Twist-teleportation based local discrimination of maximally entangled states

Mao-Sheng Li\textsuperscript{1,*} Shao-Ming Fei\textsuperscript{2,3,†} Zong-Xing Xiong\textsuperscript{4,‡} and Yan-Ling Wang\textsuperscript{5,§}

\textsuperscript{1}Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China
\textsuperscript{2}School of Mathematical Sciences, Capital Normal University, Beijing 100084, China
\textsuperscript{3}Max-Planck-Institute for Mathematics in the Sciences, 04103 Leipzig, Germany
\textsuperscript{4}Department of Mathematics, South China University of Technology, Guangzhou 510640, China and
\textsuperscript{5}School of Computer Science and Network Security, Dongguan University of Technology, Dongguan 523808, China

We study local distinguishability of maximally entangled states (MESs). Concerning the question whether any fixed number of MESs can be locally distinguishable for sufficient large dimensions, Fan and Tian \textit{et al.} have obtained two quite satisfactory results for generalized Bell states and qudit lattice states in the case of prime or prime power dimensions. Inspired by the method used in [Phys. Rev. A \textbf{70}, 022304 (2004)], we construct a general twist-teleportation scheme for any orthonormal basis with MESs. Using this teleportation scheme, we obtain necessary and sufficient conditions for one-way distinguishable sets of MESs, which include the generalized Bell states and qudit lattice states as special cases. Moreover, we present a generalized version of the results in [Phys. Rev. A \textbf{92}, 042320 (2015)] for arbitrary dimensional case.

PACS numbers: 03.67.Hk,03.65.Ud

I. INTRODUCTION

In quantum information processing, one often encounters that the subsystems of a composite system are spatially separated. Therefore, quantum manipulation of the system can be carried out only by local operations and classical communication (LOCC). The local distinguishability of quantum states plays important roles in the exploration of LOCC capabilities [1, 2]. Suppose Alice and Bob share a bipartite quantum state chosen from a set of previously known orthogonal states. Their task is to identify the given state by using only LOCC. The set of states are said to be locally distinguishable or distinguishable by LOCC if there exist LOCC protocols to identify exactly the states of the given set, otherwise the set is locally indistinguishable or indistinguishable by LOCC or nonlocal. The study on local distinguishability of quantum states has direct applications in data hiding [3] and quantum secret sharing [4].

Since Bennett \textit{et al.} discovered a locally indistinguishable $3 \otimes 3$ pure product basis in [1], much work has been focused on finding orthogonal product states or maximally entangled states which are locally indistinguishable [5–33]. One motivation for these constructions is that constructing locally indistinguishable orthogonal quantum states (product basis) helps to understand the boundary between LOCC operations and global operations (separable operations).

However, its applications in data hiding and quantum secret sharing require that participants can reveal the encoding results by using LOCC. That is to say, quantum states used to hide secrets should be able to be identified under local operations and classical communications. Therefore, in addition to constructing sets of quantum states that can not be locally distinguished, it is also very important to study the sufficient condition to ensure that a set of quantum states can be locally distinguished.

For the local distinguishability of maximally entangled states, many results have been obtained. In 2004, Fan [34] noticed that the local distinguishability is not changed under local unitary operations. By using a series of complex Hadamard matrices acting on the generalized Bell states (GBSs), it has been successfully proved that: any $l$ prime $d$-dimensional GBSs can be locally distinguished provided $l(l-1) \leq 2d$. In 2005, Nathanson showed that any three orthogonal maximally entangled states (MESs) can be distinguished by LOCC in $\mathbb{C}^d \otimes \mathbb{C}^d$, which is conjectured to be also true for higher dimensional systems [35]. The result of Fan was extended by Tian \textit{et al.} to the prime power dimensional mutually commuting qudit lattice states [36]. The classification of local distinguishability of four GBSs in $\mathbb{C}^4 \otimes \mathbb{C}^4$ has been analyzed in [37, 38]. Wang \textit{et al.} showed that any three orthogonal GBSs can be locally distinguished for any dimension $d \geq 4$ [39]. An interesting question is whether the results of Fan and Tian \textit{et al.} can be extended to arbitrary dimensional quantum systems.

The rest of this article is organized as follows. In Sec. II, we mainly discuss the relationship between maximal entangled states and unitary matrices. And we review some important MESs such as generalized Bell states and qudit lattice states. In Sec. III, for a given maximally entangled basis, we present a direct proof of teleportation scheme over unknown channels. In Sec. IV, we give a necessary and sufficient condition such that a set of special MESs can be distinguished under one-way LOCC. In fact, the problem of one-way LOCC discrimination of special MESs is equivalent to the problem of distinguishability of the corresponding unitary matrices. We
study the properties related to this equivalence problem. In Sec. V, we apply the main results obtained in Sec. IV to general qudit lattice states. We obtain a general version of the results given by Fan and Tian et al. for any dimensionality. Moreover, we step forward to consider for a given l, whether or not all l qudit lattice states can be distinguished by LOCC for large enough dimension d. Finally, we draw a conclusion and put forward some interesting problems in Sec. VI.

II. UNITARY MATRICES AND MAXIMALLY ENTANGLED STATES

Consider a $d \times d$ bipartite quantum system $\mathcal{H}_A \otimes \mathcal{H}_B$. Let $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ be the computational basis of the subsystem. The standard maximally entangled state can be expressed as $|\psi_0\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$. Any maximally entangled states can be uniquely written in the form $|\psi_U\rangle = (U \otimes I)|\psi_0\rangle$ for some unitary matrix $U$. There is a one-one correspondence between maximally entangled states in $\mathcal{H}_A \otimes \mathcal{H}_B$ and unitary matrices in $U(d)$. We call $U$ the corresponding unitary matrix of $|\psi_U\rangle$. Moreover, one has the following relation:

$$\langle \psi_V | \psi_U \rangle = \text{Tr}(V^\dagger U) = \langle V, U \rangle.$$ 

That is, the correspondence is inner product preserving. Below are two sets of important maximally entangled states: generalized Bell states and qudit lattice states.

