Lorentz quantum computer

Lorentz quantum computer

Wenhao He(何文昊)[1], Zhenduo Wang(王朕铎)[1], and Biao Wu(吴飙)[1,2,3,†]

[1] *International Center for Quantum Materials, School of Physics, Peking University, Beijing* 100871, *China*
[2] *Wilczek Quantum Center, School of Physics and Astronomy, Shanghai Jiao Tong University, Shanghai* 200240, *China*
[3] *Collaborative Innovation Center of Quantum Matter, Beijing* 100871, *China*

(Received 15 August 2022; revised manuscript received 28 November 2022; accepted manuscript online 21 December 2022)

A theoretical model of computation is proposed based on Lorentz quantum mechanics. Besides the standard qubits, this model has an additional bit, which we call hyperbolic bit (or hybit in short). A set of basic logical gates are constructed and their universality is proved. As an application, a search algorithm is designed for this computer model and is found to be exponentially faster than Grover's search algorithm.

Keywords: quantum computing, Lorentz quantum mechanics, Grover search

PACS: 03.67.Ac, 03.67.Lx, 89.70.Eg **DOI:** 10.1088/1674-1056/acad6a

1. Introduction

The theoretical models of computation had long been regarded mistakenly as a pure mathematical structure. This view was completely changed with the rise of quantum computer. This is well summarized by Deutsch,[1] "computers are physical objects, $\cdots$, what computers can or cannot do is determined by laws of physics alone". In other words, different physical theories lead to different computational models with distinct computing powers.

Currently, there are only two well established frameworks of mechanics, classical mechanics (including Maxwell equations and general relativity) and quantum mechanics (including quantum field theories).[2] Consequently, there are two types of computers, classical computer and quantum computer. It is naturally to conjecture new kinds of mechanics, and use it as a base to establish new models of computers.

We are going to discuss a computational model based on Lorentz quantum mechanics, where the dynamical evolution is complex Lorentz transformation. It was proposed in Ref. [3] as a generalization of the Bogoliubov–de Gennes equation; similar mechanics was studied a long time ago by Pauli.[4] The key feature in Lorentz mechanics, which has an indefinite metric, is that only the states with the positive norms are physically observable.

We introduce a bit called hyperbolic bit (or hybit in short). The Lorentz computer so established consists of both qubits and hybits, which are manipulated by a set of basic logical gates. The universality of these gates is rigorously proved. By construction quantum computer is a special case of Lorentz computer, we thus expect the Lorentz computer to be more powerful. This is indeed the case as we find a Lorentz search algorithm that is more powerful than the Grover's search algorithm.[5] We will discuss the physical implementation of our computer model as a single Lorentz system was recently simulated with photons.[6]

2. Lorentz quantum mechanics

Lorentz quantum mechanics was discussed in Ref. [3] as a generalization of the Bogoliubov–de Gennes equation.[3,7,8] However, this kind of generalized quantum mechanics with indefinite metric was studied a long time ago by Pauli.[4] The related mathematical structure has been studied systematically.[9] In the following, we briefly review the framework of Lorentz quantum mechanics, and then introduce the composite systems consisting of quantum systems and Lorentz systems, which are the key to our computer model.

2.1. General theory of Lorentz systems

Quantum states are vectors $|\psi\rangle$ in a Hilbert space where the inner product $\langle\psi|\psi\rangle$ is always non-negative. The states $|\psi)$ of Lorentz quantum mechanics are vectors of a linear space with inner product defined as $(\psi|\eta|\psi)$, which can be negative. The indefinite metric η is a Hermitian matrix. When η is an identity matrix, we recover the usual Hilbert space. In our following notation, when $|\ )$ is used, η is not an identity matrix; when $|\ \rangle$ is used, η is an identity matrix. The general form of Lorentz quantum mechanics is given by

$$\mathrm{i}\frac{\mathrm{d}}{\mathrm{d}t}|\psi) = \eta\hat{H}|\psi), \tag{1}$$

where $\hat{H}$ is a Hermitian Hamiltonian.

We focus our attention to the special case $\eta = \eta_{m,n}$, where[3]

$$\eta_{m,n} = \mathrm{diag}\{\underbrace{1,1,\ldots 1}_{m},\underbrace{-1,-1,\ldots -1}_{n}\}. \tag{2}$$

When $m = n$, Eq. (1) becomes the well-known Bogoliubov–de Gennes equation.[3,7] The evolution operator $\hat{\mathcal{U}}$ can be written

†Corresponding author. E-mail: wubiao@pku.edu.cn

as

$$\hat{\mathcal{U}}(t,0)=\mathrm{e}^{-\mathrm{i}\eta_{m,n}\hat{H}t}. \tag{3}$$

It can be verified that $\hat{\mathcal{U}}^{\dagger}\eta_{m,n}\hat{\mathcal{U}}=\eta_{m,n}$. This means that $\hat{\mathcal{U}}$ is a member of the generalized Lorentz group $U(m,n)$. And we call $\hat{\mathcal{U}}$ complex Lorentz transformation, under which the norm of $|\psi)$ is conserved,

$$\frac{\mathrm{d}}{\mathrm{d}t}(\psi|\eta_{m,n}|\psi)=0. \tag{4}$$

The complex Lorentz transformation $\hat{\mathcal{U}}$ is thus called isometric operator in Ref. [9]. When $n\neq 0$, the norm can be positive, negative, and zero. The positive one will be normalized to 1 and the negative one will be normalized to -1.

2.2. Single Lorentz systems

There are two kinds of quantum systems, single systems and composite systems. For example, although both of their Hilbert spaces are of dimension four, spin-3/2 is a single system and the system with two spin-1/2's is a composite system. Similarly, there are also two kinds of Lorentz systems, single systems and composite systems. In single Lorentz systems, only the states $|\phi)$ with positive norm $(\phi|\eta_{m,n}|\phi)>0$ are regarded as physical and observable.

For a quantum state $|\psi\rangle$, in a measurement regarding operator A whose eigenstates are $|\psi_j\rangle$'s, one observes $|\psi_j\rangle$ with probability $|\langle\psi_j|\psi\rangle|^2$. For a Lorentz state $|\phi)$, consider a measurement of Lorentz operator $\boldsymbol{B}$. This operator $\boldsymbol{B}$ is not necessarily Hermitian; it usually has two sets of eigenstates, left and right.[10–12] Here it is sufficient to consider only the right eigenstates $\{|\phi_j),j=1,2,\ldots,m\}$ and $\{|\varphi_j),j=1,2,\ldots,n\}$, which satisfy $(\phi_j|\eta_{m,n}|\phi_j)=1$ and $(\varphi_j|\eta_{m,n}|\varphi_j)=-1$. We thus have the following expansion:

$$|\phi)=\sum_{j=1}^{m}a_j|\phi_j)+\sum_{j=1}^{n}b_j|\varphi_j). \tag{5}$$

According to Lorentz quantum mechanics, for Lorentz state $|\phi)$, one observes $|\phi_j)$ with probability $|a_j|^2/(\sum_{j=1}^{m}|a_j|^2)$. The $|\varphi_j)$'s are not observable.

The above features of a single Lorentz system is a formalization of the results in the field of superfluidity. The excitations of a superfluid are described by the Bogoliubov–de Gennes equation, which has two sets of eigenmodes, one half of them have positive norm and the other half have negative norm. The positive ones are quasi-particles of a superfluid, such as phonons, and can be observed in experiment while the negative half are unphysical and have never been observed.[7,13] However, in the dynamics governed by the Bogoliubov–de Gennes equation, these two modes are mixed together and must be taken into account simultaneously to describe some phenomena, such as the transverse force acting on a vortex.[8] More details of Lorentz quantum mechanics can be found in Refs. [3,4].

2.3. Composite systems

We consider two basic composite systems, one consisting of a quantum system S_{q} and a single Lorentz system S_{l} and the other consisting of two single Lorentz systems S_{l1} and S_{l2}. Other composite systems can be readily derived from them.

