

Comment on “Multivariable quantum signal processing (M-QSP): prophecies of the two-headed oracle”

Hitomi Mori¹, Kaoru Mizuta^{2,3}, and Keisuke Fujii^{1,4,3,5}

¹Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan

²Department of Applied Physics, The University of Tokyo, Hongo 7-3-1, Bunkyo, Tokyo 113-8656, Japan

³Center for Quantum Computing, RIKEN, Hirosawa 2-1, Wako, Saitama 351-0198, Japan

⁴Center for Quantum Information and Quantum Biology, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan

⁵Fujitsu Quantum Computing Joint Research Division at QIQB, Osaka University, 1-2 Machikaneyama, Toyonaka 560-0043, Japan

Multivariable Quantum Signal Processing (M-QSP) [1] is expected to provide an efficient means to handle polynomial transformations of multiple variables simultaneously. However, we identified several inconsistencies in the main theorem, where necessary and sufficient conditions for achievable polynomials are provided, and its proof in Ref. [1]. Moreover, a counterexample to the conjecture in Ref. [1], based on which the main theorem is constructed, is presented in Ref. [2], meaning the requirement of the conjecture should be included as a condition in the theorem. Here we note our observations and propose the revised necessary conditions for M-QSP. We also show that these necessary conditions cannot be sufficient conditions, and thus some additional condition on top of these revisions is essentially required for the complete M-QSP theorem.

1 Introduction

Quantum algorithms have been successfully proven an advantage over classical algorithms in many computational tasks, including factoring [3], Hamiltonian simulation [4], and matrix inversion [5]. More recently, techniques called quantum signal processing (QSP) [6] and quantum singular value transform (QSVT) [7] were proposed and successfully unified these quantum algorithms within the framework. Specifically, QSP performs a polynomial transformation of an element of a signal operator represented as a single qubit gate, while QSVT is an extension of QSP to a larger dimension via qubitization, and notably these techniques provide optimal complexity in many cases.

Multivariable quantum signal processing (M-QSP) [1] is proposed as a multivariable generalization of QSP. It performs multivariable polynomial transform using multiple kinds of signal operators represented as X -rotation, which correspond to each variable. The original paper of M-QSP provided necessary and sufficient conditions on polynomials implementable with M-QSP in its main theorem (Theorem 2.3). However, we identified several

Hitomi Mori: hmori.academic@gmail.com

inconsistencies in the theorem and its proof. Separately, a counterexample to the key conjecture (Conjecture 2.1), which is about the coefficients of multivariable polynomials and on which the theorem is constructed, is found in Ref. [2], meaning the requirement of the conjecture should be included as a condition in the theorem. In this paper, we note our observations and propose the revised necessary conditions for M-QSP. We also show that these necessary conditions cannot be sufficient conditions, and thus some additional condition on top of these revisions is essentially required for the complete M-QSP theorem.

The rest of this paper is organized as follows. In Section 2 and Section 3, we explain the inconsistencies in Theorem 2.3 of Ref. [1] and its proof, respectively. We propose the revised theorem in Section 4, followed by the conclusion in Section 5.

2 Inconsistency in Theorem 2.3

In this section we show inconsistencies observed in Theorem 2.3 in Ref. [1].

Theorem 2.3 in Ref. [1]: *Let $n \in \mathbb{N}$. There exist $\Phi = \{\phi_0, \phi_1, \dots, \phi_n\} \in \mathbb{R}^{n+1}$ and $s = \{s_1, \dots, s_n\} \in \{0, 1\}^n$ such that for all $(a, b) \in \mathbb{T}^2$:*

$$U_{(s, \Phi)}(a, b) = e^{i\phi_0 \sigma_z} \prod_{k=1}^n A^{s_k}(a) B^{1-s_k}(b) e^{i\phi_k \sigma_z} = \begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix}, \quad (1)$$

where $A = \mathbb{I}(a + a^{-1})/2 + \sigma_x(a - a^{-1})/2$ and $B = \mathbb{I}(b + b^{-1})/2 + \sigma_x(b - b^{-1})/2$ if and only if $P, Q \in \mathbb{C}[a, b]$ (Laurent polynomials) and

- (i) $\deg(P) \preceq (m, n - m)$ and $\deg(Q) \preceq (m, n - m)$ for $m = |s|$ the Hamming weight of s .
- (ii) P has parity- $n(\bmod 2)$ under $(a, b) \mapsto (a^{-1}, b^{-1})$ and Q has parity- $(n - 1)(\bmod 2)$ under $(a, b) \mapsto (a^{-1}, b^{-1})$.
- (iii) P has parity $m(\bmod 2)$ under $a \mapsto -a$ and parity $m - n(\bmod 2)$ under $b \mapsto -b$ and Q has parity $m - 1(\bmod 2)$ under $a \mapsto -a$ and parity $n - m - 1(\bmod 2)$ under $b \mapsto -b$.
- (iv) For all $(a, b) \in \mathbb{T}^2$ the relation $|P|^2 + |Q|^2 = 1$ holds.
- (v) The statement of Conjecture 2.1 holds as given.

