x_{h_2}) - \sin\theta\langle x_g\rangle\frac{N_g}{N_{v_2}} \\ -\cos\theta\frac{\sqrt{p_{g_2}p_{g_3}}}{N_g N_{v_1}}(x_{g_2} - x_{g_3})\end{array} \\ \hline \text{h.c.} & \begin{array}{c}\frac{p_{h_2}x_{h_1} + p_{h_1}x_{h_2}}{N_h^2} - \frac{\cos^2\theta}{N_{v_1}^2}(p_{g_3}x_{g_2} + p_{g_2}x_{g_3}) \\ -\frac{\sin^2\theta}{\left(N_{v_2}^2/N_g^2\right)}\langle x_g\rangle - \frac{2\cos\theta\sin\theta\sqrt{p_{g_3}p_{g_2}}}{N_{v_1}N_{v_2}}\left(x_{g_2} - x_{g_3}\right)\end{array} \end{array}\right] \geq 0.$$

It is not hard to show that Mochon's transition is average non-decreasing viz. $\langle x_h\rangle - \langle x_g\rangle \geq 0$. We will set the off-diagonal elements of the matrix above to zero and show that the second diagonal element, the second eigenvalue therefore, is positive.

Setting the off-diagonal to zero one can obtain θ by solving the quadratic equation. To establish the existence of such a θ and the positivity of the inequality constraint we simplify our expressions.

So far everything was exact even though the basis and techniques were chosen based on experience. Assuming $\theta\frac{N_g}{N_{v_2}} \approx O(\delta y)$ at most (where recall $\delta y = \delta x$ is the lattice spacing which is taken to be small) one can express, to first order in $\theta\frac{N_g}{N_{v_2}}$, the aforesaid as

$$\frac{\frac{\sqrt{p_{h_1}p_{h_2}}}{N_h^2}(x_{h_1} - x_{h_2}) - \frac{\sqrt{p_{g_2}p_{g_3}}}{N_g N_{v_1}}(x_{g_2} - x_{g_3})}{\langle x_g\rangle} = \theta\frac{N_g}{N_{v_2}} + O(\delta y^2)$$

and

$$\frac{p_{h_2}x_{h_1} + p_{h_1}x_{h_2}}{N_h^2} - \left[\frac{p_{g_3}x_{g_2} + p_{g_2}x_{g_3}}{N_{v_1}^2} + 2\theta\frac{N_g}{N_{v_2}}\frac{\sqrt{p_{g_3}p_{g_2}}}{N_g N_{v_1}}(x_{g_2} - x_{g_3})\right] + O(\delta y^2) \geq 0.$$

Using the first equation, one can show that $\theta\frac{N_g}{N_{v_2}} = 0.\delta y + O(\delta y^2)$, which in turn can be used to show the inequality holds. A similar demonstration can also be given for $U_{2\to 2}$ to implement the 2 ⟶ 2 transitions which occur close to the origin.

B EMA ALGORITHM

B.1 Restricting to Reals

The reason why restricting to real numbers does not lead to a loss of generality is related to the fact that the set of allowed transitions, the so-called Expressible-By-Matrices (EBM)[6] functions[7] (see Definition 3.1 of [2]) forms a cone, K_Λ (see Lemma 3.6 of [2]). The EBM

[5] Some overhead arises from the conversion of the TIPG into a TDPG but these can be made arbitrarily small.

[6] Λ represents matrices with spectra in $[0, \Lambda]$

[7] functions and transitions are essentially equivalent representations

condition arises naturally in the dual SDP. The cone dual to K_Λ is denoted by K_Λ^*. This cone happens to be the cone of operator monotone functions (see Lemma 3.9 of [2]). We define K'_Λ and K'^*_Λ to be the corresponding sets (cones) with the added restriction to real numbers, i.e. K'_Λ is the set of EBRM (Expressible By Real Matrices) functions on the $[0, \Lambda]$ interval and K'^*_Λ is the set of *real* operator monotone functions on $[0, \Lambda]$—the set of functions $f : [0, \Lambda] \to \mathbb{R}$ such that for all real symmetric matrices H, G satisfying $H \geq G$, one has $f(H) \geq f(G)$. One can prove the following using the matrix representation of complex numbers.

