Doubling the efficiency of Hamiltonian simulation via generalized quantum signal processing

Dominic W. Berry [1,*] Danial Motlagh [2,3] Giacomo Pantaleoni [1] and Nathan Wiebe [3,4,5]

[1]*School of Mathematical and Physical Sciences, Macquarie University, Sydney, New South Wales 2109, Australia*

[2]*Xanadu, Toronto, Ontario M5G 2C8, Canada*

[3]*Department of Computer Science, University of Toronto, Toronto, Ontario M5S 2E4, Canada*

[4]*Pacific Northwest National Laboratory, Richland, Washington 521220, USA*

[5]*Canadian Institute for Advanced Research, Toronto, Ontario M5G 1M1, Canada*

(Received 6 March 2024; accepted 14 June 2024; published 12 July 2024)

Quantum signal processing provides an optimal procedure for simulating Hamiltonian evolution on a quantum computer using calls to a block encoding of the Hamiltonian. In many situations it is possible to control between forward and reverse steps with almost identical cost to a simple controlled operation. We show that it is then possible to reduce the cost of Hamiltonian simulation by a factor of 2 using the recent results of generalized quantum signal processing.

DOI: 10.1103/PhysRevA.110.012612

I. INTRODUCTION

Early quantum algorithms for Hamiltonian simulation were based on product formulas [1,2], but more advanced procedures were developed based on quantum walks [3,4] and linear combinations of unitaries [5,6]. Those algorithms provided complexity scaling logarithmic in the inverse error $1/\epsilon$ which is optimal, but the joint scaling between $\log(1/\epsilon)$ and the time t was not optimal, because it was in the form of a product rather than a sum.

Further advances using corrections improved on that $\mathcal{O}(t\log(1/\epsilon))$ complexity [7,8], but the true additive complexity was not achieved until the development of quantum signal processing by Low and Chuang [9]. That proposal was based on quantum walk steps for Hamiltonians, but Low and Chuang further generalized the procedure by using qubitization in Ref. [10]. Qubitisation generalizes the prior proposals for quantum walks and linear combinations of unitaries by using *block encoding*.

II. BLOCK ENCODING AND QUANTUM SIGNAL PROCESSING

In block encoding a Hamiltonian, an ancilla system is used and a unitary V is chosen such that

$$(\langle 0|\otimes\mathbb{1})V(|0\rangle\otimes\mathbb{1}) = \frac{H}{\lambda}\,, \tag{1}$$

where $|0\rangle$ is a state for the ancilla system. That is, preparing $|0\rangle$ on the ancilla system, applying V jointly between the ancilla and target systems, then projecting onto $|0\rangle$ for the ancilla, results in H applied to the target system up to a multiplicative factor of $1/\lambda$. The quantum walk step is then constructed by combining V with a reflection about $|0\rangle$ on the ancilla system as

$$U = i(2|0\rangle\langle 0|\otimes\mathbb{1}_s - \mathbb{1})V\,, \tag{2}$$

where $\mathbb{1}_s$ is the identity on just the target system, and $\mathbb{1}$ is on both the ancilla and target. For this construction V should be self-inverse, and it is easy to make it so in most cases. Each eigenvalue E_k of H then results in two eigenvalues $\pm e^{\pm i\arcsin(E_k/\lambda)}$ for U.

Alone, this walk operator does not directly provide us with a dynamic simulation. A technique is needed to transform the walk operator U into the Hamiltonian evolution e^{-iHt}. That is, both eigenvalues above need to be transformed into e^{-iE_kt}. If we write the eigenvalues of U as $e^{i\theta}$, then the two eigenvalues of U correspond to $\theta = \arcsin(E_k/\lambda)$ and $\theta = \pi - \arcsin(E_k/\lambda)$. In both cases it is found that $\sin\theta = E_k/\lambda$, so transforming the eigenvalues of U as $e^{i\theta}\mapsto e^{-i\tau\sin\theta}$ with $\tau := t\lambda$ gives the desired Hamiltonian evolution.

In quantum signal processing [9,11–14] this transformation is achieved by performing applications of U controlled by an ancilla qubit. For an eigenstate of U, this controlled operator corresponds to an effective X rotation on the control qubit dependent on θ. By choosing a sequence of controlled operations interspersed with Z rotations with carefully chosen angles, it is possible to enact a transformation of the form [9]

$$F_\theta := \begin{bmatrix} A(\theta)+iB(\theta) & iC(\theta)+D(\theta) \\ iC(\theta)-D(\theta) & A(\theta)-iB(\theta)\end{bmatrix}. \tag{3}$$

Low and Chuang then observed that

$$(\langle +|\otimes\mathbb{1})F_\theta(|+\rangle\otimes\mathbb{1}) = A(\theta)+iC(\theta)\,, \tag{4}$$

which implies that if $A(\theta)=\cos(\tau\sin(\theta))$ and $C(\theta) = -\sin(\tau\sin(\theta))$, but $B(\theta)=D(\theta)=0$, then this will transform the walk's eigenvalues to the correct eigenvalues for e^{-iHt}. Below we ignore the minus sign on $C(\theta)$ for simplicity, because it does not affect the analysis. In practice it is not possible to obtain these exact equalities, but they can be obtained with high accuracy with $\mathcal{O}(\lambda t+\log(1/\epsilon))$ steps. This number of steps yields simulations that have optimal combined scaling in both ϵ and t [9].

