2023 S.T. Yau High School Science Award

Research Report

The Team

Name of team member: Changxiu Ji

School: Shenzhen Middle School

Province: Guangdong

Country: China

Name of supervising teacher: Tingjing Chen

Job Title: Math Teacher

School: Shenzhen Middle School

Province: Guangdong

Country: China

Title of Research Report

Optimal Representation of (123) from the Symmetric Group S_3 in terms of Quantum Circuits

Date

24 Oct 2023

Optimal Representation of (123) from the Symmetric Group S_3 in terms of Quantum Circuits

Changxiu Ji[1]

[1]*Shenzhen Middle School, Shenzhen, 518024, China*

(Dated: October 24, 2023)

The symmetric group is one of the fundamental groups in abstract algebra, and has found extensive applications in the community of both mathematics and physics in the past years. Besides, quantum circuits are becoming more and more important in quantum communication. Quantum entanglement based methods such as Controlled-NOT gate (CNOT gate) and local unitary gates have been introduced into quantum communication. These methods have shown great importance in this field. Quantum cost is important to quantum communication. It is directly associated with the number of non-local unitary gates a quantum circuit uses. Therefore, it is important to use the least number of non-local unitary gates in quantum circuits representations for quantum cost minimization. It has been proved that the least number of CNOT gates needed to represent the element (12) in the symmetric group S_2 is three. However, there have been few theories discussing the least number of non-local unitary gates that a quantum circuit uses in order to realize certain elements in the symmetric group in existing studies. In this paper, we study the least number of CNOT gates needed for quantum circuits representation of the element (123), which is an element in the symmetric group S_3 in order to reduce quantum costs. For this purpose, we prove that the Schmidt rank of the matrix representing the element (123) of the symmetric group is 7 by using the known Strassen tensor. Secondly, this Schmidt Rank is used to prove that 2 CNOT gates are impossible to achieve the quantum circuit representation of the element (123). Thirdly, we respectively prove that it is impossible to achieve the element (123) using 3 or 4 CNOT gates by enumerating all the non-equivalent circuits according to the switch of systems and exclude them. The states of these non-equivalent circuits after passing each CNOT gate are analyzed. Then the outputs of the circuit systems are calculated to exclude these non-equivalent circuits. At last, we provide a construction of using 6 CNOT gates for quantum circuits representation of element (123). Besides, theorems have been proposed to list the non-equivalent circuits, to distinguish the states before CNOT gates and to calculate outputs if the states before and after the CNOT gates are known. It is an open question of whether 5 CNOT gates is able to achieve the circuit representing the element (123). Moreover, the theorems we developed can be used to find the optimal circuit representing other elements in the symmetric group such as (1234) and (12345).

Keywords: symmetric group, CNOT gate, quantum circuit, Schmidt rank, non-equivalent circuits

Contents

I. INTRODUCTION

Quantum circuit representation based on elements of the symmetric groups is an important research topic in quantum communication. It is the key to the minimization of quantum costs. Therefore, we study the optimal quantum circuit representation based on group theory. Group theory has been increasingly important not only on the fields of modern mathematics, but also in theoretical physics, chemistry , electrical engineering, quantum physics as well as electronic computing [1]. One of the first contributions of group theory was made by Euler (1707-83) in *Novi Commentarii Academiae Petropolitanae*. Lagrange (1763-1813) wrote his work of group theory in *Reflexions Sur la Resolution Algebrique des Equations*, which had tremendous influence [2]. The concept of permutation group and symmetric group had also been proposed [3]. The symmetric group has been increasingly important on fields of geometry [4] as well as reversible logic synthesis. Due to the extensive use of the symmetric group in its theoretical aspect, it is natural to expect that the symmetric group may find application and representation in practice.

Besides, an important application of quantum mechanics nowadays is quantum communication and computing [5]. In 1992, Bennett et al presented the super dense coding protocol for transmitting classical information by using quantum entanglement, Controlled-NOT (CNOT) gates and local unitary gates like the Hadamard and X gates in a quantum circuit [6]. One year later, quantum teleportation for the transmission of an unknown state was also constructed using a similar quantum circuit [7]. Recently, teleportation of photonic qubits over long distances of up to 1400 kilometers through an up link channel has been reported [8]. Hence, the CNOT gate plays a key role in quantum communication protocols [9].

Nowadays, quantum communication is often based on the construction of quantum circuits [10]. A quantum circuit consists of coherent quantum operations, such as qubits [11]. It can be described as a series of quantum gates, measurements and resets arranged in sequence. All quantum programs can be represented by a series of quantum circuits and non-concurrent classical computation [12].

The quantum cost of an arbitrary gate was first proposed by Barenco et al [13]. Generally, the quantum cost of a quantum circuit is the sum of the cost of all the non-unitary gates used in designing the circuit. The execution of the circuit gets more complicated as the quantum costs go higher. It is then of great importance to find a procedure that is able to compute the optimal quantum circuit. Therefore, the synthesis of any two-qubit entangled state is a recent experimental goal [14]. Although how to synthesize any such state is known [15], it is possible that the

resulting quantum circuits is not optimal, which means that the circuit uses an excessive number of CNOT gates, if the computation is done injudiciously [16]. It is then a common goal to find the optimal number of CNOT gates to achieve certain information.

It has been proved that three CNOT gates are sufficient in realizing the SWAP operation [17]. It has also been proved that the required number of CNOT and local gates of dense coding and teleportation schemes increases with dimensions [18]. Mathematically, the SWAP gate is the representation of the element (12) in the symmetric group S_2. In order to reduce quantum cost, the number of CNOT gates and local gates in the representation of other elements in the symmetric group such as (123) and (1234) should be as small as possible.

In this paper, we study the least number of CNOT gates required to achieve the quantum circuit representing the element (123). We prove that two, three and four CNOT gates assisted by local unitary gates cannot represent the element (123) of the symmetric group S_3, which we regard as the indecomposability with two, three and four CNOT gates. Firstly, we prove that the Schmidt rank of the representation matrix of the element (123) is seven by using the Strassen tensor [19] in section IV. Secondly, we use this result to prove that two CNOT gates is impossible in achieving the objective quantum circuit in section V A. Thirdly, we use an exclusive method by respectively enumerating the non-equivalent circuits using three CNOT gates and four CNOT gates assisted by a number of local unitary gates using Theorems 7, 8, and 9, mainly involving the switch of systems and then exclude these circuits respectively. The states of systems after passing each CNOT gate are analyzed using Theorem 11 for each non-equivalent circuit. Using these states, the output of certain systems in the quantum circuit are calculated according to Theorems 12 and 13. We exclude each of these non-equivalent circuits using the fact that for the circuit to achieve the element (123), the output of the circuit must be $|j,k,i\rangle$ when the input of the circuit is $|i,j,k\rangle$. Using this method, we obtain that three and four CNOT gates are impossible in achieving the objective circuit in section V B and section V C, respectively. This means that, by our research, one can conclude that the universal set of quantum gates for the realization of the element (123) contains at least five CNOT gates and enough local unitary gates. Additionally, we give the construction of the element (123) using six CNOT gates in section VI. We finally conclude in section VII.

II. CONTRIBUTIONS

1. This paper computes the Schmidt rank of the matrix of the quantum circuit representing the element (123) from the symmetric group S_3 using the Strassen tensor, which gives researchers an idea of how to calculate the Schmidt rank of other matrices representing other elements in the symmetric group.
2. This paper proposes a method of enumerating all the non-equivalent circuits using a given number of CNOT gates, which reduces a large amount of calculations one needs to make when finding the optimal circuit for certain elements in the symmetric group. This method applies the switch of system as well as the inverses of certain circuits.
3. This paper proposes a theorem that helps determine the state of the circuit if the input and the output state of the circuit is known, and several theorems calculating the output of systems if certain states are satisfied before and after a CNOT gate, which is an efficient method in excluding the non-equivalent circuit.
4. This paper proposes a way of analyzing the GHZ orbit state in the genuinely entangled state circumstance and successfully excludes some of the circuits that is difficult to calculate the corresponding outputs.
5. This paper provides a quantum circuit construction of the element (123) using 6 CNOT gates, although it is not guaranteed as the optimal circuit, it provides a relatively efficient circuit in terms of the minimization of quantum cost.

III. PRELIMINARIES

In this section, we introduce the preliminary knowledge and facts used in this paper. In Sec. III A, we review the permutation group and the symmetric group from abstract algebra. In Sec. III B, the Kronecker product of matrices and its properties is reviewed. In the remaining subsections, we introduce the facts from quantum information. In Sec. III C and III D, the single and multiqubit gates used in quantum circuits are introduced respectively. In Sec. III E, we introduce how Kronecker product is applied in quantum circuits. Finally, we introduce and study the Schmidt rank in Sec. III F.

A. Permutation Group and Symmetric Group

In this subsection, we review the permutation group and the symmetric group. Given a finite set A, a permutation of A is a function f: $A \to A$, which is one to one correspondence. We recall some properties of groups.

1. **Closure**

   If A, B are in a group G, then AB is also in this group G.

2. **Associativity**

   $(AB)C = A(BC)$, where A, B, C are all components in a group G.

3. **Identity**

   For a group G, there exists an identity element I such that for any element A in group G, $AI = IA = A$.

4. **Inverse**

   There should be an inverse of each component, so, for every component A under G, the set incorporates a component $B = A'$ such that $AA' = A'A = I$.

Next we introduce the permutation and symmetric groups.

Definition 1 *The **Permutation Group** of a finite set A is a set of permutations of A that forms a group under function composition. The **Symmetric Group** S_n is the group of all permutations of the set $\{1, 2, ...n\}$.* □

A special notation: For set $A = \{1, 2, 3\}$, a permutation α may have $\alpha(1) = 3$, $\alpha(2) = 1$, $\alpha(3) = 2$. We note this permutation α as $\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$. This notation is still not brief enough, so we introduce a form of **Cycle Notation**. We notice that in a certain permutation, there are always several kinds of cycle involving $i_1, i_2...i_n$ such that $\alpha(i_1) = i_2, \alpha(i_2) = i_3, ..\alpha(i_{n-1}) = i_n, \alpha(i_n) = i_1$. This kind of cycle is noted as $(i_1 i_2 ... i_n)$. For example, $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} = (132)$. Using this notation, we provide all of the elements in S_3.

$$S_3 = \{(1), (12), (13), (23), (123), (132)\} \tag{1}$$

B. Kronecker Product

The **Kronecker Product** is an operation on to two matrices A and B. The symbol for Kronecker product is $\bigotimes$. Assume that:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \tag{2}$$

Then this operation of Kronecker product is defined as

$$f(A,B) = A \otimes B = \begin{bmatrix} a_{11} \cdot B & a_{12} \cdot B & \cdots & a_{1n} \cdot B \\ a_{21} \cdot B & a_{22} \cdot B & \cdots & a_{2n} \cdot B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} \cdot B & a_{m2} \cdot B & \cdots & a_{mn} \cdot B \end{bmatrix}, \tag{3}$$

where $a_{ij} \cdot B$ is a partitioned matrix. Here are some properties of the Kronecker product:

1. Associativity

$$A \otimes (B \otimes C) = (A \otimes B) \otimes C. \tag{4}$$

2. Distributivity

$$\begin{aligned} A \otimes (B + C) &= (A \otimes B) + (A \otimes C). \\ (A + B) \otimes C &= (A \otimes C) + (B \otimes C). \end{aligned} \tag{5}$$

3. For scalar a, $a \otimes A = A \otimes a = a \cdot A$.

4. For scalars a and b, $a \cdot A \otimes b \cdot B = ab \cdot A \otimes B$.

5. For conforming matrices,$(A \otimes B)(C \otimes D) = AC \otimes BD$.

C. Single-qubit gate

A single qubit is a unit 2-dimensional vector and a single qubit gate is a 2×2 unitary matrix that acts on only one system of the quantum circuit. Here we introduce two common single qubit gate, the X gate and the H gate. The X gate can be represented by the following matrix

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{6}$$

The Hadamard Gate(H-Gate) is a fundamental quantum gate. H-Gate can be represented by the matrix

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{7}$$

Note that a single qubit gate K, satisfies the equation: $K \cdot K^{\dagger} = I$, where I is the identity matrix. Furthermore, we provide the general form of a single-qubit gate, in other words, a local unitary matrix A.

$$A = e^{ia} \begin{bmatrix} \cos b & e^{ic} \sin b \\ e^{id} \sin b & -e^{ic+id} \cos b \end{bmatrix} \tag{8}$$

The two column vectors of a local unitary matrix are orthogonal and $|det(A)| = 1$.

D. The family of CNOT gates

In this subsection, we introduce a family of two-qubit gates, namely the Controlled-Not (CNOT) gates. In classical computer science, the CNOT gate regards the first bit q_0 as the control bit, meaning that this bit does not change. $q_0 = q_0'$. q_1 is the target digit. If $q_0 = 0$, then the CNOT gate will not change q_1. $q_1 = q_1'$. If $q_0 = 1$, then CNOT gate will change q_1 into $1 + q_1$. In short, CNOT gate will change q_1 into $q_0 \bigoplus q_1$. In the following, we will extend the classical CNOT gate to the quantum scenario.