Lemma 5. $K_\Lambda^* = K'^*_\Lambda$*, i.e. the set of operator monotones on* $[0, \Lambda]$ = *the set of real operator monotones on* $[0, \Lambda]$.

The set of EBM functions is a closed convex cone (see Lemma 3.16 of [2]) and so is the set of EBRM functions (the proof is analogous to the EBM case). Since for closed convex cones, the bi-dual happens to be the same as the initial cone (see Theorem 5.5 of [17]), we have the following.

Corollary 6. $K'_\Lambda = K'^{**}_\Lambda = K^{**}_\Lambda = K_\Lambda$*, i.e. the set of EBRM functions on* $[0, \Lambda]$ = *the set of* Λ *valid functions (dual of EBRM functions) = the set of* Λ *valid functions (dual of EBM functions) = the set of EBM functions on* $[0, \Lambda]$.

B.2 Geometric Interpretation

Consider an unnormalised vector $|u\rangle = \sum_j u_j |h_j\rangle$ with $u_j \in \mathbb{R}$. Recall that $\{|u\rangle \mid \langle u| X_h |u\rangle = 1\}$ represents the boundary of en ellipsoid with (semi) axes $a_1 = 1/\sqrt{x_{h_1}}, a_2 = 1/\sqrt{x_{h_2}} \dots$ where $X_h = \text{diag}(x_{h_1}, x_{h_2} \dots)$. An inequality would correspond to points inside or outside the ellipsoid. If we start with some arbitrary (possibly unnormalised) vector $|u\rangle$ then the point on the ellipse along this direction will be given by $\mathcal{E}_h(|u\rangle) = |u\rangle / \sqrt{\langle u| X_h |u\rangle}$. The set $\{|u\rangle \mid \langle u| U X_g U^\dagger |u\rangle = 1\}$ also corresponds to the equation of an ellipsoid with (semi) axes $\{1/\sqrt{x_{g_i}}\}$ except that it is rotated because if we use $|u'\rangle = U |u\rangle$ then the equation reduces to the standard form in the u'_i variables which can then be used to obtain u_is by the aforesaid relations which is a rotation. We can define a similar map from a vector $|u\rangle$ to a point on the rotated ellipse as $\mathcal{E}_g(|u\rangle) = |u\rangle / \sqrt{\langle u| U X_g U^\dagger |u\rangle}$. The statement that

$$\begin{aligned} & X_h - U X_g U^\dagger \geq 0 \\ \iff & \langle u| X_h |u\rangle - \langle u| U X_g U^\dagger |u\rangle \geq 0 && \forall |u\rangle \\ \iff & \langle u| U X_g U^\dagger |u\rangle \leq 1 && \forall \{|u\rangle \mid \langle u| X_h |u\rangle = 1\} \end{aligned}$$

which in turn corresponds to the statement that every point denoted by $|u\rangle$ that is on the h ellipsoid must be on or inside the g ellipsoid. Note that if $\langle x_h\rangle - \langle x_g\rangle = 0$ then for $|u\rangle = |w\rangle$ the inequality saturates. This in turn means that even for $\mathcal{E}_h(|w\rangle)$ the inequality is saturated as it is the same vector up to a scaling. The difference is that $\mathcal{E}_h(|w\rangle)$ represents a point on the h ellipsoid. Since the inequality is saturated it means that the ellipsoids must touch at this point. Thus $\mathcal{E}_g(|w\rangle) = \mathcal{E}_h(|w\rangle)$ which one can check explicitly as well.

B.3 Weingarten Map

One way of evaluating the curvature at a point on the ellipsoid is to find a coordinate system with its origin on the said point and then consider the manifold, locally, as a function from $n-1$ coordinates to one coordinate, call it $x_n(x_1, x_2 \dots x_{n-1})$. The curvature of this object will be a generalisation of the second derivative which forms a matrix with its elements given by $\partial^2 x_n / \partial x_i \partial x_j$. The eigenvectors of this matrix are the principle directions of curvature and the corresponding eigenvalues are the curvature values.