Subsequently, it was realized that in situations requiring estimation of eigenvalues it is possible to perform phase

*Contact author: dominic.berry@mq.edu.au

estimation directly on the walk step, avoiding the need to perform Hamiltonian simulation [15,16], and further that the phase returned by each application of the walk can be doubled by a simple trick. This trick involves noting that the walk operator U step can be flipped to its inverse by moving the reflection before the block encoding unitary V. For such an application one can take advantage of the control between forward and reverse quantum walk steps to provide a factor of 2 improvement in complexity for eigenvalue estimation [17]. That then raises the question of whether such an improvement is possible for Hamiltonian simulation. In this work we show that it is indeed possible.

In Hamiltonian simulation via quantum signal processing as described in Ref. [9], there are controlled operations selecting between the identity and the walk operator U (Fig. 1(b) of Ref. [9]). The number of controlled operations is denoted N, but in Theorem 1 of that work the order is $N/2$. If the eigenvalue of U is $e^{i\theta}$, then the controlled operation (on the system eigenstate) has eigenvalues of 1 and $e^{i\theta}$. As explained below Eq. (5) of Ref. [9], by alternating how the controlled operators are performed one can equivalently obtain the rotation operator $\hat{R}_\phi(\theta)$ (p. 1 of Ref. [9]) with eigenvalues of $e^{\pm i\theta/2}$.

III. BIDIRECTIONAL QUANTUM SIGNAL PROCESSING

We propose the following strategy to obtain the doubling observed in Ref. [17] by using the above approach, but changing it to use a controlled operation that selects between U and $U^\dagger$. This would then implement $\hat{R}_\phi(2\theta)$ with eigenvalues of $e^{\pm i\theta}$. Then the upper limits for the sums over the values of k in (iii) and (iv) in Theorem 1 of Ref. [9] would be doubled to read

$$\text{(iii)} \quad A(\theta) = \sum_{k\,\text{even}=0}^{N} P_K \cos(k\theta)\,, \tag{5}$$

$$\text{(iv)} \quad C(\theta) = \sum_{k\,\text{even}=2}^{N} Q_K \sin(k\theta)\,. \tag{6}$$

In order to approximate the Hamiltonian evolution, we aim to obtain $A(\theta)$ and $C(\theta)$ given by the Jacobi-Anger expansion (Eq. (16) of Ref. [9])

$$A(\theta) \approx \cos[\tau\sin(\theta)] = J_0(\tau) + 2\sum_{k\,\text{even}>0}^{\infty} J_k(\tau)\cos(k\theta)\,, \tag{7}$$

$$C(\theta) \approx \sin[\tau\sin(\theta)] = 2\sum_{k\,\text{odd}>0}^{\infty} J_k(\tau)\sin(k\theta)\,, \tag{8}$$

where $J_k(\tau)$ are Bessel functions of the first kind. The problem is now that the control between U and $U^\dagger$ gives $C(\theta)$ with only *even* orders, whereas for the Jacobi-Anger expansion we need $C(\theta)$ with only *odd* orders.

We could address this issue by multiplying $C(\theta)$ by $e^{i\theta}$. This function now contains only even powers of $e^{i\theta}$, but it is now complex, so the result as presented in Ref. [9] no longer applies. Instead we can use the result as given in Ref. [12], which provides the theorem below.

Theorem 1 (Generalized Quantum Signal Processing). $\forall d \in \mathbb{N},\ \exists\,\vec{\theta},\vec{\phi} \in \mathbb{R}^{d+1},\ \lambda \in \mathbb{R}$ s.t:

$$\left(\prod_{j=1}^{d} R(\theta_j,\phi_j)\begin{bmatrix} U & 0 \\ 0 & \mathbb{1}\end{bmatrix}\right) R(\theta_0,\phi_0,\lambda) = \begin{bmatrix} P(U) & . \\ Q(U) & . \end{bmatrix}$$

if and only if

(1) $P,\ Q \in \mathbb{C}[z]$ and $\deg(P), \deg(Q) \leqslant d$.
(2) $\forall z \in \mathbb{C},\ |z| = 1 \Rightarrow |P(z)|^2 + |Q(z)|^2 = 1$.

Here $R(\theta,\phi,\lambda)$ is a parameterized SU(2) rotation on the ancilla qubit. For succinctness we have written $R(\theta_j,\phi_j)$ in place of $R(\theta_j,\phi_j,0)$. The functions $P(z)$ and $Q(z)$ are now general complex functions, as opposed to $A(\theta)$ and $C(\theta)$ being real functions above. Analogous results were also given in Refs. [13,14].

The convention in Ref. [12] is that only controlled U operations are performed, so the polynomials $P(U)$ and $Q(U)$ contain only non-negative powers of U. Now if we were to perform controlled applications of U^2, then we would obtain only positive even powers of U. If we perform N controlled operations then we obtain a maximum power $2N$ of U. At the end we could consider performing $(U^\dagger)^N$, which would then give us powers of U from $-N$ to N in steps of 2. But, performing N controlled applications of U^2 followed by $(U^\dagger)^N$ is logically equivalent to performing N controlled applications of U versus $U^\dagger$.

We therefore reformulate the protocol above to use directionally controlled unitaries.

Theorem 2. $\forall d \in \mathbb{N},\ \exists\,\vec{\theta},\vec{\phi} \in \mathbb{R}^{d+1},\ \lambda \in \mathbb{R}$ s.t:

$$\left(\prod_{j=1}^{d} R(\theta_j,\phi_j)\begin{bmatrix} U & 0 \\ 0 & U^\dagger\end{bmatrix}\right) R(\theta_0,\phi_0,\lambda) = \begin{bmatrix} P(U) & -Q(U)^\dagger \\ Q(U) & P(U)^\dagger \end{bmatrix}$$

if and only if

(1) $P,\ Q \in \mathbb{C}[z^{-1}, z]$ and $\deg(P), \deg(Q) \leqslant d$.
(2) $\text{Parity}(P), \text{Parity}(Q) = d \bmod 2$.
(3) $\forall z \in \mathbb{C},\ |z| = 1 \Rightarrow |P(z)|^2 + |Q(z)|^2 = 1$.

