A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias

Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, Lock Magnin

A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias

Dorit Aharonov*, André Chailloux†, Maor Ganz*,
Iordanis Kerenidis‡, and Loïck Magnin*

March 3, 2014

Mochon's proof [Moc07] of existence of quantum weak coin flipping with arbitrarily small bias is a fundamental result in quantum cryptography, but at the same time one of the least understood. Though used several times as a black box in important follow-up results [Gan09, CK09, AS10, CK11, KZ13] the result has not been peer-reviewed, its novel techniques (and in particular Kitaev's point game formalism) have not been applied anywhere else, and an explicit protocol is missing. We believe that truly understanding the existence proof and the novel techniques it relies on would constitute a major step in quantum information theory, leading to deeper understanding of entanglement and of quantum protocols in general. In this work, we make a first step in this direction. We simplify parts of Mochon's construction considerably, making about 20 pages of analysis in the original proof superfluous, clarifying some other parts of the proof on the way, and presenting the proof in a way which is conceptually easier to grasp. We believe the resulting proof of existence is easier to understand, more readable, and certainly verifiable. Moreover, we analyze the resources needed to achieve a bias ε and show that the number of qubits is $O(\log \frac{1}{\varepsilon})$, while the number of rounds is $\left(\frac{1}{\varepsilon}\right)^{O(\frac{1}{\varepsilon})}$. A true understanding of the proof, including Kitaev's point-game techniques and their applicability, as well as completing the task of constructing an explicit (and also simpler and more efficient) protocol, are left to future work.

Introduction

Coin flipping is a cryptographic primitive that enables two distrustful and far apart parties, Alice and Bob, to create a random bit that remains unbiased even if one of the players tries to force a specific outcome. It was first proposed by Blum [Blu83] and has since found numerous applications in two-party secure computation [Gol09]. In the classical world, coin flipping is possible under computational assumptions, such as the hardness of the factoring or the discrete log problems. However, in the information theoretical setting, i.e., without any computational

*The School of Computer Science and Engineering, The Hebrew University of Jerusalem, Israel
†SECRET Project — INRIA Rocquencourt, 78153 Le Chesnay Cedex, France
‡LIAFA, Université Paris Diderot; CNRS

assumptions, it has been shown by Cleve [Cle86] that in any classical protocol, one of the players can always force his or her desired outcome with probability 1.

Quantum information has given us the opportunity to revisit the notion of information theoretical security in cryptography. The first breakthrough result was a protocol of Bennett and Brassard [BB84] that showed how to securely distribute a secret key between two players in the presence of an omnipotent eavesdropper. Thenceforth, a long series of work has focused on which other cryptographic primitives are possible with the help of quantum information. Unfortunately, the subsequent results were not positive. Mayers [May97] and Lo and Chau [LC97] proved the impossibility of secure quantum bit commitment and oblivious transfer and consequently of any type of two-party secure computation [May97, LC97, DKSW07]. However, several weaker variants of these primitives have been shown to be possible [HK04, BCH+08].

The case of coin flipping is one of the most intriguing primitives in this respect. Even though the results of Mayers and of Lo and Chau show that information theoretically secure perfect coin flipping (i.e. where the resulting coin is perfectly unbiased) is impossible also in the quantum world, they left open the question of whether one can construct a quantum coin flipping protocol where no player could bias the coin with probability arbitrarily close to 0. The subject of this paper is exactly this question; we start with some historical background.

Quantum coin flipping We begin with a more precise definition of coin flipping. Two variants of quantum coin flipping (CF) have been studied: *strong coin flipping* and *weak coin flipping*. A strong coin flipping protocol with bias ε is a protocol in which Alice and Bob exchange messages such that the following holds. First, if both players follow the protocol, then they agree on the outcome and the outcome is 0 or 1 with equal probability. Moreover, it is guaranteed that neither Alice nor Bob can force the outcome 0 or 1 with probability more than $1/2 + \varepsilon$, if they try to cheat. In other words, no dishonest player (playing against an honest player) can bias the coin towards *any* of the outcomes with probability higher than ε. For weak coin flipping (WCF), Alice and Bob have an *a priori* desired coin outcome. In other words the two values of the coin can be thought of as 'Alice wins' and 'Bob wins'. A weak coin flipping protocol with bias ε guarantees that no dishonest player (playing against an honest player) can bias the coin towards his or her desired outcome with probability greater than ε. The subtle difference between the weak and strong CF versions seems unimportant at first sight; indeed, in the classical setting it does not make a difference. In the quantum world, however, the two are very different. Note that obviously, strong CF implies weak CF with the same bias.

Aharonov, Ta-Shma, Vazirani, and Yao [ATSVY00] provided the first quantum strong CF protocol with bias bounded below 1/2; strictly speaking, their bias was $\varepsilon < 0.4143$. Then, Ambainis [Amb04] described a quantum strong CF protocol with an improved bias of 1/4. Subsequently, a number of different protocols have been proposed [SR01, NS03, KN04] that achieved the same bound of 1/4.

On the other side, in a breakthrough result, Kitaev [Kit03] proved a lower bound on the best possible bias of any strong CF protocol. Using a formulation of quantum CF protocols as semidefinite programs, and the duality of semidefinite programming, he showed that the bias of any strong CF protocol is bounded from below by $1/\sqrt{2} - 1/2$ (for a proof see e.g. [ABDR04]). Kitaev's result rules out the existence of strong quantum CF protocols with arbitrarily small bias. Historically, this result had a positive, rather than a negative effect; it highlighted the fact that the difference between weak and strong CF is meaningful in the quantum setting, since its proof does not apply to the weak case. Hence, this negative result in fact gave hope that a quantum WCF protocol with arbitrarily small bias might exist.

Around that time, a series of works started to provide better and better understanding of

WCF. First, Spekkens and Rudolph [SR02] constructed a WCF protocol with bias $1/\sqrt{2}-1/2$. This is a strange coincidence, since Kitaev's lower bound of $1/\sqrt{2}-1/2$ applies solely for strong CF protocols and not for weak ones. Ambainis [Amb04] then proved that the number of rounds of communication between Alice and Bob for achieving a bias of ε in a (weak or strong) CF protocol is lower-bounded by $\Omega(\log\log 1/\varepsilon)$, and thus a WCF protocol with arbitrarily small bias, if exists, cannot be achieved with a constant number of rounds. Mochon then described a WCF protocol with bias 0.192 [Moc04]; this was the first result in which Kitaev's lower bound on strong CF was broken by an explicit WCF protocol. Mochon later showed that this protocol was a member of a family of protocols, the best ones achieving a bias of 1/6 [Moc05]. Finally, in a breakthrough result, Mochon resolved the question of the existence of near-perfect quantum weak coin flipping to the affirmative, and proved the existence of a protocol with bias ε for any $\varepsilon > 0$ [Moc07].

The work of Mochon is a major advance not only because of its result, which resolved an intriguing question which was open for a long time, but also, and perhaps mainly, because of its techniques. The central tool, used also in Mochon's earlier work [Moc05] is a formalism due to Kitaev, of *point games*. In this formalism, a protocol which is a sequence of unitaries to be applied by Alice and Bob in turns, is viewed as a semidefinite program; the dual of this program provides a bound on the security of the protocol; and, most importantly, the pair of primal and dual together are represented by *a sequence of sets of points on the 2-dimensional plane*, called a *point game*. The aim is then to construct such point games whose parameters correspond to a protocol with arbitrarily small bias. This project is highly complicated and was approached by Mochon using further ideas related to operator monotone functions; in his work achieving the almost perfect protocol [Moc07], Mochon further develops the techniques to time *independent* point games, (which he attributes to Kitaev as well); he applies quite heavy analysis to derive time independent point games with bias arbitrarily close to zero.

There have been several interesting applications of this result so far. Ganz [Gan09] and Aharon and Silman [AS10] derived a quantum leader election protocol of logarithmically many rounds, using Mochon's protocol as a subroutine. Leader election is a cryptographic primitive which generalizes CF to n players who need to choose a leader among them with equal probability. Chailloux and Kerenidis [CK09] used the result of almost perfect WCF to derive an optimal strong coin flipping protocol, of the best bias possible, namely $1/\sqrt{2}-1/2+\delta$ for arbitrarily small δ. They do this using a classical reduction from any weak CF protocol with bias ε to a strong CF protocol with bias at most $1/\sqrt{2}-1/2+2\varepsilon$. This closed the question of strong CF since this result is tight, given Kitaev's lower bound on strong CF. Mochon's weak CF protocol has also beed used in a quantum reduction to derive an optimal quantum bit commitment protocol [CK11]. More recently, this protocol has been used to allow two players to achieve correlated equilibria of games without any computational assumptions and without a mediator [KZ13].

Undoubtedly, Mochon's result is a fundamental result in quantum cryptography. Nevertheless, it remained so far one of the least understood results. In particular, the paper was not peer-reviewed, and no explicit protocol is known or had been derived from this existence proof. Moreover, all the applications of the result mentioned above use the result as a black box, and its novel and beautiful techniques were never given another interpretation, or applied in any other context. Perhaps this lack of understanding, almost 7 years after the result was derived, can be attributed at least in part to the fact that Mochon's paper is 80-page long and extremely technical. The paper delves into semidefinite programming duality, operator monotone functions, perturbation theory, time dependent and time independent point games and, in the end, arrives at an existence proof of a protocol which is non-explicit and cannot be

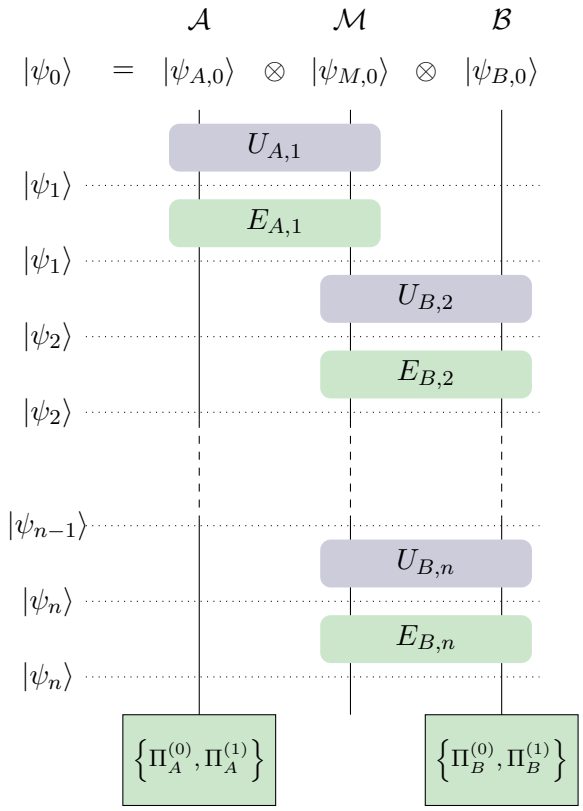

Figure 1: Representation of a coin flipping protocol. Alice and Bob start with a separable state on the spaces $\mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$. At every odd round i Alice applies a unitary $U_{A,i}$ and a projection $E_{A,i}$ on the space $\mathcal{A} \otimes \mathcal{M}$ and at every even round i Bob applies a unitary $U_{B,i}$ and a projection $E_{B,i}$ on the space $\mathcal{M} \otimes \mathcal{B}$. At the end, they measure their private registers to obtain their final outcomes.

described in a simple interactive manner between Alice and Bob.

We believe that an understanding of the proof of Mochon's breakthrough result and its techniques would constitute a major advance in quantum information theory, quantum cryptography, and quantum protocols. Possibly, it will also deepen our understanding of the flippant notion of quantum entanglement, since in essence, quantum CF is simply a protocol to distribute entanglement (more precisely, an EPR state) between two parties, where at least one of them is honest. Such an understanding of the result should probably be demonstrated by an understandable and an explicit description of a CF protocol. The contribution of this paper is far from achieving these important goals, but we believe it constitutes an important step, in that it provides a simpler, shorter proof, which is readable and verifiable, and also whose structure is conceptually comprehensible. We proceed to provide an overview of the proof and subsequently describe where and in what ways this proof deviates from Mochon's proof.

Overview of the proof

Step 1: SDPs and dual feasible points. A CF protocol is defined as in Figure 1. The first step involves presenting such an interactive protocol in terms of a semidefinite program. Define Bob's optimal cheating probability P_B^* to be the maximum probability (over any possible strategy of

Bob) that Alice outputs "1" when she plays honestly, that is, she declares Bob the winner of the coin flip. Likewise, define P_A^* to be the maximum probability (over any possible strategy of Alice) that Bob declares Alice to be the winner and outputs "0".

We can write P_B^* as the value of a semidefinite program as follows. For each round i, we consider a variable $\rho_{AM,i}$, which is the reduced density matrix of the state at time i for the union of Alice's and the message qubits. The constraints on those variables are of two types. At her turn, Alice honestly applies the operation $U_{A,i}$ (as well as a projection $E_{A,i}$, which we add for technical reasons). This happens at every odd round i. On even rounds, we only require that Alice's state on the space $\mathcal{A}$ does not change; this follows from the fact that Bob is the one to operate at those steps. We now optimize over all variables that satisfy these constraints; this corresponds to Bob optimizing his operations, in order to maximize the probability that at the end of the protocol Alice gets the outcome "1", when she performs her final projection. (Theorem 1). We can of course write P_A^* similarly as a semindefinite program with variables involving Bob's reduced density matrices.

This primal formulation is, unfortunately, not suitable for proving upper bounds on the cheating probabilities P_A^* and P_B^*, since they are defined by a maximization: any set of matrices $\{\rho_i\}$ that satisfies the constraints will lead to a lower bound on the cheating probabilities, rather than an upper bound.

We therefore consider the dual of these semidefinite programs (Theorem 2). For each primal constraint, i.e. for each protocol round, we define a dual variable $Z_{A,i}$, which is a positive semidefinite matrix that satisfies certain constraints (that arise from dualizing the primal constraints). Since the constraints are on matrices, so are the variables $Z_{A,i}$ of this dual program. Any solution of the dual program is referred to as a *dual feasible point*, and can be shown to provide an *upper bound* on Bob's optimal cheating probability, by the duality of semidefinite programming. In fact, it turns out that $P_B^* \leq \langle\psi_0|Z_{A,0} \otimes \mathbb{I}_{\mathcal{M}} \otimes \mathbb{I}_{\mathcal{B}}|\psi_0\rangle$, where $|\psi_0\rangle$ is the initially shared separable state. In other words, a dual feasible point, which is a set of matrices $\{Z_{A,i}\}$ satisfying certain constraints, can be seen as a witness to the security of the protocol against a cheating Bob. Similarly, we can write a dual SDP for Alice's cheating probability P_A^* and upper bound P_A^* by a dual feasible point $\{Z_{B,i}\}$ as $P_A^* \leq \langle\psi_0|\mathbb{I}_{\mathcal{A}} \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_{B,0}|\psi_0\rangle$.

Our goal is to find a WCF protocol, together with two dual feasible points (one for a cheating Alice and one for a cheating Bob) which would provide a certificate for the security of the protocol. Ideally, we would like to optimize over all such protocols to find the best CF protocol, and find the best possible bias. However, even though given a protocol one can find an upper bound on the cheating probability via the dual semidefinite program, this formulation of coin flipping does not provide any intuition on what type of protocols one should be looking for. The solution proposed by Mochon, following Kitaev, consists of finding a different but equivalent representation of the problem.

Step 2: Point games with EBM transitions. Kitaev [Moc07] defined a graphical way of representing a WCF protocol accompanied with two dual feasible points, one for Alice and one for Bob. He called this representation *point games*. At a high level, a point game is an ordered sequence of (possibly unnormalized) probability distributions supported each on some finite set of points on the 2-dimensional plane. (See for example Figure 2).

How are point games connected to WCF protocols and their two dual feasible points? Recall that we have bounded P_B^* by the quantity $\langle\psi_0|Z_{A,0} \otimes \mathbb{I}_{\mathcal{M}} \otimes \mathbb{I}_{\mathcal{B}}|\psi_0\rangle$ and likewise $P_A^* \leq \langle\psi_0|\mathbb{I}_{\mathcal{A}} \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_{B,0}|\psi_0\rangle$. The point game we associate with the protocol and its dual feasible points is in fact a 2-dimensional representation of the evolution of the above quantities during the protocol. More precisely, we consider the expression $\langle\psi_{n-i}|Z_{A,n-i} \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_{B,n-i}|\psi_{n-i}\rangle$ for

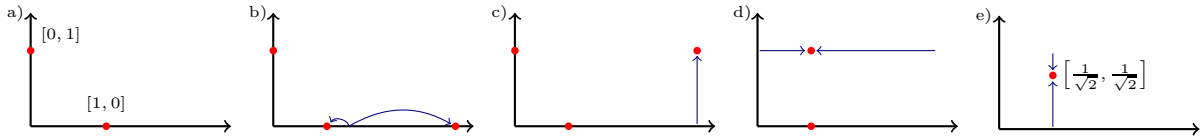

Figure 2: A "simple" point game for the [SR02] protocol with bias $1/\sqrt{2}-1/2$. The game starts with the uniform distribution over two points. The first transition, between a) and b), is a horizontal transition as the point on the x-axis is split into two points. The second transition, between b) and c) is a vertical transition as one point is raised vertically. The last two transitions are two merges, respectively horizontally and vertically. We omitted the weights of the points in the distributions to simplify the drawings.

i going from 0 to n. For each i, we associate to the above expression a distribution over points on the plane as follows. Consider the measurement of the honest state $|\psi_{n-i}\rangle$ by the observable $Z_{A,n-i} \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_{B,n-i}$. The possible outcomes can be identified with pairs of eigenvalues of the form $[z_A, z_B]$ (where z_A is an eigenvalue of $Z_{A,n-i}$ and likewise z_B is an eigenvalue of $Z_{B,n-i}$); the weight assigned to such a pair is the projection of the honest state at time $(n-i)$ onto the eigenspace corresponding to these eigenvalues. This associates with any protocol of n rounds and its dual feasible points a sequence of size n of probability distributions over points in the plane.

A key point is to classify what kind of distributions and transitions can originate from WCF protocols and two dual feasible points. As a start, it turns out that the point game that one derives this way must start with an initial uniform distribution over the two points $[0,1]$ and $[1,0]$; and a final set of points that consists of a single point $[\beta, \alpha]$. The initial uniform distribution corresponds to the fact that for an honest protocol both players agree that Alice wins with probability $1/2$ (the $[1,0]$ point) and they both agree that Bob wins with probability $1/2$ (the $[0,1]$ point). Moreover, the coordinates of the final point provide upper bounds on the optimal cheating probabilities, $P_A^* \leq \alpha$ and $P_B^* \leq \beta$.

Our goal is now to find the exact rules that the distributions and transitions between them must satisfy if they arise from a WCF and two dual feasible points. The idea is that if we have such a point game which satisfies these rules, we can (at least in principle) derive a protocol and a security guranteee from it.

To understand what transitions may occur in a point game that arises from a WCF protocol and its dual feasible points, consider two rules. First, the fact that at each round of the protocol only Alice or Bob act non-trivially on the state, is translated to the dual constraints $Z_{A,i-1} = Z_{A,i}$ for even i and $Z_{B,i-1} = Z_{B,i}$ for odd i. This implies that at even steps the points are redistributed along vertical lines whereas at odd steps they are redistributed along horizontal lines (See Figure 2).

The second rule describes how a set of points may move along the same vertical or horizontal line during one step. This is solely derived from the requirement that the operations of the cheating players must be quantum operations. More specifically, let us describe how a set of points S with first coordinates $\{x_j\}_{j\in S}$, the same second coordinate y and weights $\{w_j\}_{j\in S}$ can transition to a set of points S' with first coordinates $\{x'_k\}_{k\in S'}$, the same second coordinate y and weights $\{w'_k\}_{k\in S'}$, i.e. a horizontal transition. Let us represent the first set of points and its distribution by the function l with finite support such that $l(x_j) = w_j$, and $l(x) = 0$ everywhere else; and the second set of point and its distribution by the function r with finite support such that $r(x'_k) = w'_k$, and $r(x) = 0$ everywhere else.

Definition 1 *We say a transition from l to r is a horizontal EBM (Expressible by Matrix) line*

transition if there exist two semidefinite positive matrices $0 \preceq X \preceq Y$ *and a (not necessarily unit) vector* $|\psi\rangle$ *such that*

$$l(x) = \begin{cases} \langle\psi|\Pi_X^{[x]}|\psi\rangle & \text{if } x \in \mathrm{sp}(X) \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \quad r(x) = \begin{cases} \langle\psi|\Pi_Y^{[x]}|\psi\rangle & \text{if } x \in \mathrm{sp}(Y) \\ 0 & \text{otherwise} \end{cases}$$

where $\Pi_X^{[x]}$ *is the projector onto the eigenspace of* X *of eigenvalue* x *and* $\mathrm{sp}()$ *denotes the spectrum of the matrix.*

A transition from p *to* q *is a horizontal EBM transition if it is a horizontal EBM line transition on every horizontal line. Vertical EBM transitions are defined by symmetry. An EBM point game consists of a sequence of EBM transitions.*

It is rather easy to prove that the point games that arise from a WCF protocol and its dual feasible points are in fact EBM point games. The matrices X and Y will be defined through the dual feasible points $\{Z_{A,i}\}$ and $\{Z_{B,i}\}$ and the constraint $X \preceq Y$ will immediately follow from the dual constraints.

More importantly, the reverse implication is also true (Theorem 3): if there exists an EBM point game with initial uniform distribution $\frac{1}{2}[0,1]+\frac{1}{2}[1,0]$ and a final distribution concentrated on the point $[\beta,\alpha]$, then there exists a WCF protocol with optimal cheating probabilities $P_A^* \leq \alpha$ and $P_B^* \leq \beta$ and dual feasible points witnessing these upper bounds.

We note that the proof of this theorem is non-constructive. An EBM point game implies that for every line transition there exist matrices X and Y and a vector $|\psi\rangle$ that would witness the fact that it is an EBM line transition. However, we do not know yet of any algorithm better than brute-force for finding these matrices and vector, even when we know that they exist. Note that once these matrices and vectors are known, then we can efficiently construct a WCF protocol.

The equivalence between EBM point games and WCF protocols together with their dual feasible points, is still a bit of a mystery. This can in fact be tracked back to Kitaev's proof of the lower bound on strong coin flipping, which is far simpler but still contains the same "magic".

Nevertheless, we have reduced the question of existence of a WCF protocol with bias ε to that of the existence of an EBM point game with final point $[1/2+\varepsilon, 1/2+\varepsilon]$.

