Explicit quantum weak coin flipping protocols with arbitrarily small bias

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

November 5, 2019

Abstract

We investigate weak coin flipping, a fundamental cryptographic primitive where two distrustful parties need to remotely establish a shared random bit. A cheating player can try to bias the output bit towards a preferred value. A weak coin-flipping protocol has a bias ϵ if neither player can force the outcome towards their preferred value with probability more than $1/2 + \epsilon$. While it is known that classically $\epsilon = 1/2$, Mochon showed in 2007 that quantumly weak coin flipping can be achieved with arbitrarily small bias, i.e. $\epsilon(k) = 1/(4k + 2)$ for arbitrarily large k, and he proposed an explicit protocol approaching bias $1/6$. So far, the best known explicit protocol is the one by Arora et al, with $\epsilon(2) = 1/10$ (corresponding to $k = 2$) . In the current work, we present the construction of protocols approaching arbitrarily close to zero bias, i.e. $\epsilon(k)$ for arbitrarily large k. We connect the algebraic properties of Mochon's assignments—at the heart of his proof of existence—with the geometric properties of the unitaries whose existence he proved. It is this connection that allows us to find these unitaries analytically. In particular, we find that the key unitary involved in the bias $1/10$ protocol can be seen as an elementary example of the general solution.[1]

Contents

1 Introduction 2

2 Preliminaries 2

3 Overview of the Main Result 4

4 Ellipsoid Picture 5

5 Weingarten Iteration | Isometric Iteration using the Weingarten Map 7

6 Mochon's Assignments 11

7 f_0 Unitary | Solution to Mochon's f_0 assignment 12

8 Equivalence to Monomial Assignments 14

9 m Solutions | Solution to Mochon's Monomial Assignments 18

10 Conclusion and Outlook 24

11 Acknowledgements 24

References 24

A Ellipsoids 25
A.1 Known Results . . . 25
A.2 Normals and Curvatures/Weingarten Map . . . 25

B Lemmas for the Contact and Component conditions 27

[1] I apologise for not following the formatting requirements; I forgot and it was too late to fix it. I suppose the 10 page limit would translate to around 7 pages of this document. See this URL for improved versions.—ASA

1 Introduction

Coin flipping, or coin flipping over the telephone as it was first introduced by Blum ([Blu83]) , is an important cryptographic primitive which permits two parties that do not trust each other to remotely generate an unbiased random bit in spite of the fact that one of them might be dishonest and tries to force a specific outcome. In the classical scenario, such a protocol is only computationally secure, which means that one of the parties can always cheat and force the honest party to accept a certain outcome if they do not employ computational hardness assumptions ([Cle86]). Moving to the quantum scenario, one can distinguish between strong and weak coin flipping (WCF). In a strong coin flipping protocol, 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. It has been shown that this it is impossible to achieve perfect security in this setting ([LC98]), and in particular, there is a lower bound on the bias [Kit03] of such a protocol. For a quantum WCF protocol though, where the preferred outcome of each party is known, the situation is different. In his seminal work, Mochon [Moc07] proved the existence of a WCF protocol achieving arbitrarily close to zero bias. Based on the framework introduced by Kitaev for the study of coin flipping, he showed the aforementioned existence, which was later simplified and verified by Aharonov, Chailloux, Ganz, Kerenidis and Magnin [Aha+14]. The proof, though, was not constructive and the proposal of an explicit protocol was left as an open problem. Eleven years after the proof of existence, Arora, Roland and Weis designed an algorithm that *numerically* constructs a WCF protocol with arbitrarily small bias [ARW19; ARW18] and in the present work we report an *analytical* solution to the WCF problem.

In the next section we briefly describe the reductions of the initial problem to the final one that we aimed to solve, but we refrain from details, as they have already been thoroughly investigated and presented in previous works (see for example [Moc07; Aha+14; ARW18; ARW19]).

2 Preliminaries

We start by noting that all coin flipping protocols can be described as follows: the two parties, say Alice and Bob, are located in different places and there is a message register that they can exchange. At each step of the protocol, the player that holds the message register can apply a local unitary to it and their personal memory space. After a number of exchanges of the message register (rounds of the protocol), the players perform a final measurement on their personal memory spaces, whose outcome determines the winner (see Figure 1 from ([ARW18])). We assume that 0 outcome means that Alice won and outcome 1 means that Bob is the winner. There are two different cases. One is when both players are honest, which means that they follow the protocol and have equal probabilities of winning $P_A = P_B = 1/2$. The other arises when one of the players is cheating, therefore not following the protocol honestly and tries to force the other player to output their desired outcome. In this case the cheating party has, in principle, a higher probability of winning and we denote this probability of the cheating party as P_A^* or P_B^*, respectively. In particular, $P_{A/B}^* = \frac{1}{2} + \epsilon$, where ϵ is the *bias* of the protocol. Note that we are not interested in the case where both Alice and Bob are dishonest, as then none of them is following the protocol. In order to calculate $P_{A/B}^*$ one can write a semi-definite program (SDP) that maximises the probability of the cheating party, given that the honest party is following the protocol. Using the SDP duality, this maximisation problem can be written as a minimisation problem over the respective dual variables, which we denote by $Z_{A/B}$. While SDPs are well-studied and, in general, easy to handle, our case is not straightforward to deal with, since one has to do a double optimisation simultaneously. Even more, our goal is to also *find* a good protocol *for which* we can optimise over the cheating strategies. Therefore, a new framework was needed which would permit us to find both the protocol and its respective bias.

A groundbreaking idea was provided by Kitaev (described in Mochon's work [Moc07]) and entailed the transformation of these optimisation problems into the so-called *time-dependent point games*. A point game consists of a sequence of frames that include points on the positive quadrant of the $x - y$ plane [see figure]. A probability weight is assigned to each point and certain different moves of the points are allowed in order to advance from one frame to another. The point games that we are considering in this paper, are determined by specific initial and final configurations and there are two rules according to which we can move from one frame to another. The initial frame consists of two points with coordinates $[0, 1]$ and $[1, 0]$ and probability weight $1/2$ for each, while in the final frame there is only one point with coordinates $[\alpha, \beta]$ and probability weight 1. Starting from the initial configuration we move the points on the plane in order to attain the final frame. Denoting by z the coordinates of the points (x or y) and by p_z the respective probability weights in a certain frame of the game, we can write the aforementioned rules for the intermediate transitions between subsequent frames as follows:

$$\begin{aligned} \sum_z p_z &= \sum_{z'} p_{z'} \text{ (probability conservation)}, \\ \sum_z \frac{\lambda z}{\lambda + z} p_z &= \sum_{z'} \frac{\lambda z'}{\lambda + z'} p_{z'}, \forall \lambda > 0. \end{aligned} \tag{1}$$

We should take them into account while we are redistributing the points and this leads us to form a set of allowed moves consisting of:

- *raise* of a point along a horizontal or vertical line (increasing the respective coordinate),
- *split* of a point into several others,
- *merge* of several points into a single point.

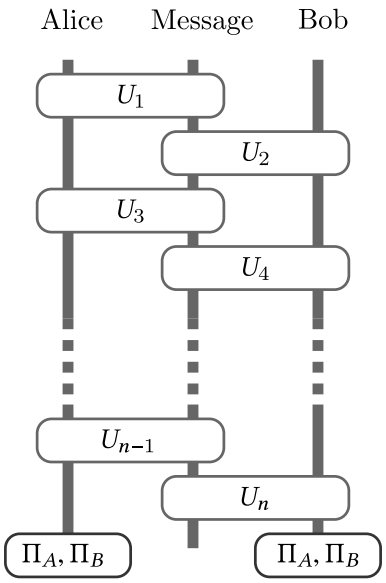

Figure 1: General description of a quantum weak coin flipping protocol

Notice that, when changing from a frame to another, the moves can either be along a vertical or a horizontal line. Moreover, the above three moves are not exhaustive; there exist more moves that satisfy the constraints.

It has been shown that for any such point game with the transitions between the frames respecting Equation (1), there exists a weak coin flipping protocol with cheating probabilities $P_A^* = \alpha + \delta$ and $P_B^* = \beta + \delta$ and vice versa. Given that δ can be made arbitrarily small, our initial task of defining a protocol and solving the associated SDPs that optimise $P_{A/B}^*$ has been reduced to the construction of a point game with the aforementioned initial and final configurations. Essentially, our goal is to find a game such that the point $[\alpha, \beta]$ of the final frame is as close to $[\frac{1}{2}, \frac{1}{2}]$ as possible, which is the zero-bias case. The constraints Equation (1) reflect, in the language of point games, the constraints on the dual variables $Z_{A/B}$ in the SDPs that we started with. To make this equivalence between the existence of point games and weak coin flipping protocols clearer we give some definitions that illustrate the relationship between the variables appearing in the dual SDP and the transitions between different frames in the point games.

Definition 1. Consider $Z \geq 0$ and let $\Pi^{[z]}$ be the projector on the eigenspace of the eigenvalue $z \in \text{spectrum}(Z)$. We have $Z = \sum_z z\Pi^{[z]}$. Let $|\psi\rangle$ be a vector (not necessarily normalised). We define the function with finite support $\text{Prob}[Z, |\psi\rangle] : [0, \infty) \to [0, \infty)$ as

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

For $Z = Z_A \otimes I_M \otimes Z_B$, (where Z_A and Z_B are the dual variables of the SDP) we can define the 2-variate function with finite support $Prob[Z_A, Z_B, |\psi\rangle] : [0, \infty) \times [0, \infty) \to [0, \infty)$ as

$$\text{Prob}[Z_A, Z_B, |\psi\rangle](z) = \begin{cases} \langle\psi|\Pi^{[z_A]} \otimes I_M \otimes \Pi^{[z_B]}|\psi\rangle & \text{if } (z_a, z_B) \in \text{span}(Z_A) \times \text{span}(Z_B) \\ 0 & \text{otherwise.} \end{cases}$$

Let $g, h : [0, \infty) \to [0, \infty)$ be two functions with finite supports. The line transition $g \to h$ is expressible by matrices (EBM) if there exist two matrices $0 \leq G \leq H$ and a vector $|\psi\rangle$ (not necessarily normalised) such that

$$g = \text{Prob}[G, |\psi\rangle] \text{ and } h = \text{Prob}[H, |\psi\rangle].$$

Definition 2. Let $p, q : [0, \infty) \times [0, \infty) \to [0, \infty)$ be two functions with finite supports.
The transition $p \to q$ is an

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

One can now accordingly define the point games that we need to consider in order to construct weak coin flipping protocols.

Definition 3. An EBM point game is a sequence of functions $\{p_0, p_1, \ldots, p_n\}$ with finite support such that

- $p_0 = \frac{1}{2}[0, 1] + \frac{1}{2}[1, 0]$,
- for all even i the transition $p_i \to p_{i+1}$ is an EBM vertical transition,

- for all odd i the transition $p_i \longrightarrow p_{i+1}$ is an EBM horizontal transition, and
- $p_n = 1[\beta, \alpha]$ for some $\alpha, \beta \in [0, 1]$.

Finding an EBM point game is still hard, however, especially because in order to verify if a transition is EBM one has to check conditions involving matrices. This is where another reduction of the original problem is needed. First, we can switch from EBM transitions to their corresponding EBM functions. If we have the EBM transition from p to q, then the corresponding EBM function is $p - q$, which is also a function with finite support. It has been shown that set of EBM functions is the same (up to the closures) with the set of the so-called *valid* functions. We will not present here neither the formal definition of a valid function, nor how the two sets can be proven to be the same, as this analysis has been presented in various previous works. What we want to highlight is that checking if a transition is EBM is equivalent to verifying the validity of a suitably constructed function. In general, for the validity of a function $h(x)$ one has to check that the following two conditions hold,

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

Thus, the difficulty of verifying whether a point game is EBM has been lifted and reduced to verifying the validity of a certain related function.

Mochon [Moc07] followed the above reductions and proved the existence of a WCF protocol that achieves arbitrarily small bias, by proposing a suitable family of point games with valid transitions. The family is parametrised, in particular, by an arbitrary integer $k > 1$ which specifies the bias, $\epsilon = \frac{1}{4k+2}$, the games approach. Nevertheless, no explicit WCF protocol was constructed and it was instead left as an open problem. Indeed, while given a WCF protocol with a certain bias it is relatively easy to find the corresponding point game, the other way around can be hard, i.e., translating the point game into a sequence of unitaries that describe the protocol is not an easy task. A step forward was recently taken in [ARW19; ARW18], where a framework called TEF (see §3 of [ARW18]), was introduced. TEF allows the conversion of point games into their corresponding protocols, granted that unitaries associated with the valid functions used by the games can be found. This association of unitaries with valid functions is closely related to the matrices which appear in the EBM description of valid functions. The advantage of TEF is that, using projectors for cheating detection, it can naturally handle situations which correspond to diverging matrices (dual variables) in the EBM description. Hence, we need not worry about such divergences if, and indeed they do, arise later in our later analysis. Using TEF, an analytical construction was given for protocols achieving biases approaching 1/10, lower than the previously ones proposed. This corresponded to Mochon's games parametrised by $k = 2$. It was shown that considering transitions expressible by *real* matrices (EBRM) is sufficient, thus simplifying the analysis. In particular, this allowed for the use of tools from geometry (which we also utilise for our construction here). Finally, to go below this bias, the so-called elliptic monotone align algorithm (EMA) was designed which numerically finds the matrices that determine a protocol with arbitrarily close to zero bias.

3 Overview of the Main Result

We base our construction here on how the protocol with bias 1/10 was constructed corresponding to Mochon's 1/10 bias point game (see §3 of [ARW19]; alternatively see §3 and §4 of [ARW18]). It was shown that in order to describe the protocol, it suffices to find the unitaries[2] corresponding to each valid function used by the game. It is not too hard to see that the following, an even weaker requirement, is enough. Suppose that a valid function can be written as a sum of valid functions. It suffices to find unitaries corresponding to each valid function which appears in the sum[3].

We consider the class of valid functions Mochon uses in his family of point games approaching bias $\frac{1}{4k+2}$ (for arbitrary k). These are of the form (see Definition 18)

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

where $0 \leq x_1 < x_2 \cdots < x_n$ are real numbers, the function $[\![x_i]\!] : [0, \infty) \longrightarrow \mathbb{R}$ is defined as $[\![x_i]\!](x) = \delta_{x_i,x}$ and $f(x)$ is a polynomial[4]. We refer to these as *f-assignments* and in particular, when f is a monomial, we refer to them as *m-assignments* (in lieu of monomial assignments). A closely related form is referred to as effectively m-assignments. We show that Mochon's f-assignments can be expressed as a sum of m-assignments and/or effectively m-assignments. We then solve the m-assignments, i.e. give formulae for the unitaries corresponding to both types of m-assignments.

Theorem 4. *Let t be Mochon's f-assignment (see Definition 18). Then there exist t'_i such that $t = \sum_i \alpha_i t'_i$ where α_i are positive and t'_i are either monomial or effectively monomial assignments (see Corollary 29). Each t'_i admits an analytic solution of the form given in Proposition 35 or Proposition 37.*

[2] Since it suffices to restrict to real matrices, henceforth by unitaries we mean orthogonal matrices.
[3] discussed towards the end of Section 8
[4] with some restrictions which we suppress for brevity

Organisation. We first show how the unitary corresponding to Mochon's f_0-assignment (where $f = x^0$) is constructed. This construction has all the basic ingredients needed for constructing the unitaries corresponding to m-assignments. To this end, we begin our discussion with the Ellipsoid Picture introduced in [ARW18; ARW19] (see §6 and §4 respectively) and give analytic formulae for all relevant quantities (see Section 4). Using the techniques introduced with the EMA algorithm, these quantities are then used to define various maps which allow us to reduce the dimension of the problem and to progressively solve it (see Section 5). After formally defining Mochon's assignment (see Section 6) we give the analytic formula for the unitary corresponding to Mochon's f_0-assignment (see Section 7). To obtain the main result, we show the equivalence of Mochon's f-assignment to sum of m-assignments as explained (see Section 8) followed by the unitaries for the m-assignments (see Section 9).

Relation to prior work. The EMA algorithm introduced in [ARW19] can numerically find the unitaries corresponding to any valid/EBM function. It relies on numerical algorithms for diagonalising matrices to reduce the dimension of the problem and for finding solutions to polynomial equations. This stymied the construction of analytic solutions. Here, we remove the need of diagonalising matrices by using three techniques. First, we recast the problem using isometries instead of unitaries, second we derive and use analytic expressions for the various geometric properties that were used, third we restrict ourselves to Mochon's assignment and connect its properties (see [Moc07]) with those appearing geometrically. In the EMA algorithm, the problem of finding solutions to polynomial equations arises as a consequence of alignment using operator monotone functions. Alignment is crucial for reducing the dimension of the problem which is what eventually leads to a solution. Here, given a Mochon's assignment, we show how to break it into a sum of valid functions in such a way that each valid function in the sum possesses a special property—it is always aligned. While this last step leads to an increase in dimensions (hence resources needed to implement the protocol), it allows us to obtain an analytic solution to the problem. To break up Mochon's assignments in this way we harness the special structure of the assignments and use the operator monotone $-1/x$ (as opposed to the more general $f_\lambda(x) = \frac{-1}{\lambda+x}$) appropriately in both the matrix and the function formalisms. Using this general construction, we show that the unitary corresponding to the key transition/function of the bias $1/10$ game has a particularly simple form, albeit at the cost of increased dimensions (see Example 24). This form is in stark contrast with that of the unitary used in the bias $1/10$ protocol which was introduced in [ARW19]. There, the unitary was found perturbatively and therefore obfuscated the underlying general mathematical structure.

Notation. We restrict to real vector spaces for the remainder of this document. By an $n \times n$ matrix $M \geq 0$ we mean that the matrix is symmetric and its eigenvalues are non-negative (greater than or equal to zero) while by $M > 0$ we mean the eigenvalues are strictly positive. We denote $\mathcal{N}(|\psi\rangle) = |\psi\rangle / \sqrt{\langle\psi|\psi\rangle}$. We also use $(a, b, c) \oplus (d, e) = (a, b, c, d, e)$. Suppose S is a 4-tuple and we wish to refer to the third element of S. We do this as

$$(*, *, p, *) := S. \tag{2}$$

In the interest of conciseness, a matrix of rank at most k is denoted by $M^{\bar{k}}$. We always use a bar in superscript to distinguish it from powers. For instance $(M^{\bar{k}})^2$ refers to the square of a rank k matrix $M^{\bar{k}}$. We continue using the notation from [ARW19] and represent, for instance, initial probabilities as $p_{g_1}, p_{g_2} \ldots$ and final probabilities as $p_{h_1}, p_{h_2} \ldots$ where g and h are not indices but simply indicate initial and final respectively.

Colour Scheme. To facilitate reading, in all technical sections we use purple for intuitive discussions, blue for proofs and black for formal statements.

4 Ellipsoid Picture

Given a positive matrix we can associate an ellipsoid with it. We introduce projectors from the outset to handle low rank matrices which become rife in the analysis later.

Notation 5. Given a projector Π, we denote the set $\{\Pi|v\rangle \,|\, |v\rangle \in \mathbb{R}^n\}$ by $\Pi\mathbb{R}^n$.

Definition 6 (Ellipsoid and Map)**.** Given an $n \times n$ matrix $G \geq 0$, let Π be a projector onto the non-zero eigenvalue eigenspace of G. The *Ellipsoidal Manifold* (or simply the *ellipsoid*) associated with G is given by $S_G := \{|s\rangle \in \Pi\mathbb{R}^n | \langle s| G |s\rangle = 1\}$. The *Ellipsoid Map*, $\mathcal{E}_G : \Pi\mathbb{R}^n \to \Pi\mathbb{R}^n$, is defined as $\mathcal{E}_G(|v\rangle) = |v\rangle / \sqrt{\langle v| G |v\rangle}$.

Note that $\langle s| H |s\rangle = 1$ is essentially of the form $\sum_i h_i s_i^2 = 1$, i.e. the equation of an ellipsoid, justifying our choice of words. We now give a (known) formula for the associated support function. To facilitate the application to low rank matrices, we introduce the use of the turnstile symbol (⊣) to represent an inverse on the non-zero subspace.

Definition 7 (Positive Inverse)**.** Given a symmetric matrix M, let $\Pi^\perp = \mathbb{I} - \Pi$ be the projector onto its null space (set of $|v\rangle$ such that $M|v\rangle = 0$). Then the *Positive Inverse* of M is defined as

$$M^{\dashv} := \Pi \left(M + \Pi^\perp\right)^{-1} \Pi.$$

Equivalently, one could use the spectral decomposition. Given $M = \sum_{i=1}^m \lambda_i |i\rangle \langle i|$ where all $\lambda_i > 0$ without loss of generality,

$$M^{\dashv} := \sum_{i=1}^m \lambda_i^{-1} |i\rangle \langle i| .$$

The curvature of the ellipsoid at a given point is given by the so-called Weingarten Map. In practice, it is easier to evaluate the Reverse Weingarten Map which is denoted by W. The positive inverse of the Reverse Weingarten Map yields the Weingarten Map. For details, see Section A. These quantities, together with the normal, for the ellipsoid admit simple analytic formulae which are given below.

Definition 8 (Normal Function, Reverse Weingarten Map, Inverse of the Weingarten Map, Orthogonal Component)**.** Given a matrix $G \geq 0$, its positive inverse $G^{\dashv}$ and a vector $|v\rangle$ (such that $G|v\rangle \neq 0$) we define the following functions. We use $\left\langle G^j \right\rangle := \langle v| G^j |v\rangle$.

- The normal function, from $G, |v\rangle$ to a vector $|u\rangle$ is defined as

$$|u(G,|v\rangle)\rangle := \frac{G|v\rangle}{\langle G^2\rangle}.$$

- The Weingarten Map from $G, |v\rangle$ to a matrix $W^{\dashv}$ is defined as

$$W^{\dashv}(G,|v\rangle) := \sqrt{\frac{\langle G\rangle}{\langle G^2\rangle}}\left(G + \frac{\left\langle G^3\right\rangle}{\langle G^2\rangle^2} G|v\rangle\langle v|G - \frac{1}{\langle G^2\rangle}\left(G|v\rangle\langle v|G^2 + G^2|v\rangle\langle v|G\right)\right).$$

- The Reverse Weingarten Map from $G, G^{\dashv}, |v\rangle$ to W is defined to be

$$W(G, G^{\dashv}, |v\rangle) := \sqrt{\frac{\langle G^2\rangle}{\langle G\rangle}}\left(G^{\dashv} - \frac{|v\rangle\langle v|}{\langle G\rangle}\right).$$

- The Orthogonal Component from $G, |v\rangle$ to $|e\rangle$ is defined to be

$$|e(G,|v\rangle)\rangle := \mathcal{N}\left[|v\rangle - \langle u|v\rangle |u\rangle\right]$$

  where $|u\rangle = |u(G,|v\rangle)\rangle$.
  The Orthogonal Component from $|v'\rangle, |v\rangle$ to $|e\rangle$ is defined to be

$$|e(|v'\rangle, |v\rangle)\rangle := \mathcal{N}[|v\rangle - \langle v'|v\rangle |v'\rangle].$$

Evaluating the Weingarten map at a given point of a rotated ellipsoid is the same as evaluating it for the unrotated ellipsoid and then rotating it. The following remark makes this precise.

