Towards an optimal generalized SWAP gate

Colin M Wilmott[1] **and Peter R Wild**[2]

[1] Department of Mathematics and Physics, Nottingham Trent University, Nottingham, NG11 8NS, United Kingdom

[2] Department of Mathematics, Royal Holloway, University of London, Surrey, TW20 0EX, United Kingdom

E-mail: wilmott@fi.muni.cz

Abstract. We present a novel approach for generalizing the SWAP gate to higher dimensions. We construct a regular quantum gate composed entirely in terms of the generalized CNOT gate to cyclically permute the states of d qudits for d prime. A key feature of the construction design relates to evaluating the periodicity of a family of recurrence relations which we achieve by exploiting generating functions and their factorization over the complex reals.

PACS numbers: 02.10.Ox, 03.67.Lx

AMS classification scheme numbers: 05B30

1. Introduction

It is increasingly evident that much effort has been made into constructing optimal quantum circuits in the sense that for a given quantum gate library there is no smaller circuit that achieves a certain task. A reason for this concerted effort has been primarily due to the difficulties associated with *decoherence*. Decoherence represents a major threat for the practical realization of quantum computing and, unfortunately, occurs when a quantum system interacts with the environment. Nevertheless, the library of realizable quantum gates has helped to mitigate the threat of noise in a quantum system. This is in addition to the considerable impact that the quantum gate library already imposes on the design and efficiency of quantum circuitry. Indeed, while an efficient use of computational resources serves to cap the total decohering time, quantum circuitry designs that move toward an optimal use of computational resources are seen as advantageous.

The minimization of quantum gate counts has been a concern of quantum computing and researchers have focused on universal n-qubit gates that contain fewest uses of CNOT gates (Möttönen *et al* (2004), Shende *et al* (2004, 2006) and Sedlák and Plesch (2008)). The reason for this is due to the high cost associated with experimentally realizing a CNOT gate (Möttönen *et al* (2004)). Constructing quantum circuits that limit the use of CNOT gates have become a important aspect of research.

However, characterizing the exact CNOT complexity for an arbitrary n-qubit operation and constructing the corresponding quantum circuit is seen as an ambitious task, even by numerical standards (Vidal and Dawson (2004)). Although researchers have done considerable work optimizing their constructions (Nielsen (2006)), it is believed that the study of quantum circuitry minimization will require different construction techniques than those presently known.

In this paper, we concern ourselves with the construction of a quantum gate to realize a generalized SWAP of d qudit systems. This gate cyclically shifts d qudit subsystems for d prime and does something similar for d other than prime. The design presented builds on previous work by Wilmott and Wild (2012), and similarly, restricts itself to using only instances of the generalized CNOT gate. Interestingly, this design uses a regular periodically repeating sequence of CNOT gates to realize the generalized SWAP but, importantly, requires less gates than the design of Wilmott and Wild (2012). The construction technique makes great use of modular binomial relationships and the sequence design exploits recurrence relations and their associated generating functions. The outline of this paper is as follows. In section 2, we introduce some preliminary material to serve as the basis for our study. Section 3 describes our construction method for a generalized SWAP gate. We demonstrate how the periodic nature of a family of recurrence relations corresponds to a regular periodically repeating structure of CNOT gates that realize a generalized SWAP of qudits. Finally, in section 4, we provide an example of our design and implement a generalized SWAP of three qutrits.

2. Preliminaries

Let $\mathcal{H}$ denote the d-dimensional Hilbert space $\mathbb{C}^d$ and let us fix each orthonormal basis state of the space $\mathcal{H}$ to correspond to an element of ring $\mathbb{Z}_d$ of integers modulo d. In this way, we have the basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\} \subset \mathcal{H}$ called the computational basis whose elements correspond to the column vectors of the identity matrix $\mathbb{I}_d$. A *qudit* is a d-dimensional quantum state $|\psi\rangle \in \mathcal{H}$ that can be written as $|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$ where $\alpha_i \in \mathbb{C}$ and $\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$. The state space of an n-qudit state is the n-fold tensor product of the principal system $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$ which possesses the set of orthonormal basis states that are given by $|i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle = |i_1 i_2 \ldots i_n\rangle$ for $i_j \in \mathbb{Z}_d$. A general state of a qudit in the n-fold space is written

$$|\psi\rangle = \sum_{(i_1 i_2 \ldots i_n) \in \mathbb{Z}_d^n} \alpha_{(i_1 i_2 \ldots i_n)} |i_1 i_2 \ldots i_n\rangle, \tag{1}$$

where $\alpha_{(i_1 i_2 \ldots i_n)} \in \mathbb{C}$ and $\sum |\alpha_{(i_1 i_2 \ldots i_n)}|^2 = 1$.

Given a pair of d-dimensional Hilbert spaces $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$, let us consider the set of $d^2 \times d^2$ unitary transformations $U \in U(d^2)$ that act on the two-qudit quantum system $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. In particular, let $\text{CNOT} \in U(d^2)$ represent the generalized controlled-NOT gate that has control qudit $|\psi\rangle \in \mathcal{H}_\mathcal{A}$ and target qudit $|\phi\rangle \in \mathcal{H}_\mathcal{B}$. The action of CNOT on the set of basis states $|m\rangle \otimes |n\rangle$ of $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ is

$$\text{CNOT} |m\rangle \otimes |n\rangle = |m\rangle \otimes |n \oplus m\rangle, \qquad m, n \in \mathbb{Z}_d, \tag{2}$$

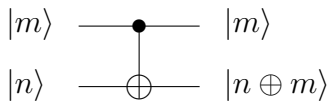

Figure 1. The CNOT gate; the control system $|m\rangle \in \mathcal{H}_{\mathcal{A}}$ remains unchanged after application whereas the state of the target system $|n\rangle \in \mathcal{H}_{\mathcal{B}}$ is transformed under modular arithmetic to the state $|n \oplus m\rangle$ with $m, n \in \mathbb{Z}_d$.

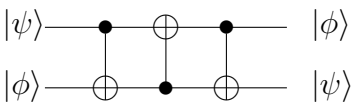

Figure 2. The SWAP gate illustrating the cyclical permutation of two qubits. System $\mathcal{H}_{\mathcal{A}}$ begins in the state $|\psi\rangle$ and ends in the state $|\phi\rangle$ while system $\mathcal{H}_{\mathcal{B}}$ begins in the state $|\phi\rangle$ and ends in the state $|\psi\rangle$.

with $\oplus$ denoting addition modulo d. Figure 1 illustrates the circuitry representation for the CNOT gate. Figure 2 presents the well-known SWAP gate that permutes the states of two qubits.

3. Towards an optimal generalized SWAP gate

We now turn to the construction of a generalized quantum SWAP gate determined completely in terms of instances of the generalized CNOT. For d prime, the effect of the gate is to cyclically permute the states of d qudit subsystems. For d other than prime, the gate permutes the states of the inputs. Wilmott (2011) has shown that pairwise swaps of two qudits that use only generalized CNOT gates cannot be implemented in dimensions $d \equiv 3 \pmod 4$. Consequently, arguing a generalized SWAP of d qudit subsystems entirely in terms of the generalized CNOT gate through a set of nearest neighbour transpositions is not possible. We now outline the problem of a generalized SWAP of d qudits before proceeding to discuss our solution method.