(i) Generalized Bell states. Let $d$ be an integer with $d \geq 2$ and $\omega_d = e^{\frac{2\pi i}{d}}$ be a primitive $d$th root of unity. We define the bit flip and phase flip operators to be

$$X_d = \sum_{i=0}^{d-1} |i+1 \mod d\rangle \langle i|, \quad Z_d = \sum_{i=0}^{d-1} |\omega_d^i i\rangle \langle i|.$$ 

The following $d^2$ orthogonal MESs are called generalized Bell states:

$$\{|\psi_{m,n}\rangle = (X_d^m Z_d^n \otimes I)|\psi_0\rangle|0 \leq m, n \leq d-1\}. \quad (1)$$

Noting that $Z_d X_d = \omega_d X_d Z_d$ one has

$$(X_d^m Z_d^n)(X_d^{m'} Z_d^{n'}) = \overline{\omega_d^{(m-n)+(m'-n')}}(X_d^m Z_d^n)(X_d^{m'} Z_d^{n'}). \quad (2)$$

where $\overline{\omega_d} = \omega_d^{d-n-m'}$. This implies that the defining matrices of GBSs are commutative up to some phases.

(ii) Qudit lattice states. Firstly, we consider a simple case $d = p^r$, that is, $d$ is a power of some prime number $p$. Let $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ be the additive group with $p$ elements. For any $r$ dimensional vectors $s = (s_1, s_2, \ldots, s_r)$ and $t = (t_1, t_2, \ldots, t_r) \in (\mathbb{Z}/p\mathbb{Z})^r$, we define unitary matrices,

$$X_{p^r}^{s_t} := (\otimes_{i=1}^r X_{p^i}^{s_i})(\otimes_{i=1}^r Z_{p^i}^{t_i}).$$

Qudit lattice states are defined to be $X_{p^r}^{s_t} \otimes I|\Psi_0\rangle$. More generally, let $d = \prod_{j=1}^l p_j^{r_j}$ be the prime decomposition of $d$. Set $s = (s^{(1)}, s^{(2)}, \ldots, s^{(l)})$ and $t = (t^{(1)}, t^{(2)}, \ldots, t^{(l)})$, with $s^{(j)}, t^{(j)} \in (\mathbb{Z}/p_j\mathbb{Z})^{r_j}$. We define a lattice unitary matrix to be

$$X^s Z^t := \otimes_{j=1}^l X_{p_j}^{s^{(j)}} Z_{p_j}^{t^{(j)}},$$

and the qudit lattice states to be $X^s Z^t \otimes I|\Psi_0\rangle$. One can easily check that a similar commutative relation to (2) holds

$$(X^s Z^t)(X^{s'} Z^{t'}) = w(s, t, s', t')(X^{s'} Z^{t'})(X^s Z^t), \quad (3)$$

where $|w(s, t, s', t')| = 1$.

If a set of orthogonal unitary basis $\{U_i\}_{i=1}^{d^2}$ of $M_d(\mathbb{C})$ satisfies the following relations

$$U_i U_j^T = w(i, j) U_j U_i, \quad \text{with } |w(i, j)| = 1,$$

then we call this basis twist commutative. Note that $X_d^t = X_d^{d-1}, Z_d^t = Z_d$. Combining these equalities with Eqs. (2) and (3), one can easily find that both generalized Bell basis and qudit lattice basis are twist commutative.

Remark: If $B_j = \{U_i^{(j)}\}_{i=0}^{d^2-1}$ is a mutually orthogonal unitary basis of $M_d(\mathbb{C})$ which is twist commutative for $j = 1, 2, \ldots, f$, with $d = \prod_{j=1}^f d_j$. Then the following set

$$\mathcal{B} = \{U^{(1)} \otimes U^{(2)} \otimes \cdots \otimes U^{(f)} \mid U^{(j)} \in B_j, j = 1, 2, \ldots, f\}$$

is also an orthogonal unitary basis of $M_d(\mathbb{C})$ which is twist commutative.

In this paper, we mainly focus on maximally entangled states $\{|\Psi_{U_i}\rangle\}$ which correspond to a twist commutative unitary basis $\{U_i\}$. Since the one to one correspondence of MES and its defining unitary matrix, we simply identify a set of MESs with the set of corresponding defining unitary matrices,

$$\mathcal{L} := \{|\psi_{U_{ni}}\rangle \mid 1 \leq i \leq l\} = \{U_{ni} \mid 1 \leq i \leq l\}. \quad (4)$$

III. TWIST QUANTUM TELEPORTATION SCHEME

Let $|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\Psi_i\rangle = \sigma_i \otimes I|\Psi_0\rangle$, where $i \in \{x, y, z\}$ and

$$\sigma_x = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \sigma_y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$ 

The quantum teleportation of a qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is based on the following equation:

$$|\psi\rangle \otimes |\Psi_0\rangle = |\Psi_0\rangle \otimes |\psi\rangle + |\Psi_x\rangle \otimes \sigma_x^\dagger |\psi\rangle + |\Psi_y\rangle \otimes \sigma_y^\dagger |\psi\rangle + |\Psi_z\rangle \otimes \sigma_z^\dagger |\psi\rangle.$$
The above teleportation scheme works \(d\)-dimensional case too [40]. Suppose \(\{ |\Psi_i\rangle \rangle | i = 0, 1, ..., d^2 - 1 \rangle\) is an mutually orthogonal maximally entangled basis of a bipartite system \(\mathcal{H} \otimes \mathcal{H} \) with \(\dim C \mathcal{H} = d\). Without loss of generality, we assume that \( |\Psi_0\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle\) under the computational basis \(\{|i\rangle \rangle | i = 0, 1, ..., d^2 - 1\rangle\). Then there exists a unique unitary matrix \(U_i\) corresponding to \(|\Psi_i\rangle\),

\[
|\Psi_i\rangle = U_i \otimes I |\Psi_0\rangle = I \otimes U_i^\dagger |\Psi_0\rangle.
\]

**Lemma 1.** For any pure states \(|\psi\rangle_c = \sum_{i=0}^{d^2-1} \alpha_i |i\rangle_c\), we have

\[
|\psi\rangle_c |\Psi_r\rangle_{AB} = \frac{1}{d} \sum_{i=0}^{d^2-1} |\Psi_i\rangle_{CA} \otimes U_i^\dagger U_r^\dagger |\psi\rangle_{AB},
\]

where the sub-indices \(A, B\) and \(C\) denote qudits \(A, B\) and \(C\), respectively.

