

On multivariate polynomials achievable with quantum signal processing

Lorenzo Laneve and Stefan Wolf

Faculty of Informatics — Università della Svizzera Italiana, 6900 Lugano, Switzerland

Quantum signal processing (QSP) is a framework which was proven to unify and simplify a large number of known quantum algorithms, as well as discovering new ones. QSP allows one to transform a signal embedded in a given unitary using polynomials. Characterizing which polynomials can be achieved with QSP protocols is an important part of the power of this technique, and while such a characterization is well-understood in the case of univariate signals, it is unclear which multivariate polynomials can be constructed when the signal is a vector, rather than a scalar. This work uses a slightly different formalism than what is found in the literature, and uses it to find simpler necessary conditions for decomposability, as well as a sufficient condition — the first, to the best of our knowledge, proven for a (generally inhomogeneous) multivariate polynomial in the context of quantum signal processing.

1 Introduction

Devising quantum algorithms is a crucial task to understand the potential applications of quantum hardware. For this purpose, a set of composable techniques allows to tackle new problems with relative ease. Notable techniques are amplitude-amplification schemes [1, 2], linear combination of unitaries [3], phase-estimation methods [4], quantum walks [5, 6, 7], and techniques based on query complexity [8, 9, 10].

Recent research developed a novel framework called *quantum signal processing* (QSP for short) [11, 12] which was shown to unify and simplify a good part of the aforementioned techniques, and beyond [13, 14]. The idea of this framework is quite simple: we have a *signal* z (typically a complex number of unitary modulus) embedded in a single-qubit *signal operator* (e.g., z is contained in the entries of the matrix). By intertwining calls to this unitary with single-qubit operations (independent of z), matrix multiplication gives us a state that is a polynomial in z . By a simple tweak (involving phase kickback and Jordan’s lemma [15]), one can decompose a high-dimensional unitary U into a direct sum of small subspaces, in which U acts like the signal operator. Within each of these subspaces, we can make z coincide with the eigenvalues of U or the singular values of a matrix *block-encoded* (e.g., the top-left block) in U . This construction allows to use QSP to transform the eigenvalues or singular values of matrices given as quantum circuits, using the polynomials implemented with the QSP protocol [16, 17, 13].

The power of this technique is that any polynomial satisfying some mild conditions is implementable by a QSP construction — employing a single control qubit —, and we can simply specify an algorithm in terms of the polynomials we would like to apply. Notable

Lorenzo Laneve: lorenzo.laneve@usi.ch

examples of such conceptual simplification are block-encoded matrix inversion [18], phase estimation based on binary search [14], Hamiltonian simulation [17, 19, 20], and state preparation [21, 22].

Given its success, recent efforts push towards efficient numerical computation of the protocol given a desired polynomial [23, 24, 25, 26, 27, 28], generally composable paradigms for quantum algorithms [29, 30], as well as extensions of the QSP ansatz to different algebras [23, 31, 32, 33, 34].

Among the possible extensions of the model, a version of QSP implementing *multivariate* polynomials was proposed [35]. In this case, the signal is a vector $\mathbf{z}$ where each component is encoded in different signal operators, and the protocol chooses which operator to call at each step. Unfortunately, while nearly any univariate polynomial can be implemented by some QSP protocol, there are some multivariate polynomials — even with a degree as small as 4 — that do not admit such decomposition [36]. A multivariate variant of QSP (M-QSP for short) is quite enticing: applications include computation of functions of commuting matrices [37], and multivariate Monte Carlo estimation (e.g., following the QSVT-based quantum state preparation scheme of [21]).

A lack of characterization of the polynomials decomposable with M-QSP protocols limits the usability of this construction, therefore finding necessary and/or sufficient conditions for applicability is crucial. This work aims at giving further progress on this task.

We use a slightly different formulation of QSP (also used in [33]) to consider a M-QSP protocol acting on a larger, three-dimensional Hilbert space (which we conjecture to be equivalent to the already-known single-qubit protocol for the class of single-qubit QSP polynomials). This enlarged protocol is a bit easier to work with (since no classical choice is involved in the protocol), and we take advantage of this to derive new, easy-to-check conditions for the (im)possibility to construct a given polynomial. We also prove that some polynomials cannot even be approximated to arbitrary precision by a sequence of constructible polynomials.

The remainder of this work is structured as follows: Section 2 starts by giving an overview of the variants of univariate QSP found across the literature, to show equivalences and connections with the protocols we are going to analyze. We then proceed with multivariate QSP in Section 3, briefly showing the protocol proposed in [35, 38], and extending it to its *analytic* variant. Section 4 then introduces the aforementioned protocol on three dimensions, proving that it contains the first one, and conjecturing (with motivations) that also the converse holds (Section 4.1). We then give a simple necessary and sufficient condition for the existence of a single protocol step that lowers the degree of a given polynomial (needed for induction arguments), extending the conditions stated in [35, 38] (Section 4.2). In Section 4.3, we prove that *any* bivariate polynomial $|\gamma(a, b)\rangle$ having non-zero coefficients for $1, a^n, b^n$ can be implemented using our three-dimensional version of M-QSP. To the best of our knowledge, this is the first result that provides a sufficient condition for full M-QSP decomposability. We conclude the work by quantifying the inapproximability of a polynomial (i.e., the best possible error guaranteed by an implementable polynomial to approximate a non-implementable one), also giving a more operational way to conclude the impossibility of a given polynomial (Section 4.4).

1.1 Preliminaries

We denote with $\mathbb{T}$ the complex unit circle, i.e., the set of complex numbers z with $|z| = 1$. A *Laurent* polynomial is a function $P(z) = \sum_{k=-n}^n p_k z^k$, i.e., a polynomial whose terms can also have negative exponents. We sometimes use the term *analytic* polynomial (term taken from complex analysis), to denote usual polynomials with only non-negative expo-

nents. Symbols written in bold represent vectors: given two vectors $\mathbf{z} = (z_1, \dots, z_m)$, $\mathbf{k} = (k_1, \dots, k_m)$, we write $\mathbf{z}^{\mathbf{k}}$, as a shorthand for $z_1^{k_1} \dots z_m^{k_m}$. We also use the bra-ket notation to denote not only quantum states, but also any non-normalized (possibly zero) vector of amplitudes. We use X, Y, Z, H to denote the three Pauli matrices and the single-qubit Hadamard gate, respectively. The notation $[d]$ represents the set $\{0, \dots, d-1\}$.

2 Univariate quantum signal processing

In quantum signal processing, the aim is to transform a signal embedded in a unitary with a polynomial. In the end, this task boils down to constructing a so-called *polynomial state*.

Definition 1. A *polynomial state* $|\gamma(\mathbf{z})\rangle$ is a polynomial vector in $\mathbf{z} \in \mathbb{T}^m$ that satisfies $\langle \gamma(\mathbf{z}) | \gamma(\mathbf{z}) \rangle \equiv 1$.

Generally, we have two ways to express a polynomial state of dimension d (for now we will restrict ourselves to the case $d = 2$, i.e., single-qubit polynomials): the first one is simply a vector whose entries are polynomials,

$$|\gamma(\mathbf{z})\rangle = \sum_{x=0}^{d-1} P_x(\mathbf{z}) |x\rangle, \quad (1)$$

where the normalization condition can be rewritten as $\sum_{x=0}^{d-1} |P_x(\mathbf{z})|^2 \equiv 1$. This representation is mainly used in applications of QSP. The second one decomposes the state as a single (vector) polynomial

$$|\gamma(\mathbf{z})\rangle = \sum_{\mathbf{k}} |\gamma_{\mathbf{k}}\rangle \mathbf{z}^{\mathbf{k}}.$$

Here $|\gamma_{\mathbf{k}}\rangle$ are the coefficients of the polynomial, which are d -dimensional vectors. This decomposition will be useful for us in this work, as we will see that many properties are more easily expressed in terms of these vectors. In this section, we recap the univariate case, which is fully characterized and well-understood in the literature [14, 23, 32]. For a signal $z \in \mathbb{T}$, we define the Laurent *signal operator*

$$\tilde{v}(z) = \begin{bmatrix} z^{-1} & 0 \\ 0 & z \end{bmatrix}$$

where we usually omit the dependency on z for simplicity. A QSP protocol now is a sequence of calls to the signal operator $\tilde{v}$ intertwined with a sequence of unitary operators which we call *signal processing operators*, or simply *processing operators*. Different variants of QSP are possible (allowing construction of polynomials requiring different criteria) by simply choosing the basis of $\tilde{v}$ and the domain of the processing operators.

