SCIENCE CHINA
Physics, Mechanics & Astronomy

• **Article** •

September 2014 Vol. 57 No. 9: 1712–1717
doi: 10.1007/s11433-014-5551-9

Universal quantum computation with qudits

LUO MingXing[1,2*] & WANG XiaoJun[3]

[1] *Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu 610031, China;*
[2] *State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), Beijing 100093, China;*
[3] *School of Electronic Engineering, Dublin City University, Dublin 9, Ireland*

Received December 4, 2013; accepted January 26, 2014; published online June 23, 2014

Quantum circuit model has been widely explored for various quantum applications such as Shors algorithm and Grovers searching algorithm. Most of previous algorithms are based on the qubit systems. Herein a proposal for a universal circuit is given based on the qudit system, which is larger and can store more information. In order to prove its universality for quantum applications, an explicit set of one-qudit and two-qudit gates is provided for the universal qudit computation. The one-qudit gates are general rotation for each two-dimensional subspace while the two-qudit gates are their controlled extensions. In comparison to previous quantum qudit logical gates, each primitive qudit gate is only dependent on two free parameters and may be easily implemented. In experimental implementation, multilevel ions with the linear ion trap model are used to build the qudit systems and use the coupling of neighbored levels for qudit gates. The controlled qudit gates may be realized with the interactions of internal and external coordinates of the ion.

universal qudit gate, qudit circuit, linear ion

PACS number(s): 03.67.Lx, 03.67.Ac, 79.70.+q

Citation: Luo M X, Wang X J. Universal quantum computation with qudits. Sci China-Phys Mech Astron, 2014, 57: 1712–1717, doi: 10.1007/s11433-014-5551-9

Quantum circuit model has been explored to undertake intractable computation tasks in regards to classical computers. The primary reason is that the quantum system possesses have different features such as entanglement or quantum correlation [1]. In comparison to the binary logic gates and Boolean algebra in the classical computation theory, the qubit gates and Pauli algebra are critical for the quantum computation based one the qubit system. However, the local qubit operations are not sufficient for synthesizing general global quantum evolutions. Thus some correlated operations are required to construct the universal quantum logic gates which are performed on a small and fixed number of qubits. Specially, global unitary transformations can be implemented using only two-qubit operation at each time [2–5], which has no analog result in the classical reversible logic. For example, three-bit gates are necessary to simulate all reversible Boolean functions [6].

The universal qubit logic may be extended the qudit logic [7–15], where the information unit is qudit system [16]. The qudit state in the d-dimensional state space may offer greater flexibility in the storage and processing of quantum information, such as improving the channel capacity [17,18], implementing special quantum gates [19–22], increasing the information security [23–28] and exploring different quantum features [29–34]. The qudit system has also been realized with different physical systems [35–38]. Unfortunately the previous schemes have had to control many freedoms in implementing the evolution of general qudit systems. The primitive qudit gates are more complex than the qubit counterparts be-

*Corresponding author (email: mxluo@home.swjtu.edu.cn)

cause of the control of all levels of one qudit system. Herein we present a set of one-qudit and two-qudit gates which are sufficient for the universal qudit computation. These gates are easily implemented using multilevel ions with the linear ion trap model. The controlling parameters are greatly reduced.

We present some primitive quidit gates. In addition we present the universal qudit circuit model for general qudit systems and the associated evolution. Included are the physical implementations of the universal qudit gates.

1 Primitive qudit gates

Let U_d be a d-dimensional transformation mapping a general qudit state to $|d-1\rangle$ such that

$$U_d(\alpha_0, \alpha_2, \cdots, \alpha_{d-1}) : \sum_{j=0}^{d-1} \alpha_j |j\rangle \mapsto |d-1\rangle. \tag{1}$$

Similar to the qubit case, U_d is not unique in terms of complex parameters $\alpha_0, \cdots, \alpha_{d-1}$. This problem has been addressed elsewhere [7] with probabilistic quantum search algorithm. Here, we define another deterministic unitary transformation to realize U_d with $d-1$ steps. In detail, U_d may be decomposed into

$$U_d = X_{d-1}(a_{d-1}, b_{d-1}) \cdots X_1(a_1, b_1), \tag{2}$$

with

$$X_j(x,y) = \begin{pmatrix} I_{j-1} & & & \\ & \frac{x}{\sqrt{|x|^2+|y|^2}} & \frac{-y}{\sqrt{|x|^2+|y|^2}} & \\ & \frac{y^*}{\sqrt{|x|^2+|y|^2}} & \frac{x^*}{\sqrt{|x|^2+|y|^2}} & \\ & & & I_{d-j-1} \end{pmatrix}, \tag{3}$$

and $a_j = \alpha_j, b_j = \sqrt{\sum_{i=0}^{j-1} \alpha_i^2}$. The new primitive transformations $X_j(x,y)$ in eq. (3) are easily implemented in physics with two freedoms such as the linear ion trap model and linear optics with multiport.

