The log of a quantum state and qubit local unitary invariants.

Graeme Mitchison[1, *]

[1] *Centre for Quantum Information and Foundations, DAMTP,*
University of Cambridge, Cambridge CB3 0WA, UK

Local unitary invariants of multipartite states fall into families related by the tracing-out of subsystems. In the case of pure qubit systems, there is a family that accounts for about half the total number of invariants and is closely connected to multipartite separability. One way to define this family is to give pure states the structure of an algebra, and define a log function in this algebra. The coefficients of the Taylor expansion of this log function, which are polynomials in the coefficients of the states, are cumulants. When twirled by local unitaries, these yield invariants. The traditional cumulant, which is a function of random variables, vanishes if its arguments belong to two or more independent sets. The equivalent of this in our context is that certain cumulant-invariants vanish when a state is separable.

I. INTRODUCTION

Given a multipartite quantum state, the action of local unitaries maps out an orbit of locally equivalent states. We can think of such orbits as forming an *entanglement space*, $\mathcal{E}$. The orbits can in principle be characterised by a complete set of invariants of this group action, and the problem of finding complete, algebraically independent sets of invariants has been much studied [8, 15–17, 20, 23]. The picture that emerges is not altogether encouraging because the number of invariants grows exponentially with the number of systems. However, there is a redeeming feature: an invariant in n systems gives rise to a set of invariants in $n+1$ systems via a tracing-out operation. This means that any invariant generates a family that grows exponentially with the number of systems, and one can therefore hope to grasp the structure of the space through these families.

I illustrate this by defining a family of invariants for pure qubit states that grows exponentially with n and asymptotically accounts for half the total number of invariants. The key to the construction of this family is the set of joint cumulants [6, 7, 11, 21, 25, 26]. Cumulants are most commonly encountered as statistical tools, or as ingredients in cluster expansions. For our purposes, they are simply polynomials in the coefficients of states that have certain desirable properties; for instance, they are closely related to the separability of multiparty states. Cumulants can be introduced in an attractive if unorthodox way by giving the space of vectors in $(\mathbb{C}^d)^{\otimes n}$ the structure of an algebra in which a Taylor series and hence analytic functions can be defined. In particular, one can define a log function with the property that

$$\log(|\psi\rangle \otimes |\phi\rangle) = \log(|\psi\rangle) + \log(|\phi\rangle),$$

for all $|\psi\rangle$ and $|\phi\rangle$; see (9) and (10) for a more precise statement. The coefficients in the log-expansion are cumulants, which is how the connection between cumulants and separability comes about.

This algebra is a rather unnatural construction, since it depends on a particular choice of basis. However, twirling with respect to local unitaries allows one to remove this artificiality and to generate a set of invariants. It turns out that these cumulant-based invariants are already known in the literature, though their relationship to cumulants is apparently not recognised. They account for five of the six independent 3-qubit invariants and eleven of the nineteen 4-qubit invariants given in [17]. Asymptotically, there are $O(2^n)$ of them whereas the total number of invariants in an n-party states is $O(2^{n+1})$. There are also other families of invariants, including a family of 4th degree polynomials that accounts for about a quarter of all invariants. Breaking down the invariants into (overlapping) hierarchical families gives a perspective on their structure and, potentially, on the entanglement of states.

There is alternative way of deriving invariants from cumulants (see Section VIII A), due to Zhou et al [27]. Despite certain formal similarities, these seem not to have a simple functional relationship to our invariants. The entanglement space $\mathcal{E}$ can be explored in other ways. Kraus [13, 14] showed how to reduce multipartite qubit states to a standard form that is invariant under local unitaries. An alternative, geometric procedure that applies to local spaces of arbitrary dimension (not just qubits) has also been proposed [22]. These methods enable one to determine if two states belong to the same orbit; invariants give a parametrisation of orbits and can be regarded as entanglement measures. All these methods give complementary insights into the structure of $\mathcal{E}$.

[*] gjm12@cam.ac.uk

II. THE ALGEBRA OF MULTI-PARTITE STATES

Let $\mathcal{A}_n^{(d)}$ be the the commutative algebra over $\mathbb{C}$ with generators e_i, $i = 1, \dots, n$ satisfying $e_i^d = 0$. An element ψ of $\mathcal{A}_n^{(d)}$ has the form

$$\psi = \sum a_{i_1 \dots i_n} e^{i_1} \dots e^{i_n},$$

where $0 \le i_k \le d-1$ and the a's are complex coefficients. Then $\psi = a + r$, where $a = a_{0\dots0}$, and r consists of at most $d^n - 1$ terms and satisfies $r^{n(d-1)+1} = 0$. Any analytic function $f : \mathcal{A}_n^{(d)} \to \mathcal{A}_n^{(d)}$ can be expanded in a Taylor series in r:

$$f(\psi) = f(a) + f'(a)r + f''(a)r^2/2! + ... \tag{1}$$

This series is finite, because of the nilpotency of r, and is thus well defined. For instance, in $\mathcal{A}_n^{(2)}$ any ψ can be written

$$\psi = a_{00} + a_{10}e_1 + a_{01}e_2 + a_{11}e_1e_2 \tag{2}$$

and if $a_{00} \neq 0$

$$\begin{aligned}\log\psi &= \log(a_{00} + r) = \log a_{00} + \log(1 + r/a_{00}) = \log a_{00} + r/a_{00} - r^2/(2a_{00}^2),\\ &= \log a_{00} + (a_{10}/a_{00})e_1 + (a_{01}/a_{00})e_2 + (a_{11}/a_{00} - a_{10}a_{01}/a_{00}^2)e_1e_2.\end{aligned} \tag{3}$$

Similarly, there is a finite polynomial for the algebra inverse; e.g.

$$\psi^{-1} = a_{00}^{-1} - (a_{10}/a_{00}^2)e_1 - (a_{01}/a_{00}^2)e_2 - (a_{11}/a_{00}^2 - 2a_{10}a_{01}/a_{00}^3)e_1e_2; \tag{4}$$

and for other functions, such as exp. These functions have all the expected properties, e.g.

$$\psi\psi^{-1} = 1, \tag{5}$$

$$\log(\psi\phi) = \log(\psi) + \log(\phi), \tag{6}$$

$$\exp(\psi + \phi) = \exp(\psi)\exp(\phi), \tag{7}$$

$$\exp(\log)(\psi) = \psi. \tag{8}$$

Now identify $e_1^{i_1} \dots e_n^{i_n}$ with the n-qudit basis element $|i_1 \dots i_n\rangle$. This sets up an isomorphism between elements ψ of $\mathcal{A}_n^{(d)}$ and unnormalised n-qudit states $|\psi\rangle$. For instance, $\psi = a_{00} + a_{10}e_1 + a_{01}e_2 + a_{11}e_1e_2$ in $\mathcal{A}_n^{(2)}$ can be identified with the two qubit state $|\psi\rangle = a_{00}|00\rangle + a_{10}|10\rangle + a_{01}|01\rangle + a_{11}|11\rangle$. One can then carry across the structure of the algebra. For instance, if $|\phi\rangle = b_{00}|00\rangle + b_{10}|10\rangle + b_{01}|01\rangle + b_{11}|11\rangle$ we have the product

$$\begin{aligned}|\psi\rangle|\phi\rangle = a_{00}b_{00}|00\rangle &+ (a_{00}b_{10} + a_{10}b_{00})|10\rangle + (a_{00}b_{01} + a_{01}b_{00})|01\rangle\\ &+ (a_{00}b_{11} + a_{10}b_{01} + a_{01}b_{10} + a_{11}b_{00})|11\rangle.\end{aligned}$$

The identity element in $\mathcal{A}_n^{(d)}$, is $|\underbrace{0\dots0}_{n}\rangle$, and the inverse, log and exponential are carried over in the obvious way from the corresponding functions in $\mathcal{A}_n^{(d)}$.