Theorem 2 (Laurent QSP in the W_z convention [23, 14]). *Let $|\gamma(z)\rangle$ be a two-dimensional Laurent polynomial state of degree n , i.e.,*

$$|\gamma(z)\rangle = P(z)|0\rangle + Q(z)|1\rangle$$

where $P, Q \in \mathbb{C}[z, z^{-1}]$ are Laurent polynomials of degree n . There exists a vector of $n+1$ phases $\phi_0, \phi_1, \dots, \phi_n \in [0, 2\pi)$ such that

$$e^{i\phi_n X} \tilde{v} e^{i\phi_{n-1} X} \tilde{v} \dots \tilde{v} e^{i\phi_0 X} |0\rangle = |\gamma(z)\rangle$$

if and only if:

- (i) $P(z)$ has real coefficients and $Q(z)$ has imaginary coefficients;
- (ii) P, Q have parity $n \bmod 2$.

This was called the W_z in [14], since the signal operator (which they called $W(\theta)$) can be seen as a Z rotation. The following variant is called W_x for obvious reasons.

Theorem 3 (Laurent QSP in the W_x convention [14]). *Let $|\gamma(z)\rangle$ be a two-dimensional Laurent polynomial state of degree n , i.e.,*

$$|\gamma(z)\rangle = P(z)|0\rangle + Q(z)|1\rangle$$

where $P, Q \in \mathbb{C}[z, z^{-1}]$ are Laurent polynomials of degree n . There exists a vector of $n+1$ phases $\phi_0, \phi_1, \dots, \phi_n \in [0, 2\pi)$ such that

$$e^{i\phi_n Z} H \tilde{v} H e^{i\phi_{n-1} Z} H \tilde{v} H \dots H \tilde{v} H e^{i\phi_0 Z} |0\rangle = |\gamma(z)\rangle$$

if and only if:

- (i) $P(z) = P(z^{-1})$ and $Q(z) = -Q(z^{-1})$ for every $z \in \mathbb{T}$;
- (ii) P, Q have parity $n \bmod 2$.

A simple conjugation of a W_x protocol with a Hadamard gate gives a W_z protocol (and vice versa). Note that the conjugated signal operator

$$H \tilde{v} H = \frac{1}{2} \begin{bmatrix} z^{-1} + z & z^{-1} - z \\ z^{-1} - z & z^{-1} + z \end{bmatrix} = \begin{bmatrix} x & -i\sqrt{1-x^2} \\ -i\sqrt{1-x^2} & x \end{bmatrix}$$

can be rewritten by replacing $x = (z + z^{-1})/2$, giving us the traditional version of quantum signal processing [11, 12], from which the quantum singular value transformation can be obtained [13, 39]. If, instead of X or Z rotations, we allow the signal-processing operators to be arbitrary unitaries in $SU(2)$, then condition (i) in both the previous theorems will lift (they are actually two subalgebras of a bigger algebra [24, 32]). We remark that using arbitrary $SU(2)$ operators does not increase the complexity of the circuit significantly, as any $SU(2)$ element can be rewritten using Euler's decomposition:

$$U = e^{i\alpha Z} e^{i\beta X} e^{i\gamma Z} \quad \alpha, \beta, \gamma \in [0, 2\pi).$$

Indeed, this decomposition, along with the fact that Z rotations commute with $\tilde{v}$, yields the protocol with double rotations of [32] (this also suggests that we do not even need the full $SU(2)$ to remove condition (i)).

We now consider a different, but more intuitive version, recently introduced in [32], which considers the following *analytic* signal operator

$$\tilde{w}(z) = \begin{bmatrix} 1 & 0 \\ 0 & z \end{bmatrix}.$$

By intertwining this operator with processing operators, we obtain a similar result.

Theorem 4 (Analytic QSP in the W_z convention [32]). *Let $|\gamma(z)\rangle$ be a two-dimensional polynomial state of degree n , i.e.,*

$$|\gamma(z)\rangle = P(z)|0\rangle + Q(z)|1\rangle$$

where $P, Q \in \mathbb{C}[z, z^{-1}]$ are polynomials of degree n . There exists a vector of $n+1$ phases $\phi_0, \phi_1, \dots, \phi_n \in [0, 2\pi)$ such that

$$e^{i\phi_n X} \tilde{w} e^{i\phi_{n-1} X} \tilde{w} \dots \tilde{w} e^{i\phi_0 X} |0\rangle = |\gamma(z)\rangle$$

if and only if:

(i) $P(z)$ has real coefficients and $Q(z)$ has imaginary coefficients for every $z \in \mathbb{T}$.

Notice how condition (ii) does not appear in analytic QSP. Indeed the constraint of definite parity is only due to the fact that in $\tilde{v}$ there is a distance of two degrees between z, z^{-1} . Similarly as with Laurent QSP, if we extend signal operators to any $SU(2)$ operator, then we would lift condition (i), implying that any analytic polynomial state can be obtained. The following result shows that there is no substantial difference between the Laurent and analytic variants.

Lemma 5 (Analytic-Laurent correspondence). *Consider a definite-parity Laurent polynomial state $|\gamma(z)\rangle$*

$$|\gamma(z)\rangle = |\gamma_{-n}\rangle z^{-n} + |\gamma_{-n+2}\rangle z^{-n+2} + \cdots + |\gamma_{n-2}\rangle z^{n-2} + |\gamma_n\rangle z^n$$

where $|\gamma_k\rangle$ are the coefficients of the polynomial. Then $|\gamma(z)\rangle$ is implemented by the Laurent QSP protocol

$$A_n \tilde{v} A_{n-1} \tilde{v} \cdots \tilde{v} A_0 |0\rangle = |\gamma(z)\rangle$$

for some sequence $\{A_k\}_k \in SU(2)$ of processing operators if and only if the analytic polynomial

$$|\gamma^a(z)\rangle = |\gamma_{-n}\rangle + |\gamma_{-n+2}\rangle z + \cdots + |\gamma_{n-2}\rangle z^{n-1} + |\gamma_n\rangle z^n$$

is implemented by the analytic QSP protocol

$$A_n \tilde{w} A_{n-1} \tilde{w} \cdots \tilde{w} A_0 |0\rangle = |\gamma^a(z)\rangle.$$

Proof. By the fact that $\tilde{v}(z) = z^{-1} \tilde{w}(z^2)$, replacing the former with the latter in the protocol gives the Laurent polynomial $z^{-n} |\gamma^a(z^2)\rangle$. If we multiply by z^n and replace $\tilde{w}(z^2)$ with $\tilde{w}(z)$, we obtain the desired polynomial. The converse can be obtained by following the argument in reverse. $\square$

Lemma 5 gives a clear one-to-one correspondence between the classes of analytic and Laurent polynomials achievable with QSP, i.e., understanding polynomials of either variant immediately implies a clear characterization on the other. This result is important as it allows us to work with the analytic variant, which is a bit easier to visualize in the subsequent sections: a useful advantage is that the degree of an analytic polynomial state being constructed with a QSP protocol only grows on one side. We remark that conditions (i) in the claims above will be preserved/converted to the counterpart in the other variant (see Table 1 for a overview of the univariate versions and their conditions).

3 Multivariate quantum signal processing

We now talk about the multivariate version of quantum signal processing. Here, the polynomial states $|\gamma(\mathbf{z})\rangle$ we want to construct transform a signal $\mathbf{z} \in \mathbb{T}^m$.

Protocol A (Laurent multivariate QSP with classical choice [35, 38]). Given a vector of phases $\mathbf{z} \in \mathbb{T}^m$, let $\tilde{v}_k = \tilde{v}(z_k) = \text{diag}(z_k^{-1}, z_k)$. Fixing a vector of choices $\mathbf{s} \in [m]^n$, the following protocol constructs a Laurent multivariate polynomial state

$$A_n \tilde{v}_{s_n} A_{n-1} \tilde{v}_{s_{n-1}} \cdots \tilde{v}_{s_1} A_0 |0\rangle = |\gamma(\mathbf{z})\rangle = P(\mathbf{z})|0\rangle + Q(\mathbf{z})|1\rangle$$

	Laurent picture [23] $\tilde{v} = \text{diag}(z^{-1}, z)$	Analytic picture [32] $\tilde{w} = \text{diag}(1, z)$
W_x convention	(i) $P(z) = P(z^{-1})$ $Q(z) = -Q(z^{-1})$ (ii) P, Q have parity $n \bmod 2$	(i) $P(z) = z^n P(z^{-1})$ $Q(z) = -z^n Q(z^{-1})$
W_z convention	(i) $P(z) \in \mathbb{R}[z, z^{-1}]$ $Q(z) \in i\mathbb{R}[z, z^{-1}]$ (ii) P, Q have parity $n \bmod 2$	(i) $P(z) \in \mathbb{R}[z]$ $Q(z) \in i\mathbb{R}[z]$
Full algebra	(i) P, Q have parity $n \bmod 2$	No additional constraints.