We define the d-dimensional phase gate Z_d as an operator

$$Z_d(\theta) = \sum_{j=0}^{d-1} \mathrm{e}^{\mathrm{i}(1-\mathrm{sgn}(d-1-j))\theta} |j\rangle\langle j|, \tag{4}$$

which alters the phase of $|d-1\rangle$ by θ without affecting other states in the qudit. The sgn denotes the sign function. This seemingly shows that $\{Z_d, X_d\}$ with $X_d = \{X_j(x,y)\}$ is sufficient to simulate all single-qudit unitary operations. Each primitive gate may be implemented by controlling no more than two complex parameters. This decomposition has greatly simplified the physical implementations of qudit gates. If R_d represents either X_d or Z_d, then the controlled-qudit gate is defined as:

$$C_2[R_d] = \begin{pmatrix} I_{d^2-d} & \\ & R_d \end{pmatrix} \tag{5}$$

acting on the two-qudit system. The identity operation I_{d^2-d} acts on the substates $|0\rangle|0\rangle, \cdots, |d-2\rangle|d-1\rangle$ while R_d acts on the remaining d substates $|d-1\rangle|0\rangle, \cdots, |d-1\rangle|d-1\rangle$ of one general two-qudit system. These gates are sufficient to construct unitary transformation of $SU(d^n)$ and proved in the next section.

2 Universal quantum qudit circuits

Herein we provide the primary result.

Theorem 1 The following qudit gates set

$$\Gamma = \{X_d, Z_d, C_2[R_d]\} \tag{6}$$

is universal for general quantum computation based on quantum circuit model.

To show the universality of Γ we have to address n-qudit operations in $SU(d^n)$. Consider an N-dimensional unitary transformation $U \in SU(d^n)$ acting on the n-qudit state. The following task is to synthesize U with Γ.

Denote the computation basis of n-qudit space $\mathbb{C}^{d^n}$ as:

$$|k\rangle = |k_1, k_2, \cdots, k_n\rangle, \quad k = 0, \cdots, d^n - 1. \tag{7}$$

$k_1, k_2, \cdots, k_n$ is the base-d representation of k and $|k_i\rangle$ denote the states of the ith qudit, $i = 1, \cdots, n$. The proof of Theorem 1 is completed by the following subsections.

2.1 Eigen-decomposition of *U*

The first step is eigen-decomposition of U. For $U \in SU(d^n)$ there exist $N = d^n$ different eigenstates $|E_j\rangle$ with corresponding eigenvalues $\mathrm{e}^{\mathrm{i}\lambda_j}$, $j = 1, 2, \cdots, d^n$. Each eigenstate is represented with the computation basis as:

$$\sum_{j=0}^{N-1} \alpha_j |j\rangle = \sum_{i_1, \cdots, i_n=0}^{d-1} \alpha_{i_1, \cdots, i_n} |i_1, i_2, \cdots, i_n\rangle \tag{8}$$

from special $\alpha_{i_1, \cdots, i_n}$. From the representation theory the unitary matrix U may be rewritten as:

$$U = \sum_{j=1}^{N} \mathrm{e}^{\mathrm{i}\lambda_j} |E_j\rangle\langle E_j| = \prod_{j=1}^{N} \Upsilon_j \tag{9}$$

with eigenoperators

$$\Upsilon_j = \sum_{s=1}^{N} \mathrm{e}^{\mathrm{i}(1-|\mathrm{sgn}(j-s)|)\lambda_s} |E_s\rangle\langle E_s|, \tag{10}$$

which generate a phase λ_j of $|E_j\rangle$ without affecting any other eigenstates, $j = 1, \cdots, N$.

Now the qudit decomposition of U is reduced to synthesize all the eigenoperators Υ_j. Notice that Υ_j can be decomposed with two basic transformations [7] as follows:

$$\Upsilon_j = U_{j,N}^{-1} Z_{j,N} U_{j,N}. \tag{11}$$

Here $U_{j,N}$ and $Z_{j,N}$ are the N-dimensional analogs of U_d and Z_d. $U_{j,N}$ transforms the jth eigenstate to $|N-1\rangle$, that is

$$U_{j,N}(\alpha_0,\cdots,\alpha_{N-1}): |E_j\rangle \mapsto |N-1\rangle \tag{12}$$

which is not unique. $Z_{j,N}$ changes the phase of $|N-1\rangle$ with the jth eigenphase λ_j, leaving other computation states unchanged, that is

$$Z_{j,N} = \sum_{s=0}^{N-1} \mathrm{e}^{\mathrm{i}(1-|\mathrm{sgn}(s-N+1)|)\lambda_j}|s\rangle\langle s|. \tag{13}$$

Combining eqs. (9)–(13) it follows that $\{Z_{j,N}, U_{j,N}\}$ is sufficient to decompose U. Similar to eq. (2) $U_{j,N}$ may be decomposed with primitive gates $X_{j,k}(x,y)$. Thus $X_{j,k}(x,y)$ and $Z_{j,N}$ are sufficient to decompose U.