Remark 9. Let $G \geq 0$ be an $n \times n$ rank k matrix and Q be an isometry from the non-trivial k dimensional subspace of G to an arbitrary k dimensional subspace. Then $W^{\dashv}(QGQ^T, Q|v\rangle) = QW^{\dashv}(G,|v\rangle)Q^T$.

Our interest in the geometry of ellipsoids stems from the following connection with matrix inequalities. These inequalities appear in EBM/EBRM transitions. Let $H \geq 0$ and $G \geq 0$. One can rewrite a matrix inequality as follows:

$$\begin{aligned} & H - OGO^T \geq 0 & \\ \iff & \langle s|H|s\rangle - \langle s|OGO^T|s\rangle \geq 0 & \forall\ |s\rangle \\ \iff & \langle s|OGO^T|s\rangle \leq 1 & \forall\ \{|s\rangle \,|\, \langle s|H|s\rangle = 1\}. \end{aligned}$$

From Definition 6 one can interpret the last step as stating that along all directions $|s\rangle$, the ellipsoid corresponding to H will be inside the ellipsoid corresponding to OGO^T. If H and G are fixed, then finding the orthogonal matrix O can be seen as rotating the G ellipsoid into an orientation such that the H ellipsoid stays inside.

Recall that a valid function is equivalent to an EBM function (see Section 2). Given a valid function $t = \sum_i p_{h_i} [\![x_{h_i}]\!] - \sum_i p_{g_i} [\![x_{g_i}]\!]$, it is easy to re-write the matrices that appear in the EBM description into a form which satisfies[5] $H \geq OGO^T$, $O|v\rangle = |w\rangle$ where $|v\rangle \doteq (\sqrt{p_{g_1}}, \sqrt{p_{g_2}} \dots)$ and $|w\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \dots)$ while $H = \mathrm{diag}(x_{h_1}, x_{h_2} \dots)$ and $G = \mathrm{diag}(x_{g_1}, x_{g_2} \dots)$. Motivated by this and foreseeing dimension reductions, we define matrix instances to facilitate further discussion.

Definition 10 ((Extended) Matrix Instance)**.** Let

- $n \geq k$ be positive integers,
- $\mathcal{H}^{\bar{k}}$ and $\mathcal{G}^{\bar{k}}$ be two k dimensional Hilbert spaces,
- $H \geq 0$, $G \geq 0$ be $n \times n$ non-zero matrices of rank at most k, such that H has support only on $\mathcal{H}_h^{\bar{k}}$ and similarly, G has support only on $\mathcal{H}_g^{\bar{k}}$,
- $|w\rangle \in \mathcal{H}_h^{\bar{k}}$ and $|v\rangle \in \mathcal{H}_g^{\bar{k}}$ be vectors of equal norm, $|u_h\rangle \in \mathcal{H}^{\bar{k}}$ and $\left|u_g\right\rangle \in \mathcal{G}^{\bar{k}}$ be vectors with unit norm,

[5](see, for instance, Lemma 60 in [ARW18]; we suppressed the details about the dimensions and the spectra of matrices)

A *matrix instance* is defined to be the tuple $\underline{\mathrm{X}}^{\bar{k}} := (H, G, |w\rangle, |v\rangle)$ while an *extended matrix instance* is defined to be the tuple $\underline{\mathrm{M}}^{\bar{k}} := \underline{\mathrm{X}}^{\bar{k}} \oplus (H^{\dashv}, G^{\dashv}, |u_h\rangle, |u_g\rangle)$.

The extended matrix instance may be *partially specified* using a blank ket, $|.\rangle$, for as-yet undefined vectors and a blank matrix, [.], for as-yet undefined matrices. We say an extended matrix instance is *completely specified* if it has no $|.\rangle$ for vectors and [.] for matrices.

The set of all matrix instances (of $n \times n$ dimensions) is denoted by $\mathbb{X}^n$ and that of extended matrix instances is denoted by $\mathbb{M}^n$. We now define some properties of the (extended) matrix instance.

- Let $Q : \mathcal{G}^{\bar{k}} \to \mathcal{H}^{\bar{k}}$ be an isometry, i.e. $Q^T Q = \mathbb{I}_h$ and $QQ^T = \mathbb{I}_g$ where $\mathbb{I}_h$ is the identity in $\mathcal{H}^{\bar{k}}$ and similarly $\mathbb{I}_g$ is the identity in $\mathcal{G}^{\bar{k}}$. We say that Q *solves* the *matrix instance* $\underline{\mathrm{X}}^{\bar{k}}$ iff
$$\begin{aligned} H &\geq QGQ^T \\ Q|v\rangle &= |w\rangle . \end{aligned}$$
Similarly we say that Q *resolves* (reverse solves) the matrix instance iff
$$\begin{aligned} H &\leq QGQ^T, \\ Q|v\rangle &= |w\rangle . \end{aligned}$$
- We say that $\underline{\mathrm{X}}^{\bar{k}}$ satisfies the *contact condition* iff $\langle w| H |w\rangle = \langle v| G |v\rangle$. This extends to $\underline{\mathrm{M}}^{\bar{k}}$.
- We say that $\underline{\mathrm{X}}^{\bar{k}}$ satisfies the *component condition* iff $\langle w| H^2 |w\rangle = \langle v| G^2 |v\rangle$. This extends to $\underline{\mathrm{M}}^{\bar{k}}$.
- We say that $\underline{\mathrm{X}}^{\bar{k}}$ has *wiggle-w room* iff H has an eigenvector $|t_h\rangle$ with eigenvalue $1/\epsilon$ which has no overlap with $|w\rangle$, viz. $H|t_h\rangle = \epsilon^{-1}|t_h\rangle$, $\langle w|t_h\rangle = 0$. When we need the vector explicitly, we say that $\underline{\mathrm{X}}^{\bar{k}}$ has *wiggle-w room* (ϵ) *along* $|t_h\rangle$. Similarly, we say that $\underline{\mathrm{X}}^{\bar{k}}$ has *wiggle-v room* ((ϵ) along $|t_g\rangle$) iff G has an eigenvector $|t_g\rangle$ with eigenvalue $1/\epsilon$ which has no overlap with $|v\rangle$, viz. $G|t_g\rangle = \epsilon^{-1}|t_g\rangle$, $\langle v|t_g\rangle = 0$. Again, when we need the vector explicitly, we say that $\underline{\mathrm{X}}^{\bar{k}}$ has *wiggle-v room (ϵ) along* $|t_g\rangle$.

The contact condition holds if the two ellipsoids represented by H and QGQ^T touch along the $|w\rangle$ direction. The component condition holds if the component of the probability vector along the corresponding normal vector is the same for both ellipsoids, i.e. if $\langle u_h|w\rangle = \langle u_g|v\rangle$ where $|u_h\rangle$ is the normal along[6] $|w\rangle$ of ellipsoid H and $|u_g\rangle$ is the normal along $|v\rangle$ for ellipsoid G. The notion of wiggle-w/v should become clear when it is next discussed.

We stress that, given a matrix instance $\underline{\mathrm{X}}$ and letting $(H, G, *, *) := \underline{\mathrm{X}}$, the extended matrix instance contains $H^{\dashv}$ and $G^{\dashv}$ as elements which are completely determined by H and G respectively. However, here we wish to find an analytic expression for these quantities. This is why we keep track of $H^{\dashv}$ as an explicit function of H (similarly for $G^{\dashv}$ and G) and the extended matrix instance is so defined to enable this.

5 Weingarten Iteration | Isometric Iteration using the Weingarten Map

Given a matrix instance, numerically one can construct the extended matrix instance trivially. However, we are interested in analytic solutions. We therefore discuss two ways of constructing extended matrix instance. The first—Normal Initialisation Map—evaluates the normals associated with a (an extended) matrix instance, resulting in a (possibly partially specified) extended matrix instance. The second—Weingarten Initialisation Map—takes a rank k (extended) matrix instance and constructs a rank $k-1$ (extended) matrix instance. Lemma 13 relates the solution of these two matrix instances under certain conditions. These results (and their extensions) are the workhorses of our construction. We successively reduce the problem, while retaining analytic expressions for all the quantities involved, until the problem is solved. The conditions we mentioned can be shown to hold for Mochon's assignments, although this requires more work and we defer it to the following sections.

The key idea used is that if two ellipsoids, one contained inside the other, touch at a point then one can deduce that at that point their normals must match and that the inner ellipsoid should be more curved than the one outside.

Definition 11 (Normal Initialisation Map)**.** Given a matrix instance $\underline{\mathrm{X}}^{\bar{k}} =: (H, G, |w\rangle, |v\rangle)$, the *normal initialisation map* $\mathscr{U} : \mathbb{X}^n \to \mathbb{M}^n$ is defined by its action
$$\underline{\mathrm{X}}^{\bar{k}} \mapsto \underline{\mathrm{X}}^{\bar{k}} \oplus (H^{\dashv}, G^{\dashv}, |u(H, |w\rangle)\rangle, |u(G, |v\rangle)\rangle).$$
Given an extended matrix instance $\underline{\mathrm{M}}^{\bar{k}}$, let $(*, \cdots *, |u_h\rangle, |u_g\rangle) := \underline{\mathrm{M}}^{\bar{k}}$ (see Equation (2)). The *normal initialisation map* $\mathscr{U} : \mathbb{M}^n \to \mathbb{M}^n$ leaves all components of $\underline{\mathrm{M}}^{\bar{k}}$ unchanged, except $|u_h\rangle$ and $|u_g\rangle$ which are mapped as (see Definition 8):
$$\begin{aligned} |u_h\rangle &\mapsto |u(H, |w\rangle)\rangle \\ |u_g\rangle &\mapsto |u(G, |v\rangle)\rangle . \end{aligned}$$

[6] Consider the point on the H ellipsoid at which a ray along $|w\rangle$ touches it. By the normal at $|w\rangle$ we mean the normal at this point (see Lemma 44).

Definition 12 (Weingarten Iteration Map). Consider a matrix instance $\underline{\mathrm{X}}^{\bar{k}} =: \left(H^{\bar{k}}, G^{\bar{k}}, \left|w^{\bar{k}}\right\rangle, \left|v^{\bar{k}}\right\rangle\right)$ and let (see Definition 8)

$$\left|v^{\overline{k-1}}\right\rangle := \left|e\left(G^{\bar{k}}, \left|v^{\bar{k}}\right\rangle\right)\right\rangle, \qquad \left|w^{\overline{k-1}}\right\rangle := \left|e\left(H^{\bar{k}}, \left|w^{\bar{k}}\right\rangle\right)\right\rangle,$$
$$G^{\overline{k-1}} := W^{\dashv}\left(G^{\bar{k}}, \left|v^{\bar{k}}\right\rangle\right), \qquad H^{\overline{k-1}} := W^{\dashv}\left(H^{\bar{k}}, \left|w^{\bar{k}}\right\rangle\right).$$

Then we define the *Weingarten Iteration Map*, $\mathscr{W} : \mathbb{X}^n \to \mathbb{X}^n$ by its action

$$\underline{\mathrm{X}}^{\bar{k}} \mapsto \left(H^{\overline{k-1}}, G^{\overline{k-1}}, \left|w^{\overline{k-1}}\right\rangle, \left|v^{\overline{k-1}}\right\rangle\right) =: \underline{\mathrm{X}}^{\overline{k-1}}.$$

Consider an extended matrix instance $\underline{\mathrm{M}}^{\bar{k}} =: \underline{\mathrm{X}}^{\bar{k}} \oplus S$ and let $\left((H^{\bar{k}})^{\dashv}, (G^{\bar{k}})^{\dashv}, *, *\right) := S$ (see Equation (2)). Let (see Definition 8)

$$(G^{\overline{k-1}})^{\dashv} := W\left(G^{\bar{k}}, (G^{\bar{k}})^{\dashv}, \left|v^{\bar{k}}\right\rangle\right), \qquad (H^{\overline{k-1}})^{\dashv} := W\left(H^{\bar{k}}, (H^{\bar{k}})^{\dashv}, \left|w^{\bar{k}}\right\rangle\right).$$

Then we define the *Weingarten Iteration Map*, $\mathscr{W} : \mathbb{M}^n \to \mathbb{M}^n$ by its action

$$\underline{\mathrm{M}}^{\bar{k}} \mapsto \underline{\mathrm{X}}^{\overline{k-1}} \oplus \left((H^{\overline{k-1}})^{\dashv}, (G^{\overline{k-1}})^{\dashv}, |.\rangle, |.\rangle\right) =: \underline{\mathrm{M}}^{\overline{k-1}}.$$

Lemma 13. *Consider a matrix instance $\underline{\mathrm{X}}^{\bar{k}}$ which satisfies both the contact condition and the component condition. Let $\underline{\mathrm{X}}^{\bar{k}} \oplus \left(\left|u_h^{\bar{k}}\right\rangle, \left|u_g^{\bar{k}}\right\rangle\right) := \mathscr{U}(\underline{\mathrm{X}}^{\bar{k}})$ and $\underline{\mathrm{X}}^{\overline{k-1}} := \mathscr{W}(\underline{\mathrm{X}}^{\bar{k}})$ (see Definition 11 and Definition 12). We assert that if $Q^{\bar{k}}$ (re)solves the matrix instance $\underline{\mathrm{X}}^{\bar{k}}$ then*

$$Q^{\bar{k}} = \left|u_h^{\bar{k}}\right\rangle \left\langle u_g^{\bar{k}}\right| + Q^{\overline{k-1}} \tag{3}$$

where $Q^{\overline{k-1}}$ (re)solves the matrix instance $\underline{\mathrm{X}}^{\overline{k-1}}$.

Proof. Let $\left(H^{\bar{k}}, G^{\bar{k}}, \left|w^{\bar{k}}\right\rangle, \left|v^{\bar{k}}\right\rangle\right) := \underline{\mathrm{X}}^{\bar{k}}$, $(*, *, *, D^{\bar{k}}) := S$ and $\left(H^{\overline{k-1}}, G^{\overline{k-1}}, \left|w^{\overline{k-1}}\right\rangle, \left|v^{\overline{k-1}}\right\rangle\right) := \underline{\mathrm{X}}^{\overline{k-1}}$. Using the ellipsoid picture (see Section 4) for the matrix inequality $H^{\bar{k}} \geq Q^{\bar{k}} G^{\bar{k}} Q^{\bar{k}T}$ it is clear that the ellipsoid corresponding to $H^{\bar{k}}$ is contained inside the ellipsoid corresponding to $Q^{\bar{k}} G^{\bar{k}} Q^{\bar{k}\dagger}$. The two ellipsoids touch along the $\left|w^{\bar{k}}\right\rangle$ direction if and only if

$$\left\langle w^{\bar{k}}\right| H^{\bar{k}} \left|w^{\bar{k}}\right\rangle = \left\langle w^{\bar{k}}\right| Q^{\bar{k}} G^{\bar{k}} Q^{\bar{k}\dagger} \left|w^{\bar{k}}\right\rangle = \left\langle v^{\bar{k}}\right| G^{\bar{k}} \left|v^{\bar{k}}\right\rangle$$

(the last step follows from noting $Q^{\bar{k}} \left|v^{\bar{k}}\right\rangle = \left|w^{\bar{k}}\right\rangle$ and the fact that $Q^{\bar{k}}$ is an isometry). This is precisely the contact condition (which is given to hold). The component condition ensures that the components of the probability vectors along their respective normals are the same, viz. $\left\langle w^{\bar{k}} | u_h^{\bar{k}}\right\rangle = \left\langle v^{\bar{k}} | u_g^{\bar{k}}\right\rangle$ (use Lemma 44). From this we can deduce three necessary conditions.

First, that Equation (3) holds. The normal along $\left|w^{\bar{k}}\right\rangle$ (see Lemma 44) of the ellipsoid $H^{\bar{k}}$ and that of the ellipsoid $Q^{\bar{k}} G^{\bar{k}} Q^{\bar{k}T}$ must be the same. This in turn means that $Q^{\bar{k}}$ must map the normal $\left|u_g^{\bar{k}}\right\rangle$ along $\left|v^{\bar{k}}\right\rangle$ for the ellipsoid $G^{\bar{k}}$ to the normal $\left|u_h^{\bar{k}}\right\rangle$ along $|w\rangle$ for the ellipsoid $H^{\bar{k}}$, viz. $\left|u_g^{\bar{k}}\right\rangle := \left|u\left(G^{\bar{k}}, \left|v^{\bar{k}}\right\rangle\right)\right\rangle \to \left|u_h^{\bar{k}}\right\rangle := \left|u\left(H^{\bar{k}}, \left|w^{\bar{k}}\right\rangle\right)\right\rangle$ (see Definition 8). Consequently,

$$Q^{\bar{k}} = \left|u_h^{\bar{k}}\right\rangle \left\langle u_g^{\bar{k}}\right| + Q^{\overline{k-1}} \tag{4}$$

where $Q^{\overline{k-1}} : \mathcal{H}_g^{\overline{k-1}} \to \mathcal{H}_h^{\overline{k-1}}$ is an isometry because the action on the normals is completely determined.

Second, note that the curvature along $\left|w^{\bar{k}}\right\rangle$ of the ellipsoid $H^{\bar{k}}$ must be greater than that of the ellipsoid $Q^{\bar{k}} G^{\bar{k}} Q^{\bar{k}T}$, viz.

$$\begin{aligned}
H^{\overline{k-1}} = W^{\dashv}\left(H^{\bar{k}}, \left|w^{\bar{k}}\right\rangle\right) &\geq W^{\dashv}\left(Q^{\bar{k}} G^{\bar{k}} Q^{\bar{k}T}, Q^{\bar{k}} \left|v^{\bar{k}}\right\rangle\right) \\
&= Q^{\bar{k}} W^{\dashv}(G^{\bar{k}}, \left|v^{\bar{k}}\right\rangle) Q^{\bar{k}T} && \text{from 9} \\
&= Q^{\overline{k-1}} \underbrace{W^{\dashv}(G^{\bar{k}}, \left|v^{\bar{k}}\right\rangle)}_{=G^{\overline{k-1}}} Q^{\overline{k-1}T} && \because \quad W^{\dashv}(G^{\bar{k}}, \left|v^{\bar{k}}\right\rangle) \left|u_g^{\bar{k}}\right\rangle = 0; \quad \text{as in the proof of Lemma 47} \\
&= Q^{\overline{k-1}} G^{\overline{k-1}} Q^{\overline{k-1}T}.
\end{aligned}$$

Finally, since $Q^{\bar{k}}\left|v^{\bar{k}}\right\rangle = \left|w^{\bar{k}}\right\rangle$ it follows that $\left(\mathbb{I}_h^{\bar{k}} - \left|u_h^{\bar{k}}\right\rangle\left\langle u_h^{\bar{k}}\right|\right) Q^{\bar{k}}\left|v^{\bar{k}}\right\rangle = \left(\mathbb{I}_h^{\bar{k}} - \left|u_h^{\bar{k}}\right\rangle\left\langle u_h^{\bar{k}}\right|\right)\left|w^{\bar{k}}\right\rangle$. Using

$$\left(\mathbb{I}_h^{\bar{k}} - \left|u_h^{\bar{k}}\right\rangle\left\langle u_h^{\bar{k}}\right|\right) Q^{\bar{k}} = \left(\mathbb{I}_h^{\bar{k}} - \left|u_h^{\bar{k}}\right\rangle\left\langle u_h^{\bar{k}}\right|\right) Q^{\bar{k}} \left(\mathbb{I}_g^{\bar{k}} - \left|u_g^{\bar{k}}\right\rangle\left\langle u_g^{\bar{k}}\right|\right)$$

in the LHS and Definition 8 for $|e(.,.)\rangle$, one obtains the equation $Q^{\overline{k-1}}\left|v^{\overline{k-1}}\right\rangle = \left|w^{\overline{k-1}}\right\rangle$. These show that $Q^{\overline{k-1}}$ indeed solves $\underline{\mathrm{X}}^{\overline{k-1}}$. Changing the direction of the inequality doesn't change any other argument, which also proves the resolve case. □

It is not hard to imagine a situation where one of the ellipsoids has been flattened; for instance in the 3 dimensional case, an ellipsoid could be flattened into a disk. This breaks our procedure of matching normals which was used to prove the lemma. In terms of matrices, this corresponds to the case where one of the eigenvalues diverges. Under these circumstances, the Normal Initialisation Map and the Iteration Map need to be redefined. Their definitions might seem arbitrary at first but the proof of Lemma 16 should justify them. The key idea here is to consider two ellipsoids, one ellipsoid inside the other, touch at a point and one of the ellipsoids is flattened as described. Then the component of the normal of the inner ellipsoid along the flattened direction is not well defined. By using this freedom and demanding consistency, the desired result can be obtained.

Definition 14 (Wiggle-w/v Normal Initialisation Map)**.** Consider a matrix instance $\underline{\mathrm{X}}^{\bar{k}}$, let $(H, G, |w\rangle, |v\rangle) := \underline{\mathrm{X}}^{\bar{k}}$ with wiggle-w room along $|t_h\rangle$ (see Definition 10). The *Wiggle-w Normal Initialisation Map* $\mathscr{U}_w : \mathbb{X}^n \to \mathbb{M}^n$ is defined by its action

$$\underline{\mathrm{X}}^{\bar{k}} \mapsto \underline{\mathrm{X}}^{\bar{k}} \oplus \left([.], [.], \cos\theta\, |u(H, |w\rangle)\rangle + \sin\theta\, |t_h\rangle, |u(G, |v\rangle)\rangle\right)$$

where $\cos\theta := \langle v|u(G, |v\rangle)\rangle / \langle w|u(H, |w\rangle)\rangle$ (see Definition 11).

Given an extended matrix instance $\underline{\mathrm{M}}^{\bar{k}}$, let $\left(*, \cdots *, |u_h\rangle, \left|u_g\right\rangle\right) := \underline{\mathrm{M}}^{\bar{k}}$ (see Equation (2)), the *Wiggle-w Normal Initialisation Map* $\mathscr{U}_w : \mathbb{M}^n \to \mathbb{M}^n$ is defined by its action on $|u_h\rangle$ and $\left|u_g\right\rangle$ (see Definition 11),

$$\begin{aligned} |u_h\rangle &\mapsto \cos\theta\, |u(H, |w\rangle)\rangle + \sin\theta\, |t_h\rangle \\ \left|u_g\right\rangle &\mapsto |u(G, |v\rangle)\rangle\,. \end{aligned}$$

Similarly, consider a matrix instance $\underline{\mathrm{X}}^{\bar{k}} =: (H, G, |w\rangle, |v\rangle)$ with wiggle-v room along $\left|t_g\right\rangle$ (see Definition 10). The *Wiggle-v Normal Initialisation Map* $\mathscr{U}_v : \mathbb{X}^n \to \mathbb{M}^n$ is defined by its action

$$\underline{\mathrm{X}}^{\bar{k}} \mapsto \underline{\mathrm{X}}^{\bar{k}} \oplus \left([.], [.], |u(H, |w\rangle)\rangle, \cos\theta\, |u(G, |w\rangle)\rangle + \sin\theta\, \left|t_g\right\rangle\right)$$

where $\cos\theta := \langle w|u(H, |w\rangle)\rangle / \langle v|u(G, |v\rangle)\rangle$ (see Definition 11).

