Quantum Entanglement and Algebraic Group Actions

Robert Furber

Wolfson College

University of Oxford

A thesis submitted in partial fulfillment of the MSc in

Mathematics and the Foundations of Computer Science

September 1, 2011

Acknowledgements

I would like to thank Bob Coecke for all of his help, especially his knowledge of the relevant physics literature (which I was not at all aware of at the start), and his advice on how to present my work, both in writing and in talks. I would also like to thank all the people I have discussed quantum physics with, such as Andreas Döring and the members of the quantum foundations discussion group.

Finally, I would like to thank both my parents, Rosemary and James Furber, for their continuing support.

Abstract

In the following we discuss how algebraic group actions can be applied to the study of quantum entanglement. The following facts are new:

- A method for calculating equations for the SLOCC class of any pure state, with no restrictions on dimensions other than those imposed by computational speed.
- A calculation of the equations defining the closure of one 4-partite state, as an example to illustrate the method.
- To my knowledge, it has not previously been observed that SLOCC classes equal if their closure is equal, although the fact about algebraic group actions is known.
- Similarly, the fact that a SLOCC class inside the closure of another must be of strictly smaller dimension.

We also discuss quotients of the space of states by the action, but do not actually compute any or prove new theorems in this area.

Contents

0.1 Introduction

Our subject of study is multipartite quantum states. To explain what these are, it is first necessary to say what a quantum state is. For basic notions of quantum computing and quantum information theory, we refer the reader to a standard text such as [27]. Each quantum system has a (complex) Hilbert space $\mathcal{H}$ associated to it. For the remainder of this dissertation we will limit discussion to finite dimensional Hilbert spaces.

A state of a quantum system is then a complex line through the origin[1] in the Hilbert space. We may also consider these as being points in the corresponding projective space $\mathbb{P}(\mathcal{H})$, but to simplify the exposition we will not use this approach. Instead, we will just call $\mathcal{H}$ itself the space of states, using the fact that each line is generated by a vector.

These are actually the pure states, which we limit ourselves to considering here, instead of mixed states as well. For information about what mixed states are, we direct the reader to standard references.

Systems for which d is the maximum number of possible outcomes for each measurement have d-dimensional Hilbert space and are known as qudits. The case that $d = 2$ is most often considered and in this case they are known as qubits. The state space for a qudit is isomorphic to $\mathbb{C}^d$ with the standard inner product.

To get the Hilbert space of a composite system, we take the tensor product of the Hilbert spaces of the components. This means an n-partite state is an element of the tensor product of n Hilbert spaces, i.e.

$$\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n = \underbrace{\mathbb{C}^d \otimes \cdots \otimes \mathbb{C}^d}_{n} = (\mathbb{C}^d)^{\otimes n} \cong \mathbb{C}^{d^n}$$

Unlike the case of a single party, where there is essentially only one kind of state, there are different kinds of multipartite state. If a state is of the form

$$\psi_1 \otimes \cdots \otimes \psi_n$$

for $\psi_i \in \mathcal{H}_i$ being states of each subsystem, then it is said to be separable. If this is not the case, then it is said to be entangled.

We will now examine an example illustrating this distinction. Consider a bipartite qubit state

$$\psi_{00}|00\rangle + \psi_{01}|01\rangle + \psi_{10}|10\rangle + \psi_{11}|11\rangle$$

[1] i.e. a 1-dimensional subspace, which topologically is a plane and is 2-dimensional as a real subspace

Where we are using the Dirac notation for states, which is to say $\{|0\rangle, |1\rangle\}$ is an orthonormal basis of $\mathbb{C}^2$, and $|ij\rangle = |i\rangle \otimes |j\rangle$ for $i, j \in \{0, 1\}$. Now $|00\rangle$ is obviously separable, and $|00\rangle + |01\rangle = |0\rangle \otimes (|0\rangle + |1\rangle)$ less obviously so. However, the Bell state $|00\rangle + |11\rangle$ is entangled, and is the archetypal example of an entangled state. However, although it is not expressed as a product of two one-party states, one face of it it would seem difficult to show that it could never be expressed as such a product. Actually, it is a solved problem to tell if a state is separable or entangled. In this case, a state is separable if and only if $\psi_{00}\psi_{11} - \psi_{01}\psi_{10} = 0$. In the previous two cases this was true, but for the Bell state $\psi_{00}\psi_{11} - \psi_{01}\psi_{10} = 1 - 0 = 1 \neq 0$. This statement can be generalized to an arbitrary number of parties and an arbitrary qu$d$it, using a generalization of the Segre variety from algebraic geometry, see [20] [25].

Before going further, it would be good to explain what entangled states are good for. The original use was in showing certain facts about quantum mechanics itself. The Einstein-Podolsky-Rosen paper[14] aimed to show that the state vector, there called the wave-function, was not a complete description of a physical system. Bell's paper about the EPR paradox[3] was aimed at refuting the possibility of a certain class of "hidden variable theories" for quantum mechanics. Bell used an inequality, and later by the use of a multipartite qubit state, the GHZ state it was possible to refine the argument so as not to use an inequality. (This is in [18], although the state discussed is a 4-partite qubit state. The article [8] uses a 3-partite state that is similar to, but not quite the same as the GHZ state explained later).

Apart from this, there has been the development of quantum protocols to do various tasks, such as quantum teleportation[4], superdense coding[6] and so on, as explained in standard references on quantum computing such as [27], but most lucidly explained in terms of the quantum graphical calculus as in the paper [10], with more explanation of this approach in [11].

Resuming our previous discussion, knowing whether a multipartite state is separable or entangled does not say everything, because there are different kinds of entanglement.

A way of seeing that there are several kinds of entanglement is to consider how local operations on the qudits can affect a multipartite state.

The operations that can be applied are of two kinds, unitary operations and measurements. Unitary operations are multiplying states by unitary matrices, i.e. matrices that are invertible and preserve the inner product. Measurements are described in more detail in the standard references, and we refer the reader to them, as we will not actually be discussing measurement very much. We will consider invertible operations because we are considering equivalence classes of states.[2]

The local operations that are not probabilistic are the unitaries. The *global* unitaries are elements of $U(d^n)$, i.e. the unitary group for a d^n-dimensional space. However not all of these transformations can be applied to qudits that are separated from each other. In fact it is only possible for separated qudits to apply unitaries to each system separately. We use the fact that a unitary matrix $u \in U(d)$ can be considered as a linear map $u : \mathbb{C}^d \to \mathbb{C}^d$, so using the fact that $\otimes$ is a functor, we have that for $u_1, u_2 \in U(d)$, we have $u_1 \otimes u_2 : \mathbb{C}^d \otimes C^d \to \mathbb{C}^d \otimes \mathbb{C}^d$. In other words, the non-probabilistic local transformations are elements of a group $U(d) \times \cdots \times U(d)$. If we consider states that can be changed into each other by these, we get LOCC equivalence, or local operations and classical communication (see [5], which considers the more general setting of mixed states). For reasons explained later (in section 0.1.4) we will find it more convenient to study the SLOCC equivalence relation between multipartite states.

SLOCC stands for stochastic local operators and classical communication, is defined in [13]. It is the local operations that can be performed with a positive probability. The sort of new operation that is allowed is that we can take H_1, for instance, and tensor it with an "ancillary" Hilbert space H_A, to get $H_1 \otimes H_A$, and take a state in $\psi \in H_1$, and produce a state $\psi_1 \otimes \psi_A$. Since the ancillary system is not spatially separated, a unitary from $U(\dim(H_1 \otimes H_A))$ can then act on this state. Then the ancilla can be measured, producing a new state in H_1 without affecting the entanglement of H_1 with the other parties.

The SLOCC equivalence uses the general linear group, i.e. the group of all invertible complex matrices, instead of the unitary group. States that are LOCC equivalent are always SLOCC equivalent, but SLOCC equivalent states are not necessarily LOCC equivalent, so there are fewer SLOCC classes, in the suitable sense than LOCC classes. For instance in the case of three qubits there is a finite number, and this was part of the motivation for introducing the definition in [13].

However, just knowing that there are certain equivalence classes of states is not enough. These sets are infinite, so we require some way of handling them other than trying to list their elements. The way we will do this is using algebraic geometry, following on from how separable and entangled states were distinguished in the previous example. The description of subsets of $\mathbb{C}^n$ by the vanishing of sets of polynomials

[2] It is also possible to consider how each state can be converted into another by local operations, and then we will find in general that more can be done.

is familiar from elementary Cartesian geometry. Our start with the use of algebraic geometry methods is to look at it from this point of view (although we will need to generalize later). So to some extent what we might like is to find equations that describe the SLOCC classes as subsets of $\mathbb{C}^{d^n}$.

For two qubits, it is known that a state is either entangled or separable, and those are the only SLOCC classes. When considering more parties than two, it is always possible to have states that are not separable, but where entanglement only exists between a few of the parties, such as the following state of three qubits

$$|000\rangle + |011\rangle = |0\rangle \otimes (|00\rangle + |11\rangle)$$

In cases such as this, the problem is reducible to entanglement of fewer parties. It is already known for three qubits that there are only two SLOCC classes that cannot be reduced to entanglement of fewer parties, the GHZ and W states, as described in [13], and shown here

$$\psi_{GHZ} = |000\rangle + |111\rangle$$
$$\psi_{W} = |100\rangle + |010\rangle + |001\rangle$$

In this case the hyperdeterminant is known which vanishes for the W state but not for the GHZ state, see [25]. The first question we deal with is whether such equations exist for all cases and if there is an effective algorithm to find them.

A second question we will look at is prompted by the fact that there are infinitely many SLOCC classes for four or more qubits (observed in [13], and investigated in [30]). We can keep track of the classes themselves by finding a space $\mathcal{H}//G_{\mathrm{SLOCC}}$ whose points are the SLOCC classes, and a quotient map $\pi : \mathcal{H} \to \mathcal{H}//G_{\mathrm{SLOCC}}$ mapping a state to its SLOCC class, that should be like a principal bundle in the appropriate sense. We will see that to do this it is not only necessary to move on from the setting of varieties and algebraic sets and move to schemes, but also that in some sense just schemes are not enough as quotient spaces even for three qubits. In the further work part we suggest to move beyond schemes to (Artin) stacks.

0.1.1 Group theoretic notions

First we will need to recall some notions about groups and group actions and prove certain facts we will be applying to the action of the d-dimensional n-partite SLOCC group G_{SLOCC} on the Hilbert space $\mathcal{H}$.

We take as given the definition of a group, a group homomorphism and the category of groups. The identity element will always be represented by the letter e.

We will be using the notion of a group action, which is a mathematical definition of what it means for the elements of a group to be (reversible) transformations applied to some set.

A group action is

- A group G.
- A set X.
- A function $\alpha : G \times X \to X$

Such that the following axioms are satisfied:

1. $\alpha(e, x) = x$ for all $x \in X$.
2. For $g, h \in G$ and $x \in X$, $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$.

From now on G, X and α will refer to a group, a set it is acting on and the action respectively whenever there is a group action under discussion, unless indicated otherwise.

The reader may notice that nothing is mentioned about the inverse of the group. In fact this is not necessary, and we prove the following lemma:

Lemma 1. *Let $\alpha : G \times X \to X$ be a group action. For all $g \in G$, $\alpha(g, -) : X \to X$ is a group action, and its inverse is $\alpha(g^{-1}, -)$.*

Proof. Consider $\alpha(g^{-1}, -) : X \to X$. The theorem will follow if it can be shown to be both a left and a right inverse.

- Left inverse: Let $x \in X$. We have $\alpha(g^{-1}, \alpha(g, x)) = \alpha(g^{-1}g, x) = \alpha(e, x) = x$. So $\alpha(g^{-1}, -) \circ \alpha(g, -) = id_X$.
- Right inverse: Let $x \in X$. We have $\alpha(g, \alpha(g^{-1}, x)) = \alpha(gg^{-1}, x) = \alpha(e, x) = x$. So $\alpha(g, -) \circ \alpha(g^{-1}, -) = id_X$.

$\square$

The *orbit* of an element x of X is $\alpha(G, x)$, i.e. every element of X such that there is a transformation in G taking x to it. The reason for this terminology is the case when $G = \mathbb{R}$ and X is a configuration space and we are considering reversible dynamics, and the transformation of the configuration space by a number t is moving each object from where it was at time 0 to where it will be at time t (or was, if t is negative). The orbit is everywhere an object would have been in the past and will be in the future, as in the case of the orbit of a comet, for instance. We will use $O(x)$ to denote the orbit of x as a subset of X, and will do this whenever there is a group action under discussion.

