

# A Complete Set of Invariants for LU-Equivalence of Density Operators

Jacob TURNER<sup>†</sup> and Jason MORTON<sup>‡</sup>

<sup>†</sup> Korteweg-de Vries Institute, University of Amsterdam, 1098 XG Amsterdam, The Netherlands

E-mail: [jacob.turner870@gmail.com](mailto:jacob.turner870@gmail.com)

URL: <http://www.jacobwadeturner.weebly.com>

<sup>‡</sup> Department of Mathematics, The Pennsylvania State University,

University Park, PA 16802, USA

E-mail: [morton@math.psu.edu](mailto:morton@math.psu.edu)

Received November 26, 2016, in final form April 28, 2017; Published online May 02, 2017

<https://doi.org/10.3842/SIGMA.2017.028>

**Abstract.** We show that two density operators of mixed quantum states are in the same local unitary orbit if and only if they agree on polynomial invariants in a certain Noetherian ring for which degree bounds are known in the literature. This implicitly gives a finite complete set of invariants for local unitary equivalence. This is done by showing that local unitary equivalence of density operators is equivalent to local GL equivalence and then using techniques from algebraic geometry and geometric invariant theory. We also classify the SLOCC polynomial invariants and give a degree bound for generators of the invariant ring in the case of  $n$ -qubit pure states. Of course it is well known that polynomial invariants are not a complete set of invariants for SLOCC.

*Key words:* quantum entanglement; local unitary invariants; SLOCC invariants; invariant rings; geometric invariant theory; complete set of invariants; density operators; tensor networks

*2010 Mathematics Subject Classification:* 20G05; 20G45; 81R05; 20C35; 22E70

## 1 Introduction

Consider the *local unitary* group  $U_{\mathbf{d}} := \times_{i=1}^n U(\mathbb{C}^{d_i})$ , a product of unitary groups where  $d = (d_1, \dots, d_n)$  are positive integer dimensions. Let  $V_i$  be a  $d_i$ -dimensional complex Hilbert space and  $V = \otimes_{i=1}^n V_i$ . Then  $U_{\mathbf{d}}$  acts on the vector space  $\text{End}(V) = \otimes_{i=1}^n \text{End}(V_i)$ ,  $\dim(V_i) = d_i$ , by linear extension of the action

$$\times_{i=1}^n g_i \cdot \left( \bigotimes_{i=1}^n M_i \right) := \bigotimes_{i=1}^n g_i M_i g_i^{-1}.$$

This in turn can be naturally extended to an action on  $\text{End}(V)^{\oplus m}$  by simultaneous conjugation.

This action on density operators is important for understanding entanglement of quantum states [3, 14, 15, 16, 21, 25, 32, 33, 35]. Many of the most important notions of entanglement are invariant under the action of  $U_{\mathbf{d}} := \times_{i=1}^n U(\mathbb{C}^{d_i})$  [11, 34]. Entanglement in turn relates to quantum computation [38, 42], quantum error correction [38], and quantum simulation [31]. Two density operators in the same  $U_{\mathbf{d}}$  orbit are said to be local unitary (LU)-equivalent.

When considering the local unitary equivalence of two mixed quantum states, one can either take two views: the first is that the entire system as a whole is related by a local unitary change of basis. In this case we look at a single density operator acted on by  $U_{\mathbf{d}}$ . The second is that by considering the same change of basis on each pure state in the mixture, one can take one mixed system to the other. In the latter case, we are looking at local unitary group acting

in a simultaneous fashion on the  $m$  pure states in the mixed state. Furthermore, our proofs are simplified by considering the problem of classifying the invariants of  $\text{End}(V)^{\oplus m}$  for all  $m$  simultaneously.

In this paper, we concern ourselves with the problem of finding a *complete set of invariants* for density operators. By this we mean a set of  $U_{\mathbf{d}}$ -invariant functions  $f_1, \dots, f_s$  such that two density operators  $\Psi_1$  and  $\Psi_2$  are in the same  $U_{\mathbf{d}}$  orbit if and only if  $f_i(\Psi_1) = f_i(\Psi_2)$  for all  $i$ . In the first part of this paper, we will restrict our attention to polynomial invariants of this action.

**Remark 1.1.** As a caveat: throughout this paper, when we say polynomial invariants, we mean those invariants that are polynomials in the ring  $\mathbb{C}[v_1, \dots, v_n]$  where the  $v_i$  are a basis for space  $\text{End}(V)$  viewed as a *complex vector space*. Quite frequently in the physics literature, the term polynomial invariant refers to polynomials in the basis of  $\text{End}(V)$  as a real vector space. This allows for invariants such as the Hermitian form. It is known that the set of all polynomial invariants found by viewing  $\text{End}(V)$  as a real vector space is complete [39]. It is an interesting consequence of our main theorem, however, that this larger set of polynomial invariants is not necessary for finding a complete set of invariants, which is important if we wish to find minimal complete sets of invariants.

We denote the ring of invariants for  $G \curvearrowright V$ ,  $V$  a vector space over a field  $k$ , by  $k[V]^G$ . We recall that  $k[V]$  is to be interpreted as the polynomial ring  $k[v_1, \dots, v_n]$  where  $v_1, \dots, v_n$  form a basis for  $V$ . This paper focuses on the completeness of these invariants; finiteness results have been found previously by exhibiting degree bounds on generators and we do not make further contributions in this regard. We show that for density operators in  $\text{End}(V)$ , polynomial invariants of degree at most

$$\max \left\{ 2, \frac{3}{8} \max\{d_i\} m^2 \dim(V)^4 (2n)^{2\delta} \right\},$$

where  $\delta = \sum_{i=1}^m (d_i - 1)$  distinguish their orbits (Corollary 4.11).

Throughout this paper, whenever possible, our theorems hold for the invariant ring  $k[\text{End}(V)]^{\text{GL}_{\mathbf{d}}}$ , where  $k$  is an algebraically closed field of characteristic zero which has a Hilbert space structure. Otherwise,  $k = \mathbb{C}$ . We wish to find a finite (and preferably small) generating set of invariants. We consider the constant

$$\beta_G(V) := \min \{d \mid k[V]^G \text{ is generated by polynomials of degree } \leq d\}.$$

Upper bounds for this constant have been studied in previous works. We discuss the specific upper bounds for  $\beta_{U_{\mathbf{d}}}(\text{End}(V)^{\oplus m})$  that arise from general bounds given in the literature, thus giving a finite set of invariants that we show is complete.

We now give a brief example to show why completeness of invariants is a non-trivial phenomenon requiring proof. Indeed, it is far from obvious that one cannot find two density operators that are not in the same local unitary orbit but take the same value for every polynomial invariant evaluated on them.

**Example 1.2.** Consider  $\mathbb{C}^2$  being acted upon by the group  $\mathbb{C}^{\times}$  in the following manner:  $\lambda.(x, y) := (\lambda x, \lambda^{-1} y)$ . It is clear that the only invariant is  $xy$ . However, if  $xy = 0$ , then there are three distinct orbits that  $(x, y)$  could be in:  $X := \{(x, 0) \mid x \in \mathbb{C} \setminus \{0\}\}$ ,  $Y := \{(0, y) \mid y \in \mathbb{C} \setminus \{0\}\}$ , or the origin. So we say that these three orbits, while distinct, cannot be separated (or distinguished) by invariants. This problem can be seen in this example in the following way: most orbits are hyperbolas defined by  $xy = c$  for  $c \neq 0$ . Therefore each of these orbits is a Euclidean closed subset.

However, for the three problematic orbits, two of them are not closed and contain the origin in their closure. As such, given any continuous function constant on  $Y$ , it is also constant on the whole  $y$ -axis. Similarly for the functions constant on  $X$ . Given any continuous function that is constant on orbits, we see that it must take the same value on  $X$  and  $Y$  since it is constant on the entire  $x$ -axis and constant on the entire  $y$ -axis and these two sets intersect.

The goal of this paper is to show that such a phenomenon does not occur if we restrict our attention to density matrices under the local unitary action.

The above example contained orbits that could not be distinguished even by all *continuous invariants* (as opposed to just the polynomial invariants) and thus we could use the Euclidean topology to understand the problem. However, since we are interested in polynomial invariants, the more natural topology is the Zariski topology. We wish to show that the Zariski closure of two  $U_{\mathbf{d}}$  orbits of two inequivalent density operators do not intersect. Throughout the paper, we will assume that we are working in the Zariski topology. When we say the closure of a set  $X$ , which we will denote  $\overline{X}$ , we will mean the Zariski closure.

We remind the reader that the Zariski closure of a set  $X$  is the largest set  $\overline{X}$ , containing  $X$ , such that every polynomial that vanishes identically on  $X$  must also vanish identically on  $\overline{X}$ . If  $X = \overline{X}$ , we say that  $X$  is *Zariski closed*. We call  $X$  *Zariski dense* in  $Y$  if every polynomial that vanishes identically on  $X$  must vanish identically on  $Y$ .

We wish to use techniques from classical invariant theory and algebraic geometry. The group  $U_{\mathbf{d}}$  does not satisfy the necessary conditions for the theorems we wish to use (it is not reductive). So instead, we consider the group  $GL_{\mathbf{d}} := \times_{i=1}^n GL(\mathbb{C}^{d_i})$ , which is reductive (over  $\mathbb{C}$ , this means that all of its rational representations are semi-simple). We shall see that for this group action, the Zariski closure of the orbits will actually coincide with its Euclidean closure. This simplifies the problem greatly. We note that throughout the paper, a  $GL_{\mathbf{d}}$  orbit or set is not assumed to be closed unless explicitly stated.

We say that a group  $G$  acts on a vector  $V$  rationally, or equivalently, is a rational representation if the map  $G \rightarrow \text{End}(V)$  is given in every coordinate by a rational function that is well-defined everywhere on  $G$ . The following two propositions tell us that studying  $GL_{\mathbf{d}}$  is sufficient. Rational functions are continuous maps *with respect to the Zariski topology* and so send Zariski dense subsets to Zariski dense subsets.

**Proposition 1.3.** *If  $H$  is a Zariski dense subgroup of  $G$  and  $\rho$  is a rational representation of  $G$  acting on a vector space  $V$ ,  $k[V]^G = k[V]^H$ .*

**Proof.** The representation  $\rho$  is a continuous map from  $G \rightarrow GL(V)$  with respect to the Zariski topology by assumption of the rationality of the representation. For every  $v \in V$ , consider the map  $\varphi_v: G \rightarrow G.v$  given by  $g \mapsto g.v$ . This is also a continuous map and it implies that for every  $v \in V$ ,  $H.v$  is dense in  $G.v$  since the continuous image of dense sets are dense. The invariant ring is the ring of polynomials which are constant on orbit closures. Since the orbit closures of  $H$  and  $G$  coincide, their invariant rings must be the same. ■

It is well known that  $U(\mathbb{C}^{d_i})$  is a Zariski dense subgroup of  $GL(\mathbb{C}^{d_i})$ , a fact sometimes known as Weyl's trick. This implies that  $U_{\mathbf{d}}$  is Zariski dense in  $GL_{\mathbf{d}}$ , so  $\mathbb{C}[\text{End}(V)^{\oplus m}]^{U_{\mathbf{d}}} = \mathbb{C}[\text{End}(V)^{\oplus m}]^{GL_{\mathbf{d}}}$ . Furthermore, the action  $GL_{\mathbf{d}} \curvearrowright \text{End}(V)^{\oplus m}$  is not faithful since conjugating a matrix  $M$  by  $\alpha I$  for  $\alpha \in \mathbb{C}$  leaves  $M$  fixed. Therefore, we have that  $\mathbb{C}[\text{End}(V)^{\oplus m}]^{SU_{\mathbf{d}}} = \mathbb{C}[\text{End}(V)^{\oplus m}]^{SL_{\mathbf{d}}} = \mathbb{C}[\text{End}(V)^{\oplus m}]^{GL_{\mathbf{d}}}$ .