Suppose the n subsystems are divided into two sets S and T. We write

$$|\psi\rangle = |\psi\rangle_S \otimes |\psi\rangle_T, \tag{9}$$

to indicate that $|\psi\rangle$ is separable with respect to these subsets, the order in which S and T appear in the tensor product not being necessarily related to the order of their indices (e.g. we might write $|\psi\rangle = |\psi\rangle_{13} \otimes |\psi\rangle_2$). Then $|\psi\rangle$ can also be written in terms of the algebra product as $|\psi\rangle = |\psi\rangle_S|\psi\rangle_T$, where $|\psi\rangle_S$ is identified with an element of the algebra that only uses those e_i with $i \in S$, and $|\psi\rangle_T$ using only those e_i with $i \in T$. From (6) we have

$$\log|\psi\rangle = \log|\psi\rangle_S + \log|\psi\rangle_T. \tag{10}$$

thus linearising the tensor product when the log is defined, i.e. when the constant coefficients in the algebra do not vanish.

The coefficients $c_{i_1\ldots i_n}$ of $\log|\phi\rangle = \sum c_{i_1\ldots i_n}|i_1\ldots i_n\rangle$ are called *cumulants*. The cumulant corresponding to $c_{i_1\ldots i_n}$ is defined for classical random variables X_i as the coefficient of $\lambda_1^{i_1}..\lambda_n^{i_n}$ in $\log\langle e^{\sum_i \lambda_i X_i}\rangle$ [21]. This follows by identifying $\langle X_1^{i_1}\ldots X_n^{i_n}\rangle$ with $a_{i_1\ldots i_n}$ and taking $a_{0\ldots 0}=1$. For instance, the equivalent of

$$c_{11} = (a_{11}a_{00} - a_{10}a_{01})/a_{00}^2, \tag{11}$$

which is the coefficient of e_1e_2 in (3), is the classical second degree cumulant $\langle X_1X_2\rangle - \langle X_1\rangle\langle X_2\rangle$. The algebra $\mathcal{A}_n^{(2)}$ can also be identified with the "moment algebra" in [1] by associating to the term $ce_{i_1}\ldots e_{i_n}$ in $\mathcal{A}_n^{(2)}$ the map that assigns to the integers $\{i_1,\ldots i_n\}$ the value c.

III. MULTIPARTITE SEPARABILITY

Write the state space for an n-party state as $(\mathbb{C}^d)_1\otimes\ldots\otimes(\mathbb{C}^d)_n$. If $\pi=\{\pi_1,\pi_2,\ldots,\pi_k\}$ is a partition of n, we say $|\phi\rangle$ is π-separable if we can write

$$|\phi\rangle = \bigotimes_{i=1}^{k} |\phi\rangle_{\pi_i}, \tag{12}$$

where each $|\phi\rangle_{\pi_i}$ is a state in the subspace $\bigotimes_{j\in\pi_i}(\mathbb{C}^d)_j$. As we have seen, we can also write this using the algebra product as

$$|\phi\rangle = |\phi\rangle_{\pi_1}\ldots|\phi\rangle_{\pi_k}. \tag{13}$$

From (6) we get

$$\log|\phi\rangle = \log|\phi\rangle_{\pi_1} + \ldots + \log|\phi\rangle_{\pi_k}. \tag{14}$$

This immediately gives a characterisation of multipartite separability. Let us say that a set of indices $i_1\ldots i_n$ *splits* the partition π if there are non-zero indices i_j in more than one subset of π.

Theorem III.1. *An n-party state $|\phi\rangle$ with $a_{0\ldots 0}\neq 0$ is π-separable if and only if $c_{i_1\ldots i_n}=0$ whenever $i_1\ldots i_n$ splits π.*

Proof. Necessity follows from the fact that the cumulants with indices splitting π are absent from the expansion (14) of $\log|\phi\rangle$. Sufficiency follows by noting that, if these cumulants are zero, we can write $\log|\phi\rangle$ in the form

$$\log|\phi\rangle = \sum_k \sum_{\{i_j=1\implies j\in\pi_k\}} c_{i_1i_2\ldots i_n}|i_1i_2\ldots i_n\rangle$$

and exponentiating this shows $|\phi\rangle$ to be π-separable. □

The condition $a_{0\ldots 0}\neq 0$ reflects the special role played by $|0\ldots 0\rangle$ as the identity in the algebra. We shall shortly give a version of this theorem (IV.2) which does not have this unpleasant restriction.

It should be emphasised that one can easily write down algebraic conditions for a pure state to be π-separable. However, the characterisation of Theorem III.1 will turn out to provide a useful starting point for making qubit invariants. It is also economical, in the sense that the vanishing of the c's gives the right number of equations to define the subspace of π-separable normalised states. Indeed, the (real parameter) dimension of this subspace is

$$d_\pi = \sum\left(2d^{|\pi_i|}-2\right),$$

the expression in brackets counting the real and imaginary parts of each coefficient of $|\psi\rangle_{\pi_i}$, with 2 subtracted for normalisation and phase invariance. On the other hand, the number N_π of index sets that split π is

$$N_\pi = (d^n-1) - \sum\left(d^{|\pi_i|}-1\right),$$

this being the total number of non-empty subsets of $\{1,\ldots,n\}$ minus those that do not split π, i.e. those where the 1-indices lie wholly within some π_i. But the total dimension of normalised states is $2d^n-2$ and, as each equation $c_{i_1\ldots i_n}=0$ contributes two constraints from the vanishing of its real and imaginary parts, we require

$$d_\pi = (2d^n-2) - 2N_\pi,$$

which is readily seen to hold.

IV. INVARIANTS FOR N-QUBIT STATES

From now on we restrict attention to qubit states. We are interested in polynomial invariants of the action of local unitaries, which we take to be the group $SU(2)^n \times U(1)$. Thus, given a state $|\psi\rangle = \sum_{i_1\dots i_n} a_{i_1\dots i_n}|i_1\dots i_n\rangle$, we seek real-valued polynomials $I(|\psi\rangle)$ in the coefficients $a_{i_1\dots i_n}$ and their complex conjugates $\bar{a}_{i_1\dots i_n}$ satisfying

$$I(g|\psi\rangle) = I(|\psi\rangle), \tag{15}$$

for any $g \in SU(2)^n \times U(1)$. Equivalently, we can express the group action on the ith copy of $SU(2)$ by

$$\rho_i(g)a_{j_1\dots j_i\dots j_n} = \sum_{k_i} g_{j_i k_i} a_{j_1\dots k_i\dots j_n}, \tag{16}$$

and extend this to any monomial $m = \prod_{q=1}^k a_{j_{q,1}\dots j_{q,n}}$ by $\rho_i(g)m = \prod \left(\rho_i(g)a_{j_{q,1}\dots j_{q,n}}\right)$. We then require the polynomial I to be invariant under $\rho_i(g)$ for all i and $g \in SU(2)$ as well as invariant under phase changes introduced by $U(1)$.