Conjecture 2.1 in Ref. [1]: *Given a unitary matrix satisfying the conditions (i)-(iv) of Theorem 2.3, the single-variable Laurent polynomial coefficients of P, Q satisfy one or both of the following relations for $\phi_A, \phi_B \in \mathbb{R}$:*

$$P_{d_A}(b) = e^{i\phi_A} Q_{d_A}(b), P_{d_B}(a) = e^{i\phi_B} Q_{d_B}(a). \quad (2)$$

Here d_A and d_B are the maximal positive degree of a, b respectively appearing in P, Q , and $P_{d_A}(b)$ denotes the single variable Laurent polynomial (in b) coefficient of the a^{d_A} term of P , and analogously for the other terms.

Here we show the inconsistency among the statements (i)-(iv). According to Theorem 2.3 (i), P and Q can be expressed as

$$P(a, b) = \sum_{j=-m}^m \sum_{k=-(n-m)}^{n-m} P_{jk} a^j b^k, \quad (3)$$

$$Q(a, b) = \sum_{j=-m}^m \sum_{k=-(n-m)}^{n-m} Q_{jk} a^j b^k. \quad (4)$$

However, from Theorem 2.3 (iii), the possible highest and lowest order term of Q are restricted as

$$Q(a, b) = \sum_{j=-(m-1)}^{m-1} \sum_{k=-(n-m-1)}^{n-m-1} Q_{jk} a^j b^k, \quad (5)$$

suggesting $\deg(Q) \preccurlyeq (m-1, n-m-1)$.

Theorem 2.3 (iv) can be rewritten as

$$\sum_{j,k} |P_{jk}|^2 + \sum_{(j,k) \neq (j',k')} P_{jk} P_{j'k'}^* e^{i(j-j')\theta_a} e^{i(k-k')\theta_b} + \sum_{j,k} |Q_{jk}|^2 + \sum_{(j,k) \neq (j',k')} Q_{jk} Q_{j'k'}^* e^{i(j-j')\theta_a} e^{i(k-k')\theta_b} = 1, \quad (6)$$

where $a = \exp(i\theta_a)$ and $b = \exp(i\theta_b)$ are substituted. Because products of orthogonal functions form orthogonal functions, $\exp(il_a\theta_a) \exp(il_b\theta_b)$ terms, where $(l_a, l_b) \equiv (j-j', k-k') \neq (0, 0)$, need to vanish. Thus, the condition of Theorem 2.3 (iv) is equivalent to

$$\sum_{j,k} (|P_{jk}|^2 + |Q_{jk}|^2) = 1 \quad (7)$$

and

$$\sum_{j,k} (P_{jk} P_{j-l_a, k-l_b}^* + Q_{jk} Q_{j-l_a, k-l_b}^*) = 0. \quad (8)$$

In the case of $(l_a, l_b) = (2m, 2(n-m))$, the only possible choice is $j = m$ and $k = n-m$, and hence Eq. (8) leads to

$$P_{m, n-m} P_{-m, -(n-m)}^* = 0, \quad (9)$$

as Q does not have the $(m, n-m)$ order term. According to Theorem 2.3 (ii), we have

$$P(a^{-1}, b^{-1}) = (-1)^n P(a, b), \quad (10)$$

which can be written down as

$$\sum_{j,k} P_{jk} a^{-j} b^{-k} = (-1)^n \sum_{j,k} P_{jk} a^j b^k \quad (11)$$

$$= (-1)^n \sum_{j,k} P_{-j-k} a^{-j} b^{-k}. \quad (12)$$

Comparing the highest term on both sides, we get the condition on the coefficient:

$$P_{-m, -(n-m)} = (-1)^n P_{m, n-m}. \quad (13)$$

Plugging this into Eq. (9), we get

$$(-1)^n |P_{m, n-m}|^2 = 0 \quad (14)$$

and this implies the $(m, n-m)$ order term of P vanishes. Repeating the same thing for other combinations of (l_a, l_b) , it turns out all coefficients other than the constant term vanish after all¹, which contradicts with Theorem 2.3 (i).

3 Inconsistency in the proof of Theorem 2.3

In this section we show inconsistencies observed in the proof of Theorem 2.3 in Ref. [1].