2.2 Controlled decomposition of $U_{j,k}$ and $Z_{j,N}$

The second step is to realize the controlled decomposition of $X_{j,k}$ and $Z_{j,N}$, which are equivalent to decomposing $U_{j,k}$ and $Z_{j,N}$ in terms of multiple controlling circuits in the next subsection. For convenience denote $C_k[R_d]$ as:

$$C_k[R_d] = \begin{pmatrix} I_{d^k-d} & \\ & R_d \end{pmatrix}, \tag{14}$$

which acts on the d^k-dimension computation basis of k-qudit space. R_d acts on the last d substates $|d-1\rangle^{\otimes n-1}|0\rangle,\cdots,|d-1\rangle^{\otimes n-1}|d-1\rangle$ while others are unchanged. This controlled qudit operation transforms the last qudit system with R_d conditional on the first $k-1$ qudits being in $|d-1,\cdots,d-1\rangle$. Notice that $Z_{j,N} = C_n[Z_d(E_j)]$ from eq. (13). For $U_{j,N}$ we have

Proposition 1 Each $U_{j,N}$ can be decomposed into some combinations of $C_k[U_d]$ and $C_k[P_d]$.

The proof is shown in Appendix.

2.3 Primitive decomposition of $C_m[R_d]$

The third step is to complete the primitive decomposition of $C_m[R_d]$ using the two-qudit gates $C_2[R_d]$. Derived from the decomposition in ref. [7] one possible decomposition is illustrated in Figure 1 for $d>2$. This circuit uses $r=\lceil (m-2)/(d-2)\rceil$ auxiliary qudits ($\lceil x\rceil$ denotes the smallest integer greater than x), where k is the remainder of $(m-2)/(d-2)$. The box represents $C_2(P_d(p,q))$, and the controlled permutation of $|p\rangle$ and $|q\rangle$. The last box contains $R_d = Z_d$ or X_d. We want to combine all these gates to implement $C_m[R_d]$, which applies R_d to the mth qudit if and only if the first $m-1$ qudits are in $|d-1\rangle^{\otimes m-1}$.

From left to right in Figure 1, the first permutation $C_2[P_d(0,1)]$ increments the first auxiliary qudit from $|0\rangle$ to $|1\rangle$ if and only if the qudit 1 is in $|d-1\rangle$. The second permutation $C_2[P_d(1,2)]$ increments the first auxiliary qudit $m+1$ from $|1\rangle$ to $|2\rangle$ if and only if the qudit 2 is in $|d-1\rangle$, and so in sequence. Continuing this way, the first auxiliary qudit reaches $|d-1\rangle$ if and only if all the first $d-1$ qudits are in $|d-1\rangle$. This information is then transferred to the second auxiliary qudit using $C_2[P_d(0,1)]$ elevating $|0\rangle$ to $|1\rangle$ provided the first auxiliary qudit is in $|d-1\rangle$. This procedure is carried out sequentially through all the first $m-1$ qudits. Finally we get that the rth auxiliary qudit reaches to $|s\rangle$ (in the case where s is remainder of $(m-2)/(d-2)$). Controlled by the last qudit, $C_2[U_d]$ acts on the qudit m, which completes the simulation of $C_m[U_d]$. The two-qudit permutation gates $C_2[P_d(p,q)]$ are reapplied to the auxiliary qudits at the end to disentangle them from the first m qudits and restore them to $|0\rangle$ for reuse.

In fact, from the proof above we have obtained general quantum circuits for $C_m[U_d]$. It takes m numbers of $C_2[R_d]$. However, this method cannot be reduced to the qubit case. Another hybrid way may be used in general case, see Figure 2. Here, an md-level auxiliary state is used to register the controlling information.

Proposition 2

$$\Gamma_d := \{X_d, Z_d, C_2[R_d]\} \tag{15}$$

is universal for the quantum computation.

Proof It is sufficient to decompose all $U\in SU(N)$ with Γ_d. From the proof in sect. 2.2 U may be decomposed into the combinations of $U_{j,k}$ and $Z_{j,N}$. Then from eq. (6) and the circuits in Figures 1 and 2 U can be decomposed with Γ_d. This completes the proof that two-qudit gates $C_2[Z_d]$ and $C_2[X_d]$ together with the one-qudit gates Z_d and X_d are universal for the quantum computation.

3 Physical realizations

The qudit state may be realized with the linear iron in trap (see Figure 3). Our scheme is derived elsewhere [7]. However, our implementation is easy using few parameters. Let $\hat{a}^\dagger$ and $\hat{a}$ be the creation and annihilation operators for the center-of-mass mode, and $\hat{\sigma}_{jj} = |j\rangle\langle j|$ be the internal projection operators for a given d-level ion in the trap. The Hamiltonian for the ion in the absence of interaction fields is defined as:

$$\hat{H}_0 = \hbar\mu_x(\hat{a}^\dagger\hat{a}+\frac{1}{2}) + \sum \hbar\omega_j\hat{\sigma}_{jj}. \tag{16}$$

The computation scheme considered is shown in Figure 3, where the transition frequencies $\omega_{j,j+1} = |\omega_{j+1}-\omega_j|$ are distinct.

