Characterization of multipartite entanglement in terms of local transformations

Youming Qiao[a], Xiaoming Sun[b], Nengkun Yu[a,c,d]

[a]*Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia*
[b]*Institute of Computing Technology, Chinese Academy of Sciences*
[c]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[d]*Department of Mathematics & Statistics, University of Guelph, Guelph, Ontario N1G 2W1, Canada*

Abstract

The degree of the generators of invariant polynomial rings of is a long standing open problem since the very initial study of the invariant theory in the 19th century. Motivated by its significant role in characterizing multipartite entanglement, we study the invariant polynomial rings of local unitary group—the tensor product of unitary group, and local general linear group—the tensor product of general linear group. For these two groups, we prove polynomial upper bounds on the degree of the generators of invariant polynomial rings. On the other hand, systematic methods are provided to to construct all homogenous polynomials that are invariant under these two groups for any fixed degree. Thus, our results can be regarded as a complete characterization of the invariant polynomial rings. As an interesting application, we show that multipartite entanglement is additive in the sense that two multipartite states are local unitary equivalent if and only if r-copies of them are LU equivalent for some r.

Keywords: local unitary equivalence, quantum entanglement, degree bound, invariant rings
2000 MSC: 13A50, 15A72, 81P40, 81R05

1. Introduction

Multipartite entanglement is considered as an essential asset to quantum information processing and computational tasks. The intriguing properties and potential applications of entanglement spark many literature dedicated to quantify it as a resource. Even though great efforts and considerable progress have been made [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13], no complete theory can be obtained.

Email addresses: `Youming.Qiao@uts.edu.au` (Youming Qiao), `sunxiaoming@ict.ac.cn` (Xiaoming Sun), `nengkunyu@gmail.com` (Nengkun Yu)

The first approach for study multipartite entanglement is to study the local unitary(LU) equivalence of multipartite states. The importance of this approach is due to the fact that multipartite entanglement is characterized by the equivalence relation under LU. Bennett *et.al.* proved the important fact that two quantum states are interconvertible by unlimited two-way classical communication (LOCC) if and only if they are interconvertible by LU [14]. The celebrated Schmidt decomposition provides the canonical form for bipartite pure states under LU, which enables us to understand bipartite entanglement completely. For multipartite system, no such decomposition is possible. Hence, understanding multipartite entanglement is much more challenging. Lots of efforts have been made to study the LU equivalent relation, see [15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25] as a very incomplete list.

In principle, this LU equivalent relation can be characterized by the ring of invariants polynomials under local unitary(LUIPs) [26, 27, 28]. From this point of view, multipartite entanglement is characterized by the ring of LUIPs. A complete description of such ring has been obtained only for bipartite system and $2 \times 2 \times n$ system [29, 30, 31]. Beyond that, and despite the extensive literature, very little is known. One related topic in the study of quantum information science is the stochastic local operations and classical communication(SLOCC). In 2013, Gour and Wallach constructed the whole set of SL-invariant polynomials (SLIPs) for pure states [32].

For the ring of LUIPs, it is already known that the ring of LUIPs is finitely generated. In order to understand the the ring of LUIPs ring, two central problems have to be addressed. The first is to construct the ring by presenting some finite generating set of LUIPs. The second problem naturally arises after the first: bound the degree of generating set, more precisely, present an explicit upper bound on the degree such that the ring of LUIPs can be generated by the LUIPs with degree lower than that bound.

In this paper, we give a characterization of multipartite entanglement by conquering the above two problems. We first provide an algorithm to construct all LUIPs for fixed degree. Secondly, we demonstrate an explicit polynomial upper bound on the degree of generators by employing modern techniques and concepts of invariant theory. As far as we know, no explicit degree bound for the ring of LUIPs was computed in the literature. As an interesting application, we are able to show that multipartite entanglement is additive in the sense that two multipartite states are LU equivalent if and only if r-copies of these two states are LU equivalent for some r.

Our main idea to construct LUIPs here is remarkably simple and feasible in all dimensions: For each party, we construct the corresponding ring of homogenous polynomials that are invariant under the local unitary group applied on that party, then the ring of LUIPs is the intersection of these rings, which can be obtained by computing the intersection of finite dimensional subspaces. To prove a polynomial upper bound on the degree of generators, new techniques on matrix semi-invariants [34, 35] are employed.

This method can also be used to study the SLOCC equivalence of multipartite states. For pure states, we provide an alternative algorithm to compute SLIPs rather than [32]. For mixed states, we focus on the so called one term SLOCC equivalence relation.

2. Preliminaries and Notations

2.1. Notations

During this paper, we consider the n-partite Hilbert space

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n,$$

where Hilbert space $\mathcal{H}_i$ has dimension d_i. Then the dimension of $\mathcal{H}$ is $\Pi_{i=1}^{n} d_i$.

Let $\mathbb{U}(s)$ be the group of $s \times s$ unitary matrices. Then local unitary(LU) group is defined as

$$\mathbb{LU} \equiv \mathbb{U}(d_1) \otimes \mathbb{U}(d_2) \otimes \cdots \otimes \mathbb{U}(d_n).$$

For $|\Psi\rangle \in \mathcal{H}$, the orbit $\mathbb{LU}|\Psi\rangle := \{g|\Psi\rangle : g \in \mathbb{LU}\}$ consists of quantum states in the LU equivalent class of $|\Psi\rangle$. The orbit characterizes the multipartite entanglement in the sense that the entanglement of $|\Psi\rangle$ is the same as that of any state in $\mathbb{LU}|\Psi\rangle$. Therefore, the goal of characterizing multipartite entanglement can be accomplished by separating different LU orbits, in other words, determining the LU equivalence relation.