We now consider transformations that turn out not to do anything.

The *stabilizer* of x, $\mathrm{stab}(x)$, is the elements $g \in G$ such that $\alpha(g, x) = x$. In the case that the set X is a set of objects and G is transforming those objects into others, the stabilizer of an individual object x is that object's "symmetries", those transformations that transform it into itself.

Lemma 2. *The set* $\mathrm{stab}(x)$ *is a subgroup of* G.

Proof. Suppose $g, h \in \mathrm{stab}(x)$. We have that $\alpha(gh, x) = \alpha(g, \alpha(h, x)) = \alpha(g, x) = x$, so $gh \in \mathrm{stab}(x)$. Since $\alpha(e, x) = x$ we have that $e \in \mathrm{stab}(x)$. Now suppose that $g \in \mathrm{stab}(x)$. By lemma 1 we have that $\alpha(g^{-1}, -)$ is the inverse of $\alpha(g, -)$, so $\alpha(g^{-1}, x) = x$ and $g^{-1} \in \mathrm{stab}(x)$. $\square$

We will now prove some basic facts about the orbits of a group action and the stabilizers that will be needed later. The first relates stabilizers of points in the same orbit.

Lemma 3. *Points on the same orbit have conjugate stabilizers. Alternatively, if* $x, y \in X$, $y \in O(x)$, *then there is a* g *such that* $\mathrm{stab}(x) = g^{-1}\mathrm{stab}(y)g$.

Proof. Since $y \in O(x)$, we have the existence of a $g \in G$ such that $\alpha(g, x) = y$. The proof proceeds in two steps:

1. To show $g^{-1}\mathrm{stab}(y)g \subseteq \mathrm{stab}(x)$:

   If $h \in \mathrm{stab}(y)$, i.e. $\alpha(h, y) = y$, we may substitute $\alpha(g, x)$ for y, getting

   $$\alpha(h, \alpha(g, x)) = \alpha(g, x)$$

   If we apply $\alpha(g^{-1}, -)$ to both sides, and use the group action axioms, we get:

   $$\alpha(g^{-1}hg, x) = \alpha(g^{-1}g, x) = \alpha(e, x) = x$$

   So $g^{-1}hg \in \mathrm{stab}(x)$. Therefore $g^{-1}\mathrm{stab}(y)g \subseteq \mathrm{stab}(x)$.

2. To show $g^{-1}\text{stab}(y)g \supseteq \text{stab}(x)$, or equivalently that $g\text{stab}g^{-1} \subseteq \text{stab}(y)$:

   Suppose $h \in \text{stab}(x)$, i.e. $\alpha(h, x) = x$. If we consider the correspoding element ghg^{-1} acting on y:

$$\alpha(ghg^{-1}, y) = \alpha(g, \alpha(h, \alpha(g^{-1}, y)))$$

   by using lemma 1, we have:

$$\begin{aligned}\alpha(ghg^{-1}, y) &= \alpha(g, \alpha(h, x)) \\ &= \alpha(g, x) \\ &= y\end{aligned}$$

   Which shows that $ghg^{-1} \in \text{stab}(y)$, and hence that $g\text{stab}(x)g^{-1} \subseteq \text{stab}(y)$.

Putting both of these statements together, we have $\text{stab}(x) = g^{-1}\text{stab}(y)g$. □

The next lemma is an important fact about the structure of the orbits.

Lemma 4. *Let $\alpha : G \times X \to X$ be a group action. If $a, b \in X$ and $\alpha(G, a) \cap \alpha(G, b)$ is non-empty, then $\alpha(G, a) = \alpha(G, b)$. That is to say, distinct orbits do not intersect.*

Proof. Since the orbits of a and b intersect, we may take $x \in \alpha(G, a) \cap \alpha(G, b)$. This implies there exist $g_a, g_b \in G$ such that $\alpha(g_a, a) = x$ and $\alpha(g_b, b) = x$.

Using lemma 1 we may deduce that $\alpha(g_a^{-1}, x) = a$, and so $\alpha(g_a^{-1}, \alpha(g_b, b)) = a$. Therefore $\alpha(g_a^{-1}g_b, b) = a$ and using lemma 1 again we also have $\alpha(g_b^{-1}g_a, a) = b$. The theorem will follow in two steps:

- Every element of $\alpha(G, a)$ is an element of $\alpha(G, b)$:

  Let $y \in \alpha(G, a)$, so there is $g_y \in G$ such that $y = \alpha(g_y, a)$. Combining this with the expression for a in terms of b, we have $y = \alpha(g_y, \alpha(g_a^{-1}g_b, b)) = \alpha(g_y g_a^{-1} g_b, b)$, and so $y \in \alpha(G, b)$.

- Every element of $\alpha(G, b)$ is an element of $\alpha(G, a)$:

  Let $y \in \alpha(G, b)$, so there is $g_y \in G$ such that $y = \alpha(g_y, b)$. Similarly to the previous case, we now have $y = \alpha(g_y, \alpha(g_b^{-1}g_a, a)) = \alpha(g_y g_b^{-1} g_a, a)$, and so $y \in \alpha(G, a)$.

Therefore $\alpha(G, a) = \alpha(G, b)$. □

0.1.1.1 The SLOCC group action

As mentioned in the introduction, a state $\psi \in \bigotimes_i \mathcal{H}_i$ is SLOCC equivalent to another state $\phi \in \bigotimes_i \mathcal{H}_i$ if and only if there are invertible matrices $X_i : \mathcal{H}_i \to \mathcal{H}_i$ such that $\left(\bigotimes_i X_i\right)\psi = \phi$. As is well known, the invertible matrices on a vector space form a group, $GL(n)$, where n is the dimension of the vector space.

For n the number of parties and d the dimension of the single party Hilbert space, we take $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$ as the n-party Hilbert space. We define now the SLOCC group, the group

$$G_{\mathrm{SLOCC}} = \underbrace{GL(d) \times \cdots \times GL(d)}_{n}$$

And the SLOCC group action:

$$\begin{aligned} \alpha \quad &: \quad G_{\mathrm{SLOCC}} \times \mathcal{H} \to \mathcal{H} \\ \alpha((g_1, ..., g_n), \psi) \quad &= \quad (g_1 \otimes \cdots \otimes g_n)\psi \end{aligned}$$

Where the group elements g_i are interpreted as matrices on the right hand side.

Theorem 5. *The map α defined above is a group action.*

Proof. It is necessary to verify the two axioms.

1. To show that $\alpha(e, x) = x$ for all $x \in \mathcal{H}$:

   Since multiplication by a matrix is a linear map, it suffices to verify that this is true for all separable x as every element of $\mathcal{H}$ is a linear combination of separable states. So let us take $x = \psi_1 \otimes \cdots \otimes \psi_n$. Note also that $e = (I, ..., I)$ where I is the identity matrix $\mathbb{C}^d \to \mathbb{C}^d$. Therefore

$$\begin{aligned} \alpha(e, x) &= \alpha((I, ..., I), \psi_1 \otimes \cdots \otimes \psi_n) \\ &= (I \otimes \cdots \otimes I)(\psi_1 \otimes \cdots \otimes \psi_n) \\ &= (I\psi_1) \otimes \cdots \otimes (I\psi_n) \\ &= \psi_1 \otimes \cdots \psi_n = x \end{aligned}$$

2. To show that for all $g, h \in G_{\mathrm{SLOCC}}$ and $x \in \mathcal{H}$, $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$:

   Again, it suffices to verify this for x a separable state, so let $x = \psi_1 \otimes \cdots \otimes \psi_n$. Also, let $g = (g_1, ..., g_n)$ and $h = (h_1, ..., h_n)$. Then

$$\begin{aligned} \alpha(g, \alpha(h, x)) &= \alpha((g_1, ..., g_n), \alpha((h_1, ..., h_n), \psi_1 \otimes \cdots \otimes \psi_n)) \\ &= \alpha((g_1, ..., g_n), (h_1\psi_1) \otimes \cdots \otimes (h_n\psi_n)) \\ &= (g_1h_1\psi_1) \otimes \cdots \otimes (g_nh_n\psi_n) \end{aligned}$$

and

$$\begin{aligned}
\alpha(gh, x) &= \alpha((g_1, ..., g_n)(h_1, ..., h_n), \psi_1 \otimes \cdots \otimes \psi_n) \\
&= \alpha((g_1 h_1, ..., g_n h_n), \psi_1 \otimes \cdots \otimes \psi_n) \\
&= (g_1 h_1 \psi_1) \otimes \cdots \otimes (g_n h_n \psi_n)
\end{aligned}$$

So the two are equal.

□

The SLOCC classes are the orbits of this action. We can use this theorem and lemma 4 to show that the SLOCC classes are equivalence classes.

As mentioned in the introduction, since the objects involved are infinite, we need more structure to work with the SLOCC classes, which is what we discuss next.

0.1.2 Algebraic varieties and algebraic sets

For those already familiar with algebraic geometry, the base field will always be $\mathbb{C}$, which is algebraically closed and of characteristic 0, which simplifies a lot of things. We recommend that the reader consult introductory texts such as [19], [16], [15], which will be referred to for results. We do not make an attempt to state results in the maximum level of generality, but nor have we made any effort to use precisely the least generality necessary.

For readers with no experience of algebraic geometry we present things in terms of subsets of n-dimensional affine space, which as a set we will identify with $\mathbb{C}^n$. Given a basis $e_1, ..., e_n$ of $\mathbb{C}^n$, we may define n functions $x_1, .., x_n : \mathbb{C}^n \to \mathbb{C}$, being the n projections from $\mathbb{C}^n$ to the 1-dimensional[3] subspace generated by each basis vector. From these functions, by using pointwise multiplication, addition and multiplication by a complex number we can get the ring of polynomial functions from $\mathbb{C}^n \to \mathbb{C}$. From these we may define the *algebraic sets*, or algebraic subsets of $\mathbb{C}^n$, which are sets that can be defined by the simultaneous vanishing of a set of polynomial functions, $\{f_1 = 0, ..., f_m = 0\}$.

Instead of the usual topology on $\mathbb{C}^n$, we will be using one adapted to polynomial functions, the Zariski topology. The closed sets in this topology are simply the algebraic sets. We refer to [19] to show that this actually defines a topology. By the usual method of restricting a topology to a subspace, we get a topology on each algebraic set as well. Any topological terminology from now on, such as open set, closed set,

[3] over $\mathbb{C}$

closure, continuous etc. refers to the Zariski topology and not the usual topology on $\mathbb{C}^n$.

Although one way to think of polynomials is as functions $\mathbb{C}^n \to \mathbb{C}$, another way is as elements of a finitely generated ring, such as $\mathbb{C}[x_1, ..., x_n]$, where x_i are just symbols. What is the relationship between the two points of view? From each subset $X \subseteq \mathbb{C}^n$ we may look at the set of all polynomial functions vanishing on it, $I(X) \subseteq \mathbb{C}[x_1, ..., x_n]$. Since anything multiplied by zero is equal to zero, any polynomial function multiplied by one vanishing on X also vanishes on X, which means that $I(X)$ is actually an ideal in $\mathbb{C}[x_1, ..., x_n]$. From any set of polynomial functions $S \subseteq \mathbb{C}^n \to \mathbb{C}$ we can define $Z(S) = \bigcap_{f \in S}\{x \in \mathbb{C}^n : f(x) = 0\}$, i.e. the common zeroes of all the functions in S. We may then consider $Z(I)$ for ideals. What is the relationship between Z and I? At first we might hope that any ideal in $\mathbb{C}[x_1, .., x_n]$ would be $I(X)$ of some set X, but this is not so, it is only the "radical" ideals for which this is true. We can see that if a function f defines a set, the function f^2 vanishes on exactly the same set, so $Z((f))$ and $Z((f^2))$ are the same. However, for sets $Z(I(X)) = X$, so that side is as expected. The full statement is Hilbert's Nullstellensatz, which will appear in a moment. However, the full statement includes a statement about irreducible sets, which is a notion we will be using, so they must be defined first. Irreducibility is a stronger criterion available for algebraic sets than connectivity. As in the case of ordinary topological spaces, an algebraic set is connected if it is not the union of two or more clopen subsets. It is *irreducible* if it is not the union of a finite number of closed sets. An irreducible algebraic set, especially when being considered as a space in its own right rather than a subset, is called a *variety*. However, some authors use the term variety to refer to any algebraic set, so sometimes, in the name of clarity, we refer to a variety as an "irreducible variety".