Here, we have provided the explicit form for all 4 blocks of polynomials generated using the above procedure; the proof for this form is given in Appendix B. Theorem 2 implies that the result of Ref. [12] equally well applies to generating functions P and Q that have positive and negative powers of U. The operator U is effectively of the form $U = e^{i\mathcal{H}} = e^{i\arcsin(H/\lambda)}$, ignoring $\pm$ and the action on the ancilla for simplicity. We can, therefore, produce

$$P(U) \approx U\cos[\tau\sin(\mathcal{H})] \approx \sum_{m=-K/2}^{K/2} J_{2m}(\tau)U^{2m+1}\,, \tag{9}$$

$$Q(U) \approx i\sin[\tau\sin(\mathcal{H})] \approx i\sum_{m=-K/2-1}^{K/2} J_{2m+1}(\tau)U^{2m+1}\,. \tag{10}$$

Here K is even and $K+1 = d$ is the number of controlled operations. In this approximation we have only odd powers of U, but they are in steps of 2 as required. It is convenient to include the factor of U in P rather than Q, so the maximum power is the same for both. The key improvement here is

that the order is the same as the number of controlled operations, not *half* as it is in standard quantum signal processing from Ref. [9] (where the number of controlled operations is denoted N).

We then remove the extra factor of U in $P(U)$ by applying an initial controlled U and a final controlled $U^\dagger$ to give

$$\begin{bmatrix} U^\dagger & 0 \\ 0 & \mathbb{1} \end{bmatrix} \begin{bmatrix} P & -Q^\dagger \\ Q & P^\dagger \end{bmatrix} \begin{bmatrix} \mathbb{1} & 0 \\ 0 & U \end{bmatrix} = \begin{bmatrix} U^\dagger P & -Q^\dagger \\ Q & P^\dagger U \end{bmatrix}. \tag{11}$$

In this form we have the blocks corresponding to approximately $\cos[\tau \sin(\mathcal{H})]$ and $i \sin[\tau \sin(\mathcal{H})]$ similar to the form in Eq. (3) from Ref. [9]. Therefore, using $|+\rangle$ on the ancilla qubit yields the Hamiltonian evolution on the target system.

IV. COMPLETING THE SUM OF SQUARES

Now the remaining problem is the requirement that $|P|^2 + |Q|^2$ is *exactly* equal to 1. This sum will not be exactly 1 because the Jacobi-Anger expansion is necessarily truncated. In fact, if we use the truncated sums as above then $|P|^2 + |Q|^2$ can be slightly larger than 1. That problem is avoided by simply multiplying those truncated sums by a factor slightly less than 1 to ensure that the sum is no larger than 1 (as used in Ref. [9]). We then need to find new functions to add such that the sum of squares is exactly 1.

For convenience we define

$$P_K(U) := J_0(\tau) + \sum_{m=-K/2}^{K/2} J_{2m}(\tau)\, U^{2m}, \tag{12}$$

$$Q_K(U) := i \sum_{m=-K/2-1}^{K/2} J_{2m+1}(\tau)\, U^{2m+1}, \tag{13}$$

where we have removed the factor of U from P. If $\alpha < 1$ is the factor needed to avoid the sum of squares being larger than 1, we need to find real functions P', Q' such that

$$\begin{aligned} &|\alpha P_K + iP'|^2 + |\alpha Q_K + Q'|^2 \\ &\quad = |\alpha P_K|^2 + |\alpha Q_K|^2 + |P'|^2 + |Q'|^2 = 1. \end{aligned} \tag{14}$$

This can alternatively be formulated as finding P', Q' such that

$$P'^2 + Q'^2 = 1 - \alpha^2 \left(P_K^2 - Q_K^2\right). \tag{15}$$

This is a problem of finding two polynomials such that the sum of squares is equal to 1. The subtlety here is that the parities of P_K and P' must match, as must those of Q_K and Q'. This is because we will be generating $U(\alpha P_K + P')$ and $\alpha Q_K + Q'$ using the procedure of Theorem 2, and these must have U to only odd orders. This means that P' must have only even orders and Q' must have only odd. Our challenge is therefore to construct P', Q' with the correct parity to give the sum of squares.

A procedure for constructing polynomials was given in Ref. [12], but that gives polynomials with the same parity, so is not suitable. To provide an alternative method for constructing polynomials, we rewrite P_K, Q_K as

$$\begin{aligned} P_K(\theta) &= J_0(\tau) + 2 \sum_{k\,\text{even}>0}^{K} J_k(\tau)\, \cos(k\theta) \\ &= J_0(\tau) + 2 \sum_{k\,\text{even}>0}^{K} J_k(\tau)\, T_k(\cos(\theta)) \\ &= J_0(\tau) + 2 \sum_{m=1}^{K/2} J_{2m}(\tau)\, T_{2m}(x), \end{aligned} \tag{16}$$

$$\begin{aligned} Q_K(\theta) &= 2i \sum_{k\,\text{odd}>0}^{K} J_k(\tau)\, \sin(k\theta) \\ &= 2i \sum_{k\,\text{odd}>0}^{K} J_k(\tau)\, \sin(\theta)\, U_{k-1}(\cos(\theta)) \\ &= 2\sqrt{x^2-1} \sum_{m=0}^{K/2} J_{2m+1}(\tau)\, U_{2m}(x), \end{aligned} \tag{17}$$

where T_k and U_k are Chebyshev polynomials of the first and second kind, respectively, and $x = \cos(\theta)$. We can then construct P', Q' by analysis of polynomials in x.