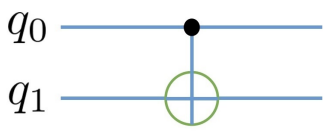

FIG. 1: CNOT gate in quantum circuits

Above is the graph of CNOT gate in quantum circuits. The black dot on the q_0 indicates the controlling system. Here is the matrix for CNOT gate for the CNOT gate in FIG. 1.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{9}$$

Note that $CNOT^2 = I$, where I is the identity matrix. This means that $CNOT^{-1} = CNOT$. Besides, CNOT gate cannot be expressed as the Kronecker Product of two single-qubit gates.

E. Application of Kronecker Product on quantum circuits

We now discuss the application of the Kronecker Product introduced in III B on quantum circuits. In the circuit below in FIG. 2, one can represent the simultaneous operation H, X by using the Kronecker Product.

$$X|q_0\rangle \otimes H|q_1\rangle = (X \otimes H)|q_0 q_1\rangle, \tag{10}$$

where gate X and H are gates mentioned in the Single-qubit section in equation 6 and 7.

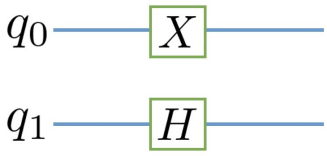

FIG. 2: X gate acting on q_0 and H gate acting on q_1

We represent this in matrix form.

$$X \otimes H = \begin{bmatrix} 0 & H \\ H & 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{bmatrix}. \tag{11}$$

More specifically, when there is no operating single-qubit gate acting on q_1 or q_0, we will use I_n to make the **Kronecker Product**. Assume that

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{12}$$

We regard

$$\langle 0| = (|0\rangle)^T = \begin{bmatrix} 1 & 0 \end{bmatrix}, \langle 1| = (|0\rangle)^T = \begin{bmatrix} 1 & 0 \end{bmatrix}. \tag{13}$$

CNOT gate can be written in the following way using equation 12 and 13.

$$CNOT = |0\rangle \cdot \langle 0| \otimes I_2 + |1\rangle \cdot \langle 1| \otimes X, \tag{14}$$

where X is the Pauli-X gate introduced in the single-qubit gate section in equation 6. Then we depict a CNOT gate that acts on system A and C using the Kronecker product in the following equation

$$CNOT_{AC} \otimes I_B = |0\rangle \cdot \langle 0| \otimes I_2 \otimes I_2 + |1\rangle \cdot \langle 1| \otimes I_2 \otimes X. \tag{15}$$

We are able to change the controlling system of a CNOT gate by adding local unitary gates on both sides of a CNOT gate. We regard $CNOT_{AB}$ as a CNOT

gate with controlling system on system A, the CNOT gate shown in FIG. 1 is an example of $CNOT_{AB}$. One can prove that

$$CNOT_{BA} = (H \otimes H)(CNOT_{AB})(H \otimes H), \tag{16}$$

where H represents the Hadamard gate mentioned in the single-qubit gate section in equation 7.

As an application of multiple CNOT gates, we present the swap gate. The effect of swap gate is to swap the position of the input ab to ba. It is already proven that the smallest number of CNOT gates that is needed to represent the swap gate is three [17]. In FIG. 3, the swap gate represented by three CNOT gates.

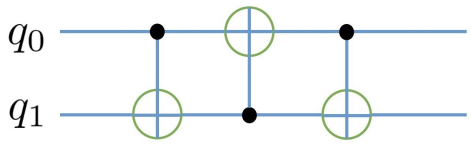

FIG. 3: Representation of Swap Gate using three CNOT Gates

F. Schmidt Rank

Next, we will introduce the Schmidt Rank of matrices.

Definition 2 *The **Schmidt Rank** of a n-partite matrix U on the n-partite Hilbert space* $\mathcal{H}_1 \bigotimes \mathcal{H}_2 \bigotimes ... \bigotimes \mathcal{H}_n = \mathcal{C}^{d_1} \bigotimes \mathcal{C}^{d_2} \bigotimes ... \bigotimes \mathcal{C}^{d_n}$ *is the minimum integer r such that* $U = \sum_{j=1}^{r} A_{j,1} \bigotimes ... \bigotimes A_{j,n-1} \bigotimes A_{j,n}$ *for some* $d_i \times d_i$ *matrix* $A_{j,i}$ *and* $i = 1, 2, ..., n$. □

Lemma 3 *There exists a matrix F such that*

$$\begin{aligned} tr(F^\dagger A_1) = ... = tr(F^\dagger A_{k-1}) = 0. \\ tr(F^\dagger A_k) \neq 0, \end{aligned} \tag{17}$$

where $A_1, A_2, ...A_k$ *are linear independent and are* $a \times n$ *matrices, where* $F^\dagger$ *means the transpose plus the complex conjugate of matrix F.*

Proof. Suppose $A_i = \left[\, |a_{1i}\rangle \;\; |a_{2i}\rangle \;\; ..... \;\; |a_{ni}\rangle \,\right]$, where all of the $|a_{ji}\rangle$ are column vectors. Next, we assume that

$$F^\dagger = \begin{bmatrix} \langle b_1| \\ \langle b_2| \\ . \\ . \\ . \\ \langle b_n| \end{bmatrix} \tag{18}$$

where $\langle b_i|$ are row vectors. Then we have

$$tr(F^\dagger \cdot A_i) = \sum_{j=1}^{n} \langle b_j|a_{ji}\rangle = \left[\ \langle b_1|\ \langle b_2|\ .....\ \langle b_n|\ \right] \cdot \begin{bmatrix} |a_{1i}\rangle \\ |a_{2i}\rangle \\ . \\ . \\ . \\ |a_{ni}\rangle \end{bmatrix}. \tag{19}$$

Since $A_1, A_2...A_n$ are linearly independent. Then the column vectors $\begin{bmatrix} |a_{1i}\rangle \\ |a_{2i}\rangle \\ . \\ . \\ . \\ |a_{ni}\rangle \end{bmatrix}$ where $1 \leq i \leq n$ are all linear independent. Therefore, there must exist a vector $\left[\ \langle b_1|\ \langle b_2|\ .....\ \langle b_n|\ \right]$ such that

$$\left[\ \langle b_1|\ \langle b_2|\ .....\ \langle b_n|\ \right] \cdot \begin{bmatrix} |a_{1i}\rangle \\ |a_{2i}\rangle \\ . \\ . \\ . \\ |a_{ni}\rangle \end{bmatrix} = \begin{cases} 0 & 1 \leq i \leq n-1 \\ 1 & i = n \end{cases} \tag{20}$$

Since this vector exists, $F^\dagger$ is obtained from this vector. □

Lemma 4 *Suppose*

$$M = \sum_{j=1}^{k} A_j \otimes B_j \in M_{a,b}(\mathcal{C}) \otimes M_{c,d}(\mathcal{C}) \tag{21}$$

and $A_1, A_2, A_3...A_k$ and $B_1, B_2, B_3...B_k$ are respectively linearly independent. Then the Schmidt rank of matrix M is k, written as $sr(M) = k$.

Proof. According to our definition, the Schmidt Rank of a certain matrix is the smallest the number of k that satisfies the equation above. Therefore, we obtain that $sr(M) \leq k$. If there exists an i such that $i < k$ such that

$$M = \sum_{j=1}^{i} A'_j \otimes B'_j \in M_{a,b}(c) \otimes M_{c,d}(c). \tag{22}$$

Then at least we have

$$\sum_{j=1}^{k} A_j \otimes B_j = \sum_{j=1}^{k-1} A'_j \otimes B'_j. \tag{23}$$

Then we multiply the matrix $F^\dagger \otimes I$ to the left side of both side of equation 23, $F^\dagger$ is the matrix we have obtained using Lemma 3.

$$\begin{aligned}\sum_{j=1}^{k}(F^\dagger \otimes I)\cdot(A_j \otimes B_j) &= \sum_{j=1}^{k}(F^\dagger \cdot A_j)\otimes(I \cdot B_j) \\ &= \sum_{j=1}^{k-1}(F^\dagger \cdot A'_j)\otimes(I \cdot B'_j).\end{aligned} \tag{24}$$

Therefore, we get

$$\sum_{i=1}^{b}\sum_{j=1}^{k}(\langle i|\otimes I)[(F^\dagger\cdot A_j)\otimes(I\cdot B_j)](|i\rangle\otimes I) = \sum_{i=1}^{b}\sum_{j=1}^{k-1}(\langle i|\otimes I)[(F^\dagger\cdot A'_j)\otimes(I\cdot B'_j)](|i\rangle\otimes I). \tag{25}$$

Notice that $\sum_{i=1}^{b}(\langle i|\cdot F^\dagger\cdot A_j\cdot|i\rangle) = tr(F^\dagger\cdot A_j)$. Therefore, recompiling equation 25:

$$\sum_{j=1}^{k} tr(F^\dagger\cdot A_j)\otimes B_j = tr(F^\dagger\cdot A_k)\cdot B_k = \sum_{j=1}^{k-1} tr(F^\dagger\cdot A'_j)\cdot B'_j. \tag{26}$$

Equation 26 implies that B_k can be linearly represented by $B'_1, B'_2, B'_3 ... B'_{k-1}$. Similarly, using this method, all of the B_i can be represented by $B'_1, B'_2, B'_3 ... B'_{k-1}$. However, this is impossible because all of the B_k are linearly independent and the space spanned by $B'_1, B'_2, B'_3 ... B'_{k-1}$ cannot have k base vectors. Therefore, we arrive at a contradiction, which means that the i in equation 22 does not exist, so k is the minimal number that satisfies the equation 21. Therefore, the lemma is proven. □

Lemma 5 *Given a tripartite matrix N, we have*

$$sr((M_1\otimes N_1\otimes P_1)N(M_2\otimes N_2\otimes P_2)) \le sr(N) \tag{27}$$

Proof. Suppose that $sr(N) = k$, then $N = \sum_{j=1}^{k} A_j\otimes B_j\otimes C_j$. Therefore,

$$(M_1\otimes N_1\otimes P_1)N(M_2\otimes N_2\otimes P_2) = \sum_{j=1}^{k}(M_1A_jM_2)\otimes(N_1B_jN_2)\otimes(P_1C_jP_2), \tag{28}$$

which means that Schmidt rank is less than or equal to k. Then the lemma is proven. □

Lemma 6 *If the matrix $M_1, N_1, P_1, M_2, N_2, P_2$ are all invertible. Then*

$$sr((M_1 \otimes N_1 \otimes P_1)N(M_2 \otimes N_2 \otimes P_2)) = sr(N). \tag{29}$$

Proof. Suppose $(M_1 \otimes N_1 \otimes P_1)N(M_2 \otimes N_2 \otimes P_2) = S$, then it is obvious according to Lemma 5 that $sr(S) \leq sr(N)$. On the other hand,

$$N = (M_1^{-1} \otimes N_1^{-1} \otimes P_1^{-1})S(M_2^{-1} \otimes N_2^{-1} \otimes N_3^{-1}) \tag{30}$$

Using Lemma 5, we have $sr(S) \geq sr(N)$, which means that $sr(S) = sr(N)$.

□

IV. SCHMIDT RANK OF THE MATRIX CORRESPONDING TO THE QUANTUM CIRCUIT REPRESENTATION OF THE ELEMENT (123)

In this section, we compute the Schmidt rank of the matrix needed to represent the element (123). Firstly, we compute the representation matrix $S_{123}|a, b, c\rangle = |b, c, a\rangle$, where S_{123} represents the matrix of three qubits and a, b, c is either 0 or 1. One can show that the expression of matrix S_{123} is

$$S_{123} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{31}$$

Next, we calculate the Schmidt rank of S_{123}. For this purpose, S_0, S_1, S_2, S_3 are defined as the 2×2 matrices:

$$S_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, S_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, S_2 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, S_3 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \tag{32}$$

Therefore, S_{123} can be written as

$$\begin{aligned} S_{123} = {} & S_0 \otimes S_0 \otimes S_0 + S_1 \otimes S_0 \otimes S_2 + S_0 \otimes S_2 \otimes S_1 + S_1 \otimes S_2 \otimes S_3 \\ & + S_2 \otimes S_1 \otimes S_0 + S_3 \otimes S_1 \otimes S_2 + S_2 \otimes S_3 \otimes S_1 + S_3 \otimes S_3 \otimes S_3. \end{aligned} \tag{33}$$

According to equation 35, we have $sr(S_{123}) \leq 8$. We now prove that the actual value of the Schmidt rank of S_{123} is 7 because it is isomorphic to the Strassen tensor [19]. According to the Strassen tensor,

$$\begin{aligned} U_S = {} & P_1 \otimes Q_2 \otimes R_0 + P_2 \otimes Q_3 \otimes R_0 + P_0 \otimes Q_0 \otimes R_1 + P_3 \otimes Q_1 \otimes R_1 \\ & + P_1 \otimes Q_1 \otimes R_2 + P_2 \otimes Q_0 \otimes R_2 + P_0 \otimes Q_3 \otimes R_3 + P_3 \otimes Q_2 \otimes R_3, \end{aligned} \tag{34}$$

where the matrices P_0, P_1, P_2, P_3 are linearly independent, and the same for the matrices in Q and R. The Strassen tensor [19] tells us that $sr(U_S) = 7$. Then we show that S_{123} is a specific representation of U_S. When $P_0 = S_3, P_1 = S_0, P_2 = S_2, P_3 = S_1$, $Q_0 = S_3, Q_1 = S_2, Q_2 = S_0, Q_3 = S_1$ and $R_0 = S_0, R_1 = S_3, R_2 = S_1, R_3 = S_2$. We recompile U_S to U'_S

$$\begin{aligned} U'_S =& S_0 \otimes S_0 \otimes S_0 + S_2 \otimes S_1 \otimes S_0 + S_3 \otimes S_3 \otimes S_3 + S_1 \otimes S_2 \otimes S_3 \\ &+ S_0 \otimes S_2 \otimes S_1 + S_2 \otimes S_3 \otimes S_1 + S_3 \otimes S_1 \otimes S_2 + S_1 \otimes S_0 \otimes S_2 \\ &= S_{123}. \end{aligned} \tag{35}$$

Equation 35 implies that S_{123} is isomorphic to U_S, which means that $sr(S_{ABC}) = 7$.