Problem 3.1 *Consider a set of d qudit quantum systems, the first system $\mathcal{A}_0$ prepared in the state $|e_0\rangle_0$, the second system $\mathcal{A}_1$ prepared in the state $|e_1\rangle_1$ and so forth, with the final system $\mathcal{A}_{d-1}$ prepared in the state $|e_{d-1}\rangle_{d-1}$ where $e_0, \ldots, e_{d-1} \in \{0, \ldots, d-1\}$. We ask the question if it is possible to construct a regular quantum network entirely in terms of generalized CNOTs to implement a generalized SWAP of d qudits such that the output of the network places system $\mathcal{A}_0$ in the state $|e_1\rangle_0$, system $\mathcal{A}_1$ in the state $|e_2\rangle_1$ and so forth, with the final system $\mathcal{A}_{d-1}$ being placed in the state $|e_0\rangle_{d-1}$.*

The following result of Wilmott and Wild (2012) states that if a generalized SWAP gate network swaps an arbitrary input basis state such as outlined in problem (3.1) then the generalized SWAP gate swaps all possible d^d sequences of input basis states.

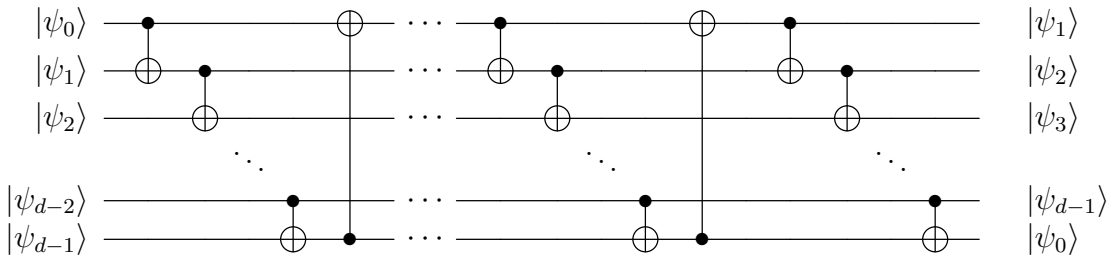

Figure 3. A generalized SWAP gate for prime dimensions. This gate cyclically permutes the states of d d-dimensional qudit states by repeatedly applying a generalized CNOT gate on $d^2 - 1$ successive pairs of states.

Theorem 3.2 *(Wilmott and Wild (2012)) Let $\mathcal{A}_0, \ldots, \mathcal{A}_{d-1}$ be d-dimensional systems with bases $|e_0\rangle_j, |e_1\rangle_j, \ldots, |e_{d-1}\rangle_j$, $j = 0, \ldots, d-1$, where $e_0, \ldots, e_{d-1} \in \mathbb{Z}_d$. Let $\mathcal{A} = \mathcal{A}_0 \otimes \cdots \otimes \mathcal{A}_{d-1}$. If a network implements a generalized SWAP on each basis state $|a_0 a_1 \ldots a_{d-1}\rangle = |a_0\rangle_0 \otimes |a_1\rangle_1 \otimes \cdots \otimes |a_{d-1}\rangle_{d-1}$ of $\mathcal{A}$ where $a_0, \ldots, a_{d-1} \in \mathbb{Z}_d$ then the network implements a generalized SWAP on any input state $|\psi\rangle = |\psi_0\rangle_0 \otimes |\psi_1\rangle_1 \otimes |\psi_{d-1}\rangle_{d-1}$.*

We now provide a construction method for a regular generalized quantum SWAP of d qudits and we present this method in figure 3. The main result of this construction technique is that our regular generalized quantum SWAP gate identifies with the d^{th}-order recurrence relation $a_{j+d} = a_{j+d-1} + a_j$ with the initial conditions $a_0 = \cdots = a_{d-1} = 1$. Through an analysis of the recurrence relation $a_{j+d} = a_{j+d-1} + a_j$, we establish that, for d prime, our regular generalized SWAP gate cyclically permutes the states of d subsystems after the application of $d^2 - 1$ generalized CNOTs. For d other than prime, we present similar findings.

Construction: Generalized quantum SWAP gate. Here we outline the construction method for a regular generalized quantum SWAP gate as given in figure 3. We will motivate the general case of a generalized SWAP of d qudits with an example of how our design method implements a SWAP of four 4-dimensional quantum states. The reason for this is two-fold; in addition to helping us to understand the design method of a regular generalized SWAP of d qudits, the example also serves to underline the implications for our design when we consider d other than prime.

Let k and l be positive integers. For non-negative integers j, let us consider the function

$$f(j) = \binom{j}{k} \bmod l. \tag{3}$$

We will use the periodic property of these integer functions to study a combinatorial problem associated with constructing a generalized SWAP gate for d qudit systems. In particular, we will illustrate how the set of modular binomial coefficients a_j given by

$$a_j = \sum_{i=0}^{j/d} \binom{j-(d-1)i}{i} \bmod d \tag{4}$$

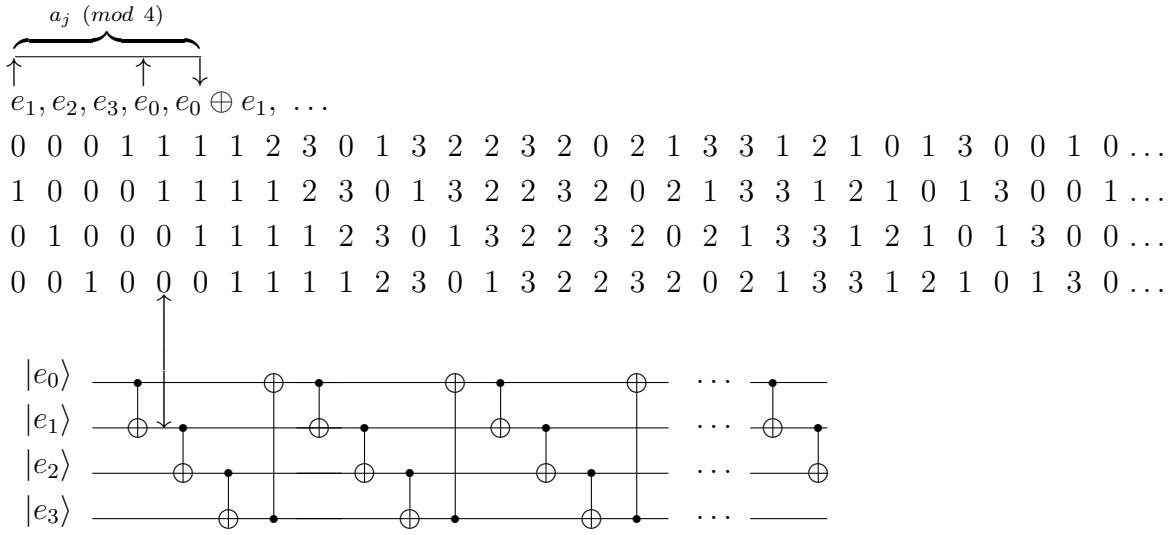

Figure 4. A quantum network composed entirely in terms of CNOT gates illustrating the permutation of four 4-dimensional states. The columns of the array describe the state of the system following the application of respective CNOT gates. In particular, system $\mathcal{A}_1$ is in the state $|e_0 + e_1\rangle_1$ following the application of the first CNOT gate. Here the sum $e_0 + e_1$ is represented as the dot product of the row vector (e_0, e_1, e_2, e_3) and the array's column vector $(1, 1, 0, 0)^{\mathrm{T}}$.

relate to problem 3.1 and the construction of a regular generalized SWAP gate for d qudits.