We will analyze the case where the polynomial we wish to construct $1 - \alpha^2(P_K^2 - Q_K^2)$ is non-negative. We can then use reasoning based on Ref. [18]. A non-negative polynomial $p(x)$ can be written as

$$p(x) = \prod_j (x - c_j)^2 \prod_k \left[(x - a_k)^2 + b_k^2\right], \tag{18}$$

where c_j, a_k, b_k are real numbers. Since $p(x)$ must be non-negative for all real x, we will need to reason about the case where $|x| > 1$ even though here we use only $|x| \leqslant 1$. If we first choose

$$q(x) = \prod_j (x - c_j) \prod_k (x - a_k + ib_k), \tag{19}$$

then $p(x)$ may be expressed as a sum of squared polynomials as [18]

$$p(x) = [\mathrm{Re}(q(x))]^2 + [\mathrm{Im}(q(x))]^2. \tag{20}$$

In our case $p(x)$ is *even*, so we know that for every root there is a corresponding negative root. Therefore for every root pair $a_k \pm ib_k$ there is a pair $-a_k \pm ib_k$; that is, for every root with (nonzero) a_k there is another with the sign of this real part flipped. That implies $q(x)$ will contain pairs of factors as

$$(x - a_k + ib_k)(x + a_k + ib_k) = \left(x^2 - a_k^2 - b_k^2\right) + 2ib_k x. \tag{21}$$

Similarly, for each root c_j there must be a corresponding negative root, so $q(x)$ will contain pairs of factors as $(x - c_j)(x + c_j) = (x^2 - c_j^2)$. We will multiply many of these to construct $q(x)$, then at the end we will be using the real and imaginary parts for P' and Q'.

A particularly useful feature is that in both cases the real part has even parity and the imaginary part has odd parity. Whenever multiplying expressions where the real and imaginary parts have different parities, we obtain a resulting

expression with the same property. That is, we have the rules

$$(\text{even} + i \times \text{odd})(\text{even} + i \times \text{odd}) \mapsto (\text{even} + i \times \text{odd}),$$

$$(\text{even} + i \times \text{odd})(\text{odd} + i \times \text{even}) \mapsto (\text{odd} + i \times \text{even}),$$

$$(\text{odd} + i \times \text{even})(\text{odd} + i \times \text{even}) \mapsto (\text{even} + i \times \text{odd}),$$

where we use *even* and *odd* to indicate general even or odd polynomials. What this means is that at the end $q(x)$ must have different parities for the real and imaginary parts. Since the real and imaginary parts are used for P', Q', we can obtain P', Q' with the desired parities.

What remains to show is that $1 - \alpha^2(P_K^2 - Q_K^2)$ is non-negative, regardless of the value of x. It is trivial that it is non-negative in the range $x \in [-1, 1]$, because the Jacobi-Anger expansion gives a result close to 1 for $P_K^2 - Q_K^2$, and we choose α to ensure it is no larger than 1. We will, therefore, only consider the case where $|x| > 1$. Our theorem can be given as follows.

Theorem 3. For $K \geqslant 2$ even, $0 \leqslant \tau \leqslant K$, and P_K, Q_K defined as

$$P_K(x) = J_0(\tau) + 2\sum_{m=1}^{K/2} J_{2m}(\tau)\, T_{2m}(x)\,,$$

$$Q_K(x) = 2\sqrt{x^2-1}\sum_{m=0}^{K/2} J_{2m+1}(\tau)\, U_{2m}(x)\,, \tag{22}$$

the inequality $P_K^2 - Q_K^2 \leqslant 1$ is satisfied for $|x| \geqslant 1$.

We prove this theorem in Appendix A. Together with the obvious result for $|x| \leqslant 1$, this shows that the polynomial $1 - \alpha^2(P_K^2 - Q_K^2)$ is non-negative as required.

Hence, what we have shown is that it is possible to construct an approximation of Hamiltonian evolution using a number of controls between U and $U^\dagger$ that is half the number of controlled unitaries normally used in quantum signal processing. We define P_K, Q_K as above and find $\alpha \approx 1$ such that $\alpha(P_K^2 - Q_K^2) \leqslant 1$ for $|x| \leqslant 1$. Then we obtain the polynomial $1 - \alpha^2(P_K^2 - Q_K^2) \geqslant 0$ for all real x, and use the procedure from Ref. [18] to find polynomials P', Q' where P' is even and Q' is odd such that $\alpha^2(P_K^2 - Q_K^2) + P'^2 + Q'^2 = 1$.

We then choose $P(U) = U(\alpha P_K(U) + iP'(U))$ and $Q(U) = \alpha Q_K(U) + Q'(U)$, and use the method of Theorem 2 to produce these polynomials with complex coefficients. We combine that with two extra controlled operations as in Eq. (11) to correct the factor on U, and then with the ancilla qubit starting in the $|+\rangle$ state we obtain the Hamiltonian evolution on the target system.

The majority of the complexity is in using Theorem 2 to produce $P(U), Q(U)$, where the number of controlled operations needed is half what it is in Ref. [9]. There are two additional controlled operations used, but these are a trivial contribution to the complexity. Hence, these modifications together enable simulation of quantum dynamics with approximately half the number of queries as in standard quantum signal processing [9]. For this speedup we just need to be able to control between U and $U^\dagger$ with similar complexity to controlling U. In most practical cases that is true, because the control can be achieved by controlling reflections on an ancilla system used in block encoding the Hamiltonian. Therefore this approach can give a factor of 2 speedup for Hamiltonian simulation very broadly. Moreover, this bidirectional form of generalized QSP could be used to achieve similar speedups for many other applications of QSP, though it would need to be shown that it is possible to complete the sum of squares (our result is specific to simulation).