**Proof:** Since \(\{|\Psi_i\rangle_{AB}\}_{i=0}^{d^2-1}\) is an orthogonal normalized basis of \(\mathcal{H}_A \otimes \mathcal{H}_B\), \(\{|\Psi_i\rangle_{CA} |j\rangle_B\}_{j=0}^{d-1}\) is an orthogonal normalized basis of \(\mathcal{H}_C \otimes \mathcal{H}_A \otimes \mathcal{H}_B\),

\[
|\psi\rangle_c |\Psi_r\rangle_{AB} = \sum_{i=0}^{d^2-1} \sum_{j=0}^{d-1} \langle \Psi_i_{CA} |i\rangle_c |\Psi_r\rangle_{AB} |\psi\rangle_{AB}.
\]

The coefficients in the right hand side of (5) can be written as

\[
\sum_{i=0}^{d^2-1} \langle \Psi_i_{CA} |i\rangle_c |\Psi_r\rangle_{AB} = \sum_{k=0}^{d-1} \sum_{m=0}^{d-1} \sum_{n=0}^{d-1} \alpha_k \langle \Psi_i_{CA} |i\rangle_c |\Psi_r\rangle_{AB} = \sum_{k=0}^{d-1} \sum_{m=0}^{d-1} \sum_{n=0}^{d-1} \alpha_k \langle \Psi_i_{CA} |i\rangle_c |\Psi_r\rangle_{AB} = \sum_{k=0}^{d-1} \sum_{m=0}^{d-1} \sum_{n=0}^{d-1} \alpha_k \langle \Psi_i_{CA} |i\rangle_c |\Psi_r\rangle_{AB} = \sum_{k=0}^{d-1} \sum_{m=0}^{d-1} \sum_{n=0}^{d-1} \alpha_k \langle \Psi_i_{CA} |i\rangle_c |\Psi_r\rangle_{AB}.
\]

Clearly

\[
\sum_{j=0}^{d^2-1} \sum_{k=0}^{d-1} \alpha_k \langle k |U_i^\dagger U_r^\dagger |j\rangle = U_r^\dagger U_i^\dagger |\psi\rangle.
\]

Combining equations (5), (6) and (7) one proves the Lemma.

Lemma 1 shows that if Alice and Bob share the maximally entangled states \(|\Psi_r\rangle_{AB}\) and Alice wants to teleport the state \(|\psi\rangle_c\) to Bob, she only needs to make a projective measurement under the basis \(\{|\Psi_i\rangle\rangle | i = 0, 1, ..., d^2 - 1\rangle\) and tell Bob the measurement outcome. However, if Alice and Bob do not know exactly which maximally entangled state they share, Bob could not recover perfectly the state \(|\psi\rangle\). But he knows that his state must be one of the \(\{U_i^\dagger U_r^\dagger |\psi\rangle\rangle | r = 0, 1, ..., d^2 - 1\rangle\). We call such teleportation scheme twist teleportation (See Fig 1).

**IV. LOCAL DISTINGUISHABILITY OF TWIST COMMUTATIVE MAXIMALLY ENTANGLED STATES**

Given a set of unitary operators \(\{U_i\}_{i=1}^d \in U(d)\), we say that they are distinguishable if there exists a unit vector \(|\alpha\rangle \in \mathbb{C}^d\) such that \(\{U_i |\alpha\rangle\}_{i=1}^d\) are pairwise orthogonal. By definition two nonorthogonal unitary matrices might be distinguishable. For example, the following two \(3 \times 3\) matrices

\[
U_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad U_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}
\]

are distinguishable as one can choose \(|\alpha\rangle = (0, 1, 0)^T\).

It should noted that \(\{U_i\}_{i=1}^d \in U(d)\) are distinguishable if and only if \(\{U_i^T |\alpha\rangle\}_{i=1}^d\) are pairwise orthogonal and only if \(\{U_i^T |\alpha\rangle\}_{i=1}^d\) are pairwise orthogonal, where \(|\alpha\rangle\) is the complex conjugation of \(|\alpha\rangle\). The following is an general version of one main result (the Theorem 1) in [20].

**Theorem 1.** Let \(\{|\Psi_i\rangle\rangle | i = 0, 1, ..., d^2 - 1\rangle\) be an orthonormal maximally entangled basis of \(\mathcal{H}_A \otimes \mathcal{H}_B\) whose corresponding unitary matrices \(S = \{U_i\}_{i=0}^{d^2-1}\) are twist commutative. Let \(L\) be a subset of \(S\). Then the states correspond to \(L\) can be distinguished by one-way LOCC from \(A \rightarrow B\), if and only if the set of unitary matrices in \(L\) are distinguishable.

**Proof:** The proof of the necessary part has been investigated by Nathanson [30]. For the sufficient part, suppose
Let $|\alpha\rangle$ be a unity vector such that $\{|U^T|\alpha\rangle\mid U \in \mathcal{L}\}$ are pairwise orthogonal. Firstly, Alice prepares the state $|\alpha\rangle$ in her ancilla system $C$. Then Alice and Bob use the state $|\Psi_U\rangle$, which needs to be identified, as the resource state to teleport Alice’s state $|\alpha\rangle$ according to the orthonormal set $\{|U^T|\alpha\rangle\}_{U \in \mathcal{L}}$, see Fig. 2.