This problem can be formalized as: For two given states $|\Psi\rangle, |\Phi\rangle \in \mathcal{H}$, determine whether there exists $g \in \mathbb{LU}$ such that

$$|\Psi\rangle = g|\Phi\rangle.$$

To demonstrate the importance of LU equivalence of pure states, we would like to point out the following fact that the problem of the LU equivalence of mixed states can be reduced to the same problem of pure states, *i.e.*, two n-partite mixed states are LU equivalent if and only if their purifications, two $n+1$-partite pure states, are LU equivalent [20], where two mixed states ρ, σ in Hilbert space $\mathcal{H}$ are called LU equivalent if there exists $(U_1 \otimes U_2 \otimes \cdots \otimes U_n) \in \mathbb{LU}$ such that $\rho = (U_1 \otimes U_2 \otimes \cdots \otimes U_n)\sigma(U_1 \otimes U_2 \otimes \cdots \otimes U_n)^\dagger$.

The LU equivalence of mixed states can be used to study the equivalence between quantum channels, where two quantum channels $\mathcal{E}$ and $\mathcal{F}$ are said to be equivalent if there are unitary channels $\mathcal{U}$ $\mathcal{V}$ such that

$$\mathcal{F} = \mathcal{V} \circ \mathcal{E} \circ \mathcal{U}.$$

Here, unitary channels $\mathcal{U}$ and $\mathcal{V}$ can be regarded as encoding channel and decoding channel, respectively. It is direct to verify that $\mathcal{E}$ and $\mathcal{F}$ have the same ability on transmit information, quantum (classical, private) capacity. One can observe that $\mathcal{E}, \mathcal{F} : L(\mathcal{H}_\mathcal{A}) :\mapsto L(\mathcal{H}_\mathcal{B})$ are equivalent if and only if their Choi-matrices are LU equivalent, where the Choi-matrix of $\mathcal{E}$ is defined as the bipartite mixed state (non-normalized) $\rho_{AA'} = (\mathcal{I}_{A'} \otimes \mathcal{E})(|\varphi\rangle\langle\varphi|)$ with $|\varphi\rangle = \sum_{j=1}^{d} |i\rangle|i\rangle$, and the noiseless channel $\mathcal{I}_{A'}$ on quantum system $\mathcal{H}_{A'}$ which has the same dimension d as system $\mathcal{H}_A$.

Another widely studied equivalence relation is the SLOCC equivalence. Two pure states $|\Psi\rangle, |\Phi\rangle \in \mathcal{H}$ are called SLOCC equivalent if there is some $g \in \mathbb{G}$ and $\lambda \in \mathbb{C}$ such that

$$g|\Psi\rangle = \lambda|\Phi\rangle$$

with $\mathbb{G} = \mathbb{SL}(d_1, \mathbb{C}) \otimes \cdots \otimes \mathbb{SL}(d_n, \mathbb{C})$ and $\mathbb{SL}(d_i, \mathbb{C})$ standing for the set of $d_i \times d_i$ invertible matrices with determinant 1.

This problem becomes much more complicated for mixed states: Two mixed states ρ, σ in Hilbert space $\mathcal{H}$ are called SLOCC equivalent if there exists $h_i = (A_{i,1} \otimes A_{i,2} \otimes \cdots \otimes A_{i,n})$ and $m_j = (B_{j,1} \otimes B_{j,2} \otimes \cdots \otimes B_{j,n})$ such that

$$\rho = \sum_i h_i \sigma h_i^\dagger,$$
$$\sigma = \sum_j m_j \rho m_j^\dagger$$

with $A_{i,k}$ and $B_{j,k}$ being $d_j \times d_j$ matrices for all i, j, k.

To determine the SLOCC equivalence between mixed states, even between pure state and mixed state, becomes very difficult. To see this, we notice that $|0\rangle|0\rangle \cdots |0\rangle$ is SLOCC equivalent to any separable states. That is, to see whether a given state is SLOCC equivalent to $|0\rangle|0\rangle \cdots |0\rangle$, we need to test whether it is separable, that problem has been widely studied and it is known to be NP-Hard [37]. To simplify the problem of SLOCC equivalence, we focus on the so called on term SLOCC equivalence. Two mixed states ρ, σ are called one term SLOCC equivalent if there exists $g \in \mathbb{G}$ and $\lambda \in \mathbb{C}$ such that

$$\rho = \lambda \; g \sigma g^\dagger.$$

2.2. Invariant Polynomials

In this subsection, we demonstrate some basic notions of invariant polynomials under LU and under SLOCC, respectively.

We use the concept of LUIPs, namely the polynomials invariant under local unitary transformations, to study the LU equivalence. Formally, a function $f : \mathcal{H} \mapsto \mathbb{C}$ is an LUIP, if $f(|\Psi\rangle)$ is the homogenous polynomial on entries of $|\Psi\rangle\langle\Psi|$(Ψ in short), and

$$f(g|\Psi\rangle) = f(|\Psi\rangle), \quad \forall g \in \mathbb{LU} \;\; \text{and} \;\; \forall |\Psi\rangle \in \mathcal{H}.$$

Notice that any polynomial can be written as a linear combination of homogenous polynomials, and the invariance follows naturally.

Let $\mathbb{C}[\mathcal{H}]^{\mathbb{LU}}$ denote the set of the LUIPs. It is direct to see that $\mathbb{C}[\mathcal{H}]^{\mathbb{LU}}$ is a ring. In other words, it is an abelian group under addition, a monoid under multiplication. Moreover, polynomial multiplication is distributive with respect to addition.

It is well known that the entanglement of bipartite state $|\Psi\rangle_{AB}$ is completely determined by its vector of Schmidt coefficients, says $(\lambda_1, \cdots, \lambda_d)(\lambda_1 \geq \cdots \geq \lambda_d)$, or equivalently determined by $\sum_{j=1}^d \lambda_j^k = \mathrm{tr}(\Psi_A)^k$ for $k \in \mathbb{N}$. By noticing that $\mathrm{tr}(\Psi_A)^k$ is value of LUIP for $|\Psi\rangle_{AB}$, we know that two bipartite states are LU equivalent if and only if LUIPs have the same value for them.

In general, multipartite quantum states $|\Psi\rangle$ and $|\Phi\rangle$ are LU equivalent if and only if $f(|\Psi\rangle) = f(|\Phi\rangle)$ holds for every LUIP f.

SL-invariant polynomials (SLIPs) can be used to study the SLOCC equivalence between quantum states.

