Analytic quantum weak coin flipping protocols with arbitrarily small bias

Atul Singh Arora, Jérémie Roland and Chrysoula Vlachou
Université libre de Bruxelles, Belgium

Abstract

Weak coin flipping (WCF) is a fundamental cryptographic primitive, where two distrustful parties need to remotely establish a shared random bit whilst having opposite preferred outcomes. A WCF protocol is said to have bias ϵ if neither party can force their preferred outcome with probability greater than $1/2+\epsilon$. Classical WCF protocols are shown to have bias $1/2$, i.e., a cheating party can always force their preferred outcome. A lower bias can only be achieved by employing extra assumptions, such as computational hardness. On the other hand, there exist quantum WCF protocols with arbitrarily small bias, as Mochon showed in his seminal work in 2007 [arXiv:0711.4114]. In particular, he proved the existence of a family of WCF protocols approaching bias $\epsilon(k) = 1/(4k+2)$ for arbitrarily large k and proposed a protocol with bias $1/6$. Last year, Arora, Roland and Weis presented a protocol with bias $1/10$ and to go below this bias, they designed an algorithm that *numerically* constructs unitary matrices corresponding to WCF protocols with arbitrarily small bias [STOC'19, p.205-216]. In this work, we present new techniques which yield a fully analytical construction of WCF protocols with bias arbitrarily close to zero, thus achieving a solution that has been missing for more than a decade. Furthermore, our new techniques lead to a simplified proof of existence of WCF protocols by circumventing the non-constructive part of Mochon's proof. We also include a concrete example illustrating a WCF protocol with bias $1/14$.

1 Introduction

Coin flipping (CF), introduced by Blum [6], is an important cryptographic primitive which permits two distrustful parties to remotely generate an unbiased random bit in spite of the fact that one of them might be dishonest and try to force a specific outcome. Like bit commitment (BC) and oblivious transfer (OT), it is a basic primitive for secure 2-party computation, a special case of secure multi-party computation, where the parties need to jointly compute a function on their inputs while keeping these inputs private. In the classical scenario, these primitives are shown to be computationally secure, and without extra assumptions (e.g. computational hardness) the dishonest party can always cheat perfectly [10]. Moving to the quantum scenario, BC and OT protocols have a non-zero lower bound on their bias [8, 7]; achieving perfect security is not possible, but still they perform better than their classical counterparts without computational hardness assumptions. The two distinct variants of CF, namely strong CF (SCF) and weak CF (WCF), behave differently in the quantum scenario. In SCF the desired outcome of each party is not known a priori, i.e., none of the parties know beforehand whether the other prefers outcome 0 or 1. Just like for quantum BC and OT, there is a lower bound on the bias of SCF protocols [14, 13]. The best known explicit quantum SCF protocols had bias $\frac{1}{4}$ [3, 18, 12]. For a quantum WCF protocol though, where the preferred outcome of each party is known, the situation is different. In his seminal work, Mochon [17] proved the existence of a family of WCF protocols achieving arbitrarily close to zero bias, thus showing that WCF is the only secure 2-party computation primitive with arbitrarily close to perfect security. Moreover, Kerenidis and Chailloux showed that perfect WCF can be used as a block box to obtain the optimal protocols for quantum SCF and BC [9, 8], i.e. the protocols with the lowest possible bias $\frac{1}{\sqrt{2}} - \frac{1}{2}$, therefore Mochon's result is highly relevant for the whole area of quantum secure 2-party (and multi-party) computation. However, his proof was not constructive and the proposal of an explicit protocol with almost zero bias was left as an open problem, while only an explicit protocol with bias $\frac{1}{6}$ was presented. In fact, first, a WCF protocol with bias $\frac{1}{\sqrt{2}} - \frac{1}{2}$ was reported [19], which incidentally matched the *lower bound* for the bias of *SCF* protocols, undermining even the existence of better WCF protocols and the distinction between them. Later, Mochon's lengthy and highly technical proof was verified and simplified [2], but still a protocol with bias below $\frac{1}{6}$ was missing. Last year Arora, Roland and Weis proposed an explicit protocol with bias $\frac{1}{10}$, and designed an algorithm that can *numerically* construct unitary matrices corresponding to protocols with arbitrarily small bias [5]. In the present work, we report the *analytical* solution to the WCF problem, by determining the unitary matrices that constitute WCF protocols with arbitrarily small bias.

2 Background and overview of the result

A quantum WCF protocol can be described as follows: the two parties, say A and B, are located in different places and, besides their local register, they also have a register that they can exchange, called the message register. At each round, the party that holds the message register can apply a local unitary on it and on their local register. After a number of rounds, the parties perform a final measurement on their local registers, and the outcome determines the winner. Assume that A wins on outcome 0, while B wins on outcome 1. If both parties are honest and follow the protocol, they have equal probabilities of winning $P_A = P_B = 1/2$. If one of the parties is cheating and tries to force the other player to output their desired outcome, then their probability of winning is, in general, higher. We denote this probability by P_A^* for A being dishonest and P_B^* for dishonest B. Let $\epsilon \geq 0$ be the smallest number such that both P_A^* and P_B^* are upper bounded by $\frac{1}{2} + \epsilon$. Then we say that the protocol has *bias* ϵ.[1] To calculate $P_{A/B}^*$ one can write a semi-definite program (SDP) that maximizes this cheating probability, given that the honest party follows the protocol. Using the SDP duality, this maximization problem can be written as a minimization problem over the respective

[1]The case where both A and B are dishonest is of no interest, as it is protocol-independent.

dual variables $Z_{A/B}$. However, the above holds given that we already have a protocol. Therefore, a new framework is needed, permitting us to find both the protocol and its bias.

A ground-breaking idea was provided by Kitaev (as Mochon describes in [17]), who transformed these SDPs into the so-called *time-dependent point games* (TDPG). A TDPG is a sequence of frames that include points on the positive quadrant of the $x - y$ plane with a probability weight assigned to each point. The TDPGs that we consider are determined by specific initial and final configurations and there are rules on how to move from one frame to the next. The initial frame has two points with coordinates $[\![0, 1]\!]$ and $[\![1, 0]\!]$ and probability weight $1/2$ each, while the final frame we want to obtain has only one point at $[\![\beta, \alpha]\!]$ with probability weight 1. Consider one frame, and restrict to the set of points along a horizontal line, i.e. points with the same y coordinate. We denote the $x-$coordinates of the ith such point by x_{g_i} and the respective probability weight by p_{g_i}, with $i \in \{1, 2 \dots n_g\}$. In the subsequent frame, restrict again to a set of points with the same y coordinate as before. Let the $x-$coordinates of the ith such point be x_{h_i} and the respective probability weight be p_{h_i}, with $i \in \{1, 2 \dots n_h\}$. The rules for transitioning between subsequent frames can be written as follows:

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

Analogous rules exist for moving points along vertical lines. Some examples of such permitted moves are the *raises*, where we move a point along a horizontal or vertical line by increasing its coordinate, the *splits*, where we split a point into several others, and the *merges*, where we merge several points into a single point.

It was shown that for any TDPG with transitions respecting Equation (1), there exists a WCF protocol with cheating probabilities $P_A^* = \alpha + \delta$ and $P_B^* = \beta + \delta$, where δ can be made arbitrarily small, and vice versa. Thus, the initial task of finding a protocol and solving the associated SDPs minimising $P_{A/B}^*$, is reduced to finding a TDPG such that the point $[\![\beta, \alpha]\!]$ of the final frame is as close to $[\![\frac{1}{2}, \frac{1}{2}]\!]$ as possible, corresponding to the zero-bias case. These TDPGs are called *expressible by matrices (EBM)* point games, and they are defined below.

Definition 1. Let $Z \geq 0$[2] be a Hermitian matrix and $\Pi^{[z]}$ be the projector on the eigenspace of the eigenvalue z of Z. Let $|\psi\rangle$ be a vector (not necessarily normalised), and define the finitely supported function $\text{Prob}[Z, |\psi\rangle] : [0, \infty) \to [0, \infty)$ as

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

Let $g, h : [0, \infty) \to [0, \infty)$ be two finitely supported functions. The line transition $g \to h$ is called *EBM* if there exist two matrices $0 \leq G \leq H$ and a vector $|\psi\rangle$, such that $g = \text{Prob}[G, |\psi\rangle]$ and $h = \text{Prob}[H, |\psi\rangle]$.

Definition 2. Let $g, h : [0, \infty) \times [0, \infty) \to [0, \infty)$ be two finitely supported functions. The transition $g \to h$ is called an

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

Definition 3. An *EBM point game* is a sequence of finitely supported functions[3] $\{g_0, g_1, \dots, g_n\}$, such that

[2] This matrix inequality denotes that Z is a positive semi-definite matrix.

[3] As explained further in Section 3, $[\![a, b]\!](x, y) := \delta_{a,x}\delta_{b,y}$ where $\delta_{r,s}$ is the Kronecker Delta.

- $g_0 = \frac{1}{2}[\![0,1]\!] + \frac{1}{2}[\![1,0]\!]$ and $g_n = 1[\![\beta,\alpha]\!]$ for some $\alpha,\beta \in [0,1]$,
- for all even (odd) i the transition $g_i \to g_{i+1}$ is an EBM vertical (horizontal) transition.

In order to verify that a transition is EBM one has to check conditions involving matrices, thus the problem remains hard and yet another reduction is needed. For an EBM transition $g \to h$, one can consider the corresponding finitely supported *EBM function* to be $h - g$. The set of EBM functions is shown to be the same (up to the closures) as the set of the so-called *valid* functions. We omit both the definition of a valid function and the proof that the two sets are same, as they have been presented in previous works [17, 2]. We only highlight that checking if a transition is EBM is equivalent to verifying the validity of a suitably constructed function which is an easier task.

Mochon, following the above reductions, proved the existence of a WCF protocol with arbitrarily small bias, by proposing a suitable family of point games with valid transitions [17]. This family is parametrised by an arbitrary integer $k \geq 1$ that specifies the bias $\epsilon = \frac{1}{4k+2}$. More precisely, $2k$ is the number of points involved in the main move of the point game. He constructed a protocol with bias $\frac{1}{6}$, but he left as an open problem the construction of a protocol with almost zero bias. This problem has remained open since then, as translating the point game into a sequence of unitaries determining the protocol is, indeed, not easy. A step forward was recently taken in [5], where a framework, TDPG-to-Explicit-protocol Framework (TEF) was introduced, which allows the conversion of TDPGs into WCF protocols, granted that unitaries associated with the valid functions used in the games can be found. More precisely, if a unitary matrix O acting on $\mathrm{span}\{|g_1\rangle, |g_2\rangle, \ldots, |h_1\rangle, |h_2\rangle, \ldots\}$, and satisfying the constraints

$$O|v\rangle = |w\rangle \quad \text{and} \quad \sum_{i=1}^{n_h} x_{h_i} |h_i\rangle\langle h_i| - \sum_{i=1}^{n_g} x_{g_i} E_h O |g_i\rangle\langle g_i| O^\dagger E_h \geq 0, \tag{2}$$

can be found for every transition of a TDPG, then an explicit WCF protocol with the corresponding bias can be obtained using the TEF. The vectors $\left\{\{|g_i\rangle\}_{i=1}^{n_g}, \{|h_i\rangle_{i=1}^{n_h}\}\right\}$ are orthonormal and E_h is a projection on $\mathrm{span}\{|h_i\rangle\}$. Furthermore, x_{g_i} and x_{h_i} are the coordinates of the points of the initial and final frame, respectively, of the line transitions, and p_{g_i} and p_{h_i} their corresponding probability weights (see also Equation (1)). Note that there exist n_g and n_h points in the initial and final frame, respectively. Finally, $|v\rangle = \sum_i \sqrt{p_{g_i}}\,|g_i\rangle / \sqrt{\sum_i p_{g_i}}$ and $|w\rangle = \sum_i \sqrt{p_{h_i}}\,|h_i\rangle / \sqrt{\sum_i p_{h_i}}$. In fact the set of transitions which satisfy Equation (2) is the same (up to the closures) as the set of valid/EBM transitions (see Appendix A). Using a perturbative method in conjunction with the TEF, the authors in [5] *analytically* constructed a protocol with bias $\frac{1}{10}$, and to go below this bias they used tools from geometry, and designed the so-called *elliptic monotone align* algorithm, that *numerically* finds the matrices determining a protocol with arbitrarily small bias.