For the first kind of composite system, if the metric of S_{q} is $\eta_{m_1,0}$ and the metric of S_{l} is $\eta_{m_2,n}$, then the metric for the composite system S_{a} is $\eta_{m_1,0}\otimes\eta_{m_2,n}$. Namely, the composite system is also a Lorentz system with indefinite metric. If the Hilbert space of S_{q} is spanned by $\{|\psi_{\mathrm{q}}^{(i)}\rangle,\ i=1,2,\ldots,m_1\}$ and the inner product space of S_{a} is spanned by $\{|\phi_{\mathrm{l}}^{(j)}),j=1,2,\ldots,m_2\}$ and $\{|\varphi_{\mathrm{l}}^{(j)}),j=1,2,\ldots,n\}$, then the composite system S_{a} is spanned by $|\psi_{\mathrm{q}}^{(i)}\rangle\otimes|\phi_{\mathrm{l}}^{(j)})$ and $|\psi_{\mathrm{q}}^{(i)}\rangle\otimes|\varphi_{\mathrm{l}}^{(j)})$. For a state $|\Phi)$ of the composite system S_{a}, it can be expanded as

$$|\Phi)=\sum_{i=1}^{m_1}\Big\{\sum_{j=1}^{m_2}a_{ij}|\psi_{\mathrm{q}}^{(i)}\rangle\otimes|\phi_{\mathrm{l}}^{(j)})+\sum_{j=1}^{n}b_{ij}|\psi_{\mathrm{q}}^{(i)}\rangle\otimes|\varphi_{\mathrm{l}}^{(j)})\Big\}. \tag{6}$$

The probability of observing $|\psi_{\mathrm{q}}^{(i)}\rangle\otimes|\phi_{\mathrm{l}}^{(j)})$ is

$$P_{ij}=\frac{|a_{ij}|^2}{\sum_{i=1}^{m_1}\sum_{j=1}^{m_2}|a_{ij}|^2}. \tag{7}$$

And $|\psi_{\mathrm{q}}^{(i)}\rangle\otimes|\varphi_{\mathrm{l}}^{(j)})$ can not be observed.

For the second kind of composite system, if the metric of S_{l1} is η_{m_1,n_1} and the metric of S_{l2} is η_{m_2,n_2}, then the metric for the composite system S_{b} is $\eta_{m_1,n_1}\otimes\eta_{m_2,n_2}$. If the Hilbert space of S_{l1} is spanned by $\{|\phi_{\mathrm{l1}}^{(j)}),j=1,2,\ldots,m_1\}$ and $\{|\varphi_{\mathrm{l1}}^{(j)}),j=1,2,\ldots,n_1\}$, and the inner product space of S_{l2} is spanned by $\{|\phi_{\mathrm{l2}}^{(j)}),j=1,2,\ldots,m_2\}$ and $\{|\varphi_{\mathrm{l2}}^{(j)}),j=1,2,\ldots,n_2\}$, then the composite system S_{b} is spanned by $|\phi_{\mathrm{l1}}^{(j_1)})\otimes|\phi_{\mathrm{l2}}^{(j_2)})$, $|\phi_{\mathrm{l}}^{(j_1)})\otimes|\varphi_{\mathrm{l2}}^{(j_2)})$, $|\varphi_{\mathrm{l1}}^{(j_1)})\otimes|\phi_{\mathrm{l2}}^{(j_2)})$, and $|\varphi_{\mathrm{l1}}^{(j_1)})\otimes|\varphi_{\mathrm{l2}}^{(j_2)})$. For a state $|\Phi)$ of the composite system S_{b}, it can be expanded as

$$\begin{aligned}|\Phi)=&\sum_{j_1=1}^{m_1}\sum_{j_2=1}^{m_2}a_{j_1j_2}|\phi_{\mathrm{l1}}^{(j_1)})\otimes|\phi_{\mathrm{l2}}^{(j_2)})\\&+\sum_{j_1=1}^{m_1}\sum_{j_2=1}^{n_2}b_{j_1j_2}|\phi_{\mathrm{l1}}^{(j_1)})\otimes|\varphi_{\mathrm{l2}}^{(j_2)})\\&+\sum_{j_1=1}^{n_1}\sum_{j_2=1}^{m_2}c_{j_1j_2}|\varphi_{\mathrm{l1}}^{(j_1)})\otimes|\phi_{\mathrm{l2}}^{(j_2)})\\&+\sum_{j_1=1}^{n_1}\sum_{j_2=1}^{n_2}d_{j_1j_2}|\varphi_{\mathrm{l1}}^{(j_1)})\otimes|\varphi_{\mathrm{l2}}^{(j_2)}).\end{aligned} \tag{8}$$

The probability of observing $|\phi_{\mathrm{l1}}^{(j_1)})\otimes|\phi_{\mathrm{l2}}^{(j_2)})$ is

$$P_{j_1j_2}=\frac{|a_{j_1j_2}|^2}{\sum_{j_1=1}^{m_1}\sum_{j_2=1}^{m_2}|a_{j_1j_2}|^2}. \tag{9}$$

And other states $|\phi_{\mathrm{l1}}^{(j_1)})\otimes|\varphi_{\mathrm{l2}}^{(j_2)})$, $|\varphi_{\mathrm{l1}}^{(j_1)})\otimes|\phi_{\mathrm{l2}}^{(j_2)})$, and $|\varphi_{\mathrm{l1}}^{(j_1)})\otimes|\varphi_{\mathrm{l2}}^{(j_2)})$ are not observable.

We note two points before discussing computing model. (1) Lorentz quantum mechanics is reduced to the usual quantum mechanics when $n = 0$ or H is block-diagonal. As a result, quantum computer is a special case of Lorentz computer; quantum communication is a special case of Lorentz communication. (2) There are also mixed states in Lorentz quantum mechanics. However, they have not been rigorously defined and their properties have not been examined. Consequently, all the related issues, such as completely positive and trace-preserving (CPTP) map, have not been addressed, either. In this work, we focus on model of computing based on Lorentz quantum mechanics and leave other issues to future work.

3. Model of Lorentz computing

DiVincenzo's well-known five criteria describe requirements to construct a quantum computer in a real world.[14] In this work we focus on a general computational model, neglect detailed realization, and assume the system not affected by the environment (so we only consider pure states below). So the five DiVincenzo's criteria can be simplified into three:

1. What represents information? (encoding)
2. How is the information processed? (computing)
3. How to extract the information? (decoding)

In a classical computer, the information is stored in bits. The information is processed with classical logical gates. For reversible classical computer, either the Fredkin gate or the Toffoli gate can serve as the universal gate.[15] At the end of computation, the output is recorded in a string of bits with each bit in a definite state, 0 or 1.

In a quantum computer, the information is stored in qubits and the information is processed with quantum logical gates. There are three universal gates, Hadamard gate $\hat{H}$, $\pi/8$ gate $\hat{T}$, and CNOT gate. These gates are unitary transformations. At the end of computation, the qubits are usually in a superposition state where each qubit is not in a definite state. A measurement is then performed so that each qubit falls into a definite state, $|0\rangle$ or $|1\rangle$; the result is then extracted.[15]

People now have realized that the classical computer embodies classical mechanics and the quantum computer is derived from quantum mechanics.[2] It is thus natural to construct a computer model based on Lorentz quantum mechanics discussed above.

In a Lorentz quantum computer, the information is stored in both qubits and hybits. This means that the Lorentz computer is a composite system consisting of both quantum systems and Lorentz systems. The information is then processed with a set of universal Lorentz quantum gates, which will be presented in the next section. These universal gates are complex Lorentz transformations and the usual quantum universal gates are a subset. At the end of computation, as in quantum computers, the qubits and hybits are in general in a superposition state where each qubit or hybit is not in a definite state. A measurement is then performed to extract information. The essential difference is that only states with $|0\rangle$'s are observable.