Figure 4 illustrates our design method to implement a SWAP of four 4-dimensional quantum states via a regular sequence of CNOT gates that act on successive pairs of quantum states. The columns of the array in figure 4 describe the states of the target quantum systems after the corresponding CNOT gates have been applied. The up-down arrow between the array and network indicates the correspondence between the system $\mathcal{A}_1$ being in the state $|e_0 + e_1\rangle_1$, where e_0+e_1 is calculated modulo 4, and the application of the first CNOT gate. The sum $e_0 + e_1$ is represented as the dot product of the row vector (e_0, e_1, e_2, e_3) and the corresponding column vector $(1, 1, 0, 0)^{\mathrm{T}}$. Therefore, the array of integers modulo 4 has its rows indexed by $\{0, 1, 2, 3\}$ and columns indexed by time $t = -3, -2, -1, 0, 1, 2, 3, \ldots$ such that column $t = 4s + j$ with $j \in \{0, 1, 2, 3\}$ corresponds to system $\mathcal{A}_j$. We denote the entries in the array by b_{it}, where $i \in \{0, 1, 2, 3\}$ and $t = -3, -2, -1, 0, 1, 2, 3, \ldots$. Putting

$$a_t = \sum_{i=0}^{3} e_i b_{it}, \quad t = -3, -2, -1, 0, 1, 2, 3, \ldots \tag{5}$$

then, for $t = 4s + j$ with $j \in \{0, 1, 2, 3\}$, the state of the system $\mathcal{A}_j$ is $|a_{4s+j}\rangle_j$. This illustrates that $\mathcal{A}_j$ has been the target of $s + (1 - \delta_{0j})$ CNOT gates.

More generally, for a network of d systems of dimension d, the periodic arrangement of CNOT gates with control system $\mathcal{A}_j$ and target system $\mathcal{A}_{j+1}$ for $j = 0, \ldots, d-1$, where $j + 1 = 0$ for $j = d - 1$, means that the sequence (a_t), where $|a_{ds+j}\rangle_j$ is the state of

system $\mathcal{A}_j$ at time $t = ds + j$ with $j \in \{0, \ldots, d-1\}$ and $\mathcal{A}_j$ has been the target of $s + (1 - \delta_{0j})$ CNOT gates, satisfies the recurrence relation

$$a_{t+d} = a_{t+d-1} + a_t \tag{6}$$

for all $t \geq -d+1$. This is because the CNOT gate replaces the state $|a_{ds+j}\rangle_j$ of $\mathcal{A}_j$ with $\left|a_{d(s+1)+j}\right\rangle_j = \left|a_{ds+j} + a_{d(s+1)+j-1}\right\rangle_j$. With initial states $|a_{-d+1}\rangle_1 = |e_1\rangle_1, \ldots, |a_{-1}\rangle_{d-1} = |e_{d-1}\rangle_{d-1}$, $|a_0\rangle_0 = |e_0\rangle_0$ the terms of the sequence (a_t) may be written as $a_t = \sum_{i=0}^{d-1} e_i b_{it}$ for sequences (b_{it}) which satisfy the recurrences $b_{i(t+d)} = b_{i(t+d-1)} + b_{it}$, $i = 0, \ldots, d-1$. Indeed,

$$\begin{aligned} a_{t+d-1} + a_t &= \sum_{i=0}^{d-1} e_i b_{i(t+d-1)} + \sum_{i=0}^{d-1} e_i b_{it} \\ &= \sum_{i=0}^{d-1} e_i (b_{i(t+d-1)} + b_{it}) \end{aligned} \tag{7}$$

and

$$a_{t+d} = \sum_{i=0}^{d-1} e_i b_{i(t+d)}. \tag{8}$$

We also note that, for $i = 0, \ldots, d-2$, the sequence (b_{it}) is a translate of the sequence $(b_{(i+1)t})$ by 1 place. In fact, these sequences are all translates of one another. We begin by considering the solution of the recurrence relation $a_{t+d} = a_{t+d-1} + a_t$ which we will show to be $a_t = \sum_{i=0}^{t/d} \binom{t-(d-1)i}{i}$.

Lemma 3.3 *Let d be a positive integer. The sequence (a_j) of integers defined by*

$$a_j = \sum_{i=0}^{j/d} \binom{j-(d-1)i}{i} \tag{9}$$

satisfies the recurrence relation $a_{j+d} = a_{j+d-1} + a_j$ having the initial conditions $a_0 = \cdots = a_{d-1} = 1$.

Proof. Clearly the sequence (a_j) as defined satisfies $a_0 = \cdots = a_{d-1} = 1$. Let l be a non-negative integer and let $m \in \{0, \ldots, d-1\}$. Then

$$a_{ld+m} = \sum_{i=0}^{l} \binom{(l-i)d+m+i}{i}, \tag{10}$$

and

$$\begin{aligned} a_{ld+m+d-1} = a_{(l+1)d+m-1} &= \sum_{i=0}^{l+1} \binom{(l+1-i)d+m+i-1}{i} \\ &= 1 + \sum_{i=1}^{l+1} \binom{(l+1-i)d+m+i-1}{i} \\ &= 1 + \sum_{i=0}^{l} \binom{(l-i)d+m+i}{i+1}. \end{aligned} \tag{11}$$

Hence, we have

$$\begin{aligned} a_{ld+m} + a_{ld+m+d-1} &= 1 + \sum_{i=0}^{l} \binom{(l-i)d+m+i+1}{i+1} \\ &= 1 + \sum_{i=1}^{l+1} \binom{(l+1-i)d+m+i}{i} \\ &= \sum_{i=0}^{l+1} \binom{(l+1-i)d+m+i}{i} \\ &= a_{(l+1)d+m} \end{aligned} \tag{12}$$

as required. □

The integer sequence (a_j) is periodic since the recurrence relation is reversible and the sequence must repeat as soon as d consecutive terms, of which there are only finitely many possibilities, are repeated. Consequently, by relating the repeated application of generalized CNOTs on successive pairs of quantum systems to the periodic nature of the recurrence relation $a_{j+d} = a_{j+d-1} + a_j$, we have established a design method that permutes the states of d qudits. This concludes the construction process for a generalized SWAP of d qudits.

The remaining issue is to investigate the nature of the permutations induced by our construction method for regular generalized SWAP gate of d qudits. This investigation necessarily involves determining the period of the sequence (a_j) for various d in order to determine how many generalized CNOTs are required for our regular generalized SWAP gate.

Lemma 3.4 *(Rosen (2000))* $\sum_{i=0}^{k} \binom{j+i}{i} = \binom{j+k+1}{k}$ *for all* $j \geq 0$.

Lemma 3.5 *Let* p *be prime and let* $j \geq -1$. *Then for* $j = p-1 \pmod p$, *we have* $\binom{p+j}{p-1} = 1 \pmod p$ *and for* $j = 0, \ldots, p-2 \pmod p$, *we have* $\binom{p+j}{p-1} = 0 \pmod p$.

Proof. Let us write $\binom{p+j}{p-1}$ as a quotient of factorials, and consequently, we have it that $\binom{p+j}{p-1} = \frac{(p+j)(p+j-1)\ldots(p)}{(j+1)!}$. Since there is a multiple of p in the numerator not cancelled by a factor in the denominator except when $j = p-1 \pmod p$, the result follows. □

Theorem 3.6 *(Lu and Tsai (2000)) Let* p *be a prime number and let* a *and* k *be any positive integers. The integer function* $\binom{j}{k}$ *modulo* p^a *for* $j \geq k$ *has period* p^{a+e} *where* $e = \lfloor log_p k \rfloor$.