V. LEAST NUMBER OF NON-LOCAL UNITARY GATES FOR QUANTUM CIRCUIT CONSTRUCTION OF THE ELEMENT (123)

A. Indecomposability with two CNOT gates

We now prove the indecomposability with two CNOT gates, which means that the combination of two CNOT gates and local unitary gates is unable to realize the matrix S_{123}. If all CNOT gates are placed on the same two qubits, then the circuit is not possible in achieving S_{123}. This is because simply multiplying local unitary gates are not possible in converting the third qubit into other qubits. We have already introduced that it is possible change the controlling system of the CNOT gate using the H gate mentioned in equation 16. Also, two systems can switch if the CNOT gates and the local unitary gates on them change responsively, which implies that a lot of quantum circuits can be converted into each other by simply multiplying some local unitary gates. The switch operation of the system is shown at FIG. 4 and FIG. 5.

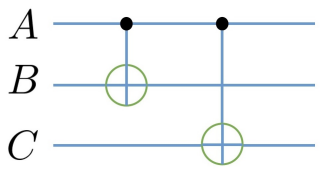

FIG. 4: The initial circuit

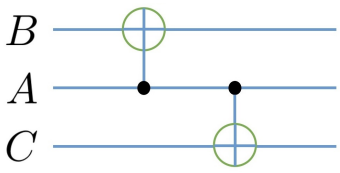

FIG. 5: the system after switching system A and B

Using the above conversion and switch on CNOT gates, we present an observation on the permutation of elements.

Theorem 7 *For a certain circuit with three systems named ABC and input $|i, j, k\rangle$, if the objective output is $|j, k, i\rangle$, then if we rearrange the systems into BCA or CAB, they are both equivalent to the original circuit in achieving* (123).

Proof. We provide a graph showing this effect in the circuit of two gates:

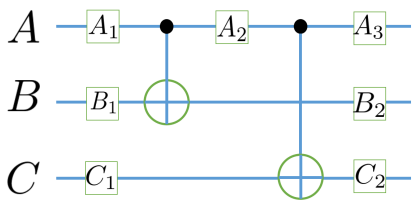

FIG. 6: original system

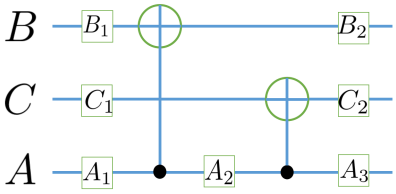

FIG. 7: switch system of BCA

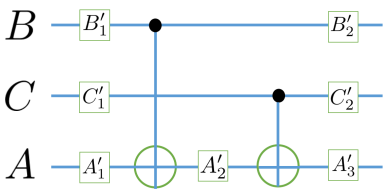

FIG. 8: adjusted switch system of BCA

Suppose that the input $|i, j, k\rangle$ in FIG. 6 and if this circuit in FIG. 6 can achieve the element of (123), then the output will be $|j, k, i\rangle$. Then by switching the systems, the input will be changed into $|j, k, i\rangle$ and the output will be $|k, i, j\rangle$, then we discover that FIG. 8 also achieves (123). So the circuits in FIG. 6, 7 and 8 are equivalent and the claim has been proven. More specifically, the local unitary matrices such as A'_1 are adjusted by A_1 by adding the local unitary gates to change the controlling side of the CNOT gates on AB and AC from FIG. 7 to 8. □

According to Theorem 7, one can show that every circuit consisting of exactly two CNOT gates without two CNOT gates on the same two systems and local unitary gates is equivalent to the circuits in FIG. 9 and FIG. 10.

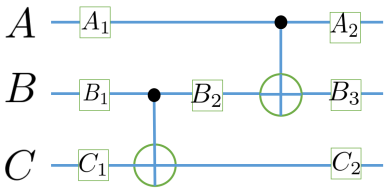

FIG. 9: representation of M_1

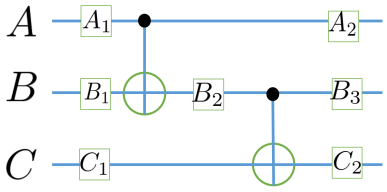

FIG. 10: representation of M_2

We regard the matrix of the circuit in FIG. 9 as M_1, the matrix of the circuit in FIG. 10 as M_2. We now prove that M_1 and M_2 are not equal to S_{123} to prove that 2 CNOT gates are not sufficient to achieve the circuit representing (123). We first provide the expression of M_1 and M_2 using the Kronecker product.

$$\begin{aligned} M_1 &= (A_2 \otimes B_3 \otimes C_2)(CNOT_{AB} \otimes I)(I \otimes B_2 \otimes I)(I \otimes CNOT_{BC})(A_1 \otimes B_1 \otimes C_1). \\ M_2 &= (A_2 \otimes B_3 \otimes C_2)(CNOT_{BC} \otimes I)(I \otimes B_2 \otimes I)(I \otimes CNOT_{AB})(A_1 \otimes B_1 \otimes C_1). \end{aligned} \tag{36}$$

According to Lemma 6, since $A_2, B_3, C_2, A_1, B_1, C_1$ are all local unitary matrices, we have $sr(M_1) = sr((CNOT_{AB} \otimes I_C)(I \otimes B_2 \otimes I)(I_A \otimes CNOT_{BC}))$. According to equation 14 and assuming that $S_0 = |0\rangle\langle 0|$ and $S_3 = |1\rangle\langle 1|$(same as the definition in equation 32). Then, we have

$$\begin{aligned} sr(M_1) =& sr((S_0 \otimes I_2 \otimes I_2 + S_3 \otimes X \otimes I_2)(I_2 \otimes B_2 \otimes I_2) \\ & (I_2 \otimes S_0 \otimes I_2 + I_2 \otimes S_3 \otimes X). \end{aligned} \tag{37}$$

Compiling up the right side of equation 37 we have

$$S_0 \otimes B_2 S_0 \otimes I_2 + S_0 \otimes B_2 S_3 \otimes X + S_3 \otimes X B_2 S_0 \otimes I_2 + S_3 \otimes X B_2 S_3 \otimes X, \tag{38}$$

which means that $sr(M_1) \leq 4$. Using the similar methods as calculating $sr(M_1)$, one can show that

$$\begin{aligned} sr(M_2) &= sr((I_A \otimes CNOT_{BC})(I \otimes B_2 \otimes I)(CNOT_{AB} \otimes I_C)) \\ &= sr(S_0 \otimes S_0 B_2 \otimes I_2 + S_3 \otimes S_0 B_2 X \otimes I_2 + \\ & S_0 \otimes S_3 B_2 \otimes X + S_3 \otimes S_3 B_2 X \otimes X). \end{aligned} \tag{39}$$

Therefore, $sr(M_2) \leq 4$. We obtain that both of M_1 and M_2 have Schmidt Rank of no more than 4.

On the other hand, we have already proven that the objective matrix S_{123} satisfy $sr(S_{123}) = 7$ in section IV, which implies that M_1 and M_2 cannot be equal to the matrix S_{123}. This means that two CNOT gates and several local unitary gates are not enough in achieving S_{123}.

B. Indecomposability with three CNOT gates

In this section, we prove the indecomposaility with three CNOT gates. We begin with two facts, namely Theorems 8 and 9. They will be useful in our classification of non-equivalent circumstances of three CNOT gates.

Theorem 8 *If a certain circuit is capable of achieving the element* (123)*, then the inverse of this circuit is capable of achieving* (132)*, and vice versa.*

Proof. Suppose the matrix representing the circuit is M. If M is able to realize the element (123), then we have $M \cdot |a, b, c\rangle = |b, c, a\rangle$. Since CNOT gates and all the other local unitary gates are invertible, we have $M^{-1} \cdot |b, c, a\rangle = |a, b, c\rangle$, which implies that the inverse of the circuit is able to achieve the element (132), proof with (132) is similar. Thus the claim is proven. □

Theorem 9 *If a certain circuit is capable of achieving the element* (123)*, then if we switch the position of any two systems, then the resulting circuit will achieve the element* (132)*. Similarly, if a certain circuit is capable of achieving the element* (132)*, then it can achieve the element* (123) *by switching any two systems.*

Proof. Suppose the original circuit's matrix is M, so we have $M \cdot |a, b, c\rangle = |b, c, a\rangle$. Suppose system A and B are switched using the switch operation mentioned in Theorem 7, and suppose the matrix of the circuit after the switch is M'. So we have $M' \cdot |b, a, c\rangle = |c, b, a\rangle$, which implies that M' can now achieve the element (132), the same proof goes for (132) and the switch of system A and C or B and C. Therefore the claim is proven. □

Using Theorems 7, 8 and 9, we obtain that the combination of three CNOT gates have the following circumstances, these are all of the non-equivalent circuits with three CNOT gates.

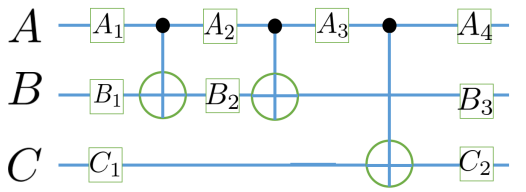

FIG. 11: circumstance 1 with three CNOT gates

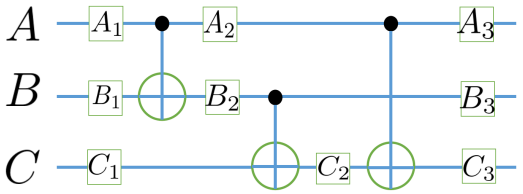

FIG. 12: circumstance 2 with three CNOT gates

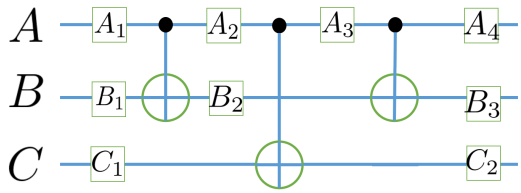

FIG. 13: circumstance 3 with three CNOT gates

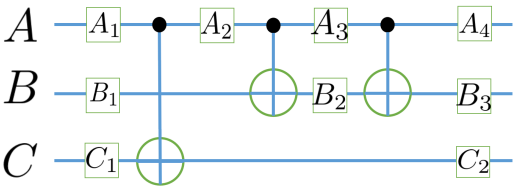

FIG. 14: circumstance 4 with three CNOT gates

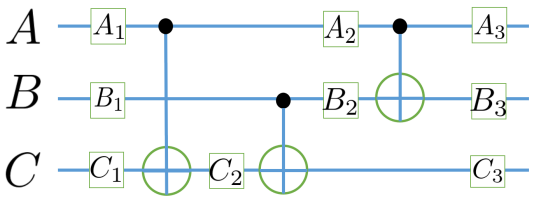

FIG. 15: circumstance 5 with three CNOT gates

Every circuit of 3 CNOT gates must be equivalent to one of the circumstances above using the switch of systems. Specifically, all of the circuits with 3 CNOT gates that is equivalent to circumstance 1 in FIG. 11 are provided in FIG. 16, 17, 18, 19, 20.

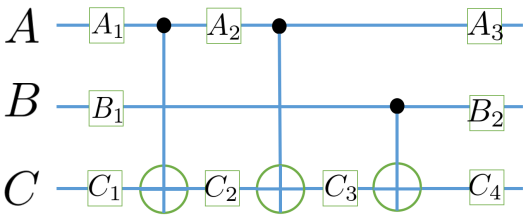

FIG. 16: equivalent circuit 1

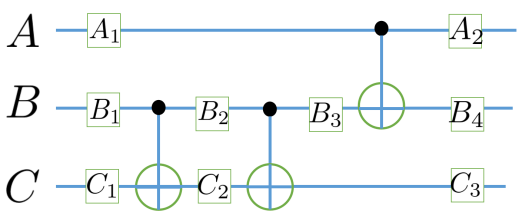

FIG. 17: equivalent circuit 2

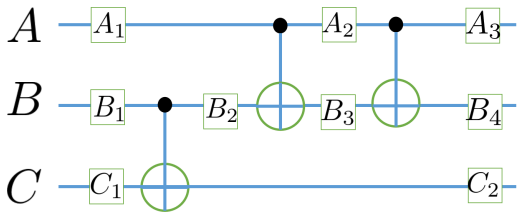

FIG. 18: equivalent circuit 3

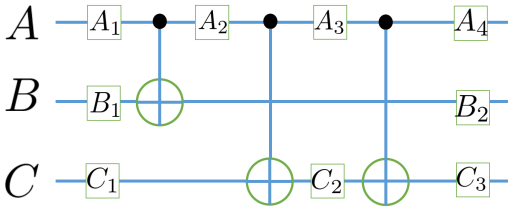

FIG. 19: equivalent circuit 4

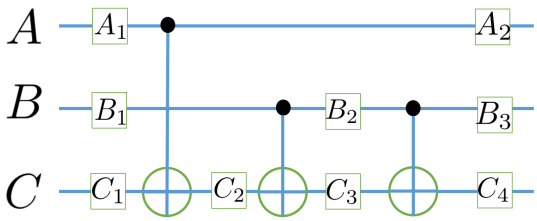

FIG. 20: equivalent circuit 5

In the following subchapters, we will prove that these circuits in FIG. 11, 12,13,14,15 are not able to realize our objective output.

