Theoretı̈CS

Protocols for Quantum Weak Coin Flipping

Atul Singh Arora [a,b,c,d] ✉ iD

Jérémie Roland [d] ✉ iD

Chrysoula Vlachou [e,f] ✉ iD

Stephan Weis [g] ✉ iD

a CQST, IIIT Hyderabad, Telangana, India

b QuICS, UMIACS, University of Maryland, College Park, Maryland, USA

c IQIM, CMS, Caltech, Pasadena, California, USA

d Université libre de Bruxelles, Brussels, Belgium

e Instituto de Telecomunicações, Lisbon, Portugal

f Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal

g Faculty of Electrical Engineering, Czech Technical University in Prague, Czech Republic

ABSTRACT. Weak coin flipping is an important cryptographic primitive—it is the strongest known secure two-party computation primitive that classically becomes secure only under certain assumptions (e.g. computational hardness), while quantumly there exist protocols that achieve arbitrarily close to perfect security. This breakthrough result was established by Mochon in 2007 [arXiv:0711.4114]. However, his proof relied on the existence of certain unitary operators which was established by a non-constructive argument. Consequently, explicit protocols have remained elusive. In this work, we give exact constructions of related unitary operators. These, together with a new formalism, yield a family of protocols approaching perfect security thereby also simplifying Mochon's proof of existence. We illustrate the construction of explicit weak coin flipping protocols by considering concrete examples (from the aforementioned family of protocols) that are more secure than all previously known protocols.

1. Introduction

The problem we study in this paper is easy to state. Suppose there are two parties, conventionally called Alice and Bob, who are placed in physically remote locations and can communicate with each other using a communication channel. They wish to exchange messages over this channel in order to agree on a random bit, while having *a priori* known opposite preferred outcomes. This is easy to do—Alice flips a coin and sends a message with the outcome to Bob. However, this requires Bob to trust Alice. Can Bob modify the scheme to be sure that Alice did not cheat? More generally, can one construct a protocol, which involves an exchange of messages over a communication channel, to decide on a random bit while ensuring that an honest party, i.e. one that follows the protocol, cannot be deceived? It turns out that if one communicates over a classical communication channel,[1] then a cheating party can always force their desired outcome on the honest party (unless one makes further assumptions, such as computational hardness). On the other hand, if Alice and Bob use a quantum communication channel, then protocols solving this problem up to vanishing errors have been shown to *exist* [32]. This seminal result was proved in 2007. However, there is a non-constructive part in its analysis, which means that while we know such protocols exist, the protocols themselves remain unknown. In this paper, we build upon the previous pioneering works to construct protocols for *quantum weak coin flipping*, as this problem is referred to in the literature.

      The coin flipping problem was introduced by Blum in 1983 [13]. It has since occupied an interesting place in the overall landscape of cryptography. To overcome the severe limitations of key distribution, public key cryptography was invented [20, 29]. In 1994 it was shown that the widely used—even today—public key cryptosystem RSA [36] can be broken using a quantum computer [37]. Interestingly, a decade earlier, a method for performing key distribution using quantum channels [11] was proposed whose security, in principle, relied only on the validity of the laws of physics. It was thus thought that quantum mechanics could also revolutionise *secure two-party computation*. This is another branch of cryptography comprising protocols in which two distrustful parties wish to jointly compute a function on their inputs without having to reveal these inputs to each other. Success here, was marred by a cascade of impossibility results. In a central result of (classical) cryptography, it was shown that a primitive called *oblivious transfer* is universal for secure two-party computation [26]. However, there exists no (classical) protocol that offers perfect security for oblivious transfer without relying on further assumptions, such as computational hardness—classical secure two-party computation with perfect security is thus impossible [19]. In fact, it was shown that even if one allows quantum communication, oblivious transfer cannot be implemented with perfect security [28, 18], extinguishing any lingering hope that quantum mechanics could serve as a panacea for

---

1   as opposed to a quantum communication channel

cryptography. *Bit commitment*, a secure two-party computation primitive weaker than oblivious transfer was subsequently targeted, but it too turned out to be impossible—in the same sense—even in the quantum setting [16]. This brings us to *coin flipping*, an even weaker secure two-party computation primitive, which comes in two variants: *strong* and *weak* coin flipping. In a coin flipping protocol the two distrustful parties need to establish a shared random bit. For strong coin flipping[2] the preferences of the parties are unknown to each other, whereas in weak coin flipping, the parties have a priori known opposite preferences (as stated earlier). While strong coin flipping suffered the same fate as that of oblivious transfer and bit commitment [17], weak coin flipping was poised for fame—it is the strongest known primitive in the two-party setting which admits no secure classical protocol, but can be implemented over a quantum channel with near perfect security [32].

More precisely, in a quantum strong coin flipping protocol a dishonest party can successfully cheat with probability at least $\frac{1}{\sqrt{2}}$ [27], and the best known explicit protocol has a cheating probability of $\frac{1}{2} + \frac{1}{4}$ [4]. As for weak coin flipping, the existence of protocols with arbitrarily-close-to-perfect security was proved non-constructively, by elaborate successive reductions of the problem based on the formalism introduced earlier by Kitaev for the study of strong coin flipping [27]. Consequently, the structure of the protocols whose existence is proved was lost. A systematic verification led to a simplified proof of existence by Aharonov, Chailloux, Ganz, Kerenidis and Magnin [3]. Yet, over a decade later, an explicit, nearly perfectly secure weak coin flipping protocol was missing, despite various approaches ranging from the distillation of a protocol using the proof of existence to numerical search [34, 35].[3] While an explicit weak coin flipping protocol has remained elusive, several connections have been discovered. In particular, (nearly) perfect weak coin flipping provides, via black-box reductions, (nearly) optimal protocols for strong coin flipping [17], bit commitment [16] and a variant of oblivious transfer [15]. It is also used to implement other cryptographic tasks such as leader election [21] and dice rolling [2].

The most significant advance in the study of weak coin flipping (WCF) was the invention of the so-called point games, attributed to Kitaev by Mochon [32]. They introduced three equivalent formalisms that can be used to describe WCF protocols and their security properties: (i) Explicit protocols given by pairs of dual semi-definite programs (SDPs), (ii) Time Dependent Point Games (TDPGs) and (iii) Time Independent Point Games (TIPGs). The existence of quantum WCF protocols with almost perfect security was established using TIPGs [32]. However, the proposal of explicit protocols was hindered by the fact that no constructive method was given for

---

2   "Strong coin flipping" is often referred to simply as "coin flipping" in the literature.

3   The known proof of existence for WCF implies that an exhaustive search, given enough time, will find an explicit WCF protocol. However, the search space is so large that this approach seems infeasible and has, indeed, been unsuccessful so far.

obtaining a protocol from a TDPG (even though, as we said, protocols and TDPG are equivalent formalisms).

In this work, we start by constructing a new framework that allows us to convert point games into protocols, granted that we can find unitaries satisfying certain constraints. We use perturbative methods in conjunction with this framework to obtain a protocol with cheating probability $\frac{1}{2} + \frac{1}{10}$, improving the former best known protocol which has cheating probability $\frac{1}{2} + \frac{1}{6}$ [31].[4] We then introduce a more systematic method for converting the point games used by Mochon (including the ones approaching perfect security) into explicit unitaries, which, in turn, can be readily converted into explicit WCF protocols. Our approach is also simpler, in at least three ways. First, prior works relied on conic duality arguments to show the equivalence between the various formalisms which was crucial to the proof of existence. Since we give exact constructions directly in the SDP formalism, this conic duality argument can be circumvented. Second, even though we do not use this equivalence for our main result, our approach is also equivalent to the various formalisms as the conic duality argument continues to hold in our approach—and is arguably easier to apply as it avoids the subtleties involving closures of cones (as detailed in Section 4.2 and Lemma 4.5). Finally, our approach produces protocols where the message register can be discarded/reset after each round, unlike prior works where the message register had to be held coherent through all rounds of the protocol (see before Section 4.1).

2.   Technical Overview

Below, we briefly introduce the various aforementioned formalisms. We need them in Section 2.2 where we informally describe our contributions. Later, in Section 3, we present these formalisms in more detail, as we subsequently build upon them.

Let us start with two elementary remarks about WCF. First, without loss of generality,[5] one can say that, if the (bit-valued) outcome of a WCF protocol is 0 it means that Alice won, while Bob wins on outcome 1. Second, there are four situations which can arise in a WCF scenario, of which only three are relevant to our discussion. Begin with the situation where both Alice and Bob are honest (denoted by HH), i.e. they both follow the protocol. We want the protocol to be such that both Alice and Bob (a) win with equal probability and (b) are in agreement with each other. In the situation where Alice is honest and Bob is cheating (denoted by HC), the protocol must protect Alice from a cheating Bob, who tries to convince her that he has won. His probability of succeeding by using his best cheating strategy is denoted by P_B^*, where the subscript denotes the cheating party. The situation where Bob is honest and Alice is cheating (denoted by CH) naturally points us to the corresponding definition of P_A^*. We do not study the CC case, as neither party follows the prescribed protocol.

---

4   Strictly speaking, these are families of protocols whose cheating probability approaches the said value asymptotically.

5   Since in a WCF protocol, the parties have opposite known preferences, this is just a matter of labeling.

As an illustration, recall the naïve (trivially insecure) WCF protocol where Alice flips a coin and reveals the outcome to Bob over the telephone. A cheating Alice can simply lie and always win against an honest Bob, viz. $P_A^* = 1$. On the other hand, a cheating Bob cannot do anything to convince Alice that he has won, unless it happens by random chance on the coin flip. This corresponds to $P_B^* = \frac{1}{2}$. We say that a protocol has *bias* ϵ if neither party can force their preferred outcome with probability greater than $1/2 + \epsilon$, for $\epsilon \geq 0$. For the aforementioned naïve protocol, the bias is $\epsilon = \max[P_A^*, P_B^*] - \frac{1}{2}$ which amounts to $\epsilon = \frac{1}{2}$ (the worst possible). Evidently, protocols that protect one party can be trivially constructed. The real challenge is constructing protocols where neither party is able to cheat against an honest party.

2.1 The three formalisms

Given a WCF protocol, it is not a priori clear how the maximum success probability of a cheating party, $P_{A/B}^*$, should be computed as the strategy space can be dauntingly large. It turns out that all quantum WCF protocols can be defined using the exchange of a (quantum) message register interleaved with the parties applying the unitaries U_i locally (see Figure 1) until a final measurement—say Π_A denoting Alice won and Π_B denoting Bob won—is made in the end. Computing P_A^* in this case reduces to a semi-definite program (SDP) in ρ (where ρ is the state held
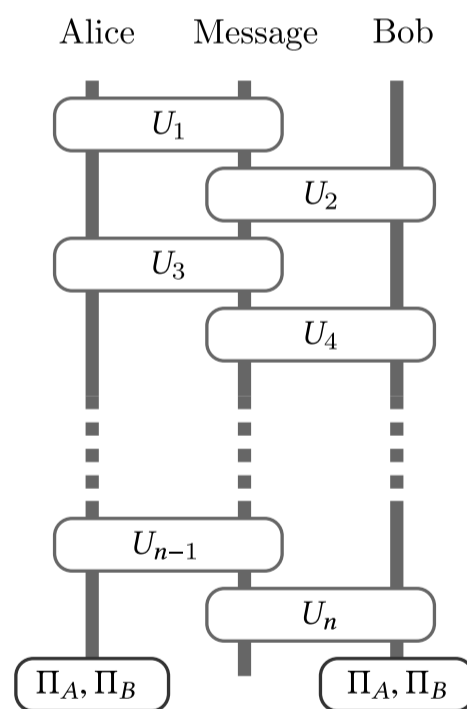

Figure 1. General structure of a WCF protocol.

by the honest party just before the measurement): maximise $P_A^* = \text{tr}(\Pi_A \rho)$ given the constraint that the honest party (Bob in this case) follows the protocol. Similarly for computing P_B^* we can define another SDP. Using SDP duality one can turn this maximisation problem over cheating strategies into a minimisation problem over dual variables $Z_{A/B}$. Any dual feasible assignment

(i.e. one that satisfies the constraints "dual to" those of the original SDP) then provides an upper bound on the cheating probabilities $P^*_{A/B}$. Handling SDPs is, in general, straightforward, but in this case, there are two SDPs, and we must optimise both simultaneously.[6] Note that we assumed that the protocol is known and we are trying to bound P^*_A and P^*_B. However, our goal is to find good protocols. Therefore, we would like a formalism which allows us to do both, construct protocols *and* find the associated P^*_A and P^*_B. Kitaev and Mochon, gave exactly such a formalism.

They converted this problem about matrices (Z, ρ and U) into a problem about points on a plane, and Mochon called it Kitaev's "Time Dependent Point Game formalism" (TDPG). Therein, we are concerned with a sequence of frames (also referred to as configurations). Each frame is a finite collection of points in the positive quadrant of the xy-plane with probability weights assigned to them. This sequence must start with a fixed frame and end with a frame that has only one point. The fixed starting frame consists of two points at $(0, 1)$ and $(1, 0)$ with equal weights $1/2$. The end frame must be a single point, say at (β, α), with weight 1. The objective of the protocol designer is to get this end point as close to the point $(\frac{1}{2}, \frac{1}{2})$ as possible by transitioning through intermediate frames (see Figure 2) following certain rules.
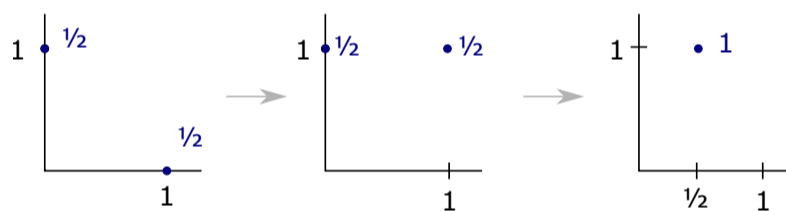

Figure 2. Point game.

The main theorem about this formalism, roughly stated, asserts that if one abides by these rules, then corresponding to every such sequence of frames, there exists a WCF protocol with $P^*_A = \alpha$, $P^*_B = \beta$.

Let us now describe these rules. Consider a given frame and focus on a set of points that fall along a vertical (or horizontal) line. Let the y (or x) coordinate of the ith point be given by z_{g_i} and its weight by p_{g_i}, and let z_{h_i} and p_{h_i} denote the corresponding quantities for the points in the subsequent frame. Then, the following conditions must hold:

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

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

From one frame to the next, we can either make a horizontal or a vertical transition. By combining these sequentially we can obtain the desired form of the final frame, i.e. a single point. The points in the frames and the rules of the transitions arise from the variables $Z_{A/B}$ of the dual SDP and their constraints, respectively. Just as the state ρ evolves through the protocol, so do the dual variables $Z_{A/B}$. The points and their weights in the TDPG are exactly the eigenvalue pairs of $Z_{A/B}$ with the probability weight assigned to them by the honest state $|\psi\rangle$ at a given step in the protocol. Given an explicit WCF protocol and a feasible assignment for the dual variables witnessing a given bias, it is straightforward to construct the TDPG. However, going backwards, constructing the WCF dual from a TDPG is non-trivial and no general construction is known.

As shall become evident shortly, it is useful to encode the points on a line and their weights into a function from the interval $[0, \infty)$ to itself. Let

$$[\![a]\!] (z) = \delta_{a,z}, \tag{2}$$

i.e. $[\![a]\!] (z)$ is zero when $z \neq a$ and one when $z = a$. The *transition* from a given frame to the next is written as $\sum_i p_{g_i} [\![z_{g_i}]\!] \rightarrow \sum_i p_{h_i} [\![z_{h_i}]\!]$. The corresponding *function* is written as $t = \sum_i p_{h_i} [\![z_{h_i}]\!] - \sum_i p_{g_i} [\![z_{g_i}]\!]$. If the transition (function) satisfies the conditions (1) and (2) above, it is termed as a *valid transition (function)* (see Proposition 3.14). If we restrict ourselves to transitions involving only one initial and one final point, i.e. $[\![z_g]\!] \rightarrow [\![z_h]\!]$, the second condition reduces to $z_g \leq z_h$. This is called a *raise*, and it means that we can increase (but not decrease) the coordinate of a *single* point. What about going from one initial point to many final points, i.e. $[\![z_g]\!] \rightarrow \sum_i p_{h_i} [\![z_{h_i}]\!]$? Note that the points before and after must lie along either a horizontal or a vertical line. The second condition in this case becomes $1/z_g \geq \langle 1/z_h \rangle$, which means that the harmonic mean of the final points must be greater than or equal to that of the initial point, where $\langle f(z_h) \rangle := \left(\sum_i f(z_{h_i}) p_{h_i} \right) / \left(\sum_j p_{h_j} \right)$. This is called a *split*. Finally, we can ask what happens upon merging many points into a single point, i.e. $\sum_i p_{g_i} [\![z_{g_i}]\!] \rightarrow [\![z_h]\!]$. The second condition becomes $\langle z_g \rangle \leq z_h$, which means that the final position must not be smaller than the average initial position. This is called a *merge*. While these three valid transitions do not exhaust the set of possible valid moves, they are enough to construct games approaching bias 1/6.

Let us consider a simple game as an example (see Figure 2). We start with the initial frame and raise the point $(1, 0)$ vertically to $(1, 1)$; this is a raise, an allowed move. Next we merge the points $(0, 1)$ and $(1, 1)$ using a horizontal merge. The *x*-coordinate of the resulting point can at best be $\frac{1}{2}.0 + \frac{1}{2}.1 = \frac{1}{2}$ where we used the fact that both points have weight 1/2. Thus, we end up with a single point having all the weight at $(\frac{1}{2}, 1)$. This formalism tells us that there must exist a protocol which yields $P_A^* = 1$ while $P_B^* = \frac{1}{2}$, which is exactly the naïve telephone protocol that we presented earlier. It is a neat consistency check but it yields the worst possible bias. This is because we did not use the split move. If we use a split once, we can, by appropriately matching

the weights, already obtain a game with $P_A^* = P_B^* = \frac{1}{\sqrt{2}}$. Various protocols corresponding to this bias were found [39, 33, 25] before the point game formalism was known. In fact, this bias, $\epsilon = \frac{1}{\sqrt{2}} - \frac{1}{2}$, is exactly the lower bound for the bias of *strong* coin flipping protocols. It was an exciting time—we imagine—as the technique used to obtain the bound for strong coin flipping fails to apply to WCF. The matter was not resolved for some time, and this protocol remained the best known implementation of WCF. Then, in 2005, Mochon showed that using multiple splits at the beginning followed by a raise, and thereafter simply using merges, one can obtain a game with bias approaching 1/6 [31]. Obtaining lower biases, however, is not a straightforward extension of the above, and we need other moves which cannot be decomposed into the three basic ones: splits, merges and raises.

2.2　Contributions

2.2.1　TEF and bias 1/10 protocol

In Section 4, we provide a framework for converting a TDPG into an explicit WCF protocol. We start by defining a "canonical form" for any given frame of a TDPG, which allows us to write the WCF dual variables, Zs, and the honest state $|\psi\rangle$ associated with each frame of the TDPG. We then define a sequence of quantum operations, unitaries and projections, which describe how Alice and Bob transition from the initial to the final frame. It turns out that there is only one non-trivial quantum operation, U, in the sequence. Using the SDP formalism we write the constraints at each step of the sequence on the Zs and show that they are indeed satisfied. The aforementioned constraints can be summarised as in Theorem 2.1 below. In Section 4, one can find the full version, Theorem 4.3, together with its proof and a detailed description of the framework. Notice that compared to Mochon's Lemma 18, the key difference in our approach is the introduction of projectors and the treatment of message registers. We defer the details to Section 4.

THEOREM 2.1 (TEF constraint (simplified)). *If a unitary matrix U acting on the space $span\{|g_1\rangle, |g_2\rangle \ldots, |h_1\rangle, |h_2\rangle \ldots\}$ satisfying the constraints*[7]

$$U |v\rangle = |w\rangle \quad and \quad \sum_i x_{h_i} |h_i\rangle \langle h_i| - \sum_i x_{g_i} E_h U |g_i\rangle \langle g_i| U^\dagger E_h \geq 0, \tag{3}$$

can be found for every transition (see Definition 3.7 and Definition 3.8) of a TDPG, then an explicit protocol with the corresponding bias can be obtained using the TDPG–to–Explicit–protocol Framework (TEF). Here, $\{\{|g_i\rangle\}, \{|h_i\rangle\}\}$ are orthonormal vectors. If the transition is horizontal, then

— *the initial points have x_{g_i} as their x-coordinate and p_{g_i} as their corresponding probability weight,*

7　　We use $A \geq B$ to mean that $A - B$ has non-negative eigenvalues; we implicitly assume that A and B are Hermitian.

— the final points have x_{h_i} as their x-coordinate and p_{h_i} as their corresponding probability weight,

— E_h is a projection onto the span $\{|h_i\rangle\}$ space,

— $|v\rangle = \sum_i \sqrt{p_{g_i}} |g_i\rangle / \sqrt{\sum p_{g_i}}$, $|w\rangle = \sum_i \sqrt{p_{h_i}} |h_i\rangle / \sqrt{\sum p_{h_i}}$.

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

The TDPG already specifies the coordinates x_{h_i}, x_{g_i} and the probabilities p_{h_i}, p_{g_i} satisfying the scalar condition Equation (1), therefore our task reduces to finding the correct U which satisfies the matrix constraints Equation (3). Given such a unitary U we show in detail how we can progressively build the sequence of unitaries corresponding to the complete WCF protocol. In fact, we need to reverse the order of the operations in the sequence we get in order to obtain the final protocol. We continue by introducing what we call the *blinkered unitary*, that satisfies the required constraints (as in Equation (3)) for split and merge moves. In particular, any valid transition from m initial to n final points that can be implemented by means of the blinkered unitary, can be seen as a combination of an $m \to 1$ merge and an $1 \to n$ split (see Section 4.3 and Appendix B). With these the former best known explicit protocol with bias 1/6 [31] can already be derived from its TDPG. We finally study the family of TDPGs with bias 1/10 and isolate the precise moves required to implement it. These cannot be produced by a combination of merges and splits, therefore, we need to go beyond blinkered unitaries. We give analytic expressions for the required unitaries and show that they satisfy the corresponding constraints. This allows us to convert Mochon's family of games with bias 1/10 into explicit protocols, thus breaking the bias 1/6 barrier. However, we essentially guessed the form that the blinkered unitary and the unitaries of the 1/10 game should have in these cases, and then showed that they indeed satisfy the required constraints. Games achieving lower biases, though, correspond to larger unitary matrices, therefore this approach becomes untenable. We overcome this issue in Section 5, where we find a way to systematically construct the unitaries for the whole family of Mochon's games achieving bias $\epsilon(k) = 1/(4k+2)$ for arbitrary integers $k > 0$.

2.2.2   Exact Unitaries for approaching zero bias using Mochon's assignments

As we saw, TEF allows us to convert any TDPG into an explicit protocol, granted that the unitaries satisfying Equation (3) can be found corresponding to each valid transition used in the game (see Theorem 2.1). Using Kitaev's and Mochon's formalism [32], we have that the following—an even weaker requirement—is enough (see Section 5.1): Suppose that a valid function (see the discussion after Equation (1)), t, can be written as a sum of valid functions. Then, in order to obtain the *effective solution* for t (see Definition 5.3), it suffices to find unitaries corresponding to the valid functions appearing in the sum. We consider the class of valid functions that Mochon uses in his family of point games approaching bias $\epsilon(k) = \frac{1}{4k+2}$ for an arbitrary integer $k > 0$.

These are of the form (see Definition 5.1)

$$t = \sum_{i=1}^{n} \frac{-f(x_i)}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!] \, ,$$

where $0 \leq x_1 < x_2 \cdots < x_n \in \mathbb{R}$, $f(x)$ is a polynomial,[8] and the notation is as in Equation (2). We refer to these as *f-assignments* and in particular, when f is a monomial, we call them *monomial assignments*. We observe that the f-assignments can be expressed as a sum of monomial assignments, and we give formulas for the unitaries corresponding to these monomial assignments. There are four types of monomial assignments—which we call balanced or unbalanced (depending on whether the number of points with negative weights in the point game is equal to the number of points with positive weight or not) and aligned or misaligned (depending on whether the power of the polynomial $f(x)$ is even or odd). The formulas for their *solutions* (see Definition 5.3) and their proofs of correctness comprise most of Section 5 whose central result is summarised in the following theorem.

THEOREM 2.2 (informal—we suppressed some constraints on f for brevity.). *Let t be an f-assignment (see Definition 5.1). Then, t can be expressed as $t = \sum_i \alpha_i t'_i$ where $\alpha_i > 0$ and t'_i are monomial assignments (see Definition 5.1). Each t'_i admits a solution (see Definition 5.3) given in either Proposition 5.9, Proposition 5.10, Proposition 5.11 or Proposition 5.12, depending on the form of t'_i.*

In Section 5.5 we illustrate, as an example, the construction of a WCF protocol with bias 1/14 from the corresponding point game by means of the TEF and the analytical solutions to the monomial assignments.

Having found these unitaries, we have effectively solved our problem, since TEF allows the conversion of point games—including the ones with arbitrarily small bias—into WCF protocols with the respective bias as illustrated in Figure 3 below.

2.3   Relation to existing pre-prints

This work is a self-contained and (presently) the most *concise* version of the main result—construction of WCF protocols with vanishing bias—in `arXiv:1811.02984` [8] (presented at STOC '19 [9]) and `arXiv:1911.13283v2` [6] (presented at SODA '21 [5]).
On the other hand, the `Cryptology ePrint 2022/1101` [7] is a self-contained, *comprehensive* version that contains all the results in `arXiv:1811.02984` [8] and `arXiv:1911.13283v1` [5] and v2 (v1 gave a geometric construction while v2 was algebraic).

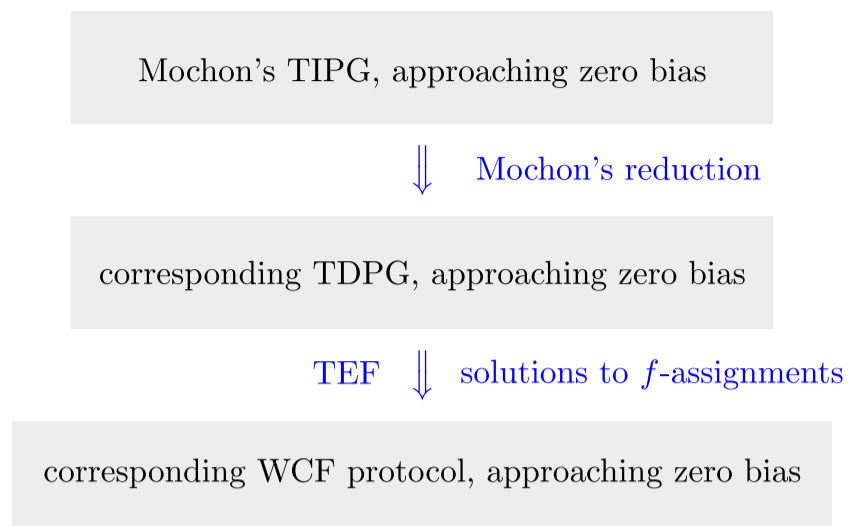8   with some restrictions which we suppress for brevity

Figure 3. Mochon constructed a Time Independent Point Game approaching zero bias which, in combination with prior results and the ones in this manuscript, results in the corresponding WCF protocol approaching zero bias.

3. Preliminaries: Existence of Almost Perfect Quantum WCF Protocols

The contents of this section are based on two works: the first is by Mochon [32]—part of which is attributed to Kitaev—and the second is by Aharonov, Chailloux, Ganz, Kerenidis and Magnin [3], who simplified and verified the former. Here, we only state specific notation and statements (without proofs) from these works that we need to present our work.

3.1 WCF protocol as an SDP and its dual

Any WCF protocol can be expressed in the following general form (see [4] and page 9 of [32]):

DEFINITION 3.1 (WCF protocol with bias ϵ). For n even, an n-message WCF protocol between two parties, Alice and Bob, is described by:

— Three Hilbert spaces: A and B corresponding to Alice's and Bob's private work-spaces (Bob does not have any access to A and, similarly, Alice to B) and a message space M.

— An initial product state $|\psi_0\rangle = |\psi_{A,0}\rangle \otimes |\psi_{M,0}\rangle \otimes |\psi_{B,0}\rangle \in A \otimes M \otimes B$.

— A set of n unitaries $\{U_1, \ldots U_n\}$ acting on $A \otimes M \otimes B$ with $U_i = U_{A,i} \otimes \mathbb{I}_B$ for i odd and $U_i = \mathbb{I}_A \otimes U_{B,i}$ for i even.

— A set of honest states $\{|\psi_i\rangle : i \in [n]\}$ defined as $|\psi_i\rangle = U_i U_{i-1} \ldots U_1 |\psi_0\rangle$.

— A set of n projectors $\{E_1, \ldots E_n\}$ acting on $A \otimes M \otimes B$ with $E_i = E_{A,i} \otimes \mathbb{I}_B$ for i odd, and $E_i = \mathbb{I}_A \otimes E_{B,i}$ for i even, such that $E_i |\psi_i\rangle = |\psi_i\rangle$.

— Two positive operator valued measures (POVMs) $\{\Pi_A^{(0)}, \Pi_A^{(1)}\}$ acting on A and $\{\Pi_B^{(0)}, \Pi_B^{(1)}\}$ acting on B.

The WCF protocol proceeds as follows:

— In the beginning, Alice holds $|\psi_{A,0}\rangle |\psi_{M,0}\rangle$ and Bob $|\psi_{B,0}\rangle$.

— 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, she sends the message qubits to Bob; on the second outcome, she ends the protocol by outputting "0", i.e, she declares herself the 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, he sends the message qubits to Alice; on the second outcome, he ends the protocol by outputting "1", i.e., he declares himself the winner.

    — 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 parties are honest, their outcomes are always the same:
$$\Pi_A^{(0)} \otimes \mathbb{I}_M \otimes \Pi_B^{(1)} |\psi_n\rangle = \Pi_A^{(1)} \otimes \mathbb{I}_M \otimes \Pi_B^{(0)} |\psi_n\rangle = 0.$$

— *Balanced:* When both parties are honest, they win with probability $1/2$:
$$P_A = \left|\Pi_A^{(0)} \otimes \mathbb{I}_M \otimes \Pi_B^{(0)} |\psi_n\rangle\right|^2 = \tfrac{1}{2} \text{ and } P_B = \left|\Pi_A^{(1)} \otimes \mathbb{I}_M \otimes \Pi_B^{(1)} |\psi_n\rangle\right|^2 = \tfrac{1}{2}.$$

— *ϵ-biased:* When Alice is honest, the probability that both parties agree on Bob winning is $P_B^* \leq \tfrac{1}{2} + \epsilon$. Conversely, when Bob is honest, the probability that both parties agree on Alice winning is $P_A^* \leq \tfrac{1}{2} + \epsilon$.

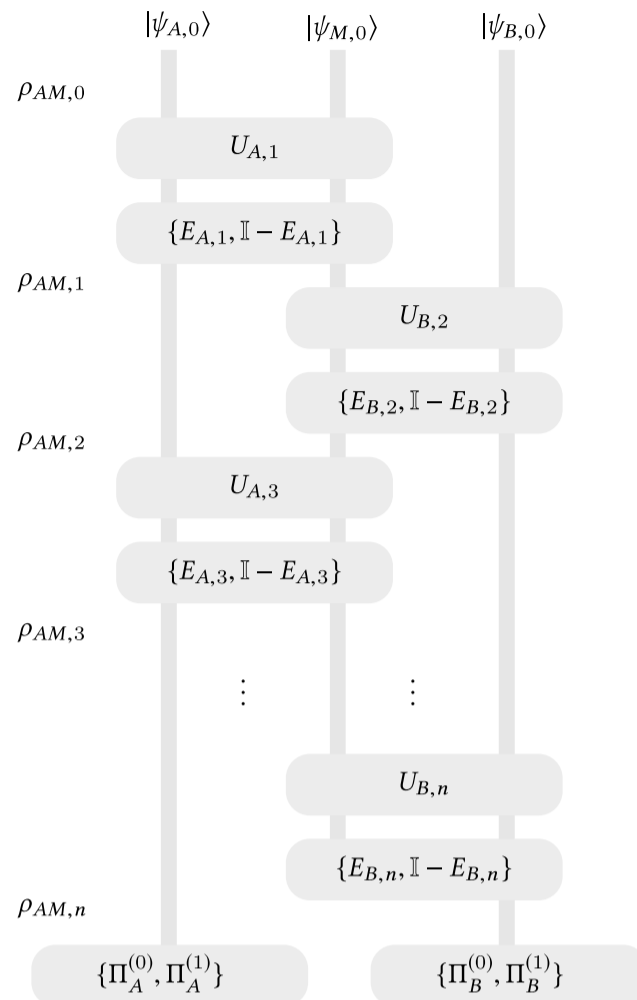For a depiction of the protocol see Figure 4.