The cumulant $c_{i_1\dots i_n}$ can be made into a polynomial $d_{i_1\dots i_n}$ by putting

$$d_{i_1\dots i_n} = a_{0\dots 0}^{\theta} c_{i_1\dots i_n}, \tag{17}$$

where θ is the the number of 1's in the set $i_1\dots i_n$. This is a homogeneous polynomial of degree θ in the a's. For instance, from (11) we have $d_{11} = a_{00}^2 c_{11} = a_{11}a_{00} - a_{10}a_{01}$. In general, we have the following formula for $d_{i_1\dots i_n}$. Let $S = \{k | i_k = 1\}$, so $|S| = \theta$ is the degree of $d_{i_1\dots i_n}$. If $A \subset S$ let a_A denote $a_{j_1\dots j_n}$ where $j_k = 1$ if $k \in A$ and $j_k = 0$ otherwise. Then

$$d_{i_1\dots i_n} = \sum_{\pi} (-1)^{|\pi|-1}(|\pi|-1)! a_{\emptyset}^{\theta-|\pi|} \prod_{i=1}^{|\pi|} a_{\pi_i}, \tag{18}$$

where the sum is over all partitions $\pi = \{\pi_1, \dots, \pi_{|\pi|}\}$ of S, $|\pi|$ being the number of subsets in the partition.

The action of local unitaries on d_{11} is given by

$$\rho_i(g)d_{11} = \Delta d_{11}, \tag{19}$$

for $i = 1, 2$, where $\Delta = \det g$. To remove the dependence on the phase Δ, i.e. to get invariance under the action of $U(1)$, we take

$$I_{11} = |d_{11}|^2. \tag{20}$$

This gives us a local unitary invariant, and there is just one such invariant for normalised 2-qubit states. The transformation of cumulants for three or more qubits is more complicated (Theorem IV.6). However, we can always get an invariant by integrating the squared modulus of $d_{i_1\dots i_n}$ over the group $SU(2)^n$, and this prompts the following:

Definition IV.1.

$$I_{i_1\dots i_n} = \gamma_{n,\theta} \int_{SU(2)^n} |\rho_1(g_1)\dots\rho_n(g_n)d_{i_1\dots i_n}|^2 dg_1\dots dg_n. \tag{21}$$

Here the integral is over the Haar measure, and the constant factor $\gamma_{n,\theta} = (\theta+1)^{n-\theta}(\theta-1)^{\theta}$ is introduced for later convenience.

We now explore the properties of these invariants. First, we note that we can give a more satisfying, basis independent, version of Theorem III.1:

Theorem IV.2 (Separability criterion)**.** *An n-qubit state $|\psi\rangle$ is π-separable if and only if $I_{i_1\dots i_n} = 0$ whenever $i_1\dots i_n$ splits π.*

Proof. Suppose $|\psi\rangle$ is π-separable, so $|\psi\rangle = \bigotimes |\psi\rangle_{\pi_i}$. If $a_{0\dots 0} \neq 0$, Theorem III.1 says that $c_{i_1\dots i_n} = 0$ and hence $d_{i_1\dots i_n} = 0$. If $a_{0\dots 0} = 0$, define $|\psi\rangle_x = \bigotimes(|\psi\rangle_{\pi_i} + x|0\dots 0\rangle_{\pi_i})$. If $x \neq 0$, $a_{0\dots 0} \neq 0$, so $d_{i_1\dots i_n} = 0$ for this state. By continuity, $d_{i_1\dots i_n} = 0$ for $x = 0$, i.e. for the original $|\psi\rangle$. Thus $I_{i_1\dots i_n} = 0$. Conversely, if $I_{i_1\dots i_n} = 0$, then $d_{i_1\dots i_n}(g|\psi\rangle) = 0$ for all g, and for some g we must have $a_{0\dots 0} \neq 0$, so Theorem III.1 can be applied. □

Next we define the action of elements $g \in SU(2)$ on our cumulant polynomials. We will need some notation.

Definition IV.3. *Define $\mathcal{S}_i$ by*

$$\mathcal{S}_i a_{l_1 \ldots 0_i \ldots l_n} = a_{l_1 \ldots 1_i \ldots l_n}, \tag{22}$$

$$\mathcal{S}_i a_{l_1 \ldots 1_i \ldots l_n} = 0. \tag{23}$$

Now, given a monomial $m = \prod_{q=1}^{\theta} a_{i_{1,q} \cdots i_{n,q}}$ of degree θ, define $\mathcal{R}_{i,k}$ to be the coefficient of x^k in $\prod(\mathbb{1} + xS_i)a_{i_{1,q} \cdots i_{n,q}}$. Extend this definition by linearity to any homogeneous polynomial of degree θ.

For instance, for $\theta = 3$ we have

$$\mathcal{R}_{i,1} m = (\mathcal{S}_i \mathbb{1}\mathbb{1} + \mathbb{1}\mathcal{S}_i \mathbb{1} + \mathbb{1}\mathbb{1}\mathcal{S}_i)\, m.$$

Note that, by virtue of the symmetry, this definition does not depend on the order of the a's in m. We can think of $\mathcal{R}_{i,k}$ as being like a raising operator (hence the 'R'). For example

$$\mathcal{R}_{3,0} d_{110} = a_{110} a_{000} - a_{100} a_{010}, \tag{24}$$

$$\mathcal{R}_{3,1} d_{110} = a_{111} a_{000} + a_{110} a_{001} - a_{101} a_{010} - a_{100} a_{011}, \tag{25}$$

$$\mathcal{R}_{3,2} d_{110} = a_{111} a_{001} - a_{101} a_{011}, \tag{26}$$

Lemma IV.4. *If $l_i = 1$ and at least one other index in $d_{l_1 \ldots l_n}$ is 1, then $\mathcal{R}_{i,\theta} d_{l_1 \ldots l_n} = \mathcal{R}_{i,\theta-1} d_{l_1 \ldots l_n} = 0$.*

Proof. Writing d for $d_{l_1 \ldots l_n}$, $\mathcal{R}_{i,\theta} d = 0$ because we cannot add θ 1's to the $\theta - 1$ a's that originally had zeros in position i. $\mathcal{R}_{i,\theta-1} d$ has 1's at position i in every a, so we can write $\mathcal{R}_{i,\theta-1} d = d(|\psi\rangle)$, where $|\psi\rangle$ is a state with $a_{l_1 \ldots 0_i \ldots l_n} = a_{l_1 \ldots 1_i \ldots l_n}$. This means that $|\psi\rangle$ factorises as $\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)_i \otimes |\psi\rangle_{\mathcal{N}-i}$. We now invoke Theorem IV.2, since $\{l_1, \ldots, l_n\}$ splits the partition $\{i\}, \{\mathcal{N} - i\}$. □

Lemma IV.5. *If we write $L_i d$ for the result of replacing all the 1's in position i in d by 0, and if $l_i = 1$, then $L_i d = 0$.*

Proof. The same argument as in the proof above shows that $L_i d = d(|\psi\rangle)$ where $|\psi\rangle$ factorises. □

Theorem IV.6 (Action of local unitaries.)**.** *Let l_i be one of the indices of $d_{l_1,\ldots,l_n}$, and let $g = \begin{pmatrix} u & v \\ w & z \end{pmatrix}$. Assume that the index set $l_1, \ldots, l_n$ contains at least two 1's. Then if $l_i = 0$,*

$$\rho_i(g) d = \sum_{k=0}^{\theta} u^{\theta-k} v^k \mathcal{R}_{i,k} d, \tag{27}$$

and if $l_i = 1$,

$$\rho_i(g) d = \Delta \sum_{k=0}^{\theta-2} u^{\theta-k-2} v^k \mathcal{R}_{i,k} d, \tag{28}$$

where d stands for $d_{l_1,\ldots,l_n}$.