In order to exclude these circuits, we first discuss the states of the circuit after each CNOT gate in each of the circuit. We call system A and B non-product if the state of these two systems cannot be written as $|a\rangle \otimes |b\rangle$. Then we provide a simple lemma.

Lemma 10 *If system A and B are non-product, then the state of AB can be written as* $|0, B_0\rangle + |1, B_1\rangle$*, where* $|B_0\rangle$ *and* $|B_1\rangle$ *are linearly independent.*

Proof. The state of system A and B can be regarded as $M \cdot |i, j\rangle$, where M is the matrix of the circuit and $|i\rangle$ and $|j\rangle$ are the inputs of system A and B. Obviously, this state must be a 4×1 matrix, so suppose

$$M|i, j\rangle = \begin{bmatrix} i_0 \\ i_1 \\ j_0 \\ j_1 \end{bmatrix}. \tag{40}$$

If we regard $|B_0\rangle = \begin{bmatrix} i_0 \\ i_1 \end{bmatrix}$ and $|B_1\rangle = \begin{bmatrix} j_0 \\ j_1 \end{bmatrix}$, we obtain the state of system A and B is equal to $|0, B_0\rangle + |1, B_1\rangle$, where $|B_0\rangle$ and $|B_1\rangle$ are linearly independent. Therefore, we have proven Lemma 10. □

We provide definitions of the state of the system A, B, C:

1. $AB \otimes C$. This means that the state can be written as $|\varphi\rangle_{AB} \otimes |c\rangle_C$, meaning that the systems of A and B are non-product. According to Lemma 10, this state can be written as $(|0, B_0\rangle + |0, B_1\rangle) \otimes |c\rangle$.

2. $AC \otimes B$. Similarly, this means that the systems of A and C are non-product while B is not. This state can be written as $|0\rangle \otimes |b\rangle \otimes |C_0\rangle + |1\rangle \otimes |b\rangle \otimes |C_1\rangle$, where $|C_0\rangle$ and $|C_1\rangle$ are linearly independent.

3. $A \otimes BC$**.** The systems of B and C are non-product while A is not. This state can be written as $|a\rangle \otimes (|0, C_0\rangle + |1, C_1\rangle)$, where $|C_0\rangle$ and $|C_1\rangle$ are linearly independent.

4. $A \otimes B \otimes C$**.** The three systems are in a **fully product state** [20], meaning that the state can be written as $|i', j', k'\rangle$.

5. ABC**.** This means any two of these three systems are non-product, we often call this **genuinely entangled state** [20]. We will introduce the form of this state afterwards.

In order to determine the state of the circuit passing each CNOT gate, we propose the following theorem.

Theorem 11 *(i) Suppose system A and B are in the state of $AB \otimes C$ (state 1). If a CNOT gate acts on either BC or AC, then system A and B are still in a non-product state.*

(ii) Suppose system B and C are in the state of $A \otimes BC$ (state 3). If a CNOT gate acts on either AB or AC, then system B and C are in a non-product state.

(iii) Suppose system A and C are in the state of $AC \otimes B$ (state 2). If a CNOT gate acts on either AB or BC, then system A and C are in a non-product state.

Proof. Without loss of generalities, we prove theorem (i) and assume that CNOT gate on AC. One can use similar methods to prove the case when the CNOT gate is on system BC or part (ii) and (iii).

The state of the system is $AB \otimes C$(state 1), using lemma 10, we suppose that the state before the CNOT gate is $(|0, B_0\rangle + |1, B_1\rangle) \otimes |C\rangle$, where $|B_0\rangle$ and $|B_1\rangle$ are

linearly independent. Then we have

$$CNOT_{AC} \cdot ((|0, B_0\rangle + |1, B_1\rangle) \otimes |C\rangle) = |0\rangle \otimes |B_0\rangle \otimes |C\rangle + |1\rangle \otimes |B_1\rangle \otimes X|C\rangle. \quad (41)$$

We discover that system A and B are still in non-product state, thus we have proven our theorem.

□

After determining the state before and after a CNOT gate in the circuit, we provide two theorems analyzing the outputs of certain systems according to the states we obtained.

Theorem 12 *Suppose a CNOT gate acts on system BC or system AC, and the input state is a three-qubit fully product state (state 4), such that the input state of system C is $|M\rangle$. If the output state is also a fully product state, then the output state of system C is $|M\rangle$ or $X|M\rangle$.*

Proof. Without loss of generalities, we assume that the CNOT gate is on system BC. The proof when the CNOT gate is on system AC is similar. Since the state before the CNOT gate is $A \otimes B \otimes C$ (state 4), we suppose the original state equals to $|N\rangle \otimes (x|0\rangle + y|1\rangle) \otimes |M\rangle$, where $|N\rangle$ is the input of system A before the CNOT gate acting on system BC and x and y are functions associated with the inputs. The state of the three system after the CNOT gate acting on BC is still $A \otimes B \otimes C$. So we have

$$\begin{aligned}(I \otimes |0\rangle\langle 0| \otimes I + I \otimes |1\rangle\langle 1| \otimes X) \cdot (|N\rangle \otimes (x|0\rangle + y|1\rangle) \otimes |M\rangle) \\ = |N\rangle \otimes x|0\rangle \otimes |M\rangle + |N\rangle \otimes y|1\rangle \otimes X|M\rangle.\end{aligned} \quad (42)$$

If $x = 0$, then the output of system C is $X|M\rangle$. When $y = 0$, then the output of system C is $|M\rangle$. On the other hand, if $x, y \neq 0$, then $|M\rangle$ and $X|M\rangle$ are linearly dependent because the state is $A \otimes B \otimes C$. So we have

$$|M\rangle = m \cdot X|M\rangle. \quad (43)$$

where m is a non-zero number. Suppose $|M\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$. Then we obtain $c_0 = \pm c_1$. It means that

$$|M\rangle = \pm X|M\rangle. \quad (44)$$

Therefore, the result is $|A_1\rangle \otimes (x|0\rangle \pm y|1\rangle) \otimes |M\rangle$. The output is still $|M\rangle$.

So the output of system C will be $|M\rangle$ and $X|M\rangle$ under all situations, thus our theorem has been proven. □

Theorem 13 *Suppose a CNOT gate acts on AC or BC, and the input state is $AB \otimes C$(state 1), such that the input state of system C is $|N\rangle$. If the output state is also $AB \otimes C$, then the output state of system C is $|N\rangle$.*

Proof. Without loss of generalities, we only prove the case when the CNOT gate is acting on AC and the proof on system BC is similar. According to lemma 10, we suppose that the input state is $|0, B_0, N\rangle + |1, B_1, N\rangle$, where $|B_0\rangle$ and $|B_1\rangle$ are linearly independent. Then we have

$$CNOT_{AC} \cdot (|0, B_0, N\rangle + |1, B_1, N\rangle) = |0, B_0, N\rangle + |1\rangle \otimes B_1 \otimes X|N\rangle. \tag{45}$$

Since the output state is $AB \otimes C$, then $X|N\rangle$ and $|N\rangle$ must be linearly independent. Similar to equation 43, the final result can be written as

$$(|0, B_0\rangle \pm |1, B_1\rangle) \otimes |N\rangle. \tag{46}$$

This means that the output of C must be $|N\rangle$, thus Theorem 13 is proven. □

We will now use these theorems to exclude the circumstances we have obtained.

1. *circumstance 1*

We show that circumstance 1 in FIG. 11 cannot represent S_{123} in this subsection. We regard the input qubit in A,B,C as $|i\rangle, |j\rangle, |k\rangle$, respectively. We first consider the first two qubits. We regard the operations on the first two qubits just before the last CNOT gate on AC as matrix J. J is shown in the following FIG. 21.

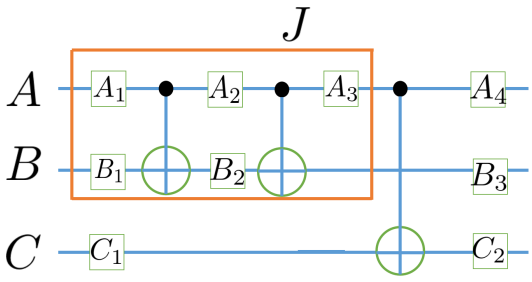

FIG. 21: matrix J

According to Theorem 11, the state of $J|i, j\rangle$ must be $A \otimes B$, otherwise system A and B will be in non-product state after the last gate acting on system A and C. Therefore, we assume $J \cdot |i, j\rangle = |a_0\rangle \otimes |a_1\rangle$. Then consider the qubit on B, whose input is $|j\rangle$, this means that for a certain local unitary gate B_3, we have $B_3 \cdot |a_1\rangle = |k\rangle$, where a_1 is a function of $|i\rangle$ and $|j\rangle$. However, $|k\rangle$ has different values of either $|0\rangle$ or $|1\rangle$, this is impossible. This tells us that circumstance 1 in FIG. 11 cannot satisfy the condition.

2. circumstance 2

Then we prove that circumstance 2 in FIG. 12 cannot achieve the element (123) in this subsection. We first consider the state after the initial qubit went through the matrix Q, Q is shown in the following picture(FIG. 22).

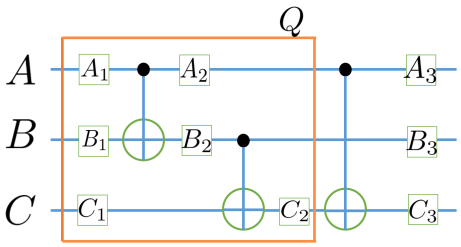

FIG. 22: matrix Q

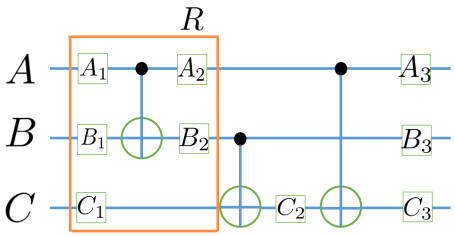

FIG. 23: matrix R

If we consider the state of $Q|i,j,k\rangle$, according to Theorem 11, system A and B cannot be in non-product state. It is the same for system A and C because the final state of the output must be $A \otimes B \otimes C$. Therefore, the state of $Q|i,j,k\rangle$ must be either $A \otimes B \otimes C$ (state 4) or $AC \otimes B$ (state 2).

We now examine a new matrix R, R is shown above in FIG. 23. We consider the state of $R \cdot |i,j,k\rangle$. Since there is only a CNOT gate acting on the system A,B, the state is either $AB \otimes C$(state 1) or $A \otimes B \otimes C$. According to Theorem 11, if $R \cdot |i,j,k\rangle$ is in the state of $AB \otimes C$, system A and B must be in non-product state after getting through the CNOT gate acting on BC. However, the state of $Q|i,j,k\rangle$ must be either $A \otimes B \otimes C$ or $AC \otimes B$, in neither conditions system B is in non-product state with A. So it is impossible for $R \cdot |i,j,k\rangle$ to be $AB \otimes C$, which means that the state of $R \cdot |i,j,k\rangle$ can only be $A \otimes B \otimes C$. Then again using Theorem 11, we get that $Q|i,j,k\rangle$ must also be in the state of $A \otimes B \otimes C$, which means that the state of either side of any CNOT gates in FIG. 12 is the state of $A \otimes B \otimes C$.

Then we can apply Theorem 12 to this circuit using the state before and after the CNOT gates we have obtained. We analyze the output of system C, Theorem 12 tells us that the output of system C has nothing to do with $|i\rangle$ or $|j\rangle$. Therefore, the output of system C cannot achieve $|i\rangle$, which means that circumstance 2 in FIG. 12 is not able to achieve (123).

3. circumstance 3

Then we exclude circumstance 3 in FIG. 13 in this subsection. Similar to the method excluding circumstance 2, we analyze the state of the circuit after two matrices T and W. T and W are provided in FIG. 24 and 25, respectively.

The state of $T|i,j,k\rangle$ must be $A \otimes B \otimes C$ (state 4) or $AB \otimes C$(state 1) according to

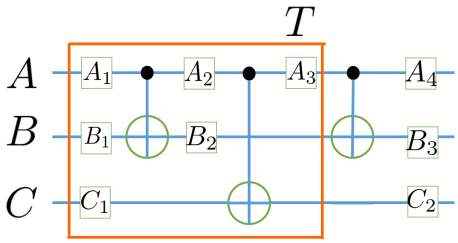

FIG. 24: matrix T

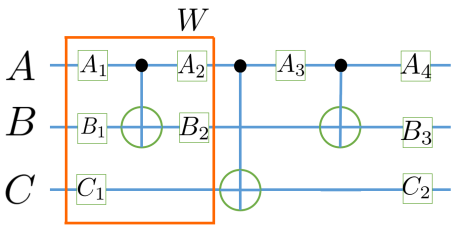

FIG. 25: matrix W

Theorem 11. Besides the state of $W|i,j,k\rangle$ must be $AB\otimes C$ or $A\otimes B\otimes C$ because it only passes through one CNOT gate on system A and B. If $W|i,j,k\rangle$ is in the state of $AB\otimes C$, then again using Theorem 11, system A and system B must be in non-product state after the CNOT gate acting on AC, which means that $T|i,j,k\rangle$ must also be in the state of $AB\otimes C$.