In the present work, we *analytically* construct explicit WCF protocols with arbitrarily small bias, and to this end, we consider the class of valid functions that Mochon uses in his family of point games approaching bias $\frac{1}{4k+2}$ for arbitrary integers $k \geq 1$. We refer to these valid functions as *f-assignments*, and when f is a monomial, we call them *monomial assignments*. We chose the term assignment to reflect the fact that these functions are assigning the appropriate probability weights to the points of the TDPGs. If we are able to construct unitaries satisfying Equation (2) with respect to the f-assignments of Mochon's TDPGs with bias $\epsilon \to 0$ (i.e. for $k \to \infty$), we have effectively solved our problem, since the aforementioned TEF enables the conversion of TDPGs to WCF protocols. We start by noticing that an even weaker condition is sufficient: suppose that a valid/EBM function can be written as a sum of valid/EBM functions; to obtain the protocol, it suffices to find unitaries corresponding to each valid function that appears in this sum (see Appendix A). We then solve the monomial assignments, i.e. we give formulae for the unitaries corresponding to monomial assignments, and show that they indeed satisfy Equation (2), obtaining, thus, an effective solution to the f-assignment. Our approach, in addition to yielding analytic WCF protocols with vanishing bias, has a feature that we would like to emphasize here. The reduction of the problem from EBM to valid functions is pivotal in the construction of Mochon's point game [17]. However, we can bypass this reduction and directly construct a WCF protocol once the matrices O, corresponding to the (effective) solutions to the transitions of the point game, which satisfy Equation (2) are known. By means of the TEF we can prove that this protocol has the same bias as the point game. Therefore, our approach is simpler than the previous ones, as it avoids the aforementioned—quite technical—reduction. Finally, in [4, 5] it was shown that functions expressible by *real* matrices (EBRM) are sufficient for obtaining the solution,[4] therefore from now on we restrict to orthogonal matrices.

3 f−assignments and their properties

We write finitely supported functions t in two ways: (1) as $t = \sum_{i=1}^{n} p_i [\![x_i]\!]$, where $|p_i| > 0$ for all $i \in \{1, 2 \ldots n\}$, and $x_i \neq x_j$ for $i \neq j$, and (2) as $t = \sum_{i=1}^{n_h} p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n_g} p_{g_i} [\![x_{g_i}]\!]$, where $p_{h_i}, p_{g_i} > 0$ and x_{h_i}, x_{g_i} are all distinct. By $[\![x_i]\!]$ we represent a point with coordinate x_i. More concretely, we have $[\![a]\!](x) = \delta_{a,x}$, where $\delta_{a,x}$ is the Kronecker delta.

Definition 4 (f-assignments)**.** Given a set of real coordinates $0 \leq x_1 < x_2 \cdots < x_n$ 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

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

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 $g = \sum_{i:p_i<0} (-p_i) [\![x_i]\!]$.

- We say 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.
- 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 the *zeroth assignment*.
- 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.

In the definition above the coordinates are real non-negative numbers, but in the next sections where we present the solutions, we consider the coordinates to be strictly positive. However, this is not really a restriction, because any f-assignment with a zero coordinate can be expressed as an f-assignment with strictly positive coordinates, in such a way that both have the same solution (see Lemma 15 in Appendix B).

Definition 5 ((Effectively) Solving an assignment)**.** 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 an orthonormal basis $\left\{ |g_1\rangle, |g_2\rangle \ldots |g_{n_g}\rangle, |h_1\rangle, |h_2\rangle \ldots |h_{n_h}\rangle \right\}$, we say that an orthogonal matrix O *solves* 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 $E_h = \sum_{i=1}^{n_h} |h_i\rangle \langle h_i|$. 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.

[4] This permitted the use of a geometric approach to achieve the numerical solution.

In Section 2, we claimed that in order to construct a WCF protocol with vanishing bias it suffices to obtain effective solutions to f−assignments. In particular, it suffices to express each f−assignment as a sum of monomial assignments and find the orthogonal matrices solving each monomial assignment appearing in the sum. In Appendix A we explain why this claim holds, and in Lemma 6 below we show how an f-assignment[5] can be trivially expressed as a sum of monomial assignments.

Lemma 6 (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 $k \leq n-2$.*[6] *Let $t = \sum_{i=1}^{n} p_i [\![x_i]\!]$ be the corresponding f-assignment. Then*

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

where $\alpha_l \geq 0$. More precisely, α_l is the coefficient of $(-x)^l$ in $f(x)$.

In the following sections we present the orthogonal matrices solving the four possible types of monomial assignments, namely balanced/unbalanced and aligned/misaligned (see Definition 4).

4 Solution to the zeroth assignment

In this section we present the solution for the simplest monomial assignment, which we call the *zeroth* assignment, since $f(x) = (-x)^0$. We start with the orthogonal matrices solving the balanced case, and prove their correctness.

Proposition 7 (Solution to balanced zeroth assignments)**.** *Let $t = \sum_{i=1}^{n} p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} p_{g_i} [\![x_{g_i}]\!]$ be a zeroth assignment over $0 < x_1 < x_2 \cdots < x_{2n}$, $\{|h_1\rangle, |h_2\rangle \dots |h_n\rangle, |g_1\rangle, |g_2\rangle \dots |g_n\rangle\}$ be an orthonormal basis, $E_h := \sum_{i=1}^{n} |h_i\rangle\langle h_i|$ be a subspace projector, and finally let*

$$X_h := \sum_{i=1}^{n} x_{h_i} |h_i\rangle\langle h_i| \doteq diag(x_{h_1}, x_{h_2} \dots x_{h_n}, \underbrace{0, 0 \dots 0}_{n\text{-}zeros}),$$

$$X_g := \sum_{i=1}^{n} x_{g_i} |g_i\rangle\langle g_i| \doteq diag(\underbrace{0, 0, \dots 0}_{n\text{-}zeros}, x_{g_1}, x_{g_2} \dots x_{g_n}),$$

$$|w\rangle := \sum_{i=1}^{n} \sqrt{p_{h_i}} |h_i\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \dots \sqrt{p_{h_n}}, \underbrace{0, 0 \dots 0}_{n\text{-}zeros})^T$$

$$|v\rangle := \sum_{i=1}^{n} \sqrt{p_{g_i}} |g_i\rangle \doteq (\underbrace{0, 0 \dots 0}_{n\text{-}zeros}, \sqrt{p_{g_1}}, \sqrt{p_{g_2}} \dots \sqrt{p_{g_n}})^T.$$

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

$$X_h \geq E_h O X_g O^T E_h \quad and \quad O|v\rangle = |w\rangle,$$

[5] with real and non-negative roots,

[6] This restriction on the number of roots is justified by the forthcoming use of the f−assignment.

where $\Pi^{\perp}_{h_{-1}} = \Pi^{\perp}_{g_{-1}} = \mathbb{I}$, $\Pi^{\perp}_{h_i}$ *:= projector orthogonal to span*$\{(X_h)^i |w\rangle, (X_h)^{i-1}|w\rangle, \dots |w\rangle\}$, $c_{h_i} := \langle w| (X_h)^i \Pi^{\perp}_{h_{i-1}} (X_h)^i |w\rangle$, *and analogously are defined the forms of* $\Pi^{\perp}_{g_i}$ *and* c_{g_i}.

Proof. Lemma 17 from Appendix B gives us the following properties of the zeroth assignment:

$$\left\langle x^k \right\rangle = 0, \qquad \text{for all } k \in \{0, 1, 2 \dots, 2n-2\}, \text{ and} \tag{3}$$

$$\left\langle x^{2n-1} \right\rangle > 0. \tag{4}$$

We define the basis of interest by essentially using the Gram-Schmidt procedure. Let

$$\begin{aligned} |w_0\rangle &:= |w\rangle \\ |w_1\rangle &:= \frac{(\mathbb{I} - |w_0\rangle\langle w_0|)(X_h)|w\rangle}{\sqrt{c_{h_1}}} \\ &\vdots \\ |w_k\rangle &:= \frac{\left(\mathbb{I} - \sum_{i=0}^{k-1} |w_i\rangle\langle w_i|\right)(X_h)^k |w\rangle}{\sqrt{c_{h_k}}}. \end{aligned} \tag{5}$$

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 in the numerator 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, as $\Pi_{h_i} := \mathbb{I} - \Pi^{\perp}_{h_i} = \sum_{j=0}^{i} \left|w_j\right\rangle\left\langle w_j\right|$. It also follows that O can be re-written as

$$O = \sum_{j=0}^{n-1} \left(\left|w_j\right\rangle\left\langle v_j\right| + \left|v_j\right\rangle\left\langle w_j\right| \right),$$

where $\left|v_j\right\rangle$ is analogously defined (by replacing h with g). It is evident that $O|v\rangle = |w\rangle$. We set $D = X_h - E_h O X_g O^T E_h$, and note that $\left\langle v_j\right| D |v_i\rangle = 0$ (because $X_h|v_i\rangle = 0$ and $E_h|v_i\rangle = 0$[7]). We assert that it has the following rank-1 form

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

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

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

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 $\langle w_i| X_h \left|w_j\right\rangle$ can be deduced by observing

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

For the analogous expression with g to be the same, we must have $2i, 2j$ and $i+j+1$ less than or equal to $2n-2$. The first two 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.

