

SCIENTIFIC REPORTS



OPEN

Graph states of prime-power dimension from generalized CNOT quantum circuit

Lin Chen^{1,2} & D. L. Zhou³

Received: 06 November 2015

Accepted: 11 May 2016

Published: 07 June 2016

We construct multipartite graph states whose dimension is the power of a prime number. This is realized by the finite field, as well as the generalized controlled-NOT quantum circuit acting on two qudits. We propose the standard form of graph states up to local unitary transformations and particle permutations. The form greatly simplifies the classification of graph states as we illustrate up to five qudits. We also show that some graph states are multipartite maximally entangled states in the sense that any bipartition of the system produces a bipartite maximally entangled state. We further prove that 4-partite maximally entangled states exist when the dimension is an odd number at least three or a multiple of four.

Maximal entanglement is the key ingredient in quantum teleportation, computing and the violation of Bell inequality. The maximally entangled state of two qubits can be created by controlled-phase gate or controlled-not (CNOT) gate. In this sense, they have the same power to create entanglement. In fact, the two gates are related by local Hadamard gates. As we know, only one type of two-qubit unitary gates and single qubit gates are enough to build a universal quantum circuit. A natural idea is to use those gates to generate maximally entangled states in many qubit case^{1–3}. The graph states and cluster states are generated by applying two-qubit phase gates to an initially product state⁴. Single-qubit gates are not involved in the generation. So the quantum circuit to create graph states is composed of controlled phase gates only. The graph states and continuous-variable cluster states are constructed to study one-way quantum computing^{4–7}. They are useful for self-testing of nonlocal correlations⁸ and their entanglement can be effectively evaluated by the Schmidt measure⁹, relative entropy of entanglement and the geometric measure of entanglement^{10,11}. Recently the graph states have been generalized to prime dimensions even in continuous variables, in terms of the encoding circuit and Hadamard matrices¹² and quantum codes and stabilizers¹³. The cluster states can also be defined using finite groups and controlled-phase gates^{14,15}.

The Hilbert space of prime-power dimensions has been studied for a few quantum-information problems, such as the mutually unbiased basis, the stabilizer code and the Clifford group underlying distillation¹⁶. In this paper we study the multi-qudit graph state when the dimension $d = p^m$ is a power of a prime number p . It ensures the existence of finite field structure, and at the same time generalizes¹². With the aid of the structure, generalized CNOT gates are defined naturally. A general N qudit state generated by a quantum circuit is constructed in Eq. (88). To simplify this state, we propose a standard form of multiqubit state in Eq. (89). Our first main result is Theorem 1, stating that the above two families are equivalent up to local unitary transformations and particle permutations. We also propose the dual graph state of the standard form in (94), and show that they are equivalent under local unitary transformation in Theorem 2. It further simplifies the structure of multiqubit graph states, and we classify them up to five parties.

Our main task is to find out the maximally entangled state by the quantum circuit composed of generalized CNOT gates. The task induces a preliminary problem: what states are called maximally entangled states of many-qudit system? The basic requirement is that any single qudit is entangled with the other systems. We further require that the many-qudit state is a maximally entangled state if any bipartition of systems produces a bipartite maximally entangled state^{1–3,17,18}. We will show that some graph states are multipartite maximally entangled states. We further prove that 4-partite maximally entangled states exist when the dimension is an odd number at least three or a multiple of four. This is another main result in our paper, as stated in Theorem 3. These results

¹School of Mathematics and Systems Science, Beihang University, Beijing 100191, China. ²International Research Institute for Multidisciplinary Science, Beihang University, Beijing 100191, China. ³Beijing National Laboratory for Condensed Matter Physics, and Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China. Correspondence and requests for materials should be addressed to L.C. (email: linchen@buaa.edu.cn) or D.L.Z. (email: zhou72@iphy.ac.cn)

imply that the maximal entanglement is universal in high dimensions. We also construct a connection between the maximal entanglement and an entropy problem recently proposed in¹⁹.

This paper is organized as follows. First we will introduce the generalized CNOT in the qudit case with the aid of the structure of finite field, and then a quantum circuit composed pure generalized CNOT gates is given. Next we prove that only bipartite graph states can be generalized from the quantum circuit of pure generalized CNOT gates. Third we analyze the maximal entanglement of these states. Finally, we give a summary of our results and open problems.

Quantum Circuit of Pure Generalized CNOT Gates

In this section we construct the generalized CNOT gates by two one-qudit operations $A(a_m)$ and $D(a_m)$. They are mathematically realized by the known finite field and the commutation relations. Using the CNOT gates we construct the quantum circuit. We will introduce a standard form of N -qudit graph state on finite field in (89), and show that any graph state is equivalent to the standard form up to local unitary transformations and particle permutations. To obtain a simpler classification of such states we propose Theorem 2 and demonstrate it by states up to five systems respectively in the figures.

Finite field and generalized CNOT gates. As is well known, when d is the power of a prime number, i.e.,

$$d = p^n, \quad (1)$$

where p is prime, and n is a positive integer, there is a field F_d . Note that the field F_d is unique up to isomorphism. The elements of the Field F_d are denoted as $\{a_i, i \in \{0, 1, \dots, d-1\}\}$, where $a_0 \equiv 0$ and $a_1 \equiv 1$ are the units for the sum and the product operations respectively.

We introduce a d -dimensional Hilbert space H_d with a natural orthonormal basis $\{|a_i\rangle\}$. With the aid of the sum and product operations in the field, two classes of basic one-qudit operations are defined

$$A(a_m)|a_i\rangle = |a_i + a_m\rangle, \quad (2)$$

$$D(a_m)|a_i\rangle = |a_m a_i\rangle. \quad (3)$$

Obviously, the operation $A(a_m)$ is unitary for any m . If $a_m \neq 0$, then $D(a_m)$ is also unitary. Since F_d is an Abelian group under the operation $+$, then we have

$$A(a_m)|s\rangle = |s\rangle, \quad (4)$$

where

$$|s\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |a_i\rangle. \quad (5)$$

We introduce the generalized CNOT gate from qudit m to qudit n labeled by a_k defined by

$$C_{mn}(a_k)|a_i\rangle_m |a_j\rangle_n = |a_i\rangle_m |a_j + a_i a_k\rangle_n, \quad (6)$$

where qudit m is the control qudit, and qudit n is the target qudit.