Step 3: Point games with valid transitions. Unfortunately, finding an EBM point game does not seem to be an easy task; yet another reduction is required. We will use a different characterisation of EBM transitions which is easier to work with. Let us first make some small technical detour and shift the view from *transitions* to *functions*. We denote the EBM transition from l to r (who are non-negative functions with finite support) by the *EBM function* $(r-l)$, which is also a function with finite support, but this time it can have positive as well as negative values. EBM functions have an interesting geometrical property: they form a convex cone. We would like to now represent EBM functions using a different language, and for that we will use duality of convex cones. Importantly, the dual of the cone of EBM functions is a well known object: it turns out to be the set of *operator monotone functions* [Bha97]. We recall that a function $f : \mathbb{R} \mapsto \mathbb{R}$ is said to be operator monotone if it preserves the order of positive definite matrices, namely, if $X \preceq Y$ as PSDs, then $f(X) \preceq f(Y)$ (also as PSDs; a function is applied on a PSD in the usual way of diagonalizing and applying the function on the eigenvalues). Consider now yet again the dual of this set. We call the dual of the set of operator monotone functions *set of valid functions*. We now use the following basic fact from convex geometry: C^{**} is the closure of the smallest convex cone containing C. Since in our case C, the set of EBM functions, is

itself a cone, this means that the sets of valid functions and EBM functions are the same, up to closures. Hence, we can show that from any point game with valid transitions, we can construct an EBM point game whose final point is arbitrarily close to the original one (Theorem 4). The map from EBM functions to valid functions, being essentially equal sets up to closures, would have been very easy had we been considering a finite dimensional space. Unfortunately, the space of functions we are handling is infinite dimensional and moreover, somewhat pathological, and hence the proof of Theorem 4 requires some technical effort. Still, in spirit, the idea is that we move to the dual of the dual and by that we gain the advantage of considering the dual of the well studied object of operator monotone functions; this turns out useful later on in the actual construction of the final point game.

The advantage is that valid functions have a very simple analytical characterization that follows from the characterisation of operator monotone functions (see Lemma 20), and hence, checking that a given function h is valid corresponds to checking two simple mathematical statements :

$$\sum_x h(x) = 0 \quad \text{and} \quad \forall \lambda > 0,\ \sum_x \frac{h(x)}{\lambda + x} \leq 0.$$

Even though verifying a valid point game is rather straightforward, finding valid point games remains again a bit of a mystery. Despite the fact that there are strong tools that enable doing this (mainly Lemma 41) there still seems to be missing an intuitive interpretation of what valid transitions are and how to construct them.

Nevertheless, finding a WCF protocol with arbitrarily small bias has been reduced to the problem of finding a point game with *valid* transitions, which ends at the point $[\beta, \alpha]$ with both α, β arbitrarily close to $1/2$.

Step 4: Time independent point game. The introduction of valid transitions makes it easier to check that a point game is valid or not. But such verification will become very tedious for point games with a bias ε which is arbitrarily small, as the number of transitions tends to infinity when ε tends to 0. More importantly, we need a tool that will help us find constructively such valid point games, rather than verifying that a given game is valid.

The last model in our sequence of reductions, also introduced by Kitaev, is called *time independent point games* (TIPG), and essentially addresses this problem. The key observation is that if f_1 and f_2 are valid functions, either both horizontal or both vertical, then $f_1 + f_2$ is also a valid function. Hence, given a valid point game with valid horizontal functions $\{h_1, h_2, \ldots, h_n\}$ and valid vertical functions $\{v_1, v_2, \ldots, v_n\}$ and final point $[\beta, \alpha]$, we can define $h = \sum_i h_i$ and $v = \sum_i v_i$, which are valid horizontal and vertical functions respectively. Moreover, we will see that if we sum these two functions then everything cancels apart form the initial and final points. In other words, we have

$$h + v = [\beta, \alpha] - \frac{1}{2}[1, 0] - \frac{1}{2}[0, 1].$$

Hence, a time independent point game is defined as one valid horizontal function h, one valid vertical function v, and one point $[\beta, \alpha]$, that satisfy together the above equation. Verifying that a TIPG is correct involves checking that only two functions are valid, this is in sharp contrast to point games with valid transitions.

It turns out that the reverse direction is also "approximately" true. This is the direction we will be interested in since we are about to design a TIPG and argue that it implies a valid point game. The approximate claim is that for all $\varepsilon > 0$, a TIPG with final point $[\beta, \alpha]$ and

valid functions h and v can be turned into a point game with valid transitions and final point $[\beta+\varepsilon, \alpha+\varepsilon]$ (Theorem 5), whose number of transitions depends on ε. Ideally we would like to start with the TIPG with final point $[\beta, \alpha]$ and exhibit a point game with valid transitions, with initial set of points $\frac{1}{2}[1,0] + \frac{1}{2}[0,1]$ and final point $[\beta, \alpha]$. Unfortunately, we do not know how to do this. However, there is a very nice trick that makes it possible: one can add a set of points that acts as a "catalyst", meaning that the points remain unchanged through the transitions and their weight can be made arbitrarily small, yet, they enable transitions that were not possible without them. To make this statement more precise, denote by h^-, h^+, v^-, and v^+ the negative and positive parts of the functions h and v. One can show that there exists a point game that, for any $\gamma > 0$, achieves $\frac{1}{2}[1,0] + \frac{1}{2}[0,1] + \gamma v^- \to [\beta, \alpha] + \gamma v^-$. Last, it is possible to remove completely these low-weight catalyst points in the expense of moving the final point to $[\beta+\varepsilon, \alpha+\varepsilon]$.

Hence, in the end, proving the existence of WCF protocol with arbitrarily small bias consists of designing two valid functions h and v, which define a TIPG with final point $[1/2+\varepsilon, 1/2+\varepsilon]$. This is the last model that is involved in this proof. See Figure 3 for a summary of the models.

Step 5: Construction. In this last part, we describe a family of point games with parameter k, whose final point is $[\alpha, \alpha] = [\frac{1}{2} + \frac{c}{k}, \frac{1}{2} + \frac{c}{k}]$ for some constant c; k can be made to be an arbitrarily large integer, making the bias arbitrarily small.

The game consists of three main steps (see Figure 4). First, the initial points are split into a large number of points along the axes. We assume that all points are on a grid of step ω (which will be inverse polynomial in k), and that $\Gamma\omega$ is the largest coordinate of a point (Γ will be a polynomial in k). Second, all the axes points are moved to two points $[\alpha - k\omega, \alpha]$ and $[\alpha, \alpha - k\omega]$, where $k\omega$ will be inverse polynomial in k. This is the main part of the construction. It involves a large number of other points on a grid, and all those points together form a *ladder* of height Γ: for each different height, there is one point on the axis and $2k$ points symmetrically put close to the diagonal (see Figure 5). Third, the last two points are raised to the final point $[\alpha, \alpha]$.

The main difficulty is to find weights for the points on the axes and the points in the ladder, such that the initial splits are valid and in addition the transitions that involve the points of the ladder in the second step, are also valid. We consider the second part of the point game as a TIPG and hence, we will need to prove the validity of only two functions. We show that for any k, we can find ω and Γ as functions of k such that the point game is valid and the final point is $\alpha = \frac{1}{2} + \frac{c}{k}$ for some constant c.

Finally, we analyse the resources of the protocols and prove that the number of qubits used in a protocol with bias ε is only $O(\log \frac{1}{\varepsilon})$, while the number of rounds is $\left(\frac{1}{\varepsilon}\right)^{O(\frac{1}{\varepsilon})}$ (Theorem 6).

We still do not have much intuition about this point game. The main problem being that we have no intuitive understanding of the large number of transitions that involve the points in the ladder during the second step of the protocol. It remains an open question to find a simpler construction that possibly also uses a smaller number of rounds.

Our contributions Our initial goal was to verify the correctness of Mochon's proof, and make it more easily verifiable to others, since the paper had never been formally peer-reviewed. During the process, we managed to simplify and shorten the construction. Our contribution is three-fold.

1. Our main technical contribution is to give a significantly simpler proof to go from valid transitions to EBM transitions (Theorem 4). This theorem makes the use of operator monotone functions in the paper clearer, since now they appear as the dual of the set of

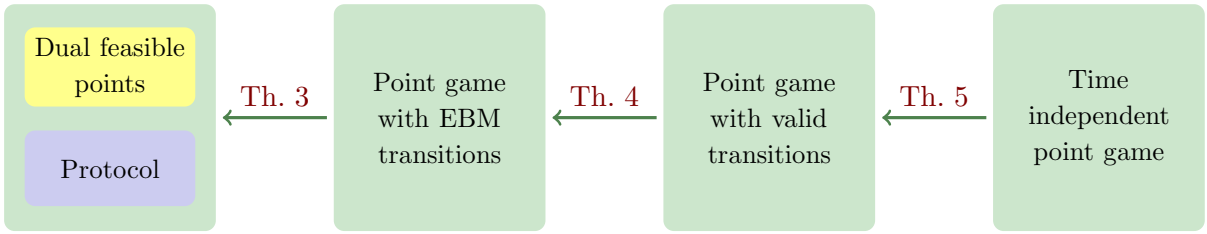

Figure 3: The succession of models we will consider. An arrow from model A to model B means that proving the existence of an ε biased protocol in A implies the existence of an $\varepsilon + \varepsilon'$ biased protocol in B (for all $\varepsilon' > 0$).

EBM functions, whereas in Mochon's paper they were not clearly motivated. Then, the definition of valid functions comes naturally as the bidual of EBM functions. We conclude the proof of the theorem by using a topological argument. This replaces about 20 pages of difficult analysis using integrals and perturbation theory in Mochon's original manuscript [Moc07, Appendix C].

2. On the conceptual side, we have reorganized Mochon's paper throughout steps 2 to 4. We emphasized the key steps of the proof and clarified some arguments which were only implicit in Mochon's paper; the proof is structurally much simpler and cleaner.

3. The point game with arbitrarily small bias that we present in Section 5 is the same as in Mochon's paper. However, in his proof he looked at the limit of $\omega \to 0$ and $\Gamma \to \infty$. While this is enough for a proof of existence, it does not give any bound on the resources needed for the protocol. Here, we make the analysis more precise and present for the first time a bound on the resources necessary to achieve bias ε. The number of qubits is $O(\log \frac{1}{\varepsilon})$ and the number of rounds is at most $\left(\frac{1}{\varepsilon}\right)^{O(\frac{1}{\varepsilon})}$ (Theorem 6).

Hopefully this work will make Mochon's proof more understandable to the community. Our work is but the beginning rather than the end, on Mochon's important result. In particular, it remains to further understand how Kitaev's formalism can be applied in a way which is both more intuitive and more general, to this as well as to other tasks. This also includes an improvement of the construction of a TIPG (step 5), which is still very heavy and should be simplified. Moreover, much of the proof is still non-explicit, and we believe this should also be attributed to our lack of understanding of it. It remains to find an explicit description of a WCF protocol that achieves bias ε for any $\varepsilon > 0$. This might have of course practical implications; moreover, understanding the quantum mechanisms behind this WCF protocol could have applications to other quantum communication protocols, and in particular, to protocols that involve distribution of entanglement in an adversarial environment.

The organization of the paper follows the five steps of the proof described above.

1 SDPs and dual feasible points

1.1 Definitions

We formally define a quantum weak coin flipping protocol with bias ε.

Definition 2 (Weak coin flipping protocol (WCF) with bias ε) *For n even, an n-message weak coin flipping protocol between two players, Alice and Bob, is described by:*

- *Three Hilbert spaces $\mathcal{A}, \mathcal{B}$ corresponding to Alice and Bob private workspaces (Bob does not have any access to $\mathcal{A}$ and Alice to $\mathcal{B}$), and a message space $\mathcal{M}$;*
- *An initial product state $|\psi_0\rangle = |\psi_{A,0}\rangle \otimes |\psi_{M,0}\rangle \otimes |\psi_{B,0}\rangle \in \mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$;*
- *A set of n unitaries $\{U_1, \dots, U_n\}$ acting on $\mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$, with $U_i = U_{A,i} \otimes \mathbb{I}_{\mathcal{B}}$ for i odd, and $U_i = \mathbb{I}_{\mathcal{A}} \otimes U_{B,i}$ for i even;*
- *A set of* honest states $\{|\psi_i\rangle,\ i \in [n]\}$ *defined by $|\psi_i\rangle = U_i U_{i-1} \cdots U_1 |\psi_0\rangle$;*
- *A set of n projectors $\{E_1, \dots, E_n\}$ acting on $\mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$, with $E_i = E_{A,i} \otimes \mathbb{I}_{\mathcal{B}}$ for i odd, and $E_i = \mathbb{I}_{\mathcal{A}} \otimes E_{B,i}$ for i even, such that $E_i|\psi_i\rangle = |\psi_i\rangle$;*
- *Two final POVM $\left\{\Pi_A^{(0)}, \Pi_A^{(1)}\right\}$ acting on $\mathcal{A}$ and $\left\{\Pi_B^{(0)}, \Pi_B^{(1)}\right\}$ acting on $\mathcal{B}$.*

The WCF protocol proceeds as follows:

1. *In the beginning, Alice holds $|\psi_{A,0}\rangle|\psi_{M,0}\rangle$ and Bob $|\psi_{B,0}\rangle$.*
2. *For $i = 1$ to n:*
   — If i is odd, Alice applies U_i and measures the resulting state with the POVM $\{E_i, \mathbb{I} - E_i\}$. On the first outcome, Alice sends the message qubits to Bob; on the second outcome, she ends the protocol by outputting "0", i.e. Alice declares herself winner.
   — If i is even, Bob applies U_i and measures the resulting state with the POVM $\{E_i, \mathbb{I} - E_i\}$. On the first outcome, Bob sends the message qubits to Alice; on the second outcome, he ends the protocol by outputting "1", i.e. Bob declares himself winner.
3. *Alice and Bob measure their part of the state with the final POVM and output the outcome of their measurements. Alice wins on outcome "0" and Bob on outcome "1".*

The WCF protocol has the following properties:

- ***Correctness**: When both players are honest, Alice and Bob's outcomes are always the same: $\Pi_A^{(0)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(1)} |\psi_n\rangle = \Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(0)} |\psi_n\rangle = 0$.*
- ***Balanced:** When both players are honest, they win with probability 1/2: $P_A = \left\| \Pi_A^{(0)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(0)} |\psi_n\rangle \right\|^2 = \frac{1}{2}$ and $P_B = \left\| \Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(1)} |\psi_n\rangle \right\|^2 = \frac{1}{2}$.*
- ***ε biased:** When Alice is honest, the probability that both players agree on Bob winning is $P_B^* \leq 1/2 + \varepsilon$. And conversely, if Bob is honest, the probability that both players agree on Alice winning is $P_A^* \leq 1/2 + \varepsilon$.*

This definition of a weak coin flipping protocol differs from the usual one in the sense that we added the projections $\{E_i\}$. The goal of these projections is to catch a cheating player, since they do not change the honest states. Intuitively they can only decrease the bias compared to a protocol without them. This can be proved, but it is not necessary in our case since we will directly prove upper bounds on the cheating probabilities for this specific type of protocols.

1.2 Cheating probabilities as SDPs

The cheating probabilities P_A^* and P_B^* cannot be easily computed from the definition above. Kitaev showed that they can be expressed as semidefinite programs (SDP) [Kit03] and a written proof can be found in [ABDR04].

Fix a weak coin flipping protocol, and assume that Alice is honest. We describe a semidefinite program with variables the states $\rho_{AM,i}$, i.e. the states after round i once Bob's workspace is traced out. The probability that Bob wins is the probability that Alice outputs "1" when applying the POVM $\left\{\Pi_A^{(0)}, \Pi_A^{(1)}\right\}$ to her part of the final state, or equivalently $\mathrm{Tr}((\Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}})\rho_{AM,n})$. Since Alice is honest, the state in her workspace is not arbitrary, but rather satisfies some constraints. In the beginning of the protocol, Alice held the state $\mathrm{Tr}_{\mathcal{M}}(\rho_{AM,0}) = |\psi_{A,0}\rangle\langle\psi_{A,0}|$. Moreover, the evolution of Alice's state is only due to her own actions, namely $\mathrm{Tr}_{\mathcal{M}}(\rho_{AM,i}) = \mathrm{Tr}_{\mathcal{M}}(\rho_{AM,i-1})$ if i is even and $\mathrm{Tr}_{\mathcal{M}}(\rho_{AM,i}) = \mathrm{Tr}_{\mathcal{M}}(E_i U_i \rho_{AM,i-1} U_i^\dagger E_i)$ if i is odd. Bob's cheating probability is the maximum over all his strategies, i.e. over all states $\{\rho_{AM,i}\}$ that satisfy these constraints.

The evolution of the states $\rho_{AM,i}$ is not unitary due to the presence of the projections, so they are not necessarily normalized. However, $\mathrm{Tr}((\Pi_A^{(1)} \otimes \mathbb{I})\rho_{AM,n})$ represents the probability that Alice and Bob agree on Bob winning when Alice is honest. If Bob got caught cheating by the projections, Alice already declared herself the winner. The non-normalization of the states $\rho_{AM,i}$ reflects the probability that the protocol ended prematurely by one of the players declaring oneself winner, because the other player was caught cheating.

This reasoning leads to the following two semidefinite programs:

Theorem 1 (Primal)
$P_B^* = \max \mathrm{Tr}((\Pi_A^{(1)} \otimes \mathbb{I}_{\mathcal{M}})\rho_{AM,n})$ *over all* $\rho_{AM,i}$ *satisfying the constraints:*

- $\mathrm{Tr}_{\mathcal{M}}(\rho_{AM,0}) = \mathrm{Tr}_{\mathcal{MB}}(|\psi_0\rangle\langle\psi_0|) = |\psi_{A,0}\rangle\langle\psi_{A,0}|$;
- *for* i *odd,* $\mathrm{Tr}_{\mathcal{M}}(\rho_{AM,i}) = \mathrm{Tr}_{\mathcal{M}}(E_i U_i \rho_{AM,i-1} U_i^\dagger E_i)$;
- *for* i *even,* $\mathrm{Tr}_{\mathcal{M}}(\rho_{AM,i}) = \mathrm{Tr}_{\mathcal{M}}(\rho_{AM,i-1})$.

$P_A^* = \max \mathrm{Tr}((\mathbb{I}_{\mathcal{M}} \otimes \Pi_B^{(0)})\rho_{MB,n})$ *over all* $\rho_{BM,i}$ *satisfying the constraints:*

- $\mathrm{Tr}_{\mathcal{M}}(\rho_{MB,0}) = \mathrm{Tr}_{\mathcal{AM}}(|\psi_0\rangle\langle\psi_0|) = |\psi_{B,0}\rangle\langle\psi_{B,0}|$;
- *for* i *even,* $\mathrm{Tr}_{\mathcal{M}}(\rho_{MB,i}) = \mathrm{Tr}_{\mathcal{M}}(E_i U_i \rho_{MB,i-1} U_i^\dagger E_i)$;
- *for* i *odd,* $\mathrm{Tr}_{\mathcal{M}}(\rho_{MB,i}) = \mathrm{Tr}_{\mathcal{M}}(\rho_{MB,i-1})$.

1.3 Upper bounds on the cheating probabilities via the dual feasible points

In order to prove upper bounds on the cheating probabilities P_A^* and P_B^* we consider the dual SDPs. The following theorem provides the dual, as well as a statement that the maximum is indeed achieved and is equal to the optimal value of the primal, namely, strong duality holds. A complete proof of this theorem can be found in [Kit03, ABDR04].

Theorem 2 (Dual)
$P_B^* = \min \mathrm{Tr}(Z_{A,0}|\psi_{A,0}\rangle\langle\psi_{A,0}|)$ *over all* $Z_{A,i}$ *under the constraints:*

① $\forall i,\ Z_{A,i} \succeq 0$;

② *for* i *odd,* $Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \succeq U_{A,i}^{\dagger} E_{A,i}(Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}}) E_{A,i} U_{A,i}$;

③ *for* i *even,* $Z_{A,i-1} = Z_{A,i}$;

④ $Z_{A,n} = \Pi_A^{(1)}$.

$P_A^* = \min \mathrm{Tr}(Z_{B,0}|\psi_{B,0}\rangle\langle\psi_{B,0}|)$ *over all* $Z_{B,i}$ *under the constraints:*

① $\forall i,\ Z_{B,i} \succeq 0$;

② *for* i *even,* $\mathbb{I}_{\mathcal{M}} \otimes Z_{B,i-1} \succeq U_{B,i}^{\dagger} E_{B,i}(\mathbb{I}_{\mathcal{M}} \otimes Z_{B,i}) E_{B,i} U_{B,i}$;

③ *for* i *odd,* $Z_{B,i-1} = Z_{B,i}$;

④ $Z_{B,n} = \Pi_B^{(0)}$.

We add one more constraint to the above dual SDPs:

⑤ $|\psi_{A,0}\rangle$ is an eigenvector of $Z_{A,0}$, i.e. there exists $\beta > 0$ such that $Z_{A,0}|\psi_{A,0}\rangle = \beta|\psi_{A,0}\rangle$,

⑤ $|\psi_{B,0}\rangle$ is an eigenvector of $Z_{B,0}$, i.e. there exists $\alpha > 0$ such that $Z_{B,0}|\psi_{B,0}\rangle = \alpha|\psi_{B,0}\rangle$.

The reason why we are adding this constraint will become clear a bit later. Notice that this constraint is not positive semidefinite, and thus the following definition is a slight abuse:

Definition 3 (Dual feasible points) *We call* dual feasible points *any two sets of matrices* $\{Z_{A,0}, \ldots, Z_{A,n}\}$ *and* $\{Z_{B,0}, \ldots, Z_{B,n}\}$ *that satisfy the corresponding conditions* ① *to* ⑤.

However, this additional constraint does not change the value of the dual SDPs:

Proposition 4 $P_A^* = \inf \alpha$ *and* $P_B^* = \inf \beta$ *where the infimum is over all dual feasible points and* α, β *are defined in constraint* ⑤ *of the definition of the dual feasible points (Definition 3).*

Proof. Fix $\{Z_{A,0}, \ldots, Z_{A,n}\}$ a set of matrices that satisfies the constraints ① to ④ and $\varepsilon > 0$. Let us construct a matrix $Z'_{A,0}$ such that the set $\{Z'_{A,0}, Z_{A,1}, \ldots, Z_{A,n}\}$ satisfies the constraints ① to ⑤ with $\alpha = \mathrm{Tr}(Z'_{A,0}|\psi_{A,0}\rangle\langle\psi_{A,0}|) = \mathrm{Tr}(Z_{A,0}|\psi_{A,0}\rangle\langle\psi_{A,0}|) + \varepsilon$.