This implies that Bob can distinguish these states by a projective measurement according to the orthonormal set $\{|U^T|\alpha\rangle\}_{U \in \mathcal{L}}$, see Fig. 2.

**Proposition 1.** Let $d_1$ and $d_2$ be two integers such that $2 \leq d_1 \leq d_2$. For any orthogonal unitary basis $\{U_i\}_{i=1}^{d_1^2}$ of $M_{d_1}(\mathbb{C})$ and $V \in U(d_2)$, the set of unitary matrices $\{U_i \otimes V\}_{i=1}^{d_2^2}$ are distinguishable.

**Proof:** Let $\{|i\rangle_A\}_{i=1}^{d_1}$ and $\{|i\rangle_B\}_{i=1}^{d_2}$ be the computational orthonormal basis of systems $A$ and $B$, respectively. Set $|\alpha\rangle = \sum_{i=1}^{d_1} |i\rangle_A |i\rangle_B$. For $1 \leq k, l \leq d_1^2$, we have

$$
\langle\alpha|U_i^T(U_i \otimes V)|\alpha\rangle = \langle\alpha|(U_i^T)^*U_i^T|\alpha\rangle = 0.
$$

Therefore the $d_1^2 \{|U_j \otimes V|\rangle\}_{j=1}^{d_1^2}$ are pairwise orthogonal.

**Proposition 2.** Let $\mathcal{L}_j$ be a set of distinguishable mutually orthogonal unitary matrices in $U(d_j)$, $j = 1, 2, ..., f$, and

$$
\mathcal{\hat{L}} = \{U^{(1)} \otimes U^{(2)} \otimes \cdots \otimes U^{(f)} \mid U^{(j)} \in \mathcal{L}_j, j = 1, 2, ..., f\}
$$

a set of unitary matrices of $U(d_1d_2 \cdots d_f)$. Then $\mathcal{\hat{L}}$ are also distinguishable.

**Proof:** Since $\mathcal{L}_j$ can be distinguished, there exists a unit vector $|\alpha_j\rangle \in \mathbb{C}^{d_j}$ such that $\{|U|\alpha_j\rangle \mid U \in \mathcal{L}_j\}$ are pairwise orthogonal. Set $|\alpha\rangle = |\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \cdots \otimes |\alpha_f\rangle$. Let $U = U^{(1)} \otimes U^{(2)} \otimes \cdots \otimes U^{(f)}$ and $V = V^{(1)} \otimes V^{(2)} \otimes \cdots \otimes V^{(f)}$ be two different elements in $\mathcal{\hat{L}}$. There must exist some $j_0$ such that $U^{(j_0)}$ and $V^{(j_0)}$ are different elements in $\mathcal{L}_{j_0}$, and

$$
\langle\alpha_{j_0}|U^{(j_0)}V^{(j_0)}|\alpha_{j_0}\rangle = 0,
$$

which implies that

$$
\langle\alpha|UV^\dagger|\alpha\rangle = \prod_{j=1}^f \langle\alpha_j|U^{(j)}V^{(j)}|\alpha_j\rangle = 0.
$$

Hence, $\{|U|\rangle \mid U \in \mathcal{\hat{L}}\}$ are indeed pairwise orthogonal and the set $\mathcal{\hat{L}}$ are distinguishable by definition.

From proposition 2, we can deduce the following corollary.

**Corollary 1.** Let $\{\psi^{(j)}_i\}_{i=0}^{d_j^2-1}$ be an orthonormal maximally entangled basis of $\mathcal{H}_A \otimes \mathcal{H}_B$, whose corresponding unitary matrices $B_j = \{U^{(j)}_i\}_{i=0}^{d_j^2-1}$ are twist commutative for $j = 1, 2, ..., f$. Suppose that the states corresponding to $\mathcal{L}_j \subseteq B_j$ can be distinguished by one-way LOCC from $A_j \rightarrow B_j$ for all $j$. Then the set corresponding to $\mathcal{\hat{L}} = \{U^{(1)} \otimes U^{(2)} \otimes \cdots \otimes U^{(f)} \mid U^{(j)} \in \mathcal{L}_{j_0}, j = 1, 2, ..., f\}$ can be also distinguished by one-way LOCC from $A \rightarrow B$ when looking the bipartite states as $\mathcal{H}_A \otimes \mathcal{H}_B := (\otimes_{j=1}^f \mathcal{H}_A_j) \otimes (\otimes_{j=1}^f \mathcal{H}_B_j)$.

**V. APPLICATION TO QUANTUM LATTICE STATES**

In 2015, Tian et al. successfully generalized Fan’s result to $p^r \otimes p^s$ system [36]. Particularly, they showed
that any l qudit lattice states in $p^l \otimes p^l$ are one-way locally distinguishable if $l(l-1) \leq 2p^l$. Based on these results and Corollary 1, we give a more general result for arbitrary dimension $d$.

**Theorem 2.** Let $d$ be an odd positive integer with prime factorization $d = p_1^{r_1}p_2^{r_2}...p_f^{r_f}$, $p_1^{r_1} < p_2^{r_2} < ... < p_f^{r_f}$. Then any set of $l$ qudit lattice states are distinguishable by one-way LOCC provided that $l(l-1) \leq 2p_1^{r_1}$.