To see the power of our method on constructing LUIPs, we apply it on studying the SLOCC equivalence where SLIP is a polynomial $f : \mathcal{H} \mapsto \mathbb{C}$ such that

$$f(g|\Psi\rangle) = f(|\Psi\rangle), \ \ \forall g \in \mathbb{G} \ \text{ and } \ \forall |\Psi\rangle \in \mathcal{H}.$$

Very recently, Gour and Wallach present an algorithm for constructing the SLIPs for fixed degree using Schur-Weyl duality.

3. Main results

In this section, we first provide a new view of LUIPs which leads to an algorithm to compute the ring of LUIPs. We also demonstrate an explicit upper bound such that any LUIP can be generated, using addition, subtraction and product, by LUIPs with degrees no more than the bound. Based on this characterization, we are able to show that two multipartite states are LU equivalent if and only if r-copies of these two states are LU equivalent for some r.

Let I_j be the identity operator of system $\mathcal{H}_j$, and $\mathbb{I}_i = \{I_j\}$, we can define group $\mathbb{U}_i$ as follows,

$$\mathbb{U}_i = \mathbb{I}_1 \otimes \cdots \otimes \mathbb{I}_{i-1} \otimes \mathbb{U}(d_i) \otimes \mathbb{I}_{i+1} \cdots \otimes \mathbb{I}_n.$$

A useful observation is

$$\mathbb{U}_i \subset \mathbb{LU}, \text{and } \ \mathbb{LU} = \mathbb{U}_1\mathbb{U}_2 \cdots \mathbb{U}_n.$$

The advantage of this observation on studying the polynomial invariants is based on the following relation between the polynomial invariants of $\mathbb{LU}$, says P, and those polynomial invariants of $\mathbb{U}_i$s, says P_is,

$$P = \bigcap_{i=1}^{n} P_i. \tag{1}$$

First, we observe that $P \subset P_i$ by noticing $\mathbb{U}_i \subset \mathbb{LU}$. Thus, $P \subset \bigcap_{i=1}^n P_i$.

On the other hand, one can verify that for any $p \in \bigcap_{i=1}^n P_i$, $g = g_1g_2 \cdots g_n \in \mathbb{LU}$ with $g_i \in \mathbb{U}_i$ and $|\varphi\rangle \in \mathcal{H}$, we have $p \in P$ by observing

$$\begin{aligned} & p(g|\varphi\rangle) \\ = \ & p(g_1 \cdots g_n|\varphi\rangle) \\ = \ & p(g_2 \cdots g_n|\varphi\rangle) \\ = \ & \cdots \\ = \ & p(|\varphi\rangle). \end{aligned}$$

Therefore, $P \supset \bigcap_{i=1}^n P_i \Rightarrow P = \bigcap_{i=1}^n P_i$.

We only need to compute P_i for fixed i, the ring of invariant polynomials under unitary group $\mathbb{U}_i$. To study the action of $\mathbb{U}_i$ on $\mathcal{H}$, one may regard the whole space $\mathcal{H}$ as a bipartite space: system $\mathcal{H}_i$ and the rest. Now, the problem becomes to compute the invariants of one party unitary for bipartite pure state. Formally, suppose $|\varphi\rangle = \sum x_{j_1\cdots j_n}|j_1 \cdots j_n\rangle$

with variables $x_{j_1\cdots j_n} \in \mathbb{C}$. According to Uhimann's theorem [33], the set of the entries of $\varphi_{\bar{i}} = Tr_i|\varphi\rangle\langle\varphi|$, those quadratic polynomials, form a generating set of P_i.

For any degree l, the relation (1) enables us to compute the whole set of degree l homogenous elements of P. One can verify that any LUIP is of even degree.

In order to accomplish the characterization of LUIPs, we need the following theorem which explicitly provides an upper bound on the degree to generate the ring of LUIPs.

Theorem 3.1. *The set of all LUIPs is generated by the LUIPs with degree no more than* $N(d_1, d_2, \cdots, d_n) = \frac{3}{8}(\prod_i d_i^2) \cdot \max(d_i)^{2n} \cdot (\sum_i d_i)^{2(\sum_i d_i^2 - n)}$.

Remark:—Although it is known that the ring of LUIPs is finitely generated, as far as we know, no explicit bound was reported in the study of quantum information theory. In modern invariant theory, such an explicit bound for the degree of generating set is known for linearly reductive algebraic group acting rationally on linear spaces [**?**]. Here, the LU group is not a linearly reductive algebraic group. In order to apply this theory on our problem, we resort to the concept "complexification" from [39]. For readability, we postpone the detailed proof of this conclusion to section 4. An upper bound for SLIPs is also included, whose detailed definition is given in the later of this paper. Note that the bound for SLIPs was not computed in the literature before this work.

Thus, two quantum states $|\Psi\rangle, |\Phi\rangle \in \mathcal{H}$ are LU equivalent if and only if $f_i(|\Psi\rangle) = f_i(|\Phi\rangle)$ holds for a basis LUIPs f_i with degree less than $N(d_1, d_2, \cdots, d_n)$.

This characterization of LUIPs can be regarded as a demonstration of the decidability of LU equivalence. Although this fact can also be observed according to Tarski-Seidenberg's famous result, our result is still valuable since it contains physical background and can bring new insight of the entanglement while Tarski-Seidenberg's result does not provide. As an illustration, the following proof of the additivity of entanglement crucially depends on the structure of LUIPs provided above.

Consider the LU equivalence of the r-copy set of states $\mathcal{H}^r := \{|\varphi\rangle^{\otimes r} : |\varphi\rangle \in \mathcal{H} = \bigotimes_{i=1}^n \mathcal{H}_i\}$, where $|\varphi\rangle^{\otimes r}$ is regarded as $n-$partite state of system $\bigotimes_{i=1}^n \mathcal{H}_i^{\otimes r}$. Thus, $|\Psi\rangle^{\otimes r}, |\Phi\rangle^{\otimes r} \in \mathcal{H}^r$ are called LU equivalent if there exists local unitary $\bigotimes_{i=1}^n U_i$ with U_i being unitaries of system $\mathcal{H}_i^{\otimes r}$ such that $|\Psi\rangle^{\otimes r} = \bigotimes_{i=1}^n U_i |\Phi\rangle^{\otimes r}$.