An example illustrating the difference between algebraic sets and varieties is that the subvarieties of $\mathbb{C}$ are single points, whereas the algebraic subsets are finite sets of points. Note also that the ideal (x^2) in $\mathbb{C}[x]$ is an example of an ideal that is not a radical ideal, it's radical being (x), and the subset of $\mathbb{C}$ being $\{0\}$.

The statement of the Nullstellensatz we give here is a modified version of that in page 4 of [19], to accomodate the fact that we do not need to use a different ground field from $\mathbb{C}$, and combining more than one statement given on that page.

Theorem 6. *If $\mathfrak{a}$ is an ideal in $A = \mathbb{C}[x_1, ..., x_n]$, and $f \in A$ a polynomial which vanishes as all points of $Z(\mathfrak{a})$, then there is an integer $r > 0$ such that $f^r \in I$. There is a one-to-one inclusion reversing correspondence between algebraic subsets of $\mathbf{A}^n$*

and radical ideals (ideals equal to their radical[4]*) given by* $Y \mapsto I(Y)$ *and* $\mathfrak{a} \mapsto Z(\mathfrak{a})$. *An algebraic set is irreducible if its ideal is a prime ideal. A maximal ideal corresponds to a point.*

Proof. See the references given for the proof in [19] for theorem 1.3A, corollary 1.4, or see [15]. □

We will also consider the rings $\mathbb{C}[x_1, ..., x_n]/I(X)$ for X an algebraic set. This gives the ring of functions on X, or the affine ring $A(X)$ of X. To some extent this ring is "independent" of the embedding in the ambient space, different embeddings of algebraic sets have isomorphic rings.

Note that if we consider elements of the ring as functions, the quotient map $\mathbb{C}[x_1, ..., x_n] \to \mathbb{C}[x_1, ..., x_n]/I(X)$ is a kind of partial evaluation of a function, and identifies functions that give identical results on all points of X. In the case the X is a singleton subset and $I(X)$ a maximal ideal, this corresponds simply to evaluation at the point contained in that singleton, as the quotient ring is isomorphic to $\mathbb{C}$. This is the generalization of the "remainder theorem" of elementary algebra.

To avoid confusion when talking about both rings and spaces, the space $\mathbb{C}^n$ will be called $\mathbf{A}^n$, as it is in algebraic geometry texts. This avoids a certain confusion – the set of points of $\mathbf{A}^n$ is isomorphic to $\mathbb{C}^n$, but $\mathbb{C}^n$ is a ring in its own right, and is isomorphic to the ring of functions on a finite set of n distinct points. We should also mention at this point that when we earlier discussed the elements of finitely generated $\mathbb{C}$ algebra, such as $f \in \mathbb{C}[x_1, ..., x_n]/I$ as being functions from $Z(I) \to \mathbf{A}^1$, we know from our discussion about the Nullstellensatz that we can consider a map $\mathbb{C}[x] \to \mathbb{C}[x_1, .., x_n]/I$, with f being the image of the generator x.

For some purposes a notion is needed that is intermediate between an algebraic set and an arbitrary set. In particular, the image of an algebraic set under an algebraic morphism[5] is not necessarily an algebraic set. To make up for this we require the notion of a constructible set. A *constructible* set is a set contained in the smallest Boolean algebra generated by the closed (or equivalently the open) sets in the Zariski topology.

Lemma 7. *Every constructible set is finite union of sets that are open subsets of their closures. In fact, we may express any constructible set* S *as a finite union* $\bigcup_i (C_i \cap \neg C_i')$, *where* C_i *and* C_i' *are closed, and* $C_i \cap \neg C_i'$ *is not empty, and we may choose* C_i *so that* $\overline{S} = \bigcup_i C_i$.

[4] $f \in \text{radical}(\mathfrak{a})$ iff there is a $r > 0$ such that $f^r \in I$

[5] This will be defined later.

Proof. Let us consider the constructible set S. By the definition of a constructible set, it is given by a Boolean expression in terms of closed sets. By repeatedly making use of the distributive laws and de Morgan's law, it is possible to convert any such expression to disjunctive normal form, or DNF. This is described in, for example [21]. An expression in DNF is one of the form

$$\begin{aligned} S &= \left(C_{1,1} \cap \cdots \cap C_{1,n_1} \cap \neg C'_{1,1} \cap \cdots \cap \neg C'_{1,n'_1}\right) \\ &\quad \cup \cdots \\ &\quad \cup \left(C_{m,1} \cap \cdots \cap C_{m,n_m} \cap \neg C'_{m,1} \cap \cdots \cap \neg C'_{m,n'_m}\right) \end{aligned}$$

Since every intersection of closed sets is closed, and every finite intersection of open sets is open, this can be simplified to

$$S = (C_1 \cap \neg C'_1) \cup \cdots \cup (C_m \cap \neg C'_m)$$

Let $X_i = C_i \cap \neg C'_i$. The theorem will be proven if we can show that X_i is an open subset of $\overline{X_i}$.

Since $X_i \subseteq \overline{X_i}$, we have that $X_i = \overline{X_i} \cap X_i$, and so $X_i = (\overline{X_i} \cap C_i) \cap \neg C'_i$. Since $\overline{X_i}$ is the smallest closed set containing X_i, and $X_i \subseteq C_i$, it must be the case that $\overline{X_i} \subseteq C_i$ and so $\overline{X_i} \cap C_i = \overline{X_i}$. Therefore $X_i = \overline{X_i} \cap \neg C'_i$. Now $\neg C'_i$ is an open set, so $\overline{X_i} \cap \neg C'_i$ is open in the subspace topology of $\overline{X_i}$. To show that the C_i can be taken to have their union be $\overline{S}$, consider that we have $S = \bigcup_{i=1}^{m}(\overline{X_i} \cap \neg C'_i)$. Using the fact that closure distributes over union, we have

$$\begin{aligned} \overline{S} &= \overline{\bigcup_{i=1}^{m}(\overline{X_i} \cap \neg C'_i)} \\ &= \bigcup_{i=1}^{m} \overline{(\overline{X_i} \cap \neg C'_i)} \end{aligned}$$

Since $\overline{X_i} \cap \neg C'_i = X_i$ as was shown earlier:

$$\overline{S} = \bigcup_{i=1}^{m} \overline{X_i}$$

So we may satisfy the last statement by picking C_i to be $\overline{X_i}$, and can satisfy the requirement that $C_i \cap \neg C'_i \neq \emptyset$ by leaving out any i where this intersection is empty. □

We also require the notion of the decomposition of a closed set into irreducible sets, so we cite the following theorem.

Theorem 8. *Every algebraic set X, can be expressed as a finite union $X = X_1 \cup \cdots \cup X_n$ of irreducible closed subsets X_i. If we require that $X_i \not\subseteq X_j$ for $i \neq j$, then the X_i are uniquely determined. They are called the irreducible components of X.*

Proof. See proposition 1.5 and corollary 1.6 on page 5 of [19] □

Note that the requirement that none of the sets contain another implies that none of them be empty, as the empty set is contained in every set.

We now show a basic fact about varieties, which is part of exercise I.1.6 in [19].

Lemma 9. *Non-empty open subsets of irreducible varieties are dense.*

Proof. Let X be an irreducible variety. Let $S \subseteq X$ be open and non-empty. The set S is the complement of a closed set C, so $X = S \cup C$, and $S \cap C = \emptyset$. We have that $S \subseteq \overline{S}$, so $X = C \cup S \subseteq C \cup \overline{S}$. Since we also have $\overline{S} \subseteq X$, we have that $C \cup \overline{S} = X$. Since S is non-empty, $C \neq X$. Assume for a contradiction that $\overline{S} \neq X$, and this implies that X is the union of two closed subsets, and hence is reducible, a contradiction. Therefore $\overline{S} = X$, or in other words, S is dense. □

This fact relates to how open sets intersect.

Lemma 10. *Two non-empty open subsets of a (irreducible) variety have a non-empty intersection.*

Proof. Let A, B be non-empty open sets in a variety X. Then $A \cap B$ is open. Suppose for a contradiction that $A \cap B = \emptyset$. Let C and D be the complements of A and B in X. The sets C and D are closed, and applying De Morgan's law to $A \cap B = \emptyset$, we have $C \cup D = X$. Since A and B are non-empty, neither C nor D is equal to X, so X is reducible, a contradiction. Therefore $A \cap B$ is non-empty. □

Lemma 11. *Let A be a constructible set, whose closure, X, is irreducible and non-empty. Then there is a non-empty set $O \subseteq A$ that is open in the subset topology of X.*

Proof. By lemma 7 we have that

$$A = \bigcup_i (C_i \cap \neg C_i')$$

and

$$X = \bigcup_i C_i$$

The unions being finite.

Since X is irreducible, there must be some j such that $C_j = X$. Then $C_j \cap \neg C'_j = X \cap C'_j$ is a non-empty subset of A, and since $\neg C'_j$ is open, it is open in the subset topology of X. $\square$

Lemma 12. *Let A be a constructible set, and $X = \overline{A}$. Let Y be an irreducible component of X, and $B = A \cap Y$. Then $\overline{B} = Y$.*

Proof. Note that if $Y = X$, then $B = A$ and so the theorem holds trivially. So for the rest of the proof we may assume that Y is a strict subset of X.

We have that $B \subseteq Y$, and since Y is closed, this implies $\overline{B} \subseteq Y$. Since Y is a strict subset of X, $X = Y \cup Z$ for some closed set Z (by using the irreducible decomposition of X, theorem 8, and the fact that the union of the other irreducible closed sets is closed), and neither $Y \subseteq Z$ nor $Z \subseteq Y$.

Suppose for a contradiction that $\overline{B}$ is a strict subset of Y. Since $Y \cap Z$ is a strict subset of Y, it must be the case that $\overline{B} \cup (Y \cap Z)$ is a strict subset of Y, or else it would be reducible, since both of those sets are closed. Therefore there is some point $p \in Y$, such that $p \notin \overline{B} \cup (Y \cap Z)$.

Let $C = A \cap Z$. Since Z is closed, we have that $\overline{C} \subseteq Z$, so in particular $p \notin \overline{C}$. So we know that $p \notin \overline{B} \cup \overline{C}$. But $X = \overline{B} \cup \overline{C}$, and $p \in X$, a contradiction. Therefore there can be no such point and $\overline{B} = Y$. $\square$

We now prove an important fact about constructible sets that have the same closure, from which our facts about the orbits will follow.

Lemma 13. *Non-empty constructible sets with the same closure have non-empty intersection.*

Proof. Let A, B non-empty constructible sets, and X their closure. We have the decomposition of X into irreducibles: $X = \bigcup_i X_i$, i ranging over a finite set. Let $A_i = A \cap X_i$, $B_i = B \cap X_i$.

By lemma 12 we have that $\overline{A_i} = \overline{B_i} = X_i$. Since X_i is irreducible and non-empty we may apply lemma 11 to get non-empty sets $O_i^A \subseteq A_i, O_i^B \subseteq B_i$ that are open in the subspace topology of X_i. Since X_i is irreducible, by lemma 10 $O_i^A \cap O_i^B \neq \emptyset$, so $A_i \cap B_i \neq \emptyset$, so $A \cap B \neq \emptyset$. $\square$

0.1.3 Algebraic groups and algebraic group actions

As suggested by the title, this section is about algebraic groups and algebraic group actions. However, to define these, we need to introduce three notions we have been putting aside: quasi-affine varieties, products, regular maps and morphisms of algebraic varieties.

0.1.3.1 Products of varieties, regular maps, and morphisms of algebraic varieties

If $X \subseteq \mathbf{A}^n$ and $Y \subseteq \mathbf{A}^m$ are affine varieties, we can consider the set $X \times Y$ as a subset of $\mathbf{A}^{n+m}$. If we use disjoint sets of variables to define X and Y, we can just take the union of the set of equations defining X in $\mathbf{A}^n$ and the set of equations defining Y in $\mathbf{A}^m$ to get a set defining $X \times Y$ in $\mathbf{A}^{n+m}$ see exercise 3.15 on page 22 of [19] for why this is irreducible. There is a standard warning about the topology on the product – it is not the product topology of the topologies of the two spaces individually.

Let X be an affine variety in $\mathbf{A}^n$. A function $f : X \to \mathbb{C}$ is a *regular* at a point $p \in X$ if there is an open set U with $p \in U$ and polynomials $g, h \in \mathbb{C}[x_1, ..., x_n]$ such that $h \neq 0$ and $f = g/h$ on U. It is a *regular map* if it is regular at every point. (see page 15 of [19]).