ACKNOWLEDGMENTS

D.W.B. worked on this project under a sponsored research agreement with Google Quantum AI. D.W.B. is also supported by Australian Research Council Discovery Projects No. DP210101367 and No. DP220101602. N.W. is supported by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Co-Design Center for Quantum Advantage under Contract No. DE-SC0012704.

APPENDIX A: PROOF OF POSITIVITY OF THE POLYNOMIAL

In this Appendix we give the proof that the polynomial is positive, as described in Theorem 3.

Proof. For $|x| \geqslant 1$ the two functions can be written as, using standard properties of Chebyshev polynomials,

$$\begin{aligned} P_K &= J_0(\tau) + 2\sum_{m=1}^{K/2} J_{2m}(\tau)\, T_{2m}(x) \\ &= J_0(\tau) + 2\sum_{m=1}^{K/2} J_{2m}(\tau)\, \cosh(2m\,\text{arcosh}|x|) \\ &= J_0(\tau) + \sum_{m=1}^{K/2} J_{2m}(\tau)(y^{2m} + y^{-2m}) \\ Q_K &= 2\sqrt{x^2-1}\sum_{m=0}^{K/2} J_{2m+1}(\tau)\, U_{2m}(x) \\ &= 2\sum_{m=0}^{K/2} J_{2m+1}(\tau)\, \sinh((2m+1)\,\text{arcosh}|x|) \\ &= \sum_{m=0}^{K/2} J_{2m+1}(\tau)\,(y^{2m+1} - y^{-(2m+1)})\,, \end{aligned} \tag{A1}$$

where

$$y = \exp(\text{arcosh}|x|) = |x| + \sqrt{x^2-1}\,. \tag{A2}$$

The case $|x| \geqslant 1$ is equivalent to $y \geqslant 1$. In order to show $P_K^2 - Q_K^2 \leqslant 1$, it is sufficient to show the three inequalities

$$P_K + Q_K \leqslant \exp(\tau(y - 1/y)/2), \tag{A3}$$

$$P_K - Q_K \leqslant \exp(-\tau(y - 1/y)/2), \tag{A4}$$

$$P_K + Q_K \geqslant 0. \tag{A5}$$

Given these inequalities, multiplying the first by the second gives $P_K^2 - Q_K^2 \leqslant 1$. The third inequality is used to ensure that multiplying $P_K - Q_K$ by $P_K + Q_K$ cannot change the sign of $P_K - Q_K$.

The first inequality in Eq. (A3) is obtained via noting that the Bessel functions $J_m(\tau)$ are non-negative for $m \geqslant \tau \geqslant 0$. Because $y \geqslant 1$ both $y^{2m} + y^{-2m}$ and $y^{2m+1} - y^{-(2m+1)}$ are non-negative as well. That gives us

$$\begin{aligned} P_K + Q_K &= \cosh(\tau(y-1/y)/2) - \sum_{m=K/2+1}^{\infty} J_{2m}(\tau)(y^{2m} + y^{-2m}) + \sinh(\tau(y-1/y)/2) \\ &\quad - \sum_{m=K/2+1}^{\infty} J_{2m+1}(\tau)\,(y^{2m+1} - y^{-(2m+1)}) \geqslant \cosh(\tau(y-1/y)/2) + \sinh(\tau(y-1/y)/2) \\ &= \exp(\tau(y-1/y)/2)\,. \end{aligned} \tag{A6}$$

We have used the fact that $2m$ and $2m+1$ are greater than K for $m > K/2$, and $K \geqslant \tau$, so the Bessel functions are all non-negative.

For the second inequality in Eq. (A4) we start by using the Maclaurin series for Bessel functions to give

$$\begin{aligned} \sum_{m=K/2+1}^{\infty} J_{2m}(\tau)\,y^{2m} - \sum_{m=K/2+1}^{\infty} J_{2m+1}(\tau)\,y^{2m+1} &= \sum_{m=K+2}^{\infty} J_m(\tau)\,(-y)^m \\ &= \sum_{m=K+2}^{\infty} \left(-\frac{\tau y}{2}\right)^m \sum_{n=0}^{\infty} \frac{(-1)^n}{n!(m+n)!}\left(\frac{\tau}{2}\right)^{2n} \\ &= \sum_{n=0}^{\infty} \frac{1}{n!}\left(\frac{\tau}{2}\right)^{2n} z^{-n} \sum_{m=K+2}^{\infty} \frac{1}{(m+n)!}(-z)^{m+n} \\ &= \sum_{n=0}^{\infty} \frac{1}{n!}\left(\frac{\tau}{2y}\right)^{n} \sum_{m=K+n+2}^{\infty} \frac{1}{m!}(-z)^m\,, \end{aligned} \tag{A7}$$

where $z := \tau y/2$. The sum over m is the remainder term of order $K+m+2$ in the expansion of $\exp(-z)$. The integral form of the remainder tells us that

$$\sum_{m=K+n+2}^{\infty} \frac{1}{m!}(-z)^m = (-1)^n \int_0^z \frac{e^{-t}}{(K+n+1)!}(z-t)^{K+n+1} dt\,. \tag{A8}$$