**Proof:** Let $\mathcal{L}$ denote the corresponding unitary matrices of any given $l$ qudit lattice states. Every matrix in $\mathcal{L}$ can be written as $f$ tensor products of unitary matrices of dimension $p_1^{r_1}$,

$$U = U^{(1)} \otimes U^{(2)} \otimes \ldots \otimes U^{(f)} \in U(p_1^{r_1})$$

for $i = 1, 2, ..., f$. For each $i \in \{1, 2, ..., f\}$, we define

$$\mathcal{L}_i = \{U^{(i)} \mid U^{(1)} \otimes U^{(2)} \otimes \ldots \otimes U^{(f)} \in \mathcal{L}\}.$$ 

Let $l_i$ denote the number of elements $\mathcal{L}_i$, $l_i := |\mathcal{L}_i| \leq l$. Then

$$l_i(l_i - 1) \leq l(l-1) \leq 2p_1^{r_1} \leq 2p_1^{r_1}.$$ 

From Tian’s results in [36], the states corresponding to $\mathcal{L}_i$ can be one-way LOCC distinguished. Due to the necessity of Theorem 1, the unitary matrices in $\mathcal{L}_i$ are distinguishable. By Corollary 1, the unitary matrices in $\mathcal{L} \subseteq \mathcal{L}_i$ are distinguishable too. From the sufficient part of Theorem 1, the set of qudit lattice states corresponding to $\mathcal{L}$ are distinguishable by one-way LOCC.

For any $l \geq 2$, we say that $d$ satisfies $\mathcal{P}(l)$ if any $l$ unitary matrices corresponding to $l$ different qudit lattice states of dimensional $d$ are distinguishable. Denote $P(l) = \{d \in \mathbb{N} \mid d$ satisfied $\mathcal{P}(l)\}$. It is obvious that $P(l) \supseteq P(l+1)$. As any two orthogonal bipartite states are distinguishable by one-way LOCC, we have that $P(2) = \{2, 3, 4, \ldots\}$. An interesting problem is to determine $P(l)$ for $l \geq 3$.

**Theorem 3.** Any three qudit lattice states in $d \otimes d$, $d \geq 3$, are distinguishable by one-way LOCC.

**Proof:** Let $d = p_1^{r_1}p_2^{r_2}...p_f^{r_f}$ be the prime factorization of $d$ with $p_1^{r_1} < p_2^{r_2} < ... < p_f^{r_f}$. If $p_1^{r_1} \geq 3(3-1)/2 = 3$, we can draw the conclusion for such $d$ by Theorem 2. Hence we only need to consider the case $p_1^{r_1} = 2$, that is, $d = 2d'$ with $d' > 1$ as $d \geq 3$. Suppose the unitary matrices corresponding to the three states are given by

$$\mathcal{L} = \{U^{(1)}_i \otimes U^{(2)}_i \in U(2), U^{(2)}_i \in U(d'), i = 1, 2, 3\}.$$

Denote $\mathcal{L}_1 = \{U^{(1)}_i \mid i = 1, 2, 3\}$ and $\mathcal{L}_2 = \{U^{(2)}_i \mid i = 1, 2, 3\}$.

(a) $|\mathcal{L}_2| = 1$. As $2 < d'$, the condition of Proposition 1 is satisfied. Hence $\mathcal{L}$ is distinguishable.

(b) $|\mathcal{L}_2| = 2$. Without loss of generality, we assume that $U^{(2)}_1 = U^{(2)}_3$. Then there exists a unit vector $|\alpha_2\rangle \in \mathbb{C}^d$ such that

$$\langle \alpha_2 | U^{(2)}_1 | \alpha_2 \rangle = \langle \alpha_2 | U^{(2)}_3 | \alpha_2 \rangle = 0.$$

Moreover, there also exists a unit vector $|\alpha_1\rangle \in \mathbb{C}^2$ such that $\langle \alpha_1 | U^{(1)}_2 | \alpha_1 \rangle = 0$.

Then for any $1 \leq i, j \leq 3$, we have

$$\langle \alpha_1 | (U^{(1)}_i \otimes U^{(2)}_i)(U^{(1)}_j \otimes U^{(2)}_j) | \alpha_1 \rangle = 0,$$

i.e., the set $\mathcal{L}$ is also distinguishable.

(c) $|\mathcal{L}_2| = 3$. Similar to the case (b), there exists a unit vector $|\alpha_2\rangle \in \mathbb{C}^d$ such that

$$\langle \alpha_2 | U^{(2)}_i | \alpha_2 \rangle = \delta_{ij}, \quad \text{for } 1 \leq i, j \leq 3.$$

Choosing an arbitrary unit vector $|\alpha_1\rangle \in \mathbb{C}^2$ and setting $|\alpha\rangle = |\alpha_1\rangle \otimes |\alpha_2\rangle$, we have the following relations

$$\langle \alpha_1 | (U^{(1)}_i \otimes U^{(2)}_i)(U^{(1)}_j \otimes U^{(2)}_j) | \alpha \rangle = \delta_{ij},$$

which implies that $\mathcal{L}$ is distinguishable.

Then the sufficient part of the Theorem 1 implies the conclusion.

As any three Bell states can not be locally distinguished, from Theorem 3 we have that $P(3) = \{3, 4, 5, \ldots\}$. In the next theorem, we try to determine the $P(4)$.

**Theorem 4.** Any 4 qudit lattice states in $d \otimes d$, $d \geq 91$, are distinguishable by one-way LOCC. Moreover,

$$\mathbb{N} \setminus \{1, 2, 3, 4, 5, 6, 10, 12, 15, 18, 20, 30, 50, 60, 90\} \subseteq P(4).$$

**Proof:** We first give two claims whose proofs will be presented in Appendix A.

- **Claim 1:** If $3 \leq d' \leq d''$ and $d'' \in P(4)$, then $d' \in P(4)$.

- **Claim 2:** If $p$ is a prime number with $p \geq 7$, then $2p \in P(4)$.

Now let $d = p_1^{r_1}p_2^{r_2}...p_f^{r_f}$ be the prime factorization of $d$ with $p_1^{r_1} < p_2^{r_2} < ... < p_f^{r_f}$. If $p_1^{r_1} \geq 4(4-1)/2 = 6$, by Theorems 1 and 2, we have $d \in P(4)$. Hence only those $d$ whose $p_1^{r_1} = 2, 3, 4, 5$ might lie outside $P(4)$. If $f = 1$, there are only four exceptional points, $d = 2, 3, 4, 5$. Hence we assume $f \geq 2$.