**Proposition 1.4.** *Two Hermitian matrices are in the same  $GL_{\mathbf{d}}$  orbit if and only if they are in the same  $U_{\mathbf{d}}$  orbit.*

**Proof.** Consider the polar decomposition of  $\otimes_{i=1}^n g_i = (\otimes_{i=1}^n p_i)(\otimes_{i=1}^n u_i)$  where the  $p_i$  are invertible Hermitian matrices and the  $u_i$  are unitary. We can assume without loss of generality

that all  $u_i = \text{id}$  since it does not change the  $U_{\mathbf{d}}$  orbit we are in. So note that  $P = \otimes_{i=1}^n p_i$  is a Hermitian matrix. Let  $H$  be Hermitian and suppose that  $PHP^{-1}$  is Hermitian. Then  $PHP^{-1} = (PHP^{-1})^\dagger = P^{-1}HP$ , implying that  $P^2HP^{-2} = H$ . This implies that either  $P$  commutes with  $H$ , and thus  $PHP^{-1}$  is in the same  $U_{\mathbf{d}}$  orbit as  $H$ , or  $P^2 = PP^\dagger = \text{id}$ , implying that  $P$  was unitary. ■

By restricting the invariant functions we study to be polynomials, Propositions 1.3 and 1.4 tell us that we can focus our attention instead on the ring  $\mathbb{C}[\text{End}(V)]^{\text{GL}_{\mathbf{d}}}$ . However, we may run into the problem that two density operators are in distinct  $\text{GL}_{\mathbf{d}}$  orbits but cannot be distinguished by invariant polynomials. We show in Section 4 that  $\text{GL}_{\mathbf{d}}$  orbits of density operators can always be separated by invariant polynomials.

## 1.1 Background

Previous work on LU-equivalence includes both the invariant theory and normal form approaches. Invariants for LU-equivalence are studied in [15] and much work has been done to understand the invariant rings especially in the case  $V_i \cong \mathbb{C}^2$  [49, 51, 52].

Many polynomial invariants (as well as other invariants) have been identified for this group action. In fact, all polynomial invariants have been found, however this fact has not been proven. We do so in this paper. Invariant based approaches are sometimes criticized because of the difficulty of interpreting the invariants [29, 48].

A necessary and sufficient condition for LU-equivalence of a generic class of multipartite pure qubit states is given by Kraus in [25] using a normal form. In [50] the non-degenerate mixed qudit case is covered. Finally a necessary and sufficient condition for LU-equivalence of multipartite mixed states, including degenerate cases, is given by Zhang et al. in [49], also based on a normal form. A similar normal form is given in [29, 30] based on HOSVD. The mixed case is treated by purification, so  $\rho \sim \rho$  if and only if  $\Psi_\rho \sim \Psi_\rho$ .

The normal form approaches work by locally diagonalizing the density operator. They require that the coefficients of the pure or mixed states be known precisely and explicitly so that the normal forms may be computed. However, given two quantum states in the laboratory, determining the density operators  $\Psi_1$  and  $\Psi_2$  is not necessarily feasible.

Nevertheless, computing the values of invariant polynomials for a density operator may not require such knowledge. Given a *bipartition*  $A : B$  of  $V$ , where  $A$  and  $B$  are complementary subsystems, and a density operator  $\rho$ , we then note the following equality

$$\text{Tr}(\text{Tr}_A(\rho)^q) = \exp((1-q)H_q^{AB}(\rho)),$$

which is a polynomial for  $q$  a natural number. The Rényi entropies [2, 3, 4, 12, 44] are a well-studied measurement of entanglement. Positive integral ( $q \in \mathbb{Z}_{\geq 1}$ ) Rényi entropies can be measured experimentally without computing the density operators explicitly [1, 7, 9, 41, 45]. This suggests that it may be possible to compute the value of  $\Psi_1$  on an invariant without computing  $\Psi_1$ . This would mean that the invariant polynomials can be expressed as a series of measurements that can be carried out on a quantum state in the laboratory. However, whether or not this is true is still unresolved.

## 1.2 Organization of the paper

In Section 2, we cover the preliminaries of invariant theory we shall need. In Section 3, we classify the invariants of  $\text{GL}_{\mathbf{d}}$  acting  $\text{End}(V)^{\oplus m}$ ; Theorem 3.5 gives the result. In Section 4 we prove the title result. Theorem 4.7 and Corollary 4.8 show that density operators can be distinguished by polynomial invariants. We then draw on results from different sources to find finite sets of polynomial invariants that are complete. Lastly, in Section 5, we discuss a related problem in the

study of quantum entanglement. Given the group  $\mathrm{SL}_{\mathbf{d}} := \times_{i=1}^n \mathrm{SL}(\mathbb{C}^{d_i})$ , there is an action on  $V$  by  $(g_1, \dots, g_n).v := (\otimes_{i=1}^n g_i)v$ . There has been much research done on computing invariants of this action, known as SLOCC. An algorithm was given that computes all such invariants [14]. For small numbers of qubits (up to four), finite generating sets are explicitly known [40, 47] (although there was a misprint in [47] that was corrected in [8]). Work has been done for higher numbers of qubits [15, 16, 33]. In Theorem 5.6, we classify all invariants for this action for any number of qubits.

## 2 Preliminaries

In this section, we state the necessary definitions and theorems we shall need for the rest of this paper.

**Definition 2.1.** A function  $f \in k[V_1 \oplus \dots \oplus V_r]$  is *multihomogeneous* of degree  $t = (t_1, \dots, t_r)$  if  $f(\lambda_1 v_1, \dots, \lambda_r v_r) = \lambda_1^{t_1} \dots \lambda_r^{t_r} f(v_1, \dots, v_r)$ .

**Definition 2.2.** Suppose  $f \in k[V_1^{\oplus t_1} \oplus \dots \oplus V_r^{\oplus t_r}]$  is a multilinear polynomial. Then the restitution of  $f$ ,  $\mathcal{R}f \in k[V_1 \oplus \dots \oplus V_r]$  is defined by

$$\mathcal{R}f(v_1, \dots, v_r) = f(\underbrace{v_1, \dots, v_1}_{t_1}, \dots, \underbrace{v_r, \dots, v_r}_{t_r}).$$

The result is a multihomogeneous function.

The notion of restitution simply makes formal the idea that if one is given a multilinear function  $f(X_1, \dots, X_m)$ , then one may force some of the variables to be equal and the resulting function is no longer multilinear. For example, the function  $\mathrm{Tr}(XY^2)$  is not multilinear in the variables  $X$  and  $Y$ . However, it may be seen as the multilinear function  $\mathrm{Tr}(XYZ)$  where we have imposed the restriction that  $Y = Z$ . Thus  $\mathrm{Tr}(XY^2)$  is a multihomogeneous function that is a restitution of the multilinear function  $\mathrm{Tr}(XYZ)$ .

By taking restitutions of multilinear invariants, we can recover generators for the ring of all invariants. An important observation that we shall use later is that if two representations have the same multilinear invariants, then their invariant rings coincide.

Invariant rings can always be generated by multihomogeneous polynomials. The reason for this is that the action of a linear group does not change the degree of the polynomials since it only involves a linear change of variables.

**Proposition 2.3** ([24]). *Let  $V_1, \dots, V_m$  be representations of a group  $G$ . Then every multihomogeneous invariant  $f \in k[V_1 \oplus \dots \oplus V_m]^G$  of degree  $t = (t_1, \dots, t_m)$  is the restitution of a multilinear invariant  $F \in k[V_1^{\oplus t_1} \oplus \dots \oplus V_m^{\oplus t_m}]^G$ .*

So while it is not true that every invariant is the restitution of a multilinear invariant, the restitutions of multilinear invariants will generate the invariant ring. Furthermore, this ring is finitely generated for certain kinds of groups.

**Theorem 2.4** ([17, 18]). *If  $W$  is a  $G$ -module and the induced action on  $k[W]$  is completely reducible, the invariant ring  $k[V]^G$  is finitely generated.*

So we know by the above Theorems that  $k[\mathrm{End}(V)^{\oplus m}]^{\mathrm{GL}_{\mathbf{d}}}$  is always finitely generated.

**Definition 2.5.** The *null cone* of an action  $G \curvearrowright V$  is the set vectors  $v$  such that  $0 \in \overline{G.v}$ . We denote it by  $\mathcal{N}_V$ . Equivalently,  $\mathcal{N}_V$  are those  $v \in V$  such that  $f(v) = f(0)$  for all invariant polynomials  $f$ .

When studying orbit closures, the following theorem is a powerful tools when dealing with reductive groups. It gives a picture of which orbits cannot be distinguished from each other by means of polynomial invariants.

**Theorem 2.6** ([6, 36]). *Given an action of an algebraic group  $G \curvearrowright V$ , the orbit closure  $\overline{G.x}$  is the union of  $G.x$  and orbits of strictly smaller dimension. An orbit of minimal dimension is closed, thus every closure  $\overline{G.x}$  contains a closed orbit. Furthermore, this closed orbit is unique.*

The following theorem gives us a way to reason about points in the orbit closure of a reductive group action that are not in the orbit. Indeed, as it turns out, all such boundary points can be found as endpoints of a path inside of the orbit. This, combined with the fact that every Zariski closed set is Euclidean closed, implies that for reductive group actions, the Zariski closure and Euclidean closure of an orbit coincide.

**Theorem 2.7** (the Hilbert–Mumford criterion [22]). *For a linearly reductive group  $G$  acting on a variety  $V$ , if  $\overline{G.w} \setminus G.w \neq \emptyset$ , then there exists a  $v \in \overline{G.w} \setminus G.w$  and a 1-parameter subgroup (or cocharacter)  $\lambda: k^\times \rightarrow G$  (where  $\lambda$  is a homomorphism of algebraic groups), such that  $\lim_{t \rightarrow 0} \lambda(t).w = v$ .*

Note that for the action of  $\mathrm{GL}_{\mathbf{d}} \curvearrowright \mathrm{End}(V)$ , if  $G.w$  is not closed, then for any  $v \in \overline{G.w} \setminus G.w$ , there is a cocharacter  $\lambda(t)$  such that  $\lim_{t \rightarrow 0} \lambda(t)w\lambda(t)^{-1} = v$ . Indeed, we know that if  $\overline{G.w} \setminus G.w \neq \emptyset$ , there is some  $v'$  and cocharacter  $\mu(t)$  such that  $\lim_{t \rightarrow 0} \mu(t)w\mu(t)^{-1} = v' = gvg^{-1}$  for some  $g \in \mathrm{GL}_{\mathbf{d}}$ . Then note that if we define  $\lambda(t) = g^{-1}\mu(t)g$ , we get a cocharacter of  $\mathrm{GL}_{\mathbf{d}}$  sending  $w$  to  $v$  as desired.

So we have that every orbit class has a unique representative given by a closed orbit and every closed orbit trivially lies in some orbit class. This motivates the definition of different types of points in  $V$  with respect to an action of  $G$ .