We now investigate the periodicity of recurrence relation $a_{j+d} = a_{j+d-1} + a_j$ for prime d and outline the implications of this result for our regular generalized SWAP gate of d qudits.

Theorem 3.7 *Let* d *be a prime. The integer sequence* (a_j) *with coefficients defined by* $a_j = \sum_{i=0}^{j/d} \binom{j-(d-1)i}{i}$ *mod* d *has period* $d^2 - 1$.

Proof. The sequence (a_j) satisfies the recurrence $a_{j+d} = a_{j+d-1} + a_j$ for all j. Since $a_0 = a_1 = \cdots = a_{d-1} = 1$, it is sufficient to show that $a_{d^2-1} = 1, a_{d^2-2} = 0, \ldots, a_{d^2-d} = 0$. This implies that $a_{j+d^2-1} = 1$ for $j = 0, \ldots, d-1$, and so $a_{j+d^2-1} = a_j$ for all $j \geq 0$. Now, for $j = 0, \ldots, d-2$,

$$\begin{aligned} a_{j+d^2-d} &= \sum_{i=0}^{\frac{j+d^2-d}{d}} \binom{j+d^2-d-(d-1)i}{i} \\ &= \sum_{i=0}^{d-1} \binom{j+i}{i}. \end{aligned} \tag{13}$$

By lemma 3.4,

$$\begin{aligned} \sum_{i=0}^{d-1} \binom{j+i}{i} &= \binom{j+d}{d-1} \bmod d \\ &= \begin{cases} 0 \bmod d & \text{for } \ 0 \leq j < d-1 \\ 1 \bmod d & \text{for } \ j = d-1. \end{cases} \end{aligned} \tag{14}$$

Thus, the period of the sequence (a_j) divides $d^2 - 1$. Next, we show that $P_a = d^2 - 1$ is the smallest period value. For $i = 0$, $\binom{j-(d-1)i}{i} = 1$ for all $j \geq 0$. Let i be such that $1 \leq i < \frac{d^2-1}{d}$. Then the sequence (c_j) with $c_j = \binom{j-(d-1)i}{i}$ satisfies $c_j = 0$ for $j = 0, \ldots, di-1$ and $c_j = 1$ for $j = di$ and is periodic with period d for $j \geq di$ by Theorem 3.6. Thus, $a_{ld} = l + 1$ for $l = 0, \ldots, d-1$. Now, any d consecutive terms of $a_0, \ldots, a_{d^2-1}$ includes a term a_{ld} for some l and thus there cannot be $d-1$ consecutive 0 and one 1 until we reach the terms a_j with $j = d^2 - d, \ldots, d^2 - 1$. This establishes the result. □

Since the period $d^2 - 1$ is coprime to d, we note that at the completion of a cycle of $d^2 - 1$ generalized CNOTs, the states of the d subsystem will have cycled around. In fact, since $d^2 - 1 = d - 1 = -1 \pmod d$, the d qudits are cyclically shifted by one position and the network implements a generalized SWAP gate; system $\mathcal{A}_0$ will be in the state $|e_1\rangle_0$, $\mathcal{A}_1$ will be in the state $|e_2\rangle_1$, …, $\mathcal{A}_{d-1}$ will be in the state $|e_0\rangle_{d-1}$. Again, this can be seen by the following argument. The sequences (b_{it}), $i = 0, \ldots, d-1$, have period $d^2 - 1$, we have $(b_{0t}, \ldots, b_{(d-1)t})$ equal to: $(0, 1, 0, \ldots, 0)$ for $t = d^2 - d$ corresponding to system $\mathcal{A}_0$; $(0, 0, 1, 0, \ldots, 0)$ for $t = d^2 - d + 1$ corresponding to system $\mathcal{A}_1$; …; $(0, \ldots, 0, 1)$ for $t = d^2 - 2$ corresponding to system $\mathcal{A}_{d-2}$; $(1, 0, \ldots, 0)$ for $t = d^2 - 1$ corresponding to system $\mathcal{A}_{d-1}$.

Now we let $d = p^m$ with p prime and we seek to evaluate the period of the sequence of integers $a_j = \sum_{i=0}^{j/p^m} \binom{j-(p^m-1)i}{i} \bmod p^m$. We then outline the implication that this result has on the nature of the permutation induced by our generalized SWAP gate.

Conjecture 3.8 *We conjecture that the period of the integer sequence (a_j) for $a_j = \sum_{i=0}^{j/p^m} \binom{j-(p^m-1)i}{i} \bmod p^m$ is $p^{m-1}(p^{2m} - 1)$; see table 1.*

d	$\lvert(a_j)\rvert$
2	$3 = 2^2 - 1$
3	$8 = 3^2 - 1$
4	$30 = 2(2^4 - 1)$
5	$24 = 5^2 - 1$
6	$\mathrm{LCM}(63, 728) = 6552$
7	$48 = 7^2 - 1$
8	$252 = 4(2^6 - 1)$
9	$240 = 3(3^4 - 1)$

Table 1. The period values for integer sequence (a_j) where $a_j = \sum_{i=0}^{j/d} \binom{j-(d-1)i}{i}) \mod d$, for small values of d.

Remark 3.9 *Table 1 gives the period of the sequence* (a_j) *for some initial values of* d. *The period values for the sequences* (a_j) *modulo all prime powers up to 3125 have been confirmed and they all agree with the conjecture. If this conjecture is indeed true then since* $gcd(p^m, p^{m-1}(p^{2m} - 1)) = p^{m-1} \neq 1$, *our quantum network does not produce a generalized SWAP gate when* $m > 1$. *Although at the end of a cycle the systems are shifted round, they are shifted* p^{m-1} *places and the systems return to their original states after* p *applications of the network. Thus, the network provides a cyclic swap on each of* p^{m-1} *groups of* p *systems, the systems of a group have indices congruent modulo* p^{m-1}.

In evaluating the period of the sequence (a_j) for $d = p^m$, $m > 1$, we have it the sequence (a_j) satisfies the recurrence $a_{j+p^m} = a_{j+p^m-1} + a_j$ for all j. We are concerning ourselves with the evaluation of the sequence coefficients $a_j = \sum_{i=0}^{j/p^m} \binom{j-(p^m-1)i}{i}$. To do this, we seek a closed form for these sequence coefficients. We outline the main approach taken.

Let $A(z)$ be the power series $\sum_{j\geq 0} a_j z^j$ and denote by $[z^j]A(z)$ the coefficient of z^j in $A(z)$; thus $[z^j]A(z) = a_j$. Obtaining the generating function for $A(z)$ is of particular importance for our problem of period evaluation. Indeed, a generating function is a clothesline on which we hang up a sequence of numbers for display (Wilf (1994)). The j^{th} term of the sequence (a_j) is the coefficient of z^j in the expansion of the generating function as a power series. Therefore, in order to find the generating function associated

the sequence (a_j), we first recall that the sequence (a_j) satisfies the recurrence relation

$$a_j = \begin{cases} 0 & \text{if} \quad j < 0 \\ 1 & \text{if} \quad j = 0, \ldots, p^m - 1 \\ a_{j-1} + a_{j-p^m} & \text{otherwise.} \end{cases} \tag{15}$$

We note that (15) can be expressed by a single equation;

$$a_j = a_{j-1} + a_{j-p^m} + [j = 0]. \tag{16}$$

Here $[j = 0]$ adds 1 when $j = 0$. Now, to obtain the generating function for $A(z)$, we multiply both sides of equation (16) by z^j and sum over j. Thus, we find

$$\begin{aligned} \sum_{j=0}^{\infty} a_j z^j &= \sum_{j=0}^{\infty} a_{j-1} z^j + \sum_{j=0}^{\infty} a_{j-p^m} z^j + \sum_{j=0}^{\infty} [j = 0] z^j \\ &= \sum_{j=0}^{\infty} a_j z^{j+1} + \sum_{j=0}^{\infty} a_j z^{j+p^m} + 1 \\ &= z \sum_{j=0}^{\infty} a_j z^j + z^{p^m} \sum_{j=0}^{\infty} a_j z^j + 1. \end{aligned} \tag{17}$$

The generating function for $A(z)$ readily demonstrated to be $1/(1 - z - z^{p^m})$. We use the following result from Graham *et al* (1994).