Table 1: Overview of the variants of univariate QSP found across the literature, with the full characterizations of the polynomial states $|\gamma(z)\rangle = P(z)|0\rangle + Q(z)|1\rangle$.

In this protocol, we follow exactly the same idea as in the univariate case, where at each step we choose a variable z_k and we apply the signal operator $\tilde{v}(z_k)$. Let n_k be the number of times k appears in $\mathbf{s}$. Necessary conditions for a polynomial state $|\gamma(\mathbf{z})\rangle$ to be implemented with Protocol A are [38]:

- (i) for every $k \in [m]$, the degree of $|\gamma(\mathbf{z})\rangle$ with respect to z_k , i.e., the maximum power of z_k with a non-zero coefficient vector, is at most n_k ;
- (ii) for every $k \in [m]$, $|\gamma(\mathbf{z})\rangle$ has parity $n_k \bmod 2$.

These conditions need to be satisfied even if the processing operators A_k are arbitrary $SU(2)$ operations. Furthermore, as in the univariate case, we have additional constraints if we restrict to a subset of signal processing operators:

- (iii^z) in the W_z convention, P must have real coefficients, and Q must have imaginary coefficients;
- (iii^x) in the W_x convention, $P(\mathbf{z}) = P(\mathbf{z}^{-1})$ and $Q(\mathbf{z}) = -Q(\mathbf{z}^{-1})$ for every choice of $\mathbf{z} \in \mathbb{T}^m$.

Moreover, it is possible to replace $\tilde{v}$ in Protocol A with $\tilde{w}$, thus obtaining an analytic version of this multivariate protocol.

Protocol B (Analytic multivariate QSP with classical choice). Given a vector of phases $\mathbf{z} \in \mathbb{T}^m$, let $\tilde{w}_k = \tilde{w}(z_k) = \text{diag}(1, z_k)$. With a vector of choices $\mathbf{s} \in [m]^n$, the following protocol constructs an analytic multivariate polynomial state

$$A_n \tilde{w}_{s_n} A_{n-1} \tilde{w}_{s_{n-1}} \cdots \tilde{w}_{s_1} A_0 |0\rangle = |\gamma(\mathbf{z})\rangle = P(\mathbf{z})|0\rangle + Q(\mathbf{z})|1\rangle$$

In the spirit of Lemma 5, whose argument is easily extended to the multivariate case, we will focus on characterizing this version.

4 A larger protocol

Unfortunately, the necessary conditions listed in the previous sections are not sufficient, as counterexamples in [36] show. Understanding which conditions are sufficient for implementability is certainly not an easy task. A condition highlighted in [38] for the W_z convention, is the following:

(iv^z) Let $\mathbf{z}_{-k}$ be obtained from $\mathbf{z}$ by removing z_k , and let $P_m(\mathbf{z}_{-k})$ be the coefficient of $P(\mathbf{z})$ of z_k^m (analogously for $Q_m(\mathbf{z}_{-k})$). There exists a k such that

$$P_{n_k}(\mathbf{z}_{-k}) \equiv e^{2\pi i \varphi} Q_{n_k}(\mathbf{z}_{-k}) .$$

If such condition holds, then one can choose $\mathbf{s}_n = k$ and the angle for the Z rotation in the processing operator to be φ . Undoing this last step on $|\gamma(\mathbf{z})\rangle$ will give a valid polynomial state with lower degree $|\gamma'(\mathbf{z})\rangle$, and the rest of the protocol could be extracted by induction. The problem, however, is that condition (iv) alone on $|\gamma(\mathbf{z})\rangle$ guarantees conditions (i)-(iii) to hold also for $|\gamma'(\mathbf{z})\rangle$, but it does not preserve condition (iv).

A huge problem of condition (iv) (besides the fact that it is only valid in the W_z convention) is that it is rather complicated to work with, as it requires the existence of *some* index k . Moreover, assuming that we have a polynomial that admits a protocol and we find at some point that more than one choice for k satisfies condition (iv), it is unclear whether any choice taken at this step will certainly lead to a full decomposition. In other words, how can we be sure that there are no “bad choices”?

Here we circumvent these structural problems by considering a slightly extended protocol (throughout this work we consider only two variables for simplicity, but we can in principle extend it to an arbitrary number).

Protocol C. Consider the following signal operator

$$\tilde{W} = \text{diag}(1, a, b)$$

We intertwine this operator with a sequence of processing operators $A_k \in SU(3)$ such that

$$A_n \tilde{W} A_{n-1} \tilde{W} \cdots \tilde{W} A_0 |0\rangle = |\gamma(a, b)\rangle .$$

Clearly, such protocol produces polynomial states of dimension 3 in general:

$$|\gamma(a, b)\rangle = P(a, b)|0\rangle + Q(a, b)|1\rangle + R(a, b)|2\rangle \quad (2)$$

4.1 Equivalence with the two-dimensional protocol

We want to restrict our attention to the polynomials of the form (2) satisfying $R(a, b) \equiv 0$. We give a formal and more comprehensive definition of this class of polynomials, which will be useful later.

Definition 6 (Effective dimension). A polynomial state $|\gamma(\mathbf{z})\rangle = \sum_{\mathbf{k}} |\gamma_{\mathbf{k}}\rangle \mathbf{z}^{\mathbf{k}}$ has *effective dimension* d if its coefficient vectors $|\gamma_{\mathbf{k}}\rangle$ span a subspace of dimension d . The same subspace is spanned by $\{|\gamma(\mathbf{z})\rangle\}_{\mathbf{z}}$.

States with $R(a, b) \equiv 0$ have effective dimension ≤ 2 . In fact, they are the only ones, up to a unitary transformation. Protocol B is a strict subset of Protocol C: we simply ignore the third dimension, choosing only processing operators of the form

$$A_k = \begin{bmatrix} A'_k & 0 \\ 0 & 1 \end{bmatrix} \quad (3)$$

where $A'_k \in SU(2)$ is the processing operator used in the two-dimensional protocol. In this way, $\tilde{W}$ will act as $\text{diag}(1, a)$ in $\text{span}\{|0\rangle, |1\rangle\}$. Whenever we choose the signal operator for b at some step, we simply use a permutation operation $S = |0\rangle\langle 0| + |1\rangle\langle 2| + |2\rangle\langle 1|$ so that $S\tilde{W}S = \text{diag}(1, b, a)$. Constraining the processing operators in this way certainly gives $R(a, b) \equiv 0$. We conjecture that also the converse is true.

Conjecture 7. *Let $|\gamma(a, b)\rangle = A_n \tilde{W} A_{n-1} \tilde{W} \cdots \tilde{W} A_0 |0\rangle$ be a construction following Protocol C. If $R(a, b) = \langle 2 | \gamma(a, b) \rangle \equiv 0$, there exist $A'_k \in SU(2)$ and permutation matrices S_k such that*

$$\begin{bmatrix} A'_n & 0 \\ 0 & 1 \end{bmatrix} S_n \tilde{W} S_n \begin{bmatrix} A'_{n-1} & 0 \\ 0 & 1 \end{bmatrix} S_{n-1} \tilde{W} S_{n-1} \cdots S_1 \tilde{W} S_1 \begin{bmatrix} A'_0 & 0 \\ 0 & 1 \end{bmatrix} |0\rangle = |\gamma(a, b)\rangle .$$

The resulting two-dimensional protocol is thus a sequence of the $SU(2)$ operators A'_k intertwined with calls to $\tilde{w}_a = \text{diag}(1, a)$, $\tilde{w}_b = \text{diag}(1, b)$, or $\tilde{w}_{ab} = \text{diag}(a, b)$, and we simply split $\tilde{w}_{ab} = X \tilde{w}_a X \tilde{w}_b$ to get the final construction compliant with Protocol B. To see why Conjecture 7 is not straightforward to prove, consider the following example:

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \xrightarrow{A'_0} \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \xrightarrow{\tilde{W}} \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ a \\ b \end{bmatrix} \xrightarrow{S\tilde{W}S} \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ ab \\ ab \end{bmatrix} \xrightarrow{A'_2} \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \sqrt{2}ab \\ 0 \end{bmatrix} .$$

The problem with this protocol is that the polynomial does not keep effective dimension 2 throughout the evolution, and thus cannot be directly translated to Protocol B. This, however, does not mean this is the only protocol achieving this polynomial; indeed the following does the trick:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \xrightarrow{A'_0} \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \sqrt{2} \end{bmatrix} \xrightarrow{\tilde{w}_a} \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \sqrt{2}a \end{bmatrix} \xrightarrow{\tilde{w}_b} \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ \sqrt{2}ab \end{bmatrix} .$$

As a general intuition, if a protocol applies a and b in superposition to two different subspaces $\mathcal{H}_a$ and $\mathcal{H}_b$, in order to return to effective dimension 2, the three polynomials need to become linearly dependent again at some point, which means that $\mathcal{H}_a$ will eventually receive also b and vice versa (in other words, a segment of the protocol will act as $a^k b^h \cdot \mathbb{1}$ on $\mathcal{H}_a \oplus \mathcal{H}_b$). If this is the case, then the same segment can be implemented by multiplying with a and b in two separate steps, always keeping the state in two dimensions. The final claim we could not prove in order to conclude Conjecture 7 is these situations are the only possible cases that prevent an immediate translation.