**Definition 2.8.** Given an action  $G \curvearrowright V$  and a point  $v \in V \setminus \{0\}$ , then  $v$  is called

- (a) an *unstable point* if  $0 \in \overline{G.v}$ ,
- (b) a *semistable point* if  $0 \notin \overline{G.v}$ ,
- (c) a *polystable point* if  $G.v$  is closed,
- (d) or a *stable point* if  $G.v$  is closed and the stabilizer of  $v$  is finite.

These definitions have been reinterpreted in terms of the study of entanglement of pure states by Klyachko [23]. For example, every stable point is in the orbit of a completely entangled state and entangled states are simply the semistable points.

Given an action of a reductive group  $G \curvearrowright V$ , there is a way to write every vector that highlights whether or not its orbit is closed and a representative in the closed orbit its orbit closure contains.

**Definition 2.9.** Given an action  $G \curvearrowright V$ , a *Jordan decomposition* of a point  $v$  is given by  $v = v_s + v_n$  where  $v_s$  is a polystable point and  $v_n$  is an unstable point.

For a rational representation of a reductive group  $G \curvearrowright V$ , such a Jordan decomposition always exists, although it is not unique. This is well known (cf. [27]), but we include a proof for completeness.

**Theorem 2.10.** *For a reductive group action  $\varphi: G \rightarrow \mathrm{GL}(V)$  a Jordan decomposition always exists.*

**Proof.** By Theorem 2.6,  $\overline{\varphi(G)v}$  contains a polystable point  $v_s$ , and by the Hilbert–Mumford criterion (Theorem 2.7), there exists a cocharacter  $\lambda(t): k^\times \rightarrow G$  such that  $\lim_{t \rightarrow 0} \varphi(\lambda(t))v$  is polystable. Since  $\varphi(\lambda(t))$  is diagonalizable, there is some  $g \in \mathrm{GL}(V)$  such that  $\lim_{t \rightarrow 0} g\varphi(\lambda(t))g^{-1}gv = gv_s$  for some  $v_s \in V$ .

Now if  $g\varphi(\lambda(t))g^{-1}$  is diagonal, then  $g\varphi(\lambda(t))v$  is the vector  $gv$  with every entry multiplied by a some non-negative power of  $t$  (since the limit exists). The unstable part of  $gv$ , denoted  $gv_n$ , is the all zero vector except for those entries of  $gv$  that get multiplied by a positive power of  $t$ . The stable part is  $gv_s = gv - gv_n$ . Then we see that  $\lim_{t \rightarrow 0} g\varphi(\lambda(t))g^{-1}gv_s = gv_s$  and so  $\lim_{t \rightarrow 0} \varphi(\lambda(t))v_s = v_s$ . Then we let  $v_n = v - v_s$ . We quickly see that  $\lim_{t \rightarrow 0} \varphi(\lambda(t))v = v_s$  and thus  $\lim_{t \rightarrow 0} \varphi(\lambda(t))v_n = 0$ . Then  $v = v_s + v_n$  is the Jordan decomposition.  $\blacksquare$

### 3 Describing the ring $k[\mathrm{End}(V)^{\oplus m}]^{\mathrm{GL}_{\mathbf{d}}}$

In this section, we describe the invariant ring  $k[\mathrm{End}(V)^{\oplus m}]^{\mathrm{GL}_{\mathbf{d}}}$  by giving a description of all multihomogeneous elements of said ring. We follow Kraft and Procesi’s (specifically Chapter 4 in [24]) treatment of the fundamental theorems, generalizing to local conjugation by  $\mathrm{GL}_{\mathbf{d}}$ ; see also Leron [28].

Let us consider the representation of  $\mathrm{GL}_{\mathbf{d}}$  given by  $\mu: \mathrm{GL}_{\mathbf{d}} = \times_{i=1}^n \mathrm{GL}(k^{d_i}) \rightarrow \mathrm{End}(V^{\otimes m})$  defined by

$$\mu(g_1, \dots, g_n) \bigotimes_{i=1}^n \bigotimes_{j=1}^m v_{ij} := \bigotimes_{i=1}^n \bigotimes_{j=1}^m g_i v_{ij}$$

extended linearly. Let  $\mathcal{S}_m^n$  be the  $n$ -fold product of the symmetric group of order  $m$ . The  $\mathrm{GL}_{\mathbf{d}}$  action commutes with the representation of  $\rho: \mathcal{S}_m^n \rightarrow \mathrm{End}(V^{\otimes m})$  defined by

$$\rho(\sigma_1, \dots, \sigma_n) \bigotimes_{i=1}^n \bigotimes_{j=1}^m v_{ij} := \bigotimes_{i=1}^n \bigotimes_{j=1}^m v_{i\sigma_i^{-1}(j)}$$

extended linearly. We will show that the centralizer of this action of  $\mathrm{GL}_{\mathbf{d}}$  is precisely the described action of  $\mathcal{S}_m^n$ . In the case of  $n = 1$ , the group algebra of  $\mathcal{S}_m$  is precisely the centralizer of  $\mathrm{GL}(V)$  acting on this space. Furthermore, over an algebraically closed field, the centralizer of the centralizer of an algebra is the original algebra. This a classical theorem called the *double centralizer theorem* (cf. [26]).

Given a representation  $\varphi: G \rightarrow \mathrm{End}(V^{\otimes m})$ , denote by  $\langle G \rangle_\varphi$  the linear span of the image of  $G$  under the map  $\varphi$ . We denote the centralizer of the image of  $\mu$  by  $\mathrm{End}_{\mathrm{GL}_{\mathbf{d}}}^\mu(V^{\otimes m})$  and the centralizer of the image of  $\rho$  by  $\mathrm{End}_{\mathcal{S}_m^n}^\rho(V^{\otimes m})$ . The following result has appeared before frequently in the literature (for example [15]) but we know of no place where a proof is written down.

**Theorem 3.1.** *Given the described representations  $\mu$  and  $\rho$ , then*

- (a)  $\mathrm{End}_{\mathcal{S}_m^n}^\rho(V^{\otimes m}) = \langle \mathrm{GL}_{\mathbf{d}} \rangle_\mu$ .
- (b)  $\mathrm{End}_{\mathrm{GL}_{\mathbf{d}}}^\mu(V^{\otimes m}) = \langle \mathcal{S}_m^n \rangle_\rho$ .

**Proof.** Part (b) follows from part (a) by the double centralizer theorem. Now consider the isomorphism  $\varphi: \mathrm{End}(V)^{\otimes m} \cong \mathrm{End}(V^{\otimes m})$  given by

$$\varphi \left( \bigotimes_{i=1}^n \bigotimes_{j=1}^m M_{ij} \right) \left( \bigotimes_{i=1}^n \bigotimes_{j=1}^m v_{ij} \right) = \bigotimes_{i=1}^n \bigotimes_{j=1}^m M_{ij} v_{ij}.$$



We want to find those elements of  $\text{End}(V^{\otimes m})$  which commute with  $\mathcal{S}_m^n$ . So let  $\sigma = (\sigma_1, \dots, \sigma_n) \in \mathcal{S}_m^n$  and consider

$$\begin{aligned} \sigma \varphi \left( \bigotimes_{i=1}^n \bigotimes_{j=1}^m M_{ij} \right) \left( \sigma^{-1} \left( \bigotimes_{i=1}^n \bigotimes_{j=1}^m v_{ij} \right) \right) &= \sigma \left( \bigotimes_{i=1}^n \bigotimes_{j=1}^m M_{ij} v_{i\sigma_i(j)} \right) \\ &= \bigotimes_{i=1}^n \bigotimes_{j=1}^m M_{i\sigma_i^{-1}(j)} v_{ij} = \varphi \left( \bigotimes_{i=1}^n \bigotimes_{j=1}^m M_{i\sigma_i^{-1}(j)} \right) \left( \bigotimes_{i=1}^n \bigotimes_{j=1}^m v_{ij} \right). \end{aligned}$$

The map  $\varphi$  induces an isomorphism from  $\text{End}_{\mathcal{S}_m^n}^\rho(V^{\otimes m})$  to the subalgebra  $\Sigma_{\mathbf{d}}$  of  $\text{End}(V)^{\otimes m}$  that is  $\mathcal{S}_m^n$  invariant under the induced action. We look at its decomposition as a  $\mathcal{S}_m^n$  module. Since  $\mathcal{S}_m^n$  acts trivially on it, every non-zero irreducible submodule will be one dimensional. Every irreducible representation of  $\mathcal{S}_m^n$  is the tensor product of  $n$  irreducible  $\mathcal{S}_m$  modules. So we see that an irreducible  $\mathcal{S}_m^n$  submodule of  $\Sigma_{\mathbf{d}}$  is spanned by a vector  $s_1 \otimes \dots \otimes s_n$  where each  $s_i$  is a symmetric tensor in  $\text{End}(V_i)^{\otimes m}$  since it is invariant under  $\mathcal{S}_m$ .

So we see that  $\Sigma_{\mathbf{d}} = \bigotimes_{i=1}^n \Sigma_m^i$  where  $\Sigma_m^i$  are the symmetric tensors of  $\text{End}(V_i)^{\otimes m}$ . However, it is known that  $\Sigma_m^i$  is generated as an algebra by elements of the form  $\bigotimes_{i=1}^m g_i$  for  $g_i \in \text{GL}(V_i)$ , i.e.,  $\Sigma_m^i = \langle \text{GL}(V_i) \rangle_{\mu_i}$ , where  $\mu_i$  is the restriction to  $\text{GL}(V_i) \curvearrowright V_i^{\otimes m}$ . This fact is the classical case of the centralizer algebra of the general linear group [5].

So we get  $\Sigma_{\mathbf{d}} = \bigotimes_{i=1}^n \langle \text{GL}(V_i) \rangle_{\mu_i}$ . However, this algebra is clearly generated as an algebra by elements of the form  $g_1^{\otimes m} \otimes \dots \otimes g_n^{\otimes m}$  and so we get that  $\Sigma_{\mathbf{d}} \cong \langle \text{GL}_{\mathbf{d}} \rangle_{\mu}$ . So we get the equality  $\text{End}_{\mathcal{S}_m^n}^\rho(V^{\otimes m}) = \langle \text{GL}_{\mathbf{d}} \rangle_{\mu}$ .  $\blacksquare$

We now define a set of multilinear polynomials that generalize the trace powers that appear in the classical setting.

**Definition 3.2.** For  $\sigma = (\sigma_1, \dots, \sigma_n) \in \mathcal{S}_m^n$ , let  $\sigma_i = (r_1 \dots r_k)(s_1 \dots s_l) \dots$  be a disjoint cycle decomposition. For such a  $\sigma \in \mathcal{S}_m^n$ , define the *trace monomials* by  $\text{Tr}_\sigma = T_{\sigma_1} \dots T_{\sigma_n}$  on  $\text{End}(V)^{\otimes m}$ , where

$$T_{\sigma_i} \left( \bigotimes_{j=1}^n M_{j1}, \dots, \bigotimes_{j=1}^n M_{jm} \right) = \text{Tr}(M_{ir_1} \dots M_{ir_k}) \text{Tr}(M_{is_1} \dots M_{is_l}) \dots$$

and extend multilinearly.

