OPEN

Geometry of Quantum Computation with Qudits

Ming-Xing Luo[1,2,3], Xiu-Bo Chen[2], Yi-Xian Yang[2] & Xiaojun Wang[4]

[1]Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu 610031, China, [2]State key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications), Beijing 100876, China, [3]State Key Laboratory of Information Security (Graduate University of Chinese Academy of Sciences), Beijing 100049, China, [4]School of Electronic Engineering, Dublin City University, Dublin 9, Ireland.

The circuit complexity of quantum qubit system evolution as a primitive problem in quantum computation has been discussed widely. We investigate this problem in terms of qudit system. Using the Riemannian geometry the optimal quantum circuits are equivalent to the geodetic evolutions in specially curved parametrization of $SU(d^n)$. And the quantum circuit complexity is explicitly dependent of controllable approximation error bound.

Quantum algorithms based on the circuit model have been explored to solve difficult problems in terms of classical computers[1], e.g., large integer factoring[2,3] and quantum searching algorithm[4]. These quantum models are composed of a sequence of quantum gates which may be generated from unitary evolution operator $U(t)$ with special Hamiltonian. The interacted gates or nonlocal quantum operations are views as the key of circuit complexity. One algorithm is computable or efficient if it can be realized with polynomial interacted gates in terms of system size[5,6]. One main goal of quantum computation is to investigate efficient quantum circuits to synthesize quantum operation[7–9].

The quantum circuit complexity for qubit systems has been investigated with different approaches such as the geometric approach[10–14]. It provides an equivalent statement as the shortest path problem in a curved geometry. The quantum circuit complexity may be reduced to the metric distance between the identity operation and desired unitary using designed Riemannian metric on the unitary space. Thus the metric distance is a good measure of the complexity of synthesizing quantum nonlocal evolution.

In comparison to the qubit system, d-dimensional quantum states (qudits for short) could be more efficient in quantum applications. With larger state space the qudit algorithms may improve channel capacity[15,16] and quantum gates implementation[17–19], increase security[20–24] and explore quantum features[25–27]. The qudit systems have also been experimentally realized[28–31]. The high-dimensional quantum system maybe provide different quantum correlations and efficient information processing. d degenerate (in the rotating-wave approximation sense) ground states may form the qudit, coherently coupled via a common excited state by pulsed external fields of the same time dependence and the same detuning[32]. The multiple photon states may also be reformed as qudit with the help of symmetric primitive states under the permutation invariance[32,33].

In this paper we focus on the circuit complexity of qudit quantum computations. The results for qubit-systems[13] and qutrit-system[14] are extended to general qudits. Algebraic methods such as eigenvalue decomposition[34,35], cosine-sine decomposition[36] or Householder Reflection decomposition[37] and qudit computation based on d-level cluster[38] have been used to find the optimal qudit circuits. In comparison to these evaluations, the quantum circuit complexity of nonlocal qudit evolutions are revalued in terms of the Riemannian geometry on $SU(d^n)$. The qudit system evolution is completely determined by the geodesic equation and the initial value of the Hamiltonian. The minimal geodesics through a desired unitary, will be investigated by deforming the known geodesics of a special metric to the geodesics of the metric of qudit circuits. Thus the qubit or qutrit systems[13,14] are improved to qudit ones, in the sense that universal qudit gates are possible to efficiently synthesize a unitary operation with controllable error, and present explicit relationship between the quantum circuit complexity and total error bound, which have not ensured in previous results[13,14]. Three-qudit system as an explicit example is presented in supplementary information.

Results

A quantum gate on n-qudit states is a unitary matrix $U \in SU(d^n)$ determined by time-dependent Hamiltonian $H(t)$ (with reduced Planck constant) according to the following Schrödinger equation,

$$i\frac{d}{dt}U(t) = H(t)U(t) \qquad (1)$$

with $U(0) = I$, $U(T) = U$ and $i = \sqrt{-1}$. The evolution time $t \in [0, T]$. H can be decomposed with the generalized Gell-Mann matrices. The Lie algebra $su(d^n)$ of $SU(d^n)$ is different from the Pauli matrices of qubits. Thus we first present necessary results of $su(d^n)$.