Figure 4. Every quantum WCF protocol can be cast into this general form.

To define the bias of the protocol, we need to know P_A^* and P_B^* corresponding to the best possible cheating strategy of the opponent. This is formalised by the following (primal) semi-definite program:

THEOREM 3.2 (Primal). *Using the notation in Definition 3.1, it holds that*

$P_B^* = \max Tr((\Pi_A^{(1)} \otimes \mathbb{I}_M)\rho_{AM,n})$ *over all $\rho_{AM,i}$ satisfying the constraints*

— $Tr_M(\rho_{AM,0}) = Tr_{MB}(|\psi_0\rangle\langle\psi_0|) = |\psi_{A,0}\rangle\langle\psi_{A,0}|,$

— *for i odd, $Tr_M(\rho_{AM,i}) = Tr_M(E_i U_i \rho_{AM,i-1} U_i^\dagger E_i)$, and*

— *for i even, $Tr_M(\rho_{AM,i}) = Tr_M(\rho_{AM,i-1})$.*

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

— $Tr_M(\rho_{MB,0}) = Tr_{AM}(|\psi_0\rangle\langle\psi_0|) = |\psi_{B,0}\rangle\langle\psi_{B,0}|,$

— *for i even, $Tr_M(\rho_{MB,i}) = Tr_M(E_i U_i \rho_{MB,i-1} U_i^\dagger E_i)$, and*

— *for i odd, $Tr_M(\rho_{MB,i}) = Tr_M(\rho_{MB,i-1})$.*

REMARK 3.3. In fact, one can restrict to unitaries without loss of generality (see page 9 of [32]) by simulating the projections as coherent measurements and absorbing them into the final measurement. Generality is not lost because (a) the projections can only improve the bias and (b) a protocol with projections can be converted into one without projections. The use of

projectors, though, simplifies the proofs, as we will see later. For instance, One could have, in addition to the measurement $\{E_i, \mathbb{I} - E_i\}$, introduced a similar measurement, say $\{F_i, \mathbb{I} - F_i\}$, before the unitary. This would yield $\operatorname{tr}_M(\rho_{AM,i}) = \operatorname{tr}_M(E_i U_i F_i \rho_{AM,i-1} F_i U_i^\dagger E_i)$ for the SDP of P_B^*.

Notice that P_B^* depends on Alice's actions specified in the protocol—as we optimise over all possible actions of Bob—and thus involves variables such as $\rho_{AM,i}$ and $U_{A,i}$. Analogously, P_A^* depends on Bob's actions.

A feasible solution to an optimisation problem is one that satisfies the constraints but is not necessarily optimal (viz. it does not necessarily achieve the highest/lowest value). Clearly, a feasible solution to the primal problems only yields a lower bound on P_A^* and P_B^*. Using standard arguments, it is easily seen that feasible solutions to the dual problems (described below) yield *upper* bounds on P_A^* and P_B^*. In fact, in our case, it has been shown that *strong duality* holds which means that the optimal values of the dual problems yield P_A^* and P_B^* exactly (and not just lower bounds). Physically, this entails that there exist cheating strategies corresponding to the optimal values of the dual problems.

THEOREM 3.4 (Dual). *Using the notation in Definition 3.1, it holds that*
$P_B^* = \min Tr(Z_{A,0} |\psi_{A,0}\rangle \langle \psi_{A,0}|)$ *over all $Z_{A,i}$ satisfying the constraints*

  1. $\forall i, Z_{A,i} \geq 0$,
  2. For i odd, $Z_{A,i-1} \otimes \mathbb{I}_M \geq U_{A,i}^\dagger E_{A,i}(Z_{A,i} \otimes \mathbb{I}_M) E_{A,i} U_{A,i}$,
  3. For i even, $Z_{A,i-1} = Z_{A,i}$, and
  4. $Z_{A,n} = \Pi_A^{(1)}$.

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

  1. $\forall i, Z_{B,i} \geq 0$,
  2. For i even, $\mathbb{I}_M \otimes Z_{B,i-1} \geq U_{B,i}^\dagger E_{B,i}(\mathbb{I}_M \otimes Z_{B,i}) E_{B,i} U_{B,i}$,
  3. For i odd, $Z_{B,i-1} = Z_{B,i}$, and
  4. $Z_{B,n} = \Pi_B^{(0)}$.

REMARK 3.5. As in Remark 3.3, we note that the dual SDP corresponding to P_B^* would have yielded the constraint

$$Z_{A,i-1} \otimes \mathbb{I}_M \geq F_{A,i} U_{A,i}^\dagger E_{A,i} \left(Z_{A,i} \otimes \mathbb{I}_M \right) E_{A,i} U_{A,i} F_{A,i} \qquad \text{for } i \text{ odd.}$$

Similarly for P_A^* and even i. Here, $F_{A,i}$ and $F_{B,i}$ are the same as F_i in Remark 3.3 for odd and even i respectively, with Alice and Bob explicitly labelled.

Below, we formally define Time Dependent Point Games (TDPGs) which were briefly described earlier in Section 1. In fact, we define two variants—TDPGs with EBM functions and those with valid functions.

3.2   TDPGs with EBM transitions/functions

Evidently, every protocol admits infinitely many representations as, in particular, there is freedom in the choice of basis. It is desirable to remove this redundancy to analyse the WCF problem. Kitaev's solution was to define *Time Dependent Point Games (TDPGs)*—a formulation equivalent to WCF protocols—that address exactly this issue. To define TDPGs, first consider, at a given step, the dual variables Z_A, Z_B as observables with $|\psi\rangle$ governing the probability. This combines the evolution of the certificates on cheating probabilities with the evolution of the honest state—the state obtained when none of the parties is cheating.[9] This idea is formalised as follows.

DEFINITION 3.6 (Prob). Consider $Z \geq 0$ and let $\Pi^{[z]}$ represent the projector on the eigenspace of eigenvalue $z \in \mathrm{spectrum}(Z)$. We have $Z = \sum_z z\Pi^{[z]}$. Let $|\psi\rangle$ be a vector, not necessarily normalized. We define the function $\mathrm{Prob}[Z, \psi] : [0, \infty) \to [0, \infty)$ as

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

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

$$\mathrm{Prob}[Z_A, Z_B, \psi](z_A, z_B) = \begin{cases} \langle\psi|\,\Pi^{[z_A]} \otimes \mathbb{I}_M \otimes \Pi^{[z_B]}\,|\psi\rangle & \text{if } (z_A, z_B) \in \mathrm{sp}(Z_A) \times \mathrm{sp}(Z_B), \\ 0 & \text{else.} \end{cases}$$

In this subsection, we consider TDPGs with EBM transitions. An *Expressible by Matrices* (EBM) transition may be viewed as a distillation of each (non-trivial) step of a protocol. It is formalised as follows.

DEFINITION 3.7 (Line Transition). A line transition is an ordered pair of finitely supported functions $g, h : [0, \infty) \to [0, \infty)$, which we denote as $g \to h$.

DEFINITION 3.8 (EBM line transition). Let $g, h : [0, \infty) \to [0, \infty)$ be two functions with finite supports. The line transition $g \to h$ is EBM if there exist two matrices $0 \leq G \leq H$ and a vector $|\psi\rangle$, not necessarily normalized, such that $g = \mathrm{Prob}\,[G, |\psi\rangle]$ and $h = \mathrm{Prob}\,[H, |\psi\rangle]$.

DEFINITION 3.9 (EBM transition). Let $g, h : [0, \infty) \times [0, \infty) \to [0, \infty)$ be two functions with finite supports. The transition $g \to h$ is an

— EBM horizontal transition if $g(., y) \to h(., y)$ is an EBM line transition for all $y \in [0, \infty)$, and

---

9   Originally, using a similar maneuver, Kitaev settled the solvability of the quantum strong coin flipping problem by giving a lower bound on its bias [27].

— EBM vertical transition if $g(x, .) \to h(x, .)$ is an EBM line transition for all $x \in [0, \infty)$.

REMARK 3.10. When clear from the context, we refer to an EBM line transition simply as an EBM transition.

We can now combine these two notions to define TDPGs with EBM transitions (also referred to as *EBM point games*). We use the following 2-variate generalisation of Equation (2), in subsequent definitions:

$$\llbracket x_g, y_g \rrbracket (x, y) = \begin{cases} 1 & x_g = x \text{ and } y_g = y \\ 0 & \text{else.} \end{cases}$$

DEFINITION 3.11 (TDPG with EBM transitions—EBM point game). An EBM point game is a sequence of functions $\{g_0, g_1, \ldots, g_n\}$ with finite support such that

— $g_0 = 1/2 \llbracket 0, 1 \rrbracket + 1/2 \llbracket 1, 0 \rrbracket$;
— for all even i, $g_i \to g_{i+1}$ is an EBM vertical transition;
— for all odd i, $g_i \to g_{i+1}$ is an EBM horizontal transition;
— $g_n = 1 \llbracket \beta, \alpha \rrbracket$ for some $\alpha, \beta \in [0, 1]$. We call $\llbracket \beta, \alpha \rrbracket$ the final point of the EBM point game.

In informal discussions, we often refer to transitions as *moves* (of the corresponding point game). As we alluded to, EBM point games may be viewed as a distillation of a WCF protocol and therefore the following should not come as a surprise.

PROPOSITION 3.12 (WCF $\implies$ EBM point game). *Given a WCF protocol with cheating probabilities P_A^* and P_B^*, along with a positive real number $\delta > 0$, there exists an EBM point game with final point $\llbracket P_B^* + \delta, P_A^* + \delta \rrbracket$.*

The converse statement—given an EBM point game the corresponding WCF protocol can be constructed—is not as easy to see, but it does indeed hold.

THEOREM 3.13 (EBM point game to protocol). *Given an EBM point game with final point $\llbracket \beta, \alpha \rrbracket$, there exists a WCF protocol with $P_A^* \leq \alpha$ and $P_B^* \leq \beta$.*

These establish the equivalence between EBM point games and WCF protocols. We use it in Section 4, to prove Theorem 4.3. The proofs of all statements made here can be found in [32, 3].

3.3   TDPGs with valid transitions/functions

To check whether a given transition is EBM is not an easy task. Kitaev and Mochon [32] introduced the following alternate characterisation of EBM line transitions to simplify the analysis.

PROPOSITION 3.14. *(Relating EBM and strictly valid transitions [32, 3]) Let $g \to h$ where $g = \sum_{i=1}^{n_g} p_{g_i} [\![x_{g_i}]\!]$ and $h = \sum_{i=1}^{n_h} p_{h_i} [\![x_{h_i}]\!]$ with all x_{g_i}, x_{h_i} being non-negative and distinct ($x_{g_i} \neq x_{g_j}$ and $x_{h_i} \neq x_{h_j}$ for every $i \neq j$), and $p_{g_i}, p_{h_i} > 0$. Then, the transition is EBM if it is* strictly valid, *i.e. the following equality holds and the inequalities are* strictly *satisfied:*

$$\sum_{i=1}^{n_h} p_{h_i} = \sum_{i=1}^{n_g} p_{g_i}$$

$$\sum_{i=1}^{n_h} p_{h_i} \frac{\lambda x_{h_i}}{\lambda + x_{h_i}} \geq \sum_{i=1}^{n_g} p_{g_i} \frac{\lambda x_{g_i}}{\lambda + x_{g_i}} \quad \forall \lambda > 0, \quad and \quad \sum_{i=1}^{n_h} x_{h_i} p_{h_i} \geq \sum_{i=1}^{n_g} x_{g_i} p_{g_i}.$$

Conversely, a transition is valid, *i.e. satisfies these inequalities, if the transition $g \to h$ is EBM.*

Using Proposition 3.14, one can consider a *TDPG with valid transitions* (or briefly, a *valid point game*), instead of looking at a TDPG with EBM transitions (or briefly, an EBM point game) as in Definition 3.11. This is simply because a TDPG with valid transitions can be converted to a TDPG with strictly valid transitions, for any $\delta > 0$ increase in the coordinates of the final point. Then, an application of Proposition 3.14 immediately gives the corresponding TDPG with EBM transitions.

How do valid transitions help? Recall that EBM transitions involved ensuring certain matrix inequalities were satisfied. Valid transitions, instead, are characterised by scalar inequalities (albeit infinitely many, one for each $\lambda > 0$) and this leads to significant simplification. For instance, one can check that the following transitions involving a single point are valid. These, as stated earlier, are already enough to construct TDPGs approaching bias 1/6.

EXAMPLE 3.15 (Point raise). $p [\![x_g]\!] \to p [\![x_h]\!]$ with $x_h \geq x_g$ is a valid transition.

◆

EXAMPLE 3.16 (Point merge). $p_{g_1} [\![x_{g_1}]\!] + p_{g_2} [\![x_{g_2}]\!] \to (p_{g_1} + p_{g_2}) [\![x_h]\!]$ with $x_h \geq \frac{p_{g_1} x_{g_1} + p_{g_2} x_{g_2}}{p_{g_1} + p_{g_2}}$ is a valid transition, or generally $\sum_i p_{g_i} [\![x_{g_i}]\!] \to (\sum_i p_{g_i}) [\![x_h]\!]$ with $x_h \geq \langle x_g \rangle$ is a valid transition. ◆

EXAMPLE 3.17 (Point split). $p_g [\![x_g]\!] \to p_{h_1} [\![x_{h_1}]\!] + p_{h_2} [\![x_{h_2}]\!]$ with $p_g = p_{h_1} + p_{h_2}$ and $\frac{p_g}{x_g} \geq \frac{p_{h_1}}{x_{h_1}} + \frac{p_{h_2}}{x_{h_2}}$ is a valid transition, or generally $(\sum_i p_{h_i}) [\![x_g]\!] \to \sum_i p_{h_i} [\![x_{h_i}]\!]$ with $\frac{1}{x_g} \geq \langle \frac{1}{x_h} \rangle$ is a valid transition. ◆

We conclude this discussion by outlining the idea behind the proof of Proposition 3.14.[10] To this end, note that whenever g and h have disjoint support, one can equivalently consider the function $t = h - g$. Then, assuming the support is indeed disjoint, one can consider EBM (valid) functions instead of EBM (valid) transitions. The advantage of considering the set of

---

10   This result was first presented by Mochon and Kitaev, but it was proved using matrix perturbation theory [32]. In [3], Aharonov, Chailloux, Ganz, Kerenidis and Magnin worked out a simpler proof, along the lines alluded to by Mochon and Kitaev, and this is the approach that we outline here.

functions (instead of transitions) is that such sets have better structure. In particular, the set of EBM functions is a convex cone, K. Interestingly, the dual of this cone, K^*, happens to be the set of *operator monotone functions* (i.e. functions such that if $X \geq Y$, then $f(X) \geq f(Y)$ for all Hermitian matrices X, Y). This set, K^*, has been widely studied and shown to admit a surprisingly elegant and simple characterisation. Consequently, the bi-dual of EBM functions, i.e. K^{**}, also admits a simple characterisation—it is exactly the set of valid functions. A standard result in conic duality [14] states that $K^{**} = \text{cl}(K)$ where cl denotes the closure. That is, the set of EBM functions and the set of valid functions are the same up to closures, which almost completes the proof. Crucially, this is exactly the step which is non-constructive in Mochon's analysis—given a valid function, there is no known general procedure for constructing the matrices which certify the function is EBM. To complete the proof, the subtlety about closures must be handled. In [3] the authors handle it by considering strictly valid functions instead of valid functions. In our approach introduced in Section 4, we show that the closure issue is naturally accounted for, by explicitly considering projectors (as in Theorem 3.2).

3.4   Time-Independent Point Games (TIPGs)

The point game formalism can be further simplified, and it is in this simplified formalism that Mochon constructed his family of point games achieving arbitrarily small bias. Instead of considering the entire *sequence* of horizontal and vertical transitions, he focused on just two functions (hence the name *time-independent*), as described below.

DEFINITION 3.18 (TIPG). A *time-independent point game (TIPG)* is a valid horizontal function, denoted by a, and a valid vertical function, denoted by b, such that

$$a + b = 1 [\![\beta, \alpha]\!] - \frac{1}{2} [\![0, 1]\!] - \frac{1}{2} [\![1, 0]\!]$$

for some $\alpha, \beta > 1/2$. Further
— we call the point $[\![\beta, \alpha]\!]$ the final point of the game, and
— we call the set $\mathcal{S} = (\text{supp}(a) \cup \text{supp}(b)) \setminus \text{supp}(a + b)$, the set of intermediate points.

REMARK 3.19. When clear from the context, we may use the word TIPG even when $a + b$ is not necessarily $[\![\beta, \alpha]\!] - \frac{1}{2}([\![0, 1]\!] + [\![1, 0]\!])$ but some other function, c, with finite support in $[0, \infty) \times [0, \infty)$ satisfying $\sum_{x \in \text{supp}(c)} c(x) = 0$.

It is straightforward to show that every valid point game (as defined above) corresponds to a TIPG with the same final point (β, α). Explicitly, if the valid point game with final point $[\![\beta, \alpha]\!]$ is specified by $a_1, a_2 \ldots a_n$ valid horizontal and $b_1, b_2 \ldots b_n$ valid vertical functions, then the corresponding TIPG is specified by $a = \sum_{i=1}^{n} a_i$ and $b = \sum_{i=1}^{n} b_i$, which are horizontally and vertically valid, respectively, and satisfy $a + b = [\![\beta, \alpha]\!] - \frac{1}{2} [\![0, 1]\!] - \frac{1}{2} [\![1, 0]\!]$. Surprisingly, the converse was also shown to hold.

THEOREM 3.20 (TIPG to valid point games **[32, 3]**). *Given a TIPG with a valid horizontal function a and a valid vertical function b such that $a + b = 1 [\![\beta, \alpha]\!] - \frac{1}{2} [\![0, 1]\!] - \frac{1}{2} [\![1, 0]\!]$, one can construct, for all $\epsilon > 0$, a valid point game with its final point being $[\![\beta + \epsilon, \alpha + \epsilon]\!]$, where the number of transitions depends on ϵ and each transition is either*

  — *a point raise, a point merge, a point split, or*
  — *the horizontally valid function a, scaled down, or*
  — *the vertically valid function b, scaled down,*

where the scaling factor also depends on ϵ.

   In words, the theorem says that every TIPG can be converted to a valid TDPG with almost the same final point, using essentially the same non-trivial moves encoded in a and b. However, this seems counter-intuitive because it is not a priori clear how a time ordered sequence of transitions can be extracted from a time-independent point game. For instance, one might run into causal loops—we expect a point to be present to create another point which in turn is required to produce the first point. To overcome such issues, the key idea is to use a so-called *catalyst state*: (i) Deposit a small amount of weight wherever a assigns negative weight. (ii) Run a scaled down round of a and b (the scaling is proportional to the weight deposited in the beginning). (iii) Repeat (ii) until almost all the weight has been transferred to the final point. (iv) Absorb the catalyst state into the final point, at a small cost to the bias.
   Among these, performing step (iv), needs most care. The weight in step (i) determines the number of times step (ii) must be repeated. That, in turn, determines the number of rounds the protocol requires. While in this work, we do not focus on the resources required to implement WCF, we nonetheless state the following which, in particular, relates the bias to the round complexity (number of rounds of communication) of point games. The latter, (using our results in Section 4) can be used to obtain protocols with (essentially) the same bias and round complexity.[11]

COROLLARY 3.21 (**[3]**). *Consider a TIPG with a valid horizontal function $a = a^+ - a^-$ and a valid vertical function $b = b^+ - b^-$ such that $a + b = [\![\beta, \alpha]\!] - \frac{1}{2} [\![0, 1]\!] - \frac{1}{2} [\![1, 0]\!]$ where a^+, a^-, b^+, b^- are finitely supported functions that take values in $[0, \infty)$ with disjoint support (i.e. $supp(a^+) \cap supp(a^-) = \emptyset$ and similarly for b^+ and b^-). Let Γ be the largest coordinate of all the points that appear in the TIPG. Then, for all $\epsilon > 0$, one can construct a point game with $O \left(\frac{\|b\| \Gamma^2}{\epsilon^2} \right)$ valid transitions and final point $[\![\beta + \epsilon, \alpha + \epsilon]\!]$.*

---

11   However, this particular result is not a new contribution.

3.5 Mochon's TIPG achieving bias $\varepsilon(k) = 1/(4k+2)$

We can now explain how Mochon [32] proved the existence of WCF protocols with arbitrarily small bias. He constructed a family of TIPGs, parametrised by an integer $k > 0$, such that the final point is $[\![\frac{1}{2} + e(k), \frac{1}{2} + e(k)]\!]$, where $e(k) = 1/(4k+2)$ (see Figure 5a).

(a) Mochon's TIPG for $k = 2$.
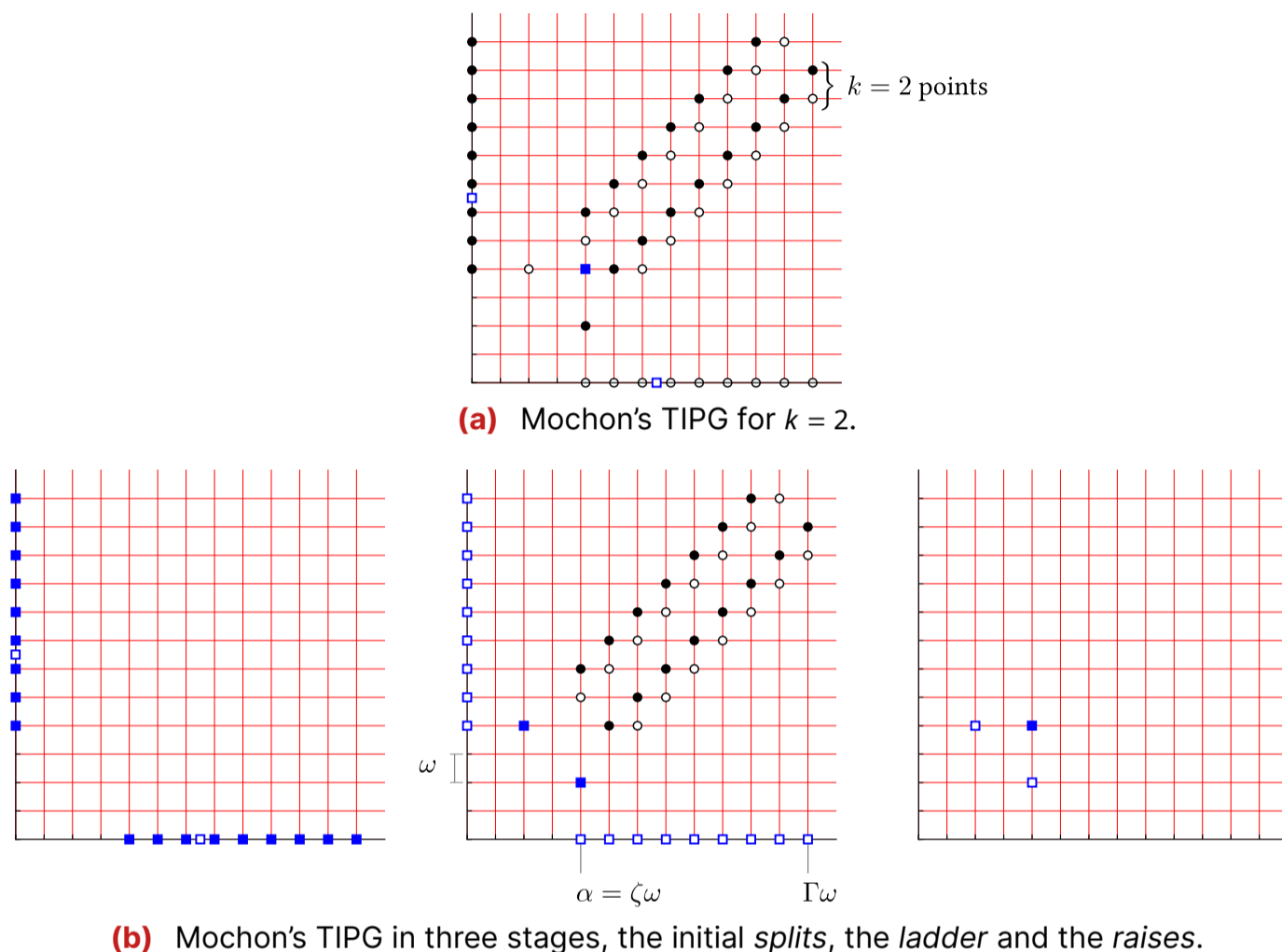
(b) Mochon's TIPG in three stages, the initial *splits*, the *ladder* and the *raises*.

Figure 5. Mochon's TIPG. The unfilled squares represent initial points of a TIPG (i.e. points with negative weight in $a + b$) and the filled squares point represent final points (i.e. points with positive weight in $a + b$). Filled circles carry negative weight and unfilled circles carry positive weight for the horizontally valid function. For the vertically valid function, it is the other way around. Thus, when the functions are added, the points corresponding to these circles cancel—except *for circles on the axes*: circles along the y-axis represent points present only in the horizontally valid function and circles along the x-axis represent those only in the vertically valid function. Note that in both cases, they have negative weight.

The overall structure of these games is easy to describe. Apart from their initial points, $[\![0, 1]\!]$ and $[\![1, 0]\!]$, all the other points involved are placed on a regular lattice, i.e. at locations of the form $[\![a\omega, b\omega]\!]$ where $a, b \in \mathbb{N}$ and $\omega \in (0, \infty)$. The final point of the games is $[\![\alpha, \alpha]\!]$ for $\alpha = \zeta\omega = \frac{1}{2} + O\left(\frac{1}{k}\right)$ where $\zeta \in \mathbb{N}$, and in general, they have the following three stages (see Figure 5b):

1. *Split.* The point $[\![0, 1]\!]$ is vertically split into many points along the y-axis. The resulting points lie between $\zeta\omega$ and $\Gamma\omega$ with $\zeta, \Gamma \in \mathbb{N}$. Analogously, the point $[\![1, 0]\!]$ is horizontally split into many points along the x-axis.

2. *Ladder.* This is the main non-trivial move of the games parametrised by an integer $k > 0$, and it consists of points along the diagonal and along the axes (see the second image in Figure 5b). The points on the axes are transformed by the ladder into the final points $[\![\alpha - k\omega, \alpha]\!]$ and $[\![\alpha, \alpha - k\omega]\!]$.

3. *Raise.* The two points $[\![\alpha - k\omega, \alpha]\!]$ and $[\![\alpha, \alpha - k\omega]\!]$ are raised to the final point $[\![\alpha, \alpha]\!]$.

For each integer $k > 0$ there exist parameters $\omega, \Gamma \in (0, \infty)$ such that the two initial splits are valid, the *ladder* corresponds to a horizontally and vertically valid function, and $\alpha = \frac{1}{2} + O\left(\frac{1}{k}\right)$.

The key technical tool that Mochon introduced is the following: given a set of point coordinates, he constructed a way of assigning non-trivial weights to them such that this assignment is valid while still retaining considerable freedom. This weight assignment is parametrised by a polynomial and works for essentially all polynomials up to a certain degree. In other words, he simplified the validity condition by restricting to a class of functions which are easy to manipulate and are valid by construction.

LEMMA 3.22 (Mochon's assignment is valid[32, 3])**.** *Let*

— *$x_1, x_2 \ldots x_n$ be distinct, non-negative real numbers, and*

— *f be a polynomial of degree at most $n - 1$ satisfying $f(-\lambda) \geq 0$ for all $\lambda \geq 0$.*

Then,

$$a = \sum_{i=1}^{n} \frac{-f(x)}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!] \tag{4}$$

is a valid function.

These functions, which are later referred to as f-assignments, play a crucial role in our systematic construction of WCF protocols corresponding to the TIPGs described above (see Section 5).

4. TDPG-to-Explicit-protocol Framework (TEF) and Bias 1/10 Game and Protocol

In this section, we give a framework for converting a TDPG (with EBM or valid transitions) into an explicit protocol, approaching the same bias. In fact, we introduce a slightly different condition which is similar to the EBM condition but involves projectors. These conditions (valid, EBM and the one we introduce) are equivalent but we defer this discussion to the appendix. This is because, in the present and subsequent section, we explicitly construct the matrices to show the required conditions are satisfied for TDPGs of interest. In particular, we begin

by constructing the appropriate matrices corresponding to the three *basic* moves involving a single point—raise, split and merge (Example 3.15, Example 3.17 and Example 3.16 resp.). These already recover the bias 1/6 protocol from the bias 1/6 TDPG. To go below, we construct matrices for *advanced* moves that take three points to two points (and also two points to two points), corresponding to Mochon's TDPG approaching bias 1/10. Together with the three *basic* moves, these allow us to construct protocols approaching bias 1/10. The construction of *advanced* moves is perturbative. Thus, going below 1/10 requires more work and that is covered in the next section.

Remark about prior work. To establish the equivalence between TDPG and WCF protocols, prior works [3] and [32] also showed a way to convert a TDPG into a WCF protocol. However, one of the primary differences compared to our work is that, as we alluded to in the introduction, the message register in our case decouples after each round as we suitably place projectors (which correspond to cheat detection). This leads to simplifications—both mathematical and practical.

4.1   The framework

We want to construct a WCF protocol such that its dual (see Theorem 3.4) corresponds to a given TDPG. We therefore start with a frame of a TDPG, and sequentially build dual variables and rotations. These rotations specify a WCF protocol and the dual variables are such that they constitute a feasible solution to the dual of this WCF protocol. The key property of this dual feasible solution is that it certifies that the WCF protocol we obtain has the same bias as that encoded in the final frame of the TDPG we started with.

Recall that TDPGs are formulated in terms of *Prob* (see Definition 3.6). The most natural way to construct the matrices Zs and the vector $|\psi\rangle$ (which appear in the definition of *Prob*) is the following: Given an arbitrary frame of a TDPG, construct an entangled state that encodes the weight and define Zs to contain the coordinates corresponding to these weights. We formalise these as the *Canonical Form*.

DEFINITION 4.1 (Canonical Form). The tuple $(|\psi\rangle, Z^A, Z^B)$ is said to be in the Canonical Form with respect to a set of points in a frame $\sum_i P_i [\![x_i, y_i]\!]$ of a TDPG[12] if $|\psi\rangle = \sum_i \sqrt{P_i} |ii\rangle_{AB} \otimes |\varphi\rangle_M$, $Z^A = \sum x_i |i\rangle \langle i|_A$ and $Z^B = \sum y_i |i\rangle \langle i|_B$ where $|\varphi\rangle_M$ represents the state of extra uncoupled registers which might be present.

The label $|ii\rangle$ corresponds to a point with coordinates x_i, y_i and weight P_i in the frame (see also Figure 6a). It is tempting to imagine that we systematically construct, from each frame of a TDPG, a canonical form of $|\psi\rangle$ s and Zs, and deduce the unitaries from the evolution of the state $|\psi\rangle$. This approach suffers from two issues: (a) the unitaries are not necessarily decomposable

---

12   One could define the canonical form for any frame but we only use it for those arising from TDPGs.

into moves by Alice and Bob who communicate only through the message register, and, (b) the constraints imposed on consecutive Zs (by, say, a TDPG with EBM transitions), that take the form $Z_{n-1} \otimes \mathbb{I} \geq U_n^\dagger (Z_n \otimes \mathbb{I}) U_n$, are not satisfied in general.

We design our framework to overcome these issues. Before we delve into the details, we clarify how the output of the framework relates to a WCF protocol. The framework outputs variables indexed as $|\psi_{(i)}\rangle$, $Z_{(i)}$, $U_{(i)}$ (see Definition 3.11 and Proposition 3.12) and they are produced in the reverse time convention (relative to the WCF protocol). This means that the variables at the ith step of the protocol (which follows the forward time convention) are given by $|\psi_i\rangle = |\psi_{(N-i)}\rangle$, $Z_i = Z_{(N-i)}$ and $U_i = U_{(N-i)}^\dagger$. In fact, this extends naturally to the case where one additionally has projectors, e.g. $U_i E_i = E_{(N-i)} U_{(N-i)}^\dagger$.