To implement $X_d(j,j+1)$ it is sufficient to couple the jth neighboring level with the $j+1$th level. The jth neighboring transition is driven by the near-resonant laser field with its standing-wave configuration along the trap axis,

$$\begin{aligned} \boldsymbol{E}(\hat{x},t) &= \boldsymbol{\epsilon}_{j,j+1}(E_{j,j+1}\mathrm{e}^{-\alpha_{j,j+1}t}+\text{c.c.})\cos(k_{j,j+1}\hat{x}+\varphi) \\ &= \boldsymbol{\epsilon}_{j,j+1}(E_{j,j+1}\mathrm{e}^{-\alpha_{j,j+1}t}+\text{c.c.})\Big[-\frac{\eta_{j,j+1}}{\sqrt{n}}(\hat{a}^\dagger+\hat{a})\sin(\varphi) \end{aligned}$$

$$+\cos(\varphi) + O(\eta_{j,j+1}^2)\Big]. \tag{17}$$

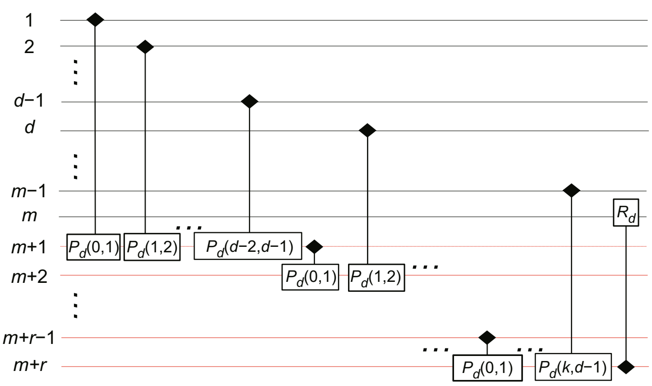

Figure 1 (Color online) Schematic circuit of $C_m[R_d]$ with $C_2[R_d]$. Horizontal lines denote qudits, with the black lines denoting m controlling qudits and the red lines denoting auxiliary qudits being initialized to $|0\rangle$. Vertical lines represent the two-qudit controlled gates, originating from the control qudit (which is required to be in $|d-1\rangle$ for the gate to apply) and terminating in a box on the target qudit.

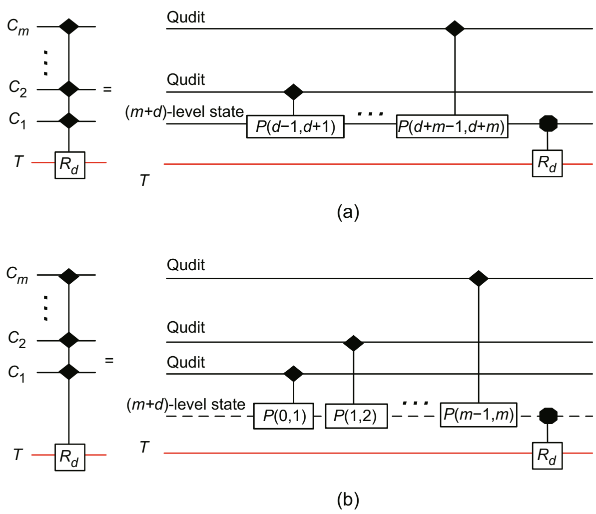

Figure 2 (Color online) Quantum circuit of multiple controlled qudit operations. Dashed line is an $(m+d)$-level auxiliary state. (a) Controlling state is $(m+d)$-level. (b) Auxiliary state is $(m+d)$-level.

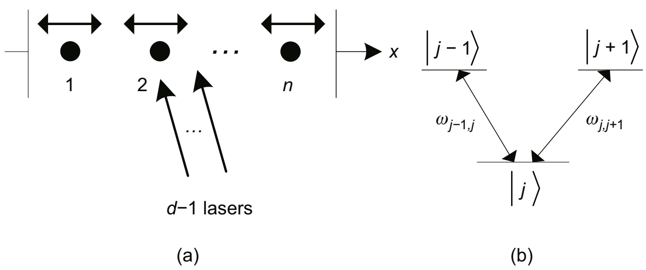

Figure 3 Iron implementation. (a) Linear ion trap, with n ions. Trap axis is along x. (b) Level scheme for a d-level ion, with one of neighboring transitions $\omega_{j-1,j}$ or $\omega_{j,j+1}$.

Here $E_{j,j+1}$ and $\alpha_{j,j+1}$ are the complex field amplitudes and field frequencies (respectively) corresponding to the atomic transitions, $\boldsymbol{\epsilon}_{j,j+1}$ and $k_{j,j+1}$ are the associated polarizations and wave vector components respectively. The new Hamiltonian is defined as:

$$\hat{H}_{\text{dip}} = -\left[\boldsymbol{d}_{j,j+1}\hat{\sigma}^{\dagger}_{j,j+1} + \boldsymbol{d}^{*}_{j,j+1}\hat{\sigma}^{\dagger}_{j,j+1}\right]\boldsymbol{E}(\hat{x},t). \tag{18}$$