[7]The conclusion holds even without the projector as O maps span$(|v_1\rangle, |v_2\rangle, \dots |v_n\rangle)$ to span$(|w_1\rangle, |w_2\rangle \dots |w_n\rangle)$ 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 $\left\langle x_h^k \right\rangle$ and $\left\langle x_g^k \right\rangle$ respectively, only terms with $k > 2n-2$ would remain; the others would get cancelled due to Equation (3). Using Equation (5), 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 $c_{h_{n-1}} = c_{h_{n-1}}(\left\langle x_h^{2n-2}\right\rangle, \left\langle x_h^{2n-3}\right\rangle, \ldots, \left\langle x_h^{1}\right\rangle)$ does not depend on $\left\langle x_h^{2n-1}\right\rangle$ (we proceed analogously for $c_{g_{n-1}}$). Further, $c_{h_{n-1}} = c_{g_{n-1}} =: c_{n-1}$. We thus have

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

using Equation (4). Thus, $X_h - E_h O X_g O^T E_h \geq 0$. Note that we assumed $\mathrm{span}\{|w\rangle, X_h|w\rangle, X_h^2|w\rangle, \ldots, X_h^n|w\rangle\}$ equals to $\mathrm{span}\{|h_1\rangle, |h_2\rangle \ldots |h_n\rangle\}$ which is justified by Lemma 16, presented in Appendix B. □

Before proceeding to the unbalanced zeroth assignments, let us try to better understand the above result and see why it doesn't work unchanged in the unbalanced case. We could write $D_{ij} = \langle w_i| D |w_j\rangle$ and note that the maximum power l which appears as $\left\langle x^l_{g/h}\right\rangle$ is given by $\max\{2i, 2j, i+j+1\}$. This yields a matrix with each term depending on the power as

$$D = \begin{bmatrix} D_{00}(\langle x\rangle) & & & & \text{h.c.} & \\ D_{10}(\langle x^2\rangle, \ldots) & D_{11}(\langle x^3\rangle, \ldots) & & & & \\ D_{20}(\langle x^4\rangle, \ldots) & D_{21}(\langle x^4\rangle, \ldots) & D_{22}(\langle x^5\rangle, \ldots) & & & \\ D_{30}(\langle x^6\rangle, \ldots) & D_{31}(\langle x^6\rangle, \ldots) & D_{32}(\langle x^6\rangle, \ldots) & D_{33}(\langle x^7\rangle, \ldots) & & \\ D_{40}(\langle x^8\rangle, \ldots) & D_{41}(\langle x^8\rangle, \ldots) & D_{42}(\langle x^8\rangle, \ldots) & D_{43}(\langle x^8\rangle, \ldots) & D_{44}(\langle x^9\rangle, \ldots) & \\ & & & & & \ddots \end{bmatrix}.$$

For brevity, we represent this dependence as

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

Consider the balanced m_0 case over $\{x_1, x_2, x_3, x_4\}$, where we have $\langle x\rangle = \langle x^2\rangle = 0$ and $\langle x^3\rangle > 0$. This is a two-dimensional case, thus

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

If we now try to use the same procedure for an unbalanced zeroth assignment over $\{x_1, x_2 \ldots x_5\}$, we will have $\langle x\rangle = \langle x^2\rangle = \langle x^3\rangle = 0$ and $\langle x^4\rangle > 0$. If we try to solve in three dimensions, we would obtain

$$\mathcal{M}(D) = \begin{bmatrix} 0 & 0 & \langle x^4\rangle \\ 0 & 0 & \langle x^4\rangle \\ \langle x^4\rangle & \langle x^4\rangle & \langle x^5\rangle \end{bmatrix} \tag{6}$$

which does not seem to work directly. It turns out that the projector that was present in Equation (2), gets rid of the troublesome part and yields a zero matrix. We see it in this example first and then generalize it. The 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 orthogonal matrix as before, except that we leave $|v_2\rangle$ unchanged, i.e. $O = \sum_{i=0}^{1} |w_i\rangle\langle v_i| + |v_2\rangle\langle v_2|$. We can now show that $D' = X_h - E_h O X_g O^T E_h \geq 0$ because every vector in $|\psi\rangle \in \mathrm{span}\{|v_0\rangle, |v_1\rangle, |v_2\rangle\}$ satisfies $D'|\psi\rangle = 0$ (as $X_h|\psi\rangle = 0$ and $E_h|\psi\rangle = 0$). This means that it suffices to restrict to a 2×2 matrix in $\mathrm{span}\{|w_0\rangle, |w_1\rangle\}$. But, from Equation (6), we already know that this is zero, hence $D' = 0$.

Proposition 8 (Solution to unbalanced zeroth 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 a zeroth assignment over $0 < x_1 < x_2 \cdots < x_{2n-1}$, $\{|h_1\rangle, |h_2\rangle \dots |h_{n-1}\rangle, |g_1\rangle, |g_2\rangle \dots |g_n\rangle\}$ be an orthonormal basis, $E_h := \sum_{i=1}^{n} |h_i\rangle\langle h_i|$ a subspace projector, and finally let*

$$X_h := \sum_{i=1}^{n-1} x_{h_i} |h_i\rangle\langle h_i| \doteq diag(x_{h_1}, x_{h_2} \dots x_{h_{n-1}}, \underbrace{0, 0, \dots 0}_{n\ zeros}),$$

$$X_g := \sum_{i=1}^{n} x_{g_i} |g_i\rangle\langle g_i| \doteq diag(\underbrace{0, 0, \dots 0}_{n-1\ zeros}, x_{g_1}, x_{g_2} \dots x_{g_{n-1}}, x_{g_n}),$$

$$|w\rangle := \sum_{i=1}^{n-1} \sqrt{p_{h_i}} |h_i\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}}, \dots \sqrt{p_{h_{n-1}}}, \underbrace{0, 0 \dots 0}_{n\ zeros})^T,$$

$$|v\rangle := \sum_{i=1}^{n} \sqrt{p_{g_i}} |g_i\rangle \doteq (\underbrace{0, 0, \dots 0}_{n-1\ zeros}, \sqrt{p_{g_1}}, \sqrt{p_{g_2}} \dots \sqrt{p_{g_{n-1}}}, \sqrt{p_{g_n}})^T.$$

Then,

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

satisfies

$$X_h \geq E_h O X_g O^T E_h \quad and \quad E_h O |v\rangle = |w\rangle,$$

where $\Pi^{\perp}_{h_{-1}} = \Pi^{\perp}_{g_{-1}} = \mathbb{I}$, $\Pi^{\perp}_{h_i} :=$ projector orthogonal to $\mathrm{span}\{(X_h)^i|w\rangle, (X_h)^{i-1}|w\rangle, \dots |w\rangle\}$, $c_{h_i} := \langle w| (X_h)^i \Pi^{\perp}_{h_{i-1}} (X_h)^i |w\rangle$, and analogous are the forms of $\Pi^{\perp}_{g_i}$ and c_{g_i}.

Proof. By using again Lemma 17 from Appendix B, we have

$$\left\langle x^k \right\rangle = 0 \ \text{ for } \ k \in \{0, 1, \dots 2n-3\}, \tag{7}$$

and

$$\left\langle x^{2n-2} \right\rangle > 0.$$

We define the basis, almost exactly as before, we set $|w_0\rangle := |w\rangle$ and for each integer k satisfying $0 \leq k \leq n-2$ 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 define $|v_0\rangle := |v\rangle$ and for each integer satisfying $0 \leq k \leq n-1$ we have

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

Note that this means $O = \sum_{i=0}^{n-2} (|w_i\rangle\langle v_i| + |v_i\rangle\langle w_i|) + |v_{n-1}\rangle\langle v_{n-1}|$ and so $E_h O|v\rangle = |w\rangle$ follows directly. Also, to establish $D := X_h - E_h O X_g O^T E_h \geq 0$, note that it suffices to show that $\langle w_i| D |w_j\rangle \geq 0$ for integers i, j satisfying $0 \leq i, j \leq n-2$. This is because, as we saw in the previous case, $D|v_i\rangle = 0$ as $X_h|v_i\rangle = 0$ and $E_h|v_i\rangle = 0$. As before, we indicate the term with the highest power of X_h appearing in $|w_k\rangle$, for k in $\{0, 1 \ldots n-2\}$, by

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

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

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

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

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

and similarly

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

The highest possible power is obtained when $i = j = n-2$. This yields $2n-3$ and thus, using Equation (7), we conclude that $\langle w_i| D |w_j\rangle$ is zero for all $0 \leq i, j \leq n-2$, establishing in fact that $D = 0$. □

5 Solution to the monomial assignments

In this section we present the solutions to the monomial assignments of order higher than zero. There are four different cases, depending on the number of points and the degree of the monomial (balanced/unbalanced and aligned/misaligned, see Definition 4). One could find a single expression for all, but this does not seem to aid clarity, therefore we present and prove the four cases separately. Our approach is essentially the same as before. The main additional technique that we introduce here is the use of the pseudo-inverses $X_h^{\dashv}$ and $X_g^{\dashv}$.[8]

Proposition 9 (Solution to balanced aligned monomial assignments)**.** *Let $m = 2b$ be an even non-negative integer, $t = \sum_{i=1}^n x_{h_i}^m p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^n x_{g_i}^m p_{g_i} [\![x_{g_i}]\!]$ a monomial assignment over $0 < x_1 < x_2 \cdots < x_{2n}$, $\{|h_1\rangle, |h_2\rangle \ldots |h_n\rangle, |g_1\rangle, |g_2\rangle \ldots |g_n\rangle\}$ an orthonormal basis, and finally let*

$$X_h := \sum_{i=1}^n x_{h_i} |h_i\rangle\langle h_i| \doteq diag(x_{h_1}, x_{h_2} \ldots x_{h_n}, \underbrace{0, 0 \ldots 0}_{n \text{ zeros}}),$$

$$X_g := \sum_{i=1}^n x_{g_i} |g_i\rangle\langle g_i| \doteq diag(\underbrace{0, 0, \ldots 0}_{n \text{ zeros}}, x_{g_1}, x_{g_2} \ldots x_{g_n}),$$

$$|w\rangle := \sum_{i=1}^n \sqrt{p_{h_i}} |h_i\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_n}}, \underbrace{0, 0, \ldots 0}_{n \text{ zeros}})^T \quad and \quad |w'\rangle := (X_h)^b |w\rangle ,$$

$$|v\rangle := \sum_{i=1}^n \sqrt{p_{g_i}} |g_i\rangle \doteq (\underbrace{0, 0, \ldots 0}_{n \text{ zeros}}, \sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_n}})^T \quad and \quad |v'\rangle := (X_g)^b |v\rangle .$$

[8] For any Hermitian matrix A with spectral decomposition $A = \sum_i a_i |i\rangle\langle i|$ (including zero eigenvalues), we denote by $A^{\dashv}$ its pseudo-inverse $A^{\dashv} := \sum_{i:|a_i|>0} a_i^{-1} |i\rangle\langle i|$.

Then,

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

satisfies

$$X_h \geq E_h O X_g O^T E_h \quad \text{and} \quad E_h O |v'\rangle = |w'\rangle ,$$

where $E_h := \sum_{i=1}^{n} |h_i\rangle \langle h_i|$, *and for brevity, by* X_h^{-k} *we mean* $(X_h^{\dashv})^k$ *for* $k > 0$ *(similarly for* X_g*),*

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

$c_{h_i} := \langle w'| (X_h)^i \Pi^{\perp}_{h_i} (X_h)^i |w'\rangle$, *and analogous are the forms of* $\Pi^{\perp}_{g_i}$ *and* c_{g_i}.