It is clear by construction that the usual quantum computer is a special case of Lorentz computer when hybits are not used. This means that the Lorentz computer is potentially more powerful than quantum computer. This is indeed the case. An algorithm of Lorentz computer is designed for random search; it is exponentially faster than the Grover algorithm.[5,15]

3.1. Hybits

There are two kinds of bits in a Lorentz computer. The first is the familiar qubits, whose computational basis is made of $|0\rangle$ and $|1\rangle$. The second is unique to Lorentz computer and we call it hyperbolic bit (or hybit for short) as its state vector stays on a hyperbolic surface. For a hybit, its general state is represented as

$$|\psi) = a|0) + b|1) = \begin{pmatrix} a \\ b \end{pmatrix}, \tag{10}$$

where $|0)$ and $|1)$ are the computational basis satisfying

$$(0|\eta_{1,1}|0) = 1, \quad (1|\eta_{1,1}|1) = -1, \quad (1|\eta_{1,1}|0) = 0. \tag{11}$$

For a Lorentz computer made of N_q qubits and N_h hybits, its state space is of dimension $2^{N_\mathrm{q}+N_\mathrm{h}}$ and spanned by direct products

$$|\psi_1\rangle \otimes \cdots \otimes |\psi_{N_\mathrm{q}}\rangle \otimes |\psi_1) \otimes \cdots \otimes |\psi_{N_\mathrm{h}}). \tag{12}$$

Such a computer is a composite system with the following metric:

$$\eta = \underbrace{\eta_{2,0} \otimes \cdots \otimes \eta_{2,0}}_{N_\mathrm{q}} \otimes \underbrace{\eta_{1,1} \otimes \cdots \otimes \eta_{1,1}}_{N_\mathrm{h}}. \tag{13}$$

The state $|\Phi)$ of a Lorentz computer can be expanded in the computational basis

$$|\Phi) = \sum_{j=1}^{2^{N_\mathrm{q}+N_\mathrm{h}}} a_j |\psi_j), \tag{14}$$

where

$$\begin{aligned} |\psi_j) &= |d_1\rangle \otimes |d_2\rangle \cdots |d_{N_\mathrm{q}}\rangle \otimes |d_1) \otimes |d_2) \cdots \otimes |d_{N_\mathrm{h}}) \\ &= |d_1, d_2 \cdots, d_{N_\mathrm{q}}, \bar{d}_1, \bar{d}_2, \ldots, \bar{d}_{N_\mathrm{h}}\rangle, \end{aligned} \tag{15}$$

with d_j and $\bar{d}_j$ being either 0 or 1. In the above and from now on, for simplicity, we used and will use $|\bar{0}\rangle = |0)$ and $|\bar{1}\rangle = |1)$. According to Lorentz quantum mechanics introduced in the last section, any component with at least one $|1)$, e.g., $|1, 0, \ldots, 0, \bar{1}, \bar{0}, \ldots, \bar{0}\rangle$, is not observable.

The simplest Lorentz computer consists of one qubit and one hybit. Its general state is given by

$$|\Phi) = a_1|0, \bar{0}\rangle + a_2|0, \bar{1}\rangle + a_3|1, \bar{0}\rangle + a_4|1, \bar{1}\rangle. \tag{16}$$

Upon measurement, the probability of observing $|0,\bar{0}\rangle$ is $\frac{{a_1}^2}{{a_1}^2+{a_3}^2}$ while the probability of $|1,\bar{0}\rangle$ is $\frac{{a_3}^2}{{a_1}^2+{a_3}^2}$. The other two states, $|0,\bar{1}\rangle$ and $|1,\bar{1}\rangle$, are not observable.

Note that the case of $N_{\rm h}=0$ is completely equivalent to quantum computer. In other words, quantum computer is a special case of Lorentz computer just as reversible classical computer is a special case of quantum computer.

3.2. Universal gates

With qubits and hybits, we are ready to design logical gates for Lorentz computer. Similar to quantum computer, there also exists a set of universal gates for Lorentz computer. The universality, which we shall prove in Appendix A, ensures that any operator can be approximated to an arbitrary precision with the universal gates. In other words, one can use these gates to construct a set of complex Lorentz transformations, which is a dense set in all complex Lorentz transformations.

In the following text, $\hat{\sigma}_x,\hat{\sigma}_y$ and $\hat{\sigma}_z$ are the standard Pauli operators with the following matrices:

$$\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \begin{pmatrix}0&-{\rm i}\\{\rm i}&0\end{pmatrix},\quad \begin{pmatrix}1&0\\0&-1\end{pmatrix}, \tag{17}$$

respectively.

We find that the Lorentz universal gates can be divided into three sets, $\{\hat{H},\hat{T}\}$, $\{\hat{\tau},\hat{T}\}$, and $\{\hat{\Lambda}_1^{\rm qq}(\hat{\sigma}_z),\hat{\Lambda}_1^{\rm ql}(\hat{\sigma}_z),\hat{\Lambda}_1^{\rm lq}(\hat{\sigma}_z),\hat{\Lambda}_1^{\rm ll}(\hat{\sigma}_z)\}$. The first set $\{\hat{H},\hat{T}\}$ consists of Hadamard gate $\hat{H}$ and $\pi/8$ gate $\hat{T}$

$$\hat{H}=\frac{1}{\sqrt{2}}(\hat{\sigma}_x+\hat{\sigma}_z), \tag{18}$$

$$\hat{T}={\rm e}^{-{\rm i}\frac{\pi}{8}}\begin{pmatrix}{\rm e}^{{\rm i}\pi/8}&0\\0&{\rm e}^{-{\rm i}\pi/8}\end{pmatrix}. \tag{19}$$

These two operators are single qubit universal, which means that they operate on single qubits and the combination of these two gates can approximate any single qubit transformation to an arbitrary precision. They are denoted by symbols in Fig. 2.

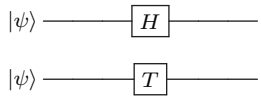

Fig. 1. Symbols for single qubit gates $\hat{H}$ and $\hat{T}$.

The second set operates on single hybits, consisting of $\pi/8$ gate $\hat{T}$ and gate $\hat{\tau}$

$$\hat{\tau}=\sqrt{2}\hat{\sigma}_z+{\rm i}\hat{\sigma}_x=\begin{pmatrix}\sqrt{2}&{\rm i}\\{\rm i}&-\sqrt{2}\end{pmatrix}. \tag{20}$$

It can be verified that $\hat{\tau}^\dagger\eta_{1,1}\hat{\tau}=\eta_{1,1}$, $(\hat{T})^\dagger\eta_{1,1}\hat{T}=\eta_{1,1}$. These two gates are single hybit universal.

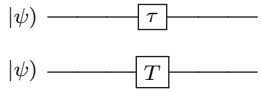

Fig. 2. Symbols for single hybit gates $\hat{\tau}$ and $\hat{T}$.

The operators in the last set, $\hat{\Lambda}_1^{\rm qq}(\hat{\sigma}_z)$, $\hat{\Lambda}_1^{\rm ql}(\hat{\sigma}_z)$, $\hat{\Lambda}_1^{\rm lq}(\hat{\sigma}_z)$ and $\hat{\Lambda}_1^{\rm ll}(\hat{\sigma}_z)$, are four types of controlled-Z operators with the same matrix representation

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}. \tag{21}$$

They differ from each other by the control and target bits being a qubit or a hybit as indicated by the superscript. Their circuits are shown in Fig. 3. The subscript indicates that there is only one control bit in the gate. We will discuss gates with more than one control bits in Appendix A.

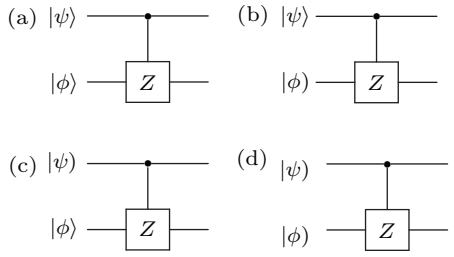

Fig. 3. Four different controlled-Z gates. (a) Circuit for $\hat{\Lambda}_1^{\rm qq}(\hat{\sigma}_z)$. (b) Circuit for $\hat{\Lambda}_1^{\rm ql}(\hat{\sigma}_z)$. (c) Circuit for $\hat{\Lambda}_1^{\rm lq}(\hat{\sigma}_z)$. (d) Circuit for $\hat{\Lambda}_1^{\rm ll}(\hat{\sigma}_z)$.