We can exchange the order of the integral and sum to give

$$\begin{aligned} \sum_{m=K+2}^{\infty} J_m(\tau)\,(-y)^m &= \int_0^z dt\, e^{-t}(z-t)^{K+1} \sum_{n=0}^{\infty} \frac{1}{n!(K+n+1)!}\left(-\frac{\tau(z-t)}{2y}\right)^n \\ &= \int_0^z dt\, e^{-t}(z-t)^{K+1} J_{K+1}(\sqrt{2\tau(z-t)/y})\left(\frac{2y}{\tau(z-t)}\right)^{K/2+1/2} \\ &= \int_0^z dt\, e^{-t} J_{K+1}(\sqrt{2\tau(z-t)/y})\left(\frac{2y(z-t)}{\tau}\right)^{K/2+1/2} \\ &= \frac{\tau y^{K+2}}{2} \int_0^1 dt\, e^{-(1-t)\tau y/2} J_{K+1}(\tau\sqrt{1-t})(1-t)^{K/2+1/2}\,. \end{aligned} \tag{A9}$$

The second line is obtained by using the Maclaurin series for Bessel functions again. Now for $t \in [0,1]$ and $K \geqslant \tau$ we have $K+1 > \tau\sqrt{1-t}$, and so the Bessel function is non-negative.

Hence the entire expression is an integral over a non-negative expression and must be non-negative. Therefore

$$\sum_{m=K/2+1}^{\infty} J_{2m}(\tau)\,y^{2m} \geqslant \sum_{m=K/2+1}^{\infty} J_{2m+1}(\tau)\,y^{2m+1}\,, \tag{A10}$$

which implies

$$\sum_{m=K/2+1}^{\infty} J_{2m}(\tau)\,(y^{2m} + y^{-2m}) \geqslant \sum_{m=K/2+1}^{\infty} J_{2m+1}(\tau)\,(y^{2m+1} - y^{-(2m+1)})\,. \tag{A11}$$

The left and right sides are the errors in the expansions for cosh and sinh, so this implies that

$$\cosh(\tau(y-1/y)/2) - P_K \geqslant \sinh(\tau(y-1/y)/2) - Q_K \Rightarrow P_K - Q_K \leqslant \exp(-\tau(y-1/y)/2)\,, \tag{A12}$$

which gives Eq. (A4) as required.

Next we will show the third inequality from Eq. (A5), that $P_K + Q_K$ is non-negative. We obtain

$$P_K + Q_K = \exp(\tau(y-1/y)/2) - \sum_{m=K+2}^{\infty} J_m(\tau)[y^m + (-y)^{-m}]\,. \tag{A13}$$

Similarly to Eq. (A9) we obtain

$$\sum_{m=K+2}^{\infty} J_m(\tau)\, y^m = \frac{\tau y^{K+2}}{2} \int_0^1 dt\, e^{(1-t)\tau y/2} J_{K+1}(\tau\sqrt{t})\, t^{K/2+1/2}\,, \tag{A14}$$

$$\sum_{m=K+2}^{\infty} J_m(\tau)\,(-y)^{-m} = \frac{\tau}{2\,y^{K+2}} \int_0^1 dt\, e^{-(1-t)\tau/2y} J_{K+1}(\tau\sqrt{t})\, t^{K/2+1/2}\,. \tag{A15}$$

The second integral is easily bounded as

$$\int_0^1 dt\, e^{-(1-t)\tau/2y} J_{K+1}(\tau\sqrt{t})\, t^{K/2+1/2} < \int_0^1 dt\, J_{K+1}(\tau\sqrt{t})\, t^{K/2+1/2} < J_{K+1}(\tau) \int_0^1 dt\, t^{K/2+1/2} < J_{K+1}(\tau)\frac{2}{K+3}\,. \tag{A16}$$

The upper bound on the second integral is therefore

$$\sum_{m=K+2}^{\infty} J_m(\tau)\,(-y)^{-m} \leqslant \frac{\tau}{2\,y^{K+2}} J_{K+1}(\tau)\frac{2}{K+3} \leqslant \frac{J_{K+1}(\tau)}{y^{K+2}}\,. \tag{A17}$$

For the first integral we obtain

$$\begin{aligned}
\int_0^1 dt\, e^{-t\tau y/2} J_{K+1}(\tau\sqrt{t})\, t^{K/2+1/2} &\leqslant \left(\int_0^1 dt\, e^{-t\tau y/2} J_{K+1}^2(\tau\sqrt{t})\right)^{1/2} \left(\int_0^1 dt\, e^{-t\tau y/2}\, t^{K+1}\right)^{1/2} \\
&< \left(\frac{2}{\tau^2}\int_0^\infty dg\, e^{-g^2 y/2\tau}\, g\, J_{K+1}^2(g)\right)^{1/2} \left(\int_0^1 dt\, e^{-t\tau y/2}\, t^{K+1}\right)^{1/2} \\
&= \left(\frac{2}{\tau y} e^{-\tau/y} I_{K+1}(\tau/y)\right)^{1/2} \left(\left(\frac{2}{\tau y}\right)^{K+2} \frac{1}{(K+1)!}\right)^{1/2}\,,
\end{aligned} \tag{A18}$$

where I is the modified Bessel function. In the first line we have used the Cauchy-Schwarz inequality. The second line is just a change of variables and extending the integral to infinity. For the evaluation of the integral in the final line see Ref. [19], Eq. (10.22.67). Now using Eq. (6.25) of Ref. [20] we have

$$I_{K+1}(\tau/y) \leqslant \frac{\cosh(\tau/y)}{(K+1)!}\left(\frac{\tau}{2y}\right)^{K+1}\,. \tag{A19}$$

That enables us to obtain the bound on the first sum

$$\begin{aligned}
\sum_{m=K+2}^{\infty} J_m(\tau)\, y^m &\leqslant \frac{\tau y^{K+2}}{2} e^{\tau y/2} \left(\frac{2}{\tau y} e^{-\tau/y} \frac{\cosh(\tau/y)}{(K+1)!} \left(\frac{\tau}{2y}\right)^{K+1} \left(\frac{2}{\tau y}\right)^{K+2} \frac{1}{(K+1)!}\right)^{1/2} \\
&\leqslant \frac{\cosh^{1/2}(\tau/y)}{(K+1)!} e^{\tau(y-1/y)/2} \leqslant \frac{e^{K/2}}{(K+1)!} e^{\tau(y-1/y)/2}\,.
\end{aligned} \tag{A20}$$

In the last line we have used $y \geqslant 1$, the upper bound on cosh, and the fact we choose $K \geqslant \tau$, so $\cosh^{1/2}(\tau/y) \leqslant e^K$.

