Quantum Information Processing, Vol. 4, No. 2, June 2005 (© 2005)
DOI: 10.1007/s11128-005-4480-y

Existence of the Exact CNOT on a Quantum Computer with the Exchange Interaction

Y. Kawano,[1] K. Kimura,[2] H. Sekigawa,[1] M. Noro,[3] K. Shirayanagi,[1] M. Kitagawa,[4] and M. Ozawa[5]

Received October 24, 2004; accepted February 8, 2005

We prove the existence of the exact CNOT gate on a quantum computer with the nearest-neighbor exchange interaction in the serial operation mode. Its existence has been an open problem, though a concrete sequence of exchange operations, which is approximately locally equivalent to the exact CNOT, has already been found. We found the exact values of time parameters (exchange rates between qubits) by using computer algebraic techniques such as Gröbner bases and resultants. These techniques have been widely used for finding rigorous solutions of simultaneous algebraic equations, and here are applied to finding quantum gates on the decoherence-free subsystem for the first time.

KEY WORDS: Quantum computation; decoherence-free subsystem; computer algebra; Gröbner basis; resultant.

PACS: 02.70.Wz, 03.65.Yz, 03.67.Lx.

1. INTRODUCTION

The study of quantum computation explosively advanced after Shor discovered a quantum algorithm that solves factorization problems much

[1]NTT Communication Science Laboratories, NTT Corporation, 3-1, Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-0198, Japan.
[2]Graduate School of Informatics, Kyoto University, Yoshida-Honmachi, Sakyo-ku, Kyoto, 606-8501, Japan.
[3]Department of Mathematics, Kobe University, Nada-ku, Kobe, 657-8501, Japan.
[4]Graduate School of Engineering Science, Osaka University, Toyonaka-shi, Osaka, 560-8531, Japan; Also at NTT Communication Science Laboratories, NTT Corporation, 3-1, Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-0198, Japan; Japan Science and Technology Agency, Japan.
[5]Graduate School of Information Sciences, Tohoku University, Aoba-ku, Sendai, 980-8579, Japan; Also at Japan Science and Technology Agency, Japan.

faster than a classical computer. Shor also found a quantum error-collecting code, which set the course for a breakthrough in fault-tolerant quantum computation. The error-correcting code was generalized, and since then many quantum codes have been proposed (cf. Chapter 10 in Ref. 1). The theory of quantum error-correcting codes tells us how much gate error is allowed for performing quantum computation when these codes are used. If gate errors in a quantum circuit are below the threshold, the quantum computation can be performed by correcting the quantum state after each gate.

The importance of fault-tolerant quantum computation has let to the study of another type of quantum error-correcting strategy called the *decoherence-free subsystem* (DFS).[2–7] Simply speaking, a DFS means the quantum computation in a subspace essentially invariant to noises from the environment. Quantum error-correcting codes are used for correcting control errors of quantum gates, while a DFS targets the circumvention of global errors caused by a uniform electromagnetic field that changes over time. Kempe *et al.*[3] describes these error-corrections as active and passive, respectively.

DiVincenzo and co-workers[8] have proposed explicit schemes for single-qubit rotations and for the CNOT on a DFS using three qubits as a logical qubit. In this model, $|0_L\rangle$ (logical zero) and $|1_L\rangle$ (logical one) are defined as $(1/\sqrt{2})(|01\rangle - |10\rangle)|0\rangle$ and $(1/\sqrt{6})(2|001\rangle - |010\rangle - |100\rangle)$, respectively, and quantum operations on the logical qubits are performed by the nearest-neighbor exchange interaction (the isotropic Heisenberg interaction). They considered two operation modes: serial and parallel. The serial mode allows one exchange interaction at a time, while the parallel mode allows using exchange interactions simultaneously between any neighboring pair of qubits at a time. Constructing quantum gates in the serial mode is more difficult than that in the parallel mode.

In the serial mode, they have shown that any single-qubit rotation can be performed precisely in principle, whereas the set of the diagram and the exchange rates between qubits (The diagram will be called the *19-gate sequence* in this paper. See Fig. 1.) proposed as the CNOT in their paper is an approximate one whose absolute inaccuracy to the CNOT is no greater than 6×10^{-5}. These values of the exchange rates are obtained by computational numerical search, and the exact values may not be found even if we greatly extend the computation time. Nevertheless, they state without any mathematical proof that 'further fine-tuning of these time parameters (exchange rates) would give the CNOT to any desired accuracy.' There seems to be no simple evidence that the exact CNOT exists on this model. Their research has been developed in Refs. 9, 10 and more accurate

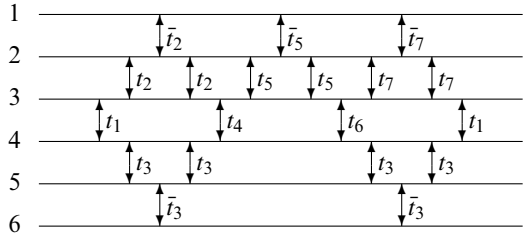

Fig. 1. This shows the diagram proposed by DiVincenzo and co-workers.[8] It will be called the 19-gate sequence in this paper. Each horizontal line represents a physical qubit. The upper three lines represent the first logical qubit, and the lower three represent the second. Variables $t_1, \ldots, t_7$ are time parameters for exchange interactions between qubits, while $\bar{t}_j$ is a value that satisfies $\tan(\pi t_j)\tan(\pi \bar{t}_j) = -2$ for each t_j. The diagram becomes approximately locally equivalent to the CNOT, when $t_1 = 0.410899$, $t_2 = 0.207110$, $t_3 = 0.2775258$, $t_4 = 0.640505$, $t_5 = 0.414720$, $t_6 = 0.147654$, $t_7 = 0.813126$.

solutions have been found using numerical search plus other techniques. However, the existence of the exact CNOT still remains an open problem.

In this paper, we solve this open problem. We obtained the exact values of time parameters (exchange rates) so that the 19-gate sequence makes the exact CNOT. Values for the exact CNOT are as follows: The value of t_1 is obtained by taking arccosine of a real solution of an integer-coefficient *12-degree* polynomial equation; those of t_4 and t_6 are obtained by taking arccosines of real solutions of integer-coefficient *24-degree* polynomial equations; those of t_3 and t_5 are obtained by taking arctangents of real solutions of integer-coefficient *48-degree* polynomial equations; and those of t_2 and t_7 are obtained by taking arctangents of real solutions of integer-coefficient *96-degree* polynomial equations. The following is one set of exact solutions given in units such that the SWAP gate corresponds to $t = 1/2$: $t_1 = 0.4108988797...$, $t_2 = 0.2071066664...$, $t_3 = 0.2775259469...$, $t_4 = 0.6405019519...$, $t_5 = 0.4147161436...$, $t_6 = 0.1476552801...$, and $t_7 = 0.8131082111....$ There are no other solutions around this one.

We obtained the exact values by the following strategy. We first represented the condition where the 19-gate sequence makes the exact CNOT by simultaneous equations with variables whose absolute values are 1, and then solved these equations by computer algebraic techniques, such as Gröbner bases and resultants.[11,12] Finally, we checked whether the

absolute values of them were 1. We used the computer software Maple[13] and Risa/Asir[14].

The key techniques are Gröbner bases and resultants. A Gröbner basis is a good generating set for an ideal in a polynomial ring and can be used for analyzing the solutions of simultaneous polynomial equations. A resultant gives the necessary conditions of solutions of simultaneous polynomial equations. Both are known as useful tools for solving simultaneous polynomial equations and have been deeply studied in the field of computer algebra. Our study applies these techniques to the construction of quantum gates in a DFS for the first time.

The rest of the paper organized as follows. We will give background materials in Section 2, which covers the DFS and describes fundamental notions of the Gröbner bases and resultants. Section 3 presents the main theorem. Section 4 concludes the paper. In Appendix A, we give the polynomials that represent the condition of time parameters so that the 19-gate sequence makes the exact CNOT. We calculated Gröbner bases of the ideal generated from those polynomials, which are shown in Appendix B. Values (to 50 decimal places) of time parameters for the exact CNOT are shown in Appendix C.