3.1 Regarding the proof of “ $\Rightarrow$ ”:

When we assume the $(n-1)$ th order (the $(m-1)$ th order in a) sequence $U_{(\tilde{s}, \tilde{\Phi})}$ satisfies the conditions, we get

$$U_{(\tilde{s}, \tilde{\Phi})} = \begin{pmatrix} \tilde{P} & \tilde{Q} \\ -\tilde{Q}^* & \tilde{P}^* \end{pmatrix}, \quad (15)$$

$$\tilde{P}(a^{-1}, b^{-1}) = (-1)^{n-1} \tilde{P}(a, b), \quad (16)$$

$$\tilde{Q}(a^{-1}, b^{-1}) = (-1)^{n-2} \tilde{Q}(a, b), \quad (17)$$

$$\tilde{P}(-a, b) = (-1)^{m-1} \tilde{P}(a, b), \quad (18)$$

$$\tilde{Q}(-a, b) = (-1)^{m-2} \tilde{Q}(a, b). \quad (19)$$

Then for the n th order (the m th order in a), which can be obtained by applying $Ae^{i\phi_n \sigma_z}$ from the right side, we get

$$U_{(s, \Phi)} = \begin{pmatrix} e^{i\phi_n} \left(\frac{a+a^{-1}}{2} \tilde{P} + \frac{a-a^{-1}}{2} \tilde{Q} \right) & e^{-i\phi_n} \left(\frac{a-a^{-1}}{2} \tilde{P} + \frac{a+a^{-1}}{2} \tilde{Q} \right) \\ \cdot & \cdot \end{pmatrix}. \quad (20)$$

Therefore, if we consider each element in $U_{(s, \Phi)}$, we have

$$\begin{aligned} P(a^{-1}, b^{-1}) &= e^{i\phi_n} \left(\frac{a+a^{-1}}{2} \tilde{P}(a^{-1}, b^{-1}) - \frac{a-a^{-1}}{2} \tilde{Q}(a^{-1}, b^{-1}) \right) \\ &= (-1)^{n-1} P(a, b), \end{aligned} \quad (21)$$

$$\begin{aligned} Q(a^{-1}, b^{-1}) &= e^{-i\phi_n} \left(-\frac{a-a^{-1}}{2} \tilde{P}(a^{-1}, b^{-1}) + \frac{a+a^{-1}}{2} \tilde{Q}(a^{-1}, b^{-1}) \right) \\ &= (-1)^{n-2} Q(a, b), \end{aligned} \quad (22)$$

$$\begin{aligned} P(-a, b) &= e^{i\phi_n} \left(-\frac{a+a^{-1}}{2} \tilde{P}(-a, b) - \frac{a-a^{-1}}{2} \tilde{Q}(-a, b) \right) \\ &= (-1)^m e^{i\phi_n} \left(\frac{a+a^{-1}}{2} \tilde{P}(a, b) - \frac{a-a^{-1}}{2} \tilde{Q}(a, b) \right), \end{aligned} \quad (23)$$

¹This can be seen by first considering $(l_a, l_b) = (2m, 2(n-m)-2), (2m, 2(n-m)-4), \dots, (2m, -2(n-m))$, where we find all P_{m*} become 0. The same goes for P_{*n-m} . Then we next consider $(l_a, l_b) = (2m-2, 2(n-m)-2), (2m-2, 2(n-m)-4), \dots, (2m-2, -2(n-m))$ and we find Q_{m-1*} vanish. Continuing this we find that all the coefficients other than the constant term vanish.

$$\begin{aligned}
Q(-a, b) &= e^{-i\phi_n} \left(-\frac{a - a^{-1}}{2} \tilde{P}(-a, b) - \frac{a + a^{-1}}{2} \tilde{Q}(-a, b) \right) \\
&= (-1)^{m-1} e^{-i\phi_n} \left(\frac{a - a^{-1}}{2} \tilde{P}(a, b) - \frac{a + a^{-1}}{2} \tilde{Q}(a, b) \right). \tag{24}
\end{aligned}$$

However, to prove Theorem 2.3 (ii), Eq. (21) and Eq. (22) need to be $(-1)^n P(a, b)$ and $(-1)^{n-1} Q(a, b)$, and to prove Theorem 2.3 (iii), Eq. (23) and Eq. (24) be $(-1)^m P(a, b)$ and $(-1)^{m-1} Q(a, b)$. Therefore, the statement is not proven, as it does not hold for the n th order (the m th order in a).