Let e_{jk} denotes the d-by-d matrix with a 1 in the j, k position and zeros elsewhere, a basis can be described as follows:

$$u_{jk}^d = e_{jk} + e_{kj}, 1 \le j < k \le d, \qquad (2)$$

$$u_{jk}^d = i(e_{jk} - e_{kj}), 1 \le k < j \le d, \qquad (3)$$

$$u_{jj}^d = \mathrm{diag}(1, \cdots, 1, -j, 0_{d-2j}), j = 1, \cdots, d-1 \qquad (4)$$

Here, diag represents the diagonal matrix, 0_{d-2j} denotes the zeros of length $d - 2j$. Thus $\{u_{jk}^d\}$ are traceless and Hermitian matrices which are generalizations of Pauli matrices for qudit systems. These matrices combined with identity matrix $I_d := u_{dd}^d$ span the vector space of $d \times d$ Hermitian matrix

$$\begin{pmatrix} x_{11} & z_{12} & z_{13} & \cdots & z_{1d} \\ \bar{z}_{12} & x_{22} & z_{23} & \cdots & z_{2d} \\ \bar{z}_{13} & \bar{z}_{23} & x_{33} & \cdots & z_{3d} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \bar{z}_{1d} & \bar{z}_{2d} & \bar{z}_{3d} & \cdots & x_{dd} \end{pmatrix} \qquad (5)$$

with real x_{jj} and complex z_{jk}, and are also named with generalized Gell-Mann matrices. They construct one group representation of $su(d)$ and other representations may be obtained by arbitrary unitary transformations. From the unitary matrix representation a recursive parametrization of the unitary matrix U_d is followed as

$$U_d = e^{\sum_{j,k=1}^d \alpha_{jk} u_{jk}^d} \qquad (6)$$

with special coefficients α_{jk}.

Let $x_\ell = u_{jk}^d$ with $\ell = jd + k$ and

$$X_\ell^s = I^{\otimes s-1} \otimes x_\ell \otimes I^{\otimes d-s} \qquad (7)$$

be an operator acting on the s-th qudit with x_ℓ and the rest qudits with identity operation I, $\ell = 1, \cdots, d^2$. The basis of $su(d^n)$ is constituted by $\{Y_t^{P_t}\}$, $t = 1, \cdots, n$, $P_t = \{i_1, \cdots, i_t\}$ with all possible $1 < i_1 < \cdots < i_k \le n$, where

$$Y_t^{P_t} = \prod_{k=1}^t x_{j_k}^{i_k} \qquad (8)$$

Y_t^P denotes all operators with generalized Gell-Mann matrices $x_{j_1}, \cdots, x_{j_k}$ acting on t qudits at sites $P = \{i_1, \cdots, i_k\}$, respectively, and rest with identity. The element in $\{Y_t^{P_t}\}$ may be named as t-body.

To evaluate the error bound[13,14] the norm of an operator A is defined by

$$\|A\| = \max_{\|x\|=1} \|Ax\| \qquad (9)$$

which is equivalent to the operator norm given by $\langle A, B \rangle = \mathrm{tr}A^\dagger B$. The norm of generalized Gell-Mann matrices satisfies

$\|u_{jk}\| = 1, j \ne k$, and $\|u_{kk}\| = k$ with $k = 1, \cdots, d-1$. If we replace these not normalized u_{kk} with $\frac{1}{k}u_{kk}$, the generalized Gell-Mann matrices are then normal with respect to the operator norm[14], still denoted by $\{Y_t^{P_t}\}$, is normalized.

Our main result is the following theorem

Main theorem. *For any small constant ε, each unitary $U_A \in SU(d^n)$ may be synthesized using $O(\varepsilon^{-2})$ one- and two-qudit gates, with error $\|U - U_A\| \le \varepsilon$.*

To complete the proof necessary lemmas should be proved. Notice that the generalized Gell-Mann matrices have the following communication relations $[x_j, x_k] = 0$ or $c_{jk}x_s$ for suitable constants c_{jk} and generalized Gell-Mann matrix x_s, specially, each generalized Gell-Mann matrix x_s may be generated by the Lie product of two other generalized Gell-Mann matrices x_j and x_k. By using the tensor product $(x_1 \otimes x_2)(x_3 \otimes x_4) = (x_1 x_3) \otimes (x_2 x_4)$, it easily follows that $x_{\ell_1} \otimes x_s \otimes x_{\ell_2} = [x_{\ell_1} \otimes (1/\sqrt{c_{jk}})x_j \otimes I_d, I_d \otimes (1/\sqrt{c_{jk}})x_k \otimes x_{\ell_2}]$. Thus all 3-body interaction may be generated by 1-body and 2-body. By induction it is not difficult to prove the following lemma.

Lemma 1. The 1-body and 2-body are universal for $SU(d^n)$.

This lemma may be reformed as: all s-body items ($s \ge 3$) in the basis of $su(d^n)$ can be generated by the Lie bracket products of 1-body and 2-body items. With the lemma only problem is to address the approximate accuracy under the limited 2-body items.