Conjecture 8. *Let $|\gamma(\mathbf{z})\rangle, |\gamma'(\mathbf{z})\rangle$ be polynomial states of effective dimension ≤ 2 such that*

$$|\gamma(\mathbf{z})\rangle = A_m \tilde{W} A_{m-1} \cdots A_1 \tilde{W} |\gamma'(\mathbf{z})\rangle$$

but any intermediate state has effective dimension > 2 . Then the operator

$$A_m \tilde{W} A_{m-1} \cdots A_1 \tilde{W}$$

acts as $a^k b^h \cdot U$ in some pair of subspaces $\mathcal{H} \rightarrow \mathcal{H}'$ of dimension $d \geq 2$, for some $U \in SU(d)$, $k, h \in \mathbb{N}$.

Conjecture 7 would follow directly, since every unitary of the form $a^k b^h \cdot U$ can be implemented trivially, keeping only polynomials with effective dimension 2 (here, the construction $U_1^\dagger \tilde{w}_a^k \tilde{w}_b^h X \tilde{w}_a^k \tilde{w}_b^h X U_2$ is an example of such protocol, where $U = U_1^\dagger U_2$ such that U_1, U_2 map our state within $\text{span}\{|0\rangle, |1\rangle\}$).

We highlight that Conjecture 8 becomes trivial when we replace the bound on the effective dimension above, from 2 to 1: such state would be of the form $a^k b^h |\psi\rangle$ for some quantum state $|\psi\rangle$ independent of a, b . We would necessarily have $|\gamma(\mathbf{z})\rangle = a^k b^h |\phi\rangle$, $|\gamma'(\mathbf{z})\rangle = a^{k'} b^{h'} |\psi\rangle$, with $k' \leq k, h' \leq h$ ($\tilde{W}$ cannot decrease the degree of the polynomial state). The claim follows by taking any $U : |\psi\rangle \mapsto |\phi\rangle$.

4.2 Conditions for extractability of one step

We now give some conditions for the existence of an instance of Protocol C to construct a given polynomial state $|\gamma(\mathbf{z})\rangle$. These conditions work for general three-dimensional polynomials, but we remember that in the case such polynomial has effective dimension 2 we can also retrieve a construction in the sense of Protocol B (provided Conjecture 7 holds).

Before we dive into stating necessary and/or sufficient conditions, we first provide an intuition on what happens throughout an evolution of Protocol C. We start from the state $A_0|0\rangle$, which is an arbitrary three-dimensional quantum state (in other words, the coefficient vector $|\gamma_{0,0}\rangle = A_0|0\rangle$, and $|\gamma_{\mathbf{k}}\rangle = 0$ for $\mathbf{k} \neq (0,0)$). An application of $\tilde{W}$ splits the space into the three components $\{|0\rangle, |1\rangle, |2\rangle\}$ of the computational basis, more explicitly

$$\tilde{W} \begin{bmatrix} \psi_0 \\ \psi_1 \\ \psi_2 \end{bmatrix} = \psi_0|0\rangle + \psi_1|1\rangle a + \psi_2|2\rangle b,$$

which means that, after one step, the coefficient vectors $|\gamma_{0,0}\rangle, |\gamma_{1,0}\rangle, |\gamma_{0,1}\rangle$ are pairwise orthogonal (the choice of the subsequent processing operator A_1 does not alter this fact). We can see the evolution of the coefficient vectors as propagation in a lattice (see Figure 1): after n steps, the points corresponding to non-zero coefficients form a right triangle with the two short sides of length n . Before applying A_n , we can see that the coefficient vectors satisfy the following conditions:

- $|\gamma_{k,0}\rangle \in \text{span}\{|0\rangle, |1\rangle\}$ for $0 \leq k \leq n$;
- $|\gamma_{0,k}\rangle \in \text{span}\{|0\rangle, |2\rangle\}$ for $0 \leq k \leq n$;
- $|\gamma_{k,n-k}\rangle \in \text{span}\{|1\rangle, |2\rangle\}$ for $0 \leq k \leq n$.

These three sets of vectors correspond to the three sides of the triangle in Figure 1. In particular, notice that the three endpoints of the triangle must satisfy two of these conditions, and in particular, they will be pairwise orthogonal.

Theorem 9 (Necessary and sufficient condition for the extraction of one step). *Let $|\gamma(a,b)\rangle = \sum_{k,h} |\gamma_{k,h}\rangle a^k b^h$ be a three-dimensional polynomial state of degree n . There exists $A_n \in SU(3)$ such that $\tilde{W}^\dagger A_n^\dagger |\gamma(a,b)\rangle$ has degree $n-1$ if and only if there exists an orthonormal basis $|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle$ such that*

- (i) $\langle \psi_2 | \gamma_{k,0} \rangle = 0$ for $0 \leq k \leq n$;
- (ii) $\langle \psi_1 | \gamma_{0,k} \rangle = 0$ for $0 \leq k \leq n$;
- (iii) $\langle \psi_0 | \gamma_{k,n-k} \rangle = 0$ for $0 \leq k \leq n$.

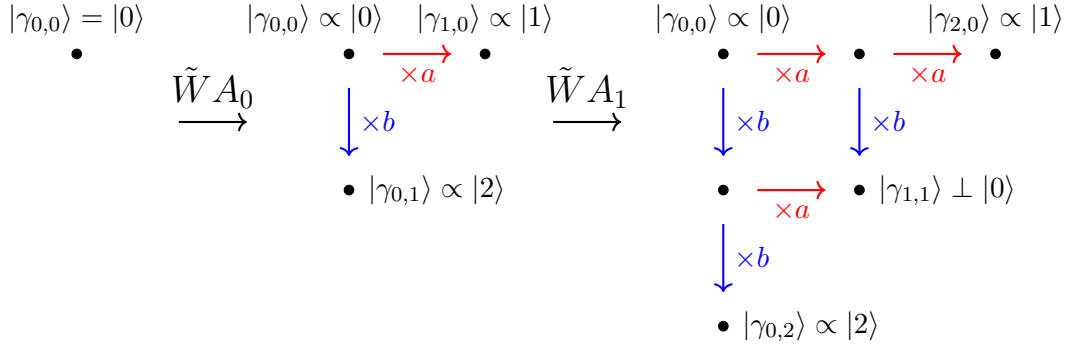


Figure 1: Evolution of the coefficient vectors of a three-dimensional polynomial state throughout two steps of Protocol C. The evolution can be visualized as a propagation on a two-dimensional lattice, where each point (x, y) corresponds to the coefficient vector of $a^x b^y$. Right after applying $\tilde{W}$, the coefficient vectors on the boundaries are proportional to an element of the computational basis. The processing operators A_k can change the basis of these vectors, but not the inner product between them.