Lemma 3.10 (Graham *et al* (1994)) $\frac{1}{(1-\alpha z)^{i+1}} = \sum_{n=0}^{\infty} \binom{i+n}{i} \alpha^n z^n$.

In seeking to evaluate the coefficients $a_j = [z^j]A(z) = [z^j]1/(1 - z - z^{p^m})$, let us consider a finite sum of the series $1/(1 - \alpha z)^{i+1}$;

$$S(z) = \frac{\beta_1}{(1 - \alpha_1 z)^{i_1+1}} + \cdots + \frac{\beta_N}{(1 - \alpha_N z)^{i_N+1}}. \tag{18}$$

We see that $[z^j]S(z)$ is the finite sum of coefficients given by

$$[z^j]S(z) = \beta_1 \binom{i_1 + j}{i_1} \alpha_1^j + \cdots + \beta_N \binom{i_N + j}{i_N} \alpha_N^j. \tag{19}$$

Let us now write $A(z) = 1/B(z)$ where $B(z) = 1 - z - z^{p^m}$. We have the following result.

Lemma 3.11 *$B(z)$ possesses a set of distinct roots.*

Proof. Let us suppose that $B(z)$ possessing a set of repeated roots. It then follows that $B(z)$ and its derivative $B'(z)$ share a set of common roots (lemma 5.6, Herstein (1975)). Now, since

$$B'(z) = -1 - p^m(z)^{p^m-1}, \tag{20}$$

a repeated root α satisfies $B'(\alpha) = 1 - p^m(\alpha)^{p^m-1} = 0$, and consequently, $\alpha^{p^m-1} = -1/p^m$. Whence, $\alpha^{p^m} = -\alpha/p^m$. Furthermore, as $B(\alpha)$ vanishes, we have it that $1-\alpha+\alpha/p^m = 0$, or equivalently, $1-\alpha(1-1/p^m) = 0$. We deduce that $\alpha = p^m/(p^m-1)$ is the only candidate for a repeating root. Therefore, as a consequence of being a root

of $B'(z)$, it follows that $\alpha = p^m/(p^m-1)$ should satisfy the equation $\alpha^{p^m-1} = -1/p^m$. That is, $\frac{(p^m)^{p^m-1}}{(p^m-1)^{p^m-1}} = \frac{-1}{p^m}$. However, since $(p^m)^{p^m} \equiv 0 \pmod p$ and $-(p^m-1)^{p^m-1} \equiv -1 \pmod p$, this implies that $\alpha = p^m/(p^m-1)$ is not a root of $B'(z)$. Therefore, $B(z)$ possesses a set of distinct roots. □

By putting $B(z)$ in the form $B(z) = (z-b_1)\dots(z-b_{p^m})$ and then taking reciprocals α_k of b_k, $k = 1, \dots, p^m$, we establish a correspondence with the polynomial $(1-\alpha_1 z)\dots(1-\alpha_{p^m} z)$. It follows that

$$\begin{aligned} A(z) &= \frac{1}{((1-\alpha_1 z)\dots(1-\alpha_{p^m} z))} \\ &= \frac{\beta_1}{(1-\alpha_1 z)} + \dots + \frac{\beta_{p^m}}{(1-\alpha_{p^m} z)} \end{aligned} \tag{21}$$

for some β_l, $l = 1, \dots, p^m$. Note that $1/(1-\alpha z)$ is a special case of lemma 3.10 with $i = 0$.

Theorem 3.12 *Let α_k, $k = 1, \dots, p^m$, be reciprocals of the roots of $B(z) = 1 - z - z^{p^m}$. We claim that*

$$[z^j]A(z) = \sum_{l=1}^{p^m} \beta_l \alpha_l^j, \tag{22}$$

where $\beta_l = -\alpha_l / B'(1/\alpha_l)$.

Proof. We have

$$\lim_{z \to 1/\alpha_l} (z - 1/\alpha_l) A(z) = \lim_{z \to 1/\alpha_l} (z - 1/\alpha_l) \mathrm{S}(z), \tag{23}$$

where $\mathrm{S}(z)$ is the special case of (19) with $i_l = 0$. Now,

$$\begin{aligned} \lim_{z \to 1/\alpha_l} (z - 1/\alpha_l) A(z) &= \lim_{z \to 1/\alpha_l} (z - 1/\alpha_l) \frac{1}{B(z)} \\ &= \lim_{z \to 1/\alpha_l} \frac{z - 1/\alpha_l}{B(z) - B(1/\alpha_l)} \\ &= \frac{1}{B'(1/\alpha_l)} \end{aligned} \tag{24}$$

while

$$\begin{aligned} \lim_{z \to 1/\alpha_l} (z - 1/\alpha_l) \mathrm{S}(z) &= \lim_{z \to 1/\alpha_l} (z - 1/\alpha_l) \sum_{k=1}^{p^m} \frac{\beta_k}{(1-\alpha_k z)} \\ &= \lim_{z \to 1/\alpha_l} \frac{\beta_l (z - 1/\alpha_l)}{-\alpha_l (z - 1/\alpha_l)} \\ &= \frac{\beta_l}{-\alpha_l}. \end{aligned} \tag{25}$$

Consequently, $\beta_l = \frac{-\alpha_l}{B'(1/\alpha_l)}$, for $l = 1, \dots, p^m$, since

$$\lim_{z \to 1/\alpha_l} (z - 1/\alpha_l) \frac{\beta_k}{(1-\alpha_k z)} \tag{26}$$

vanishes for $k \neq l$. The result follows. □

Example 3.13 *Theorem 3.12 allows us to efficiently evaluate the set of sequence coefficients* $a_j = \sum_{i=0}^{j/p^m} \binom{j-(p^m-1)i}{i}$ *mod* p^m *for which we were able to conjecture that the period value* $p^{m-1}(p^{2m}-1)$*. As an example, we present the case when* $p^m = 4$*. The generating function for this sequence is* $1 - z - z^4$ *and the reciprocals of the roots of this function are*

$$\begin{aligned}
\alpha_1 &= -.8191725134, \\
\alpha_2 &= .219447421 - .9144736630\iota, \\
\alpha_3 &= .219447421 + .9144736630\iota, \\
\alpha_4 &= 1.380277569.
\end{aligned}$$

Since $\beta_l = \frac{-\alpha_l}{B'(1/\alpha_l)}$*, we have*

$$\begin{aligned}
\beta_1 &= .1305102698, \\
\beta_2 &= .1610008758 + .1534011260\iota, \\
\beta_3 &= .1610008758 - .1534011260\iota, \\
\beta_4 &= .5474879784.
\end{aligned}$$