Let us start with an informal outline of our framework. Assume that a canonical description is given. Let the labels on the points we want to transform be $\{g_i\}$, and let us also assume that we wish to apply a horizontal transition, i.e. Alice performs the non-trivial step. Let the labels of the points that will be left unchanged be $\{k_i\}$ (see Figure 6b). We can write the state as

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

We[13] want Bob to send his part of $|g_i\rangle$ states to Alice through the message register. One way is to conditionally swap to obtain

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

This way, all the points align along the y-axis, while the respective x-coordinates remain the same due to the fact that it is a horizontal transition.[14] Let $\{h_i\}$ be the labels of the new points after the transformation. We assume that h_i, g_i and k_i index orthonormal vectors. Alice can update the probabilities and labels by locally performing a unitary to obtain

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

It is precisely this step that yields the non-trivial constraint. Bob must now accept this by 'unswapping' to get

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

As we mentioned, relative to the actual protocol, the sequence is in the reverse time convention. Note also that we add a few extra frames to the final TDPG to go from a given frame to the next

---

13   To be explicit, for $X \in \{\mathcal{A}, \mathcal{M}, \mathcal{B}\}$, the Hilbert space X is the span of the orthonormal vectors $\{\{|g_i\rangle_X\}_i, \{|k_i\rangle_X\}_i, \{|h_i\rangle_X\}_i, |m\rangle\}$

14   Intuitively, this is because we relax the dual variable Z^B and make all the points have the same $y_{\max}$ coordinate (where $y_{\max}$ is the highest y coordinate among the points of interest), as explained in Step *2. Bob sends to Alice* below.
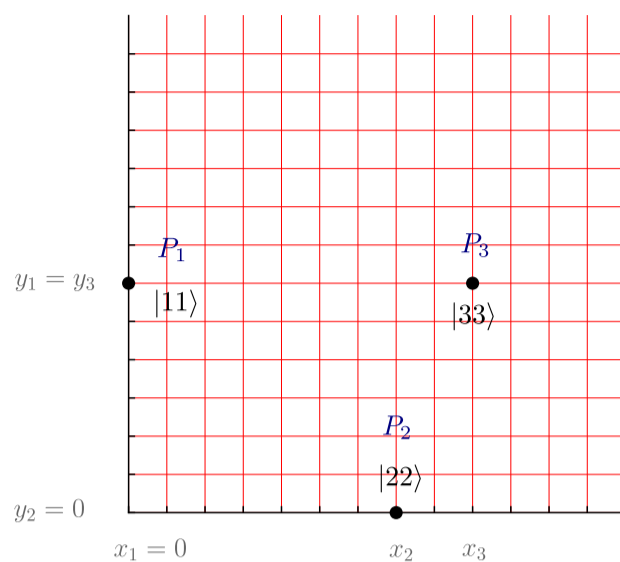
(a) Frame of a TDPG
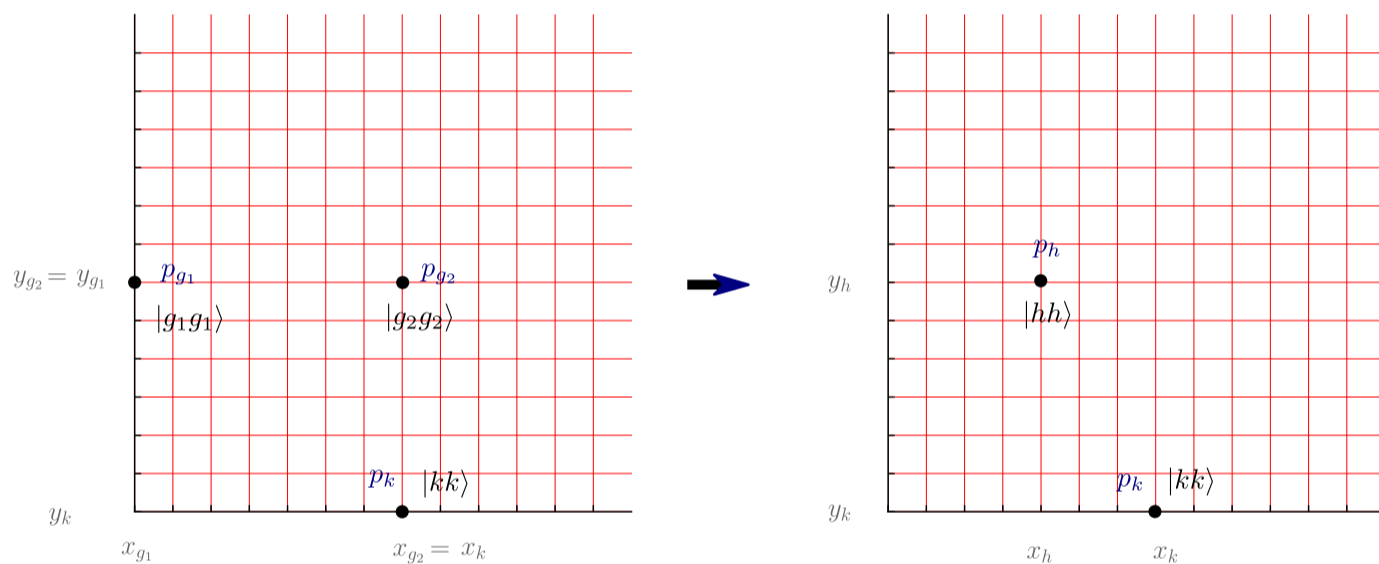
(b) The points that are unchanged from one frame to another are labelled by $\{k_i\}$.
Among the points that change, the initial ones are labelled by $\{g_i\}$ and the final ones by $\{h_i\}$.

Figure 6. Illustrations for the Canonical Form

of the original TDPG. This is irrelevant, when resource usage is not of interest, as the bias does not change.

   We now fill in the details and show that at each step, one can ensure certain matrix inequalities hold. (For the non-trivial step, a matrix inequality is assumed to hold, instead.) These inequalities, are exactly the inequalities in the constraints of the dual SDP (see Theorem 3.4), and, in turn, ensure that one directly obtains a dual of the WCF protocol corresponding to the TDPG of interest.

1. **First frame.**

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

$$Z^A_{(1)} = \sum_i x_{g_i}\,|g_i\rangle\,\langle g_i|_A + \sum_i x_{k_i}\,|k_i\rangle\,\langle k_i|_A$$

$$Z^B_{(1)} = \sum_i y_{g_i}\,|g_i\rangle\,\langle g_i|_B + \sum_i y_{k_i}\,|k_i\rangle\,\langle k_i|_B\,.$$

PROOF. Follows from the assumption of starting with a Canonical Form. ∎

2. **Bob sends to Alice.** With $y \geq \max\{y_{g_i}\}$ the following

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

$$U_{(1)} = U^{\mathrm{SWP}\{\vec{g},m\}}_{BM}$$

$$Z^A_{(2)} = Z^A_{(1)} \quad \text{and} \quad Z^B_{(2)} = y\mathbb{I}^{\{\vec{g},m\}}_B + \sum_i y_{k_i}\,|k_i\rangle\,\langle k_i|_B\,,$$

is a viable choice, i.e. it satisfies the properties

$$(1) \quad |\psi_{(2)}\rangle = U_{(1)}\,|\psi_{(1)}\rangle\,,$$

and

$$(2) \quad U^\dagger_{(1)}\left(Z^B_{(2)} \otimes \mathbb{I}_M\right) U_{(1)} \geq \left(Z^B_{(1)} \otimes \mathbb{I}_M\right).$$

PROOF. We have to prove that the above properties (1) and (2) are satisfied. (1) It follows trivially from the defining action of $U_{(1)}$.

(2) For ease of notation, let $U = U_{(1)}$ and note that $U^\dagger = U$, so that we can write

$$U\left(Z^B_{(2)} \otimes \mathbb{I}_M\right) U$$

$$= y\left(U\left(\mathbb{I}^{\{\vec{g},m\}}_B \otimes \mathbb{I}^{\{\vec{g},m\}}_M\right) U + U\;\underbrace{\left(\mathbb{I}^{\{\vec{g},m\}}_B \otimes \mathbb{I}^{\{\vec{k},\vec{h}\}}_M\right)}_{\text{outside } U\text{'s action space}}\; U\right) + U\;\underbrace{\left(\sum_i y_{k_i}\,|k_i\rangle\,\langle k_i| \otimes \mathbb{I}\right)}_{\text{outside } U\text{'s action space}}\; U$$

$$= Z_{(2)} \otimes \mathbb{I}_M \geq Z_{(1)} \otimes \mathbb{I}_M$$

so long[15] as $y \geq y_{g_i}$, which is guaranteed by the choice of y. ∎

---

15   By the action space of U we mean the space where U acts non-trivially.

3. **Alice's non-trivial step.** Consider the following choice

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

$$E_{(2)} U_{(2)} = E_{(2)} \left(|w\rangle\langle v| + \text{other terms acting on span}\{\,|h_i h_i\rangle, |g_i g_i\rangle\}\right)_{AM}$$

$$Z^A_{(3)} = \sum_i x_{h_i} |h_i\rangle\langle h_i| + \sum_i x_{k_i} |k_i\rangle\langle k_i| \quad \text{and} \quad Z^B_{(3)} = Z^B_{(2)}$$

where

$$|v\rangle = \frac{\sum_i \sqrt{p_{g_i}}\,|g_i g_i\rangle}{\sqrt{\sum_i p_{g_i}}}, \ |w\rangle = \frac{\sum_i \sqrt{p_{h_i}}\,|h_i h_i\rangle}{\sqrt{\sum_i p_{h_i}}}, E_{(2)} = \left(\sum |h_i\rangle\langle h_i|_A + \sum |k_i\rangle\langle k_i|_A\right) \otimes \mathbb{I}_M$$

subject to the condition

$$\sum x_{h_i} |h_i h_i\rangle\langle h_i h_i| \geq \sum x_{g_i} E_{(2)} U_{(2)} |g_i g_i\rangle\langle g_i g_i| U^\dagger_{(2)} E_{(2)} \tag{5}$$

and the conservation of probability, viz. $\sum p_{g_i} = \sum p_{h_i}$. We claim that this choice is viable, i.e. it satisfies the conditions (1) $E_{(2)} |\psi_{(3)}\rangle = U_{(2)} |\psi_{(2)}\rangle$, and (2) $Z^A_{(3)} \otimes \mathbb{I}_M \geq E_{(2)} U_{(2)} \left(Z^A_{(2)} \otimes \mathbb{I}_M\right) U^\dagger_{(2)} E_{(2)}$.

PROOF. We must show that (1) and (2) as above hold. For (1) we observe that $E_{(2)} |\psi_{(3)}\rangle = |\psi_{(3)}\rangle$ and the statement holds by construction of $U_{(2)}$.

(2) Consider the space $\mathcal{H} = \text{span}\,\{|g_1 g_1\rangle, |g_2 g_2\rangle \ldots, |h_1 h_1\rangle, |h_2, h_2\rangle \ldots\}$ which is a subspace of $\mathcal{A} \otimes \mathcal{M}$ (space of Alice and the message register). One can write $\mathcal{A} \otimes \mathcal{M} = \mathcal{H} \oplus \mathcal{H}^\perp$. We separate all expressions which act on the $\mathcal{H}$ space from the rest. We start with the RHS, excluding the $U_{(2)}$'s,

$$Z^A_{(2)} \otimes \mathbb{I}_M = \underbrace{\sum x_{g_i} |g_i g_i\rangle\langle g_i g_i|}_{\text{I}} + \sum x_{g_i} |g_i\rangle\langle g_i| \otimes (\mathbb{I} - |g_i\rangle\langle g_i|) + \sum x_{k_i} |k_i\rangle\langle k_i| \otimes \mathbb{I}.$$

Note that $Z^A_{(2)} \otimes \mathbb{I}_M$ is block diagonal with respect to $\mathcal{H} \oplus \mathcal{H}^\perp$, with term I making the first block (corresponding to $\mathcal{H}$), and the rest constituting the second block. Next consider the LHS,

$$Z^A_{(3)} \otimes \mathbb{I}_M = \underbrace{\sum x_{h_i} |h_i h_i\rangle\langle h_i h_i|}_{\text{I}} + \sum x_{h_i} |h_i\rangle\langle h_i| \otimes (\mathbb{I} - |h_i\rangle\langle h_i|) + \sum x_{k_i} |k_i\rangle\langle k_i| \otimes \mathbb{I},$$

which is also block diagonal with respect to $\mathcal{H} \oplus \mathcal{H}^\perp$ and has only term I in the first block. Consequently, only on these will $U_{(2)}$ have a non-trivial action (as $U_{(2)}$ is of the form $\begin{bmatrix} U & 0 \\ 0 & \mathbb{I}_{\mathcal{H}^\perp} \end{bmatrix}$ wrt $\mathcal{H} \oplus \mathcal{H}^\perp$). Let us first evaluate the non-$\mathcal{H}$ part where we only need to apply the projector. The result after separating equations where possible is

$$\sum x_{h_i} |h_i\rangle\langle h_i| \otimes (\mathbb{I} - |h_i\rangle\langle h_i|) \geq 0, \text{ and } \sum (x_{k_i} - x_{k_i}) |k_i\rangle\langle k_i| \otimes \mathbb{I} \geq 0,$$

which imply $x_{h_i} \geq 0$. The non-trivial part yields

$$\sum x_{h_i} |h_i h_i\rangle\langle h_i h_i| \geq \sum x_{g_i} E_{(2)} U_{(2)} |g_i g_i\rangle\langle g_i g_i| U^\dagger_{(2)} E_{(2)}$$

completing the proof.   ∎

4. **Bob accepts Alice's change.** The following holds:

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

$$E_{(3)}U_{(3)} = E_{(3)}U_{BM}^{\mathrm{SWP}\{\vec{h},m\}}$$

$$Z_{(4)}^A = Z_{(3)}^A \quad \text{and} \quad Z_{(4)}^B = y\sum_i \left|h_i\right\rangle\left\langle h_i\right| + \sum_i y_{k_i}\left|k_i\right\rangle\left\langle k_i\right|_B,$$

where $E_{(3)} = \left(\sum \left|h_i\right\rangle\left\langle h_i\right| + \sum \left|k_i\right\rangle\left\langle k_i\right|\right)_B \otimes \mathbb{I}_M$.

PROOF. We have to prove:

$$(1) \quad E_{(3)}\left|\psi_{(4)}\right\rangle = U_{(3)}\left|\psi_{(3)}\right\rangle$$

and

$$(2) \quad Z_{(4)}^B \otimes \mathbb{I}_M \geq E_{(3)}U_{(3)}\left(Z_{(3)}^B \otimes \mathbb{I}_M\right)U_{(3)}^\dagger E_{(3)}.$$

Condition (1) can be shown by a direct application of $U^\dagger E$ on $\left|\psi_{(4)}\right\rangle$, where E, U denote $E_{(3)}$ and $U_{(3)}$, respectively, in this proof for ease of notation.
Condition (2) can be established by first noting that

$$EU\left(\mathbb{I}_B^{\{\vec{g},m\}} \otimes \mathbb{I}_M^{\{\vec{h},\vec{g},\vec{k},m\}}\right)U^\dagger E = EU\left(\mathbb{I}_B^{\{m\}} \otimes \mathbb{I}_M^{\{\vec{h},\vec{g},\vec{k},m\}}\right)U^\dagger E + E\left(\mathbb{I}_B^{\{\vec{g}\}} \otimes \mathbb{I}_M^{\{\vec{h},\vec{g},\vec{k},m\}}\right)E$$

$$= EU\left(\mathbb{I}_B^{\{m\}} \otimes \mathbb{I}_M^{\{\vec{h},m\}}\right)U^\dagger E = \sum \left|h_i\right\rangle\left\langle h_i\right| \otimes \mathbb{I}_M^{\{m\}}.$$

Since the other term in $Z_{(3)}^B \otimes \mathbb{I}$ is not in the action space of U it follows that

$$EU(Z_{(3)}^B \otimes \mathbb{I})U^\dagger E = y\sum \left|h_i\right\rangle\left\langle h_i\right| \otimes \mathbb{I}_M^{\{m\}} + \sum y_{k_i}\left|k_i\right\rangle\left\langle k_i\right| \otimes \mathbb{I}_M.$$

It only remains to show that $Z_{(4)}^B \otimes \mathbb{I}_M \geq EU\left(Z_{(3)}^B \otimes \mathbb{I}_M\right)U^\dagger E$ which holds as $y\sum \left|h_i\right\rangle\left\langle h_i\right| \otimes \mathbb{I}_M \geq y\sum \left|h_i\right\rangle\left\langle h_i\right| \otimes \mathbb{I}_M^{\{m\}}$ and the y_{k_i} term is common.   ∎

Suppose that for each transition in the TDPG, the equation corresponding to Equation (5) can be satisfied. Then, as asserted, using the previous four steps for each transition, one directly obtains a WCF protocol together with a feasible solution to its corresponding dual (as in Theorem 3.4 with projectors) certifying that the WCF protocol has the same bias as the TDPG. Formally (using the notation above) we have the following.

DEFINITION 4.2 (TEF constraint). A transition

$$\sum_{i=1}^{n_k} p_{k_i}\left[\!\left[x_{k_i}\right]\!\right] + \sum_{i=1}^{n_g} p_{g_i}\left[\!\left[x_{g_i}\right]\!\right] \rightarrow \sum_{i=1}^{n_h} p_{h_i}\left[\!\left[x_{h_i}\right]\!\right] + \sum_{i=1}^{n_k} p_{k_i}\left[\!\left[x_{k_i}\right]\!\right] \tag{6}$$

satisfies the *TEF constraint* if there is a unitary matrix $U_{(2)}$ that satisfies the inequality

$$\sum_{i=1}^{n_h} x_{h_i} |h_i h_i\rangle \langle h_i h_i|_{AM} \geq \sum_{i=1}^{n_g} x_{g_i} E_{(2)}^h U_{(2)} |g_i g_i\rangle \langle g_i g_i|_{AM} U_{(2)}^\dagger E_{(2)}^h \tag{7}$$

and the honest action constraint $U_{(2)} |v\rangle = |w\rangle$, where $|h_i\rangle, |g_i\rangle$ are orthonormal basis vectors,

$$|v\rangle = \mathcal{N}\left(\sum \sqrt{p_{g_i}} |g_i g_i\rangle_{AM}\right) \quad \text{and} \quad |w\rangle = \mathcal{N}\left(\sum \sqrt{p_{h_i}} |h_i h_i\rangle_{AM}\right)$$

for $\mathcal{N}(|\psi\rangle) = |\psi\rangle / \sqrt{\langle\psi|\psi\rangle}$, $E^h = \left(\sum_{i=1}^{n_h} |h_i\rangle \langle h_i|_A + \sum |k_i\rangle \langle k_i|_A\right) \otimes \mathbb{I}_M$ with $U_{(2)}$'s non-trivial action restricted to span $\{\{|g_i g_i\rangle_{AM}\}, \{|h_i h_i\rangle_{AM}\}\}$, and $|k_i\rangle$ correspond to the points that are left unchanged in the transition.

THEOREM 4.3. *Suppose for each transition of a TDPG, the TEF constraint (see Definition 4.2) can be satisfied. Then, there exists a WCF protocol that has the same TDPG (up to some repetition in frames[16]).*

We implicitly used Remark 3.5 and Theorem 3.4.

4.2   TEF Functions/Transitions

It is evident that the TEF constraint (see Definition 4.2 above) can be simplified by neglecting the parts of the Hilbert space where $U_{(2)}$ behaves as identity. Thus, an equivalent formulation of Definition 4.2 is the following.

DEFINITION 4.4 (TEF constraint (simpler formulation), unitary solves a transition/function, **TEF transitions/functions).** Let $g \to h$ be a transition (see Definition 3.7), with the associated function $t = h - g = \sum_{i=1}^{n_h} p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n_g} p_{g_i} [\![x_{g_i}]\!]$, where all p_{h_i} and p_{g_i} are positive and let $\{\{|g_i\rangle\}_{i=1}^{n_g}, \{|h_i\rangle\}_{i=1}^{n_h}\}$ constitute an orthonormal basis, spanning $\mathcal{H}$. We say U (acting on $\mathcal{H}$) *solves* the transition t if U satisfies the following *TEF constraint*,

$$\sum_{i=1}^{n_h} x_{h_i} |h_i\rangle \langle h_i| \geq \sum_{i=1}^{n_g} x_{g_i} EU |g_i\rangle \langle g_i| U^\dagger E, \quad \text{and} \quad EU \underbrace{\sum_{i=1}^{n_g} \sqrt{p_{g_i}} |g_i\rangle}_{|v\rangle} = \underbrace{\sum_{i=1}^{n_h} \sqrt{p_{h_i}} |h_i\rangle}_{|w\rangle},$$

where $E = \sum_{i=1}^{n_h} |h_i\rangle \langle h_i|$. The transition (function) is a *TEF transition (function)* if there is a unitary matrix that solves it.

As alluded to earlier, one may use TEF functions (instead of EBM or valid functions), without loss of generality.

LEMMA 4.5 (TEF = **closure of EBM = valid**). *The set of the TEF functions, the set of valid functions and the closure of the set of the EBM functions are the same.*

We defer the proof of Lemma 4.5 to Appendix A as we do not need it to prove our result. We do note, however, that Lemma 4.5 above, allows one to circumvent the notion of strictly valid functions, (arguably) simplifying the analysis.

4.3　Special case: the blinkered unitary

In this subsection, we use the more explicit notation from Definition 4.2, Section 4.1 to illustrate how TEF easily allows one to construct WCF protocols approaching bias 1/6. To this end, we introduce an important class of unitaries we call *Blinkered Unitaries*. For clarity, to describe the TEF constraint (as in Definition 4.2), we use U instead of $U_{(2)}$ and E instead of $E^h_{(2)}$. Given a transition (as in Equation (6)), the associated Blinkered Unitary is defined as

$$U = |w\rangle\langle v| + |v\rangle\langle w| + \sum_i |v_i\rangle\langle v_i| + \sum_i |w_i\rangle\langle w_i| + \mathbb{I}^{\text{outside }\mathcal{H}},$$

where $\mathcal{H} = \text{span}\{|g_1 g_1\rangle, |g_2 g_2\rangle \dots, |h_1 h_1\rangle, |h_2, h_2\rangle \dots\}$. We can ignore the last term and restrict our analysis to the $\mathcal{H}$-operator space, where $|v\rangle, \{|v_i\rangle\}$ form a complete orthonormal basis with respect to $\text{span}\{|g_i g_i\rangle\}$, and so do $|w\rangle, \{|w_i\rangle\}$ for $\text{span}\{|h_i h_i\rangle\}$. What makes blinkered unitaries useful is that they satisfy the TEF constraint (as stated in Definition 4.2), when the transition is a non-trivial *basic* move, i.e. a merge (see Example 3.16) or a split (see Example 3.17).

— Merge: $g_1, g_2 \rightarrow h_1$
Using the definitions, we have

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

with $N = \sqrt{p_{g_1} + p_{g_2}}$ and $U = |w\rangle\langle v| + |v\rangle\langle w| + |v_1\rangle\langle v_1| = U^\dagger$. We evaluate

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

Using these, the TEF constraint $x_h\,|h_1 h_1\rangle\langle h_1 h_1| \geq \sum x_{g_i} EU\,|g_i g_i\rangle\langle g_i g_i|\,U^\dagger E$ becomes $x_h \geq \frac{p_{g_1} x_{g_1} + p_{g_2} x_{g_2}}{N^2}$, which is precisely the merge condition (see Example 3.16).

— Split: $g_1 \rightarrow h_1, h_2$
Again, from the definitions, we construct

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

with $N = \sqrt{p_{h_1} + p_{h_2}}$ and $U = |v\rangle\langle w| + |w\rangle\langle v| + |w_1\rangle\langle w_1| = U^\dagger$. We evaluate $EU\,|g_1 g_1\rangle = |w\rangle$ which we substitute into the TEF constraint to obtain

$$x_{h_1}\,|h_1 h_1\rangle\langle h_1 h_1| + x_{h_2}\,|h_2 h_2\rangle\langle h_2 h_2| - x_{g_1}\,|w\rangle\langle w| \geq 0.$$

This yields the matrix equation

$$\begin{bmatrix} x_{h_1} & \\ & x_{h_2} \end{bmatrix} - \frac{x_{g_1}}{N^2} \begin{bmatrix} p_{h_1} & \sqrt{p_{h_1} p_{h_2}} \\ \sqrt{p_{h_1} p_{h_2}} & p_{h_2} \end{bmatrix} \geq 0$$

$$\mathbb{I} \geq \frac{x_{g_1}}{N^2} \begin{bmatrix} \frac{p_{h_1}}{x_{h_1}} & \sqrt{\frac{p_{h_1}}{x_{h_1}} \frac{p_{h_2}}{x_{h_2}}} \\ \sqrt{\frac{p_{h_1}}{x_{h_1}} \frac{p_{h_2}}{x_{h_2}}} & \frac{p_{h_2}}{x_{h_2}} \end{bmatrix}$$

$$\frac{x_{g_1}}{N^2} \left(\frac{p_{h_1}}{x_{h_1}} + \frac{p_{h_2}}{x_{h_2}} \right) \leq 1,$$

where in the first step we used the fact that for $F > 0$, $F - M \geq 0 \equiv \mathbb{I} - \sqrt{F}^{-1} M \sqrt{F}^{-1} \geq 0$, and the last equation is obtained by writing the matrix as $|\psi\rangle \langle\psi|$, and then demanding $1 \geq \langle\psi|\psi\rangle$. This last equation is exactly the split condition (see Example 3.17).

The above two conditions can be readily generalized for an $m \to 1$ point merge and a $1 \to n$ points split, respectively (see Appendix Appendix B). Furthermore, for a general $m \to n$: $g_1, g_2 \ldots g_m \to h_1, h_2 \ldots h_n$ transition, the TEF constraint corresponding to the Blinkered Unitary reduces to the following scalar condition (see Appendix Appendix B for a proof),

$$\frac{1}{\sum_{i=1}^{m} p_{g_i} x_{g_i}} \geq \sum_{i=1}^{n} p_{h_i} \frac{1}{x_{h_i}}.$$

In words, the general $m \to n$ transition affected by the blinkered unitary may be viewed as an $m \to 1$ merge followed by a $1 \to n$ split.

Consequently, blinkered unitaries are enough to convert the 1/6 game into an explicit protocol. However, they fall short for point games going below this bias which seem to require *advanced* moves—moves beyond splits and merges. Next, we construct the unitaries for such moves to obtain WCF protocols approaching bias 1/10.

4.4   Approaching bias 1/10

In Section 3.5 we briefly outlined Mochon's family of TIPGs approaching bias $\epsilon(k) = 1/(4k + 2)$, where k is the number of points involved in the non-trivial step. Here, we detail the game for $k = 2$, and explicitly find the unitaries that solve the transitions used in the game.

All of Mochon's TIPGs, assume an equally spaced n-point lattice given by $x_j = x_0 + j\delta x$ where $\delta x = \delta y$ is small and x_0 is specified shortly.[17] Similarly $y_j = y_0 + j\delta y$ and we define $\Gamma_{k+1} = y_{n-k} = x_{n-k}$. We focus on the "ladder" stage (see Figure 5b). We first constrain the weights of points along the x-axis, by requiring that they arise from the splitting of one point with weight $1/2$ at $(1, 0)$ (similarly for the y-axis). Let $P(x_j)$ denote the probability weight associated with

---

17   Essentially, x_0 provides a bound on P_B^*.

the point $(x_j, 0)$ which is such that

$$\sum_{j=1}^{n} P(x_j) = \frac{1}{2} \text{ and } \sum_{j=1}^{n} \frac{P(x_j)}{x_j} = \frac{1}{2}.$$

Similarly with the point $(0, y_j)$ we associate $P(y_j)$ where $y_j = x_j$ as we also assume that $x_0 = y_0$. These choices explicitly impose symmetry between Alice and Bob which in turn means that we only have to do the analysis for one of them.

We now use Mochon's assignment (see Equation (4)) to (partially) specify weights on points along vertical lines (see Figure 7). In particular, given set of points (with distinct y-coordinates but the same x-coordinate), we use

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

to specify the weight on the point (x_l, y_j) where $f(y_i) = (y_{-2} - y_i)(\Gamma_1 - y_i)(\Gamma_2 - y_i)$.
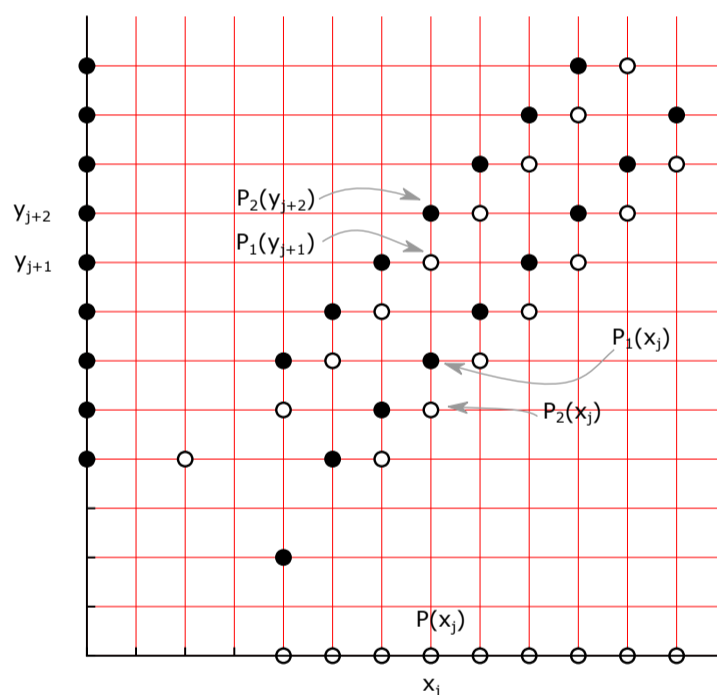
Figure 7. 1/10-bias TIPG: The $3 \to 2$ move

Applying the assignment to the points highlighted in Figure 7 yields

$$P_2(y_{j+2}) = \frac{-f(y_{j+2})c(x_j)}{4 \cdot 3(\delta y)^2 y_{j+2}}, \quad P_1(y_{j+1}) = \frac{-f(y_{j+1})c(x_j)}{3 \cdot 2(\delta y)^2 y_{j+1}},$$

$$P_1(x_j) = \frac{-f(y_{j-1})c(x_j)}{3 \cdot 2(\delta y)^2 y_{j-1}}, \quad P_2(x_j) = \frac{-f(y_{j-2})c(x_j)}{4 \cdot 3(\delta y)^2 y_{j-2}}, \quad P(x_j) = \frac{f(0)c(x_j)\delta y}{y_{j+2}y_{j+1}y_{j-1}y_{j-2}}$$

where we added the minus sign to account for the fact that f is negative for coordinates between y_{-2} and Γ_1. Imposing the symmetry constraint $P_1(y_j) = P_1(x_j)$ we get $c(x_j) = \frac{c_0 f(x_j)}{x_j}$, where c_0 is a constant. Similarly, the symmetry constraint for P_2 entails $P_2(y_j) = P_2(x_j)$. Finally, we can evaluate $P(x_j) = \frac{c_0 x_0 (x_0 - x_j)}{x_j^5} \delta x + O(\delta x^2)$ which, in the limit $\delta x \to 0$, means that

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

This evaluates to

$$x_0 \int_{x_0}^{\Gamma} \left(\frac{1}{x^5} - \frac{1}{x^6} \right) dx = \int_{x_0}^{\Gamma} \left(\frac{1}{x^4} - \frac{1}{x^5} \right) dx \Rightarrow x_0 = \frac{3}{5} \implies \epsilon = \frac{3}{5} - \frac{1}{2} = \frac{1}{10}$$

as expected. These calculations help us below when we explicitly find unitaries that solve the *advanced* moves which appear in this game. These unitaries, together with those for the basic moves and TEF, yield WCF protocols approaching bias $1/10$. Henceforth, we use the simpler notation introduced in Section 4.2 for clarity.

4.4.1 The $3 \to 2$ move and its validity

Our goal here is to find a unitary that solve the move taking 3 points to 2 points, as highlighted in Figure 7. To this end, we first setup some notation and write down the TEF constraint corresponding to a general 3 to 2 move, using it. We then show how to construct the appropriate unitary that satisfies this TEF constraint.