The proof relies on the following fact: there exists $\Lambda > 0$ such that:

$$Z'_{A,0} = (\langle\psi_{A,0}|Z_{A,0}|\psi_{A,0}\rangle + \varepsilon)|\psi_{A,0}\rangle\langle\psi_{A,0}| + \Lambda(\mathbb{I} - |\psi_{A,0}\rangle\langle\psi_{A,0}|) \succeq Z_{A,0}.$$

As a consequence $Z'_{A,0} \otimes \mathbb{I}_{\mathcal{M}} \succeq Z_{A,0} \otimes \mathbb{I}_{\mathcal{M}}$, hence $\{Z'_{A,0}, Z_{A,1}, \ldots, Z_{A,n}\}$ is a dual feasible point and also $\mathrm{Tr}(Z'_{A,0}|\psi_{A,0}\rangle\langle\psi_{A,0}|) = \mathrm{Tr}(Z_{A,0}|\psi_{A,0}\rangle\langle\psi_{A,0}|) + \varepsilon$.

We now prove that, indeed, there exists $\Lambda > 0$, for which $Z'_{A,0} \succeq Z_{A,0}$. Let $|\phi\rangle$ be a vector in $\mathcal{A}$ and decompose it as $|\phi\rangle = a|\psi_{A,0}\rangle + b|\psi_{A,0}^{\perp}\rangle$ where $\langle\psi_{A,0}|\psi_{A,0}^{\perp}\rangle = 0$. We can restrict ourselves to $b \in \mathbb{R}$ and $|a|^2 + |b|^2 = 1$, thus we have:

$$\langle\phi|(Z'_{A,0} - Z_{A,0})|\phi\rangle = |a|^2 \varepsilon + b^2(\Lambda - \langle\psi_{A,0}^{\perp}|Z_{A,0}|\psi_{A,0}^{\perp}\rangle) - 2b\Re(a\langle\psi_{A,0}^{\perp}|Z_{A,0}|\psi_{A,0}\rangle). \qquad (1)$$

We show how to pick a Λ independent of $|\phi\rangle$, i.e. of a, b and $|\psi_{A,0}^{\perp}\rangle$, so that the above expression is always non-negative:

Case $a = 0$ We want $\Lambda \geq \langle\psi_{A,0}^{\perp}|Z_{A,0}|\psi_{A,0}^{\perp}\rangle$ for all $|\psi_{A,0}^{\perp}\rangle$. Hence, we need to choose $\Lambda \geq \|Z_{A,0}\|$.

Case $a \neq 0$ See Equation (1) as a polynomial in b. The leading coefficient being non negative, we need to pick Λ so that the discriminant is negative. The discriminant reads $4\Re(a\langle\psi^{\perp}_{A,0}|Z_{A,0}|\psi_{A,0}\rangle)^2 - 4\,|a|^2\,\varepsilon(\Lambda - \langle\psi^{\perp}_{A,0}|Z_{A,0}|\psi^{\perp}_{A,0}\rangle)$. Since for any complex number x, $\Re(x) \leq |x|$, it is sufficient to have, $|a|^2\left|\langle\psi^{\perp}_{A,0}|Z_{A,0}|\psi_{A,0}\rangle\right|^2 - |a|^2\,\varepsilon(\Lambda - \langle\psi^{\perp}_{A,0}|Z_{A,0}|\psi^{\perp}_{A,0}\rangle) \leq 0$. Since $a \neq 0$, we want $\Lambda \geq \frac{1}{\varepsilon}(\left|\langle\psi^{\perp}_{A,0}|Z_{A,0}|\psi_{A,0}\rangle\right|^2 - \langle\psi^{\perp}_{A,0}|Z_{A,0}|\psi^{\perp}_{A,0}\rangle)$. Hence, we need to choose $\Lambda \geq \|Z_{A,0}\|^2/\varepsilon$.

Choosing $\Lambda \geq \max\{\|Z_{A,0}\|, \|Z_{A,0}\|^2/\varepsilon\}$ concludes the proof.

□

Let us note that the primal formulation sets constraints on the evolution of ρ_{i-1} to ρ_i, starting from a fixed state ρ_0, and the optimization quantity that depends on ρ_n. In the dual formulation, the constraints are on the evolution of Z_i to Z_{i-1}, starting form a fixed Z_n and the optimisation quantity depends on Z_0. For this reason we will reverse the time evolution and consider point games that run backwards in time.

2 Point games with EBM transitions

In the previous section we saw how to upper-bound the cheating probability of any weak coin flipping protocol by looking at the dual SDP formulation of the protocol and by providing dual feasible points, namely sets of matrices $\{Z_{A,0}, \ldots, Z_{A,n}\}$ and $\{Z_{B,0}, \ldots, Z_{B,n}\}$ that satisfy a number of conditions. One can think of these matrices as a security witness of the protocol.

As we have explained, in order to keep track of the two cheating probabilities together, we will be interested in the quantity $\langle\psi_i|Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_{B,i}|\psi_i\rangle$. For $i = 0$, this quantity indeed provides an upper bound on the product of the two cheating probabilities (this only holds for $i = 0$, since the state $|\psi_0\rangle$ is separable). Note also that this is the same quantity used by Kitaev in the proof of the lower bound on quantum strong coin flipping [Kit03].

This motivates the definition of EBM point games as graphical representations of the above quantity. This section is devoted to first formally defining EBM point games, and then showing that they are equivalent to WCF protocols and their dual feasible points. We first define the following function *prob*.

Definition 5 (prob) *Let Z be a positive semidefinite matrix and denote by $\Pi^{[z]}$ the projector on the eigenspace of eigenvalue $z \in \mathrm{sp}(Z)$. We have $Z = \sum_z z\Pi^{[z]}$. Let $|\psi\rangle$ be a (not necessarily unit) vector. We define the function with finite support* $\mathrm{prob}[Z, \psi] : [0, \infty) \to [0, \infty)$ *as:*

$$\mathrm{prob}[Z, \psi](z) = \begin{cases} \langle\psi|\Pi^{[z]}|\psi\rangle & \text{if } z \in \mathrm{sp}(Z) \\ 0 & \text{otherwise.} \end{cases}$$

If $Z = Z_A \otimes \mathbb{I}_{\mathcal{M}} \otimes Z_B$, using the same notation, we define the 2-variate function with finite support $\mathrm{prob}[Z_A, Z_B, \psi] : [0, \infty) \times [0, \infty) \to [0, \infty)$ *as:*

$$\mathrm{prob}[Z_A, Z_B, \psi](z_A, z_B) = \begin{cases} \langle\psi|\Pi^{[z_A]} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi^{[z_B]}|\psi\rangle & \text{if } (z_A, z_B) \in (\mathrm{sp}(Z_A), \mathrm{sp}(Z_B)) \\ 0 & \text{otherwise.} \end{cases}$$

We now define EBM transitions and EBM point games.

Definition 6 (EBM line transition) *Let $l, r : [0, \infty) \to [0, \infty)$ be two functions with finite supports. The line transition $l \to r$ is* expressible by matrices *(EBM) if there exist two positive semidefinite*

matrices $0 \preceq X \preceq Y$ *and a (not necessarily unit) vector* $|\psi\rangle$ *such that* $l = \text{prob}[X, \psi]$ *and* $r = \text{prob}[Y, \psi]$.

Definition 7 (EBM transition) *Let* $p, q : [0,\infty) \times [0,\infty) \to [0,\infty)$ *be two functions with finite supports. The transition* $p \to q$ *is an* EBM horizontal transition *if for all* $y \in [0,\infty)$, $p(\cdot, y) \to q(\cdot, y)$ *is an EBM line transition, and an* EBM vertical transition *if for all* $x \in [0,\infty)$, $p(x, \cdot) \to q(x, \cdot)$ *is an EBM line transition.*

Definition 8 (EBM point game) *An* EBM point game *is a sequence of functions* $\{p_0, p_1, \cdots, p_n\}$ *with finite support such that:*

- $p_0 = 1/2[0,1] + 1/2[1,0]$*;*
- *For all even* i, $p_i \to p_{i+1}$ *is an EBM vertical transition;*
- *For all odd* i, $p_i \to p_{i+1}$ *is an EBM horizontal transition;*
- $p_n = 1[\beta, \alpha]$.

For completeness, we first show how to go from a given WCF protocol accompanied with two dual feasible points to an EBM point game.

Proposition 9 *Given a WCF protocol with cheating probabilities* P_A^* *and* P_B^**, then, for any* $\delta > 0$*, there exists an EBM point game with final point* $[P_B^* + \delta, P_A^* + \delta]$.

Proof. From Proposition 4, we have that $P_A^* = \inf \alpha$ and $P_B^* = \inf \beta$, where the infimum is taken over all dual feasible points, α is the eigenvalue of $Z_{A,0}$ that corresponds to the eigenvector $|\psi_{A,0}\rangle$ and similarly for β. Hence, for any $\delta > 0$ there exist two dual feasible points $\{Z_{A,i}\}$ and $\{Z_{B,i}\}$ with $\alpha = P_A^* + \delta$ and $\beta = P_B^* + \delta$.

Let

$$\begin{aligned} p_{n-i} &= \text{prob}[Z_{A,i}, Z_{B,i}, \psi_i] \\ &= \sum_{(z_{A,i}, z_{B,i}) \in \left(\text{sp}(Z_{A,i}), \text{sp}(Z_{B,i})\right)} \langle \psi_i | \Pi^{[z_{A,i}]} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi^{[z_{B,i}]} | \psi_i \rangle \; [z_{A,i}, z_{B,i}]. \end{aligned} \tag{2}$$

We show that the sequence of functions $\{p_0, \ldots, p_n\}$ is indeed an EBM point game with $p_n = [P_B^* + \delta, P_A^* + \delta]$. We first get the initial and final condition:

$$\begin{aligned} p_0 &= \text{prob}[Z_{A,n}, Z_{B,n}, \psi_n] = \text{prob}[\Pi_A^{(1)}, \Pi_B^{(0)}, \psi_n] = \frac{1}{2}[1,0] + \frac{1}{2}[0,1], \\ p_n &= \text{prob}[Z_{A,0}, Z_{B,0}, \psi_0] = 1[\beta, \alpha] = [P_B^* + \delta, P_A^* + \delta]. \end{aligned}$$

Recall that we added an extra condition in Theorem 2, namely that $|\psi_{A,0}\rangle$ and $|\psi_{B,0}\rangle$ are eigenstates of $Z_{A,0}$ and $Z_{B,0}$ respectively. This condition ensures us that the game ends with one final point, and not several points.

We now show that $p_i \to p_{i+1}$ are EBM transitions. Let us assume that i is odd. According to Equation (2), the function p_{n-i} (resp. p_{n-i+1}) corresponds to the matrix Z_i (resp. Z_{i-1}) and the state $|\psi_i\rangle$ (resp. $|\psi_{i-1}\rangle$). Since i is odd, the conditions of the dual SDP state that $Z_{B,i} = Z_{B,i-1}$ and also $|\psi_i\rangle = E_{A,i} U_{A,i} \otimes \mathbb{I}_{\mathcal{B}} |\psi_{i-1}\rangle$. Using this we will now prove that the points only move horizontally and moreover, the total weight on every horizontal line remains unchanged (thus so does the total weight). To see this, write:

$$p_{n-i+1} = \sum_{(z_{A,i-1},z_{B,i-1})} \langle\psi_{i-1}|\Pi^{[z_{A,i-1}]} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi^{[z_{B,i-1}]}|\psi_{i-1}\rangle \ [z_{A,i-1}, z_{B,i-1}].$$

$$\begin{aligned} p_{n-i} &= \sum_{(z_{A,i},z_{B,i-1})} \langle\psi_i|\Pi^{[z_{A,i}]} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi^{[z_{B,i-1}]}|\psi_i\rangle \ [z_{A,i}, z_{B,i-1}], \\ &= \sum_{(z_{A,i},z_{B,i-1})} \langle\psi_{i-1}|U_{A,i}^\dagger E_{A,i}(\Pi^{[z_{A,i}]} \otimes \mathbb{I}_{\mathcal{M}})E_{A,i}U_{A,i} \otimes \Pi^{[z_{B,i-1}]}|\psi_{i-1}\rangle \ [z_{A,i}, z_{B,i-1}]. \end{aligned}$$

First, notice that $\mathrm{sp}(Z_{B,i}) = \mathrm{sp}(Z_{B,i-1})$ and hence the possible values for the second coordinate of the points remain the same. Second, the sum of the weights of the points in each horizontal line with second coordinate $z_{B,i-1}$ remains the same and equal to $\langle\psi_{i-1}|\mathbb{I}_{\mathcal{A}} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi^{[z_{B,i-1}]}|\psi_{i-1}\rangle$. Note that the projections E_i leave the honest states unchanged. Note also that for every $z_{B,i-1}$, i.e. for every horizontal line, we can define the functions

$$\begin{aligned} p_{n-i+1}(\cdot, z_{B,i-1}) &= \mathrm{prob}[Z_{A,i-1} \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi^{[z_{B,i-1}]}, \psi_{i-1}], \\ p_{n-i}(\cdot, z_{B,i-1}) &= \mathrm{prob}[U_{A,i}^\dagger E_{A,i}(Z_{A,i} \otimes \mathbb{I}_{\mathcal{M}})E_{A,i}U_{A,i} \otimes \Pi^{[z_{B,i-1}]}, \psi_{i-1}], \end{aligned}$$

and from the dual SDP condition ② in Theorem 2, we have $Z_{A,i-1}\otimes\mathbb{I}_{\mathcal{M}}\otimes\Pi^{[z_{B,i-1}]} \succeq U_{A,i}^\dagger E_{A,i}(Z_{A,i}\otimes \mathbb{I}_{\mathcal{M}})E_{A,i}U_{A,i}\otimes\Pi^{[z_{B,i-1}]}$. From there, we conclude that $p_{n-i} \to p_{n-i+1}$ is a horizontal EBM transition. Similarly, for i even, the points move only vertically and the total weight on every vertical line remains unchanged. □

Quite surprisingly, the reverse implication is also true.

Theorem 3 (EBM to protocol) *Given an EBM point game with final point $[\beta, \alpha]$, there exists a WCF protocol and two dual feasible points proving that the optimal cheating probabilities are $P_A^* \leq \alpha$ and $P_B^* \leq \beta$.*

The proof of this fact is somewhat lengthy, though rather simple. In Lemma 10 we show that for every EBM line transition, there exist matrices X and Y and a vector $|\psi\rangle$ that certify that the transition is EBM and they have some extra nice properties. This is the non-constructive part of the proof, since we do not know how to find these matrices in an efficient way. Given these matrices and vectors it is not hard to construct the WCF protocol, namely define the honest states, the unitaries, and the projections. Alice and Bob will share a superposition of all points that appear in the EBM game and they will take turns changing the amplitudes according to the distributions over these points specified by the EBM transitions.

Proof. Consider an EBM point game with transitions $p_0 \to p_1 \to \cdots \to p_n = [\beta, \alpha]$ and let us define the sets of all possible first and second coordinates z_A and z_B of all the points that appear in the game:

$$\begin{aligned} S_A &= \{z_A \geq 0 \mid \exists i \in \{0, \ldots, n\},\ \exists z_B \geq 0,\ p_i(z_A, z_B) > 0\}, \\ S_B &= \{z_B \geq 0 \mid \exists i \in \{0, \ldots, n\},\ \exists z_A \geq 0,\ p_i(z_A, z_B) > 0\}. \end{aligned}$$

We wish to find a protocol (honest states, unitaries, projections) and dual feasible points that guarantee that in this protocol Alice's and Bob's cheating probabilities are upper-bounded by α

and β respectively. The idea is the following: every point $[z_A, z_B]$ of the game will be represented as an orthogonal state $|0, z_A\rangle|z_A, z_B\rangle|z_B, 0\rangle \in \mathcal{A} \otimes \mathcal{M} \otimes \mathcal{B}$, where

$$\begin{aligned}\mathcal{A} &= \text{span}\{|b, z_A\rangle,\ b \in \{0,1\},\ z_A \in S_A\},\\ \mathcal{M} &= \mathcal{A}' \otimes \mathcal{B}' = \text{span}\{|z_A, z_B\rangle,\ z_A \in S_A,\ z_B \in S_B\},\\ \mathcal{B} &= \text{span}\{|z_B, b\rangle,\ b \in \{0,1\},\ z_B \in S_B\}.\end{aligned}$$

The honest state $|\psi_i\rangle$ of the protocol at round i will be

$$|\psi_i\rangle = \sum_{z_A \in S_A, z_B \in S_B} \sqrt{p_{n-i}(z_A, z_B)}|0, z_A\rangle|z_A, z_B\rangle|z_B, 0\rangle.$$

The message space $\mathcal{M}$ contains the states that correspond to all the points of the game so that both players have alternate access to them and can manipulate their amplitudes by applying a unitary operation. The role of the unitary U_i is to transform the state $|\psi_{i-1}\rangle$ to the state $|\psi_i\rangle$, in other words $U_i|\psi_{i-1}\rangle = |\psi_i\rangle$. Moreover, we need to ensure that when Alice (resp. Bob) applies a unitary, then it corresponds to a horizontal (resp. vertical) line transition; in other words that the sum of the squares of the amplitudes of the states with a fixed second (resp. first) coordinate remains unchanged. The way to achieve this, is to force Alice to perform a unitary on the message space and her workspace which only uses the second coordinate of the points as a control (similarly we need to force Bob to perform a unitary which only uses the first coordinate of the points as a control). For this reason, Alice (resp. Bob) keeps a copy of the first (resp. second) coordinate of the points and each has a qubit that becomes 1 (via the unitary operation) when they catch the other player cheating, ie. not using the coordinate as control. We define the cheating detection projections $E_{A,i} = E_A = \sum_{z_A} |0, z_A, z_A\rangle\langle 0, z_A, z_A| \otimes \mathbb{I}_{\mathcal{B}'}$ and $E_{B,i} = E_B = \sum_{z_B} \mathbb{I}_{\mathcal{A}'} \otimes |z_B, z_B, 0\rangle\langle z_B, z_B, 0|$ that allow Alice and Bob to prematurely end the protocol and declare themselves winner. Note these projections leave the honest states invariant.

It remains to find the unitaries U_i and the matrices Z_i. Let us assume that i is odd (similarly for i even), hence the transition $p_{n-i} \to p_{n-i+1}$ is horizontal; that is Alice applies the unitary $U_i = U_{A,i} \otimes \mathbb{I}_{\mathcal{B}}$. Since we want this unitary to use the second coordinate only as control we have $U_{A,i} = \sum_{z_B} U_{A,i}^{(z_B)} \otimes |z_B\rangle\langle z_B|$. Define the (non-normalized) states $|\psi_{i-1}^{(z_B)}\rangle = \sum_{z_A \in S_A} \sqrt{p_{n-i+1}(z_A, z_B)}|0, z_A, z_A\rangle$. Then in order to have $U_i|\psi_{i-1}\rangle = |\psi_i\rangle$, we need that $U_{A,i}^{(z_B)}|\psi_{i-1}^{(z_B)}\rangle = |\psi_i^{(z_B)}\rangle$.

We will show, in fact, that the state $|\psi_{i-1}^{(z_B)}\rangle$ can be rewritten in a different basis, so that the amplitudes are now given by the function p_{n-i}. Then, the unitaries $U_{A,i}^{(z_B)}$ will just perform this basis change. More precisely, we find the unitaries $U_{A,i}^{(z_B)}$ for $i = 1, \ldots, n$ and a single matrix $Z_A (= Z_{A,0} = \cdots = Z_{A,n-1})$ by expressing each EBM line transition $p_{n-i}(\cdot, z_B) \to p_{n-i+1}(\cdot, z_B)$ as $\text{prob}[X, \psi] \to \text{prob}[Y, \psi]$, where the matrices X, Y and the state $|\psi\rangle$ satisfy the properties of the following lemma:

Lemma 10 *Let $l \to r$ be an EBM line transition and denote by* $\text{supp}(l)$ *and* $\text{supp}(r)$ *the supports of l and r respectively. Let S be a set such that* $\text{supp}(l) \cup \text{supp}(r) \subseteq S$ *and* $\Lambda > \max\{z : z \in S\}$. *Given a set of orthonormal vectors $\{|z\rangle, z \in S\}$, there exists a family of $|S|$ orthonormal vectors $\{|\varphi(z)\rangle,\ z \in S\}$ in the $2|S|^2$-dimensional space* $\text{span}\{|b, z, z'\rangle,\ b \in \{0,1\},\ z, z' \in S\}$ *such that*

- *the state $|\psi\rangle = \sum_z \sqrt{r(z)}|0, z, z\rangle$ can be expressed as $|\psi\rangle = \sum_z \sqrt{l(z)}|\varphi(z)\rangle$,*

- $l = \text{prob}[X, \psi]$ *and* $r = \text{prob}[Y, \psi]$, *with* $0 \preceq X \preceq Y$, *and*

$$Y = \sum_{z \in S} z|0,z,z\rangle\langle 0,z,z| + \Lambda \sum_{z \in S} |1,z,z\rangle\langle 1,z,z| \quad \textit{and} \quad X = \sum_{z \in S} z|\varphi(z)\rangle\langle\varphi(z)|.$$

We defer the proof of this lemma to the end of the section and continue with the proof of the theorem.

For each $z_B \in S_B$ and each EBM line transition $p_{n-i}(\cdot, z_B) \to p_{n-i+1}(\cdot, z_B)$, we apply Lemma 10 with $S = S_A$. This defines

$$\begin{aligned} X_i^{(z_B)} &= \sum_{z_A \in S_A} z_A |\varphi_i^{(z_B)}(z_A)\rangle\langle\varphi_i^{(z_B)}(z_A)|, \\ Y &= \sum_{z_A \in S_A} z_A |0,z_A,z_A\rangle\langle 0,z_A,z_A| + \Lambda \sum_{z_A \in S_A} |1,z_A,z_A\rangle\langle 1,z_A,z_A|, \\ |\psi_{i-1}^{(z_B)}\rangle &= \sum_{z_A \in S_A} \sqrt{p_{n-i+1}(z_A,z_B)}|0,z_A,z_A\rangle = \sum_{z_A} \sqrt{p_{n-i}(z_A,z_B)}|\varphi_i^{(z_B)}(z_A)\rangle. \end{aligned}$$

We can now define the unitary $U_{A,i}^{(z_B)}$ by its action on a subspace of $\mathcal{A} \otimes \mathcal{A}'$:

$$U_{A,i}^{(z_B)} : |\varphi_i^{(z_B)}(z_A)\rangle \mapsto |0,z_A,z_A\rangle.$$

We complete $U_{A,i}^{(z_B)}$ so that it is a unitary on $\mathcal{A} \otimes \mathcal{A}'$. Note that we have:

$$\begin{aligned} U_{A,i}^{(z_B)} \sum_{z_A} \sqrt{p_{n-i+1}(z_A,z_B)}|0,z_A,z_A\rangle &= U_{A,i}^{(z_B)} \sum_{z_A} \sqrt{p_{n-i}(z_A,z_B)}|\varphi_i^{(z_B)}(z_A)\rangle, \\ &= \sum_{z_A} \sqrt{p_{n-i}(z_A,z_B)}|0,z_A,z_A\rangle, \end{aligned}$$

and thus have $U_i|\psi_{i-1}\rangle = |\psi_i\rangle$. Moreover, by the definition of the unitary and the cheating detection projection, we can see that indeed Bob is forced to use the first coordinate only as control. Note that we also have $X_i^{(z_B)} = U_{A,i}^\dagger E_A Y E_A U_{A,i}$.