We have chosen the controlled-Z gate instead of the control-NOT (CNOT) gate, which is more frequently used in quantum computing. The reason is that the CNOT gate may fail to be a complex Lorentz transformation. For example, we have

$$\hat{\Lambda}_1^{\rm ql}(\hat{\sigma}_x)^\dagger(\eta_{2,0}\otimes\eta_{1,1})\hat{\Lambda}_1^{\rm ql}(\hat{\sigma}_x)\neq\eta_{2,0}\otimes\eta_{1,1}. \tag{22}$$

This indicates that the CNOT gate is not a complex Lorentz transformation when the control and target bits are qubit and hybit, respectively. In this case, the CNOT gate does not preserve the norm of the system, i.e., does not respect the light cone. However, the control-Z gates are always complex Lorentz transformations whatever the control and target bits are.

4. Application: Search algorithm

For the Lorentz computer described in the previous section, we propose a search algorithm which is faster than Grover's search algorithm for quantum computer.

We make use of n qubits for search along with one oracle qubit and one hybit. The task is to find out the target state $|x\rangle$ out of 2^n vectors $|00\ldots0\rangle,|00\ldots1\rangle,\ldots,|11\ldots1\rangle$, which are stored in the n qubits. The key in our algorithm is operator $\hat{Q}=\hat{O}\hat{\Lambda}_1^{\rm ql}(\hat{V})\hat{O}$ as shown in Fig. 4. The oracle operator $\hat{O}$ is defined as[15]

$$\hat{O}=(\hat{I}-|x\rangle\langle x|)\otimes\hat{I}_{\rm o}+|x\rangle\langle x|\otimes(|0_{\rm o}\rangle\langle 1_{\rm o}|+|1_{\rm o}\rangle\langle 0_{\rm o}|), \tag{23}$$

where $\hat{I}_o$ is the identity operator for the oracle qubit. Suppose the $n+1$ qubits are in the following state:

$$|\Phi_0\rangle \otimes |0_o\rangle = \frac{1}{\sqrt{N}}\left(\sum_{j=0}^{2^n-1}|j\rangle\right)\otimes|0_o\rangle, \tag{24}$$

where $N = 2^n$. When it is acted upon by $\hat{O}$, it becomes

$$\hat{O}|\Phi_0\rangle \otimes |0_o\rangle = \frac{1}{\sqrt{N}}\Big(\sum_{j=0,j\neq x}^{2^n-1}|j\rangle\otimes|0_o\rangle + |x\rangle\otimes|1_o\rangle\Big). \tag{25}$$

It shows that operator $\hat{O}$ flips the oracle qubit for the target item $|x\rangle$. The control gate $\hat{\Lambda}_1^{\rm ql}(\hat{V})$ has the oracle qubit as its control bit and the hybit as its target bit with the Lorentz transformation

$$\hat{V} = \begin{pmatrix} \cosh\chi & \sinh\chi \\ \sinh\chi & \cosh\chi \end{pmatrix}, \tag{26}$$

where χ is a positive constant. The algorithm goes as follows.

1. Initialize the computer with Hadamard gates on each qubit (except the oracle qubit) and the state becomes

$$|\Phi_0\rangle \otimes |0_o\rangle \otimes |0\rangle. \tag{27}$$

2. Apply operator $\hat{Q}$ on the state vector for k times, and get $\hat{Q}^k|\Phi_0\rangle$

3. Measure the n qubits and the hybit.

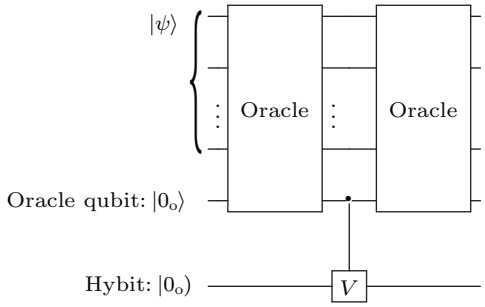

Fig. 4. Circuit for operator $\hat{Q}$.

The time complexity of our algorithm is $O(\log N)$ as we shall prove below. Making use of $\hat{O}$ and $\hat{V}$, we get

$$\begin{aligned}&\hat{Q}^k\left(|\Phi_0\rangle\otimes|0_o\rangle\otimes|0\rangle\right)\\ =\ &(\hat{I}-|x\rangle\langle x|+\cosh(k\chi|x\rangle\langle x|)|\Phi_0\rangle\otimes|0_o\rangle\otimes|0\rangle\\ &+(\sinh(k\chi)|x\rangle\langle x|)|\Phi_0\rangle\otimes|0_o\rangle\otimes|1\rangle.\end{aligned} \tag{28}$$

According to the theory of Lorentz mechanics, the probability of getting $|x\rangle$ is

$$P = \frac{\frac{1}{N}\cosh^2 k\chi}{1-\frac{1}{N}+\frac{1}{N}\cosh^2 k\chi}. \tag{29}$$

It is clear that $P\approx 1$ when $k\approx\frac{1}{\chi}\ln N$. So, the time complexity of our algorithm is $O(\log N)$.

For quantum computer, Grover's algorithm can be simulated with Hamiltonians.[16–19] Similarly, our search algorithm can also be implemented with a Hamiltonian

$$\hat{\mathcal{H}} = |x\rangle\langle x|\otimes(\eta_{1,1}\hat{\mathcal{H}}_0), \tag{30}$$

in which $e^{i\eta_{1,1}\hat{\mathcal{H}}_0} = \hat{V}$.

This Lorentz search algorithm with exponential speedup can be used to solve NP problems efficiently. Any computation problem can be converted into a search problem of finding the proper solution out of all possible solutions. For an NP problem, which has $N = 2^n$ possible solutions,[20] our algorithm requires to invoke the oracle $O(\log N) = O(n)$ times, while the time complexity for running the oracle is polynomial $O(n^p)$ by definition. As a result, the solution can be searched and found in a polynomial time scale with our Lorentz search algorithm. In other words, all NP problems can be solved efficiently on a Lorentz computer. It is not clear whether NP-hard problems, such as maximum independent set problem,[21,22] can be solved efficiently on a Lorentz computer.

5. Discussion and conclusion

Our model of Lorentz computer may remind people of standard quantum computer with postselection.[23] In the final step, that only the components with $|0\rangle$ are observable is equivalent to postselecting $|0\rangle$ and discarding $|1\rangle$. For convenience, we call it hyper-postselection. (1) Hyper-postselection is inspired by physics related to Bogoliubov–de Genne equation,[7,8,13] not an arbitrary assumption or a mathematical trick. (2) It works only on hybits and does not work on qubits. (3) Due to the search algorithm presented in the last section, it is clear that our Lorentz computer with hyper-postselection is at least as powerful as standard quantum computer with postselection. The search algorithm is the first algorithm that we found for the Lorentz computer; more powerful algorithms may come up in the future.

There are other theoretical models of computer, which can also outperform the standard quantum computer. One is called digital memcomputing machine that is classical[24,25] and the other is called quantum computer with closed timelike curve (CTC).[26] They both allow dynamical evolution along a closed timelike world line, which has not been found to exist in nature. Adding nonlinearity to quantum mechanics may also speed up computing.[27] However, this claim is very doubtful as nonlinearity in classical mechanics has never been found to speed up computing. The reason is that any nonlinear dynamics in a short time step can be approximated by linear gates. Nonlinear quantum dynamics can certainly be approximated with linear gates as well. In fact, the effectiveness of quantum computing with CTC or nonlinearity has been seriously questioned.[28]

In constructing our Lorentz computer, we have assumed that the Lorentz mechanics is fundamentally different from quantum mechanics in the spirit of how Pauli discussed this kind of mechanics in 1940s.[4] However, as the Bogoliubov–de Gennes equation is an approximation of a more fundamental quantum equation,[7,13] it is possible that our computer model can be constructed approximately in experiments. In fact, a Lorentz system was already demonstrated in a photon experiment with postselection.[6]

In summary, we have set up a computational model based on Lorentz mechanics. This model consists of both qubits and hybits along with a set of universal logical gates. We have designed a search algorithm for Lorentz computer, which is exponentially faster than the Grover algorithm. This explicitly shows that Lorentz computer is more powerful than quantum computer.