Recall from Definition 4.4 that

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

and let

$$|v_1\rangle = \frac{\sqrt{p_{g_3}} |g_2\rangle - \sqrt{p_{g_2}} |g_3\rangle}{N_{v_1}}, \quad |v_2\rangle = \frac{-\frac{(p_{g_2} + p_{g_3})}{\sqrt{p_{g_1}}} |g_1\rangle + \sqrt{p_{g_2}} |g_2\rangle + \sqrt{p_{g_3}} |g_3\rangle}{N_{v_2}}$$

where $N_{v_1}^2 = p_{g_3} + p_{g_2}$ and $N_{v_2}^2 = \frac{(p_{g_2} + p_{g_3})^2}{p_{g_1}} + p_{g_2} + p_{g_3}$. Also,

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

Now we define

$$|v_1'\rangle = \cos\theta |v_1\rangle + \sin\theta |v_2\rangle \text{ and } |v_2'\rangle = \sin\theta |v_1\rangle - \cos\theta |v_2\rangle,$$

where $\cos\theta \approx 1$, and the full unitary as

$$U = |w\rangle \langle v| + (\alpha |v_1'\rangle + \beta |w_1\rangle) \langle v_1'| + |v_2'\rangle \langle v_2'| + (\beta |v_1'\rangle - \alpha |w_1\rangle) \langle w_1| + |v\rangle \langle w|,$$

where $|\alpha|^2 + |\beta|^2 = 1$ for $\alpha, \beta \in \mathbb{C}$.[18] We need terms of the form $EU\,|g_i\rangle$ with $E = \mathbb{I}^{\{h_i\}}$. This entails that EU acts on the $\{|g_i\rangle\}$ space as

$$EUE_g = |w\rangle\langle v| + \beta\,|w_1\rangle\langle v_1'| = |w\rangle\langle v| + \beta\,|w_1\rangle\,(\cos\theta\,\langle v_1| + \sin\theta\,\langle v_2|),$$

where E_g is the projector on the $\{|g_i\rangle\}$ space. Consequently we have

$$EU\,|g_1\rangle = \frac{\sqrt{p_{g_1}}}{N_g}\,|w\rangle + \left[\cos\theta\cdot 0 - \sin\theta\frac{p_{g_2}+p_{g_3}}{\sqrt{p_{g_1}}N_{v_2}}\right]\beta\,|w_1\rangle$$

$$EU\,|g_2\rangle = \frac{\sqrt{p_{g_2}}}{N_g}\,|w\rangle + \left[\cos\theta\frac{\sqrt{p_{g_3}}}{N_{v_1}} + \sin\theta\frac{\sqrt{p_{g_2}}}{N_{v_2}}\right]\beta\,|w_1\rangle$$

$$EU\,|g_3\rangle = \frac{\sqrt{p_{g_3}}}{N_g}\,|w\rangle + \left[-\cos\theta\frac{\sqrt{p_{g_2}}}{N_{v_1}} + \sin\theta\frac{\sqrt{p_{g_3}}}{N_{v_2}}\right]\beta\,|w_1\rangle.$$

Recall that the TEF constraint requires

$$\sum x_{h_i}\,|h_i\rangle\langle h_i| - \sum x_{g_i}EU\,|g_i\rangle\langle g_i|\,U^\dagger E \geq 0$$

where the first sum becomes

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

in the $|w\rangle, |w_1\rangle$ basis. Since we plan to use the $3 \to 2$ move with one point on the axis, we take $x_{g_1} = 0$. Consequently we only need to evaluate

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

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

which means that the constraint equation becomes

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

Since this transition is average non-decreasing viz. $\langle x_h\rangle - \langle x_g\rangle \geq 0$ (see Lemma C.2 and Lemma 5.2), we set the off-diagonal elements of the matrix above to zero and show that the second diagonal element is positive. Setting the off-diagonal to zero one can obtain θ by solving the quadratic equation in terms of β although the expression is not particularly pretty. To establish existence and positivity we need to simplify our expressions.

---

18   There is some freedom in choosing U in the sense that $\alpha\,|v\rangle + \beta\,|w_1\rangle$ would also work instead of $\alpha\,|v_1'\rangle + \beta\,|w_1\rangle$ (in that case $|v\rangle\langle w|$ should be replaced by $|v_1\rangle\langle w|$), as these do not influence the constraint equation.

So far, everything was exact. To proceed, we write $\theta \frac{N_g}{N_{v_2}} = O(\delta y)$ at most (where $\delta y = \delta x$ is the lattice spacing) and we take δy to be small. Thus, to first order in $\theta \frac{N_g}{N_{v_2}}$, the constraints become

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

and

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

If our claim is wrong when we evaluate $\theta \frac{N_g}{N_{v_2}}$, we will get zero order terms but as we show later, indeed, $\theta \frac{N_g}{N_{v_2}} = O(\delta y^2)$. With respect to Figure 7 we have

$$P_2(y_{j+2}) = p_{h_2} = \frac{-f(y_{j+2})}{4 \cdot 3\delta y^2 y_{j+2}}, \quad P_1(y_{j+1}) = p_{g_3} = \frac{-f(y_{j+1})}{3 \cdot 2\delta y^2 y_{j+1}}$$

$$P_1(x_j) = p_{h_1} = \frac{-f(y_{j-1})}{3 \cdot 2\delta y^2 y_{j-1}}, \quad P_2(x_j) = p_{g_2} = \frac{-f(y_{j-2})}{4 \cdot 3\delta y^2 y_{j-2}}, \quad P(x_j) = p_{g_1} = \frac{f(0)\delta y}{y_{j+2} y_{j+1} y_{j-1} y_{j-2}},$$

where we assumed $f(0) > 0$ and $f(y) < 0$ for $y > y_0'$, $y_0' = y_0 + \delta y$, and we scaled by δy. We now convert all expressions to first order in δy:

$$f(y_{j+m}) = f(y_j) + \frac{\partial f}{\partial y} m \delta y + O(\delta y^2) \implies \frac{1}{y_{j+m}} = \frac{1}{y_j} - m \frac{\delta y}{y_j^2} + O(\delta y^2),$$

where $\frac{\partial f}{\partial y}$ is $\frac{\partial f(y)}{\partial y}\big|_{y_j}$. We define and evaluate

$$P_k^m = \frac{-f(y_{j+m})}{k\delta y^2 y_{j+m}} = \frac{1}{k y_j \delta y^2}\left[-f - m\delta y \left(\frac{\partial f}{\partial y} - \frac{f}{y_j} \right) + O(\delta y^2) \right],$$

where f means $f(y_j)$. In this notation

$$p_{h_2} = P_{12}^2, \ p_{h_1} = P_6^{-1} \quad \text{and} \quad p_{g_2} = P_{12}^{-2}, \ p_{g_3} = P_6^1.$$

With an eye on the off-diagonal condition we evaluate

$$P_{k_1}^{m_1} P_{k_2}^{m_2} = \frac{1}{k_1 k_2}\left(\frac{1}{y_j \delta y^2} \right)^2 \left[f^2 + f\delta y \left(\frac{\partial f}{\partial y} - \frac{f}{y_j} \right)(m_1 + m_2) + O(\delta y^2) \right]$$

and

$$P_{k_1}^{m_1} + P_{k_2}^{m_2} = \frac{1}{y_j \delta y^2}\left[-\left(\frac{1}{k_1} + \frac{1}{k_2} \right) f - \left(\frac{m_1}{k_1} + \frac{m_2}{k_2} \right) \delta y \left(\frac{\partial f}{\partial y} - \frac{f}{y_j} \right) + O(\delta y^2) \right].$$

Moreover, we have

$$\sqrt{p_{h_1} p_{h_2}} = \sqrt{P_{12}^2 P_6^{-1}} = \frac{1}{y_j \delta y^2}\sqrt{\frac{1}{12 \cdot 6}\left[f^2 + f\delta y \left(\frac{\partial f}{\partial y} - \frac{f}{y_j} \right) + O(\delta y^2) \right]}$$

$$N_h^2 = P_{12}^2 + P_6^{-1} = \frac{1}{4 y_j \delta y^2}\left[-f + O(\delta y^2) \right],$$

and similarly

$$\sqrt{p_{g_2}p_{g_3}} = \sqrt{P_{12}^{-2}P_6^1} = \frac{1}{y_j\delta y^2}\sqrt{\frac{1}{12\cdot 6}\left[f^2 - f\delta y\left(\frac{\partial f}{\partial y} - \frac{f}{y_j}\right) + O(\delta y^2)\right]}$$

$$N_g^2 = P_{12}^{-2} + P_6^1 + p_{g_1} = \frac{1}{4y_j\delta y^2}\left[-f + O(\delta y^2)\right] \text{ and } N_{v_1}^2 = \frac{1}{4y_j\delta y^2}\left[-f + O(\delta y^2)\right],$$

where we already neglected the terms that contribute to the ratio $\frac{N_g}{N_{v_2}}$ in higher than first order. Actually, for $\beta = 1$

$$\theta\frac{N_g}{N_{v_2}} = \frac{4\sqrt{\frac{1}{12\cdot 6}}(-3\delta y)\left[f(\mathcal{X} + \frac{\delta y}{2f}\left(\frac{\partial f}{\partial y} - \frac{f}{y_j}\right)) - f(\mathcal{X} - \frac{\delta y}{2f}\left(\frac{\partial f}{\partial y} - \frac{f}{y_j}\right)) + O(\delta y^2)\right]}{\langle x_g\rangle} = O(\delta y^2).$$

This shows that to first order the off-diagonal term is zero for $\theta = 0$. Now, we show that the second diagonal element is positive to first order in δy. Using the fact that $\theta\frac{N_g}{N_{v_2}} = O(\delta y^2)$, the positivity condition reads

$$\frac{p_{h_2}x_{h_1} + p_{h_1}x_{h_2}}{N_h^2} - \frac{p_{g_3}x_{g_2} + p_{g_2}x_{g_3}}{N_{v_1}^2} + O(\delta y^2) \geq 0,$$

which, in turn, becomes

$$\frac{P_{12}^2 y_{j-1} + P_6^{-1}y_{j+2}}{N_h^2} - \frac{P_6^1 y_{j-2} + P_{12}^{-2}y_{j+1}}{N_{v_1}^2} + O(\delta y^2) = 2\delta y + O(\delta y^2) \geq 0.$$

This establishes that U solves the $3 \to 2$ transition, for a closely spaced lattice. Note that only the proof of validity was done perturbatively to first order in δy. The unitary itself is known exactly, as θ can be obtained by solving the quadratic. Using $f(y) = (y_0' - y)(\Gamma_1 - y)(\Gamma_2 - y)$ we can implement the last two moves in Figure 7 as they constitute a $3 \to 1$ and a $2 \to 1$ merge. The only remaining task is to implement the $2 \to 2$ move of the last step, because previously we assumed $\sqrt{p_{g_2}} \neq 0$.

4.4.2   The $2 \to 2$ move and its validity

Using the notation from the previous section, our goal is now to construct a unitary that solves the 2 to 2 move as highlighted in Figure 8. To this end, consider the following unitary

$$U = |w\rangle\langle v| + (\alpha|v\rangle + \beta|w_1\rangle)\langle v_1| + |v\rangle\langle w| + (\beta|v\rangle - \alpha|w_1\rangle)\langle w_1|$$

where as before $|\alpha|^2 + |\beta|^2 = 1$,

$$|v\rangle = \frac{1}{N_g}\left(\sqrt{p_{g_1}}|g_1\rangle + \sqrt{p_{g_2}}|g_2\rangle\right), |w\rangle = \frac{1}{N_h}\left(\sqrt{p_{h_1}}|h_1\rangle + \sqrt{p_{h_2}}|h_2\rangle\right),$$

$$|v_1\rangle = \frac{1}{N_g}\left(\sqrt{p_{g_2}}|g_1\rangle - \sqrt{p_{g_1}}|g_2\rangle\right) \text{ and } |w_1\rangle = \frac{1}{N_h}\left(\sqrt{p_{h_2}}|h_1\rangle - \sqrt{p_{h_1}}|h_2\rangle\right).$$

We evaluate the constraint equation using

$$EU\,|g_1\rangle = \frac{\sqrt{p_{g_1}}\,|w\rangle + \beta e^{-i\phi_g}e^{i\phi_h}\sqrt{p_{g_2}}\,|w_1\rangle}{N_g}\,,\ EU\,|g_2\rangle = \frac{\sqrt{p_{g_2}}\,|w\rangle - \beta e^{-i\phi_g}e^{i\phi_h}\sqrt{p_{g_1}}\,|w_1\rangle}{N_g},$$

and

$$EU\,|g_1\rangle\langle g_1|\,U^\dagger E = \frac{1}{N_g^2}\begin{array}{c|cc} & \langle w| & \langle w_1| \\ \hline |w\rangle & p_{g_1} & \beta e^{i(\phi_h-\phi_g)}\sqrt{p_{g_2}p_{g_1}} \\ |w_1\rangle & \text{h.c.} & |\beta|^2\,p_{g_2} \end{array}$$

as

$$\begin{bmatrix} \langle x_h\rangle - \langle x_g\rangle & \frac{1}{N_g^2}\left[\sqrt{p_{h_1}p_{h_2}}(x_{h_1}-x_{h_2}) - \beta\sqrt{p_{g_1}p_{g_2}}(x_{g_1}-x_{g_2})\right] \\ \text{h.c.} & \frac{1}{N_g^2}\left[p_{h_2}x_{h_1} + p_{h_1}x_{h_2} - |\beta|^2\,(p_{g_2}x_{g_1} + p_{g_1}x_{g_2})\right] \end{bmatrix} \geq 0,$$

where we absorbed the phase freedom in β, a free parameter, which will be fixed shortly. We use the same strategy as above and take the first diagonal element to be zero. We must show that

$$\sqrt{\frac{p_{h_1}p_{h_2}}{p_{g_1}p_{g_2}}}\frac{(x_{h_1}-x_{h_2})}{(x_{g_1}-x_{g_2})} = \beta \leq 1,\ \text{and}\ \frac{1}{N_g^2}\left[p_{h_2}x_{h_1} + p_{h_1}x_{h_2} - |\beta|^2\,(p_{g_2}x_{g_1} + p_{g_1}x_{g_2})\right] \geq 0.$$

For this transition $f(y_{j-2}) = 0$, which we use to write

$$f(y_{j+k}) = \left.\frac{\partial f}{\partial y}\right|_{y_{j-2}}(k+2)\delta y = -(k+2)\alpha\delta y,\ \text{with}\ \alpha = -\left.\frac{\partial f}{\partial y}\right|_{y_{j-2}} = (\Gamma_1 - y_{j-2})(\Gamma_2 - y_{j-2}).$$

From Figure 8 we have

$$p_{h_1} = P_1(x_j) = \frac{-f(y_{j-1})}{3\cdot 2\delta y^2\,y_{j-1}} = \frac{\alpha + O(\delta y)}{6\delta y\,y_j},\ p_{h_2} = P_2(y_{j+2}) = \frac{-f(y_{j+2})}{4\cdot 3\delta y^2\,y_{j+2}} = \frac{\alpha + O(\delta y)}{3\delta y\,y_j}$$

$$x_{h_1} = y_{j-1},\ x_{h_2} = y_{j+2}$$

while

$$p_{g_1} = P(x_j) = \frac{f(0)\delta y}{y_{j+2}y_{j+1}y_{j-1}y_{j-2}} = \frac{f(0)\delta y + O(\delta y^2)}{y_j^4},\ p_{g_2} = P_1(y_{j+1}) = \frac{-f(y_{j+1})}{3\cdot 2\delta y^2\,y_{j+1}} = \frac{\alpha + O(\delta y)}{2\delta y\,y_j}$$

$$x_{g_1} = 0,\ x_{g_2} = y_{j+1}.$$
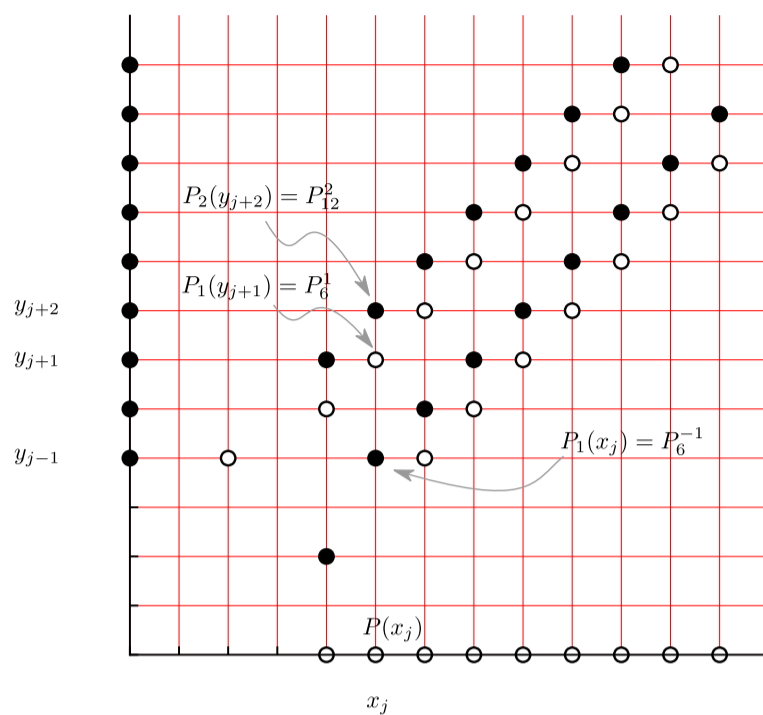
Figure 8. The first $2 \rightarrow 2$ transition

This entails

$$\beta = \sqrt{\frac{p_{h_1} p_{h_2}}{p_{g_1} p_{g_2}} \frac{(x_{h_1} - x_{h_2})}{(x_{g_1} - x_{g_2})}} = \sqrt{\frac{y_0' \alpha + O(\delta y)}{f(0)}} = \sqrt{\frac{(\Gamma_1 - y_{j-2})(\Gamma_2 - y_{j-2}) + O(\delta y)}{\Gamma_1 \Gamma_2}} \leq 1,$$

where we used $f(0) = y_0' \Gamma_1 \Gamma_2$ and the fact that δy is small compared to Γs. Analogously, for the second condition we have

$$\frac{1}{N_g^2} \left[p_{h_2} x_{h_1} + p_{h_1} x_{h_2} - |\beta|^2 \left(p_{g_2} x_{g_1} + p_{g_1} x_{g_2} \right) \right] \geq \frac{1}{N_g^2} \left[p_{h_2} x_{h_1} + p_{h_1} x_{h_2} - p_{g_2} x_{g_1} \right]$$

$$= \frac{1}{2\delta y N_g^2} \left[\alpha + O(\delta y) \right] = \frac{1}{2\delta y N_g^2} \left[(\Gamma_1 - y_{j-2})(\Gamma_2 - y_{j-2}) + O(\delta y) \right] \geq 0,$$

where the last step holds for δy small enough. The $2 \rightarrow 2$ move corresponding to the leftmost (see Figure 9) and bottom-most set of points can be shown to satisfy the TEF constraint similarly.
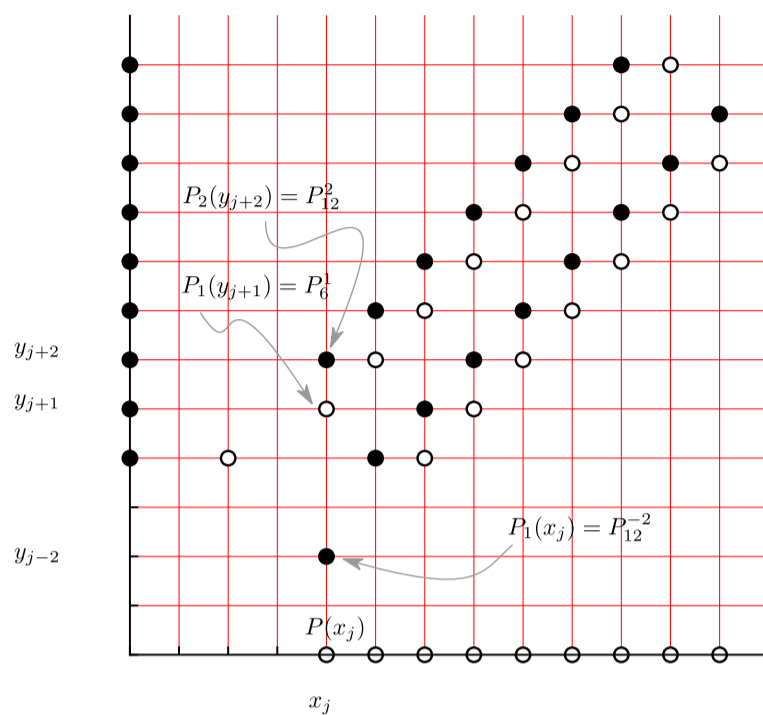
Figure 9. The final $2 \to 2$ transition.

5. Approaching Bias $\varepsilon(k) = 1/(4k + 2)$

While we succeeded at constructing the unitaries involved in the bias $1/10$ protocol, we did not follow any systematic procedure. Here, we construct the unitaries corresponding to the valid functions that characterise Mochon's point games (see Definition 5.1). These, together with the TEF, allow us to construct explicit WCF protocols with bias approaching $\epsilon(k) = 1/(4k + 2)$ for arbitrary integers $k > 0$.

Before we begin, we clarify the notation we use.

— For a Hermitian matrix A with spectral decomposition (including zero eigenvalues) $A = \sum_i a_i |i\rangle \langle i|$, we define the pseudo-inverse or the generalised inverse of A as

$$A^{\dashv} := \sum_{i:|a_i|>0} a_i^{-1} |i\rangle \langle i| .$$

— We write functions t with finite support in the following two ways (unless otherwise stated): (1) as $t = \sum_{i=1}^{n} p_i \llbracket x_i \rrbracket$ where we assume $p_i > 0$ for all $i \in \{1, 2 \ldots n\}$ and that $x_i \neq x_j$ for $i \neq j$ and (2) as $t = \sum_{i=1}^{n_h} p_{h_i} \llbracket x_{h_i} \rrbracket - \sum_{i=1}^{n_g} p_{g_i} \llbracket x_{g_i} \rrbracket$ where p_{h_i} and p_{g_i} are strictly positive and x_{h_i} and x_{g_i} are all distinct.

5.1   The f–assignments

Even though we already described Mochon's assignment (see Lemma 3.22) in Section 3, we now state it formally as an f-assignment, to facilitate the analysis that follows.

DEFINITION 5.1 (f-assignments). Given a set of real numbers $0 \leq x_1 < x_2 \cdots < x_n$ and a polynomial of degree at most $n - 2$ satisfying $f(-\lambda) \geq 0$ for all $\lambda \geq 0$, an f-*assignment* is given by the function

$$t = \sum_{i=1}^{n} \underbrace{\frac{-f(x_i)}{\prod_{j \neq i}(x_j - x_i)}}_{:=p_i} [\![x_i]\!] = h - g,$$

(up to a positive multiplicative factor) where h contains the positive part of t and g the negative part (without any common support), viz. $h = \sum_{i:p_i>0} p_i [\![x_i]\!]$ and $g = \sum_{i:p_i<0} (-p_i) [\![x_i]\!]$.
  — When f is a monomial, viz. has the form $f(x) = cx^q$, where $c > 0$ and $q \geq 0$ we call the assignment a *monomial assignment*. For $q = 0$ we call the assignment an f_0-*assignment*.
  — We say that an assignment is *balanced* if the number of points with negative weights, $p_i < 0$, equals the number of points with positive weights, $p_i > 0$. We say an assignment is *unbalanced* if it is not balanced.
  — We say that a monomial assignment is *aligned* if the degree of the monomial is an even number ($q = 2(b - 1), b \in \mathbb{N}$). We say that a monomial assignment is *misaligned* if it is not aligned.

An f_0-assignment starts with a point that has a negative weight regardless of the total number of points and thereafter, the sign alternates. With this as the base structure, working out the signs of the weights for monomial assignments gets easier. The only mathematical property that is needed to find an analytic solution, turns out to be the following.

LEMMA 5.2. *Fix integers $m \leq n - 2$ and $n \geq 2$. Consider an f-assignment of the form $t = \sum_i \frac{-(-x_i)^m}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!]$ for n points $0 \leq x_1 < \cdots < x_n$ and use it to implicitly define p_{h_i} and p_{g_i} as follows: $t = \sum_i (x_{h_i})^m p_{h_i} [\![x_{h_i}]\!] - \sum_i (x_{g_i})^m p_{g_i} [\![x_{g_i}]\!]$. Let $\langle x^l \rangle := \sum_i (x_{h_i})^l p_{h_i} - \sum_i (x_{g_i})^l p_{g_i}$. Then, $\langle x^l \rangle = 0$ for $0 \leq l \leq n - 2$. Further, $\langle x^{n-1} \rangle := \sum_i (x_{h_i})^{n-1} p_{h_i} - \sum_i (x_{g_i})^{n-1} p_{g_i} = (-1)^{m+n}$ which is strictly positive when $n + m$ is even (i.e. when t is unbalanced misaligned and balanced aligned (see Definition 5.1)).*

We defer the proofs to Appendix C.1.

Suppose that the f-assignment[19] can be decomposed into a sum of valid functions, and let us call these valid functions in the decomposition, *constituents*. Recall, from Section 4.2, that

---

valid functions are the same as TEF functions—functions that can be *solved* using some unitary U. Later, we show how to choose the decomposition such that the constituents can be *solved*. We call such a solution, an *effective solution*, and its definition is presented below.

DEFINITION 5.3 (Effectively Solving a function (extends Definition 4.4)). Given a finitely supported function $t = \sum_{i=1}^{n_h} p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n_g} p_{g_i} [\![x_{g_i}]\!]$ and $\{|g_1\rangle, |g_2\rangle \dots |g_{n_g}\rangle, |h_1\rangle, |h_2\rangle \dots |h_{n_h}\rangle\}$ an orthonormal basis, we say that a unitary matrix O *solves*[20] t if O satisfies the following: $O |v\rangle = |w\rangle$ and $X_h \geq E_h O X_g O^T E_h$ where $|v\rangle = \sum_{i=1}^{n_g} \sqrt{p_{g_i}} |g_i\rangle$, $|w\rangle = \sum_{i=1}^{n_h} \sqrt{p_{h_i}} |h_i\rangle$, $X_h = \sum_{i=1}^{n_h} x_{h_i} |h_i\rangle \langle h_i|$, $X_g = \sum_{i=1}^{n_g} x_{g_i} |g_i\rangle \langle g_i|$ and the projector $E_h = \sum_{i=1}^{n_h} |h_i\rangle \langle h_i|$. Moreover, we say that t has an *effective solution* if $t = \sum_{i \in I} t_i'$ and t_i' has a solution for all $i \in I$, where I is a finite set.

Before constructing these effective solutions, we briefly justify a claim we made in Section 2.2.2: to implement a valid function (and in particular, an f-assignment), it suffices to implement the constituent functions. The difficulty is that the constituent functions might be negative at various locations, where there are no points present. A similar difficulty was encountered while transforming a TIPG into a TDPG, and it was handled using *catalyst states* (as in [32, 3]). We outlined this procedure in Section 3.4 after Theorem 3.20. For the f-assignment of the TIPG, one can again use such a procedure: create the catalyst state, apply a scaled down version of the constituent functions, repeat until the f-function has been nearly implemented, and finally absorb the catalyst state with a vanishing increase in the final point. This results in a TDPG that uses only constituent functions. The unitary matrices for the constituent functions are, thus, sufficient to get a TDPG with the same bias as for the f-assignment. This motivates Definition 5.3 below. We can then apply the TEF from Section 4 to the TDPG and obtain a WCF protocol approaching the same bias as the TIPG that we started with, in the limit of infinite rounds of communication.

Returning to the construction of effective solutions, we first give a decomposition of an f-assignment into a sum of monomial assignments (for another possible decomposition, see Appendix C.2)

LEMMA 5.4 (f-assignment as a sum of monomials). *Consider a set of real coordinates satisfying* $0 \leq x_1 < x_2 \cdots < x_n$ *and let* $f(x) = (r_1 - x)(r_2 - x) \dots (r_k - x)$ *where* $k \leq n - 2$ *and* $r_i > 0$. *Let* $t = \sum_{i=1}^n p_i [\![x_i]\!]$ *be the corresponding f-assignment. Then, there exists* $\alpha_l \geq 0$, *such that*

$$t = \sum_{l=0}^{k} \alpha_l \left(\sum_{i=1}^{n} \frac{-(-x_i)^l}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!] \right).$$

In the following sections, we construct solutions to monomial assignments. The analysis there uses matrix inverses and having a coordinate equal to zero breaks the argument. Mochon's

---

TIPGs, however, do have support on the axes. To avoid these concerns, we translate (any of) Mochon's TIPG horizontally and vertically by an arbitrarily small amount $\delta_{\text{origin}} > 0$. Clearly, the corresponding final point (which encodes the bias) also only increases by the same arbitraryl small amount, δ_{origin}. We make two additional elementary observations: (i) the translated point game is also a TIPG as the moves involved in the resulting point game stay valid even after translation (see Lemma 5.5 below, with $c = \delta_{\text{origin}}$), and (ii) Mochon's f assignment on $\{x_1, \ldots x_n\}$ after translation by δ_{origin} can be seen as an f' assignment on the translated coordinates $\{x_1 + \delta_{\text{origin}}, \ldots, x_n + \delta_{\text{origin}}\}$ with $f'(x + \delta_{\text{origin}}) = f(x)$ (see Lemma 5.6 below, with $c = \delta_{\text{origin}}$). Together with the discussion preceding Lemma 5.4, we conclude that one can construct protocols corresponding to the translated point game, granted one can construct effective solutions to f' assignments on positive coordinates where f' is a polynomial with non-negative roots.

LEMMA 5.5. *Suppose* $t = \sum_{i=1}^{n_h} p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n_g} p_{g_i} [\![x_{g_i}]\!]$ *is solved by O. Then, for all* $c \geq 0$, $t = \sum_{i=1}^{n_h} p_{h_i} [\![x_{h_i} + c]\!] - \sum_{i=1}^{n_g} p_{g_i} [\![x_{g_i} + c]\!]$ *is also solved by O.*

PROOF SKETCH. Define $X_h := \sum_{i=1}^{n_h} x_{h_i} |h_i\rangle$, $X_g := \sum_{i=1}^{n_g} x_{g_i} |g_i\rangle$. If t is solved by O then we must have $X_h \geq E_h O X_g O^T E_h$. We show this implies $X_h + c\mathbb{I}_h \geq E_h O(X_g + c\mathbb{I}_g)O^T E_h$, where $\mathbb{I}_h := \sum_{i=1}^{n_h} |h_i\rangle \langle h_i|$ and $\mathbb{I}_g := \sum_{i=1}^{n_g} |g_i\rangle \langle g_i|$ which in turn means that t' is also solved by O. To this end, observe that

$$X_h \geq E_h O X_g O^T E_h \iff E_h(X_h - O X_g O^T)E_h \geq 0 \qquad \because X_h = E_h X_h E_h$$
$$\iff E_h(X_h + c\mathbb{I}_{hg} - O(X_g - c\mathbb{I}_{hg})O^T)E_h \geq 0 \iff X_h + c\mathbb{I}_h \geq E_h O(X_g + c\mathbb{I}_{hg})O^T E_h,$$

where $\mathbb{I}_{hg} := \mathbb{I}$. Further,

$$X_g + c\mathbb{I}_{hg} \geq X_g + c\mathbb{I}_g \implies E_h O(X_g + c\mathbb{I}_{hg})O^T E_h \geq E_h O(X_g + c\mathbb{I}_g)O^T E_h$$

which together yield

$$X_h \geq E_h O X_g O^T E_h \implies X_h + c\mathbb{I}_h \geq E_h O(X_g + c\mathbb{I}_g)O^T E_h.$$

as asserted. ∎

LEMMA 5.6. *Consider a set of real coordinates satisfying* $0 < x_1 + c < x_2 + c \cdots < x_n + c$ *where* $c > 0$ *and let* $f'(x) = (a_1 + c - x)(a_2 + c - x) \ldots (a_k + c - x)$. *Let* $t' = \sum_{i=1}^{n} p_i' [\![x_i']\!]$ *be the corresponding f-assignment (see Definition 5.1) with* $x_i' := x_i + c$. *Then* $p_i = p_i'$.

PROOF. Note that $f'(x_i + c) = f(x_i)$ and $\prod_{j \neq i}(x_j - x_i) = \prod_{j \neq i}(x_j' - x_i)$. Using this and the definition of f-assignment (see Definition 5.1), it follows that $p_i' = p_i$. ∎

Henceforth, we restrict ourselves to f-assignments defined on positive coordinates. Having decomposed the f-assignment into a sum of monomial assignments, we now give a solution

to monomial assignments. We start with f_0-assignments (monomial assignment where the monomial is a constant) to convey the key idea behind the construction and subsequently build on this idea to solve the four types of monomial assignments.

5.2   Solution to the f_0-assignment

Let us solve the f_0-assignment. We first look at the balanced case, where the number of points involved, $2n$, is even. This corresponds to an $n \to n$ transition, i.e. a transition from n initial points to n final points.