We now need to define Z_A acting only on the space $\mathcal{A}$. We take $Z_A = \sum_{z_A \in S_A} z_A|0,z_A\rangle\langle 0,z_A| + \Lambda \sum_{z_A \in S_A} |1,z_A\rangle\langle 1,z_A|$ and note that the support of $\text{prob}[Y, \psi_{i-1}^{(z_B)}]$ is equal to the support of $\text{prob}[Z_A \otimes \mathbb{I}_{\mathcal{A}'}, \psi_{i-1}^{(z_B)}]$.

In other words, by the definition of the honest states, the projections, the unitaries and the dual feasible point, we have shown that any EBM line transition can be expressed as

$$\begin{aligned} p_{n-i+1}(\cdot, z_B) &= \text{prob}[Y, \psi_{i-1}^{(z_B)}] = \text{prob}[Z_A \otimes \mathbb{I}_{\mathcal{A}'}, \psi_{i-1}^{(z_B)}] = \text{prob}[Z_A \otimes \mathbb{I}_{\mathcal{M}} \otimes \Pi^{[z_B]}, \psi_{i-1}], \\ p_{n-i}(\cdot, z_B) &= \text{prob}[X, \psi_{i-1}^{(z_B)}] = \text{prob}[U_{A,i}^{(z_B)\dagger} E_A (Z_A \otimes \mathbb{I}_{\mathcal{A}'}) E_A U_{A,i}^{z_B}, \psi_{i-1}^{(z_B)}] \\ &= \text{prob}[U_{A,i}^\dagger E_A (Z_A \otimes \mathbb{I}_{\mathcal{M}}) E_A U_{A,i} \otimes \Pi^{[z_B]}, \psi_{i-1}]. \end{aligned}$$

This is precisely the type of EBM line transitions that arose when we started from a protocol and a dual feasible point.

We need to verify that the Z_A's we defined are a dual feasible point. According to the constraints of the dual, we pick $Z_{A,n} = \Pi_A^{(1)} = |0,1\rangle\langle 0,1|$. Since the initial points of the point

game are $[0,1]$ and $[1,0]$, then 1 is an eigenvalue of Z_A, so we have $\Pi_A^{(1)} \preceq Z_A$, i.e. $Z_{A,n} \preceq Z_{A,n-1}$. For $i = \{0, \ldots, n-1\}$, we have

$$\begin{aligned}
U_{A,i}^\dagger E_A (Z_A \otimes \mathbb{I}_{\mathcal{M}}) E_A U_{A,i} &= U_{A,i}^\dagger \left(\sum_{z_A} z_A |0, z_A, z_A\rangle\langle 0, z_A, z_A| \otimes \sum_{z_B} |z_B\rangle\langle z_B| \right) U_{A,i}, \\
&= \sum_{z_B} \sum_{z_A} z_A U_{A,i}^{(z_B)\dagger} |0, z_A, z_A\rangle\langle 0, z_A, z_A| U_{A,i}^{(z_B)} \otimes |z_B\rangle\langle z_B|, \\
&= \sum_{z_B} X_i^{(z_B)} \otimes |z_B\rangle\langle z_B|, \\
&\preceq Y \otimes \mathbb{I}_{\mathcal{B}'}, \\
&= \left(\sum_{z_A \in S_A} z_A |0, z_A, z_A\rangle\langle 0, z_A, z_A| + \Lambda |1, z_A, z_A\rangle\langle 1, z_A, z_A| \right) \otimes \mathbb{I}_{\mathcal{B}'}, \\
&\preceq \left(\sum_{z_A, z'_A \in S_A} z_A |0, z_A, z'_A\rangle\langle 0, z_A, z'_A| + \Lambda |1, z_A, z'_A\rangle\langle 1, z_A, z'_A| \right) \otimes \mathbb{I}_{\mathcal{B}'}, \\
&= Z_A \otimes \mathbb{I}_{\mathcal{M}}.
\end{aligned}$$

To see that the first inequality is correct, consider a state $|\zeta\rangle$ in $\mathcal{A} \otimes \mathcal{M}$, $|\zeta\rangle = \sum_{z_B} |\zeta_{z_B}\rangle |z_B\rangle$. We get $\langle\zeta| \left(\sum_{z_B} X_i^{(z_B)} \otimes |z_B\rangle\langle z_B| \right) |\zeta\rangle = \sum_{z_B} \langle \zeta_{z_B} | X_i^{(z_B)} | \zeta_{z_B} \rangle \leq \sum_{z_B} \langle \zeta_{z_B} | Y | \zeta_{z_B} \rangle = \langle \zeta | Y \otimes \mathbb{I}_{\mathcal{B}'} | \zeta \rangle$ by Lemma 10, hence $\sum_{z_B} X_i^{(z_B)} \otimes |z_B\rangle\langle z_B| \preceq Y \otimes \mathbb{I}_{\mathcal{B}'}$. □

Proof of Lemma 10. Let $l \to r$ be an EBM line transition, so by definition there exist two positive semidefinite matrices $X_0 \preceq Y_0$ and a vector $|\psi_0\rangle$ such that $l = \text{prob}[X_0, \psi_0]$ and $r = \text{prob}[Y_0, \psi_0]$. We will now make a succession of transformations to X_0, Y_0, and $|\psi_0\rangle$ in order to show that they can satisfy the properties of the Lemma.

Notice that the size of the matrices X_0 and Y_0 is unknown. We first see that we can decrease their size to at most $|S|$. We start by diagonalizing X_0 and Y_0:

$$X_0 = \sum_x x \Pi_{X_0}^{[x]} \qquad \text{and} \qquad Y_0 = \sum_y y \Pi_{Y_0}^{[y]}.$$

To remove the multiplicities of the eigenvalues, we go into the Hilbert space $\mathcal{H}$, spanned by $\{\Pi_{X_0}^{[x]} |\psi_0\rangle, \Pi_{Y_0}^{[y]} |\psi_0\rangle\}$. This space has dimension at most $|\text{supp}(p) \cup \text{supp}(q)| \leq |S|$. We define the new $|\psi\rangle = \Pi_{\mathcal{H}} |\psi_0\rangle$ as the projection of $|\psi_0\rangle$ on $\mathcal{H}$ and the matrices X and Y by

$$X = \sum_x x \Pi_X^{[x]} \quad \text{and} \qquad Y = \sum_y y \Pi_Y^{[y]},$$

where $\Pi_X^{[x]}$ is the projector onto the one-dimensional space spanned by $\Pi_{X_0}^{[x]} |\psi_0\rangle$ and $\Pi_Y^{[y]}$ is the projector onto the one-dimensional space spanned by $\Pi_{Y_0}^{[y]} |\psi_0\rangle$. These matrices have size at most $|S|$. By construction, the matrices X, Y and the vector $|\psi\rangle$ satisfy the four properties

- $X \preceq Y$;
- $l = \text{prob}[X, \psi]$ and $r = \text{prob}[Y, \psi]$;
- The eigenvalues of X are in $\text{supp}(l)$ with multiplicity 1;

- The eigenvalues of Y are in $\mathrm{supp}(r)$ with multiplicity 1.

Then, we will append the values in S that are not yet into the spectra of X and Y. This is done by increasing the dimension of the matrices and the vector $|\psi\rangle$ by the following algorithm:
For each z in S do:

- if z is in the spectrum of X but not Y, $X \leftarrow X \oplus [0]$ and $Y \leftarrow Y \oplus [z]$;
- if z is in the spectrum of Y but not X, $X \leftarrow X \oplus [z]$ and $Y \leftarrow Y \oplus [\Lambda]$;
- if z is neither in the spectrum of X nor Y, $X \leftarrow X \oplus [z]$ and $Y \leftarrow Y \oplus [z]$.

The output of this algorithm are matrices of size less or equal to $2\,|S|$. We append extra 0 to X and extra Λ to Y until they have exactly size $2\,|S|$. We also increase the dimension of $|\psi\rangle$ by appending 0's.

We have constructed two matrices $0 \preceq X \preceq Y$ and a vector $|\psi\rangle$ of dimension $2\,|S|$ such that $l = \mathrm{prob}[X, \psi]$ and $r = \mathrm{prob}[Y, \psi]$. Moreover the spectrum of X is exactly $\{0\} \cup S$ and all non zero eigenvalues have multiplicity one; the spectrum of Y is exactly $S \cup \{\Lambda\}$ and all the eigenvalues in S have multiplicity one. Thus, they can be decomposed as:

$$X = \sum_{z \in S} z |u_z\rangle\langle u_z| \quad \text{and} \qquad Y = \sum_{z \in S} z |v_z\rangle\langle v_z| + \Lambda P,$$

where the $\{|u_z\rangle\}$ and $\{|v_z\rangle\}$ are orthonormal families of vectors and P is the projector onto the complement of $\mathrm{span}\{|v_z\rangle\}$.

We now increase the size of X, Y, and $|\psi\rangle$ by appending 0's to all of them until they reach size $2|S|^2$. In particular, we can write $X = \sum_{z \in S} z |u'_z\rangle\langle u'_z|$ and $Y = \sum_{z \in S} z |v'_z\rangle\langle v'_z| + \Lambda P'$ where $|u'_z\rangle = |u_z\rangle \otimes |0^S\rangle$, $|v'_z\rangle = |v_z\rangle \otimes |0^S\rangle$, and $P' = P \otimes |0^S\rangle\langle 0^S|$. As a consequence, P' is a projector on a $|S|$-dimensional subspace of the $2|S|^2$-dimensional space. Then, let U be a unitary that maps $|v'_z\rangle$ to $|0, z, z\rangle$ and sends P' to $\sum_z |1, z, z\rangle\langle 1, z, z|$ (Such unitary exists since P' is a projector onto a space of size $|S|$ orthogonal to the space spanned by the vectors $\{|u'_z\rangle,\ z \in S\}$). We define $|\varphi(z)\rangle = U e^{i\theta_z} |u'_z\rangle$ so that applying U to X, Y, and $|\psi\rangle$ leads to:

$$X = \sum_{z \in S} z |\varphi(z)\rangle\langle\varphi(z)| \ ; \ Y = \sum_{z \in S} z |0, z, z\rangle\langle 0, z, z| + \Lambda |1, z, z\rangle\langle 1, z, z| \text{ and } |\psi\rangle = \sum_z \sqrt{l(z)} |\varphi(z)\rangle.$$

□

3 Point games with valid transitions

Here is where we stand now: we have defined points games with EBM transitions, starting at points $1/2[0, 1] + 1/2[1, 0]$ and ending at some point $[\beta, \alpha]$. We have also shown that for each point game with final point $[\beta, \alpha]$, we can construct a weak coin flipping protocol and dual feasible points proving that the cheating probabilities are $P^*_A \leq \alpha$ and $P^*_B \leq \beta$. The final goal will thus be to find an EBM point game with final point $[1/2 + \varepsilon, 1/2 + \varepsilon]$ for any $\varepsilon > 0$.

This task is quite challenging. We do not currently know of a direct way to handle EBM transitions (prob functions, matrices, vectors). The aim of this Section is to find an alternative characterization of EBM transitions that is easier to manipulate; those would be called valid transitions. For that matter, we turn to the help of convex geometry. If the space which we are considering were finite dimensional, a rather simple argument would suffice; we explain it below, but unfortunately we do not know how to make this simple argument work in the infinite dimensional case and hence more elaborate work is needed.

3.1 Moving between transitions and functions

The first idea is to shift our view from transitions to functions, instead of considering transitions $p \to q$, we will look at functions $(q - p)$. The reasons behind this change are the following: it is easier to have one function $(q - p)$ than a pair (p, q); the set of functions arising from EBM transitions has "good" geometry; and for all intents and purposes functions and transitions behave the same.

We start by defining the set K of EBM functions and explain how point games with functions are equivalent to point games with transitions. This will allow us in the following subsections to look at the geometric properties of K. We remark that in anticipation of the difficulties arising in infinite dimensions, we will also provide these definitions with a parameter Λ. For $\Lambda = \infty$ we have precisely the set of EBM functions, however later on we will need to consider sets with a finite $\Lambda > 0$. For now, it might be instructive to just think of Λ as ∞ and consider only the first items of the following definitions and lemmata.

Definition 11 (K, EBM functions) *A function $h : [0, \infty) \to \mathbb{R}$ with finite support is an* EBM function *if the line transition $h^- \to h^+$ is EBM, where $h^+ : [0, \infty) \to [0, \infty)$ and $h^- : [0, \infty) \to [0, \infty)$ denote respectively the positive and the negative part of h ($h = h^+ - h^-$). We denote by K the set of EBM functions.*

For any finite $\Lambda \in (0, \infty)$, a function $h : [0, \Lambda) \to \mathbb{R}$ with finite support is an EBM function with support on $[0, \Lambda]$ *if the line transition $h^- \to h^+$ is expressible by matrices with spectrum in $[0, \Lambda]$, where h^+ and h^- denote respectively the positive and the negative part of h. We denote by K_Λ the set of EBM functions with support on $[0, \Lambda]$.*

As with transitions, we can also extend the notions of horizontal and vertical transitions to functions.

Definition 12 *A $\mathcal{P}$-function $h : [0, \infty) \to \mathbb{R}$ is a function with finite support that has the property $\mathcal{P}$. A function $t : [0, \infty) \times [0, \infty) \to \mathbb{R}$ is a*

- horizontal $\mathcal{P}$-function *if for all $y \geq 0$, $t(\cdot, y)$ is a $\mathcal{P}$-function;*
- vertical $\mathcal{P}$-function *if for all $x \geq 0$, $t(x, \cdot)$ is a $\mathcal{P}$-function.*

For now, we have only have seen $\mathcal{P}$ being EBM, but we later see other properties, namely, valid and strictly valid. These definitions are useful for defining point games with $\mathcal{P}$-functions. To see how, consider a point game $1/2[0, 1] + 1/2[1, 0] \to p_1 \to p_2 \to \cdots \to p_n$ and define the functions $t_0 = 1/2[0, 1] + 1/2[1, 0]$ and $t_i = p_i - p_{i-1}$. It is easy to see that we have $p_i = \sum_{j=0}^{i} t_i$. Hence:

Definition 13 (Point game with $\mathcal{P}$- functions) *A point game with $\mathcal{P}$-functions is a set $\{t_1, \ldots, t_n\}$ of n $\mathcal{P}$-functions alternatively horizontal and vertical such that:*

- $1/2[0, 1] + 1/2[1, 0] + \sum_{i=1}^{n} t_i = [\beta, \alpha]$;
- $\forall j \in \{1, n\}, 1/2[0, 1] + 1/2[1, 0] + \sum_{i=1}^{j} t_i \geq 0$.

We call $[\beta, \alpha]$ the final point of the game.

The first condition simply rewrites the initial and final points; the second one expresses the fact that the p_i's are non-negative.

We have seen how a point game with EBM transitions can be translated into a point game with EBM functions. The reverse also holds:

Lemma 14 *Given a point game with n EBM functions and final point $[\beta, \alpha]$, we can construct a point game with n EBM transitions and final point $[\beta, \alpha]$.*

Proof. Let us define $p_i = \sum_{j=1}^{i} f_j + 1/2[0,1] + 1/2[0,1]$. As a consequence, we have $p_0 = 1/2[0,1] + 1/2[0,1]$, $p_n = [\beta, \alpha]$, and for all $i \in \{0, n\}, p_i \geq 0$. Moreover, we have $p_{i+1} = p_i + f_{i+1}^+ - f_{i+1}^- \geq 0$. Since f_{i+1}^+ and f_{i+1}^- have disjoint support, $\zeta = p_i - f_{i+1}^- \geq 0$. We can rewrite the transition $p_i \to p_{i+1}$ by $\zeta + f_{i+1}^- \to \zeta + f_{i+1}^+$. This is an EBM transition since f_{i+1} is an EBM function. □

As a consequence, from now on we can equivalently use functions or transitions, depending on what is most handy.

3.2 Operator monotone functions and valid functions

We have defined the set K of EBM functions. First, we show that the set K is a convex cone.

Definition 15 (Convex cone) *A set C in a vector space V is a cone if for all $x \in C$ and all $\lambda > 0$, $\lambda x \in C$. It is convex if for all $x, y \in C$, $x + y \in C$.*

Let us first describe the normed vector space we will be working in. This is the set V of functions from $[0, \infty)$ to $\mathbb{R}$ with finite support. V is an infinite dimensional vector space spanned by the canonical basis $\{[x]\}_{x \in [0,\infty)}$ where $[x](y) = \delta_{x,y}$ is the Kronecker delta function. Each element v of V can be written as $v = \sum_x v(x)[x]$. The usual norm on this space is the 1-norm, which is defined for any $v = \sum_x v(x)[x]$ as $\|v\|_1 = \sum_x |v(x)|$.

Lemma 16 *K is a convex cone. Also, for any $\Lambda \in (0, \infty)$, K_Λ is a convex cone.*

Proof. Fix $\Lambda > 0$. Let $g, h \in K_\Lambda$, so $g^- \to g^+$ and $h^- \to h^+$ are two EBM line transitions, i.e. we can write them as: $g^- = \text{prob}[X_g, \psi_g]$, $g^+ = \text{prob}[Y_g, \psi_g]$, $h^- = \text{prob}[X_h, \psi_h]$ and $h^+ = \text{prob}[Y_h, \psi_h]$. (note that the dimensions of X_g and Y_g are not necessarily the same as the ones of X_h and Y_h)

K_Λ is a cone since for all $\lambda \geq 0$, $\lambda g = \lambda g^+ - \lambda g^- = \text{prob}[Y_g, \sqrt{\lambda}|\psi_g\rangle] - \text{prob}[X_g, \sqrt{\lambda}|\psi_g\rangle]$ and hence $\lambda g^- \to \lambda g^+$ is expressible by matrices with spectra in in $[0, \Lambda]$.

Let us finally show K_Λ is convex. It is enough to prove that $g + h \in K_\Lambda$. Construct $X = X_g \oplus X_h = \begin{bmatrix} X_g & 0 \\ 0 & X_h \end{bmatrix}$, $Y = Y_g \oplus Y_h = \begin{bmatrix} Y_g & 0 \\ 0 & Y_h \end{bmatrix}$ and $|\psi\rangle = |\psi_g\rangle \oplus |\psi_h\rangle = \begin{bmatrix} \psi_g \\ \psi_h \end{bmatrix}$. We now have

$$g^- + h^- = \text{prob}[X, \psi] \quad \text{and} \quad g^+ + h^+ = \text{prob}[Y, \psi].$$

Since we also have that $\text{sp}(X), \text{sp}(Y) \subset [0, \Lambda]$, we can conclude that K_Λ is convex. Notice that this proof holds for $\Lambda = \infty$, hence K is also convex. □

Let us now consider the dual cone of the set of EBM functions, denoted by K^*.

Definition 17 (Dual cone) *Let C be a cone in a normed vector space V. We denote by V' the space of continuous linear functionals from V to $\mathbb{R}$. The dual cone of a set $C \subseteq V$ is*

$$C^* = \{\Phi \in V' \mid \forall h \in C,\ \Phi(h) \geq 0\}.$$

It turns out that the dual cone of the set K of EBM functions is exactly the set of operator monotone functions and a similar characterization holds for any K_Λ.

Definition 18 (Operator monotone functions) *A function $f : [0, \infty) \to \mathbb{R}$ is* operator monotone *if for all positive semidefinite matrices $X \preceq Y$, we have $f(X) \preceq f(Y)$.*

A function $f : [0, \Lambda] \to \mathbb{R}$ is operator monotone on $[0, \Lambda]$ *if for all positive semidefinite matrices $X \preceq Y$ with spectrum in $[0, \Lambda]$, we have $f(X) \preceq f(Y)$.*

We now show that the set K^* is indeed equal to the set of operator monotone functions, up to an isomorphism. Indeed, note that there is a bijective mapping between $\Phi \in V'$ and f_Φ where f_Φ is a function on reals defined by $f_\Phi(x) = \Phi([x])$. This gives us by linearity of Φ that for a function $h = \sum_x h(x)[x]$ we have $\Phi(\sum_x h(x)[x]) = \sum_x h(x) f_\Phi(x)$. With this mapping, we can see elements of K^*_Λ as functions on reals. Up to this mapping, the set K^*_Λ is the set of operator monotone functions on $[0, \Lambda]$.

Lemma 19 *$\Phi \in K^*$ if and only if f_Φ is operator monotone on $[0, \infty]$. Also, for any $\Lambda \in (0, \infty)$, $\Phi \in K^*_\Lambda$ if and only if f_Φ is operator monotone on $[0, \Lambda]$.*

Proof. Fix $\Lambda > 0$. Forward implication. We first notice that $\Phi \in K^*_\Lambda$ implies

$$\forall h \in K_\Lambda, \ \sum_x f_\Phi(x) h(x) \geq 0. \tag{3}$$

This is immediate from the definition of f_Φ. We now prove that a function f with finite support on $[0, \Lambda]$ satisfies Equation (3) if and only if f is operator monotone on $[0, \Lambda]$. The proof of this equivalence is based on the following observation:

$$\sum_{x \in \mathrm{sp}(X)} f(x) \operatorname{prob}[X, \psi](x) = \sum_{x \in \mathrm{sp}(X)} f(x) \langle \psi | \Pi^{[x]} | \psi \rangle = \langle \psi | \sum_{x \in \mathrm{sp}(X)} f(x) \Pi^{[x]} | \psi \rangle = \langle \psi | f(X) | \psi \rangle.$$

Then,

$$\begin{aligned}
&\forall h \in K_\Lambda, \ \sum_x f(x) h(x) \geq 0 \\
&\qquad \Leftrightarrow \forall |\psi\rangle, \ \forall\, 0 \preceq X \preceq Y \text{ with } \mathrm{sp}(X), \mathrm{sp}(Y) \subset [0, \Lambda], \\
&\qquad\qquad \sum_x f(x) \left(\operatorname{prob}[Y, \psi](x) - \operatorname{prob}[X, \psi](x) \right) \geq 0 \\
&\qquad \Leftrightarrow \forall |\psi\rangle, \ \forall\, 0 \preceq X \preceq Y \text{ with } \mathrm{sp}(X), \mathrm{sp}(Y) \subset [0, \Lambda], \ \langle \psi | f(X) | \psi \rangle \leq \langle \psi | f(Y) | \psi \rangle \\
&\qquad \Leftrightarrow \forall\, 0 \preceq X \preceq Y \text{ with } \mathrm{sp}(X), \mathrm{sp}(Y) \subset [0, \Lambda], \ f(X) \preceq f(Y) \\
&\qquad \Leftrightarrow f \text{ is operator monotone on } [0, \Lambda].
\end{aligned}$$

For the reverse implication, consider a pair (f_Φ, Φ) where f_Φ is a function with finite support on $[0, \Lambda]$ and Φ is its associated function in V'. Hence by the previous series of equivalence, we have $\forall h \in K_\Lambda, \ \Phi(h) \geq 0$. In order to prove that $\Phi \in K^*_\Lambda$ we need to show that Φ is continuous. Since f_Φ is operator monotone on $[0, \Lambda]$, f_Φ is increasing and $\forall x \in [0, \Lambda], \ f_\Phi(x) \in [f_\Phi(0), f_\Phi(\Lambda)]$, which means that $\|f_\Phi\|_\infty < +\infty$. Thus, for any $h = \sum_x h(x)[x]$, we have $\Phi_f(h) = \sum_x h(x) f_\Phi(x) \leq \|h\|_1 \|f_\Phi\|_\infty$, and hence Φ is continuous.