Note that $\alpha_{j,j+1} = \omega_{j,j+1}$ if tunes the jth and $(j+1)$th lasers to the resonance. Thus H_{dip} is reduced to a time-independent interaction under the rotating-wave approximation, that is

$$\hat{H}_{\text{dip},v} = -\hbar\left[\Omega_{j,j+1}\hat{\sigma}^{\dagger}_{j,j+1} + \Omega^{*}_{j,j+1}\hat{\sigma}^{\dagger}_{j,j+1}\right] \tag{19}$$

with the Rabi frequency $\Omega_{j,j+1} = (\boldsymbol{d}_{j,j+1}\cdot\epsilon_{j,j+1}E_{j,j+1})/\hbar$. The unitary evolution operator is given as:

$$\hat{V} = \exp\left(-\mathrm{i}(t/\hbar)\hat{H}_{\text{dip},V}\right), \tag{20}$$

which is sufficient to generate the single-qudit gate X_d (up to an overall phase factor)

$$X_j = \begin{pmatrix} I_{j-1} & & \\ & Y_j & \\ & & I_{d-j-1}\end{pmatrix}, \tag{21}$$

with

$$Y_j = \begin{pmatrix} \cos|\Omega_{j,j+1}|t & \mathrm{i}e^{\mathrm{i}\phi_{j,j+1}}\sin|\Omega_{j,j+1}|t \\ \mathrm{i}e^{-\mathrm{i}\phi_{j,j+1}}\sin|\Omega_{j,j+1}|t & \cos|\Omega_{j,j+1}|t\end{pmatrix}.$$

Here, $\phi_{j,j+1}$ is the phase of $\Omega_{j,j+1}$. The phase flip Z_d may be realized by $Z_d = [U_d^{-1}L_dU_d]$ with general phase rotation $L_d = Z_d|_{|d-1\rangle}$, L_d is performed on the classical state $|d-1\rangle$. Moreover, the permutation $P_d(j, j+1)$ is also followed from eq. (21) for $|\Omega_{j,j+1}|t = \pi/2$ and $\phi_{j,j+1} = \pi/2$.

Consider the controlled-qudit gate $C_2[R_d]$. Detuning each laser above or below resonance by the trap frequency, $\alpha_{j,j+1} = \omega_{j,j+1} \pm \mu_x$, we find that

$$\hat{H}_{\text{dip},U_+} = -\frac{\eta_{j,j+1}\hbar}{\sqrt{q}}\left[\Omega_{j,j+1}\hat{\sigma}^{\dagger}_{j,j+1}\hat{a}^{\dagger} + \Omega^{*}_{j,j+1}\hat{\sigma}^{\dagger}_{j,j+1}\hat{a}\right],$$

$$\hat{H}_{\text{dip},U_-} = -\frac{\eta_{j,j+1}\hbar}{\sqrt{q}}\left[\Omega_{j,j+1}\hat{\sigma}^{\dagger}_{j,j+1}\hat{a}^{\dagger} + \Omega^{*}_{j,j+1}\hat{\sigma}^{\dagger}_{j,j+1}\hat{a}\right]. \tag{22}$$

Their time evolution operators are thus

$$\hat{U}_{\pm} = \exp\left(-\mathrm{i}(t/\hbar)\hat{H}_{\text{dip},U_{\pm}}\right), \tag{23}$$

which conditionally couple the internal and external coordinates of the ion. Thus $C_2[R_d]$ may be implemented using $\hat{U}_{\pm}$ and V interactions, and auxiliary d levels in each ion, see ref. [7] for detail. The primary difference is that only two parameters $\Omega_{j,j+1}$ and $\phi_{j,j+1}$ are required in implementation while $2d-2$ parameters should be controlled simultaneously for the qudit operations in ref. [7].

4 Discussions and conclusion

Let us consider a general unitary $U \in SU(N)$. From eq. (9) there are N eigenoperators Γ_j defined in eq. (10). Each is reduced to three global primitive rotations defined in eq. (11). Then from the proof of the Proposition 1, one $C_m[P_d]$ and $C_n[U_d]$ are used to eliminate $d-1$ substates of one eigenstate. Thus it requires no more than $3d^{n-1}$ multiple controlled operations to decompose $U_{j,N}$. Finally from the decomposition in Figure 1, m numbers of $C_2[R_d]$ or $C_2[P_d]$ are needed for $C_m[R_d]$ or $C_m[P_d]$ respectively. $C_2[U_d]$ may be further decomposed into $d-1$ numbers of $C_2[X_j]$ using eq. (2). Therefore, the total number of the primitive operations is given as:

$$L \leqslant 2N \times 3d^{n-1} \times n \times (d-2) + N \times n \leqslant 6nd^{2n} + nd^n \quad (24)$$

for a general n-qudit unitary operation. Of course, this bound may be reduced if one reconsiders the number of different $C_m[P_d]$ for $C_n[U_d]$.

One advantage of our qudit model is the logarithmic reduction in the number of separate quantum systems needed to span the quantum memory, that is, $k = \log_2 d$. Using a similar construction, we find that the circuit complexity of the qudit simulation is $O(nd^{2n})$ which is lower than that in ref. [7]. This represents an upper bound on the circuit complexity and shows $(\log_2 d)^2$ advantage over the qubit case. Of course, note that no logarithmic scaling in the global dimension N, which is natural in terms of the unitary parameterizing. This is similar to the qubit case, where special sparse unitary transformations (with sparse eigenoperator representations) admit efficient simulations in terms of the elementary qubit gates. In comparison to the proof in ref. [7], our primitive qudit gates are easy in physical implementations with few free parameters. Their scheme is dependent of the indeterministic qudit operation U_d with many free parameters. Of course, the detailed circuit in sect. 3 is also different. The other advantage of our qudit model is simplicity of primitive gates which are easily realizable in physics by controlling few parameters simultaneously.