Proof. When $l_i = 0$ and $m = \prod_{q=1}^{\theta} a_{j_{q_1} \cdots j_{q_n}}$,

$$\rho_i(g) m = \prod_{q=1}^{\theta} \left(u a_{j_{q,1} \ldots 0_i \ldots j_{q,n}} + v a_{j_{q,1} \ldots 1_i \ldots j_{q,n}} \right), \tag{29}$$

and it is clear that the coefficient of u^θ is the original monomial m, and the coefficient of $u^{\theta-k} v^k$ is $\mathcal{R}_{i,k} d$.

When $l_i = 1$,

$$\rho_i(g) m = \left(w a_{j_{p,1} \ldots 0_i \ldots j_{p,n}} + z a_{j_{p,1} \ldots 1_i \ldots j_{p,n}} \right) \prod_{q=1, q \neq p}^{\theta} \left(u a_{j_{q,1} \ldots 0_i \ldots j_{q,n}} + v a_{j_{q,1} \ldots 1_i \ldots j_{q,n}} \right), \tag{30}$$

where $a_{j_{p,1} \ldots \ldots j_{p,n}}$ is the unique a in m that has a 1 at position i. The coefficient of $z v^{\theta-1}$ is $\mathcal{R}_{i,\theta-1} d$, which is zero by Lemma IV.4, and for $k \leq \theta - 2$ the coefficient of $u^{\theta-k-2} v^k (uz)$ is $cP_{i,k} d$. The coefficient of $u^{\theta-1} w$ is Ld, which is zero by Lemma IV.5, and for $k \geq 0$, the coefficient of $u^{\theta-k-2} v^k (vw)$ is $\mathcal{R}_{i,k+1}(Ld) - \mathcal{R}_{i,k} d = -\mathcal{R}_{i,k} d$. Since $\Delta = uz - vw$, the theorem follows. □

The polynomials $\mathcal{R}_{i,k}d$ appearing in equations (27) and (28) form an irreducible representation for $SU(2)$. To see this, let $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then, for $l_i = 0$, applying $\rho_i(h)$ to (27) gives

$$\sum_{k=0}^{\theta} u^{\theta-k}v^k\left(\rho_i(h)\mathcal{R}_{i,k}d\right) = \rho_i(h)\rho_i(g)d = \rho_i(gh) = \sum_{k=0}^{\theta}(ua+vc)^{\theta-k}(ub+vd)^k\mathcal{R}_{i,k}d, \tag{31}$$

and equating coefficients of $u^{\theta-k}v^k$ in the left- and right-hand sides of (31) gives the action of h at position i on all the polynomials $\mathcal{R}_{i,k}d$ and thus defines the representation matrix, which can easily be recognised as the symmetric representation with Young diagram (θ). When $l_i = 1$, the same argument applied to (28) shows that we obtain the representation with Young diagram $(\theta-1, 1)$. Classically, cumulants were called "half-invariants" [5, 25] because, if c is the classical joint cumulant in the random variables $X_1 \dots X_n$, then c is mapped to $z^n c$ when X_i is transformed by the affine map $X_i \to zX_i + w$. The equivalent of an affine map in our setting is the group of matrices $\begin{pmatrix} 1 & 0 \\ w & z \end{pmatrix}$ with $z \neq 0$. From Theorem IV.6 we see that the representation becomes 1-dimensional, sending $d \to z^\theta d$.

Theorem IV.7 (Formula for invariants)**.** *If the index set $i_1, \dots, i_n$ contains at least two 1's, then*

$$I_{i_1,\dots,i_n} = \sum_{k_1,\dots,k_n}\left|\prod_{p=1}^{n}\left(\alpha^{i_p}_{k_p}\mathcal{R}_{i_p,k_p}\right)d_{i_1,\dots,i_n}\right|^2. \tag{32}$$

Here, if $i_p = 0$, k_p ranges from 0 to θ, and $\alpha^0_{k_p} = \binom{\theta}{k_p}^{-1}$. If $i_p = 1$, k_p ranges from 0 to $\theta-2$, and $\alpha^1_{k_p} = \binom{\theta-2}{k_p}^{-1}$

Proof. Combining (21) and Theorem IV.6 we get terms from $\int|\rho_i(g)d|^2dg$ such as $\int|u|^{2(\theta-k)}|v|^{2k}dg|\mathcal{R}_{i,k}d|^2$, and the integral can be calculated by using Schur's lemma:

$$\begin{aligned}\binom{p+q}{p}\int|u|^{2p}|v|^{2q}dg &= \langle\psi_{p,q}|\int g^{\otimes(p+q)}|0\rangle\langle 0|^{\otimes(p+q)}(g^\dagger)^{\otimes(p+q)}dg|\psi_{p,q}\rangle && (33)\\ &= \dim\mathsf{Sym}^{p+q}(\mathbb{C}^2)^{-1}\langle\psi_{p,q}|P_{Sym}|\psi_{p,q}\rangle && (34)\\ &= \dim\mathsf{Sym}^{p+q}(\mathbb{C}^2)^{-1} && (35)\\ &= (p+q+1)^{-1}. && (36)\end{aligned}$$

Here P_{Sym} is the projector onto the symmetric representation, and $|\psi_{p,q}\rangle$ is the normalised weight vector $\binom{p+q}{p}^{-1}\sum_\sigma|i_{\sigma(1)}\dots i_{\sigma(p+q)}\rangle$, with $i_1 = \dots = i_p = 0$, $i_{p+1} = \dots = i_{p+q} = 1$, and with the sum taken over all permutations in S_{p+q}. There are $n-\theta$ indices i_p that are zero, where $(p+q+1) = \theta+1$, and θ indices i_p that are 1, where $(p+q+1) = \theta-1$. These terms therefore cancel the constant $\gamma_{n,\theta} = (\theta+1)^{n-\theta}(\theta-1)^\theta$ in (21), and the $\alpha^{i_p}_{k_p}$'s come from the factor $\binom{p+q}{p}$ in (33).

There are also cross-terms in $\int|\rho_i(g)d|^2dg$, but these have the form $\int u^{(\theta-k)}v^k\overline{u}^{(\theta-j)}\overline{v}^j dg\left(\mathcal{R}_{i,k}d\overline{\mathcal{R}_{i,j}d}\right)$, and

$$\int u^{(\theta-k)}v^k\overline{u}^{(\theta-j)}\overline{v}^j dg = \langle\psi_{\theta-k,k}|\psi_{\theta-j,j}\rangle, \tag{37}$$

which vanishes for $j \neq k$ since distinct weight vectors are orthogonal. □

As examples, consider the case of three qubits. From (32) we find

$$I_{110} = |\mathcal{R}_{3,0}d_{110}|^2 + \frac{1}{2}|\mathcal{R}_{3,1}d_{110}|^2 + |\mathcal{R}_{3,2}d_{110}|^2, \tag{38}$$

which is a polynomial invariant of degree 4. The terms are given explicitly by (24), (25) and (26). There are two other 4th degree invariants, I_{101} and I_{011} obtained by permuting the indices. We also have

$$I_{111} = \sum_{i,j,k=0}^{1}|\mathcal{R}_{1,i}\mathcal{R}_{2,j}\mathcal{R}_{3,k}d_{111}|^2, \tag{39}$$

which is of degree 6. The theorem excludes the case where there is a single 1 in the index set. For instance, we have $d_{100} = a_{100}$. If we apply Definition 21 with $\gamma_{n,1} = 2^n$, we find $I_{100} = \langle\psi|\psi\rangle$, and this result is independent of the ordering of the indices. This holds for any n, i.e. $I_{10^{n-1}} = \langle\psi|\psi\rangle$, where 0^k stands for a string of k 0's, and again the ordering of indices is immaterial. This invariant is often included in the list, assuming that states are not normalised.