2. PRELIMINARIES

2.1. Three-qubit Decoherence-free System

We consider a quantum system that consists of n spin-(1/2) particles. Let $\sigma_x, \sigma_y, \sigma_z$ be Pauli matrices, i.e.,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and } \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We define $\sigma_x^j, \sigma_y^j, \sigma_z^j$ as

$$\sigma_w^j = \underbrace{I \otimes I \otimes \cdots \otimes \sigma_w \otimes \cdots \otimes I \otimes I}_{n}$$

$(w = x, y, z)$ in n spin-(1/2) particles. Let $\vec{S}_j = (\sigma_x^j, \sigma_y^j, \sigma_z^j)$ be the jth spin qubit. Heisenberg Hamiltonian between qubits is defined as

$$H_{\text{Heis}} = \frac{1}{2} \sum_{i \neq j} J_{ij}^H \vec{S}_i \cdot \vec{S}_j.$$

We assume $J_{ij}^H = J$ when i and j are successive numbers (i.e., they are adjacent), and $J_{ij}^H = 0$ otherwise. Then,

$$H_{\text{Heis}} = J \sum_{j=1}^{n-1} \vec{S}_j \cdot \vec{S}_{j+1}. \tag{1}$$

By the Schrödinger equation,

$$U(t)|\psi\rangle = \exp\left(\frac{-itJH_{\text{Heis}}}{\hbar}\right)|\psi\rangle. \tag{2}$$

Let E_{jk} be the swap operation between the jth and kth qubits. Since $2 \cdot E_{jk} - I = \vec{S}_j \cdot \vec{S}_k$, we have $e^{-it} \cdot \exp(2itE_{jk}) = \exp(it\vec{S}_j \cdot \vec{S}_k)$ for any real value t, i.e., unitary operators made by Heisenberg interaction (1) is equivalent to the swap operation up to a phase. Equation (2) implies

$$U(t)|\psi\rangle = \exp\left(\frac{-2itJ\sum E_{jj+1}}{\hbar}\right)|\psi\rangle$$

up to a phase. By changing the time scale, we define

$$U_{jj+1}(t) = \exp\left(\pi i t E_{jj+1}\right).$$

$U_{jj+1}(t) = \exp(\pi i t E_{jj+1})$ is the identity when $t = 0, 1, 2, \ldots$, and the swap when $t = \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \ldots$ Here, t is called the time parameter. By selecting the value of the time parameter, partial exchange can be performed by $U_{jj+1}(t)$.

As is well-known, the set of exchange operations is not universal. Therefore, we encode a logical qubit into three spin-(1/2) particles so that the set of exchange operations becomes universal on the quantum computer by logical qubits.

We split physical qubits into blocks, each of which consists of three particles. The logical zero and one, denoted by $|0_L\rangle$ and $|1_L\rangle$, is defined as

$$|0_L\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}|010\rangle - \frac{1}{\sqrt{2}}|100\rangle, \text{ and}$$
$$|1_L\rangle \stackrel{\text{def}}{=} \frac{2}{\sqrt{6}}|001\rangle - \frac{1}{\sqrt{6}}|010\rangle - \frac{1}{\sqrt{6}}|100\rangle.$$

Then, $U_{12}(t)$ is a rotation around the z axis of the logical Bloch sphere made by the logical zero and one. $U_{23}(t)$ is a rotation around the axis of 120° from the z axis of the logical Bloch sphere. Any single-qubit

rotation on the logical Bloch sphere can then be performed by $U_{12}(t)$ and $U_{23}(t)$.

We assume that six spin-(1/2) qubits are in a queue, and that interactions between adjacent qubits can be performed. Let E_{jj+1} $(j = 1, 2, \ldots, 5)$ be the swaps between the jth and $(j+1)$-st qubits.

The Hilbert space where the total spin 1 and $S_z^{\text{total}} = 1$ in the six-qubit system is nine-dimensional. This Hilbert space is denoted $\widetilde{\mathcal{H}}$. Let $\mathcal{H}$ be the Hilbert space spanned by $\{|0_L\rangle|0_L\rangle, |0_L\rangle|1_L\rangle, |1_L\rangle|0_L\rangle, |1_L\rangle|1_L\rangle\}$. Then, $\mathcal{H} \subseteq \widetilde{\mathcal{H}}$.

Exchange operations make an evolution on the whole nine-dimensional Hilbert space $\widetilde{\mathcal{H}}$.[3] This means that states in $\mathcal{H}$ may leak to the outside of $\mathcal{H}$ by exchange operations. We say that a sequence of exchange operations becomes a *gate* on the encoded qubits when the leak is null (after operating the sequence of exchange operations).

The gate made by a sequence of exchange operations can be expressed as follows. First, we introduce a basis of the nine-dimensional Hilbert space $\mathcal{H}$, $|a_1\rangle, \ldots, |a_9\rangle$, where $|a_1\rangle = |0_L\rangle|0_L\rangle$, $|a_2\rangle = |0_L\rangle|1_L\rangle$, $|a_3\rangle = |1_L\rangle|0_L\rangle$, $|a_4\rangle = |1_L\rangle|1_L\rangle$. The swaps $E_{12}, \ldots, E_{56}$ can then be represented by 9×9 matrices on the basis. Unitary operators $U_{12}(x)$, $U_{23}(x)$, $U_{34}(x)$, $U_{45}(x)$, and $U_{56}(x)$ can also be calculated by the definitions $U_{jj+1}(x) = \exp(\pi i x E_{jj+1})$ for $j = 1, \ldots, 5$. A sequence of exchange operations is then expressed by a sequence of pairs $((U_{j_1 j_1+1}, t_1), \ldots, (U_{j_n j_n+1}, t_n))$ comprising a unitary operator and the parameter value.

Given a sequence of exchange operations, $((U_{i_1 i_1+1}, t_1), \ldots, (U_{i_n i_n+1}, t_n))$, let $A(\vec{t})$, $B(\vec{t})$, $C(\vec{t})$, $D(\vec{t})$ $(\vec{t} = (t_1, \ldots, t_n))$ be matrices such that

$$U_{i_n i_n+1}(t_n) \cdots U_{i_2 i_2+1}(t_2) U_{i_1 i_1+1}(t_1) = \begin{pmatrix} A(\vec{t}) & B(\vec{t}) \\ C(\vec{t}) & D(\vec{t}) \end{pmatrix}, \tag{3}$$

where $A(\vec{t})$, $B(\vec{t})$, $C(\vec{t})$, and $D(\vec{t})$ are 4×4, 4×5, 5×4, and 5×5 matrices, respectively. Then, the sequence of exchange operations is called the gate $A(\vec{t})$ on the encoded qubits if $B(\vec{t}) = 0$. ($C(\vec{t}) = 0$ is also true if $B(\vec{t}) = 0$, since the matrix (3) is unitary.)

The following fact is shown in Ref. 8; There is a set of time parameters $t_1, \ldots, t_7$ such that the sequence of exchange operations shown in Fig. 1 is approximately *locally equivalent* to the CNOT.

Here, local equivalence is defined as follows.

Definition 1. Let A and A' be two-qubit quantum gates. A is locally equivalent to A' if there are single-qubit rotations $R_1, \ldots, R_4$ such that $A = (R_1 \otimes R_2) A' (R_3 \otimes R_4)$.

The notion of local equivalence is characterized by a set of numbers, which is called the Makhlin invariant.

Definition 2. Let M be an element in $SU(4)$. Define $M_B = Q^\dagger M Q$, where

$$Q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & i \\ 0 & i & 1 & 0 \\ 0 & i & -1 & 0 \\ 1 & 0 & 0 & -i \end{pmatrix}.$$

Set $m = M_B^T M_B$, $M_1 = tr^2(m)/16 det M$, and $M_2 = (tr^2(m) - tr(m^2))/4 det M$. We call (M_1, M_2) the Makhlin invariant of M.

Theorem 1[16]. *A is locally equivalent to A' iff the Makhlin invariants of A and A' are the same.*

Example 1. The Makhlin invariants of the identity, the CNOT, the SWAP, and the root SWAP are $(1, 3)$, $(0, 1)$, $(-1, -3)$, $(i/4, 0)$, respectively.

DiVincenzo and his co-workers[8] state that

1. the Makhlin invariant of $A(t_1, \ldots, t_7)$ is approximately equal to (0,1), and
2. all elements in $B(t_1, \ldots, t_7)$ are approximately equal to 0,

when $t_1 = 0.410899(2)$, $t_2 = 0.207110(20)$, $t_3 = 0.2775258(12)$, $t_4 = 0.640505(8)$, $t_5 = 0.414720(10)$, $t_6 = 0.147654(12)$, $t_7 = 0.813126(12)$. Here, the values in the parenthesis show the uncertainty of the values of the last digits. Using a computer search technique, they found that this set of solution satisfies the condition. They state that 'further fine-tuning of these time parameters would give the CNOT to any desired accuracy.'

More accurate solutions have been obtained by numerical search plus other techniques (cf. Refs. 9, 10). However, these strategies cannot be used for proving the existence of the exact CNOT. In this paper, we will prove algebraically the existence of the exact CNOT by solving the simultaneous equations that represent

1. the Makhlin invariant of $A(t_1, \ldots, t_7)$ is (0,1), and
2. all elements in $B(t_1, \ldots, t_7)$ are 0.

2.2. Gröbner Bases and Resultants

In this section, we explain Gröbner bases, which can transform simultaneous equations into the equivalent ones, and resultants, a kind of

powerful transformation tools, which transform simultaneous equations under necessary conditions, and other techniques. See[11,12,15] for details.

First, we explain the correspondence between simultaneous equations and ideals. Consider simultaneous equations $f_1 = \cdots = f_l = 0$, where $f_i \in \mathbb{C}[x_1, \ldots, x_n]$. Let $\langle f_1, \ldots, f_m \rangle$ be

$$\left\{ \sum_{i=1}^{l} a_i f_i \;\middle|\; a_i \in \mathbb{C}[x_1, \ldots, x_n] \right\}$$

the ideal generated by $f_1, \ldots, f_l$. Then, two systems of simultaneous equations $f_1 = \cdots = f_l = 0$ and $g_1 = \cdots = g_m = 0$ have the same zeros if and only if the two ideals, $\langle f_1, \ldots, f_l \rangle$ and $\langle g_1, \ldots, g_m \rangle$, are equal. Therefore, if we find a good basis $\{g_1, \ldots, g_m\}$ of the ideal $\langle f_1, \ldots, f_l \rangle$, then, computing the common zeros of $g_1 = \cdots = g_m = 0$, we can find the common zeros of $f_1 = \cdots = f_l = 0$. The Gröbner basis is one such good basis.