First, we notice that

$$C_{mn}(a_k)|s, a_j\rangle_{mn} = A_n(a_j)D_n(a_k)|B\rangle_{mn}, \quad (7)$$

where

$$|B\rangle_{mn} = \frac{1}{\sqrt{d}} \sum_i |a_i, a_i\rangle_{mn}. \quad (8)$$

In addition, when $d=2$ and $a_k=1$, the gate $C_{mn}(1)$ is the CNOT gate. Therefore any $C_{mn}(a_k)$ with $a_k \neq 0$ is a generalized CNOT gate, which can generate the two-qudit maximal entangled state from a separable state.

Commutation relations for related unitary transformations. Before investigating the properties of the generated states, let us first calculate the basic commutation relations for related unitary transformations widely used throughout the paper. The proof of these relations will be given in the end of this subsection. First we study the one qudit case. According to the definitions given in Eq. (2) and Eq. (3), we have

$$A_m(a_i)A_m(a_j) = A_m(a_i + a_j), \quad (9)$$

$$D_m(a_i)D_m(a_j) = D_m(a_i a_j). \quad (10)$$

The commutation relations between A_m and D_m are

$$D_m(a_i)A_m(a_j) = A_m(a_i a_j)D_m(a_i). \quad (11)$$

In addition, we also have

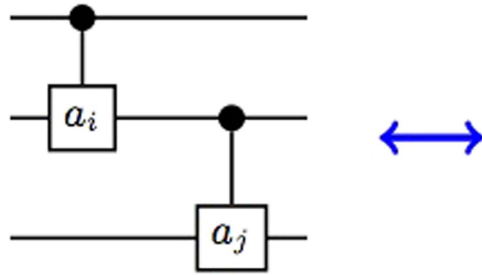


Figure 1. Circuit representation of Eq. (21). The gate diagram and Fig. 2 both represent the same unitary transformation.

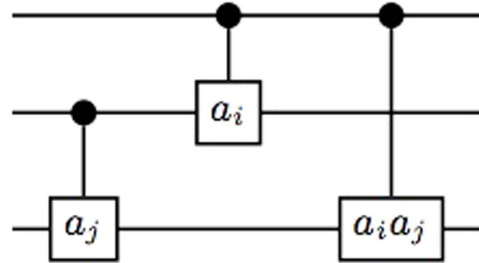


Figure 2. Circuit representation of Eq. (21).

$$A_m(0) = D_m(1) = I_m. \tag{12}$$

Next we study the two-qudit case. The first set of relations are

$$C_{mn}(a_i)A_m(a_j) = A_n(a_i a_j)A_m(a_j)C_{mn}(a_i), \tag{13}$$

$$C_{mn}(a_i)A_n(a_j) = A_n(a_j)C_{mn}(a_i), \tag{14}$$

$$C_{mn}(a_i)D_m(a_j) = D_m(a_j)C_{mn}(a_i a_j), \tag{15}$$

$$C_{mn}(a_i)D_n(a_j) = D_n(a_j)C_{mn}(a_j^{-1} a_i). \tag{16}$$

The second set of relations includes two equations. The first equation is

$$C_{mn}(a_i)C_{mn}(a_j) = C_{mn}(a_i + a_j), \tag{17}$$

which is easy to prove but important in simplifying our graph gates. The second equation is

$$C_{mn}(a_i)C_{nm}(a_j) = \begin{cases} D_m(A^{-1})D_n(A)C_{nm}(A a_j)C_{mn}(A^{-1} a_i) & \text{if } A \neq 0, \\ W_{mn}D_m(a_i)D_n(a_j)C_{mn}(a_j^{-1}), & \text{if } A=0, \end{cases} \tag{18}$$

where $A = 1 + a_i a_j$, W_{mn} is the swap gate between the qudits m and n .

Third we study the three-qudit case. The relations for three qudits are given by

$$C_{mn}(a_i)C_{ml}(a_j) = C_{ml}(a_j)C_{mn}(a_i), \tag{19}$$

$$C_{mn}(a_i)C_{ln}(a_j) = C_{ln}(a_j)C_{mn}(a_i), \tag{20}$$

$$C_{nl}(a_j)C_{mn}(a_i) = C_{ml}(a_i a_j)C_{mn}(a_i)C_{nl}(a_j). \tag{21}$$

Here we use two circuits to represent Eq. (21) as shown in Figs 1 and 2.

Finally we give the proof of relations in Eqs (11)–(21), respectively.

The proof of Eq. (11):

Notice that the identity operator for the m -th particle is

$$I_m = \sum_{\alpha} |a_{\alpha}\rangle \langle a_{\alpha}| \quad (22)$$

$$\equiv |a_{\alpha}\rangle \langle a_{\alpha}|, \quad (23)$$

where we take the Einstein's rule for repeated indexes. Then

$$D_m(a_i)A_m(a_j) \quad (24)$$

$$= D_m(a_i)A_m(a_j)I_m \quad (25)$$

$$= D_m(a_i)A_m(a_j)|a_{\alpha}\rangle \langle a_{\alpha}| \quad (26)$$

$$= D_m(a_i)|a_{\alpha} + a_j\rangle \langle a_{\alpha}| \quad (27)$$

$$= |a_i a_{\alpha} + a_i a_j\rangle \langle a_{\alpha}| \quad (28)$$

$$= A_m(a_i a_j)|a_i a_{\alpha}\rangle \langle a_{\alpha}| \quad (29)$$

$$= A_m(a_i a_j)D_m(a_i). \quad (30)$$

The proof of Eq. (13):

$$C_{mn}(a_i)A_m(a_j) \quad (31)$$

$$= C_{mn}(a_i)A_m(a_j)|a_{\alpha}, a_{\beta}\rangle \langle a_{\alpha}, a_{\beta}| \quad (32)$$

$$= C_{mn}(a_i)|a_{\alpha} + a_j, a_{\beta}\rangle \langle a_{\alpha}, a_{\beta}| \quad (33)$$

$$= |a_{\alpha} + a_j, a_{\beta} + a_i a_{\alpha} + a_i a_j\rangle \langle a_{\alpha}, a_{\beta}| \quad (34)$$