Proposition 10 (Solution to balanced misaligned monomial assignments). *Let* $m = 2b - 1$ *be an odd non-negative integer,* $t = \sum_{i=1}^{n} x_{h_i}^{m} p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} x_{g_i}^{m} p_{g_i} [\![x_{g_i}]\!]$, *a monomial assignment over* $0 < x_1 < x_2 \dots < x_{2n}$, $\{|h_1\rangle , |h_2\rangle \dots |h_n\rangle , |g_1\rangle , |g_2\rangle \dots |g_n\rangle\}$ *an orthonormal basis, and finally let*

$$X_h := \sum_{i=1}^{n} x_{h_i} |h_i\rangle \langle h_i| \doteq diag(x_{h_1}, x_{h_2} \dots x_{h_n}, \underbrace{0, 0 \dots 0}_{n \text{ zeros}}),$$

$$X_g := \sum_{i=1}^{n} x_{g_i} |g_i\rangle \langle g_i| \doteq diag(\underbrace{0, 0, \dots 0}_{n \text{ zeros}}, x_{g_1}, x_{g_2} \dots x_{g_n}),$$

$$|w\rangle := (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \dots \sqrt{p_{h_n}}, \underbrace{0, 0 \dots 0}_{n \text{ zeros}}) \quad \text{and} \quad |w'\rangle := (X_h)^{b-\frac{1}{2}} |w\rangle ,$$

$$|v\rangle := (\underbrace{0, 0, \dots 0}_{n \text{ zeros}}, \sqrt{p_{g_1}}, \sqrt{p_{g_2}} \dots \sqrt{p_{g_n}}) \quad \text{and} \quad |v'\rangle := (X_g)^{b-\frac{1}{2}} |v\rangle .$$

Then,

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

satisfies

$$X_h \geq E_h O X_g O^T E_h \quad \text{and} \quad E_h O |v'\rangle = |w'\rangle ,$$

where $E_h := \sum_{i=1}^{n} |h_i\rangle \langle h_i|$, *and for brevity, by* X_h^{-k} *we mean* $(X_h^{\dashv})^k$ *for* $k > 0$ *(similarly for* X_g*),*

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

$c_{h_i} := \langle w'| (X_h)^i \Pi^{\perp}_{h_i} (X_h)^i |w'\rangle$, *and analogous are the forms of* $\Pi^{\perp}_{g_i}$ *and* c_{g_i}.

For the proofs and concrete examples of balanced aligned and misaligned monomial assignments, see Appendix C.

We similarly proceed to the unbalanced monomial assignments, aligned and misaligned. Below, we state the solution for both cases, while in Appendix D we prove their correctness and give concrete examples illustrating their construction.

Proposition 11 (Solution to the unbalanced aligned monomial assignments). *Let $m = 2b$ be an even non-negative integer, $t = \sum_{i=1}^{n-1} x_{h_i}^m p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} x_{g_i}^m p_{g_i} [\![x_{g_i}]\!]$ a monomial 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 let*

$$X_h := \sum_{i=1}^{n-1} x_{h_i} |h_i\rangle\langle h_i| \doteq diag(x_{h_1}, x_{h_2} \ldots x_{h_{n-1}}, \underbrace{0, 0 \ldots 0}_{n\ zeros}),$$

$$X_g := \sum_{i=1}^{n} x_{g_i} |g_i\rangle\langle g_i| \doteq diag(\underbrace{0, 0, \ldots 0}_{n-1\ zeros}, x_{g_1}, x_{g_2} \ldots x_{g_n}),$$

$$|w\rangle := (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_{n-1}}}, \underbrace{0, 0 \ldots 0}_{n\ zeros}) \quad and \quad |w'\rangle := (X_h)^b |w\rangle,$$

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

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

satisfies

$$X_h \geq E_h O X_g O^T E_h \quad and \quad E_h O |v'\rangle = |w'\rangle,$$

where for brevity, by X_h^{-k} we mean $(X_h^{\dashv})^k$ for $k > 0$ (similarly for X_g), $c_{h_i}, c_{g_i}, \Pi_{h_i}^{\perp}, \Pi_{g_i}^{\perp}$ are as defined in Proposition 9.

Proposition 12 (Solution to the unbalanced misaligned monomial assignments). *Let $m = 2b - 1$ be an odd non-negative integer, $t = \sum_{i=1}^{n} x_{h_i}^m p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n-1} x_{g_i}^m p_{g_i} [\![x_{g_i}]\!]$ a monomial assignment over $0 < x_1 < x_2 \cdots < x_{2n-1}$, $\{|h_1\rangle, |h_2\rangle \ldots |h_n\rangle, |g_1\rangle, |g_2\rangle \ldots |g_{n-1}\rangle\}$ be an orthonormal basis, and finally let*

$$X_h := \sum_{i=1}^{n} x_{h_i} |h_i\rangle\langle h_i| \doteq diag(x_{h_1}, x_{h_2} \ldots x_{h_n}, \underbrace{0, 0 \ldots 0}_{n-1\ zeros}),$$

$$X_g := \sum_{i=1}^{n-1} x_{g_i} |g_i\rangle\langle g_i| \doteq diag(\underbrace{0, 0, \ldots 0}_{n\ zeros}, x_{g_1}, x_{g_2} \ldots x_{g_{n-1}}),$$

$$|w\rangle := (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_n}}, \underbrace{0, 0 \ldots 0}_{n-1\ zeros}) \quad and \quad |w'\rangle := (X_h)^{b-\frac{1}{2}} |w\rangle,$$

$$|v\rangle := (\underbrace{0, 0, \ldots 0}_{n\ zeros}, \sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_{n-1}}}) \quad and \quad |v'\rangle := (X_g)^{b-\frac{1}{2}} |v\rangle.$$

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

satisfies
$$X_h \geq E_h O X_g O^T E_h \quad and \quad E_h O \left| v' \right\rangle = \left| w' \right\rangle,$$

where for brevity, by X_h^{-k} we mean $(X_h^{+})^k$ for $k > 0$ (similarly for X_g), $c_{h_i}, c_{g_i}, \Pi^{\perp}_{h_i}, \Pi^{\perp}_{g_i}$ are as defined in Proposition 10.

Combining all the above, we can now state our main result:

Theorem 13. *Let t be an f-assignment (see Definition 4) with f having real positive roots. Then, in order to obtain its effective solution (see Definition 5), it suffices to write it as $t = \sum_i \alpha_i t_i'$ (see Lemma 6), where α_i are positive and t_i' are monomial assignments. Furthermore, each monomial assignment t_i' admits an exact solution given in Proposition 9, Proposition 10, Proposition 11, or Proposition 12.*

Proof. We established that in order to determine the effective solution to an $f-$assignment t, it is sufficient to express it as a sum of monomial assignments $t_{i'}$ and find the solution for each one of them (see Appendix A). A monomial assignment can be balanced/unbalanced and aligned/misaligned (see Definition 4). The solution in each case is given by either Proposition 9, Proposition 10, Proposition 11, or Proposition 12. ◻

In Appendix E we directly apply Theorem 13 to analytically construct a WCF protocol with bias approaching $\frac{1}{14}$, as an example.

6 Conclusions and future work

We presented the analytical construction of explicit WCF protocols achieving arbitrarily close to zero bias, by means of Mochon's family of TDPGs [17], described by the respective $f-$assignments. Using the TEF from [5], these TDPGs can be converted into WCF protocols with the corresponding bias. In order to obtain the solution for an $f-$assignment, we argued that it suffices to write it as a sum of monomial assignments and find the solution for each term of the sum separately. For all four different types of monomial assignments, we constructed the corresponding solutions and proved that indeed satisfy the required conditions as stated in Equation (2) and the analysis following it. Importantly enough, our approach does not use the reduction of EBM functions to valid functions and it admits, thus, a simple and clear description. We also presented an example illustrating the construction of a WCF protocol with bias $\frac{1}{14}$.

There exist several related problems that deserve further study. First, one could try to find analytic solutions corresponding to $f-$assignments in fewer dimensions (assuming that they exist). This way, the only shortcoming of our approach concerning resource requirements could be improved: while expressing the f-assignment as a sum of monomial assignments we are increasing the dimensions, which in turn corresponds to an increase in the number of qubits required. One could also try to find analytic solutions for the Pelchat-Hoyer point games [11], which is another family of point games giving rise to WCF protocols with arbitrarily close to zero bias. Moreover, given the recently improved bound on the number of rounds of communication needed to achieve a certain bias ϵ [15], one can investigate whether there exist protocols matching these bounds. Finally, while one expects the bias to increase in the presence of noise, a thorough study of such effects is needed in order to determine the robustness of WCF protocols against noise.

Acknowledgements

We are thankful to Tom Van Himbeeck, Kishor Bharti, Stefano Pironio and Ognyan Oreshkov for various insightful discussions. We acknowledge support from the Belgian Fonds de la Recherche Scientifique – FNRS under grant no R.50.05.18.F (QuantAlgo). The QuantAlgo project has received funding from the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme. ASA further acknowledges the FNRS for support through the FRIA grants, 3/5/5 – MCF/XH/FC – 16754 and F 3/5/5 – FRIA/FC – 6700 FC 20759.

A Decomposing TEF functions into sums of TEF functions

In this first part of the appendix we present how one can construct a WCF protocol with bias ϵ, by decomposing the TEF functions (i.e., the functions that satisfy Equation (2) for some unitary matrix O[9]) of a so-called *time-independent point game* (TIPG)[10] with the same bias ϵ into a sum of TEF functions. This way, we establish our claim that, to convert Mochon's TIPGs (achieving vanishing bias) which rely non-trivially only on transitions defined by f-assignments, it is sufficient to find an effective solution thereof. In particular, it is sufficient to express an f-assignment as a sum of monomial assignments and find the solution to each one of them. In Lemma 14, we show that the set of TEF functions is the same as the set of valid functions, which in turn is the same as the closure of the set of EBM functions.[11] Henceforth, for simplicity, we only use the term valid functions. Our demonstration requires techniques and results from previous works [17, 1, 4, 5], which we do not present here in detail; we only refer to them and outline how they are used in our analysis. We recall from [17, 2] the basic idea behind the conversion of a TIPG into a TDPG (see, for e.g., the proof of Theorem 5 in [2]). The primary hinderance is that for applying a valid function in a TDPG, the places where the function is negative must already have points with at least as much weight. This corresponds to finding a time dependent ordering of the valid functions which define a TIPG, however, in general, TIPGs do not admit such simple orderings. This difficulty is surpassed by introducing the so-called *catalyst state*, which is a set of points with vanishing weights. They are a scaled-down compensation for the negative weights which arise. In their presence, an accordingly scaled-down version of the valid functions can be applied, repeatedly, until their cumulative effect is essentially the same as that of having applied the valid functions unaltered. The catalyst state, after this procedure, is effectively unchanged. The weight of the catalyst state costs us an increase in the bias. However, the weight can be made arbitrarily small, at the expense of extra rounds of communication. Our case is not very different. Suppose that the valid functions used in the TIPG are decomposed into a sum of valid functions. Let us call these valid functions (present in the decomposition), *constituent functions*. Then, we can convert the TIPG into a TDPG which only uses the constituent functions by essentially using the same technique. This is because the difficulty in constructing TDPGs using the constituent functions is of the same nature. In particular, it is possible that the constituent functions are negative at various locations, but there are no points present there. We can again use a catalyst state, scale the constituent functions accordingly, and proceed thereafter as in the original proof [1], to obtain the corresponding TDPG. The TEF from [4, 5] is then applied for this TDPG resulting in a WCF protocol approaching the same bias as the TIPG that we started with, in the limit of infinite rounds of communication.