To define a Gröbner basis, we need some preparations. Let $\mathbb{N}$ be the set of nonnegative integers.

Definition 3 [monomial ordering]. Let K be a field. A monomial ordering on $K[x_1, \ldots, x_n]$ is any relation on the set of monomials x^α, $\alpha \in \mathbb{N}^n$ satisfying:

1. $<$ is a total ordering on $\mathbb{N}^n$.
2. If $\alpha < \beta$ and $\gamma \in \mathbb{N}^n$, then $\alpha + \gamma < \beta + \gamma$.
3. Every nonempty subset of $\mathbb{N}^n$ has a minimal element under $<$.

Definition 4. Let K be a field and let $<$ be a monomial order on $K[x_1, \ldots, x_n]$. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $K[x_1, \ldots, x_n]$.

1. The multidegree of f is

$$\text{multideg}(f) = \max\{\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0\}.$$

2. The leading term of f is

$$\text{LT}(f) = a_{\text{multideg(f)}} x^{\text{multideg(f)}}.$$

Once we choose a monomial ordering, then, for any ideal I of $K[x_1, \ldots, x_n]$, we can define its ideal of leading terms.

Definition 5. Let $I \subset K[x_1, \ldots, x_n]$ be an ideal other than $\{0\}$.

1. We denote by $\text{LT}(I)$ the set of leading terms of elements of I.
2. We denote by $\langle \text{LT}(I) \rangle$ the ideal generated by the elements of $\text{LT}(I)$.

After preparing the above definitions, we can define a Gröbner basis.

Definition 6 [Gröbner basis]. Let I be an ideal of $K[x_1, \ldots, x_n]$. Fix a monomial order. A finite subset $\{g_1, \ldots, g_m\}$ of I is said to be a Gröbner basis if $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m) \rangle$.

Then the following statement holds (see [11,12,15] for the proof).

Theorem 2. Fix a monomial order. Then every ideal other than $\{0\}$ has a Gröbner basis. Furthermore, for any Gröbner basis $\{g_1, \ldots, g_m\}$ for an ideal I, $I = \langle g_1, \ldots, g_m \rangle$.

To compute the simultaneous zeros of the polynomials $f_i(x_1, \ldots, x_n)$ $(i = 1, \ldots, l)$, we take a good monomial ordering on $K[x_1, \ldots, x_n]$ and compute the Gröbner basis $\{g_1, \ldots, g_m\}$ of the ideal $\langle f_1, \ldots, f_l \rangle$. It is desirable that the Gröbner basis consists of polynomials, one of which is a polynomial only in a variable x_i and the others are the polynomials of the form $x_j - h_j(x_i)$, where $h_j(x_i) \in K[x_i]$. This style of the basis is called the shape basis. See [11,12,15] for details about the shape basis and computation methods for a Gröbner basis such as Buchberger's algorithm.

Next, we explain resultants. Let $f(x) = \sum_{i=0}^{l} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$. Then the following $(l+m) \times (l+m)$ matrix

$$\left.\begin{pmatrix} a_l & a_{l-1} & \ldots & a_1 & a_0 & 0 & \ldots & & 0 \\ 0 & a_l & a_{l-1} & \ldots & a_1 & a_0 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & a_l & a_{l-1} & \ldots & a_1 & a_0 & 0 \\ 0 & \ldots & & 0 & a_l & a_{l-1} & \ldots & a_1 & a_0 \\ b_m & b_{m-1} & \ldots & b_1 & b_0 & 0 & \ldots & & 0 \\ 0 & b_n & b_{m-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & b_m & b_{m-1} & \ldots & b_1 & b_0 & 0 \\ 0 & \ldots & & 0 & b_m & b_{m-1} & \ldots & b_1 & b_0 \end{pmatrix}\right\} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\end{matrix}}\right\} l \end{matrix}$$

is said to be the Sylvester matrix of f and g with respect to x, and its determinant is said to be the resultant of f and g with respect to x, denoted $\mathrm{Res}(f, g, x)$. Here, the coefficients a_i's and b_i's may be polynomials in other variables than x.

Let f and g be polynomials in $x_1, \ldots, x_n$ with coefficients in $\mathbb{C}$. Then, $\mathrm{Res}(f, g, x_1) \in \mathbb{C}[x_2, \ldots, x_n]$ and

$$\mathrm{Res}(f, g, x_1) = Af + Bg,$$

where A, $B \in \mathbb{C}[x_1, \ldots, x_n]$ (See for example [11]). Therefore, when two polynomials f and $g \in \mathbb{C}[x_1, \ldots, x_n]$ have a common zero at $x_1 = \alpha_1, \ldots,$

$x_n = \alpha_n$, the polynomial $\mathrm{Res}(f, g, x_1) \in \mathbb{C}[x_2, \ldots, x_n]$ has a zero at $x_2 = \alpha_2$, $\ldots$, $x_n = \alpha_n$. Unfortunately, the converse is not true. Consider the following example.

$$f_1(x_1, x_2) = x_1 x_2 + 1,$$
$$f_2(x_1, x_2) = x_1 x_2 - 1.$$

Clearly, the simultaneous equations $f_1 = f_2 = 0$ have no solution; however, the resultant $\mathrm{Res}(f_1, f_2, x_1) = -2x_2$ has a zero at $x_2 = 0$. Transformations utilizing resultants are only necessary condition transformations; however, they can transform the original problems to subproblems. To recover the sufficiency, we add the original equations into the subproblems.

We introduce two other techniques, saturation and prime ideal decomposition. In our setting, we should treat the conditions $D_j \neq 0$ (See Section 3.2 for D_js). We can treat these conditions by adding a new variable t and an equation $tD_j - 1 = 0$. This technique is called saturation.

Next, we introduce prime ideal decomposition. For example, we consider the following simultaneous equations.

$$x^2 + y^2 - 3 = 0,$$
$$xy - 1 = 0.$$

The Gröbner basis in the lexicographic order $y < x$ (See [11,12,15]) is as follows.

$$-y^4 + 3y^2 - 1 = 0,$$
$$x + y^3 - 3y = 0.$$

The left side of the first equation can be factorized as follows.

$$-y^4 + 3y^2 - 1 = -(y^2 - y - 1)(y^2 + y - 1)$$

Therefore, the simultaneous equations are transformed into two subproblems:

$$y^2 - y - 1 = 0,$$
$$x + y^3 - 3y = 0$$

and

$$y^2 + y - 1 = 0,$$
$$x + y^3 - 3y = 0.$$

The prime ideal decomposition can treat these procedures systematically.

3. MAIN THEOREM

Our main theorem is given below.

Theorem 3. There exist values of time parameters $t_1, \ldots, t_7$ such that the 19-gate sequence is exactly locally equivalent to the CNOT. More precisely, there exist values of time parameters $t_1, \ldots, t_7$ such that they satisfy the conditions

1. $A(t_1, \ldots, t_7)$ is locally equivalent to the CNOT, and
2. $B(t_1, \ldots, t_7) = 0$.

Our strategy to prove the theorem can be split into three stages.

1. Represent the conditions by algebraic equations with seven variables $r_1, \ldots, r_7$ whose absolute values are 1.
2. Solve the algebraic equations by computer using Gröbner bases and the resultants, and check if the absolute values of the obtained solutions of $r_1, \ldots, r_7$ are 1.
3. Compute numerical values of $t_1, \ldots, t_7$.