Given an extended matrix instance $\underline{\mathrm{M}}^{\bar{k}}$, let $\left(*, \cdots *, |u_h\rangle, \left|u_g\right\rangle\right) := \underline{\mathrm{M}}^{\bar{k}}$ (see Equation (2)), the *Wiggle-v Normal Initialisation Map* $\mathscr{U}_v : \mathbb{M}^n \to \mathbb{M}^n$ is defined by its action on $|u_h\rangle$ and $\left|u_g\right\rangle$ (see Definition 11),

$$\begin{aligned} |u_h\rangle &\mapsto |u(H, |w\rangle)\rangle \\ \left|u_g\right\rangle &\mapsto \cos\theta\, |u(G, |v\rangle)\rangle + \sin\theta\, \left|t_g\right\rangle\,. \end{aligned}$$

Definition 15 (Wiggle-w/v Iteration Map)**.** Consider an extended matrix instance $\underline{\mathrm{M}}^{\bar{k}}$ and let

$$\left(H^{\bar{k}}, G^{\bar{k}}, \left|w^{\bar{k}}\right\rangle, \left|v^{\bar{k}}\right\rangle, (H^{\bar{k}})^{\dashv}, (G^{\bar{k}})^{\dashv}, \left|u_h^{\bar{k}}\right\rangle, \left|u_g^{\bar{k}}\right\rangle\right) := \underline{\mathrm{M}}^{\bar{k}}.$$

Further, let (see Definition 11)

$$\begin{aligned} \left|v^{\overline{k-1}}\right\rangle &= \left|e\left(G^{\bar{k}}, \left|v^{\bar{k}}\right\rangle\right)\right\rangle, & \left|w^{\overline{k-1}}\right\rangle &= \left|e\left(\left|u_h^{\bar{k}}\right\rangle, \left|w^{\bar{k}}\right\rangle\right)\right\rangle, \\ G^{\overline{k-1}} &= W^{\dashv}\left(G^{\bar{k}}, \left|v^{\bar{k}}\right\rangle\right), & H^{\overline{k-1}} &= W^{\dashv}\left(H^{\bar{k}}, \mathcal{N}\left((H^{\bar{k}})^{\dashv}\left|u_h^{\bar{k}}\right\rangle\right)\right), \\ (G^{\overline{k-1}})^{\dashv} &= W\left(G^{\bar{k}}, (G^{\bar{k}})^{\dashv}, \left|v^{\bar{k}}\right\rangle\right), & (H^{\overline{k-1}})^{\dashv} &= W\left(H^{\bar{k}}, (H^{\bar{k}})^{\dashv}, \mathcal{N}\left((H^{\bar{k}})^{\dashv}\left|u_h^{\bar{k}}\right\rangle\right)\right). \end{aligned}$$

The *Wiggle-w Iteration Map* $\mathscr{W}_w : \mathbb{M}^n \to \mathbb{M}^n$ is defined by its action

$$\underline{\mathrm{M}}^{\bar{k}} \mapsto \left(H^{\overline{k-1}}, G^{\overline{k-1}}, \left|w^{\overline{k-1}}\right\rangle, \left|v^{\overline{k-1}}\right\rangle, (H^{\overline{k-1}})^{\dashv}, (G^{\overline{k-1}})^{\dashv}, |.\rangle, |.\rangle\right) =: \mathrm{M}^{\overline{k-1}}.$$

Similarly, consider an extended matrix instance $\underline{\mathrm{M}}^{\bar{k}}$ and let

$$\left(H^{\bar{k}}, G^{\bar{k}}, \left|w^{\bar{k}}\right\rangle, \left|v^{\bar{k}}\right\rangle, (H^{\bar{k}})^{\dashv}, (G^{\bar{k}})^{\dashv}, \left|u_h^{\bar{k}}\right\rangle, \left|u_g^{\bar{k}}\right\rangle\right) := \underline{\mathrm{M}}^{\bar{k}}.$$

Further, let (see Definition 11)

$$\left|v^{\overline{k-1}}\right\rangle = \left|e\left(\left|u_g^{\bar{k}}\right\rangle, \left|v^{\bar{k}}\right\rangle\right)\right\rangle, \qquad \left|w^{\overline{k-1}}\right\rangle = \left|e\left(H^{\bar{k}}, \left|w^{\bar{k}}\right\rangle\right)\right\rangle,$$
$$G^{\overline{k-1}} = W^{\dashv}\left(G^{\bar{k}}, \mathcal{N}\left((G^{\bar{k}})^{\dashv}\left|u_g^{\bar{k}}\right\rangle\right)\right), \qquad H^{\overline{k-1}} = W^{\dashv}\left(H^{\bar{k}}, \left|w^{\bar{k}}\right\rangle\right),$$
$$(G^{\overline{k-1}})^{\dashv} = W\left(G^{\bar{k}}, (G^{\bar{k}})^{\dashv}, \mathcal{N}\left((G^{\bar{k}})^{\dashv}\left|u_g^{\bar{k}}\right\rangle\right)\right), \qquad (H^{\overline{k-1}})^{\dashv} = W\left(H^{\bar{k}}, (H^{\bar{k}})^{\dashv}, \left|w^{\bar{k}}\right\rangle\right).$$

The *Wiggle-v Iteration Map* $\mathscr{W}_v : \mathbb{M}^n \to \mathbb{M}^n$ is defined by its action

$$\underline{M}^{\bar{k}} \mapsto \left(H^{\overline{k-1}}, G^{\overline{k-1}}, \left|w^{\overline{k-1}}\right\rangle, \left|v^{\overline{k-1}}\right\rangle, (H^{\overline{k-1}})^{\dashv}, (G^{\overline{k-1}})^{\dashv}, |.\rangle, |.\rangle\right) =: \mathrm{M}^{\overline{k-1}}.$$

While the following result holds only for $\epsilon \to 0$, this is not unphysical (see the discussion before Proposition 22).

Lemma 16. *Consider an extended matrix instance $\underline{M}^{\bar{k}}$ with wiggle-w room ϵ along $\left|t_h^{\bar{k}}\right\rangle$ (see Definition 10). Assume it is completely specified (see Definition 10), and it satisfies both $\mathscr{U}_w(\underline{M}^{\bar{k}}) = \underline{M}^{\bar{k}}$ (see Definition 14) and the contact condition (see Definition 10). Let $\left(*, \cdots *, \left|u_h^{\bar{k}}\right\rangle, \left|u_g^{\bar{k}}\right\rangle\right) := \underline{M}^{\bar{k}}$ and $\underline{M}^{\overline{k-1}} := \mathscr{W}_w(M^{\overline{k-1}})$ (see Definition 15). We assert that if $Q^{\bar{k}}$ solves $\underline{M}^{\bar{k}}$ in the limit of $\epsilon \to 0$, then*

$$Q^{\bar{k}} = \left|u_h^{\bar{k}}\right\rangle \left\langle u_g^{\bar{k}}\right| + Q^{\overline{k-1}} \tag{5}$$

where $Q^{\overline{k-1}}$ solves $\underline{M}^{\overline{k-1}}$.

Similarly, consider an extended matrix instance $\underline{M}^{\bar{k}}$ with wiggle-v room ϵ along $\left|t_h^{\bar{k}}\right\rangle$ (see Definition 10). Assume it is completely specified (see Definition 10), and it satisfies both $\mathscr{U}_v(\underline{M}^{\bar{k}}) = \underline{M}^{\bar{k}}$ and the contact condition. Let $\left(*, \cdots *, \left|u_h^{\bar{k}}\right\rangle, \left|u_g^{\bar{k}}\right\rangle\right) := \underline{M}^{\bar{k}}$ and $\underline{M}^{\overline{k-1}} := \mathscr{W}_v(M^{\overline{k-1}})$. We assert that if $Q^{\bar{k}}$ resolves $\underline{M}^{\bar{k}}$ in the limit of $\epsilon \to 0$, then

$$Q^{\bar{k}} = \left|u_h^{\bar{k}}\right\rangle \left\langle u_g^{\bar{k}}\right| + Q^{\overline{k-1}}$$

where $Q^{\overline{k-1}}$ resolves $\underline{M}^{\overline{k-1}}$.

Proof. We outline the argument here. It is based on the one given in Section 7.3.2 of [ARW18]. The basic idea is that the component of the normal along the $\left|t_h^{\bar{k}}\right\rangle$ direction can be taken to be arbitrary in the limit of $\epsilon \to 0$. To see this, is it helpful to consider a slightly different sequence of matrix instances, parametrised by ϵ, $\underline{\mathrm{X}}'^{\bar{k}}(\epsilon) =: \left(H'^{\bar{k}}(\epsilon), G'^{\bar{k}}(\epsilon), \left|w'^{\bar{k}}(\epsilon)\right\rangle, \left|v'^{\bar{k}}(\epsilon)\right\rangle\right)$, which converges as $\epsilon \to 0$ to $\lim_{\epsilon\to 0} \underline{\mathrm{X}}^{\bar{k}}(\epsilon) =: \left(H^{\bar{k}}, G^{\bar{k}}, \left|w^{\bar{k}}\right\rangle, \left|v^{\bar{k}}\right\rangle\right)$ (see Figure 2). One can use operator monotones (we omit the details here) to construct such a sequence explicitly and show that the solution of all these instances is the same as a function of ϵ. While the parameters specifying the matrix instances converge, the normal $\left|u_h'^{\bar{k}}(\epsilon)\right\rangle = \left|u\left(H'^{\bar{k}}(\epsilon), \left|w'^{\bar{k}}(\epsilon)\right\rangle\right)\right\rangle$, which is a derived quantity, does not converge to $\left|u\left(H^{\bar{k}}, \left|w^{\bar{k}}\right\rangle\right)\right\rangle$, viz.

$$\lim_{\epsilon\to 0}\left|u_h^{\bar{k}}(\epsilon)\right\rangle \neq \left|u\left(H'^{\bar{k}}, \left|w'^{\bar{k}}\right\rangle\right)\right\rangle.$$

This is because a small wiggle in $\left|w^{\bar{k}}\right\rangle$ can significantly affect the calculation of the normal as the curvature along one of the directions diverges. Hence, given $H^{\bar{k}}$ evaluating the normal along $\lim_{\epsilon\to 0}\left|w^{\bar{k}}(\epsilon)\right\rangle$ is not the same as evaluating the normal along $\left|w^{\bar{k}}\right\rangle$.

We can iterate $\underline{\mathrm{X}}'^{\bar{k}}(\epsilon)$ using Definition 12 and Lemma 13, and because the complete solution doesn't depend on ϵ, we can use it to iterate $\underline{\mathrm{X}}^{\bar{k}}$. Since along $\left|t_h^{\bar{k}}\right\rangle$ is where curvature diverges as $\epsilon \to 0$, the component of the normal along this direction gets ill defined. Using the aforesaid reasoning, we can deduce that[7]

$$\lim_{\epsilon\to 0}\left|u_h'^{\bar{k}}(\epsilon)\right\rangle = \cos\theta\left|u\left(H^{\bar{k}}, \left|w^{\bar{k}}\right\rangle\right)\right\rangle + \sin\theta\left|t_h^{\bar{k}}\right\rangle$$

where $\cos\theta$ remains to be fixed. As was argued in the proof of Lemma 13, $\left\langle u_h'^{\bar{k}}(\epsilon)|w'^{\bar{k}}(\epsilon)\right\rangle = \left\langle u_g'^{\bar{k}}(\epsilon)|v'^{\bar{k}}(\epsilon)\right\rangle$ which in the limit $\epsilon \to 0$ becomes

$$\cos\theta\left\langle u\left(H^{\bar{k}}, \left|w^{\bar{k}}\right\rangle\right)|w^{\bar{k}}\right\rangle = \left\langle u_g^{\bar{k}}|v^{\bar{k}}\right\rangle$$

(since $\left\langle w^{\bar{k}}|t_h^{\bar{k}}\right\rangle = 0$) fixing $\cos\theta$. Defining $\left|u_h^{\bar{k}}\right\rangle := \lim_{\epsilon\to 0}\left|u_h'^{\bar{k}}(\epsilon)\right\rangle$ justifies Definition 14.

[7] subtleties about degeneracies in $\left|t_h^{\bar{k}}\right\rangle$ are not hard to handle and can be adapted from the discussion in [ARW18]

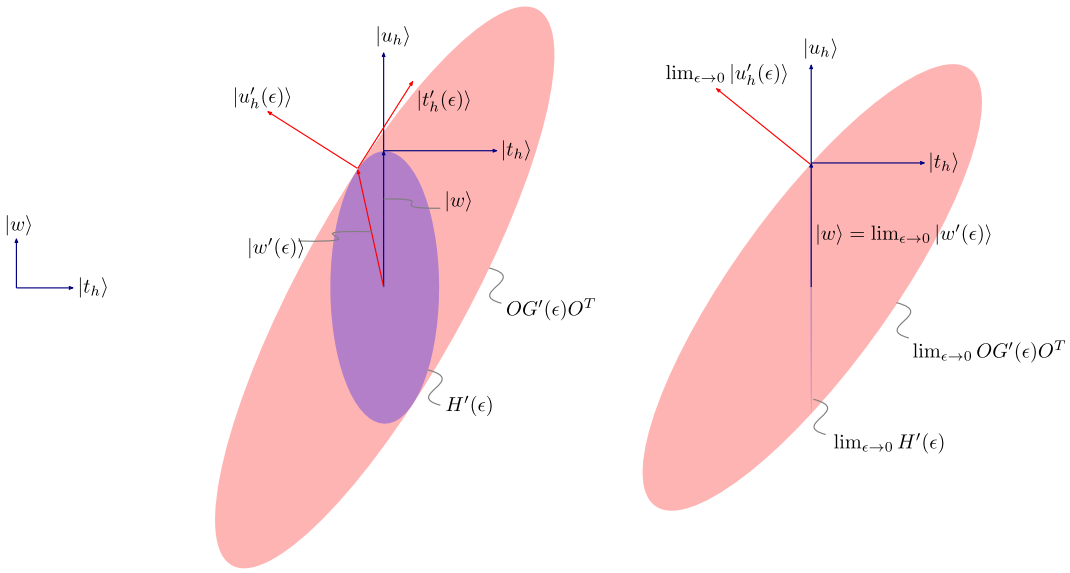

Figure 2: The infinite curvature case, where the wiggle-v method is applied. Physically, this translates into using projectors in the protocol.

Using $\mathscr{W}(\underline{X}'^{\bar{k}}(\epsilon)) = \underline{X}'^{\overline{k-1}}(\epsilon) =: \left(H'^{\overline{k-1}}(\epsilon), G'^{\overline{k-1}}(\epsilon), \left|w'^{\overline{k-1}}(\epsilon)\right\rangle, \left|v'^{\overline{k-1}}(\epsilon)\right\rangle\right)$, in the limit $\epsilon \to 0$, is used to define

$$\underline{X}^{\overline{k-1}} =: \left(H^{\overline{k-1}}, G^{\overline{k-1}}, \left|w^{\overline{k-1}}\right\rangle, \left|v^{\overline{k-1}}\right\rangle\right).$$

Since the diverging term is in $H'^{\bar{k}}(\epsilon)$ and not in $G'^{\overline{k-1}}(\epsilon)$ it follows that $G^{\overline{k-1}}$ and $\left|v^{\overline{k-1}}\right\rangle$ can be evaluated using the usual rule specified by the Weingarten Iteration Map, $\mathscr{W}$ on on $\underline{X}^{\bar{k}}$. This justifies the $G, |v\rangle$ part of Definition 15. The relatively non-trivial part is to show that $H^{\overline{k-1}}$ and $\left|w^{\overline{k-1}}\right\rangle$ can be equivalently defined using the correct normal, $\left|u_h^{\bar{k}}\right\rangle$. We used the fact that we can run the following observation backwards: given a direction of contact $|w\rangle$, the normal to the ellipsoid represented by H is along $H|w\rangle$, viz. given a normal along $|u\rangle$, one can obtain the (direction of) point of contact as $H^{-1}|u\rangle$. As we argued above, $\left|w^{\bar{k}}\right\rangle$ can not be reliably used to derive quantities and therefore $\left|u_h^{\bar{k}}\right\rangle$ (together with the said observation) is used to evaluate the Weingarten map[8], as defined in Definition 15.

If Q solves $\underline{X}'^{\bar{k}}(\epsilon)$ then from Lemma 13 we know that $Q^{\bar{k}} = \left|u_h'^{\bar{k}}(\epsilon)\right\rangle\left\langle u_g'^{\bar{k}}(\epsilon)\right| + Q^{\overline{k-1}}(\epsilon)$, where note that only the decomposition depends on ϵ ($Q^{\bar{k}}$ solves $\underline{X}'^{\bar{k}}(\epsilon)$ but doesn't on ϵ). Taking the limit (and using the correct normals) we obtain the claimed result Equation (5). □

Consider $H > 0, G > 0$. Then $H \geq OGO^T$ is equivalent to $H^{-1} \leq OG^{-1}O^T$. We shall see that at some point, we must consider the latter as our matrix instance. We formalise this procedure for later use.

Definition 17 (Flip Map)**.** Consider an extended matrix instance $\underline{M}^{\bar{n}} =: \left(H, G, |w\rangle, |v\rangle, H^{-1}, G^{-1}, |u_h\rangle, \left|u_g\right\rangle\right)$. We define the *Flip Map* $\mathscr{F} : \mathbb{M}^n \to \mathbb{M}^n$ as $\underline{M}^{\bar{n}} \mapsto \left(H^{-1}, G^{-1}, |w\rangle, |v\rangle, H, G, |u_h\rangle, \left|u_g\right\rangle\right) =: \mathscr{F}(M^{\bar{n}})$.

We have introduced the notation and the main tools we need to construct an analytic solution of one class of Mochon's assignment—the f_0 assignment.

6 Mochon's Assignments

We define Mochon's assignments (these were the only class of valid functions used by Mochon in the construction of his games which achieve arbitrarily small biases; together with the merge, split and raise). We use the notation introduced in [Mil19].

Definition 18 (Mochon's f-assignment, f_0-assignment, balanced assignment)**.** [Moc07; ARW18] Let $[\![a]\!] : \mathbb{R} \to \mathbb{R}$ be a function defined as

$$[\![a]\!](x) = \delta_{a,x} = \begin{cases} 1 & \text{if } a = x \\ 0 & \text{else.} \end{cases}$$

[8] It is not hard to see why $H^{\overline{k-1}}$ does not diverge as ϵ goes to zero (granted there was only one diverging eigenvalue in $H^{\bar{k}}$ to start with). The idea is simply to use reverse Weingarten; this suppresses the divergence into zero, then one projects out a rank one subspace. If there was only one zero eigenvalue, if the subspace includes this eigenspace (spanned by a single eigenvector), then the resulting matrix would not have any zero eigenvalues. This can then be inverted to obtain the Weingarten map which is now finite and well defined.

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

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

(up to a positive multiplicative factor) where h contains the positive part of t and g the negative part (without any common support), viz. $h = \sum_{i:p_i>0} p_i [\![x_i]\!]$ and $g = \sum_{i:p_i<0} (-p_i) [\![x_i]\!]$.

- When the polynomial f has degree 0, we call the assignment an *f_0-assignment.*
- When f is a monomial, viz. has the form $f(x) = x^k$, we call the assignment a *monomial-assignment* or an *m_k-assignment.*
- 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, $p_i > 0$.

It is easy to see that Mochon's f_0-assignment starts with a point that has a negative weight, regardless of the number points used to define the assignment. Thereafter, the sign alternates. With this as the base structure, working out the signs of the weights for m-assignments is facilitated. These considerations become relevant when we construct analytic solutions. However, the only mathematical property of Mochon's assignments which is needed to find an analytic solution, turns out to be the following.

Lemma 19. *[Moc07; ARW18] Let $t = \sum_{i=1}^{n} p_i [\![x_i]\!]$ be Mochon's f_0-assignment for a set of real numbers $0 \leq x_1 < x_2 \cdots < x_n$. Then for $0 \leq k \leq n-2$,*

$$\left\langle x^k \right\rangle = 0$$

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

7 f_0 Unitary | Solution to Mochon's f_0 assignment

We finally give an analytic solution to one class of Mochon's assignments—the f_0 assignment. An f_0 assignment can either be defined on an even number of points or an odd number of points. We start with the former, which is balanced and therefore easier to solve.

Proposition 20 (The balanced f_0 Solution)**.** *Let $t = h - g = \sum_{i=1}^{2n} p_i [\![x_i]\!]$ be Mochon's f_0 assignment for the set of real numbers $0 \leq x_1 < x_2 \cdots < x_{2n}$. Let $h = \sum_{i=1}^{n} p_{h_i} [\![x_{h_i}]\!]$, $g = \sum_{i=1}^{n} p_{g_i} [\![x_{g_i}]\!]$ where p_{h_i} and p_{g_i} are strictly positive, and $\{x_{h_i}\}$ and $\{x_{g_i}\}$ are all distinct. Consider the matrix instance $\underline{X} \coloneqq (X_h, X_g, |v\rangle, |w\rangle)$ where $X_h \doteq diag(x_{h_1}, x_{h_2} \ldots x_{h_n})$, $X_g \doteq diag(x_{g_1}, x_{g_2} \ldots x_{g_n})$, $|w\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_n}})$, $|v\rangle \doteq (\sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_n}})$. The orthogonal matrix*

$$O = \sum_{k=1}^{n} \left|u_h^{\bar{k}}\right\rangle \left\langle u_g^{\bar{k}}\right|$$

solves $\underline{X} =: \underline{X}^{\bar{n}}$ (see Definition 10) where the Weingarten Iteration Map (see Definition 12) is used to evaluate $\underline{X}^{\overline{k-1}} = \mathscr{W}(\underline{X}^{\bar{k}})$ which in turn is used to obtain $\left|u_h^{\bar{k}}\right\rangle$ and $\left|u_g^{\bar{k}}\right\rangle$ using the Normal Initialisation Map (see Definition 11) for all k, starting from $k = n$.

To prove Proposition 20, we use the following lemma which follows from Lemma 48 and Lemma 51 (proved in Section B).

Lemma 21 (Up Contact/Component Lemma)**.** *Consider the matrix instance $\underline{X}^{\bar{n}} := (H^{\bar{n}}, G^{\bar{n}}, \left|w^{\bar{n}}\right\rangle, \left|v^{\bar{n}}\right\rangle)$. Suppose the Weingarten Iteration Map (see Definition 12) is applied l times to obtain $\underline{X}^{\overline{n-l}} := \left(H^{\overline{n-l}}, G^{\overline{n-l}}, \left|w^{\overline{n-l}}\right\rangle, \left|v^{\overline{n-l}}\right\rangle\right)$. Then,*

$$\left\langle v^{\overline{n-l}}\right| \left(G^{\overline{n-l}}\right)^m \left|v^{\overline{n-l}}\right\rangle = r\left(\left\langle (G^{\bar{n}})^{m-1}\right\rangle, \left\langle (G^{\bar{n}})^{m}\right\rangle \ldots, \left\langle (G^{\bar{n}})^{2l+m}\right\rangle\right)$$

where $m \geq 1$ and r is a multi-variate function which does not have any implicit dependence on $\left\langle (G^{\bar{n}})^i\right\rangle := \left\langle v^{\bar{n}}\right| (G^{\bar{n}})^i \left|v^{\bar{n}}\right\rangle$. The corresponding statement involving H's and $|w\rangle$'s also holds.