Lemma 14 (TEF = Closure of EBM = valid)**.** *The set of the TEF functions (as defined above), the set of valid functions (for the definition, see e.g. [17, 1]) and the closure of the set of the EBM functions (for the definition*

[9] As already mentioned, restricting to real matrices is enough (see [5]), therefore we assume that the matrices O are orthogonal without loss of generality.

[10] TIPGs are presented and studied in numerous previous works [17, 1, 5].

[11] and the same holds for the closure of the set of EBRM functions, see [4, 5].

see Section 2) are the same.

Proof outline. We start by observing that the set of EBM functions is an open set. From Definition 1 we can see that the matrix H may have eigenvectors which have no support on $|\psi\rangle$. Consequently, one can consider a sequence of EBM functions t_i such that the $\lim_{i\to\infty} t_i = t$ is well-defined, while the associated matrix $\lim_{i\to\infty} H_i$ has a diverging eigenvalue. Such a case arises, for instance, when we have a merge move in the point game. For concreteness, let x_{g_1}, x_{g_2} be the coordinates of two points that are going to be merged into a single point with coordinate $x_h = p_{g_1}x_{g_1} + p_{g_2}x_{g_2}$, and let p_{g_1}, p_{g_2} be their respective probability weights, with $p_{g_1} + p_{g_2} = 1$. Furthermore, let $t_i = [\![x_h + 1/i]\!] - p_{g_1}[\![x_{g_1}]\!] - p_{g_2}[\![x_{g_2}]\!]$. One can verify that for all finite values of i, t_i is EBM, but its limit $t = [\![x_h]\!] - p_{g_1}[\![x_{g_1}]\!] - p_{g_2}[\![x_{g_2}]\!]$ is not EBM (we omit the details for the sake of brevity), thus concluding that the set of EBM functions is open.

To show that the closure of this set is the same as the set of the TEF functions, we need to establish that the limit of any such sequence belongs to the set of TEF functions. This requires a combination of certain results from Section 5 of [4]. In particular, the relationship between the so-called *canonical orthogonal form* and the *canonical projective form* permits one to trade the divergence of such a matrix H for appropriate projectors. This is exactly the origin of the projectors E_h that appear in our analysis. The matrices $H \geq G$ and the vector $|\psi\rangle$ corresponding to an EBM transition, can be expressed in the canonical orthogonal form,[12] $X_h \geq OX_gO^T$. Essentially, the same orthogonal matrix O also satisfies the TEF inequality.[13] (Equation (2)) The TEF inequality may, in fact, be seen as the limit where H's eigenvalues diverge to infinity. Thus, the limit t of the sequence t_i indeed belongs to the set of TEF functions and this argument readily extends to all relevant sequences.

Finally, in Section 3 of [1] the authors prove that the set of valid functions is the same as the closure of the set of EBM functions. In particular, they start by observing that the set of EBM functions is a convex cone K, and its dual cone K^* is the set of operator monotone functions. The bi-dual K^{**} is the set of valid functions, and the fact that $K^{**} = \mathrm{cl}(K)$ completes the proof. Since we just showed that the closure of the set of EBM functions is the same as the set of TEF functions, we can also conclude that the set of valid functions is the same as the set of TEF functions.

□

B Useful lemmas

Lemma 15. *Consider a set of real coordinates* $0 \leq x_1 < x_2 \cdots < x_n$ *and let* $f(x) = (a_1 - x)(a_2 - x)\dots(a_k - x)$, *where* $k \leq n-2$ *and the roots* $\{a_i\}_{i=1}^k$ *of* f *are non-negative. Let* $t = \sum_{i=1}^n p_i [x_i]$ *be the corresponding* f*-assignment. Consider a set of real coordinates* $0 < x_1 + c < x_2 + c \cdots < x_n + c$, *where* $c > 0$ *and let* $f'(x) = (a_1 + c - x)(a_2 + c - x)\dots(a_k + c - x)$. *Let* $t' = \sum_{i=1}^n p'_i [x'_i]$ *be the corresponding* f*-assignment with* $x'_i := x_i + c$. *The solution to* t *and to* t' *are the same.*

Proof. Note that $p'_i = p_i$ as the c's cancel. We write $t = \sum_{i=1}^{n_h} p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n_g} p_{g_i} [\![x_{g_i}]\!]$ and 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 that $X_h + c\mathbb{I}_h \geq E_h O(X_g + c\mathbb{I}_g)O^T E_h$ where $\mathbb{I}_h := \sum_{i=1}^{n_h} |h_i\rangle\langle h_i|$ and $\mathbb{I}_g := \sum_{i=1}^{n_g} |g_i\rangle\langle g_i|$. Together with the observation that $p'_i = p_i$, this establishes that O also solves t'. Since c is an arbitrary real number, it follows that O solves t if and only if it solves t'.

[12] X_h and X_g are diagonal matrices containing the eigenvalues of H and G, respectively. We suppress further details.

[13] The TEF inequality is closely related to the canonical projective form.

We now establish $X_h \geq E_h O X_g O^T E_h \iff X_h + c\mathbb{I}_h \geq E_h O(X_g + c\mathbb{I}_g)O^T E_h$. Observe that

$$\begin{aligned}
& X_h \geq E_h O X_g O^T E_h \\
\iff & E_h(X_h - O X_g O^T)E_h \geq 0 && \because X_h = E_h X_h E_h \\
\iff & E_h(X_h + c\mathbb{I}_{hg} - O(X_g - c\mathbb{I}_{hg})O^T)E_h \geq 0 \\
\iff & X_h + c\mathbb{I}_h \geq E_h O(X_g + c\mathbb{I}_{hg})O^T E_h, && \text{where } \mathbb{I}_{hg} := \mathbb{I}.
\end{aligned}$$

Further,

$$\begin{aligned}
& X_g + c\mathbb{I}_{hg} \geq X_g + c\mathbb{I}_g \\
\iff & E_h O(X_g + c\mathbb{I}_{hg})O^T E_h \geq E_h O(X_g + c\mathbb{I}_g)O^T E_h
\end{aligned}$$

which together yield

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

□

Lemma 16. *Consider an n-dimensional vector space. Given a diagonal matrix $X = diag(x_1, x_2 \dots x_n)$ and a vector $|c\rangle = (c_1, c_2 \dots, c_n)$ where all the x_is are distinct and all the c_i are non-zero, the vectors $|c\rangle, X|c\rangle, \dots X^{n-1}|c\rangle$ 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.

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

is non-zero. To see this, we note 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, this concludes the proof. □

Lemma 17. *Let $t = \sum_{i=1}^n p_i [x_i]$ be the zeroth assignment for a set of real numbers $0 \leq x_1 < x_2 \dots < x_n$. Then for $0 \leq k \leq n-2$,*

$$\left\langle x^k \right\rangle = 0 \quad \textit{and} \quad \left\langle x^{n-1} \right\rangle > 0,$$

where $\left\langle x^k \right\rangle = \sum_{i=1}^n p_i (x_i)^k$.

Proof. For the proof, see Section 4 and Appendix B of [4]. Most of the work had already been done by Mochon [17]. □

C Proofs and examples for balanced monomial assignments

Proof of Proposition 9

Proof. The orthonormal basis (over $\text{span}\{|h_1\rangle, |h_2\rangle \dots |h_n\rangle\}$) of interest here is

$$\left|w'_i\right\rangle := \frac{\Pi^{\perp}_{h_i}(X_h)^i \left|w'\right\rangle}{\sqrt{c_{h_i}}} \tag{8}$$

which entails

$$\Pi^{\perp}_{h_i} = \begin{cases} \mathbb{I}_h & i = 0 \\ \mathbb{I}_h - \sum_{j=i+1}^{0} \left|w'_j\right\rangle \left\langle w'_j\right| & i < 0 \\ \mathbb{I}_h - \sum_{j=-b}^{i-1} \left|w'_j\right\rangle \left\langle w'_j\right| & i > 0 \end{cases} \tag{9}$$

where $\mathbb{I}_h := E_h$. We define $\left|v'_i\right\rangle$ and $\Pi^{\perp}_{g_i}$ analogously. Our strategy would be to keep track of both the highest and lowest power l, in $\langle w'| X^l_h |w'\rangle$ and $\langle v'| X^l_g |v'\rangle$, which appear in the matrix elements $\left\langle w'_i\right| D \left|w'_j\right\rangle$. We use $\left\langle x^l_h\right\rangle' := \langle w'| X^l_h |w'\rangle = \langle w| X^{l+2b}_h |w\rangle$ and similarly $\left\langle x^l_g\right\rangle' := \langle v'| X^l_g |v'\rangle = \langle w| X^{l+2b}_g |w\rangle$. To this end, we denote the minimum and maximum powers l, by

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

We define $D := X_h - E_h O X_g O^T E_h \doteq \left\langle w'_i\right| (X_h - E_h O X_g O^T E_h) \left|w'_j\right\rangle$. It suffices to restrict to the span of $\{\left|w'_i\right\rangle\}$ basis, because $X_h \left|v'_i\right\rangle = 0$ and $E_h \left|v'_i\right\rangle = 0$. The lowest power l, appearing in D is for $i = j = -b$ (as $-b \le i, j \le n - b - 1$). This can be evaluated to be $-2b$ by observing that

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

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

$$\mathcal{M}(\langle w'_i|) X_h \mathcal{M}(|w'_j\rangle) = \left(\left\langle x^{-2b}_h\right\rangle' \left\langle x^{-2b}_h\right\rangle' \left\langle x^{-2b+1}_h\right\rangle', \left\langle x^{2i}_h\right\rangle' \left\langle x^{2j}_h\right\rangle' \left\langle x^{i+j+1}_h\right\rangle'\right),$$

therefore $l = \max\{2i, 2j, i + j + 1\}$. As argued for the zeroth assignment $l = 2n - 2b - 1$ for $i = j = n - b - 1$ or otherwise strictly less than $2n - 2b - 1$. Thus, only the $D_{n-b-1,n-b-1}$ term in D depends on $\left\langle x^{2n-2b-1}_h\right\rangle'$. Except for this term, all other terms depend, at most, on $\left\langle x^{-2b}_h\right\rangle', \left\langle x^{-2b+1}_h\right\rangle', \dots \left\langle x^{2n-2b-2}_h\right\rangle'$, i.e. $\left\langle x^0_h\right\rangle, \left\langle x^1_h\right\rangle, \dots \left\langle x^{2n-2}_h\right\rangle$. The analogous argument for $\left\langle v'_i\right| X_g \left|v'_j\right\rangle$, the observation that $\left\langle w'_i\right| D \left|w'_j\right\rangle = \left\langle w'_i\right| X_h \left|w'_j\right\rangle - \left\langle v'_i\right| X_g \left|v'_j\right\rangle$, and the fact that $\left\langle x^0\right\rangle = \left\langle x^1\right\rangle = \dots = \left\langle x^{2n-2}\right\rangle = 0$ entail that these terms vanish. It remains to establish that $D_{n-b-1,n-b-1} \ge 0$. This is easily seen by noting that in $\left\langle w'_{n-b-1}\right| D \left|w'_{n-b-1}\right\rangle$, the only term which would not get cancelled due to the aforesaid reasoning, must come from the part of $\left|w'_{n-b-1}\right\rangle$ containing $X^{n-b-1}_h |w'\rangle$. It suffices to show that the coefficient of this term is positive, as we know that $\left\langle x^{2n-2b-1}\right\rangle' = \left\langle x^{2n-1}\right\rangle > 0$. Further, from Equation (9) and Equation (8), we know that the coefficient is $1/c_{h_{n-b-1}}$. This establishes $D \ge 0$. □

Example of balanced aligned and misaligned monomial assignments

Let us consider a concrete example of a balanced aligned monomial assignment with $2n = 8$ and $m = 2b = 2$ (see Figure 1a). 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

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

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

and

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

respectively. Note that the highest power l of $\langle x_h^l \rangle$ that appears in $\langle w_i' | X_h | w_j' \rangle$ is $l = 7$ 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 is positive, as $\langle x^7 \rangle > 0$.