3.1. First Stage

To represent the conditions by equations, we first introduce a basis of the nine-dimensional Hilbert space, which is the eigenspace of the total spin is 1 and $S_z^{\text{total}} = 1$ in six qubits. The following is one of the bases of the space.

$$
\begin{aligned}
|a_9\rangle &\stackrel{\text{def}}{=} \frac{1}{2}(|01\rangle - |10\rangle)(|01\rangle - |10\rangle)|00\rangle, \\
|a_8\rangle &\stackrel{\text{def}}{=} \frac{1}{\sqrt{3}}(2E_{23} - I)|a_9\rangle, \\
|a_7\rangle &\stackrel{\text{def}}{=} \frac{1}{\sqrt{3}}(2E_{45} - I)|a_9\rangle, \\
|a_6\rangle &\stackrel{\text{def}}{=} \frac{1}{\sqrt{3}}(2E_{23} - I)|a_7\rangle, \\
|a_5\rangle &\stackrel{\text{def}}{=} \frac{1}{2\sqrt{2}}(3E_{34} - I)|a_6\rangle, \\
|a_4\rangle &\stackrel{\text{def}}{=} \frac{1}{2\sqrt{2}}(3E_{56} - I)|a_7\rangle, \\
|a_3\rangle &\stackrel{\text{def}}{=} \frac{1}{2\sqrt{2}}(3E_{56} - I)|a_6\rangle,
\end{aligned}
$$

$$|a_2\rangle \stackrel{\text{def}}{=} \frac{1}{2\sqrt{2}}(3E_{56} - I)|a_5\rangle,$$
$$|a_1\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{15}}(4E_{45} - I)|a_2\rangle.$$

None of $\{|a_1\rangle, \ldots, |a_9\rangle\}$ coincides with four states $\{|0_L\rangle|0_L\rangle,\ |0_L\rangle|1_L\rangle,\ |1_L\rangle|0_L\rangle,\ |1_L\rangle|0_L\rangle\}$. To describe the swap operations by matrices on a basis including these four states, we introduce a translation matrix S defined by

$$S = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & \frac{2\sqrt{2}}{3} & 0 & 0 & \frac{1}{3} & 0 & 0 \\
0 & 0 & \frac{2\sqrt{2}}{3} & 0 & 0 & \frac{1}{3} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & \frac{\sqrt{3}}{2} & 0 & -\frac{1}{6} & 0 & 0 & \frac{\sqrt{2}}{3} & 0 & 0 \\
\frac{\sqrt{3}}{2} & 0 & -\frac{1}{6} & 0 & 0 & \frac{\sqrt{2}}{3} & 0 & 0 & 0 \\
0 & -\frac{1}{2} & 0 & -\frac{1}{2\sqrt{3}} & 0 & 0 & \frac{\sqrt{6}}{3} & 0 & 0 \\
-\frac{1}{2} & 0 & -\frac{1}{2\sqrt{3}} & 0 & 0 & \frac{\sqrt{6}}{3} & 0 & 0 & 0
\end{pmatrix}.$$

It can be easily checked that $S^{-1} = S^T$, i.e., S is an orthogonal matrix. Let $|b_1\rangle, \ldots, |b_9\rangle$ be $S^{-1}|a_1\rangle, \ldots, S^{-1}|a_9\rangle$, respectively. Then, $|b_1\rangle = |0_L\rangle|0_L\rangle$, $|b_2\rangle = |1_L\rangle|0_L\rangle$, $|b_3\rangle = |0_L\rangle|1_L\rangle$, $|b_4\rangle = |1_L\rangle|1_L\rangle$. $\{|b_1\rangle, \ldots, |b_9\rangle\}$ is another basis of the nine-dimensional Hilbert space. S is the translation from $\{|b_1\rangle, \ldots, |b_9\rangle\}$ to $\{|a_1\rangle, \ldots, |a_9\rangle\}$.

The operators $U_{12}(x), \ldots, U_{56}(x)$ can be represented by 9×9 matrices. We introduce new operators: $U_{123}(t) = U_{23}(t)U_{12}(\bar{t})U_{23}(t)$ and $U_{456}(t) = U_{45}(t)U_{56}(\bar{t})U_{45}(t)$, where t and $\bar{t}$ satisfy the t-$\bar{t}$ relation. The 19-gate sequence can be written by

$$U_{34}(t_1)U_{456}(t_3)U_{123}(t_7)U_{34}(t_6)U_{123}(t_5)U_{34}(t_4)U_{123}(t_2)U_{456}(t_3)U_{34}(t_1).$$

Thus, the conditions that the 19-gate sequence is locally equivalent to the CNOT can be represented by simultaneous equations of $t_1, \ldots, t_7$.

However, the equations that represent the conditions contain exponentials, since $U_{jj+1}(t) = \exp(\pi i t E_{jj+1})$. In order to represent the conditions by algebraic equations, we introduce seven new variables: $r_1, r_2, \ldots, r_7$, defined as $r_1 = \exp(2\pi i t_1)$, $r_2 = \exp(2\pi i(t_2 + \bar{t}_2))$, $r_3 = \exp(2\pi i(t_3 + \bar{t}_3))$, $r_4 = \exp(2\pi i t_4)$, $r_5 = \exp(2\pi i(t_5 + \bar{t}_5))$, $r_6 = \exp(2\pi i t_6)$, and $r_7 = \exp(2\pi i(t_7 + \bar{t}_7))$, where t_j and $\bar{t}_j$ satisfy $\tan(\pi t_j)\tan(\pi \bar{t}_j) = -2$ (the t-$\bar{t}$ relation). Since $t_1, \ldots, t_7$ are real numbers, $r_1, \ldots, r_7$ must satisfy

$$|r_j| = 1 \quad \text{for} \quad j = 1, ..., 7. \tag{4}$$

All elements in $U_{jj+1}(t)$ are then represented by fractions of integer-coefficient polynomials of $r_1, \ldots, r_7$. We solved the condition that the 19-gate sequence is locally equivalent to the CNOT using Maple software and obtained seven fractions of integer-coefficient polynomials.

$$P = \left\{ \frac{N_1}{D_1}, \frac{N_2}{D_2}, \frac{N_3}{D_3}, \frac{N_4}{D_4}, \frac{N_5}{D_5}, \frac{N_6}{D_6}, \frac{N_7}{D_7} \right\}.$$

$N_1, \ldots, N_7$ and $D_1, \ldots, D_7$ will be given in Appendix A. Thus, zeros of (4) and P satisfy the condition that the 19-gate sequence is locally equivalent to the CNOT.

3.2. Second Stage

We find the common zeros of the set of the polynomials P'

$$P' = \{N_1, N_2, N_3, N_4, N_5, N_6, N_7\},$$

under the conditions that denominators are not zero; that is, $D_j \neq 0$ ($j = 1, \ldots, 7$), and $|r_j| = 1$. The denominator conditions are equivalent to the following (see Appendix A):

$$r_1 r_3 - r_3 - 2r_1 - 1 \neq 0, \tag{5}$$

$$2r_1 r_3 + 7r_3 + 2r_1 - 2 \neq 0, \tag{6}$$

$$2r_1^2 r_3 + 2r_1^2 - 3r_3 r_1 + r_3 + 6r_1 + 1 \neq 0, \tag{7}$$

$$4r_1 + 1 \neq 0, \tag{8}$$

$$r_1 r_3 + 2r_3 - 2r_1 + 2 \neq 0, \tag{9}$$

$$r_1 - 1 \neq 0, \tag{10}$$

$$r_4 - 1 \neq 0, \tag{11}$$

$$r_6 - 1 \neq 0. \tag{12}$$

Using techniques described in Section 2, we finally obtain 12 components of the solutions, and we immediately find that 11 components do not satisfy the absolute value condition since the monomials r_j's appear (which means that $r_j = 0$).

Below, we examine the last component V (see Appendix B). Let the monomial ordering be the lexicographic order $r_2 < r_1 < r_3 < r_4 < r_5 < r_6 < r_7$ and compute the Gröbner basis. Then the basis is the shape basis. Add the

polynomials $x+iy-r_2$ and x^2+y^2-1, reduce the polynomials in V by the relation $x^2+y^2-1=0$ and compute the Gröbner basis $V \cup \{x+iy-r_2, x^2+y^2-1\}$ with the lexicographic order in $y<x<r_2<r_1<r_3<r_4<r_5<r_6<r_7$. Then, we find that x and r_j's are polynomials in y. That is, the real parts and the imaginary parts of $r_1, \ldots, r_7$ are rational polynomials of y. We write them as $R_j(y)$ and $I_j(y)$. Let $f(y)$ be the minimal polynomial of y.

$$
\begin{aligned}
f(y) = & -39031585969656430161819346100554240000y^{24} \\
& -13034178206275816025220581634519763968000y^{22} \\
& -67384276977353415814988614987562350021017 6y^{20} \\
& +36477892398915518145717504186102663263577 6y^{18} \\
& +61331854630376629467218543356999880782168 32y^{16} \\
& -13854926979243219590587010385949871627682624y^{14} \\
& +10774683492876675732753422160410527517858967y^{12} \\
& -14179569755091322945336021182490210366684 56y^{10} \\
& -21525844801267961276318221750478493153924 96y^{8} \\
& +83375859401509954156611965307705387160396 8y^{6} \\
& +52095028092680191026935578295687475255552y^{4} \\
& -46622214916288265789457107993467999119360y^{2} \\
& -10659808451805770720564390069926170624.
\end{aligned}
$$

We have confirmed that the 24-degree polynomial $f(y)$ divides $R_j(y)^2+I_j(y)^2-1$ for $j=1, \ldots, 7$. It is necessary that y is real to guarantee the absolute value condition $|r_j|=1$, and this divisibility implies that it is also the sufficient condition. We can construct all solutions of $r_j = R_j(y) + i \cdot I_j(y)$ from the real solutions y of $f(y)=0$.

3.3. Third Stage

To compute the numerical values of t_j's, we first compute the real roots of $f(y)=0$. Using Sturm's algorithm, we find that there are no multiple roots and four real roots. Note that $f(y)$ does not change with substitutions $y \mapsto -y$, $1 \pm y$. There exists one and only one real root y_0 in the interval $I=[l, h]$, where

$$l = -0.897002652566584189575219794815031860716828511573 88$$

and $h = l + 10^{-50}$.