Appendix A: Proof of university

This appendix gives a proof of universality for the following three sets of gates:

$$\{\hat{H},\hat{T}\},\ \ \{\hat{\tau},\hat{T}\},$$
$$\{\hat{\Lambda}_1^{\rm qq}(\hat{\sigma}_z),\hat{\Lambda}_1^{\rm ql}(\hat{\sigma}_z),\hat{\Lambda}_1^{\rm lq}(\hat{\sigma}_z),\hat{\Lambda}_1^{\rm ll}(\hat{\sigma}_z)\}\}.$$

The mathematical meaning of universality means that any operator can be approximated to an arbitrary precision with the universal gates.

Before laying out the proof in details in five steps, we point out that $\{\hat{H},\hat{T}\}$ is single qubit universal as already shown in quantum computation.[15,29]

A1. From $\{\hat{\tau},\hat{T}\}$ to arbitrary single hybit operators

The $\{\hat{\tau},\hat{T}\}$ is single qubit universal, which means that any operator $\hat{\mathcal{U}}$ for single hybit can be approximated by matrix product of a sequence of operator $\hat{\tau}$ and operator $\hat{T}$, for example, $\hat{\tau}\hat{\tau}\hat{T}\hat{\tau}\cdots$. Error of the approximation $||\hat{\mathcal{U}}-\hat{\tau}\hat{\tau}\hat{T}\hat{\tau}\cdots||$ can be reduced to arbitrary small.

A single hybit operator is an element in group $U(1,1)$ or $SU(1,1)$ represented by a matrix[3]

$$\begin{pmatrix}\zeta & \gamma^*\\ \gamma & \zeta^*\end{pmatrix},\quad \zeta\in\mathbb{C},\gamma\in\mathbb{C} \tag{A1}$$

or as an exponential map $\mathrm{e}^{-\mathrm{i}\theta(\mathrm{i}\hat{\sigma}_x n_x+\mathrm{i}\hat{\sigma}_y n_y+\hat{\sigma}_z n_z)}=\mathrm{e}^{\mathrm{i}\theta\boldsymbol{n}\cdot\hat{\boldsymbol{\sigma}}}$ in which $n_x,n_y,n_z\in\mathbb{R},\boldsymbol{n}=(\mathrm{i}n_x,\mathrm{i}n_y,n_z),\hat{\boldsymbol{\sigma}}=(\hat{\sigma}_x,\hat{\sigma}_y,\hat{\sigma}_z)$. Note that we make no distinction between $U(m,n)$ and $SU(m,n)$ for the reason that an arbitrary overall phase is trivial.

The elements in $SU(1,1)$ fall into three categories: space rotation, lightlike rotation, and pseudo rotation.

$$\mathrm{e}^{-\mathrm{i}\theta(\mathrm{i}\hat{\sigma}_x n_x+\mathrm{i}\hat{\sigma}_y n_y+\hat{\sigma}_z n_z)}$$
$$=\begin{cases}\cos\theta\hat{I}-\mathrm{i}\sin\theta(\mathrm{i}\hat{\sigma}_x n_x+\mathrm{i}\hat{\sigma}_y n_y+\hat{\sigma}_z n_z)\\ \quad \text{if}-n_x^2-n_y^2+n_z^2=1,\\ \\ \hat{I}-\mathrm{i}\theta(\mathrm{i}\hat{\sigma}_x n_x+\mathrm{i}\hat{\sigma}_y n_y+\hat{\sigma}_z n_z)\\ \quad \text{if}-n_x^2-n_y^2+n_z^2=0,\\ \\ \cosh\theta\hat{I}-\mathrm{i}\sinh\theta(\mathrm{i}\hat{\sigma}_x n_x+\mathrm{i}\hat{\sigma}_y n_y+\hat{\sigma}_z n_z)\\ \quad \text{if}-n_x^2-n_y^2+n_z^2=-1.\end{cases} \tag{A2}$$

It is easy to verify that the operators $\{\hat{\tau},\hat{T}\}$ are all space rotation. But surprisingly, not only can we generate all the space rotations in $U(1,1)$ with them, but also all the lightlike rotations and pseudo rotations.

Consider an operator

$$\begin{aligned}\hat{P}&=\hat{T}\hat{\tau}\\ &=\sqrt{2}\sin\frac{\pi}{8}\hat{I}+\mathrm{i}\left(\mathrm{i}\hat{\sigma}_x\cos\frac{\pi}{8}+\mathrm{i}\hat{\sigma}_y\sin\frac{\pi}{8}+\sqrt{2}\hat{\sigma}_z\cos\frac{\pi}{8}\right)\\ &=\cos\theta_0 I+\mathrm{i}\sin\theta_0(\mathrm{i}\hat{\sigma}_x n_x+\mathrm{i}\hat{\sigma}_y n_y+\hat{\sigma}_z n_z),\end{aligned} \tag{A3}$$

in which $\theta_0=\arccos(\sqrt{2}\sin\frac{\pi}{8})$. It can be proved that θ_0/π is an irrational number according to the theory of cyclotomic polynomial[30] by noticing the fact that the minimal polynomial of $\mathrm{e}^{\mathrm{i}\theta_0}$ in $\mathbb{Z}[n]$, $x^8-4x^6-2x^4-4x+1$, is not a cyclotomic polynomial. This means that, with an appropriate integer n, $\hat{P}^n=\cos n\theta_0 I+\mathrm{i}\sin n\theta_0(\mathrm{i}\hat{\sigma}_x n_x+\mathrm{i}\hat{\sigma}_y n_y+\hat{\sigma}_z n_z)$ can approximate the space rotation along spacelike axis $\boldsymbol{n}_1=(\mathrm{i}n_x,\mathrm{i}n_y,n_z)$ for an arbitrary angle with arbitrary precision. Thus we get space rotation $\mathrm{e}^{\mathrm{i}\theta\boldsymbol{n}_1\cdot\hat{\boldsymbol{\sigma}}}$ for arbitrary θ.

Applying similarity transformations to this operator, we can obtain another two space rotations

$$\hat{T}\,\mathrm{e}^{\mathrm{i}\theta_1\boldsymbol{n}_1\cdot\hat{\boldsymbol{\sigma}}}\hat{T}^\dagger=\mathrm{e}^{\mathrm{i}\theta_1\boldsymbol{n}_2\cdot\hat{\boldsymbol{\sigma}}}, \tag{A4}$$
$$\hat{T}^2\,\mathrm{e}^{\mathrm{i}\theta_2\boldsymbol{n}_1\cdot\hat{\boldsymbol{\sigma}}}(\hat{T}^2)^\dagger=\mathrm{e}^{\mathrm{i}\theta_2\boldsymbol{n}_3\cdot\hat{\boldsymbol{\sigma}}} \tag{A5}$$

for arbitrary θ along axis $\boldsymbol{n}_2$ and $\boldsymbol{n}_3$. Noticing the linearly independence of $\boldsymbol{n}_1$, $\boldsymbol{n}_2$ and $\boldsymbol{n}_3$, we can write any vector $\theta\boldsymbol{n}$ into the linear superposition of them

$$\theta\boldsymbol{n}=\alpha_1\boldsymbol{n}_1+\alpha_2\boldsymbol{n}_2+\alpha_3\boldsymbol{n}_3. \tag{A6}$$

So, any single hybit operator can be written as

$$\mathrm{e}^{\mathrm{i}\theta\boldsymbol{n}\cdot\hat{\boldsymbol{\sigma}}}=\mathrm{e}^{\mathrm{i}(\alpha_1\boldsymbol{n}_1\cdot\hat{\boldsymbol{\sigma}}+\alpha_2\boldsymbol{n}_2\cdot\hat{\boldsymbol{\sigma}}+\alpha_3\boldsymbol{n}_3\cdot\hat{\boldsymbol{\sigma}})}. \tag{A7}$$

Applying Baker–Hausdorff formula with a large enough integer ℓ

$$\mathrm{e}^{\mathrm{i}\theta\boldsymbol{n}\cdot\hat{\boldsymbol{\sigma}}}\approx(\mathrm{e}^{\mathrm{i}\frac{\alpha_1}{\ell}\boldsymbol{n}_1\cdot\hat{\boldsymbol{\sigma}}}\,\mathrm{e}^{\mathrm{i}\frac{\alpha_2}{\ell}\boldsymbol{n}_2\cdot\hat{\boldsymbol{\sigma}}}\,\mathrm{e}^{\mathrm{i}\frac{\alpha_3}{\ell}\boldsymbol{n}_3\cdot\hat{\boldsymbol{\sigma}}})^\ell, \tag{A8}$$

we can see that $\mathrm{e}^{\mathrm{i}\theta\boldsymbol{n}\cdot\hat{\boldsymbol{\sigma}}}$ is written in the form of product of rotations along $\boldsymbol{n}_1,\boldsymbol{n}_2$, or $\boldsymbol{n}_3$, which we already know how to generate.