Similarly, one can conclude that it is also another possibility that $W|i,j,k\rangle$ is $A\otimes B\otimes C$ and $T|i,j,k\rangle$ is $A\otimes B\otimes C$. We list the two possibilities of $W|i,j,k\rangle$ to $T|i,j,k\rangle$ below:

1. $A\otimes B\otimes C\to A\otimes B\otimes C$,
2. $AB\otimes C\to AB\otimes C$.

We then discuss these two possibilities in details.

If both $W|i,j,k\rangle$ and $T|i,j,k\rangle$ are in the state of $A\otimes B\otimes C$, according to Theorem 12, the output of system C can only be $C_2C_1|k\rangle$ or $C_2XC_1|k\rangle$, where C_1, C_2 are local unitary gates in FIG. 13. Obviously, it is not able to realize $|i\rangle$.

If both $W|i,j,k\rangle$ and $T|i,j,k\rangle$ are in the state of $AB\otimes C$, then Theorem 13 is applied to the second CNOT gate, which acts on system A and C in FIG. 13. We obtain that the final output of system C must be $C_2C_1|k\rangle$ and cannot achieve $|i\rangle$.

Therefore, both possible states of circuits in FIG. 13 are not able to achieve the objective output, so we have excluded this circumstance.

4. circumstance 4

Next we exclude circumstance 4 in FIG. 14 in this subsection. We consider the output of system C after matrix L acting on system AC in FIG. 26. Suppose that the input is $|i,j,k\rangle$.

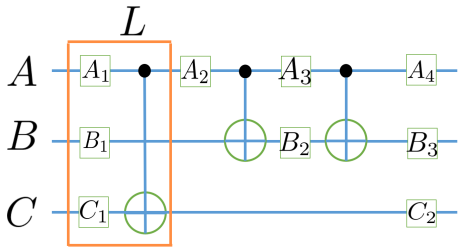

FIG. 26: matrix L

According to Theorem 11, $L|i,j,k\rangle$ must be in the state of $A\otimes B\otimes C$, applying Theorem 12, we get that the final output of system C is $C_2C_1|k\rangle$ or $C_2XC_1|k\rangle$ in FIG. 14, which cannot realize $|i\rangle$. Therefore, circumstance 4 in FIG. 14 is excluded.

5. circumstance 5

Next we exclude circumstance 5 in FIG. 15. We notice that the circuit in circumstance 5 is basically the inverse of the circuit in circumstance 2 in FIG. 12. Therefore, according to Theorem 8, the fact that circuit in circumstance 5 is able to achieve the element (123) is equivalent to the fact that the circuit in circumstance 2 achieving (132), so we instead prove that the circuit in FIG. 12 cannot achieve the element (132).

Since the final output must be in the form of $A\otimes B\otimes C$ in realizing the element (132), similar to the method discussed in circumstance 2 (section V B 2), we obtain that $Q|i,j,k\rangle$ and $R|i,j,k\rangle$ are all in the state of $A\otimes B\otimes C$. Therefore, according to Theorem 12, the final output of system C is only associated with $|k\rangle$, it is incapable of realizing the objective output $|j\rangle$, which implies that the circuit in FIG. 12 is not able to achieve the element (132). And this means that circumstance 5 in FIG. 15 is also impossible of achieving the element (123).

C. Indecomposability with four CNOT gates

In this section, we prove the indecomposability with four CNOT gates. We have already proved that it is not possible to achieve our objective state if four of the CNOT gates are acting on the same two systems. Since four CNOT gates cover a lot of circumstances, we categorize them into three sections, $3+1$, $2+2$, $2+1+1$. Section $3+1$ means that there are 3 CNOT gates on the same two systems, such as AB and another acting on the other systems. $2+2$ means that there are two pairs of two gates on different two gates, for example, there are 2 gates on AB and 2 gates are on AC. We will first find the non-equivalent circuits of these classes and exclude them respectively in the following sections.

1. Three AB gates and one AC gate (3+1 type)

In this section, we prove that the $3+1$ type is impossible. Again using Theorem 8 and 9, we obtain that non-equivalent circumstances of the $3+1$ section as the following.

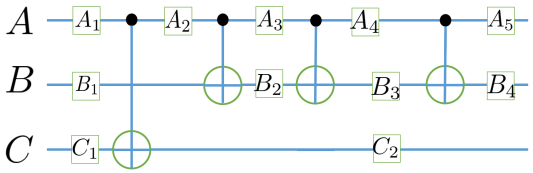

FIG. 27: 3+1 circumstance 1

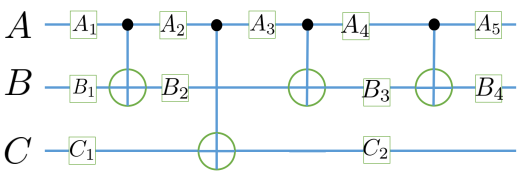

FIG. 28: 3+1 circumstance 2

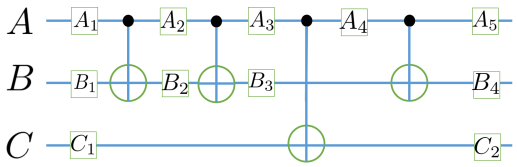

FIG. 29: 3+1 circumstance 3

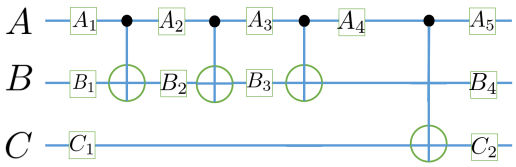

FIG. 30: 3+1 circumstance 4

Assuming that the input is $|i,j,k\rangle$ for system A, B and C respectively, we now exclude all of these circumstances.

Circumstance 1

We briefly exclude circumstance 1 of $3+1$ in FIG. 27. Similar to the method used in excluding the circumstance 14 in the section of three CNOT gates V B 4, the states of the circuit after the first CNOT gate must be $A \otimes B \otimes C$. Using Theorem 12 on the first CNOT gate, we can exclude this circumstance (FIG. 27) directly because the theorem shows that the final output of system C is either $C_2C_1|k\rangle$ or $C_2XC_1|k\rangle$, which cannot achieve $|i\rangle$.

Circumstance 2 and 3

We now exclude circumstance 2 and 3 of FIG. 28 and FIG. 29. Similar to the circumstance 3 in three CNOT gates section V B 3, we obtain that the state of the circuit before and after the CNOT gate acting on AC is both $AB \otimes C$ or both $A \otimes B \otimes C$. For $AB \otimes C$, we apply Theorem 13, and we obtain that the final output of system C is $C_2C_1|k\rangle$. For $A \otimes B \otimes C$, applying Theorem 12, we obtain that the final output of system C is $C_2C_1|k\rangle$ or $C_2XC_1|k\rangle$. Both results are not

able to realize $|i\rangle$. So both circumstances have been excluded.

Circumstance 4

To exclude circumstance 4 of "3+1" in FIG. 30, examine the last CNOT gate that acts on system A and C, using Theorem 11, we get that the state before the last CNOT gate must be $A \otimes B \otimes C$. Then using Theorem 12, the final output of system C must be $C_2C_1|k\rangle$ or $C_2XC_1|k\rangle$, which cannot achieve $|i\rangle$. So this circumstance has been excluded.

2. Two AB gates and two AC gates (2+2 type)

In this section, we first find out all of the non-equivalent circuits of the "2+2" circumstance and then we exclude each of them in the following subsections. Here we provide all of the non-equivalent circuits.

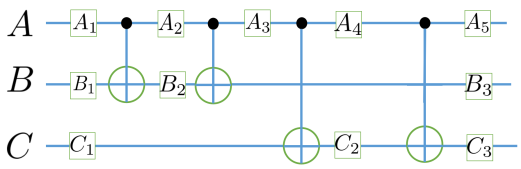

FIG. 31: 2+2 circumstance 1

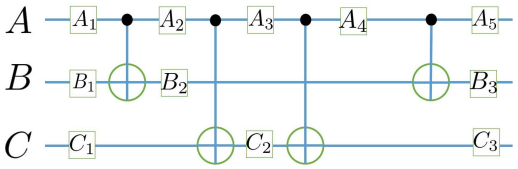

FIG. 32: 2+2 circumstance 2

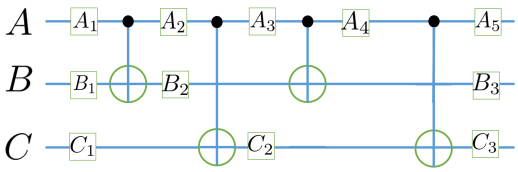

FIG. 33: 2+2 circumstance 3

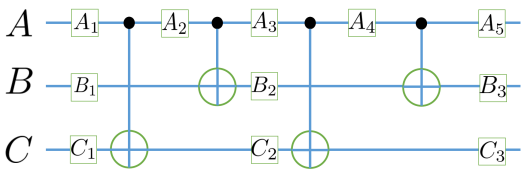

FIG. 34: 2+2 circumstance 4

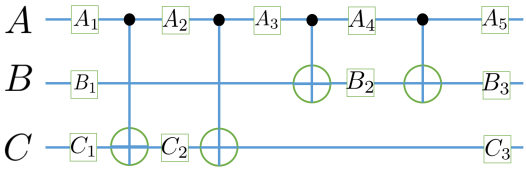

FIG. 35: 2+2 circumstance 5

Circumstance 1

We now exclude circumstance 1 of $2 + 2$ in FIG. 31. According to Theorem 11, the state of the circuit after the first two CNOT gates (both acting on system AB) must be $A \otimes B \otimes C$ because the next two CNOT gates are all acting on system A

and C. Therefore, we assume that after getting through the local unitary matrix A_3 in FIG. 31, the state of system A and B can be written as $|a\rangle \otimes |b\rangle$. Notice that $|b\rangle$ is a function of $|i\rangle$ and $|j\rangle$, the input of system A and B. And the final output of system B is $B_3|b\rangle$. However, the objective output of system B is $|k\rangle$, which is impossible.

Circumstance 2

We now exclude circumstance 2 of $2+2$ in FIG. 32. Using Theorem 11, we obtain that the state of the circuit of circumstance 2 of $2+2$ in FIG. 32 must satisfy one of the following four conditions.

1. $AB \otimes C \to AB \otimes C \to AB \otimes C$.
2. $A \otimes B \otimes C \to A \otimes B \otimes C \to A \otimes B \otimes C$.
3. $A \otimes B \otimes C \to AC \otimes B \to A \otimes B \otimes C$.
4. $AB \otimes C \to ABC \to AB \otimes C$.

The state of the circuit listed above is the state after the first, second and third CNOT gate.

For condition 1, using Theorem 13 for the two CNOT gates acting on system A and C, we obtain that output of system C must be $C_3C_2C_1|k\rangle$, which cannot be $|i\rangle$. For condition 2, using Theorem 12 for the two CNOT gates on system A and C, we obtain that the output of system C is a function of $|k\rangle$. Therefore, it cannot achieve $|i\rangle$. For condition 3, applying apply Theorem 12 to the two CNOT gates acting on system A and B , we get that the output of system B must be a function of $|j\rangle$ and it is not able to achieve $|k\rangle$. This leaves us with condition 4, $AB \otimes C \to ABC \to AB \otimes C$.

Recall that the ABC state is between the CNOT gate on system AC and the unitary gate A_3 in FIG. 32. And ABC state means that any of the two system are in non-product state (state 5). It is known that any ABC state can be written as one of these two forms ([21]):

1. The GHZ orbit

$$(P \otimes Q \otimes R)(|000\rangle + |111\rangle), \tag{47}$$

   where P, Q, R are all 2×2 invertible matrices.

2. The W orbit

$$(J \otimes K \otimes L)(|001\rangle + |010\rangle + |100\rangle), \tag{48}$$

where J, K, L are all 2×2 invertible matrices.

Subsequently, we exclude both orbits to exclude condition 4. Firstly, we prove the following lemma.

Lemma 14 *An ABC state in the W orbit cannot be turned into the state $AB \otimes C$, $AC \otimes B$, $A \otimes BC$ by passing only one CNOT gate.*

Proof. Up to the system permutation, we only need to prove that the state of $AB \otimes C$ cannot turn into the W orbit through one CNOT gate. Obviously passing through a CNOT gate on AB is not able to turn $AB \otimes C$ to the W orbit because system C is independent.

Then we prove that passing through a CNOT gate acting on AC is not possible either. Since the original state is $AB \otimes C$, we suppose that the original state is $(|0, B_0\rangle + |1, B_1\rangle) \otimes |c'\rangle$, where $|B_0\rangle$ and $|B_1\rangle$ are linearly independent. Then we have

$$CNOT_{AC}((|0, B_0\rangle + |1, B_1\rangle) \otimes |c'\rangle) = |0, B_0, c'\rangle + |1, B_1\rangle \otimes X|c'\rangle. \tag{49}$$

This cannot be W orbit because the Schmidt rank of this is two, while any element in the W orbit has Schmidt Rank three.