One can observe that if $|\Psi\rangle, |\Phi\rangle$ are LU equivalence then $|\Psi\rangle^{\otimes r}, |\Phi\rangle^{\otimes r}$ are LU equivalence in the above sense. Here, we are interested in the converse direction.

For the bipartite case, one can conclude that the converse is also true by using the following argument: Without loss of generality, assume $|\Psi\rangle_{AB} = \sum_{j=1}^d \sqrt{\lambda_j}|jj\rangle$ and $|\Phi\rangle_{AB} = \sum_{j=1}^d \sqrt{\delta_j}|jj\rangle$. Since $|\Psi\rangle_{AB}^{\otimes r}, |\Phi\rangle_{AB}^{\otimes r}$ are LU-equivalent, we know that $\Psi_A^{\otimes r}$ and $\Phi_A^{\otimes r}$ share eigenvalues with Ψ_A and Ψ_A being the reduced density matrices of $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ respectively. Thus, $\sum_{j=1}^d \lambda_j^{rk} = \sum_{j=1}^d \delta_j^{rk}$ for all k, and one can conclude that the Schmidt coefficients λ_is are identical with δ_is. That is, $|\Psi\rangle, |\Phi\rangle$ are LU-equivalent.

Interestingly, the converse is also true for general multipartite system. To prove such a claim, we need to use a new tool rather than Schmidt coefficients–the LUIPs.

Theorem 3.2. *If* $|\Psi\rangle^{\otimes r}, |\Phi\rangle^{\otimes r}$ *are LU equivalent for some* $r \in \mathbb{N}$*, then* $|\Psi\rangle, |\Phi\rangle$ *are LU equivalent.*

Proof:— Consider the local unitary invariants of $\mathcal{H}^r = \{|\varphi\rangle^{\otimes r} : |\varphi\rangle \in \mathcal{H}\}$, where these invariants are regarded as polynomials of $|\varphi\rangle\langle\varphi|$ with $|\varphi\rangle = \sum x_{j_1\cdots j_n}|j_1\cdots j_n\rangle$ and variables $x_{j_1\cdots j_n} \in \mathbb{C}$. The set of local unitary invariants is the intersection of rings Q_i, where Q_i is the ring generated by the entries of $tr_i\varphi^{\otimes r} = (tr_i\varphi)^{\otimes r}$.

We have the relation between the local unitary invariants of $\mathcal{H}^r$ and the LUIPs of the original system $\mathcal{H}$ as follows: Suppose $f_1, f_2, \cdots, f_k$ of degree $2l_1, 2l_2, \cdots, 2l_k$ are LUIPs of the original system. We have f_j lies in the linear span of the entries of $(tr_i\varphi)^{\otimes l_i}$. Then $\Pi_{j=1}^r f_j$ is a local unitary invariants of $\mathcal{H}^r$ for the case $\sum l_k$ divisible by r. To see this, we only need to observe that $\Pi_{j=1}^r f_j$ is an element of Q_i since $\Pi_{j=1}^r f_j$ can be generated by entries of $(tr_i\varphi)^{\otimes \sum_{i=1}^k l_i} = [(tr_i\varphi)^{\otimes r}]^{\otimes \sum_{i=1}^k l_i/r}$, therefore, it can be generated by entries of $(tr_i\varphi)^{\otimes r}$.

For any LUIP of the original system $\mathcal{H}$, g with degree $2l$, we now show that $g(|\Psi\rangle) = g(|\Phi\rangle)$. To see this, we first choose a degree 2 LUIP f_0 be the square of 2-norm function, which satisfies that $f_0(|\Psi\rangle) \equiv f_0(|\Phi\rangle)$ according to the LU equivalence of $|\Psi\rangle^{\otimes r}, |\Phi\rangle^{\otimes r}$. Then the following equation is valid with $i + l$ divisible by r,

$$f_0^i(|\Psi\rangle)g(|\Psi\rangle) = f_0^i(|\Phi\rangle)g(|\Phi\rangle)$$

Therefore, $g(|\Psi\rangle) = g(|\Phi\rangle)$ is valid for any LUIP g.

By invoking the result that LUIPs are sufficient to separate any two distinct orbits under local unitary, we can conclude that $|\Psi\rangle, |\Phi\rangle$ are LU equivalent. ■

Similar statements are true for mixed states, and for quantum channels by recalling the relation of LU equivalence between pure states, mixed states, and unitary equivalence between quantum channels.

4. SLOCC equivalence and SLIPs

In the following, we provide an alternative algorithm to construct SLIPs. It is direct to verify that we only need to compute the invariant polynomials of group $\mathbb{SL}_i$, with $\mathbb{SL}_i = I_1 \otimes \cdots \otimes I_{i-1} \otimes \mathbb{SL}(d_i) \otimes I_{i+1} \cdots \otimes I_n$. We regard the multipartite state as a bipartite pure state which is isomorphic to a matrix, says X, and the action of the group is the left matrix multiplication, *i.e.*, $X \to LX$ with $det(L) = 1$. Fortunately, the invariant polynomials of such map are fully characterized by the ring generated by the determinant of all square matrix with columns catching from X, see [36] for more details. Then, it is direct to obtain the invariant ring of $\mathbb{SL}_i$, says R_i. After that, we can present an algorithm to construct the ring of SLIPs for the multipartite system $\mathcal{H}$, which is $\bigcap_{i=1}^n R_i$.

Observe that R_i is generated by polnomials with degree d_i, the local dimension, then the degree of any element of R_i is divisible by d_i. One can confirm the following result which was obtained by Gour and Wallach in [32]

Observation 1. *Any SLIP has degree divisible by* $lcm\{d_1, d_2, \cdots, d_n\}$*, the least common multiple of* $d_1, d_2, \cdots, d_n$.