3.2 Regarding the proof of “ $\Leftarrow$ ”:

After we assume the statement for the $(n-1)$ th order (the $(m-1)$ th order in a) sequence $U_{(\tilde{s}, \tilde{\Phi})}$ is true (i.e. polynomial satisfies the conditions (i)-(v) $\Rightarrow U_{(\tilde{s}, \tilde{\Phi})}$ exists), we assume the n th order (the m th order in a) P, Q satisfy the conditions. Thus,

$$\deg(P) \preccurlyeq (m, n-m), \tag{25}$$

$$\deg(Q) \preccurlyeq (m, n-m), \tag{26}$$

$$P(a^{-1}, b^{-1}) = (-1)^n P(a, b), \tag{27}$$

$$Q(a^{-1}, b^{-1}) = (-1)^{n-1} Q(a, b), \tag{28}$$

$$P(-a, b) = (-1)^m P(a, b), \tag{29}$$

$$Q(-a, b) = (-1)^{m-1} Q(a, b). \tag{30}$$

Assuming $P_{d_A}(b) = e^{2i\phi_n} Q_{d_A}(b)$ from Conjecture 2.1 holds, where d_A is the highest degree of a , we define

$$\begin{aligned}
\begin{pmatrix} \tilde{P} & \tilde{Q} \\ -\tilde{Q}^* & \tilde{P}^* \end{pmatrix} &\equiv \begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix} e^{-i\phi_n \sigma_z} A^\dagger \\
&= \begin{pmatrix} \frac{a+a^{-1}}{2} e^{-i\phi_n} P - \frac{a-a^{-1}}{2} e^{i\phi_n} Q & -\frac{a-a^{-1}}{2} e^{-i\phi_n} P + \frac{a+a^{-1}}{2} e^{i\phi_n} Q \\ \cdot & \cdot \end{pmatrix}. \tag{31}
\end{aligned}$$

Because the highest terms cancel out in Eq. (31),

$$\deg(\tilde{P}) \preccurlyeq (m-1, n-m), \tag{32}$$

$$\deg(\tilde{Q}) \preccurlyeq (m-1, n-m). \tag{33}$$

Then we want to apply the assumption for the $(n-1)$ th order (the $(m-1)$ th order in a) to $\tilde{P}, \tilde{Q}$ to show there exist the solution $\Phi = (\tilde{\Phi}, \phi_n)$ and $s = (\tilde{s}, 1)$ but cannot because they do not satisfy the conditions (ii)-(iii).

$$\tilde{P}(a^{-1}, b^{-1}) = (-1)^n \tilde{P}(a, b) \tag{34}$$

$$\tilde{Q}(a^{-1}, b^{-1}) = (-1)^{n-1} \tilde{Q}(a, b) \tag{35}$$

$$\tilde{P}(-a, b) = (-1)^{m-1} \frac{a + a^{-1}}{2} e^{-i\phi_n} P(a, b) - (-1)^m \frac{a - a^{-1}}{2} e^{i\phi_n} Q(a, b) \tag{36}$$

$$\tilde{Q}(-a, b) = -(-1)^{m-1} \frac{a - a^{-1}}{2} e^{-i\phi_n} P(a, b) + (-1)^m \frac{a + a^{-1}}{2} e^{i\phi_n} Q(a, b) \tag{37}$$

Therefore, the statement is not proven, as it does not hold for the n th order (the m th order in a).

4 Prospects of M-QSP

The inconsistencies discussed in sections 2 and 3 can be resolved by revising the conditions (ii) and (iii). Also, it is known that there exists a counterexample for Conjecture 2.1, as is pointed out in Ref. [2]:

$$P(a, b) = \frac{6}{25} \sqrt{\frac{37}{493}} \left[a^2 b^2 + a^{-2} b^{-2} - \left(\frac{122}{37} + \frac{8i}{37} \right) (b^2 + b^{-2}) + \left(\frac{114}{37} + \frac{56i}{37} \right) (a^{-2} b^2 + a^2 b^{-2}) + \left(\frac{362}{111} - \frac{248i}{111} \right) (a^2 + a^{-2}) + \frac{692}{111} - \frac{719i}{222} \right], \quad (38)$$

$$Q(a, b) = \frac{6}{25} \sqrt{\frac{37}{493}} \left[a^2 b^2 - a^{-2} b^{-2} - \left(\frac{122}{37} + \frac{66i}{37} \right) (b^2 - b^{-2}) + \left(\frac{56}{37} + \frac{114i}{37} \right) (a^{-2} b^2 - a^2 b^{-2}) + \left(\frac{362}{111} - \frac{418i}{111} \right) (a^2 - a^{-2}) \right]. \quad (39)$$

This means the conjecture is not a natural result of conditions (i)-(iv) and needs to be included as the condition (v). In this section, we prove these revised conditions make the necessary condition of M-QSP, where we provide the proof that follows the original paper as well as a simpler alternative. Moreover, we show that the complete reconstruction of the M-QSP Theorem is not straightforward. Because of the condition (v), “ $\Leftarrow$ ” of the theorem no longer holds, meaning some additional condition is required for the valid M-QSP Theorem.