A2. From controlled-Z gate $\hat{\Lambda}_1(\hat{\sigma}_z)$ to controlled-V gate $\hat{\Lambda}_1(\hat{V})$

For simplicity, we shall omit the superscripts and write $\hat{\Lambda}_k^{\rm qq}(\hat{v})$, $\hat{\Lambda}_k^{\rm ql}(\hat{v})$, $\hat{\Lambda}_k^{\rm lq}(\hat{v})$, or $\hat{\Lambda}_k^{\rm ll}(\hat{v})$ as $\hat{\Lambda}_k(\hat{v})$ when the control and target bits are clear, or no confusion would arise. Here k denotes the number of the control bits.

We are going to construct the controlled-V gate, $\hat{\Lambda}_1(\hat{V})$, where $\hat{V}$ denotes an arbitrary unitary operator when the target bit is a qubit, or an arbitrary complex Lorentz operator when the target bit is a hybit. If the target bit is qubit, corresponding to Figs. 3(a) and 3(c), the proof is exactly the same as in quantum computing.[15,29] We only need to give the proof when the target bit is a hybit, as shown in Figs. 3(b) and 3(d). For these two cases, the metric is $\mathrm{diag}(1,-1,1,-1)$ or $\mathrm{diag}(1,-1,-1,1)$.

With the following similarity transformation:

$$(\hat{I}\otimes\hat{V})\hat{\Lambda}_1(\hat{\sigma}_z)(\hat{I}\otimes\hat{V})^{-1}=\hat{\Lambda}_1(\hat{V}\hat{\sigma}_z\hat{V}^{-1}), \tag{A9}$$

it is clear that when $\hat{V}$ goes through all the single hybit operators, $\hat{\Lambda}_1(\hat{\sigma}\cdot\boldsymbol{n})$ for arbitrary $\boldsymbol{n}\cdot\boldsymbol{n}=1$ can be generated. We consider three specific such operators $\hat{\Lambda}(\hat{\sigma}_z)$, $\hat{\Lambda}(\hat{\sigma}_z\cosh\alpha+\mathrm{i}\hat{\sigma}_y\sinh\alpha)$, $\hat{\Lambda}(\hat{\sigma}_z\cosh\beta+\mathrm{i}\hat{\sigma}_x\sinh\beta)$, in which α and β are two unequal and nonzero real numbers. The product of these three operators is

$$\begin{aligned}\hat{P}'&=\hat{\Lambda}_1(\hat{\sigma}_z)\hat{\Lambda}_1(\hat{\sigma}_z\cosh\alpha+\mathrm{i}\hat{\sigma}_y\sinh\alpha)\\&\quad\hat{\Lambda}_1(\hat{\sigma}_z\cosh\beta+\mathrm{i}\hat{\sigma}_x\sinh\beta)\\&=\hat{\Lambda}_1(\mathrm{i}(\sinh\alpha\sinh\beta\hat{I}-\mathrm{i}(\cosh\alpha\cosh\beta\hat{\sigma}_z\\&\quad+\mathrm{i}\cosh\alpha\sinh\beta\hat{\sigma}_x-\mathrm{i}\sinh\alpha\cosh\beta\hat{\sigma}_y)))\\&=\hat{\Lambda}_1(\mathrm{i}\,\mathrm{e}^{-\mathrm{i}\arccos(\sinh\alpha\sinh\beta)\hat{\boldsymbol{\sigma}}\cdot\boldsymbol{n}})\end{aligned} \tag{A10}$$

with

$$\boldsymbol{n}=(\mathrm{i}\cosh\alpha\sinh\beta,-\mathrm{i}\sinh\alpha\cosh\beta,\sinh\alpha\sinh\beta). \tag{A11}$$

If we choose α,β such that $\sinh\alpha\cosh\beta<1$ and $\arccos(\sinh\alpha\sinh\beta)/\pi$ is irrational, we can generate $\hat{\Lambda}_1(\mathrm{e}^{\mathrm{i}\theta\hat{\boldsymbol{\sigma}}\cdot\boldsymbol{n}})$ for arbitrary θ with $\hat{P'}^k$. Then we can generate $\hat{\Lambda}_1(\hat{V})$ for all $\hat{V}\in SU(1,1)$ using the same trick as the previous section.

And we notice that

$$\begin{pmatrix}1&0\\0&\mathrm{e}^{\mathrm{i}\phi}\end{pmatrix}\otimes\hat{I}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&\mathrm{e}^{\mathrm{i}\phi}&0\\0&0&0&\mathrm{e}^{\mathrm{i}\phi}\end{pmatrix}=\hat{\Lambda}_1(\mathrm{e}^{\mathrm{i}\phi}). \tag{A12}$$

So we have $\hat{\Lambda}_1(\mathrm{e}^{\mathrm{i}\phi}\hat{V})=\hat{\Lambda}_1(\mathrm{e}^{\mathrm{i}\phi})\hat{\Lambda}_1(\hat{V})$, and thus obtain $\hat{\Lambda}_1(\hat{V}_0)$ for arbitrary $\hat{V}_0\in U(1,1)$

A3. From controlled-V gate $\hat{\Lambda}_1(\hat{V})$ to controlled-V gate $\hat{\Lambda}_k(\hat{V})$ with k control bits

We denote controlled-V gate with k control bits as $\hat{\Lambda}_k(\hat{V})$, and we are going to generate $\hat{\Lambda}_k(\hat{\sigma}_z)$ for arbitrary positive integer k and arbitrary type of control and target bits (qubit or hybit). The following proof holds whether the bits are qubits, hybits or both, so the superscript of $\hat{\Lambda}_k(\hat{V})$ is omitted.

We are first to construct $\hat{\Lambda}_2(\hat{V})$ for arbitrary $\hat{V}$. $\hat{\Lambda}_2(\hat{V})$ is an 8×8 matrix, which we denote as a 4×4 matrix with each element being a 2×2 matrix. Consider operator $\hat{W}_3(\hat{V}\hat{\sigma}_z\hat{V}^{-1})$, whose circuit representation is shown in Fig. A1; the subscript indicates the number of relevant qubits and hybits is 3,

$$\hat{W}_3(\hat{V}\hat{\sigma}_z\hat{V}^{-1})=\begin{pmatrix}\hat{I}&0&0&0\\0&\hat{V}\hat{\sigma}_z\hat{V}^{-1}&0&0\\0&0&\hat{V}\hat{\sigma}_z\hat{V}^{-1}&0\\0&0&0&\hat{I}\end{pmatrix}. \tag{A13}$$

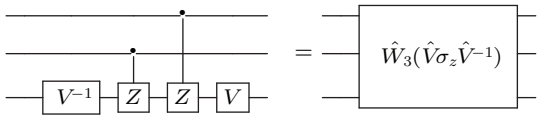

Fig. A1. Circuit for operator $\hat{W}_3(\hat{V}\hat{\sigma}_z\hat{V}^{-1})$.