5.2.1   The balanced case

PROPOSITION 5.7 (Solution to balanced f_0-assignments). *Let*

— $t = \sum_{i=1}^n p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^n p_{g_i} [\![x_{g_i}]\!]$ *be an f_0-assignment over $\{x_1, x_2 \ldots x_{2n}\}$*
— $\{|h_1\rangle, |h_2\rangle \ldots |h_n\rangle, |g_1\rangle, |g_2\rangle \ldots |g_n\rangle\}$ *be an orthonormal basis, and*
— *finally*

$$X_h := \sum_{i=1}^n x_{h_i} |h_i\rangle \langle h_i| \doteq diag(x_{h_1}, \ldots x_{h_n}, \underbrace{0, \ldots 0}_{n\text{-}zeros}), X_g := \sum_{i=1}^n x_{g_i} |g_i\rangle \langle g_i| \doteq diag(\underbrace{0, \ldots 0}_{n\text{-}zeros}, x_{g_1}, \ldots x_{g_n}),$$

$$|w\rangle := \sum_{i=1}^n \sqrt{p_{h_i}} |h_i\rangle \doteq (\sqrt{p_{h_1}}, \ldots \sqrt{p_{h_n}}, \underbrace{0, \ldots 0}_{n\text{-}zeros})^T, |v\rangle := \sum_{i=1}^n \sqrt{p_{g_i}} |g_i\rangle \doteq (\underbrace{0, \ldots 0}_{n\text{-}zeros}, \sqrt{p_{g_1}}, \ldots \sqrt{p_{g_n}})^T.$$

Then,

$$O := \sum_{i=0}^{n-1} \left(\frac{\Pi^{\perp}_{h_{i-1}} (X_h)^i |w\rangle \langle v| (X_g)^i \Pi^{\perp}_{g_{i-1}}}{\sqrt{c_{h_i} c_{g_i}}} + h.c. \right)$$

satisfies $X_h \geq E_h O X_g O^T E_h$ and $O|v\rangle = |w\rangle$, where $E_h := \sum_{i=1}^n |h_i\rangle \langle h_i|$, $\Pi^{\perp}_{h_{-1}} = \Pi^{\perp}_{g_{-1}} = \mathbb{I}$,

$$\Pi^{\perp}_{h_i} := \text{projector orthogonal to } span\{(X_h)^i |w\rangle, (X_h)^{i-1} |w\rangle, \ldots |w\rangle\}, c_{h_i} := \langle w| (X_h)^i \Pi^{\perp}_{h_{i-1}} (X_h)^i |w\rangle,$$

and analogously

$$\Pi^{\perp}_{g_i} := \text{projector orthogonal to } span\{(X_g)^i |v\rangle, (X_g)^{i-1} |v\rangle, \ldots |v\rangle\}, c_{g_i} := \langle v| (X_g)^i \Pi^{\perp}_{g_{i-1}} (X_g)^i |v\rangle.$$

PROOF. Using Lemma 5.2 for $2n$ points, we get

$$\langle x^k \rangle = 0 \quad \text{for} \quad k \in \{0, 1, 2 \ldots, 2n - 2\}, \tag{8}$$

and

$$\langle x^{2n-1} \rangle > 0. \tag{9}$$

We define the basis of interest here, essentially using the Gram-Schmidt method. Let

$$
\begin{aligned}
|w_0\rangle &:= |w\rangle \\
|w_1\rangle &:= \frac{(\mathbb{I} - |w_0\rangle \langle w_0|)(X_h)|w\rangle}{\sqrt{c_{h_1}}} \\
&\vdots \\
|w_k\rangle &:= \frac{\left(\mathbb{I} - \sum_{i=0}^{k-1} |w_i\rangle \langle w_i|\right)(X_h)^k |w\rangle}{\sqrt{c_{h_k}}}.
\end{aligned}
\tag{10}
$$

We indicate the term with the highest power of X_h appearing in $|w_k\rangle$ by

$$
\mathcal{M}(|w_k\rangle) = \left\langle x_h^{2k}\right\rangle \cdot (X_h)^k |w\rangle
$$

where the scalar factor represents the dependence on the highest power of x_h (appearing as $\left\langle x_h^l\right\rangle$) in $|w_k\rangle$. For instance, here the $\left\langle x_h^{2k}\right\rangle$ factor comes from $\sqrt{c_{h_k}}$. Note that the projectors can be expressed in terms of these vectors more concisely,

$$
\Pi_{h_i} := \mathbb{I} - \Pi_{h_i}^{\perp} = \sum_{j=0}^{i} |w_j\rangle \langle w_j|.
$$

It also follows that O can be re-written as $O = \sum_{j=0}^{n-1}\left(|w_j\rangle \langle v_j| + |v_j\rangle \langle w_j|\right)$, where $|v_j\rangle$ is analogously defined. It is evident that $O|v\rangle = |w\rangle$. Let $D = X_h - E_h O X_g O^T E_h$ and note that $\left\langle v_j \middle| D \middle| v_i\right\rangle = 0$ (because $X_h |v_i\rangle = 0$ and $E_h |v_i\rangle = 0$[21]). We assert that it has the following rank-1 form

$$
D = \begin{bmatrix} 0 & \cdots & & 0 \\ \vdots & \ddots & & \vdots \\ 0 & \cdots & & \langle w_{n-1}| D |w_{n-1}\rangle \end{bmatrix}
$$

in the $(|w_0\rangle, |w_1\rangle, \ldots |w_{n-1}\rangle)$ basis, together with $\langle w_{n-1}| D |w_{n-1}\rangle > 0$. To see this, we simply compute

$$
\langle w_i| D |w_j\rangle = \langle w_i| X_h |w_j\rangle - \langle w_i| O X_g O^T |w_j\rangle = \langle w_i| X_h |w_j\rangle - \langle v_i| X_g |v_j\rangle.
$$

For (i, j) for any $0 \le i, j \le n-1$ except for the case where both $i = j = n-1$, the two terms are the same. This is because the term with the highest possible power l (of $\left\langle x^l\right\rangle$) in $\langle w_i| X_h |w_j\rangle$ can be deduced by observing

$$
\mathcal{M}(\langle w_i|) X_h \mathcal{M}(|w_j\rangle) = \left\langle x_h^{2i}\right\rangle \cdot \left\langle x_h^{2j}\right\rangle \cdot \left\langle x_h^{i+j+1}\right\rangle.
\tag{11}
$$

For the analogous expression with gs to be the same, we must have $2i, 2j$ and $i + j + 1 \le 2n - 2$, using Equation (8). The first two conditions are always satisfied (for $0 \le i, j \le n-1$). The last can only be violated when $i = j = n-1$. This establishes that the matrix has the asserted form.

---

21   The conclusion holds even without the projector as O maps $\text{span}(|v_1\rangle, |v_2\rangle, \ldots |v_n\rangle)$ to $\text{span}(|w_1\rangle, |w_2\rangle \ldots |w_n\rangle)$ on which X_g has no support.

To prove the positivity of $\langle w_{n-1}| D |w_{n-1}\rangle$, consider $\langle w_{n-1}| X_h |w_{n-1}\rangle$ and $\langle v_{n-1}| X_g |v_{n-1}\rangle$. When these terms are expanded in powers of $\langle x_h^k\rangle$ and $\langle x_g^k\rangle$ respectively, only terms with $k > 2n - 2$ would remain; the others would get canceled due to Equation (8). From Equation (10) it follows that

$$\langle w_{n-1}| D |w_{n-1}\rangle = \frac{1}{c_{h_{n-1}}} \langle w| (X_h)^{2n-2+1} |w\rangle - \frac{1}{c_{g_{n-1}}} \langle v| (X_g)^{2n-2+1} |v\rangle$$

and it is not hard to see that $c_{h_{n-1}} = c_{h_{n-1}}(\langle x_h^{2n-2}\rangle, \langle x_h^{2n-3}\rangle, \ldots, \langle x_h^1\rangle)$ does not depend on $\langle x_h^{2n-1}\rangle$ (and analogously for $c_{g_{n-1}}$). Also, $c_{h_{n-1}} = c_{g_{n-1}} =: c_{n-1}$. We thus have

$$\langle w_{n-1}| D |w_{n-1}\rangle = \frac{\langle x_h^{2n-1}\rangle}{c_{n-1}} > 0$$

using Equation (9). Hence, $X_h - E_h O X_g O^T E_h \geq 0$.

In the above, we assumed $\text{span}\{|w\rangle, X_h |w\rangle, X_h^2 |w\rangle, \ldots, X_h^n |w\rangle\}$ equals $\text{span}\{|h_1\rangle, |h_2\rangle \ldots |h_n\rangle\}$ which is justified by Lemma C.1. ∎

5.2.2 The unbalanced case

We now consider unbalanced f_0-assignments. We start by reviewing the result we just proved from a slightly different perspective. This helps us see where the previous analysis fails, when applied in the present case. We write $D_{ij} = \langle w_i| D |w_j\rangle$, and note that the maximum power, l, which appears as $\langle x_{g/h}^l\rangle$ is given by $\max\{2i, 2j, i + j + 1\}$. This yields a matrix with each term depending on the power as

$$D = \begin{bmatrix} D_{00}(\langle x\rangle) & & & \\ D_{10}(\langle x^2\rangle, \ldots) & D_{11}(\langle x^3\rangle, \ldots) & & \text{h.c.} \\ D_{20}(\langle x^4\rangle, \ldots) & D_{21}(\langle x^4\rangle, \ldots) & D_{22}(\langle x^5\rangle, \ldots) & \\ & & & \ddots \end{bmatrix}.$$

We represent this dependence as

$$\mathcal{M}(D) = \begin{bmatrix} \langle x\rangle & & & \\ \langle x^2\rangle & \langle x^3\rangle & & \\ \langle x^4\rangle & \langle x^4\rangle & \langle x^5\rangle & \\ & & & \ddots \end{bmatrix}.$$

For concreteness, consider the balanced f_0-case over $\{x_1, x_2, x_3, x_4\}$, where $\langle x\rangle = \langle x^2\rangle = 0$ and $\langle x^3\rangle > 0$. For this two-dimensional case, we have

$$\mathcal{M}(D) = \begin{bmatrix} 0 & 0 \\ 0 & \langle x^3\rangle \end{bmatrix} \geq 0.$$

Using the same method for an f_0-assignment over $\{x_1, x_2 \ldots x_5\}$, we have $\langle x \rangle = \langle x^2 \rangle = \langle x^3 \rangle = 0$ and $\langle x^4 \rangle > 0$, and trying to solve in three dimensions, we would obtain

$$\mathcal{M}(D) = \begin{bmatrix} 0 & 0 & \langle x^4 \rangle \\ 0 & 0 & \langle x^4 \rangle \\ \langle x^4 \rangle & \langle x^4 \rangle & \langle x^5 \rangle \end{bmatrix} \tag{12}$$

which does not seem to work directly. It turns out that the projector appearing in the TEF constraint, removes the troublesome part and yields a zero matrix. This unbalanced assignment takes three points to two points. We define $X_h := \mathrm{diag}(x_{h_1}, x_{h_2}, 0, 0, 0)$, $|w\rangle = (\sqrt{p_{h_1}}, \sqrt{p_{h_2}}, 0, 0, 0)$ along with $|w_0\rangle := |w\rangle$ and $|w_1\rangle := (\mathbb{I} - |w_0\rangle \langle w_0|) X_h |w_0\rangle$. We can write $E_h = \sum_{i=0}^{1} |w_i\rangle \langle w_i|$ and have the same unitary as before, except that now $|v_2\rangle$ is left unchanged, i.e. $O = \sum_{i=0}^{1} |w_i\rangle \langle v_i| + |v_2\rangle \langle v_2|$. We can show that $D' = X_h - E_h O X_g O^T E_h \geq 0$ because every vector $|\psi\rangle$ in the subspace $\mathrm{span}\{|v_0\rangle, |v_1\rangle, |v_2\rangle\}$ satisfies $D' |\psi\rangle = 0$ (as $X_h |\psi\rangle = 0$ and $E_h |\psi\rangle = 0$). This entails that it suffices to restrict to a 2×2 matrix in $\mathrm{span}\{|w_0\rangle, |w_1\rangle\}$. From 12 this is zero, hence $D' = 0$. By generalizing this example, we can obtain the solution for an unbalanced f_0-assignment, as presented in the following Proposition:

PROPOSITION 5.8 (Solution to unbalanced f_0-assignments). *Let*

— $t = \sum_{i=1}^{n-1} p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} p_{g_i} [\![x_{g_i}]\!]$, *be an f_0-assignment over $0 < x_1 < x_2 \cdots < x_{2n-1}$*

— $\{|h_1\rangle, |h_2\rangle \ldots |h_{n-1}\rangle, |g_1\rangle, |g_2\rangle \ldots |g_n\rangle\}$ *be an orthonormal basis, and*

— *finally*

$$X_h := \sum_{i=1}^{n-1} x_{h_i} |h_i\rangle \langle h_i| \doteq \mathrm{diag}(x_{h_1}, \ldots x_{h_{n-1}}, \underbrace{0, \ldots 0}_{n \text{ zeros}}), X_g := \sum_{i=1}^{n} x_{g_i} |g_i\rangle \langle g_i| \doteq \mathrm{diag}(\underbrace{0, \ldots 0}_{n-1 \text{ zeros}}, x_{g_1}, \ldots, x_{g_n}),$$

$$|w\rangle := \sum_{i=1}^{n-1} \sqrt{p_{h_i}} |h_i\rangle \doteq (\sqrt{p_{h_1}}, \ldots \sqrt{p_{h_{n-1}}}, \underbrace{0, \ldots 0}_{n \text{ zeros}})^T, |v\rangle := \sum_{i=1}^{n} \sqrt{p_{g_i}} |g_i\rangle \doteq (\underbrace{0, \ldots 0}_{n-1 \text{ zeros}}, \sqrt{p_{g_1}}, \ldots \sqrt{p_{g_n}})^T$$

— *and $E_h := \sum_{i=1}^{n-1} |h_i\rangle \langle h_i|$.*

Then,

$$O := \left(\sum_{i=0}^{n-2} \frac{\Pi_{h_{i-1}}^{\perp} (X_h)^i |w\rangle \langle v| (X_g)^i \Pi_{g_{i-1}}^{\perp}}{\sqrt{c_{h_i} c_{g_i}}} + h.c. \right) + \frac{\Pi_{g_{n-2}}^{\perp} (X_g)^{n-1} |v\rangle \langle v| (X_g)^{n-1} \Pi_{g_{n-2}}^{\perp}}{c_{g_i}}$$

satisfies $X_h \geq E_h O X_g O^T E_h$ and $E_h O |v\rangle = |w\rangle$, where $\Pi_{h_{-1}}^{\perp} = \Pi_{g_{-1}}^{\perp} = \mathbb{I}$,

$\Pi_{h_i}^{\perp} :=$ *projector orthogonal to $\mathrm{span}\{(X_h)^i |w\rangle, (X_h)^{i-1} |w\rangle, \ldots |w\rangle\}$, $c_{h_i} := \langle w| (X_h)^i \Pi_{h_{i-1}}^{\perp} (X_h)^i |w\rangle$,*

and analogously

$\Pi_{g_i}^{\perp} :=$ *projector orthogonal to $\mathrm{span}\{(X_g)^i |v\rangle, (X_g)^{i-1} |v\rangle, \ldots |v\rangle\}$, $c_{g_i} := \langle v| (X_g)^i \Pi_{g_{i-1}}^{\perp} (X_g)^i |v\rangle$.*

PROOF. In this case, we use Lemma 5.2 for $2n - 1$ points. We have

$$\langle x^k \rangle = 0 \tag{13}$$

but this time, $k \in \{0, 1, \ldots 2n - 3\}$ and $\langle x^{2n-2} \rangle > 0$. We define the basis similarly by setting $|w_0\rangle := |w\rangle$ and for all $k \in \mathbb{Z}$ satisfying $0 \le k \le n - 2$ we have

$$|w_k\rangle := \frac{\Pi^{\perp}_{h_{k-1}} (X_h)^k |w\rangle}{\sqrt{c_{h_k}}} = \frac{\left(\mathbb{I} - \sum_{i=0}^{k-1} |w_i\rangle \langle w_i| \right) (X_h)^k |w\rangle}{\sqrt{c_{h_k}}}.$$

We also define $|v_0\rangle := |v\rangle$ and for all $k \in \mathbb{Z}$ satisfying $0 \le k \le n - 1$ we have

$$|v_k\rangle := \frac{\Pi^{\perp}_{g_{k-1}} (X_g)^k |v\rangle}{\sqrt{c_{g_k}}} = \frac{\left(\mathbb{I} - \sum_{i=0}^{k-1} |v_i\rangle \langle v_i| \right) (X_g)^k |v\rangle}{\sqrt{c_{h_k}}}.$$

This means that $O = \sum_{i=0}^{n-2} (|w_i\rangle \langle v_i| + |v_i\rangle \langle w_i|) + |v_n\rangle \langle v_n|$ and so $E_h O |v\rangle = |w\rangle$ follows directly. To establish $D := X_h - E_h O X_g O^T E_h \ge 0$, it suffices to show $\langle w_i| D |w_j\rangle \ge 0$ for $i, j \in \mathbb{Z}$ satisfying $0 \le i, j \le n - 2$. Just as in the balanced case, this is because $D |v_i\rangle = 0$, as $X_h |v_i\rangle = 0$ and $E_h |v_i\rangle = 0$. As before, we denote the highest-power term of X_h appearing in $|w_k\rangle$, for k in $\{0, 1 \ldots n - 2\}$, by

$$\mathcal{M}(|w_k\rangle) = \langle x_h^{2k} \rangle \cdot (X_h)^k |w\rangle$$

and analogously, the highest power of X_g appearing in $|v_k\rangle$ for k in $\{0, 1, \ldots n - 2\}$, by

$$\mathcal{M}(|v_k\rangle) = \langle x_g^{2k} \rangle \cdot (X_g)^k |v\rangle.$$

Again, the highest power l of $\langle x^l \rangle$ in $\langle w_i| D |w_j\rangle$ is $\max\{2j, 2i, i + j + 1\}$ which can be deduced by evaluating

$$\mathcal{M}(\langle w_i|) X_h \mathcal{M}(|w_j\rangle) = \langle x_h^{2j} \rangle \cdot \langle x_h^{2i} \rangle \cdot \langle x_h^{i+j+1} \rangle, \text{ and similarly}$$

$$\mathcal{M}(\langle v_i|) E_h O X_g O E_h \mathcal{M}(|v_i\rangle) = \langle x_g^{2j} \rangle \cdot \langle x_g^{2i} \rangle \cdot \langle x_g^{i+j+1} \rangle.$$

The highest possible power is attained for $i = j = n - 2$. This yields $2n - 3$ and thus, using Equation (13), we conclude that $\langle w_i| D |w_j\rangle = 0$ for all $0 \le i, j \le n - 2$. ∎

5.3   Solution to monomial assignments

As described in Section 5.1, there are four different types of monomial assignments depending on whether they are balanced or unbalanced and aligned or misaligned (nomenclature is justified below). While one could find a single expression for all of them, it does not seem to aid clarity. We, therefore, present the four solutions separately. To go beyond the solutions to f_0-assignments, we additionally need to use pseudo-inverses X_h^{-1} and X_g^{-1}. However, the key idea is essentially unchanged.

5.3.1 The balanced case

Even (resp. odd) monomials align properly (resp. do not align properly) at the bottom (see Figure 10a). This justifies our choice to call them aligned (resp. misaligned).
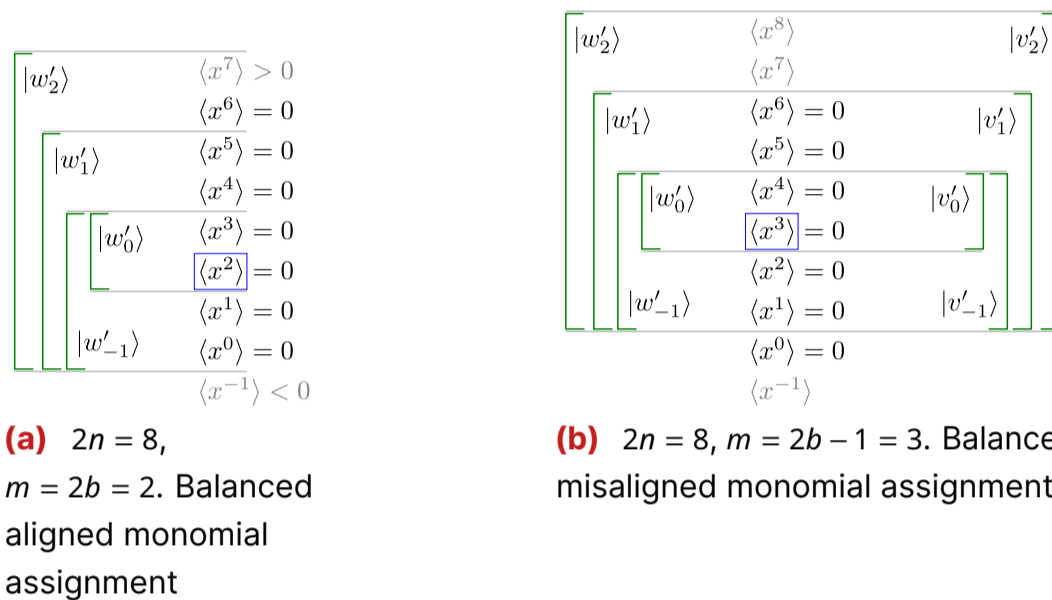

(a) $2n = 8$, $m = 2b = 2$. Balanced aligned monomial assignment

(b) $2n = 8$, $m = 2b − 1 = 3$. Balanced misaligned monomial assignment

Figure 10. Balanced monomial assignments. These are explained after the proof of Proposition 5.9.

PROPOSITION 5.9 (Solution to balanced aligned monomial assignments). *Let*

— *$m = 2b$ be an even non-negative integer*
— *$t = \sum_{i=1}^{n} x_{h_i}^m p_{h_i} [\![x_{h_i}]\!] − \sum_{i=1}^{n} x_{g_i}^m p_{g_i} [\![x_{g_i}]\!]$, be a monomial assignment over $0 < x_1 < x_2 \cdots < x_{2n}$*
— *$\{|h_1\rangle, |h_2\rangle \ldots |h_n\rangle, |g_1\rangle, |g_2\rangle \ldots |g_n\rangle\}$ be an orthonormal basis, and*
— *finally*

$$X_h := \sum_{i=1}^{n} x_{h_i} |h_i\rangle \langle h_i| \doteq diag(x_{h_1}, \ldots x_{h_n}, \underbrace{0, \ldots 0}_{n \ zeros}), X_g := \sum_{i=1}^{n} x_{g_i} |g_i\rangle \langle g_i| \doteq diag(\underbrace{0, \ldots 0}_{n \ zeros}, x_{g_1}, \ldots x_{g_n}),$$

$$|w\rangle := \sum_{i=1}^{n} \sqrt{p_{h_i}} |h_i\rangle \doteq (\sqrt{p_{h_1}}, \ldots \sqrt{p_{h_n}}, \underbrace{0, \ldots 0}_{n \ zeros})^T \ and \ |w'\rangle := (X_h)^b |w\rangle,$$

$$|v\rangle := \sum_{i=1}^{n} \sqrt{p_{g_i}} |g_i\rangle \doteq (\underbrace{0, \ldots 0}_{n \ zeros}, \sqrt{p_{g_1}}, \ldots \sqrt{p_{g_n}})^T \ and \ |v'\rangle := (X_g)^b |v\rangle.$$

Then,

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

satisfies $X_h \geq E_h O X_g O^T E_h$ and $E_h O |v'\rangle = |w'\rangle$, where we write $(X_{h/g})^{-k}$ instead of $(X_{h/g}^{-1})^k$ (for $k > 0$), $E_h := \sum_{i=1}^n |h_i\rangle \langle h_i|, c_{h_i} := \langle w'| (X_h)^i \Pi_{h_i}^{\perp} (X_h)^i |w'\rangle$

$$\Pi_{h_i}^{\perp} := \begin{cases} \text{projector orthogonal to } \mathrm{span}\{(X_h)^{-|i|+1} |w'\rangle, (X_h)^{-|i|+2} |w'\rangle \ldots, |w'\rangle\} & i < 0 \\ \text{projector orthogonal to } \mathrm{span}\{(X_h)^{-b} |w'\rangle, (X_h)^{-b+1} |w'\rangle, \ldots (X_h)^{i-1} |w'\rangle\} & i > 0 \\ \mathbb{I} & i = 0, \end{cases}$$

and analogously $c_{g_i} := \langle v'| (X_g)^i \Pi_{g_i}^{\perp} (X_g)^i |v'\rangle$ and

$$\Pi_{g_i}^{\perp} := \begin{cases} \text{projector orthogonal to } \mathrm{span}\{(X_g)^{-|i|+1} |v'\rangle, (X_g)^{-|i|+2} |v'\rangle \ldots, |v'\rangle\} & i < 0 \\ \text{projector orthogonal to } \mathrm{span}\{(X_g)^{-b} |v'\rangle, (X_g)^{-b+1} |v'\rangle, \ldots (X_g)^{i-1} |v'\rangle\} & i > 0 \\ \mathbb{I} & i = 0. \end{cases}$$

PROOF. The orthonormal basis of interest here is

$$|w_i'\rangle := \frac{\Pi_{h_i}^{\perp} (X_h)^i |w'\rangle}{\sqrt{c_{h_i}}}, \text{ which entails} \tag{14}$$

$$\Pi_{h_i}^{\perp} = \begin{cases} \mathbb{I}_h & i = 0 \\ \mathbb{I}_h - \sum_{j=i+1}^0 |w_j'\rangle \langle w_j'| & i < 0 \\ \mathbb{I}_h - \sum_{j=-b}^{i-1} |w_j'\rangle \langle w_j'| & i > 0 \end{cases} \tag{15}$$

where $\mathbb{I}_h := E_h$. We define $|v_i'\rangle$ and $\Pi_{g_i}^{\perp}$ analogously. Here, we keep track of both the highest and lowest power, l in $\langle w'| X_h^l |w'\rangle$ and $\langle v'| X_g^l |v'\rangle$, which appear in the matrix elements $\langle w_i'| D |w_j'\rangle$. To this end, we use $\langle x_h^l \rangle' := \langle w'| X_h^l |w'\rangle = \langle w| X_h^{l+2b} |w\rangle$ and $\langle x_g^l \rangle' := \langle v'| X_g^l |v'\rangle = \langle v| X_g^{l+2b} |v\rangle$. We denote the minimum and maximum powers, l, by

$$\mathcal{M}(|w_i'\rangle) = \begin{cases} \left(\langle x_h^0 \rangle' |w'\rangle, \langle x_h^0 \rangle' |w'\rangle \right) & i = 0 \\ \left(\left\langle x_h^{-2|i|} \right\rangle' (X_h)^{-|i|} |w'\rangle, \langle x_h^0 \rangle' |w'\rangle \right) & i < 0 \\ \left(\langle x_h^{-2b} \rangle' (X_h)^{-b} |w'\rangle, \langle x_h^{2i} \rangle' (X_h)^i |w'\rangle \right) & i > 0, \end{cases}$$

and we define $D := X_h - E_h O X_g O^T E_h \doteq \langle w_i'| (X_h - E_h O X_g O^T E_h) |w_j'\rangle$, as usual. It suffices to restrict to the span of the $\{|w_i'\rangle\}$ basis because $X_h |v_i'\rangle = 0$ and $E_h |v_i'\rangle = 0$. The lowest power, l, appearing in D is attained for $i = j = -b$ (as $-b \leq i, j \leq n - b - 1$). This can be evaluated to be $-2b$ by observing that

$$\mathcal{M}(\langle w_{-b}'|) X_h \mathcal{M}(|w_{-b}'\rangle) = \left(\langle x_h^{-2b} \rangle' \langle x_h^{-2b} \rangle' \langle x_h^{-2b+1} \rangle', \langle x_h^0 \rangle' \langle x_h^0 \rangle' \langle x_h \rangle' \right),$$

where we multiplied component-wise. To find the highest power, l, in the matrix D, note that for $i, j > 0$ we have

$$\mathcal{M}(\langle w_i'|) X_h \mathcal{M}(|w_j'\rangle) = \left(\langle x_h^{-2b} \rangle' \langle x_h^{-2b+1} \rangle' \langle x_h^{-2b} \rangle', \langle x_h^{2i} \rangle' \langle x_h^{2j} \rangle' \langle x_h^{i+j+1} \rangle' \right)$$

so $l = \max\{2i, 2j, i+j+1\}$. As argued for the f_0-assignment, $l = 2n - 2b - 1$ for $i = j = n - b - 1$, otherwise $l < 2n - 2b - 1$. Thus, only the $D_{n-b-1,n-b-1}$ term in D, depends on $\langle x_h^{2n-2b-1}\rangle'$. All other terms, at most, depend on $\langle x_h^{-2b}\rangle', \langle x_h^{-2b+1}\rangle', \dots \langle x_h^{2n-2b-2}\rangle'$, i.e. $\langle x_h^0\rangle, \langle x_h^1\rangle, \dots \langle x_h^{2n-2}\rangle$. The analogous argument for $\langle v_i'| X_g |v_j'\rangle$, the observation that $\langle w_i'| D |w_j'\rangle = \langle w_i'| X_h |w_j'\rangle - \langle v_i'| X_g |v_j'\rangle$, and the fact that $\langle x^0\rangle = \langle x^1\rangle = \dots = \langle x^{2n-2}\rangle = 0$ entail that these terms vanish. It remains to show that $D_{n-b-1,n-b-1} \geq 0$. Noting that in $\langle w_{n-b-1}'| D |w_{n-b-1}'\rangle$, the only term which would not get cancelled due to the aforesaid reasoning, must come from the part of $|w_{n-b-1}'\rangle$ containing $X_h^{n-b-1} |w'\rangle$. It suffices to show that the coefficient of this term is positive because we know that $\langle x^{2n-2b-1}\rangle' = \langle x^{2n-1}\rangle > 0$. We know this coefficient to be exactly $1/c_{h_{n-b-1}}$ (see Equation (15) and Equation (14)) establishing that $D \geq 0$.   ∎

To proceed further, it is helpful to have a more concise way of viewing the proof. Let us consider a concrete example of a balanced aligned monomial assignment with $2n = 8$ and $m = 2b = 2$ (see Figure 10a). We represent the range of dependence of $\langle w_0'| X_h |w_0'\rangle$ on $\langle x_h^l\rangle$ diagrammatically by enclosing in a left bracket, the terms $\langle x^3\rangle = \langle x\rangle'$ and $\langle x^2\rangle = \langle x^0\rangle'$ (replacing $|w\rangle$ with $|w_0'\rangle$) and writing $|w_0'\rangle$ next to it. Similarly, for $|w_{-1}'\rangle, |w_1'\rangle$ and $|w_2'\rangle$ we enclose in a left bracket, the terms

$$\{\langle x^0\rangle, \langle x^1\rangle, \langle x^2\rangle, \langle x^3\rangle\} = \left\{\langle x^{-2}\rangle', \langle x^{-1}\rangle', \dots \langle x\rangle'\right\},$$

$$\{\langle x^0\rangle, \langle x^1\rangle, \dots, \langle x^5\rangle\} = \left\{\langle x^{-2}\rangle', \langle x^{-1}\rangle', \dots \langle x^3\rangle'\right\},$$

$$\text{and } \{\langle x^0\rangle, \langle x^1\rangle, \dots \langle x^7\rangle\} = \left\{\langle x^{-2}\rangle', \langle x^{-1}\rangle', \dots \langle x^5\rangle'\right\},$$

respectively. The highest power l of $\langle x_h^l\rangle$ that appears in $\langle w_i'| X_h |w_j'\rangle$ is $l = 7$ when (and only when) $i = j = 2$. Thus, the matrix D, restricted to the subspace spanned by the $\{|w_i'\rangle\}$ basis (again, we can safely ignore the subspace $\text{span}\{|v_i'\rangle\}$ because $D |v_i'\rangle = 0$), has only one non-zero entry which we saw was positive as $\langle x^7\rangle > 0$.