If the three endpoints $|\gamma_{0,n}\rangle, |\gamma_{n,0}\rangle, |\gamma_{0,0}\rangle$ are non-zero, then the conditions above are equivalent to

$$(i') \quad \langle \gamma_{0,n} | \gamma_{k,0} \rangle = 0 \text{ for } 0 \leq k \leq n;$$

$$(ii') \quad \langle \gamma_{n,0} | \gamma_{0,k} \rangle = 0 \text{ for } 0 \leq k \leq n;$$

$$(iii') \quad \langle \gamma_{0,0} | \gamma_{k,n-k} \rangle = 0 \text{ for } 0 \leq k \leq n.$$

Proof. We have already shown condition (i)-(iii) to be necessary, we prove their sufficiency. The polynomial $|\gamma'(a, b)\rangle = \tilde{W}^\dagger A_n^\dagger |\gamma(a, b)\rangle$ has degree $n - 1$ if and only if $|\gamma'_{k,n-k}\rangle = 0$ for every $0 \leq k \leq n$ (higher-degree coefficients will be zero by construction). Moreover, we need $|\gamma'_{-1,k}\rangle = |\gamma'_{k,-1}\rangle = 0$ for $0 \leq k \leq n$ in order to have a valid analytic polynomial. Since $A_n^\dagger \sum_{k,h} |\gamma_{k,h}\rangle a^k b^h = \sum_{k,h} A_n^\dagger |\gamma_{k,h}\rangle a^k b^h$, this degree reduction will be guaranteed if the following conditions are true:

- $A_n^\dagger |\gamma_{k,0}\rangle \in \text{span}\{|0\rangle, |1\rangle\}$ for $0 \leq k \leq n$;
- $A_n^\dagger |\gamma_{0,k}\rangle \in \text{span}\{|0\rangle, |2\rangle\}$ for $0 \leq k \leq n$;
- $A_n^\dagger |\gamma_{k,n-k}\rangle \in \text{span}\{|1\rangle, |2\rangle\}$ for $0 \leq k \leq n$.

Taking $A_n : |j\rangle \mapsto |\psi_j\rangle$ satisfies this condition. Furthermore, conditions (i)-(iii) imply the following:

$$|\gamma_{0,n}\rangle \propto |\psi_2\rangle, \quad |\gamma_{n,0}\rangle \propto |\psi_1\rangle, \quad |\gamma_{0,0}\rangle \propto |\psi_0\rangle$$

because these three vectors must satisfy two of the three conditions (the only subtlety here is that they might be zero). If all of them are non-zero, then by conditions (i')-(iii') they are pairwise orthogonal, proving that also (i)-(iii) implies (i)-(iii). $\square$

These extend and simplify the necessary condition given in [36]. In the univariate case, conditions (i)-(iii) boil down to $\langle \gamma_0 | \gamma_n \rangle = 0$, i.e., the coefficient vectors at the two endpoints must be orthogonal (which is in turn guaranteed by the fact that $\langle \gamma(z) | \gamma(z) \rangle \equiv 1$). This allows to apply induction easily, proving Theorems 2-4. Unfortunately, unlike in the univariate case, the conditions of Theorem 9 are not sufficient for the existence of a

full protocol implementing $|\gamma(a, b)\rangle$: although $\tilde{W}^\dagger A_n^\dagger |\gamma(a, b)\rangle$ has lower degree, it is not guaranteed that the new polynomial in turn satisfies these conditions.

We apply our result to a concrete example (converted to analytic from [36]):

$$\begin{aligned} P(a, b) &= a^2 b^2 + 1 - \frac{122 + 8i}{37}(ab^2 + a) + \frac{362 - 248i}{111}(a^2 b + b) + \\ &\quad + \frac{114 + 56i}{37}(a^2 + b^2) + \left(\frac{692}{111} - \frac{719i}{222}\right) ab \\ Q(a, b) &= a^2 b^2 - 1 - \frac{122 + 66i}{37}(ab^2 - a) + \\ &\quad - \frac{56 + 114i}{37}(a^2 - b^2) + \frac{362 - 418i}{111}(a^2 b - b) \end{aligned}$$

Although $|\gamma(a, b)\rangle = P(a, b)|0\rangle + Q(a, b)|1\rangle$ is a polynomial state (up to a normalization factor), it does not satisfy the conditions of Theorem 9: the two sets of vectors $\{|\gamma_{0,1}\rangle, |\gamma_{0,2}\rangle\}, \{|\gamma_{1,0}\rangle, |\gamma_{2,0}\rangle\}$ are both linearly independent, and they span $\{|0\rangle, |1\rangle\}$. This means that there cannot exist $|\psi_2\rangle, |\psi_1\rangle$ satisfying conditions (i) and (ii) of Theorem 9 (they would need to be both $\propto |2\rangle$). We state the sufficient condition we just used for the non-implementability of a two-dimensional polynomial state more explicitly.

Corollary 10. *Let $|\gamma(a, b)\rangle = P(a, b)|0\rangle + Q(a, b)|1\rangle = \sum_{k,h} |\gamma_{k,h}\rangle a^k b^h$ be a polynomial state of degree n . If it holds that*

$$\text{span}\{|\gamma_{k,0}\rangle\}_k = \text{span}\{|\gamma_{0,k}\rangle\}_k = \text{span}\{|0\rangle, |1\rangle\},$$

then $|\gamma(a, b)\rangle$ cannot be implemented with Protocol C (and thus, not even with Protocol B).

This gives a very simple condition to check in order to prove the impossibility. An important remark is that this claim does not need Conjecture 7 to hold, since we proved that Protocol B is at least a subset of Protocol C.

4.3 A sufficient condition for decomposability

We use what we found in the previous section to first show a constructive result, i.e., a *sufficient* condition for the existence of an instance of Protocol C.

Theorem 11. *Let $|\gamma(a, b)\rangle = \sum_{k,h} |\gamma_{k,h}\rangle a^k b^h$ be a polynomial state of degree n such that the coefficient vectors $|\gamma_{0,0}\rangle, |\gamma_{n,0}\rangle, |\gamma_{0,n}\rangle$, i.e., the coefficients of $1, a^n, b^n$ are non-zero. Then there exist $A_0, \dots, A_n \in SU(3)$ such that*

$$A_n \tilde{W} A_{n-1} \tilde{W} \cdots \tilde{W} A_0 |0\rangle = |\gamma(a, b)\rangle.$$

Proof. The claim is trivial for $n = 0$, since any zero-degree polynomial is simply a quantum state $|\psi\rangle$, and any A_0 containing $|\psi\rangle$ as first column does the trick. Therefore, let us consider $n > 0$.

Since $|\gamma_{0,0}\rangle, |\gamma_{n,0}\rangle, |\gamma_{0,n}\rangle \neq 0$, the conditions (i')-(iii') of Theorem 9 must hold in order for a unitary A_n to lower the degree. This is actually guaranteed by the normalization condition:

$$\langle \gamma(\mathbf{z}) | \gamma(\mathbf{z}) \rangle = \sum_{\mathbf{k}, \mathbf{h}} \langle \gamma_{\mathbf{k}} | \gamma_{\mathbf{h}} \rangle \mathbf{z}^{\mathbf{h}-\mathbf{k}} = \sum_{\mathbf{j}} \sum_{\mathbf{k}} \langle \gamma_{\mathbf{k}} | \gamma_{\mathbf{k}+\mathbf{j}} \rangle \mathbf{z}^{\mathbf{j}} \stackrel{!}{=} 1$$

The coefficient of $\mathbf{z}^{\mathbf{j}}$ for $\mathbf{j} \neq 0$ must be zero. In particular

- by taking $\mathbf{j} = (k, -n)$, we obtain $\langle \gamma_{0,n} | \gamma_{k,0} \rangle = 0$, condition (i');
- by taking $\mathbf{j} = (-n, k)$, we obtain $\langle \gamma_{n,0} | \gamma_{0,k} \rangle = 0$, condition (ii');
- by taking $\mathbf{j} = (k, n-k)$, we obtain $\langle \gamma_{0,0} | \gamma_{k,n-k} \rangle = 0$, condition (iii').

Thus, by Theorem 9, there exists a unitary A_n such that $\tilde{W}^\dagger A_n^\dagger |\gamma(a, b)\rangle$ has degree $n-1$. In order to conclude the induction step we only need to prove that $1, a^{n-1}, b^{n-1}$ have a non-zero coefficient in the new polynomial. Consider $|\gamma'(a, b)\rangle = A_n^\dagger |\gamma(a, b)\rangle$. By linearity, $A_n^\dagger$ is simply applied to each $|\gamma_{k,h}\rangle$, thus the three endpoints are still non-zero after the application of $A_n^\dagger$. By considering $|\gamma'(a, b)\rangle = P(a, b)|0\rangle + Q(a, b)|1\rangle + R(a, b)|2\rangle$, since the degree of $|\gamma'(a, b)\rangle$ will be lowered by $\tilde{W}^\dagger$, this means that

- only P has the constant term, $|\gamma_{0,0}\rangle \propto |0\rangle$;
- only Q has the a^n term, $|\gamma_{n,0}\rangle \propto |1\rangle$;
- only R has the b^n term, $|\gamma_{0,n}\rangle \propto |2\rangle$.