$$= A_m(a_j)A_n(a_i a_j)|a_{\alpha}, a_{\beta} + a_i a_{\alpha}\rangle \langle a_{\alpha}, a_{\beta}| \quad (35)$$

$$= A_m(a_j)A_n(a_i a_j)C_{mn}(a_i). \quad (36)$$

The proof of Eq. (14):

$$C_{mn}(a_i)A_n(a_j) \quad (37)$$

$$= C_{mn}(a_i)A_n(a_j)|a_{\alpha}, a_{\beta}\rangle \langle a_{\alpha}, a_{\beta}| \quad (38)$$

$$= C_{mn}(a_i)|a_{\alpha}, a_{\beta} + a_j\rangle \langle a_{\alpha}, a_{\beta}| \quad (39)$$

$$= |a_{\alpha}, a_{\beta} + a_j + a_i a_{\alpha}\rangle \langle a_{\alpha}, a_{\beta}| \quad (40)$$

$$= A_n(a_j)|a_{\alpha}, a_{\beta} + a_i a_{\alpha}\rangle \langle a_{\alpha}, a_{\beta}| \quad (41)$$

$$= A_n(a_j)C_{mn}(a_i). \quad (42)$$

The proof of Eq. (15):

$$C_{mn}(a_i)D_m(a_j) \quad (43)$$

$$= C_{mn}(a_i)D_m(a_j)|a_{\alpha}, a_{\beta}\rangle \langle a_{\alpha}, a_{\beta}| \quad (44)$$

$$= C_{mn}(a_i)|a_j a_{\alpha}, a_{\beta}\rangle \langle a_{\alpha}, a_{\beta}| \quad (45)$$

$$= |a_j a_\alpha, a_\beta + a_i a_j a_\alpha\rangle \langle a_\alpha, a_\beta| \quad (46)$$

$$= D_m(a_j) |a_\alpha, a_\beta + a_i a_j a_\alpha\rangle \langle a_\alpha, a_\beta| \quad (47)$$

$$= D_m(a_j) C_{mn}(a_i a_j). \quad (48)$$

The proof Eq. (16):

$$C_{mn}(a_i) D_n(a_j) \quad (49)$$

$$= C_{mn}(a_i) D_n(a_j) |a_\alpha, a_\beta\rangle \langle a_\alpha, a_\beta| \quad (50)$$

$$= C_{mn}(a_i) |a_\alpha, a_\beta a_j\rangle \langle a_\alpha, a_\beta| \quad (51)$$

$$= |a_\alpha, a_\beta a_j + a_i a_\alpha\rangle \langle a_\alpha, a_\beta| \quad (52)$$

$$= D_n(a_j) |a_\alpha, a_\beta + a_j^{-1} a_i a_\alpha\rangle \langle a_\alpha, a_\beta| \quad (53)$$

$$= D_n(a_j) C_{mn}(a_j^{-1} a_i). \quad (54)$$

If $A \neq 0$, then

$$C_{mn}(a_i) C_{nm}(a_j) \quad (55)$$

$$= C_{mn}(a_i) C_{nm}(a_j) |a_\alpha, a_\beta\rangle \langle a_\alpha, a_\beta| \quad (56)$$

$$= C_{mn}(a_i) |a_\alpha + a_j a_\beta, a_\beta\rangle \langle a_\alpha, a_\beta| \quad (57)$$

$$= |a_\alpha + a_j a_\beta, a_\beta + a_i a_\alpha + a_i a_j a_\beta\rangle \langle a_\alpha, a_\beta| \quad (58)$$

$$= |a_\alpha + a_j a_\beta, A a_\beta + a_i a_\alpha\rangle \langle a_\alpha, a_\beta| \quad (59)$$

$$= D_n(A) |a_\alpha + a_j a_\beta, a_\beta + a_i A^{-1} a_\alpha\rangle \langle a_\alpha, a_\beta| \quad (60)$$

$$= D_n(A) C_{nm}(a_j) |A^{-1} a_\alpha, a_\beta + a_i A^{-1} a_\alpha\rangle \langle a_\alpha, a_\beta| \quad (61)$$

$$= D_n(A) C_{nm}(a_j) D_m(A^{-1}) |a_\alpha, a_\beta + a_i A^{-1} a_\alpha\rangle \langle a_\alpha, a_\beta| \quad (62)$$

$$= D_n(A) C_{nm}(a_j) D_m(A^{-1}) C_{mn}(a_i A^{-1}) \quad (63)$$

$$= D_n(A) D_m(A^{-1}) C_{nm}(a_j A) C_{mn}(a_i A^{-1}). \quad (64)$$

If $A = 0$, then

$$C_{mn}(a_i) C_{nm}(a_j) \quad (65)$$

$$= |a_\alpha + a_j a_\beta, a_i a_\alpha\rangle \langle a_\alpha, a_\beta| \quad (66)$$

$$= W_{mn} |a_i a_\alpha, a_\alpha + a_j a_\beta\rangle \langle a_\alpha, a_\beta| \quad (67)$$

$$= W_{mn} D_m(a_i) D_n(a_j) |a_\alpha, a_j^{-1} a_\alpha + a_\beta\rangle \langle a_\alpha, a_\beta| \quad (68)$$

$$= W_{mn} D_m(a_i) D_n(a_j) C_{mn}(a_j^{-1}), \quad (69)$$

where W_{mn} is the swap gate between the m -th qudit and the n -th qudit.