A direct extension of this analysis to the balanced misaligned monomial assignment fails, as we can see concretely in the case with $2n = 8$ and $m = 2b - 1 = 3$ (see Figure 10b). From hindsight, we write both the $|v_i'\rangle$s and the $|w_i'\rangle$s. We start with $|w_0'\rangle = X_h^{3/2} |w\rangle$ and $|v_0'\rangle = X_g^{3/2} |v_0\rangle$, and as before, enclose the terms $\{\langle x^0\rangle' = \langle x^3\rangle, \langle x^1\rangle' = \langle x^4\rangle\}$ in a left bracket. We then multiply $|w_0'\rangle$ with X_h^{-1} (and $|v_0'\rangle$ with X_g^{-1} respectively) and project out the components along the previous vectors. We represent these by $|w_{-1}'\rangle$ and $|v_{-1}'\rangle$, and in the figure we enclose the terms $\{\langle x\rangle = \langle x^{-2}\rangle', \langle x^2\rangle = \langle x^{-1}\rangle' \dots \langle x^4\rangle = \langle x\rangle'\}$ in the left and right brackets. We do not go lower, because then we pickup a dependence on $\langle x^{-1}\rangle$ which persists for subsequent vectors. In general, we stop after taking b steps down (here $b = 1$). We go up by multiplying $|w_0'\rangle$ with X_h (and $|v_0'\rangle$ with X_g resp.) and projecting out the components along the previous vectors. We represent these by $|w_1'\rangle$ and $|v_1'\rangle$, and in the figure we enclose the terms $\{\langle x\rangle = \langle x^{-2}\rangle', \langle x^2\rangle = \langle x^{-1}\rangle' \dots \langle x^6\rangle = \langle x^3\rangle'\}$ in the brackets. Finally, we construct $|w_2'\rangle$

and $|v'_2\rangle$ by taking a step up using X_h and X_g, respectively. These are essentially fixed to be the vectors orthogonal to the previous ones, once we restrict to $\text{span}\{|h_1\rangle, |h_2,\rangle \dots |h_n\rangle\}$ and $\text{span}\{|g_1\rangle, |g_2,\rangle \dots |g_n\rangle\}$. Taking a step down using X_h^{-1} and X_g^{-1} we could have constructed $|w'_{-2}\rangle$ and $|v'_{-2}\rangle$, but these are the same as $|w'_2\rangle$ and $|v'_2\rangle$, as we have a 3-dimensional space. If we were to use $O = \sum_{i=-1}^{2} \left(|w'_i\rangle \langle v'_i| + \text{h.c.} \right)$ then we would have obtained dependence on $\langle x^7 \rangle$ in the row corresponding to $|w'_2\rangle$ and a dependence on $\langle x^8 \rangle$ for the term $\langle w'_2 | D | w'_2 \rangle$. This already hints that the matrix is negative because it has the form $\begin{bmatrix} 0 & b \\ b & c \end{bmatrix}$ with $b \neq 0$; thus this choice cannot work. We therefore define $O := \left(\sum_{i=-1}^{1} |w'_i\rangle \langle v'_i| + \text{h.c.} \right) + |w'_2\rangle \langle w'_2| + |v'_2\rangle \langle v'_2|$. Further, instead of using

$$X_h \geq E_h O X_g O^T E_h \tag{16}$$

for establishing positivity, we equivalently use

$$E_h \geq (X_h^{-1})^{1/2} O X_g O^T (X_h^{-1})^{1/2}, \tag{17}$$

which is easily obtained by multiplying by $(X_h^{-1})^{1/2}$ on both sides. The reason is that to establish positivity, we must include $|w'_2\rangle$ in the basis (we can neglect the null vectors of E_h), and even though the RHS of Equation (16) would not contribute, the LHS would get non-trivial contributions along the rows. Using the inverses allows us to remove this dependence. To see this, note that $\text{span}\{|w'_{-1}\rangle, |w'_0\rangle \dots |w'_2\rangle\}$ equals the h-space, i.e. $\text{span}\{|h_1\rangle, |h_2\rangle \dots |h_n\rangle\}$. Further, $\text{span}\{X_h^{1/2} |w'_i\rangle\}_{i=-1}^{2}$ also equals the h-space (but the vectors are not, in general, orthonormal any more). Finally, observe that $X_h^{1/2} |w'_2\rangle$ is a null vector of the RHS of Equation (17). Therefore, to prove the positivity it suffices to restrict to $\text{span}\{X_h^{1/2} |w'_i\rangle\}_{i=-1}^{1}$. An arbitrary normalized vector in this space can be written as

$$|\psi\rangle = \frac{\sum_{i=-1}^{1} \alpha_i X_h^{1/2} |w'_i\rangle}{\sqrt{\sum_{i,j=-1}^{1} \alpha_i \alpha_j \langle w'_i | X_h | w'_j \rangle}} \implies X_g^{1/2} O^T (X_h^{-1})^{1/2} |\psi\rangle = \frac{\sum_{i=-1}^{1} \alpha_i X_g^{1/2} |v'_i\rangle}{\sqrt{\sum_{i,j=-1}^{1} \alpha_i \alpha_j \langle w'_i | X_h | w'_j \rangle}}$$

$$\implies \langle \psi | (X_h^{-1})^{1/2} O X_g O^T (X_h^{-1})^{1/2} |\psi\rangle = \frac{\sum_{i,j=-1}^{1} \alpha_i \alpha_j \langle v'_i | X_g | v'_j \rangle}{\sum_{i,j=-1}^{1} \alpha_i \alpha_j \langle w'_i | X_h | w'_j \rangle} = 1,$$

where we get equality by noting that $\langle v'_i | X_g | v'_j \rangle$s depend on (at most) $\{\langle x_g \rangle, \langle x_g^2 \rangle \dots \langle x_g^6 \rangle\}$ and analogously $\langle w'_i | X_h | w'_j \rangle$ depend on (at most) $\{\langle x_h \rangle, \langle x_h^2 \rangle \dots \langle x_h^6 \rangle\}$, which are the same as $\langle x^i \rangle = 0$ for $i \in \{0, 1, \dots 6\}$. Since we proved the RHS of Equation (17) equals 1 for all normalized $|\psi\rangle$s, we conclude that we have the correct unitary.

PROPOSITION 5.10 (Solution to balanced misaligned monomial assignments). *Let*

— *$m = 2b - 1$ be an odd non-negative integer (i.e. $b \geq 1$)*

— *$t = \sum_{i=1}^{n} x_{h_i}^m p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} x_{g_i}^m p_{g_i} [\![x_{g_i}]\!]$, be a monomial assignment over $\{x_1, x_2 \dots x_{2n}\}$*

— *$(|h_1\rangle, |h_2\rangle \dots |h_n\rangle, |g_1\rangle, |g_2\rangle \dots |g_n\rangle)$ be an orthonormal basis*

— *finally*

$$X_h := \sum_{i=1}^{n} x_{h_i} |h_i\rangle \langle h_i| \doteq diag(x_{h_1}, \ldots x_{h_n}, \underbrace{0, \ldots 0}_{n \text{ zeros}}), X_g := \sum_{i=1}^{n} x_{g_i} |g_i\rangle \langle g_i| \doteq diag(\underbrace{0, \ldots 0}_{n \text{ zeros}}, x_{g_1}, \ldots x_{g_n}),$$

$$|w\rangle := (\sqrt{p_{h_1}}, \ldots \sqrt{p_{h_n}}, \underbrace{0, \ldots 0}_{n \text{ zeros}}) \text{ and } |w'\rangle := (X_h)^{b-\frac{1}{2}} |w\rangle$$

$$|v\rangle := (\underbrace{0, \ldots 0}_{n \text{ zeros}}, \sqrt{p_{g_1}}, \ldots \sqrt{p_{g_n}}) \text{ and } |v'\rangle := (X_g)^{b-\frac{1}{2}} |v\rangle .$$

Then,

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

satisfies $X_h \geq E_h O X_g O^T E_h$ *and* $E_h O |v'\rangle = |w'\rangle$, *where we write* $X_{h/g}^{-k}$ *instead of* $(X_{h/g}^{-1})^k$ *for* $k > 0$, $c_{h_i} := \langle w'| (X_h)^i \Pi_{h_i}^{\perp} (X_h)^i |w'\rangle$,

$$\Pi_{h_i}^{\perp} := \begin{cases} \text{projector orthogonal to span}\{(X_h^{-1})^{|i|-1} |w'\rangle, (X_h^{-1})^{|i|-2} |w'\rangle \ldots, |w'\rangle\} & i < 0 \\ \text{projector orthogonal to span}\{(X_h^{-1})^{b-1} |w'\rangle, (X_h^{-1})^{b-2} |w'\rangle, \ldots, |w'\rangle, X_h |w'\rangle, \ldots (X_h)^{i-1} |w'\rangle\} & i > 0 \\ \mathbb{I} & i = 0, \end{cases}$$

and analogously $c_{g_i} := \langle v'| (X_g)^i \Pi_{g_i}^{\perp} (X_g)^i |v'\rangle$,

$$\Pi_{g_i}^{\perp} := \begin{cases} \text{projector orthogonal to span}\{(X_g^{-1})^{|i|-1} |v'\rangle, (X_g^{-1})^{|i|-2} |v'\rangle \ldots, |v'\rangle\} & i < 0 \\ \text{projector orthogonal to span}\{(X_g^{-1})^{b-1} |v'\rangle, (X_g^{-1})^{b-2} |v'\rangle, \ldots |v'\rangle, X_g |v'\rangle, \ldots (X_g)^{i-1} |v'\rangle\} & i > 0 \\ \mathbb{I} & i = 0. \end{cases}$$

PROOF. The proof is very similar to that of Proposition 5.9. The orthonormal basis of interest here is

$$|w_i'\rangle := \frac{\Pi_{h_i}^{\perp} (X_h)^i |w'\rangle}{\sqrt{c_{h_i}}}$$

which entails

$$\Pi_{h_i}^{\perp} = \begin{cases} \mathbb{I}_h & i = 0 \\ \mathbb{I}_h - \sum_{j=i-1}^{0} |w_j'\rangle \langle w_j'| & i < 0 \\ \mathbb{I}_h - \sum_{j=-b+1}^{i} |w_j'\rangle \langle w_j'| & i > 0 \end{cases}$$

where $\mathbb{I}_h := E_h$. We define $|v_i'\rangle$ and $\Pi_{g_i}^{\perp}$ analogously. Our strategy is to keep track of the highest and lowest powers, l, in $\langle w'| X_h^l |w'\rangle$ and $\langle v'| X_g^l |v'\rangle$, which appear in the matrix elements $\langle w_i'| X_h |w_j'\rangle$ and $\langle v_i'| X_g |v_j'\rangle$. For brevity we write $\langle x_h^l\rangle' := \langle w'| X_h^l |w'\rangle$ and $\langle x_g^l\rangle' := \langle v'| X_g^l |v'\rangle$. The minimum

and maximum powers, l, are denoted by

$$\mathcal{M}(|w_i'\rangle) = \begin{cases} \left(\langle x_h^0\rangle' |w'\rangle, \langle x_h^0\rangle' |w'\rangle\right) & i = 0 \\ \left(\langle x_h^{-2|i|}\rangle' (X_h)^{-|i|} |w'\rangle, \langle x_h^0\rangle' |w'\rangle\right) & i < 0 \\ \left(\langle x_h^{-2(b-1)}\rangle' (X_h)^{-(b-1)} |w'\rangle, \langle x_h^{2i}\rangle' (X_h)^i |w'\rangle\right) & i > 0. \end{cases}$$

Establishing $X_h \geq E_h O X_g O^T E_h$ is equivalent to establishing

$$E_h \geq X_h^{-1/2} O X_g O^T X_h^{-1/2}. \tag{18}$$

It is easy to see that $X_h^{1/2} |w_{n-b}'\rangle$ is a vector with zero eigenvalue for the RHS as $X_g O^T |w_{n-b}'\rangle = 0$. Any vector $|\psi\rangle \in \text{span}\{|g_1\rangle, |g_2\rangle \ldots |g_n\rangle\}$ is a vector with zero eigenvalue for both the LHS and the RHS. Thus, for the positivity we can restrict to $\text{span}\{|h_1\rangle, |h_2\rangle, \ldots |h_n\rangle\}\setminus\text{span}\{X_h^{1/2} |w_{n-b}'\rangle\}$, i.e. to vectors in the h-space orthogonal to $X_h^{1/2} |w_{n-b}'\rangle$. It turns out to be easier to test for positivity on a larger space. It is clear that $\text{span}\left\{X_h^{1/2} |w_i'\rangle\right\}_{i=-b+1}^{n-b} = \text{span}\{|h_1\rangle, |h_2\rangle \ldots |h_n\rangle\} = \text{span}\{|w_i'\rangle\}_{i=-b+1}^{n-b}$, (due to Lemma C.1). As neglecting vectors with components along $X_h^{1/2} |w_{n-b}'\rangle$ suffices to satisfy Equation (18), we can restrict to $\text{span}\{X_h^{1/2} |w_i'\rangle\}_{i=-b+1}^{n-b-1}$ (which might still contain vectors with components along $X_h^{1/2} |w_{n-b}'\rangle$ as the basis vectors are not orthogonal but it only means that we check for positivity over a larger set of vectors). These ensure that the troublesome vectors $|w_{n-b}'\rangle$ and $|v_{n-b}'\rangle$ do not appear in the remaining analysis. Let $|\psi\rangle = \left(\sum_{i=-b+1}^{n-b-1} \alpha_i X_h^{1/2} |w_i'\rangle\right) / c$ where $c = \sqrt{\langle\psi|\psi\rangle}$. To establish Equation (18), it is enough to show that for all choices of α_is,

$$1 \geq \langle\psi| X_h^{-1/2} O X_g O^T X_h^{-1/2} |\psi\rangle = \frac{\sum_{i,j=-b+1}^{n-b-1} \alpha_i \alpha_j \langle v_i'| X_g |v_j'\rangle}{\sum_{i,j=-b+1}^{n-b-1} \alpha_i \alpha_j \langle w_i'| X_h |w_j'\rangle} = 1 \tag{19}$$

where the second step follows from $X_g^{1/2} O^T X_h^{-1/2} |\psi\rangle = \sum_{i=-b+1}^{n-b-1} \alpha_i X_g^{1/2} |v_i'\rangle$ and the last step follows from the counting argument below. Start by noting that

$$\langle x_h^i\rangle' = \langle x_h^{i+2b-1}\rangle \text{ and } \langle x^0\rangle = \langle x\rangle = \cdots = \langle x^{2n-2}\rangle = 0. \tag{20}$$

To determine the highest power of l in $\langle w'| X_h^l |w'\rangle$ which appears in the matrix elements $\langle w_i'| X_h |w_j'\rangle$ (for $-b + 1 \leq i, j \leq n - b - 1$) it suffices to consider the expectation values $\langle w_{n-b-1}'| X_h |w_{n-b-1}'\rangle$. To this end, we evaluate

$$\mathcal{M}(\langle w_{n-b-1}'|) X_h \mathcal{M}(|w_{n-b-1}'\rangle)$$
$$= \left(\langle x_h^{-2(b-1)}\rangle' \langle x_h^{-2(b-1)}\rangle' \langle x_h^{-2(b-1)+1}\rangle', \langle x_h^{2(n-b-1)}\rangle' \langle x_h^{2(n-b-1)}\rangle' \langle x_h^{2(n-b-1)+1}\rangle'\right)$$
$$= \left(\langle x_h\rangle \langle x_h\rangle \langle x_h^2\rangle, \langle x_h^{2n-3}\rangle \langle x_h^{2n-3}\rangle \langle x_h^{2n-2}\rangle\right).$$

The highest power is, manifestly, $l = 2n - 2$. To find the lowest power l in $\langle w'| X_h^l |w'\rangle$ appearing in $\langle w_i'| X_h |w_j'\rangle$ (for $-b + 1 \leq i, j \leq n - b - 1$) it suffices to consider $\langle w_{-b+1}'| X_h |w_{-b+1}'\rangle$. To this end,

we evaluate

$$\mathcal{M}(\langle w'_{-b+1}|)X_h\mathcal{M}(|w'_{-b+1}\rangle) = \left(\left\langle x_h^{-2(b-1)}\right\rangle' \left\langle x_h^{-2(b-1)}\right\rangle' \left\langle x_h^{-2(b-1)+1}\right\rangle', \langle x_h^0\rangle' \langle x_h^0\rangle' \langle x_h\rangle'\right)$$

$$= \left(\langle x_h\rangle \langle x_h\rangle \langle x_h^2\rangle, \langle x_h^{2b-1}\rangle \langle x_h^{2b-1}\rangle \langle x_h^{2b}\rangle\right).$$

The lowest power is, manifestly, $l = 1$. We thus conclude that the numerator of Equation (19) is a function of $\langle x_h\rangle, \langle x_h^2\rangle, \ldots \langle x_h^{2n-2}\rangle$ and, an analogous argument entails that the denominator is a function of $\langle x_g\rangle, \langle x_g^2\rangle, \ldots \langle x_g^{2n-2}\rangle$ with the same form. Using Equation (20), we conclude that the numerator and the denominator are the same.   ∎

5.3.2   The unbalanced case

The techniques we have used so far also work when the number of points in a monomial assignment are odd (i.e. for unbalanced monomial assignments), both aligned and misaligned. We illustrate how the solution is constructed by considering a concrete example of an unbalanced aligned monomial assignment. We start with $2n - 1 = 7$ points and $m = 2b = 2$ (see Figure 11a). We use the diagrammatic representation introduced previously. In this case, we have 4 initial and 3 final points; the standard basis is $\{|g_1\rangle, |g_2\rangle, \ldots |g_4\rangle, |h_1\rangle, |h_2\rangle, |h_3\rangle\}$.

(a) $2n - 1 = 7$; $m = 2b = 2$. Unbalanced aligned monomial assignment.

(b) $2n - 1 = 7$; $m = 2b - 1 = 1$. Unbalanced misaligned monomial assignment.

Figure 11. Unbalanced monomial assignments. These are explained at the start of Section 5.3.2.

The basis of interest is again constructed by starting at $|w'\rangle$ and using X_h^{-1} until we reach $\langle x^0\rangle$, and then by using X_h until the space is spanned (analogously for $|v'\rangle$ with X_g^{-1} and X_g). It is $\{|v'_{-1}\rangle, |v'_0\rangle, |v'_1\rangle, |v'_2\rangle\}$ and $\{|w'_{-1}\rangle, |w'_0\rangle, |w'_1\rangle\}$. In the same vein as the earlier solutions, we define $O := \sum_{i=-1}^{1}\left(|w'_i\rangle \langle v'_i| + \text{h.c.}\right) + |v'_2\rangle \langle v'_2|$. In $X_h \geq E_h O X_g O^T E_h$, the $|v'_2\rangle$ term is removed by

the projector, $E_h := \sum_{i=1}^{3} |h_i\rangle \langle h_i|$. Using $\langle x^0 \rangle = \langle x \rangle = \cdots = \langle x^5 \rangle = 0$ and the counting arguments from before, it follows that $D = X_h - E_h O X_g O^T E_h = 0$.

For an unbalanced misaligned monomial assignment let us consider the example with $2n - 1 = 7$ and $m = 2b - 1 = 1$ (see Figure 11b). We have 3 initial and 4 final points; the standard basis is

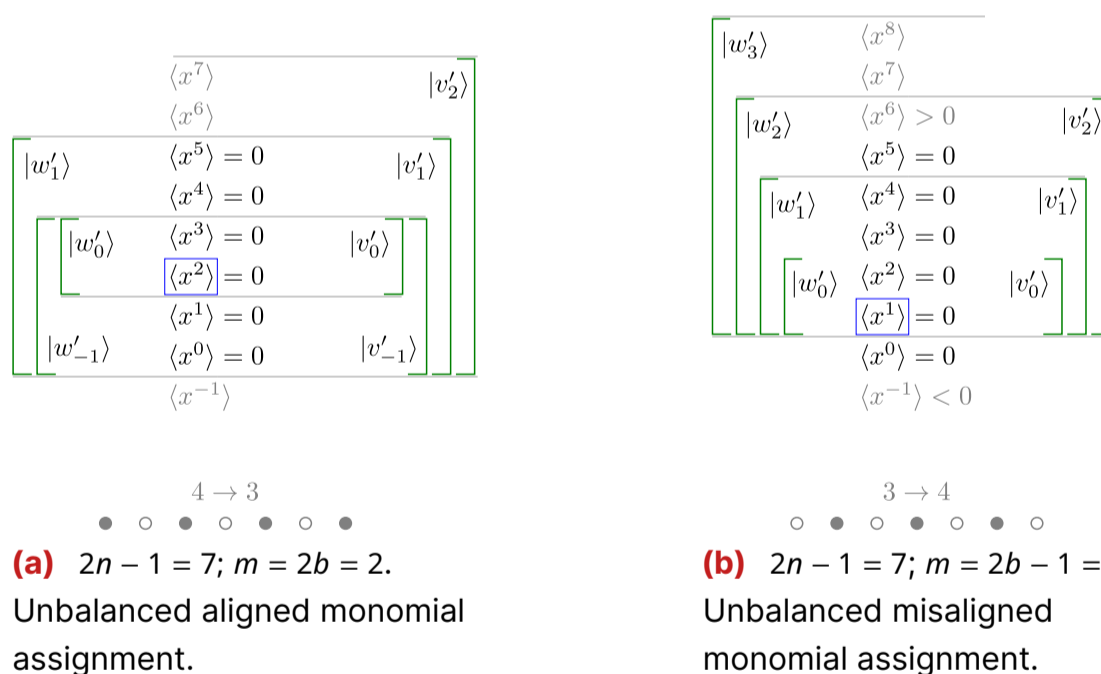$\{|g_1\rangle, |g_2\rangle, |g_3\rangle, |h_1\rangle, |h_2\rangle, \ldots |h_4\rangle\}$. We construct the basis of interest by starting at $|w'\rangle$ and using X_h until the space is spanned (analogously for $|v'\rangle$ with X_g). More generally, we first go down for $b - 2$ steps (which is zero in this case), until $\langle x \rangle$ is reached in the diagram. The bases are $\{|v'_0\rangle, |v'_1\rangle, |v'_2\rangle\}$ and $\{|w'_0\rangle, |w'_1\rangle, |w'_2\rangle, |w'_3\rangle\}$. As before, we define $O := \sum_{i=0}^{2} \left(|w'_i\rangle \langle v'_i| + \text{h.c.} \right) + |w'_3\rangle \langle w'_3|$. This time we use $E_h \geq X_h^{-1/2} O X_g O^T X_h^{-1/2}$ which is equivalent to $X_h \geq E_h O X_g O^T E_h$ for $E_h := \sum_{i=1}^{4} |h_i\rangle \langle h_i|$. Using an argument similar to the balanced misaligned case, we can reduce the positivity condition to

$$1 \geq \frac{\sum_{i,j=0}^{2} \alpha_i \alpha_j \langle v'_i | X_g | v'_j \rangle}{\sum_{i,j=0}^{2} \alpha_i \alpha_j \langle w'_i | X_h | w'_j \rangle}$$

but the counting argument doesn't make the fraction 1. This is because we now have an $\langle x_h^6 \rangle$ dependence in the denominator and an $\langle x_g^6 \rangle$ dependence in the numerator. However, we also know that this term only appears in $\langle w'_2 | X_h | w'_2 \rangle$ that too with a positive coefficient (as we saw in the unbalanced f_0−assignment). Further, we know $\langle x_h^6 \rangle > \langle x_g^6 \rangle$ and therefore we can conclude that the numerator is smaller than the denominator ensuring the inequality is always satisfied. We state the general solution for both these cases and prove their correctness below.

PROPOSITION 5.11 (Solution to unbalanced aligned monomial assignments). *Let*

— *$m = 2b$ be an even non-negative integer*
— *$t = \sum_{i=1}^{n-1} x_{h_i}^m p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} x_{g_i}^m p_{g_i} [\![x_{g_i}]\!]$, be a monomial assignment over $\{x_1, x_2 \ldots x_{2n-1}\}$*
— *$(|h_1\rangle, |h_2\rangle \ldots |h_{n-1}\rangle, |g_1\rangle, |g_2\rangle \ldots |g_n\rangle)$ be an orthonormal basis*
— *finally*

$$X_h := \sum_{i=1}^{n-1} x_{h_i} |h_i\rangle \langle h_i| \doteq diag(x_{h_1}, \ldots x_{h_{n-1}}, \underbrace{0, \ldots 0}_{n \ zeros}), X_g := \sum_{i=1}^{n} x_{g_i} |g_i\rangle \langle g_i| \doteq diag(\underbrace{0, \ldots 0}_{n-1 \ zeros}, x_{g_1}, \ldots x_{g_n}),$$

$$|w\rangle := (\sqrt{p_{h_1}}, \ldots \sqrt{p_{h_{n-1}}}, \underbrace{0 \ldots 0}_{n \ zeros}) \ and \ |w'\rangle := (X_h)^b |w\rangle,$$

$$|v\rangle := (\underbrace{0, 0, \ldots 0}_{n-1 \ zeros}, \sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_n}}) \ and \ |v'\rangle := (X_g)^b |v\rangle.$$

Then

$$O := \sum_{i=-b}^{n-b-2} \left(\frac{\Pi_{h_i}^{\perp} (X_h)^i |w'\rangle \langle v'| (X_g)^i \Pi_{g_i}^{\perp}}{\sqrt{c_{h_i} c_{g_i}}} + h.c. \right) + \frac{\Pi_{g_{n-b-1}}^{\perp} (X_g)^{n-b-1} |v'\rangle \langle v'| (X_g)^{n-b-1} \Pi_{g_{n-b-1}}^{\perp}}{c_{g_{n-b-1}}}$$

satisfies $X_h \geq E_h O X_g O^T E_h$ and $E_h O |v'\rangle = |w'\rangle$, where by $X_{h/g}^{-k}$ we mean $(X_{h/g}^{-1})^k$ for $k > 0$, and all $c_{h_i}, c_{g_i}, \Pi_{h_i}^\perp, \Pi_{g_i}^\perp$ are as defined in Proposition 5.9.

PROOF. Many observations from the proof of Proposition 5.9 carry over to this case. We import the definitions of $\{|w_i'\rangle\}_{i=-b}^{n-b-2}$ and $\{|v_i'\rangle\}_{i=-b}^{n-b-1}$, together with the observations that

$$\mathcal{M}(\langle w_{-b}'|) X_h \mathcal{M}(|w_{-b}'\rangle))$$

has no dependence on a term $\langle x_h^l \rangle'$ with $l < -2b$ and that

$$\mathcal{M}(\langle w_{n-b-2}'|) X_h \mathcal{M}(|w_{n-b-2}'\rangle))$$

has no dependence on a term $\langle x_h^l \rangle'$ with $l > 2n - 2b - 4 + 1 = 2n - 3 - 2b$. We can restrict to $\text{span}\{|w_{-b}'\rangle, |w_{-b+1}'\rangle \ldots |w_{n-b-2}'\rangle\}$ to establish the positivity of $D := X_h - E_h O X_g O^T E_h$. Using the analogous observation for $\mathcal{M}(\langle v_{-b}'|) X_g \mathcal{M}(|v_{-b}'\rangle)$ and $\mathcal{M}(\langle v_{n-b-2}'|) X_g \mathcal{M}(|v_{n-b-2}'\rangle)$, along with the fact that $\langle x^l \rangle' = \langle x^{l+2b} \rangle$ and $\langle x^0 \rangle = \langle x^1 \rangle = \cdots = \langle x^{2n-3} \rangle = 0$, it follows that $D = 0$. ∎

PROPOSITION 5.12 (Solution to unbalanced misaligned monomial assignments). *Let*

— *$m = 2b - 1$ be an odd non-negative integer*
— *$t = \sum_{i=1}^n x_{h_i}^m p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n-1} x_{g_i}^m p_{g_i} [\![x_{g_i}]\!]$ be a monomial assignment over $\{x_1, x_2 \ldots x_{2n-1}\}$*
— *$(|h_1\rangle, |h_2\rangle \ldots |h_n\rangle, |g_1\rangle, |g_2\rangle \ldots |g_{n-1}\rangle)$ be an orthonormal basis*
— *finally*

$$X_h := \sum_{i=1}^n x_{h_i} |h_i\rangle \langle h_i| \doteq diag(x_{h_1}, \ldots x_{h_n}, \underbrace{0, \ldots 0}_{n-1 \text{ zeros}}) X_g := \sum_{i=1}^{n-1} x_{g_i} |g_i\rangle \langle g_i| \doteq diag(\underbrace{0, \ldots 0}_{n \text{ zeros}}, x_{g_1}, \ldots x_{g_{n-1}}),$$

$$|w\rangle := (\sqrt{p_{h_1}}, \ldots \sqrt{p_{h_n}}, \underbrace{0, \ldots 0}_{n-1 \text{ zeros}}) \text{ and } |w'\rangle := (X_h)^{b-\frac{1}{2}} |w\rangle,$$

$$|v\rangle := (\underbrace{0, \ldots 0}_{n \text{ zeros}}, \sqrt{p_{g_1}}, \ldots \sqrt{p_{g_{n-1}}}) \text{ and } |v'\rangle := (X_g)^{b-\frac{1}{2}} |v\rangle.$$

Then

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

satisfies $X_h \geq E_h O X_g O^T E_h$ and $E_h O |v'\rangle = |w'\rangle$, where by $X_{h/g}^{-k}$ we mean $(X_{h/g}^{-1})^k$ for $k > 0$, and all $c_{h_i}, c_{g_i}, \Pi_{h_i}^\perp, \Pi_{g_i}^\perp$ are as defined in Proposition 5.10.

PROOF. For this proof, we can use the definitions and observations from the proof of Proposition 5.10. We import the definitions of $\{|w_i'\rangle\}_{i=-b+1}^{n-b}$ and $\{|v_i'\rangle\}_{i=-b+1}^{n-b-1}$ along with the observation that

$$\mathcal{M}(\langle w_{-b+1}'|) X_h \mathcal{M}(|w_{-b+1}'\rangle))$$

has no dependence on a term $\langle x_h^l \rangle'$ with $l < -2b + 2$ and

$$\mathcal{M}(\langle w'_{n-b-1}|)X_h \mathcal{M}(|w'_{n-b-1}\rangle)$$

has no dependence on a term $\langle x^l \rangle$ with $l > 2n - 2b - 1$. Also from the previous proof we have that establishing $X_h \geq E_h O X_g O^T E_h$ is equivalent to establishing

$$1 \geq \frac{\sum_{i,j=-b+1}^{n-b-1} \alpha_i \alpha_j \left\langle v'_i \middle| X_g \middle| v'_j \right\rangle}{\sum_{i,j=-b+1}^{n-b-1} \alpha_i \alpha_j \left\langle w'_i \middle| X_h \middle| w'_j \right\rangle}$$

for all real $\{\alpha_i\}_{i=-b+1}^{n-b-1}$. We know that $\langle x \rangle = \langle x^2 \rangle = \cdots = \langle x^{2n-3} \rangle = 0$. As we have the dependence on $\langle x_h^{2n-2} \rangle$, we can't conclude that the fraction is one. However, as we saw in the proof of Proposition 5.9, dependence on $\langle x_h^{2n-2} \rangle$ in the denominator only appears in the $\left\langle w'_{n-b-1} \middle| X_h \middle| w'_{n-b-1} \right\rangle$ term, that too with the positive coefficient, $1/c_{h_{n-b-1}}$. The analogous statement holds for the numerator. This, using $\langle x^{2n-2} \rangle > 0$, entails that the denominator is larger than or equal to the numerator, concluding the proof. ∎

5.4 Main result

Our observations so far can be combined to prove Theorem 2.2, which we formally state here.

THEOREM 5.13. *Let t be an f-assignment (see Definition 5.1) on strictly positive coordinates. Suppose f has real and strictly positive roots. Then, t admits an effective solution (see Definition 5.3). More explicitly, decompose $t = \sum_i \alpha_i t'_i$ where α_i are positive and t'_i are monomial assignments (see Definition 5.1 and Lemma 5.4). Then, each t'_i admits a solution given by either Proposition 5.9, Proposition 5.10, Proposition 5.11, or Proposition 5.12.*

PROOF. In Section 5.1 we established that it suffices to express an f-assignment as a sum of monomial assignments and find the solution for each one of them, in order to find the solution to the f-assignment. A monomial assignment now, can be balanced or unbalanced and aligned or misaligned (see Definition 5.1). The solution in each case is given by either Proposition 5.9, Proposition 5.10, Proposition 5.11, or Proposition 5.12. ∎

5.5 Example: a bias-1/14 protocol

We conclude the discussion by briefly outlining how all the pieces fit together to give a WCF protocol with bias 1/14 as an example. The f-assignment for the TIPG approaching bias $\epsilon(3) = 1/14$ ($k = 3$ for $\epsilon(k) = \frac{1}{4k+2}$) has the following form. Let

$$x'_0 = 0 < r'_1 < r'_2 < x'_1 < x'_2 < x'_3 < x'_4 < x'_5 < x'_6 < r'_3 < r'_4 < r'_5.$$

This is an f-assignment on $\{x'_0, x'_1 \ldots x'_6\}$ with $f'(x) = (r'_1 - x)(r'_2 - x)(r'_3 - x)(r'_4 - x)(r'_5 - x)$ viz.

$$t' = \sum_{i=0}^{6} \frac{-f'(x'_i)}{\prod_{j \neq i}(x'_j - x'_i)} [\![x'_i]\!].$$

Figure 12 details how this TIPG can be viewed as three stages of the corresponding TDPG: the split, the ladder and the merge.
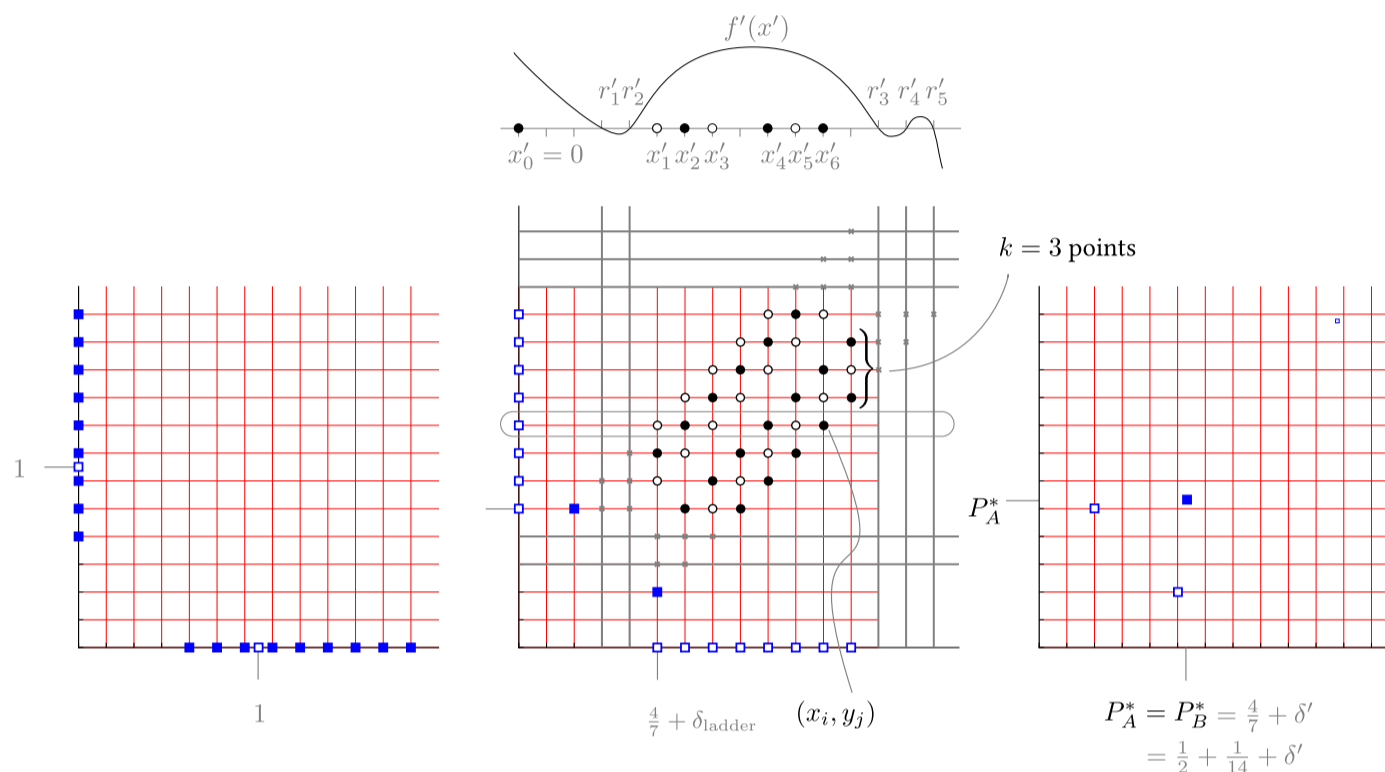

Figure 12. The TDPG (or equivalently, the reversed protocol) approaching bias $\epsilon(k = 3) = 1/14$ may be seen as proceeding in three stages, as illustrated by the three images (left to right). *First*, the initial points (indicated by unfilled squares) are split along the axes (indicated by the filled squares). *Second*, the points on the axes (unfilled squares) are transferred, by means of the ladder described in Section 3.5 (indicated by the circles), into two final points (filled squares). *Third*, the two points from the previous step (unfilled squares) and the catalyst state (indicated, after being raised into one point by the little unfilled box) are merged into the final point (filled box). The second stage is illustrated by the TIPG,—or more precisely, by its main move, the ladder—approaching bias 1/14. The weight of these points is given (up to a constant) by the f–assignment shown above. The roots of the polynomial correspond to the locations of the vertical lines and the location of the points in the graph is representative of the general construction.