□

Using this lemma, we can obtain that the ABC state in the fourth condition in item 4 for FIG. 32 cannot be in the W orbit because it turns into the state $AB \otimes C$ in only one CNOT gate.

Next, it remains to exclude condition 4 when the GHZ orbit in equation 47 changes into the form of $AB \otimes C$ through one CNOT gate. For this purpose, we prove the following lemma showing the properties of elements in the GHZ orbit.

Lemma 15 *Suppose $|\varphi\rangle = |a_0, b_0, c_0\rangle + |a_1, b_1, c_1\rangle$ is in the GHZ orbit.*

(i) There exists an element $M \in GL(2, C) \times GL(2, C) \times GL(2, C)$ such that $M|\varphi\rangle = |0, 0, 0\rangle + |1, 1, 1\rangle$.

(ii) If $|\varphi\rangle = |d_0, f_0, g_0\rangle + |d_1, f_1, g_1\rangle$, then we have one case $|a_0, b_0, c_0\rangle = |d_0, f_0, g_0\rangle$, $|a_1, b_1, c_1\rangle = |d_1, f_1, g_1\rangle$, or the other case $|a_0, b_0, c_0\rangle = |d_1, f_1, g_1\rangle$, $|a_1, b_1, c_1\rangle = |d_0, f_0, g_0\rangle$.

(iii) Besides, up to the adjust of the modulus length of the vectors, we have one case $|a_0\rangle = |d_0\rangle, |b_0\rangle = |f_0\rangle, |c_0\rangle = |g_0\rangle, |a_1\rangle = |d_1\rangle, |b_1\rangle = |f_1\rangle, |c_1\rangle = |g_1\rangle$, and similar for the other case.

Proof. (i) Since $|\varphi\rangle$ is in the GHZ orbit, there exists matrices P, Q, R such that $|\varphi\rangle = (P \otimes Q \otimes R)(|0, 0, 0\rangle + |1, 1, 1\rangle)$, where P, Q, R are all invertible matrices. Then $M = P^{-1} \otimes Q^{-1} \otimes R^{-1}$ satisfy the equation $M|\varphi\rangle = |0, 0, 0\rangle + |1, 1, 1\rangle$.

(ii) We first notice that $|a_0\rangle$ and $|a_1\rangle$ are linearly independent, similarly $|b_0\rangle$ and $|b_1\rangle$ and others are all linearly independent. Since all of the corresponding vectors are linearly independent, we obtain that $|a_0, b_0\rangle + |a_1, b_1\rangle$ cannot be written as the form of $c \otimes d$, or in other words, a product form.

Next we prove that $|d_0\rangle$ or $|d_1\rangle$ must be linearly dependent with $|a_0\rangle$. If not, then vectors $|a_0\rangle, |d_0\rangle, |d_1\rangle$ are pairwise linear independent, which means that there exists a vector $\langle x|$ such that $\langle x|a_0\rangle = 0, \langle x|d_0\rangle \neq 0, \langle x|d_1\rangle \neq 0$. Then we have

$$(\langle x| \otimes I \otimes I) \cdot (|a_0, b_0, c_0\rangle + |a_1, b_1, c_1\rangle) = (\langle x| \otimes I \otimes I) \cdot (|d_0, f_0, g_0\rangle + |d_1, f_1, g_1\rangle). \quad (50)$$

Compiling the equation above,

$$\langle x|a_1\rangle \cdot (|b_1, c_1\rangle) = \langle x|d_0\rangle \cdot |f_0, g_0\rangle + \langle x|d_1\rangle \cdot |f_1, g_1\rangle. \quad (51)$$

However, $|f_0\rangle, |f_1\rangle$ are linearly independent, so do $|g_0\rangle$ and $|g_1\rangle$. Therefore, it is impossible for the right side of the equation to be written as the form of $|c, d\rangle$, which contradicts to the equation we have obtained. So we have proved that $|a_0\rangle$ must be linearly associated with at least one of $|d_0\rangle$ and $|d_1\rangle$. Suppose that $|d_0\rangle$ is linearly dependent with $|a_0\rangle$.

Therefore, we are able to adjust the modulo length such that $|a_0\rangle = |d_0\rangle$. Correspondingly, we have $|a_1\rangle = |d_1\rangle$. Since $|a_0\rangle = |d_0\rangle, |a_1\rangle = |d_1\rangle$, there exists a vector $\langle x|$ such that $\langle x|a_0\rangle = \langle x|d_0\rangle = 0, \langle x|a_1\rangle = \langle x|d_1\rangle \neq 0$. Multiplying $\langle x| \otimes I \otimes I$ to both sides of the original state $|a_0, b_0, c_0\rangle + |a_1, b_1, c_1\rangle = |d_0, f_0, g_0\rangle + |d_1, f_1, g_1\rangle$ we get

$$|b_1, c_1\rangle = |f_1, g_1\rangle. \quad (52)$$

Using similar analysis used above, we obtain that $|b_1\rangle$ is linearly associated with $|f_1\rangle$. Therefore, we are still able to adjust the modulo length of these vectors such that $|b_1\rangle = |f_1\rangle$. Then we obtain that $|c_1\rangle = |g_1\rangle$.

Similarly, there exists a $\langle y|$, such that $\langle y|a_1\rangle = 0, \langle y|a_0\rangle \neq 0$, and similarly by multiplying $\langle y| \otimes I \otimes I$ to both sides of the equation, we obtain

$$|b_0, c_0\rangle = |f_0, g_0\rangle. \quad (53)$$

And we obtain that $|b_0\rangle = |f_0\rangle$ and $|c_0\rangle = |g_0\rangle$. Therefore, lemma 15 has been proven.

□

Then we analyze the circuit in FIG. 32 in terms of condition 4. Recall that we are handling with the GHZ orbit. So we assume that the state between the CNOT

gate and the matrix A_3 is $|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle$. Then we have

$$\begin{aligned} CNOT_{AC}(|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle) &= (|0, d_0\rangle + |1, d_1\rangle) \otimes |e\rangle \\ CNOT_{AC} \cdot (A_3 \otimes I \otimes C_2) \cdot (|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle) &= (|0, f_0\rangle + |1, f_1\rangle) \otimes |h\rangle. \end{aligned} \tag{54}$$

Then we have

$$|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle = |0, d_0, e\rangle + |1, d_1\rangle \otimes X|e\rangle. \tag{55}$$

Using this in the second equation:

$$(A_3 \otimes I \otimes C_2) \cdot (|0, d_0, e\rangle + |1, d_1\rangle \otimes X|e\rangle) = |0, f_0, h\rangle + |1, f_1\rangle \otimes X|h\rangle. \tag{56}$$

Then according to Lemma 15, we obtain that $C_2|e\rangle = |h\rangle$ or $C_2|e\rangle = X|h\rangle$. Recall that for the circuit in FIG. 32 to achieve the element (123), the output must be $|j, k, i\rangle$ when the input is $|i, j, k\rangle$, which implies that$|e\rangle = C_1|k\rangle$, $|h\rangle = C_3^{-1}|i\rangle$. This means that $C_2C_1|k\rangle = C_3^{-1}|i\rangle$ or $C_2C_1|k\rangle = XC_3^{-1}|i\rangle$. However, since C_1, C_2, C_3 are local unitary matrices in FIG. 32, these two equations are not impossible. Therefore we have excluded the case of GHZ orbit of condition 4.

So we have excluded all conditions. We conclude that the circuit in FIG. 32 is not able to realize the element (123).

Circumstance 3

We exclude the circuit in FIG. 33. Again, using Theorem 11, we consider all the possible states of the circuit in FIG. 33.

1. $A \otimes B \otimes C \to A \otimes B \otimes C \to A \otimes B \otimes C$.
2. $A \otimes B \otimes C \to AC \otimes B \to AC \otimes B$.
3. $AB \otimes C \to AB \otimes C \to A \otimes B \otimes C$.
4. $AB \otimes C \to ABC \to AC \otimes B$.

For condition 1, similar as the previous circuit we have analyzed, applying Theorem 12, the output of system C must be only relevant with $|k\rangle$, which cannot achieve $|i\rangle$. So this condition is impossible.

For condition 2, applying Theorem 12 and Theorem 13 to the two CNOT gates that act on AB, the output of system B must be $B_3B_2XB_1|j\rangle$ or $B_3B_2B_1|j\rangle$, which cannot be turned into $|k\rangle$. Therefore, this condition is impossible either.

For condition 3, applying Theorem 12 and Theorem 13 to the two CNOT gates that act on AC, the output of system C is $C_3XC_2C_1|k\rangle$ or $C_3C_2C_1|k\rangle$, which is impossible in achieving $|i\rangle$.

This leaves us with the condition 4, $AB \otimes C \to ABC \to AC \otimes B$. Suppose the state of the circuit just after the second CNOT gate (on AC, the ABC state in the condition) is $|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle$. Then depicting the state of the circuit, we have

$$\begin{aligned} CNOT_{AC}(|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle) &= (|0, d_0\rangle + |1, d_1\rangle) \otimes |e\rangle, \\ CNOT_{AB} \cdot (A_3 \otimes I \otimes C_2) \cdot (|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle) &= (|0, h, f_0\rangle + |1, h, f_1\rangle), \end{aligned} \tag{57}$$

where $|d_0\rangle, |d_1\rangle$ are linearly independent and $|f_0\rangle$ and $|f_1\rangle$ are linearly independent. Similar as the previous circumstance, we obtain

$$(A_3 \otimes I \otimes C_2) \cdot (|0, d_0, e\rangle + |1, d_1\rangle \otimes X|e\rangle) = |0, h, f_0\rangle + |1\rangle \otimes X|h\rangle \otimes |f_1\rangle. \tag{58}$$

In this equation, $|e\rangle = C_1|k\rangle$ and $|h\rangle = B_3^{-1}|k\rangle$ in order for the circuit to achieve the element (123). This means that $|d_0\rangle = B_3^{-1}|k\rangle, |d_1\rangle = XB_3^{-1}|k\rangle$ or $|d_0\rangle = XB_3^{-1}|k\rangle, |d_1\rangle = B_3^{-1}|k\rangle$. Therefore, from system A and B in FIG. 33, we obtain that

$$CNOT \cdot ((A_1 \otimes B_1) \cdot |i, j\rangle) = |0\rangle \otimes B_3^{-1}|k\rangle + |1\rangle \otimes XB_3^{-1}|k\rangle \tag{59}$$

or

$$CNOT \cdot ((A_1 \otimes B_1) \cdot |i, j\rangle) = |0\rangle \otimes XB_3^{-1}|k\rangle + |1\rangle \otimes B_3^{-1}|k\rangle. \tag{60}$$

It is obvious that both equations are impossible because the left side of equation 59 and 60 is independent of $|k\rangle$. Therefore, we have excluded the last condition 4.

In conclusion, the circuit in FIG. 33 is not able to realize the element (123).

Circumstance 4

We now exclude the circuit in circumstance 4 in FIG. 34. We discover that this circumstance is the inverse of the circuit of circumstance 3 in FIG. 33. Then according to Theorem 8, we only have to consider whether circumstance 3 is capable of achieving the element (132), returning to the conditions we have mentioned (V C 2). It is easy to exclude the first three conditions applying Theorem 11 and Theorem 12 like in circumstance 3.

Then we reexamine condition 4 of $AB \otimes C \to ABC \to AC \otimes B$. Since the state of the circuit does not change, equation 58 still holds. If the circuit in FIG. 34 is able to achieve the element (132), then $|e\rangle = C_1|k\rangle$ and $|h\rangle = B_3^{-1}|i\rangle$ in equation

58. According to Lemma 15, we obtain that $|d_0\rangle = B_3^{-1}|i\rangle, |d_1\rangle = XB_3^{-1}|i\rangle$ or $|d_0\rangle = XB_3^{-1}|i\rangle, |d_1\rangle = B_3^{-1}|i\rangle$. This means for the circuit in FIG. 32, we get

$$CNOT((A_1 \otimes B_1) \cdot |i,j\rangle) = |0\rangle \otimes B_3^{-1}|i\rangle + |1\rangle \otimes XB_3^{-1}|i\rangle \tag{61}$$

or

$$CNOT((A_1 \otimes B_1) \cdot |i,j\rangle) = |0\rangle \otimes XB_3^{-1}|i\rangle + |1\rangle \otimes B_3^{-1}|i\rangle \tag{62}$$

Both are impossible in achieving the objective state $|k,i,j\rangle$ because in both equations $|j\rangle$ disappears from the system. Therefore, the circuit of circumstance 3 in FIG. 33 cannot achieve the element (132). Then we conclude that this circumstance 4 in FIG. 34 cannot achieve the element (123).

Circumstance 5

We now exclude circumstance 5 of $2+2$ in FIG. 35. Supposing that the circuit is able to achieve $|j,k,i\rangle$, using Theorem 11, we know that the state of the circuit after the first two CNOT gates on system A and C must be $A \otimes B \otimes C$. Moreover, the state of system C at this time must be $C_3^{-1}|i\rangle$. Since the last two CNOT gates act only on system A and B, the state of system A at this time must only be a function of $|k\rangle$, we regard it as $g(k)$.