The proof of Eq. (19):

$$C_{mn}(a_i)C_{ml}(a_j) \quad (70)$$

$$= C_{mn}(a_i)C_{ml}(a_j)|a_\alpha, a_\beta, a_\gamma\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (71)$$

$$= C_{mn}(a_i)|a_\alpha, a_\beta, a_\gamma + a_j a_\alpha\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (72)$$

$$= |a_\alpha, a_\beta + a_i a_\alpha, a_\gamma + a_j a_\alpha\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (73)$$

$$= C_{ml}(a_j)|a_\alpha, a_\beta + a_i a_\alpha, a_\gamma\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (74)$$

$$= C_{ml}(a_j)C_{mn}(a_i). \quad (75)$$

The proof of Eq. (20):

$$C_{mn}(a_i)C_{ln}(a_j) \quad (76)$$

$$= C_{mn}(a_i)C_{ln}(a_j)|a_\alpha, a_\beta, a_\gamma\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (77)$$

$$= C_{mn}(a_i)|a_\alpha, a_\beta + a_j a_\gamma, a_\gamma\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (78)$$

$$= |a_\alpha, a_\beta + a_j a_\gamma + a_i a_\alpha, a_\gamma\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (79)$$

$$= C_{ln}(a_j)|a_\alpha, a_\beta + a_i a_\alpha, a_\gamma\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (80)$$

$$= C_{ln}(a_j)C_{mn}(a_i). \quad (81)$$

The proof of Eq. (21):

$$C_{mn}(a_i)C_{nl}(a_j) \quad (82)$$

$$= C_{mn}(a_i)C_{nl}(a_j)|a_\alpha, a_\beta, a_\gamma\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (83)$$

$$= C_{mn}(a_i)|a_\alpha, a_\beta, a_\gamma + a_j a_\beta\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (84)$$

$$= |a_\alpha, a_\beta + a_i a_\alpha, a_\gamma + a_j a_\beta\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (85)$$

$$= C_{nl}(a_j)|a_\alpha, a_\beta + a_i a_\alpha, a_\gamma - a_i a_j a_\alpha\rangle\langle a_\alpha, a_\beta, a_\gamma|_{mnl} \quad (86)$$

$$= C_{nl}(a_j)C_{mn}(a_i)C_{ml}(-a_i a_j). \quad (87)$$

Quantum circuit based on controlled gates. Since a controlled gate can generate a two-qudit maximally entangled state, and a two-qudit gate is enough to entangle a complex quantum circuit, a natural generalization is to apply the controlled gates to generate many-qudit maximally entangled state by a quantum circuit.

A quantum circuit based on the controlled gates $C_{mn}(a_k)$ is an N -qudit circuit with a series of controlled gates operating on, see an example as shown in Fig. 3. Up to local unitaries, a general N qudit ($d = p^m$) state generated by a quantum circuit is

$$|G\rangle = \prod_{\tau} C_{m_\tau n_\tau}(b_\tau) \otimes_i |c_i\rangle_i, \quad (88)$$

where $c_i \in \{s, 0\}$, $b_\tau \in F_{d^m}$, $\tau \in \{1, 2, \dots, M\}$ with M being the number of the controlled gates, and $(m_\tau, n_\tau) \in \{1, 2, \dots, N\}$.

A central problem is to investigate the possible types of entangled states through a series of the above controlled operations with some given initial states. The difficulties in simplifying the circuit lies in the facts that the number of controlled gates M may be very large, and these controlled gates do not commute with each other in general.

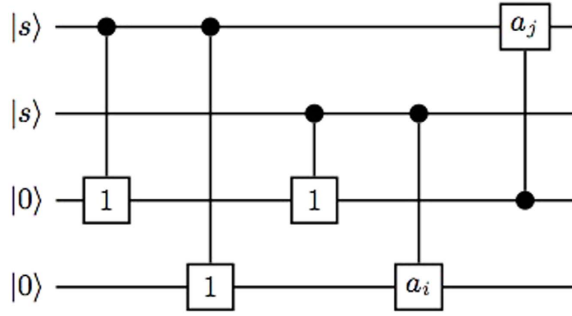


Figure 3. A quantum circuit to generate 4-qudit graph state.

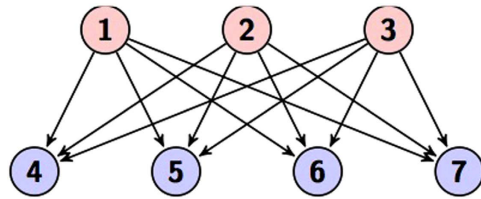


Figure 4. A bipartite graph state with $N=7$ and $S=\{1, 2, 3\}$, and the labels $\{b_{ij}\}$ are omitted.

Graph State on Finite Field

According to the initial state of an N -qudit circuit state in Eq. (88), we divide the N qudits into two sets: the set of qudits with the initial state $|s\rangle$ and the set of qudits with the initial state $|0\rangle$, denoted as S and O respectively. The sets could be empty. Now we introduce a standard form of N -qudit graph state on finite field as

$$\prod_{i \in S, j \in O} C_{ij}(b_{ij})|S\rangle, \tag{89}$$

where $b_{ij} \in F_d$, and

$$|S\rangle = \otimes_{i \in S} |s\rangle_i \otimes_{j \in O} |0\rangle_j. \tag{90}$$

This state is called a graph state because all the controlled gates in the circuit commute, and it can be represented as a directed bipartite graph. An example of a graph state for $N=7$ and the set $S=\{1, 2, 3\}$ is demonstrated in Fig. 4.

One of our central results is the following theorem:

Theorem 1 Any state in Eq. (88) is equivalent to the standard form in Eq. (89) up to local unitary transformations and particle permutations.

A direct way to prove the above theorem is to show a state in the standard form under the action of any generalized CNOT gate will still be a standard one. More precisely, we only need to show

$$C_{mn}(a_r) \prod_{i \in S, j \in O} C_{ij}(b_{ij})|S\rangle = W \prod_{k=1}^N D(c_k) \prod_{i \in S, j \in O} C_{ij}(d_{ij})|S\rangle, \tag{91}$$

where $m, n \in \{1, 2, \dots, N\}$, $a_r, b_{ij}, c_k, d_{ij} \in F_d$ and the SWAP gate W represents an arbitrary particle permutations. It can be proved by directly applying the commutation relations given in the last section. As the proof is long, we give another more concise proof.