Note that the proof holds for K^*, the set of operator monotone functions, up to the same mapping. □

Operator monotone functions are very well studied objects. In particular, we have the following analytic characterization:

Lemma 20 ([Bha97]) *Any operator monotone function $f : [0, \infty) \to \mathbb{R}$ can be written as*

$$f(t) = c_0 + c_1 t + \int_0^{+\infty} \frac{\lambda t}{\lambda + t} \mathrm{d}w(\lambda),$$

for a measure w satisfying $\int_0^{+\infty} \frac{\lambda}{1+\lambda} \mathrm{d}w(\lambda) < +\infty$.
Any operator monotone function $f : [0, \Lambda] \to \mathbb{R}$ can be written as

$$f(t) = c_0 + c_1 t + \int \frac{\lambda t}{\lambda + t} \mathrm{d}w(\lambda),$$

with the integral ranging over $\lambda \in (-\infty, -\Lambda) \cup (0, +\infty)$.

This characterization is what makes the usage of duality in our context helpful. In particular, we can now consider the dual of the set of operator monotone functions, K^*. This dual is denoted K^{**}, and is called the set of *valid functions*.

Definition 21 (Valid function) *A function $h : [0, \infty) \to \mathbb{R}$ with finite support is* valid *if for every operator monotone function $f : [0, \infty) \to \mathbb{R}$, we have $\sum_{x \in \mathrm{supp}(h)} f(x)h(x) \geq 0$.*

The above is just restating the definition of the dual, but we provide it here for easier readability. Valid functions are strongly related to EBM functions since the bidual of a convex cone is the closure of the original cone:

Lemma 22 ([BV04]) *Let $C \subseteq V$ be a convex cone, then $C^{**} = \mathrm{cl}(C)$.*

Unfortunately K is not closed, so the valid functions are a superset of the EBM functions. In the next subsection, we see how we could circumvent this problem easily if we were in finite dimensions.

3.3 The remaining of an "easy" argument

Our goal remains to find an easy characterization of the set of EBM functions. So far, we have defined the set of EBM functions K, looked at its dual K^*, which is the set of operator monotone functions, and at the dual of the set of operator monotone functions, K^{**}, which we called the set of valid functions. However K^{**} is larger than K, but intuitively not much larger since it is the closure of K, and K and K^{**} have the same interior since K is convex:

Fact 23 *Let C be a convex set, then $\mathrm{int}(C) = \mathrm{int}(\mathrm{cl}(C))$.*

Moreover, in finite dimensions, the interior of a dual cone can be expressed directly as a function of the primal cone:

Lemma 24 ([BV04]) *Let C be a cone in finite dimensional vector space V, then $\mathrm{int}(C^*) = \{\Phi \in V' \,|\, \forall h \in C - \{0\},\ \Phi(h) > 0\}$.*

This motivates the following definition.

Definition 25 (Strictly valid function) *A function $h : [0, \infty) \to \mathbb{R}$ with finite support is* strictly valid *if for every non-constant operator monotone function $f : [0, \infty) \to \mathbb{R}$, we have $\sum_{x \in \mathrm{supp}(h)} f(x)h(x) > 0$.*

At this point, if we were in finite dimensions, we could directly conclude that strictly valid functions are also EBM functions. However, we are in infinite dimensions and this line of reasoning fails. The main difficulty lies in the fact that, as most cones in infinite dimensions, K and K^{**} have empty interiors whereas the set of strictly valid functions is not empty, and thus

the set of strictly valid functions is not the interior of the set of valid functions. Nonetheless strictly valid functions play a similar role as we will prove the same statement, that strictly valid functions are EBM functions, but with a more cumbersome proof.

3.4 Strictly valid functions are EBM functions

Here is the main idea: We will look not at the set of EBM functions but at closed subsets of this set, that we have defined as K_Λ, for finite $\Lambda > 0$. Since these sets are closed, we can exactly characterize them by their bidual. In other words, $K_\Lambda^{**} = K_\Lambda$. Now, if we look again at a strictly valid function, we can prove that it is in K_Λ for some Λ and hence in K. Hence, the set of strictly valid functions, which has a simple characterization as the strict dual of operator monotone functions, is a subset of EBM functions.

The core of the argument is that for any finite $\Lambda > 0$, K_Λ is closed. Note that K, however, is not closed.

Definition 26 (Closed set) *A set C in a topological space V is closed if for any sequence $\{t_i\}_i$ of points in C that converges to a point t, we have $t \in C$.*

Lemma 27 *For any finite $\Lambda > 0$, K_Λ is closed.*

Proof. Fix a finite $\Lambda > 0$. Let $\{t_i\}_{i\in\mathbb{N}}$ be a converging sequence of functions in K_Λ, and denote the limit of this sequence $t = \lim_{i\to\infty} t_i$. The rest of the proof is devoted to show that $t \in K_\Lambda$. Denote $t = \sum_x t(x)[x]$ and S the support of t, that is the set $S = \{x : t(x) \neq 0\}$. Note that t is an element of V so t has finite support. Since the t_i are EBM, we write $t_i = \mathrm{prob}[Y_i, \psi_i] - \mathrm{prob}[X_i, \psi_i]$, with $0 \preceq X_i \preceq Y_i$. Each of the X_i's and Y_i's can be diagonalized:

$$X_i = \sum_{x^{(i)}} x^{(i)} \Pi^{[x^{(i)}]} \quad \text{and} \quad Y_i = \sum_{y^{(i)}} y^{(i)} \Pi^{[y^{(i)}]},$$

where $\Pi^{[x^{(i)}]}$ is the projector onto the eigenspace of X_i with eigenvalue $x^{(i)}$. Since there will be no confusion, we drop the exponent (i) from now on. Let us define the matrices:

$$A_i = \sum_{x\in S} x\Pi^{[x]} + \sum_{x\notin S} 0 \cdot \Pi^{[x]} \quad \text{and} \quad B_i = \sum_{y\in S} y\Pi^{[y]} + \sum_{y\notin S} \Lambda \cdot \Pi^{[y]}.$$

First note that we immediately have $0 \preceq A_i \preceq X_i \preceq Y_i \preceq B_i$ so we can define an EBM function $t'_i = \mathrm{prob}[B_i, \psi_i] - \mathrm{prob}[A_i, \psi_i]$. The dimension of the matrices A_i are not necessarily identical, but this is not a problem. As done in the proof of Lemma 10 ("getting rid of the multiplicities" and "appending the missing eigenvalues"), we construct the positive semidefinite matrices A'_i, B'_i of size $s = 2\,|S|$ and the vectors $|\psi'_i\rangle$ also of dimension s such that $t'_i = \mathrm{prob}[B'_i, \psi'_i] - \mathrm{prob}[A'_i, \psi'_i]$. Notice also that the spectra of the A'_i and the B'_i are in the interval $[0, \Lambda]$.

We show that $\lim_{i\to\infty} t'_i = t$. We write each t_i as $t_i = u_i + v_i$, where $u_i = \sum_{x\in S} t_i(x)[x]$ and $v_i = \sum_{x\notin S} t_i(x)[x]$. Let $\varepsilon_i = \sum_{x\notin S} t_i(x)$. Since $\lim_{i\to\infty} t_i = t$, we have $\lim_{i\to\infty} \varepsilon_i = 0$. Our construction of t'_i implies that $t'_i = u_i + \varepsilon_i^+[\Lambda] - \varepsilon_i^-[0]$ with $\varepsilon_i^+ + \varepsilon_i^- = \varepsilon_i$. This means in particular that $\|t'_i - t_i\|_1 \leq \varepsilon_i$. Since $\lim_{i\to\infty} \varepsilon_i = 0$ and $\lim_{i\to\infty} t_i = t$, we conclude that $\lim_{i\to\infty} t'_i = t$.

We will now show that the limit of the sequence $\{t'_i\}_{i\in\mathbb{N}}$ is an element $t' \in K_\Lambda$ which will conclude the proof. We consider the sequence of triplets $\{(A'_i, B'_i, |\psi'_i\rangle)\}_{i\in\mathbb{N}}$. Let X_Λ^s the set of positive semidefinite matrices with spectrum in $[0, \Lambda]$ and Y^s the set of quantum states of dimension s. An element of the sequence is an element of $X_\Lambda^s \times X_\Lambda^s \times Y^s$. Since X_Λ^s and Y^s are two compact sets, $X_\Lambda^s \times X_\Lambda^s \times Y^s$ is also a compact set. This means that our sequence of triplets has an accumulation point $(A', B', |\psi'\rangle)$ even if this sequence does not necessarily converge.

Let us now define $t' = \text{prob}[B', \psi'] - \text{prob}[A', \psi']$. Since $0 \preceq A' \preceq B'$, we have $t' \in K_\Lambda$. We can also see that t' is an accumulation point of the sequence $\{t'_i\}_i$. Since the sequence of t'_i's converges to t, we conclude that $t = t'$ and $t \in K_\Lambda$. □

Since K_Λ is a closed convex cone, it is characterized by its dual cone.

Corollary 28 *For any finite $\Lambda > 0$, $K_\Lambda = \{h \in V \mid \forall \Phi \in K_\Lambda^*,\ \Phi(h) \geq 0\}$.*

Using the characterization of operator monotone functions on $[0, \Lambda]$ given by Lemma 20, we can restate Corollary 28 and characterize EBM functions on $[0, \Lambda]$ by three necessary and sufficient properties:

Corollary 29 *A function $h : [0, \Lambda] \to \mathbb{R}$ with finite support on $[0, \Lambda]$ is EBM on $[0, \Lambda]$ if and only if $\sum_x h(x) = 0$, $\sum_x xh(x) \geq 0$, and $\forall \lambda \in (-\infty, -\Lambda] \cup (0, \infty)$, $\sum_x \frac{\lambda x}{\lambda + x} h(x) \geq 0$.*

Our goal is to show that every strictly valid function is an EBM function. For this, we first find a characterization of strictly valid functions that looks similar to conditions Corollary 29.

Lemma 30 *Let $h : [0, \infty) \to \mathbb{R}$ be a function with finite support such that $\sum_x h(x) = 0$. The function h is a strictly valid function if and only if for all $\lambda > 0$, $\sum_x \frac{-h(x)}{\lambda + x} > 0$, and is valid if and only if this inequality is large.*

Proof. An immediate consequence of Lemma 20 and the definition of strictly valid functions is that h is a strictly valid function if and only if

❶ $\sum_x h(x) = 0$;

❷ for all $\lambda > 0$, $\sum_x \frac{\lambda x}{\lambda + x} h(x) > 0$;

❸ $\sum_x x \cdot h(x) > 0$.

Condition ❸ is implied by condition ❷ in the limit $\lambda \to \infty$. Moreover, for all $\lambda > 0$ we have:

$$\sum_x \frac{\lambda x}{\lambda + x} h(x) > 0 \Leftrightarrow \sum_x \left(1 + \frac{-\lambda}{\lambda + x}\right) h(x) \geq 0 \Leftrightarrow \sum_x \frac{-1}{\lambda + x} h(x) > 0.$$

The last equivalence is shown by using property ❶.

The proof can be easily extended to handle the case of valid functions. □

We are now ready to show the main statement of this subsection:

Lemma 31 *Any strictly valid function is an EBM function.*

Proof. Fix h, a strictly valid function. We prove that there exists a $\Lambda > 0$ such that h is EBM on $[0, \Lambda]$ and hence is EBM. The proof easily extends to horizontal and vertical functions.

The conditions of Lemma 30 are very close to the conditions in Corollary 29. We just need to show that there exists a $\Lambda > 0$ such that

$$\forall \lambda < -\Lambda, \quad \sum_x \frac{\lambda x}{\lambda + x} h(x) \geq 0.$$

We have $\lim_{\lambda \to -\infty} \sum_x \frac{\lambda x}{\lambda + x} h(x) = \sum_x x\ h(x) > 0$. Consider the quantity $\sum_x \frac{\lambda x}{\lambda + x} h(x)$ as a function of λ. It is continuous in λ, so there exists a $\Lambda > 0$ such that

$$\forall \lambda < -\Lambda, \quad \sum_x \frac{\lambda x}{\lambda + x} h(x) \geq 0.$$

□

3.5 From valid functions to EBM functions

We have seen so far that a point game with strictly valid functions implies a point game with EBM functions. In this section we extend this result to valid functions, since, in the end, it will be easier to find a point game with valid transitions than with strictly valid ones. Note that for all $\Lambda > 0$, $K_\Lambda \subset K \subset K^{**}$, hence every EBM function is a valid function and thus a point game with EBM functions is also a point game with valid functions. More importantly, we prove that the converse is also "approximately" true:

Theorem 4 (Valid to EBM) *Given a point game with $2m$ valid functions and final point $[\beta, \alpha]$ and any $\varepsilon > 0$, we can construct a point game with $2m$ EBM functions and final point $[\beta + \varepsilon, \alpha + \varepsilon]$.*

The rest of this subsection is devoted to proving this theorem.

To prove Theorem 4, we, first, use Lemma 31 that shows that a point game with strictly valid functions is a point game with EBM functions. Second, we show how to transform a point game with valid functions and final point $[\beta, \alpha]$ into a point game with strictly valid functions, hence EBM functions, and final point $[\beta + \varepsilon, \alpha + \varepsilon]$ for any $\varepsilon > 0$.

Lemma 32 *Fix $\varepsilon > 0$. Given a point game with $2m$ valid functions and final point $[\beta, \alpha]$, we can construct a point game with $2m$ strictly valid functions and final point $[\beta + \varepsilon, \alpha + \varepsilon]$.*

Proof. Consider a game with valid functions $\{t_1, \cdots, t_{2m}\}$. We will construct a new game with strictly valid functions $\{t'_1, \cdots, t'_{2m}\}$. The idea to ensure strict validity, is to shift each point by an extra ε/m to the right for horizontal functions and to shift them up by ε/m for vertical functions. After $2m$ funtions (m horizontal and m vertical), the final point will then be $[\beta + \varepsilon, \alpha + \varepsilon]$ as desired.

For all $i \in \{1, 2m\}$ and $\forall (x, y) \in [0, \infty)$, we define the shifted functions as:

$$t'_i(x,y) = t_i^+(x - i\varepsilon/m, y - (i-1)\varepsilon/m) - t_i^-(x - (i-1)\varepsilon/m, y - (i-1)\varepsilon/m) \quad \text{if } i \text{ is odd,}$$
$$t'_i(x,y) = t_i^+(x - (i-1)\varepsilon/m, y - i\varepsilon/m) - t_i^-(x - (i-1)\varepsilon/m, y - (i-1)\varepsilon/m) \quad \text{if } i \text{ is even.}$$

Fix i even. We prove that the function t'_i is a strictly valid horizontal function. Note first that $\sum_x t'_i(x,y) = \sum_x t_i(x,y) = 0$. Then, for all $y \in [0, \infty)$ and for all non-constant operator monotones functions we have:

$$\begin{aligned}
\sum_{x \in \text{supp}(t_i'^+)} t_i'^+(x,y) f(x) &= \sum_{x \in \text{supp}(t'_i)} t_i^+(x - i\varepsilon/m, y - (i-1)\varepsilon/m) f(x) \\
&= \sum_{x \in \text{supp}(t_i^+)} t_i^+(x, y - (i-1)\varepsilon/m) f(x + i\varepsilon/m) \\
&\geq \sum_{x \in \text{supp}(t_i^-)} t_i^-(x, y - (i-i)\varepsilon/m) f(x + i\varepsilon/m) \\
&= \sum_{x \in \text{supp}(t_i^-)} t_i'^-(x + (i-1)\varepsilon/m, y) f(x + i\varepsilon/m) \\
&= \sum_{x \in \text{supp}(t_i'^-)} t_i'^-(x,y) f(x + \varepsilon/m), \\
&> \sum_{x \in \text{supp}(t_i'^-)} t_i'^-(x,y) f(x).
\end{aligned}$$

The first inequality follows from the validity of t_i and by noticing that if $f(x)$ is an operator monotone function in x then $f(x + (i+1)\varepsilon/m)$ is also an operator monotone function in x. The second strict inequality follows from the fact that every no constant operator monotone function is strictly increasing. A similar proof holds for vertical functions. □

3.6 Examples of valid line transitions

As we said earlier, we can go back-and-forth between functions and transitions. Functions are more suited for proving equivalences between different types of point games, transitions are more suited for describing the point games and mapping them back to protocols.

For the sake of completeness, we define now valid and strictly valid transitions and provide some examples of valid or strictly valid transitions.

Definition 33 *Let $l, r : [0,\infty) \to [0,\infty)$ be two functions with finite support. The transition $l \to r$ is valid (resp. strictly valid) if the function $r - l$ is valid (resp. strictly valid).*

Let us now have a quick look at three transitions. Despite their simple expressions, these transitions play an important role in creating point games with arbitrarily small bias, and we will use them in the next two sections. Moreover, by using only these three transitions, Mochon gives a family of point games converging to final point $[2/3, 2/3]$ [Moc07], i.e. a protocol with bias arbitrarily close to $1/6$.

Point raise $w[x] \to w[x']$ with $x' \geq x$.
It is easy to see that for every operator monotone function f, $wf(x) \leq wf(x')$ if and only if $x' \geq x$. By taking $f(x) = x$, we see that the condition is necessary. It is also sufficient since every operator monotone function is increasing.

Point merge $w_1[x_1] + w_2[x_2] \to (w_1 + w_2)[x_3]$ with $x_3 \geq \frac{w_1 x_1 + w_2 x_2}{w_1 + w_2}$.
Again, for every operator monotone function f, $w_1 f(x_1) + w_2 f(x_2) \leq (w_1 + w_2) f(x_3)$ if and only if $x_3 \geq \frac{w_1 x_1 + w_2 x_2}{w_1 + w_2}$. By taking $f(x) = x$, the above condition is necessary. This condition is also sufficient because operator monotone functions are concave.

Point split $w[x] \to w_1[x_1] + w_2[x_2]$ with $w = w_1 + w_2$ and $\frac{w}{x} \geq \frac{w_1}{x_1} + \frac{w_2}{x_2}$.
For every operator monotone function f, $wf(x) \leq w_1 f(x_1) + w_2 f(x_2)$ if and only if $\frac{w}{x} \geq \frac{w_1}{x_1} + \frac{w_2}{x_2}$. By considering the function $f(x) = -\frac{1}{\lambda + x}$ and the case where $\lambda \to 0$, we have $-\frac{w}{x} \leq -\frac{w_1}{x_1} - \frac{w_2}{x_2}$ which shows that the above condition is necessary. We now show that the above condition is also sufficient. Assume that $\frac{w}{x} \geq \frac{w_1}{x_1} + \frac{w_2}{x_2}$. We want to verify that $wf(x) \leq w_1 f(x_1) + w_2 f(x_2)$ for $f(x) = -\frac{1}{\lambda + x}$. Let $q = \frac{1}{x}, q'_i = \frac{1}{x_i}$. Let a function $g(t) = -\frac{t}{1 + \lambda t}$. We have $-\frac{1}{\lambda + x} = g(q)$ and $-\frac{1}{\lambda + x_i} = g(q_i)$. This gives us

$$wf(x) = g(q) \leq g\left(\frac{w_1 q_1 + w_2 q_2}{w_1 + w_2}\right) \leq w_1 g(q_1) + w_2 g(q_2) = w_1 f(x_1) + w_2 f(x_2).$$

The first inequality holds because g is decreasing and the second inequality holds because g is convex. The special case of $f(x) = x$ follows by considering the limit $\lambda \to \infty$ when considering function $f(x) = \frac{\lambda x}{\lambda + x} = \lambda\left(1 + \lambda \cdot \frac{-1}{\lambda + x}\right)$.

A last property that will be useful later on is that no valid point game puts any weight on the point $[0, 0]$.

Lemma 34 *A point game with valid transitions has no transition involving the point* $[0,0]$.

Proof. It is sufficient to prove that there is no valid line transition $l \to w[0] + (1-w)r$ where l and r are positive functions with finite support and $l(0) = r(0) = 0$. By contradiction, assume there exists such transition. In that case the second condition of Lemma 30 implies that for all $\lambda > 0$, we have $(1-w)\sum_x \frac{-\lambda}{\lambda+x} r(x) - w \geq \sum_x \frac{-\lambda}{\lambda+x} l(x)$. The contradiction is obtained by taking the limit $\lambda \to 0$. □

4 Time independent point games

In the previous section, we showed that if there exists a point game with valid transitions and final point $[\beta, \alpha]$, then for any $\varepsilon > 0$, there exists a weak coin flipping protocol with $P_A^* \leq \alpha + \varepsilon$ and $P_B^* \leq \beta + \varepsilon$. Moreover, given a line transition, it is easy to verify whether it is valid or not. Nevertheless, it is still not straightforward how to find a valid point game with arbitrarily small bias. We now introduce the last model, namely *time independent point games* (TIPG).

As its name suggests, the idea behind a time independent point game is to remove the time ordering of the transitions. This is done by dropping the second condition in Definition 13, imposing that all the points should exist before being "transitioned", and by summing together all the horizontal functions on one hand, and all the vertical ones on the other hand.

Definition 35 (Time independent point game) *A* time independent point game *is a valid horizontal function h and a valid vertical function v such that*

$$h + v = 1[\beta, \alpha] - \frac{1}{2}[0,1] - \frac{1}{2}[1,0],$$

for some $\alpha, \beta > 1/2$. We call the point $[\beta, \alpha]$ the final point of the game.

The interest of this model in comparison to point games with valid transitions is obvious: we only need to find two valid functions, instead of a sequence with an appropriate order. Even simpler, since $h + v = 0$ almost everywhere (except in $[0,1]$, $[1,0]$, and $[\beta, \alpha]$), our task basically boils down to finding a single valid function.