The time-dependent Hamiltonian $H(t)$ is represented as

$$H = \sum_{j \in \mathcal{I}_1} h_j \sigma_j + \sum_{s \in \mathcal{I}_2} h_s \sigma_s' \qquad (10)$$

where $\mathcal{I}_1$ denotes all possible one and two-body interactions, $\mathcal{I}_2$ denotes all other more-body interactions, h_j are real coefficients, i.e., σ_j denotes all possible $Y_1^{P_1}$, $Y_2^{P_2}$ defined in equation (8) and σ_s' denotes all possible $Y_t^{P_t}(t \ge 3)$ defined in equation (8). The cost of unitary operation U synthesization with Hamiltonian is defined as, similar to the qubit case,

$$F(H) = \left(\sum_{j \in \mathcal{I}_1} h_j^2 + p \sum_{s \in \mathcal{I}_2} h_s^2 \right)^{1/2} \qquad (11)$$

where $p > 0$ is the penalty paid for three-and more-body items[13,14]. This cost gives rise to a natural distance in $SU(d^n)$. A curve $\mathcal{C}_U$ between the identity operation I and U is a smooth function,

$$\mathcal{C}_U : \begin{cases} U(t) : [0, T] \mapsto SU(d^n) \\ U(0) = I, U(T) = U \end{cases} \qquad (12)$$

The curve length is given by $D(\mathcal{C}_U) \equiv \int_0^T F(H(t))dt$. $D(\mathcal{C}_U)$ is invariant under different parameterizations of $\mathcal{C}_U$, letting $F(H(t)) = 1$ by rescaling $H(t)$ the evolution time $T = D(\mathcal{C}_U)$. The distance $D(I, U)$ between I and U is defined by

$$D(I, U) = \min_{\forall \mathcal{C}_U} d(\mathcal{C}_U) \qquad (13)$$

The function $F(H(\cdot))$ has defined a norm associated to a right invariant Riemannian metric[13] whose metric tensor $\mathfrak{g}$ is presented as

$$\mathfrak{g}_{\sigma_1, \sigma_2} = \begin{cases} 0, & \text{if } \sigma_1 \ne \sigma_2 \\ 1, & \text{if } \sigma_1 = \sigma_2 \text{ and } \sigma_i \text{ are } 1 \text{ or } 2-\text{body} \\ p, & \text{if } \sigma_1 = \sigma_2 \text{ and } \sigma_i \text{ are no less than } 3-\text{body} \end{cases} \qquad (14)$$

With this metric the distance $D(I, U)$ equals to the shortest path of the geodesic equation $\left\langle \frac{d}{dt}H(t), J(t) \right\rangle = i\langle H(t), [H(t), J(t)] \rangle$. Here $\langle \cdot, \cdot \rangle$ is the inner product on the tangent space $su(d^n)$, and J is an arbitrary

operator in $su(d^n)$. The Lemma 1 with the basis $\{Y_t^{P_t}\}$ of $su(d^n)$ shows all q-body items ($q \geq 3$) may be generated by Lie bracket products of 1-body and 2-body items. Thus the metric in equation (14) is reasonable to find the minimal length solution to the geodesic equation[13], because the multiple-body items will be ignorable for large p. The one- and two-body items mainly contribute to the solution.

Based on the statement above the Hamiltonian $H(t)$ may be projected onto one- and two-qudit items $H_2(t)$. The projection error is controllable in terms of large penalty p. And then the evolution according to $H_2(t)$ is divided into small time intervals and approximated by a constant mean Hamiltonian over each interval. Moreover, the evolution according to the constant mean Hamiltonian over each interval may be composed of a sequence of one- and two-qudit quantum gates[13,14]. The main problem is to evaluate the total errors introduced by these approximations.

Lemma 2. *If $U \in SU(d^n)$ is generated by $H(t)$ satisfying $\|H(t)\| \leq c$ in time interval $[0, T]$, then*

$$\left\| U - e^{-i\bar{H}T} \right\| \leq e^{cT} - 1 - cT = O(c^2 T^2) \quad (15)$$

where $\bar{H} = \dfrac{1}{T}\int_0^T H(t)dt$ is the mean Hamiltonian.

Proof. The unitary operator $U(t)$ has defined one Dyson operator[38] with the evolution $|\psi(t)\rangle = U(t)|\psi(0)\rangle$. Its Tomonaga-Schrödinger equation is defined

$$i\frac{d}{dt}U(t)|\psi(0)\rangle = H(t)U(t)|\psi(0)\rangle \quad (16)$$

with $U(t) = I - i\int_0^t H(t_1)U(t_1)dt_1$ and $U(T) = U$. This representation leads to the Neumann series of $U(T)$ as

$$U(T) = \sum_{m=0}^{\infty}(-i)^m \int_0^T\int_0^{t_1}\cdots\int_0^{t_{m-1}} H(t_1)H(t_2)\cdots H(t_m)dt_1 dt_2\cdots dt \quad (17)$$

with $t_1 > t_2 > \cdots > t_m$. The second term is $-i\int_0^T H(t_1)dt_1 = -i\bar{H}T$.