Second, we compute the numerical value for t_2. Put $\tau_2 = \tan(\pi t_2)$ and $\bar{\tau}_2 = \tan(\pi \bar{t}_2)$. Then, we have

$$y = \sin(2\pi(t_2 + \bar{t}_2)) = \frac{6\tau_2^3 - 12\tau_2}{\tau_2^4 + 5\tau_2^2 + 4},$$

considering the relation $\tau_2 \bar{\tau}_2 = -2$. In $f(y) = 0$, substitute y into $(6\tau_2^3 - 12\tau_2)/(\tau_2^4 + 5\tau_2^2 + 4)$ and cancel the denominator ($\tau_2^4 + 5\tau_2^2 + 4$ is positive for any real value τ_2). Then, we get a 96-degree equation in τ_2, which has no multiple roots and 16 real roots. Among 16 real roots, the real root τ_{20} in the interval $[0.76122, 0.76123]$ satisfies the equation

$$\frac{6\tau_{20}^3 - 12\tau_{20}}{\tau_{20}^4 + 5\tau_{20}^2 + 4} = y_0.$$

Computing τ_{20} with sufficient accuracy, we realize that $t_2 = \arctan(\tau_{20}/\pi)$ is in the interval $[l_2, h_2]$, where

$$l_2 = 0.207106666493953556546114196045020769325571621163 04$$

and $h_2 = l_2 + 10^{-50}$.

Third, we explain how to compute t_1. The computation for t_4 and t_6 are similar. First, take the 22-degree polynomial $R_1(y)$, which is the real part of r_1. By checking that $R_1'(y)$ has no real root in the interval I, we know that $R_1(y)$ is monotone in the interval I. Therefore, we can easily compute the interval containing $R_1(y_0)$ by computing only the endpoints of the interval I (or subintervals of I) containing y_0. For example, $R_1(y_0) = \cos(2\pi t_1)$ is in the interval

$$[-0.847340700899631619985673967372807978195254162289901986073 75,$$

$$-0.847340700899631619985673967372807978195254162289901986073 74].$$

From this interval we know that $t_1 = \arccos(R_1(y_0))/(2\pi)$ is in the interval $[l_1, h_1]$, where

$$l_1 = 0.410898879757181446365233362885976241946328339587 85$$

and $h_1 = l_1 + 10^{-50}$.

Finally, we describe the calculation for t_7. The computation for t_3 and t_5 are similar to that for t_7. To compute t_7, first we take the 23-degree polynomial $I_7(y)$, which is the imaginary part of r_7. $I_7(y_0)$ is in the interval $[0.9699291, 0.9699292]$. Next, we compute the minimal polynomial r_7, which is 24-degree. The imaginary part y_7 of r_7 satisfies the same equation for y. Put $\tau_7 = \tan(\pi t_7)$ and $\bar{\tau}_7 = \tan(\pi \bar{t}_7)$. Then, we have

$$y_7 = \sin(2\pi(t_7 + \bar{t}_7)) = \frac{6\tau_7^3 - 12\tau_7}{\tau_7^4 + 5\tau_7^2 + 4},$$

considering the relation $\tau_7 \bar{\tau}_7 = -2$. In $f(y_7) = 0$, substitute y_7 into $(6\tau_7^3 - 12\tau_7)/(\tau_7^4 + 5\tau_7^2 + 4)$ and cancel the denominator ($\tau_7^4 + 5\tau_7^2 + 4$ is positive for any real value τ_7). Then, we get a 96-degree equation in τ_7, which has no multiple roots and 16 real roots. Among these 16 real roots, the real root τ_{70} in the interval $[-0.66542, -0.66541]$ satisfies the equation

$$\frac{6\tau_{70}^3 - 12\tau_{70}}{\tau_{70}^4 + 5\tau_{70}^2 + 4} = I_7(y_0).$$

Computing τ_{70} with sufficient accuracy, we realize that $t_7 = \arctan(\tau_{70}/\pi)$ is in the interval $[l_7, h_7]$, where

$$l_7 = 0.8131082111163056380371183861058099057489557394483 2$$

and $h_7 = l_7 + 10^{-50}$. The above interval for t_7 is a little out of the range $[0.813114, 0.813138]$ that DiVincenzo and co-workers[8] have proposed.

4. CONCLUDING REMARKS

We proved the existence of the exact CNOT on a quantum computer with the nearest–neighbor exchange interaction in the serial mode. Computer algebraic techniques such as Gröbner bases and resultants were used for this purpose. Values for the exact CNOT are obtained as follows: The value of t_1 is obtained by taking arccosine of a real solution of an integer-coefficient *12-degree* polynomial equation; those of t_4 and t_6 are obtained by taking arccosines of real solutions of integer-coefficient *24-degree* polynomial equations; those of t_3 and t_5 are obtained by taking arctangents of real solutions of integer-coefficient *48-degree* polynomial equations; and those of t_2 and t_7 are obtained by taking arctangents of real solutions of integer-coefficient *96-degree* polynomial equations. We confirmed that there is a set of values of time parameters for the exact CNOT around the one proposed by DiVincenzo and co-workers.[8]

We found the exact values of time parameters so that the 19-gate sequence makes the exact CNOT; however, the existence of a shorter sequence that can make the exact CNOT is an open problem. If there exists such a sequence, we might be able to find it using the strategy in this paper. Even if there is no such sequence, our approach could be used, because Gröbner bases tell us of not only the existence of zeros of polynomials but also of the non-existence of them.

Appendix A. Polynomial Functions Obtained in the First Stage

The condition P is written as

$$P = \left\{ \frac{N_1}{D_1}, \frac{N_2}{D_2}, \frac{N_3}{D_3}, \frac{N_4}{D_4}, \frac{N_5}{D_5}, \frac{N_6}{D_6}, \frac{N_7}{D_7} \right\}.$$

Here, $N_1, \ldots, N_7$ and $D_1, \ldots, D_7$ are the following polynomials.