The closed form for the binomial coefficients $a_j = \sum_{i=0}^{j/4} \binom{j-3i}{i}$ *is*

$$\begin{aligned}
a_j = &(.1305102698)(-.8191725134)^j \\
&+ (.1610 + .1534\iota)(.2194 - .9144\iota)^j \\
&+ (.1610 - .1534\iota)(.2194 + .9144\iota)^j \\
&+ (.5474879784)(1.380277569)^j.
\end{aligned}$$

Input: for j from 0 to 20 do; a_j *mod d; end;*
Output: 1,1,1,1,2,3,0,1,3,2,2,3,2,0,2,1,3,3,1,2,1. This example is interesting and should be compared with figure 4 and table 1. Since the integer sequence $a_j = \sum_{i=0}^{j/4} \binom{j-3i}{i}$ *mod 4 has period equivalent to 2 mod 4, the corresponding generalized SWAP gate transposes states of first and third quantum systems and the states of second and fourth quantum systems.*

Remark 3.14 *Interestingly, the sequence* (a_j) *can be identified as a hypergeometric series of the form*

$$ {}_{p^m}F_{p^m-1}\left[\begin{array}{ccccc} \frac{-j}{p^m}, & \frac{-j+1}{p^m}, & \ldots, & \left(\frac{-j+p^m-1}{p^m}\right) & \\ & & & & ; -\frac{(p^m)^{p^m}}{(p^{m-1})^{p^{m-1}}} \\ \frac{-j}{p^m-1}, & \frac{-j+1}{p^m-1}, & \ldots, & \frac{-j+p^m-2}{p^m-1} & \end{array}\right]. \tag{27}$$

The process of simply identifying a given hypergeometric series often reveals the closed form of the series. Petkovsek et al (1996) provide a library of known hypergeometric series together with their closed forms. Unfortunately, the library of closed forms listed within does not include a closed form for the binomial sums $\sum_{i=0}^{j/p^m} \binom{j-(p^m-1)i}{i}$.

Next we consider period of the sequence coefficients $a_j = \sum_{i=0}^{j/d} \binom{j-(d-1)i}{i}$ mod d for composite d with prime factorization $d = p_1^{m_1} \ldots p_r^{m_r}$. For such d, we determine the

period of the integer sequence (a_j) by first determining the period of (a_j) mod $p_t^{m_t}$ for each $t = 1, \ldots, r$. The period of (a_j) mod $p_t^{m_t}$ for $t = 1, \ldots, r$ is given by the j for which $\sum_{i=1}^{j/d} \binom{j-(d-1)i}{i}$ mod $p_t^{m_t}$ equals 1 and which has a preceding sequence $(a_{j-d+1}, \ldots, a_{j-1})$ $= (0, \ldots, 0)$ mod $p_t^{m_t}$. Since the mapping

$$\lambda_{d,(p_1^{m_1} \ldots p_r^{m_r})} : \mathbb{Z}_d \mapsto \mathbb{Z}_{p_1^{m_1}} \times \cdots \times \mathbb{Z}_{p_r^{m_r}} \tag{28}$$

is well-defined, the period of integer sequence (a_j) mod d is readily established as the lcm $\{|(a_j) \text{ mod } p_t^{m_t}|\}_{t=1}^r$. This claim coincides with the results of table 1.

Theorem 3.15 *Let* $a_j = \sum_{i=0}^{j/d} \binom{j-(d-1)i}{i}$ *mod* d *where* $d = p_1^{m_1} \ldots p_r^{m_r}$. *Consider the set of sequences* $\{(a_j) \text{ mod } p_t^{m_t}\}$, $t = 1, \ldots, r$. *Let* $|(a_j)|$ *denote the period of the integer sequence* (a_j). *Let* $\{|(a_j) \text{ mod } p_t^{m_t}|\}$ *denote the period values of* $\{(a_j) \text{ mod } p_t^{m_t}\}$, *for* $t = 1, \ldots, r$, *respectively. Then, the period of* (a_j) *is lcm* $\{|(a_j) \text{ mod } p_t^{m_t}|\}$, *for* $t = 1, \ldots, r$.

Having investigated the integer sequence $a_j = \sum_{i=0}^{j/d} \binom{j-(d-1)i}{i}$ mod d for various d, we recall the results of table 1. Firstly, table 1 outlines the number of generalized CNOT gates required to implement a permutation of d qudits. This is in accordance with the periodicity of the integer sequence (a_j). Secondly, the use of these integer sequences has permitted us to determine for which dimensions our construction will implement a generalized SWAP of d qudits. In particular, we have a generalized SWAP gate in those dimensions d for which the period of the integer sequence (a_j) is equivalent to -1 mod d. For dimensions d where a generalized SWAP gate is not possible then the period of (a_j) describes a permutation, other than the cyclic permutation sought, of the d input qudit states. For example, figure 4 describes how translates of the integer sequence (a_j) mod 4 explains a permutation of four 4-dimensional states. Table 1 records that for such dimensions the period of the corresponding integer sequence is equivalent to 2 mod 4. Therefore, in this instance our network induces a permutation of the four input 4-dimensional quantum states such that the state $|e_0\rangle_0$ of the first quantum system $\mathcal{A}_0$ is transposed with the state $|e_2\rangle_2$ of the third quantum system $\mathcal{A}_2$ so that the quantum system $\mathcal{A}_0$ is in the state $|e_2\rangle_0$ and the quantum system $\mathcal{A}_2$ is in the state $|e_0\rangle_2$. Correspondingly, the state $|e_1\rangle_1$ of the second quantum system $\mathcal{A}_1$ is transposed with the state $|e_3\rangle_3$ of the fourth quantum system $\mathcal{A}_3$ so that the quantum system $\mathcal{A}_1$ is in the state $|e_3\rangle_1$ and the quantum system $\mathcal{A}_3$ is in the state $|e_1\rangle_3$. Observe also that the period of the integer sequence $a_j = \sum_{i=0}^{j/6} \binom{j-5.i}{i}$ mod 6 is obtained by the least common multiple of the period values of the sequences $\sum_{i=0}^{j/6} \binom{j-5.i}{i}$mod 2 and $\sum_{i=0}^{j/6} \binom{j-5.i}{i}$mod 3. The periods of these sequences are 63 and 728, respectively. By theorem 3.15, the period of (a_j) mod 6 is then 6552. However, since 6552 is equivalent to 0 mod 6, our network acts trivially on the set of six input quantum states.

4. Swapping three qutrits

We now describe how our construction may be used to implement a generalized SWAP of three qutrits. The design features closely follow those illustrated in figure 4.

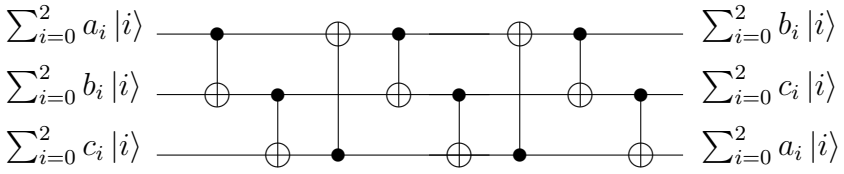

Figure 5. A qutrit SWAP gate that cyclically permutes the states of three qutrits. This gate is composed of eight two-qutrit CNOT gates.