Suppose that $A_1|i\rangle = \begin{bmatrix} a_0(i) \\ a_1(i) \end{bmatrix}$, $A_2 = \begin{bmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{bmatrix}$, $C_1|k\rangle = |C_1\rangle$. Then we calculate the state of the circuit after the first CNOT gate on system A and C

$$\begin{aligned} CNOT_{AC}(A_1|i\rangle \otimes |C_1\rangle) &= CNOT_{AC} \cdot (\begin{bmatrix} a_0(i) \\ a_1(i) \end{bmatrix} \otimes |C_1\rangle) \\ &= a_0(i) \cdot |0\rangle \otimes |C_1\rangle + a_1(i) \cdot |1\rangle \otimes X|C_1\rangle. \end{aligned} \tag{63}$$

And we calculate the state after the second CNOT gate on system A and C

$$\begin{aligned} &CNOT_{AC} \cdot (a_0(i)A_2|0\rangle \otimes C_2|C_1\rangle + a_1(i)A_2|1\rangle \otimes C_2X|C_1\rangle) \\ &= a_0(i) \cdot b_{00} \cdot |0\rangle \otimes C_2|C_1\rangle + a_0(i) \cdot b_{10} \cdot |1\rangle \otimes XC_2|C_1\rangle \\ &+ a_1(i) \cdot b_{01} \cdot |0\rangle \otimes C_2X|C_1\rangle + a_1(i) \cdot b_{11} \cdot |1\rangle \otimes XC_2X|C_1\rangle \\ &= g(k) \otimes C_3^{-1}|i\rangle. \end{aligned} \tag{64}$$

Since $a_0(i), a_1(i), b_{00}, b_{01}, b_{10}, b_{11}$ are all coefficients, then we have

$$\begin{aligned} &a_0(i) \cdot b_{00} \cdot C_2|C_1\rangle + a_1(i) \cdot b_{01} \cdot C_2X|C_1\rangle \propto \\ &a_0(i) \cdot b_{10}\rangle \cdot XC_2|C_1\rangle + a_1(i) \cdot b_{11} \cdot XC_2X|C_1\rangle \propto C_3^{-1}|i\rangle. \end{aligned} \tag{65}$$

Since $|C_1\rangle = C_1|k\rangle$, getting $|k\rangle = |0\rangle, |1\rangle$, we get the following equations.

$$\begin{aligned}
(a_0(i)\cdot b_{00}\cdot C_2 + a_1(i)\cdot b_{01}\cdot C_2X)\cdot C_1|0\rangle &= f_0(i)\cdot C_3^{-1}|i\rangle.\\
(a_0(i)\cdot b_{00}\cdot C_2 + a_1(i)\cdot b_{01}\cdot C_2X)\cdot C_1|1\rangle &= f_1(i)\cdot C_3^{-1}|i\rangle.\\
(a_0(i)\cdot b_{10}\cdot XC_2 + a_1(i)\cdot b_{11}\cdot XC_2X)\cdot C_1|0\rangle &= f_2(i)\cdot C_3^{-1}|i\rangle.\\
(a_0(i)\cdot b_{10}\cdot XC_2 + a_1(i)\cdot b_{11}\cdot XC_2X)\cdot C_1|1\rangle &= f_3(i)\cdot C_3^{-1}|i\rangle.
\end{aligned} \tag{66}$$

From equation 64 and 66, we also know that

$$\begin{aligned}
f_0(i)|0\rangle + f_2(i)|1\rangle &= g(0),\\
f_1(i)|0\rangle + f_3(i)|1\rangle &= g(1).
\end{aligned} \tag{67}$$

Analyzing equations 66,

$$\begin{aligned}
C_2\cdot(a_0(i)\cdot b_{00}\cdot I_2 + a_1(i)\cdot b_{01}\cdot X) &= C_2\cdot\begin{bmatrix} a_0(i)\cdot b_{00} & a_1(i)\cdot b_{01}\\ a_1(i)\cdot b_{01} & a_0(i)\cdot b_{00}\end{bmatrix},\\
XC_2\cdot(a_0(i)\cdot b_{10}\cdot I_2 + a_1(i)\cdot b_{11}\cdot X) &= XC_2\cdot\begin{bmatrix} a_0(i)\cdot b_{10} & a_1(i)\cdot b_{11}\\ a_1(i)\cdot b_{11} & a_0(i)\cdot b_{10}\end{bmatrix}.
\end{aligned} \tag{68}$$

The first two equations in equations 66 show us that the two column vectors of the matrix $(a_0(i)\cdot b_{00}\cdot C_2 + a_1(i)\cdot b_{01}\cdot C_2X)\cdot C_1$ are linearly related, so do the two column vectors in the matrix $(a_0(i)\cdot b_{10}\cdot XC_2 + a_1(i)\cdot b_{11}\cdot XC_2X)\cdot C_1$. Therefore, we get

$$\begin{aligned}
det((a_0(i)\cdot b_{00}\cdot C_2 + a_1(i)\cdot b_{01}\cdot C_2X)\cdot C_1) = 0.\\
det((a_0(i)\cdot b_{10}\cdot XC_2 + a_1(i)\cdot b_{11}\cdot XC_2X)\cdot C_1) = 0.
\end{aligned} \tag{69}$$

Since C_1 is a local unitary matrix and has determinant not equal to 0. According to equation 68 and 69, we have

$$\begin{aligned}
(a_0(i)\cdot b_{00})^2 = (a_1(i)\cdot b_{01})^2.\\
(a_1(i)\cdot b_{11})^2 = (a_0(i)\cdot b_{10})^2.
\end{aligned} \tag{70}$$

It is obvious that $a_0(i), a_1(i)$ cannot both be 0, otherwise equation 64 will all be 0, which is impossible. If $a_0(i) = 0, a_1(i) \neq 0$, from equation 70, we get $b_{01} = 0, b_{11} = 0$. However, it is impossible since A_2 is a local unitary matrix. Similarly, $a_0(i) \neq 0, a_1(i) = 0$ is impossible either.

So we have $a_0(i), a_1(i) \neq 0$, since A_2 is a local unitary matrix, $b_{00}b_{11} \neq b_{01}b_{10}$, the according to equation 70, we have $b_{00}b_{11} = -b_{01}b_{10}$. Since for any local unitary matrix, the modulo length of its determinant is 1, then we have

$$\begin{aligned}
|b_{00}b_{11}| = \frac{1}{2} = |b_{01}b_{10}|,\\
b_{00}\bar{b}_{01} + b_{10}\bar{b}_{11} = 0.
\end{aligned} \tag{71}$$

Then

$$|b_{00}|^2 + |b_{01}|^2 = 1 = \frac{1}{4|b_{11}|^2} + \frac{1}{4|b_{10}|^2} = \frac{1}{4|b_{11}b_{10}|^2}. \tag{72}$$

So $|b_{11}b_{10}| = \frac{1}{2}$, similarly $|b_{01}b_{00}| = \frac{1}{2}$. Therefore, we get $|b_{00}| = |b_{01}| = |b_{10}| = |b_{11}| = \frac{\sqrt{2}}{2}$.

According to equation 70, $|a_0(i)| = |a_1(i)|$. Hence, either $a_0(i) \cdot b_{00} = a_1(i) \cdot b_{01}, a_1(i) \cdot b_{11} = -a_0(i) \cdot b_{10}$ or $a_0(i) \cdot b_{00} = -a_1 \cdot b_{01}, a_1(i) \cdot b_{11} = a_0 \cdot b_{10}$.

1. If $a_0(i) \cdot b_{00} = a_1(i) \cdot b_{01}, a_1(i) \cdot b_{11} = -a_0(i) \cdot b_{10}$, recompiling equations 66 and take $|i\rangle$ as $|0\rangle$ and $|1\rangle$ we get the equations below.

   When $|i\rangle = 0$,

$$\begin{aligned} a_0(0) \cdot b_{00} C_2(I+X) \cdot C_1|0\rangle &= f_0(0) \cdot C_3^{-1}|0\rangle. \\ a_0(0) \cdot b_{00} C_2(I+X) \cdot C_1|1\rangle &= f_1(0) \cdot C_3^{-1}|0\rangle. \\ a_0(0) \cdot b_{10} X C_2(I-X) \cdot C_1|0\rangle &= f_2(0) \cdot C_3^{-1}|0\rangle. \\ a_0(0) \cdot b_{10} X C_2(I-X) \cdot C_1|1\rangle &= f_3(0) \cdot C_3^{-1}|0\rangle. \end{aligned} \tag{73}$$

   When $|i\rangle = 1$:

$$\begin{aligned} a_0(1) \cdot b_{00} C_2(I+X) \cdot C_1|0\rangle &= f_0(1) \cdot C_3^{-1}|1\rangle \\ a_0(1) \cdot b_{00} C_2(I+X) \cdot C_1|1\rangle &= f_1(1) \cdot C_3^{-1}|1\rangle \\ a_0(1) \cdot b_{10} X C_2(I-X) \cdot C_1|0\rangle &= f_2(1) \cdot C_3^{-1}|1\rangle \\ a_0(1) \cdot b_{10} X C_2(I-X) \cdot C_1|1\rangle &= f_3(1) \cdot C_3^{-1}|1\rangle \end{aligned} \tag{74}$$

   We analyze the first equations of equations 73 and equations 74. If $f_0(0), f_0(1) \neq 0$, notice that this means that $|0\rangle$ and $|1\rangle$ are linearly related, which is impossible. This means that at least one of $f_0(0), f_0(1)$ is zero.

   Suppose that $f_0(0) = 0$, then we have: $a_0(0) \cdot b_{00} C_2(I+X) C_1|0\rangle = 0$, since $a_0(0), b_{00} \neq 0$, we have $C_2(I+X)C_1|0\rangle = 0$, then we get $f_0(1) = 0$. Therefore, we have obtained that $f_0(i) = 0$. We can also get to this conclusion when $f_0(1) = 0$.

   Using similar methods, we are able to get that $f_1(0) = 0, f_1(1) = 0, f_2(0) = 0, f_2(1) = 0, f_3(0) = 0, f_3(1) = 0$, which is impossible because the result of equation 64 will be 0. Therefore, we have excluded the possibility of $a_0(i) \cdot b_{00} = a_1(i) \cdot b_{01}, a_1(i) \cdot b_{11} = -a_0(i) \cdot b_{10}$.

2. If $a_0b_{00} = -a_1b_{01}, a_1b_{11} = a_0b_{10}$, similarly, then we have:

$$\begin{aligned}
a_0(0)\cdot b_{00}C_2(I-X)\cdot C_1|0\rangle &= f_0(0)\cdot C_3^{-1}|0\rangle.\\
a_0(0)\cdot b_{00}C_2(I-X)\cdot C_1|1\rangle &= f_1(0)\cdot C_3^{-1}|0\rangle.\\
a_0(0)\cdot b_{10}XC_2(I+X)\cdot C_1|0\rangle &= f_2(0)\cdot C_3^{-1}|0\rangle.\\
a_0(0)\cdot b_{10}XC_2(I+X)\cdot C_1|1\rangle &= f_3(0)\cdot C_3^{-1}|0\rangle.\\
a_0(1)\cdot b_{00}C_2(I-X)\cdot C_1|0\rangle &= f_0(1)\cdot C_3^{-1}|1\rangle.\\
a_0(1)\cdot b_{00}C_2(I-X)\cdot C_1|1\rangle &= f_1(1)\cdot C_3^{-1}|1\rangle.\\
a_0(1)\cdot b_{10}XC_2(I+X)\cdot C_1|0\rangle &= f_2(1)\cdot C_3^{-1}|1\rangle.\\
a_0(1)\cdot b_{10}XC_2(I+X)\cdot C_1|1\rangle &= f_3(1)\cdot C_3^{-1}|1\rangle.
\end{aligned} \tag{75}$$

Similarly, we get that $f_0(0) = f_0(1) = f_1(0) = f_1(1) = f_2(0) = f_2(1) = f_3(0) = f_3(1) = 0$, this is impossible.

Therefore, we have excluded both possibilities, which means that there do not exist local unitary matrices satisfying equation 64. This means that circumstance 5 in FIG. 35 is impossible to achieve the element (123).

Up to now, we have excluded all of the circuits in the $2+2$ circumstances having 4 CNOT gates.

3. Two AB gates, one AC gate and one BC gate (2+1+1 type)

In this section we will exclude all of the circuits in "2+1+1". We first provide all of the non-equivalent circuits by using Theorem 7, 8, and 9.