$$\begin{aligned}
N_1 &= (-12r_1r_3^3 + 4r_1^3r_3^3 + 8r_3^3 - 6r_1^3r_3^2 + 30r_1r_3^2 - 24r_1^2r_3^2 - 24r_1^3r_3 - 21r_1^2r_3 - 30r_1r_3 - 6r_3 - 14r_1^3 + 2 \\
&\quad + 3r_1^2 + 9r_1) - (-r_3 + r_1r_3 - 1 - 2r_1)(r_1r_3 + 2r_3 + 2 - 2r_1)(2r_1r_3 + 7r_3 - 2 + 2r_1)r_6r_4r_7r_5r_2 \\
N_2 &= 3(-26 + 785r_1r_3 - 582r_1r_3^2 - 1599r_1^2r_3^2 + 2195r_1^2r_3 - 229r_1 + 88r_3 - 607r_1^2 - 30r_3^2 - 142r_1r_3^3 + 506r_1^2r_3^3 \\
&\quad + 2481r_1^3r_3 + 603r_1^3r_3^2 + 538r_1^4r_3^3 + 4r_1^4r_3^4 - 92r_1^5r_3^3 + 1302r_1^5r_3^2 + 1684r_1^5r_3 - 56r_1^5r_3^4 + 156r_1^6r_3^2 + 788r_1^6r_3 \\
&\quad + 8r_1^6r_3^4 - 148r_1^6r_3^3 - 4r_1r_3^4 - 196r_1^2r_3^4 - 558r_1^3r_3^3 + 204r_1^3r_3^4 + 150r_1^4r_3^2 + 2914r_1^4r_3 - 104r_3^3 - 342r_1^3 + 382r_1^4 \\
&\quad + 476r_1^6 + 346r_1^5 + 40r_3^4) + r_2r_7(4r_1 + 1)(2r_1r_3 + 7r_3 - 2 + 2r_1)(2r_1^2r_3 + 2r_1^2 - 3r_1r_3 + 6r_1 + r_3 + 1)(r_1r_3 \\
&\quad + 2r_3 + 2 - 2r_1)(-r_3 + r_1r_3 - 1 - 2r_1)(r_5r_6r_4 + 2r_5r_6 + 2r_5r_4 + 4r_5 - 2r_6r_4 + 2r_6 + 2r_4 - 2) \\
N_3 &= 3(14 - 461r_1r_3 + 636r_1r_3^2 + 1023r_1^2r_3^2 - 788r_1^2r_3 + 103r_1 - 64r_3 + 169r_1^2 + 66r_3^2 - 254r_1r_3^3 - 584r_1^2r_3^3 \\
&\quad + 258r_1^3r_3 - 1044r_1^3r_3^2 + 38r_1^4r_3^3 - 148r_1^4r_3^4 - 352r_1^5r_3^3 - 267r_1^5r_3^2 + 356r_1^5r_3 + 80r_1^5r_3^4 - 102r_1^6r_3^2 + 166r_1^6r_3 \\
&\quad + 28r_1^6r_3^4 - 86r_1^6r_3^3 + 4r_1r_3^4 + 352r_1^2r_3^4 + 1182r_1^3r_3^3 - 228r_1^3r_3^4 - 312r_1^4r_3^2 + 533r_1^4r_3 + 56r_3^3 - 204r_1^3 - 427r_1^4 \\
&\quad + 154r_1^6 + 191r_1^5 - 88r_3^4) + r_7(4r_1 + 1)(2r_1r_3 + 7r_3 - 2 + 2r_1)(2r_1^2r_3 + 2r_1^2 - 3r_1r_3 + 6r_1 + r_3 + 1)(r_1r_3 + 2r_3 \\
&\quad + 2 - 2r_1)(-r_3 + r_1r_3 - 1 - 2r_1)(r_5r_6r_4 - r_5r_6 + 2r_5r_4 - 2r_5 - 2r_6r_4 - r_6 + 2r_4 + 1) \\
N_4 &= 3(14 - 461r_1r_3 + 636r_1r_3^2 + 1023r_1^2r_3^2 - 788r_1^2r_3 + 103r_1 - 64r_3 + 169r_1^2 + 66r_3^2 - 254r_1r_3^3 - 584r_1^2r_3^3 \\
&\quad + 258r_1^3r_3 - 1044r_1^3r_3^2 + 38r_1^4r_3^3 - 148r_1^4r_3^4 - 352r_1^5r_3^3 - 267r_1^5r_3^2 + 356r_1^5r_3 + 80r_1^5r_3^4 - 102r_1^6r_3^2 + 166r_1^6r_3 \\
&\quad + 28r_1^6r_3^4 - 86r_1^6r_3^3 + 4r_1r_3^4 + 352r_1^2r_3^4 + 1182r_1^3r_3^3 - 228r_1^3r_3^4 - 312r_1^4r_3^2 + 533r_1^4r_3 + 56r_3^3 - 204r_1^3 - 427r_1^4 \\
&\quad + 154r_1^6 + 191r_1^5 - 88r_3^4) + r_2(4r_1 + 1)(2r_1r_3 + 7r_3 - 2 + 2r_1)(2r_1^2r_3 + 2r_1^2 - 3r_1r_3 + 6r_1 + r_3 + 1)(r_1r_3 + 2r_3 \\
&\quad + 2 - 2r_1)(-r_3 + r_1r_3 - 1 - 2r_1)(r_5r_6r_4 + 2r_5r_6 - r_5r_4 - 2r_5 - 2r_6r_4 + 2r_6 - r_4 + 1) \\
N_5 &= 3(-4 + 346r_1r_3 - 1272r_1r_3^2 - 1542r_1^2r_3^2 + 166r_1^2r_3 + 10r_1 + 80r_3 + 106r_1^2 - 204r_3^2 + 1156r_1r_3^3 - 80r_1^2r_3^3 \\
&\quad + 144r_1^3r_3 - 3780r_1^3r_3^2 - 1030r_1^4r_3^3 - 28r_1^4r_3^4 - 676r_1^5r_3^3 - 1455r_1^5r_3^2 - 472r_1^5r_3 + 224r_1^5r_3^4 - 282r_1^6r_3^2 - 62r_1^6r_3 \\
&\quad + 52r_1^6r_3^4 - 98r_1^6r_3^3 - 152r_1r_3^4 + 64r_1^2r_3^4 + 744r_1^3r_3^3 - 432r_1^3r_3^4 - 2400r_1^4r_3^2 - 202r_1^4r_3 - 16r_3^3 - 3r_1^3 - 262r_1^4 \\
&\quad + 70r_1^6 + 83r_1^5 + 272r_3^4) + (4r_1 + 1)(2r_1r_3 + 7r_3 - 2 + 2r_1)(2r_1^2r_3 + 2r_1^2 - 3r_1r_3 + 6r_1 + r_3 + 1)(r_1r_3 + 2r_3 \\
&\quad + 2 - 2r_1)(-r_3 + r_1r_3 - 1 - 2r_1)(2r_5r_6r_4 - 2r_5r_6 - 2r_5r_4 + 2r_5 - 4r_6r_4 - 2r_6 - 2r_4 - 1)
\end{aligned}$$

$$N_6 = (-1+2r_1^2-r_1+4r_3-4r_3^2+r_1r_3+2r_1r_3^2+4r_1^2r_3+2r_1^2r_3^2)+r_4r_6(r_1r_3+2r_3+2-2r_1)(-r_3+r_1r_3-1-2r_1)$$