However, as we explained after Lemma 5.4, our construction only works when the coordinates involved in the f-assignment are positive (and not zero). Implementing the approach described there, we fix an arbitrarily small $\delta_{\text{origin}} > 0$ and consider a δ_{origin}-translated version Mochon's TIPG approaching bias $\epsilon(3) + \delta_{\text{origin}} = 1/14 + \delta_{\text{origin}}$. The translated TIPG is also valid (see Lemma 5.5). Figure 13 details how this translated TIPG can be viewed as three stages of the corresponding TDPG. The relevant f-assignment is (see Lemma 5.6) then defined on $\{x_0, x_1 \ldots x_6\}$ where $x_i = x'_i + \delta_{\text{origin}}$, with $f(x) = (r_1 - x)(r_2 - x) \ldots (r_5 - x)$ where $r_i = r'_i + \delta_{\text{origin}}$
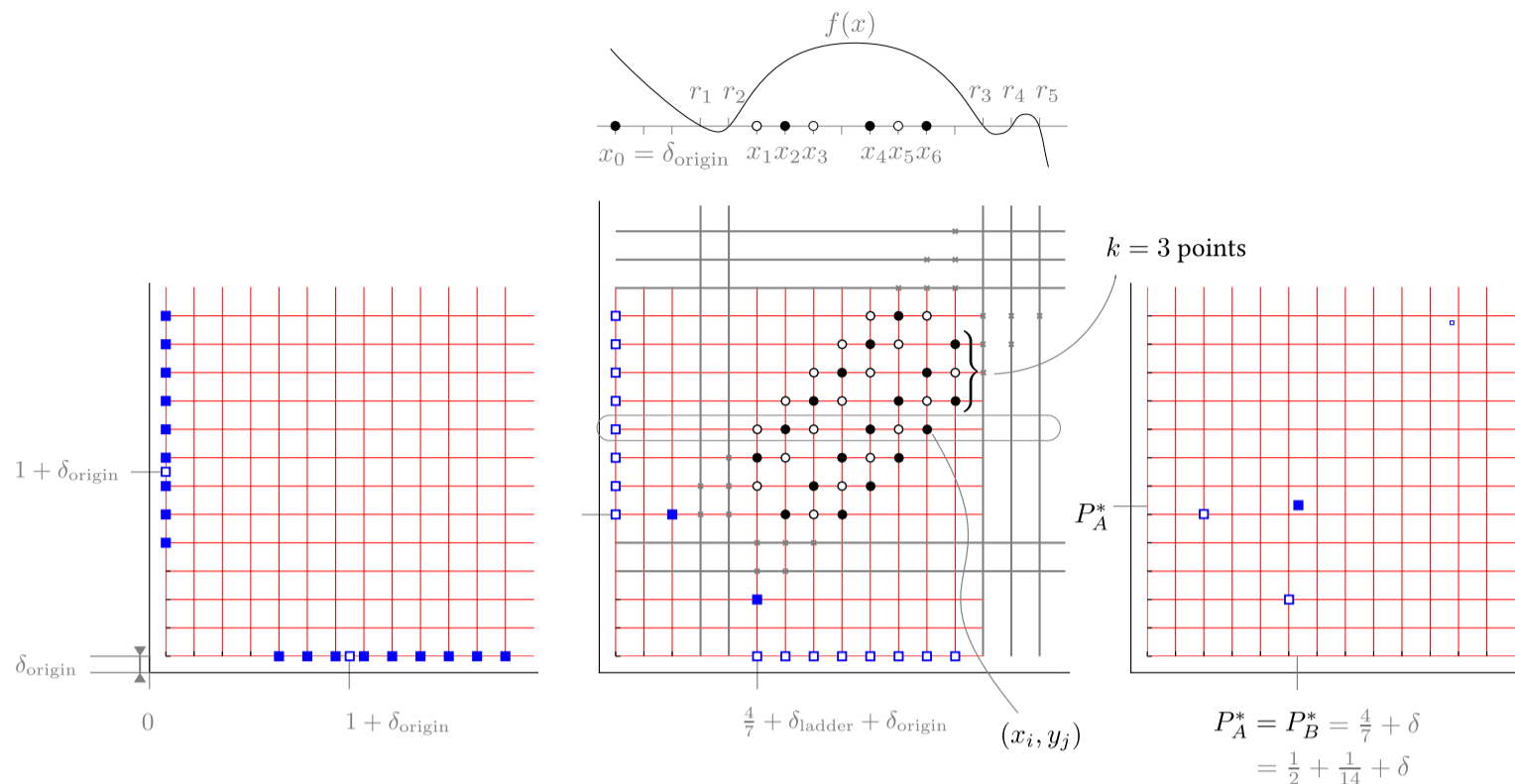
Figure 13. The δ_{origin}-translated TDPG (or equivalently, the reversed protocol) approaching bias $\epsilon(k = 3) + \delta_{\text{origin}} = 1/14 + \delta_{\text{origin}}$ may also be seen as proceeding in three stages, as illustrated by the three images (left to right). The difference compared to Figure 12 is that everything is translated by δ_{origin}. In particular, the function f' has been replaced with f, the coordinates $(x'_0, \ldots x'_6)$ and the roots $(r'_1, \ldots r'_5)$ have been replaced by $(x_0, \ldots x_6)$ and $(r_1, \ldots r_5)$ respectively. The split and the merge can be implemented just as before, while the ladder can be implemented, granted one can (effectively) solve the f-assignments (which are now all defined on positive coordinates) as illustrated above.

viz.

$$t = \sum_{i=0}^{6} \frac{-f(x_i)}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!].$$

We decompose t into a sum of monomial assignments, i.e.

$$t = \underbrace{\sum_{i=0}^{6} \frac{-r_1 r_2 r_3 r_4 r_5}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!]}_{\text{I}} + \underbrace{\sum_{i=0}^{6} \frac{-\overbrace{(r_2 r_3 r_4 r_5 + r_1 r_3 r_4 r_5 + r_1 r_2 r_3 r_5 + r_1 r_2 r_3 r_4)}^{:=\alpha_1}(-x_i)}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!]}_{\text{II}}$$

$$+ \underbrace{\sum_{i=0}^{6} \frac{-\alpha_2(-x_i)^2}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!]}_{\text{III}} + \underbrace{\sum_{i=0}^{6} \frac{-\alpha_3(-x_i)^3}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!]}_{\text{IV}} + \underbrace{\sum_{i=0}^{6} \frac{-\alpha_4(-x_i)^4}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!]}_{\text{V}} + \underbrace{\sum_{i=0}^{6} \frac{-\alpha_5(-x_i)^5}{\prod_{j \neq i}(x_j - x_i)} [\![x_i]\!]}_{\text{VI}},$$

where α_l is the coefficient of $(-x)^l$ in $f(x)$. Since the total number of points in each assignment are 7, they are unbalanced monomial assignments. Terms I, III and V each have an even powered monomial therefore they correspond to the aligned case. Their solutions, thus, are given in Proposition 5.11. Analogously, the remaining terms II, IV and VI each have an odd powered

monomial therefore they correspond to the misaligned case. Their solutions, thus, given in Proposition 5.12.

Let us now see how all these pieces fit together to give the full protocol. We describe the procedure in the language of TDPGs each step of which can be thought of as a short-hand to denote an exchange and manipulation of qubits between Alice and Bob, granted that the associated unitaries are known. As we have already done all the hard work in finding these unitaries,[22] we can now proceed at this level of description. Concretely, the δ_{origin}-translated bias $1/14$ game (see Figure 12) proceeds as follows:

1. The first frame. This simply corresponds to the function

$$\frac{1}{2} \left([\![\delta_{\text{origin}}, 1 + \delta_{\text{origin}}]\!] + [\![1 + \delta_{\text{origin}}, \delta_{\text{origin}}]\!] \right).$$

2. The split. Deposit weights along the axis as specified by the TIPG; more precisely, split the point $[\![\delta_{\text{origin}}, 1 + \delta_{\text{origin}}]\!]$ into a set of points along the y–axis (offset by δ_{origin}) and analogously, split the point $[\![1 + \delta_{\text{origin}}, \delta_{\text{origin}}]\!]$ into a set of points along the x–axis (offset by δ_{origin}), to match the distribution of points along the axes by the δ_{origin}-translated bias $1/14$ game.

3. The Catalyst State. Deposit a small amount of weight, δ_{catalyst}, at all the points that appear in the translated TIPG. This can be done by raising the points which are along the y–axis, i.e. if the points along the axes are denoted as $\sum_i p_{\text{split},i} [\![\delta_{\text{origin}}, y_i]\!]$, then raise them to obtain $\sum_i (p_{\text{split},i} - \delta_{\text{split},i}) [\![\delta_{\text{origin}}, y_i]\!] + \sum_{i,j} \delta_{\text{catalyst}} [\![x_i, y_j]\!]$, where $\delta_{\text{catalyst}} > 0$ can be chosen to be arbitrarily small and the second sum is over points (x_i, y_j) which appear in the translated TIPG (excluding those along the axes (offset by $\delta_{\text{origin}})$[23]).

4. The Ladder.
   a. Denote the monomial decomposition of the valid functions by constituent valid functions. Globally scale these constituent valid functions sufficiently so that no negative weight appears when they are applied.
   b. Apply all the scaled down constituent horizontal valid functions.
   c. Apply all the scaled down constituent vertical valid functions.
   d. Repeat these two steps until all the weight has been transferred from the axes into the two final points of the ladder.[24]

The unitaries corresponding to these constituent valid functions correspond to the solutions of the monomial assignments.

---

22   In this section we found the unitaries for f-assignments and in Section 4 we found those corresponding to splits and merges.

23   One needs to use the analogous procedure, i.e. use $\sum_i p_{\text{split},i} [\![x_i, \delta_{\text{origin}}]\!]$ as well for the one point of the TIPG which has a y–coordinate smaller than that of the points along the y–axis.

24   It would automatically become impossible to apply the moves once the weights on the axes becomes sufficiently small.

5. Raise and merge. Raise and merge the last two points into the point

$$(1 - \delta_{\text{sum-catalyst}}) \left[\!\!\left[\frac{4}{7} + \delta_{\text{ladder}} + \delta_{\text{origin}}, \frac{4}{7} + \delta_{\text{ladder}} + \delta_{\text{origin}} \right]\!\!\right]$$

where $\delta_{\text{sum-catalyst}}$ represents the total weight used by the catalyst, while δ_{ladder} comes from the truncation of the ladder. Then, using the method developed in the proof of Theorem 3.20 in [3, 32], the catalyst state can be absorbed to obtain a single point $\left[\!\!\left[\frac{4}{7} + \delta, \frac{4}{7} + \delta \right]\!\!\right]$. Thus, $P_A^* = P_B^* = \frac{1}{2} + \frac{1}{14} + \delta$, where δ can be made arbitrarily small by making the catalyst state smaller, the ladder longer and choosing a smaller translation parameter δ_{origin}.

The protocol is the reverse: it starts with a single point corresponding to uncorrelated states and whose coordinates encode the cheating probabilities, and ends with two points along the axis (offset by δ_{origin}) with equal weights, corresponding to the state $\frac{|AA\rangle + |BB\rangle}{\sqrt{2}}$.

6.   Future Work

Now that we have quantum WCF protocols, one can investigate questions about optimality, relaxation of underlying assumptions and connections to other cryptographic primitives.

Optimality Various questions about the optimality of WCF protocols are unanswered.

— *Mochon's Games.* In Section 5, in order to find the solution to the f-assignment, we expressed it as a sum of monomial assignments; this yields an increase in dimensions, which in turn corresponds to an increase in the number of qubits required.[25] One approach towards reducing this, could be to understand the connection between the perturbatively defined unitary from Section 4 and the exact one in Section 5, corresponding to the 1/10-bias protocols. Another approach could be to try reducing the dimension using a standard technical lemma from [32], which is stated as Lemma A.2 here.

— *Round complexity.* Recently, Miller [30] established that round efficient (in terms of the bias) quantum WCF is impossible. However, unlike conventional security parameters (that must be taken to be large to have any practically relevant security), the security of quantum WCF is information theoretic, even for a fixed bias. Thus, it is conceivable that practical (in terms of round complexity) WCF protocols can be constructed for a fixed bias, say, 0.01. On the other hand, Miller's lower bound applies to TIPGs and there is scope for improvement by bounding the rounds needed to convert certain families of TIPGs to TDPGs.

---

25   The dimension of the Hilbert space is expected to scale exponentially with the number of points involved in the f-assignment.

— *Pelchat-Høyer games.* Pelchat and Høyer [24] proposed another family of TIPGs which achieve arbitrarily low bias as well. It will be interesting to see if an explicit WCF protocol can be obtained corresponding to these games, potentially, in fewer dimensions.

— *Framework.* Constructing general tools to optimise and test the optimality of a TIPG for the number of points (and rounds, as mentioned above) in the associated TDPG would be very useful to both constructing better protocols as well as benchmarking the existing ones. For instance, we have a WCF protocol which uses constant space and approaches bias $\epsilon = 1/6$. However, if we go lower and consider say a Mochon's next TIPG with bias $\epsilon = 1/10$, then the corresponding TDPG suddenly seems to require points that tend to infinity as the TDPG approaches bias $1/10$. It is unclear whether this is an artefact of our construction or a fundamental characteristic.

Relaxing assumptions The assumptions we made to obtain the protocols are not realistic.

— *System size.* The size of the incoming system containing the message is assumed to be known, however, this is hard to enforce physically. One possibility is to impose a more physically realistic constraint, such restricting the average energy in the fibre optic implementing the channel, as analysed in [23].

— *Noise.* Adding noise in a WCF protocol can cause a disagreement even when both parties are honest. It has been shown that in the absence of noise but in the present of losses, WCF can still be performed with a certain bias [12]. An interesting question is whether there exist lower bounds to the lossy but noiseless setting. Returning to noise, it is clear that quantum computation is realistic due to error correction. This, however, does not necessarily mean that WCF can be performed in such a setting, as it is not obvious how we can correct errors in this adversarial scenario without compromising the security. Thus, a systematic study of noise in the adversarial setting is crucial and recent techniques in this direction [22] may help.

— *Device Dependence.* Device-independent WCF protocols have been suggested and involve the exchange of quantum boxes [1]. Their bias, however, remains quite high and since then, only modest progress has been reported [10]. Furthermore, no lower bound on the bias is known. The first step could be to redefine the protocol in a generalizable way; perhaps construct successively worse protocols—by, for instance, using fewer boxes—and subsequently, consider them as belonging to the same family. One could try to use PR-boxes or non-signalling boxes to understand the behaviour better. A complementary approach could be to construct the analogue of the Kitaev/Mochon framework where instead of qubits and unitaries, one studies more abstract objects which simulate the exchange of boxes and are only constrained by their statistics. Recently, WCF protocols were also considered in the context of general probabilistic theories [38], that are used to extend the

impossibility results theories beyond quantum. They used conic duality which is the key point of Kitaev/Mochon frameworks and hence, this approach could be a starting point.

A fundamental connection It is known that nearly perfect WCF implies optimal strong coin flipping [17]. Does this work the other way around? This question may be more general than quantum, since the construction in [17] is purely classical. One way of proceeding could be to try and construct optimal strong coin flipping protocols directly by adapting the Kitaev/Mochon technique and using known, simpler protocols as a starting point. The insight might not only help answer this question but also yield another construction for nearly perfect WCF.

Acknowledgements

References

[1] **Nati Aharon**, **André Chailloux**, **Iordanis Kerenidis**, **Serge Massar**, **Stefano Pironio**, and **Jonathan Silman**. Weak coin flipping in a device-independent setting. *Revised Selected Papers of the 6th Conference on Theory of Quantum Computation, Communication, and Cryptography - Volume 6745*, TQC 2011, pages 1–12, Madrid, Spain. Springer-Verlag New York, Inc., 2014.　DOI　(61)

[2] Nati Aharon and Jonathan Silman. Quantum dice rolling: a multi-outcome generalization of quantum coin flipping. *New Journal of Physics*, 12(3):033027, 2010. DOI   (3)

[3] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias. *SIAM Journal on Computing*, 45(3):633–679, 2014. DOI   (3, 11, 16–19, 21, 22, 40, 60, 64, 73)

[4] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. *Journal of Computer and System Sciences*, 68(2):398–416, 2004. DOI   (3, 11)

[5] Atul Singh Arora, Jérémie Roland, and Chrysoula Vlachou. Analytic quantum weak coin flipping protocols with arbitrarily small bias. *Proceedings of the 32nd Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '21, pages 919–938, Virtual Event, Virginia. Society for Industrial and Applied Mathematics, 2021. DOI   (10)

[6] Atul Singh Arora, Jérémie Roland, and Chrysoula Vlachou. Explicit quantum weak coin flipping protocols with arbitrarily small bias. *arXiv:1911.13283v1*, 2019. DOI   (10)

[7] Atul Singh Arora, Jérémie Roland, Chrysoula Vlachou, and Stephan Weis. Solutions to quantum weak coin flipping. Cryptology ePrint Archive, Paper 2022/1101, 2022. https://eprint.iacr.org/2022/1101. URL   (10)

[8] Atul Singh Arora, Jérémie Roland, and Stephan Weis. Quantum weak coin flipping. *arXiv:1811.02984*, 2018. DOI   (10)

[9] Atul Singh Arora, Jérémie Roland, and Stephan Weis. Quantum weak coin flipping. *Proceedings of the 51st Annual (ACM) (SIGACT)) Symposium on Theory of Computing (STOC) 2019*, pages 205–216. ACM Press, 2019. DOI   (10)

[10] Atul Singh Arora, Jamie Sikora, and Thomas Van Himbeeck. Improving device-independent weak coin flipping protocols. *arXiv:2404.17079*, 2024. DOI   (61)

[11] Charles H. Bennett and Gilles Brassard. Public-key distribution and coin tossing. *Int. Conf. on Computers, Systems and Signal Processing*, pages 175–179, 1984. DOI   (2)

[12] Guido Berlín, Gilles Brassard, Félix Bussières, and Nicolas Godbout. Fair loss-tolerant quantum coin flipping. *Physical Review A*, 80(6), 2009. DOI   (61)

[13] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *ACM SIGACT News*, 15(1):23–27, 1983. DOI   (2)

[14] Stephen Boyd and Lieven Vandenberghe. Convex Optimization. Cambridge University Press, 2004. DOI   (18)

[15] André Chailloux, Gus Gutoski, and Jamie Sikora. Optimal bounds for semi-honest quantum oblivious transfer. *Chicago Journal of Theoretical Computer Science, 2016*, October 11, 2013. URL   (3)

[16] André Chailloux and Iordanis Kerenidis. Optimal Bounds for Quantum Bit Commitment. *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 354–362, 2011. DOI   (3)

[17] André Chailloux and Iordanis Kerenidis. Optimal Quantum Strong Coin Flipping. *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 527–533, 2009. DOI   (3, 62)

[18] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for quantum oblivious transfer. *Quantum Information & Computation*, 13(1-2):158–177, 2013. DOI   (2)

[19] Roger Colbeck. Impossibility of secure two-party classical computation. *Phys. Rev. A*, 76:062308, 6, 2007. DOI   (2)

[20] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. DOI   (2)

[21] Maor Ganz. Quantum Leader Election. *arXiv:0910.4952v2*, 2009. DOI   (3)

[22] Gus Gutoski, Ansis Rosmanis, and Jamie Sikora. Fidelity of quantum strategies with applications to cryptography. *Quantum*, 2:89, 2018. DOI   (61)

[23] Thomas Van Himbeeck, Erik Woodhead, Nicolas J. Cerf, Raúl García-Patrón, and Stefano Pironio. Semi-device-independent framework based on natural physical assumptions. *Quantum*, 1:33, 2017. DOI   (61)

[24] Peter Høyer and Edouard Pelchat. Point Games in Quantum Weak Coin Flipping Protocols. Master's thesis, University of Calgary, 2013. URL   (61)

[25] Iordanis Kerenidis and Ashwin Nayak. Weak coin flipping with small bias. *Information Processing Letters*, 89(3):131–135, 2004. DOI   (8)

[26] Joe Kilian. Founding crytpography on oblivious transfer. *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, STOC '88, pages 20–31, Chicago, Illinois, USA. Association for Computing Machinery, 1988. DOI   (2)

[27] Alexei Kitaev. Quantum coin flipping. Talk at the 6th workshop on Quantum Information Processing, 2003. Talk at the 6th workshop on Quantum Information Processing   (3, 15)

[28] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Phys. Rev. A*, 56:1154–1162, 2, 1997. DOI   (2)

[29] Ralph C. Merkle. Secure communications over insecure channels. *Commun. ACM*, 21(4):294–299, 1978. DOI   (2)

[30] Carl A. Miller. The impossibility of efficient quantum weak coin flipping. *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC)*. Association for Computing Machinery, New York, NY, USA, 2020., pages 916–929. URL   (60)

[31] Carlos Mochon. Large family of quantum weak coin-flipping protocols. *Phys. Rev. A*, 72:022341, 2005. DOI   (4, 8, 9)

[32] **Carlos Mochon**. Quantum weak coin flipping with arbitrarily small bias. *arXiv:0711.4114*, 2007. `DOI` (2, 3, 9, 11, 13, 16, 17, 19–22, 40, 60, 64, 73)

[33] **Ashwin Nayak and Peter Shor**. Bit-commitment-based quantum coin flipping. *Phys. Rev. A*, 67:012304, 1, 2003. `DOI`   (8)

[34] **Ashwin Nayak, Jamie Sikora, and Levent Tunçel**. A search for quantum coin-flipping protocols using optimization techniques. *Mathematical Programming*, 156(1-2):581–613, 2014. `DOI`   (3)

[35] **Ashwin Nayak**, **Jamie Sikora**, and **Levent Tunçel**. Quantum and classical coin-flipping protocols based on bit-commitment and their point games, April 16, 2015. `URL`   (3)

[36] **Ronald L. Rivest**, **Adi Shamir**, and **Leonard M. Adleman**. Cryptographic communications system and method, 1977. U.S. Patent US4405829A   (2)

[37] **Peter W. Shor**. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE Comput. Soc. Press, 1994. `DOI`   (2)

[38] **Jamie Sikora and John H. Selby**. Impossibility of coin flipping in generalized probabilistic theories via discretizations of semi-infinite programs. *Phys. Rev. Res.* 2:043128, 4, 2020. `DOI`   (61)

[39] **Robert W. Spekkens and Terry Rudolph**. Quantum protocol for cheat-sensitive weak coin flipping. *Phys. Rev. Lett. vol 89, 227901 (2002)*, 89(22), February 21, 2002. `DOI`   (8)

A.   Proof of Lemma 4.5

For the proof that the closure of EBM functions equals the set of valid functions, the reader is referred to [3]. At the end of Section 3.3 we also outlined the main arguments. Here, we prove the following:

LEMMA A.1. *The closure of the set of EBM functions equals the set of TEF functions.*

For simplicity, in the following discussion, we restrict to transitions (see Definition 3.7) with disjoint support. This allows us to use transitions and functions interchangeably, as explained at the end of Section 3.3.

The proof uses the following characterization of EBM functions presented in Lemma A.2, which is originally due to Mochon [32] (the proof therein had a minor error, though, that we correct).

Below, when we say EBM transition with spectrum in $[a, b]$, we refer to an EBM transition with the additional constraint that the matrices H, G, as introduced in Definition 3.8, have eigenvalues in the interval $[a, b]$.

LEMMA A.2. *Consider the transition $g \to h$ where $g := \sum_{i=1}^{m} p_{g_i} [\![x_{g_i}]\!]$ and $h := \sum_{i=1}^{m} p_{h_i} [\![x_{h_i}]\!]$. For every EBM transition $g \to h$ with spectrum in $[a, b]$ there exists a unitary matrix U, diagonal matrices X_h, X_g (with no multiplicities except possibly those of a and b) of size at most $m + n - 1$*

such that

$$
U \begin{bmatrix} X_{g_1} & & & & & \\ & \ddots & & & & \\ & & X_{g_{n_g}} & & & \\ & & & a & & \\ & & & & \ddots & \end{bmatrix} U^\dagger \leq \begin{bmatrix} X_{h_1} & & & & & \\ & \ddots & & & & \\ & & X_{h_{n_h}} & & & \\ & & & b & & \\ & & & & \ddots & \end{bmatrix} = X_h, \tag{21}
$$

$$\underbrace{}_{:=X_g}$$

and the vector $|\psi\rangle := (\sqrt{p_{h_1}}, \dots, \sqrt{p_{h_n}}, 0 \dots 0)^T = U(\sqrt{p_{g_1}}, \dots \sqrt{p_{g_m}}, 0 \dots 0)^T.$

We will prove this lemma shortly. Let us first see how this almost immediately yields Lemma A.1.

PROOF SKETCH OF LEMMA A.1. In this proof, we restrict to EBM functions with spectrum in $[a, b] \subseteq [0, \infty)$. For any such EBM transition $g \to h$, one can verify that Equation (21) implies the following (for any $b' \geq b$ and an appropriate $\tilde{U}$)

$$
\tilde{U} \left[\begin{array}{ccc|ccc} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ \hline & & & X_{g_1} & & \\ & & & & \ddots & \\ & & & & & X_{g_m} \end{array} \right] \tilde{U}^\dagger \leq
$$

$$
\tilde{U} \left[\begin{array}{ccc|ccc} a & & & & & \\ & \ddots & & & & \\ & & a & & & \\ \hline & & & X_{g_1} & & \\ & & & & \ddots & \\ & & & & & X_{g_n} \end{array} \right] \tilde{U}^\dagger \leq \left[\begin{array}{ccc|ccc} X_{h_1} & & & & & \\ & \ddots & & & & \\ & & X_{h_m} & & & \\ \hline & & & b & & \\ & & & & \ddots & \\ & & & & & b \end{array} \right]
$$

$$
\leq \left[\begin{array}{ccc|ccc} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ \hline & & & b' & & \\ & & & & \ddots & \\ & & & & & b' \end{array} \right] \left[\begin{array}{ccc|ccc} X_{h_1} & & & & & \\ & \ddots & & & & \\ & & X_{h_m} & & & \\ \hline & & & 1/b' & & \\ & & & & \ddots & \\ & & & & & 1/b' \end{array} \right] \left[\begin{array}{ccc|ccc} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ \hline & & & b' & & \\ & & & & \ddots & \\ & & & & & b' \end{array} \right]
$$

■

where the matrices are of size $m + n$. The inequality involving the first and the last term may equivalently be expressed as

$$
\begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ \hline & & & 1/b' & & \\ & & & & \ddots & \\ & & & & & 1/b' \end{bmatrix} \tilde{U} \begin{bmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ \hline & & & x_{g_1} & & \\ & & & & \ddots & \\ & & & & & x_{g_m} \end{bmatrix} \tilde{U}^\dagger \begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ \hline & & & 1/b' & & \\ & & & & \ddots & \\ & & & & & 1/b' \end{bmatrix}
$$

$$
\leq \begin{bmatrix} x_{h_1} & & & & & \\ & \ddots & & & & \\ & & x_{h_m} & & & \\ \hline & & & 1/b' & & \\ & & & & \ddots & \\ & & & & & 1/b' \end{bmatrix} . \quad (22)
$$

This condition yields, in the $b' \to \infty$ limit,

$$
E_h \tilde{U} \underbrace{\left(\sum_{i=1}^n x_{g_i} |g_i\rangle \langle g_i| \right)}_{:=G'} \tilde{U}^\dagger E_h \leq \underbrace{\left(\sum_{i=1}^m x_{h_i} |h_i\rangle \langle h_i| \right)}_{:=H'} \quad (23)
$$

where $(|g_i\rangle)_{i=1}^n$ represent the last n coordinates, $(|h_i\rangle)_{i=1}^m$ represent the first m coordinates and $E_h := \sum_{i=1}^m |h_i\rangle \langle h_i|$. Further, for $|v\rangle = \sum_{i=1}^n \sqrt{p_{g_i}} |g_i\rangle$, one can check that $\tilde{U} |v\rangle = \sum_{i=1}^m \sqrt{p_{h_i}} |h_i\rangle$ using the definition of $|\psi\rangle$ and $\tilde{U}$. Thus, any EBM transition $g \to h$ is also a TEF transition.

One can easily extend this reasoning to establish that the closure of EBM functions is also contained in the set of TEF functions. Consider a sequence of EBM functions $(h_i - g_i)_{i=1}^\infty$ with support in $[a_i, b_i] \subseteq [0, \infty)$ such that the limiting function, $h - g$ is well defined (i.e. support of $h - g$ is contained in $[0, \infty)$; support of a function f is simply $x : f(x) \neq 0$) but $h - g$ is not EBM. The only way this can happen is if $b_i \to \infty$ tends to infinity as $i \to \infty$. However, using the reasoning above, one can consider Equation (22) and there, it is clear that the limiting procedure yields Equation (23) which is precisely the TEF constraint. Thus, the limiting function is a TEF function.

One can similarly argue that every TEF function is contained in the closure of EBM functions.

PROOF OF LEMMA A.2. Let $n_g := n$ and $n_h := m$. An EBM entails that we are given $G \leq H$ with their spectrum in $[a, b]$ and a $|\psi\rangle$ such that

$$
g = \text{Prob}[G, |\psi\rangle] = \sum_{i=1}^{n_g} p_{g_i} [\![x_{g_i}]\!]
$$

and

$$h = \text{Prob}[H, |\psi\rangle] = \sum_{i=1}^{n_h} p_{h_i} [\![x_{h_i}]\!]$$

with $p_{g_i}, p_{h_i} > 0$ and $x_{g_i} \neq x_{g_j}$, $x_{h_i} \neq x_{h_j}$ for $i \neq j$ but the dimension and multiplicities can be arbitrary. First we show that one can always choose the eigenvectors $|g_i\rangle$ of G with eigenvalue x_{g_i} such that

$$|\psi\rangle = \sum_{i=1}^{n_g} \sqrt{p_{g_i}} |g_i\rangle .$$

Consider P_{g_i} to be the projector on the eigenspace with eigenvalue x_{g_i}. Note that

$$|g_i\rangle := \frac{P_{g_i} |\psi\rangle}{\sqrt{\langle\psi| P_{g_i} |\psi\rangle}}$$

fits the bill. Similarly we choose/define $|h_i\rangle$ so that

$$|\psi\rangle = \sum_{i=1}^{n_h} \sqrt{p_{h_i}} |h_i\rangle .$$

Consider now the projector onto the $\{|g_i\rangle\}$ space

$$\Pi_g = \sum_{i=1}^{n_g} |g_i\rangle \langle g_i| .$$

Note that this will not have all eigenvectors with eigenvalues $\in \{x_{g_i}\}$. Similarly we define

$$\Pi_h = \sum_{i=1}^{n_h} |h_i\rangle \langle h_i| .$$

We further define $G' := \Pi_g G \Pi_g + a(\mathbb{I} - \Pi_g)$ and $H' := \Pi_h H \Pi_h + b(\mathbb{I} - \Pi_h)$. These definitions are useful as we can show

$$G' \leq H'.$$

From $G = \Pi_g G \Pi_g + (\mathbb{I} - \Pi_g)G(\mathbb{I} - \Pi_g)$ we can conclude that $\Pi_g G \Pi_g + a(\mathbb{I} - \Pi_g) \leq G$. This entails $G' \leq G$. Using a similar argument one can also establish that $H \leq H'$. Combining these we get $G' \leq H'$.