With that defined, it is possible to define a morphism of varieties. A *morphism* of varieties $\phi : X \to Y$ is a continuous map such that for every open set $V \subseteq Y$ and for every regular function $f : V \to \mathbb{C}$, the function $f \circ \phi : \phi^{-1}(V) \to \mathbb{C}$ is regular.

Lemma 14. *Let X, Y be affine varieties. Let $\phi : X \to Y$ be a map defined by equations $y_i = f_i(x_1, ..., x_n)$ where $\{y_i\}$ and $\{x_i\}$ are the coordinate functions on Y and X respectively, and f_i are polynomials. Then ϕ is a morphism.*

Proof. The equations given above define a $\mathbb{C}$-algebra homomorphism $A(Y) \to A(X)$. By proposition 3.5 on page 19 of [19] there is an isomorphism between $\mathbb{C}$-algebra homomorphisms $A(Y) \to \mathcal{O}(X) \cong A(X)$ (the isomorphism on the right is by theorem 3.2 (a) on page 17) and morphisms $X \to Y$, which are given by the same equations. $\square$

0.1.3.2 Definition of an algebraic group and algebraic group action

An *algebraic group* is simply a group that is also an algebraic variety. More specifically, it is:

- An affine variety G

- A multiplication map, a morphism $\mu : G \times G \to G$.
- An identity element, a point $e \in G$.
- An inverse map, a morphism ${}^{-1} : G \to G$

Satisfying the usual group axioms. This is analogous to the definition of topological groups and Lie groups, and all three of these fall under the definition of an "internal group in a cartesian category" (see [22]).

Note that this is a more restrictive definition than is commonly used for an algebraic group, in particular under this definition $SL(n)$ is not an algebraic group as it is not irreducible, seeing as it is not connected. However, this is not important for the examples being studied here.

An *algebraic group action* is:

- An algebraic group G
- An algebraic variety X
- An algebraic morphism $\alpha : G \times X \to X$

Such that these satisfy the group action axioms.

The previous terminology for group actions, such as orbits and stabilizers, is used unchanged in the case of algebraic group actions.

The underlying set functor is denoted $U : \mathrm{Var}(\mathbb{C}) \to \mathrm{Set}$. For a variety $U(X)$ is simply the set of points. For a map of varieties $f : X \to Y$, $U(f)$ is just the underlying function mapping the points of X to the points of Y.

U is faithful because morphisms are defined to be functions themselves, with an extra condition imposed, so if they are equal as set-theoretic functions they are equal as morphisms.

Theorem 15. *G_{SLOCC} is an (affine) algebraic group.*

Proof. From its definition, $G_{\mathrm{SLOCC}} = \underbrace{GL(d) \times \cdots \times GL(d)}_{n}$. Each factor $GL(d)$ is the set of $d \times d$ invertible matrices, an open subset of $\mathbf{A}^{d^2}$ defined by the non-vanishing of the determinant. This is an algebraic subset of $\mathbf{A}^{d^2+1}$: if we call the coordinates g_{ij} for $i, j \in \{1, ..., d\}$ and the last one y, then $GL(d)$ is defined by $y \det(g_{ij}) - 1 = 0$. It is also a variety – any decomposition of $GL(d)$ into finitely many proper closed subsets would imply such a decomposition of $\mathbf{A}^{n^2}$, since it is an open subset of it, and this is is impossible. Therefore G_{SLOCC} is an affine variety, being a finite product of such. It could also be considered an open subset of $\mathbf{A}^{nd^2}$.

The multiplication map $\mu : G_{\text{SLOCC}} \times G_{\text{SLOCC}} \to G_{\text{SLOCC}}$ is given by the usual matrix multiplication. To be more definite, take $g_{i,ab}, h_{i,ab}, k_{i,ab}$ to be coordinate functions on each of the three copies of G_{SLOCC}, considered as an open subset of $\mathbf{A}^{nd^2}$, with $i \in \{1, ..., n\}$ and $a, b \in \{1, ..., d\}$. Now μ can be expressed:

$$k_{i,ab} = \sum_{c=1}^{d} g_{i,ac} h_{i,cb}$$

We may apply lemma 14 to see that this defines an algebraic morphism.

The inverse map $^{-1} : G \to G$ is given by Cramer's rule. We do not reproduce this here, but only note that it is necessary to divide by the determinant. This is given using the extra variable y, which is equal to $\det(g_{ij})^{-1}$ to avoid having to make use of locally defined functions, and this is the reason for the underlying variety not being the whole of $\mathbf{A}^{n^2}$. This defines a morphism by using 14 again.

The identity element is exactly as expected with no real extras introduced by the algebraic setting.

Associativity and the property of the inverse for morphisms follow from their being true for G_{SLOCC} as a (set) group, by using the faithfulness of U, the underlying set functor. $\square$

Corollary 16. *With G_{SLOCC}, $\mathcal{H}$ and α as in theorem 5, α is an algebraic group action.*

Proof. Like the above, all that is really necessary is to show that α is a morphism, as the identities needed to prove the axioms follow from the fact that they hold set theoretically.

The group action $\alpha : G_{\text{SLOCC}} \times \mathcal{H} \to \mathcal{H}$ is given by taking a tuple of invertible matrices $(g_1, ..., g_n) \in G_{\text{SLOCC}}$, taking the tensor $g_1 \otimes \cdots \otimes g_n$, and multiplying that by an element $\psi \in \mathcal{H}$.

If we use x_j and y_i as coordinates on the two copies of $\mathcal{H}$, with $i, j \in \{0, ..., d^n - 1\}$, then α is given by

$$y_i = \sum_{j=0}^{d^n-1} \left(\begin{pmatrix} g_{1,11} & \cdots & g_{1,1d} \\ \vdots & \ddots & \vdots \\ g_{1,d1} & \cdots & g_{1,dd} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} g_{n,11} & \cdots & g_{n,1d} \\ \vdots & \ddots & \vdots \\ g_{n,d1} & \cdots & g_{n,dd} \end{pmatrix} \right)_{ij} x_j$$

The inner $\otimes$ meaning a Kronecker product, i.e. what the tensor amounts to on explicitly given matrices.

Like in the case of the group itself, we may use lemma 14 to show that α is a morphism, and use the faithfulness of U to see that the group action axioms follow from the fact that the maps still exist and so must still satsify the required identities. $\square$

We are nearly in position to prove the first main theorem about the orbits. But first, we must explain about Chevalley's theorem, which is the reason for all the previous theorems about constructible sets, and to state it we need to explain a bit about schemes and morphisms of finite type.

0.1.3.3 Affine schemes, morphisms of finite type and Chevalley's theorem

In order to show that certain standard results are applicable in the setting we have been using, we must make reference to schemes. For an introduction to schemes see [16] and chapter II of [19]. Since we will not be proving results about schemes, only combining results cited, we do not always fully explain all the terms in the definitions, leaving that to the above references.

Shortly after seeing the Nullstellensatz, we saw that it was possible to get a ring from any algebraic set X in $\mathbf{A}^n$ by taking the ring $R = \mathbb{C}[x_1, ..., x_n]/I(X)$, which we see is the ring of globally defined regular functions on X. The Nullstellensatz established a geometric relationship between ideals in the rings $\mathbb{C}[x_1, ..., x_n]$ and subsets of $\mathbf{A}^n$, so one is lead to wonder if a similar relationship can be established between ideals in the rings such as R and subsets of X as a topological space in its own right. This is the beginning of affine schemes. Affine schemes are defined by taking spectra of rings. The *spectrum* of a ring R, $\mathrm{Spec}(R)$, is a topological space whose points are the prime ideals of R. For each ideal $\mathfrak{a} \subseteq R$, the set $V(\mathfrak{a})$ is the set of all prime ideals containing $\mathfrak{a}$. The closed sets of the topology on $\mathrm{Spec}(R)$ are the sets of the form $V(\mathfrak{a})$. We refer to lemma 2.1 on page 70 of [19] to show that this makes a topology. In fact, to get the affine scheme, we define a sheaf of rings $\mathcal{O}$ on $\mathrm{Spec}(R)$, the *structure sheaf*, that is, we give a ring $\mathcal{O}(U)$ for each open set U of $\mathrm{Spec}(R)$, and for each inclusion $U_1 \subseteq U_2$ we get a ring homomorphism $\mathcal{O}(i_{1,2}) : \mathcal{O}(U_2) \to \mathcal{O}(U_1)$. Also, we have the functions can be patched together from open sets if they agree on the intersections. The definition of this sheaf is given in the previous reference, but in the case of the affine ring of an algebraic set, $\mathcal{O}(U)$ is simply the regular functions defined on U, and the map for each inclusion is just restriction of the domain of a function. An affine scheme is the space $\mathrm{Spec}(R)$ as well as the sheaf $\mathcal{O}$.

For an algebraic set X, the topological space $X' = \mathrm{Spec}(\mathbb{C}[x_1, ..., x_n]/I(X))$ is not quite the same as X with the Zariski topology as a subspace of $\mathbf{A}^n$. The difference is that for each closed set of X that is not a point, X' has an extra point inside, because the points of X' were the prime ideals and not the maximal ideals. However, if we consider the subset of closed points, the subspace topology on this set can be seen to be the Zariski topology, since the definition of a closed set is essentially the same.

We give the definition of a scheme from page 74 of [19]. A *scheme* is a topological space X, a sheaf of rings $\mathcal{O}_X$ such that it is a "locally ringed space" and each point in the topological space has an open neighbourhood U such that the restriction of $\mathcal{O}_X$ to U is isomorphic to the spectrum of a ring. These are called "affine neighbourhoods".

A morphism of affine schemes is given by a continuous map and a morphism of sheaves from the direct image of the domain's structure sheaf to the codomain's structure sheaf. However, we do not require this notion, because by proposition 2.3 on page 73 of [19], every morphism from $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ actually comes from a ring homomorphism $R \to S$.

An affine scheme *over* $\mathbb{C}$ is an affine scheme with a morphism to $\mathrm{Spec}(\mathbb{C})$, and the category $\mathrm{Sch}(\mathbb{C})$ is the slice category of schemes over $\mathrm{Spec}(\mathbb{C})$. By what we just said, an affine scheme over $\mathrm{Spec}(\mathbb{C})$ is the spectrum functor applied to a map $\mathbb{C} \to R$, which is to say, it is a ring R being given the structure of a $\mathbb{C}$-algebra.

We will use the following fact from page 78 of [19]:

Theorem 17. *There is a fully faithful functor $t : \mathrm{Var}(\mathbb{C}) \to \mathrm{Sch}(\mathbb{C})$ from the category of varieties over $\mathbb{C}$ to the category of schemes over $\mathbb{C}$.*

Now, we need the definition of a *morphism of finite type*.

Paraphrasing page 84 of [19], a morphism $f : X \to Y$ of schemes is of finite type if there is a covering of Y by open affine subsets $V_i = \mathrm{Spec}(B_i)$ such that for each i, $f^{-1}(V_i)$ can be covered by *finitely many* open affine subsets $U_{ij} = \mathrm{Spec}(A_{ij})$, where each A_{ij} is a finitely generated B_i-algebra. This means that each $A_{ij} = B_i[x_1, .., x_{n_{ij}}]/I$ for some ideal I.

In the following we have implicitly moved from the affine variety to the corresponding affine scheme, and will do so again in future without further warning.

Corollary 18. *The morphism $\alpha : G_{\mathrm{SLOCC}} \times \mathcal{H} \to \mathcal{H}$ is of finite type.*

Proof. By the expression for $y_{k_1k_2...k_n}$ in terms of $x_{j_1j_2...j_n}$ and the group coordinates in corollary 16, the $\mathbb{C}$-algebra homomorphism is:

$$f : \mathbb{C}[y_{k_1k_2...k_n}] \to \mathbb{C}[x_{j_1j_2...j_n}, g_{i,ab}, y_i]/(y_1 \det g_{1,ab} - 1, y_2 \det g_{2,ab} - 1, ..., y_n \det g_{n,ab} - 1)$$

It constructs $\mathbb{C}[y_{k_1k_2...k_n}]$ as a finitely generated $\mathbb{C}[x_{j_1j_2...j_n}, g_{i,ab}, y_i]/(y_1 \det g_{1,ab} - 1, y_2 \det g_{2,ab} - 1, ..., y_n \det g_{n,ab} - 1)$-algebra since only finitely many equations are involved. □

We now state Chevalley's theorem:

Theorem 19. *Let $f : X \to Y$ be a morphism of finite type of Noetherian schemes. The image of a constructible subset of X is a constructible subset of Y.*

Proof. Either see exercise 3.19 on page 94 of [19], or alternatively, take affine charts (finitely many, by the hypothesis that f is of finite type) on Y, and apply the affine version of the theorem in corollary 14.7 on page 315 of [15]. Then use the fact that we only need to take a finite union, so the union of the images is a constructible set in Y. □

We need a lemma on "finite-typeness" so that we can apply a theorem later.