Proof. Let the initial state $|S\rangle$ be $|s\rangle^{\otimes k} |0\rangle^{\otimes (N-k)}$ with $k \in [1, N-1]$. Using (6) we can show that $C_{mn}(a_r) |0, s\rangle = |0, s\rangle$ for any $a_r \in F_d$. It follows from (88) that up to local unitaries any graph state can be expressed as

$$\begin{aligned} |G\rangle &= \left(\prod_{\alpha=1}^M C_{m_\alpha n_\alpha}(b_\alpha) \right) \left(d^{-k/2} \sum_{j_1, \dots, j_k} |a_{j_1}, \dots, a_{j_k}\rangle |0\rangle^{\otimes (N-k)} \right) \\ &= d^{-k/2} \sum_{j_1, \dots, j_k} \left| \sum_{i=1}^k c_{i,1} a_{j_i} \right\rangle \otimes \dots \otimes \left| \sum_{i=1}^k c_{i,N} a_{j_i} \right\rangle, \end{aligned} \tag{92}$$

where $c_{i,q} \in F_d$ is the linear combination of b_α by (6). The $k \times N$ matrix $[c_{i,q}]$ has the same rank as that of $[I_k, 0]$, because the former is obtained from the latter via the operation $\prod_{\alpha=1}^M C_{m_\alpha n_\alpha}(b_\alpha)$. So $[c_{i,q}]$ has rank k . Up to the

permutation of vertices, we may assume that the first k column vectors in $[c_{i,q}]$ are linearly independent. The last $N - k$ column vectors in $[c_{i,q}]$ are the linear combinations of them. Let $b_{1,1}, \dots, b_{k,N} \in \mathbb{F}_d$ be the coefficients in the linear combination. From (92) we have

$$\begin{aligned} |G\rangle &= \prod_{j=1}^k \prod_{l=k+1}^N C_{j,l}(b_{j,l}) d^{-k/2} \sum_{j_1, \dots, j_k} \left| \sum_{i=1}^k c_{i,1} a_{j_i} \right\rangle_1 \otimes \dots \otimes \left| \sum_{i=1}^k c_{i,k} a_{j_i} \right\rangle_k \\ &\quad \otimes |0\rangle_{k+1} \otimes \dots \otimes |0\rangle_N \\ &= \prod_{j=1}^k \prod_{l=k+1}^N C_{j,l}(b_{j,l}) |s\rangle^{\otimes k} |0\rangle^{\otimes (N-k)}. \end{aligned} \tag{93}$$

The second equality follows from the fact that $\prod_{\alpha=1}^k C_{m_{\alpha} n_{\alpha}}(b_{\alpha}) |s\rangle^{\otimes k} = |s\rangle^{\otimes k}$ for any gate $\prod_{\alpha=1}^k C_{m_{\alpha} n_{\alpha}}(b_{\alpha})$ and any $b_{\alpha} \in \mathbb{F}_d$. Hence we can generate $|G\rangle$ by performing the gate $\prod_{j=1}^k \prod_{l=k+1}^N C_{j,l}(b_{j,l})$ on the initial state $|s\rangle^{\otimes k} |0\rangle^{\otimes (N-k)}$. The time order of $C_{j,l}(b_{j,l})$ in the gate is random, because they commute. This completes the proof. \square

The main conclusion from the above theorem is that up to local unitary transformations and particle permutations all the states generated by the controlled gate circuit are the directed bipartite graph states, and the graph contains only the edges from $|s\rangle$ to $|0\rangle$, which greatly simplifies our investigations on possible types of entanglement created by the controlled gate circuit.

The dual graph state for the graph state specified by Eqs (89) and (90) is

$$\prod_{i \in O, j \in S} C_{ij}(b_{ji}) |O\rangle, \tag{94}$$

where

$$|O\rangle = \otimes_{i \in O} |s\rangle_i \otimes_{j \in S} |0\rangle_j. \tag{95}$$

Theorem 2. *The two graph states given in Eqs (89) and (94) for two dual graphs are local unitary equivalent.*

Proof. For a finite field with $d = p^n$ and p a prime, the element is represented as $a = \sum_{i=0}^{n-1} a_i \alpha^i$, where a_i are F_p elements, represented by integers modulo p , i.e., $a_i \in \{0, 1, \dots, p - 1\}$ and α is one root of the equation for an irreducible polynomial of degree n over the finite field with cardinality p . For example, when $p = 3$ and $n = 2$, the corresponding irreducible polynomial may be taken as $x^2 + x + 2$, α is one root of $x^2 + x + 2 = 0$, and any element in the field with cardinality 9 is represented as $a_0 + a_1 \alpha$ with $a_0, a_1 \in \{0, 1, 2\}$. When α^i is regarded as the bases, the element in the finite field can be denoted as a vector \vec{a} . Then we introduce the discrete Fourier transformation of the states $|a\rangle$ as

$$|\vec{b}\rangle' = \frac{1}{\sqrt{d}} \sum_{\vec{a}} \omega^{\vec{a} \cdot \vec{b}} |\vec{a}\rangle, \tag{96}$$

where

$$\omega = e^{i \frac{2\pi}{p}}, \tag{97}$$

$$\vec{a} \cdot \vec{b} = \sum_{i=0}^{n-1} a_i b_i \pmod{p}. \tag{98}$$

Therefore we define the Hadamard transformation as

$$H = \sum_{\vec{b}} |\vec{b}\rangle' \langle \vec{b}| = \frac{1}{\sqrt{d}} \sum_{\vec{a}, \vec{b}} \omega^{\vec{a} \cdot \vec{b}} |\vec{a}\rangle \langle \vec{b}|. \tag{99}$$

Then

$$C_{mn}(\vec{d}) = \sum_{\vec{a}, \vec{b}} |\vec{a}\rangle \langle \vec{a}| \otimes |\vec{b} + \vec{d}\vec{a}\rangle \langle \vec{b}|. \tag{100}$$

Therefore

$$H_n C_{mn}(\vec{d}) H_n^\dagger = \sum_{\vec{a}, \vec{b}} \omega^{\vec{d}\vec{a} \cdot \vec{b}} |\vec{a}, \vec{b}\rangle \langle \vec{a}, \vec{b}|. \tag{101}$$

Let $\alpha^j (\alpha^k)$ with $k \in \{0, 1, \dots, n - 1\}$ and $j \in \{0, 1, \dots, 2 * (n - 1)\}$ denote the coefficient of term α^k in the expression α^j . Then we have

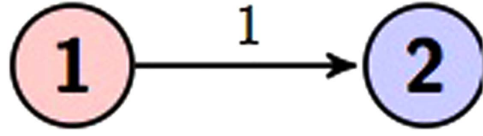


Figure 5. Two qudit graph.