With this assumption, there are altogether six algebraically independent invariants for three qubits [16, 23]. A further invariant is needed in order to have a Hilbert basis [9], which has the property that every invariant can be written as a polynomial in the basis elements. However, the seventh invariant can be expressed in terms of Sudbery's six if one is allowed a square root, and from the point of view of a quantum information theorist rather than an algebraist, a complete, algebraically independent set serves to characterise the orbits.

Following [23], five of Sudbery's set of six are the second-degree polynomial $J_1 = \langle\psi|\psi\rangle$, the three fourth-degree polynomials $J_2 = \mathsf{tr}\rho_3^2$, $J_3 = \mathsf{tr}\rho_2^2$, $J_4 = \mathsf{tr}\rho_1^2$ and the sixth-degree polynomial $J_5 = 3\mathsf{tr}\left[(\rho_1 \otimes \rho_2)\rho_{12}\right] - \mathsf{tr}(\rho_1^3) - \mathsf{tr}(\rho_2^3)$, where $\rho_1 = \mathsf{tr}_{23}|\psi\rangle\langle\psi|$, $\rho_2 = \mathsf{tr}_{13}|\psi\rangle\langle\psi|$, $\rho_3 = \mathsf{tr}_{12}|\psi\rangle\langle\psi|$, and $\rho_{12} = \mathsf{tr}_3|\psi\rangle\langle\psi|$. A straightforward calculation shows that our invariants can then be expressed in terms of these polynomials by

$$\begin{aligned}
I_{100} = I_{010} = I_{001} &= J_1, \\
4I_{110} &= J_1^2 + J_2 - J_3 - J_4, \\
4I_{101} &= J_1^2 + J_3 - J_2 - J_4, \\
4I_{011} &= J_1^2 + J_4 - J_2 - J_3, \\
6I_{111} &= 5J_1^3 - 3J_1\left(J_2 + J_3 + J_4\right) + 4J_5.
\end{aligned}$$

Alternatively, they can be identified with five of the list given in [17]: I_{001} is their A_{111}, I_{110} is B_{002}, and I_{111} is C_{111}.

Next we consider the question of independence of the invariants. We can quickly eliminate certain types of functional dependence by using the separability criterion, Theorem IV.2. For instance, we cannot have $I_{110} = f(I_{111}, I_{101}, I_{011})$ for any function f because all the invariants on the right-hand side are zero for any $\{12\}\{3\}$-separable state, whereas I_{110} can take a range of values according to the choice of the state. However, we cannot use the separability criterion to rule out a relation of the form $I_{111} = f(I_{011}, I_{101}, I_{110})$, say. Our next aim is to prove that the invariants are in fact algebraically independent, i.e. that there can be no non-trivial polynomial relation between them.

Theorem IV.8 (Algebraic independence). *A polynomial relationship between the invariants* $I_{i_1\ldots i_n}$

$$\sum \alpha_{i_{1,1}\ldots i_{k,n}} I^{j_1}_{i_{1,1}\ldots i_{1,n}} \ldots I^{j_k}_{i_{k,1}\ldots i_{k,n}} = 0, \tag{40}$$

can only hold if each $\alpha_{i_{1,1}\ldots i_{k,n}} = 0$.

Proof. Consider the neighbourhood of the fully separable state $|0\ldots 0\rangle$, where the $a_{i_1\ldots i_n}$'s with not all $i_j = 0$ are small. From (32) and (18) we see that the expansion of the invariants in lowest degree terms in these small variables only has contributions from the term $a_{j_1\ldots j_n} a^{\theta-1}_{0\ldots 0}$ in $d_{j_1\ldots j_n}$, and from the corresponding term where operators $\mathcal{R}_{i,1}$ applied to positions where the index $j_i = 0$. Thus, assuming that the indices $i_1, \ldots, i_n$ include at least two 1's, we have

$$I_{i_1\ldots i_n} \approx x^{\theta-1}_{0\ldots 0} \sum_{i_{t_1}=0}^{1} \cdots \sum_{i_{t_{n-\theta}}=0}^{1} \left(\theta^{-\sum_j i_{t_j}}\right) x_{i_1\ldots i_{t_1}\ldots i_{t_2}\ldots i_n}, \tag{41}$$

where $x_{j_1\ldots j_n} = |a_{j_1\ldots j_n}|^2$, and $t_1 \ldots t_{n-\theta}$ denote the positions of indices in $i_1, \ldots, i_n$ that are zero. We also have the special case

$$I_{10\ldots 0} = \sum_{i_1=0}^{1} \cdots \sum_{i_n=0}^{1} x_{i_1\ldots i_n}.$$

Let us write $I_1 = I_{10\ldots 0} - x_{0\ldots 0}$, and $x_1 = x_{10\ldots 0} + x_{010\ldots 0} + \ldots x_{0\ldots 01}$. Then the lowest degree expansion defines an invertible map A. For instance, for $n = 3$ this map is given by

$$A = \begin{array}{c} \\ x_1 \\ x_{110} \\ x_{101} \\ x_{011} \\ x_{111} \end{array} \begin{array}{c} \begin{array}{ccccc} I_1 & I_{110} & I_{101} & I_{011} & I_{111} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & x_{000} & 0 & 0 & 0 \\ 1 & 0 & x_{000} & 0 & 0 \\ 1 & 0 & 0 & x_{000} & 0 \\ 1 & \frac{1}{2}x_{000} & \frac{1}{2}x_{000} & \frac{1}{2}x_{000} & x_{000}^2 \end{pmatrix} \end{array}$$

This extends to a map A^{poly} from polynomials in the I's to polynomials in the x's. Since A is invertible, the same is true of A^{poly}. If we now take the lowest degree terms in (40), they map to a polynomial in the x's whose coefficients must be zero, since the x's are independent variables. Applying the inverse of A^{poly}, we deduce that the corresponding coefficients in (40) are zero. Looking at the next highest degree terms in (40), we again deduce that their coefficients are zero. And so on for the whole I-polynomial. □

We can therefore conclude that we get $2^n - n$ independent invariants from cumulants, namely one invariant, the squared-amplitude, from the first-degree cumulants, and $2^n - n - 1$ from the second and higher degree cumulants. On the other hand, the total number of independent invariants [3] for $n \geq 3$ is $N_i = 2^{n+1} - (3n+1)$. Thus asymptotically there are $N_i/2$ cumulant-based invariants.

V. THE HIERARCHICAL STRUCTURE OF INVARIANTS

The 3-qubit invariants I_{011}, I_{101} and I_{110} are closely related to the 2-qubit invariant I_{11}. We obtain I_{110} from I_{11} by adding a '0' index in the third position to I_{11} and twirling. More generally, we wish to make an $(n+1)$-qubit invariant from an n-qubit invariant J. Phase invariance requires every term in J to be a product of an equal number of a's and $\bar{a}$'s. Given a monomial $m = \prod a_{j_1 \dots j_n} \bar{a}_{k_1 \dots k_n}$ in J, of degree θ in the a's and $\bar{a}$'s, we define

$$m_0 = (\theta + 1) \int_{SU(2)} \rho_i(g) \prod a_{j_1 \dots 0_i \dots j_n} \bar{a}_{k_1 \dots 0_i \dots k_n} dg. \tag{42}$$

We refer to this process as *lifting* and use a subscript '0' to denote a lifted index. Table I shows lifts of I_{11} and I_{111} up to five qubits. We say that an invariant together with its lifts constitute a *family*.