Choosing $t_j \leq \dfrac{T}{L(j+1)}$ for an integer L, then $\int_0^T\int_0^{t_1}\cdots\int_0^{t_{m-1}}dt_1 dt_2\cdots dt_m = T^m/(m!L^m)$ because of $T\Pi_{j=1}^{m-1}t_j \leq T^m/(m!L^{m-1})$. Thus we have

$$\left\| e^{-i\bar{H}T} - U \right\| = \left\| \sum_{j=0}^{\infty}\frac{(-i\bar{H}T)^j}{j!} - \sum_{m=0}^{\infty}(-i)^m\int_0^T\int_0^{t_1}\cdots\int_0^{t_{m-1}}\prod_{k=1}^{m}H(t_k)dt_1 dt_2\cdots dt_m \right\|$$

$$\leq \sum_{m=0}^{\infty}\left(\left\| \frac{(-i\bar{H}T)^m}{m!} \right\| + \int_0^T\int_0^{t_1}\cdots\int_0^{t_{m-1}}\left\| \prod_{k=1}^{m}H(t_k) \right\|dt_1 dt_2\cdots dt_m \right)$$

$$\leq \sum_{m=2}^{\infty}\left(\frac{c^m T^m}{m!} + \frac{Lc^m T^m}{L^m m!} \right) \quad (18)$$

$$= e^{cT} - 1 - cT + Le^{cT/L} - L - cT$$

$$\leq e^{cT} - 1 - cT$$

for $L \to \infty$, from the standard norm inequality $\|XY\| \leq \|X\|\|Y\|$ and the condition $\|H(t)\| \leq c$.

Lemma 3. *Suppose $U_2 \in SU(d^n)$ is a unitary matrix generated by $H_2(t)$ with evolution time T. Then*

$$\|U - U_2\| \leq d^n p^{-1/2}D(\mathcal{C}_U) \quad (19)$$

Proof. Assume two time-dependent Hamiltonians $H(t)$ and $\hat{H}(t)$ (with reduced Planck constant) generate $U(t)$ and $V(t)$ respectively

$$i\frac{d}{dt}U(t) = H(t)U(t), i\frac{d}{dt}V(t) = \hat{H}(t)V(t) \quad (20)$$

with $U(0) = V(0) = I$, $U(T) = U$ and $V(T) = V$. Using the triangle inequality and unitary invariance of operator norm, we obtain

$$\|U - V\| = \|V^*U - I\|$$

$$= \int_0^T\left\| iV(t)^*\big(\hat{H}(t) - H(t)\big)U(t) \right\|dt$$

$$\leq \int_0^T\left\| V(t)^*\big(H(t) - \hat{H}(t)\big)U(t) \right\|dt \quad (21)$$

$$= \int_0^T\left\| H(t) - \hat{H}(t) \right\|dt$$

Here, $U - V = \int_0^T i\big(\hat{H}(t)V(t) - H(t)U(t)\big)dt$ is used. The Euclidean norm of $H(t) = \sum_j h_j\sigma_j$ is given by $\|H(t)\|_2^2 = \sum_{j=1}^{N}h_j^2$. From the Cauchy-Schwartz inequality it follows

$$\|H(t)\| = \left\| \sum_j h_j\sigma_j \right\| \leq \sum_j |h_j| \leq d^n\left(\sum_{j=1}^{N}h_j^2 \right)^{1/2} = d^n\|H\|_2 \quad (22)$$

Therefore from equations (21) and (22) the distance

$$D(\mathcal{C}_U) = \int_0^T F(H(t))dt$$

$$\geq \int_0^T F(H(t) - H_2(t))dt$$

$$= \int_0^T\left(\sum_{ij}ph_{ij}^2 \right)^{1/2}dt \quad (23)$$

$$= \int_0^T\sqrt{p}\|H\|_2 dt$$

$$\geq \frac{\sqrt{p}}{d^n}\int_0^T\|H(t) - H_2(t)\|dt$$

$$\geq \frac{\sqrt{p}}{d^n}\|U - U_2\|$$

Lemma 4. *The distance $D(I, U)$ always has a supremum independent of p in terms of large p.*

To prove this lemma, the Chow's theorem[39] is required. Let M be a connected manifold and $\mathcal{G}$ a connection on a principal G-bundle. The Chow's Theorem states that the tangent space $M_x = H_xM \oplus V_xM$ at any point $q \in M$ with the horizontal space H_xM and vertical space V_xM ($V_xM \cong g$, g denotes Lie algebra of G). Denote $\{Z_i^h\}$ as a local frame of H_qM, then any two points on M can be connected by a horizontal curve if iterated Lie brackets of $\{Z_i^h\}$ evaluated at q span the tangent space M_x.