Consider the projector

$$\Pi := \text{projector on span}\{\{|g_i\rangle\}_{i=1}^{n_g}, \{|h_i\rangle\}_{i=1}^{n_h}\}$$

and note that this has at most $n_g + n_h - 1$ dimension because $|\psi\rangle$ lives in the span of $\{|g_i\rangle\}$ and in the span of $\{|h_i\rangle\}$ so one of the basis vectors at least is not independent. Now note that

$$G'' := \Pi G' \Pi \leq \Pi H' \Pi =: H''$$

because we can always conjugate an inequality by a positive semi-definite matrix on both sides. Note also that $\Pi \ket{\psi} = \ket{\psi}$ which means the matrices and the vectors have the claimed dimension. We now establish that $\text{Prob}[H'', \ket{\psi}] = h$ and $\text{Prob}[G'', \ket{\psi}] = g$. For this we first write the projector tailored to the g basis as $\Pi = \Pi_g + \Pi_{g_\perp}$ where $\Pi_{g_\perp}$ is meant to enlarge the space to the $\text{span}\{h_i\}_{i=1}^{n_h}$. With this we evaluate

$$G'' = \left(\Pi_g + \Pi_{g_\perp}\right) \left[\Pi_g G \Pi_g + a(\mathbb{I} - \Pi_g)\right] \left(\Pi_g + \Pi_{g_\perp}\right)$$
$$= \Pi_g G \Pi_g + a\Pi_{g_\perp}.$$

Manifestly then $\text{Prob}[G'', \ket{\psi}] = g$. By a similar argument one can establish the h claim. Note that that G'' and H'' have no multiplicities except possibly in a and b respectively. Thus we conclude we can always restrict to the claimed dimension and form.   ∎

B.   Blink $m \to n$ transition

B.1   Completing an orthonormal basis

Consider an orthonormal complete set of basis vectors $\{\ket{g_i}\}$ and a vector $\ket{v} = \frac{\sum_i \sqrt{p_i}\ket{g_i}}{\sqrt{\sum_i p_i}}$. We describe a scheme for constructing vectors $\ket{v_i}$ such that $\{\ket{v}, \{\ket{v_i}\}\}$ is a complete orthonormal set of basis vectors. We can do it inductively, but here instead we choose to do it by examples, as we believe it helps gain some intuition and demonstrates the generalizable argument right away. We define the first vector to be

$$\ket{v_1} = \frac{\sqrt{p_1}\ket{g_1} - \frac{p_1}{\sqrt{p_2}}\ket{g_2}}{\sqrt{p_1 + \frac{p_1^2}{p_2}}} = \frac{\sqrt{p_1}\ket{g_1} - \sqrt{p_2}\ket{g_2}}{\sqrt{p_1 + p_2}},$$

which is normalized and orthogonal to $\ket{v}$. The next vector is

$$\ket{v_2} = \frac{\sqrt{p_1}\ket{g_1} + \sqrt{p_2}\ket{g_2} - \frac{(p_1+p_2)}{\sqrt{p_3}}\ket{g_3}}{\sqrt{p_1 + p_2 + \frac{(p_1+p_2)^2}{p_3}}}$$

which is again normalized and orthogonal to $\ket{v_1}$.

Similarly we can construct the $(k+1)^{\text{th}}$ basis vector as

$$\ket{v_k} = \frac{\sum_{i=1}^{k} \sqrt{p_k}\ket{g_k} - \frac{\sum_{i=1}^{k} p_k}{\sqrt{p_{k+1}}}\ket{g_{k+1}}}{N_k},$$

where $N_k = \sqrt{\sum_{i=1}^{k} p_k + \frac{(\sum_{i=1}^{k} p_k)^2}{p_{k+1}}}$ and, thus, obtain the full set.

B.2 Analysis of the 3 → 2 transition

Recall that the constraint equation is

$$\underbrace{\sum x_{h_i} |h_{ii}\rangle \langle h_{ii}|}_{\text{I}} + \underbrace{x\mathbb{I}^{\{g_{ii}\}}}_{\text{II}} \geq \underbrace{\sum x_{g_i} U |g_{ii}\rangle \langle g_{ii}| U^\dagger}_{\text{III}},$$

where we have introduced the notation $|h_{ii}\rangle = |h_i h_i\rangle$. The $g_1, g_2, g_3 \rightarrow h_1, h_2$ transition requires us to know

$$U = |v\rangle \langle w| + |w\rangle \langle v| + |v_1\rangle \langle v_1| + |v_2\rangle \langle v_2| + |w_1\rangle \langle w_1|.$$

Using the procedure above we can evaluate the vectors of interest as

$$|v\rangle = \frac{\sqrt{p_{g_1}} |g_{11}\rangle + \sqrt{p_{g_2}} |g_{22}\rangle + \sqrt{p_{g_3}} |g_{33}\rangle}{N_g}, \quad |v_1\rangle = \frac{\sqrt{p_{g_1}} |g_{11}\rangle - \frac{p_{g_1}}{\sqrt{p_{g_2}}} |g_{22}\rangle}{N_{g_1}},$$

$$|v_2\rangle = \frac{\sqrt{p_{g_1}} |g_{11}\rangle + \sqrt{p_{g_2}} |g_{22}\rangle - \frac{(p_{g_1}+p_{g_2})}{\sqrt{p_{g_3}}} |g_{33}\rangle}{N_{g_2}},$$

$$|w\rangle = \frac{\sqrt{p_{h_1}} |h_{11}\rangle + \sqrt{p_{h_2}} |h_{22}\rangle}{N_h} \quad \text{and} \quad |w_1\rangle = \frac{\sqrt{p_{h_2}} |h_{11}\rangle - \sqrt{p_{h_1}} |h_{22}\rangle}{N_h},$$

where N_g, N_{g_1}, N_{g_2}, N_h are normalization factors. In fact we want to express the constraints in this basis, and to evaluate the first term of the LHS in the constraint equation we use the above to find

$$|h_{11}\rangle = \frac{\sqrt{p_{h_1}} |w\rangle + \sqrt{p_{h_2}} |w_1\rangle}{N_h} \quad \text{and} \quad |h_{22}\rangle = \frac{\sqrt{p_{h_2}} |w\rangle - \sqrt{p_{h_1}} |w_1\rangle}{N_h},$$

which leads to

$$\text{I} = x_{h_1} |h_{11}\rangle \langle h_{11}| + x_{h_2} |h_{22}\rangle \langle h_{22}|$$

$$= \frac{1}{N_h^2} \left[\begin{array}{c|cc} & \langle w| & \langle w_1| \\ \hline |w\rangle & p_{h_1} x_{h_1} + p_{h_2} x_{h_2} & \sqrt{p_{h_1} p_{h_2}} (x_{h_1} - x_{h_2}) \\ |w_1\rangle & \sqrt{p_{h_1} p_{h_2}} (x_{h_1} - x_{h_2}) & p_{h_2} x_{h_1} + p_{h_1} x_{h_2} \end{array} \right].$$

Evaluation of II is nearly trivial after expressing the identity in this basis

$$\text{II} = x(|v\rangle \langle v| + |v_1\rangle \langle v_1| + |v_2\rangle \langle v_2|) = \left[\begin{array}{c|ccc} & \langle v| & \langle v_1| & \langle v_2| \\ \hline |v\rangle & x & & \\ |v_1\rangle & & x & \\ |v_2\rangle & & & x \end{array} \right].$$

For the last term $\text{III} = \underbrace{x_{g_1} U |g_{11}\rangle \langle g_{11}| U^\dagger}_{\text{(i)}} + \underbrace{x_{g_2} U |g_{22}\rangle \langle g_{22}| U^\dagger}_{\text{(ii)}} + \underbrace{x_{g_3} U |g_{33}\rangle \langle g_{33}| U^\dagger}_{\text{(iii)}}$, we evaluate

$$U |g_{11}\rangle = \frac{\sqrt{p_{g_1}}}{N_g} |w\rangle + \frac{\sqrt{p_{g_1}}}{N_{g_1}} |v_1\rangle + \frac{\sqrt{p_{g_1}}}{N_{g_2}} |v_2\rangle ,$$

$$U |g_{22}\rangle = \frac{\sqrt{p_{g_2}}}{N_g} |w\rangle + \frac{\left(-\frac{p_{g_1}}{\sqrt{p_{g_2}}}\right)}{N_{g_1}} |v_1\rangle + \frac{\sqrt{p_{g_2}}}{N_{g_2}} |v_2\rangle \text{ and}$$

$$U |g_{33}\rangle = \frac{\sqrt{p_{g_3}}}{N_g} |w\rangle + 0 |v_1\rangle + \frac{\left(-\frac{p_{g_1}+g_{g_2}}{\sqrt{p_{g_3}}}\right)}{N_{g_2}} |v_2\rangle .$$

For the first term we have $\text{(i)} = x_{g_1} p_{g_1}$

	$\langle v_1|$	$\langle v_2|$	$\langle w|$
$|v_1\rangle$	$\frac{1}{N_{g_1}^2}$	$\frac{1}{N_{g_1} N_{g_2}}$	$\frac{1}{N_{g_1} N_g}$
$|v_2\rangle$	$\frac{1}{N_{g_2} N_{g_1}}$	$\frac{1}{N_{g_2}^2}$	$\frac{1}{N_{g_2} N_g}$
$|w\rangle$	$\frac{1}{N_g N_{g_1}}$	$\frac{1}{N_g N_{g_2}}$	$\frac{1}{N_g^2}$

For the second term, we re-write $U |g_{22}\rangle = \sqrt{p_{g_2}} \left(\frac{1}{N_g} |w\rangle - \frac{1}{N'_{g_1}} |v_1\rangle + \frac{1}{N_{g_2}} |v_2\rangle \right)$ with $N'_{g_1} = \frac{p_{g_2}}{p_{g_1}} N_{g_1}$,

to obtain $\text{(ii)} = x_{g_2} p_{g_2}$

	$\langle v_1|$	$\langle v_2|$	$\langle w|$
$|v_1\rangle$	$\frac{1}{N'^2_{g_1}}$	$-\frac{1}{N'_{g_1} N_{g_2}}$	$-\frac{1}{N'_{g_1} N_g}$
$|v_2\rangle$	$-\frac{1}{N_{g_2} N'_{g_1}}$	$\frac{1}{N_{g_2}^2}$	$\frac{1}{N_{g_2} N_g}$
$|w\rangle$	$-\frac{1}{N_g N'_{g_1}}$	$\frac{1}{N_g N_{g_2}}$	$\frac{1}{N_g^2}$

and finally $U |g_{33}\rangle = \sqrt{p_{g_3}} \left(\frac{1}{N_g} |w\rangle + 0 |v_1\rangle - \frac{1}{N'_{g_2}} |v_2\rangle \right)$ with $N'_{g_2} = \frac{p_{g_3}}{p_{g_1}+p_{g_2}}$,

to get $\text{(iii)} = x_{g_3} p_{g_3}$

	$\langle v_1|$	$\langle v_2|$	$\langle w|$
$|v_1\rangle$			
$|v_2\rangle$		$\frac{1}{N'^2_{g_2}}$	$-\frac{1}{N'_{g_2} N_g}$
$|w\rangle$		$-\frac{1}{N_g N'_{g_2}}$	$\frac{1}{N_g^2}$

Now we can combine all of these into a single matrix and try to obtain some simpler constraints.

$$M \overset{\text{def}}{=}$$

	$\langle v|$	$\langle v_1|$	$\langle v_2|$	$\langle w|$	$\langle w_1|$
$|v\rangle$	x				
$|v_1\rangle$		$x - \frac{x_{g_1} p_{g_1}}{N_{g_1}^2} - \frac{x_{g_2} p_{g_2}}{N'^2_{g_1}}$	$-\frac{x_{g_1} p_{g_1}}{N_{g_1} N_{g_2}} + \frac{x_{g_2} p_{g_2}}{N'_{g_1} N_{g_2}}$	$-\frac{x_{g_1} p_{g_1}}{N_{g_1} N_g} + \frac{x_{g_2} p_{g_2}}{N'_{g_1} N_g}$	
$|v_2\rangle$		$-\frac{x_{g_1} p_{g_1}}{N_{g_2} N_{g_1}} + \frac{x_{g_2} p_{g_2}}{N_{g_2} N'_{g_1}}$	$x - \frac{x_{g_1} p_{g_1}}{N_{g_2}^2} - \frac{x_{g_2} p_{g_2}}{N_{g_2}^2} - \frac{x_{g_3} p_{g_3}}{N'^2_{g_2}}$	$-\frac{x_{g_1} p_{g_1}}{N_{g_2} N_g} - \frac{x_{g_2} p_{g_2}}{N_{g_2} N_g} + \frac{x_{g_3} p_{g_3}}{N'_{g_2} N_g}$	
$|w\rangle$		$-\frac{x_{g_1} p_{g_1}}{N_g N_{g_1}} + \frac{x_{g_2} p_{g_2}}{N_g N'_{g_1}}$	$-\frac{x_{g_1} p_{g_1}}{N_g N_{g_2}} - \frac{x_{g_2} p_{g_2}}{N_g N_{g_2}} + \frac{x_{g_3} p_{g_3}}{N_g N'_{g_2}}$	$\frac{p_{h_1} x_{h_1} + p_{h_2} x_{h_2}}{N_h^2} - \frac{1}{N_g^2} \sum_i x_{g_i} p_{g_i}$	$\frac{\sqrt{p_{h_1} p_{h_2}}}{N_h^2} (x_{h_1} - x_{h_2})$
$|w_1\rangle$				$\frac{\sqrt{p_{h_1} p_{h_2}}}{N_h^2} (x_{h_1} - x_{h_2})$	$\frac{p_{h_2} x_{h_1} + p_{h_1} x_{h_2}}{N_h^2}$

$\geq 0.$

Despite this appearing to be a complicated expression, we can conclude that it is always so that the larger x is the looser is the constraint. To show this and simplify the calculation, note that M can be split into a scalar condition, $x \geq 0$ – from the $|v\rangle\langle v|$ part – and a sub-matrix which we choose to write as

	$\langle v_1 \vert$ $\langle v_2 \vert$	$\langle w \vert$ $\langle w_1 \vert$
$\vert v_1 \rangle$ $\vert v_2 \rangle$	C	B^T
$\vert w \rangle$ $\vert w_1 \rangle$	B	A

$$\geq 0.$$

We have that $\begin{bmatrix} C & B^T \\ B & A \end{bmatrix} \geq 0 \iff \begin{bmatrix} A & B \\ B^T & C \end{bmatrix} \geq 0 \iff C \geq 0,\ A - BC^{-1}B^T \geq 0,\ (\mathbb{I} - CC^{-1})B^T = 0,$

using Shur's Complement condition for positivity where C^{-1} is the generalized inverse. We can take x to be sufficiently large so that $C > 0$ and thereby make sure that $\mathbb{I} - CC^{-1} = 0$. Then, the only condition of interest is

$$A - BC^{-1}B^T \geq 0.$$

Actually, we can do even better than this. Note that if $C > 0$ then $C^{-1} > 0$ and that the second term is of the form

$$\underbrace{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}}_{B} \underbrace{\begin{bmatrix} \alpha & \gamma \\ \gamma & \beta \end{bmatrix}}_{C^{-1}} \underbrace{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}}_{B^T} = \begin{bmatrix} \begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} \alpha & \gamma \\ \gamma & \beta \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} & 0 \\ 0 & 0 \end{bmatrix} \geq 0,$$

because $C^{-1} > 0$. We can therefore write the constraint equation as $A \geq BC^{-1}B^T \geq 0$ and note that $A \geq 0$ is a necessary condition. This also becomes a sufficient condition in the limit that $x \to \infty$ because $C^{-1} \to 0$ in that case. Thus, we have reduced the analysis to simply checking if

$$\begin{bmatrix} \frac{p_{h_1} x_{h_1} + p_{h_2} x_{h_2}}{N_h^2} - \frac{1}{N_g^2} \sum_i x_{g_i} p_{g_i} & \frac{\sqrt{p_{h_1} p_{h_2}}}{N_h^2} (x_{h_1} - x_{h_2}) \\ \frac{\sqrt{p_{h_1} p_{h_2}}}{N_h^2} (x_{h_1} - x_{h_2}) & \frac{p_{h_2} x_{h_1} + p_{h_1} x_{h_2}}{N_h^2} \end{bmatrix} \geq 0.$$

This is a 2×2 matrix and can be checked for positivity using the trace and determinant method or we can use again Schur's Complement conditions. Here, however, we intend to use a more general technique. Let us introduce

$$\langle x_g \rangle \stackrel{\text{def}}{=} \frac{1}{N_g^2} \sum_i x_{g_i} p_{g_i}, \quad \left\langle \frac{1}{x_h} \right\rangle \stackrel{\text{def}}{=} \frac{1}{N_h^2} \sum_i \frac{p_{h_i}}{x_{h_i}}.$$

Term (I) and one element from term (III) constitute a matrix A which can be written as

$$A = x_{h_1} |h_{11}\rangle \langle h_{11}| + x_{h_2} |h_{22}\rangle \langle h_{22}| - \langle x_g \rangle |w\rangle \langle w| = \begin{array}{c|cc} & \langle h_{11}| & \langle h_{22}| \\ \hline |h_{11}\rangle & x_{h_1} & \\ |h_{22}\rangle & & x_{h_2} \end{array} - \langle x_g \rangle |w\rangle \langle w|.$$

We use $F - M \geq 0 \iff \mathbb{I} - \sqrt{F}^{-1} M \sqrt{F}^{-1} \geq 0$ for $F > 0$, to obtain $\mathbb{I} \geq \langle x_g \rangle |w''\rangle \langle w''|$, where $|w''\rangle = \frac{\sqrt{\frac{p_{h_1}}{x_{h_1}}}|h_{11}\rangle + \sqrt{\frac{p_{h_2}}{x_{h_2}}}|h_{22}\rangle}{N_h}$. Normalizing this we get $|w'\rangle = \frac{|w''\rangle}{\sqrt{\langle \frac{1}{x_h} \rangle}}$ which entails $\mathbb{I} \geq \langle x_g \rangle \langle \frac{1}{x_h} \rangle |w'\rangle \langle w'|$ and

that leads us to the final condition $\frac{1}{\langle x_g \rangle} \geq \langle \frac{1}{x_h} \rangle$.

In fact all the techniques used in reaching this result can be extended to the $m \to n$ transition case as well and so the aforesaid result holds in general.

C.   Approaching bias $\varepsilon(k) = 1/(4k + 2)$

LEMMA C.1. *Consider an n-dimensional vector space, a diagonal matrix $X = diag(x_1, x_2 \ldots x_n)$ and a vector $|c\rangle = (c_1, c_2 \ldots, c_n)$ where all the x_is are distinct and all the c_i are non-zero. Then, the vectors $|c\rangle, X |c\rangle, \ldots X^{n-1} |c\rangle$ span the vector space.*

PROOF. We write the vectors as

$$|\tilde{w}_i\rangle = X^{i-1} |c\rangle = \begin{bmatrix} x_1^{i-1} c_1 \\ x_2^{i-1} c_2 \\ \vdots \\ x_n^{i-1} c_n \end{bmatrix}.$$

We show that the set of vectors are linearly independent, which is equivalent to showing that the determinant of the matrix containing the vectors as rows (or equivalently as columns) is non-zero, i.e.

$$\det \left(\underbrace{\begin{bmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & & x_n \\ x_1^2 & x_2^2 & & x_n^2 \\ \vdots & & \ddots & \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{bmatrix}}_{:=\tilde{X}} \begin{bmatrix} c_1 & & & \\ & c_2 & & \\ & & \ddots & \\ & & & c_n \end{bmatrix} \right) = c_1 \cdot c_2 \cdot \ldots c_n \cdot \det \tilde{X}$$

is non-zero. Notice that $\tilde{X}$ is the so-called Vandermonde matrix (restricted to being a square matrix) and its determinant, known as the Vandermonde determinant, is $\det(\tilde{X}) = \prod_{1 \leq i \leq j \leq n}(x_j - x_i) \neq 0$ as x_is are distinct. As c_is are all non-negative our proof is complete.   ∎

C.1   Proof of 5.2

In our proof we will need the following C.2, which gives a property of the $f-$assignments.

LEMMA C.2. $\sum_{i=1}^{n} \frac{f(x_i)}{\prod_{j \neq i}(x_j - x_i)} = 0$ where $f(x_i)$ is a polynomial of order $k \leq n - 2$ where $x_i \in \mathbb{R}$ are distinct.

The proof can be found in [32, 3].

PROOF OF 5.2. The equality $\langle x^k \rangle = 0$ for $k \leq n - 2$ is a direct consequence of C.2, and we proceed to prove the inequality $\langle x^{n-1} \rangle > 0$. Suppose for now that (we prove it in the end)

$$\sum_{i=1}^{n} \frac{x_i^{n-1}}{\prod_{j \neq i}(x_j - x_i)} = (-1)^{n-1}. \tag{24}$$

Define $p(x_i) = \frac{-(-x_i)^m}{\prod_{j \neq i}(x_j - x_i)}$ so that $t = \sum_i p(x_i) [\![x_i]\!]$. Observe that

$$\langle x^{n-1} \rangle = \sum_i x_i^{n-m-1} p(x_i)$$

$$= \sum_i (-1)^m x_i^{n-1} \frac{-1}{\prod_{j \neq i}(x_j - x_i)}$$

$$= (-1)^m (-1) \sum_i \frac{x_i^{n-1}}{\prod_{j \neq i}(x_j - x_i)}$$

$$= (-1)^m (-1)(-1)^{n-1} = (-1)^{m+n}$$

where we used Equation Equation (24).

It remains to prove Equation Equation (24). We show that $d(n) = \sum_{i=1}^{n} \frac{x_i^{n-1}}{\prod_{j \neq i}(x_j - x_i)} = (-1)^{n-1}$ by induction. The base of the induction gives us $d(2) = \frac{x_1}{x_2 - x_1} + \frac{x_2}{x_1 - x_2} = -1$. We continue by assuming that it holds for $d(n)$ and take

$$d(n+1) = \sum_{i=1}^{n+1} \frac{x_i^n}{\prod_{j \neq i}(x_j - x_i)} = \sum_{i=1}^{n+1} \frac{-(x_{n+1} - x_i)x_i^{n-1} + x_{n+1}x_i^{n-1}}{\prod_{j \neq i}(x_j - x_i)}$$

$$= -\sum_{i=1}^{n+1} (x_{n+1} - x_i) \frac{x_i^{n-1}}{\prod_{j \neq i}(x_j - x_i)} + x_{n+1} \underbrace{\sum_{i=1}^{n+1} \frac{x_i^{n-1}}{\prod_{j \neq i}(x_j - x_i)}}_{= 0, \text{ from C.2}}$$

$$= -\sum_{i=1}^{n} \frac{x_{n+1} - x_i}{x_{n+1} - x_i} \frac{x_i^{n-1}}{\prod_{j \neq i, n+1}(x_j - x_i)} + (x_{n+1} - x_{n+1}) \frac{x_{n+1}^{n-1}}{\prod_{j \neq n+1}(x_j - x_{n+1})} = -d(n).$$

This completes the proof.   ■

C.2   Restricted decomposition into f_0-assignments

The monomial decomposition we presented in Section 5.1 is not unique. Here, we give another useful decomposition that, however, only works in a restricted case; that is when the roots of f are right roots, as described below.

LEMMA C.3 (f **with right roots to** f_0). *Consider a set of real coordinates satisfying $0 < x_1 < x_2 \cdots < x_n$ and let $f(x) = (r_1 - x)(r_2 - x)\ldots(r_k - x)$ where $k \leq n - 2$ and the roots $\{r_i\}_{i=1}^k$ of f are right roots, i.e. they are such that for every root r_i there exists a distinct coordinate $x_j < r_i$. Let $t = \sum_{i=1}^n p_i \llbracket x_i \rrbracket$ be the corresponding f-assignment. Then, there exist f_0-assignments, $\{t_{0;j}\}$, on a subset of $(x_1, x_2 \ldots x_n)$, such that $t = \sum_{i=1}^m \alpha_i t_{0;i}$ where $\alpha_i > 0$ is a real number and $m > 0$ is an integer.*

PROOF. For simplicity, assume that $x_i < r_i$, $\forall i$, but the argument works in general. We can, then, write

$$
\begin{aligned}
t &= \sum_{i=1}^n \frac{-f(x_i)}{\prod_{j\neq i}(x_j - x_i)} \llbracket x_i \rrbracket \\
&= \sum_{i=1}^n \left(\frac{-(r_1 - x_i)(r_2 - x_i)\ldots(r_k - x_i)}{\prod_{j\neq i}(x_j - x_i)} + \frac{-(x_1 - x_i)(r_2 - x_i)\ldots(r_k - x_i)}{\prod_{j\neq i}(x_j - x_i)} \right) \llbracket x_i \rrbracket \\
&= (r_1 - x_1) \sum_{i=1}^n \frac{-(r_2 - x_i)\ldots(r_k - x_i)}{\prod_{j\neq i}(x_j - x_i)} \llbracket x_i \rrbracket + \sum_{i=2}^n \frac{-(r_2 - x_i)\ldots(r_k - x_i)}{\prod_{j\neq i,1}(x_j - x_i)} \llbracket x_i \rrbracket,
\end{aligned}
$$

where the first term has the same form that we started with (except for a positive constant which is irrelevant for the EBM/ validity condition, see Proposition 3.14) but with the polynomial having one less degree. The second term also has the same form, except that the number of points involved has been reduced. Note how this process relies crucially on the fact that $r_1 - x_1 > 0$; otherwise the term on the left would, by itself, not correspond to a valid move. This process can be repeated until we obtain a sum of f_0-assignments on various subsets of $(x_1, x_2 \ldots x_n)$. ∎

The advantage of this decomposition is that we can immediately apply it to the f-assignment of the bias-1/10 game. This is relevant because constructing solutions to f_0-assignments is relatively easy and so they, together with this result, allow us to derive the 1/10 bias protocol circumventing the perturbative approach that we used in Section 4.

EXAMPLE C.4 (The main $1/10$ **move.).** The key move in the 1/10-bias point game has its coordinates given by x_0, x_1, x_2, x_3, x_4 and roots given by l_1, r_1, r_2 which satisfy $x_0 < l_1 < x_1 < x_2 < x_3 < x_4 < r_1 < r_2$. Each root is a right root here because $x_0 < l_1, x_3 < r_1, x_4 < r_2$. Hence, from C.3, this assignment can be expressed as a combination of f_0-assignments defined over subsets of the initial set of coordinates and each f_0-assignment admits a simple solution given by Proposition 5.7 and Proposition 5.8 .   ◆
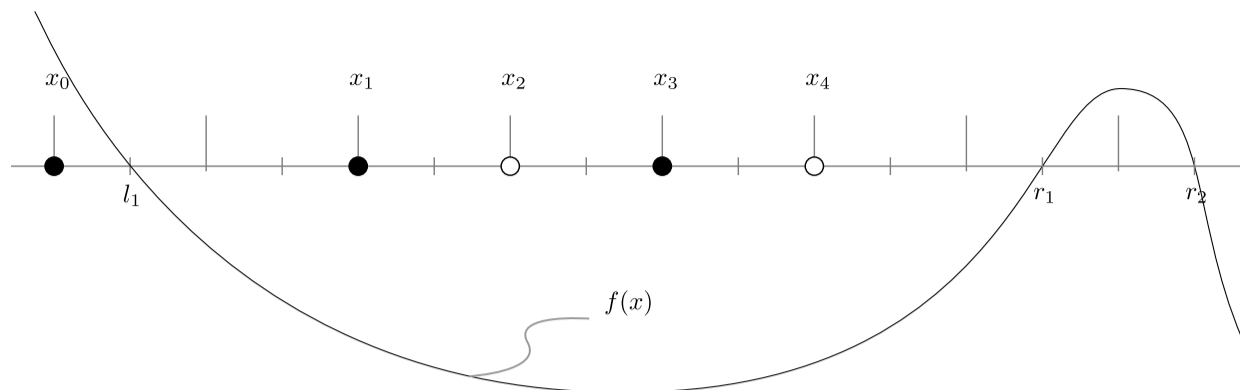
Figure 14. The main 1/10 move involves $n = 5$ points. f has $k = 3$ roots, all of which are right roots.

Another simple example is the class of f-assignments describing merge moves (see Example 3.16). We place the roots of f in such a way that all points, except one, have negative weights.
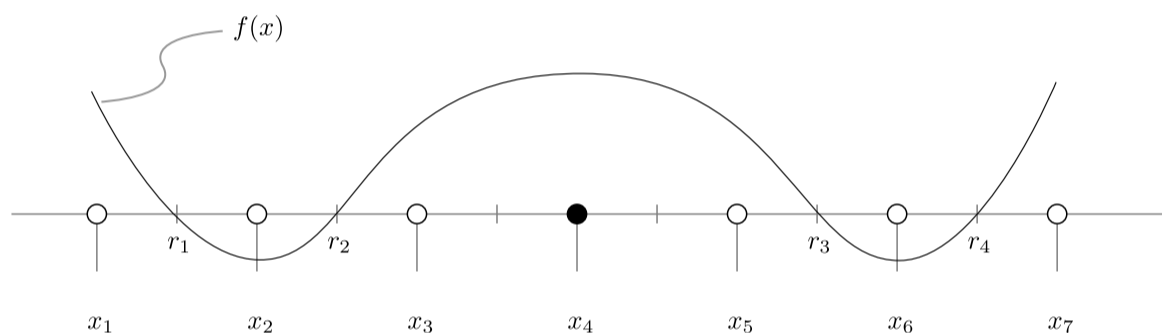

Figure 15. Merge involving $n = 7$ points. f has in total $k = n - 3 = 4$ right roots.

EXAMPLE C.5 (Merge). For merges (see Figure 15) we only get right-roots and hence, we can write them as sums of f_0-assignments and obtain the solution using Proposition 5.7 and Proposition 5.8. For n points, the polynomial has degree $n - 3$ and so $\langle x \rangle = 0$, just as expected for a merge.   ◆

This scheme fails for moves corresponding to lower bias games. For instance, the main move of the bias 1/14 game has its coordinates given by $x_0, x_1, x_2, x_3, x_4, x_5, x_6$ and the roots of f are l_1, l_2, r_1, r_2, r_3 satisfying $x_0 < l_1 < l_2 < x_1 < x_2 \cdots < x_6 < r_1 < r_2 < r_3$. Here, we can either consider l_1 to be a right root, in which case l_2 is a left root (i.e. a root which is not a right root). Or we can consider l_2 to be a right root in which case l_1 becomes a left root. Thus for games with bias 1/14 and less, we must revert to 5.4, which means we can not – at least by this scheme – avoid finding the solution to all the monomial assignments.

Since we mentioned the merge move, for completeness let us consider also the split move (see Example 3.17). The situation (see Figure 16) is similar to that of merge but with one key

distinction: the polynomial has degree $n - 2$; it has $n - 3$ right roots and one left root. Thus, it can not be expressed as a sum of f_0-assignments using C.3. Of course, merges and splits by themselves are not of much interest in this discussion because we already know that the Blinkered Unitary solves them both (see Section 4.3).
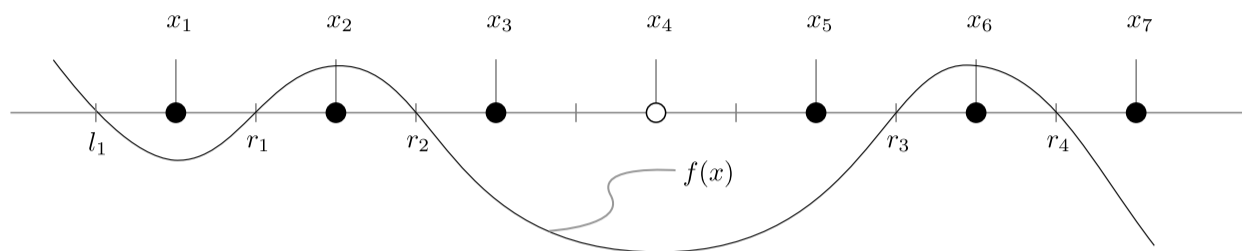

Figure 16. Split involving 7 points. f has $k = n - 2 = 5$ roots; 4 right and one left.