Proof of Proposition 20. We have already done most of the work. Now only a counting argument remains. At the base level, we have the matrix instance $\underline{X} =: \underline{X}^{\bar{n}} =: (G^{\bar{n}}, H^{\bar{n}}, \left|v^{\bar{n}}\right\rangle, \left|w^{\bar{n}}\right\rangle)$. To use the Weingarten iteration once, we must show $\underline{X}^{\bar{n}}$ satisfies the contact condition (see Definition 10 and Lemma 13), viz.

$$\left\langle w^{\bar{n}}\right| H^{\bar{n}} \left|w^{\bar{n}}\right\rangle - \left\langle v^{\bar{n}}\right| G^{\bar{n}} \left|v^{\bar{n}}\right\rangle = \left\langle H^{\bar{n}}\right\rangle - \left\langle G^{\bar{n}}\right\rangle = \sum_{i=1}^{n} p_{h_i} x_{g_i} - \sum_{i=1}^{n} p_{g_i} x_{g_i} = \sum_{i=1}^{n} p_i x_i = \langle x \rangle$$

vanishes which it does due to Lemma 19. After iterating for l steps, suppose the matrix instance one obtains is $\underline{X}^{\overline{n-l}}$. To check if another Weingarten iteration is possible, we must check if the contact condition holds, i.e. if

$$\left\langle w^{\overline{n-l}}\right| H^{\overline{n-l}} \left|w^{\overline{n-l}}\right\rangle - \left\langle v^{\overline{n-l}}\right| G^{\overline{n-l}} \left|v^{\overline{n-l}}\right\rangle = r\left(\left\langle (H^{\bar{n}})^1\right\rangle, \left\langle (H^{\bar{n}})^2\right\rangle \ldots, \left\langle (H^{\bar{n}})^{2l+1}\right\rangle\right) - r\left(\left\langle (G^{\bar{n}})^1\right\rangle, \left\langle (G^{\bar{n}})^2\right\rangle \ldots, \left\langle (G^{\bar{n}})^{2l+1}\right\rangle\right)$$

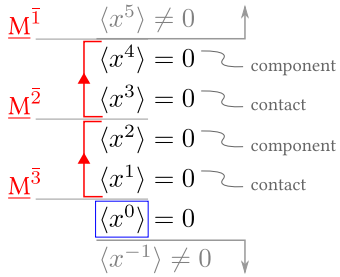

Figure 3: Power diagram for a balanced f_0 assignment with $2n = 6$ points. Starting upwards from $\langle x^0\rangle$, two iterations are completed before encountering the instance where the contact condition does not hold and the normals do not match.

vanishes. We used Lemma 21 (with $m = 1$) to obtain the RHS. Note that

$$\left\langle (H^{\bar{n}})^k \right\rangle - \left\langle (G^{\bar{n}})^k \right\rangle = \left\langle x^k \right\rangle . \tag{6}$$

If $2l + 1 \leq 2n - 2$ then from Lemma 19 it follows that both terms become identical and hence the difference indeed vanishes.[9] A similar argument can be used to obtain the condition $2l+2 \leq 2n-2$ which corresponds to the component condition (see Definition 10). Assuming $O^{\bar{n}}$ solves $\underline{X}^{\bar{n}}$, until $l = n - 2$ (included), one can iterate (using the Weingarten Iteration Map, $\mathscr{W}$, and the Normal Initialisation Map, $\mathscr{U}$) to obtain $\left|u_h^{\bar{n}}\right\rangle, \left|u_h^{\overline{n-1}}\right\rangle, \ldots, \left|u_h^{\overline{n-l}}\right\rangle, \ldots, \left|u_h^{\bar{1}}\right\rangle$ and similarly $\left|u_g^{\bar{n}}\right\rangle, \left|u_g^{\overline{n-1}}\right\rangle, \ldots, \left|u_g^{\overline{n-l}}\right\rangle, \ldots, \left|u_g^{\bar{1}}\right\rangle$ which completely determine $O^{\bar{n}}$. □

While we have proved the proposition, it is helpful to represent the main argument succinctly through a diagram (see Figure 3), for later proofs. We start right above $\langle x^0\rangle$ with the matrix instance $\underline{X}^{\bar{n}}$. Set $n = 3$ for concreteness. The contact condition at this step corresponds to $\langle x^1\rangle = 0$ which is true as the power is less than or equal to $2n - 2$ (here, $2n - 2 = 4$). We used Lemma 19. We can thus apply the Weingarten iteration and this is indicated by the arrow from $\langle x^1\rangle$ to $\langle x^2\rangle$. This yields $\underline{X}^{\overline{n-1}}$ and we can proceed with checking if $\langle x^3\rangle = 0$, which it is as the power is ≤ 4, and therefore we can again iterate to obtain $\underline{X}^{\overline{n-2}}$ which in this illustration is $\underline{X}^{\bar{1}}$. At this point, we have solved the problem as we can evaluate $\left|u_h^{\bar{3}}\right\rangle, \left|u_h^{\bar{2}}\right\rangle, \left|u_h^{\bar{1}}\right\rangle$ and $\left|u_g^{\bar{3}}\right\rangle, \left|u_g^{\bar{2}}\right\rangle, \left|u_g^{\bar{1}}\right\rangle$ form $\underline{X}^{\bar{3}}, \underline{X}^{\bar{2}}, \underline{X}^{\bar{1}}$ respectively to write $O = \sum_{k=1}^{3} \left|u_h^{\bar{k}}\right\rangle \left\langle u_g^{\bar{k}}\right|$. Note that having an even number of total points, $x_1 < x_2 \cdots < x_{2n}$, ensures there is proper pairing in the diagram, e.g. the contact condition for $\underline{X}^{\bar{2}}$ corresponds to $\langle x^3\rangle = 0$, however, in addition we also have $\langle x^4\rangle = 0$. When the number of points is odd, this ceases to be the case at the last step and we use wiggle-w to complete the solution. This is explained next. It must noted that even though the solution works in the limit of $\epsilon \to 0$, this is not unphysical. This corresponds to allowing projections in the description of the protocol (see §5 of [ARW18]).

Proposition 22 (The unbalanced f_0 Solution)**.** *Let $t = h - g = \sum_{i=1}^{2n-1} p_i [\![x_i]\!]$ be Mochon's f_0 assignment for the set of real numbers $0 \leq x_1 < x_2 \cdots < x_{2n-1} < x_{2n}$. Let $h = \sum_{i=1}^{n-1} p_{h_i} [\![x_{h_i}]\!]$, $g = \sum_{i=1}^{n} p_{g_i} [\![x_{g_i}]\!]$ where p_{h_i} and p_{g_i} are strictly positive, and $\{x_{h_i}\}$ and $\{x_{g_i}\}$ are all distinct. Consider the matrix instance $\underline{X}$:=$(X_h, X_g, |v\rangle, |w\rangle)$ where $X_h \doteq diag(x_{h_1}, x_{h_2} \ldots x_{h_{n-1}}, 1/\epsilon)$, $X_g \doteq diag(x_{g_1}, x_{g_2} \ldots x_{g_{n-1}}, x_{g_n})$, $|w\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_{n-1}}}, 0)$, $|v\rangle \doteq \left(\sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_n}}, \sqrt{p_{g_n}}\right)$. In the limit of $\epsilon \to 0$, the orthogonal matrix*

$$O = \sum_{k=1}^{n} \left|u_h^{\bar{k}}\right\rangle \left\langle u_g^{\bar{k}}\right|$$

solves $\underline{X} =: \underline{X}^{\bar{n}}$ (see Definition 10) where the Weingarten Iteration Map (see Definition 12) is used to evaluate $\underline{X}^{\overline{k-1}} = \mathscr{W}(\underline{X}^{\bar{k}})$ until $k = 2$, starting from $k = n$. The Normal Initialisation Map (see Definition 11) is used until $k = 3$ to obtain $\left|u_h^{\bar{k}}\right\rangle$ and $\left|u_g^{\bar{k}}\right\rangle$, viz. $\mathscr{U}(\underline{X}^{\bar{k}}) =: \left(*, \cdots *, \left|u_h^{\bar{k}}\right\rangle, \left|u_g^{\bar{k}}\right\rangle\right)$. The Wiggle-w Normal Initialisation Map (see Definition 11) is used to evaluate $\left|u_h^{\bar{2}}\right\rangle$ and $\left|u_g^{\bar{2}}\right\rangle$, viz. $\mathscr{U}_w(\underline{X}^{\bar{2}}) =: \left(*, *, \left|w^{\bar{2}}\right\rangle, \left|v^{\bar{2}}\right\rangle\right) \oplus \left(*, *, \left|u_h^{\bar{2}}\right\rangle, \left|u_g^{\bar{2}}\right\rangle\right)$. Finally, $\left|u_h^{\bar{1}}\right\rangle := \left|e\left(\left|u_h^{\bar{2}}\right\rangle, \left|w^{\bar{2}}\right\rangle\right)\right\rangle$ and $\left|u_g^{\bar{1}}\right\rangle := \left|e\left(\left|u_g^{\bar{2}}\right\rangle, \left|v^{\bar{2}}\right\rangle\right)\right\rangle$.

Proof. The argument is essentially the same as that for the balanced case until the very last step. After iterating for l steps, suppose the matrix instance one obtains is $\underline{X}^{\overline{n-l}}$. To check if another Weingarten iteration is possible, we must check if

$$\left\langle w^{\overline{n-l}}\right| \left(H^{\overline{n-l}}\right)^m \left|w^{\overline{n-l}}\right\rangle - \left\langle v^{\overline{n-l}}\right| \left(G^{\overline{n-l}}\right)^m \left|v^{\overline{n-l}}\right\rangle = r\left(\left\langle (H^{\bar{n}})^m\right\rangle, \left\langle (H^{\bar{n}})^{m+1}\right\rangle \ldots, \left\langle (H^{\bar{n}})^{2l+m}\right\rangle\right) - r\left(\left\langle (G^{\bar{n}})^m\right\rangle, \left\langle (G^{\bar{n}})^{m+1}\right\rangle \ldots, \left\langle (G^{\bar{n}})^{2l+m}\right\rangle\right)$$

vanishes for both $m = 1$ and $m = 2$, viz.

$$\left\langle x^{2l+1}\right\rangle = 0, \left\langle x^{2l+2}\right\rangle = 0 \tag{7}$$

and their lower power analogues (see Equation (6)). The $m = 1$ case is the contact condition and $m = 2$ is the component condition (see Definition 10). If $2l + 2 \leq 2n - 3$ then from Lemma 19 (with $n \to 2n - 1$) it follows that both terms become identical and hence

[9] The number of points here is $2n$; in the Lemma they are denoted by n.

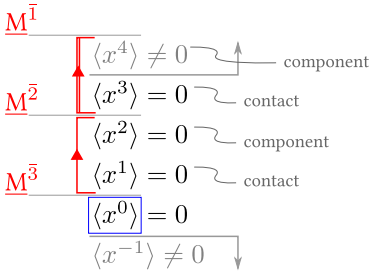

Figure 4: Power Diagram representative of an unbalanced f_0 assignment with 5 points (again $n = 3$). Starting upwards from $\langle x^0 \rangle$, one iteration is completed before encountering the instance where the contact condition still holds but the normals do not match, thus the wiggle-w method is employed.

the difference indeed vanishes. Consequently, until $l = n - 3$ (included), one can iterate to obtain $\underline{X}^{\bar{n}}, \underline{X}^{\overline{n-1}}, \ldots \underline{X}^{\bar{3}}, \underline{X}^{\bar{2}}$ which in turn can be used to determine $\left|u_h^{\bar{n}}\right\rangle, \left|u_h^{\overline{n-1}}\right\rangle, \ldots, \left|u_h^{\bar{3}}\right\rangle$ and similarly $\left|u_g^{\bar{n}}\right\rangle, \left|u_g^{\overline{n-1}}\right\rangle, \ldots, \left|u_g^{\bar{3}}\right\rangle$ (see Definition 11). Since $\left\langle x^{2n-3=2(n-2)+1}\right\rangle = 0$ but $\left\langle x^{2n-2=2(n-2)+2}\right\rangle \neq 0$ (essentially Equation (7) with $l = n - 2$), we can Definition 14 on $\underline{X}^{\overline{2=n-(n-2)}}$ to determine $\left|u_h^{\bar{2}}\right\rangle$ and $\left|u_g^{\bar{2}}\right\rangle$. The vectors $\left|w^{\bar{1}}\right\rangle$ and $\left|v^{\bar{1}}\right\rangle$ are fixed by the requirement that O is orthogonal (and that $O|v\rangle = |w\rangle$). As before, if we start with assuming that O solves the matrix instance $\underline{X}^{\bar{n}}$, then using Lemma 13 (and towards the end Lemma 16), we completely determine $O = \sum_{k=1}^{n} \left|u_h^{\bar{k}}\right\rangle \left\langle u_g^{\bar{k}}\right|$, proving the assumption to be correct. □

The argument can again be concisely represented using a diagram (see Figure 4). For concreteness, set $n = 3$ in which case, we must use a wiggle-v step at $\underline{X}^{\bar{2}}$ which is represented by a double-lined arrow from $\langle x^3 \rangle$ to $\langle x^4 \rangle$. As we shall see, this argument can be extended to work with monomial assignments as well. The difference is that we start not at the bottom of the diagram, but higher up, depending on the order of the monomial.

8 Equivalence to Monomial Assignments

In this section we show that Mochon's f-assignments can be expressed as sums of monomial assignments (or effectively monomial assignments). This reduction depends on the placement of the roots of f. If the roots of f are to the right of the coordinates (made precise below) then the result follows directly.

Lemma 23 (f with right-roots to f_0)**.** *Consider a set of real coordinates satisfying* $0 < x_1 < x_2 \cdots < x_n$ *and let* $f(x) = (r_1 - x)(r_2 - x) \ldots (r_k - x)$ *where* $k \leq n - 2$ *and the roots* $\{r_i\}_{i=1}^{n}$ *of* f *are right-roots, i.e. they are such that for every root* r_i *there exists a distinct coordinate* $x_j < r_i$*. Let* $t = \sum_{i=1}^{n} p_i [\![x_i]\!]$ *be the corresponding Mochon's* f *assignment. Then there exist* f_0 *assignments,* $\{t_j^0\}$*, on a subset of* $(x_1, x_2 \ldots x_n)$ *such that* t *is a sum of* f_0 *assignments, viz.* $t = \sum_{i=1}^{m} \alpha_i t_i^0$ *where* $\alpha_i > 0$ *is a real number and* $m > 0$ *is an integer.*

Proof. For simplicity, assume that $x_i < r_i$ but the argument works in the aforementioned general case. One can then write

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

where the first term has the same form that we started with (except for a positive constant which is irrelevant to the validity condition; see Equation (1)) but with the polynomial having one less degree. The second term also has the same form, except that the number of points involved has been reduced. Note how this process relies crucially on the fact that $r_1 - x_1$ is positive (else the term on the left would, by itself, not correspond to a valid move). This process can be repeated until we obtain a sum of f_0 assignments on various subsets of $(x_1, x_2 \ldots x_n)$. □

We can immediately apply this result to the f-assignment Mochon uses in the bias 1/10 game.

Example 24 (The main 1/10 move.)**.** The key move in Mochon's 1/10 bias game has its coordinates given by x_0, x_1, x_2, x_3, x_4 and roots given by l_1, r_1, r_2 which satisfy $x_0 < l_1 < x_1 < x_2 < x_3 < x_4 < r_1 < r_2$. Each root is a right root here because $x_0 < l_1$, $x_3 < r_1$, $x_4 < r_2$ for instance. Hence, this assignment can be expressed as a combination of f_0 assignments defined over subsets of the initial set of coordinates and each f_0 assignment admits a simple solution (see Proposition 35 and Proposition 37).

This scheme fails for moves corresponding to lower bias Mochon's games. For instance, the bias $1/14$ move has its coordinates given by $x_0, x_1, x_2, x_3, x_4, x_5, x_6$ and the roots of f by l_1, l_2, r_1, r_2, r_3 which satisfy $x_0 < l_1 < l_2 < x_1 < x_2 \cdots < x_6 < r_1 < r_2 < r_3$. Here we can either consider l_1 to be a right-root, in which case l_2 is a left-root—a root which is not a right-root. Or we can consider l_2 to be a right-root, in which case l_1 becomes a right-root.

Another example is to consider f-assignments which are merges. We place the roots of f in such a way that all points, except one, have negative weights.

Example 25 (Merge)**.** For merges (see Figure 5), we only get right-roots and hence, we can write them (the merges) as sums of f_0 solutions. The polynomial has degree $n-3$ (if the move involves n points) and so $\langle x \rangle = 0$, just as expected, for a merge.

Split is another counter-example but it paves the way for generalisation of the lemma.

Remark 26. For splits (see Figure 6) the situation is similar but with one key distinction: the polynomial has degree $n-2$; it has $n-3$ right-roots but 1 left-root (a root which is not a right-root). We use l_i henceforth to denote left-roots.

- This means that $\langle x \rangle > 0$ as expected, for a split. Further, this means that $\langle 1/(x - r_1) \rangle = 0$.
- Removing the "right roots", one can reduce the problem to one involving just one root, at l_1.
- A split is not representable as a sum of f_0 solutions—it starts with positive weight and all valid f_0 assignments must start with negative weights
- If one uses the operator monotone $-1/x$ on the split, one obtains essentially the merge configuration (with the containment condition reversed due to the minus sign).

We construct a systematic procedure for harnessing this duality. Recall that an EBRM function is equivalent to a valid function (up to closures). Consider EBRM functions with the spectra of their matrices in $[\chi, \xi]$. Similarly, consider valid functions with support in $[\chi, \xi]$. A similar statement relating the two can be given.

Lemma 27. *[see Lemma 85 in [ARW18]] A function $t = \sum_i p_i [\![x_i]\!]$ is EBRM on $[\chi, \xi]$ if and only if it is $[\chi, \xi]$ valid (corresponds to requiring $\sum p_i f_\lambda(x_i) \geq 0$ for all $\lambda \in (-\infty, \infty) \backslash [-\xi, -\chi]$ with $f_\lambda(x) = -1/(\lambda + x)$).*

This is of interest to us because it lets us replace $[\![x_i]\!]$ with $[\![1/x_i]\!]$ at the cost of a minus sign. Mochon's f-assignments have a structure which transforms in a useful way under $x_i \to 1/x_i$. We can combine these to show that monomial and effectively monomial assignments are equally easy to solve; if O solves one, O^T solves the other. Further, we can use the transformation to convert left-roots into right-roots. Later, we combine these to show that any f-assignment can be expressed as a sum of monomial assignments and/or effectively monomial assignment. We now state and prove these statements.

Lemma 28. *Let $\chi, \xi > 0$. A function $t = \sum_i p_i [\![x_i]\!]$ is $[\chi, \xi]$ EBRM if and only if $t' = \sum_i -p_i [\![1/x_i]\!]$ is $[1/\xi, 1/\chi]$ EBRM. Further, if O solves the matrix instance corresponding to t with spectrum in $[\chi, \xi]$ then O^T solves that of t' with spectrum in $[1/\xi, 1/\chi]$.*

Proof. We start with the only if part ($\implies$). We are given H, G with spectrum in $[\chi, \xi]$ and a vector $|w\rangle$ such that $t = \text{Prob}[H, |w\rangle] - \text{Prob}[G, |w\rangle]$ and $H \geq G$. Further, $H \geq G \iff H^{-1} \leq G^{-1}$. By using spectral decomposition, one should be able to see that $t' = \text{Prob}[G^{-1}, |w\rangle] - \text{Prob}[H^{-1}, |w\rangle]$. Defining $H' = G^{-1}$, $G' = H^{-1}$, $|w'\rangle = |w\rangle$, we have $t' = \text{Prob}[H', |w'\rangle] - \text{Prob}[G', |w'\rangle]$ and $H' \geq G'$ where G' and H' have their spectrum in $[1/\xi, 1/\chi]$. The same argument should also work for the other direction. The last statement is seen to be true by using a basis in which $H = X_h$ is diagonal, writing $G = OX_gO^T$ and noting $O^{-1} = O^T$. □

Corollary 29 (Effectively monomial assignment)**.** *Let $0 < x_1 < x_2 \cdots < x_n$. Then, O^T solves a matrix instance corresponding to*

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

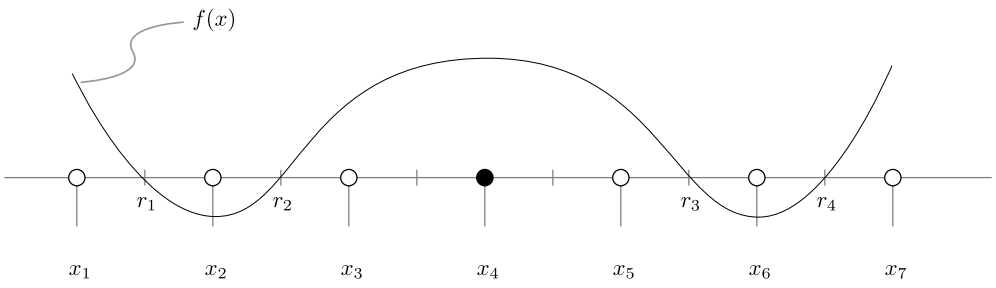

Figure 5: Merge involving $n = 7$ points. f has in total $n-3$ right roots.

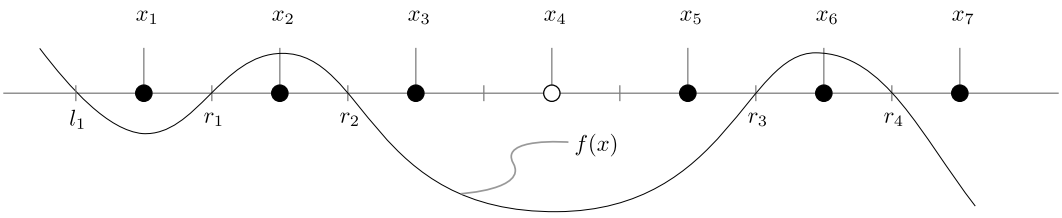

Figure 6: Split involving 7 points. f has in total $n-2$ roots (4 right and 1 left).

if and only if O solves the corresponding matrix instance associated with the monomial assignment

$$t' = \sum_{i=1}^{n} \frac{-\left(-\frac{1}{x_i}\right)^k}{\prod_{i\neq j}(\frac{1}{x_j}-\frac{1}{x_i})} \left[\!\left[\frac{1}{x_i}\right]\!\right] = \sum_{i=1}^{n} \frac{-(-\omega_i)^k}{\prod_{i\neq j}(\omega_j-\omega_i)} [\![\omega_i]\!]$$

where $\omega_i := 1/x_i$. We therefore refer to t as effectively a monomial assignment.

Lemma 30 (Left-roots to Right-roots)**.** *Consider a set of real coordinates satisfying $0 < x_1 < x_2 \cdots < x_n$ and let $f(x) = (l_1 - x)(l_2 - x)\ldots(l_k - x)$ where $k \leq n-2$ and the roots $\{l_i\}_{i=1}^n$ of f are positive and on the left of the coordinates, i.e. each $l_i < x_1$ and $l_i > 0$. Let*

$$t = \sum_{i=1}^{n} p_i [\![x_i]\!] = \sum_{i=1}^{n} \frac{-(l_1-x_i)(l_2-x_i)\ldots(l_k-x_i)}{\prod_{i\neq j}(x_j-x_i)} [\![x_i]\!]$$

be the corresponding Mochon's f assignment. Let

$$t' = \sum_{i=1}^{n} \frac{-(r_1-\omega_i)(r_2-\omega_i)\ldots(r_k-\omega_i)(-\omega_i)^{n-2-k}}{\prod_{i\neq j}(\omega_j-\omega_i)} [\![\omega_i]\!]$$

where $r_i = 1/l_i$, and $\omega_i = 1/x_i$. Note that the roots r_i are right-roots, i.e. each $r_i > \omega_1$ and $\omega_n < \omega_{n-1} \cdots < \omega_1$. If O solves the matrix instance associated with t then O^T solves the corresponding matrix instance of t'.