Proof of lemma 4. The connection and completeness of $SU(d^n)$ gives one choice to find the tangent space M_I as its Lie algebra $su(d^n)$ at the identity matrix I. Thus I and $U \in SU(d^n)$ is connected by a unique geodesic link associated the Riemannian metric in equation (14). The distance $D(I, U)$ is monotonically increased in the penalty p. Moreover, from the Lemma 1 $su(d^n)$ may be generated with iterated Lie brackets of 1-body and 2-body items in the basis $\{Y_t^{P_t}\}$. With the Chow's Theorem the curve connecting I and U in horizontal subspace is unique in terms of the metric in equation (14)

because of the invariance of $su(d^n)$. Otherwise, special geodesic with initial tangent vector in $su(d^n)$ may be existed. Hence $D(I, U)$ has an optimal upper bound d_0 independent of p.

Lemma 5[14]. If A and B are two unitary matrices, then

$$\left\|A^k - B^k\right\| \leq k\|A - B\| \tag{24}$$

for any integer k.

Based the unitary invariance this lemma is easily followed from

$$\left\|A^k - B^k\right\| \leq \|A - B\| \left\|A^{k-1} + A^{k-2}B + \cdots + B^{k-1}\right\|$$
$$\leq \|A - B\| \left(\left\|A^{k-1}\right\| + \left\|A^{k-2}B\right\| + \ldots + \left\|B^{k-1}\right\|\right) \tag{25}$$
$$= k\|A - B\|$$

Lemma 6. *Suppose $H(t)$ only contains one- and two-body Hamiltonian with $|h_j| \leq 1$ at time interval $[0, T]$. Then there is a unitary U_A satisfying*

$$\left\|e^{-iHT} - U_A\right\| \leq cn^2 T^2 N^{-1} \tag{26}$$

and being synthesized using at most Nd^4n^2 one- and two-qudit gates, where c is a constant and N is large integer.

Proof. Divide the interval $[0, T]$ into N intervals of size T/N. In every interval, define a unitary matrix

$$U_{T/N} = e^{-ih_1\sigma_1\frac{T}{N}} e^{-ih_2\sigma_2\frac{T}{N}} \cdots e^{-ih_L\sigma_L\frac{T}{N}} \tag{27}$$

where $L = d^2(d^2 - 1)(n^2 - n)/2 = O(n^2)$ ($d^2 - 1$ generators of $su(d^n)$) denotes the total number of possible one- and two-body interactions in $H(t)$. From the Trotter formula[40] ($e^{i(A + B)t} = e^{iAt}e^{iBt} + O(t^2)$ for two Hermitian matrices A and B) there exists a constant c such that

$$\left\|e^{-iH\frac{T}{N}} - U_{T/N}\right\| = \left\|e^{-i\left(\sum_{j=1}^{L} h_j\sigma_j\right)\frac{T}{N}} - e^{-ih_1\sigma_1\frac{T}{N}} e^{-ih_2\sigma_2\frac{T}{N}} \cdots e^{-ih_L\sigma_L\frac{T}{N}}\right\|$$
$$\leq cn^2 T^2 N^{-2} \tag{28}$$

Using the Lemma 5

$$\left\|e^{-iHT} - U_{T/N}^N\right\| \leq N\left\|e^{-iH\frac{T}{N}} - U_{T/N}\right\| \leq cn^2 T^2 N^{-1} \tag{29}$$

which means that one can approximate e^{iHT} with at most $NL \leq Nd^4n^2$ quantum gates. The error is controlled by the division number N.

With these lemmas we can prove main Theorem.

Discussion

The present Theorem have explained the circuits complexity of in quantum computation with n-qudit systems in terms of the Riemannian geometry. Similar to the qubit case[12,13] and qutrit case[14] the optimal quantum circuit is reduced to the shortest path problem based on special curved geometry of $SU(d^n)$. The qudit systems present different algebraic derivations from qubits and qutrits. Especially to realize the unitary invariance of the norm we take use of operator norm in equation (9) similar to the qutrit case while the norm $\|M\|_1 = \max_{\langle\phi|\phi\rangle = 1}\{|\langle\phi|M|\phi\rangle|\}$ used before is not unitary invariant[12,13]. For instance, consider

$$M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ & & O \end{pmatrix}, U = \begin{pmatrix} a & b \\ b^* & -a^* \\ & & I \end{pmatrix} \tag{30}$$

O denotes zero matrix. One has $\|M\|_1 = 1/2$ and $\|MU\|_1 = \max_{x^2+y^2}|axy + b^*y^2| \neq 1/2$. Generally, one has $\|M\|_1 \leq \|M\|$ from

the Cauchy-Schwartz inequality. The equal case $\|M\|_1 = \|M\|$ is derived from $M^\dagger M = I$ or $M^\dagger = M$.