Lifting can also be understood in terms of tracing-out operations. Let us write a mixed state of n qubits as

$$\rho = \sum_{i_1, \dots i_n; j_1, \dots j_n} a^{j_1, \dots j_n}_{i_1, \dots i_n} \bigotimes_{r=1}^{n} |i_r\rangle\langle j_r| \tag{43}$$

The following rules, applied to each monomial, enable one to interconvert between a pure state invariant J of degree θ in the a's and $\bar{a}$'s, and a mixed state invariant $\hat{J}$ of degree θ in the coefficients of (43):

$$J \to \hat{J}: \quad \prod_{r=1}^{\theta} a_{i_1^r, \dots i_n^r} \prod_{s=1}^{\theta} \bar{a}_{j_1^s, \dots j_n^s} \longrightarrow \frac{1}{\theta!} \sum_{\sigma \in S_\theta} \prod_{r=1}^{\theta} a^{j_1^{\sigma(r)}, \dots j_n^{\sigma(r)}}_{i_1^r, \dots i_n^r} \tag{44}$$

$$\hat{J} \to J: \quad \prod_{r=1}^{\theta} a^{j_1^r, \dots, j_n^r}_{i_1^r, \dots, i_n^r} \longrightarrow \prod_{r=1}^{\theta} a_{i_1^r, \dots, i_n^r} \prod_{r=1}^{\theta} \bar{a}_{j_1^r, \dots, j_n^r} \tag{45}$$

Proposition V.1. *If $\rho_i(g) J = J$ then $\rho_i(g) \hat{J} \rho_i(g)^\dagger = \hat{J}$.*

Proof. The following diagram commutes

$$\begin{tikzcd} J \arrow[r, "\rho_i(g)"] \arrow[d] & J \arrow[d] \\ \hat{J} \arrow[r, "\rho_i(g)^{\mathrm{conj}}"] & \hat{J} \end{tikzcd}$$

□

The following is immediate:

Proposition V.2.

$$\hat{J}(|\psi\rangle\langle\psi|) = J(|\psi\rangle).$$

Proposition V.3. *If $|\psi\rangle$ is an n-qubit state and $J_{p_1 \dots p_k}$ a polynomial invariant, then*

$$J_{p_1 \dots p_k 0^{n-k}}(|\psi\rangle) = \hat{J}_{p_1 \dots p_k}(\mathsf{tr}_{n-k} |\psi\rangle\langle\psi|),$$

where 0^{n-k} means a string of $(n-k)$ '0' indices, and tr_{n-k} means tracing out the last $(n-k)$ systems.

Proof. Let us see how this works in a simple case. The generalisation is then straightforward. So consider the monomial $m = a_{i_1 i_2} a_{j_1 j_2} \bar{a}_{k_1 k_2} \bar{a}_{l_1 l_2}$ of a 4th degree 2-qubit invariant $J_{p_1 p_2}$. Under the map (44) m becomes $\widehat{m} = \frac{1}{2}\left(a^{k_1 k_2}_{i_1 i_2} a^{l_1 l_2}_{j_1 j_2} + a^{l_1 l_2}_{i_1 i_2} a^{k_1 k_2}_{j_1 j_2}\right)$. The monomial m lifts, by (42), to

$$m_0 = (\theta + 1) \int \rho_3(g) a_{i_1 i_2 0} a_{j_1 j_2 0} \bar{a}_{k_1 k_2 0} \bar{a}_{l_1 l_2 0} dg \tag{46}$$

in $J_{p_1 p_2 0}(|\psi\rangle)$ for a 3-qubit state $|\psi\rangle$, and $(\theta + 1) = 3$. We therefore wish to show that $m_0 = \widehat{m}$, where the coefficients $a^{k_1 k_2}_{i_1 i_2}$, etc., in $\widehat{m}$ come from $\mathsf{tr}_3|\psi\rangle\langle\psi|$. This gives

$$\begin{aligned} \widehat{m} = {} & \frac{1}{2}\left(a_{i_1 i_2 0}\bar{a}_{k_1 k_2 0} + a_{i_1 i_2 1}\bar{a}_{k_1 k_2 1}\right)\left(a_{j_1 j_2 0}\bar{a}_{l_1 l_2 0} + a_{j_1 j_2 1}\bar{a}_{l_1 l_2 1}\right) \\ & + \frac{1}{2}\left(a_{i_1 i_2 0}\bar{a}_{l_1 l_2 0} + a_{i_1 i_2 1}\bar{a}_{l_1 l_2 1}\right)\left(a_{j_1 j_2 0}\bar{a}_{k_1 k_2 0} + a_{j_1 j_2 1}\bar{a}_{k_1 k_2 1}\right), \end{aligned} \tag{47}$$

and from (46) we have

$$m_0 = \int \left(u a_{i_1 i_2 0} + v a_{i_1 i_2 1}\right)\left(u a_{j_1 j_2 0} + v a_{j_1 j_2 1}\right)\overline{\left(u a_{k_1 k_2 0} + v a_{k_1 k_2 1}\right)}\;\overline{\left(u a_{l_1 l_2 0} + v a_{l_1 l_2 1}\right)}.dg \tag{48}$$

Comparing (47) and (48), and using (33), (36) and (37), we see that $m_0 = \widehat{m}$. This argument is unchanged when J is an n-qubit invariants (we just permute notationally more cumbersome blocks of indices). When the degree, 2θ, is arbitrary, a term in $\widehat{m}$ that has p 0's in the a's in the lifted index position occurs $p!(\theta - p)!$ times in the generalisation of (47). With the normlising factor $1/\theta!$ from (44), we obtain the coefficient $\int |u|^{2p}|v|^{2\theta-2p}$ of the corresponding term in m_0, as given by (48). □

Proposition V.3 provides an alternative definition of lifting via tracing-out of subsystems. Combining this Proposition with Proposition V.2 we get

Corollary V.4. *If* $|\psi\rangle = |\mu\rangle_k \otimes |\nu\rangle_{n-k}$ *then*

$$J_{i_1 \ldots i_k 0^{n-k}}(|\psi\rangle) = J_{i_1 \ldots i_k}(|\mu\rangle).$$

The third, equivalent, definition of lifting comes from a technique called transvection, invented by Cayley in the 19th century heyday of invariant theory. Transvection is a useful device for generating invariants; understanding it will enable us to interpret the 4-qubit invariants given in [17] in the language used here.

The *fundamental form* for a n-qubit state is the polynomial f in the a's and the variables $x_0^{(j)}$, $x_1^{(j)}$, for $1 \le j \le n$ given by

$$f = \sum_{i_1, \ldots, i_n} a_{i_1 \ldots i_n} x^{(1)}_{i_1} \ldots x^{(n)}_{i_n} \tag{49}$$

If we let $g \in SU(n)$ act on the ith index of a's by the usual transpose action (16) and upon the $x^{(i)}$'s via the inverse, $g^\dagger$, then one easily checks that $\rho(g)f = f$. More generally, a *covariant* of weight q is a polynomial p in the a's and x's satisfying

$$\rho_i(g)p = \Delta_i^q p. \tag{50}$$

Given two covariants, p and q, we define $\langle p, q\rangle$, by $\langle \mu(a)|\nu(a)\rangle = \mu(a)\overline{\nu(a)}$ for expressions in the a's, and, for each i,

$$\langle (x_0^{(i)})^{p_i}(x_1^{(i)})^{q_i} | (x_0^{(i)})^{p'_i}(x_1^{(i)})^{q'_i}\rangle = \delta_{p_i, p'_i}\delta_{q_i, q'_i} p_i! q_i!. \tag{51}$$

This is sometimes called the *derivative inner product* because we obtain it by setting $x_j^{(i)}$ on the lefthand side to $\partial/\partial x_j^{(i)}$ and applying these derivatives to (unchanged) x's on the righthand side.