Appendix

Proof of Proposition 1 The proof is completed by induction. For each eigenstate,

$$|E\rangle = \sum_{j=0}^{N-1} \hat{\alpha}_j |j\rangle = \sum_{i_1 \cdots i_n = 0}^{d-1} \alpha_{i_1,\cdots,i_n} |i_1, \cdots, i_n\rangle. \quad (a1)$$

Firstly, for the substate $\sum_{i_n=0}^{d-1} \alpha_{d-1,\cdots,d-1,i_n} |d-1\rangle^{\otimes n-1} |i_n\rangle$, using one multiple controlled qudit operation $C_n[U_d]$ defined in eq. (14) $|E\rangle$ is changed into a new state, that is

$$|E\rangle \mapsto \sum_{j=0}^{N-d-1} \hat{\alpha}_j |j\rangle + \beta_{N-1} |N-1\rangle. \quad (a2)$$

Here, the first $n-1$ qudits $|d-1\rangle^{\otimes n-1}$ is controlling term and $\beta_{N-1} = \sqrt{\sum_{j=0}^{d-1} |\alpha_{d-1,\cdots,d-1,j}|^2}$.

Secondly, using one multiple controlled permutation $C_{n-1}[P_d(i_{n-1}, d-1)] \otimes I_d$ the substate $\sum_{i_n=0}^{d-2} \alpha_{d-1,\cdots,d-1,i_{n-1},i_n} |d-1, \cdots, d-1, i_{n-1}, i_n\rangle$ of $|E\rangle$ in eq. (a2) is changed into $\sum_{i_n=0}^{d-2} \alpha_{d-1,\cdots,d-1,i_{n-1},i_n} |d-1, \cdots, d-1, d-1, i_n\rangle$ for each $i_{n-1} = 0, \cdots, d-1$. Here,

$$C_m[P_d(i_{n-1}, d-1)] = \begin{pmatrix} I_{d^m-d} & \\ & P_d(i_{n-1}, d-1) \end{pmatrix} \quad (a3)$$

is performed on the first m qudits, and so

$$P_d(j, d-1) = |j\rangle\langle d-1| + |d-1\rangle\langle j| + \sum_{i \neq j, d-1} |i\rangle\langle i|. \quad (a4)$$

Followed this transformation $C_n[U_d]$ is used to reduce the new substate, see Figure 1 with $k=1$. After these controlled operations for $i_{n-1} = d-1, \cdots, 0$ the eigenstate $|E\rangle$ is reduced to a new state, that is

$$|E\rangle \mapsto \sum_{i_1,\cdots,i_n=0, \prod_{j=1}^{n} i_j \neq (d-1)^{n-2}}^{d-1} \alpha_{i_1,\cdots,i_n} |i_1, \cdots, i_n\rangle + \tilde{\beta}_N |N-1\rangle \quad (a5)$$

with $\tilde{\beta}_N = \sqrt{\sum_{j_1,j_2=0}^{d-1} |\alpha_{d-1,\cdots,d-1,j_1,j_2}|^2}$. Here, the controlled permutation is not required for $i_{n-1} = d-1$.

Thirdly the reduction method above can be generalized to other substates by induction. Assume that one obtains the reduced eigenstate

$$|\hat{E}\rangle = \sum_{i_1,\cdots,i_n=0, i_1\cdots i_{k+1} \neq d^{k+1}}^{d-1} \alpha_{i_1,\cdots,i_n} |i_1, \cdots, i_n\rangle + \beta_N^* |N-1\rangle, \quad (a6)$$

then it can be further reduced to

$$\sum_{i_1,\cdots,i_n=0, \prod_{j=1}^{k} i_j \neq (d-1)^k}^{d-1} \alpha_{i_1,\cdots,i_n} |i_1, \cdots, i_n\rangle + \beta_N^{**} |N-1\rangle \quad (a7)$$

with one constant β_N^{**}. In detail, this step can be shown by induction.

a) $\sum_{i_n=0}^{d-2} \alpha_* |d-1\rangle^{k-1} |i_k\rangle |d-1\rangle^{n-k-1} |i_n\rangle$ of $|\hat{E}\rangle$ in eq. (a7) is changed into $\sum_{i_n=0}^{d-2} \alpha_{d-1,\cdots,d-1,i_n} |d-1, \cdots, d-1, i_n\rangle$ using the controlled permutation $C_{k+1}[P_d(i_k, d-1)] \otimes I_{d^{n-1-k}}$ for each $i_k = d-1, \cdots, 0$. Here α_* denote the corresponding coefficients of substates for convenience. Then one special $C_n[U_d]$ is used to complete the reduction task. After these operations for all $i_{n-1} = d-1, \cdots, 0$ the substate $\sum_{i_n=0}^{d-2} \alpha_* |d-1\rangle^{k-1} |i_k\rangle |d-1\rangle^{n-k-1} |i_n\rangle$ of $|\hat{E}\rangle$ is reduced to $\hat{\beta}_N |N-1\rangle$ with some constant $\hat{\beta}_N$.