If $p_1^{r_1} = 3, 4, 5$, then $p_1^{r_1}$ can not be greater than 6 for $2 \leq i \leq f$. Otherwise, **Claim 1** and **Proposition 2** would imply that $d \in P(4)$. For example, $d = 3 \times 4 \times 7 \times 19^2$. Then $7 \times 19^3 \in P(4)$ imply that $7 \times 19^2 \in P(4)$ by **Proposition 2**. Hence $4 \times 7 \times 19^2 \in P(4)$ by **Claim 1**. So is $d$. Therefore, this contributes four exceptional cases $d = 3 \times 4 \times 5 \times 4 \times 5$ and $3 \times 4 \times 5$. 


If \( p_f^i = 2 \), then \( p_f \leq 5 \). Otherwise \( 2p_f \in P(4) \) by Claim 2. With similar argument above, we have \( d \in P(4) \). Hence, \( f = 2 \) or 3. If \( f = 2 \), then \( d = 2 \times 3^i \) or \( d = 2 \times 5^i \) with \( i \leq 2 \). Otherwise, we can decompose \( d = 6 \times 3^{i-1} \) or \( d = 10 \times 5^{i-1} \) and apply Claim 1 to obtain \( d \in P(4) \). If \( f = 3 \), then \( d = 2 \times 3^i \times 5^j \) with \( i \leq 2 \) and \( j = 1 \).

VI. CONCLUSION AND DISCUSSION

We have studied the problem of local distinguishability of maximally entangled states based on twist teleportation. Focusing on maximally entangled basis whose corresponding unitary matrices \( S = \{U_i\}_{i=1}^d \) are twist commutative, we have shown that the maximally entangled states corresponding to \( \{U\}_{U \epsilon L} \subseteq S \) are one-way LOCC distinguishable if and only if the set of unitary matrices \( \{U\}_{U \epsilon L} \) are distinguishable. Applying our results to the lattice qudit settings, we have obtained a general version of Fan’s and Tian’s results: if \( d = \prod_{l=1}^i p_l^{i_l} \) with \( p_1^{i_1} < p_2^{i_2} < \cdots < p_d^{i_d} \), then any \( l \) lattice states are one-way LOCC distinguishable if \( l(l-1)/2 \leq p_l^{i_l} \). For given \( l \), one might wonder whether any \( l \) lattice states are LOCC distinguishable if the dimension \( d \) is large enough. By using the main criterion we obtained, we have demonstrated that this is true for \( l = 3 \) and 4. There are also some interesting questions remained open, for example, how to determine whether a set of unitary matrices is distinguishable or not? For \( l \geq 5 \), whether there exist some \( N(l) \) such that if \( d \geq N(l) \) then any \( l \) qudit lattice states are distinguishable? And can one determine the set \( P(l) \)? Our approach might might further investigations on local distinguishability of bipartite or multipartite states.

Acknowledgments This work is supported by the NSFC 11571119, NSFC 11675113, NSFC 11871295, and Beijing Municipal Commission of Education (KM201810011009).

APPENDIX A

Proof of Claim 1: Suppose the unitary matrices corresponding to the four qudit lattice states are given by \( L = \{U^{(1)}_i \otimes U^{(2)}_i | U^{(1)}_i \in U(d'), U^{(2)}_i \in U(d'') \}, i = 1, 2, 3, 4 \) . Denote \( L_1 = \{U^{(1)}_i | i = 1, 2, 3, 4 \}, L_2 = \{U^{(2)}_i | i = 1, 2, 3, 4 \} \).

We separate the arguments into four cases according to the cardinality of \( L_2 \).

(a) \( |L_2| = 1 \). As \( d' \leq d'' \) the condition of Proposition 1 is fulfilled, hence \( L \) is distinguishable.

(b) \( |L_2| = 2 \). Without loss of generality, there are two subcases: i) \( U^{(2)}_1 = U^{(2)}_2 = U^{(2)}_3 \neq U^{(2)}_4 \). In this case, \( U^{(2)}_1, U^{(2)}_2, U^{(2)}_3 \) are pairwise different. Since the three states are distinguished by oneway LOCC, there exists \( \alpha_1 \) such that \( \langle \alpha_1 | U^{(1)}_i | U^{(1)}_j \rangle | \alpha_1 \rangle = 0 \) for \( 1 \leq i \neq j \leq 3 \). Clearly, there exists \( \alpha_2 \), \( \langle \alpha_2 | U^{(2)}_1 | U^{(2)}_2 \rangle | \alpha_2 \rangle = 0 \) for \( i = 1, 2, 3 \) and \( | \alpha_2 \rangle = | \alpha_1 \rangle \otimes | \alpha_2 \rangle \) is just the vector we wanted. ii) \( U^{(2)}_1 = U^{(2)}_2 \neq U^{(2)}_3 = U^{(2)}_4 \). For this case, we need to find a vector \( | \alpha_1 \rangle \) such that \( \langle \alpha_1 | U^{(1)}_i | U^{(1)}_j \rangle | \alpha_1 \rangle = 0 \) and \( | \alpha_1 | U^{(1)}_i | U^{(1)}_j \rangle | \alpha_1 \rangle = 0 \). To show that the above conditions can be fulfilled, we define \( \bar{L}_1 = \{I, U^{(1)}_1 U^{(1)}_2, U^{(1)}_3 U^{(1)}_4 \} \). As \( |L_1| \leq 3 \), by Theorem 1 and theorem 3, we can find \( | \alpha_1 \rangle \) such that \( \langle \alpha_1 | U^{(1)}_1 | \alpha_1 \rangle = 0 \) for \( U \in \Delta(\bar{L}_1) \). Since both \( U^{(1)}_1 U^{(1)}_2 \) and \( U^{(1)}_3 U^{(1)}_4 \) are in \( \Delta(\bar{L}_1) \), we complete the proof.