Proof. This lemma lets us convert the left-roots into right-roots at the expense of a "monomial term". Let us denote the weights for an m_0 assignment on $\{x_i\}$ (see Definition 18) by

$$p_{0;i} = \frac{-c'}{\prod_{j\neq i}(x_j - x_i)}$$

where $c' > 0$ is an arbitrary positive real number. Similarly, let the weights for the m_{n-2} assignment on $\{x_i\}$ be given by

$$p_{n-2;i} = \frac{-(-x_i)^{n-2}c'}{\prod_{j\neq i}(x_j - x_i)} = (-x_i)^{n-2}p_{0;i}.$$

An m_0 assignment on $\{1/x_i\}$ is given by

$$\begin{aligned} q_{0;i} &= \frac{-c}{\prod_{j\neq i}\left(\frac{1}{x_j}-\frac{1}{x_i}\right)} \\ &= \frac{-x_i^{n-2}c\prod_j x_j}{(-1)^{n-1}\prod_{j\neq i}(x_j-x_i)} \xrightarrow{c'} = -(-x_i)^{n-2}p_{0;i} = -p_{n-2;i}. \end{aligned}$$

This means that the m_0 assignment on $\{1/x_i\}$ is exactly the same as the m_{n-2} assignment on $\{x_i\}$, with a minus sign. It is easy to generalise this connection to obtain

$$\begin{aligned} q_{0;i} &= -p_{n-2;i} \\ q_{1;i} &= -p_{n-3;i} \\ q_{2;i} &= -p_{n-4;i} \\ &\vdots \\ q_{n-3;i} &= -p_{1;i} \\ q_{n-2;i} &= -p_{0;i}. \end{aligned}$$

Note that the weight on $[\![x_i]\!]$ in t

$$\begin{aligned}
&= (l_1 - x_i)(l_2 - x_i)\dots(l_k - x_i)\,(p_{0;i}) \\
&= (-l_1x_i)\left(\frac{1}{l_1} - \frac{1}{x_i}\right)(-l_2x_i)\left(\frac{1}{l_2} - \frac{1}{x_i}\right)\dots(-l_kx_i)\left(\frac{1}{l_k} - \frac{1}{x_i}\right)p_{0;i} \\
&= (l_1l_2\dots l_k)\,(-x_i)^k(r_1 - \omega_i)(r_2 - \omega_i)\dots(r_k - \omega_i)p_{0;i} \\
&= (r_1 - \omega_i)(r_2 - \omega_i)\dots(r_k - \omega_i)p_{k;i} \\
&= -(r_1 - \omega_i)(r_2 - \omega_i)\dots(r_k - \omega_i)q_{n-2-k;i}
\end{aligned}$$

where in the second step, we used

$$\left(\frac{1}{l_1} - \frac{1}{x_i}\right) = \frac{x_i - l_1}{l_1x_i} = -\frac{l_1 - x_i}{l_1x_i}$$

and the definitions $1/l_i = r_i$, $1/x_i = \omega_i$. Using Lemma 28 with $\chi \to 0$ and $\xi \to \infty$, we obtain t'. □

Proposition 31. *Consider a set of real coordinates satisfying $0 < x_1 < x_2 \cdots < x_n$ and let $f(x) = (a_1 - x)(a_2 - x)\dots(a_k - x)$ where $k \le n-2$ and the roots $\{a_i\}_{i=1}^k$ of f are positive, i.e. $a_i > 0$. Let $t = \sum_{i=1}^n p_i\,[\![x_i]\!]$ be the corresponding Mochon's f-assignment. Then*

$$t = \sum_i \alpha_i t'_i$$

(construction is given in the proof) where $\alpha_i > 0$ and either

- *t'_i is an f_0 assignment on a subset $S \subset \{x_1, x_2 \dots x_n\}$, i.e. it is of the form*

$$t'_i = \sum_{i\in S} \frac{-1}{\prod_{i\in s/\{j\}}(x_j - x_i)}\,[\![x_i]\!]\,,$$

- *or t'_i is* effectively a monomial assignment *(see Corollary 29), i.e. it is of the form*

$$t'_i = \sum_{i\in S} \frac{\left(-\frac{1}{x_i}\right)^k}{\prod_{i\in s/\{j\}}\left(\frac{1}{x_j} - \frac{1}{x_i}\right)}\,[\![x_i]\!]$$

where $S \subset \{x_1, x_2 \dots x_n\}$ and $k \le |S| - 2$.

Proof. One can start by using Lemma 23 to remove all the right-roots and obtain $t = \sum_i \alpha_i t''_i$ where $\alpha_i > 0$. For each i, t''_i will be a Mochon's f-assignment on some subset of $\{x_1, x_2 \dots x_n\}$. The f-assignments which are also f_0 assignments already have the desired form. The remaining ones, will necessarily correspond to f-assignments with f having all their roots to the left of x_1. One can now use Lemma 30 to shift all these roots to the right of all the new coordinates which are a subset of $\{1/x_1, 1/x_2 \dots 1/x_n\}$. Again, Lemma 23 can be used to remove all the right-roots to obtain m-assignments on subsets of $\{1/x_1, 1/x_2 \dots 1/x_n\}$. Using Corollary 29 we obtain the claimed form. □

In our results so far, we required the coordinates to be strictly positive. However, this is not really a restriction because any Mochon's 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.

Lemma 32. *Consider a set of real coordinates satisfying $0 \le x_1 < x_2 \cdots < x_n$ and let $f(x) = (a_1 - x)(a_2 - x)\dots(a_k - x)$ where $k \le n-2$ 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 Mochon's f-assignment. Consider a set of real coordinates satisfying $0 < x_1 + c < x_2 + c \cdots < x_n + c$ where $c > 0$ and let $f'(x) = (a_1 + c - x)(a_2 + c - x)\dots(a_k + c - x)$. Let $t' = \sum_{i=1}^n p'_i\,[\![x'_i]\!]$ be the corresponding Mochon's f-assignment with $x'_i := x_i + c$. The solution to the matrix instance corresponding to these two functions is the same.*

Proof. This is a direct consequence of the fact that $p'_i = p_i$ (as the cs cancel) and that $X_h \ge OX_gO^T$ if and only if $X_h + c\mathbb{I} \ge O(X_g + c\mathbb{I})O^T$. □

Now it only remains to solve monomial assignments which is described in the next section.

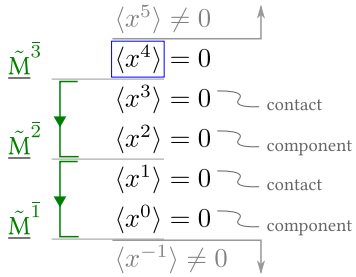

Figure 7: Power diagram representative of the simplest monomial assignment for $2n = 6$ points.

9 m Solutions | Solution to Mochon's Monomial Assignments

Recall that the f_0-assignment corresponded to starting at the bottom, i.e. at $\langle x^0\rangle$, in the diagram (see Section 7). We now consider the simplest monomial problem which corresponds to starting at the top, i.e. $\langle x^{2n-2}\rangle$, in the diagram (explained below). Intuitively, while earlier every iteration was leading to an increase in the power of x (in terms of the form $\langle x^k\rangle$), here every iteration leads to a decrease in the power. This is because we start with inverting the matrices. Later, we use a combination of these strategies to construct the solution.

Example 33 (Solving the Simplest Monomial Problem.)**.** Suppose the assignment we wish to solve is

$$t = \sum_{i=1}^{2n} -\frac{(-x_i)^{2n-2}}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!] = \sum_{i=1}^{2n} \tilde{p}_i [\![x_i]\!]$$

where $0 < x_1 < x_2 \cdots < x_n$. This can be solved using the f_0 solution (see Proposition 20) by writing $t = \sum_{i=1}^{2n} \frac{1}{\prod_{j\neq i}(\omega_j - \omega_i)} [\![x_i]\!]$ where $\omega_i = 1/x_i$, which is in turn equivalent to solving $t' = \sum_{i=1}^{2n} -\frac{1}{\prod_{j\neq i}(\omega_j - \omega_i)} [\![\omega_i]\!]$ (see Corollary 29 with $k = 0$). Instead, we solve this problem using another method—we use $X^{\dashv}$s instead of Xs as in the usual f_0 solution and the fact that $\sum_i \tilde{p}_i x_i^{-k} = 0$ for $k \leq 2n-2$ (see Lemma 19). Let the matrix instance corresponding to t, which we write as

$$t = \sum_{i=1}^{n} \tilde{p}_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} \tilde{p}_{g_i} [\![x_{g_i}]\!] = \sum_{i=1}^{n} x_{h_i}^{2n-2} p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} x_{g_i}^{2n-2} p_{g_i} [\![x_{g_i}]\!],$$

be given by $\underline{X}^{\bar{n}} := \left(X_h^{\bar{n}}, X_g^{\bar{n}}, (X_h^{\bar{n}})^{n-1}\left|w^{\bar{n}}\right\rangle, (X_g^{\bar{n}})^{n-1}\left|v^{\bar{n}}\right\rangle\right)$ where

$$X_h^{\bar{n}} \doteq \mathrm{diag}(x_{h_1}, x_{h_2} \ldots x_{h_n}), \qquad X_g^{\bar{n}} \doteq \mathrm{diag}(x_{g_1}, x_{g_2} \ldots x_{g_n}),$$
$$\left|w^{\bar{n}}\right\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_n}}), \qquad \left|v^{\bar{n}}\right\rangle \doteq (\sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_n}}).$$

Solving the matrix instance $\underline{X}^{\bar{n}}$ requires us to find an orthogonal matrix O such that $X_h^{\bar{n}} \geq O X_g^{\bar{n}} O^T$ and $O(X_g^{\bar{n}})^{n-1}\left|v^{\bar{n}}\right\rangle = (X_h^{\bar{n}})^{n-1}\left|w^{\bar{n}}\right\rangle$. The matrix inequality can be equivalently written as $\tilde{X}_h^{\bar{n}} \leq O \tilde{X}_g^{\bar{n}} O^T$ where $\tilde{X}_h^{\bar{n}} = (X_h^{\bar{n}})^{-1}$ and $\tilde{X}_g^{\bar{n}} = (X_g^{\bar{n}})^{-1}$. Note that under a change of the direction of the matrix inequality the arguments used in the proof of Weingarten Iteration (see Lemma 13) go through unchanged. We can therefore consider the matrix instance $\tilde{\underline{X}}^{\bar{n}} := \left(\tilde{X}_h^{\bar{n}}, \tilde{X}_g^{\bar{n}}, \left|\tilde{w}^{\bar{n}}\right\rangle, \left|\tilde{v}^{\bar{n}}\right\rangle\right)$ where $\left|\tilde{w}^{\bar{n}}\right\rangle := (X_h^{\bar{n}})^{n-1}\left|w^{\bar{n}}\right\rangle$ and $\left|\tilde{v}^{\bar{n}}\right\rangle := (X_g^{\bar{n}})^{n-1}\left|v^{\bar{n}}\right\rangle$. After iterating for l steps, suppose the matrix instance one obtains is $\tilde{\underline{X}}^{\overline{n-l}}$. To check if another isometric iteration is possible, we must check if the contact condition (see Definition 10) holds, i.e. if

$$\begin{aligned}\left\langle \tilde{w}^{\overline{n-l}}\right| \tilde{H}^{\overline{n-l}} \left|\tilde{w}^{\overline{n-l}}\right\rangle - \left\langle \tilde{v}^{\overline{n-l}}\right| \tilde{G}^{\overline{n-l}} \left|\tilde{v}^{\overline{n-l}}\right\rangle &= r\left(\left\langle \tilde{w}^{\bar{n}}\right|(\tilde{X}_h^{\bar{n}})^1\left|\tilde{w}^{\bar{n}}\right\rangle, \left\langle \tilde{w}^{\bar{n}}\right|(\tilde{X}_h^{\bar{n}})^2\left|\tilde{w}^{\bar{n}}\right\rangle \ldots, \left\langle \tilde{w}^{\bar{n}}\right|(\tilde{X}_h^{\bar{n}})^{2l+1}\left|\tilde{w}^{\bar{n}}\right\rangle\right) \\ &\quad - r\left(\left\langle \tilde{v}^{\bar{n}}\right|(\tilde{X}_g^{\bar{n}})^1\left|\tilde{v}^{\bar{n}}\right\rangle, \left\langle \tilde{v}^{\bar{n}}\right|(\tilde{X}_g^{\bar{n}})^2\left|\tilde{v}^{\bar{n}}\right\rangle \ldots, \left\langle \tilde{v}^{\bar{n}}\right|(\tilde{X}_g^{\bar{n}})^{2l+1}\left|\tilde{v}^{\bar{n}}\right\rangle\right) \\ &= r\left(\left\langle (X_h^{\bar{n}})^{2n-3}\right\rangle, \left\langle (X_h^{\bar{n}})^{2n-4}\right\rangle \ldots, \left\langle (X_h^{\bar{n}})^{2n-2l-1}\right\rangle\right) - r\left(\left\langle (X_g^{\bar{n}})^{2n-3}\right\rangle, \left\langle (X_g^{\bar{n}})^{2n-4}\right\rangle \ldots, \left\langle (X_g^{\bar{n}})^{2n-2l-1}\right\rangle\right)\end{aligned}$$

vanishes. We used Lemma 21 (with $m = 1$) to obtain the RHS and we continue using the convention that $\left\langle (X_h^{\bar{n}})^k\right\rangle = \left\langle w^{\bar{n}}\right|(X_h^{\bar{n}})^k\left|w^{\bar{n}}\right\rangle$ and similarly $\left\langle (X_h^{\bar{n}})^k\right\rangle = \left\langle v^{\bar{n}}\right|(X_g^{\bar{n}})^k\left|v^{\bar{n}}\right\rangle$. Recall that (see Equation (6))

$$\left\langle (H^{\bar{n}})^k\right\rangle - \left\langle (G^{\bar{n}})^k\right\rangle = \left\langle x^k\right\rangle. \tag{8}$$

If $0 \leq 2n - 2l - 1 \leq 2n - 2$ then from Lemma 19 it follows that both terms become identical and hence the difference indeed vanishes (one can similarly verify the component condition). Hence, until $l = n - 2$ (included), one can apply the Weingarten Iteration to obtain $\left|\tilde{u}_h^{\bar{n}}\right\rangle, \left|\tilde{u}_h^{\overline{n-1}}\right\rangle, \ldots, \left|\tilde{u}_h^{\overline{n-l}}\right\rangle, \ldots, \left|\tilde{u}_h^{\bar{1}}\right\rangle$ and similarly $\left|\tilde{u}_g^{\bar{n}}\right\rangle, \left|\tilde{u}_g^{\overline{n-1}}\right\rangle, \ldots, \left|\tilde{u}_g^{\overline{n-l}}\right\rangle, \ldots, \left|\tilde{u}_g^{\bar{1}}\right\rangle$ which completely determine $O = \sum_{i=1}^{n} \left|\tilde{u}_h^i\right\rangle\left\langle \tilde{u}_g^i\right|$. The argument can, as before, be concisely represented using a diagram (see Figure 7).

Before we start mixing the two approaches, we state a result which helps us keep track of the powers which appear in the contact and component conditions of matrix instances, after we have made a certain number of iterations in both directions. This can be proved by combining Lemma 49, Lemma 50 and Lemma 51 (see Section B).

Lemma 34 (Up-then-Down Contact/Component Lemma)**.** *Consider the extended matrix instance*

$$\underline{M'^{\bar{n}}} := \mathscr{U}(H'^{\bar{n}}, G'^{\bar{n}}, \left|w'^{\bar{n}}\right\rangle, \left|v'^{\bar{n}}\right\rangle, (H'^{\bar{n}})^{\dashv}, (G'^{\bar{n}})^{\dashv}, |.\rangle, |.\rangle).$$

Suppose the Normal Initialisation Map and the Weingarten Iteration Map (see Definition 11 and Definition 12) are applied k times to obtain $\underline{M'^{\overline{n-k}}}$, viz. applying $\underline{M'^{\overline{i-1}}} = \mathscr{U}(\mathscr{W}(\underline{M'^{\bar{i}}}))$ k times. Let $n-k=d$ and consider $\underline{\tilde{M}^{\bar{d}}} = \mathscr{U}(\mathscr{F}(\underline{M'^{\bar{d}}}))$. Suppose the Normal Initialisation Map and the Weingarten Iteration map are applied l more times to obtain $\underline{\tilde{M}^{\overline{d-l}}} =: \left(\tilde{H}^{\overline{n-l}}, \tilde{G}^{\overline{n-l}}, \left|\tilde{w}^{\overline{n-l}}\right\rangle, \left|\tilde{v}^{\overline{n-l}}\right\rangle, *, \cdots *\right)$. Then,

$$\left\langle \tilde{v}^{\overline{n-k-l}} \right| \left(\tilde{G}^{\overline{n-k-l}}\right)^{\mu} \left| \tilde{v}^{\overline{n-k-l}} \right\rangle = r\left(\left\langle (G'^{\bar{n}})^{-(2l+\mu)} \right\rangle, \ldots, \left\langle (G'^{\bar{n}})^{2k-1+\mu} \right\rangle, \left\langle (G'^{\bar{n}})^{2k+\mu} \right\rangle\right)$$

where $\mu \geq 1$ and r is a multi-variate function which does not depend on any $\left\langle (G'^{\bar{n}})^{i} \right\rangle := \left\langle v'^{\bar{n}} \right| (G'^{\bar{n}})^{i} \left| v'^{\bar{n}} \right\rangle$ other than through its arguments[10]. The corresponding statement involving Hs and $|w\rangle$s also holds.

A monomial problem can either be balanced or unbalanced. We find the solution in these two cases separately, starting with the former. Recall that if a solution requires $\epsilon \to 0$, it does not correspond to anything unphysical (see the discussion before Proposition 22).

Proposition 35 (Solving the Balanced Monomial Problem)**.** *Let*

$$t = \sum_{i=1}^{2n} -\frac{(-x_i)^m}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!] = \sum_{i=1}^{n} x_{h_i}^m p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n} x_{g_i}^m p_{g_i} [\![x_{g_i}]\!]$$

be a balanced monomial assignment for the set of real numbers $0 < x_1 < x_2 \cdots < x_{2n-1} < x_{2n}$ (see Definition 18; it enforces $0 \leq m \leq 2n-2$) where p_{h_i} and p_{g_i} are strictly positive and $\{x_{h_i}\}$ and $\{x_{g_i}\}$ are all distinct. Consider the corresponding matrix instance $\underline{X^{\bar{\eta}}} := (X_h^{\bar{\eta}}, X_g^{\bar{\eta}}, (X_h^{\bar{\eta}})^b |v\rangle, (X_g^{\bar{\eta}})^b |w\rangle)$ where

- *if $b = m/2$ is an integer (the* aligned case*) then $\eta = n$, $j' = j = 1$,*

$$X_h^{\bar{n}} \doteq diag(x_{h_1}, x_{h_2} \ldots x_{h_n}), \qquad X_g^{\bar{n}} \doteq diag(x_{g_1}, x_{g_2} \ldots x_{g_n}),$$
$$\left|w^{\bar{n}}\right\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_n}}), \qquad \left|v^{\bar{n}}\right\rangle \doteq (\sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_n}}).$$

- *else if $b = m/2$ is not an integer (the* misaligned case*) then $\eta = n+1$, $j' = 3$, $j = 4$,*

$$X_h^{\overline{n+1}} \doteq diag(x_{h_1}, x_{h_2} \ldots x_{h_n}, 1/\varepsilon), \qquad X_g^{\overline{n+1}} \doteq diag(x_{g_1}, x_{g_2} \ldots x_{g_n}, \varepsilon),$$
$$\left|w^{\overline{n+1}}\right\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_n}}, 0), \qquad \left|v^{\overline{n+1}}\right\rangle \doteq (\sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_n}}, 0).$$

Let $k = \left\lfloor \frac{2n-2-m}{2} \right\rfloor$. In the limit of $\epsilon \to 0$, the matrix instance is solved by

$$O = \sum_{i=\eta}^{\eta-k+1} \left|u_h'^{\bar{i}}\right\rangle \left\langle u_g'^{\bar{i}}\right| + \sum_{i=\eta-k}^{j} \left|\tilde{u}_h^{\bar{i}}\right\rangle \left\langle \tilde{u}_g^{\bar{i}}\right| + (1-\delta_{j,j'}) \sum_{i=j'}^{1} \left|u_h'^{\bar{i}}\right\rangle \left\langle u_g'^{\bar{i}}\right|$$

where the terms for the left sum are evaluated in the same way for both cases (i.e. regardless of the alignment). We start with $\underline{M'^{\bar{\eta}}} := \mathscr{U}\left(\underline{X^{\bar{\eta}}} \oplus \left((X_h^{\bar{\eta}})^{-1}, (X_g^{\bar{\eta}})^{-1}, |.\rangle, |.\rangle\right)\right)$ (see Definition 10, Definition 11, Definition 12) and define

$$\underline{M'^{\bar{l}}} =: \left(*, \cdots *, \left|u_h'^{\bar{l}}\right\rangle, \left|u_h'^{\bar{i}}\right\rangle\right) \qquad \eta - k + 1 \leq l \leq \eta$$

using the relation

$$\underline{M'^{\overline{l-1}}} := \mathscr{U}(\mathscr{W}(\underline{M'^{\bar{l}}})) \qquad \eta - k + 1 \leq l - 1 \leq \eta - 1.$$

The terms for the middle sum are also the same in both cases. We start with

$$\underline{\tilde{M}^{\overline{\eta-k}}} := \mathscr{U}(\mathscr{F}(\underline{M'^{\overline{\eta-k}}}))$$

[10](e.g. if $r(x) = e^x$ and we are interested in $r(\alpha)$ then r doesn't depend on α other than through its argument)

and using the relations

$$\underline{\tilde{M}}^{\overline{l-1}} := \mathscr{U}(\mathscr{W}(\underline{\tilde{M}}^{\bar{l}})) \qquad\qquad j' \le l-1 \le \eta - k - 1$$

define

$$\left(*, \cdots *, \left|\tilde{u}_h^{\bar{l}}\right\rangle, \left|\tilde{u}_g^{\bar{l}}\right\rangle\right) := \underline{\tilde{M}}^{\bar{l}} \qquad\qquad j \le l \le \eta - k.$$

At this point, the aligned problem is solved. To solve the misaligned problem we define (see Definition 17, Definition 14, Definition 15)

$$\underline{\tilde{M}}^{\bar{3}} := \mathscr{U}_v(\mathscr{W}(\underline{\tilde{M}}^{\bar{4}}))$$
$$\underline{M}'^{\bar{2}} := \mathscr{U}_w(\mathscr{F}(\mathscr{W}_v(\underline{\tilde{M}}^{\bar{3}}))) =: \left(*, *, \left|w'^{\bar{2}}\right\rangle, \left|v'^{\bar{2}}\right\rangle, *, *, \left|u_h'^{\bar{2}}\right\rangle, \left|u_g'^{\bar{2}}\right\rangle\right)$$

$\left|u_h'^{\bar{1}}\right\rangle := \left|e\left(\left|u_h'^{\bar{2}}\right\rangle, \left|w'^{\bar{2}}\right\rangle\right)\right\rangle$ *and* $\left|u_g'^{\bar{1}}\right\rangle := \left|e\left(\left|u_g'^{\bar{2}}\right\rangle, \left|v'^{\bar{2}}\right\rangle\right)\right\rangle$.