**Theorem 3.3.** *The multilinear invariants of  $\text{End}(V)^{\otimes m}$  under the adjoint action of  $\text{GL}_{\mathbf{d}}$  are generated by the  $\text{Tr}_\sigma$ .*

**Proof.** Let  $F$  denote the space of multilinear functions from  $\text{End}(V)^{\otimes m} \cong (V \otimes V^*)^{\otimes m} \rightarrow k$ . We caution that  $F$  is *not* the set of *linear functions* from  $\text{End}(V)^{\otimes m}$  to  $k$ , but the set of functions  $f(M_1, \dots, M_m)$  from  $\text{End}(V)^{\otimes m}$  to  $k$  that is multilinear, i.e., linear in each of the  $m$  arguments. We recall that the universal property of tensor products states that the set of functions from  $V \oplus W$  to  $k$  that are linear in both arguments is isomorphic to the space  $(V \otimes W)^*$ . Extending this, we can identify  $F$  with  $[(V \otimes V^*)^{\otimes m}]^*$  by the universal property of tensor product. We note that there is an  $\text{GL}_{\mathbf{d}}$ -equivariant isomorphism  $\beta: [(V \otimes V^*)^{\otimes m}]^* \xrightarrow{\cong} [V^{\otimes m} \otimes (V^{\otimes m})^*]^*$  induced by rearranging the order of the tensor product in the obvious way and the canonical isomorphism  $(V^*)^{\otimes m} \xrightarrow{\cong} (V^{\otimes m})^*$ . We also have an isomorphism of the spaces

$$\alpha: \text{End}(V^{\otimes m}) \xrightarrow{\cong} [V^{\otimes m} \otimes (V^{\otimes m})^*]^*$$

given by  $\alpha(A)(v \otimes \phi) = \phi(Av)$  and extending linearly, which is  $\text{GL}(V^{\otimes m})$ -equivariant. Since  $\text{GL}_{\mathbf{d}}$  is a subgroup of  $\text{GL}(V^{\otimes n})$ , we get a  $\text{GL}_{\mathbf{d}}$ -equivariant isomorphism  $\text{End}(V^{\otimes m}) \xrightarrow{\cong} F$  by the map  $\beta^{-1} \circ \alpha$ . This induces an isomorphism

$$\text{End}_{\text{GL}_{\mathbf{d}}}^\mu(V^{\otimes m}) \cong F^{\text{GL}_{\mathbf{d}}},$$

where  $F^{\text{GL}_{\mathbf{d}}}$  are the  $\text{GL}_{\mathbf{d}}$ -invariant multilinear functions.



Since  $V^{\otimes m} \cong V_1^{\otimes m} \otimes \cdots \otimes V_n^{\otimes m}$ , we can write  $\alpha = \bigotimes_{i=1}^n \alpha_i$  where  $\alpha_i$  are the induced isomorphisms  $\text{End}(V_i^{\otimes m}) \xrightarrow{\cong} [V_i^{\otimes m} \otimes (V_i^{\otimes m})^*]^*$ . Note that the following holds for the isomorphism  $\alpha_i$ :

- (a)  $\text{Tr}(\alpha_i^{-1}(v \otimes \varphi)) = \varphi(v)$ ,
- (b)  $\alpha_i^{-1}(v_1 \otimes \varphi_1) \circ \alpha_i^{-1}(v_2 \otimes \varphi_2) = \alpha_i^{-1}(v_1 \otimes \varphi_1(v_2) \varphi_2)$ .

We explain these two equalities in more familiar terms. Equality (a) is the statement that  $\text{Tr}(vu^T) = u^T v = \langle u, v \rangle$  for  $u, v$  in some vector space  $U$  and  $\langle \cdot, \cdot \rangle$  the usual inner product. Equality (b) is similar, stating that  $(v_1 u_1^T)(v_2 u_2^T) = v_1(u_1^T v_2)u_2^T = \langle u_1, v_2 \rangle (v_1 u_2^T)$  for  $u_1, u_2, v_1, v_2$  any vectors in some vector space  $U$ .

Since  $\text{End}_{\text{GL}_d}^\mu(V^{\otimes m}) \cong F^{\text{GL}_d}$ , by Theorem 3.1, the images of  $\sigma \in \mathcal{S}_m^n$  under  $\alpha$  are the generators of  $F^{\text{GL}_d}$ . For  $\sigma = (\sigma_1, \dots, \sigma_n)$ , we have

$$\begin{aligned} \alpha(\sigma) \left( \bigotimes_{i=1}^n \bigotimes_{j=1}^m v_{ij} \otimes \bigotimes_{i=1}^n \bigotimes_{j=1}^m \phi_{ij} \right) &= \left( \bigotimes_{i=1}^n \bigotimes_{j=1}^m \phi_{ij} \right) \left( \bigotimes_{i=1}^n \bigotimes_{j=1}^m v_{i\sigma_i^{-1}(j)} \right) \\ &= \prod_{i=1}^n \phi_{im}(v_{i\sigma_i^{-1}(m)}) = T_{\sigma_1^{-1}} \cdots T_{\sigma_n^{-1}} = \text{Tr}_{\sigma^{-1}}, \end{aligned}$$

where the first equality is a consequence of equality (a) and the second equality is a consequence of equality (b) above.  $\blacksquare$

Consider a vector of natural numbers  $P = (p_1, \dots, p_{|P|})$  with elements from  $[m] := \{1, \dots, m\}$ . We extend Definition 2.1 slightly.

**Definition 3.4.** Given a vector  $P = (p_1, \dots, p_{|P|})$  with all  $p_i \in [m]$ , and  $\sigma \in \mathcal{S}_{|P|}^n$ , define the polynomials on  $\text{End}(V)^{\oplus m}$  by their action on simple tensors in  $\bigotimes_{i=1}^n \text{End}(V_i)$ ,

$$\text{Tr}_\sigma^P = \text{Tr}_\sigma \left( \bigotimes_{j=1}^n M_{j p_1}, \dots, \bigotimes_{j=1}^n M_{j p_{|P|}} \right)$$

and extending multilinearly to  $\text{End}(V)^{\oplus m}$ .

Note that Definition 3.4 differs from Definition 3.2 in that it allows for repetition of a matrix in the arguments. So we see that it is precisely a restitution of the multilinear invariants given in Definition 3.4. We now prove this formally.

**Theorem 3.5.** *The ring of  $\text{GL}_d$ -invariants of  $\text{End}(V)^{\oplus m}$  is generated by the  $\text{Tr}_\sigma^P$ .*

**Proof.** We observed previously that the multihomogeneous invariants generate all the invariants. Let  $W = \text{End}(V)$ . Consider a multihomogeneous invariant function of degree  $\alpha = (\alpha_1, \dots, \alpha_m)$  (where some of the  $\alpha_i$  might be zero) in  $k[W^{\oplus m}]$ . It is the restitution of a multilinear invariant in  $k[W^{\oplus \alpha_1} \oplus \cdots \oplus W^{\oplus \alpha_m}]$ . Let  $|\alpha| = \sum_{i=1}^m \alpha_i$ .

By Proposition 2.3, we need only look at the restitutions of  $\text{Tr}_\sigma$ , for  $\sigma \in \mathcal{S}_{|\alpha|}^n$ . What we get is the following:

$$\text{Tr}_\sigma \left( \underbrace{M_1, \dots, M_1}_{\alpha_1}, \dots, \underbrace{M_m, \dots, M_m}_{\alpha_m} \right). \quad (3.1)$$

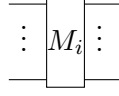
We now define

$$P = \left( \underbrace{1, \dots, 1}_{\alpha_1}, \dots, \underbrace{m, \dots, m}_{\alpha_m} \right)$$

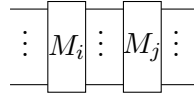
and we see that  $\text{Tr}_\sigma^P$  is equal to the function in equation (3.1).  $\blacksquare$

We can visualize the invariants  $\text{Tr}_\sigma^P$  in an intuitive way. For those familiar with tensor networks, they will recognize the following diagrams. For those unfamiliar, for this particular situation, the rules are very simple. Those interested in knowing more about these invariants as tensor networks can see [3].

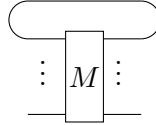
We represent the matrix  $M_i \in \text{End}(V)^{\oplus m}$  by the following picture:



In the picture, there are  $n$  wires on both sides of the box. Each wire represents one of the vector spaces in  $V = \bigotimes_{i=1}^n V_i$ . The following picture describes how to represent the multiplication  $M_i M_j$ :



Given a matrix  $M \in \text{End}(V)$ , we can take a partial trace relative to one of its subsystems. Suppose we trace out the subsystem  $V_1$ . In the diagram, this would look like the following:



Every invariant can be built up by combining these two procedures in any way possible until there are no more “hanging” wires. The resulting picture is a series of loops aligned in  $n$  rows. The loops are given by the disjoint cycle decomposition of some permutation and so each invariant is specified by some element in  $\mathcal{S}_m^n$  as we saw before.

**Example 3.6.** We consider a specific invariant for  $(M_1, M_2) \in \text{End}(V_1 \otimes V_2)^{\oplus 2}$ :

$$\text{Tr}_{(23),(12)}^{(1,1,2)}(M_1, M_2) = \text{Diagram}$$

The disjoint cycle decomposition of the first permutation is  $(1)(23)$  telling us that in the top row the first box receives a loop and the next two boxes receive a joint loop. Similarly in the bottom row, we see that  $(12)(3)$  tells that the first two boxes receive a joint loop and last box a loop on its own. The vector  $(1, 1, 2)$  tells us that the boxes are labeled  $M_1, M_1, M_2$  in that order.

### 3.1 Restrictions on the $\text{Tr}_\sigma^P$

Much is known about the ring of invariants of  $\text{End}(V)^{\oplus m}$  under the adjoint representation of  $\text{GL}(V)$  including that it is Cohen–Macaulay and Gorenstein [19]; see Formanek [13] for an exposition.

The following theorem about generators of this invariant ring is classical [24, Section 2.5].

**Theorem 3.7** ([24]). *The ring  $k[\text{End}(V)^{\oplus m}]^{\text{GL}(V)}$  is generated by*

$$\text{Tr}(M_{i_1} \cdots M_{i_\ell}), \quad 1 \leq i_1, \dots, i_\ell \leq m,$$

where  $\ell \leq \dim(V)^2$ . If  $\dim(V) \leq 3$ ,  $\ell \leq \binom{\dim(V)+1}{2}$  suffices [24, 43].

Furthermore, it is well known that  $k[\text{End}(V)]^{\text{GL}(V)}$  is generated by the polynomials  $\text{Tr}(M^k)$  for  $1 \leq k \leq \dim(V)$  and that furthermore, these polynomials are algebraically independent (cf. [24]).

Note that the degree of  $\text{Tr}_\sigma^P$  as a polynomial in the matrix entries equals  $|P|$ . Theorem 3.7 does not provide a bound on the generating degree for the invariant ring of the *local* action  $k[\text{End}(V)^{\oplus m}]^{\text{GL}^{\mathbf{a}}}$ . The reason is that some trace monomials do not factorize into trace monomials of smaller degree, for example see Example 3.6. If it could, we could separate it as two separate invariants placed adjacent to each other.

It is an interesting question to know if one can determine when such an invariant can be factorized. Unfortunately, this problem is NP-complete as we will show by reducing to the following problem. Suppose we are given  $n$  multisets  $S_1, \dots, S_n$ . Define  $\Sigma(S_i) := \sum_{j \in S_i} j$ . Now suppose  $\Sigma(S_i) = \Sigma(S_j)$  for all  $i, j$ . Then we want to know if every set admits a partition  $S_j = A_j \sqcup B_j$  such that  $\Sigma(A_j) = \Sigma(A_i)$  for all  $i, j$  and likewise for the sets  $B_i$ . Deciding this problem is NP-complete if  $n > 1$  [46].