(c) \( |L_2| = 3 \). We can assume \( U^{(2)}_3 = U^{(2)}_4 \) without loss of generality. We then have \( | \alpha_1 \rangle \) and \( | \alpha_2 \rangle \) such that \( \langle \alpha_2 | U^{(2)}_i | U^{(2)}_j \rangle | \alpha_2 \rangle = 0 \), \( 1 \leq i \neq j \leq 3 \), \( \langle \alpha_1 | U^{(1)}_3 | U^{(1)}_4 \rangle | \alpha_1 \rangle = 0 \).

Then \( | \alpha \rangle = | \alpha_1 \rangle \otimes | \alpha_2 \rangle \) is the vector we needed.

(d) \( |L_2| = 4 \). As \( L_2 \) is distinguishable, we can find \( | \alpha_2 \rangle \) such that \( \langle \alpha_2 | U^{(2)}_i | U^{(2)}_j \rangle | \alpha_2 \rangle = 0 \), \( 1 \leq i \neq j \leq 4 \).

One can then choose an arbitrary unit vector \( | \alpha_1 \rangle \in \mathbb{C}^d \) such that \( | \alpha \rangle = | \alpha_1 \rangle \otimes | \alpha_2 \rangle \) is a vector we wanted.

Proof of Claim 2: Let \( d = 2p \) and suppose that the unitary matrices corresponding to the four qudit lattice states are given by \( L = \{U^{(1)}_i \otimes U^{(2)}_i | U^{(1)}_i \in U(2), U^{(2)}_i \in U(p), i = 1, 2, 3, 4 \} \). Denote \( L_1 = \{U^{(1)}_i | i = 1, 2, 3, 4 \}, L_2 = \{U^{(2)}_i | i = 1, 2, 3, 4 \} \). If \( |L_2| \leq 1 \) or 3 or 4, we can prove that \( L \) is distinguishable with a similar argument as above. We only need to consider the case \( |L_2| = 2 \). In this case, up to a local unitary equivalence, we find that \( \Delta(L) \subseteq \{X_2 \otimes I, Y_2 \otimes I, Z_2 \otimes I, X_2 \otimes X_p, Y_2 \otimes X_p, Z_2 \otimes X_p, I \otimes X_p \} \) for some \( 1 \leq l \leq p-1 \). Let \( | \alpha \rangle = \sum_{i=0}^{l} \sum_{j=0}^{p-1} \alpha_{ij} | i \rangle | j \rangle \). There exist some nontrivial solutions \( | \alpha \rangle \) such that \( \langle \alpha | U \rangle | \alpha \rangle = 0 \) for \( U \in \Delta(L) \). In fact, that \( \langle \alpha | X_2 \otimes I | \alpha \rangle = 0 \), \( \langle \alpha | Y_2 \otimes I | \alpha \rangle = 0 \), \( \langle \alpha | X_2 \otimes X_p | \alpha \rangle = 0 \), \( \langle \alpha | Y_2 \otimes X_p | \alpha \rangle = 0 \), \( \langle \alpha | Z_2 \otimes X_p | \alpha \rangle = 0 \), \( \langle \alpha | I \otimes X_p | \alpha \rangle = 0 \), \( \langle \alpha | Z_2 \otimes I_p | \alpha \rangle = 0 \).
is equivalent to that
\begin{align*}
\sum_{j=0}^{p-1} \overline{\alpha_{0j} \alpha_{1j}} &= \sum_{j=0}^{p-1} \alpha_{1j} \alpha_{0j} = 0, \\
\sum_{j=0}^{p-1} \overline{\alpha_{0j} \gamma_{1j}^{\alpha}} &= \sum_{j=0}^{p-1} \alpha_{1j} \gamma_{0j}^{\alpha} = 0, \\
\sum_{j=0}^{p-1} \overline{\alpha_{0j} \gamma_{0j}^{\alpha}} &= \sum_{j=0}^{p-1} \alpha_{1j} \gamma_{1j}^{\alpha} = 0, \\
\sum_{j=0}^{p-1} |\alpha_{0j}|^2 &= \sum_{j=0}^{p-1} |\alpha_{1j}|^2,
\end{align*}
respectively. There exists some $1 \leq j_0 \leq p - 1$ such that $j_0 - l \neq 0$ and $j_0 + l \neq p$. If we set
\begin{align*}
(\alpha_{00}, \alpha_{01}, \ldots, \alpha_{0p-1}) &= (1, 0, 0, \cdots, 0, 1, 0, \cdots, 0), \\
(\alpha_{10}, \alpha_{11}, \ldots, \alpha_{1p-1}) &= (1, 0, 0, \cdots, 0, -1, 0, \cdots, 0).
\end{align*}
(only the first and the $j_0$-th coordinates are nonzero), then $|\alpha|$ satisfies all the equations above. Hence $L$ is distinguishable.