Proof. We first prove that O solves $\underline{X}^{\bar{n}}$ in the *aligned case* (i.e. when $b = m/2$ is an integer; see Figure 8, note that $\eta = n$ in this case). We denote the components of $\underline{M}'^{\bar{l}}$ by

$$\left(H'^{\bar{l}}, G'^{\bar{l}}, \left|w'^{\bar{l}}\right\rangle, \left|v'^{\bar{l}}\right\rangle, * \ldots, *\right) := \underline{M}'^{\bar{l}}.$$

To start with, we check if $\underline{M}'^{\bar{n}}$ satisfies the contact condition, which corresponds to

$$\left\langle w'^{\bar{n}}\right| H'^{\bar{n}} \left|w'^{\bar{n}}\right\rangle = \left\langle v'^{\bar{n}}\right| G'^{\bar{n}} \left|v'^{\bar{n}}\right\rangle.$$

The LHS is simply $\left\langle w^{\bar{n}}\right| (X_h^{\bar{n}})^{2b+1} \left|w^{\bar{n}}\right\rangle = \left\langle (X_h^{\bar{n}})^{m+1}\right\rangle$ and similarly the RHS is $\left\langle (X_g^{\bar{n}})^{m+1}\right\rangle$. The condition can then be expressed as $\left\langle x^{m+1}\right\rangle = 0$. The component condition similarly can be expressed as $\left\langle x^{m+2}\right\rangle = 0$. From Lemma 19, we know that these conditions hold for $m+2 \le 2n-2$, i.e. $m \le 2n-4$ (see Figure 8; with $2n = 10$, this means that m can be at most 8 for the conditions to hold). Assuming $m \le 2n-4$ we[11] can apply the Weingarten Iteration Map (Definition 12) and use Lemma 13 (along with the Normal Initialisation Map Definition 11) to construct a part of the solution, viz. use $\underline{M}'^{\overline{l-1}} := \mathscr{U}(\mathscr{W}(\underline{M}'^{\bar{l}}))$. Suppose we iterate κ times to obtain $\underline{M}'^{\overline{n-\kappa}}$ (note that κ and k are distinct). The contact condition now corresponds to

$$\left\langle w'^{\overline{n-\kappa}}\right| H'^{\overline{n-\kappa}} \left|w'^{\overline{n-\kappa}}\right\rangle = \left\langle v'^{\overline{n-\kappa}}\right| G'^{\overline{n-\kappa}} \left|v'^{\overline{n-\kappa}}\right\rangle.$$

The RHS can be written as

$$r\left(\left\langle w'^{\bar{n}}\right| (H'^{\bar{n}})^1 \left|w'^{\bar{n}}\right\rangle, \left\langle w'^{\bar{n}}\right| (H'^{\bar{n}})^2 \left|w'^{\bar{n}}\right\rangle \ldots \left\langle w'^{\bar{n}}\right| (H'^{\bar{n}})^{2\kappa+1} \left|w'^{\bar{n}}\right\rangle\right)$$

using Lemma 21 (similarly for the LHS). The contact condition can then be expressed as $\left\langle x^{2\kappa+1+m}\right\rangle = 0$ (the lower power terms also satisfy this condition if the highest power term does). Proceeding similarly, the component condition can be expressed as $\left\langle x^{2\kappa+2+m}\right\rangle = 0$. From Lemma 19, we know that these conditions hold if $2\kappa+2+m \le 2n-2$ which yields $\kappa \le n-b-2 = k-1$. Hence, we can deduce that if O solves the matrix instance then it must have the form $O = \sum_{l=1}^{n-k+1} \left|u_h'^{l}\right\rangle \left\langle u_g'^{l}\right| + Q^{\overline{n-k}}$ where $Q^{\overline{n-k}}$ is an isometry acting on the orthogonal space which remains to be determined. To proceed, we can apply the Weingarten Iteration Map to $\underline{M}'^{\overline{n-k+1}}$ and obtain $\mathscr{W}(\underline{M}'^{\overline{n-k+1}}) =: \underline{M}'^{\overline{n-k}}$ but this instance satisfies neither the contact condition nor the component condition (corresponds to $\underline{M}'^{\bar{3}}$ in Figure 8). This can be remedied by now proceeding as we did in Example 33.

For this paragraph, let $(H, G, |w\rangle, |v\rangle, H^{\dashv}, G^{\dashv}, *, *) := \underline{M}'^{\overline{n-k}}$. Solving $\underline{M}'^{\overline{n-k}}$ corresponds to finding a Q such that $Q|v\rangle = |w\rangle$ and $H \ge QGQ^T$. The matrix inequality can be equivalently be written as $H^{\dashv} \le QG^{\dashv}Q^T$. Intuitively, using H and G to evaluate the normals led to contact/component conditions which correspond to increasing powers in the condition $\left\langle x^l\right\rangle = 0$. Using $H^{\dashv}$ and $G^{\dashv}$ should decrease the powers and thereby allow us to proceed. We formalise this and use Lemma 34 to bolster the intuition.

We evaluate

$$\underline{\tilde{M}}^{\overline{n-k}} = \mathscr{U}(\mathscr{F}(\mathscr{W}(\underline{M}'^{\overline{n-k+1}}))$$

and let $\underline{\tilde{M}}^{\bar{l}} =: \left(\tilde{H}^{\bar{l}}, \tilde{G}^{\bar{l}}, \left|\tilde{w}^{\bar{l}}\right\rangle, \left|\tilde{v}^{\bar{l}}\right\rangle\right)$ (this step is indicated by the small triangles next to $\underline{M}'^{\bar{3}}$ and $\underline{\tilde{M}}^{\bar{3}}$ in Figure 8). We write the contact/component condition for $\underline{\tilde{M}}^{\overline{n-k-l}}$, the matrix instance one obtains after iterating l times using $\underline{\tilde{M}}^{\overline{l-1}} := \mathscr{U}(\mathscr{W}(\underline{\tilde{M}}^{\bar{l}}))$ starting with $\underline{\tilde{M}}^{\overline{n-k}}$. The contact condition

$$\left\langle \tilde{w}^{\overline{n-k-l}}\right| \tilde{H}^{\overline{n-k-l}} \left|\tilde{w}^{\overline{n-k-l}}\right\rangle = \left\langle \tilde{v}^{\overline{n-k-l}}\right| \tilde{G}^{\overline{n-k-l}} \left|\tilde{v}^{\overline{n-k-l}}\right\rangle$$

[11] The $m = 2n-3$ case can't arise here by the alignment assumption; the $m = 2n-2$ case becomes a special case which we have seen already—the simplest monomial assignment, Example 33.

effectively becomes $\langle x^{-(2l+1)+m}\rangle = 0$ using Lemma 34, noting that the lowest power is relevant here, and that $|w'^{\bar{n}}\rangle = (X_h^{\bar{n}})^{m/2}|w^{\bar{n}}\rangle$ (similarly for $|v'^{\bar{n}}\rangle$). We can similarly see that the component condition yields $\langle x^{-(2l+2)+m}\rangle = 0$. From Lemma 19, we know that these conditions hold if $0 \leq -(2l+2)+m$ which yields $l \leq b-1$. This means that the rank, i.e. $n-k-l$ until which the contact/component condition holds is $\cancel{n-n}+1+\cancel{b-b}+1 = 2$ (included) where we used $k = n-b-1$. Hence we deduce that if $Q^{\overline{n-k}}$ resolves $\tilde{\underline{M}}^{\overline{n-k}}$ then it must have the form $Q^{\bar{k}} = \sum_{l=n-k}^{1} |\tilde{u}_h^l\rangle\langle\tilde{u}_g^l|$ (using Lemma 13) which completely specifies $Q^{\bar{k}}$, proving (together with the previous argument) that O solves $\underline{M}^{\bar{n}}$.

We now prove that O solves $\underline{X}^{\overline{n+1}}$ in the misaligned case (i.e. when $m/2$ is not an integer; see Figure 8). We can proceed as in the aligned case until the contact/component condition is violated. In this case, after κ steps the condition is $\langle x^{2\kappa+2+m}\rangle = 0$ which holds until $2\kappa+2+m \leq 2n-2$ (using Lemma 19). This corresponds to $\kappa \leq \frac{2n-2-m}{2} - 1$ which yields $\kappa \leq k-1$. Hence $\underline{M}'^{\overline{\eta-k+1}}$ will be the last instance satisfying the required contact/component conditions (this corresponds to $\underline{M}'^{\bar{5}}$ in Figure 8; use $(n+1)-(k-1)$ with $n=5, k=2$). Supposing O solves $\underline{X}^{\overline{n+1}}$ we deduce (using Lemma 13 and the arguments from the previous case) that it must have the form $O = \sum_{l=\eta}^{\eta-k+1} |u_h'^l\rangle\langle u_g'^l| + Q^{\overline{\eta-k}}$. At the instance $\underline{M}'^{\overline{\eta-k}} = \mathscr{W}(\underline{M}'^{\eta-k+1})$ we flip as before to obtain $\tilde{\underline{M}}^{\overline{\eta-k}} = \mathscr{U}(\mathscr{F}(\underline{M}'^{\overline{\eta-k}}))$ (these are indicated by the triangles next to $\underline{M}'^{\bar{4}}$ and $\tilde{\underline{M}}^{\bar{4}}$ in Figure 8). We proceed as before to write the contact/component condition after l iterations, $\langle x^{-(2l+2)+m}\rangle = 0$ which from Lemma 19 holds if $0 \leq -(2l+2)+m$. This in turn yields $l \leq m/2-1$ entailing that the rank, i.e. $\eta-k-l$ until which the contact/component condition holds is $\cancel{\eta}+1-(\cancel{\eta}-1+\lfloor -m/2\rfloor)-(\lfloor m/2\rfloor-1) = 4$ (this corresponds to $\tilde{\underline{M}}^{\bar{4}}$ in Figure 8). Continuing with the argument for the form of O, we can deduce (again, using Lemma 13 and the previous reasoning) that $Q^{\overline{\eta-k}} = \sum_{l=\eta-k}^{4} |\tilde{u}_h^l\rangle\langle\tilde{u}_g^l| + Q^{\bar{3}}$. Since $\tilde{\underline{M}}^{\bar{4}}$ satisfies the required contact/component conditions, we can iterate once more. However, at this point, only the contact condition holds but the component condition does not (see Figure 8). Consider $\tilde{\underline{M}}^{\bar{3}} = \mathscr{U}_v(\mathscr{W}(\tilde{\underline{M}}^{\bar{4}}))$ and let $(\tilde{H}^{\bar{3}}, \tilde{G}^{\bar{3}}, *, \cdots *) := \tilde{\underline{M}}^{\bar{3}}$. We can not apply Lemma 13 on $\tilde{\underline{M}}^{\bar{3}}$ but we can apply Lemma 16 as $\tilde{\underline{M}}^{\bar{3}}$ has wiggle-v room ϵ along $|n+1\rangle$ (see Definition 10). To see this, note that the probability vectors had no component along $|n+1\rangle$ and that we inverted the matrices using the flip map. This yields $Q^{\bar{3}} = |\tilde{u}_h^{\bar{3}}\rangle\langle\tilde{u}_g^{\bar{3}}| + Q^{\bar{2}}$. The lemma also lets us proceed by the application of the Wiggle-v Iteration map (see Definition 15) $\tilde{\underline{M}}^{\bar{2}} = \mathscr{W}_v(\tilde{\underline{M}}^{\bar{3}})$. Since at this point even the contact condition does not hold, we again apply the flip map (and the wiggle-w initialisation map as justified next) to obtain $\underline{M}'^{\bar{2}} = \mathscr{U}_w(\mathscr{F}(\tilde{\underline{M}}^{\bar{2}}))$. Instead of decreasing the power of x, the contact condition of this instance corresponds to increasing the power of x, i.e. the contact condition for $\underline{M}'^{\bar{2}}$ corresponds to $\langle x^{2(k-1)+2+m+1}\rangle = 0$ which in turn holds if $2k+m+1 \leq 2n-2$. Indeed, $0 = \cancel{2n-2} + 2\lfloor -m/2\rfloor + m + 1 \leq \cancel{2n-2} = 0$ (substituting for $n=5, k=2, m=3$ we get $8 = 2.2+3+1 \leq 2.5-2 = 8$). Since $\underline{M}'^{\bar{2}}$ has wiggle-w room ϵ along $|n+1\rangle$, we were justified at applying the wiggle-w initialisation map (see Lemma 16). This, and the orthogonality of O, determine the form of $Q^{\bar{2}} = |u_h'^{\bar{2}}\rangle\langle u_g'^{\bar{2}}| + |u_h'^{\bar{1}}\rangle\langle u_g'^{\bar{1}}|$ which completely determines the solution, O.

□

In the case of an unbalanced monomial problem, either there is a misalignment at the top or at the bottom. If the misalignment is at the top, it is cleaner to start with going downwards. To facilitate the tracking of powers, we state a result similar to Lemma 34, where we start with going downwards. This can be proved by combining Lemma 49, Lemma 50 and Lemma 51 (see Section B).

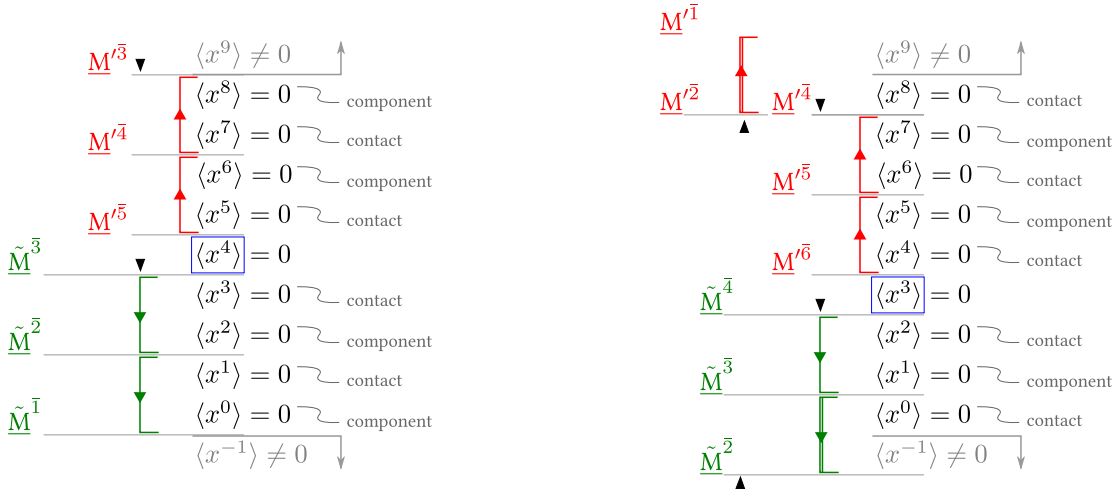

Figure 8: Power diagram representative of the aligned (left) and misaligned (right) balanced monomial assignment for $2n = 10$ with $m = 4$ (left) and $m = 3$ (right).

Lemma 36 (Down-then-Up Contact/Component Lemma). *Consider the matrix instance*

$$\underline{\tilde{M}}^{\bar{n}} := \mathscr{U}((H'^{\bar{n}})^{\dashv}, (G'^{\bar{n}})^{\dashv}, \left|w'^{\bar{n}}\right\rangle, \left|v'^{\bar{n}}\right\rangle, H'^{\bar{n}}, G'^{\bar{n}}, |.\rangle, |.\rangle).$$

Suppose the Normal Initialisation Map and the Weingarten Iteration Map (see Definition 11 and Definition 12) are applied k times to obtain $\underline{\tilde{M}}^{\overline{n-k}}$, viz. applying $\underline{\tilde{M}}^{\overline{i-1}} = \mathscr{U}(\mathscr{W}(\underline{\tilde{M}}^{\bar{i}}))$ k times. Let $n-k=d$ and consider $\underline{M'}^{\bar{d}} = \mathscr{U}(\mathscr{F}(\underline{\tilde{M}}^{\bar{d}}))$. Suppose the Normal Initialisation Map and the Weingarten Iteration map are applied l more times to obtain $\underline{M'}^{\overline{d-l}} =: \left(H'^{\overline{n-l}}, G'^{\overline{n-l}}, \left|w'^{\overline{n-l}}\right\rangle, \left|v'^{\overline{n-l}}\right\rangle, *, \cdots *\right)$. Then,

$$\left\langle v'^{\overline{n-k-l}}\right| \left(G'^{\overline{n-k-l}}\right)^{\mu} \left|v'^{\overline{n-k-l}}\right\rangle = r\left(\left\langle (G'^{\bar{n}})^{-(2k+\mu)}\right\rangle, \ldots, \left\langle (G'^{\bar{n}})^{2l+\mu-1}\right\rangle, \left\langle (G'^{\bar{n}})^{2l+\mu}\right\rangle\right)$$

where $\mu \geq 1$ and r is a multi-variate function which does not depend on any $\left\langle (G'^{\bar{n}})^{i}\right\rangle := \left\langle v'^{\bar{n}}\right| (G'^{\bar{n}})^{i} \left|v'^{\bar{n}}\right\rangle$ other than through its arguments[12]. The corresponding statement involving Hs and $|w\rangle$s also holds.

Finally, we state the solution to the unbalanced monomial problem.

Proposition 37 (Solving the Unbalanced Monomial Problem). *Let*

$$t = \sum_{i=1}^{2n-1} -\frac{(-x_i)^m}{\prod_{j\neq i}(x_j - x_i)} [\![x_i]\!] = \sum_{i=1}^{n_h} x_{h_i}^m p_{h_i} [\![x_{h_i}]\!] - \sum_{i=1}^{n_g} x_{g_i}^m p_{g_i} [\![x_{g_i}]\!]$$

be an unbalanced monomial assignment for the set of real numbers $0 < x_1 < x_2 \cdots < x_{2n-1}$ (see Definition 18) where p_{h_i} and p_{g_i} are strictly positive and $\{x_{h_i}\}$ and $\{x_{g_i}\}$ are all distinct. Consider the corresponding matrix instance $\underline{X}^{\bar{n}} := (X_h^{\bar{n'}}, X_g^{\bar{n'}}, (X_h^{\bar{n'}})^b |v\rangle, (X_g^{\bar{n'}})^b |w\rangle)$ where

- *if $n_h = n$ (the Wiggle-v case; corresponds to odd m)*

$$X_h^{\bar{n}} \doteq diag(x_{h_1}, x_{h_2} \ldots x_{h_{n-1}}, x_{h_n}), \qquad X_g^{\bar{n}} \doteq diag(x_{g_1}, x_{g_2} \ldots x_{g_{n-1}}, \epsilon),$$
$$\left|w^{\bar{n}}\right\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_{n-1}}}, \sqrt{p_{h_n}}), \qquad \left|v^{\bar{n}}\right\rangle \doteq (\sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_{n-1}}}, 0),$$

- *else if $n_g = n$ (the Wiggle-w case; corresponds to even m)*

$$X_h^{\bar{n}} \doteq diag(x_{h_1}, x_{h_2} \ldots x_{h_{n-1}}, 1/\epsilon), \qquad X_g^{\bar{n}} \doteq diag(x_{g_1}, x_{g_2} \ldots x_{g_{n-1}}, x_{g_n}),$$
$$\left|w^{\bar{n}}\right\rangle \doteq (\sqrt{p_{h_1}}, \sqrt{p_{h_2}} \ldots \sqrt{p_{h_{n-1}}}, 0), \qquad \left|v^{\bar{n}}\right\rangle \doteq (\sqrt{p_{g_1}}, \sqrt{p_{g_2}} \ldots \sqrt{p_{g_{n-1}}}, \sqrt{p_{g_n}}).$$

Consider the Wiggle-v case. Let $k = \frac{2n-3-m}{2}$ (this will be an integer as m is odd). In the limit of $\epsilon \to 0$,

$$O = \sum_{i=n}^{n-k+1} \left|u_h'^{\bar{i}}\right\rangle \left\langle u_g'^{\bar{i}}\right| + \sum_{i=n-k}^{1} \left|\tilde{u}_h^{\bar{i}}\right\rangle \left\langle \tilde{u}_g^{\bar{i}}\right|$$

solves the matrix instance $\underline{X}^{\bar{n}}$ where the terms in the sum are as defined. We start with $\underline{M'}^{\bar{n}} := \mathscr{U}(\underline{X}^{\bar{n}} \oplus \left((X_h^{\bar{n}})^{-1}, (X_g^{\bar{n}})^{-1}, |.\rangle, |.\rangle\right)$ (see Definition 11, Definition 12) and using the relation

$$\underline{M'}^{\overline{l-1}} := \mathscr{U}(\mathscr{W}(\underline{M'}^{\bar{l}})) \qquad n-k+1 \leq l-1 \leq n-1,$$

define

$$\left(*, \cdots *, \left|u_h'^{\bar{l}}\right\rangle, \left|u_g'^{\bar{l}}\right\rangle\right) := \underline{M'}^{\bar{l}} \qquad n-k+1 \leq l \leq n$$

These define the terms for the first sum. For terms for the second sum we start with

$$\underline{\tilde{M}}^{\overline{n-k}} := \mathscr{U}(\mathscr{F}(\underline{M'}^{\overline{n-k}}))$$

and using the relation

$$\underline{\tilde{M}}^{\overline{l-1}} := \mathscr{U}(\mathscr{W}(\underline{\tilde{M}}^{\bar{l}})) \qquad 3 \leq l-1 \leq n-k-1,$$

[12](e.g. if $r(x) = e^x$ and we are interested in $r(\alpha)$ then r doesn't depend on α other than through its argument)

define

$$\left(*,\cdots *,\left|\tilde{u}_h^{\bar{l}}\right\rangle,\left|\tilde{u}_g^{\bar{l}}\right\rangle\right) := \underline{\tilde{M}}^{\bar{l}} \qquad 2 \le l \le n-k.$$

Finally, we define (see Definition 14)

$$\underline{\tilde{M}}^{\bar{2}} := \mathscr{U}_v(\mathscr{W}(\underline{\tilde{M}}^{\bar{3}})) =: \left(*,*,\left|\tilde{w}^{\bar{2}}\right\rangle,\left|\tilde{v}^{\bar{2}}\right\rangle,*\cdots *\right),$$

$\left|\tilde{u}_h^{\bar{1}}\right\rangle := \left|e\left(\left|\tilde{u}_h^{\bar{2}}\right\rangle,\left|\tilde{w}^{\bar{2}}\right\rangle\right)\right\rangle$ *and* $\left|\tilde{u}_g^{\bar{1}}\right\rangle := \left|e\left(\left|\tilde{u}_g^{\bar{2}}\right\rangle,\left|\tilde{v}^{\bar{2}}\right\rangle\right)\right\rangle$.