It is easy to construct a time independent point game with final point $[\beta, \alpha]$ from a point game with valid horizontal functions $(h_1, h_2, \ldots, h_n)$, valid vertical functions $(v_1, v_2, \ldots, v_n)$ and final point $[\beta, \alpha]$. As a matter of fact, we take $h = \sum_{i=1}^n h_i$ and $v = \sum_{i=1}^n v_i$. More interestingly, the reverse also holds:

Theorem 5 (TIPG to valid point games) *Given a time independent point game with a valid horizontal function h and a valid vertical function v such that $h + v = 1[\beta, \alpha] - \frac{1}{2}[0,1] - \frac{1}{2}[1,0]$, we can construct, for all $\varepsilon > 0$, a valid point game with final point $[\beta + \varepsilon, \alpha + \varepsilon]$ and a number of transitions that depends on ϵ.*

Before we prove the above theorem let us define *transitively valid transitions*.

Definition 36 (Transitively valid transition) *Let $p, q : [0,\infty) \times [0,\infty) \to [0,\infty)$ be two functions with finite support. The transition $p \to q$ is* transitively valid *if there exists a sequence of valid transitions $p_0 \to p_1, p_1 \to p_2, \cdots, p_{m-1} \to p_m$ such that $p = p_0$ and $q = p_m$.*

Our goal is to show that for every $\varepsilon > 0$ the transition $\frac{1}{2}[0,1] + \frac{1}{2}[1,0] \to 1[\beta + \varepsilon, \alpha + \varepsilon]$ is transitively valid, which implies the theorem.

We start by the following technical lemma:

Lemma 37 *If $p' \to q'$ is a transitively valid transition and $\zeta : [0,\infty) \times [0,\infty) \to [0,\infty)$ is a non-negative function with finite support, then $\delta p' + \zeta \to \delta q' + \zeta$ is also a transitively valid transition for all $\delta > 0$.*

Proof. It suffices to prove the statement for a line transition. Consider a valid line transition $l \to r$ and a non-negative function with finite support ξ, then for all $\delta > 0$, $\delta l + \xi \to \delta r + \xi$ is also a valid transition since $\delta(r - l)$ is a valid function. □

In the following construction of a valid point game from a time indepedent point game, we also keep track of the number of valid transitions we need, which will correspond to the number of rounds of the protocol. We make this more precise at the end of the section.

Proof of Theorem 5. The proof consists of three main parts.

Part 1: First, we show that the transition from $\frac{1}{2}[0,1] + \frac{1}{2}[1,0]$ to $[\beta,\alpha]$ is transitively valid in the presence of an extra set of points that we refer to as a "catalyst", since these points remain unchanged through the transition and their weight can be made arbitrarily small. Let us write $v = v^+ - v^-$, where v^+ and v^- are positive functions with disjoint supports and $h = h^+ - h^-$, where h^+ and h^- are again positive functions with disjoint supports. Then, for any $\gamma > 0$, we show that the following transition is transitively valid:

$$\frac{1}{2}[0,1] + \frac{1}{2}[1,0] + \gamma v^- \to [\beta,\alpha] + \gamma v^-. \tag{4}$$

More precisely, we decompose this transitively valid transition into a sequence of $2\lceil 1/\gamma \rceil$ valid transitions.

By definition of v and h, $v^- \to v^+$ is a valid vertical transition and $h^- \to h^+$ is a valid horizontal transition. Hence, since $\frac{1}{2}[0,1] + \frac{1}{2}[1,0]$ is non-negative, we have by Lemma 37, that

$$\frac{1}{2}[0,1] + \frac{1}{2}[1,0] + v^- \to \frac{1}{2}[0,1] + \frac{1}{2}[1,0] + v^+$$

is a valid vertical transition. Moreover, remark that $h + v = (h^+ - h^-) + (v^+ - v^-) = -(\frac{1}{2}[0,1] + \frac{1}{2}[1,0]) + [\beta,\alpha]$ implies $\frac{1}{2}[0,1] + \frac{1}{2}[1,0] + v^+ = [\beta,\alpha] + h^- - h^+ + v^-$. Define the function with finite support $\zeta = [\beta,\alpha] - h^+ + v^-$. ζ is a positive function: the only place where ζ could be negative is on the support of h^+. But $\zeta + h^- = \frac{1}{2}[0,1] + \frac{1}{2}[1,0] + v^+$ is non negative and $\mathrm{supp}(h^+) \cap \mathrm{supp}(h^-) = \emptyset$ so ζ is non negative. By Lemma 37, we get that $\zeta + h^- \to \zeta + h^+ = [\beta,\alpha] + v^-$ is a valid horizontal transition since $h^- \to h^+$ is a valid horizontal transition and ζ is non negative. This shows that the transition

$$\frac{1}{2}[0,1] + \frac{1}{2}[1,0] + v^- \to [\beta,\alpha] + v^- \tag{5}$$

is transitively valid and can be decomposed into a sequence of two valid transitions. It remains to show how to reduce the weight associated to v^- in the transition.

Lemma 38 *Suppose we have a transitively valid transition $p + \xi \to q + \xi$, then for any $\gamma > 0$, the transition $p + \gamma\xi \to q + \gamma\xi$ is transitively valid.*

Proof. Pick γ' the largest inverse of an integer such that $\gamma \geq \gamma'$, that is $\gamma' = 1/\lceil 1/\gamma \rceil$. By Lemma 37, the following transition

$$p + \gamma'\xi = (1-\gamma')p + \gamma'(p+\xi) \to (1-\gamma')p + \gamma'(q+\xi) = (1-\gamma')p + \gamma'\xi + \gamma' q$$

is transitively valid, since $\gamma'(p+\xi) \to \gamma'(q+\xi)$ is transitively valid and $(1-\gamma')p$ is non-negative. If we repeat one more time, we can see that the following transition is again transitively valid

$$\begin{aligned}(1-\gamma')p + \gamma'\xi + \gamma' q = (1-2\gamma')p + \gamma'\,(p+\xi) + \gamma' q \\ \to (1-\gamma')p + \gamma'\,(q+\xi) + \gamma' q = (1-2\gamma')p + \gamma'\xi + 2\gamma' q.\end{aligned}$$

By repeating this process $1/\gamma' = \lceil 1/\gamma \rceil$ times, we end up with $q + \gamma'\xi$ and by adding on both sides $(\gamma - \gamma')\xi$, we obtain that the transition $p + \gamma\xi \to q + \gamma\xi$ is transitively valid. □

From this Lemma, we conclude the proof that the transition of Equation (4) is transitively valid. Note that we also showed that the transition in Equation (4) can be decomposed into a sequence of $2\lceil 1/\gamma \rceil$ valid transitions.

Part 2: The second part of the proof consists in showing how to construct this small weight catalyst. In fact, we start from our initial distribution of points $\frac{1}{2}[0,1] + \frac{1}{2}[1,0]$ and by using a small part of their weight we construct the catalyst. Then, by performing the transitively valid transition we explained in Part 1, we can move to the final point $[\beta, \alpha]$ with weight almost one; nevertheless there is a small weight left in other points that we will deal with in Part 3.

More precisely, let us define

$$m = \min_{(x,y)\in \mathrm{supp}(v^-)} \{\max\{x,y\}\}.$$

By Lemma 34, $v^-(0,0) = 0$ and hence $m > 0$. In addition, for all $(x,y) \in \mathrm{supp}(v^-)$ it holds that ($x \geq m$ or $y \geq m$). This means, that there exist $a, b \geq 0$ with $\sum_{x,y} v^-(x,y) = \|v^-\| = a+b$ such that the transition

$$a[0,m] + b[m,0] \to v^- \tag{6}$$

is transitively valid. All points $[x,y]$ in the support of v^- can be reached through a point raise of $[0,m]$ or $[m,0]$, and thus the transition Equation (6) can be decomposed into a sequence of two valid transitions.

Let us now assume that $m < 1$ (in fact, the case $m \geq 1$ is simpler and we will consider it afterwards). Let m_x, m_y such that

$$[0,1] \to \frac{am}{a+b}[0,m] + \frac{b + a(1-m)}{a+b}[0,m_y] \text{ and } [1,0] \to \frac{bm}{a+b}[m,0] + \frac{a + b(1-m)}{a+b}[m_x,0] \tag{7}$$

are valid line transitions (such m_x, m_y always exist).

For any $\delta > 0$, we prove that the following transitions are transitively valid:

$$\begin{aligned}
\frac{1}{2}[0,1]+\frac{1}{2}[1,0] \to & \frac{1-\delta}{2}[0,1]+\frac{\delta am}{2(a+b)}[0,m]+\frac{\delta(b+a(1-m))}{2(a+b)}[0,m_y] \\
& +\frac{1-\delta}{2}[1,0]+\frac{\delta bm}{2(a+b)}[m,0]+\frac{\delta(a+b(1-m))}{2(a+b)}[m_x,0] \quad \text{by Equation (7)} \\
\to & (1-\delta)\left(\frac{1}{2}[0,1]+\frac{1}{2}[1,0]+\frac{\delta m}{2(1-\delta)(a+b)}v^-\right) \\
& + \frac{\delta(b+a(1-m))}{2(a+b)}[0,m_y]+\frac{\delta(a+b(1-m))}{2(a+b)}[m_x,0] \quad \text{by Equation (6)} \\
\to & (1-\delta)[\beta,\alpha]+\frac{\delta m}{2(a+b)}v^- \\
& + \frac{\delta(b+a(1-m))}{2(a+b)}[0,m_y]+\frac{\delta(a+b(1-m))}{2(a+b)}[m_x,0] \quad \text{by Equation (4)}
\end{aligned}$$

For $m \geq 1$, we start by considering the raises $[0,1] \to [0,m]$ and $[1,0] \to [m,0]$ and then continue as above. Let $\xi = \frac{m}{2(a+b)}v^- + \frac{b+a(1-m)}{2(a+b)}[0,m_y] + \frac{a+b(1-m)}{2(a+b)}[m_x,0]$. We have shown that for any $\delta > 0$, the transition

$$\frac{1}{2}[1,0]+\frac{1}{2}[0,1] \to (1-\delta)[\beta,\alpha]+\delta\xi \tag{8}$$

is transitively valid. Note that we also showed that the transition in Equation (8) can be decomposed into a sequence of $2+2+2\left\lceil\frac{2(1-\delta)\|v^-\|}{\delta m}\right\rceil$ valid transitions.

Part 3: In this part, we get rid of the $\delta\xi$ in Equation (8) by merging it with the final point $[\beta,\alpha]$. This has as effect that the final point moves to $[\beta+\varepsilon,\alpha+\varepsilon]$. To do this, we use the following Lemma.

Lemma 39 *Given $\varepsilon > 0$ and a function $\xi : [0,\infty) \times [0,\infty) \to [0,\infty)$ with finite support and $\sum_{(x,y)\in\text{supp}(\xi)} \xi(x,y) = 1$, there exists $0 < \delta < 1$ such that $(1-\delta)[\beta,\alpha]+\delta\xi \to [\beta+\varepsilon,\alpha+\varepsilon]$ is transitively valid.*

Proof. By point raising, there exist values n_x and n_y such that $\xi \to [n_x,n_y]$ is transitively valid. Moreover, by further point raising, we can have $n_x > \beta+\varepsilon$ and $n_y > \alpha+\varepsilon$. We pick δ and δ' such that the following two point merges are valid:

$$\begin{aligned}
\delta'[n_x,\alpha]+\delta[n_x,n_y] &\to (\delta+\delta')[n_x,\alpha+\varepsilon], \\
(1-\delta-\delta')[\beta,\alpha+\varepsilon]+(\delta'+\delta)[n_x,\alpha+\varepsilon] &\to [\beta+\varepsilon,\alpha+\varepsilon].
\end{aligned}$$

This is possible by taking $\delta,\delta' > 0$ that satisfy $\delta'\alpha+\delta n_y = (\delta+\delta')(\alpha+\varepsilon)$ and $(1-\delta-\delta')\beta+(\delta'+\delta)n_x = \beta+\varepsilon$. In other words,

$$\delta = \frac{\varepsilon^2}{(n_x-\beta)(n_y-\alpha)} \quad \text{and} \quad \delta' = \frac{\varepsilon}{n_x-\beta}\left(1-\frac{\varepsilon}{n_y-\alpha}\right).$$

We conclude that

$$\begin{aligned}
(1-\delta)[\beta,\alpha]+\delta\xi &\to (1-\delta)[\beta,\alpha]+\delta[n_x,n_y] && \xi\to[n_x,n_y] \text{ transitively valid}\\
&\to (1-\delta-\delta')[\beta,\alpha]+\delta'[n_x,\alpha]+\delta[n_x,n_y] && \text{valid point raise}\\
&\to (1-\delta-\delta')[\beta,\alpha]+(\delta'+\delta)[n_x,\alpha+\varepsilon] && \text{valid merge}\\
&\to (1-\delta-\delta')[\beta,\alpha+\varepsilon]+(\delta'+\delta)[n_x,\alpha+\varepsilon] && \text{valid point raise}\\
&\to [\beta+\varepsilon,\alpha+\varepsilon] && \text{valid merge.}
\end{aligned}$$

□

Note that the transition in Lemma 39 can be decomposed into a sequence of six valid transitions.

This concludes the proof of the Theorem 5. □

Number of rounds The proof of Theorem 5 gives an explicit way of constructing a valid point game with final point $[\beta+\varepsilon,\alpha+\varepsilon]$ from any time independent point game with final point $[\beta,\alpha]$. This construction creates a point game with $10+2\left\lceil\frac{2(1-\delta)\|v^-\|}{\delta m}\right\rceil$ valid transitions where $\delta=\frac{\varepsilon^2}{(n_x-\beta)(n_y-\alpha)}$ and v^-,m,n_x,n_y,α and β are parameters of the original TIPG. In the TIPGs we will consider, we have that $m\geq\frac{1}{2}$ and let $\Gamma=\max\{n_x,n_y\}$. Note also that $\|v^-\|=\|v\|/2=\|h\|/2$. Then, the number of transitions is $O\left(\frac{\|h\|\Gamma^2}{\varepsilon^2}\right)$. This corresponds to the number of rounds of the protocol. Hence, we can restate Theorem 5 as

Corollary 40 *Assume there exists a time independent game 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 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 $O\left(\frac{\|h\|\Gamma^2}{\varepsilon^2}\right)$ valid transitions and final point $[\beta+\varepsilon,\alpha+\varepsilon]$.*

5 Construction of a time independent point game 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 $\left(\frac{1}{\varepsilon}\right)^{O(\frac{1}{\varepsilon})}$.

5.1 Overview of the game

First, to simplify the analysis, we will place all points, except the initial points $[0,1]$ and $[1,0]$, on a regular grid of step ω, i.e. all points can be written as $[a\omega,b\omega]$ for some $a,b\in\mathbb{N}$.

We will describe a family of protocols parametrized by k, whose final point $[\alpha,\alpha]$ is such that $\alpha=\zeta\omega=\frac{1}{2}+O(\frac{1}{k})$. Hence, to achieve a small bias ε, one needs to use the protocol with $k=O(\frac{1}{\varepsilon})$.

The point game with parameter k consists of the three following steps

Split: The point $[0,1]$ is split into points on the vertical axis between positions $\alpha=\zeta\omega$ and $\Gamma\omega$, and same for the point $[1,0]$. See a) in Figure 4. The weight of the points $[0,j\omega]$ and $[j\omega,0]$ for $\zeta\leq j\leq\Gamma$ is given by a function split(j), so that the transitions are valid (in fact, they will be strictly valid).

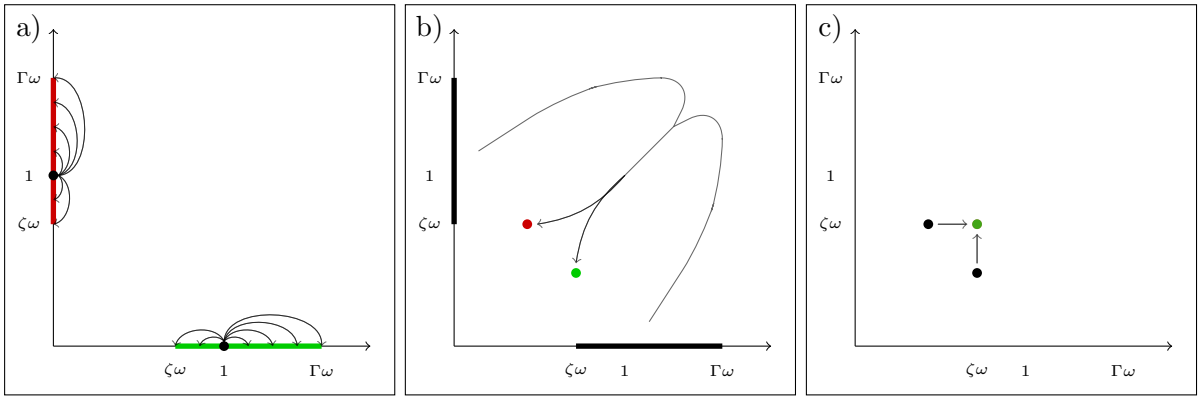

Figure 4: Schematic representation of the game. The initial points are in black, the final points are colored in red if they are part of the horizontal ladder and in green of the vertical ladder. The arrows represents the idea of the movements of the points. a) Each point is split into many points (represented by a line) on their axes. b) The ladder combines the points on the axes into 2 points. c) The raises create the final point of the game.

Ladder of width k: The points on the axes will be transitioned to two final points $[\alpha - k\omega, \alpha]$ and $[\alpha, \alpha - k\omega]$. See b) in Figure 4. This transition is transitively valid, meaning that there exists a sequence of valid transitions starting from the points on the axes and ending at the two final points. These transitions use more points on the grid, in fact, points whose x and y coordinates are between $\alpha - k\omega$ and $\Gamma\omega$. Moreover, on every line, except the two axes, there are at most $2k + 1$ points.

Raise: The two points are raised into a final point $[\alpha, \alpha]$. See c) in Figure 4. This raise is valid.

More formally:

$$\frac{1}{2}[0,1] + \frac{1}{2}[1,0] \xrightarrow{\text{split}} \sum_{j=\zeta}^{\Gamma} \text{split}(j)[0, j\omega] + \sum_{j=\zeta}^{\Gamma} \text{split}(j)[j\omega, 0] \tag{9}$$

$$\xrightarrow{\text{ladder}} \frac{1}{2}[\alpha - k\omega, \alpha] + \frac{1}{2}[\alpha, \alpha - k\omega] \tag{10}$$

$$\xrightarrow{\text{raise}} 1[\alpha, \alpha]$$

The next two sections are devoted to proving that for any k there exist values for the parameters ω and Γ, such that the two initial splits are valid, the ladder is a transitively valid transition, and $\alpha = \frac{1}{2} + O(\frac{1}{k})$.

5.2 The ladder

5.2.1 Description

We define a *ladder* as a time independent point game, described by a valid horizontal function h_{lad} and a valid vertical function v_{lad} such that

$$h_{\text{lad}} + v_{\text{lad}} = \frac{1}{2}[\alpha - k\omega, \alpha] + \frac{1}{2}[\alpha, \alpha - k\omega] - \sum_{j=\zeta}^{\Gamma} \text{split}(j)\left([0, j\omega] + [j\omega, 0]\right),$$

where for each axis, split(j) is a distribution on points on the axis that arises from a split of the initial point $[0,1]$ or $[1,0]$ (see Section 3.6 for the definition of a split); its exact parameters will be defined shortly.

Our goal is to find functions h_{lad} and v_{lad} that may put weight also on other points on the grid, such that both h_{lad} and v_{lad} are valid functions. Moreover, we need to do this while finding a function split(j) such that the initial split is a valid transition.

We restrict ourselves to symmetric point games, i.e. games where the horizontal function h and the vertical function v satisfy:

$$v(x,y) = -h(x,y) \quad \text{and also} \quad h(x,y) = -h(y,x), \tag{11}$$

except for the final and initial points. This implies that there are no points on the diagonal, i.e. $\forall z,\ h(z,z) = v(z,z) = 0$ and that if h_{lad} is a valid function, then v_{lad} will be valid too.

In fact, we do not know of a simple way of transitioning the points on the axes to the two final points. To do so, we must add new points and perform a sequence of transitions that will gradually transition the points on the axes to the final two points. We now describe these extra points.

We call a *rung* in the ladder, the function corresponding to the points at a fixed height, i.e. $h_{\text{rung}}(\cdot, y) = \sum_x h(x,y)$ for some y. Our ladder will have rungs from height $\alpha = \zeta\omega$ to $\Gamma\omega$. A *ladder of width* k has rungs that have $2k$ points centered on the diagonal and one point on the y-axis. More formally for $\zeta \le j \le \Gamma$, the x-coordinate of the points of the rung at height $j\omega$ are

$$\{0,\ (j-k)\,\omega,\ (j-k+1)\,\omega, \ldots,\ (j-1)\omega,\ (j+1)\omega, \ldots, (j+k-1)\,\omega,\ (j+k)\,\omega\}\,. \tag{12}$$

Note that we will have $k\omega \ll \zeta\omega$, meaning that all points are at least a constant away from the axes. Some principles governing the ladder are shown in Figure 5. First in a), we give a schematic representation of all the points defined in Equation (12) that are the horizontal part of the ladder. For every point of the vertical axis, we consider $2k$ new points on the same height and centered on the diagonal.The vertical part is constructed using the symmetry relation (11) we imposed. Both, the horizontal part and the vertical part of the ladder are represented in b). By symmetry, we also have that if a point is in the horizontal and in the vertical part of the ladder, the sum of its weights is null. All these points are located on the overlap of the two parts of the ladder. There are then only a few remaining points: the initial points on the axes, the final points in $[\alpha - k\omega, \alpha]$ and $[\alpha, \alpha - k\omega]$ and 4 "triangles". We get rid of these triangles by considering ladders where the weight on these triangles is 0. Hence, all the points we consider are shown in c).

5.2.2 Finding weights for the points in the ladder

Our goal, now, is to find weights for the points on the axes and the remaining points on the plane such that the function h_{lad} is valid. By symmetry, v_{lad} will also be valid. As we have said, $h_{\text{lad}} = \sum_{j=\zeta}^{\Gamma} h^j_{\text{rung}}$, where h^j_{rung} is the rung function on height $j\omega$.

Note that when finding the functions h^j_{rung}, we also fix the weights on the points of the original split (this gives an explicit definition of the split function in Equation (9)). In Section 5.3 we show that for any k, we can choose parameters Γ and ω such that this split is valid, and such that $\alpha = \frac{1}{2} + O(\frac{1}{k})$.