In the following, we study the equivalence between general mixed states under the action by SLOCC by employing local invariant polynomials. Two quantum states ρ and σ of system

$\mathcal{H}$ are called equivalent under one term SLOCC if there exists invertible $d_i \times d_i$ matrices A_i such that

$$\rho = (A_1 \otimes A_2 \otimes \cdots)\sigma(A_1 \otimes A_2 \otimes \cdots)^\dagger.$$

This definition captures the SLOCC equivalence between pure states and keeps the tensor structure of the group, which enables us to characterize the local invariants. One can verify that

Proposition 1. *ρ and σ are equivalent under one term SLOCC if and only if there is some $s \in \mathbb{SLU}$ such that $|\Psi\rangle$ is proportional to $s|\Phi\rangle$, where $|\Psi\rangle, |\Phi\rangle \in \mathcal{H} \otimes \mathcal{H}_{n+1}$ are some purification of ρ, σ with d_{n+1} being the dimension of $\mathcal{H}_{n+1}$, and*

$$\mathbb{SLU} \equiv \mathbb{SL}(d_1) \otimes \mathbb{SL}(d_2) \otimes \cdots \otimes \mathbb{SL}(d_n) \otimes \mathbb{U}(d_{n+1}).$$

Now we are ready to study the local invariant polynomials of $\mathbb{SLU}$: We define invariant polynomials of $\mathbb{SLU}$ as follows. A function $f : \mathcal{H} \otimes \mathcal{H}_{n+1} \mapsto \mathbb{C}$ is an invariant polynomial of $\mathbb{SLU}$, if $f(|\Psi\rangle)$ is the homogenous polynomial on entries of Ψ, and

$$f(s|\Psi\rangle) = f(|\Psi\rangle), \ \ \forall s \in \mathbb{SLU} \ \text{ and } \ \forall |\Psi\rangle \in \mathcal{H} \otimes \mathcal{H}_{n+1}.$$

Given $|\varphi\rangle = \sum x_{j_1 \cdots j_{n+1}} |j_1 \cdots j_{n+1}\rangle$ with variables $x_{j_1 \cdots j_{n+1}} \in \mathbb{C}$, one can notice that the invariant ring, T_{n+1}, of the action of $\mathbb{U}(d_{n+1})$ is generated by $tr_{n+1}\varphi$, some polynomials of entries of φ. For $i < n+1$, one can obtain the invariant ring of $\mathbb{SL}_i$–R_i, as our previous argument in the study of SLOCC equivalence between pure states. Note that one can not directly compute the intersection of R_i and T_{n+1} since unlike T_{n+1}, R_i is generated by polynomials of $|\varphi\rangle$, not entries of φ. In order to characterize the local invariant polynomials of $\mathbb{SLU}$, one should define T_i be the ring generated by elements of R_i and R_i^*, with R_i^* standing for the complex conjugate ring of R_i. Thus, $\bigcap_{i=1}^{n+1} T_i$ is the ring of local invariant polynomials of $\mathbb{SLU}$.

5. Proof of Theorem 1

In this section, we give a detailed proof of the upper bound on the degree of generators of LUIPs (Theorem 1) and SLIPs respectively. Before doing so, we recall the celebrated result of Derksen [**?**] on the degree bounds in invariant theory.

Let G be a linearly reductive algebraic group over an algebraically closed field K of characteristic 0, acting rationally on an $s-$dimensional vector space V, specified as follows. G is given by polynomials $h_1, \ldots, h_\ell \in K[z_1, \ldots, z_t]$ such that G is the zero set of these polynomials. The action of G on V is as follows: there are polynomials $a_{i,j}$ for $i, j \le s$, $a_{i,j} \in K[z_1, \ldots, z_t]$ such that $g : G \to \mathbb{GL}(V)$ is given by $g \to (a_{i,j}(g))_{1 \le i,j \le s}$, where $\mathbb{GL}(V)$ is the general linear group of V, *i.e.*, the group of invertible matrices.

By fixing a basis of V, the polynomial functions over V are identified as $R = K[x_1, \ldots, x_s]$, and G induces an action on R. The invariant ring of G on V, denoted as R^G, consists of polynomials in R invariant under G, *i.e.*,

$$R^G = \{r : r(g \cdot v) = r(v), r \in R, \ \forall g \in G, v \in V\}.$$

It is known that R^G is finitely generated. The question here is to derive an explicit degree bound for this finite generation. To obtain this degree bound, another intermediate quantity is useful, and for this we recall the concept of nullcone of R^G: it is defined as the common zero set of all homogeneous polynomials in R^G with positive degree.

Let $\beta(V, G)$ be the minimal k such that R^G is generated by invariants of degree less than k, and $\sigma(V, G)$ be the minimal k such that the invariants of degree less than k defines the nullcone of R^G. Derksen shows that [**?**]

$$\sigma(V, G) \leq H^{t-d} A^d, \text{ and } \beta(V, G) \leq \max(2, \frac{3}{8} s \cdot \sigma(V, G)^2),$$

where $A = \max\{\deg(a_{i,j}) \mid i, j \leq s\}$, $H = \max \deg(h_i)$, and $d = \dim(G)$, the dimension of G as an algebraic variety [38].

To begin with, let us apply Derksen's bound to obtain an explicit upper bound for the degree to generate the ring of SLIPs. Let $\mathbb{S} = \mathbb{SL}(d_1, \mathbb{C}) \times \cdots \times \mathbb{SL}(d_n, \mathbb{C})$ acts on $\mathcal{H}$ in the natural way, where $\mathbb{SL}(d_i, \mathbb{C})$ is the group of invertible $d_i \times d_i$ matrices with determinant 1. In this case R is a polynomial ring over $\mathbb{C}$ in $\prod_i d_i$ variables, identified as the coordinate ring of $\mathcal{H}$. Our object is then the invariant ring $R^{\mathbb{S}}$.