Lemma 20. *If X, Y, Z are schemes of finite type over $\mathbb{C}$ and $f : X \times Y \to Z$ is a morphism of finite type, and y is a geometric point*[6] *of Y, then the map $f_y : X \to Z$ is also of finite type.*

Proof. The morphism f_y is the result of substituting the geometric point y for the variable ranging through Y. That is to say,

$$f_y = f \circ (\mathrm{id}_X, y)$$

Now id_X is of finite type, as is y itself. The construction $(-, -)$ of two finite type morphisms is finite type, because the tensor of two finitely generated algebras is finitely generated. Since the composition of two morphisms of finite type is of finite type, we have that f_y is of finite type, as required. □

Combining all of the results so far, we prove that orbits are determined by their closures.

Theorem 21. *Let $\alpha : G \times X \to X$ be an algebraic group action, with the morphism α being of finite type. Let x, y be two geometric points in X. If $\overline{O(x)} = \overline{O(y)}$ then $O(x) = O(y)$, i.e. if two orbits have the same closure, they are equal.*

[6] That is to say, a morphism $\mathrm{Spec}(\mathbb{C}) \to Y$, and the corresponding prime ideal of Y that is the pre-image of the zero ideal in $\mathbb{C}$

Proof. Let $\alpha : G \times X \to X$ be an algebraic group action, and x, y two points of X. The function $\alpha_x = \alpha(-, x) : G \to X$ has as its image the orbit of x. By lemma 20 α_x is of finite type, and so by Chevalley's theorem (theorem 19) the orbit is a constructible set. We assume that $\overline{O(x)} = \overline{O(y)}$, a single closed subset of X that we will call Z. $O(x)$ and $O(y)$ are non-empty constructible sets with the same closure, Z. It follows by lemma 13 that $O(x) \cap O(y)$ is not empty. If we take the underlying sets of the varieties G and X then α is a group action of sets and we may apply lemma 4 and deduce that $\alpha_x(G) = \alpha_y(G)$. $\square$

Note that this is false for topological group actions. An example of this is the action of $\mathbb{Z}$ on the circle by irrational rotations. Each orbit is dense in this case, but there are uncountably many orbits and they all have the same closure.

0.1.3.4 Algorithmic calculation of the closure of the image

If we consider a map of affine varieties $f : X \to Y$. If we want to find the image of Y, we should consider the polynomials $x : Y \to \mathbf{A}^1$ that vanish on $f(X)$, i.e. $x \circ f : X \to \mathbf{A}^1$ is the zero map. If we take $X = \mathrm{Spec}(S)$ and $Y = \mathrm{Spec}(R)$ and $\phi : R \to S$ such that $\mathrm{Spec}(\phi) = f$, this corresponds to looking for elements in $\ker \phi$. However, this can only obtain the closure of the image, which is not necessarily equal to the image. This has been the reason for looking at what we can do with closures of constructible sets so far.

We can find the closure of the image of a morphism using the method described in pages 361-362 of [15], done using Gröbner bases.

To describe this, if $R = \mathbb{C}[x_i]$[7] and $S = \mathbb{C}[y_j]/I$, and $\phi : R \to S$ to be defined by some set of equations

$$x_i = f_i$$

Where f_i are expressed in terms of y_j. This defines the morphism $f = \mathrm{Spec}(\phi)$.

However, these equations could also be considered to define an ideal in $T = \mathbb{C}[x_i, y_j]$ and as such define the graph of the map algebraically. Now, as proposition 15.30 on page 362 of [15] states, if we have a map $\phi : S = \mathbb{C}[x_1, ..., x_r] \to R$ we have that $\ker \phi = I \cap S$, so we can get the closure of the image if we know how to eliminate variables from ideals.

[7] We can always extend the codomain of the function to $\mathbf{A}^n$ for some n, and hence let R be a free polynomial ring.

The elimination can be accomplished using Gröbner bases of the ideals, as described in [15]. The definition of a Gröbner basis is discussed there. It is a special kind of generating set for an ideal in a polynomial ring.

I originally used my own implementation of the Buchberger algorithm for Gröbner basis computations, but found my implementation to be too slow, so I used Sage [29]. In particular, I used the `elimination_ideal` function to compute the ideal discussed above, and this function does the computations using Singular [12], which chooses from more than one algorithm.

The particular algebraic group action involved is the action of G_{SLOCC} on $\mathcal{H}$. In the case of three qubits I have used this algorithm to show that the GHZ state has a dense orbit, and that the closure of the orbit of the W state is given by the hyperdeterminant, recapitulating the previous work on the subject. I have also calculated a set of equations defining the closure of the orbit of $|0000\rangle + |1111\rangle$, a four qubit state, which I give in an appendix.

By combining theorem 21 with the algorithm for the closure of an orbit of a state it is possible to tell if two states have the same orbit as the closures will be the same. However, the orbit depends a great deal on the exact value of the point, and non-generic orbits such as the W-state can be perturbed into a state with a different stabilizer by an arbitrarily small change in position. Therefore for actual computations it is not a good idea to normalize the states by dividing by an irrational number approximated using floating point, but one should instead use unnormalized states directly.

0.1.3.5 The orbit inside the closure

It is nice to have the closure of the orbit, but it would be even better to calculate the orbit exactly. We will show how it is possible to get the set $\overline{O(x)} \backslash O(x)$, and hence the equations for the orbit as a constructible set (in fact, a difference of two closed sets). We describe the theorems necessary to show that the approach is correct here.

To show that the closure of an orbit is a union of orbits, we need a lemma about how functions can separate points from closed sets.

Lemma 22. *Let X be an algebraic set. Suppose S is a closed subset of X and y a point in X that is not in S. Then there exists an algebraic function which vanishes on S but is not zero at y.*

Proof. Using the Nullstellensatz (theorem 6) we will convert this statement to a statement about ideals. For each set we have the corresponding radical ideal, $I(X)$,

$I(S)$ and $I(\{y\})$ with the inclusion relations between the ideals being reversed with respect to the inclusions of sets. The elements of $I(S)$ are the algebraic functions that vanish on S. So the statement to be shown is that there is an $f \in I(S)$ such that $f(y) \neq 0$, i.e. $f \notin I(\{y\})$. Now $y \notin S$, i.e. $\{y\} \not\subseteq S$, so in terms of ideals, $I(S) \not\subseteq I(\{y\})$. Therefore there must exist some $f \in I(S)$ such that $f \notin I(\{y\})$, which is enough to prove the lemma. $\square$

Lemma 23. *$\overline{O(x)}$ is a (disjoint by lemma 4) union of orbits, as a set. Equivalently, if $y \in \overline{O(x)} \backslash O(x)$, $O(y) \subset \overline{O(x)}$.*

Proof. Suppose $y \in \overline{O(x)} \backslash O(x)$, and assume for a contradiction that $z \in O(y)$, but $z \notin \overline{O(x)}$. Since $\overline{O(x)}$ is closed, by lemma 22 there exists an algebraic function f that vanishes on $\overline{O(x)}$ but is nonzero on z.

Since $z \in O(y)$, we have that there is a $g \in G$ such that $\alpha(g, y) = z$, and so by lemma 1 $\alpha(g^{-1}, z) = y$. So define $f_{g^{-1}} = f \circ \alpha(g^{-1}, -) : X \to \mathbb{C}$. Now $f_{g^{-1}}(y) = f(\alpha(g^{-1}, y)) = f(z) \neq 0$, by definition. We also have that $f_{g^{-1}}(O(x)) = f(\alpha(g^{-1}, O(x))) = f(O(x)) = 0$ by the definition of f. Since $f_{g^{-1}}^{-1}(0)$ must be a closed set by the continuity of the two functions defining it, it must be the case that $f_{g^{-1}}(\overline{O(x)}) = 0$, and hence that $f_{g^{-1}}(y) = 0$, a contradiction. $\square$

Lemma 24. *The preimage of an ideal under a ring homomorphism is an ideal. The preimage of a prime ideal is a prime ideal.*

Proof. Let $f : R \to S$ be a ring homomorphism, and I an ideal of S. Suppose $y \in f^{-1}(I)$ and $r \in R$. We need to know if $ry \in f^{-1}(I)$ or not, or equivalently, whether or not $f(ry) \in I$. Now

$$f(ry) = f(r)f(y)$$

and since $y \in f^{-1}(I)$, we have $f(y) \in I$, and since $f(r) \in S$, and I is an ideal this implies that $f(r)f(y) \in I$, thus showing $f^{-1}(I)$ is an ideal in R.

Now let us consider prime ideals. Let $\mathfrak{p}$ be a prime ideal in S. Recall that being a prime ideal means that if $x, y \in S$ and $xy \in \mathfrak{p}$, then either x or y was already an element of $\mathfrak{p}$. Now let us consider $f^{-1}(\mathfrak{p})$, already known to be an ideal by the above, and $x, y \in R$, such that $xy \in f^{-1}(\mathfrak{p})$. This implies $f(xy) \in \mathfrak{p}$, so $f(x)f(y) \in \mathfrak{p}$, and by primeness of $\mathfrak{p}$, either $f(x) \in \mathfrak{p}$ or $f(y) \in \mathfrak{p}$, so either $x \in f^{-1}(\mathfrak{p})$ or $y \in f^{-1}(\mathfrak{p})$, as required. $\square$

For the following we will need this topological lemma.

Lemma 25. *Let X be a topological space, and C a closed subset. Let D be a set closed in the subspace topology of C. Then D is closed in X. Also, if D is irreducible in C, it is also so in X.*

Proof. Since D is closed in the subspace topology of C, there is a closed set $E \subseteq X$ such that $E \cap C = D$. Since the intersection of closed sets is closed, D is closed.

For the second statement, if D is irreducible, i.e. is not the finite union of more than one closed set in C, it cannot be reducible in X, because the sets composing it must already have been contained in C. □

In order to prove facts about the dimension, we give Hartshorne's version of the definition of dimension at the bottom of page 5 of [19] The definition of dimension is that the dimension of X is the supremum of all integers n such that there is a chain $Z_0 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X.

This definition can also be obtained by applying the Nullstellensatz (theorem 6) to the definition of the Krull dimension, as described on page 227 of [15].

Lemma 26. *A closed strict subset of an irreducible variety has strictly smaller dimension.*

Proof. Let X be an irreducible algebraic variety and S a strict closed subset. Let $C_0 \subset \cdots \subset C_d$ be a chain of irreducible closed subsets of S of the maximum length. By lemma 25, these make a chain of irreducible closed sets in X. We may then extend the chain to $C_0 \subset \cdots \subset C_d \subset X$, the last inclusion also being strict because $C_d \subseteq S \subset X$. This chain is longer, so $\dim X > \dim S$. □

Lemma 27. *If A, B are closed sets, then* $\dim A \cup B = \max\{\dim A, \dim B\}$.

Proof. If $A \subseteq B$ or $B \subseteq A$ then $A \cup B = B$ or A respectively, so the statement is trivial.

Therefore we may assume that $A \not\subseteq B$ and $B \not\subseteq A$.

If $S \subseteq A \cup B$, then $S = S_A \cup S_B$ for some sets $S_A \subseteq A$ and $S_B \subseteq B$. Therefore if S is irreducible, either $S_A = S_B$ and $S \subseteq A \cap B$ or one of the sets is empty.

Let $C_1 \subset \cdots \subset C_d$ be a chain of irreducible subsets of $A \cup B$ of maximum length. Since C_d is irreducible, it is in either A or B, and therefore the entire chain is contained in either A or B, so $\dim A \cup B \leq \max\{\dim A, \dim B\}$.

On the other hand, any chain of irreducible subsets of A or B is also one in $A \cup B$, so $\dim A \cup B \geq \max\{\dim A, \dim B\}$. Therefore the two sides are equal. □

Now we are able to prove a theorem distinguishing orbits disjoint from $O(x)$ inside $\overline{O(x)}$, the theorem that they have a different dimension.

Theorem 28. *If $y \in \overline{O(x)}$, then $\dim \overline{O(y)} = \dim \overline{O(x)}$ iff $y \in O(x)$.*

Proof.

- If $y \in O(x)$, then $y \in O(y) \cap O(x)$ so by lemma 4 $O(y) = O(x)$, so $\dim \overline{O(y)} = \dim \overline{O(x)}$ trivially.