Revised necessary condition of M-QSP: Let $n \in \mathbb{N}$. There exist $\Phi = \{\phi_0, \phi_1, \dots, \phi_n\} \in \mathbb{R}^{n+1}$ and $s = \{s_1, \dots, s_n\} \in \{0, 1\}^n$ such that for all $(a, b) \in \mathbb{T}^2$:

$$U_{(s, \Phi)}(a, b) = e^{i\phi_0 \sigma_z} \prod_{k=1}^n A^{s_k}(a) B^{1-s_k}(b) e^{i\phi_k \sigma_z} = \begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix}, \quad (40)$$

where $A = \mathbb{I}(a + a^{-1})/2 + \sigma_x(a - a^{-1})/2$ and $B = \mathbb{I}(b + b^{-1})/2 + \sigma_x(b - b^{-1})/2$ **only if** $P, Q \in \mathbb{C}[a, b]$ (Laurent polynomials) and

- (i) $\deg(P) \preceq (m, n-m)$ and $\deg(Q) \preceq (m, n-m)$ for $m = |s|$ the Hamming weight of s .
- (ii') P has **even parity** under $(a, b) \mapsto (a^{-1}, b^{-1})$ and Q has **odd parity** under $(a, b) \mapsto (a^{-1}, b^{-1})$.
- (iii') P has parity $m \pmod{2}$ under $a \mapsto -a$ and parity $m - n \pmod{2}$ under $b \mapsto -b$ and Q has parity **$m \pmod{2}$** under $a \mapsto -a$ and parity **$n - m \pmod{2}$** under $b \mapsto -b$.
- (iv) For all $(a, b) \in \mathbb{T}^2$ the relation $|P|^2 + |Q|^2 = 1$ holds.
- (v') **For $m \geq 1$ and $n - m \geq 1$, $P_m(b) = e^{2i\varphi} Q_m(b)$ and/or $P_{n-m}(a) = e^{2i\varphi'} Q_{n-m}(a)$, where $\varphi, \varphi' \in \mathbb{R}$ and $P_m(b)$ denotes the single variable Laurent polynomial coefficient of the highest a^m term of P , and the same goes for others.**

Proof. The following proof by induction focuses on changing the degree of a , but the same discussion can be applied to b . For $n = 0$, $P = e^{i\phi_0}$ and $Q = 0$ satisfy (i), (ii'), (iii'),

and (iv), where (v') is not relevant for this degree. For $n = k - 1, m = l - 1$, assume the statement holds.

$$U_{(\tilde{s}, \tilde{\Phi})} = \begin{pmatrix} \tilde{P} & \tilde{Q} \\ -\tilde{Q}^* & \tilde{P}^* \end{pmatrix} \quad (41)$$

$$\deg(\tilde{P}) \preccurlyeq (l - 1, k - l) \quad (42)$$

$$\deg(\tilde{Q}) \preccurlyeq (l - 1, k - l) \quad (43)$$

$$\tilde{P}(a^{-1}, b^{-1}) = \tilde{P}(a, b) \quad (44)$$

$$\tilde{Q}(a^{-1}, b^{-1}) = -\tilde{Q}(a, b) \quad (45)$$

$$\tilde{P}(-a, b) = (-1)^{l-1} \tilde{P}(a, b) \quad (46)$$

$$\tilde{Q}(-a, b) = (-1)^{l-1} \tilde{Q}(a, b) \quad (47)$$

For $n = k, m = l$, the sequence is calculated as

$$\begin{aligned} U_{(s, \Phi)} &\equiv \begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix} \\ &= \begin{pmatrix} \tilde{P} & \tilde{Q} \\ -\tilde{Q}^* & \tilde{P}^* \end{pmatrix} A e^{i\phi_k \sigma_z} \\ &= \begin{pmatrix} e^{i\phi_k} \left(\frac{a+a^{-1}}{2} \tilde{P} + \frac{a-a^{-1}}{2} \tilde{Q} \right) & e^{-i\phi_k} \left(\frac{a-a^{-1}}{2} \tilde{P} + \frac{a+a^{-1}}{2} \tilde{Q} \right) \\ \cdot & \cdot \end{pmatrix}, \end{aligned} \quad (48)$$

where $\Phi = (\tilde{\Phi}, \phi_k)$ and $s = (\tilde{s}, 1)$, and P and Q satisfy

$$\deg(P) \preccurlyeq (l, k - l), \quad (49)$$

$$\deg(Q) \preccurlyeq (l, k - l), \quad (50)$$

$$P(a^{-1}, b^{-1}) = P(a, b), \quad (51)$$

$$Q(a^{-1}, b^{-1}) = -Q(a, b), \quad (52)$$

$$P(-a, b) = (-1)^l P(a, b), \quad (53)$$

$$Q(-a, b) = (-1)^l Q(a, b). \quad (54)$$

Also, $|P|^2 + |Q|^2 = 1$ is satisfied because of the unitarity of the operations. If we take a look at the highest terms in a in Eq. (48), we have