$$\begin{aligned}
N_7 = {} & -r_1^2r_6r_4(-8+16r_5r_6r_4+20r_3^2r_5r_7r_1^2r_4-28r_2r_6r_1^2-46r_5r_3r_7r_6r_1r_4+10r_3^2r_5r_7r_6r_4-20r_3^2r_5r_7r_6r_1r_4 \\
& +68r_5r_3r_7r_6r_1^2r_4-40r_3^2r_5r_7r_1r_4-8r_3^2r_5r_6r_1r_4+10r_3^2r_2+92r_3r_7r_6r_1r_4+40r_3^2r_7r_6r_1r_4-40r_5r_3r_6r_1r_4 \\
& +10r_3^2r_5r_7r_6r_1^2r_4-20r_3^2r_2r_5r_6r_1r_4+16r_3r_4+70r_3^2r_2r_5r_7r_6r_4-28r_1^2r_3-2r_1^2r_3^2+4r_1r_3^2+20r_1r_3-68r_6r_4 \\
& -16r_5r_4-16r_5r_6+100r_3^2r_2r_7r_6r_1r_4-22r_5r_3r_7r_6r_4-92r_5r_3r_7r_1r_4+10r_5r_7r_6r_1r_4-22r_3r_2r_5r_6r_4 \\
& +20r_3^2r_5r_7r_6r_1+46r_5r_3r_7r_6r_1-56r_1+8r_3-16r_6-16r_4+4r_7+16r_5+4r_2-98r_1^2-2r_3^2+46r_6r_4r_7r_5r_2 \\
& +16r_5r_3r_6-22r_3r_7+40r_3r_6r_1+22r_3r_7r_6-46r_3r_7r_1-10r_7r_6r_1-112r_6r_1+16r_3r_6+10r_7r_1-4r_7r_6 \\
& +46r_3r_7r_6r_1-112r_1r_4-100r_3r_6r_1r_4+44r_3r_7r_6r_4-92r_3r_7r_1r_4-20r_7r_6r_1r_4+40r_5r_3r_6r_1+22r_5r_3r_7r_6 \\
& +92r_5r_3r_7r_1-10r_5r_7r_6r_1+112r_5r_6r_1r_4-16r_5r_3r_6r_4+40r_5r_1r_3r_4-44r_5r_3r_7r_4+20r_5r_7r_1r_4+4r_5r_7r_6r_4 \\
& -476r_6r_1r_4-40r_3r_6r_4+40r_1r_3r_4-44r_3r_7r_4+20r_7r_1r_4-8r_7r_6r_4+16r_5r_3r_4-40r_5r_1r_3+44r_5r_3r_7 \\
& -112r_5r_6r_1-20r_5r_7r_1-4r_5r_7r_6-112r_5r_1r_4+8r_5r_7r_4+8r_7r_4+112r_5r_1-16r_5r_3-8r_5r_7-68r_3r_7r_6r_1^2 \\
& +140r_3r_6r_1^2r_4+136r_3r_7r_1^2r_4+28r_7r_6r_1^2r_4-56r_5r_3r_6r_1^2-136r_5r_3r_7r_1^2+14r_5r_7r_6r_1^2+196r_5r_6r_1^2r_4-56r_5r_1^2r_3r_4 \\
& -28r_5r_7r_1^2r_4-196r_6r_1^2-14r_7r_1^2-196r_1^2r_4+196r_5r_1^2-56r_3r_6r_1^2+68r_3r_7r_1^2+14r_7r_6r_1^2-833r_6r_1^2r_4-56r_1^2r_3r_4 \\
& -28r_7r_1^2r_4+56r_5r_1^2r_3-196r_5r_6r_1^2+28r_5r_7r_1^2-196r_5r_1^2r_4-10r_3^2r_2r_4+10r_3^2r_2r_1^2-20r_3^2r_2r_1+68r_3r_2r_1^2 \\
& -50r_3^2r_2r_7+20r_3^2r_2r_6-136r_3r_7r_6r_1^2r_4+56r_5r_3r_6r_1^2r_4+136r_5r_3r_7r_1^2r_4-14r_5r_7r_6r_1^2r_4-68r_5r_3r_7r_6r_1^2 \\
& +10r_2r_1+8r_2r_6-4r_2r_4-2r_2r_7-8r_2r_5-14r_2r_1^2-22r_3r_2+44r_3r_2r_6r_4+22r_3r_2r_5r_4-44r_3r_2r_5r_6 \\
& +20r_3^2r_2r_5r_6-40r_3^2r_2r_6r_1+50r_3^2r_2r_7r_6+100r_3^2r_2r_7r_1-92r_3r_2r_6r_1-40r_3r_2r_7r_1-20r_3r_2r_7r_6+46r_3r_2r_1r_4 \\
& -20r_3^2r_2r_6r_4+20r_3^2r_2r_1r_4+50r_3^2r_2r_7r_4-10r_3^2r_2r_5r_4+40r_3^2r_2r_5r_1+100r_3^2r_2r_5r_7-20r_3r_2r_7r_4+92r_3r_2r_5r_1 \\
& -40r_3r_2r_5r_7+136r_3r_2r_6r_1^2+20r_3r_2r_7r_1^2-68r_3r_2r_1^2r_4-136r_3r_2r_5r_1^2+20r_3^2r_2r_6r_1^2-50r_3^2r_2r_7r_1^2-10r_3^2r_2r_1^2r_4 \\
& -20r_3^2r_2r_5r_1^2+4r_2r_5r_6r_4-4r_2r_7r_6r_1-20r_2r_6r_1r_4-140r_3^2r_2r_5r_7r_6r_1r_4+70r_3^2r_2r_5r_7r_6r_1^2r_4-100r_3^2r_2r_5r_7r_1r_4 \\
& -160r_3r_2r_5r_7r_6r_1r_4-100r_3^2r_2r_5r_7r_6r_1+40r_3r_2r_7r_6r_1-100r_3^2r_2r_7r_6r_1+40r_3^2r_2r_6r_1r_4-50r_3^2r_2r_7r_6r_4 \\
& -100r_3^2r_2r_7r_1r_4-40r_3r_2r_7r_6r_1r_4-40r_3^2r_2r_5r_6r_1+50r_3^2r_2r_5r_7r_6-200r_3^2r_2r_5r_7r_1+40r_3r_2r_5r_7r_6r_1 \\
& -46r_3r_2r_5r_6r_1r_4+10r_3^2r_2r_5r_6r_4+20r_3^2r_2r_5r_1r_4+50r_3^2r_2r_5r_7r_4+40r_3r_2r_5r_7r_1r_4+80r_3r_2r_5r_7r_6r_4 \\
& +92r_3r_2r_6r_1r_4+40r_3r_2r_7r_1r_4+20r_3r_2r_7r_6r_4-20r_3^2r_2r_5-46r_3r_2r_1-44r_3r_2r_6+22r_3r_2r_4+20r_3r_2r_7 \\
& +44r_3r_2r_5-8r_2r_6r_4-4r_2r_5r_4+8r_2r_5r_6+20r_2r_6r_1+4r_2r_7r_1+2r_2r_7r_6-10r_2r_1r_4+2r_2r_7r_4 \\
& -20r_2r_5r_1+4r_2r_5r_7-2r_2r_7r_1^2+14r_2r_1^2r_4+28r_2r_5r_1^2-92r_3r_2r_5r_6r_1+80r_3r_2r_5r_7r_1-20r_3r_2r_5r_7r_6 \\
& +46r_3r_2r_5r_1r_4-20r_3r_2r_5r_7r_4+50r_3^2r_2r_7r_6r_1^2-20r_3^2r_2r_6r_1^2r_4+50r_3^2r_2r_7r_1^2r_4+20r_3r_2r_7r_6r_1^2r_4+20r_3^2r_2r_5r_6r_1^2 \\
& +100r_3^2r_2r_5r_7r_1^2-20r_3r_2r_5r_7r_6r_1^2+68r_3r_2r_5r_6r_1^2r_4-10r_3^2r_2r_5r_1^2r_4-20r_3r_2r_5r_7r_1^2r_4-20r_3r_2r_7r_6r_1^2 \\
& -136r_3r_2r_6r_1^2r_4-20r_3r_2r_7r_1^2r_4+136r_3r_2r_5r_6r_1^2-40r_3r_2r_5r_7r_1^2-68r_3r_2r_5r_1^2r_4-50r_3^2r_2r_7r_6r_1^2r_4 \\
& +10r_3^2r_2r_5r_6r_1^2r_4+50r_3^2r_2r_5r_7r_1^2r_4+80r_3r_2r_5r_7r_6r_1^2r_4+50r_3^2r_2r_5r_7r_6r_1^2-4r_3^2r_4+10r_3^2r_7-4r_3^2r_6+4r_3^2r_5 \\
& -92r_2r_5r_7r_6r_1r_4+4r_2r_7r_6r_1r_4-4r_2r_5r_7r_6r_1+10r_2r_5r_6r_1r_4-4r_2r_5r_7r_1r_4-4r_2r_7r_1r_4-2r_2r_7r_6r_4 \\
& +20r_2r_5r_6r_1-8r_2r_5r_7r_1+2r_2r_5r_7r_6-10r_2r_5r_1r_4+2r_2r_5r_7r_4+2r_2r_7r_6r_1^2+28r_2r_6r_1^2r_4+2r_2r_7r_1^2r_4 \\
& -28r_2r_5r_6r_1^2+4r_2r_5r_7r_1^2+14r_2r_5r_1^2r_4-2r_2r_7r_6r_1^2r_4+2r_2r_5r_7r_6r_1^2-14r_2r_5r_6r_1^2r_4+2r_2r_5r_7r_1^2r_4 \\
& +46r_2r_5r_7r_6r_1^2r_4+20r_3^2r_7r_6r_1+88r_3^2r_6r_1r_4-20r_3^2r_7r_6r_4-40r_3^2r_7r_1r_4+8r_3^2r_5r_6r_1-10r_3^2r_5r_7r_6+40r_3^2r_5r_7r_1 \\
& +4r_3^2r_5r_6r_4+8r_3^2r_5r_1r_4+20r_3^2r_5r_7r_4-10r_3^2r_7r_6r_1^2-44r_3^2r_6r_1^2r_4+20r_3^2r_7r_1^2r_4-4r_3^2r_5r_6r_1^2-20r_3^2r_5r_7r_1^2 \\
& -4r_3^2r_5r_1^2r_4-4r_3^2r_5r_6+8r_3^2r_6r_1-10r_3^2r_7r_6-20r_3^2r_7r_1-44r_3^2r_6r_4+8r_3^2r_1r_4+20r_3^2r_7r_4-4r_3^2r_5r_4-8r_3^2r_5r_1 \\
& -20r_3^2r_5r_7-4r_3^2r_6r_1^2+10r_3^2r_7r_1^2-4r_3^2r_1^2r_4+4r_3^2r_5r_1^2-20r_3^2r_7r_6r_1^2r_4+4r_3^2r_5r_6r_1^2r_4-10r_3^2r_5r_7r_6r_1^2)- \\
& (-1+2r_5r_6r_4-8r_2r_6r_1^2-4r_6r_4-2r_5r_4-2r_5r_6+2r_5r_7r_6r_1r_4-4r_1-2r_6-2r_4+2r_7+2r_5+2r_2-4r_1^2 \\
& +2r_6r_4r_7r_5r_2-2r_7r_6r_1-8r_6r_1+2r_7r_1-2r_7r_6-8r_1r_4-4r_7r_6r_1r_4-2r_5r_7r_6r_1+8r_5r_6r_1r_4+4r_5r_7r_1r_4 \\
& +2r_5r_7r_6r_4-16r_6r_1r_4+4r_7r_1r_4-4r_7r_6r_4-8r_5r_6r_1-4r_5r_7r_1-2r_5r_7r_6-8r_5r_1r_4+4r_5r_7r_4+4r_7r_4 \\
& +8r_5r_1-4r_5r_7+8r_7r_6r_1^2r_4+4r_5r_7r_6r_1^2+8r_5r_6r_1^2r_4-8r_5r_7r_1^2r_4-8r_6r_1^2-4r_7r_1^2-8r_1^2r_4+8r_5r_1^2+4r_7r_6r_1^2 \\
& -16r_6r_1^2r_4-8r_7r_1^2r_4-8r_5r_6r_1^2+8r_5r_7r_1^2-8r_5r_1^2r_4-4r_5r_7r_6r_1^2r_4+2r_2r_1+4r_2r_6-2r_2r_4-4r_2r_7-4r_2r_5 \\
& -4r_2r_1^2+2r_2r_5r_6r_4-8r_2r_7r_6r_1-4r_2r_6r_1r_4-4r_2r_6r_4-2r_2r_5r_4+4r_2r_5r_6+4r_2r_6r_1+8r_2r_7r_1+4r_2r_7r_6
\end{aligned}$$

$$
\begin{aligned}
&-2r_2r_1r_4+4r_2r_7r_4-4r_2r_5r_1+8r_2r_5r_7-4r_2r_7r_1^2+4r_2r_1^2r_4+8r_2r_5r_1^2-4r_2r_5r_7r_6r_1r_4+8r_2r_7r_6r_1r_4\\
&-8r_2r_5r_7r_6r_1+2r_2r_5r_6r_1r_4-8r_2r_5r_7r_1r_4-8r_2r_7r_1r_4-4r_2r_7r_6r_4+4r_2r_5r_6r_1-16r_2r_5r_7r_1+4r_2r_5r_7r_6\\
&-2r_2r_5r_1r_4+4r_2r_5r_7r_4+4r_2r_7r_6r_1^2+8r_2r_6r_1^2r_4+4r_2r_7r_1^2r_4-8r_2r_5r_6r_1^2+8r_2r_5r_7r_1^2+4r_2r_5r_1^2r_4-4r_2r_7r_6r_1^2r_4\\
&+4r_2r_5r_7r_6r_1^2-4r_2r_5r_6r_1^2r_4+4r_2r_5r_7r_1^2r_4+2r_2r_5r_7r_6r_1^2r_4)(1+8r_1^2r_3+4r_1^2r_3^2-8r_1r_3^2-4r_1r_3+2r_6r_4+4r_1\\
&-4r_3+4r_1^2+4r_3^2+4r_3r_6r_1r_4+8r_6r_1r_4+4r_3r_6r_4-8r_3r_6r_1^2r_4+8r_6r_1^2r_4-4r_3^2r_6r_1r_4+2r_3^2r_6r_1^2r_4+2r_3^2r_6r_4),
\end{aligned}
$$