Note that $\mathbb{S}$ is the zero locus of $\det(z_{i,j}^{(k)})_{i,j \in [d_k]} = 1$, $k = 1, \ldots, n$. In this setting, $t = \sum_i d_i^2$, $H = \max\{d_i \mid 1 \leq i \leq n\}$, $\dim(\mathbb{S}) = t - n$, and $A = n$. Thus

$$\sigma(\mathcal{H}, \mathbb{S}) \leq \max(d_i)^n \cdot n^{\sum_i d_i^2 - n}.$$

As $s = \dim(R^{\mathbb{S}}) \leq \prod_i d_i$, we get

$$\beta(\mathcal{H}, \mathbb{S}) \leq \frac{3}{8} \cdot (\prod_i d_i) \cdot \max(d_i)^{2n} \cdot n^{\sum_i 2d_i^2 - 2n}.$$

Therefore, the whole set of SLIPs can be generated by SLIPs with degree no more than $\frac{3}{8} \cdot (\prod_i d_i) \cdot \max(d_i)^{2n} \cdot n^{\sum_i 2d_i^2 - 2n}$.

Now we prove Theorem 1.

Proof of Theorem 1:—For a linear operation ρ in $\mathcal{H}$, $g \in \mathbb{LU} \leq \mathbb{GL}(\mathcal{H})$ acts on ρ by sending ρ to $g\rho g^\dagger = g\rho g^{-1}$. Let R be the polynomial ring in $(\prod_i d_i)^2$ variables, identified as the coordinate ring of $L(\mathcal{H}, \mathcal{H})$, and $R^{\mathbb{LU}}$ be LUIPs, *i.e.*, the invariant ring of local unitary operations.

It is not feasible to apply Derksen's bound directly, as $\mathbb{U}$ cannot be viewed as zero set of polynomials over algebraically closed field $\mathbb{C}$. This can be fixed by considering the complexification. (For the notion of complexification of compact groups, we refer the reader to [39, Page 546]. For our purpose here, the concept of complexification associates a compact connected semisimple Lie group with a semisimple connected complex Lie group, s.t. their irreducible representations "match.") In our case, the complexification of $\mathbb{U}$ yields $\mathbb{G} = \mathbb{GL}(d_1, \mathbb{C}) \times \cdots \times \mathbb{GL}(d_n, \mathbb{C}) \leq \mathbb{GL}(\mathcal{H})$. Recall that we can view R as the space of representations of $\mathbb{LU}$ and $\mathbb{G}$, and note that each invariant polynomial corresponds to the identity representation. Then by the correspondence between irreducible representations of $\mathbb{LU}$ and $\mathbb{G}$, $R^{\mathbb{LU}} = R^{\mathbb{G}}$. Thus it is enough to get a degree bound for the action of $\mathbb{G}$.

To get a degree bound for the action of $\mathbb{G}$ on R, we further notice that for this particular action, the invariants of $\mathbb{G}$ and $\mathbb{S} = \mathbb{SL}(d_1, \mathbb{C}) \times \cdots \times \mathbb{SL}(d_n, \mathbb{C})$ coincide. This allows us to apply Derksen's bounds to the group action of $\mathbb{S}$ as follows.

Firstly $s = \dim(R^{\mathbb{S}}) \leq \prod_i d_i^2$. To bound $\sigma(\mathcal{H}, \mathbb{S})$, we observe that $t = \sum_i d_i^2$, $H = \max\{d_i \mid i = 1, \ldots, n\}$, $d = \dim(\mathbb{S}) = t - n$, and $A = \sum_i d_i$. Thus

$$
\begin{aligned}
& \sigma(L(\mathcal{H}, \mathcal{H}), \mathbb{G}) \\
= \; & \sigma(L(\mathcal{H}, \mathcal{H}), \mathbb{S}) \\
\leq \; & \max(d_i)^n \cdot (\sum_i d_i)^{\sum_i d_i^2 - n}, \\
\Rightarrow \; & \beta(\text{Ł}(\mathcal{H}, \mathcal{H}), \mathbb{G}) \\
= \; & \beta(L(\mathcal{H}, \mathcal{H}), \mathbb{S}) \\
\leq \; & \frac{3}{8}(\prod_i d_i^2) \cdot \max(d_i)^{2n} \cdot (\sum_i d_i)^{2(\sum_i d_i^2 - n)}.
\end{aligned}
$$

■

It is worth mentioning that the bounds present here is not optimal in general.

6. LUIPs for two-qubit, three qubit system

In this section, a set of local unitary invariant polynomials(LUIPs) for two-qubit system is obtained by using our method as an illustrating example.

For two-qubit system, let $|\psi\rangle_{AB} = \sum_{ij=0,1} x_{ij}|ij\rangle$, then

$$
\rho_A = \begin{pmatrix} |x_{00}|^2 + |x_{01}|^2 & x_{00}x_{10}^* + x_{01}x_{11}^* \\ x_{00}^* x_{10} + x_{01}^* x_{11} & |x_{10}|^2 + |x_{11}|^2 \end{pmatrix} \quad \rho_B = \begin{pmatrix} |x_{00}|^2 + |x_{10}|^2 & x_{00}x_{01}^* + x_{10}x_{11}^* \\ x_{00}^* x_{01} + x_{10}^* x_{11} & |x_{01}|^2 + |x_{11}|^2 \end{pmatrix}.
$$

Let S_A, S_B be sets of polynomials as,

$$
\begin{aligned}
S_A &= \{|x_{00}|^2 + |x_{01}|^2, x_{00}x_{10}^* + x_{01}x_{11}^*, x_{00}^* x_{10} + x_{01}^* x_{11}, |x_{10}|^2 + |x_{11}|^2\}, \\
S_B &= \{|x_{00}|^2 + |x_{10}|^2, x_{00}x_{01}^* + x_{10}x_{11}^*, x_{00}^* x_{01} + x_{10}^* x_{11}, |x_{01}|^2 + |x_{11}|^2\}.
\end{aligned}
$$

According to the method of our main result, we can compute the LUIPs as following.