As $\tilde{W}^\dagger$ simply shifts these coefficients, we can conclude that the polynomial $\tilde{W} |\gamma'(a, b)\rangle = \tilde{W}^\dagger A_n^\dagger |\gamma(a, b)\rangle$ has degree $n-1$, with the coefficients of $1, a^{n-1}, b^{n-1}$ being non-zero. This concludes the proof by applying the induction step. $\square$

Here we treat the case of two variables for simplicity, but it is possible to define a protocol on a $(d+1)$ -level system and d variables (we leave the full argument in Appendix A for completeness).

Example 12. Let $\omega = e^{2\pi i/3}$ be the cube root of unity and given $\vec{r} = (r_1, r_2, \dots, r_n) \in \mathbb{Z}_3^n$, we define its Fourier path as

$$f(\vec{r}) = \omega^{r_n r_{n-1} + r_{n-1} r_{n-2} + \dots + r_2 r_1}$$

Let $S_{k,h}$ be the set of all paths that have k occurrences of 1 and h occurrences of 2. We can define the triple of polynomials:

$$\begin{aligned} P(a, b) &= \sum_{k+h \leq n} \left(\sum_{\vec{r} \in S_{k,h}} f(\vec{r}) \right) a^k b^h \\ Q(a, b) &= \sum_{k+h \leq n} \left(\sum_{\vec{r} \in S_{k,h}} f(\vec{r}) \omega^{r_n} \right) a^k b^h \\ R(a, b) &= \sum_{k+h \leq n} \left(\sum_{\vec{r} \in S_{k,h}} f(\vec{r}) \omega^{2r_n} \right) a^k b^h \end{aligned}$$

In other words, the coefficients of $a^k b^h$ are summing the Fourier paths over all the possible choices containing k 1's and h 2's (the phase difference between P, Q, R can represent the $(n+1)$ -th choice). An induction argument on the paths can show that these polynomials sum up to 1 (up to an omitted multiplicative constant). Moreover, the sets $S_{n,0}, S_{0,n}$ and $S_{0,0}$ contain exactly one path, and therefore this triple satisfies the conditions of Theorem 11, which then gives an instance of Protocol C. It turns out that the processing operator are equal to the quantum Fourier transform over $\mathbb{Z}_3$, while A_0 prepares the state $(1, \omega^2, \omega^2)/\sqrt{3}$.

4.4 Inapproximability

Another result we can derive is a proof that some polynomial states are not only impossible to be implemented exactly, but they are even impossible to approximate with good precision by a QSP protocol.

Theorem 13. *Let $|\gamma(a, b)\rangle$ be a two-dimensional polynomial state of degree n . Consider:*

$$q(\gamma) = \min \left\{ \max_{0 \leq x, y \leq n} \left| \det \begin{bmatrix} |\gamma_{x,0}\rangle & |\gamma_{y,0}\rangle \end{bmatrix} \right|, \max_{0 \leq x, y \leq n} \left| \det \begin{bmatrix} |\gamma_{0,x}\rangle & |\gamma_{0,y}\rangle \end{bmatrix} \right| \right\}.$$

Any polynomial state $|\gamma'(a, b)\rangle$ satisfying $\| |\gamma(a, b)\rangle - |\gamma'(a, b)\rangle \| < q(\gamma)/2$ for any $a, b \in \mathbb{T}$ cannot be implemented.

This also gives a more practical method to check conditions of Theorem 10. Indeed, if $q(\gamma) > 0$ then both spans have dimension 2, and the polynomial cannot be implemented. However, this does not exclude that some non-implementable polynomials have $q(\gamma) = 0$ (indeed, taken any such polynomial $|\gamma(a, b)\rangle$, then $|\gamma'(a, b)\rangle = A\tilde{W}|\gamma(a, b)\rangle$, albeit impossible to construct, satisfies $q(\gamma') = 0$ regardless of $q(\gamma)$).

Proof. We show that such $|\gamma'(a, b)\rangle$ has $q(\gamma') > 0$. Assuming that $\sup_{a,b \in \mathbb{T}} \| |\gamma(a, b)\rangle - |\gamma'(a, b)\rangle \|^2 < \epsilon^2$, we also have:

$$\frac{1}{(2\pi)^2} \int_0^{2\pi} \int_0^{2\pi} \| |\gamma(e^{i\theta}, e^{i\eta})\rangle - |\gamma'(e^{i\theta}, e^{i\eta})\rangle \|^2 d\theta d\eta < \epsilon^2$$

Using Parseval's identity [40], we conclude that

$$\sum_{k,h} \| |\gamma'_{k,h}\rangle - |\gamma_{k,h}\rangle \|^2 < \epsilon^2$$

and, in particular, this inequality holds for each term of the sum. By the fact that $|\det[a, b]| \leq \|a\| \|b\|$ (direct consequence of the Cauchy-Schwarz inequality), and that $\det[a, b] - \det[a, c] = \det[a, b - c]$, along with a standard application of the triangle inequality, we obtain, for $0 \leq x, y \leq n$:

$$\begin{aligned} \left| \det \begin{bmatrix} |\gamma_{x,0}\rangle & |\gamma_{y,0}\rangle \end{bmatrix} - \det \begin{bmatrix} |\gamma'_{x,0}\rangle & |\gamma'_{y,0}\rangle \end{bmatrix} \right| &< 2\epsilon \\ \left| \det \begin{bmatrix} |\gamma_{0,x}\rangle & |\gamma_{0,y}\rangle \end{bmatrix} - \det \begin{bmatrix} |\gamma'_{0,x}\rangle & |\gamma'_{0,y}\rangle \end{bmatrix} \right| &< 2\epsilon \end{aligned}$$

This implies that $|q(\gamma) - q(\gamma')| < 2\epsilon$ and, in particular, $q(\gamma') > 0$ if we take $\epsilon = q(\gamma)/2$. $\square$

By a simple calculation, the counterexample shown in Section 4.2, has $q(\gamma) = 144/10625 \simeq 0.013$.

5 Discussion and conclusions

In this work we consider the problem of multivariate quantum signal processing. Instead of previous work [35], where the signal (a or b) to “blend” at each step is chosen classically, we define here a protocol acting on a three-dimensional space, where essentially the choice of the variable can be made in superposition, which makes the evolution easier to understand and to decompose.

While Protocol C produces three-dimensional polynomials in general, Conjecture 7 states that, whenever our desired polynomial has effective dimension 2, then a construction using three dimensions can be turned into a bi-dimensional one (perhaps by increasing its length by at most a factor of 2). While we show a possible direction of the proof, its gist requires a deeper understanding of what we can do with Protocol C. We also remark that, whereas Conjecture 7 would turn the protocol into a single-qubit one, even if the conjecture turns out to be false, Protocol C can still be implemented with two qubits, although we would need to implement general $SU(3)$ unitaries (it is possible to obtain a phase factor decomposition using 8 rotations by, e.g., the Euler decomposition by the Gell-Mann matrices [41], or the Sinkhorn normal form [42]). Moreover, we remind that Laurent polynomials are always obtainable from analytic polynomials even in this case, by shifting all the coefficients with an operator $a^{-k}b^{-k}\mathbb{1}$ (in applications such as quantum eigenvalue transformation, this is possible by calling the unitaries for a, b unconditionally — this trick was also exploited in [33, 43]).

We then state necessary or sufficient conditions for decomposability into Protocol C: we first give a necessary and sufficient condition (Theorem 9) for the existence of a processing operator $A \in SU(3)$ that lowers the degree of the polynomial (usually needed in induction arguments which aim at finding a decomposition). These conditions come from the intuition that m -variable M-QSP protocols can be seen as a propagation in a m -dimensional lattice, where each point represents a coefficient of the multivariate polynomial.

These conditions are used to prove a sufficient condition for decomposability, namely that any n -degree polynomial having a non-zero constant term, as well as non-zero a^n, b^n terms, can be constructed using Protocol C. This is the first constructive result ever proven for a multivariate polynomial in the context of quantum signal processing. This proves that, in some sense, the behaviour of multivariate polynomials closely follows the univariate case, with the only exception that “degenerate” univariate schemes (the ones that do not reach the n -th degree term with n steps) simply produce polynomials with degree $< n$, while multivariate polynomials without the a^n term are not necessarily of degree $< n$. With similar arguments, an analogous result for polynomials in d variables and a $d + 1$ dimensional protocol is given in Appendix A, which also gives a sufficient condition for *homogeneous quantum signal processing* with general number of variables, a problem left open in [36] (indeed, in order to obtain the homogeneous version we simply replace the 1 in the signal operator with a new variable). We remark that this condition is certainly not necessary, since the polynomial $(1, ab, 0)/\sqrt{2}$ can be easily implemented in two steps (indeed, any polynomial state with effective dimension 2 cannot satisfy this condition).