$$
\begin{aligned}
D_1 &= (r_1r_3-r_3-2r_1-1)(r_1r_3+2r_3-2r_1+2)(2r_1r_3+7r_3+2r_1-2),\\
D_2 &= (4r_1+1)(2r_1r_3+7r_3+2r_1-2)(2r_1^2r_3+2r_1^2-3r_1r_3+r_3+6r_1+1)(r_1r_3+2r_3-2r_1+2)(r_1r_3-r_3-2r_1-1),\\
D_3 &= (4r_1+1)(2r_1r_3+7r_3+2r_1-2)(2r_1^2r_3+2r_1^2-3r_1r_3+r_3+6r_1+1)(r_1r_3+2r_3-2r_1+2)(r_1r_3-r_3-2r_1-1),\\
D_4 &= (4r_1+1)(2r_1r_3+7r_3+2r_1-2)(2r_1^2r_3+2r_1^2-3r_1r_3+r_3+6r_1+1)(r_1r_3+2r_3-2r_1+2)(r_1r_3-r_3-2r_1-1),\\
D_5 &= (4r_1+1)(2r_1r_3+7r_3+2r_1-2)(2r_1^2r_3+2r_1^2-3r_1r_3+r_3+6r_1+1)(r_1r_3+2r_3-2r_1+2)(r_1r_3-r_3-2r_1-1),\\
D_6 &= (r_1r_3+2r_3-2r_1+2)(r_1r_3-r_3-2r_1-1),\\
D_7 &= (r_1-1)^4(r_6-1)^2(r_4-1)^2.
\end{aligned}
$$

Appendix B. Gröbner Basis Obtained in the Second Stage

The following is the Gröbner basis V obtained in the second stage.

$$
\begin{aligned}
&\langle 16r_1^{12}-12r_1^{11}-315r_1^{10}-270r_1^9+963r_1^8+1740r_1^7+1831r_1^6+1740r_1^5+963r_1^4-270r_1^3-315r_1^2-12r_1+16,\\
&19688997290379300r_2^2+(13342220859532912r_1^{11}-9025798437480212r_1^{10}-263412163625611277r_1^9\\
&-24423869690590749 02r_1^8+787347579309412429r_1^7+150263842510448 2204r_1^6+162045949076064 2441r_1^5\\
&+158041569067239 9176r_1^4+92924403786323 2397r_1^3-12271634517383 8558r_1^2-21850813167598 6453r_1\\
&-7449591529544452)r_2+4184386317878320r_1^{11}+7219809598397980r_1^{10}-9172343102209 4945r_1^9\\
&-27255882223528 0070r_1^8+108321338134086865r_1^7+108717613442628 1540r_1^6+148702796715272 8085r_1^5\\
&+151842261622422 7760r_1^4+129516815427181 3145r_1^3+480888700491118 370r_1^2-268680005533325905r_1\\
&-127689352357977520,\\
&1131975r_3-3697024r_1^{11}+4419904r_1^{10}+70949504r_1^9+30728974r_1^8-238941943r_1^7-298598858r_1^6\\
&-282189047r_1^5-260427802r_1^4-87152204r_1^3+121556561r_1^2+33278731r_1-10519741,\\
&55465469280r_6+(24556192240r_1^{11}-121558064500r_1^{10}-404020369445r_1^9+1597919868110r_1^8\\
&+3190314059245r_1^7-3245079126700r_1^6-8000005406935r_1^5-9880935800300r_1^4-11272721707795r_1^3\\
&-8372694166130r_1^2-673290192565r_1+672404027500)r_2+88323416944r_1^{11}-194130043924r_1^{10}\\
&-1632898358669r_1^9+1000496774726r_1^8+7294051389253r_1^7+2106675007628r_1^6-2919497971183r_1^5\\
&-5019841976468r_1^4-9317109549931r_1^3-10291179288266r_1^2-1265131770061r_1+853220161876,\\
&-55465469280r_4+(24556192240r_1^{11}-121558064500r_1^{10}-404020369445r_1^9+1597919868110r_1^8\\
&+3190314059245r_1^7-3245079126700r_1^6-8000005406935r_1^5-9880935800300r_1^4-11272721707795r_1^3\\
&-8372694166130r_1^2-673290192565r_1+672404027500)r_2+32218984864r_1^{11}-23724321784r_1^{10}\\
&-631776626414r_1^9-554533353544r_1^8+187565747219 8r_1^7+348265311870 8r_1^6+390048465138 2r_1^5\\
&+385814865245 2r_1^4+234170576113 4r_1^3-184709675696r_1^2-449339959366r_1-70729884884,\\
&1223262755325r_5+6137450188864r_1^{11}-6991418111824r_1^{10}-118092874249844r_1^9-57613170322234r_1^8\\
&+391421961044758r_1^7+514627779872963r_1^6+503533812975257r_1^5+474101125684372r_1^4
\end{aligned}
$$

$$+186511604998229r_1^3 - 173987677844891r_1^2 - 51545756230966r_1 + 15367299773596,$$
$$19688997290379300r_7 + 19688997290379300r_2 + 13342220859532912r_1^{11} - 9025798437480212r_1^{10}$$
$$-263412163625611277r_1^9 - 244238969059074902r_1^8 + 787347579309412429r_1^7 + 150263842510448220 4r_1^6$$
$$+162045949076064244 1r_1^5 + 158041569067239917 6r_1^4 + 92924403786323239 7r_1^3 - 122716345173838558r_1^2$$
$$-218508131675986453r_1 - 7449591529544452\rangle$$

Appendix C. Values of the Time Parameters

The following table shows values (to 50 decimal places) of time parameters of the 19-gate sequence that makes a gate locally equivalent to the exact CNOT.

$$t_1 = 0.41089887975718144636523336288597624194632833958785\ldots$$
$$t_2 = 0.20710666649395355654611419604502076932557162116304\ldots$$
$$\bar{t}_2 = 0.61576323853243438299853635074802330810574399122390\ldots$$
$$t_3 = 0.27752594692148754979835485968172499669087169408382\ldots$$
$$\bar{t}_3 = 0.67082929327922853371730044242213587584965409778897\ldots$$
$$t_4 = 0.64050195194064278992122222135915364572272517521372\ldots$$
$$t_5 = 0.41471614361026407845944669412078743421039387278530\ldots$$
$$\bar{t}_5 = 0.84017093370645648134274736683463875195351138258104\ldots$$
$$t_6 = 0.14765528017545878894148896649867378972197173397274\ldots$$
$$t_7 = 0.81310821111630563803711838610580990574895573944832\ldots$$
$$\bar{t}_7 = 0.39776246248510275550567762561269578427232753957876\ldots$$

ACKNOWLEDGEMENT

We thank Go Kato, Yasuhiro Takahashi, Seiichiro Tani, and Rodney Van Meter for their helpful comments.

REFERENCES

1. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
2. D. Bacon, J. Kempe, D. P. DiVincenzo, D. A. Lidar, and K. B. Whaley, *Phys. Rev. Lett.* **85**, 1758 (2000).
3. J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, *Phys. Rev. A* **63**, 042307 (2001).
4. J. Kempe, D. Bacon, D. P. DiVincenzo, and K. B. Whaley, *Quant. Inf. Comput.* **1**, 241 (2001).

5. J. Kempe and K.B. Whaley, *Phys. Rev. A* **65**, 052330 (2002).
6. D. Bacon, Ph.D thesis, UC Berkeley (2003).
7. D. A. Lidar and K. B. Whaley, *Irreversible Quantum Dynamics*, F. Benatti, R. Floreanini (eds.) (Springer Lecture Notes in Physics vol. 622, Berlin, 2003), p.83.
8. D. P. DiVincenzo, D. Bacon, J. Kempe, S. Burkard, and K. B. Whaley, *Nature* **408**, 339 (2000).
9. M. Hsieh, J. Kempe, S. Myrgren, and K. B. Whaley, *Quant. Inf. Proc.* **2**, 289 (2003).
10. E. S. Myrgren and K. B. Whaley, *Quant. Inf. Proc.* **2**, 309 (2003).
11. D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, (Springer-Verlag, New York, 1992).
12. D. Cox, J. Little and D. O'Shea, *Using Algebraic Geometry*, (Springer-Verlag, New York, 1998).
13. http://www.maplesoft.com/
14. http://www.math.kobe-u.ac.jp/Asir/
15. T. Becker and V. Weispfenning, *Gröbner Bases*, (Springer-Verlag, New York, 1993).
16. Y. Makhlin, *Quant. inf. Proc.* **1**, 243 (2002).