Moreover, the main theorem is more efficient than previous results[12–14]. Our result shows that the approximation error for synthesizing quantum qudit operation can be close to zero in terms of nonlocal quantum gate cost. However, it[12,13] reads

$$\|U - U_A\| \leq \frac{D(I,U)}{2^n} + 2D(I,U)\delta^{-1}\left(e^{\frac{3n\delta}{\sqrt{2}}} - \left(1 + \frac{3n\delta}{\sqrt{2}}\right)\right) + c_2 D(I,U)n^4\delta^2 \tag{31}$$

which is inexplicit because $D(I, U)$ depends p and the sum of the last two terms may be lower bounded with nonzero constant by choosing $\delta = 1/(n^2 D(I, U))$. Therefore the approximation interval length δ should be smaller such as $1/(n^k D(I, U))$ with $k > 3$. Moreover, their error bounds have not shown explicit relationship between the approximation error and total nonlocal gate cost. Our result presents that the number of approximate nonlocal quantum operations is the order of ε^{-2} with the approximation error bound ε. In comparison to the previous results[34–38], the present geometric way shows the relationship between the quantum approximation and the evolution of special geodesic equation. With the quantum circuit model the detailed circuit has to be found for generating U while one needs to find the shortest geodesic curve linking I and U for geometric method. So, these results may be considered as different quantum approximations with their own features.

Methods

The Lemmas 2–6 are used to prove Main Theorem. Let $H(t)$ (at time $[0, T]$) be the time-dependent normalized Hamiltonian generating the minimal geodesic of length $d(I, U) = T$. Let $H_2(t)$ be the projected Hamiltonian with only the one- and two-body items and generating U_2 with evolution time T. From the Lemma 3 it follows that

$$\|U - U_2\| \leq p^{-1/2}d^n T \tag{32}$$

Divide the time interval $[0, T]$ into N equal parts with length $\delta = T/N$. Let U_2^j be the unitary generated by $H_2(t)$ with evolution time δ in the j-th time interval, and U_M^j be the unitary generated by the mean Hamiltonian $\bar{H} = \delta^{-1}\int_{(j-1)\delta}^{j\delta} H_2(t)dt$ with evolution time δ. $F(H_2(t)) = \sqrt{\sum_j h_j^2} \leq 1$ because $F(H)^2 = \sum_j h_j^2 + p\sum_{i,j} h_{ij}^2 = 1$ with reasonable scaling. Hence $\|H_2(t)\| = \left\|\sum_j h_j\sigma_j\right\| \leq \sum_j |h_j| \leq L\left(\sum_{j=1}^{L} h_j^2\right)^{1/2} \leq d^2 n$ where $L = d^2(d^2 - 1)(n^2 - n)/2$ is the number of one- and two-body items in $H(t)$, i.e. the number of terms in $H_2(t)$. Then from the Lemma 2 it follows that

$$\left\|U_2^j - U_M^j\right\| \leq e^{d^2 n\delta} - (1 + d^2 n\delta) \tag{33}$$

Moreover, from the Lemma 6 there exists a unitary U_A^j synthesized using at most Nd^4n^2 one- and two-qudit gates, and satisfies

$$\left\|U_M^j - U_A^j\right\| = \left\|e^{-i\bar{H}^j\delta} - U_A^j\right\| \leq cn^2 T^2 N^{-3} \tag{34}$$

with bounded $\bar{H}^j$ on every time interval and $c = d^2 n$.

In the follow we show that how to construct U_2 and U_A in terms of U_2^j and U_A^j, respectively. In fact, U_2 is generated using of $H_2^j(t)$ as

$$\frac{d}{dt}U_2^j(t) = -iH_2^j(t)U_2^j(t) \tag{35}$$

with $U_2^1(0) = I, U_2^k((k-1)\delta) = U_2^{k-1}$, and defined on $[(j-1)\delta, j\delta]$ for $j = 1, \cdots, N$. Letting U_2^j be an identity operator on time interval $[0, N\delta]$ except $[(j-1)\delta, j\delta]$. $U_2 = U_2^N U_2^{N-1} \cdots U_2^1$ is generated by the Hamiltonians $H_2^1(t), \cdots, H_2^N(t)$. U_A can be generated similarly. Therefore

$$\|U_2 - U_A\| = \left\|U_2^N U_2^{N-1} \cdots U_2^1 - U_A^N U_A^{N-1} \cdots U_2^1\right\|$$
$$\leq \left\|U_2^1 - U_A^1\right\| + \left\|U_2^N U_2^{N-1} \cdots U_2^2 - U_A^N U_A^{N-1} \cdots U_A^2\right\|$$
$$\vdots \tag{36}$$
$$\leq \sum_{j=1}^{N} \left\|U_2^j - U_A^j\right\|$$