Hence our total upper bound is

$$\sum_{m=K+2}^{\infty} J_m(\tau)[y^m + (-y)^{-m}] \leqslant \frac{e^{K/2}}{(K+1)!} e^{\tau(y-1/y)/2} + \frac{J_{K+1}(\tau)}{y^{K+2}} \leqslant \left(\frac{e^{K/2}}{(K+1)!} + J_{K+1}(K+1)\right) e^{\tau(y-1/y)/2}\,. \tag{A21}$$

We have used $y \geqslant 1$ and the fact that $J_{K+1}(\tau) \leqslant J_{K+1}(K+1)$ for $\tau \leqslant K+1$ [21]. Next we aim to show that the expression in round brackets is less than 1. We can use standard upper bounds for Bessel functions (Eq. (10.14.2) of Ref. [19])

to give for $K \geqslant 2$

$$J_{K+1}(K+1) < \frac{(2/9)^{1/3}}{\Gamma(2/3)(K+1)^{1/3}} \leqslant \frac{(2/9)^{1/3}}{\Gamma(2/3)3^{1/3}} \leqslant 0.32\,. \tag{A22}$$

In the second line we used the fact that the function on the first line is monotonically decreasing in K. We also have for $K \geqslant 2$

$$\frac{e^{K/2}}{(K+1)!} \leqslant \frac{e^{2/2}}{(2+1)!} < 0.46\,, \tag{A23}$$

because the expression is again monotonically decreasing in K. Hence we find that for positive even K the expression in round brackets in the last line of Eq. (A21) is less than 1, and therefore

$$\sum_{m=K+2}^{\infty} J_m(\tau)[y^m + (-y)^{-m}] < e^{\tau(y-1/y)/2} \Rightarrow P_K + Q_K = e^{\tau(y-1/y)/2} - \sum_{m=K+2}^{\infty} J_m(\tau)[y^m + (y)^{-m}] > 0\,. \tag{A24}$$

This is the third inequality in Eq. (A5), as required.

Thus we have shown the three inequalities needed to give $P_K^2 - Q_K^2 \leqslant 1$, proving the theorem. ■

APPENDIX B: BLOCK FORM FOR GENERALIZED QUANTUM SIGNAL PROCESSING

Here we show that the block form of the operator implemented in Theorem 2 is in fact of the form

$$\begin{bmatrix} P & -Q^\dagger \\ Q & P^\dagger \end{bmatrix}. \tag{B1}$$

Consider the approach for the proof of Theorem 3 of Ref. [12]. Equation (9) of that work is, for the initial rotation,

$$R(\theta_0, \phi_0, \lambda) = \begin{bmatrix} e^{i(\lambda+\phi)}\cos(\theta)\mathbb{1} & e^{i\phi}\sin(\theta)\mathbb{1} \\ e^{i\lambda}\sin(\theta)\mathbb{1} & -\cos(\theta)\mathbb{1} \end{bmatrix}. \tag{B2}$$

Here we modify it by a global phase factor to

$$R(\theta_0, \phi_0, \lambda) = \begin{bmatrix} i\,e^{i(\lambda+\phi)/2}\cos(\theta)\mathbb{1} & i\,e^{i(\phi-\lambda)/2}\sin(\theta)\mathbb{1} \\ i\,e^{-i(\phi-\lambda)/2}\sin(\theta)\mathbb{1} & -i\,e^{-i(\lambda+\phi)/2}\cos(\theta)\mathbb{1} \end{bmatrix}. \tag{B3}$$

This is of the form in Eq. (B1) with

$$P = i\,e^{i(\lambda+\phi)/2}\cos(\theta)\mathbb{1}, \tag{B4}$$

$$Q = i\,e^{i(\phi-\lambda)/2}\sin(\theta)\mathbb{1}. \tag{B5}$$

Next, we will show that the form in Eq. (B1) holds in general by using an inductive step similar to Eq. (10) of Ref. [12]. First, when performing controlled operations $|0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes U^\dagger$, that step becomes

$$\begin{bmatrix} e^{i\phi}\cos(\theta)U & e^{i\phi}\sin(\theta)U^\dagger \\ \sin(\theta)U & -\cos(\theta)U^\dagger \end{bmatrix}\begin{bmatrix} \hat{P}(U) & . \\ \hat{Q}(U) & . \end{bmatrix} = \begin{bmatrix} P(U) & . \\ Q(U) & . \end{bmatrix}. \tag{B6}$$