**Proposition 3.8.** *For  $n > 1$ , deciding if  $\text{Tr}_\sigma^P$  factorizes is NP-complete.*

**Proof.** The containment of this decision problem in NP is clear. We simply need to prove hardness. Suppose we could decide this problem, then we could decide it for  $\text{Tr}_\sigma^P(M)$ , the case when  $m = 1$ . Then define the set  $S_i$  to be the cycle lengths in the disjoint cycle decomposition in  $\sigma_i$ . We see that  $\Sigma(S_i) = \Sigma(S_j)$  for all  $i, j$ . Furthermore, we see that  $\text{Tr}_\sigma^P(M)$  factors if and only if every set  $S_i$  admits a partition  $S_i = A_i \sqcup B_i$  such that  $\Sigma(A_i) = \Sigma(A_j)$  for all  $i, j$  and likewise for the sets  $B_i$ . ■

Proposition 3.8 cautions us about the wisdom of trying to find minimal complete sets of invariants by simply enumerating them and checking to see if they are redundant. This approach will involve solving many instances of an NP-complete problem. However, such an enumeration procedure was recently proposed in [14] for SLOCC invariants. We will see later, that such invariants for  $n$ -qubit systems are of the form  $\text{Tr}_\sigma^P$  where the inputs are matrices of restricted form.

Theorem 3.7 does allow us to restrict the functions  $\text{Tr}_\sigma^P$  that act as candidates for generators for the ring  $k[\text{End}(V)]^{\text{GL}^{\mathbf{a}}}$  (Proposition 3.11).

**Definition 3.9.** The *size* of  $T_{\sigma_i}^P$  is defined to be the size of the largest cycle in the disjoint cycle decomposition of  $\sigma_i$ .

**Definition 3.10.** Given a minimal set of generators, the *girth* of  $k[\text{End}(V)^{\oplus m}]^{\text{GL}^{\mathbf{a}}}$  is a tuple  $(w_1, \dots, w_n)$  where  $w_i$  is the maximum size of any  $T_{\sigma_i}^P$  appearing in a generator. The girth of a function  $\text{Tr}_\sigma^P$  is a tuple  $(s_1, \dots, s_n)$ , where  $s_i$  is the size of  $T_{\sigma_i}^P$ .

Note that the girth of the simple case  $k[\text{End}(V)]^{\text{GL}(k^{d_i})}$  is simply the minimum  $\ell$  such that the functions  $\{\text{Tr}(M_{i_1} \cdots M_{i_\ell}) : 1 \leq i_1, \dots, i_\ell \leq m\}$  generate it. We put a partial ordering on girth as follows:  $(w_1, \dots, w_n) < (w'_1, \dots, w'_n)$  if there exists  $i$  such that  $w_i < w'_i$  and for no  $j$  do we have  $w'_j < w_j$ . The girth is bounded locally by the square of the dimension.

**Proposition 3.11.** *If  $(w_1, \dots, w_n)$  is the girth of  $k[\text{End}(V)^{\oplus m}]^{\text{GL}^{\mathbf{a}}}$ , then  $w_i \leq y_i$ , where  $y_i$  is the girth of  $k[\text{End}(V_i)^{\oplus m}]^{\text{GL}(k^{d_i})}$ . In particular for  $V = V_1 \otimes \cdots \otimes V_n$ , the girth of  $k[\text{End}(V)^{\oplus m}]^{\text{GL}^{\mathbf{a}}}$  is bounded by  $(d_1^2, \dots, d_n^2)$ . If  $d_i \leq 3$ , then the girth is bounded by  $((\binom{d_1+1}{2}, \dots, \binom{d_n+1}{2}))$ .*

**Proof.** First note that  $T_{\sigma_i}^P$  lies in the invariant ring  $R_i = k[\text{End}(V_i)^{\oplus m}]^{\text{GL}(k^{d_i})}$ . Thus it has size at most  $y_i$ , where  $y_i$  is the girth of  $R_i$ . Now apply Theorem 3.7. ■

## 4 Closed orbits

We first give an a sufficient condition for  $(M_1, \dots, M_m) \in \text{End}(V^{\oplus m})$  to have a closed  $\text{GL}_{\mathbf{d}}$  orbit, where  $V$  is a Hilbert space throughout this section. We show that, in particular, tuples of normal matrices over  $\mathbb{C}$  satisfy the given properties. Since density operators are Hermitian, they are immediately normal.

**Theorem 4.1** ([36]). *Given a reductive group acting rationally on vector space, for two distinct closed orbits, there is a polynomial invariant that takes different values on each.*

So we seek to show that normal matrices have closed orbits. This will show that polynomial invariants serve as a complete set of invariants when restricted to density operators. As we noted before, the Zariski closures and Euclidean closures of orbits coincide for reductive groups acting rationally. As such, Theorem 4.1 implies that two closed orbits are distinguishable by continuous invariants if and only if they are distinguishable by polynomial invariants. Returning to Remark 1.1, this implies that we need not consider the more general notion of polynomial invariants as often defined in the literature in order to find a complete set of invariants.

**Definition 4.2.** A decomposition  $V = W \oplus W^\perp$ ,  $W, W^\perp \neq \{0\}$ , is said to be *separable* if there exists a cocharacter of  $\text{GL}_{\mathbf{d}}$ ,  $\lambda(t)$  such that  $\forall w \in W$ ,  $\lim_{t \rightarrow 0} \lambda(t)w = 0$ , and  $\forall w \in W^\perp$ ,  $w \neq 0$ ,  $\lim_{t \rightarrow 0} \lambda(t)w \neq 0$ . We call  $\lambda(t)$  a *separating subgroup* of the decomposition (this group is not unique).

**Caveat:** The definition of a separable decomposition depends on the order in which the summands are written. If  $V = W \oplus W^\perp$  is a separable decomposition, it is not necessarily the case that  $W^\perp \oplus W$  is also a separable decomposition.

Given an arbitrary cocharacter of  $\text{GL}_{\mathbf{d}}$ , it is not clear that there is necessarily a separable decomposition that one can associate to it. The following lemma allows us to replace a cocharacter by one that does have a separable decomposition associated to it that does not affect limits.

**Lemma 4.3.** *Let  $\lambda(t)$  be a cocharacter of  $\text{GL}_{\mathbf{d}}$ . Then there exists another cocharacter  $\mu(t)$  such that the following assertions hold:*

- (a)  $\lim_{t \rightarrow 0} \lambda(t)M\lambda(t)^{-1} = \lim_{t \rightarrow 0} \mu(t)M\mu(t)^{-1}$  for all  $M \in \text{End}(V)$  such that the limit exists,
- (b)  $\mu(0) := \lim_{t \rightarrow 0} \mu(t)$  exists,
- (c) unless  $\lambda(t) = t^\alpha \text{id}$ , then  $\mu(0)$  has two nontrivial eigenspaces with eigenvalues 0, 1.

**Proof.** We can diagonalize  $\lambda(t)$  by some element  $g \in \text{GL}_{\mathbf{d}}$ . Thus it suffices to prove the above statements for diagonal cocharacters. If  $\lambda(t)$  is a diagonal cocharacter, the diagonal entries are of the form  $t^{\alpha_i}$ ,  $\alpha_i \in \mathbb{Z}$  (cf. [24]). Let  $\alpha_m$  be the most negative exponent, or if all  $\alpha_i$  are strictly positive, then let  $\alpha_m$  be the smallest positive exponent. Then let  $\mu(t) = t^{-\alpha_m} \lambda(t)$ . We see that for any  $M \in \text{End}(V)$ ,  $\lambda(t)M\lambda(t)^{-1} = \mu(t)M\mu(t)^{-1}$ . Therefore  $\lim_{t \rightarrow 0} \lambda(t)M\lambda(t)^{-1} = \lim_{t \rightarrow 0} \mu(t)M\mu(t)^{-1}$  whenever the limit exists.

Furthermore, we see that  $\mu(t)$  has diagonal entries all non-negative powers of  $t$ . Therefore,  $\lim_{t \rightarrow 0} \mu(t)$  exists and is in fact equal to  $\mu(0)$ . Furthermore, unless  $\mu(t) = t^\alpha \text{id}$ ,  $\mu(0)$  will have both zeros and ones on the diagonal. Thus it will have to non-trivial eigenspaces with eigenvalues 0, 1. ■

We now show how to construct separable decompositions as it is not clear that they necessarily exist. We must use cocharacters of the form as in Lemma 4.3.

**Lemma 4.4.** *Given a cocharacter as in Lemma 4.3, except for  $\lambda(t) = t^\alpha \text{id}$ , we can associate it to a separable decomposition for which it is the separating subgroup.*

**Proof.** Let  $\mu(t)$  be a cocharacter as in Lemma 4.3. Then we know that  $\mu(0) := \lim_{t \rightarrow 0} \mu(t)$  exists and is a matrix. Then  $\mu(0)$  has two eigenspaces, one attached to eigenvalue 1 and the other to eigenvalue 0. Let  $W$  be the null space of  $\mu(0)$ . Then consider the decomposition  $V = W \oplus W^\perp$ . Then  $\forall w \in W$ ,  $\lim_{t \rightarrow 0} \mu(t)w = \mu(0)w = 0$ , and  $\forall w \in W^\perp$  then  $\lim_{t \rightarrow 0} \mu(t)w = \mu(0)w$ , which projects  $W^\perp$  onto the eigenspace attached to the eigenvalue 1. This means that the only  $v \in W^\perp$  such that  $\mu(0)v = 0$  is  $v = 0$ . So this a separable decomposition for which  $\mu(t)$  is the separating subgroup. ■

Let us analyze which decompositions are separable. Let us first analyze the case that  $\lambda(t) = \bigotimes_{i=1}^n \lambda_i(t)$  is as in Lemma 4.3 and is diagonal. Then  $\lambda_i(t)$  is diagonal and can be taken to have diagonal entries with all non-negative powers of  $t$ . Thus, for every  $i$ , we can decompose  $V_i = W_i \oplus W_i^\perp$  where  $\lim_{t \rightarrow 0} \lambda(t)w = 0$  for all  $w \in W_i$  and  $\lambda(t)w = w$  for all  $w \in W_i^\perp$ . Then  $(W_1^\perp \otimes \dots \otimes W_n^\perp)^\perp$  gets sent to zero by  $\lambda(t)$ . It is easy to see that every separable decomposition for a diagonal cocharacter is of the form

$$(W_1^\perp \otimes \dots \otimes W_n^\perp)^\perp \oplus (W_1^\perp \otimes \dots \otimes W_n^\perp).$$

From here, it is easy to see that every separable decomposition is of the same form by taking the  $\text{GL}_{\mathbf{d}}$  orbits of diagonal cocharacters.

Given a matrix  $M \in \text{End}(V)$ , we are interested in separable decompositions  $W \oplus W^\perp$  such that  $M(W) \subseteq W$ . Let  $P_W$  and  $P_{W^\perp}$  be the projection operators onto each of the two subspaces. Then define  $M|_W := P_W(M)$  and  $M|_{W^\perp} := P_{W^\perp}(M)$ .