Degree 2 LUIP lies in the intersection of subspaces spanned by S_A and S_B, one only need to deal with the following equation:

$$
\begin{aligned}
& \alpha_0(|x_{00}|^2 + |x_{01}|^2) + \alpha_1(x_{00}x_{10}^* + x_{01}x_{11}^*) + \alpha_2(x_{00}^* x_{10} + x_{01}^* x_{11}) + \alpha_3(|x_{10}|^2 + |x_{11}|^2) \\
\equiv \; & \beta_0(|x_{00}|^2 + |x_{10}|^2) + \beta_1(x_{00}x_{01}^* + x_{10}x_{11}^*) + \beta_2(x_{00}^* x_{01} + x_{10}^* x_{11}) + \beta_3(|x_{01}|^2 + |x_{11}|^2).
\end{aligned}
$$

By comparing the coefficients of this equation, we know that $\alpha_0 = \alpha_3 = \beta_0 = \beta_3$ and $\alpha_1 = \alpha_2 = \beta_1 = \beta_2 = 0$, which means that the only (up to a scalar) degree 2 LUIP is

$$
\langle\psi|\psi\rangle = \sum_{ij=0,1} |x_{ij}|^2.
$$

The degree 4 LUIPs lies in the intersection of the subspaces spanned by S_A^2 and S_B^2, one only need to deal with the following equation:

$$\begin{aligned}
& \alpha_0(|x_{00}|^2+|x_{01}|^2)^2+\alpha_1(|x_{00}|^2+|x_{01}|^2)(x_{00}x_{10}^*+x_{01}x_{11}^*)+\alpha_2(|x_{00}|^2+|x_{01}|^2)(x_{00}^*x_{10}+x_{01}^*x_{11})\\
+ \; & \alpha_3(|x_{00}|^2+|x_{01}|^2)(|x_{10}|^2+|x_{11}|^2)+\alpha_4(x_{00}x_{10}^*+x_{01}x_{11}^*)^2+\alpha_5(x_{00}x_{10}^*+x_{01}x_{11}^*)(x_{00}^*x_{10}+x_{01}^*x_{11})\\
+ \; & \alpha_6(x_{00}x_{10}^*+x_{01}x_{11}^*)(|x_{10}|^2+|x_{11}|^2)+\alpha_7(x_{00}^*x_{10}+x_{01}^*x_{11})^2+\alpha_8(x_{00}^*x_{10}+x_{01}^*x_{11})(|x_{10}|^2+|x_{11}|^2)\\
+ \; & \alpha_9(|x_{10}|^2+|x_{11}|^2)^2\\
\equiv \; & \beta_0(|x_{00}|^2+|x_{10}|^2)^2+\beta_1(|x_{00}|^2+|x_{10}|^2)(x_{00}x_{01}^*+x_{10}x_{11}^*)+\beta_2(|x_{00}|^2+|x_{10}|^2)(x_{00}^*x_{01}+x_{10}^*x_{11})\\
+ \; & \beta_3(|x_{00}|^2+|x_{10}|^2)(|x_{01}|^2+|x_{11}|^2)+\beta_4(x_{00}x_{01}^*+x_{10}x_{11}^*)^2+\beta_5(x_{00}x_{01}^*+x_{10}x_{11}^*)(x_{00}^*x_{01}+x_{10}^*x_{11})\\
+ \; & \beta_6(x_{00}x_{01}^*+x_{10}x_{11}^*)(|x_{01}|^2+|x_{11}|^2)+\beta_7(x_{00}^*x_{01}+x_{10}^*x_{11})^2+\beta_8(x_{00}^*x_{01}+x_{10}^*x_{11})(|x_{01}|^2+|x_{11}|^2)\\
+ \; & \beta_9(|x_{01}|^2+|x_{11}|^2)^2.
\end{aligned}$$

By comparing the coefficients of this equation, we know that $\alpha_0=\alpha_9=\beta_0=\beta_9=\frac{\alpha_3+\alpha_5}{2}=\frac{\beta_3+\beta_5}{2}$ and $\alpha_1=\alpha_2=\alpha_4=\alpha_6=\alpha_7=\alpha_8=\beta_1=\beta_2=\beta_4=\beta_6=\beta_7=\beta_8=0$, which means that the degree 4 LUIPs are spanned by

$$\begin{aligned}
& (|x_{00}|^2+|x_{01}|^2+|x_{10}|^2+|x_{11}|^2)^2=tr^2(\rho_A)=tr^2(\rho_B),\\
& (|x_{00}|^2+|x_{01}|^2)^2+(|x_{10}|^2+|x_{11}|^2)^2+2|x_{00}x_{10}^*+x_{01}x_{11}^*|^2\\
= \; & (|x_{00}|^2+|x_{10}|^2)^2+(|x_{01}|^2+|x_{11}|^2)^2+2|x_{00}x_{01}^*+x_{10}x_{11}^*|^2=tr(\rho_A^2)=tr^2(\rho_B^2).
\end{aligned}$$

It is well known that for two-qubit pure states, the degree 2 and 4 LUIPs can generate the whole ring of LUIPs.

7. Conclusion

In this paper, we give a characterization of multipartite entanglement by exploiting a systematic method to describe the ring of all LUIPs. More precisely, we then provide an algorithm to construct a set of generators of the ring of LUIPs. By employing our structure description of LUIPs, we are able to show that multipartite entanglement is additive in the sense that two multipartite states are LU equivalent if and only if r-copies of these two states are LU equivalent for some r. This idea gives an alternative way to study the multipartite entanglement in terms of equivalence classes of states under SLOCC, even for mixed states.

Acknowledgements. We thank Prof. John Watrous, Prof. Debbie Leung and Dr. M. Grassl for their comments and Dr. S. Szalay's suggestion of references. NY is supported by NSERC, NSERC DAS, CRC, CIFAR and DE180100156. JQ is supported by the Singapore Ministry of Education and the National Research Foundation and DE150100720. XS is supported by the National Natural Science Foundation of China Grant 61170062, 61222202.

References

[1] T. A. Brun, O. Cohen, Parametrization and distillability of three-qubit entanglement, Phys. Lett. A **281**, 2-3 (2001).