$$\begin{aligned} \vec{d}\vec{a} \cdot \vec{b} &= \sum_{i,j,k} d_i a_j b_k \alpha^{i+j} (\alpha^k) \\ &= \sum_{i,j,k} d_i a_j b_k \alpha^{i+j+(n-1-j-k)} (\alpha^{k+(n-1-j-k)}) \\ &= \sum_{i,j,k} d_i a_j b_k \alpha^{i+(n-1-k)} (\alpha^{n-1-j}) \\ &= \vec{d}\vec{b}' \cdot \vec{a}', \end{aligned}$$

where

$$b'_{n-1-k} = b_k, \tag{102}$$

$$a'_{n-1-j} = a_j. \tag{103}$$

So we introduce local unitary transformation

$$V|\vec{a}\rangle = |\vec{a}'\rangle. \tag{104}$$

Therefore we have

$$\begin{aligned} &H_m^\dagger V_m V_n H_n C_{nm}(\vec{d}) H_n^\dagger V_n^\dagger V_m^\dagger H_m \\ &= H_m^\dagger V_m V_n \sum_{\vec{a}, \vec{b}} \omega^{\vec{d}\vec{b}' \cdot \vec{a}'} |\vec{a}, \vec{b}\rangle \langle \vec{a}, \vec{b}| V_n^\dagger V_m^\dagger H_m \\ &= H_m^\dagger \sum_{\vec{a}, \vec{b}} \omega^{\vec{d}\vec{b}' \cdot \vec{a}'} |\vec{a}', \vec{b}'\rangle \langle \vec{a}', \vec{b}'| H_m \\ &= H_m^\dagger \sum_{\vec{a}, \vec{b}} \omega^{\vec{d}\vec{b}' \cdot \vec{a}'} |\vec{a}, \vec{b}\rangle \langle \vec{a}, \vec{b}| H_m \\ &= \sum_{\vec{a}, \vec{b}} |\vec{a} + \vec{d}\vec{b}, \vec{b}\rangle \langle \vec{a}, \vec{b}| \\ &= C_{nm}(\vec{d}). \end{aligned} \tag{105}$$

In addition,

$$V_n H_n |0\rangle_n = |s\rangle_n, \tag{106}$$

$$H_m^\dagger V_m |s\rangle_m = |0\rangle_m. \tag{107}$$

Therefore we have

$$\otimes_{m \in S} H_m^\dagger V_m \otimes_{n \in O} V_n H_n \prod_{i \in S, j \in O} C_{ij}(b_{ij}) |S\rangle = \prod_{i \in O, j \in S} C_{ij}(b_{ji}) |O\rangle. \tag{108}$$

This completes our proof. □

This theorem implies that we can restrict ourselves in the cases where the cardinality of S is less than or equal to the cardinality of O , i.e. $[N/2]$.

Now let us apply the above theorems to study the possible types of entanglement generated by the controlled gates for $N=3, 4, 5$ with the help of Eqs (15) and (16). There is only one type of two qudit graph state, which is the qudit Bell state in Fig. 5. Note that if we replace 1 by a finite field element a_k , then we can convert the resulting state into the state by the element 1 using local unitary operations $D(a_m)$. Mathematically, Theorem 1 says that we need to investigate the state $\prod_{i \in S, j \in O} C_{ij}(b_{ij}) |S\rangle$, where $b_{ij} \in F_d$ and $|S\rangle = |s, s\rangle, |s, 0\rangle$ or $|0, 0\rangle$. It is easy to see that the state is a product state unless $|S\rangle = |s, 0\rangle$. In this case, the state becomes the qudit Bell state $\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |a_j, a_j\rangle$.

Similar arguments show that there is also one type of three qudit graph state, which is a generalized GHZ state in Fig. 6:

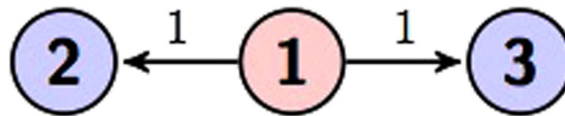


Figure 6. Three qudit graph.

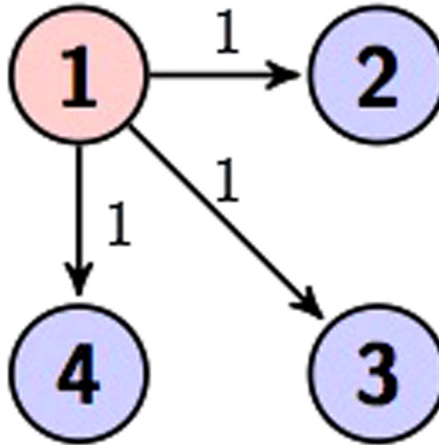


Figure 7. Four qudit graph states.

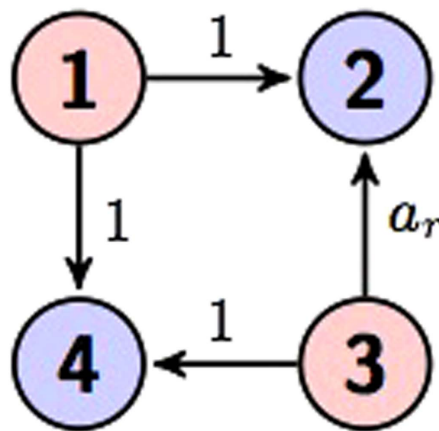


Figure 8. Four qudit graph states.

There are two types of four qudit graph states. One is four qudit GHZ state in Fig. 7. The other type in Fig. 8 has a more fruitful configuration, which will be studied in next section. As proved in Theorem 1, any graph state, say the generalized cluster state illustrated by a line connecting all vertices is locally equivalent to one of the types.

There are also two types of five qudit graph states in Figs 9 and 10.

Entanglement Properties of Qudit Graph States

In this section we study the maximal entanglement of graph states defined in previous sections. The state in Fig. 8 can be written as

$$|\psi(a_r)\rangle = d^{-1} \sum_{i,k} |a_i, a_i + a_r a_k, a_k, a_i + a_k\rangle, \tag{109}$$

where $a_r \in F_d$, the dimension $d = p^n$ with a prime p and positive integer n . We have

Lemma 1. $|\psi(a_r)\rangle$ is a maximally entangled state when $a_r \in F_d \setminus \{a_0, a_1\}$.