**Proposition 4.5.** *For every separable decomposition  $V = W \oplus W^\perp$  such that  $M(W) \subseteq W$ ,  $M|_W \oplus M|_{W^\perp}$  is in the orbit closure of  $M$ .*

**Proof.** We can write  $M$  as

$$M = \begin{array}{c} W \quad W^\perp \\ W \\ W^\perp \end{array} \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}.$$

We know that  $W = (W_1^\perp \otimes \dots \otimes W_n^\perp)^\perp$  for subspaces  $W_i \subseteq V_i$ . Then we let  $\lambda(t) = \bigotimes_{i=1}^m \lambda_i(t)$  where

$$\lambda_i(t) = \begin{array}{c} W_i \quad W_i^\perp \\ W_i \\ W_i^\perp \end{array} \begin{pmatrix} tI & 0 \\ 0 & I \end{pmatrix}.$$

Then we see that

$$\lambda(t) = \begin{array}{c} W \quad W^\perp \\ W \\ W^\perp \end{array} \begin{pmatrix} tQ(t) & 0 \\ 0 & I \end{pmatrix},$$

where  $Q(t)$  is a diagonal matrix with non-zero entries being non-negative powers of  $t$ . In particular, it is invertible. Then we have that

$$\begin{aligned} & \begin{array}{cc} W & W^\perp \\ W & \begin{pmatrix} tQ(t) & 0 \\ 0 & I \end{pmatrix} \\ W^\perp & \begin{pmatrix} 0 & I \end{pmatrix} \end{array} \cdot \begin{array}{cc} W & W^\perp \\ W & \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \\ W^\perp & \begin{pmatrix} 0 & C \end{pmatrix} \end{array} \cdot \begin{array}{cc} W & W^\perp \\ W & \begin{pmatrix} t^{-1}Q(t^{-1}) & 0 \\ 0 & I \end{pmatrix} \\ W^\perp & \begin{pmatrix} 0 & I \end{pmatrix} \end{array} \\ &= \begin{array}{cc} W & W^\perp \\ W & \begin{pmatrix} A & tQ(t)B \\ 0 & C \end{pmatrix} \\ W^\perp & \begin{pmatrix} 0 & C \end{pmatrix} \end{array}, \end{aligned}$$

which we see takes  $M \rightarrow M|_W \oplus M|_{W^\perp}$  as  $t \rightarrow 0$ .  $\blacksquare$

**Theorem 4.6.** *A matrix  $M$  has a closed  $\mathrm{GL}_{\mathbf{d}}$  orbit if there exists some  $M' \in \mathrm{GL}_{\mathbf{d}} \cdot M$  such that for every separable decomposition  $V = W \oplus W^\perp$  satisfying  $M'(W) \subseteq W$ , then  $M'(W^\perp) \subseteq W^\perp$ .*

**Proof.** Suppose that  $M$  does not have a closed orbit, so it can be written as  $M = M_s + M_n$  where  $M_s$  has a closed orbit and  $M_n$  is in the null cone. Then by Theorem 2.7, there is a cocharacter  $\lambda(t)$  taking  $M \rightarrow M_s$ . We can assume that  $\lambda(t)$  satisfies the properties of Lemma 4.3. Letting  $W$  be the kernel of  $\lambda(0)$ , we see that  $V = W \oplus W^\perp$  is a separable decomposition.

Let  $w \in W$ . We note that  $\lambda(t)Mw = \lambda(t)M\lambda(t)^{-1}\lambda(t)w$ . We know that  $\lambda(t)M\lambda(t)^{-1}$  is a matrix in which only non-negative powers of  $t$  appears. Furthermore, every entry of  $\lambda(t)w$  is scaled by some positive power of  $t$ . Therefore every element of  $\lambda(t)Mw$  is scaled by a positive power of  $t$ , so  $\lim_{t \rightarrow 0} \lambda(t)Mw = 0$ . Therefore  $M(W) \subseteq W$ .

Notice that a similar argument shows that  $M_s(W) \subseteq W$  and therefore we can write

$$M_s = \begin{array}{cc} W & W^\perp \\ W & \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \\ W^\perp & \begin{pmatrix} 0 & C \end{pmatrix} \end{array}.$$

However, by Proposition 4.5, we can assume that  $B = 0$ . That is to say,  $M_s(W^\perp) \subseteq M_s(W^\perp)$ .

If  $u \in W^\perp$ , then  $\lim_{t \rightarrow 0} \lambda(t)u$  lies in the eigenspace of  $\lambda(0)$  attached to the eigenvalue of 1 (it may not be the case that this eigenspace is orthogonal to the kernel of  $\lambda(0)$ ). However, we note that  $\lambda(t)M_n\lambda(t)^{-1}$  has every entry scaled by a positive power of  $t$ , and thus  $\lambda(t)M\lambda(t)^{-1}\lambda(t)u$  has all entries scaled by some positive power of  $t$  and thus  $\lim_{t \rightarrow 0} \lambda(t)M_nu = 0$ . This implies that  $M_nu$  is in  $W$  and therefore, and since  $M_s(u) \in W^\perp$ ,  $W^\perp$  is not an invariant subspace.  $\blacksquare$

We can show that matrices that respect orthogonal decompositions have closed orbits. The prime example are normal matrices as these are precisely the matrices with an orthogonal basis by the spectral theorem.

**Theorem 4.7.** *For  $\mathrm{GL}_{\mathbf{d}} \curvearrowright \mathrm{End}(V)^{\oplus m}$ , tuples of normal matrices have closed orbits.*

**Proof.** It suffices to show that for  $\mathrm{GL}_{\mathbf{d}} \curvearrowright \mathrm{End}(V)$ , matrices with an orthogonal eigenbasis have closed orbits. Then the result follows from the fact that, if such a  $(M_1, \dots, M_m)$  acted on by  $\mathrm{GL}_{\mathbf{d}}$  did not have a closed orbit, then projecting onto some coordinate, say  $i$ , would induce a non-trivial limit point, implying that the matrix  $M_i$  did not have a closed orbit.

Let  $M$  have an orthogonal eigenbasis. Then let  $V = W \oplus W^\perp$  be a separable decomposition such that  $M(W) \subseteq W$ . It must be that  $W$  is a direct sum of eigenspaces of  $M$  (here, by eigenspace, we mean any subspace which  $M$  acts on by scaling). Since the eigenspaces of  $M$  are orthogonal (in the sense that given two vectors in two different eigenspaces, they are orthogonal), we immediately have that  $W^\perp$  is a direct sum of eigenspaces. Thus  $W^\perp$  is an invariant subspace of  $M$ . Then applying Theorem 4.6, we get that  $M$  has a closed orbit.  $\blacksquare$

**Corollary 4.8.** *The  $\mathrm{GL}_{\mathbf{d}}$  orbits of tuples of density matrices are closed, so they can be separated by polynomial invariants. Moreover, two Hermitian matrices are in the same  $\mathrm{GL}_{\mathbf{d}}$  orbit if and only if they are in the same  $\mathrm{U}_{\mathbf{d}}$  orbit.*

**Proof.** We know from Proposition 1.4 that two density operators are in the same  $\mathrm{GL}_{\mathbf{d}}$  orbit if and only if they are in the same  $\mathrm{U}_{\mathbf{d}}$  orbit. We know from Theorem 4.7 that tuples of density operators have closed orbits. We know from Theorem 4.1 that two closed orbits can be distinguished by invariants if and only if they are distinct. ■

**Corollary 4.9.** *The functions  $\mathrm{Tr}_{\sigma}^P$  form a complete set of invariants for tuples of density operators under the action of  $\mathrm{U}_{\mathbf{d}}$ .*

**Proof.** This follows from Corollary 4.8 and Theorem 3.5. ■

So we know that two tuples of density operators are not in the same  $\mathrm{U}_{\mathbf{d}}$  orbit if and only if there is some  $\mathrm{Tr}_{\sigma}^P$  on which they take different values. We know from Theorem 2.4, that there exists a finite set of functions  $\mathrm{Tr}_{\sigma}^P$  that forms a complete system of invariants. This theorem does not tell us what such a finite set may be. However, we have a bound given by the following result.

**Theorem 4.10** ([10]). *Let  $\rho: G \rightarrow \mathrm{GL}(V)$  be a reductive group acting rationally. Let  $f_1, \dots, f_{\ell}$  be homogeneous invariants, with maximum degree  $\gamma$ , such that their vanishing locus is  $\mathcal{N}_V$ . Then*

$$\beta_G(V) \leq \max \left\{ 2, \frac{3}{8} \dim(k[V]^G) \gamma^2 \right\}.$$

Furthermore,  $\gamma$  is bounded by  $CA^m$  where  $C$  is the degree of  $G$  as a variety and  $m = \dim(\rho(G))$ . Since  $\rho$  is a rational map, it can be viewed as a vector valued function with a rational function in each coordinate. Then  $A$  is defined to be the maximum degree of any of these coordinate rational functions.

As we noted earlier,  $\mathrm{GL}_{\mathbf{d}}$  can be replaced by  $\mathrm{SL}_{\mathbf{d}} := \times_{i=1}^n \mathrm{SL}(V_i)$  since this group action has the same invariant ring.

**Corollary 4.11.** *The polynomials  $\mathrm{Tr}_{\sigma}^P$  of girth at most  $(d_1^2, \dots, d_n^2)$  and degree at most*

$$\max \left\{ 2, \frac{3}{8} \max\{d_i\} m^2 \dim(V)^4 (2n)^{2\delta} \right\},$$

where  $\delta = \sum_{i=1}^n (d_i - 1)$ , give a finite complete set of invariants for LU-equivalence of  $m$ -tuples of density operators.

**Proof.** The first part of the statement follows from Proposition 3.11. The degree bound comes from Theorem 4.10 and the following facts.  $\mathrm{SL}_{\mathbf{d}}$  is defined by equations of degrees  $d_i$  since  $\mathrm{SL}_{\mathbf{d}}$  consists of tuples of matrices each of determinant one, so  $C \leq \max d_i$ . It is easy to see that  $A = 2n$  as taking the Kronecker product of  $n$  matrices gives monomials of degree  $n$  in the entries of the original matrices and conjugation is a quadratic action. Since the representation of  $\mathrm{SL}_{\mathbf{d}}$  is faithful  $\dim(\rho(\mathrm{SL}_{\mathbf{d}})) = \dim(\mathrm{SL}_{\mathbf{d}}) = \sum_{i=1}^n (d_i - 1)$ . Lastly, we note that  $\dim(k[V]^G) \leq \dim(k[V]) = \dim(V)$  for any  $G \curvearrowright V$ . ■



## 5 SLOCC invariants for any number of qubits

We now wish to relate the invariants of  $\mathrm{SL}_2 := \times_{i=1}^n \mathrm{SL}(\mathbb{C}^2)$  by left multiplication on  $V^{\oplus m}$ , where  $V = (\mathbb{C}^2)^{\otimes n}$ , to the invariants of  $\mathrm{SL}_2$  by conjugation on  $\mathrm{End}(V)^{\oplus m}$ . The relevant property we use is that the action of  $\mathrm{SL}_2$  on  $V^{\oplus m}$  is *self-dual*. This means that the standard action of  $\mathrm{SL}_2$  on  $\mathbb{C}^2$  is isomorphic to the representation of  $\mathrm{SL}_2$  on  $(\mathbb{C}^2)^*$  given by  $g \cdot \varphi = \varphi(g^{-1})$ . To state this more formally:

**Definition 5.1.** A representation  $\rho: G \rightarrow \mathrm{GL}(V)$  is called self-dual if  $\rho \simeq \rho^*$ , where  $\rho^*$  is the induced contragradient representation on  $V^*$ .

The action of  $\mathrm{SL}(\mathbb{C}^2)$  on  $\mathbb{C}^2$  by left multiplication is self-dual. Let  $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ . Then for any  $g \in \mathrm{SL}(\mathbb{C}^2)$ ,  $TgT^{-1} = (g^{-1})^T$ . We consider the map  $\phi: \mathbb{C}^2 \rightarrow (\mathbb{C}^2)^*$  given by  $\phi(v) = (Tv)^T$ . Then

$$\phi(gv) = (Tgv)^T = (TgT^{-1}Tv)^T = (Tv)^T g^{-1}.$$

This gives an equivariant isomorphism between the standard action of  $\mathrm{SL}(\mathbb{C}^2)$  and its induced contragradient representation.