b) $\sum_{i_n=0}^{d-2} \alpha_* |d-1\rangle^{k-1} |i_k\rangle |d-1\rangle^{n-k-2} |i_{n-1} i_n\rangle$ of $|\hat{E}\rangle$ for each $i_k, i_{n-1} = 0, \cdots, d-2$ may be changed into $\sum_{i_n=0}^{d-2} \alpha_* |d-1, \cdots, d-1, i_n\rangle$ using $[C_{n-1}[P_d(i_k, d-1)] \otimes I_{d^2}][C_{n-2}[P_d(i_{n-1}, d-1)] \otimes I_{d^3}]$. Here α_* denote the corresponding coefficients of substates for convenience. The controlling qudits are $1, \cdots, k-1, k+1, \cdots, n-2$ while $1, \cdots, k-1, k+1, \cdots, n-1$ for the second. These controlled

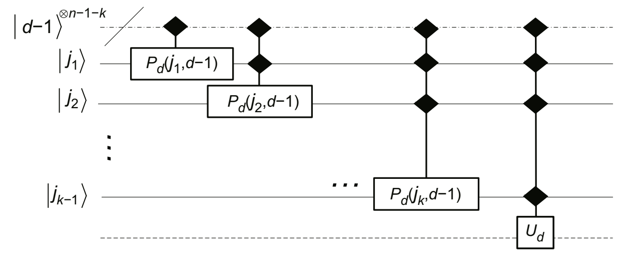

Figure a1 Schematic quantum circuit of substates' reduction. Dash-dot line denotes the combination of first $n-1-k$ qudits as $|d-1\rangle^{\otimes n-1-k}$. Dash line denotes the nth qudit as $\sum_{i_n=0}^{d-2}|i_n\rangle$. $P_d(s,t)$ denotes the permutation operation of $|s\rangle$ and $|t\rangle$. Substate is $\sum_{i_n=0}^{d-2}\alpha_{d-1,\cdots,d-1,j_1,\cdots,j_k,i_n}|d-1,\cdots,d-1,j_1,\cdots,j_k,i_n\rangle+\beta|d-1\rangle^{\otimes n}$ for each $j_1,\cdots,j_k=0,\cdots,d-2$.

operations can be easily implemented by permuting the particles in implementations. Then a new reduced substate is followed using another $C_n[U_d]$.

c) Assume that the substate $\sum_{i_k,i_{n-s+1},\cdots,i_n=0}^{d-1}\alpha_*|d-1,\cdots,d-1,i_k,d-1,\cdots,d-1,i_{n-s+1},\cdots,i_{n-1},i_n\rangle$ of $|E\rangle$ has been reduced to $|N-1\rangle$ using some controlled operations $C_m[P_d]\otimes I_{d^3}$ and $C_n[U_d]$. The substate $\sum_{i_n=0}^{d-1}\alpha_*|d-1,\cdots,d-1,i_k,d-1,\cdots,d-1,i_{n-s+1},\cdots,i_{n-1},i_n\rangle$ of $|\hat{E}\rangle$ may be reduced to $c|N-1\rangle$ with some constant c because it is changed into $\sum_{i_n=0}^{d-1}\alpha_{d-1,\cdots,d-1,i_n}|d-1,\cdots,d-1,i_n\rangle$ using multiple controlled permutations $[C_{n-1}[P_d(i_k,d-1)]\otimes I_{d^2}][C_{n-2}[P_d(i_{n-s},d-1)]\otimes I_{d^3}]\cdots[C_{n-s+1}[P_d(i_{n-1},d-1)]\otimes I_{d^3}]$, see Figure a1 with arranged order of qudits. The new substate may be reduced from another $C_n[U_d]$. Thus we have completed the proof for this step.

Finally when $k=1$, the eigenstate $|E\rangle$ is reduced to $|d-1\rangle^{\otimes n}$.

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61303039 and 11226336), the Fundamental Research Funds for the Central Universities (Grant No. 2682014CX095) and the Science Foundation Ireland (SFI) under the International Strategic Cooperation Award Grant Number SFI/13/ISCA/2845.