If p is a covariant, then $\langle p, p\rangle$ is an invariant, so any means of generating covariants also supplies us with invariants. Transvection is just such a means. Given two covariants, $p(x_j^{(i)})$, $q(y_j^{(i)})$, define the *transvectant* by

$$(p, q)^{i_1 \ldots i_k} = \Omega_{i_1} \ldots \Omega_{i_k}(pq)\Big|_{y \to x} \quad \text{where } \Omega_i X = \frac{\partial}{\partial x_0^{(i)}}\frac{\partial}{\partial y_1^{(i)}} - \frac{\partial}{\partial x_1^{(i)}}\frac{\partial}{\partial y_0^{(i)}}. \tag{52}$$

The vertical bar indicates that, after applying the differential operators Ω_i, we change the y's to x's, so $(p, q)^{i_1 \cdots i_k}$ is a polynomial in a's and x's. A classical theorem [19] asserts that, for any binary indices $i_1 \ldots i_k$, $(p, q)^{i_1 \cdots i_k}$ is a covariant if p and q are. Starting with the fundamental form, we can build up a wealth of covariants p and derive invariants $\langle p|p\rangle$ from them (see Table II).

TABLE I: Some 2, 3, 4, and 5-qubit invariants related by lifting.

2 qubits	**3 qubits**	**4 qubits**	**5 qubits**
I_{10}	I_{100}	I_{1000}	I_{10000}
I_{11}	$I_{110}, I_{101}, I_{011}$	$I_{1100}, I_{1010}, I_{0110}, I_{1001}, I_{0101}, I_{0011}$	I_{11000}, I_{10100}, etc. (10)
-	-	G_{1111}	$G_{11110}, G_{11101}, G_{11011}, G_{10111}, G_{01111}$
-	I_{111}	$I_{1110}, I_{1101}, I_{1011}, I_{0111}$	I_{11100}, I_{11010}, etc. (10)
-	H_{222}	$H_{2220}, H_{2202}, H_{2022}, H_{0222}$	H_{22200}, H_{22020}, etc. (10)

TABLE II: Sixteen of the nineteen four-qubit invariants in transvectant notation.

Invariants	Corresponding covariants	number	degree
I_{1000}	f	1	2
G_{1111}	$(f,f)^{1111}$	1	4
I_{1100}	$(f,f)^{1100}$	6	4
I_{1110}	$(f,(f,f)^{1100})^{0010}$	4	6
H_{2220}	$(f,(f,(f,f)^{1100})^{0010})^{1110}$	4	8

Example V.5. *For two-qubit states, $f = \sum a_{ij} x_i^{(1)} x_j^{(2)}$. Take $p = (f,f)^{11}$. Then $p = d_{11}$ and $\langle p|p\rangle = |d_{11}|^2 = I_{11}$. For three-qubit states, $f = \sum a_{ijk} x_i^{(1)} x_j^{(2)} x_k^{(3)}$. Take $\iota_{110} = (f,f)^{110}$. Applying (52) we get*

$$\iota_{110} = (f,f)^{110} = d_{110}(x_0^{(3)})^2 + \mathcal{R}_{3,1} d_{110}(x_0^{(3)} x_1^{(3)}) + \mathcal{R}_{3,2} d_{110}(x_1^{(3)})^2.$$

Using the derivative formula for the inner product (51) we find that $\langle \iota_{110}|\iota_{110}\rangle = 4I_{110}$.

More generally, we have the following result:

Theorem V.6. *Let*

$$\iota_{1^k 0^{n-k}} = (f,(f,\ldots(f,f)^{110\ldots0})^{001\ldots0}\ldots)^{0\ldots010^{n-k}}.$$

Then

$$\langle \iota_{1^k 0^{n-k}} | \iota_{1^k 0^{n-k}} \rangle = \xi I_{1^k 0^{n-k}},$$

where $\xi = 4((k-2)!)^k (k!)^{n-k}$.

Proof. Consider first the terms in $\iota_{1^k 0^{n-k}}$ where the subscript in every x is 0.The first transvectant step, $(f,f)^{110\ldots0}$, yields terms

$$\sum_{i_3\ldots i_n; j_3\ldots j_n} (a_{11 i_3\ldots i_n} a_{00 j_3\ldots j_n} - a_{10 i_3\ldots i_n} a_{01 j_3\ldots j_n})\, x_{i_3}^{(3)} x_{j_3}^{(3)} \ldots x_{i_n}^{(n)} x_{j_n}^{(n)}. \tag{53}$$

If $k = 2$, the restriction to x_0's means that we get

$$\iota_{11(0^{n-2})}|_{x_0} = d_{11(0^{n-2})} \left(x_0^{(3)} \ldots x_0^{(n)}\right)^2.$$

If $k > 2$, at the next transvectant step we set the x's in (53) to y's, multiply by the fundamental form f and apply Ω_3 to get

$$\Omega_3 \left[\sum_{k_1\ldots k_n} a_{k_1\ldots k_n} x_{k_1}^{(1)} \ldots x_{k_n}^{(n)}\right] \left[\sum_{i_3\ldots i_n; j_1\ldots j_n} (a_{11 i_3\ldots i_n} a_{00 j_3\ldots j_n} - a_{10 i_3\ldots i_n} a_{01 j_3\ldots j_n})\, y_{i_3}^{(3)} y_{j_3}^{(3)} \ldots y_{i_n}^{(n)} y_{j_n}^{(n)}\right]\Bigg|_{y\to x}.$$

If we are restricted to x_0's, we must have $k_1 = k_2 = 0$ since no further Ω operations are applied in these index positions and so these x's will be unchanged. Only certain sets of indices are consistent with a y_0 remaining after applying Ω_3 to $x^{(3)}_{k_3}y^{(3)}_{i_3}y^{(3)}_{j_3}$; namely (1) $k_3 = 0$, $i_3 = 1$, $j_3 = 0$; (2) $k_3 = 0$, $i_3 = 0$, $j_3 = 1$; (3) $k_3 = 1$, $i_3 = 0$, $j_3 = 0$. The result of this operation is of the form

$$\sum_{i,jk}(\alpha_{i,j,k} + \beta_{i,j,k})x^{(1)}_0 x^{(2)}_0 x^{(3)}_0 x^{(4)}_{i_4} x^{(4)}_{j_4} x^{(4)}_{k_4} \ldots x^{(n)}_{i_n} x^{(n)}_{j_n} x^{(n)}_{k_n},$$

where $\alpha_{i,jk}$, $\beta_{i,j,k}$ are terms in the a's with compound indices $i = \{i_4 \ldots i_n\}$, etc., and $\alpha_{i,jk}$ comes from the conditions (1) and (2) above on index sets:

$$\alpha_{i,j,k} = a_{000k_4\ldots k_n}\mathcal{R}_{3,1}\left[a_{110i_4\ldots i_n}a_{000j_4\ldots j_n} - a_{010i_4\ldots i_n}a_{100j_4\ldots j_n}\right],$$

whereas from condition (3) we get

$$\beta_{i,j,k} = a_{001k_4\ldots k_4}\left[a_{110i_4\ldots i_n}a_{000j_4\ldots j_n} - a_{010i_4\ldots i_n}a_{100j_4\ldots j_n}\right].$$