**Lemma 5.2.** *The action of  $\rho: \mathrm{SL}_2 \rightarrow \mathrm{GL}(V^{\oplus m})$  by left multiplication is self-dual.*

**Proof.** Let  $\phi: V^{\oplus m} \rightarrow (V^*)^{\oplus m}$  be the linear map given by  $\phi(\bigoplus_{i=1}^m v_i) = \bigoplus_{i=1}^m (T^{\otimes n} v_i)^T$ . Let  $g = \otimes_{i=1}^n g_i \in \rho(\mathrm{SL}_2)$ . Then

$$\begin{aligned} \phi(g \bigoplus_{i=1}^m v_i) &= \bigoplus_{i=1}^m (T^{\otimes n} g v_i)^T = \bigoplus_{i=1}^m (T^{\otimes n} g (T^{-1})^{\otimes n} T^{\otimes n} v_i)^T \\ &= \bigoplus_{i=1}^m (T^{\otimes n} v_i)^T (\otimes_{i=1}^n T g_i T^{-1})^T \\ &= \bigoplus_{i=1}^m (T^{\otimes n} v_i)^T (\otimes_{i=1}^n (g_i^{-1})^T)^T = \bigoplus_{i=1}^m (T^{\otimes n} v_i)^T g^{-1}. \quad \blacksquare \end{aligned}$$

Let  $G \curvearrowright V$  be a self-dual representation, given by  $\rho$ . Then there is an isomorphism  $\phi: \rho \rightarrow \rho^*$ . Since it is a linear map, there is a matrix  $S$  such that  $\phi(v) = (Sv)^T$ . Then

$$\phi(\rho(g)v) = (S\rho(g)v)^T = (Sv)^T (S\rho(g)S^{-1})^T = (Sv)^T g^{-1}.$$

Thus we have that a representation  $\rho$  is self-dual if and only if there exists a matrix  $S$  such that  $S\rho(g)S^{-1} = \rho(g^{-1})^T$  for all  $g \in G$ .

Suppose the representation  $\rho: G \rightarrow \mathrm{GL}(V)$  on  $V$  is self-dual. Let  $\phi: \rho \rightarrow \rho^*$  be the equivariant isomorphism. This induces an action on  $V^{\oplus m}$ , which is clearly self-dual. Then there is an equivariant inclusion of  $\psi: V^{\oplus m} \hookrightarrow (V \oplus V^*)^{\oplus m}$  given by

$$\begin{aligned} \bigoplus_{i=1}^m v_i &\mapsto \bigoplus_{i=1}^m (v_i, \phi(v_i)), \\ g \cdot \bigoplus_{i=1}^m (v_i, \phi(v_i)) &= \bigoplus_{i=1}^m (\rho(g)v_i, \rho^*(g)\phi(v_i)). \end{aligned}$$

So let us consider the invariants on  $(V \oplus V^*)^{\oplus m}$  with the above action. We first look at the multilinear invariants; from these we can construct all invariants. Let  $I$  be the ideal defining the image of  $V \oplus V^*$  inside of  $\mathrm{End}(V)$  under the Segre embedding. Recall that the Segre embedding of  $V \oplus W$  is the map  $(v, w) \mapsto v \otimes w$ . Also recall that the ideal defining a variety is the set of polynomials that vanish identically on the variety. The image of the Segre embedding is  $G$ -stable and so its ideal is also  $G$ -stable.

**Proposition 5.3** ([37]). *Let  $G$  act on a subvariety  $X \subseteq V$ . If  $G$  is reductive, and its ideal,  $I \subseteq k[V]$ , is a  $G$ -stable ideal, then  $k[V]^G/(I \cap k[V]^G) \cong (k[V]/I)^G$ .*

**Lemma 5.4.**  $\mathbb{C}[(V \oplus V^*)^{\oplus m}]^G \cong \mathbb{C}[\text{End}(V)^{\oplus m}]^G/(I \cap \mathbb{C}[\text{End}(V)^{\oplus m}]^G)$ .

**Proof.** The multilinear invariants are elements of  $\text{End}(V)^{\oplus m}$  of degree  $d$  are elements of the space  $(\text{End}(V)^{\otimes d})^*$  by the universal property of tensor product. The multilinear invariants of  $(V \oplus V^*)$  of degree  $d$ , are also elements of  $(\text{End}(V)^{\otimes d})^*$ , lying in the image of the Segre embedding  $V \oplus V^* \hookrightarrow \text{End}(V)$ . Furthermore, notice that the action of  $G$  on  $(V \oplus V^*)^{\oplus d}$  and on  $\text{End}(V)^{\oplus d}$  both turn into the action on  $\text{End}(V)^{\otimes m}$  given by

$$g \cdot \bigotimes_{i=1}^d M_i = \bigotimes_{i=1}^d \rho(g) M_i \rho(g)^{-1}.$$

So the multilinear invariants are the same and by Proposition 2.3, the restitutions are the same. Proposition 5.3 finishes the proof.  $\blacksquare$

Of course, we are not interested in the entire space  $(V \oplus V^*)^{\oplus m}$  but rather the subset defined by the image of  $\phi: V^{\oplus m} \hookrightarrow (V \oplus V^*)^{\oplus m}$ . This is also a  $G$ -invariant variety.

Let  $\tilde{\phi}: V^{\oplus m} \rightarrow \text{End}(V)^{\oplus m}$  be the map given by  $\bigoplus_{i=1}^m v_i \mapsto \bigoplus_{i=1}^m (v_i \otimes v_i^T) S^T$ . For the case that  $m = 1$ , the image of  $V \in \text{End}(V)$  is matrices of the form  $v \otimes (v^T S^T)$ , which is isomorphic to the Veronese variety of matrices of the form  $v \otimes v^T$ . Thus the image of  $V^{\oplus m} \in \text{End}(V)^{\oplus m}$  is isomorphic to a direct sum of these Veronese varieties.

Now consider its ideal  $I \subset \mathbb{C}[\text{End}(V)^{\oplus m}]$ . The action of  $G$  on  $\text{End}(V)^{\oplus m}$  induces an action on the coordinate ring. As  $I$  defines an  $G$ -invariant variety, it is clear that  $I$  is a  $G$ -stable ideal.

**Theorem 5.5.** *Suppose  $\rho: G \rightarrow \text{GL}(V)$  acting on  $V^{\oplus m}$  is self-dual and reductive. Let  $I$  be the ideal of  $\text{Im}(\tilde{\phi})$ . Then*

$$\mathbb{C}[V^{\oplus m}]^G \cong \mathbb{C}[\text{End}(V)^{\oplus m}]^G/(I \cap \mathbb{C}[\text{End}(V)^{\oplus m}]^G).$$

**Proof.** By Lemma 5.4,  $\mathbb{C}[(V \oplus V^*)^{\oplus m}]^G \cong \mathbb{C}[\text{End}(V)^{\oplus m}]^G/(I \cap \mathbb{C}[\text{End}(V)^{\oplus m}]^G)$ . The invariants of  $\mathbb{C}[\text{End}(V)^{\oplus m}]$  are interpreted as invariants of  $V^{\oplus m}$  by precomposition with  $\tilde{\phi}$ . Then the result follows from follows from Proposition 5.3.  $\blacksquare$

We know that  $\text{SL}_2$  is self-dual by Lemma 5.2. Unfortunately,  $\text{SL}(\mathbb{C}^n)$  is self-dual only when  $n = 2$ . So this method only works for the group  $\text{SL}_2$ . We relate this to the invariant ring  $\mathbb{C}[\text{End}(V)^{\oplus m}]^{\text{SL}_2}$ , which we have already described.

For the case  $\text{SL}_2$ ,  $\tilde{\phi}: V \rightarrow \text{End}(V)$  is given by  $\tilde{\phi}(v) = v \otimes v^T (T^{\otimes n})^T$  which extends naturally to a map  $\tilde{\phi}: V^{\oplus m} \rightarrow \text{End}(V)^{\oplus m}$ . Then we define

$$\tilde{\text{Tr}}_{\sigma}^P(v_{m_1}, \dots, v_{m_\ell}) := \text{Tr}_{\sigma}^M(\tilde{\phi}(v_{m_1}), \dots, \tilde{\phi}(v_{m_\ell})).$$

This turns the polynomials  $\text{Tr}_{\sigma}^P$  into polynomials in  $\mathbb{C}[V^{\oplus m}]$ . These polynomials generate the ring of invariants. However, we haven't accounted for the relations introduced among them from restricting the variety defined by the image of  $\tilde{\phi}$ , so many of these polynomials will be redundant.

**Theorem 5.6.** *The functions  $\tilde{\text{Tr}}_{\sigma}^P$  of degree at most*

$$\max \left\{ 2, \frac{3}{2} m^2 \dim(V)^2 (n)^{6n} \right\}$$

*generate the invariants for  $\mathbb{C}[V^{\oplus m}]^{\text{SL}_2}$  on  $n$  qubits.*

**Proof.** By Lemma 5.2, the action of  $\mathrm{SL}_2$  on  $V$  by left multiplication is self-dual and reductive. Then by Theorem 5.5, the generators of  $\mathbb{C}[\mathrm{End}(V)]^{\mathrm{SL}_2}$  applied to the image of  $\tilde{\phi}$  gives a generating set for  $\mathbb{C}[V]^{\mathrm{SL}_2}$ . The bound comes from applying Theorem 4.10. The degree of  $\mathrm{SL}_2$  is at most two as it is defined by determinants of  $2 \times 2$  matrices.  $\dim(\mathbb{C}[V^{\oplus m}]^{\mathrm{SL}_2}) \leq \dim(V)$ ,  $A$  is  $n$  as we are taking a Kronecker product of  $n$  matrices, and  $\mathrm{SL}_2$  has dimension  $3n$ . ■

While Theorem 5.6 gives a complete accounting of all the polynomial SLOCC invariants for an  $n$  qubit system, as well as a finite generating set of the ring, further work is necessary. The most obvious problem is that the degree bound is obtained by appealing to a general degree bound for reductive group actions. There is no reason to expect that it is optimal; indeed, we conjecture that a degree bound exists that is polynomial in the dimension of  $V$ . For small  $n$ , explicit generating sets are known and the following table compares these degree bounds to the ones given by Theorem 5.6, for  $m = 1$ .

| $n$ | Known minimal degree bounds | Degree bound from Theorem 5.6 |
|-----|-----------------------------|-------------------------------|
| 1   | 0 (trivial)                 | 6                             |
| 2   | 2 (classical)               | $24 \cdot 2^{12}$             |
| 3   | 4 [40]                      | $96 \cdot 3^{18}$             |
| 4   | 6 [32]                      | $384 \cdot 4^{24}$            |

We see that the above degree bound is very far off. While one might be tempted to algorithmically find minimal sets of invariants by enumerating all invariants, the above bound does not give an indication of how long such an enumeration would take. The known minimal degree bounds have been found by a variety of methods. However, as the number of qubits grows, the general approach has been an analysis of the Hilbert series of the rings to determine degrees of generators along with the computations of covariants. For 5 qubits, this method is already computationally prohibitive. As such, if any progress is to be made in this direction, a better theoretical understanding of these invariants is necessary rather than relying on computation.