Consider the Wiggle-w case. Let $k = \frac{m}{2}$ *(this will be an integer as m is even). In the limit of* $\epsilon \to$,

$$O = \sum_{i=n}^{n-k+1} \left|\tilde{u}_h^{\bar{i}}\right\rangle\left\langle\tilde{u}_g^{\bar{i}}\right| + \sum_{i=n-k}^{1} \left|u_h'^{\bar{i}}\right\rangle\left\langle u_g'^{\bar{i}}\right|$$

solves the matrix instance $\underline{X}^{\bar{n}}$ *where the terms in the sum are as defined. We start with* $\tilde{M}^{\bar{n}} := \mathscr{U}\left(\mathscr{F}\left(\underline{X}^{\bar{n}} \oplus \left((X_h^{\bar{n}})^{-1},(X_g^{\bar{n}})^{-1},|.\rangle,|.\rangle\right)\right)\right)$ *(see Definition 11, Definition 17, Definition 12) and define*

$$\underline{\tilde{M}}^{\bar{l}} =: \left(*,\cdots *,\left|u_h'^{\bar{l}}\right\rangle,\left|u_g'^{\bar{l}}\right\rangle\right) \qquad n-k+1 \le l \le n$$

$$\underline{\tilde{M}}^{\bar{l}} := \mathscr{U}(\mathscr{W}(\underline{\tilde{M}}^{\bar{l}}) \qquad n-k+1 \le l-1 \le n-1.$$

These define the terms for the first sum. For terms for the second sum we start with

$$\underline{M'}^{\overline{n-k}} := \mathscr{U}(\mathscr{F}(\underline{\tilde{M}}^{\overline{n-k}}))$$

and using

$$\underline{M'}^{\overline{l-1}} := \mathscr{U}(\mathscr{W}(\underline{M'}^{\bar{l}})) \qquad 3 \le l-1 \le n-k-1,$$

define

$$\left(*,\cdots *,\left|u_h'^{\bar{l}}\right\rangle,\left|u_g'^{\bar{l}}\right\rangle\right) :=\underline{M'}^{\bar{l}} \qquad 2 \le l \le n-k.$$

Finally, we define (see Definition 14)

$$\underline{M'}^{\bar{2}} := \mathscr{U}_w(\mathscr{W}(\underline{M'}^{\bar{3}})) =: (*,*,\left|w'^{\bar{2}}\right\rangle,\left|v'^{\bar{2}}\right\rangle,*\cdots *),$$

$\left|u_h'^{\bar{1}}\right\rangle := \left|e\left(\left|u_h'^{\bar{2}}\right\rangle,\left|w'^{\bar{2}}\right\rangle\right)\right\rangle$ *and* $\left|u_g'^{\bar{1}}\right\rangle := \left|e\left(\left|u_g'^{\bar{2}}\right\rangle,\left|u_h'^{\bar{2}}\right\rangle\right)\right\rangle$.

Proof. From Figure 9 it is clear that the wiggle-v case is essentially the same as the balanced misaligned monomial until the second to last step (the wiggle-w step after wiggle-v is not needed). From Figure 9 it is also clear the wiggle-w case is essentially the same as the wiggle-v case except that we must start with going downwards (decreasing powers of $\langle x^\mu\rangle$), i.e. using $\underline{\tilde{M}}^{\bar{n}}$ and then flip to $\underline{M'}^{\bar{k}}$ to go upwards and end with a wiggle-w. The arguments for the contact/component conditions go through unchanged using Lemma 36. □

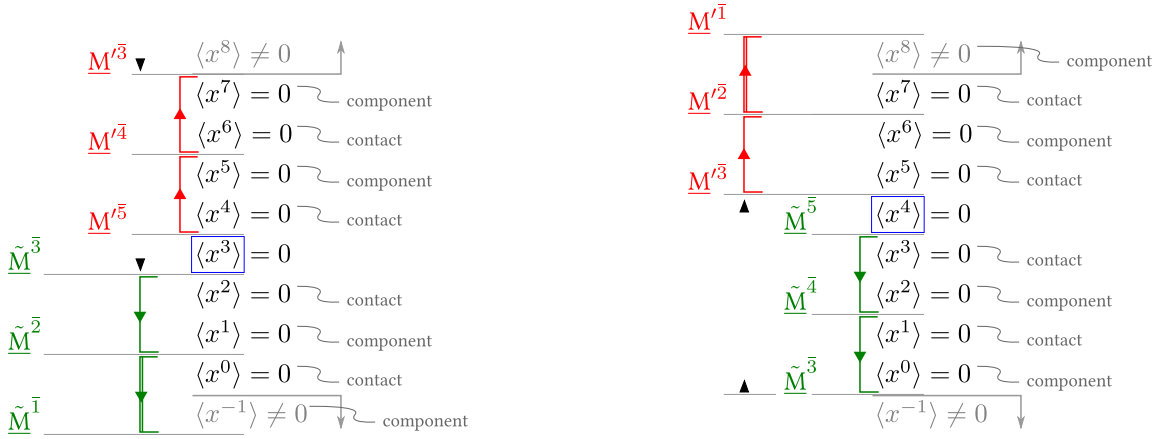

Figure 9: Power diagram representative of the unbalanced monomial assignment for $n = 4$ ($2n-1 = 9$) with $m = 3$ (left; wiggle-v case) and $m = 4$ (right; wiggle-w case).

Combining the results together, we prove Theorem 4.

Proof of Theorem 4. From Lemma 32 we can find an f-assignment which has the same solution as the one given but has all coordinates strictly positive. Henceforth, we consider this assignment. From Proposition 31 one can express this assignment as a sum of monomial and/or effectively monomial assignments. From Corollary 29 it follows that an effectively monomial assignment can be solved using the solution of the corresponding monomial assignment. Since a monomial assignment is either balanced, in which case its solution is given by Proposition 35, or it is unbalanced, in which case its solution is given by Proposition 37. □

We conclude this section with a remark about the implementation of the valid functions whose sum is the f function—the valid function corresponding to an f-assignment—we originally wished to implement. The difficulty is that the valid functions which constitute the sum might have assigned a negative weight to a point which is a assigned positive weight by the f assignment. This difficulty can be almost trivially addressed by using the "catalyst state" that Kitaev/Mochon had introduced to convert a Time Independent Point Game into a Time Dependent Point Game (see §4.1 of [Moc07] or the proof of Theorem 5 from [Aha+14]). The basic idea there is to introduce a small negative weight and apply the valid functions by appropriately scaling them down (so that the negative weight suffices) repeatedly to have the same effect as having applied the unscaled valid function. The small negative weight can be made arbitrarily small at the expense of communication rounds, thereby having a vanishing effect on the bias. This technique also lets us apply the valid functions which constitute the sum instead of applying the given f function.

10 Conclusion and Outlook

In this work we presented the analytical construction of explicit WCF protocols achieving arbitrarily close to zero bias based on Mochon's games. There exist several open problems that deserve further study. First, finding (assuming they exist) analytic unitaries corresponding to Mochon's assignments in fewer dimensions. Perhaps the Pelchat-Hoyer point games [HP13], which is also a family of point games that give rise to WCF protocols with arbitrarily close to zero bias, admit neater analytic unitaries as they are not very well-studied. Second, given the recently improved bound on communication[Mil19], are there protocols matching the bounds on resources? Third, how sensitive/robust are weak coin flipping protocols to/against noise? While we expect the bias to increase in the presence of noise, a thorough study of such effects is needed in order to assess the magnitude of sensitivity to it.

11 Acknowledgements

We are thankful to Ognyan Oreshkov and Tom Van Himbeeck 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.

References

[Aha+14] 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.

[ARW18] Atul Singh Arora, Jérémie Roland and Stephan Weis. "Quantum Weak Coin Flipping". In: (6th Nov. 2018). arXiv: http://arxiv.org/abs/1811.02984v1 [quant-ph].

[ARW19] 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.

[Blu83] 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.

[Cle86] 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.

[Hag89] William W. Hager. "Updating the Inverse of a Matrix". In: *SIAM Review* 31.2 (June 1989), pp. 221–239. DOI: 10.1137/1031049.

[HP13] 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.

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

[LC98] 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.

[Mil19] Carl A. Miller. "The Impossibility of Efficient Quantum Weak Coin-Flipping". In: (22nd Sept. 2019). arXiv: http://arxiv.org/abs/1909.10103v1 [quant-ph].

[Moc07] Carlos Mochon. "Quantum weak coin flipping with arbitrarily small bias". In: *arXiv:0711.4114* (2007). arXiv: 0711.4114.

[Sch09] Rolf Schneider. *Convex Bodies: The Brunn-Minkowski Theory*. Cambridge University Press, 2009. DOI: 10.1017/cbo9781139003858.

[SM50] Jack Sherman and Winifred J. Morrison. "Adjustment of an Inverse Matrix Corresponding to a Change in One Element of a Given Matrix". In: *The Annals of Mathematical Statistics* 21.1 (Mar. 1950), pp. 124–127. DOI: 10.1214/aoms/1177729893.

A Ellipsoids

A.1 Known Results

Consider a curve in the plane specified by f. The curvature is related to the rate of change of tangents, i.e. the second derivative of f. For a surface in arbitrary dimensions specified by f, the corresponding quantity becomes a matrix $\partial_i \partial_j f$. The eigenvalues of this matrix tell us the curvature along the corresponding eigenvector. While in principle, it is possible to find this matrix by following this approach, in practice it becomes rather cumbersome[13]. Using more sophisticated mathematics one can easily obtain an analytic solution to this problem, for ellipsoids. The *Weingarten map*, defined intuitively is the differential of the normal at a given point on the manifold. This turns out to be effectively the same as finding the aforementioned matrix of second derivatives.

Definition 38 (Weingarten Map (informal))**.** (see[14] § 2.5 of Schneider [Sch09]) Let K be a manifold specified by the heads of vectors in $\mathbb{R}^n$. Denote the tangent space of K at $|x\rangle \in K$ by $T_{|x\rangle}K$. Let $|u_K(|x\rangle)\rangle$ be the outer unit normal vector of K at $|x\rangle$. The map $|u_k(|x\rangle)\rangle : K \to \mathbb{S}^{n-1} \subset \mathbb{R}^n$ as defined is called the *spherical image map* (or *Gauss map*) of the interior of the manifold K. Its differential at $|x\rangle$, $d(|u_K\rangle)_k =: W_x$ maps $T_{|x\rangle}K$ to itself. The linear map $W_x : T_{|x\rangle}K \to T_{|x\rangle}K$ is called the *Weingarten map*.

A related quantity, known as the *Reverse Weingarten map*, is easier to calculate. This is of interest because of the following result.

Theorem 39 (Informal)**.** *[Sch09] Inverse of the Weingarten map equals the reverse Weingarten map, for well behaved surfaces.*

We omit the exact statement of the theorem and the definition of the Reverse Weingarten map as they are not directly relevant to the discussion. We simply work with a formula for the Weingarten map as described.

Definition 40 (Support Function)**.** [Sch09] Given a manifold specified by a set S of vectors, and a normalised vector $|u\rangle$, the support function

$$h_S(|u\rangle) := \sup_{|s\rangle \in S} \langle s|u\rangle .$$

Theorem 41 (Formula for evaluating the Reverse Weingarten Map (Informal))**.** *(see[15] § 2.5 of [Sch09]) Consider a convex surface specified by a set S of vectors. Given a normalised vector $|u\rangle$, the reverse Weingarten map, W, evaluated along the normal specified by $|u\rangle$ is given by*

$$W = \left.\frac{\partial^2 h_S(|u'\rangle)}{\partial u'_i \partial u'_j}\right|_u$$

where $h_S(|u'\rangle)$ is the support function.

Assuming we can invert a matrix, using Theorem 41 and Theorem 39 one can obtain the Weingarten map. We apply this to the case of ellipsoids.

A.2 Normals and Curvatures/Weingarten Map

Lemma 42. *(See § 6.2 of Arora, Roland and Weis [ARW18]) Given an $n \times n$ matrix $G \geq 0$, the support function corresponding to the ellipsoid S_G along a normal $|u\rangle$ of the manifold is given by*

$$h_{S_G}(|u\rangle) = \sqrt{\langle u| G^{\dagger} |u\rangle}.$$

Remark 43. Given an $n \times n$ matrix $G \geq 0$, note that $S_G = \{\mathcal{E}_G(|v\rangle) \,|\, \langle v|v\rangle = 1, |v\rangle \in \Pi\mathbb{R}^n\}$.

In our analysis, we typically know the position at which we wish to evaluate the curvature The calculation of the support function requires the normal at that point. To this end, we give a formula for evaluating the latter.

Lemma 44 (Normal)**.** *Given an $n \times n$ matrix $G \geq 0$, consider the manifold S_G associated with it. Let $|v\rangle \in \Pi\mathbb{R}^n$ be a vector such that $\mathcal{E}_G(|v\rangle)$ is well defined ($\langle v| G |v\rangle \neq 0$) where Π is as defined in Definition 6. The normal at $\mathcal{E}_G(|v\rangle)$ (which we also refer to as the normal along $|v\rangle$) is given by $|u\rangle = G|v\rangle / \sqrt{\langle v| G^2 |v\rangle}$.*

Proof. Consider the case where $G = \mathrm{diag}(x_{g_1}, x_{g_2} \ldots x_{g_n})$ and let $|v\rangle = (v_1, v_2 \ldots v_n)$. The surface S_G is determined by the constraint $\langle v| G |v\rangle = 1$ which is equivalent to $\sum_{i=1}^n x_{g_i} v_i^2 = 1$. Changing the constant 1 can be thought of as scaling the surface. Treating $\sum_{i=1}^n x_{g_i} v_i^2$ as a scalar function, its gradient will point along the outward normal: $|u\rangle \propto \sum_{j=1}^n \frac{\partial}{\partial v_j} \sum_{i=1}^n x_{g_i} v_i^2 \, |j\rangle \propto \sum_{j=1}^n x_{g_j} v_j \, |j\rangle \propto G|v\rangle$. □

[13] as one must choose a coordinate system with its origin at the point of interest, aligned along the normal and re-express all the quantities

[14] Note, their convention for T and K is slightly different; Informal because there are qualifying conditions on K which we suppressed.

[15] Informal because qualifying conditions on the surface are missing, among other technicalities.

With these ingredients we can evaluate the Reverse Weingarten Map.

Lemma 45 (Reverse Weingarten Map). *Given an $n \times n$ matrix $G \geq 0$, and a vector $|v\rangle \in \Pi\mathbb{R}^n$ where Π is as defined in Definition 6, the reverse Weingarten Map associated with the surface S_G, evaluated at the point $\mathcal{E}_G(|v\rangle)$ is given by*

$$W_G := \sqrt{\frac{\langle G^2\rangle}{\langle G\rangle}}\left(G^{\dashv} - \frac{|v\rangle\langle v|}{\langle G\rangle}\right)$$

where $\langle G^j\rangle := \langle v| G^j |v\rangle$.

Proof. We prove this for the case where $G > 0$ (the case for $G \geq 0$ follows analogously by restricting to the non-zero eigenspace). Let the spectral decomposition of G be given by

$$G = \sum_{i=1}^{n} x_{g_i} |g_i\rangle\langle g_i|$$

and let $|v\rangle = \sum_{i=1}^n c_i |g_i\rangle$. Recall that the normal along $|v\rangle$ (see Lemma 44) is given by $|u\rangle = G|v\rangle / \sqrt{\langle v| G^2 |v\rangle}$. Writing $|u\rangle = \sum_{i=1}^n u_i |g_i\rangle$, u_is are fixed. Then the support function evaluated along the normal $|u\rangle$ is given by (we use h to denote $h_{S_G}(|u\rangle)$ for brevity)

$$\begin{aligned}
h = \sqrt{\langle u| G^{\dashv} |u\rangle} &= \sqrt{\sum_{i=1}^{n} x_{g_i}^{-1} u_i^2} && \text{using Lemma 42}\\
\implies (W_G)_{ij} = \frac{\partial^2 h}{\partial u_i \partial u_j} &= -\frac{1}{h^3} x_{g_j}^{-1} x_{g_i}^{-1} u_j u_i + \frac{x_{g_i}^{-1}}{h}\delta_{ij} && \text{using Theorem 41}\\
\implies W_G &= -\frac{1}{h^3} G^{\dashv}|u\rangle\langle u| G^{\dashv} + \frac{G^{\dashv}}{h}
\end{aligned}$$

where we used the more general notation $G^{\dashv} = G^{-1}$ in our case. Substituting $|u\rangle$ in the expression for h and for W_G we obtain the required result, viz. $h = \sqrt{\frac{\langle G\rangle}{\langle G^2\rangle}}$ and

$$W_G = \frac{1}{h} G^{\dashv} - \frac{1}{h^3}\frac{|v\rangle\langle v|}{\langle G^2\rangle} = \sqrt{\frac{\langle G^2\rangle}{\langle G\rangle}} G^{\dashv} - \frac{\cancel{\langle G^2\rangle}\sqrt{\langle G^2\rangle}}{\langle G\rangle\sqrt{\langle G\rangle}}\frac{|v\rangle\langle v|}{\cancel{\langle G^2\rangle}} = \sqrt{\frac{\langle G^2\rangle}{\langle G\rangle}}\left(G^{\dashv} - \frac{|v\rangle\langle v|}{\langle G\rangle}\right).$$

When $G \geq 0$ and has zero eigenvalues, the spectral decomposition would have m elements with $m < n$ elements, viz. $G = \sum_{i=1}^m x_{g_i} |g_i\rangle\langle g_i|$. The summation $\sum_{i=1}^m x_{g_i}^{-1} u_i^2$ would then correspond to $\langle u| G^{\dashv} |u\rangle$. Similar replacements can be made to generalise the proof. □

Inverting the Reverse Weingarten Map is also not too hard due to the following result. Combining it, we obtain the Weingarten map.

Theorem 46 (Sherman-Morrison formula). *[SM50; Hag89] Let A be an $n \times n$ invertible matrix and let $|a\rangle$, $|b\rangle$ be vectors (in n-dimensions). Then, $(A + |a\rangle\langle b|)$ is invertible if and only if $1 + \langle b| A^{-1} |a\rangle \neq 0$. Further, if this is the case, then*

$$(A + |a\rangle\langle b|)^{-1} = A^{-1} - \frac{A^{-1}|a\rangle\langle b| A^{-1}}{1 + \langle b| A^{-1} |a\rangle}.$$

Lemma 47 (Weingarten Map). *Given an $n \times n$ matrix $G \geq 0$, the Weingarten Map associated with the surface S_G, evaluated at the point $\mathcal{E}_G(|v\rangle)$ is given by*

$$W_G^{\dashv} = \sqrt{\frac{\langle G\rangle}{\langle G^2\rangle}}\left(G + \frac{\langle G^3\rangle}{\langle G^2\rangle^2} G|v\rangle\langle v| G - \frac{1}{\langle G^2\rangle}\left(G|v\rangle\langle v| G^2 + G^2|v\rangle\langle v| G\right)\right)$$

where $\langle G\rangle := \langle v| G |v\rangle$.

Proof. Again, we prove this for the case $G > 0$ and the proof for the case where $G \geq 0$ follows analogously. By a direct computation, it is clear that $W_G G|v\rangle = 0$ (see Lemma 45). It is therefore not surprising that a direct application of Theorem 46 yields

$$W^{-1} = \sqrt{\frac{\langle G\rangle}{\langle G^2\rangle}}\left(G + \frac{G|v\rangle\langle v| G}{\langle G\rangle .0}\right) \tag{9}$$

where (after pulling out the $1/\sqrt{\langle G^2\rangle/\langle G\rangle}$ factor) we set $A = G^{\dashv} = G^{-1}$ (in this case) and $|a\rangle = |b\rangle = G|v\rangle/\sqrt{\langle G\rangle}$. Using proper interpolations (for instance one could use $|a\rangle = -|b\rangle = (1-\epsilon)G|v\rangle/\sqrt{\langle G\rangle}$ instead of $G|v\rangle/\sqrt{\langle G\rangle}$), one can make the second term well behaved and have it diverge only as some parameter vanishes ($\epsilon = 0$). The quantity we are interested in $W^{\dashv} = \Pi_u^{\perp} W \Pi_u^{\perp}$ where

$\Pi_u^\perp = \mathbb{I} - |u\rangle\langle u|$ and $|u\rangle = G|v\rangle/\sqrt{\langle G\rangle}$. If the positive inverse is to be well defined, the second term (in Equation (9)) should disappear after the projection, viz. $\Pi_u^\perp G|v\rangle\langle v|G\Pi_u^\perp$ should vanish. Indeed, it does because $G|v\rangle \propto |u\rangle$. The non-vanishing contribution must then come from the first term (in Equation (9)) $\Pi_u^\perp G\Pi_u^\perp = (\mathbb{I} - |u\rangle\langle u|)\,G\,(\mathbb{I} - |u\rangle\langle u|)$ which entails

$$W^{-1} = \sqrt{\frac{\langle G\rangle}{\langle G^2\rangle}}\Pi_u^\perp G\Pi_u^\perp = \sqrt{\frac{\langle G\rangle}{\langle G^2\rangle}}\,(G - G|u\rangle\langle u| - |u\rangle\langle u|G + \langle u|G|u\rangle|u\rangle\langle u|)$$
$$= \sqrt{\frac{\langle G\rangle}{\langle G^2\rangle}}\left(G - \frac{G^2|v\rangle\langle v|G}{\langle G^2\rangle} - \frac{G|v\rangle\langle v|G^2}{\langle G^2\rangle} + \frac{\langle G^3\rangle}{\langle G^2\rangle}\frac{G|v\rangle\langle v|G}{\langle G^2\rangle}\right).$$

The case for $G \geq 0$ where G has zero eigenvalues carries through. This can be seen by viewing the Sherman Morrison formula as a "correction" to an inverse when one entry of the matrix is changed. The inverse of G we are interested in is the positive inverse G^{-1}. The entry of the matrix that we change is in this positive subspace. Restricting the analysis to this subspace, the matrix G can be viewed as positive, viz. $G > 0$, yielding the required generalisation. □

All of these results justify the definitions introduced in Section 4.

B Lemmas for the Contact and Component conditions

Lemma 48. *Consider the matrix instance* $\underline{X}^{\bar{n}} := (H^{\bar{n}}, G^{\bar{n}}, |w^{\bar{n}}\rangle, |v^{\bar{n}}\rangle)$. *Suppose that the Weingarten Iteration Map (see Definition 12) is applied* l *times to obtain* $\underline{X}^{\overline{n-l}} := \left(H^{\overline{n-l}}, G^{\overline{n-l}}, \left|w^{\overline{n-l}}\right\rangle, \left|v^{\overline{n-l}}\right\rangle\right)$. *Then, for any* l, *the expectation value* $\left\langle v^{\overline{n-l}}\right| G^{\overline{n-l}} \left|v^{\overline{n-l}}\right\rangle$ *is a function of the expectation values* $\langle v^{\bar{n}}|(G^{\bar{n}})^p|w^{\bar{n}}\rangle = \langle (G^{\bar{n}})^p\rangle$, *where the powers* p *range from* 0 *to* $2l+1$ *at most. The corresponding statement involving* H*s and* $|w\rangle$*s also holds.*

Proof. Using once the Weingarten Iteration Map, we obtain:

$$\left|v^{\overline{n-1}}\right\rangle = |v^{\bar{n}}\rangle - \tfrac{\langle G^{\bar{n}}\rangle}{\langle (G^{\bar{n}})^2\rangle} G^{\bar{n}}|v^{\bar{n}}\rangle$$
$$G^{\overline{n-1}} = G^{\bar{n}} + \tfrac{\langle (G^{\bar{n}})^3\rangle}{\langle (G^{\bar{n}})^2\rangle^2} G^{\bar{n}}|v^{\bar{n}}\rangle\langle v^{\bar{n}}|G^{\bar{n}} - \tfrac{1}{\langle (G^{\bar{n}})^2\rangle}\left(G^{\bar{n}}|v^{\bar{n}}\rangle\langle v^{\bar{n}}|(G^{\bar{n}})^2 + (G^{\bar{n}})^2|v^{\bar{n}}\rangle\langle v^{\bar{n}}|G^{\bar{n}}\right). \tag{10}$$

If we continue to iterate accordingly and express everything in terms of $|v^{\bar{n}}\rangle$ and $G^{\bar{n}}$, which are known, after l steps we will obtain:

$$\left|v^{\overline{n-l}}\right\rangle = \textstyle\sum_{i=0}^{l} \alpha_i (G^{\bar{n}})^i |v^{\bar{n}}\rangle$$
$$G^{\overline{n-l}} = G^{\bar{n}} + \textstyle\sum_{i,j=0}^{l+1} \alpha_{i,j} (G^{\bar{n}})^i |v^{\bar{n}}\rangle\langle v^{\bar{n}}|(G^{\bar{n}})^j, \tag{11}$$

where the multiplicative factors a_i and $a_{i,j}$ also contain terms of the form $\langle (G^{\bar{n}})^p\rangle$, in which p ranges between the minimum and maximum powers appearing in the sum (see remark at the end of the proof).