We now explain why a direct extension of the analysis to the balanced misaligned monomial assignment fails and subsequently see how to remedy the situation. Consider the case with $2n = 8$ and $m = 2b - 1 = 3$ (see Figure 1b). 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 continue by multiplying $|w_0'\rangle$ with X_h^{-1} (and $|v_0'\rangle$ with X_g^{-1}, respectively) and projecting out the components along the previous vectors. We represent these by $|w_{-1}'\rangle$ and $|v_{-1}'\rangle$ and in the figure, 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 continue further, because in this case a dependence on $\langle x^{-1} \rangle$ arises and persists for subsequent vectors. In general, we stop after taking b (which equals 1 here) steps downwards. We can move upwards 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, 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 $|v_{-2}'\rangle$ respectively but they are the same as $|w_2'\rangle$ and $|v_2'\rangle$. If we were to use $O = \sum_{i=-1}^{2} (|w_i'\rangle \langle v_i'| + \text{h.c.})$, we would have obtained dependence on $\langle x^7 \rangle$ in the last row (corresponding to $|w_2'\rangle$) and a dependence on $\langle x^8 \rangle$ for the last term (i.e. $\langle w_2' | D | w_2' \rangle$). This already hints that the matrix is negative because it has the form $\begin{bmatrix} 0 & b \\ b & c \end{bmatrix}$ with $b \neq 0$, which means that the determinant is $-b^2$, entailing there's a negative eigenvalue; thus this choice can not work. We therefore define $O := (\sum_{i=-1}^{1} |w_i'\rangle \langle v_i'| + \text{h.c.}) + |w_2'\rangle \langle w_2'| + |v_2'\rangle \langle v_2'|$. Furthermore, instead of using

$$X_h \geq E_h O X_g O^T E_h \tag{10}$$

for establishing positivity, we equivalently use

$$E_h \geq (X_h^{\dashv})^{1/2} O X_g O^T (X_h^{\dashv})^{1/2}. \tag{11}$$

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 (10) would not contribute, the LHS would get non-trivial contributions along the rows (as was the case earlier). Using the form with the inverses lets us 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, $\text{span}\{X_h^{1/2}\left|w_i'\right\rangle\}_{i=-1}^{2}$ also equals the h-space (but the vectors are not, in general, orthonormal any more). Finally, observe that $X_h^{1/2}\left|w_2'\right\rangle$ is a null vector of the RHS of Equation (11). Therefore, to prove the positivity, it suffices to restrict to $\text{span}\{X_h^{1/2}\left|w_i'\right\rangle\}_{i=-1}^{1}$. An arbitrary normalised vector in this space can be written as

$$\begin{aligned}
|\psi\rangle &= \frac{\sum_{i=-1}^{1}\alpha_i X_h^{1/2}\left|w_i'\right\rangle}{\sqrt{\sum_{i,j=-1}^{1}\alpha_i\alpha_j\left\langle w_i'\right|X_h\left|w_j'\right\rangle}} \\
\implies X_g^{1/2}O^T(X_h^{\dashv})^{1/2}|\psi\rangle &= \frac{\sum_{i=-1}^{1}\alpha_i X_g^{1/2}\left|v_i'\right\rangle}{\sqrt{\sum_{i,j=-1}^{1}\alpha_i\alpha_j\left\langle w_i'\right|X_h\left|w_j'\right\rangle}} \\
\implies \langle\psi|(X_h^{\dashv})^{1/2}OX_gO^T(X_h^{\dashv})^{1/2}|\psi\rangle &= \frac{\sum_{i,j=-1}^{1}\alpha_i\alpha_j\left\langle v_i'\right|X_g\left|v_j'\right\rangle}{\sum_{i,j=-1}^{1}\alpha_i\alpha_j\left\langle w_i'\right|X_h\left|w_j'\right\rangle} = 1,
\end{aligned}$$

where we got the equality by noting that $\left\langle v_i'\right|X_g\left|v_j'\right\rangle$s depend on (at most) $\left\{\left\langle x_g\right\rangle,\left\langle x_g^2\right\rangle\ldots\left\langle x_g^6\right\rangle\right\}$ and analogously $\left\langle w_i'\right|X_h\left|w_j'\right\rangle$ depend on (at most) $\{\langle x_h\rangle,\langle x_h^2\rangle\ldots\langle x_h^6\rangle\}$, concluding that they are the same as $\left\langle x^i\right\rangle = 0$ for $i\in\{0,1,\ldots 6\}$. Since we proved that the RHS of Equation (11) is one for all normalised $|\psi\rangle$s, we infer that we have the correct orthogonal matrix.

Proof of Proposition 10

Proof. The proof is very similar to that of Proposition 9. The orthonormal basis (over $\{|h_1\rangle,|h_2\rangle\ldots|h_n\rangle\}$) of interest here is

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

which entails

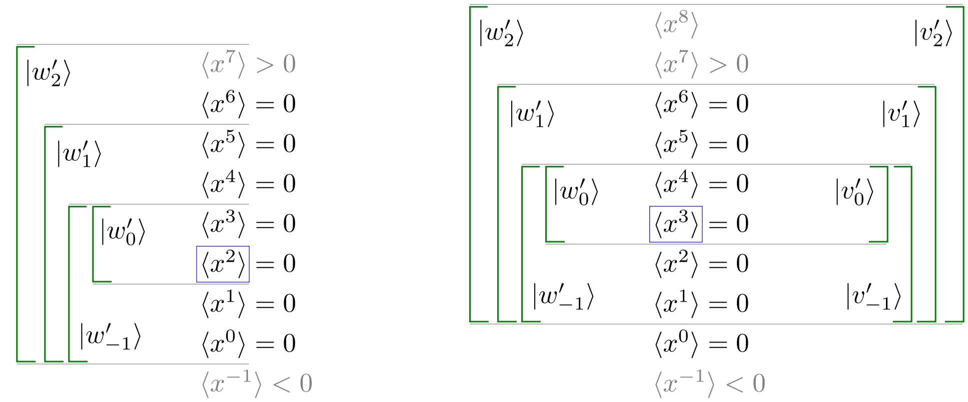
$$\Pi_{h_i}^{\perp} = \begin{cases}\mathbb{I}_h & i=0\\ \mathbb{I}_h - \sum_{j=i-1}^{0}\left|w_j'\right\rangle\left\langle w_j'\right| & i<0\\ \mathbb{I}_h - \sum_{j=-b+1}^{i}\left|w_j'\right\rangle\left\langle w_j'\right| & i>0\end{cases},$$

where $\mathbb{I}_h := E_h$. We define $\left|v_i'\right\rangle$ 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 $\left\langle w_i'\right|X_h\left|w_j'\right\rangle$ and $\left\langle v_i'\right|X_g\left|v_j'\right\rangle$. For brevity, as before, we use $\left\langle x_h^l\right\rangle' := \langle w'|X_h^l|w'\rangle$ and similarly $\left\langle x_g^l\right\rangle' := \langle v'|X_g^l|v'\rangle$. To this end, we denote the minimum and maximum powers l, by

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

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

$$E_h \geq X_h^{-1/2}OX_gO^TX_h^{-1/2}. \tag{12}$$



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

(b) $2n = 8$, $m = 2b - 1 = 3$; Balanced (aligned) monomial assignment.

Figure 1: Depicting balanced monomial assignments with simple examples.

It is easy to see that $X_h^{1/2}\left|w'_{n-b}\right\rangle$ is a null vector (vector with zero eigenvalue) for the RHS as $X_g O^T\left|w'_{n-b}\right\rangle = 0$. Any vector $|\psi\rangle$ in span$\{|g_1\rangle, |g_2\rangle \dots |g_n\rangle\}$ is a null vector for both the LHS and the RHS. Thus, we can restrict to span$\{|h_1\rangle, |h_2\rangle, \dots |h_n\rangle\}\backslash$span$\{X_h^{1/2}\left|w'_{n-b}\right\rangle\}$, i.e. to vectors in the h-space orthogonal to $X_h^{1/2}\left|w'_{n-b}\right\rangle$, in order to establish positivity. It turns out to be easier to test for positivity on a possibly larger space. It is clear that span$\left\{X_h^{1/2}\left|w'_i\right\rangle\right\}_{i=-b+1}^{n-b}$ = span$\{|h_1\rangle, |h_2\rangle \dots |h_n\rangle\}$ (because it also equals span$\{|w'\rangle_i\}_{i=-b+1}^{n-b}$, due to Lemma 16). As neglecting vectors with components along $X_h^{1/2}\left|w'_{n-b}\right\rangle$ suffices for establishing positivity of Equation (12), we can restrict to span$\{X_h^{1/2}\left|w'_i\right\rangle\}_{i=-b+1}^{n-b-1}$, which might still contain vectors with components along $X_h^{1/2}\left|w'_{n-b}\right\rangle$, as the basis vectors are not orthogonal. Let $|\psi\rangle = \left(\sum_{i=-b+1}^{n-b-1}\alpha_i X_h^{1/2}\left|w'_i\right\rangle\right)/c$ where $c = \sqrt{\langle\psi|\psi\rangle}$. To establish Equation (12), it is enough to show that for all choices of α_is,

$$
\begin{aligned}
1 &\geq \langle\psi| X_h^{-1/2} O X_g O^T X_h^{-1/2} |\psi\rangle \\
&= \frac{\sum_{i,j=-b+1}^{n-b-1}\alpha_i\alpha_j\left\langle v'_i\right| X_g \left|v'_j\right\rangle}{\sum_{i,j=-b+1}^{n-b-1}\alpha_i\alpha_j\left\langle w'_i\right| X_h \left|w'_j\right\rangle} \\
&= 1,
\end{aligned}
\tag{13}
$$

where the second step follows from the fact that $X_g^{1/2}O^T X_h^{-1/2}|\psi\rangle = \sum_{i=-b+1}^{n-b-1}\alpha_i X_g^{1/2}\left|v'_i\right\rangle$, and the last step follows from a counting argument which we give below.