The form of operator $\hat{W}_3(\hat{V}\hat{\sigma}_z\hat{V}^{-1})$ is similar to operator $\hat{\Lambda}_1(\hat{V}\hat{\sigma}_z\hat{V}^{-1})$ in the previous section, then we can generate

$$\hat{W}_3(\hat{V}_0)=\begin{pmatrix}\hat{I}&0&0&0\\0&\hat{V}_0&0&0\\0&0&\hat{V}_0&0\\0&0&0&\hat{I}\end{pmatrix} \tag{A14}$$

for arbitrary V_0 using the same technique. Specially we can generate

$$\hat{W}_3(\hat{\sigma}_z^{-\frac{1}{2}})=\begin{pmatrix}\hat{I}&0&0&0\\0&\hat{\sigma}_z^{-\frac{1}{2}}&0&0\\0&0&\hat{\sigma}_z^{-\frac{1}{2}}&0\\0&0&0&\hat{I}\end{pmatrix} \tag{A15}$$

with which we can construct $\hat{\Lambda}_2(\hat{\sigma}_z)$ with the circuit in Fig. A2.

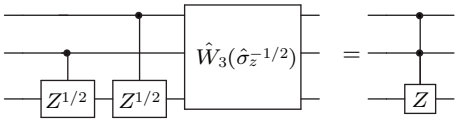

Fig. A2. Circuit for operator $\hat{\Lambda}_2(\hat{\sigma}_z)$.

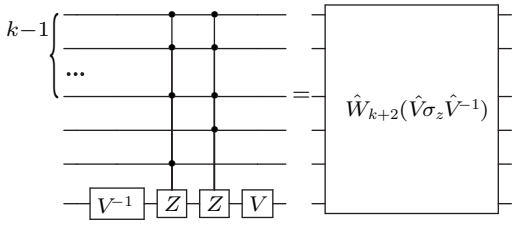

Fig. A3. The k-control-bit version of Fig. A1.

We have already obtained operator $\hat{\Lambda}_2(\hat{\sigma}_z)$ using $\hat{\Lambda}_1(\hat{\sigma}_z)$ and single qubit or single hybit operators. Applying the same steps, we can generate $\hat{\Lambda}_{k+1}(\hat{\sigma}_z)$ using $\hat{\Lambda}_k(\hat{\sigma}_z)$ and single qubit or hybit operators, as described in Figs. A3 and A4. With $\hat{\Lambda}_k(\hat{\sigma}_z)$, $\hat{\Lambda}_{k+1}(\hat{V})$ can be straightforwardly generated in the same way as generating $\hat{\Lambda}_1(\hat{V})$ with $\hat{\Lambda}_1(\hat{\sigma}_z)$.

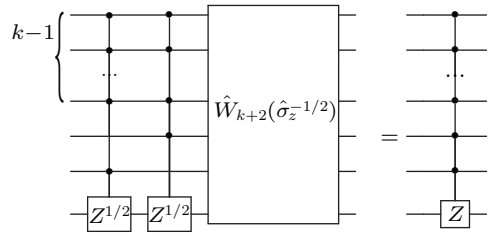

Fig. A4. The k-control-bit version of Fig. A2.

A4. Arbitrary operators can be factorized into two-level matrices

Similar to standard quantum computing,[15] two-level matrix can be defined in $U(m,n)$. We denote it as $\hat{b}_{i,j}(\hat{V})$, in which $1 \le i < j \le m+n$ and

$$\hat{V} = \begin{pmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{pmatrix} \tag{A16}$$

is a unitary or complex Lorentz matrix. $\hat{b}_{i,j}(\hat{V})$ can be represented in the form of matrix

$$\begin{array}{l} \\ \\ \\ i\text{-th row} \\ \\ \\ \\ \\ j\text{-th row} \\ \\ \\ \end{array} \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & V_{11} & 0 & \cdots & 0 & V_{12} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & V_{21} & 0 & \cdots & 0 & V_{22} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}. \tag{A17}$$

When restricted on the subspace spanned by $\{|i\rangle, |j\rangle\}$, we simply have $\hat{b}_{i,j}(\hat{V}) = \hat{V}$. As $\hat{b}_{i,j}(\hat{V}) \in U(m,n)$, $\hat{V}$ is a complex Lorentz matrix matrix when $1 \le i \le m < j \le m+n$, or a unitary matrix otherwise. When restricted on the orthogonal complement space $\hat{b}_{i,j}(\hat{V})$ is an identity matrix.

For any operator $A \in U(m,n)$ in which $m \ge 2$ and $n \ge 2$, consider $A^{(1)} = \hat{b}_{1,2}(\hat{V})A$, which is in the form of matrix

$$\begin{pmatrix} A^{(1)}_{1,1} \\ A^{(1)}_{2,1} \end{pmatrix} = \begin{pmatrix} V_{11} & V_{12} \\ -V^*_{12} & V^*_{11} \end{pmatrix} \begin{pmatrix} A_{1,1} \\ A_{2,1} \end{pmatrix}, \tag{A18}$$

where $A_{k,l}$ and $A^{(1)}_{k,l}$ denote the k-th row l-th column element of matrix A and $A^{(1)}$, respectively ($A^{(2)}_{k,l}, A^{(3)}_{k,l}$ in the following text are similar). We can choose appropriate $\hat{V}$ such that $A^{(1)}_{2,1} = 0$. We continue this procedure with $\hat{b}_{1,j}$ $(j = 3,4,\ldots,m)$ and obtain $A^{(2)} = \hat{b}_{1,m}\cdots\hat{b}_{1,3}A^{(1)}$ such that $A^{(2)}_{2,1} = \cdots = A^{(2)}_{m,1} = 0$. To make $A_{j,1} = 0$ with $j > m+1$, we can use a different set of $\hat{b}_{i,j}$ and obtain $A^{(3)} = \hat{b}_{m+1,m+n}\cdots\hat{b}_{m+1,m+2}A^{(2)}$ such that $A^{(3)}_{2,1} = \cdots = A^{(3)}_{m,1} = A^{(3)}_{m+2,1} = \cdots = A^{(3)}_{m+n,1} = 0$. To make $A_{m+1,1} = 0$, we use $A^{(4)} = \hat{b}_{1,m+1}(\hat{V}')A^{(3)}$,

$$\begin{pmatrix} A^{(4)}_{1,1} \\ A^{(4)}_{m+1,1} \end{pmatrix} = \begin{pmatrix} V'_{11} & V'_{12} \\ V'^*_{12} & V'^*_{11} \end{pmatrix} \begin{pmatrix} A^{(3)}_{1,1} \\ A^{(3)}_{m+1,1} \end{pmatrix}. \tag{A19}$$

By choosing appropriate values for the elements of $\hat{V}'$, we can make $A^{(4)}_{1,1} = 1$ and $A^{(4)}_{m+1,1} = 0$, for the reason that

$$A^{(3)2}_{1,1} - A^{(3)\ 2}_{m+1,1} = \sum_{i=1}^{m} A^{(3)2}_{i,1} - \sum_{i=m+1}^{m+n} A^{(3)2}_{i,1} = 1. \tag{A20}$$

We now have $A_{1,2} = \cdots = A_{1,m+n} = 0$. As column vectors in matrix $A^{(4)}$ are orthogonal to each other, we have $A_{2,1} = \cdots = A_{m+n,1} = 0$. Thus we have reduced matrix A into a block matrix

$$\left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & U(m-1,n) & \\ 0 & & & \end{array}\right). \tag{A21}$$

By induction, we can reduce A into an identity matrix $\hat{I}$ using a series of two-level matrices. This is equivalent to the assertion that arbitrary operators A can be factorized into a series of two-level matrices.

A5. From $\hat{\Lambda}_{N-1}(\hat{V})$ to two-level matrices

In this section, our goal is to construct all the two-level matrices using $\hat{\Lambda}_{N-1}(\hat{V})$, where N is the total number of qubits and hybits. The following proof holds whether the bits are qubits, hybits, or both, so the superscripts of $\hat{\Lambda}_k(\hat{V})$ are omitted.