We conclude the work by giving a simpler, easy-to-check, necessary condition for decomposability of a bivariate polynomial, involving a quantity $q(\gamma)$. We use such a simpler condition to prove that some polynomials are even hard to approximate with arbitrary precision. This confirms that the set of non-constructible polynomials has non-zero measure, formally proving a claim that was shown numerically in [36].

A natural question would be whether a multivariate QSVT could arise directly from (a restriction of) Protocol C, without having to resort to Conjecture 7, perhaps with a three-dimensional extension of the cosine-sine decomposition [39]. Another question left open is to understand whether there is an extension of the Fejér-Riesz theorem [44, 45] (used also for polynomial completion in univariate QSP [23] and single-qubit multivariate QSP [35]) allowing to complete a given polynomial $P(a, b)$ with a pair of polynomials $Q(a, b), R(a, b)$ satisfying the sufficient condition of Theorem 11. Moreover, it is a possible future direction to understand whether the above conditions can be extended to the case of non-commutative signals, a case relevant for quantum eigenvalue transformation involving

a set of non-commuting unitaries. We hope these results shed some light on M-QSP, giving directions for future works towards finding a full characterization of the multivariate polynomials.

Acknowledgements

We would like to thank Yuki Ito for useful feedback on Theorem 13. The authors acknowledge support from the Swiss National Science Foundation (SNSF), project No. 200020-214808.

References

- [1] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. “Quantum Amplitude Amplification and Estimation”. *Quantum Computation and Information* **305**, 53–74 (2002).
- [2] Lov K. Grover. “A Fast Quantum Mechanical Algorithm for Database Search”. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. Pages 212–219. Association for Computing Machinery (1996).
- [3] Andrew M Childs and Nathan Wiebe. “Hamiltonian simulation using linear combinations of unitary operations”. *Quantum Information and Computation* **12**, 901–924 (2012).
- [4] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. “Quantum Algorithm for Linear Systems of Equations”. *Physical Review Letters* **103**, 150502 (2009).
- [5] Mario Szegedy. “Quantum speed-up of Markov chain based algorithms”. In *45th Annual IEEE Symposium on Foundations of Computer Science*. Pages 32–41. (2004).
- [6] A Ambainis. “Quantum walk algorithm for element distinctness”. In *45th Annual IEEE Symposium on Foundations of Computer Science*. Pages 22–31. (2004).
- [7] Simon Apers, András Gilyén, and Stacey Jeffery. “A Unified Framework of Quantum Walk Search”. In *Leibniz International Proceedings in Informatics (LIPIcs)*. Volume 187 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 6:1–6:13. Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2021).
- [8] Arjan Cornelissen, Stacey Jeffery, Maris Ozols, and Alvaro Piedrafita. “Span programs and quantum time complexity”. In *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*. Volume 170 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 26:1–26:14. Schloss Dagstuhl–Leibniz-Zentrum für Informatik (2020).
- [9] Andrew M Childs, Robin Kothari, Matt Kovacs-Deak, Aarthi Sundaram, and Daochen Wang. “Quantum divide and conquer” (2022). [arXiv:2210.06419](https://arxiv.org/abs/2210.06419).
- [10] Aleksandrs Belovs, Stacey Jeffery, and Duyal Yolcu. “Taming Quantum Time Complexity”. *Quantum* **8**, 1444 (2024).
- [11] Guang Hao Low, Theodore J. Yoder, and Isaac L. Chuang. “Methodology of Resonant Equiangular Composite Quantum Gates”. *Physical Review X* **6**, 41067 (2016).
- [12] Guang Hao Low. “Quantum signal processing by single-qubit dynamics”. Thesis. Massachusetts Institute of Technology. (2017). url: <https://dspace.mit.edu/handle/1721.1/1115025>.

- [13] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. “Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics”. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*. Pages 193–204. ACM (2019).
- [14] John M. Martyn, Zane M. Rossi, Andrew K. Tan, and Isaac L. Chuang. “A Grand Unification of Quantum Algorithms”. *PRX Quantum* **2**, 40203 (2021).
- [15] Camille Jordan. “Essai sur la géométrie à n dimensions”. *Bulletin de la Société mathématique de France* **2**, 103–174 (1875).
- [16] Guang Hao Low and Isaac L. Chuang. “Optimal Hamiltonian Simulation by Quantum Signal Processing”. *Physical Review Letters* **118**, 010501 (2017).
- [17] Guang Hao Low and Isaac L. Chuang. “Hamiltonian Simulation by Uniform Spectral Amplification” (2017). [arXiv:1707.05391](#).
- [18] Seth Lloyd, Bobak T. Kiani, David R. M. Arvidsson-Shukur, Samuel Bosch, Giacomo De Palma, William M. Kaminsky, Zi-Wen Liu, and Milad Marvian. “Hamiltonian singular value transformation and inverse block encoding” (2021). [arXiv:2104.01410](#).
- [19] Guang Hao Low and Isaac L. Chuang. “Hamiltonian Simulation by Qubitization”. *Quantum* **3**, 163 (2019).
- [20] John M. Martyn, Yuan Liu, Zachary E. Chin, and Isaac L. Chuang. “Efficient fully-coherent quantum signal processing algorithms for real-time dynamics simulation”. *The Journal of Chemical Physics* **158**, 024106 (2023).
- [21] Sam McArdle, András Gilyén, and Mario Berta. “Quantum state preparation without coherent arithmetic” (2022). [arXiv:2210.14892](#).
- [22] Lorenzo Laneve. “Robust black-box quantum-state preparation via quantum signal processing” (2023). [arXiv:2305.04705](#).
- [23] Jeongwan Haah. “Product Decomposition of Periodic Functions in Quantum Signal Processing”. *Quantum* **3**, 190 (2019).
- [24] Rui Chao, Dawei Ding, Andras Gilyen, Cupjin Huang, and Mario Szegedy. “Finding Angles for Quantum Signal Processing with Machine Precision” (2020). [arXiv:2003.02831](#).
- [25] Yulong Dong, Xiang Meng, K Birgitta Whaley, and Lin Lin. “Efficient phase-factor evaluation in quantum signal processing”. *Physical Review A* **103**, 42419 (2021).
- [26] Yulong Dong, Lin Lin, Hongkang Ni, and Jiasu Wang. “Infinite quantum signal processing”. *Quantum* **8**, 1558 (2024).
- [27] Jiasu Wang, Yulong Dong, and Lin Lin. “On the energy landscape of symmetric quantum signal processing”. *Quantum* **6**, 850 (2022).
- [28] Kaoru Mizuta and Keisuke Fujii. “Recursive quantum eigenvalue and singular-value transformation: Analytic construction of matrix sign function by Newton iteration”. *Physical Review Research* **6**, L012007 (2024).
- [29] Zane M. Rossi and Isaac L. Chuang. “Semantic embedding for quantum algorithms”. *Journal of Mathematical Physics* **64**, 122202 (2023).
- [30] Zane M. Rossi, Jack L. Ceroni, and Isaac L. Chuang. “Modular quantum signal processing in many variables” (2023). [arXiv:2309.16665](#).
- [31] Zane M. Rossi, Victor M. Bastidas, William J. Munro, and Isaac L. Chuang. “Quantum signal processing with continuous variables” (2023). [arXiv:2304.14383](#).