For a normalised direction vector $|n\rangle$ the support function (see Section 2.5 of [16]) corresponding to an ellipsoid $X = \text{diag}(x_1, x_2 \dots)$ is given by

$$h(n) = \sqrt{\langle n| X^{-1} |n\rangle} = \sqrt{\sum_i x_i^{-1} n_i^2}. \tag{5}$$

The derivative of the support function, $\partial h / \partial n_i = \frac{x_i^{-1} n_i}{h(n)}$, yields the point on the ellipsoid where the tangent plane corresponding to the direction $|n\rangle$ touches the said ellipsoid, i.e. the normal at the point $\sum_i \partial h / \partial n_i |i\rangle$ is given by $|n\rangle$. The second derivative of the support function, known as the reverse Weingarten map,

$$\partial_j \partial_i h(n) = \frac{1}{h} \left(-\frac{x_j^{-1} x_i^{-1} n_i n_j}{h^2} + x_i^{-1} \delta_{ij} \right) \tag{6}$$

contains as eigenvalues the radii of curvature at the aforesaid point and as eigenvectors the principle directions of curvature, except for $|n\rangle$ which happens to be an eigenvector with zero eigenvalue. The curvature value is the inverse of the radius of curvature. The Weingarten map can be computed by inverting the reverse Weingarten map. If instead of the normal only the point is known, at which this map must be evaluated, then one can use the gradient to first find this normal and then apply the aforesaid. The normal at a point of contact $|c\rangle = \sum_i c_i |i\rangle$ is $|n(c)\rangle = \sum_i x_i c_i |i\rangle / \sqrt{\sum_j x_j^2 c_j^2}$.

B.4 Curvature and Reduction

Let the size of the matrices X_g and X_h be $n \times n$. We had concluded that the curvature of the $\mathcal{E}_{X_g}$ ellipsoid at the point $|v\rangle / \sqrt{\langle v| X_g |v\rangle}$ must be more than the curvature of the $\mathcal{E}_{X_h}$ ellipsoid at the point $|w\rangle / \sqrt{\langle w| X_h |w\rangle}$. To make this precise, let the reverse Weingarten maps at these points be $W_g = \sum_{i=1}^{n-1} c_{g_i}^{-1} |t_{g_i}\rangle \langle t_{g_i}|$ and $W_h = \sum_{i=1}^{n-1} c_{h_i}^{-1} |t_{h_i}\rangle \langle t_{h_i}|$ respectively ($\{|t_{g_i}\rangle\}$ lie in the tangent plane of the X_g ellipsoid at $|v\rangle / \sqrt{\langle v| X_g |v\rangle}$; similarly for $\{|t_{h_i}\rangle\}$).

There is some $\tilde{O}_{ij} \in \mathbb{R}$ satisfying $\sum_j \tilde{O}_{ij} \tilde{O}_{jk} = \delta_{ik}$, such that the required solution can be written as

$$\begin{aligned} O &= |n_h\rangle \langle n_g| + \sum_{i,j} \tilde{O}_{ij} |t_{h_i}\rangle \langle t_{g_j}| \\ &= \left(\underbrace{|n_h\rangle \langle n_h| + \sum_{i,j} \tilde{O}_{ij} |t_{h_i}\rangle \langle t_{h_j}|}_{=O^{(n-1)}} \right) \left(\underbrace{|n_h\rangle \langle n_g| + \sum_i |t_{h_i}\rangle \langle t_{g_i}|}_{=\bar{O}^{(n)}} \right) \end{aligned}$$

where $|n_g\rangle$ and $|n_h\rangle$ are the normal vectors (not to be confused with the size of the matrix, n) and $O^{(n-1)}$ is a unitary that acts on the tangent space of the X_h ellipsoid. The Weingarten map W_g gets transformed to $O W_g O^T$ when X_g is rotated to $O X_g O^T$. Consider the point $|w\rangle / \sqrt{\langle w| X_h |w\rangle}$, which is shared by both the $\mathcal{E}_{X_h}$

and the $\mathcal{E}_{OX_gO^T}$ ellipsoid. It must be so that along all directions in the tangent plane, the X_h ellipsoid (the smaller one, remember larger X_h means smaller ellipsoid) must have a smaller radius of curvature than the OX_gO^T ellipsoid, i.e. for all $|t\rangle \in \text{span}\{\left|t_{h_i}\right\rangle\}$, $\langle t| W'_h |t\rangle \leq \langle t| OW'_gO^T |t\rangle$. Restricting to the tangent space, without loss of generality as the eigenvalue along the normal vector is anyway zero, one can deduce that the statement is equivalent to $W_h \leq OW_gO^T$. Explicitly, it means $\sum_{i=1}^{n-1} c_{h_i}^{-1} \left|t_{h_i}\right\rangle \left\langle t_{h_i}\right| \leq \sum_{i=1}^{n-1} c_{g_i}^{-1} O \left|t_{g_i}\right\rangle \left\langle t_{g_i}\right| O^T$. Using the form of O deduced above, one obtains $\sum_{i=1}^{n-1} c_{h_i}^{-1} \left|t_{h_i}\right\rangle \left\langle t_{h_i}\right| \leq \sum_{i=1}^{n-1} c_{g_i}^{-1} O^{(n-1)} \left|t_{h_i}\right\rangle \left\langle t_{h_i}\right| O^{(n-1)T}$. This in turn entails