- The nontrivial case is then to show that $\dim \overline{O(y)} = \dim \overline{O(x)}$ implies $y \in O(x)$, or equivalently that $y \notin O(x)$ implies $\dim \overline{O(y)} \neq \dim \overline{O(x)}$.

  So suppose that $y \in \overline{O(x)}$ but $y \notin O(x)$. We may decompose $\overline{O(x)}$ into irreducible closed sets as $Z_1 \cup .. \cup Z_k$ for some k, by 8. Define $A_i = O(x) \cap Z_i$. By lemma 12 $\overline{A_i} = Z_i$, and by lemma 11 A_i contains a non-empty set O_i that is open in the subspace topology with respect to Z_i. By the fact that $y \notin O(x)$ and lemma 4, $O(y) \subseteq \overline{O(x)} \backslash O(x)$, so $O(y) \cap Z_i \subseteq Z_i \backslash O_i$, and we will let $Y_i = Z_i \backslash O_i$, which is a closed set in Z_i, and hence a closed set by lemma 25. By lemma 26, $\dim Y_i < \dim Z_i$. Let Y_j be a set of maximum dimension amongst the Y_i sets. Then by lemma 27

$$\dim \bigcup_i Y_i = \dim Y_j < \dim Z_j \leq \dim \bigcup_i Z_i = \dim \overline{O(x)}$$

  Since $O(y) \subseteq \bigcup_i Y_i$, $\overline{O(y)} \subseteq \bigcup_i Y_i$, and so $\dim \overline{O(y)} \leq \dim \bigcup_i Y_i$.

  Putting these statements together, $\dim \overline{O(y)} < \dim \overline{O(x)}$.

□

The theorem above is what gives us the method for finding the equations for the complement of the orbit in its closure. By lemma 23, we have that the action $\alpha : G \times X \to X$ when restricted from $G \times X$ to $G \times \overline{O(x)}$, can have the codomain restricted to $\overline{O(x)}$. Since we required group actions to act on varieties, we use lemma 24 and the fact that the closure of the image of α_p is given by the kernel of the map of affine rings the other way, and that X is a variety, so the zero ideal of its affine ring is prime, to show that $\overline{O(x)}$ is irreducible in the case of the G_{SLOCC} group action. Let us call this group action $\beta : G \times \overline{O(x)} \to \overline{O(x)}$. We will consider the family of maps parameterized by $p \in \overline{O(x)}$, $\beta_p : G \to \overline{O(x)}$, obtained by evaluating β at p.

The space $O(p)$, as a constructible subset of X, and is a scheme in its own right. We can consider the map $\alpha_p : G \to O(p)$. Now we already know that G is non-singular (in fact all algebraic groups in characteristic 0 are non-singular).

Lemma 29. *For each point $p \in X$, $O(p)$, as a scheme, is non-singular.*

Proof. By corollary 8.16 on page 178 of [19], it is non-singular on an open set, so there is some (closed) point $q \in O(p)$ at which $O(p)$ is non-singular. Since $q \in O(p)$, there is some $g \in G$ such that $\alpha(g, p) = q$. Since $\alpha(g^{-1}, -)$ is the inverse of $\alpha(g, -)$, this means there is an automorphism of $O(p)$ taking p to q, so they have isomorphic local rings, so q is also non-singular, and therefore $O(p)$ is non-singular. □

We refer to [19] for the definitions of tangent spaces and so on. Now consider the maps $\alpha_p : G \to O(p)$. They are smooth maps because the action α is smooth, as it is also a Lie group action. So by proposition 10.4 on page 270 of [19], at every closed point the map of tangent spaces is surjective, so the rank of the map is the dimension of the tangent space of the image point. Since $O(p)$ is non-singular by lemma 29, the dimension of the tangent space is the same as that of $O(p)$. If the point is the identity element of $e \in G$, this implies that the rank of the linear map $T\alpha_p : TG_e \to TO(p)_p$ is equal to the dimension of $O(p)$.For convenience, let $k = \dim \overline{O(x)}$. If we allow p to vary in $\overline{O(x)}$, and include the tangent space of $O(p)$ in that of $\overline{O(x)}$, we get a family of matrices, a map $\overline{O(x)} \to (TG_e^* \otimes \mathbb{C}^k)$, a family of matrices. We have that the rank is less than k iff all the $k \times k$ minors of it are zero. So equations vanishing on the locus where the dimension of the orbit is less than $\dim \overline{O(x)}$ are given by these determinants in terms of the coordinate functions giving p on $\dim \overline{O(x)}$.

Therefore we may calculate equations and inequations defining the SLOCC class of any (pure) state at all.

0.1.4 LOCC equivalence, and mixed states

It is not possible to use the methods developed above for LOCC equivalence as the unitary group is not an algebraic group. In fact it is not even a complex Lie group, because compact complex Lie groups are commutative, see page 119 of [17]. It is, however, a real algebraic group, in the sense of real algebraic geometry[7], by defining the real and imaginary parts of the complex variables as separate real variables.

It is then possible to use the Tarski-Seidenberg theorem (in the form of corollary 1.4.7 on page 20 of [7]) instead of Chevalley's theorem and semi-algebraic sets (Boolean combinations of subsets of $\mathbb{R}^n$ defined by polynomial inequalities) instead of constructible sets to show that the orbits are semi-algebraic. In fact we can show that the orbits are all closed, by using the classical topologies on $U(n)$ and $\mathbb{R}^n$: $U(n)$ is compact, and $\mathbb{R}^n$ is Hausdorff, and the image of a compact space in a Hausdorff space is closed. However, it is difficult to find fast implementations of the algorithms to perform these operations, so I have not made an implementation of these and refined the results for LOCC. The usual algorithm is cylindrical algebraic decomposition, but a faster algorithm (only a single exponential in the number of variables instead of a double exponential) is described in chapter 13 of [2] but there is as yet no standard implementation and I did not in the end have time to produce my own implementation.

0.2 Quotients and the space of SLOCC classes

If we consider the relevant dimension of $\mathcal{H}$ and G_{SLOCC} as n, the number of parties, becomes larger and larger, something is apparent. As $\dim \mathcal{H} = d^n$ and $\dim G_{\mathrm{SLOCC}} = nd^2$, one grows linearly with n, and the other exponentially. Since the dimension of the orbit must be less than the dimension of the group, this means that the situation with three qubits, where there is a finite set of SLOCC classes, is quite exceptional. So the question comes up of how to understand the set of all SLOCC classes, rather than each SLOCC class individually as we have been dealing with up to now.

One way to do classification of all SLOCC classes would be to take the quotient space of X by G. If we consider the set theoretic quotient, we have a map $\phi : X \to X//G$. Each element of $X//G$ corresponds to an orbit. However, just using the set is too unwieldy and we need some more constructive method. One way to do this is to define the structure of an algebraic variety, or something similar to that, on the set of orbits.

To understand how this works algebraically, consider what the functions from $X//G$ to $\mathbf{A}^1$ would be. Each function $f : X//G \to \mathbf{A}^1$ could be considered as a function $g : X \to \mathbf{A}^1$ by composing with ϕ. The function g would have the same value on points that are identified by ϕ, i.e. it would be invariant under the action of G.

The invariant functions form a subring of the coordinate ring of X. Since we already looked at the spectrum as a way of getting a space from a ring, we could consider taking the spectrum of the ring of invariants.

Mumford has a book on how to take quotients of schemes by reductive algebraic groups [26]. Mumford distinguishes between a “categorical quotient” and a “geometric quotient”, and although the process described above gets a categorical quotient, if we want a space whose points correspond to the orbits of the action, what is wanted is a “geometric quotient”. However, this is only obtained if the action is closed, i.e. if all of the orbits are closed. This can be seen not to be the case for even three qubits, when the GHZ state had a dense orbit but was not the only SLOCC class.

In relation to this, the ring of covariants (which includes the invariants) has been computed for four qubits in the paper [9]. Also the paper [24] has computed the Hilbert series of the invarants for 5 qubits and states that computing the invariants for 5 qubits is computationally out of reach. So it would seem that this way is blocked, although I discuss this more in the section on future work.

0.3 Future Work

The first thing I will be trying is to try some 5-qubit states on a faster computer, to see what can be found in that case.

To fix up the problem of the quotient space not having the right points in it, I propose to use the orbit groupoid or the quotient stack, as described in [23] on pages 11,17 and 29 (example 4.6.1). The thing to do would then be to decompose it according to the conjugacy class of stabilizers associated to each orbit. But I do not know how to do this in arbitrary cases, although this is effectively what has been done in cases where a full classification is known, such as 3 and 4 qubits. We note that the stack can be discussed as an internal groupoid in the category of schemes, as was done in part of the paper [1].

With regard to the computational problem of finding the invariants, the method used is designed to work on a completely arbitrary group action. But in fact we know that the group action is a tensor product of representations of $PGL(d)$. From the theorem called theorem 10 in [28] we know that for compact groups G_1, G_2 the tensor of irreducible[8] representations is irreducible and that every representation of $G_1 \times G_2$ can be decomposed into tensor products of irreducible representations of G_1 and G_2. Now $GL(d)$ is not compact, so the theorem does not apply directly, but we can instead use the "unitarian trick" (see page 129 of [17]), taking the compact real form of $GL(d)$ to show that this holds for representations of $GL(d)$. I suspect there should be some kind of "Künneth formula" for invariants, perhaps that is already known, that could help with calculating the invariants of the action of G_{SLOCC} on $\mathcal{H}$ from the fact that the representation theory of $PGL(d)$ is essentially completely known using the theory of Lie algebras and the Weyl group.

[8] This is a completely different kind of irreducible from what we have previously been discussing. It means that the representation has no invariant subspace.

The representation theory could also be used to improve calculation of the polynomials vanishing on a given orbit. I hope that in the long run it will not be necessary to write out all of the terms in the polynomials, as seen in the appendix, but rather to be able to abbreviate them, just as it is not necessary to write out the full formula for determinants when they are being used.

.1 Appendix 1

If we express a state as $\sum_i \psi_i|i\rangle$ with i being a number expressed in binary, we may express the SLOCC classes with ψ_i as the variables.

The equations for the ideal defining the closure of the SLOCC class of $|0000\rangle + |1111\rangle$:

$$\begin{aligned} & \psi_{0111} * \psi_{1010} * \psi_{1101} - \psi_{0110} * \psi_{1011} * \psi_{1101} - \psi_{0111} * \psi_{1001} * \psi_{1110} \\ + \quad & \psi_{0101} * \psi_{1011} * \psi_{1110} + \psi_{0110} * \psi_{1001} * \psi_{1111} - \psi_{0101} * \psi_{1010} * \psi_{1111} \end{aligned}$$

$$\begin{aligned} & \psi_{0011} * \psi_{1010} * \psi_{1101} - \psi_{0010} * \psi_{1011} * \psi_{1101} - \psi_{0011} * \psi_{1001} * \psi_{1110} \\ + \quad & \psi_{0001} * \psi_{1011} * \psi_{1110} + \psi_{0010} * \psi_{1001} * \psi_{1111} - \psi_{0001} * \psi_{1010} * \psi_{1111} \end{aligned}$$

$$\begin{aligned} & \psi_{0011} * \psi_{0110} * \psi_{1101} - \psi_{0010} * \psi_{0111} * \psi_{1101} - \psi_{0011} * \psi_{0101} * \psi_{1110} \\ + \quad & \psi_{0001} * \psi_{0111} * \psi_{1110} + \psi_{0010} * \psi_{0101} * \psi_{1111} - \psi_{0001} * \psi_{0110} * \psi_{1111} \end{aligned}$$

$$\begin{aligned} & \psi_{0111} * \psi_{1011} * \psi_{1100} - \psi_{0110} * \psi_{1011} * \psi_{1101} - \psi_{0111} * \psi_{1001} * \psi_{1110} \\ + \quad & \psi_{0011} * \psi_{1101} * \psi_{1110} + \psi_{0110} * \psi_{1001} * \psi_{1111} - \psi_{0011} * \psi_{1100} * \psi_{1111} \end{aligned}$$

$$\begin{aligned} & \psi_{0110} * \psi_{1011} * \psi_{1100} - \psi_{0110} * \psi_{1010} * \psi_{1101} - \psi_{0100} * \psi_{1011} * \psi_{1110} \\ + \quad & \psi_{0010} * \psi_{1101} * \psi_{1110} + \psi_{0100} * \psi_{1010} * \psi_{1111} - \psi_{0010} * \psi_{1100} * \psi_{1111} \end{aligned}$$