From equations (33), (34) and (36) the approximation error

$$
\begin{aligned}
\|U - U_A\| &\leq \|U - U_2\| + \|U_2 - U_A\| \\
&\leq p^{-1/2} d^n T + \sum_{j=1}^{N} \left\| U_2^j - U_A^j \right\| \\
&\leq p^{-1/2} d^n T + \sum_{j=1}^{N} \left(\left\| U_2^j - U_M^j \right\| + \left\| U_M^j - U_A^j \right\| \right) \\
&\leq p^{-1/2} d^n T + N \left(e^{d^2 n \delta} - \left(1 + d^2 n \delta\right) \right) + c_1 n^2 T^2 N^{-2} \\
&= p^{-1/2} d^n T + T \delta^{-1} \left(e^{d^2 n \delta} - \left(1 + d^2 n \delta\right) \right) + c_1 n^2 \delta^2 \\
&= p^{-1/2} d^n T + c_0 T d^4 n^2 \delta + c_1 n^2 \delta^2 \\
&\leq c \varepsilon
\end{aligned}
\tag{37}
$$

for a constant $c = d^n d_0 + c_0 d_0 d^4 n^2 + c_1 n^2$, where $e^{d^2 n \delta} - \left(1 + d^2 n \delta\right) = O\left(d^4 n^2 \delta^2\right)$ and c_0 is a constant. Choose a suitable penalty p so that $D(I, U) = T$ satisfies $8 d_0/9 \leq T \leq d_0$ from the Lemma 4 and $p^{-1/2} \leq \varepsilon$, and small $\delta = \frac{T}{N} (N \to \infty)$ satisfying $\delta \leq \varepsilon$. Since U_A^j may be synthesized with $Nd^4 n^2$ one- and two-body gates the total number is $N^2 d^4 n^2 = O(\varepsilon^{-2})$ one- and two-body gates.