Note that

$$\left\langle x_h^i\right\rangle' = \left\langle x_h^{i+2b-1}\right\rangle$$

and

$$\left\langle x^0\right\rangle = \langle x\rangle = \dots = \left\langle x^{2n-2}\right\rangle = 0. \tag{14}$$

To determine the highest power l in $\langle w'| X_h^l |w'\rangle$ which appears in the matrix elements $\left\langle w'_i\right| X_h \left|w'_j\right\rangle$ (for

$-b+1 \le i, j \le n-b-1$) it suffices to consider $\left\langle w'_{n-b-1} \right| X_h \left| w'_{n-b-1} \right\rangle$. To this end, we evaluate

$$\begin{aligned}
&\mathcal{M}(\left\langle w'_{n-b-1} \right|) X_h \mathcal{M}(\left| w'_{n-b-1} \right\rangle) \\
&= \left(\left\langle x_h^{-2(b-1)} \right\rangle' \left\langle x_h^{-2(b-1)} \right\rangle' \left\langle x_h^{-2(b-1)+1} \right\rangle', \left\langle x_h^{2(n-b-1)} \right\rangle' \left\langle x_h^{2(n-b-1)} \right\rangle' \left\langle x_h^{2(n-b-1)+1} \right\rangle' \right) \\
&= \left(\langle x_h \rangle \langle x_h \rangle \left\langle x_h^2 \right\rangle, \left\langle x_h^{2n-3} \right\rangle \left\langle x_h^{2n-3} \right\rangle \left\langle x_h^{2n-2} \right\rangle \right).
\end{aligned}$$

The highest power is $l = 2n-2$. To find the lowest power of l in $\langle w' | X_h^l | w' \rangle$ which appears in the matrix elements $\left\langle w'_i \right| X_h \left| w'_j \right\rangle$ (for $-b+1 \le i, j \le n-b-1$) it suffices to consider $\left\langle w'_{-b+1} \right| X_h \left| w'_{-b+1} \right\rangle$. To this end, we evaluate

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

The lowest power is $l = 1$. We thus conclude that the numerator in Equation (13) is a function of $\langle x_h \rangle, \left\langle x_h^2 \right\rangle, \ldots \left\langle x_h^{2n-2} \right\rangle$, and analogously the denominator is a function of $\langle x_g \rangle, \left\langle x_g^2 \right\rangle, \ldots \left\langle x_g^{2n-2} \right\rangle$ with the same form. Using Equation (14), we obtain that the numerator and the denominator are the same. □

D Proofs and examples for unbalanced monomial assignments

Proof of Proposition 11

Proof. Many observations from the proof of Proposition 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 $\left\langle x_h^l \right\rangle'$ with l smaller than $-2b$ (which corresponds to $\langle x_h \rangle$), and that $\mathcal{M}(\langle w'_{n-b-2}|) X_h \mathcal{M}(|w'_{n-b-2}\rangle)$ has no dependence on $\left\langle x_h^l \right\rangle'$ with l greater than $2n-2b-4+1 = 2n-3-2b$. We can restrict to $\mathrm{span}\{|w'_{-b}\rangle, |w'_{-b+1}\rangle \ldots |w'_{n-b-2}\rangle\}$ 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 $\left\langle x^l \right\rangle' = \left\langle x^{l+2b} \right\rangle$ and $\left\langle x^0 \right\rangle = \left\langle x^1 \right\rangle = \cdots = \left\langle x^{2n-3} \right\rangle = 0$, it follows that D is zero. □

Proof of Proposition 12

Proof. For this proof, we can use the definitions and observations from the proof of Proposition 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 $\left\langle x_h^l \right\rangle'$ with l smaller than $-2b+2$ (which corresponds to $\langle x_h \rangle$), and

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

has no dependence on $\left\langle x^l \right\rangle$ with l greater than $2n-2b-1$ (which corresponds to $\left\langle x_h^{2n-2} \right\rangle$, as $2n-2b-1+(2b-1) = 2n-2$). From the previous proof, we also have that establishing $X_h \ge E_h O X_g O^T E_h$ is equivalent to establishing that

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

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 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 9, dependence on $\langle x_h^{2n-2} \rangle$ in the denominator only appears in the $\langle w'_{n-b-1} | X_h | w'_{n-b-1} \rangle$ term 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. □

Examples of unbalanced aligned and misaligned monomial assignments

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 2a). We use the same diagrammatic representation as before. In this case, we have 4 initial and 3 final points and the basis is $\{|g_1\rangle, |g_2\rangle, \ldots |g_4\rangle, |h_1\rangle, |h_2\rangle, |h_3\rangle\}$. We construct the basis of interest by starting at $|w'\rangle$ and using X_h^{-1} first until we reach $\langle x^0 \rangle$, followed by using X_h until the space is spanned (analogously for $|v'\rangle$). We get $\{|v'_{-1}\rangle, |v'_0\rangle, |v'_1\rangle, |v'_2\rangle\}$ and $\{|w'_{-1}\rangle, |w'_0\rangle, |w'_1\rangle\}$. In the same vein as the previous 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 $D = X_h - E_h O X_g O^T E_h$ is zero.

We now move on to unbalanced misaligned monomial assignment. Consider $2n-1 = 7$ points and $m = 2b-1 = 1$. In this case, we have 3 initial and 4 final points and the 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 $|v'\rangle$). That is, we first go downwards for $b - 2$ steps (which is zero in this case), until $\langle x \rangle$ is reached in the diagram. The basis is $\{|v'_0\rangle, |v'_1\rangle, |v'_2\rangle\}$ 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

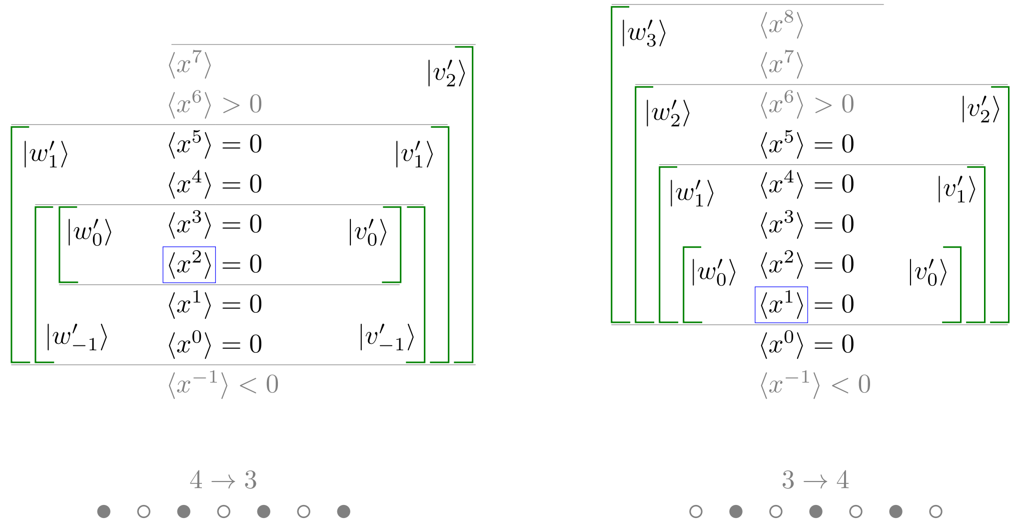
$$1 \geq \frac{\sum_{i,j=0}^{2} \alpha_i \alpha_j \langle v'_i | X_g | v'_j \rangle}{\sum_{i,j=0}^{2} \alpha_i \alpha_j \langle w'_i | X_h | w'_j \rangle},$$

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 $\langle x_g^6 \rangle$ 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. Furthermore, 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.

E Constructing a WCF protocol approaching bias 1/14

In this last part of the appendix we show how one can construct an explicit WCF protocol, in particular a protocol approaching bias $\epsilon = \frac{1}{14}$, corresponding to the point game with the same bias, that is for $k = 3$ in $\epsilon(k) = \frac{1}{4k+2}$, we obtain $\epsilon(3) = \frac{1}{14}$. Several results and techniques presented in previous works, such as [16, 17, 1, 5], are required for this construction. We will only refer to them when they are needed.

The TDPG with bias $\frac{1}{14}$ includes the basic moves we mentioned in Section 2, namely the split, merge and raise moves, as well as the main moves which are needed for the so-called *ladder*, as illustrated in Figure 3. We only need to determine the orthogonal matrix O for these main moves, as the matrices corresponding



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

(b) $2n - 1 = 7$; $m = 2b - 1 = 1$. Odd unbalanced monomial assignment.

Figure 2: Depicting unbalanced monomial assignment with simple examples.

to the split and the merge moves are given by the so-called *blinkered unitary*, as presented in Equation 3 of [5], and the raise move is trivial, as it just increases the coordinate. The weights on the points constituting the ladder are given by the f-assignment. For our example (the bias $\frac{1}{14}$ case), the f-assignment is on a set of points seven points $\{x_0', x_1' \dots x_6'\}$, and the corresponding polynomial has degree five which we write as $f'(x) = (r_1' - x)(r_2' - x)(r_3' - x)(r_4' - x)(r_5' - x)$. More explicitly, the f-assignment is given by

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

The placement of the roots of the polynomial with respect to the points is the following (see also Figure 3):

$$x_0' = 0 < r_1' < r_2' < x_1' < x_2' < x_3' < x_4' < x_5' < x_6' < r_3' < r_4' < r_5'.$$

The assignment t' includes a point with zero coordinate, while the orthogonal matrices O (in Proposition 9, Proposition 10, Proposition 11, and Proposition 12) solve (monomial) assignments whose points have strictly positive coordinates. As already mentioned in Section 3, this is not really a restriction, as Lemma 15 permits us to alternatively consider an f-assignment on the points $\{x_0, x_1 \dots x_6\}$ where $x_i = x_i' + c$ and $f(x) = (r_1 - x)(r_2 - x) \dots (r_5 - x)$ where $r_i = r_i' + c$, for a positive number c. The resulting assignment

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

has the same solution as that of t'. We decompose t into a sum of monomial assignments as

$$
\begin{aligned}
t =& \underbrace{\sum_{i=0}^{6} \frac{-r_1 r_2 r_3 r_4 r_5}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!]}_{\mathrm{I}} + \underbrace{\sum_{i=0}^{6} \frac{-\overbrace{(r_2r_3r_4r_5 + r_1r_3r_4r_5 + r_1r_2r_3r_5 + r_1r_2r_3r_4)}^{:=\alpha_1}(-x_i)}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!]}_{\mathrm{II}} \\
&+ \underbrace{\sum_{i=0}^{6} \frac{-\alpha_2(-x_i)^2}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!]}_{\mathrm{III}} + \underbrace{\sum_{i=0}^{6} \frac{-\alpha_3(-x_i)^3}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!]}_{\mathrm{IV}} \\
&+ \underbrace{\sum_{i=0}^{6} \frac{-\alpha_4(-x_i)^4}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!]}_{\mathrm{V}} + \underbrace{\sum_{i=0}^{6} \frac{-\alpha_5(-x_i)^5}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!]}_{\mathrm{VI}},
\end{aligned}
$$

where α_l is the coefficient of $(-x)^l$ in $f(x)$. Since the total number of points in each term is 7, the monomial assignments are unbalanced. Terms I, III and V each have an even powered monomial, therefore they correspond to the aligned case. Their solutions, thus, are readily obtained from Proposition 11. Analogously, the remaining terms II, IV and VI have an odd powered monomial, therefore they correspond to the misaligned case. Their solutions, thus, are readily obtained from Proposition 12.