Next, we assume that the form in Eq. (B1) holds for $\hat{P}$, $\hat{Q}$, and adjust the global phase factors to give

$$\begin{bmatrix} i\,e^{i\phi/2}\cos(\theta)U & i\,e^{i\phi/2}\sin(\theta)U^\dagger \\ i\,e^{-i\phi/2}\sin(\theta)U & -i\,e^{-i\phi/2}\cos(\theta)U^\dagger \end{bmatrix}\begin{bmatrix} \hat{P} & -\hat{Q}^\dagger \\ \hat{Q} & \hat{P}^\dagger \end{bmatrix}$$

$$= \begin{bmatrix} i\,e^{i\phi/2}\cos(\theta)U\hat{P} + i\,e^{i\phi/2}\sin(\theta)U^\dagger\hat{Q} & -i\,e^{i\phi/2}\cos(\theta)U\hat{Q}^\dagger + i\,e^{i\phi/2}\sin(\theta)U^\dagger\hat{P}^\dagger \\ i\,e^{-i\phi/2}\sin(\theta)U\hat{P} - i\,e^{-i\phi/2}\cos(\theta)U^\dagger\hat{Q} & -i\,e^{-i\phi/2}\sin(\theta)U\hat{Q}^\dagger - i\,e^{-i\phi/2}\cos(\theta)U^\dagger\hat{P}^\dagger \end{bmatrix}. \tag{B7}$$

If we set

$$P = i\,e^{i\phi/2}\cos(\theta)U\hat{P} + i\,e^{i\phi/2}\sin(\theta)U^\dagger\hat{Q}\,, \tag{B8}$$

$$Q = i\,e^{-i\phi/2}\sin(\theta)U\hat{P} - i\,e^{-i\phi/2}\cos(\theta)U^\dagger\hat{Q}, \tag{B9}$$

then we obtain

$$\begin{bmatrix} i\,e^{i\phi/2}\cos(\theta)U & i\,e^{i\phi/2}\sin(\theta)U^\dagger \\ i\,e^{-i\phi/2}\sin(\theta)U & -i\,e^{-i\phi/2}\cos(\theta)U^\dagger \end{bmatrix}\begin{bmatrix} \hat{P} & -\hat{Q}^\dagger \\ \hat{Q} & \hat{P}^\dagger \end{bmatrix} = \begin{bmatrix} P & -Q^\dagger \\ Q & P^\dagger \end{bmatrix}. \tag{B10}$$

Hence we have shown the inductive step for Eq. (B1), so it must hold in general.

This form can also be obtained from Lemma 3 of Ref. [13], also given as Lemma 1 in Ref. [14]. That Lemma is similar to what we have provided here, except it is presented in terms of Laurent polynomials in $e^{ix/2}$, $e^{-ix/2}$. That can be obtained by alternating controlled U and controlled $U^\dagger$ operations, similar to Low and Chuang. Replacing that with a control between U and $U^\dagger$ gives the corresponding result with Laurent polynomials in e^{ix}, e^{-ix}, as we give in Theorem 2 (with $z = e^{ix}$). Note that interleaving controlled U and controlled $U^\dagger$ operations only gives the form of Lemma 1 in Ref. [14] with even d (given as L in that work). Nevertheless, Lemma 3 of Ref. [13] was proved in a general sense without requiring the z rotations to be obtained by controlled U and $U^\dagger$ operations, so their derivation also holds true for odd d.

[1] S. Lloyd, Science **273**, 1073 (1996).

[2] D. W. Berry, G. Ahokas, R. Cleve, and B. C. Sanders, Commun. Math. Phys. **270**, 359 (2007).

[3] A. M. Childs, Commun. Math. Phys. **294**, 581 (2010).

[4] D. W. Berry and A. M. Childs, Quantum Inf. Comput. **12**, 0029 (2012).

[5] A. M. Childs and N. Wiebe, Quantum Inf. Comput. **12**, 901 (2012).

[6] D. W. Berry, A. M. Childs, R. Cleve, R. Kothari, and R. D. Somma, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14 (ACM, New York, 2014), pp. 283–292.

[7] D. W. Berry and L. Novo, Quantum Inf. Comput. **16**, 1295 (2016).

[8] L. Novo and D. Berry, Quantum Inf. Comput. **17**, 623 (2017).

[9] G. H. Low and I. L. Chuang, Phys. Rev. Lett. **118**, 010501 (2017).

[10] G. H. Low and I. L. Chuang, Quantum **3**, 163 (2019).

[11] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe, in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019 (ACM, New York, NY, 2019), pp. 193–204.

[12] D. Motlagh and N. Wiebe, PRX Quantum **5**, 020368 (2024).

[13] Z. Yu, H. Yao, M. Li, and X. Wang, in *Advances in Neural Information Processing Systems*, edited by S. Koyejo, S. Mohamed, A. Agarwal, D. Belgrave, K. Cho, and A. Oh (Curran Associates, Inc., Red Hook, NY, 2022), Vol. 35, pp. 27810–27823.

[14] Y. Wang, L. Zhang, Z. Yu, and X. Wang, Phys. Rev. A **108**, 062413 (2023).

[15] D. W. Berry, M. Kieferová, A. Scherer, Y. R. Sanders, G. H. Low, N. Wiebe, C. Gidney, and R. Babbush, npj Quantum Inf. **4**, 22 (2018).

[16] D. Poulin, A. Kitaev, D. S. Steiger, M. B. Hastings, and M. Troyer, Phys. Rev. Lett. **121**, 010501 (2018).

[17] R. Babbush, C. Gidney, D. W. Berry, N. Wiebe, J. McClean, A. Paler, A. Fowler, and H. Neven, Phys. Rev. X **8**, 041015 (2018).

[18] W. Rudin, Am. Math. Mon. **107**, 813 (2000).

[19] DLMF, NIST Digital Library of Mathematical Functions, https://dlmf.nist.gov/, Release 1.1.12 of 2023-12-15, F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider, R. F. Boisvert, C. W. Clark, B. R. Miller, B. V. Saunders, H. S. Cohl, and M. A. McClain, eds.

[20] Y. L. Luke, J. Approximation Theory **5**, 41 (1972).

[21] R. B. Paris, SIAM J. Math. Anal. **15**, 203 (1984).