In this instance, we make use of the integer sequence (a_j) with coefficients $a_j = \sum_{i=0}^{j/3} \binom{j-2.i}{i} \bmod 3$ to construct a regular network illustrating the cyclical permutations of three qutrits. Figure 4 depicts the resulting network design. Here, we supposing that the first quantum system $\mathcal{A}_0$ prepared in the state $|a\rangle$, the second system $\mathcal{A}_1$ prepared in the state $|b\rangle$ and the third system $\mathcal{A}_2$ prepared in the state $|c\rangle$. Implementing the qutrit SWAP depicted in figure 4, puts system $\mathcal{A}_0$ in the state $|b\rangle$, system $\mathcal{A}_1$ in the state $|c\rangle$ and system $\mathcal{A}_2$ in the state $|a\rangle$. Appendix B explicitly describes the set of state changes that arise during the application of this gate.

5. Conclusion

Using a regular periodically repeating sequence of CNOT gates, we constructed a generalized SWAP gate that cyclically shift d qudit subsystems for d prime. For d other than prime, our design induces a permutation of qudit subsystems. Our design method made great use of modular binomial relations and illustrated that the problem of quantum circuit design may be recast as a problem of period determination for recurrence relations.

Acknowledgments

The authors would like to thank Prof. Matthew G. Parker, Prof. Gary McGuire and Prof. Rüdiger Schack for helpful comments and suggestions.

Appendix A

We explicitly provide the set output states corresponding to the actions of the successive CNOT gates depicted in figure 4 for the input state $|a\rangle \otimes |b\rangle \otimes |c\rangle$. The state of the

system after the application of the initial CNOT gate is

$$a_0b_0c_0\,|000\rangle + a_0b_0c_1\,|001\rangle + a_0b_0c_2\,|002\rangle + a_0b_1c_0\,|010\rangle + a_0b_1c_1\,|011\rangle + a_0b_1c_2\,|012\rangle + a_0b_2c_0\,|020\rangle + a_0b_2c_1\,|021\rangle + a_0b_2c_2\,|022\rangle + a_1b_0c_0\,|110\rangle + a_1b_0c_1\,|111\rangle + a_1b_0c_2\,|112\rangle + a_1b_1c_0\,|120\rangle + a_1b_1c_1\,|121\rangle + a_1b_1c_2\,|122\rangle + a_1b_2c_0\,|100\rangle + a_1b_2c_1\,|101\rangle + a_1b_2c_2\,|102\rangle + a_2b_0c_0\,|220\rangle + a_2b_0c_1\,|221\rangle + a_2b_0c_2\,|222\rangle + a_2b_1c_0\,|200\rangle + a_2b_1c_1\,|201\rangle + a_2b_1c_2\,|202\rangle + a_2b_2c_0\,|210\rangle + a_2b_2c_1\,|211\rangle + a_2b_2c_2\,|212\rangle\,. \tag{A.1}$$

The action of the second CNOT gate on (A.1) is

$$a_0b_0c_0\,|000\rangle + a_0b_0c_1\,|001\rangle + a_0b_0c_2\,|002\rangle + a_0b_1c_0\,|011\rangle + a_0b_1c_1\,|012\rangle + a_0b_1c_2\,|010\rangle + a_0b_2c_0\,|022\rangle + a_0b_2c_1\,|020\rangle + a_0b_2c_2\,|021\rangle + a_1b_0c_0\,|111\rangle + a_1b_0c_1\,|112\rangle + a_1b_0c_2\,|110\rangle + a_1b_1c_0\,|122\rangle + a_1b_1c_1\,|120\rangle + a_1b_1c_2\,|121\rangle + a_1b_2c_0\,|100\rangle + a_1b_2c_1\,|101\rangle + a_1b_2c_2\,|102\rangle + a_2b_0c_0\,|222\rangle + a_2b_0c_1\,|220\rangle + a_2b_0c_2\,|221\rangle + a_2b_1c_0\,|200\rangle + a_2b_1c_1\,|201\rangle + a_2b_1c_2\,|202\rangle + a_2b_2c_0\,|211\rangle + a_2b_2c_1\,|212\rangle + a_2b_2c_2\,|210\rangle\,. \tag{A.2}$$

The action of the third CNOT gate given in figure 4 on (A.2) is

$$a_0b_0c_0\,|000\rangle + a_0b_0c_1\,|101\rangle + a_0b_0c_2\,|202\rangle + a_0b_1c_0\,|111\rangle + a_0b_1c_1\,|212\rangle + a_0b_1c_2\,|010\rangle + a_0b_2c_0\,|222\rangle + a_0b_2c_1\,|020\rangle + a_0b_2c_2\,|121\rangle + a_1b_0c_0\,|211\rangle + a_1b_0c_1\,|012\rangle + a_1b_0c_2\,|110\rangle + a_1b_1c_0\,|022\rangle + a_1b_1c_1\,|120\rangle + a_1b_1c_2\,|221\rangle + a_1b_2c_0\,|100\rangle + a_1b_2c_1\,|201\rangle + a_1b_2c_2\,|002\rangle + a_2b_0c_0\,|122\rangle + a_2b_0c_1\,|220\rangle + a_2b_0c_2\,|021\rangle + a_2b_1c_0\,|200\rangle + a_2b_1c_1\,|001\rangle + a_2b_1c_2\,|102\rangle + a_2b_2c_0\,|011\rangle + a_2b_2c_1\,|112\rangle + a_2b_2c_2\,|210\rangle\,. \tag{A.3}$$

The remaining CNOT gates of figure 4 yield the following respective outcomes;

$$a_0b_0c_0\,|000\rangle + a_0b_0c_1\,|111\rangle + a_0b_0c_2\,|222\rangle + a_0b_1c_0\,|121\rangle + a_0b_1c_1\,|202\rangle + a_0b_1c_2\,|010\rangle + a_0b_2c_0\,|212\rangle + a_0b_2c_1\,|020\rangle + a_0b_2c_2\,|101\rangle + a_1b_0c_0\,|201\rangle + a_1b_0c_1\,|012\rangle + a_1b_0c_2\,|120\rangle + a_1b_1c_0\,|022\rangle + a_1b_1c_1\,|100\rangle + a_1b_1c_2\,|211\rangle + a_1b_2c_0\,|110\rangle + a_1b_2c_1\,|221\rangle + a_1b_2c_2\,|002\rangle + a_2b_0c_0\,|102\rangle + a_2b_0c_1\,|210\rangle + a_2b_0c_2\,|021\rangle + a_2b_1c_0\,|220\rangle + a_2b_1c_1\,|001\rangle + a_2b_1c_2\,|112\rangle + a_2b_2c_0\,|011\rangle + a_2b_2c_1\,|122\rangle + a_2b_2c_2\,|200\rangle \tag{A.4}$$

$$a_0b_0c_0\,|000\rangle + a_0b_0c_1\,|112\rangle + a_0b_0c_2\,|221\rangle + a_0b_1c_0\,|120\rangle + a_0b_1c_1\,|202\rangle + a_0b_1c_2\,|011\rangle + a_0b_2c_0\,|210\rangle + a_0b_2c_1\,|022\rangle + a_0b_2c_2\,|101\rangle + a_1b_0c_0\,|201\rangle + a_1b_0c_1\,|010\rangle + a_1b_0c_2\,|122\rangle + a_1b_1c_0\,|021\rangle + a_1b_1c_1\,|100\rangle + a_1b_1c_2\,|212\rangle + a_1b_2c_0\,|111\rangle + a_1b_2c_1\,|220\rangle + a_1b_2c_2\,|002\rangle + a_2b_0c_0\,|102\rangle + a_2b_0c_1\,|211\rangle + a_2b_0c_2\,|020\rangle + a_2b_1c_0\,|222\rangle + a_2b_1c_1\,|001\rangle + a_2b_1c_2\,|110\rangle + a_2b_2c_0\,|012\rangle + a_2b_2c_1\,|121\rangle + a_2b_2c_2\,|200\rangle \tag{A.5}$$