$$P_l(b) = \frac{e^{i\phi_k}}{2} \left(\tilde{P}_{l-1}(b) + \tilde{Q}_{l-1}(b) \right), \quad (55)$$

$$Q_l(b) = \frac{e^{-i\phi_k}}{2} \left(\tilde{P}_{l-1}(b) + \tilde{Q}_{l-1}(b) \right), \quad (56)$$

which satisfy $P_l(b) = e^{2i\phi_k} Q_l(b)$. Therefore, the statement holds. $\square$

The same can be proven without using induction, so we show the alternate proof as well.

Alternate Proof. (i) is obviously satisfied, as the maximal degree of a and b are the number of applications of A and B , respectively. Inversion parity of (ii') can be seen by noting the transformation of $a \mapsto a^{-1}$ and $b \mapsto b^{-1}$ are equivalent to $A \mapsto \sigma_z A \sigma_z$ and $B \mapsto \sigma_z B \sigma_z$,

respectively. Under these transformations,

$$\begin{aligned}
U_{(s,\Phi)}(a^{-1}, b^{-1}) &= e^{i\phi_0\sigma_z} \prod_{k=1}^n (\sigma_z A^{s_k}(a) \sigma_z) (\sigma_z B^{1-s_k}(b) \sigma_z) e^{i\phi_n\sigma_z} \\
&= \sigma_z U_{(s,\Phi)}(a, b) \sigma_z \\
&= \begin{pmatrix} P(a, b) & -Q(a, b) \\ Q^*(a, b) & P^*(a, b) \end{pmatrix}.
\end{aligned} \tag{57}$$

Comparing this with Eq. (40), we get

$$P(a^{-1}, b^{-1}) = P(a, b), \tag{58}$$

$$Q(a^{-1}, b^{-1}) = -Q(a, b). \tag{59}$$

(iii') can also be checked easily by observing $a \mapsto -a$ and $b \mapsto -b$ correspond to $A \mapsto -A$ and $B \mapsto -B$, respectively. By simply counting the number of A and B in Eq. (40), we see

$$P(-a, b) = (-1)^m P(a, b), \tag{60}$$

$$P(a, -b) = (-1)^{n-m} P(a, b), \tag{61}$$

$$Q(-a, b) = (-1)^m Q(a, b), \tag{62}$$

$$Q(a, -b) = (-1)^{n-m} Q(a, b). \tag{63}$$

(iv) is also satisfied because of the unitarity of the operations. To see (v'), define

$$U_{(\tilde{s}, \tilde{\Phi})} = e^{i\phi_0\sigma_z} \prod_{k=1}^{n-1} A^{s_k}(a) B^{1-s_k}(b) e^{i\phi_k\sigma_z} = \begin{pmatrix} \tilde{P} & \tilde{Q} \\ -\tilde{Q}^* & \tilde{P}^* \end{pmatrix}, \tag{64}$$

then $U_{(s,\Phi)}$ can be computed as

$$U_{(s,\Phi)} = U_{(\tilde{s}, \tilde{\Phi})} A^{s_n} B^{1-s_n} e^{i\phi_n\sigma_z}. \tag{65}$$

When $s_n = 1$, we have the following relation on the highest terms in a :

$$P_m(b) = \frac{e^{i\phi_n}}{2} (\tilde{P}_{m-1}(b) + \tilde{Q}_{m-1}(b)), \tag{66}$$

$$Q_m(b) = \frac{e^{-i\phi_n}}{2} (\tilde{P}_{m-1}(b) + \tilde{Q}_{m-1}(b)). \tag{67}$$

These satisfy $P_m(b) = e^{2i\phi_n} Q_m(b)$. When $s_n = 0$, we have $P_{n-m}(a) = e^{2i\phi_n} Q_{n-m}(a)$ from the similar discussion, so (v') is satisfied. $\square$

However, these conditions (i)-(v') are actually not sufficient, i.e. " $\Leftarrow$ " of the M-QSP Theorem does not hold just with this revision. We show this by a counterexample, where conditions (i)-(v') are satisfied but no $U_{(s,\Phi)}$ can be constructed. Note that this counterexample is constructed based on the counterexample for Conjecture 2.1, but this proves the insufficiency of the conditions, which is another non-trivial task.