$$\begin{aligned} & \psi_{0101} * \psi_{1011} * \psi_{1100} - \psi_{0100} * \psi_{1011} * \psi_{1101} - \psi_{0101} * \psi_{1001} * \psi_{1110} \\ + \quad & \psi_{0001} * \psi_{1101} * \psi_{1110} + \psi_{0100} * \psi_{1001} * \psi_{1111} - \psi_{0001} * \psi_{1100} * \psi_{1111} \end{aligned}$$

$$
\begin{aligned}
& \psi_{0111} * \psi_{1010} * \psi_{1100} - \psi_{0110} * \psi_{1010} * \psi_{1101} - \psi_{0111} * \psi_{1000} * \psi_{1110} \\
+ \quad & \psi_{0010} * \psi_{1101} * \psi_{1110} + \psi_{0110} * \psi_{1000} * \psi_{1111} - \psi_{0010} * \psi_{1100} * \psi_{1111}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0101} * \psi_{1010} * \psi_{1100} - \psi_{0100} * \psi_{1010} * \psi_{1101} - \psi_{0101} * \psi_{1000} * \psi_{1110} \\
+ \quad & \psi_{0000} * \psi_{1101} * \psi_{1110} + \psi_{0100} * \psi_{1000} * \psi_{1111} - \psi_{0000} * \psi_{1100} * \psi_{1111}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0011} * \psi_{1010} * \psi_{1100} - \psi_{0010} * \psi_{1011} * \psi_{1100} - \psi_{0011} * \psi_{1000} * \psi_{1110} \\
+ \quad & \psi_{0000} * \psi_{1011} * \psi_{1110} + \psi_{0010} * \psi_{1000} * \psi_{1111} - \psi_{0000} * \psi_{1010} * \psi_{1111}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0111} * \psi_{1001} * \psi_{1100} - \psi_{0111} * \psi_{1000} * \psi_{1101} - \psi_{0101} * \psi_{1001} * \psi_{1110} \\
+ \quad & \psi_{0001} * \psi_{1101} * \psi_{1110} + \psi_{0101} * \psi_{1000} * \psi_{1111} - \psi_{0001} * \psi_{1100} * \psi_{1111}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0110} * \psi_{1001} * \psi_{1100} - \psi_{0110} * \psi_{1000} * \psi_{1101} - \psi_{0100} * \psi_{1001} * \psi_{1110} \\
+ \quad & \psi_{0000} * \psi_{1101} * \psi_{1110} + \psi_{0100} * \psi_{1000} * \psi_{1111} - \psi_{0000} * \psi_{1100} * \psi_{1111}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0011} * \psi_{1001} * \psi_{1100} - \psi_{0001} * \psi_{1011} * \psi_{1100} - \psi_{0011} * \psi_{1000} * \psi_{1101} \\
+ \quad & \psi_{0000} * \psi_{1011} * \psi_{1101} + \psi_{0001} * \psi_{1000} * \psi_{1111} - \psi_{0000} * \psi_{1001} * \psi_{1111}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0010} * \psi_{1001} * \psi_{1100} - \psi_{0001} * \psi_{1010} * \psi_{1100} - \psi_{0010} * \psi_{1000} * \psi_{1101} \\
+ \quad & \psi_{0000} * \psi_{1010} * \psi_{1101} + \psi_{0001} * \psi_{1000} * \psi_{1110} - \psi_{0000} * \psi_{1001} * \psi_{1110}
\end{aligned}
$$

$$\psi_{0011} * \psi_{0110} * \psi_{1100} - \psi_{0010} * \psi_{0111} * \psi_{1100} - \psi_{0011} * \psi_{0100} * \psi_{1110}$$
$$+ \quad \psi_{0000} * \psi_{0111} * \psi_{1110} + \psi_{0010} * \psi_{0100} * \psi_{1111} - \psi_{0000} * \psi_{0110} * \psi_{1111}$$

$$\psi_{0011} * \psi_{0101} * \psi_{1100} - \psi_{0001} * \psi_{0111} * \psi_{1100} - \psi_{0011} * \psi_{0100} * \psi_{1101}$$
$$+ \quad \psi_{0000} * \psi_{0111} * \psi_{1101} + \psi_{0001} * \psi_{0100} * \psi_{1111} - \psi_{0000} * \psi_{0101} * \psi_{1111}$$

$$\psi_{0010} * \psi_{0101} * \psi_{1100} - \psi_{0001} * \psi_{0110} * \psi_{1100} - \psi_{0010} * \psi_{0100} * \psi_{1101}$$
$$+ \quad \psi_{0000} * \psi_{0110} * \psi_{1101} + \psi_{0001} * \psi_{0100} * \psi_{1110} - \psi_{0000} * \psi_{0101} * \psi_{1110}$$

$$\psi_{0101} * \psi_{0110} * \psi_{1011} - \psi_{0100} * \psi_{0111} * \psi_{1011} - \psi_{0011} * \psi_{0101} * \psi_{1110}$$
$$+ \quad \psi_{0001} * \psi_{0111} * \psi_{1110} + \psi_{0011} * \psi_{0100} * \psi_{1111} - \psi_{0001} * \psi_{0110} * \psi_{1111}$$

$$\psi_{0111} * \psi_{1001} * \psi_{1010} - \psi_{0111} * \psi_{1000} * \psi_{1011} - \psi_{0011} * \psi_{1001} * \psi_{1110}$$
$$+ \quad \psi_{0001} * \psi_{1011} * \psi_{1110} + \psi_{0011} * \psi_{1000} * \psi_{1111} - \psi_{0001} * \psi_{1010} * \psi_{1111}$$

$$\psi_{0110} * \psi_{1001} * \psi_{1010} - \psi_{0110} * \psi_{1000} * \psi_{1011} - \psi_{0010} * \psi_{1001} * \psi_{1110}$$
$$+ \quad \psi_{0000} * \psi_{1011} * \psi_{1110} + \psi_{0010} * \psi_{1000} * \psi_{1111} - \psi_{0000} * \psi_{1010} * \psi_{1111}$$

$$\psi_{0101} * \psi_{1001} * \psi_{1010} - \psi_{0101} * \psi_{1000} * \psi_{1011} - \psi_{0001} * \psi_{1010} * \psi_{1101}$$
$$+ \quad \psi_{0000} * \psi_{1011} * \psi_{1101} + \psi_{0001} * \psi_{1000} * \psi_{1111} - \psi_{0000} * \psi_{1001} * \psi_{1111}$$

$$
\begin{aligned}
&\psi_{0100} * \psi_{1001} * \psi_{1010} - \psi_{0100} * \psi_{1000} * \psi_{1011} - \psi_{0001} * \psi_{1010} * \psi_{1100} \\
+\quad &\psi_{0000} * \psi_{1011} * \psi_{1100} + \psi_{0001} * \psi_{1000} * \psi_{1110} - \psi_{0000} * \psi_{1001} * \psi_{1110}
\end{aligned}
$$

$$
\begin{aligned}
&\psi_{0101} * \psi_{0110} * \psi_{1010} - \psi_{0100} * \psi_{0111} * \psi_{1010} - \psi_{0010} * \psi_{0101} * \psi_{1110} \\
+\quad &\psi_{0000} * \psi_{0111} * \psi_{1110} + \psi_{0010} * \psi_{0100} * \psi_{1111} - \psi_{0000} * \psi_{0110} * \psi_{1111}
\end{aligned}
$$

$$
\begin{aligned}
&\psi_{0011} * \psi_{0101} * \psi_{1010} - \psi_{0001} * \psi_{0111} * \psi_{1010} - \psi_{0010} * \psi_{0101} * \psi_{1011} \\
+\quad &\psi_{0000} * \psi_{0111} * \psi_{1011} + \psi_{0001} * \psi_{0010} * \psi_{1111} - \psi_{0000} * \psi_{0011} * \psi_{1111}
\end{aligned}
$$

$$
\begin{aligned}
&\psi_{0011} * \psi_{0100} * \psi_{1010} - \psi_{0001} * \psi_{0110} * \psi_{1010} - \psi_{0010} * \psi_{0100} * \psi_{1011} \\
+\quad &\psi_{0000} * \psi_{0110} * \psi_{1011} + \psi_{0001} * \psi_{0010} * \psi_{1110} - \psi_{0000} * \psi_{0011} * \psi_{1110}
\end{aligned}
$$

$$
\begin{aligned}
&\psi_{0101} * \psi_{0110} * \psi_{1001} - \psi_{0100} * \psi_{0111} * \psi_{1001} - \psi_{0001} * \psi_{0110} * \psi_{1101} \\
+\quad &\psi_{0000} * \psi_{0111} * \psi_{1101} + \psi_{0001} * \psi_{0100} * \psi_{1111} - \psi_{0000} * \psi_{0101} * \psi_{1111}
\end{aligned}
$$

$$
\begin{aligned}
&\psi_{0011} * \psi_{0110} * \psi_{1001} - \psi_{0010} * \psi_{0111} * \psi_{1001} - \psi_{0001} * \psi_{0110} * \psi_{1011} \\
+\quad &\psi_{0000} * \psi_{0111} * \psi_{1011} + \psi_{0001} * \psi_{0010} * \psi_{1111} - \psi_{0000} * \psi_{0011} * \psi_{1111}
\end{aligned}
$$

$$
\begin{aligned}
&\psi_{0011} * \psi_{0100} * \psi_{1001} - \psi_{0010} * \psi_{0101} * \psi_{1001} - \psi_{0001} * \psi_{0100} * \psi_{1011} \\
+\quad &\psi_{0000} * \psi_{0101} * \psi_{1011} + \psi_{0001} * \psi_{0010} * \psi_{1101} - \psi_{0000} * \psi_{0011} * \psi_{1101}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0101} * \psi_{0110} * \psi_{1000} - \psi_{0100} * \psi_{0111} * \psi_{1000} - \psi_{0001} * \psi_{0110} * \psi_{1100} \\
+ \quad & \psi_{0000} * \psi_{0111} * \psi_{1100} + \psi_{0001} * \psi_{0100} * \psi_{1110} - \psi_{0000} * \psi_{0101} * \psi_{1110}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0011} * \psi_{0110} * \psi_{1000} - \psi_{0010} * \psi_{0111} * \psi_{1000} - \psi_{0001} * \psi_{0110} * \psi_{1010} \\
+ \quad & \psi_{0000} * \psi_{0111} * \psi_{1010} + \psi_{0001} * \psi_{0010} * \psi_{1110} - \psi_{0000} * \psi_{0011} * \psi_{1110}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0011} * \psi_{0101} * \psi_{1000} - \psi_{0001} * \psi_{0111} * \psi_{1000} - \psi_{0010} * \psi_{0101} * \psi_{1001} \\
+ \quad & \psi_{0000} * \psi_{0111} * \psi_{1001} + \psi_{0001} * \psi_{0010} * \psi_{1101} - \psi_{0000} * \psi_{0011} * \psi_{1101}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0010} * \psi_{0101} * \psi_{1000} - \psi_{0001} * \psi_{0110} * \psi_{1000} - \psi_{0010} * \psi_{0100} * \psi_{1001} \\
+ \quad & \psi_{0000} * \psi_{0110} * \psi_{1001} + \psi_{0001} * \psi_{0100} * \psi_{1010} - \psi_{0000} * \psi_{0101} * \psi_{1010}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0011} * \psi_{0100} * \psi_{1000} - \psi_{0001} * \psi_{0110} * \psi_{1000} - \psi_{0010} * \psi_{0100} * \psi_{1001} \\
+ \quad & \psi_{0000} * \psi_{0110} * \psi_{1001} + \psi_{0001} * \psi_{0010} * \psi_{1100} - \psi_{0000} * \psi_{0011} * \psi_{1100}
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0111} * \psi_{1000} * \psi_{1011} * \psi_{1101} - \psi_{0110} * \psi_{1001} * \psi_{1011} * \psi_{1101} \\
- \quad & \psi_{0111} * \psi_{1001}^2 * \psi_{1110} + \psi_{0101} * \psi_{1001} * \psi_{1011} * \psi_{1110} \\
+ \quad & \psi_{0011} * \psi_{1001} * \psi_{1101} * \psi_{1110} - \psi_{0001} * \psi_{1011} * \psi_{1101} * \psi_{1110} \\
+ \quad & \psi_{0110} * \psi_{1001}^2 * \psi_{1111} - \psi_{0101} * \psi_{1000} * \psi_{1011} * \psi_{1111} \\
- \quad & \psi_{0011} * \psi_{1000} * \psi_{1101} * \psi_{1111} + \psi_{0000} * \psi_{1011} * \psi_{1101} * \psi_{1111} \\
+ \quad & \psi_{0001} * \psi_{1000} * \psi_{1111}^2 - \psi_{0000} * \psi_{1001} * \psi_{1111}^2
\end{aligned}
$$