We have already done the hard work, which is to find the matrices which (effectively) solve the $f-$assignments for each move of the point game, and we can now describe how the pieces fit together to give the WCF protocol. We outline the steps of the associated TDPG, since, using the TEF, they can be seen as a short-hand to denote an exchange and manipulation of quantum systems (e.g. qubits) by the two parties executing the WCF protocol, granted that the associated unitaries are known (for details, see the description of the TEF in [5]). Then, the WCF protocol consists of the same steps implemented in the reverse order. Here, we should clarify that, in fact, we convert a TIPG approaching bias $\frac{1}{14}$, into a TDPG following the technique presented, for instance, in the proof of Theorem 5 in [1] with the minor modifications we outlined in Appendix A. Being familiar with the relationship between TIPGs and TDPGs and the related techniques facilitates the understanding of the construction that follows.

Steps of the point game

1. The initial frame corresponds to the function $\frac{1}{2}\left([\![0,1]\!] + [\![1,0]\!]\right)$.

2. The split move: the point $[\![0,1]\!]$ is split into a set of points along the $y-$axis and analogously, the point $[\![1,0]\!]$ is split into a set of points along the $x-$axis. The number of points resulting from the splits and their respective weights match the distribution of points along the axis as specified by the TIPG we started with.

3. The catalyst state [17, 1, 5]: Deposit a small amount of weight, δ_{catalyst}, at all the points that appear in the TIPG. This can be done, for instance, by raising (the $x-$coordinates) of the points which are along the $y-$axis, i.e. if the points along the axes are denoted as $\sum_i p_{\text{split},i} [\![0, y_i]\!]$ then raise them to obtain $\sum_i (p_{\text{split},i} - \delta_{\text{split},i}) [\![0, y_i]\!] + \sum_{i,j} \delta_{\text{catalyst}} [\![x_i, y_j]\!]$ where $\delta_{\text{catalyst}} > 0$ can be chosen to be arbitrarily small and the second sum is over the points (x_i, y_j) which appear in the TIPG (excluding the points on the axes[14]).

[14] One needs to use the analogues procedure, i.e. use $\sum_i p_{\text{split},i} [\![x_i, 0]\!]$ as well for the one point of the TIPG which has a $y-$coordinate smaller than that of the points along the $y-$axis.

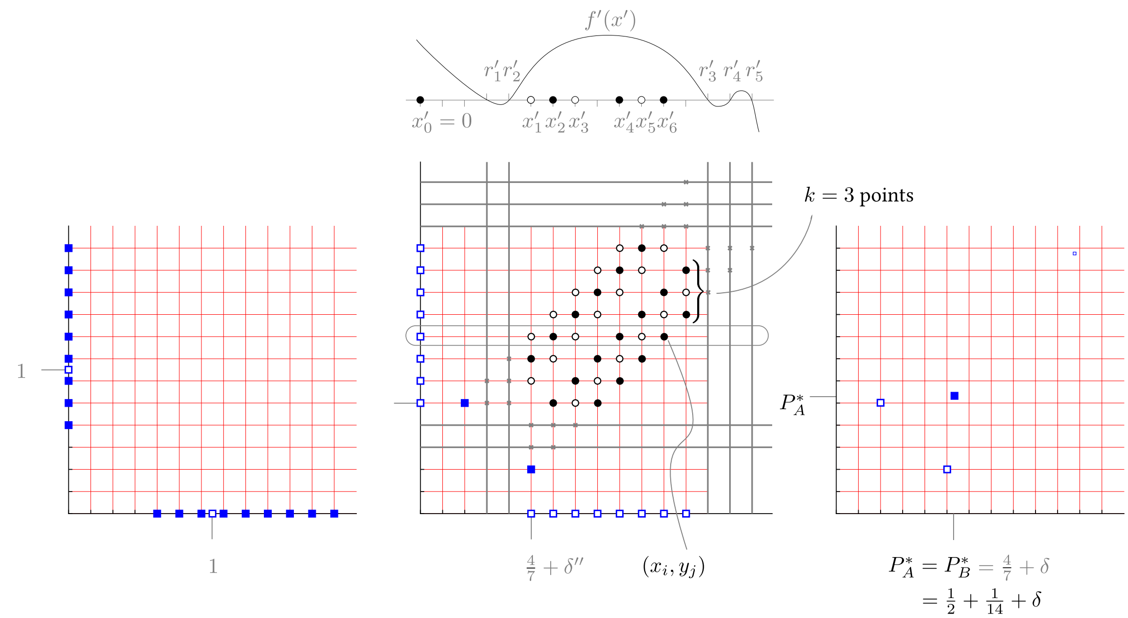


Figure 3: The TDPG (or equivalently, the reversed protocol) approaching bias $\epsilon(k = 3) = \frac{1}{14}$ may be seen as proceeding in three stages, as illustrated by the three images (left to right). *First*, the initial points (indicated by unfilled squares) are split along the axes (indicated by the filled squares). *Second*, the points on the axes (unfilled squares) are transferred, via the ladder (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 Mochon's TIPG (or more precisely, the ladder) approaching bias 1/14. Its typical move is highlighted. The weight of these points is given (up to a multiplicative 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.

4. The ladder:

   (a) The *constituent functions*, i.e., the valid functions resulting from the decomposition of the valid function of the TIPG, are globally scaled such that no negative weight appears when they are applied.

   (b) All the scaled down constituent horizontal functions are applied.

   (c) All the scaled down constituent vertical functions are applied.

   (d) The above two steps are repeated until all the weight has been transferred from the axes points to the two final points of the ladder.[15]

5. The raise and merge moves: the last two points are raised and merged into the point $(1-\delta') \left[\!\left[\frac{4}{7} + \delta'', \frac{4}{7} + \delta'' \right]\!\right]$, where δ' is the weight introduced by the catalyst state, and δ'' comes from the truncation of the ladder. The catalyst state can then be absorbed (see, e.g. the proof of Theorem 5 in [1]) to obtain a single point $\left[\!\left[\frac{4}{7} + \delta, \frac{4}{7} + \delta \right]\!\right]$, where δ can be made arbitrarily small.

This final point, $\left[\!\left[\frac{4}{7} + \delta, \frac{4}{7} + \delta \right]\!\right]$ with a vanishing $\delta > 0$, of the point game is, in fact, the starting point of the WCF protocol. It corresponds to the initial uncorrelated state of the two parties, A and B, and the

[15] Once the weight on the axes points diminishes sufficiently, it becomes impossible to apply the moves again.

coordinates represent the cheating probabilities of each party, $P^*_{A/B} = \frac{4}{7} + \delta = \frac{1}{2} + \frac{1}{14} + \delta$. The steps of the point game are followed in the reverse order, and the WCF protocol ends with two points of equal weights along the axis (these are exactly the points in the initial frame of the point game) corresponding to a correlated state between A and B, $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

References

[1] Nati Aharon et al. "Weak Coin Flipping in a Device-Independent Setting." In: *Revised Selected Papers of the 6th Conference on Theory of Quantum Computation, Communication, and Cryptography - Volume 6745*. TQC 2011. Madrid, Spain: Springer-Verlag New York, Inc., 2014, pp. 1–12. ISBN: 978-3-642-54428-6. DOI: 10.1007/978-3-642-54429-3_1. URL: http://dx.doi.org/10.1007/978-3-642-54429-3_1.

[2] Dorit Aharonov et al. "A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias." In: *SIAM Journal on Computing* 45.3 (Jan. 2014), pp. 633–679. DOI: 10.1137/14096387x. arXiv: 1402.7166.

[3] Andris Ambainis. "A new protocol and lower bounds for quantum coin flipping." In: *Journal of Computer and System Sciences* 68.2 (2004), pp. 398–416. DOI: 10.1016/j.jcss.2003.07.010. arXiv: 0204022 [quant-ph].

[4] Atul Singh Arora, Jérémie Roland, and Stephan Weis. "Quantum Weak Coin Flipping." In: (Nov. 6, 2018). arXiv: http://arxiv.org/abs/1811.02984v1 [quant-ph].

[5] Atul Singh Arora, Jérémie Roland, and Stephan Weis. "Quantum weak coin flipping." In: *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing - STOC 2019*. ACM Press, 2019. DOI: 10.1145/3313276.3316306.

[6] Manuel Blum. "Coin Flipping by Telephone a Protocol for Solving Impossible Problems." In: *SIGACT News* 15.1 (Jan. 1983), pp. 23–27. ISSN: 0163-5700. DOI: 10.1145/1008908.1008911. URL: http://doi.acm.org/10.1145/1008908.1008911.

[7] AndrÃ© Chailloux, Gus Gutoski, and Jamie Sikora. "Optimal bounds for semi-honest quantum oblivious transfer." In: *Chicago Journal of Theoretical Computer Science, 2016* (Oct. 11, 2013). arXiv: http://arxiv.org/abs/1310.3262v2 [quant-ph].

[8] Andre Chailloux and Iordanis Kerenidis. "Optimal Bounds for Quantum Bit Commitment." In: *52nd FOCS*. 2011, pp. 354–362. DOI: 10.1109/FOCS.2011.42. arXiv: 1102.1678.

[9] André Chailloux and Iordanis Kerenidis. "Optimal Quantum Strong Coin Flipping." In: *50th FOCS*. 2009, pp. 527–533. DOI: 10.1109/FOCS.2009.71. arXiv: 0904.1511.

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

[11] Peter Høyer and Edouard Pelchat. "Point Games in Quantum Weak Coin Flipping Protocols." MA thesis. University of Calgary, 2013. URL: http://hdl.handle.net/11023/873.

[12] I. Kerenidis and A. Nayak. "Weak coin flipping with small bias." In: *Information Processing Letters* 89.3 (Feb. 2004), pp. 131–135. DOI: 10.1016/j.ipl.2003.07.007.

[13] A. Kitaev. "Quantum coin flipping." Talk at the 6th workshop on Quantum Information Processing. 2003.

[14] Hoi-Kwong Lo and H.F. Chau. “Why quantum bit commitment and ideal quantum coin tossing are impossible.” In: *Physica D: Nonlinear Phenomena* 120.1 (1998). Proceedings of the Fourth Workshop on Physics and Consumption, pp. 177–187. ISSN: 0167-2789. DOI: https://doi.org/10.1016/S0167-2789(98)00053-0. URL: http://www.sciencedirect.com/science/article/pii/S0167278998000530.

[15] Carl A. Miller. “The Impossibility of Efficient Quantum Weak Coin-Flipping.” In: (Sept. 22, 2019). arXiv: http://arxiv.org/abs/1909.10103v1 [quant-ph].

[16] Carlos Mochon. “Large family of quantum weak coin-flipping protocols.” In: *Phys. Rev. A* 72 (2005), p. 022341. DOI: 10.1103/PhysRevA.72.022341. arXiv: 0502068 [quant-ph].

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

[18] Ashwin Nayak and Peter Shor. “Bit-commitment-based quantum coin flipping.” In: *Phys. Rev. A* 67 (1 Jan. 2003), p. 012304. DOI: 10.1103/PhysRevA.67.012304. URL: https://link.aps.org/doi/10.1103/PhysRevA.67.012304.

[19] R. W. Spekkens and Terry Rudolph. “Quantum Protocol for Cheat-Sensitive Weak Coin Flipping.” In: *Physical Review Letters* 89.22 (Nov. 2002). DOI: 10.1103/physrevlett.89.227901.