Define polynomials $\tilde{P}$ and $\tilde{Q}$ for $n = 4$ and $m = 2$ as in Eq. (38) and Eq. (39), which satisfy conditions (i), (ii'), (iii'), and (iv) but not (v'). Note that the coefficients of $\tilde{P}$ and $\tilde{Q}$ are all nonzero except for $\tilde{Q}_{00}$, the constant term of $\tilde{Q}$, which is restricted to zero by the condition (ii'). Taking the contraposition of the revised necessary conditions of M-QSP,

there exists no $U_{(s,\Phi)}$ for $\tilde{P}$ and $\tilde{Q}$. We construct P and Q for $n = 5$ and $m = 3$ by Eq. (48) with a phase angle φ .

$$\begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix} \equiv \begin{pmatrix} \tilde{P} & \tilde{Q} \\ -\tilde{Q}^* & \tilde{P}^* \end{pmatrix} A e^{i\varphi\sigma_z} \quad (68)$$

Because $\tilde{P}$ and $\tilde{Q}$ satisfy (i), (ii'), (iii'), and (iv), P and Q also satisfy (i), (ii'), (iii'), and (iv). Regarding (v'), we have

$$P_3(b) = \frac{e^{i\varphi}}{2}(\tilde{P}_2(b) + \tilde{Q}_2(b)), \quad (69)$$

$$Q_3(b) = \frac{e^{-i\varphi}}{2}(\tilde{P}_2(b) + \tilde{Q}_2(b)), \quad (70)$$

so $P_3(b) = e^{2i\varphi}Q_3(b)$ is satisfied. If we look at the highest and lowest degrees in b , this suggests $P_{32} = e^{2i\varphi}Q_{32}$ and $P_{3-2} = e^{2i\varphi}Q_{3-2}$. Using (ii'), the latter relationship can be restated in terms of the highest degree in b , and we have $P_{32} = e^{2i\varphi}Q_{32}$ and $P_{-32} = -e^{2i\varphi}Q_{-32}$. Because these coefficients are all nonzero, $P_2(a) = e^{2i\varphi'}Q_2(a)$ cannot be satisfied. Therefore, P and Q satisfy (v') only for the highest order terms of a . Now we assume that there exists $U_{(s,\Phi)}$ for these P and Q , which satisfy (i)-(v').

$$\begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix} = U_{(s,\Phi)} \quad (71)$$

Because of $P_3(b) = e^{2i\varphi}Q_3(b)$ and $P_2(a) \neq e^{2i\varphi'}Q_2(a)$, the last operator needs to be A rather than B . Then we can express this $U_{(s,\Phi)}$ as

$$U_{(s,\Phi)} = \left(e^{i\phi_0\sigma_z} \prod_{k=1}^4 A^{s_k}(a) B^{1-s_k}(b) e^{i\phi_k\sigma_z} \right) A e^{i\phi_5\sigma_z}. \quad (72)$$

Rewriting the equation as

$$U_{(s,\Phi)} e^{-i\phi_5\sigma_z} A^\dagger = e^{i\phi_0\sigma_z} \prod_{k=1}^4 A^{s_k}(a) B^{1-s_k}(b) e^{i\phi_k\sigma_z}, \quad (73)$$

we see the highest degree term of a on the left-hand side needs to vanish so that both sides have the same degree. Calculating the left-hand side as

$$\begin{aligned} U_{(s,\Phi)} e^{-i\phi_5\sigma_z} A^\dagger &= \begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix} e^{-i\phi_5\sigma_z} A^\dagger \\ &= \begin{pmatrix} \frac{a+a^{-1}}{2} e^{-i\phi_5} P - \frac{a-a^{-1}}{2} e^{i\phi_5} Q & -\frac{a-a^{-1}}{2} e^{-i\phi_5} P + \frac{a+a^{-1}}{2} e^{i\phi_5} Q \\ \cdot & \cdot \end{pmatrix}, \end{aligned} \quad (74)$$

we get the condition on the highest degree terms of a as

$$e^{-i\phi_5} P_3(b) - e^{i\phi_5} Q_3(b) = e^{-i\phi_5} P_3(b) (1 - e^{2i(\phi_5-\varphi)}) = 0. \quad (75)$$