$$\begin{aligned}
&\psi_{0001} * \psi_{0110} * \psi_{1011} * \psi_{1101} - \psi_{0000} * \psi_{0111} * \psi_{1011} * \psi_{1101} \\
- \quad &\psi_{0011} * \psi_{0101} * \psi_{1001} * \psi_{1110} + \psi_{0001} * \psi_{0111} * \psi_{1001} * \psi_{1110} \\
+ \quad &\psi_{0010} * \psi_{0101} * \psi_{1001} * \psi_{1111} - \psi_{0001} * \psi_{0110} * \psi_{1001} * \psi_{1111} \\
- \quad &\psi_{0001} * \psi_{0010} * \psi_{1101} * \psi_{1111} + \psi_{0000} * \psi_{0011} * \psi_{1101} * \psi_{1111}
\end{aligned}$$

$$\begin{aligned}
&\psi_{0001} * \psi_{0110} * \psi_{1010} * \psi_{1101} - \psi_{0000} * \psi_{0110} * \psi_{1011} * \psi_{1101} \\
- \quad &\psi_{0010} * \psi_{0101} * \psi_{1001} * \psi_{1110} + \psi_{0000} * \psi_{0101} * \psi_{1011} * \psi_{1110} \\
+ \quad &\psi_{0010} * \psi_{0100} * \psi_{1001} * \psi_{1111} - \psi_{0001} * \psi_{0100} * \psi_{1010} * \psi_{1111}
\end{aligned}$$

$$\begin{aligned}
&\psi_{0001} * \psi_{0110} * \psi_{1010} * \psi_{1100} - \psi_{0000} * \psi_{0110} * \psi_{1010} * \psi_{1101} \\
- \quad &\psi_{0001} * \psi_{0110} * \psi_{1000} * \psi_{1110} - \psi_{0010} * \psi_{0100} * \psi_{1001} * \psi_{1110} \\
+ \quad &\psi_{0000} * \psi_{0110} * \psi_{1001} * \psi_{1110} + \psi_{0000} * \psi_{0010} * \psi_{1101} * \psi_{1110} \\
+ \quad &\psi_{0010} * \psi_{0100} * \psi_{1000} * \psi_{1111} - \psi_{0000} * \psi_{0010} * \psi_{1100} * \psi_{1111}
\end{aligned}$$

$$\begin{aligned}
&\psi_{0001} * \psi_{0110}^2 * \psi_{1000} - \psi_{0010} * \psi_{0100} * \psi_{0111} * \psi_{1000} \\
+ \quad &\psi_{0010} * \psi_{0100} * \psi_{0110} * \psi_{1001} - \psi_{0000} * \psi_{0110}^2 * \psi_{1001} \\
- \quad &\psi_{0001} * \psi_{0100} * \psi_{0110} * \psi_{1010} + \psi_{0000} * \psi_{0100} * \psi_{0111} * \psi_{1010} \\
- \quad &\psi_{0001} * \psi_{0010} * \psi_{0110} * \psi_{1100} + \psi_{0000} * \psi_{0010} * \psi_{0111} * \psi_{1100} \\
+ \quad &\psi_{0001} * \psi_{0010} * \psi_{0100} * \psi_{1110} - \psi_{0000}^2 * \psi_{0111} * \psi_{1110} \\
- \quad &\psi_{0000} * \psi_{0010} * \psi_{0100} * \psi_{1111} + \psi_{0000}^2 * \psi_{0110} * \psi_{1111}
\end{aligned}$$

$$
\begin{aligned}
& \psi_{0011} * \psi_{0100} * \psi_{0111} * \psi_{1011} * \psi_{1101} - \psi_{0010} * \psi_{0101} * \psi_{0111} * \psi_{1011} * \psi_{1101} \\
- & \psi_{0011} * \psi_{0101}^2 * \psi_{1011} * \psi_{1110} + \psi_{0001} * \psi_{0101} * \psi_{0111} * \psi_{1011} * \psi_{1110} \\
+ & \psi_{0011}^2 * \psi_{0101} * \psi_{1101} * \psi_{1110} - \psi_{0001} * \psi_{0011} * \psi_{0111} * \psi_{1101} * \psi_{1110} \\
+ & \psi_{0010} * \psi_{0101}^2 * \psi_{1011} * \psi_{1111} - \psi_{0001} * \psi_{0100} * \psi_{0111} * \psi_{1011} * \psi_{1111} \\
- & \psi_{0011}^2 * \psi_{0100} * \psi_{1101} * \psi_{1111} + \psi_{0001} * \psi_{0010} * \psi_{0111} * \psi_{1101} * \psi_{1111} \\
+ & \psi_{0001} * \psi_{0011} * \psi_{0100} * \psi_{1111}^2 - \psi_{0001} * \psi_{0010} * \psi_{0101} * \psi_{1111}^2
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0001} * \psi_{0100} * \psi_{0111} * \psi_{1011} * \psi_{1101} - \psi_{0000} * \psi_{0101} * \psi_{0111} * \psi_{1011} * \psi_{1101} \\
- & \psi_{0011} * \psi_{0101}^2 * \psi_{1001} * \psi_{1110} + \psi_{0001} * \psi_{0101} * \psi_{0111} * \psi_{1001} * \psi_{1110} \\
+ & \psi_{0001} * \psi_{0011} * \psi_{0101} * \psi_{1101} * \psi_{1110} - \psi_{0001}^2 * \psi_{0111} * \psi_{1101} * \psi_{1110} \\
+ & \psi_{0010} * \psi_{0101}^2 * \psi_{1001} * \psi_{1111} - \psi_{0001} * \psi_{0100} * \psi_{0111} * \psi_{1001} * \psi_{1111} \\
- & \psi_{0001} * \psi_{0011} * \psi_{0100} * \psi_{1101} * \psi_{1111} - \psi_{0001} * \psi_{0010} * \psi_{0101} * \psi_{1101} * \psi_{1111} \\
+ & \psi_{0000} * \psi_{0011} * \psi_{0101} * \psi_{1101} * \psi_{1111} + \psi_{0000} * \psi_{0001} * \psi_{0111} * \psi_{1101} * \psi_{1111} \\
+ & \psi_{0001}^2 * \psi_{0100} * \psi_{1111}^2 - \psi_{0000} * \psi_{0001} * \psi_{0101} * \psi_{1111}^2
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0001} * \psi_{0010} * \psi_{0111} * \psi_{1011} * \psi_{1101} - \psi_{0000} * \psi_{0011} * \psi_{0111} * \psi_{1011} * \psi_{1101} \\
- & \psi_{0011}^2 * \psi_{0101} * \psi_{1001} * \psi_{1110} + \psi_{0001} * \psi_{0011} * \psi_{0111} * \psi_{1001} * \psi_{1110} \\
+ & \psi_{0001} * \psi_{0011} * \psi_{0101} * \psi_{1011} * \psi_{1110} - \psi_{0001}^2 * \psi_{0111} * \psi_{1011} * \psi_{1110} \\
+ & \psi_{0010} * \psi_{0011} * \psi_{0101} * \psi_{1001} * \psi_{1111} - \psi_{0001} * \psi_{0010} * \psi_{0111} * \psi_{1001} * \psi_{1111} \\
- & \psi_{0001} * \psi_{0010} * \psi_{0101} * \psi_{1011} * \psi_{1111} + \psi_{0000} * \psi_{0001} * \psi_{0111} * \psi_{1011} * \psi_{1111} \\
- & \psi_{0001} * \psi_{0010} * \psi_{0011} * \psi_{1101} * \psi_{1111} + \psi_{0000} * \psi_{0011}^2 * \psi_{1101} * \psi_{1111} \\
+ & \psi_{0001}^2 * \psi_{0010} * \psi_{1111}^2 - \psi_{0000} * \psi_{0001} * \psi_{0011} * \psi_{1111}^2
\end{aligned}
$$

$$
\begin{aligned}
& \psi_{0001} * \psi_{0100} * \psi_{1010}^2 * \psi_{1100} - \psi_{0010} * \psi_{0100} * \psi_{1000} * \psi_{1011} * \psi_{1100} \\
- \; & \psi_{0001} * \psi_{0010} * \psi_{1010} * \psi_{1100}^2 + \psi_{0000} * \psi_{0010} * \psi_{1011} * \psi_{1100}^2 \\
+ \; & \psi_{0010} * \psi_{0100} * \psi_{1000} * \psi_{1010} * \psi_{1101} - \psi_{0000} * \psi_{0100} * \psi_{1010}^2 * \psi_{1101} \\
- \; & \psi_{0001} * \psi_{0100} * \psi_{1000} * \psi_{1010} * \psi_{1110} + \psi_{0000} * \psi_{0100} * \psi_{1000} * \psi_{1011} * \psi_{1110} \\
+ \; & \psi_{0001} * \psi_{0010} * \psi_{1000} * \psi_{1100} * \psi_{1110} - \psi_{0000}^2 * \psi_{1011} * \psi_{1100} * \psi_{1110} \\
- \; & \psi_{0000} * \psi_{0010} * \psi_{1000} * \psi_{1101} * \psi_{1110} + \psi_{0000}^2 * \psi_{1010} * \psi_{1101} * \psi_{1110}
\end{aligned}
$$

Bibliography

[1] M. Artin. Versal deformations and algebraic stacks. *Inventiones Mathematicae*, **27**:165–189, 1974. 10.1007/BF01390174.

[2] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*. Springer Verlag, 2003.

[3] John S. Bell. On the Einstein-Podolsky-Rosen Paradox. *Physics*, **1**:195–200, 1964.

[4] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, **70**:1895–1899, Mar 1993.

[5] Charles H. Bennett, Sandu Popescu, Daniel Rohrlich, John A. Smolin, and Ashish V. Thapliyal. Exact and asymptotic measures of multipartite pure state entanglement, 1999.

[6] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, **69**:2881–2884, Nov 1992.

[7] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real Algebraic Geometry*. Springer Verlag, 1998.

[8] Dik Bouwmeester, Jian-Wei Pan, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement. *Physical Review Letters*, **82**(7):1345+, February 1999.

[9] Emmanuel Briand, Jean-Gabriel Luque, and Jean-Yves Thibon. A complete set of covariants of the four qubit system, 2003.

[10] Bob Coecke. Kindergarten Quantum Mechanics. October 2005.

[11] Bob Coecke. Quantum Picturalism. *Contemporary Physics*, **51**:59–83, 2010.

[12] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. Singular 3-1-3 — A computer algebra system for polynomial computations. 2011. http://www.singular.uni-kl.de.

[13] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *PHYS.REV.A*, **62**:062314, 2000.

[14] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review*, **47**:777–780, 1935.

[15] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer Verlag, 1994.

[16] David Eisenbud and Joe Harris. *The Geometry of Schemes*. Springer Verlag, 2000.

[17] William Fulton and Joe Harris. *Representation Theory: A First Course*. Springer Verlag, 2004.

[18] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Going Beyond Bell's Theorem, December 2007.

[19] Robin Hartshorne. *Algebraic Geometry*. Springer Verlag, 1977.

[20] Hoshang Heydari. General pure multipartite entangled states and the segre variety. *J. Phys. A: Math. Gen. 39*, pages 9839–9845, 2006.

[21] Daniel Kroening and Ofer Strichman. *Decision Procedures: An Algorithmic Point of View*, page 10. Springer Verlag, 2008.

[22] Saunders Mac Lane. *Categories for the Working Mathematician, Second Edition*, page 75. Springer Verlag, 1997.

[23] Gérard Laumon and Laurent Moret-Bailly. *Champs algébriques*. Springer Verlag, 2000.

[24] Jean-Gabriel Luque and Jean-Yves Thibon. Algebraic invariants of five qubits. *Journal of Physics A: Mathematical and General*, **39**:361, 2006.

[25] Akimasa Miyake. Classification of multipartite entangled states by multidimensional determinants. *Phys. Rev. A*, **67**(1):012108, Jan 2003.

[26] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric Invariant Theory, Third Enlarged Edition.* Springer Verlag, 1994.

[27] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[28] Jean-Pierre Serre. *Linear Representations of Finite Groups.* Springer Verlag, 1977.

[29] W. A. Stein et al. *Sage Mathematics Software (Version 4.7).* The Sage Development Team, 2011. `http://www.sagemath.org`.

[30] 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.