$$X_h^{(n-1)} \geq O^{(n-1)} X_g^{(n-1)} O^{(n-1)T}$$

where $X_h^{(n-1)} := \text{diag}(c_{h_1}, c_{h_2} \dots c_{h_{n-1}})$ and $X_g^{(n-1)} := \text{diag}(c_{g_1}, c_{g_2} \dots c_{g_{n-1}})$. This is of the same form as the one we started with, except in one less dimension. It remains to show that the equality constraint involving the vectors also has the corresponding form. Substitute in $O|v\rangle = |w\rangle$ the form of O as determined earlier, i.e.

$$O = \left(\left|n_h^{(n)}\right\rangle \left\langle n_h^{(n)}\right| + O^{(n-1)}\right) \bar{O}^{(n)}$$

to obtain $\left(|n_h\rangle \langle n_h| + O^{(n-1)}\right) \bar{O}^{(n)} |v\rangle = |w\rangle$. Since $O^{(n-1)}$ can not influence the $|n_h\rangle$ component of the vector $\bar{O}^{(n)} |v\rangle$, one can project it out to obtain

$$O^{(n-1)} \underbrace{\left(\bar{O}^{(n)} |v\rangle - \langle n_h| \bar{O}^{(n)} |v\rangle |n_h\rangle\right)}_{:=\left|v^{(n-1)}\right\rangle}$$
$$= \underbrace{|w\rangle - \langle n_h|w\rangle |w\rangle}_{:=\left|w^{(n-1)}\right\rangle}$$

which has the claimed form, concluding the demonstration.

B.5 Connection with Operator Monotone Functions

Using the notation from Section 4, let $[\chi, \xi]$ be the smallest interval containing the spectra of both X_h and X_g. Assume that the eigenvectors of X_h which have no overlap with $|w\rangle$ have eigenvalue ξ; similarly for X_g, $|v\rangle$ and χ. The claim is that the matrix instance $\underline{X} = (X_h, X_g, |w\rangle, |v\rangle)$ has a solution if and only if $\langle w| X_h |w\rangle \geq \langle v| X_g |v\rangle$ and $\langle w| f_\lambda(X_h) |w\rangle \geq \langle v| f_\lambda(X_g) |v\rangle$ for all $\lambda \in (-\infty, -\xi) \cup (-\chi, \infty)$. Further, if the solution is tight, then either $\langle w| X_h |w\rangle = \langle v| X_g |v\rangle$ or there exists a λ in the stated range such that $\langle w| f_\lambda(X_h) |w\rangle = \langle v| f_\lambda(X_g) |v\rangle$.

This result also admits an intuitive geometric interpretation. To establish $\mathcal{E}_{X_h}$ is inside $\mathcal{E}_{OX_gO^T}$, which essentially means we look at all different directions and make sure the h ellipsoid is inside the g ellipsoid, we can instead look along a single direction $|w\rangle$ and check that all the different ellipsoids $\mathcal{E}_{f(X_h)}$ are inside the corresponding $\mathcal{E}_{Of(X_g)O^T}$ ellipsoids along just this direction, for every operator monotone f in the class indicated earlier.

The statement essentially follows from a combination of two results: (1) the generalisation of Corollary 3.18 of [2] (which characterises EBM functions on $[0, \Lambda]$ using operator monotone functions) to an arbitrary interval $[\chi, \xi]$ and (2) the connection between the set of EBRM functions K'_Λ and the set of EBM functions K_Λ (see Subsection B.1). The qualification about the tightness of the solution can be proved by using $X_h > X_g$ if and only if $f_\lambda(X_h) > f_\lambda(X_g)$.