[1] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Quantum nonlocality without entanglement, Phys. Rev. A 59, 1070 (1999).
[2] J. Walgate and L. Hardy, Nonlocality Asymmetry and Distinguishing Bipartite States, Phys. Rev. Lett. 89, 147901 (2002).
[3] D. P. DiVincenzo, D.W. Leung and B.M. Terhal, Quantum data hiding, IEEE Trans. Inf. Theory 48, 580 (2002).
[4] R. Rahaman, M.G. Parker, Quantum scheme for secret sharing based on local distinguishability, Phys. Rev. A 91, 022330 (2015).
[5] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, B. M. Terhal, Unextendible Product Bases and Bound Entanglement, Phys. Rev. Lett. 82, 585 (1999).
[6] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Local Indistinguishability: More Nonlocality with Less Entanglement, Phys. Rev. Lett. 90, 047902 (2003).
[7] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Unextendible product bases, uncomputable product bases and bound entanglement, Comm. Math. Phys. 238, 379 (2003).
[8] S. De Rinaldis, Distinguishability of complete and unextendible product bases, Phys. Rev. A 70, 022309 (2004).
[9] Y. Feng and Y.-Y. Shi, Characterizing Locally Indistinguishable Orthogonal Product States, IEEE Trans. Inf. Theory 55, 2799 (2009).
[10] Y.-H. Yang, F. Gao, G.-J. Tian, T.-Q. Cao, and Q.-Y. Wen, Local distinguishability of orthogonal quantum states in a $2 \otimes 2 \otimes 2$ system, Phys. Rev. A 88, 042301 (2013).
[11] Z.-C. Zhang, F. Gao, G.-J. Tian, T.-Q. Cao and Q.-Y. Wen, Nonlocality of orthogonal product basis quantum states, Phys. Rev. A 90, 022313 (2014).
[12] Z.-C. Zhang, F. Gao, S.-J. Qin, Y.-H. Yang, and Q.-Y. Wen, Nonlocality of orthogonal product states, Phys. Rev. A 92, 012332 (2015).
[13] Y.-L. Wang, M.-S. Li, Z.-J. Zheng, and S.-M. Fei, Nonlocality of orthogonal product-basis quantum states, Phys. Rev. A 92, 032313 (2015).
[14] Z.-C. Zhang, F. Gao, Y. Cao, S.-J. Qin, and Q.-Y. Wen, Local indistinguishability of orthogonal product states, Phys. Rev. A 93, 012314 (2016).
[15] G.-B. Xu, Q.-Y. Wen, S.-J. Qin, Y.-H. Yang, and F. Gao, Quantum nonlocality of multipartite orthogonal product states, Phys. Rev. A 93, 032341 (2016).
[16] Z.-C. Zhang, K.-J. Zhang, F. Gao, Q.-Y. Wen, and C. H. Oh, Construction of nonlocal multipartite quantum states, Phys. Rev. A 95, 052344 (2017).
[17] S. Halder, Several nonlocal sets of multipartite pure orthogonal product states, Phys. Rev. A 98, 022303 (2018).
[18] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local Distinguishability of Multipartite Orthogonal Quantum States. Phys. Rev. Lett. 85, 4972 (2000).
[19] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Distinguishability of Bell States, Phys. Rev. Lett. 87, 277902 (2001).
[20] S. Ghosh, G. Kar, A. Roy and D. Sarkar, Distinguishability of maximally entangled states, Phys. Rev. A 70, 022304 (2004).
[21] N. Yu, R. Duan, and M. Ying, Four Locally Indistinguishable Ququd-Ququd Orthogonal Maximally Entangled States, Phys. Rev. Lett. 109, 020506 (2012).
[22] A. Cosentino, Positive partial transpose indistinguishable states via semidefinite programming, Phys. Rev. A 87, 012312 (2013).
[23] A. Cosentino and V. Russo, Small sets of locally indistinguishable orthogonal maximally entangled states, Quantum Information & Computation, 14, 1098–1106 (2014).
[24] M.-S. Li, Y.-L. Wang, S.-M. Fei and Z.-J. Zheng, $d$ locally indistinguishable maximally entangled states in $\mathbb{C}^d \otimes \mathbb{C}^d$, Phys. Rev. A 91, 042318 (2015).
[25] S. X. Yu and C. H. Oh, Detecting the local indistinguishability of maximally entangled states, arXiv:1502.01274v1.
[26] S. Bandypadhyay and M. Nathanson, Tight bounds on the distinguishability of quantum states under separable measurements, Phys. Rev. A 88, 052313 (2013).
[27] N. Yu, R. Duan, and M. Ying, Distinguishability of quantum states by positive operator-valued measures with positive partial transpose, IEEE Trans. Inform. Theory 60, 2069 (2014).
[28] S. Bandypadhyay, A. Cosentino, N. Johnston, V. Russo, J. Watrous, and N. Yu, Limitations on separable measurements by convex optimization, IEEE Trans. Inform. Theory 61, 3593 (2015).
[29] S. Bandypadhyay, S. Ghosh, and G. Kar, LOCC distinguishability of unilaterally transformable quantum states, New J. Phys. 13 123013 (2011).
[30] M. Nathanson, Three maximally entangled states can require two-way local operations and classical communication for local discrimination, Phys. Rev. A 88, 062316 (2013).
[31] Z.-C. Zhang, Q.-Y. Wen, F. Gao, G.-J. Tian and T.-Q. Cao, One-way LOCC indistinguishability of maximally entangled states, Quantum Inf. Proc.13, 795 (2014).
[32] Z.-C. Zhang, K.-Q. Feng, F. Gao and Q.-Y. Wen, Distinguishing maximally entangled states by one-way local operations and classical communication, Phys. Rev. A 91, 012329 (2015).

[33] G.-J. Tian, S.-X. Yu, F. Gao, Q.-Y. Wen and C.H. Oh, Local discrimination of four or more maximally entangled states, Phys. Rev. A 91, 052314 (2015).

[34] H. Fan, Distinguishability and Indistinguishability by Local Operations and Classical Communication, Phys. Rev. Lett. 92, 177905 (2004).

[35] M. Nathanson, Distinguishing bipartite orthogonal states using LOCC: Best and worst cases, J. Math. Phys. (N.Y.) 46, 062103 (2005).

[36] G.-J. Tian, S.-X. Yu, F. Gao, Q.-Y. Wen and C.H. Oh, Local discrimination of qudit lattice states via commutativity, Phys. Rev. A 92, 042320 (2015).

[37] G.-J. Tian, S.-X. Yu, F. Gao and Q.-Y. Wen, Classification of locally distinguishable and indistinguishable sets of maximally entangled states, Phys. Rev. A 94, 052315 (2016).

[38] T. Singal, R. Rahaman, S. Ghosh, G. Kar, Necessary condition for local distinguishability of maximally entangled states: Beyond orthogonality preservation, Phys. Rev. A 96, 042314 (2017).

[39] Y.-L. Wang, M.-S. Li, S.-M. Fei and Z.-J. Zheng, The local distinguishability of any three generalized Bell states, Quantum Inf. Process. 16, 126 (2017).

[40] R. F. Werner, All teleportation and dense coding schemes. J. Phys. A: Math. Gen. 34 (35): 7081 (2001).