Indeed, we can use induction to prove that equation (11) holds for all l.
The base of the induction $l = 1$ immediately gives us equation (10).
For the $l+1$ instance, using the Weingarten Iteration Map, we have:

$$\left|v^{\overline{n-l-1}}\right\rangle = \left|v^{\overline{n-l}}\right\rangle - \tfrac{\langle G^{\overline{n-l}}\rangle}{\langle (G^{\overline{n-l}})^2\rangle}(G^{\overline{n-l}})\left|v^{\overline{n-l}}\right\rangle$$
$$G^{\overline{n-l-1}} = G^{\bar{n}} + \tfrac{\langle (G^{\overline{n-l}l})^3\rangle}{\langle (G^{\overline{n-l}})^2\rangle^2} G^{\overline{n-l}}\left|v^{\overline{n-l}}\right\rangle\left\langle v^{\overline{n-l}}\right| G^{\overline{n-l}} - \tfrac{1}{\langle (G^{\overline{n-l}})^2\rangle}\overline{n-l}\left(G^{\overline{n-l}}\left|v^{\overline{n-l}}\right\rangle\left\langle v^{\overline{n-l}}\right|(G^{\overline{n-l}})^2 + (G^{\overline{n-l}})^2\left|v^{\overline{n-l}}\right\rangle\left\langle v^{\overline{n-l}}\right| G^{\overline{n-l}}\right).$$

Replacing $G^{\overline{n-l}}$ and $\left|v^{\overline{n-l}}\right\rangle$ from equation (11), we get

$$\left|v^{\overline{n-l-1}}\right\rangle = \textstyle\sum_{i=0}^{l+1} \alpha_i (G^{\bar{n}})^i |v^{\bar{n}}\rangle$$
$$G^{\overline{n-l-1}} = G^{\bar{n}} + \textstyle\sum_{i,j=0}^{l+2} \alpha_{i,j} (G^{\bar{n}})^i |v^{\bar{n}}\rangle\langle v^{\bar{n}}|(G^{\bar{n}})^j, \tag{12}$$

which proves that equation (11) is valid for all l.
We can now complete our proof by expressing $\left\langle v^{\overline{n-l}}\right| G^{\overline{n-l}} \left|v^{\overline{n-l}}\right\rangle$ in terms of $\langle G^{\bar{n}}\rangle$. Substituting from equation (11), we get:

$$\left\langle v^{\overline{n-l}}\right| G^{\overline{n-l}} \left|v^{\overline{n-l}}\right\rangle = \sum_{i=0}^{l} \alpha_i \left\langle v^{\bar{n}}\right|(G^{\bar{n}})^{i+1} \sum_{j=0}^{l} \alpha_j (G^{\bar{n}})^j \left|v^{\bar{n}}\right\rangle + \sum_{i=0}^{l} \alpha_i \left\langle v^{\bar{n}}\right|(G^{\bar{n}})^i \sum_{i',j'=0}^{l+1} \alpha_{i',j'} (G^{\bar{n}})^{i'} \left|v^{\bar{n}}\right\rangle \left\langle v^{\bar{n}}\right|(G^{\bar{n}})^{j'} \sum_{j=0}^{l} \alpha_j (G^{\bar{n}})^j \left|v^{\bar{n}}\right\rangle. \tag{13}$$

In equation (13), we see that the minimum expectation value is $\langle (G^{\bar{n}})^0\rangle$, while the maximum is $\langle (G^{\bar{n}})^{2l+1}\rangle$, which concludes the proof. □

Notice that we left a_i and $a_{i,j}$ undetermined and we even used the same notation for them (obviously a_i and $a_{i,j}$ are different in equation (11), equation (12) and equation (13)). In the context of our proof their specific form was not relevant, but what was rather important are the minimum and maximum powers p in $\langle (G^{\bar{n}})^p \rangle$ that contain and might appear in $\left\langle v^{\overline{n-l}} \right| G^{\overline{n-l}} \left| v^{\overline{n-l}} \right\rangle$. To estimate them, it suffices to observe that the minimum power that appears in $\left| v^{\overline{n-l}} \right\rangle$ comes from the first term $\left| v^{\bar{n}} \right\rangle$ and is 0, while the maximum power in the a_i 's that appears in $\left| v^{\overline{n-l}} \right\rangle$ comes from $\langle (G^{\overline{n-l+1}})^2 \rangle$ (see the Weingarten Iteration Map formula) and is equal to $2l$. In $G^{\overline{n-l}}$, However, we can find an even higher power appearing in the $a_{i,j}$'s coming from $\langle (G^{\overline{n-l+1}})^3 \rangle$ (see the Weingarten Iteration Map formula) which is equal to $2l+1$. In total these powers are always between the minimum and maximum powers on equation (13), thus the factors a_i and $a_{i,j}$ do not need to be specified.

Lemma 49. *Consider the extended matrix instance* $\underline{M}^{\bar{n}} := \mathscr{U}(H^{\bar{n}}, G^{\bar{n}}, \left| w^{\bar{n}} \right\rangle, \left| v^{\bar{n}} \right\rangle, (H^{\bar{n}})^{\dashv}, (G^{\bar{n}})^{\dashv}, |.\rangle, |.\rangle)$. *Suppose the Normal Initialisation Map and the Weingarten Iteration Map (see Definition 11 and Definition 12) are applied l times to obtain* $\underline{M}^{\overline{n-l}}$, *viz. applying* $\underline{M}^{\overline{i-1}} = \mathscr{U}(\mathscr{W}(\underline{M}^{\dot{i}}))$ *l times. Then, for any l, the expectation value* $\left\langle v^{\overline{n-l}} \right| (G^{\overline{n-l}})^{\dashv} \left| v^{\overline{n-l}} \right\rangle$ *is a function of the expectation values* $\left\langle v^{\bar{n}} \right| (G^{\bar{n}})^p \left| w^{\bar{n}} \right\rangle = \langle (G^{\bar{n}})^p \rangle$, *where the powers p range from 0 to $2l+1$ at most. The corresponding statement involving Hs and $|w\rangle$s also holds.*

Proof. First, we need to specify the form of $(G^{\overline{n-l}})^{\dashv}$ as a function of $G^{\bar{n}}$ and $\left| v^{\bar{n}} \right\rangle$. The first iteration gives:

$$\begin{aligned} \left| v^{\overline{n-1}} \right\rangle &= \left| v^{\bar{n}} \right\rangle - \tfrac{<G^{\bar{n}}>}{\langle (G^{\bar{n}})^2 \rangle} G^{\bar{n}} \left| v^{\bar{n}} \right\rangle \\ (G^{\overline{n-1}})^{\dashv} &= (G^{\bar{n}})^{\dashv} - \tfrac{\left| v^{\bar{n}} \right\rangle \left\langle v^{\bar{n}} \right|}{\langle G^{\bar{n}} \rangle}. \end{aligned} \tag{14}$$

Continuing the iterations to l, we obtain:

$$\begin{aligned} \left| v^{\overline{n-l}} \right\rangle &= \textstyle\sum_{i=0}^{l} \alpha_i (G^{\bar{n}})^i \left| v^{\bar{n}} \right\rangle \text{ (from Lemma 1)} \\ (G^{\overline{n-l}})^{\dashv} &= (G^{\bar{n}})^{\dashv} + \textstyle\sum_{i,j=0}^{l-1} \alpha_{i,j} (G^{\bar{n}})^i \left| v^{\bar{n}} \right\rangle \left\langle v^{\bar{n}} \right| (G^{\bar{n}})^j. \end{aligned} \tag{15}$$

Indeed, by induction we can prove that equation (15) holds for all l.
The base of the induction $l = 1$ immediately gives us equation (14), which holds.
For the $l+1$ instance, the Weingarten Iteration Map gives us:

$$\begin{aligned} \left| v^{\overline{n-l-1}} \right\rangle &= \left| v^{\overline{n-l}} \right\rangle - \tfrac{\langle G^{\overline{n-l}} \rangle}{\langle (G^{\overline{n-l}})^2 \rangle} (G^{\overline{n-l}}) \left| v^{\overline{n-l}} \right\rangle \\ (G^{\overline{n-l-1}})^{\dashv} &= (G^{\overline{n-l}})^{\dashv} - \tfrac{\left| v^{\overline{n-l}} \right\rangle \left\langle v^{\overline{n-l}} \right|}{\langle G^{\overline{n-l}} \rangle}. \end{aligned} \tag{16}$$

Replacing $G^{\overline{n-l}}$ and $\left| v^{\overline{n-l}} \right\rangle$ from equation (15), we get

$$\begin{aligned} \left| v^{\overline{n-l-1}} \right\rangle &= \textstyle\sum_{i=0}^{l+1} \alpha_i (G^{\bar{n}})^i \left| v^{\bar{n}} \right\rangle \\ (G^{\overline{n-l-1}})^{\dashv} &= (G^{\bar{n}}) + \textstyle\sum_{i,j=0}^{l} \alpha_{i,j} (G^{\bar{n}}) \left| v^{\bar{n}} \right\rangle \left\langle v^{\bar{n}} \right| (G^{\bar{n}})^j, \end{aligned} \tag{17}$$

which concludes our inductive proof.

Now that we proved that equation (15) holds for any l, we can proceed to the corresponding expectation value:

$$\begin{aligned} \langle (G^{\overline{n-l}})^{\dashv} \rangle = \left\langle v^{\overline{n-l}} \right| (G^{\overline{n-l}}) \left| v^{\overline{n-l}} \right\rangle = \textstyle\sum_{i,j=0}^{l} \alpha_i \alpha_j \left\langle v^{\bar{n}} \right| (G^{\bar{n}})^{i+j-1} \left| v^{\bar{n}} \right\rangle \\ + \textstyle\sum_{i=0}^{l} \left\langle v^{\bar{n}} \right| (G^{\bar{n}})^i \sum_{i',j'=0}^{l-1} \alpha_{i',j'} (G^{\bar{n}})^{i'} \left| v^{\bar{n}} \right\rangle \left\langle v^{\bar{n}} \right| (G^{\bar{n}})^{j'} \sum_{j=0}^{l} \alpha_j (G^{\bar{n}})^j \left| v^{\bar{n}} \right\rangle, \end{aligned} \tag{18}$$

where we have used $(G^{\bar{n}})^{\dashv} = (G^{\bar{n}})^{-1}$, since $G^{\bar{n}}$ is full rank.
We observe that the minimum power in the expectation value is $\langle (G^{\bar{n}}) \rangle$, while the maximum is $\langle (G^{\bar{n}})^{2l-1} \rangle$. Recall though (from previous Lemma) that in the multiplicative factors α_i and $\alpha_{i,j}$ there are higher powers in the expectation values $\langle (G^{\bar{n}})^{2l+1} \rangle$, which from now on will be the highest. Since we are iterating with respect to $G^{\dashv}$ the powers are not growing anymore, but they rather decrease and we are interested on the minimum powers that are reduced at each iteration. □

Lemma 50. *Consider the extended matrix instance* $\underline{\tilde{M}}^{\bar{\bar{n}}} := \mathscr{U}((H^{\bar{n}})^{\dashv}, (G^{\bar{n}})^{\dashv}, \left| \tilde{w}^{\bar{n}} \right\rangle, \left| \tilde{v}^{\bar{n}} \right\rangle, H^{\bar{n}}, G^{\bar{n}}, |.\rangle, |.\rangle)$. *Suppose the Normal Initialisation Map and the Weingarten Iteration Map (see Definition 11 and Definition 12) are applied k times to obtain* $\underline{\tilde{M}}^{\overline{n-k}}$, *viz. applying* $\underline{\tilde{M}}^{\overline{i-1}} = \mathscr{U}(\mathscr{W}(\underline{\tilde{M}}^{\dot{i}}))$ *k times. Then, for any k, the expectation value* $\left\langle \tilde{v}^{\overline{d-k}} \right| \tilde{G}^{\overline{d-k}} \left| \tilde{v}^{\overline{d-k}} \right\rangle$ *is a function of the expectation values* $\left\langle v^{\bar{n}} \right| (G^{\bar{n}})^p \left| w^{\bar{n}} \right\rangle = \langle (G^{\bar{n}})^p \rangle$, *where the minimum power p that might appear is $-(2k+1)$. The corresponding statement involving Hs and $|w\rangle$s also holds.*

Proof. The first iteration gives:

$$\left|\tilde{v}^{\overline{d-1}}\right\rangle = \left|\tilde{v}^{\bar{d}}\right\rangle - \frac{\langle\tilde{G}^{\bar{d}}\rangle}{\langle(\tilde{G}^{\bar{d}})^2\rangle}\tilde{G}^{\bar{d}}\left|\tilde{v}^{d}\right\rangle$$
$$\tilde{G}^{\overline{d-1}} = \tilde{G}^{\bar{d}} + \frac{\langle(\tilde{G}^{\bar{d}})^3\rangle}{\langle(\tilde{G}^{\bar{d}})^2\rangle^2}\tilde{G}^{\bar{d}}\left|\tilde{v}^{\bar{d}}\right\rangle\left\langle\tilde{v}^{\bar{d}}\right|\tilde{G}^{\bar{d}} - \frac{1}{\langle(\tilde{G}^{\bar{d}})^2\rangle}\left(\tilde{G}^{\bar{d}}\left|\tilde{v}^{\bar{d}}\right\rangle\left\langle\tilde{v}^{\bar{d}}\right|(\tilde{G}^{\bar{d}})^2 + (\tilde{G}^{\bar{d}})^2\left|\tilde{v}^{\bar{d}}\right\rangle\left\langle\tilde{v}^{\bar{d}}\right|\tilde{G}^{\bar{d}}\right). \tag{19}$$

Continuing for k iterations, we can prove by induction that:

$$\left|\tilde{v}^{\overline{d-k}}\right\rangle = \sum_{i=0}^{k}\alpha_i(G^{\bar{n}})^{i-k}\left|v^{\bar{n}}\right\rangle$$
$$\tilde{G}^{\overline{d-k}} = (G^{\bar{n}})^{-1} + \sum_{i,j=0}^{k}\alpha_{i,j}(G^{\bar{n}})^{i-(k+1)}\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^{j-(k+1)}. \tag{20}$$

Indeed, the base of the induction $k = 1$ gives us equation (19), which holds.
For $k + 1$, we obtain:

$$\left|\tilde{v}^{\overline{d-k-1}}\right\rangle = \left|\tilde{v}^{\overline{d-k}}\right\rangle - \frac{\langle\tilde{G}^{\overline{d-k}}\rangle}{\langle(\tilde{G}^{\overline{d-k}})^2\rangle}\tilde{G}^{\overline{d-k}}\left|\tilde{v}^{\overline{d-k}}\right\rangle$$
$$\tilde{G}^{\overline{d-k-1}} = \tilde{G}^{\overline{d-k}} + \frac{\langle(\tilde{G}^{\overline{d-k}})^3\rangle}{\langle(\tilde{G}^{\overline{d-k}})^2\rangle^2}\tilde{G}^{\overline{d-k}}\left|\tilde{v}^{\overline{d-k}}\right\rangle\left\langle\tilde{v}^{\overline{d-k}}\right|\tilde{G}^{\overline{d-k}} - \frac{1}{\langle(\tilde{G}^{\overline{d-k}})^2\rangle}\left(\tilde{G}^{\overline{d-k}}\left|\tilde{v}^{\overline{d-k}}\right\rangle\left\langle\tilde{v}^{\overline{d-k}}\right|(\tilde{G}^{\overline{d-k}})^2 + (\tilde{G}^{\overline{d-k}})^2\left|\tilde{v}^{\overline{d-k}}\right\rangle\left\langle\tilde{v}^{\overline{d-k}}\right|\tilde{G}^{\overline{d-k}}\right).$$

Substituting $\left|\tilde{v}^{\overline{d-k}}\right\rangle$ and $\tilde{G}^{\overline{d-k}}$ from equation (20), we get:

$$\left|\tilde{v}^{\overline{d-k-1}}\right\rangle = \sum_{i=0}^{k+1}\alpha_i(G^{\bar{n}})^{i-k-1}\left|v^{\bar{n}}\right\rangle$$
$$\tilde{G}^{\overline{d-k-1}} = (G^{\bar{n}})^{-1} + \sum_{i,j=0}^{k+1}\alpha_{i,j}(G^{\bar{n}})^{i-k-2}\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^{j-k-2}, \tag{21}$$

which confirms that equation (20) holds for all k.
Thus, for any k the corresponding expectation value can be written as:

$$\left\langle\tilde{v}^{\overline{d-k}}\right|\tilde{G}^{\overline{d-k}}\left|\tilde{v}^{\overline{d-k}}\right\rangle = \sum_{i=0}^{k}\alpha_i\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^{i-k}(G^{\bar{n}})^{-1}\sum_{j=0}^{k}\alpha_j(G^{\bar{n}})^{j-k}\left|v^{\bar{n}}\right\rangle$$
$$+\sum_{i=0}^{l+k}\alpha_i\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^{i-k}\sum_{i',j'=0}^{k}\alpha_{i',j'}(G^{\bar{n}})^{i'-(k+1)}\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^{j'-(k+1)}\sum_{j=0}^{k}\alpha_j(G^{\bar{n}})^{j-k}\left|v^{\bar{n}}\right\rangle. \tag{22}$$

We observe that the minimum power that can appear in the expectation values is $-(2k+1), \forall k$. Recall that the multiplicative factorsα_i and $\alpha_{i,j}$, also contain terms of the form $\langle(G^{\bar{n}})^p\rangle$, which behave as explained in the previous lemmas. □

Lemma 51. *Consider the matrix instance $\underline{X}^{\bar{n}} := (H^{\bar{n}}, G^{\bar{n}}, \left|w^{\bar{n}}\right\rangle, \left|v^{\bar{n}}\right\rangle)$. Using the Weingarten Iteration Map once, we obtain:*

$$\left|v^{\overline{n-1}}\right\rangle = \left|v^{\bar{n}}\right\rangle - \frac{\langle G^{\bar{n}}\rangle}{\langle(G^{\bar{n}})^2\rangle}G^{\bar{n}}\left|v^{\bar{n}}\right\rangle$$
$$G^{\overline{n-1}} = G^{\bar{n}} + \frac{\langle(G^{\bar{n}})^3\rangle}{\langle(G^{\bar{n}})^2\rangle^2}G^{\bar{n}}\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|G^{\bar{n}} - \frac{1}{\langle(G^{\bar{n}})^2\rangle}\left(G^{\bar{n}}\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^2 + (G^{\bar{n}})^2\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|G^{\bar{n}}\right). \tag{23}$$

Then, for any power m, the expectation value $\left\langle v^{\overline{n-1}}\right|(G^{\overline{n-1}})^m\left|v^{\overline{n-1}}\right\rangle$ can be expressed in terms of the expectation values $\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^p\left|v^{\bar{n}}\right\rangle = \langle(G^{\bar{n}})^p\rangle$ with p being at most $m + 2$. The corresponding statement involving Hs and $|w\rangle$s also holds.

Proof. The first step is to prove that for any power m:

$$(G^{\overline{n-1}})^m = (G^{\bar{n}})^m + \sum_{i,j=0}^{m+1}\alpha_{i,j}(G^{\bar{n}})^i\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^j \tag{24}$$

Note that some of the $\alpha_{i,j}$ can be zero.
Indeed, we can use induction to prove equation (24).
The base of the induction $m = 1$ gives us equation (23), which holds.
Then, the power $m + 1$ is:

$$(G^{\overline{n-1}})^{m+1} = (G^{\overline{n-1}})^m \cdot G^{\overline{n-1}}, \tag{25}$$

and substituting from equation (23) and equation (24), we get:

$$(G^{\overline{n-1}})^{m+1} = \left[(G^{\bar{n}})^m + \sum_{i,j=0}^{m+1}\alpha_{i,j}(G^{\bar{n}})^i\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^j\right]\cdot\left[G^{\bar{n}} + \frac{\langle(G^{\bar{n}})^3\rangle}{\langle(G^{\bar{n}})^2\rangle^2}G^{\bar{n}}\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|G^{\bar{n}} - \frac{1}{\langle(G^{\bar{n}})^2\rangle}\left(G^{\bar{n}}\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^2 + (G^{\bar{n}})^2\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|G^{\bar{n}}\right)\right]$$
$$= (G^{\bar{n}})^{m+1} + \sum_{i,j=0}^{m+2}\alpha_{i,j}(G^{\bar{n}n})^i\left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^j,$$

which proves that equation (24) holds for all m.
With this in place, we can proceed to prove our main claim about the corresponding expectation value:

$$\begin{aligned}\left\langle v^{\overline{n-1}}\right| (G^{\overline{n-1}})^m \left|v^{\overline{n-1}}\right\rangle &= \left(\left\langle v^{\bar{n}}\right| - \tfrac{\langle G^{\bar{n}}\rangle}{\langle (G^{\bar{n}\,n})^2\rangle}\left\langle v^{\bar{n}}\right| G^{\bar{n}}\right)\left((G^{\bar{n}})^m + \textstyle\sum_{i,j=0}^{m+1}\alpha_{i,j}(G^{\bar{n}})^i \left|v^{\bar{n}}\right\rangle\left\langle v^{\bar{n}}\right|(G^{\bar{n}})^j\right)\left(\left|v^{\bar{n}}\right\rangle - \tfrac{\langle G^{\bar{n}}\rangle}{\langle (G^{\bar{n}})^2\rangle} G^{\bar{n}}\left|v^{\bar{n}}\right\rangle\right)\\ &= \langle (G^{\bar{n}\,n})^m\rangle + a\langle (G^{\bar{n}})^{m+1}\rangle + b\langle (G^{\bar{n}})^{m+2}\rangle + \textstyle\sum_{i,j=0}^{m+2}\alpha_{i,j}\langle (G^{\bar{n}})^i\rangle\langle (G^{\bar{n}})^j\rangle\\ &= \textstyle\sum_{i,j=0}^{m+2}\alpha'_{i,j}\langle (G^{\bar{n}})^i\rangle\langle (G^{\bar{n}})^j\rangle,\end{aligned}$$

which completes our proof that the highest power that can appear is $m+2$ for any m. Notice that we did not fully specified the scalar factors $a, b, \alpha_{i,j}, \alpha'_{i,j}$, as it is easy to verify that they do not contain any higher powers. □