1 Nielsen M A, Chuang I S. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000. 50–100
2 DiVincenzo D P. Two-bit gates are universal for quantum computation. Phys Rev A, 1995, 51: 1015–1022
3 Sleator T, Weinfurter H. Realizable universal quantum logic gates. Phys Rev Lett, 1995, 74: 4087–4090
4 Barenco A. A universal two-bit gate for quantum computation. Proc R Soc London Ser A, 1995, 449: 679–683
5 Barenco A, Bennett C H, Cleve R, et al. Elementary gates for quantum computation. Phys Rev A, 1995, 52: 3457–3467
6 Toffoli T. Reversible computing. Lect Notes Comput Sci, 1980, 84: 632–644
7 Muthukrishnan A, Stroud Jr C R. Multivalued logic gates for quantum computation. Phys Rev A, 2000, 62: 052309
8 Brennen G K, O'Leary D P, Bullock S S. Criteria for exact qudit universality. Phys Rev A, 2005, 71: 052318
9 Brylinski J L, Brylinski R. Universal quantum gates. In: Brylinski R K, Chen G, eds. Mathematics of Quantum Computation. Boca: Chapman & Hall/CRC Press, 2002. 99–113
10 Daboul J, Wang X, Sanders B C. Quantum gates on hybrid qudits. J Phys A-Math Gen, 2003, 36: 2525
11 Brennen G K, Bullock S S, O'Leary D P. Efficient circuits for exact-universal computationwith qudits. Quantum Inf Comput, 2006, 6: 436–454
12 Zhou D L, Zeng B, Xu Z, et al. Quantum computation based on d-level cluster state. Phys Rev A, 2003, 68: 062303
13 Bullock S S, O'Leary D P, Brennen G K. Asymptotically optimal quantum circuits for d-level systems. Phys Rev Lett, 2005, 94: 230502
14 Li W D, Gu Y J, Liu K, et al. Efficient universal quantum computation with auxiliary Hilbert space. Phys Rev A, 2013, 88: 034303
15 Mischuck B, Molmer K. Qudit quantum computation in the Jaynes-Cummings model. Phys Rev A, 2013, 87: 022341
16 Gottesman D. Fault-tolerant computation with higher dimensional systems. Chaos Soliton Fractal, 1999, 10: 1749–1758
17 Fujiwara M, Takeoka M, Mizuno J, et al. Exceeding the classical capacity limit in a quantum optical channel. Phys Rev Lett, 2003, 90: 167906
18 Cortese J. Holevo-Schumacher-Westmoreland channel capacity for a class of qudit unital channels. Phys Rev A, 2004, 69: 022302
19 Collins D, Gisin N, Linden N, et al. Bell inequalities for arbitrarily high-dimensional systems. Phys Rev Lett, 2002, 88: 040404
20 Ralph T C, Resch K, Gilchrist A. Efficient Toffoli gates using qudits. Phys Rev A, 2007, 75: 022313
21 Lanyon B P, Weinhold T J, Langford N K, et al. Manipulating biphotonic qutrits. Phys Rev Lett, 2008, 100: 060504
22 Lanyon B P, Barbieri M, Almeida M P, et al. Simplifying quantum logic using higher-dimensional Hilbert spaces. Nat Phys, 2009, 5: 134–140
23 Nikolopoulos G M, Ranade K S, Alber G. Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication. Phys Rev A, 2006, 73: 032325
24 Molina-Terriza G, Vaziri A, Rehacek J, et al. Triggered qutrits for quantum communication protocols. Phys Rev Lett, 2004, 92: 167903
25 Groblacher S, Jennewein T, Vaziri A, et al. Experimental quantum cryptography with qutrits. New J Phys, 2006, 8: 75
26 Bruß D, Macchiavello C. Optimal eavesdropping in cryptography with three-dimensional quantum states. Phys Rev Lett, 2002, 88: 127901
27 Cerf N J, Bourennane M, Karlsson A, et al. Security of quantum key distribution using d-level systems. Phys Rev Lett, 2002, 88: 127902
28 Karimipour K, Bahraminasab A, Bagherinezhad S. Quantum key distribution for d-level systems with generalized Bell states. Phys Rev A, 2002, 65: 052331
29 Ann K, Jaeger G. Entanglement sudden death in qubit-qutrit systems. Phys Lett A, 2008, 372: 579–583
30 Song W, Chen L, Zhu S L. Sudden death of distillability in qutrit-qutrit systems. Phys Rev A, 2009, 80: 012331
31 Walborn S P, Lemelle D S, Almeida M P, et al. Quantum key distribution with higher-order alphabets using spatially encoded qudits. Phys Rev Lett, 2006, 96: 090501
32 Chen L B, Lu H. Nonlocal unambiguous discrimination among N nonorthogonal qudit states lying in a higher-dimensional Hilbert space. Sci China-Phys Mech Astron, 2012, 55: 55–59
33 Zhang Z Y, Liu Y M, Zhang W, et al. Criterion and flexibility of operation difficulty for perfect teleportation of arbitrary n-qutrit state with $(n:n)$-qutrit pure state. Sci China-Phys Mech Astron, 2011, 54: 1476–1480
34 Cao Y, Peng S G, Zheng C, et al. Quantum Fourier transform and phase estimation in qudit system. Commun Theor Phys, 2011, 55: 790–794
35 Ivanov P A, Kyoseva E S, Vitanov N V. Engineering of arbitrary $U(N)$ transformations by quantum Householder reflections. Phys Rev A, 2006, 74: 022323
36 O'ullivan-Hale M N, Khan I A, Boyd R W, et al. Pixel entanglement: Experimental realization of optically entangled $d=3$ and $d=6$ qudits. Phys Rev Lett, 2005, 94: 220501
37 Rousseaux B, Guerin S, Vitanov N V. Arbitrary qudit gates by adiabatic passage. Phys Rev A, 2013, 87: 032328
38 Neeley M, Ansmann M, Bialczak R C, et al. Emulation of a quantum spin with a superconducting phase qudit. Science, 2009, 7: 722–725