$$a_0b_0c_0\,|000\rangle + a_0b_0c_1\,|012\rangle + a_0b_0c_2\,|021\rangle + a_0b_1c_0\,|120\rangle + a_0b_1c_1\,|102\rangle + a_0b_1c_2\,|111\rangle + a_0b_2c_0\,|210\rangle + a_0b_2c_1\,|222\rangle + a_0b_2c_2\,|201\rangle + a_1b_0c_0\,|001\rangle + a_1b_0c_1\,|010\rangle + a_1b_0c_2\,|022\rangle + a_1b_1c_0\,|121\rangle + a_1b_1c_1\,|100\rangle + a_1b_1c_2\,|112\rangle + a_1b_2c_0\,|211\rangle + a_1b_2c_1\,|220\rangle + a_1b_2c_2\,|202\rangle + a_2b_0c_0\,|002\rangle + a_2b_0c_1\,|011\rangle + a_2b_0c_2\,|020\rangle + a_2b_1c_0\,|122\rangle + a_2b_1c_1\,|101\rangle + a_2b_1c_2\,|110\rangle + a_2b_2c_0\,|212\rangle + a_2b_2c_1\,|221\rangle + a_2b_2c_2\,|200\rangle \tag{A.6}$$

$$a_0b_0c_0\,|000\rangle + a_0b_0c_1\,|012\rangle + a_0b_0c_2\,|021\rangle + a_0b_1c_0\,|100\rangle + a_0b_1c_1\,|112\rangle + a_0b_1c_2\,|121\rangle + a_0b_2c_0\,|200\rangle + a_0b_2c_1\,|212\rangle + a_0b_2c_2\,|221\rangle + a_1b_0c_0\,|001\rangle + a_1b_0c_1\,|010\rangle + a_1b_0c_2\,|022\rangle + a_1b_1c_0\,|101\rangle + a_1b_1c_1\,|110\rangle + a_1b_1c_2\,|122\rangle + a_1b_2c_0\,|201\rangle + a_1b_2c_1\,|210\rangle + a_1b_2c_2\,|222\rangle + a_2b_0c_0\,|002\rangle + a_2b_0c_1\,|011\rangle + a_2b_0c_2\,|020\rangle + a_2b_1c_0\,|102\rangle + a_2b_1c_1\,|111\rangle + a_2b_1c_2\,|120\rangle + a_2b_2c_0\,|202\rangle + a_2b_2c_1\,|211\rangle + a_2b_2c_2\,|220\rangle \tag{A.7}$$

$$a_0b_0c_0\,|000\rangle + a_0b_0c_1\,|010\rangle + a_0b_0c_2\,|020\rangle + a_0b_1c_0\,|100\rangle + a_0b_1c_1\,|110\rangle + a_0b_1c_2\,|120\rangle + a_0b_2c_0\,|200\rangle + a_0b_2c_1\,|210\rangle + a_0b_2c_2\,|220\rangle + a_1b_0c_0\,|001\rangle + a_1b_0c_1\,|011\rangle + a_1b_0c_2\,|021\rangle + a_1b_1c_0\,|101\rangle + a_1b_1c_1\,|111\rangle + a_1b_1c_2\,|121\rangle + a_1b_2c_0\,|201\rangle + a_1b_2c_1\,|211\rangle + a_1b_2c_2\,|221\rangle + a_2b_0c_0\,|002\rangle + a_2b_0c_1\,|012\rangle + a_2b_0c_2\,|022\rangle + a_2b_1c_0\,|102\rangle + a_2b_1c_1\,|112\rangle + a_2b_1c_2\,|122\rangle + a_2b_2c_0\,|202\rangle + a_2b_2c_1\,|212\rangle + a_2b_2c_2\,|222\rangle\,. \tag{A.8}$$

Now, the state of the system recorded in (A.8) follows the application of the final CNOT gate of figure 4. State (A.8) may be rewritten as

$$b_0c_0a_0\,|000\rangle + b_0c_0a_1\,|001\rangle + b_0c_0a_2\,|002\rangle + b_0c_1a_0\,|010\rangle + b_0c_1a_1\,|011\rangle + b_0c_1a_2\,|012\rangle + b_0c_2a_0\,|020\rangle + b_0c_2a_1\,|021\rangle + b_0c_2a_2\,|022\rangle + b_1c_0a_0\,|100\rangle + b_1c_0a_1\,|101\rangle + b_1c_0a_2\,|102\rangle + b_1c_1a_0\,|110\rangle + b_1c_1a_1\,|111\rangle + b_1c_1a_2\,|112\rangle + b_1c_2a_0\,|121\rangle + b_1c_2a_1\,|121\rangle + b_1c_2a_2\,|122\rangle + b_2c_0a_0\,|200\rangle + b_2c_0a_1\,|201\rangle + b_2c_0a_2\,|202\rangle + b_2c_1a_0\,|210\rangle + b_2c_1a_1\,|211\rangle + b_2c_1a_2\,|212\rangle + b_2c_2a_0\,|220\rangle + b_2c_2a_1\,|221\rangle + b_2c_2a_2\,|222\rangle\,, \tag{A.9}$$

and this has the required form $|b\rangle \otimes |c\rangle \otimes |a\rangle$.

References

Shende V, Markov I L and Bullock S 2004 Minimal universal two-qubit controlled-NOT-based circuits *Phys. Rev. A* **69** 062321

Vatan F and Williams C 2004 Optimal quantum circuits for general two-qubit gates *Phys. Rev. A* **69** 032315

Möttönen M, Bergholm V, Vatiainen J J and Salomaa M M 2004 Quantum circuits for general multiqubit gates *Phys. Rev. Lett* **93** 130502

Sedlák M and Plesch M 2008 Towards optimization of quantum circuits *Cent. Eur. J. Phys.* **6** 128–34

Shende V, Markov I L and Bullock S 2006 Synthesis of quantum logic circuits *Proc. 2005 Asia and South Pacific Design Automation Conf.* 272–75

Vidal G and Dawson C M 2004 Universal quantum circuit for two-qubit transformations with three controlled-NOT gates *Phys. Rev. A* **69** 010301

Nielsen M A 2006 A geometric approach to quantum circuit lower bounds *Quantum Information & Computation* **6** 213–62

Graham R L, Knuth D E and Patashnik O 1994 *Concrete Mathematics: A Foundation for Computer Science* (Reading, MA: Addison-Wesley)

Herstein I N 1975 *Topics in Algebra* (New York: Wiley and Sons)

Lu C J and Tsai S C 2000 The periodic property of binomial coefficients modulo m and its applications *10th SIAM Conference on Discrete Mathematics, Minneapolis, Minnesota, USA*

Petkovsek M, Wilf H and Zeilberger D 1996 $A = B$ (Wellesley, MA: A K Peters)

Rosen K H 2000 *Handbook of Discrete and Combinatorial Mathematics* (CRC Press)

Wilf H S 1994 *Generating Functionology* (San Diego, CA: Academic)

Wilmott C M 2011 On swapping the states of two qudits *Int. J. Quant. Inf.* **9** 1511–17

Wilmott C M and Wild P R 2012 On a generalized quantum SWAP gate *Int. J. Quant. Inf.* **X** XXXX–XX