ACKNOWLEDGMENTS

We are thankful to Nicolas Cerf, Mathieu Brandeho and Ognyan Oreshkov for various insightful discussions. We acknowledge support from the Belgian Fonds de la Recherche Scientifique – FNRS under grants no F.4515.16 (QUICTIME) and R.50.05.18.F (QuantAlgo). ASA further acknowledges the FNRS for support through the FRIA grants 3/5/5 – MCF/XH/FC – 16754 and F 3/5/5 – FRIA/FC – 6700 FC 20759.

REFERENCES

[1] N Aharon and J Silman. 2010. Quantum dice rolling: a multi-outcome generalization of quantum coin flipping. *New Journal of Physics* 12, 3 (mar 2010), 033027. https://doi.org/10.1088/1367-2630/12/3/033027

[2] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. 2014. A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias. *SIAM J. Comput.* 45, 3 (jan 2014), 633–679. https://doi.org/10.1137/14096387x arXiv:1402.7166

[3] Andris Ambainis. 2004. A new protocol and lower bounds for quantum coin flipping. *J. Comput. System Sci.* 68, 2 (2004), 398–416. https://doi.org/10.1016/j.jcss.2003.07.010 arXiv:quant-ph/0204022

[4] André Chailloux, Gus Gutoski, and Jamie Sikora. 2013. Optimal bounds for semi-honest quantum oblivious transfer. (2013). arXiv:1310.3262v2 http://arxiv.org/abs/1310.3262v2

[5] André Chailloux and Iordanis Kerenidis. 2009. Optimal Quantum Strong Coin Flipping. In *50th FOCS*. 527–533. https://doi.org/10.1109/FOCS.2009.71 arXiv:0904.1511

[6] Andre Chailloux and Iordanis Kerenidis. 2011. Optimal Bounds for Quantum Bit Commitment. In *52nd FOCS*. 354–362. https://doi.org/10.1109/FOCS.2011.42 arXiv:1102.1678

[7] R Cleve. 1986. Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing - STOC '86*. ACM Press. https://doi.org/10.1145/12130.12168

[8] Maor Ganz. 2009. Quantum Leader Election. (2009). arXiv:0910.4952v2 https://arxiv.org/abs/0910.4952v2

[9] I. Kerenidis and A. Nayak. 2004. Weak coin flipping with small bias. *Inform. Process. Lett.* 89, 3 (feb 2004), 131–135. https://doi.org/10.1016/j.ipl.2003.07.007

[10] A. Kitaev. 2003. Quantum coin flipping. (2003). Talk at the 6th workshop on Quantum Information Processing.

[11] Carlos Mochon. 2005. Large family of quantum weak coin-flipping protocols. *Phys. Rev. A* 72 (2005), 022341. https://doi.org/10.1103/PhysRevA.72.022341 arXiv:quant-ph/0502068

[12] Carlos Mochon. 2007. Quantum weak coin flipping with arbitrarily small bias. *arXiv:0711.4114* (2007). arXiv:0711.4114

[13] Ashwin Nayak and Peter Shor. 2003. Bit-commitment-based quantum coin flipping. *Phys. Rev. A* 67 (Jan 2003), 012304. Issue 1. https://doi.org/10.1103/PhysRevA.67.012304

[14] Ashwin Nayak, Jamie Sikora, and Levent Tunçel. 2014. A search for quantum coin-flipping protocols using optimization techniques. *Mathematical Programming* 156, 1-2 (may 2014), 581–613. https://doi.org/10.1007/s10107-015-0909-y arXiv:1403.0505

[15] Ashwin Nayak, Jamie Sikora, and Levent Tunçel. 2015. Quantum and classical coin-flipping protocols based on bit-commitment and their point games. (2015). arXiv:1504.04217v1 http://arxiv.org/abs/1504.04217v1

[16] Rolf Schneider. 2009. *Convex Bodies: The Brunn-Minkowski Theory.* Cambridge University Press. https://doi.org/10.1017/cbo9781139003858

[17] Barry Simon. 2009. *Convexity.* Cambridge University Press. https://doi.org/10.1017/cbo9780511910135

[18] R. W. Spekkens and Terry Rudolph. 2002. Quantum Protocol for Cheat-Sensitive Weak Coin Flipping. *Physical Review Letters* 89, 22 (nov 2002). https://doi.org/10.1103/physrevlett.89.227901