- [32] Danial Motlagh and Nathan Wiebe. “Generalized Quantum Signal Processing”. [PRX Quantum](#) **5**, 020368 (2024).
- [33] Lorenzo Laneve. “Quantum signal processing over $SU(N)$ ” (2024). [arXiv:2311.03949](#).
- [34] V. M. Bastidas and K. J. Joven. “Complexification of Quantum Signal Processing and its Ramifications” (2024). [arXiv:2407.04780](#).
- [35] Zane M. Rossi and Isaac L. Chuang. “Multivariable quantum signal processing (M-QSP): Prophecies of the two-headed oracle”. [Quantum](#) **6**, 811 (2022).
- [36] Balázs Németh, Blanka Kövér, Boglárka Kulcsár, Roland Botond Miklósi, and András Gilyén. “On variants of multivariate quantum signal processing and their characterizations” (2023). [arXiv:2312.09072](#).
- [37] Yonah Borns-Weil, Tahsin Saffat, and Zachary Stier. “A Quantum Algorithm for Functions of Multiple Commuting Hermitian Matrices” (2023). [arXiv:2302.11139](#).
- [38] Hitomi Mori, Kaoru Mizuta, and Keisuke Fujii. “Comment on “Multivariable quantum signal processing (M-QSP): Prophecies of the two-headed oracle””. [Quantum](#) **8**, 1512 (2024).
- [39] Ewin Tang and Kevin Tian. “A CS guide to the quantum singular value transformation” (2023). [arXiv:2302.14324](#).
- [40] Elias M. Stein and Rami Shakarchi. “Fourier Analysis: An Introduction”. Princeton University Press. (2011). url: <https://press.princeton.edu/books/hardcover/9780691113845/fourier-analysis>.
- [41] Martin Roelfs. “Geometric Invariant Decomposition of $SU(3)$ ”. [Advances in Applied Clifford Algebras](#) **33**, 5 (2022).
- [42] Martin Idel and Michael M. Wolf. “Sinkhorn normal form for unitary matrices”. [Linear Algebra and its Applications](#) **471**, 76–84 (2015).
- [43] Dominic W. Berry, Danial Motlagh, Giacomo Pantaleoni, and Nathan Wiebe. “Doubling the efficiency of Hamiltonian simulation via generalized quantum signal processing”. [Physical Review A](#) **110**, 012612 (2024).
- [44] Jeffrey S. Geronimo and Hugo J. Woerdeman. “Positive extensions, Fejér-Riesz factorization and autoregressive filters in two variables”. [Annals of Mathematics](#) **160**, 839–906 (2004).
- [45] Abdulmtalib Hussen and Abdelbaset Zeyani. “Fejer-Riesz Theorem and Its Generalization”. [International Journal of Scientific and Research Publications \(IJSRP\)](#) **11**, 286–292 (2021).

A Proof for more than two variables

For completeness, we provide a proof for Theorems 9 and 11 in the case of $m \geq 3$ variables. Analogously to what we did in two variables, we define a $(m + 1)$ -dimensional protocol, where the signal operator is

$$\tilde{W} = \text{diag}(1, z_1, \dots, z_m)$$

and the processing operators are $A_k \in SU(m + 1)$.

Theorem 14. *Let $|\gamma(\mathbf{z})\rangle = \sum_{\mathbf{k}} |\gamma_{\mathbf{k}}\rangle \mathbf{z}^{\mathbf{k}}$ be a polynomial state of degree n in m variables and $m + 1$ dimensions. There exists $A_n \in SU(m + 1)$ such that $\tilde{W}^\dagger A_n^\dagger |\gamma(\mathbf{z})\rangle$ has degree $n - 1$ if and only if there exists an orthonormal basis $\{|\psi_j\rangle\}_{0 \leq j \leq m}$ such that*

(i) $\langle \psi_j | \gamma_{\mathbf{k}} \rangle = 0$, for $1 \leq j \leq m$, and every $\mathbf{k} \geq 0$ such that $k_j = 0$;

(ii) $\langle \psi_0 | \gamma_{\mathbf{k}} \rangle = 0$ for every $\mathbf{k} \geq 0$ such that $\sum_j k_j = n$.

If the $m + 1$ endpoints $\{|\gamma_{\mathbf{e}_j}\rangle\}_{0 \leq j \leq m}$ are non-zero, the above conditions are equivalent to

(i') $\langle \gamma_{n\mathbf{e}_j} | \gamma_{\mathbf{k}} \rangle = 0$, for $1 \leq j \leq m$, and every $\mathbf{k} \geq 0$ such that $k_j = 0$;

(ii') $\langle \gamma_0 | \gamma_{\mathbf{k}} \rangle = 0$, for every $\mathbf{k} \geq 0$ such that $\sum_j k_j = n$.

Condition (i) says that $|\psi_j\rangle$ — which will be mapped to the subspace where $\tilde{W}$ multiplies by z_j — must be orthogonal to the coefficients of the terms where z_j already has degree 0, as to avoid any negative coefficient. Similarly, the second condition ensures that the subspace that does not lower any degree is orthogonal to the vectors that has the maximum degree n , so that they are all lowered and the final polynomial can be of degree $n - 1$.

Proof. Following the same reasoning of Theorem 9, $|\gamma'(\mathbf{z})\rangle = \tilde{W}^\dagger A_n^\dagger |\gamma(\mathbf{z})\rangle$ is of degree $n - 1$ if and only if $|\gamma'_{\mathbf{k}}\rangle = 0$ for every $\mathbf{k}$ of degree n , and every $\mathbf{k}$ that contains negative entries. Therefore, we need $A_n^\dagger$ to satisfy

- $\langle j | A_n^\dagger | \gamma_{\mathbf{k}} \rangle = 0$ for every $1 \leq j \leq m$ and $\mathbf{k} \geq 0$ with $k_j = 0$, to avoid negative degrees;
- $\langle 0 | A_n^\dagger | \gamma_{\mathbf{k}} \rangle = 0$ for every $\mathbf{k} \geq 0$ with $\sum_j k_j = n$, to reduce the degree.

By conditions (i)-(ii), the choice $A_n : |j\rangle \mapsto |\psi_j\rangle$ suffices. The endpoints $|\gamma_0\rangle, |\gamma_{n\mathbf{e}_j}\rangle$ need to satisfy m out of the $m + 1$ conditions, thus implying $|\gamma_{n\mathbf{e}_j}\rangle \propto |\psi_j\rangle$, while $|\gamma_0\rangle \propto |\psi_0\rangle$, implying that (i)-(ii) and (i')-(ii') are equivalent whenever these $m + 1$ endpoints are non-zero. $\square$

Theorem 15. Let $|\gamma(\mathbf{z})\rangle = \sum_{\mathbf{k}, h} |\gamma_{\mathbf{k}}\rangle \mathbf{z}^{\mathbf{k}} \mathbf{z}^h$ be a polynomial state of degree n in m variables and $(m + 1)$ -dimensions such that the coefficient of $1, z_1^n, \dots, z_m^n$ are all non-zero. Then there exist $A_0, \dots, A_n \in SU(m + 1)$ such that

$$A_n \tilde{W} A_{n-1} \tilde{W} \cdots \tilde{W} A_0 |0\rangle = |\gamma(\mathbf{z})\rangle .$$

Proof. For $n = 0$ the claim is trivial, since the polynomial state is a constant quantum state and can be chosen as $A_0 |0\rangle$.

For $n > 0$, since the endpoints are non-zero, the conditions (i')-(ii') of Theorem 14 must hold in order for a degrading A_n to exist. By writing down the normalization condition we obtain:

$$\langle \gamma(\mathbf{z}) | \gamma(\mathbf{z}) \rangle = \sum_{\mathbf{k}, \mathbf{h}} \langle \gamma_{\mathbf{k}} | \gamma_{\mathbf{h}} \rangle \mathbf{z}^{\mathbf{h} - \mathbf{k}} = \sum_{\mathbf{h}} \sum_{\mathbf{k}} \langle \gamma_{\mathbf{k}} | \gamma_{\mathbf{k} + \mathbf{h}} \rangle \mathbf{z}^{\mathbf{h}} \stackrel{!}{=} 1$$

The coefficient of $\mathbf{z}^{\mathbf{h}}$ for $\mathbf{h} \neq 0$ must be zero. In particular

- by taking $\mathbf{h} = \mathbf{k}' - n\mathbf{e}_j$ for $\mathbf{k}' \geq 0$ with $k'_j = 0$, we get $\langle \gamma_{n\mathbf{e}_j} | \gamma_{\mathbf{k}'} \rangle = 0$, condition (i');
- by taking $\mathbf{h}$ of degree n , we obtain $\langle \gamma_0 | \gamma_{\mathbf{h}} \rangle = 0$, condition (ii').

This yields a A_n that lower the degree of $|\gamma'(\mathbf{z})\rangle = \tilde{W}^\dagger A_n^\dagger |\gamma(\mathbf{z})\rangle$, by Theorem 14. Moreover, $|\gamma'(\mathbf{z})\rangle$ must have a non-zero coefficient in z_j^{n-1} for each j , otherwise $A_n \tilde{W} |\gamma'(\mathbf{z})\rangle$ would not be able to produce a term of degree z_j^n . The same reasoning applied to the constant term, and the claim follows by the induction step. $\square$