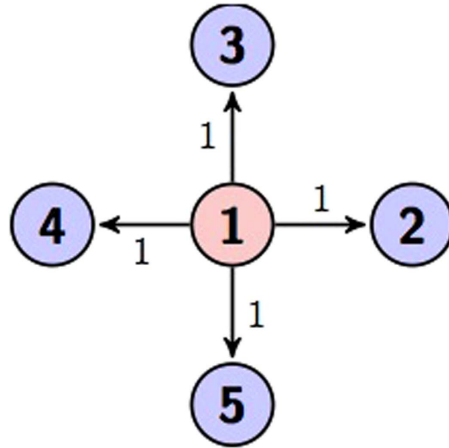


Figure 9. Five qudit graph states.

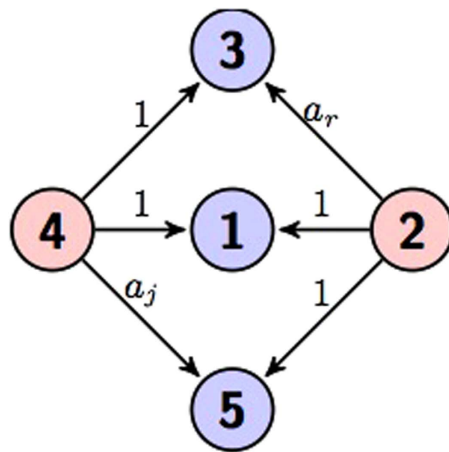


Figure 10. Five qudit graph states.

Proof. Since F_d is a field and $a_r \in F_d \setminus \{a_0, a_1\}$, we have $F_d = a_r F_d = a_i + F_d$ for any $a_i \in F_d$. So $|a_i, a_i + a_r a_k\rangle$ is an o. n. basis in $\mathbb{C}^d \otimes \mathbb{C}^d$. One can similarly verify that all three bipartite reduced density operators of $|\psi(a_r)\rangle$ respectively w. r. t. the bipartitions 12:34, 13:24 and 14:23 are maximally mixed states. It implies that the bipartition between one particle and other three particles is a bipartite Bell state. So $|\psi(a_r)\rangle$ is a maximally entangled state. \square

If $n = 1$ then d is a prime number. This case has been studied in¹² and is a special case of the lemma. The case $d = 2$ is excluded in the lemma, and it coincides with the known result that 4-qubit maximally entangled state does not exist². we demonstrate them by a simple example. We set $a_r = 2, a_j = j$ and $d = 4$ in (109), and obtain

$$\begin{aligned}
 |\psi(2)\rangle = & \frac{1}{4}(|0000\rangle + |0211\rangle + |0322\rangle + |0133\rangle \\
 & + |1101\rangle + |1310\rangle + |1223\rangle + |1032\rangle \\
 & + |2202\rangle + |2013\rangle + |2120\rangle + |2331\rangle \\
 & + |3303\rangle + |3112\rangle + |3021\rangle + |3230\rangle),
 \end{aligned}
 \tag{110}$$

by using the computation rule in Table 1. On the other hand, Lemma 1 does not hold when d is replaced by any integer which is not a prime power.

Next we give an example of maximal entanglement beyond the primer-power dimension. The state

$$|P'\rangle = d^{-1} \sum_{i,k} |i, i - k, k, i + k\rangle
 \tag{111}$$

appeared in¹², in which d was considered as a prime number. We point out that the state can be defined for any integer d . One can straightforwardly show that $|P'\rangle$ is a maximally entangled state for any odd $d \geq 3$, and is not a maximally entangled state for any even $d > 1$. The two families of states $|\psi(a_r)\rangle$ and $|P'\rangle$ show that 4-partite maximally entangled states are universal in high dimensional spaces. Indeed we have

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0
×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Table 1. The two tables respectively account for the addition and multiplication operations for F_4 . The proof of Lemma 1 also holds when F_d is replaced by any finite domain, because it coincides with the finite field.

Theorem 3. *The maximally entangled 4-partite pure state exists when the dimension d is an odd number at least three, or a multiple of four.*

Proof. The state $|P\rangle$ validates the assertion when d is an odd number at least three. So the first assertion holds. It remains to prove the second assertion when d is a multiple of four. We may assume $d = 2^m \prod_{j=1}^k p_j$ where $m \geq 2, k \geq 0$, and $p_j \geq 3$ are prime numbers. The first assertion implies that the maximally entangled state with every system of dimension p_j exists. Let the state be $|\psi_j\rangle$ on the system $A_j B_j C_j D_j$ such that $\dim \mathcal{H}_{A_j} = \dim \mathcal{H}_{B_j} = \dim \mathcal{H}_{C_j} = \dim \mathcal{H}_{D_j} = p_j$. Lemma 1 implies that the maximally entangled state with every system of dimension 2^m exists. Let the state be $|\varphi\rangle$ on the system $A_0 B_0 C_0 D_0$ such that $\dim \mathcal{H}_{A_0} = \dim \mathcal{H}_{B_0} = \dim \mathcal{H}_{C_0} = \dim \mathcal{H}_{D_0} = 2^m$. We combine the corresponding above systems to obtain a new 4-partite system $ABCD$, i.e.,

$$A = A_0 A_1 \cdots A_k, \tag{112}$$

$$B = B_0 B_1 \cdots B_k, \tag{113}$$

$$C = C_0 C_1 \cdots C_k, \tag{114}$$

$$D = D_0 D_1 \cdots D_k. \tag{115}$$

Now we construct a new 4-partite pure state $|\psi\rangle_{ABCD}$ via the tensor product of corresponding states as follows

$$|\psi\rangle_{ABCD} = |\varphi\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle. \tag{116}$$

Since $|\varphi\rangle$ and the $|\psi_i\rangle$'s are all maximally entangled states, $|\psi\rangle_{ABCD}$ is the maximally entangled state of system dimension d . Since d is a multiple of four, the second assertion holds. \square

The above proof indeed shows an analytical way of constructing the 4-partite maximally entangled states in designated dimensions. In spite of the above results, we do not have any example of 4-partite maximally entangled state with dimension equal to the multiple of two and any positive odd number. We conjecture they might not exist. This is true when the odd number is one². So the first challenge is to construct a 4-partite maximally entangled state with dimension 6. It easily reminds us of the construction of mutually unbiased basis of dimension 6, which is a long-standing problem in quantum physics.