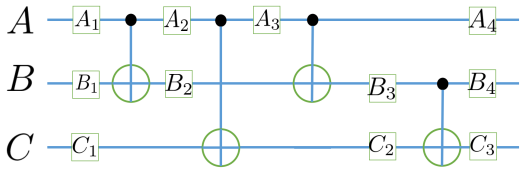

FIG. 36: 2+1+1 circumstance 1

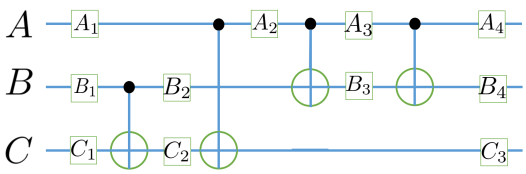

FIG. 37: 2+1+1 circumstance 2

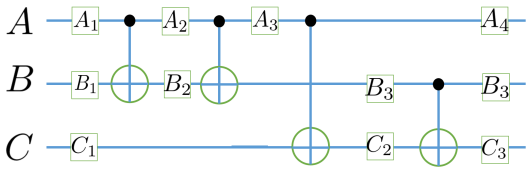

FIG. 38: 2+1+1 circumstance 3

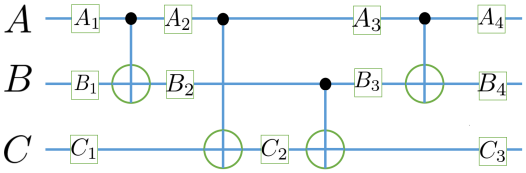

FIG. 39: 2+1+1 circumstance 4

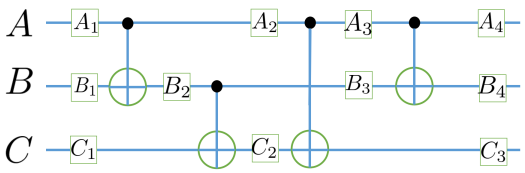

FIG. 40: 2+1+1 circumstance 5

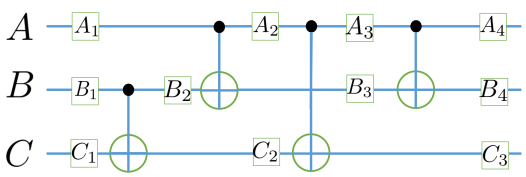

FIG. 41: 2+1+1 circumstance 6

In the following subsections, we will exclude all of these circumstances. Applying Theorem 8, we analyze these circuits by pairing up with their inverses.

Circumstance 1 and 6

Using Theorem 8, we obtain that we only have to consider whether circuit 1 in FIG. 36 is capable of achieving the element (123) and (132) to exclude circumstance 1 and circumstance 6 in FIG. 41. According to Theorem 11, in order for it to achieve the element (123), the state of the circuit in circumstance 1 in FIG. 36 must be the following conditions.

1. $AB \otimes C \to AB \otimes C \to A \otimes B \otimes C$.
2. $A \otimes B \otimes C \to A \otimes B \otimes C \to A \otimes B \otimes C$.
3. $AB \otimes C \to ABC \to A \otimes BC$.

For condition 1, applying Theorem 12 and Theorem 13 to the CNOT gates on AC and BC, we obtain that the output of system C is a function of $|k\rangle$, which is unable to achieve either $|i\rangle$ or $|j\rangle$. For condition 2, it is obvious that this condition is impossible by applying Theorem 12 to system C.

This leaves us with condition 3, similar to the method used in V C 2 in circumstance 3 in 2+2, applying Lemma 14, we know that this ABC state must be GHZ orbit. Supposing that the state of the circuit is $|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle$ just after the second CNOT gate in FIG. 36. According to the state of the circuit, we have

$$\begin{aligned} CNOT_{AC} \cdot (|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle) &= (|0, d_0\rangle + |1, d_1\rangle) \otimes |e\rangle, \\ CNOT_{AB} \cdot (A_3 \otimes I \otimes I) \cdot (|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle) &= |f\rangle \otimes (|0, g_0\rangle + |1, g_1\rangle). \end{aligned} \tag{76}$$

Compiling up we get

$$\begin{aligned} |x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle &= |0, d_0, e\rangle + |1, d_1\rangle \otimes X|e\rangle, \\ (A_3 \otimes I \otimes I) \cdot (|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle) &= |f\rangle \otimes H|0\rangle \otimes (\langle 0|H|0\rangle|g_0\rangle + \langle 0|H|1\rangle|g_1\rangle) \\ &\quad + HXH|f\rangle \otimes H|1\rangle \otimes (\langle 1|H|0\rangle|g_0\rangle + \langle 1|H|1\rangle|g_1\rangle) \end{aligned} \tag{77}$$

where H is the Hadamard gate we have mentioned in the Single-qubit gate section in the Preliminaries, we also used the equation $CNOT_{AB} = (H \otimes H) \cdot (CNOT_{BA}) \cdot (H \otimes H)$ we have mentioned in equation 16. According to Theorem 15, we have $A_3|0\rangle = |f\rangle$ or $A_3|0\rangle = H \cdot X \cdot H \cdot |f\rangle$.

When the circuit is able to achieve (123), $|f\rangle = A_4^{-1}|j\rangle$ and the equation is impossible, similarly when the circuit is able to achieve (132), $|f\rangle = A_4^{-1}|k\rangle$, the equation is still impossible to achieve. Therefore, we have excluded both circumstances.

Circumstance 2 and 3

We now exclude circumstance 2 in FIG. 37. According to Theorem 11, in order for it to achieve the element (123), the state of the circuit in circumstance 2 in FIG. 37 must be the following conditions.

1. $A \otimes B \otimes C \to A \otimes B \otimes C \to AB \otimes C$.
2. $A \otimes B \otimes C \to A \otimes B \otimes C \to A \otimes B \otimes C$.

Notice in both conditions, we are able to calculate the output of system C using Theorem 12, the output of system C is a function of $|k\rangle$, which means that it cannot achieve $|i\rangle$. Therefore, we have excluded this circumstance. Similarly, this output also cannot achieve $|j\rangle$, which also means that it cannot achieve the element (132), then according to Theorem 8, circumstance 3 in FIG. 38 is also impossible.

Circumstance 4 and 5

Using Theorem 11, we again enumerate the different conditions of circumstance 4 in FIG. 39.

1. $A \otimes B \otimes C \to A \otimes B \otimes C \to A \otimes B \otimes C$.
2. $AB \otimes C \to AB \otimes C \to AB \otimes C$.
3. $AB \otimes C \to ABC \to AB \otimes C$.

For condition 1, using Theorem 12, we obtain that the output of system C cannot realize $|i\rangle$. For condition 2, using Theorem 13, we obtain that the output of system C must be $C_3C_2C_1|k\rangle$, (C_1, C_2, C_3 are matrices shown in FIG. 39) and it cannot realize $|i\rangle$.

This leaves us with condition 3. Using Theorem 8, we prove that circumstance 4 in FIG. 39 cannot achieve the element (123) and (132). From Lemma 14, we know that the ABC state must be a GHZ orbit. Using similar methods like V C 2

in circumstance 3 in 2+2, supposing that the the state of circuit 4 in FIG. 39 just after the second CNOT gate is $|x_0, y_0, z_0\rangle + |x_1, y_1, z_1\rangle$. Then we have

$$\begin{aligned} CNOT_{AC} \cdot (|x_0, y_0, z_0\rangle) &= (|0, d_0\rangle + |1, d_1\rangle) \otimes |g\rangle. \\ CNOT_{BC} \cdot (I \otimes I \otimes C_2) \cdot (|x_0, y_0, z_0\rangle) &= (|p, 0\rangle + |q, 1\rangle) \otimes |r\rangle. \end{aligned} \tag{78}$$

Then we get

$$\begin{aligned} |x_0, y_0, z_0\rangle &= |0, d_0, g\rangle + |1, d_1\rangle \otimes X|g\rangle, \\ (I \otimes I \otimes C_2) \cdot (|x_0, y_0, z_0\rangle) &= |p, 0, r\rangle + |q, 1\rangle \otimes X|r\rangle. \end{aligned} \tag{79}$$

If the circuit in FIG. 39 are able to the element (123), then $|g\rangle = C_1|k\rangle, |r\rangle = C_3^{-1}|i\rangle$. Using Lemma 15, we obtain that $C_2|g\rangle = |r\rangle$ or $C_2|g\rangle = X|r\rangle$, which means that $C_2C_1|k\rangle = C_3^{-1}|i\rangle$ or $C_2C_1|k\rangle = XC_3^{-1}|i\rangle$. Both are impossible since $|i\rangle$ and $|k\rangle$ are independent inputs, which means that circuit is not able to achieve the objective element (123).

If the circuit in FIG. 39 is able to achieve the element (132). Then in equation 78, $|g\rangle = C_1|k\rangle, |r\rangle = C_3^{-1}|j\rangle$. This means that $C_2C_1|k\rangle = C_3^{-1}|j\rangle$ or $C_2C_1|k\rangle = XC_3^{-1}|j\rangle$, which is still impossible to achieve. Therefore, we have excluded both circumstances in FIG. 39 and 40, and up to now, we have excluded all the non-equivalent circuits in the $2 + 1 + 1$ section.

VI. QUANTUM CIRCUIT OF THE ELEMENT (123) USING SIX CNOT GATES

Up to now, we have proven the indecomposability with two, three, four CNOT gates of the element (123). In this section, we provide a construction of S_{123} using 6 CNOT gates in FIG. 42, basically using 2 SWAP gates.

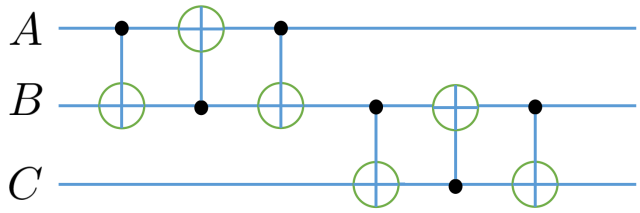

FIG. 42: Using 6 CNOT gates

VII. CONCLUSION

We have shown that the Schmidt rank of the matrix representing the element (123) of the symmetric group is seven based on the known Strassen tensor. We also proved the indecomposability of the element (123) with two, three or four CNOT

gates. It is an open problem whether one can realize the element using at exactly five CNOT gates plus local unitary gates. An idea is to explore the equivalence between the products of some CNOT gates and local unitary gates. For example, the CNOT gate controlled from system A can be modified by that controlled from system B plus some Hadamard gates.

On the other hand, we have provided the construction using six CNOT gates. Further, one can also extend the representation to elements in the symmetric group of higher order, such as $(1234), (12345)$ and so on. Due to the exponentially increasing number of elements in S_n with the number of qubits, one needs to show that the cost of necessary number of CNOT gates implementing elements for any given n is the same first of all. Then it suffices to study the necessary number of CNOT gates realizing the element $(12...n)$.

[1] S. Sternberg and M. E. Mayer, Physics Today **48**, 62 (2000).
[2] J. Lagrange, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin (1770).
[3] T. W. Judson, *Abstract algebra: theory and applications* (2020).
[4] M. A. Nielsen and I. L. Chuang, Mathematical Structures in Computer Science **17**, 1115 (2002).
[5] C. Macchiavello, G. M. Palma, and A. Zeilinger, *Quantum Computing and Quantum Communication with Electrons* (2001).
[6] C. H. Bennett and S. J. Wiesner, Physical review letters **69**, 2881 (1992).
[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Physical review letters **70**, 1895 (1993).
[8] J.-G. Ren, P. Xu, H.-L. Yong, et al., Nature **549**, 70 (2017), ISSN 0028-0836, URL <GotoISI>://WOS:000409388700034.
[9] A. Gueddana, R. Chatta, and N. Boudriga, in *Optical Communication Systems, International Conference on, DCNET/ICE-B/OPTICS. OPTICS 2012 (378-387)* (2012).
[10] Y. Patel, Ph.D. thesis, UC Berkeley (2010).
[11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Quantum Computation and Quantum Information: 10th Anniversary Edition, 2011).
[12] S. Efendi, M. Zarlis, P. Sihombing, et al., in *IOP Conference Series: Materials Science and Engineering* (IOP Publishing, 2021), vol. 1088, p. 012082.
[13] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Physical review A **52**, 3457 (1995).
[14] C. P. Williams, S. H. Clearwater, et al., *Explorations in quantum computing* (Springer, 1998).
[15] L. Song and C. P. Williams, in *Quantum Information and Computation* (SPIE, 2003), vol. 5105, pp. 195–203.
[16] G. Cybenko, Computing in science & engineering **3**, 27 (2001).
[17] Farrokh, Vatan, Colin, and Williams, Physical Review A **69**, 32315 (2004).
[18] X. Qiu and L. Chen, Phys. Rev. A **105**, 062451 (2022), URL https://link.aps.org/doi/10.1103/PhysRevA.105.062451.
[19] J. M. Landsberg, Representation theory **381**, 3 (2012).
[20] Y. Shen and L. Chen, Journal of Physics A: Mathematical and Theoretical **53**, 125302 (2020).
[21] W. Dür, G. Vidal, and J. I. Cirac, Physical Review A **62**, 062314 (2000).

VIII. ACKNOWLEDGMENT

Upon the completion of this essay, I would like to take this opportunity to express my sincere gratitude to my supervisor, Tingjing Chen, also my math teacher in Shenzhen Middle School. She has given me important advice on how to organize the structure of my essay. She also helps me to understand this topic more deeply, guide me through the early stages of learning quantum circuits and the Kronecker Product. She advised me to read the Chinese version of the book *Quantum Computing and Principles of Quantum Information* by Giuliano Benenti, Giulio Casati and Giuliano Strini, which has been the start of my research. Without her help and encouragement, this essay will be impossible. Moreover, she has also given me much advice on the methods of doing research and learning what other scientists have done in this field, which is of great value to my future academic life.

I am also obliged to thank my professor Rick Sommer, whom I met in the math summer camp SUMaC (Stanford University Math Camp). I was first introduced to abstract algebra when I read a book called A First Course in Abstract Algebra by John B.Fraleigh and I deepened my understanding of this field after listening to Rick's lectures. I asked him a lot of questions and I was stimulated to finish my researches linking abstract algebra and quantum circuits together.

Last but not least, I would like to express my gratitude to all the friends and family members who have offered my help and support. I have faced a lot of challenges in the process of writing this essay, and it was the encouragement of my parents that help me solve these problems. Without their help, I could not have finished my study.