[2] J. Kempe, Multiparticle entanglement and its applications to cryptography, Phys. Rev. A **60**, 910 (1999).
[3] W. Dür, G. Vidal, and J. I. Cirac, Three qubits can be entangled in two inequivalent ways, Phys. Rev. A **62**, 062314 (2000).
[4] J. Eisert and H. J. Briegel, Schmidt measure as a tool for quantifying multiparticle entanglement, Phys. Rev. A **64**, 022306 (2001).
[5] M. Hein, J. Eisert, and H. J. Briegel, Multiparty entanglement in graph states, Phys. Rev. A **69**, 062311 (2004).
[6] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde, Four qubits can be entangled in nine different ways, Phys. Rev. A **65**, 052112 (2002).
[7] G. Gour and N. R. Wallach, Necessary and sufficient conditions for local manipulation of multipartite pure quantum states, New J. Phys. **13** 073013 (2011).
[8] G. Gour and N. R. Wallach, All Maximally Entangled Four Qubits States, J. Math. Phy. **51**, 112201 (2010).
[9] N. Yu, R. Duan and M. Ying, Optimal simulation of a perfect entangler, Phys. Rev. A **81**, 032328 (2010).
[10] N. Yu, E. Chitambar, C. Guo, and R. Duan, Tensor rank of the tripartite state $|W\rangle^{\otimes n}$ Phys. Rev. A **81**, 014301 (2010).
[11] N. Yu, C. Guo, and R. Duan, Obtaining a W State from a Greenberger-Horne-Zeilinger State via Stochastic Local Operations and Classical Communication with a Rate Approaching Unity, Phys. Rev. Lett. **112**, 160401 (2014).
[12] N. Yu, Multipartite W-type state is determined by its single-particle reduced density matrices among all W-type states, Phys. Rev. A **87**, 052310 (2013).
[13] A. Miyake, F. Verstraete, Multipartite entanglement in $2 \times 2 \times n$ quantum systems, Phys. Rev. A **69**, 012101 (2004).
[14] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, A.V. Thapliyal, Exact and asymptotic measures of multipartite pure-state entanglement, Phys. Rev. A **63**, 012307 (2000).
[15] S. Szalay, All degree six local unitary invariants of k qudits, J. Phys. A **45**, 065302, (2012).
[16] M. W. Hero and J. F. Willenbring, Stable Hilbert series as related to the measurement of quantum entanglement, Discrete Mathematics, 309(23-24):6508-6514, (2009).
[17] M, W. Hero, J. F. Willenbring, and L. K. Williams, The measurement of quantum entanglement and enumeration of graph coverings, arXiv:0911.0222.
[18] P. Vrana, Local unitary invariants for multipartite quantum systems, J. Phys. A, **44**, 115302, 2011.
[19] P. Vrana, On the algebra of local unitary invariants of pure and mixed quantum states, J. Phys. A, **44** 225304, 2011.
[20] S. Albeverio, S. M. Fei, P. Parashar, W. L. Yang, Nonlocal properties and local invariants for bipartite systems, Phys. Rev. A **68**, 010303(2003).
[21] Z. Wang, H. Wang, Z. Wang, S. Fei, Local unitary equivalent consistence for n-party states and their (n-1)-party reduced density matrices, Chin. Phys. Lett. **28**, 020302 (2011).
[22] C. Zhou, T. G. Zhang, S. M. Fei, N. Jing, and X. Li-Jost, Local unitary equivalence of arbitrary dimensional bipartite quantum states Phys. Rev. A **86**, 010303(2012).
[23] A. Osterloh, D. Z. Djokovic, On polynomial invariants of several qubits, J. Math. Phys. 50, 033509 (2009).
[24] B. Kraus, Local Unitary Equivalence of Multipartite Pure States, Phys. Rev. Lett. **104**, 020504(2010).
[25] B. Kraus, Local unitary equivalence and entanglement of multipartite pure states, Phys. Rev. A 82, 032121(2010).
[26] E.M. Rains, Polynomial invariants of quantum codes, IEEE Transactions on Information Theory, **46**, 1 (2000).
[27] D. A. Meyer, N. R. Wallach, Global entanglement in multiparticle systems, Mathematics of quantum computation, 77-97. (2002).
[28] M. Grassl, M. Rotteler and T. Beth, Computing local invariants of quantum-bit systems, Phys. Rev.

A **58**, 1833 (1998).
[29] Y. Makhlin, Nonlocal properties of two-qubit gates and mixed states and optimization of quantum computations, Quant. Info. Proc. **1**, 243-252 (2002).
[30] A. Sudbery, On local invariants of pure three-qubit states, J. Phys. A **34**, 643-652 (2001).
[31] N. R. Wallach, The Hilbert series of measures of entanglement for 4 qubits, Acta Appl. Math. **86**, 203-220 (2005).
[32] G. Gour, and N. R. Wallach, Classification of Multipartite Entanglement of All Finite Dimensionality, Phys. Rev. Lett. **111**, 060502 (2013).
[33] A. Uhlmann, The "transition probability" in the state space of a *-algebra, Rep. Math. Phys. **9**, 2730-79 (1976).
[34] Harm Derksen, and Visu Makam, Polynomial degree bounds for matrix semi-invariants, arXiv:1512.03393.
[35] Gabor Ivanyos, and Youming Qiao, and K. V. Subrahmanyam, Constructive noncommutative rank computation in deterministic polynomial time over fields of arbitrary characteristics, arXiv:1512.03531.
[36] H Kraft and C. Procesi, Classical invariant theory, a primer(1996).
[37] L. Gurvits, Classical deterministic complexity of Edmonds problem and quantum entanglement, Proceedings of the 35th ACM Symposium on Theory of Computing, ACM Press, New York, 2003.
[38] Let W be an algebraic set defined as the set of the common zeros of an ideal I in a polynomial ring $R = K[x_1, \dots, x_n]$ over a field K, and let $A = R/I$ be the algebra of the polynomials over W. Then the dimension of W is: The maximal length d of the chains $V_0 \subset V_1 \subset \dots \subset V_d$ of distinct nonempty subvarieties.
[39] M. A. Naĭmark, A. I. Štern, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 246. Springer-Verlag, New York, 1982.