Finally as a more independent interest, we construct the connection between maximal entanglement and the entropy problem recently proposed in¹⁹. The problem asks to construct (or exclude the existence of) a tripartite quantum state ρ_{ABC} such that $\text{rank} \rho_{AB} > \text{rank} \rho_{AC} \cdot \text{rank} \rho_{BC}$. The problem turns out to be hard and constructing the connection might be helpful to finding out its solution.

Lemma 2. *Let ρ_{ABC} be a tripartite state whose bipartite reduced density matrices are all maximally mixed states $\frac{1}{d^2} I_d \otimes I_d$. Then*

- (i) ρ_{ABC} exists and $\text{rank} \rho_{ABC} \geq d$.
- (ii) The maximally entangled 4-partite pure state exists if and only if there is a ρ_{ABC} such that $\text{rank} \rho_{ABC} = d$.

Proof. (i) A trivial example is $\rho_{ABC} = \frac{1}{d^3} I_d \otimes I_d \otimes I_d$. Let $|\psi\rangle_{ABCD}$ be the purification of ρ_{ABC} . Then $\text{rank} \rho_{AB} = \text{rank} \rho_{CD} = d^2 \leq \text{rank} \rho_C \text{rank} \rho_D$. Since $\text{rank} \rho_C = d$, we have $\text{rank} \rho_{ABC} = \text{rank} \rho_D \geq d$.

(ii) We prove the “if” part. Suppose there is a tripartite state ρ_{ABC} of rank d , whose bipartite reduced density matrices are all maximally mixed states $\frac{1}{d^2}I_d \otimes I_d$. Let $|\psi\rangle_{ABCD}$ be the purification of ρ_{ABC} . So $|\psi\rangle_{ABCD} \in \mathcal{H}$ is maximally entangled. The “only if” part can be similarly proved. This completes the proof. \square

Conclusions

We have constructed multipartite graph states with prime-power dimension using the generalized CNOT quantum circuit. We have proven that the graphs states are equivalent to a simple and operational standard form up to local unitary transformations and particle permutations. We also showed that some graph states are multipartite maximally entangled states, and that 4-partite maximally entangled states exist when the dimension is an odd number at least three or a multiple of four. The next question is to study graph states defined by generalized controlled-phase gates. Another problem is to quantify the entanglement of these graphs states in terms of multipartite entanglement measures, such as the geometric measure of entanglement and relative entropy of entanglement. Constructing the potential link between maximal entanglement and the mutually unbiased basis for dimension six may be a long-term goal of receiving more attention.

References

1. Facchi, P., Florio, G., Parisi, G. & Pascazio, S. Maximally multipartite entangled states. *Phys. Rev. A* **77**, 060304 (2008).
2. Gour, G. & Wallach, N. R. All maximally entangled four-qubit states. *J. Math. Phys.* **51**, 112201 (2010).
3. de Vicente, J. I., Spee, C. & Kraus, B. Maximally entangled set of multipartite quantum states. *Phys. Rev. Lett.* **111**, 110502 (2013).
4. Briegel, H. J. & Raussendorf, R. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.* **86**, 910–913 (2001).
5. Raussendorf, R. & Briegel, H. J. A one-way quantum computer. *Phys. Rev. Lett.* **86**, 5188–5191 (2001).
6. Zhou, D. L., Zeng, B., Xu, Z. & Sun, C. P. Quantum computation based on d-level cluster state. *Phys. Rev. A* **68**, 062303 (2003).
7. Menicucci, N. C. *et al.* Universal quantum computation with continuous-variable cluster states. *Phys. Rev. Lett.* **97**, 110501 (2006).
8. McKague, M. Self-testing graph states. *arXiv: quant-ph/1010.1989* (2010).
9. Eisert, J. & Briegel, H. J. Schmidt measure as a tool for quantifying multiparticle entanglement. *Phys. Rev. A* **64**, 022306 (2001).
10. Zhu, H., Chen, L. & Hayashi, M. Additivity and non-additivity of multipartite entanglement measures. *New J. Phys.* **12**, 083002 (2010).
11. Hajdudsek, M. & Murao, M. Direct evaluation of pure graph state entanglement. *New J. Phys.* **15**, 013039 (2013).
12. Gaeta, M., Klimov, A. & Lawrence, J. Maximally entangled states of four nonbinary particles. *Phys. Rev. A* **91**, 012332 (2015).
13. Cui, S. X., Yu, N. & Zeng, B. Generalized Graph States Based on Hadamard Matrices. *arXiv: quant-ph/1502.07195* (2015).
14. Schlingemann, D. & Werner, R. F. Quantum error-correcting codes associated with graphs. *Phys. Rev. A* **65**, 012308 (2001).
15. Brell, C. G. Generalized cluster states based on finite groups. *New J. Phys.* **17**, 023029 (2015).
16. Bombin, H. & Delgado, M. A. M. Entanglement distillation protocols and number theory. *Phys. Rev. A* **72**, 032313 (2005).
17. Helwig, W. Absolutely Maximally Entangled Qudit Graph States. *arXiv: quant-ph/1306.2879* (2013).
18. Goyeneche, D., Alsina, D., Latorre, J. I., Riera, A. & Życzkowski, Z. Absolutely Maximally Entangled states, combinatorial designs and multi-unitary matrices. *arXiv: quant-ph/1506.08857* (2015).
19. Cadney, J., Huber, M., Linden, N. & Winter, A. Inequalities for the ranks of multipartite quantum states. *Linear Algebra Appl.* **452**, 153–171 (2014).

Acknowledgements

We thank Li Yu for pointing out refs 14 and 15, making useful comments on Fig. 7 and the conclusion. We also thank Markus Grassl for pointing out refs 17 and 18. LC was supported by the NSF of China (Grant No. 11501024), and the Fundamental Research Funds for the Central Universities (Grant Nos 30426401 and 30458601). DLZ was supported by NSF of China (Grants No. 11475254 and Grant No. 11175247) and NKBRSF of China (Grant Nos 2012CB922104 and 2014CB921202).

Author Contributions

L.C. prepared the abstract, introduction and D.L.Z. prepared all figures. All authors wrote and reviewed the main manuscript.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Chen, L. and Zhou, D. L. Graph states of prime-power dimension from generalized CNOT quantum circuit. *Sci. Rep.* **6**, 27135; doi: 10.1038/srep27135 (2016).



This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>