1. Deutsch, D. Quantum computational networks. *Proc. R. Soc. Lond. A* **425**, 73–90 (1989).
2. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).
3. Li, J., Peng, X., Du, J. F. & Suter, D. An efficient exact quantum algorithm for the integer square-free decomposition problem. *Sci. Rep.* **2**, 260 (2012).
4. Grover, L. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79**, 325–328 (1997).
5. Deutsch, D. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A* **400**, 97–117 (1985).
6. Sleator, T. & Weinfurter, H. Realizable universal quantum logic Gates. *Phys. Rev. Lett.* **74**, 4087–4090 (1995).
7. Shende, V., Bullock, S. S. & Markov, I. L. Synthesis of quantum-logic circuits. *IEEE Tran. Comput. AID Design* **26**, 1000–1010 (2006).
8. Zhang, J., Vala, J., Sastry, S. & Whaley, K. B. Exact two-qubit universal quantum circuit. *Phys. Rev. Lett.* **91**, 027903 (2003).
9. Jordan, S. P. & Wocjan, P. Efficient quantum circuits for arbitrary sparse unitaries. *Phys. Rev. A* **80**, 062301 (2009).
10. Zanardia, P. & Rasettia, M. Holonomic quantum computation. *Phys. Lett. A* **264**, 94–99 (1999).
11. Nielsen, M. A., Dowling, M. R., Gu, M. & Doherty, A. C. Optimal control, geometry, and quantum computing. *Phys. Rev. A* **73**, 062323 (2006).
12. Dowling, M. R. & Nielsen, M. A. The geometry of quantum computation. *Quantum Inf. & Comput.* **8**, 861–899 (2008).
13. Nielsen, M. A., Dowling, M. R., Gu, M. & Doherty, A. C. Quantum computation as geometry. *Science* **311**, 1133 (2006).
14. Li, B., Yu, Z.-H. & Fei, S.-M. Geometry of quantum computation with qutrits. *Sci. Rep.* **3**, 2594 (2013).
15. Fujiwara, M., Takeoka, M., Mizuno, J. & Sasaki, M. Exceeding the classical capacity limit in a quantum optical channel. *Phys. Rev. Lett.* **90**, 167906 (2003).
16. Cortese, J. Holevo-Schumacher-Westmoreland channel capacity for a class of qudit unital channels. *Phys. Rev. A* **69**, 022302 (2004).
17. Collins, D., Gisin, N., Linden, N., Massar, S. & Popescu, S. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.* **88**, 040404 (2002).
18. Ralph, T. C., Resch, K. & Gilchrist, A. Efficient Toffoli gates using qudits. *Phys. Rev. A* **75**, 022313 (2007).
19. Lanyon, B. P. *et al.* Manipulating biphotonic qutrits. *Phys. Rev. Lett.* **100**, 060504 (2008).
20. Lanyon, B. P. *et al.* Simplifying quantum logic using higher-dimensional Hilbert spaces. *Nat. Phys.* **5**, 134–140 (2009).
21. Nikolopoulos, G. M., Ranade, K. S. & Alber, G. Error tolerance of twobasis quantum-key-distribution protocols using qudits and two-way classical communication. *Phys. Rev. A* **73**, 032325 (2006).
22. Molina-Terriza, G., Vaziri, A., Rehacek, J., Hradil, Z. & Zeilinger, A. Triggered qutrits for quantum communication protocols. *Phys. Rev. Lett.* **92**, 167903 (2004).
23. Groblacher, S., Jennewein, T., Vaziri, A., Weihs, G. & Zeilinger, A. Experimental quantum cryptography with qutrits. *New J. Phys.* **8**, 75 (2006).
24. Bruss, D. & Macchiavello, C. Optimal eavesdropping in cryptography with three-dimensional quantum states. *Phys. Rev. Lett.* **88**, 127901 (2002).
25. Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using *d*-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
26. Karimipour, K., Bahraminasab, A. & Bagherinezhad, S. Quantum key distribution for *d*-level systems with generalized Bell states. *Phys. Rev. A* **65**, 052331 (2002).
27. Ann, K. & Jaeger, G. Entanglement sudden death in qubit-qutrit systems. *Phys. Lett. A* **372**, 579–583 (2008).
28. Song, W., Chen, L. & Zhu, S.-L. Sudden death of distillability in qutrit-qutrit systems. *Phys. Rev. A* **80**, 012331 (2009).
29. Vetesi, T., Pironio, S. & Brunner, N. Closing the detection loophole in Bell experiments using qudits. *Phys. Rev. Lett.* **104**, 060401 (2010).
30. Ivanov, P. A., Kyoseva, E. S. & Vitanov, N. V. Engineering of arbitrary *U(N)* transformations by quantum Householder reflections. *Phys. Rev. A* **74**, 022323 (2006).
31. O'ullivan-Hale, M. N., Khan, I. A., Boyd, R. W. & Howell, J. C. Pixel entanglement: experimental realization of optically entangled *d* = 3 and *d* = 6 qudits. *Phys. Rev. Lett.* **94**, 220501 (2005).
32. Neves, L. *et al.* Generation of entangled states of qudits using twin photons. *Phys. Rev. Lett.* **94**, 100501 (2005).
33. Neeley, M. *et al.* Emulation of a quantum spin with a superconducting phase qudit. *Science* **7**, 722–725 (2009).
34. Muthukrishnan, A. & Stroud, C. R. Jr. Multivalued logic gates for quantum computation. *Phys. Rev. A* **62**, 052309 (2000).
35. Brennen, G. K., Bullock, S. S. & O'Leary, D. P. Efficient circuits for exactuniversal computation with qudits. *Quantum Inf. & Comput.* **6**, 436–454 (2006).
36. Nakajima, Y., Kawano, Y., Sekigawa, H., Nakanishi, M., Yamashita, S. & Nakashima, Y. Synthesis of quantum circuits for *d*-level systems by using cosine-sine decomposition. *Quantum Inf. & Comput.* **9**, 423–443 (2009).
37. Bullock, S. S., O'Leary, D. P. & Brennen, G. K. Asymptotically optimal quantum circuits for *d*-level systems. *Phys. Rev. Lett.* **94**, 230502 (2005).
38. Zhou, D. L., Zeng, B., Xu, Z. & Sun, C. P. Quantum computation based on *d*-level cluster state. *Phys. Rev. A* **68**, 062303 (2003).
39. Lucarelli, D. Chow's theorem and universal holonomic quantum computation. *J. Phys. A: Math. Gen.* **35**, 5107 (2002).
40. Trotter, H. F. On the product of semi-groups of operators. *Proc. Amer. Math. Soc.* **10**, 545–551 (1959).

Acknowledgments

Author contributions

M.X. proposed the theoretical method. M.X. and X.B. and X.W. wrote the main manuscript text. M.X. and X.B. and Y.X. reviewed the manuscript.

Additional information