We notice that $\hat{\Lambda}_{N-1}(\hat{V})$ can be considered as a special kind of two-level matrices $\hat{b}_{i,j}$ where only one qubit (or hybit) between $|i\rangle$ and $|j\rangle$ is different, while the rest of qubits (or hybits) are all $|1\rangle$ (or $|1\rangle$), for example,

$$|i\rangle = |1,1,0,1,1\rangle \otimes |1,1\rangle, \tag{A22}$$

$$|j\rangle = |1,1,1,1,1\rangle \otimes |1,1\rangle. \tag{A23}$$

Different from $\hat{\Lambda}_{N-1}(\hat{V})$, $\hat{b}_{i,j}$ of which the Hamming distance between i and j is 1 also requires only one different qubit (or hybit) between $|i\rangle$ and $|j\rangle$ but imposes no constraint on the rest of the qubits and hybits, for example,

$$|i\rangle = |1,1,0,0,0\rangle \otimes |1,0\rangle, \tag{A24}$$

$$|j\rangle = |1,1,1,0,0\rangle \otimes |1,0\rangle. \tag{A25}$$

For the case of $N = 2$, only $\hat{b}_{i,j}(\hat{\sigma}_z)$ with $|i\rangle = |00\rangle$, $|j\rangle = |01\rangle$ is not a controlled-Z gate $\Lambda_1(\sigma_z)$. It can be constructed as

$$\hat{b}_{i,j}(\hat{\sigma}_z) = \hat{\Lambda}_1(\hat{\sigma}_z)(\hat{I} \otimes \hat{\sigma}_z). \tag{A26}$$

Noticing that $\hat{b}_{i,j}$ with the Hamming distance between $|i\rangle$ and $|j\rangle$ equal to 1 can be obtained by exchanging $|0\rangle$ and $|1\rangle$ (or $|0\rangle$ and $|1\rangle$) for some qubits (hybits), we can obtain such $\hat{b}_{i,j}(\hat{V})$ for $N > 2$ by applying steps in Appendix A2 but substitute

some $\hat{\Lambda}_1(\hat{\sigma}_z)$ operators with the operator in Eq. (A26), as the substitution essentially exchange $|0\rangle$ and $|1\rangle$ (or $|0)$ and $|1)$) for the control bits.

Now we are going to generate $\hat{b}_{i,j}$ of which the Hamming distance between i and j is 2. We can always find a basis vector $|k\rangle$ such that the Hamming distances between i,k and j,k are both 1, and we are to generate $\hat{b}_{i,j}$ by $\hat{b}_{i,k}$ and $\hat{b}_{j,k}$. Considering the subspace spanned by $\{|i\rangle,|j\rangle,|k\rangle\}$, by symmentry, we only need to consider three kinds of metric: diag$(1,1,1)$, diag$(-1,1,1)$ and diag$(1,1,-1)$.

For each case, we construct $\hat{b}_{i,j}$ with $\hat{b}_{i,k}$ and $\hat{b}_{j,k}$ in the form of matrix restricted on the subspace. If the metric is diag$(1,1,1)$,

$$\begin{pmatrix} \zeta & \gamma & 0 \\ -\gamma^* & \zeta^* & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \zeta & 0 & \gamma \\ 0 & 1 & 0 \\ -\gamma^* & 0 & \zeta^* \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{A27}$$

If the metric is diag$(-1,1,1)$,

$$\begin{pmatrix} \zeta & \gamma & 0 \\ \gamma^* & \zeta^* & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \zeta & 0 & \gamma \\ 0 & 1 & 0 \\ \gamma^* & 0 & \zeta^* \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{A28}$$

If the metric is diag$(1,1,-1)$,

$$\begin{aligned} &\begin{pmatrix} \zeta & \gamma & 0 \\ -\gamma^* & \zeta^* & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \frac{\sqrt{1+\gamma^2}}{\zeta^*} & 0 & -\sqrt{2}\frac{\gamma}{\zeta^*} \\ 0 & 1 & 0 \\ -\sqrt{2}\frac{\gamma^*}{\zeta} & 0 & \frac{\sqrt{1+\gamma^2}}{\zeta} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{2} & -1 \\ 0 & -1 & \sqrt{2} \end{pmatrix} \\ &\quad \begin{pmatrix} \sqrt{1+\gamma^2} & 0 & \gamma \\ 0 & 1 & 0 \\ \gamma^* & 0 & \sqrt{1+\gamma^2} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{\sqrt{2}}{\zeta} & \frac{\sqrt{1+\gamma^2}}{\zeta^*} \\ 0 & \frac{\sqrt{1+\gamma^2}}{\zeta} & \frac{\sqrt{2}}{\zeta^*} \end{pmatrix}. \end{aligned} \tag{A29}$$

In above identities, ζ and γ are arbitrary complex numbers. By induction, we can generate $\hat{b}_{i,j}$ of which the Hamming distance between i and j is arbitrary. This concludes the proof.

Acknowledgements

We thank Qi Zhang for helpful discussion. We are supported by the National Key R&D Program of China (Grant Nos. 2017YFA0303302 and 2018YFA0305602), the National Natural Science Foundation of China (Grant No. 11921005), and Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01).

References

[1] Deutsch D 1997 *Fabric Of Reality* (New York: Penguin Books)
[2] Wu B 2022 *Frank Wilczek – 50 Years of Theoretical Physics* Ed. Niemi A, Kphua K K and Shapere A (World Scientific) pp. 281–290
[3] Zhang Q and Wu B 2018 *New J. Phys.* **20** 013024
[4] Pauli W 1943 *Rev. Mod. Phys.* **15** 175
[5] Grover L K 1997 *Phys. Rev. Lett.* **79** 325
[6] Li Q, Zhang C J, Cheng Z D, Liu W Z, Wang J F, Yan F F, Lin Z H, Xiao Y, Sun K, Wang Y T, Tang J S, Xu J S, Li C F and Guo G C 2019 *Optica* **6** 67
[7] Wu B and Niu Q 2003 *New J. Phys.* **5** 104
[8] Zhang C, Dudarev A M and Niu Q 2006 *Phys. Rev. Lett.* **97** 040401
[9] Bognar J 1974 *Indefinite inner product space* (New York: Springer-Verlag)
[10] Mostafazadeh A 2002 *Journal of Mathematical Physics* **43** 205
[11] Mostafazadeh A 2002 *Journal of Mathematical Physics* **43** 2814
[12] Mostafazadeh A 2002 *Journal of Mathematical Physics* **43** 3944
[13] Pethick C J and Smith H 2002 *Bose-Einstein condensation in dilute gases* (Cambridge: Cambridge University Press)
[14] DiVincenzo D P 2000 *Fortschritte der Physik Progress of Physics* **48** 771
[15] Nielson M A and Chuang I L 2000 *Quantum computing and quantum information* (Cambridge: Cambridge University Press)
[16] Farhi E and Gutmann S 1998 *Phys. Rev. A* **57** 2403
[17] van Dam W, Mosca M and Vazirani U 2001 *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, Newport Beach, CA, USA, pp. 279–287
[18] Roland J and Cerf N J 2002 *Phys. Rev. A* **65** 042308)
[19] Wilczek F, Hu H Y and Wu B 2020 *Chin. Phys. Lett.* **37** 050304
[20] Karp R M 1972 *Reducibility among Combinatorial Problems* (Boston, MA: Springer US) pp. 85–103
[21] Xiao M and Nagamochi H 2017 *Information and Computation* **255** 126
[22] Yu H, Wilczek F and Wu B 2021 *Chin. Phys. Lett.* **38** 030304
[23] Aaronson S 2005 *Proceedings of the Royal Society A* **461** 3473
[24] Traversa F L and Di Ventra M 2017 *Chaos* **27** 023107
[25] Zhang Y H and Ventra M D 2021 *Chaos* **31** 063127
[26] Bacon D 2004 *Phys. Rev. A* **70** 032309
[27] Abrams D S and Lloyd S 1998 *Phys. Rev. Lett.* **81** 3992
[28] Bennett C H, Leung D, Smith G and Smolin J A 2009 *Phys. Rev. Lett.* **103** 170502
[29] Boykin P O, Mor T, Pulver M, Roychowdhury V and Vatan F 1999 40*th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039)* (IEEE) pp. 486–494
[30] Dummit D S and Foote R M 2004 *Abstract Algebra* vol. 3 (Wiley Hoboken)