Finding valid functions h^j_{rung} is not an easy task. Let us assume that $h^j_{\text{rung}} = \sum_i w_i[x_i]$ and that we would like to verify that the function is valid. According to Lemma 30, it would be necessary to prove that for all $\lambda > 0$, $\sum_i \frac{-w_i}{\lambda + x_i} = \frac{-\sum_i w_i \prod_{k \neq i}(\lambda + x_k)}{\prod_k (\lambda + x_k)} \ge 0$. In practice, this means

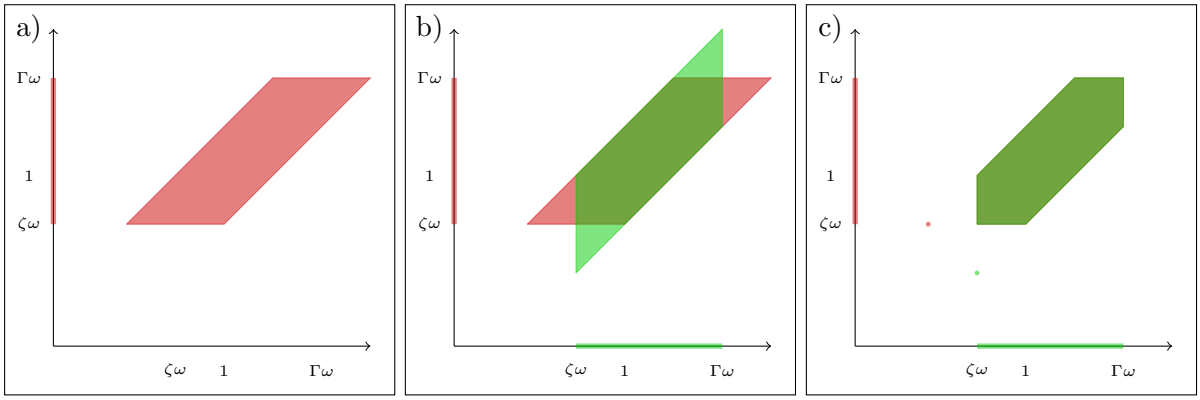

Figure 5: Schematic construction of the ladder. a) The horizontal part of the ladder. b) Superposition of the horizontal part and the vertical part of the ladder. By symmetry, the sum of the weights of the point in the overlap is 0. Except the final points, the weights of the points in the 4 "triangles" with no overlap will be set to 0 by truncation. c) All the points actually involved in the ladder transition.

checking that the polynomial $f(-\lambda) = -\sum_i w_i \prod_{k\neq i}(\lambda + x_k) \geq 0$ for all $\lambda < 0$. In other words, from a given function we can construct a polynomial f such that the validity of the function holds when $f(\lambda) \geq 0$ for all $\lambda < 0$. The following Lemma basically does the reverse. Given a low degree polynomial f with $f(\lambda) \geq 0$ for all $\lambda < 0$, we construct a valid function h_{rung} by assigning weights $\frac{-f(x_i)}{\prod_{k\neq i}(x_k - x_i)}$ to $[x_i]$.

Lemma 41 *Let $x_1, \ldots, x_{2k+1} \in \mathbb{R}_+$ be different points, $f \in \mathbb{R}[X]$ be a real polynomial such that:*

- *the absolute value of its leading coefficient is 1,*
- $\deg(f) \leq 2k - 1$,
- $\forall x < 0,\ f(x) \geq 0$,

then $\forall C > 0$ the following function h_{rung} is a valid function:

$$h_{\text{rung}} = \sum_{i=1}^{2k+1} \frac{-C \cdot f(x_i)}{\prod_{j\neq i}(x_j - x_i)} [x_i]\,. \tag{13}$$

This lemma gives us some freedom in the choice of the polynomials. At height $j\omega$ we are looking for a function $h_{\text{rung}}(\cdot, j\omega)$ of the form

$$h^j_{\text{rung}} = \frac{-C_j \cdot f(0, j\omega)}{\prod_{\substack{l=-k \\ l\neq 0}}^{k}((j+l)\omega)}[0, j\omega] + \sum_{\substack{i=-k \\ i\neq 0}}^{k} \frac{-C_j \cdot f((j+i)\omega, j\omega)}{-(j+i)\omega \prod_{\substack{l\neq i \\ l\neq 0}}((l-i)\,\omega)}\,[(j+i)\omega, j\omega]\,.$$

Note that the first term corresponds to the point on the axis and the remaining $2k$ points are centered on the diagonal (see Equation (12) for the x-coordinate of the points of the rung at height $j\omega$).

We start by taking $C_j = C/j\omega$, so that the weights are symmetric and we can add the rung functions more easily. We have

$$h^j_{\text{rung}} = \frac{-C \cdot f(0, j\omega)}{\prod_{l=-k}^{k}((j+l)\omega)}[0, j\omega] + \sum_{\substack{i=-k \\ i\neq 0}}^{k} \frac{C \cdot f((j+i)\omega, j\omega)}{((j+i)\omega)(j\omega)\prod_{\substack{l\neq i \\ l\neq 0}}((l-i)\omega)}[(j+i)\omega, j\omega]\,.$$

Adding all the rungs of different heights, we get:

$$h_{\text{lad}} = \sum_{j=\zeta}^{\Gamma}\left(\frac{-C \cdot f(0, j\omega)}{\prod_{l=-k}^{k}((j+l)\omega)}[0, j\omega] + \sum_{\substack{i=-k \\ i\neq 0}}^{k} \frac{C \cdot f((j+i)\,\omega,\ j\omega)}{((j+i)\omega)(j\omega)\prod_{\substack{l\neq i \\ l\neq 0}}((l-i)\omega)}[(j+i)\omega,\ \ j\omega]\right). \quad (14)$$

Now, we need to ensure that when we add the the functions h_{lad} and v_{lad} we are only left with the points on the axes and the two final points $[\alpha - k\omega, \alpha]$ and $[\alpha, \alpha - k\omega]$. Since they are symmetric functions, this means that it is necessary and sufficient to put zero weight on the points that appear only in h_{lad} or only in v_{lad}. This corresponds to the ladder truncation we described in Figure 5. To do so, we choose the symmetric polynomial f so that the weight on the points with x-coordinate in $\{\alpha - (k-1)\omega, \alpha - (k-2)\omega, \ldots, \alpha - \omega\}$ as well as in $\{(\Gamma + 1)\omega, \ldots, (\Gamma + k)\omega\}$ is zero (both for the horizontal and vertical function). Since we want a polynomial of degree at most $2k-1$ on each variable, we have only one possibility:

$$f(x, y) = (-1)^{k+1}\prod_{i=1}^{k-1}(\alpha - i\omega - x)(\alpha - i\omega - y)\prod_{i=1}^{k}(\Gamma\omega + i\omega - x)(\Gamma\omega + i\omega - y)\,. \quad (15)$$

When we look at the polynomial $f(x, y)$ as a polynomial on one variable, then it needs to satisfy the hypothesis of Lemma 41. Indeed, the absolute value of its leading coefficient is 1, its degree is $2k-1$ and $\forall\, \zeta \leq j \leq \Gamma$ and $\forall x < 0$ we have $f(x, j\omega) \geq 0$. This is true, since the only negative terms in the product are the $(k-1)$ negative values $(\alpha - i\omega - j\omega)$ and another $(k+1)$ from the $(-1)^{k+1}$ factor.

Hence, we conclude that h_{lad} is a valid horizontal function (and similarly v_{lad} is a valid vertical function). Since $v_{\text{lad}}(x, y) = -h_{\text{lad}}(x, y)$ everywhere except on the points on the axes and $[\alpha, \alpha - k\omega]$ and $[\alpha - k\omega, \alpha]$, adding the two function leaves us with the desired outcome. We have proved that

Lemma 42 *The function h_{lad} as defined in Equation (14) and Equation (15) and, by symmetry, the function v_{lad}, are valid functions that satisfy*

$$h_{\text{lad}} + v_{\text{lad}} = \frac{1}{2}[\alpha - k\omega, \alpha] + \frac{1}{2}[\alpha, \alpha - k\omega] - \sum_{j=\zeta}^{\Gamma}\text{split}(j)\,([0, j\omega] + [j\omega, 0])$$

with

$$\text{split}(j) = \frac{C \cdot f(0, j\omega)}{\prod_{l=-k}^{k}((j+l)\omega)}. \quad (16)$$

In Section 5.3, we will see that for every k, we can find values for the parameters C, ω and Γ and take $\alpha = \frac{1}{2} + \frac{c}{k}$ for some constant c, such that the two initial splits defined by the function $\text{split}(j)$ are valid. Before that, we provide the proof of Lemma 41.

5.2.3 Proof of Lemma 41

We start with the following technical Lemma

Lemma 43 *Let $x_1, \dots, x_m$ be m (≥ 2) distinct values in $\mathbb{R}$ and f a polynomial such that* $\deg(f) \leq m-2$, *then*

$$\sum_{i=1}^{m} \frac{f(x_i)}{\prod_{j\neq i}(x_j - x_i)} = 0.$$

Proof. By induction on $\deg(f)$. For $\deg(f) = 0$ we need to prove that $\sum_{i=1}^{m} \prod_{j\neq i} \frac{1}{x_j - x_i} = 0$. This proof is also done by induction, this time on the number of points. The initialization is trivial. For $m > 2$ and $1 < i < m$ we have the identity:

$$\frac{1}{(x_1 - x_i)(x_m - x_i)} = \frac{1}{x_m - x_1}\left(\frac{1}{x_1 - x_i} - \frac{1}{x_m - x_i}\right).$$

which gives us:

$$\begin{aligned}
\sum_{i=1}^{m}\prod_{\substack{j=1\\j\neq i}}^{m} \frac{1}{x_j - x_i} &= \prod_{j=2}^{m}\frac{1}{x_j - x_1} + \frac{1}{x_m - x_1}\sum_{i=2}^{m-1}\prod_{\substack{j=2\\j\neq i}}^{m-1}\frac{1}{x_j - x_i}\left(\frac{1}{x_1 - x_i} - \frac{1}{x_m - x_i}\right) + \prod_{j=1}^{m-1}\frac{1}{x_j - x_m} \\
&= \frac{1}{x_m - x_1}\left[\sum_{i=2}^{m-1}\left(\prod_{\substack{j=1\\j\neq i}}^{m-1}\frac{1}{x_j - x_i} - \prod_{\substack{j=2\\j\neq i}}^{m}\frac{1}{x_j - x_i}\right) + \prod_{j=2}^{m-1}\frac{1}{x_j - x_1} - \prod_{j=2}^{m-1}\frac{1}{x_j - x_m}\right] \\
&= \frac{1}{x_m - x_1}\left(\sum_{i=1}^{m-1}\prod_{\substack{j=1\\j\neq i}}^{m-1}\frac{1}{x_j - x_i} - \sum_{i=2}^{m}\prod_{\substack{j=2\\j\neq i}}^{m}\frac{1}{x_j - x_i}\right)
\end{aligned}$$

by induction, each of the terms in the parenthesis is 0. That concludes the proof for $\deg(f) = 0$. If $\deg(f) \leq k$, there exists a constant $\kappa \neq 0$ and a polynomial g with $\deg(g) < k$ such that $f(x) = \kappa \prod_{j=1}^{k}(x_j - x) + g(x)$. We then have:

$$\sum_{i=1}^{m}\frac{f(x_i)}{\prod_{\substack{j=1\\j\neq i}}^{m}(x_j - x_i)} = \underbrace{\kappa \sum_{i=k+1}^{m}\prod_{\substack{j=k+1\\j\neq i}}^{m}\frac{1}{x_j - x_i}}_{=0 \text{ initialization case}} + \underbrace{\sum_{i=1}^{m}\frac{g(x_i)}{\prod_{\substack{j=1\\j\neq i}}^{m}(x_j - x_i)}}_{=0 \text{ by induction}}.$$

□

Proof of Lemma 41. Fix $C > 0$. We have two statements to show: first that $\sum_x h_{\text{rung}}(x) = 0$. This is immediate using the previous lemma. Secondly, let us fix $\lambda > 0$, we need to show that $Q = \sum_x \left(\frac{-1}{\lambda + x}\right) h_{\text{rung}}(x) \geq 0$.

$$Q \geq 0 \iff \sum_{i=1}^{2k+1}\frac{1}{\lambda + x_i}\cdot\frac{f(x_i)}{\prod_{\substack{j=1\\j\neq i}}^{2k+1} x_j - x_i} \geq 0 \qquad \text{since } C > 0.$$

Using Lemma 43, with the points $\{-\lambda, x_1, \ldots, x_{2k+1}\}$ we have:

$$\frac{f(-\lambda)}{\prod_{j=1}^{2k+1}(x_j-(-\lambda))} + \sum_{i=1}^{2k+1} \frac{f(x_i)}{((-\lambda)-x_i)\prod_{\substack{j=1\\ j\neq i}}^{2k+1}(x_j-x_i)} = 0.$$

Combining the two previous equations, we get:

$$Q \geq 0 \iff \frac{f(-\lambda)}{\prod_{j=1}^{2k+1}(x_j-(-\lambda))} \geq 0.$$

By assumption, $f(-\lambda) \geq 0$ and all the terms $(x_j + \lambda)$ are positive.

□

5.3 Validity of initial splits

Here we show that for every k, we can find values for the parameters C, ω, and Γ as functions of k, and take $\alpha = \frac{1}{2} + \frac{c}{k}$ for some constant c, such that the two initial splits defined in Equation (16) by the function $\text{split}(j)$ are valid.

Lemma 44 (The splits are valid) *For any k, we can find ω and Γ, such that by taking $\alpha = \frac{1}{2} + \frac{c}{k}$ for some constant c, the functions*

$$h_{\text{split}} = \sum_{j=\zeta}^{\Gamma} \text{split}(j)[j\omega, 0] - \frac{1}{2}[1,0] \quad \text{and} \quad v_{\text{split}} = \sum_{j=\zeta}^{\Gamma} \text{split}(j)[0, j\omega] - \frac{1}{2}[0,1]$$

are valid functions, where $\text{split}(j) = \frac{C \cdot f(0,j\omega)}{\prod_{l=-k}^{k}((j+l)\omega)}$ *and* $C = \frac{1}{2} \cdot \left(\sum_{j=\zeta}^{\Gamma} \frac{f(0,j\omega)}{\prod_{l=-k}^{k} \omega(j+l)} \right)^{-1}$.

Proof. We consider the vertical split (similarly for the horizontal one). By the analysis of point splits in Section 3.6, it suffices to verify two conditions: first, that $\sum_{j=\zeta}^{\Gamma} \text{split}(j) = \frac{1}{2}$, which holds for our choice of C. Second, we need to show that

$$\frac{1}{2} > \sum_{j=\zeta}^{\Gamma} \frac{C \cdot f(0, j\omega)}{j\omega \prod_{l=-k}^{k} \omega\,(j+l)}.$$

By replacing the value of C we get:

$$\sum_{j=\zeta}^{\Gamma} \frac{f(0,j\omega)}{\prod_{l=-k}^{k} \omega\,(j+l)} > \sum_{j=\zeta}^{\Gamma} \frac{f(0,j\omega)}{j\omega \prod_{l=-k}^{k} \omega\,(j+l)}.$$

We know that

$$\begin{aligned} f(0,j\omega) &= (-1)^{k+1} \prod_{i=1}^{k-1} (\alpha - i\omega)(\alpha - i\omega - j\omega) \prod_{i=1}^{k} (\Gamma\omega + i\omega)(\Gamma\omega + i\omega - j\omega) \\ &= \left[\prod_{i=1}^{k-1} (j\omega - (\alpha - i\omega)) \prod_{i=1}^{k} (\Gamma\omega + i\omega - j\omega) \right] \left[\prod_{i=1}^{k-1} (\alpha - i\omega) \prod_{i=1}^{k} (\Gamma\omega + i\omega) \right]. \end{aligned}$$

We can divide each side of the inequality with the square of the second bracket, which is independent of j and non-zero, and have

$$\sum_{j=\zeta}^{\Gamma} p(j\omega) > \sum_{j=\zeta}^{\Gamma} \frac{p(j\omega)}{j\omega} \quad \text{with} \quad p(j\omega) = \prod_{i=1}^{k-1} \frac{j\omega - (\alpha - i\omega)}{\alpha - i\omega} \prod_{i=1}^{k} \frac{\Gamma\omega + i\omega - j\omega}{\Gamma\omega + i\omega} \prod_{i=-k}^{k} \frac{1}{j\omega + i\omega}. \quad (17)$$

To conclude the proof we will need to show that Inequality (17) holds for $\alpha = \frac{1}{2} + \frac{c}{k}$ for some constant c and for some chosen ω and Γ. This is done in Section 5.3.1; an alternative proof is given in Section 6. □

5.3.1 Concluding the proof of existence

To conclude the proof of Lemma 44, and with it the proof of existence of a WCF protocol with an arbitrarily small bias, we will need to show that Inequality (17) holds for $\alpha = \frac{1}{2} + \frac{c}{k}$ for some constant c and for some chosen ω and Γ. In this subsection we do exactly this. To this end, we provide the following technical lemma. This lemma shows that Inequality (17) can be simplified by approximating p by the function $f(x) = \left(\frac{x-\alpha}{\alpha}\right)^{k-1} x^{-2k-1}$ and the sum by an integral. The approximation of p by f is quantified by the function E and the approximation of the sum by the integrals by the functions ϵ_l and ϵ_r.

Lemma 45 *Fix any values for the parameters ω, Γ, α, such that $\omega < 1$, $\Gamma\omega^2 > 1$, and $\alpha > 1/2$. Define the functions $f(x) = \left(\frac{x-\alpha}{\alpha}\right)^{k-1} x^{-2k-1}$, $\tilde{f}(x) = f(x)/x$, $\epsilon_l(\omega, \Gamma) = \Gamma\omega^4 \left|f''\right|_\infty$, $\epsilon_r(\omega, \Gamma) = \Gamma\omega^4 \left|\tilde{f''}\right|_\infty$, and $E(\omega) = \frac{(1+2k\omega)^{2k+1}}{(1-4k\omega)^{4k+1}}$. If the following inequality holds*

$$\int_{\alpha}^{\Gamma\omega^2} f(x)\mathrm{d}x - \epsilon_l(\omega, \Gamma) > E(\omega) \left[\int_{\alpha}^{\infty} \tilde{f}(x)\mathrm{d}x + \epsilon_r(\omega, \Gamma)\right], \quad (18)$$

then Inequality (17) also holds for the same ω, Γ, and α.

The proof of this lemma is delayed to the next subsection. This lemma implies that in order to prove Lemma 44, we just need to find Γ, ω satisfying $\omega < 1, \Gamma\omega^2 > 1$ and $\alpha = \frac{1}{2} + \frac{c}{k}$ for some constant c.

We introduce the Beta function $B(a, b)$. In Section 6 we will also need a related function, the Regularized Incomplete Beta function $I(z; a, b)$. These two functions are defined by:

$$B(a, b) = \int_0^1 t^{a-1}(1-t)^{b-1}\mathrm{d}t = \alpha^a \int_{\alpha}^{\infty} (t-\alpha)^{b-1} t^{-a-b}\mathrm{d}t,$$
$$I(z; a, b) = \frac{1}{B(a, b)} \int_0^z t^{a-1}(1-t)^{b-1}\mathrm{d}t = \frac{\alpha^a}{B(a, b)} \int_{\alpha/z}^{\infty} (t-\alpha)^{b-1} t^{-a-b}\mathrm{d}t.$$

Both functions have very nice form when a and b are integers

$$I(z; a, b) = \sum_{j=a}^{a+b-1} \binom{a+b-1}{j} z^j (1-z)^{a+b-1-j} \quad \text{and} \quad B(a, b) = \frac{(a-1)!(b-1)!}{(a+b-1)!}. \quad (19)$$

We now prove our final lemma which concludes the proof of Lemma 44.

Lemma 46 *For any k, we can find Γ, ω such that Inequality (18) is satisfied for any $\alpha > \frac{k+1}{2k+1}$*

Proof. Let us take $\Gamma = \omega^{-3}$, so that when we look at the limit $\omega \to 0$, we have $\Gamma \to \infty$, $\Gamma\omega^2 \to \infty$ and $\Gamma\omega^4 \to 0$. We have

$$\lim_{\omega\to 0} \int_\alpha^{\Gamma\omega^2} f(x)\mathrm{d}x - \epsilon_l(\omega,\Gamma) = \int_\alpha^\infty f(x)\mathrm{d}x$$

and

$$\lim_{\omega\to 0} E(\omega)\left[\int_\alpha^\infty \tilde{f}(x)\mathrm{d}x + \epsilon_r(\omega,\Gamma)\right] = \int_\alpha^\infty \tilde{f}(x)\mathrm{d}x.$$

Using the Beta function, we have $\int_\alpha^\infty f(x)\mathrm{d}x = \frac{B(k+1,k)}{\alpha^{2k+2}}$ and $\int_\alpha^\infty \tilde{f}(x)\mathrm{d}x = \frac{B(k+2,k)}{\alpha^{2k+3}}$ which implies

$$\int_\alpha^\infty f(x)\mathrm{d}x > \int_\alpha^\infty \tilde{f}(x)\mathrm{d}x \quad \text{for } \alpha > \frac{B(k+2,k)}{B(k+1,k)} = \frac{k+1}{2k+1}.$$

From there, we have

$$\lim_{\omega\to 0} \int_\alpha^{\Gamma\omega^2} f(x)\mathrm{d}x - \epsilon_l(\omega,\Gamma) > \lim_{\omega\to 0} E(\omega)\left[\int_\alpha^\infty \tilde{f}(x)\mathrm{d}x + \epsilon_r(\omega,\Gamma)\right].$$

This means that we can find a small ω and $\Gamma = \omega^{-3}$ such that Inequality (18) holds for any $\alpha > \frac{k+1}{2k+1}$. □

Together with the proof of Lemma 45 (see Section 5.3.2 below) this concludes the proof of existence of a WCF protocol.

In Section 6, we analyze the resources needed for the protocol, in terms of qubits and number of rounds. To do this, we need to have explicit expressions of ω, Γ as a function of k. Unfortunately, Lemma 46 only shows the existence of ω, Γ without expliciting what those terms are. In Section 6, we provide a more detailed version of Lemma 46 that allows us to keep track of the resources. Before that, we provide the proof of Lemma 45.

5.3.2 Proof of Lemma 45

Proof. Step 1: Approximation of p by f. First note that, since $\Gamma\omega^2 > 1$, Inequality (17) holds if the following inequality holds

$$\sum_{j=\zeta}^{\Gamma\omega} p(j\omega) > \sum_{j=\zeta}^{\Gamma\omega} \frac{p(j\omega)}{j\omega}.$$

Notice than for $j > \Gamma\omega$ we have $j\omega > 1$.