Therefore, ϕ_5 is either φ or $\varphi + \pi$. When $\phi_5 = \varphi$, Eq. (73) becomes

$$\begin{aligned} U_{(s,\Phi)} e^{-i\varphi\sigma_z} A^\dagger &= \begin{pmatrix} \tilde{P} & \tilde{Q} \\ -\tilde{Q}^* & \tilde{P}^* \end{pmatrix} \\ &= e^{i\phi_0\sigma_z} \prod_{k=1}^4 A^{s_k}(a) B^{1-s_k}(b) e^{i\phi_k\sigma_z}, \end{aligned} \quad (76)$$

meaning $\tilde{P}$ and $\tilde{Q}$ have $U_{(\tilde{s}, \tilde{\Phi})}$. This contradicts with the fact that $\tilde{P}$ and $\tilde{Q}$ do not have $U_{(\tilde{s}, \tilde{\Phi})}$. Similarly, when $\phi_5 = \varphi + \pi$,

$$\begin{aligned} U_{(s, \Phi)} e^{-i(\varphi + \pi)\sigma_z} A^\dagger &= \begin{pmatrix} -\tilde{P} & -\tilde{Q} \\ \tilde{Q}^* & -\tilde{P}^* \end{pmatrix} \\ &= e^{i\phi_0\sigma_z} \prod_{k=1}^4 A^{s_k}(a) B^{1-s_k}(b) e^{i\phi_k\sigma_z} \end{aligned} \quad (77)$$

is also inconsistent with the assumption. Thus, there exists no $U_{(s, \Phi)}$ for these P and Q satisfying (i)-(v').

Therefore, the revised necessary conditions (i)-(v') are not sufficient for the existence of $U_{(s, \Phi)}$. To construct the valid M-QSP Theorem, some additional condition is required.

5 Conclusion

We discussed inconsistencies appearing in the original paper of M-QSP [1] and provided a revised theorem on polynomials implementable with M-QSP. After modifying the inconsistencies, it turned out the currently known conditions are in fact only necessary conditions and not sufficient. Under this circumstance, the important future research is to find necessary and sufficient conditions for M-QSP as ones for QSP [7, Theorem 3]. Another key direction is to identify, even partly, the polynomials to which M-QSP is applicable.

5.1 Developments after preprint release

After the appearance of this paper, many variants of M-QSP have been proposed, but unfortunately, the necessary and sufficient conditions are still not clarified in any protocol. In Ref. [2], they use W_z convention (e.g. signal operators are expressed as Z -rotation) and rotation operators are generalized to $SU(2)$, where only necessary conditions are revealed. Similarly in Ref. [8], they employ an extended version of W_z convention and they use $SU(3)$ operator as rotation operators. Here, they give sufficient but not necessary conditions, and it is unclear how these conditions can be translated into the original M-QSP framework. Ref. [9] develops their protocol as the iterated version of standard QSP in W_x convention (e.g. signal operators are expressed as X -rotation), where they also provide the application to bosonic quantum simulation.

Compared with these methods, the original M-QSP framework has the advantage in its simplicity: it can be characterized by phase angles and ordering parameters, and the implementation is straightforward. As its potential application, it can provide an efficient algorithm for quantum state preparation, which is a task to prepare a state with a specific function encoded in the amplitudes [10]. Toward the actual application, Ref. [11] proposes a decision program to determine if a given pair of polynomials (P, Q) is implementable with M-QSP. However, any practical example of a polynomial P that is implementable with M-QSP nor the way to construct the complementary polynomial Q is not known yet.

Acknowledgement

This work is supported by MEXT Quantum Leap Flagship Program (MEXTQLEAP) Grant No. JPMXS0120319794, and JST COI-NEXT Program Grant No. JPMJPF2014.

References

- [1] Zane M. Rossi and Isaac L. Chuang. “Multivariable quantum signal processing (MQSP): prophecies of the two-headed oracle”. [Quantum](#) **6**, 811 (2022).
- [2] 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](#).
- [3] Peter W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. [Proceedings 35th Annual Symposium on Foundations of Computer Science](#), 124-134 (1994).
- [4] Seth Lloyd. “Universal quantum simulators”. [Science](#) **273**, 1073–1078 (1996).
- [5] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. “Quantum algorithm for linear systems of equations”. [Phys. Rev. Lett.](#) **103**, 150502 (2009).
- [6] Guang H. Low, Theodore J. Yoder, and Isaac L. Chuang. “Methodology of resonant equiangular composite quantum gates”. [Phys. Rev. X](#) **6**, 041067 (2016).
- [7] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. “Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics”. [Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing](#), 193–204 (2019).
- [8] Lorenzo Laneve and Stefan Wolf. “On multivariate polynomials achievable with quantum signal processing” (2024). [arXiv:2407.20823](#).
- [9] Niladri Gomes, Hokiat Lim, and Nathan Wiebe. “Multivariable qsp and bosonic quantum simulation using iterated quantum signal processing” (2024). [arXiv:2408.03254](#).
- [10] Hitomi Mori, Kosuke Mitarai, and Keisuke Fujii. “Efficient state preparation for multivariate monte carlo simulation” (2024). [arXiv:2409.07336](#).
- [11] Yuki Ito, Hitomi Mori, Kazuki Sakamoto, and Keisuke Fujii. “Polynomial time constructive decision algorithm for multivariable quantum signal processing” (2024). [arXiv:2410.02332](#).