The second issue is that the above invariants might not all be necessary. Indeed, for the case of four qubits, this turned out to be the case [47], although this case was special as there were a finite number of normal forms describing all of the orbits. A classification in terms of geometric properties was later carried out for four qubits [20]. This is not likely to be the case as the number of qubits grows. Nevertheless, there may be relations (although necessarily non-algebraic) among the invariants as a result of restricting to quantum states.

## Acknowledgements

The authors would like to acknowledge the helpful comments of the reviewers which greatly improved and strengthened this paper. J. Turner would like to thank Lluís Vena for helpful discussions. The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement No 339109.

## References

- [1] Abanin D.A., Demler E., Measuring entanglement entropy of a generic many-body system with a quantum switch, *Phys. Rev. Lett.* **109** (2012), 020504, 5 pages, [arXiv:1204.2819](https://arxiv.org/abs/1204.2819).
- [2] Baez J.C., Renyi Entropy and Free Energy, [arXiv:1102.2098](https://arxiv.org/abs/1102.2098).
- [3] Biamonte J., Bergholm V., Lanzagorta M., Tensor network methods for invariant theory, *J. Phys. A: Math. Theor.* **46** (2013), 475301, 19 pages, [arXiv:1209.0631](https://arxiv.org/abs/1209.0631).
- [4] Biamonte J.D., Morton J., Turner J., Tensor network contractions for #SAT, *J. Stat. Phys.* **160** (2015), 1389–1404, [arXiv:1405.7375](https://arxiv.org/abs/1405.7375).

- 
- [5] Brauer R., On algebras which are connected with the semisimple continuous groups, *Ann. of Math.* **38** (1937), 857–872.
- [6] Brion M., Representations of quivers, in Geometric Methods in Representation Theory. I, *Sémin. Congr.*, Vol. 24, Soc. Math. France, Paris, 2012, 103–144.
- [7] Cardy J., Measuring entanglement using quantum quenches, *Phys. Rev. Lett.* **106** (2011), 150404, 4 pages, [arXiv:1012.5116](https://arxiv.org/abs/1012.5116).
- [8] Chterental O., Djokovic D.Z., Normal forms and tensor ranks of pure states of four qubits, in Linear Algebra Research Advances, Editor G.D. Ling, Nova Science Publishers, New York, 2007, 133–167, [quant-ph/0612184](https://arxiv.org/abs/quant-ph/0612184).
- [9] Daley A.J., Pichler H., Schachenmayer J., Zoller P., Measuring entanglement growth in quench dynamics of bosons in an optical lattice, *Phys. Rev. Lett.* **109** (2012), 020505, 5 pages, [arXiv:1205.1521](https://arxiv.org/abs/1205.1521).
- [10] Derksen H., Kemper G., Computational invariant theory, *Encyclopaedia of Mathematical Sciences*, Vol. 130, Springer, Heidelberg, 2015.
- [11] Dür W., Vidal G., Cirac J.I., Three qubits can be entangled in two inequivalent ways, *Phys. Rev. A* **62** (2000), 062314, 12 pages, [quant-ph/0005115](https://arxiv.org/abs/quant-ph/0005115).
- [12] Eisert J., Cramer M., Plenio M.B., Colloquium: Area laws for the entanglement entropy, *Rev. Modern Phys.* **82** (2010), 277–306.
- [13] Formanek E., The polynomial identities and invariants of  $n \times n$  matrices, *CBMS Regional Conference Series in Mathematics*, Vol. 78, Amer. Math. Soc., Providence, RI, 1991.
- [14] Gour G., Wallach N.R., Classification of multipartite entanglement of all finite dimensionality, *Phys. Rev. Lett.* **111** (2013), 060502, 5 pages, [arXiv:1304.7259](https://arxiv.org/abs/1304.7259).
- [15] Grassl M., Rötteler M., Beth T., Computing local invariants of quantum-bit systems, *Phys. Rev. A* **58** (1998), 1833–1839, [quant-ph/9712040](https://arxiv.org/abs/quant-ph/9712040).
- [16] Hero M.W., Willenbring J.F., Stable Hilbert series as related to the measurement of quantum entanglement, *Discrete Math.* **309** (2009), 6508–6514.
- [17] Hilbert D., Ueber die Theorie der algebraischen Formen, *Math. Ann.* **36** (1890), 473–534.
- [18] Hilbert D., Ueber die vollen Invariantensysteme, *Math. Ann.* **42** (1893), 313–373.
- [19] Hochster M., Roberts J.L., Rings of invariants of reductive groups acting on regular rings are Cohen–Macaulay, *Adv. Math.* **13** (1974), 115–175.
- [20] Holweck F., Luque J.-G., Thibon J.-Y., Entanglement of four-qubit systems: a geometric atlas with polynomial compass II (the tame world), *J. Math. Phys.* **58** (2017), 022201, 33 pages, [arXiv:1606.05569](https://arxiv.org/abs/1606.05569).
- [21] Johansson M., Ericsson M., Singh K., Sjöqvist E., Williamson M.S., Topological phases and multiqubit entanglement, *Phys. Rev. A* **85** (2012), 032112, 11 pages, [arXiv:1202.0716](https://arxiv.org/abs/1202.0716).
- [22] Kempf G.R., Instability in invariant theory, *Ann. of Math.* **108** (1978), 299–316.
- [23] Klyachko A., Coherent states, entanglement, and geometric invariant theory, [quant-ph/0206012](https://arxiv.org/abs/quant-ph/0206012).
- [24] Kraft H., Procesi C., Classical invariant theory, a primer, 1996, available at <https://math.unibas.ch/uploads/x4epersdb/files/primernew.pdf>.
- [25] Kraus B., Local unitary equivalence of multipartite pure states, *Phys. Rev. Lett.* **104** (2010), 020504, 4 pages, [arXiv:0909.5152](https://arxiv.org/abs/0909.5152).
- [26] Landsberg J.M., Tensors: geometry and applications, *Graduate Studies in Mathematics*, Vol. 128, Amer. Math. Soc., Providence, RI, 2012.
- [27] Le Bruyn L., Procesi C., Semisimple representations of quivers, *Trans. Amer. Math. Soc.* **317** (1990), 585–598.
- [28] Leron U., Trace identities and polynomial identities of  $n \times n$  matrices, *J. Algebra* **42** (1976), 369–377.
- [29] Li J.-L., Qiao C.-F., Classification of arbitrary multipartite entangled states under local unitary equivalence, *J. Phys. A: Math. Theor.* **46** (2013), 075301, 14 pages, [arXiv:1111.4379](https://arxiv.org/abs/1111.4379).
- [30] Liu B., Li J.-L., Li X., Qiao C.-F., Local unitary classification of arbitrary dimensional multipartite pure states, *Phys. Rev. Lett.* **108** (2012), 050501, 4 pages, [arXiv:1105.1517](https://arxiv.org/abs/1105.1517).
- [31] Lloyd S., Universal quantum simulators, *Science* **273** (1996), 1073–1078.
- [32] Luque J.-G., Thibon J.-Y., Polynomial invariants of four qubits, *Phys. Rev. A* **67** (2003), 042303, 5 pages, [quant-ph/0212069](https://arxiv.org/abs/quant-ph/0212069).

- [33] Luque J.-G., Thibon J.-Y., Algebraic invariants of five qubits, *J. Phys. A: Math. Gen.* **39** (2006), 371–377, [quant-ph/0506058](#).
- [34] Luque J.-G., Thibon J.-Y., Toumazet F., Unitary invariants of qubit systems, *Math. Structures Comput. Sci.* **17** (2007), 1133–1151, [quant-ph/0604202](#).
- [35] Maciżek T., Oszmaniec M., Sawicki A., How many invariant polynomials are needed to decide local unitary equivalence of qubit states?, *J. Math. Phys.* **54** (2013), 092201, 15 pages, [arXiv:1305.3894](#).
- [36] Mumford D., Fogarty J., Kirwan F., Geometric invariant theory, *Ergebnisse der Mathematik und ihrer Grenzgebiete (2)*, Vol. 34, 3rd ed., Springer-Verlag, Berlin, 1994.
- [37] Nagata M., Invariants of a group in an affine ring, *J. Math. Kyoto Univ.* **3** (1963), 369–377.
- [38] Nielsen M.A., Chuang I.L., Quantum computation and quantum information, *Cambridge University Press*, Cambridge, 2000.
- [39] Onishchik A.L., Vinberg E.B., Lie groups and algebraic groups, *Springer Series in Soviet Mathematics*, Springer-Verlag, Berlin, 1990.
- [40] Parfenov P.G., Orbits and their closures in the spaces  $\mathbb{C}^{k_1} \otimes \dots \otimes \mathbb{C}^{k_r}$ , *Sb. Math.* **192** (2001), 89–112.
- [41] Pichler H., Bonnes L., Daley A.J., Läuchli A.M., Zoller P., Thermal versus entanglement entropy: a measurement protocol for fermionic atoms with a quantum gas microscope, *New J. Phys.* **15** (2013), 063003, 17 pages, [arXiv:1302.1187](#).
- [42] Raussendorf R., Briegel H.J., A one-way quantum computer, *Phys. Rev. Lett.* **86** (2001), 5188–5191.
- [43] Razmyslov Ju.P., Trace identities of full matrix algebras over a field of characteristic zero, *Math. USSR Izv.* **8** (1974), 727–760.
- [44] Rényi A., On measures of entropy and information, in Proc. 4th Berkeley Sympos. Math. Statist. and Prob., Vol. I, University California Press, Berkeley, Calif., 1961, 547–561, available at [http://digitalassets.lib.berkeley.edu/math/ucb/text/math\\_s4\\_v1\\_article-27.pdf](http://digitalassets.lib.berkeley.edu/math/ucb/text/math_s4_v1_article-27.pdf).
- [45] Schachenmayer J., Lanyon B.P., Roos C.F., Daley A.J., Entanglement growth in quench dynamics with variable range interactions, *Phys. Rev. X* **3** (2013), 031015, 16 pages, [arXiv:1305.6880](#).
- [46] Turner J., On subtilings of polyomino tilings, [arXiv:1602.05784](#).
- [47] Verstraete F., Dehaene J., De Moor B., Verschelde H., Four qubits can be entangled in nine different ways, *Phys. Rev. A* **65** (2002), 052112, 5 pages, [quant-ph/0109033](#).
- [48] Williamson M.S., Ericsson M., Johansson M., Sjöqvist E., Sudbery A., Vedral V., Wootters W.K., Geometric local invariants and pure three-qubit states, *Phys. Rev. A* **83** (2011), 062308, 8 pages, [arXiv:1102.4222](#).
- [49] Zhang T.-G., Zhao M.-J., Li M., Fei S.-M., Li-Jost X., Criterion of local unitary equivalence for multipartite states, *Phys. Rev. A* **88** (2013), 042304, 6 pages, [arXiv:1310.2042](#).
- [50] Zhang T.-G., Zhao M.-J., Li-Jost X., Fei S.-M., Local unitary invariants for multipartite states, *Internat. J. Theoret. Phys.* **52** (2013), 3020–3025, [arXiv:1307.6659](#).
- [51] Zhou C., Zhang T.-G., Fei S.-M., Jing N., Li-Jost X., Local unitary equivalence of arbitrary dimensional bipartite quantum states, *Phys. Rev. A* **86** (2012), 010303, 4 pages, [arXiv:1207.2688](#).
- [52] Ziman M., Štelmachovič P., Bužek V., On the local unitary equivalence of states of multi-partite systems, *Fortschr. Phys.* **49** (2001), 1123–1131, [quant-ph/0107016](#).