The first order of business is to show that the term $\prod_{i=1}^k \frac{\Gamma\omega+i\omega-j\omega}{\Gamma\omega+i\omega} \approx 1$. We have

$$1 \geq \prod_{i=1}^k \frac{\Gamma\omega + i\omega - j\omega}{\Gamma\omega + i\omega} \geq \left(1 - \frac{j}{\Gamma}\right)^k \geq (1-\omega)^k.$$

Hence for all $j \in [\zeta, \Gamma\omega]$ we have

$$(1-\omega)^k \prod_{i=1}^{k-1} \frac{j\omega - (\alpha - i\omega)}{\alpha - i\omega} \prod_{i=-k}^{k} \frac{1}{j\omega + i\omega} < p(j\omega) < \prod_{i=1}^{k-1} \frac{j\omega - (\alpha - i\omega)}{\alpha - i\omega} \prod_{i=-k}^{k} \frac{1}{j\omega + i\omega}.$$

We now bound all the term in the products individually,

$$(1-\omega)^k\left(\frac{j\omega-\alpha}{\alpha}\right)^{k-1}\left(\frac{1}{j\omega+k\omega}\right)^{2k+1}<p(j\omega)<\left(\frac{j\omega-\alpha+k\omega}{\alpha-k\omega}\right)^{k-1}\left(\frac{1}{j\omega-k\omega}\right)^{2k+1}.$$

This means that the following inequality is a sufficient condition for Inequality (17):

$$(1-\omega)^k\sum_{j=\zeta}^{\Gamma\omega}\left(\frac{j\omega-\alpha}{\alpha}\right)^{k-1}\left(\frac{1}{j\omega+k\omega}\right)^{2k+1}>\sum_{j=\zeta}^{\Gamma\omega}\left(\frac{j\omega-\alpha+k\omega}{\alpha-k\omega}\right)^{k-1}\left(\frac{1}{j\omega-k\omega}\right)^{2k+1}\frac{1}{j\omega}. \quad (20)$$

We want to take the terms in $k\omega$ out of the sum in order to keep only terms in $j\omega$ and hence be able to replace the sums by integrals. For the LHS, we have:

$$\frac{1}{j\omega+k\omega}=\frac{1}{j\omega}\cdot\frac{1}{(1+\frac{k\omega}{j\omega})}>\frac{1}{j\omega}\cdot\frac{1}{1+2k\omega}$$

since $j\omega\geq\alpha>1/2$.

For the RHS, we first shift the sum in order to remove the term $k\omega$ in the numerator.

$$\begin{aligned}\sum_{j=\zeta}^{\Gamma\omega}\left(\frac{j\omega-\alpha+k\omega}{\alpha-k\omega}\right)^{k-1}\left(\frac{1}{j\omega-k\omega}\right)^{2k+1}\frac{1}{j\omega}&=\sum_{j=\zeta+k}^{\Gamma\omega+k}\left(\frac{j\omega-\alpha}{\alpha-k\omega}\right)^{k-1}\left(\frac{1}{j\omega-2k\omega}\right)^{2k+1}\frac{1}{j\omega-k\omega}\\&<\sum_{j=\zeta+k}^{\Gamma\omega+k}\left(\frac{j\omega-\alpha}{\alpha-k\omega}\right)^{k-1}\left(\frac{1}{j\omega-2k\omega}\right)^{2k+2}.\end{aligned}$$

We now bound the terms in the new RHS. We have

$$\frac{1}{\alpha-k\omega}<\frac{1}{\alpha}\cdot\frac{1}{1-2k\omega}<\frac{1}{\alpha}\cdot\frac{1}{1-4k\omega}\quad\text{and}\quad\frac{1}{j\omega-2k\omega}<\frac{1}{j\omega}\cdot\frac{1}{1-4k\omega}. \quad (21)$$

Plugging these inequalities in the LHS and RHS of Equation (20), we get that the following inequality is a sufficient condition for Inequality (17).

$$\frac{(1-\omega)^k}{(1+2k\omega)^{2k+1}}\sum_{j=\zeta}^{\Gamma\omega}\left(\frac{j\omega-\alpha}{\alpha}\right)^{k-1}\left(\frac{1}{j\omega}\right)^{2k+1}>\frac{1}{(1-4k\omega)^{(3k+1)}}\sum_{j=\zeta+k}^{\Gamma\omega+k}\left(\frac{j\omega-\alpha}{\alpha}\right)^{k-1}\left(\frac{1}{j\omega}\right)^{2k+2}$$

Consequently, using $(1-\omega)\geq(1-4k\omega)$, we have that if the following inequality holds

$$\sum_{j=\zeta}^{\Gamma\omega}\left(\frac{j\omega-\alpha}{\alpha}\right)^{k-1}\left(\frac{1}{j\omega}\right)^{2k+1}>E(\omega)\sum_{j=\zeta+k}^{\Gamma\omega+k}\left(\frac{j\omega-\alpha}{\alpha}\right)^{k-1}\left(\frac{1}{j\omega}\right)^{2k+2}$$

with $E(\omega)=\frac{(1+2k\omega)^{2k+1}}{(1-4k\omega)^{4k+1}}$, then Inequality (17) also holds.

Step 2: Approximating sums by integrals. The two sums can be approximately computed by replacing them by an integral, using the so-called rectangle method:

$$\begin{aligned}\omega\sum_{j=\zeta}^{\Gamma\omega}\left(\frac{j\omega-\alpha}{\alpha}\right)^{k-1}\left(\frac{1}{j\omega}\right)^{2k+1}&>\int_{\alpha}^{\Gamma\omega^2}f(x)\mathrm{d}x-\frac{\Gamma\omega^2-\alpha}{24}\omega^2\left|f''\right|_\infty,\\\omega\sum_{j=\zeta+k}^{\Gamma\omega+k}\left(\frac{j\omega-\alpha}{\alpha}\right)^{k-1}\left(\frac{1}{j\omega}\right)^{2k+2}&<\int_{\alpha+k\omega}^{\Gamma\omega^2+k\omega}\tilde{f}(x)\mathrm{d}x+\frac{\Gamma\omega^2-\alpha}{24}\omega^2\left|\tilde{f}''\right|_\infty,\end{aligned}$$

where $\tilde{f}(x) = f(x)/x$. Notice that the error terms are upper-bounded by $\epsilon_l(\omega, \Gamma) = \Gamma\omega^4 \left|f''\right|_\infty$ and $\epsilon_r(\omega, \Gamma) = \Gamma\omega^4 \left|\tilde{f}''\right|_\infty$ respectively.

Last, observe that $\int_{\alpha+k\omega}^{\Gamma\omega^2+k\omega} \tilde{f}(x)\mathrm{d}x < \int_\alpha^\infty \tilde{f}(x)\mathrm{d}x$ since $\tilde{f} \geq 0$ on $[\alpha, +\infty)$. □

6 Resources of the protocol

We now provide an alternative way to finishing the proof of existence provided in Section 5.3.1, which allows us to analyze the resources needed for the protocol. In Section 6.1, we provide a more detailed version of Lemma 46 that allows us to keep track of the resources. In Section 6.2, we show that the number of qubits used for a protocol with bias ε is $O(\log \frac{1}{\varepsilon})$, while the number of rounds is $\left(\frac{1}{\varepsilon}\right)^{O(\frac{1}{\varepsilon})}$.

6.1 Refined analysis of strict validity of initial splits

Given Lemma 45, we will find specific values for the parameters α, ω, and Γ for which Equation (18) is satisfied. These parameters will allow us to calculate the resources necessary for the protocol.

Lemma 47 *For any k, by taking $\alpha = \frac{1}{2} + \frac{c}{k}$ for some constant c, $\omega = k^{-4}$ and $\Gamma = 2k^8$, Inequality (18) holds.*

Note first, that the values $\alpha = \frac{1}{2} + \frac{c}{k}$ for some constant c, $\omega = k^{-4}$ and $\Gamma = 2k^8$ satisfy the assumptions of the Lemma 45.

Proof. We are going to prove that for the chosen values of ω and Γ, it is sufficient to chose $\alpha > \frac{k+1}{2k+1} + O\left(\frac{1}{k^2}\right) = \frac{1}{2} + \frac{1}{4k+2} + O\left(\frac{1}{k^2}\right)$ for Inequality (18) to hold.

We have

$$\begin{aligned}\int_\alpha^{\Gamma\omega^2} f(x)\mathrm{d}x &= \int_\alpha^\infty f(x)\mathrm{d}x - \int_{\Gamma\omega^2}^\infty f(x)\mathrm{d}x = \frac{B(k+1,k)}{\alpha^{2k+2}} - B(k+1,k)\frac{I(\alpha/\Gamma\omega^2; k+1, k)}{\alpha^{2k+2}} \\ &= \frac{B(k+1,k)}{\alpha^{2k+2}}(1 - I(\alpha/\Gamma\omega^2; k+1, k)).\end{aligned}$$

Recall that we have $\Gamma\omega^2 = 2$, and use Equation (19) to get

$$1 - I(\alpha/2; k+1, k) = \sum_{j=0}^{k} \binom{2k}{j} \left(\frac{\alpha}{2}\right)^j \left(1 - \frac{\alpha}{2}\right)^{2k-j}.$$

Since we have $\alpha/2 < 1/2$, we can use the Chernoff bound [Che52]:

$$1 - I(\alpha/2; k+1, k) > 1 - \alpha^k e^{(k-k\alpha)} = 1 - e^{k(1-\alpha+\log\alpha)} > 1 - e^{-\Omega(k)}. \tag{22}$$

Let us now bound the error term $\epsilon_l(\omega, \Gamma) = \epsilon_l(k^{-4}, 2k^8) = 2k^{-8}\left|f''\right|_\infty$. We have

$$f''(x) = \frac{1}{\alpha^{k+1}}\left[(k-1)(k-2)\frac{(x-\alpha)^{k-3}}{x^{2k+1}} - 2(k-1)(2k+1)\frac{(x-\alpha)^{k-2}}{x^{2k+2}} + (2k+1)(2k+2)\frac{(x-\alpha)^{k-1}}{x^{2k+3}}\right]$$

hence, $|f''(x)| \leq O\left(\frac{k^2}{\alpha^k}\right)\frac{(x-\alpha)^{k-3}}{x^{2k+1}}$. We define $g(x) = \frac{(x-\alpha)^{k-3}}{x^{2k+1}}$ and we find that $g'(x) = 0 \Leftrightarrow x = \alpha\frac{2k+1}{k+4}$, thus

$$|g|_\infty = \frac{1}{\alpha^{k+2}}\left(\frac{k-3}{k+4}\right)^{k-3}\left(\frac{k+4}{2k+1}\right)^{2k+1}.$$

Recall that $\epsilon_l(\omega,\Gamma) = \Gamma\omega^4 \left|f''\right|_\infty$. Using the fact that $\lim_{k\to\infty}(1+\Theta(1/k))^k = \Theta(1)$, we get

$$\begin{aligned}|g|_\infty &= \frac{1}{\alpha^{k+2}}\left(\frac{k-3}{k+4}\right)^{k-3}\left(\frac{k+4}{2k+1}\right)^{2k+1} \\ &\leq \frac{1}{\alpha^{k+2}}\frac{1}{2^{2k+1}}\left(1+\frac{7}{2k+1}\right)^{k} \leq O\Big((4\alpha)^{-k}\Big)\,.\end{aligned}$$

From there, we have $|f''|_\infty \leq O\Big(\frac{k^2}{(2\alpha)^{2k}}\Big)$ and in turn

$$\epsilon_l(k^{-4},2k^8) \leq 2k^{-8}\left|f''\right|_\infty \leq O\Big(k^{-6}(2\alpha)^{-2k}\Big)\,. \tag{23}$$

Using a similar technique, we also get

$$\epsilon_r(k^{-4},2k^8) \leq O\Big(k^{-6}(2\alpha)^{-2k}\Big)\,. \tag{24}$$

The last term to bound is $E(\omega) = E(k^{-4}) = \frac{\left(1+2k^{-3}\right)^{2k+1}}{\left(1-4k^{-3}\right)^{4k+1}}$. Since $\left(1+O(k^{-3})\right)^k = 1+O(k^{-2})$, we get

$$E(k^{-4}) = 1+O\big(k^{-2}\big)\,. \tag{25}$$

To conclude, in Inequality (18), we replace all the terms by their asymptotic equivalent computed in Equations (22), (23), (24), and (25):

$$\frac{B(k+1,k)}{\alpha^{2k+2}} > \frac{B(k+2,k)}{\alpha^{2k+3}} + O\left(\frac{1}{k^2}\right)\frac{B(k+2,k)}{\alpha^{2k+3}} + O\left(\frac{k^{-6}}{(2\alpha)^{2k}}\right).$$

This means that Inequality (18) holds for

$$\alpha > \frac{k+1}{2k+1} + O\left(\frac{1}{k^2}\right) + O\left(\frac{1}{k^6 2^{2k} B(k+1,k)}\right) = \frac{1}{2} + O\left(\frac{1}{k}\right).$$

We used Sterling's formula to show that the last term is $o(\frac{1}{k})$, since we have $\frac{1}{B(k+1,k)} = O\Big(\frac{\sqrt{k}(2k/e)^{2k}}{(k/e)^{2k}}\Big) = O(\sqrt{k}2^{2k})$. □

6.2 Bounds on the resources of the protocol

We are now ready to quantify the necessary resources for the protocol.

Theorem 6 *For all $\varepsilon > 0$, there exists a quantum weak coin flipping protocol with cheating probabilities $P_A^* = P_B^* < 1/2+\varepsilon$ with $O(\log\frac{1}{\varepsilon})$ qubits and $\left(\frac{1}{\varepsilon}\right)^{O(\frac{1}{\varepsilon})}$ messages.*

Proof. We consider the above TIPG with $k = \lceil\frac{c}{\varepsilon}\rceil$, $\omega = k^{-4}$, $\Gamma = 2k^8$ and $\alpha = \frac{1}{2}+\frac{c}{k} = \frac{1}{2}+\varepsilon$ where c is a constant such that Lemma 44 holds with this α for each k.

Step 1: Number of qubits. It is clear from the different steps of the construction that the number of qubits needed is equal to the logarithm of the number of different points in the point game. The number of points are no more than $O(\Gamma k) = O(k^9)$, which implies that the number of qubits is $O(\log\frac{1}{\varepsilon})$.

Step 2: Number of rounds. By Corollary 40, we need to to upper-bound $\|h\|$ where

$$\|h\| = 1/2 + \sum_{j=\zeta}^{\Gamma} \sum_{\substack{i=-k \\ i\neq 0}}^{k} \frac{C \cdot |f((j+i)\,\omega,\, j\omega)|}{((j+i)\omega)(j\omega) \prod_{\substack{l\neq i \\ l\neq 0}} \omega\,|l-i|}.$$

The other terms in the Corollary are all polynomial in k. We will do some crude approximations in the terms below, but the asymptotic behaviour is not going to change. The main property is that there are points in the ladder, for example the ones at the edges, whose weight is of the order $k^{O(k)}$.

Let us first bound C defined by $\frac{1}{2C} = \sum_{\zeta}^{\Gamma} \frac{f(0,j\omega)}{\prod \omega(j+l)}$. Since all the terms in the sum are positive, we can lower bound the sum by the term for $j = \zeta$. We have

$$\begin{aligned} f(0,\zeta\omega) &= \prod_{i=1}^{k-1}(\alpha - i\omega)(i\omega) \prod_{i=1}^{k}(\Gamma\omega + i\omega)(\Gamma\omega + i\omega - \alpha) \geq (\alpha - k\omega)^{k-1}(\omega)^{k-1}(\Gamma\omega)^{k}(\Gamma\omega - \alpha)^{k} \\ &\geq k^{\Omega(k)}, \end{aligned}$$

and the denominator by,

$$\prod_{l\neq 0}(\alpha + l\omega) \leq (\alpha + k\omega)^{2k} = 2^{-O(k)}.$$

This gives us $C \leq k^{-O(k)}$.

Now, note that the norm is given by a sum with a number of terms polynomial in k, hence it suffices to give an upper bound on the ratio

$$S = \frac{|f((j+i)\,\omega,\, j\omega)|}{((j+i)\omega)(j\omega) \prod_{\substack{l\neq i \\ l\neq 0}} \omega\,|l-i|}.$$

The numerator can be bounded by:

$$\begin{aligned} |f((j+i)\omega, j\omega)| &= \prod_{l=1}^{k-1}((j+i+l)\omega - \alpha)((j+l)\omega - \alpha) \prod_{l=1}^{k}(\Gamma\omega + (l-i-j)\omega)(\Gamma\omega + (l-j)\omega) \\ &\leq (\Gamma\omega + 2k\omega - \alpha)^{4k-2} = k^{O(k)}, \end{aligned}$$

and the denominator by,

$$((j+i)\omega)(j\omega) \prod_{\substack{l\neq i \\ l\neq 0}} \omega\,|l-i| \geq (\alpha - k\omega)\alpha\omega^{2k-1}(k!)^2 \geq k^{-\Omega(k)}.$$

Thus $S \leq k^{O(k)}$.

Hence, we have proved that $\|h\| \leq k^{O(k)}$. Using Corollary 40, we finally get that the number of rounds is upper-bounded by $\left(\frac{1}{\varepsilon}\right)^{O(\frac{1}{\varepsilon})}$. □

We see that the protocol is very efficient in the number of qubits that it uses. However, our analysis shows that the number of rounds is exponential. It could be the case that by choosing different values for ω and Γ, one can reduce the number of rounds. Nevertheless, our intuition, backed with numerical evidence, is that for this protocol one would always need an exponential number of rounds. Another way would be to try to find a more efficient way to turn a TIPG into a point game with valid transitions. Last, it remains open to find a simpler and more efficient point game that can be easily transformed into an easy-to-describe protocol.

Acknowledgments

We would like to thank Peter Høyer for useful comments on a preliminary version of the paper.

References

[ABDR04] Andris Ambainis, Harry Buhrman, Yevgenity Dodis, and Hein Rörig. Multiparty quantum coin flipping. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259. IEEE Computer Society, 2004. arXiv:quant-ph/0304112, doi:10.1109/CCC.2004.19.

[Amb04] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. *Journal of Computer and System Sciences*, 68:398–416, 2004. arXiv:quant-ph/0204022, doi:10.1016/j.jcss.2003.07.010.

[AS10] Netanel Aharon and Jonathan Silman. Quantum dice rolling: a multi-outcome generalization of quantum coin flipping. *New Journal of Physics*, 12(3):033027, 2010. arXiv:0908.1682, doi:10.1088/1367-2630/12/3/033027.

[ATSVY00] Dorit Aharonov, Ammon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. Quantum bit escrow. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 705–714. ACM, 2000. arXiv:quant-ph/0004017, doi:10.1145/335305.335404.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, page 175. IEEE Computer Society, 1984. URL: http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf.

[BCH+08] Harry Buhrman, Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo, and Stephanie Wehner. Possibility, impossibility and cheat-sensitivity of quantum bit string commitment. *Physical Review A*, 78:022316, 2008. arXiv:quant-ph/0504078, doi:10.1103/PhysRevA.78.022316.

[Bha97] Rajendra Bhatia. *Matrix analysis*, volume 169 of *Graduate texts in mathematics*. Springer-Verlag, 1997.

[Blu83] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15:23–27, 1983. URL: http://www.comp.nus.edu.sg/~hugh/presentations/cs3235/lect9/Coin_flipping.pdf, doi:10.1145/1008908.1008911.

[BV04] Stephen P. Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[Che52] Herman Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *The Annals of Mathematical Statistics*, 23(4):493–507, 1952. doi:10.1214/aoms/1177729330.

[CK09] André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *Proceeding of the 44th Annual IEEE Symposium on Foundations of Computer Science*, pages 527–533. IEEE Computer Society, 2009. arXiv:0904.1511, doi:10.1109/FOCS.2009.71.

[CK11] André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*. IEEE Computer Society, 2011. arXiv:1102.1678, doi:10.1109/FOCS.2011.42.

[Cle86] Richard Cleve. Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, STOC '86, pages 364–369. ACM, 1986. doi:10.1145/12130.12168.

[DKSW07] Giacomo Mauro D'Ariano, Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: the possible and the impossible. *Physical Review A*, 76:032328, 2007. arXiv:quant-ph/0605224, doi:10.1103/PhysRevA.76.032328.

[Gan09] Maor Ganz. Quantum leader election. 2009. arXiv:0910.4952.

[Gol09] Oded Goldreich. *Foundations of Cryptography*, volume 2: Basic Applications. Cambridge University Press, 2009.

[HK04] Lucien Hardy and Adrian Kent. Cheat sensitive quantum bit commitment. *Physical Review Letters*, 92:157901, 2004. arXiv:quant-ph/9911043, doi:10.1103/PhysRevLett.92.157901.

[Kit03] Alexei Kitaev. Quantum coin flipping. Talk at the 6th workshop on Quantum Information Processing, 2003.

[KN04] Iordanis Kerenidis and Ashwin Nayak. Weak coin flipping with small bias. *Information Processing Letters*, 89(3):131 – 135, 2004. arXiv:quant-ph/0206121, doi:10.1016/j.ipl.2003.07.007.

[KZ13] Iordanis Kerenidis and Shengyu Zhang. A quantum protocol for sampling correlated equilibria unconditionally and without a mediator. In *Theory of Quantum Computation, Communication, and Cryptography*, volume 7582 of *Lecture Notes in Computer Science*, pages 13–28. Springer Berlin Heidelberg, 2013. arXiv:1104.1770, doi:10.1007/978-3-642-35656-8_2.

[LC97] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997. arXiv:quant-ph/9603004, doi:10.1103/PhysRevLett.78.3410.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, 1997. arXiv:quant-ph/9605044, doi:10.1103/PhysRevLett.78.3414.

[Moc04] Carlos Mochon. Quantum weak coin-flipping with bias of 0.192. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 2–11. IEEE Computer Society, 2004. arXiv:quant-ph/0403193, doi:10.1109/FOCS.2004.55.

[Moc05] Carlos Mochon. Large family of quantum weak coin-flipping protocols. *Physical Review A*, 72:022341, 2005. arXiv:quant-ph/0502068, doi:10.1103/PhysRevA.72.022341.

[Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrary small bias. 2007. arXiv:0711.4114.

[NS03] Ashwin Nayak and Peter W. Shor. Bit-commitment-based quantum coin flipping. *Physical Review A*, 67:012304, 2003. arXiv:quant-ph/0206123, doi:10.1103/PhysRevA.67.012304.

[SR01] Robert W. Spekkens and Terry Rudolph. Degrees of concealments and bindingness in quantum bit commitment protocols. *Physical Review A*, 65(01):012310, 2001. arXiv:quant-ph/0106019, doi:10.1103/PhysRevA.65.012310.

[SR02] Robert W. Spekkens and Terry Rudolph. Quantum protocol for cheat-sensitive weak coin flipping. *Physical Review Letters*, 89:227901, 2002. arXiv:quant-ph/0202118, doi:10.1103/PhysRevLett.89.227901.