If $k = 3$ this simplifies to

$$\iota_{111(0^{n-3})}|_{x_0} = \left[a_{000(0^{n-3})}\mathcal{R}_{3,1}d_{110(0^{n-3})} - 2a_{001(0^{n-3})}d_{110(0^{n-3})}\right]\left(x^{(1)}_0 x^{(2)}_0 x^{(3)}_0\right)\left(x^{(4)}_0 \ldots x^{(n)}_0\right)^3. \tag{54}$$

Using (18), a straightforward calculation shows that

$$d_{111(0^{n-3})} = a_{000(0^{n-3})}\mathcal{R}_{3,1}d_{110(0^{n-3})} - 2a_{001(0^{n-3})}d_{110(0^{n-3})}. \tag{55}$$

Repeating the above argument, we have

$$\iota_{1^k0^{n-k}}|_{x_0} = d_{1^k0^{n-k}}\left(x^{(1)}_0 \ldots x^{(k)}_0\right)^{k-2}\left(x^{(k+1)}_0 \ldots x^{(n)}_0\right)^k, \tag{56}$$

and the generalisation of (55) is

$$d_{1^k0^{n-k}} = a_{0^n}\mathcal{R}_{k,1}d_{1^{k-1}0^{n-k+1}} - 2a_{0^{k-1}10^{n-k+1}}d_{1^{k-1}0^{n-k+1}}. \tag{57}$$

This last equation has a straightforward interpretation. When evaluating $f(\psi)$ by the Taylor series (1), the coefficient of, say, e_1 can be obtained by differentiating $\frac{\partial}{\partial e_1}f(\psi)$ and setting $e_i = 0$, for all i. Writing $\psi = a + r$, where $a = a_{0\ldots0}$, we find

$$\frac{\partial}{\partial e_1}f(a+r)|_{e_i=0} = f'(a+r)\frac{\partial}{\partial e_1}r|_{e_i=0} = f'(a)a_{10\ldots0} = f'(a)\mathcal{R}_{1,1}a.$$

We can interpret the last expression above as the formal derivative of $f(\psi)$ using the raising operator $\mathcal{R}_{1,1}$, and similarly the coefficient of any product $e_{i_1} \ldots e_{i_q}$ is the result of formal derivatives by $\mathcal{R}_{i_1,1} \ldots \mathcal{R}_{i_q,1}$. This can indeed be taken as the *definition* of the expansion of $f(\psi)$, as in [1]. For the log function, the coefficient of $e_1 \ldots e_{k-1}$ is $c_{1^{k-1}0^{n-k+1}}$, and the coefficient of $e_1 \ldots e_k$, namely $c_{1^k0^{n-k}}$ is obtained by applying $\mathcal{R}_{k,1}$ to $c_{1^{k-1}0^{n-k+1}}$. Differentiating $\log(\psi)$ and using $c_{1^q0^{n-q}} = d_{1^q0^{n-q}}(a_{0^n})^{-q}$ gives (57).

From (56) and the definition of the inner product (51) we find that

$$\langle(\iota_{1^k0^{n-k}}|_{x_0})\,|\,(\iota_{1^k0^{n-k}}|_{x_0})\rangle = \xi|d_{1^k0^{n-k}}|^2,$$

where ξ is the constant given in the Proposition. With the restriction to x_0's we therefore get, up to the factor ξ, the term in the formula for $I_{1^k0^{n-k}}$ (Theorem IV.7) where $k_p = 0$ for all p. To complete the proof, one observes that, allowing k $x^{(i)}_1$'s introduces k 1's into the a's at position i, and is equivalent to applying $\mathcal{R}_{i_p,k_p}$ to $d_{1^k0^{n-k}}$. The values of the coefficients $\alpha^{i_p}_{k_p}$ are given by the derivative inner product.

□

This enables us to recognise some of the four-qubit invariants in [17]. Up to a constant factor, our I_{1000}, I_{1100} and I_{1110} correspond to their A_{1111}, $\langle B_{0022}|B_{0022}\rangle$ and $\langle C_{1113}|C_{1113}\rangle$, respectively. We use different letters for the invariants, and our subscripts indicate the total number of 1's at a given position in successive transvection operations; see Table II.

We now come to the third way of defining the lift. Suppose that a covariant $p_{l_1\ldots l_n}$ is derived by some sequence of transvectant operations. Define its ith lift $p_{l_1\ldots 0_i \ldots l_n}$ by adding an index position in the ith position in the ground form, and applying the same transvectant operations, but with an '0' added to the transvectant indices in the ith position.

Proposition V.7. *If $P_{l_1\dots l_n} = \langle p_{l_1\dots l_n}|p_{l_1\dots l_n}\rangle$ is the invariant derived from the covariant $p_{l_1\dots l_n}$, then the ith lift of $P_{l_1\dots l_n}$ is given by $P_{l_1\dots 0_i\dots l_n} = \langle p_{l_1\dots 0_i\dots l_n}|p_{l_1\dots 0_i\dots l_n}\rangle$.*

Proof. Because there is a 0 at position i in the transvectant indices, Ω_i is never applied during the transvection operations. This means that we get all possible products of $x_0^{(i)}$ and $x_1^{(i)}$, and the terms with k $x_1^{(i)}$'s correspond to products of a's with k 1's in index position 1. □

As an example, consider the invariant of highest degree for 3-qubits in [17]. It is given (in our notation) by $H_{222} = \langle h_{222}|h_{222}\rangle$, where

$$h_{222} = (f, (f, (f, f)^{110})^{001})^{111}. \tag{58}$$

Equivalently, $H_{222} = |\mathrm{Det}(|\psi\rangle)|^2$, where $\mathrm{Det}(|\psi\rangle) = a_{ijk}a_{i'j'm}a_{npk'}a_{n'p'm'}\epsilon_{ii'}\epsilon_{jj'}\epsilon_{kk'}\epsilon_{mm'}\epsilon_{nn'}\epsilon_{pp'}$ is the hyperdeterminant [18]. H_{222} is I_6 in [23], and is closely related to the 3-tangle [4], $\tau = 2|\mathrm{Det}(|\psi\rangle)|$. From (58), the lift of h_{222} at position 4 is $h_{2220} = (f, (f, (f, f)^{1100})^{0010})^{1110}$, and therefore by Proposition V.7 $H_{2220} = \langle h_{2220}|h_{2220}\rangle$ is the lift at position 4 of H_{222}. In the terminology of [17], H_{222} is D_{000} and H_{2220} is $\langle D_{0004}|D_{0004}\rangle$.

Another example is obtained by putting $g_{1111} = (f, f)^{1111}$ and setting $G_{1111} = \langle g_{1111}|g_{1111}\rangle$. This 4th degree invariant can be written

$$G_{1111} = a_{0000}a_{1111} - (a_{1000}a_{0111} + \text{ permutations }) + (a_{1100}a_{0011} + \text{ permutations }).$$

In general, for each k, we add a new $2k$-party invariant $G_{1^{2k}} = \langle g_{1^{2k}}|g_{1^{2k}}\rangle$, where $g_{1^{2k}} = (f, f)^{1^{2k}}$. Together with all its lifts, the G family comprises $\binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \ldots = 2^{n-1} - 1$ independent invariants of degree 4 for an n-qubit system. This coincides with the family B_d in [17].

VI. CONCLUSIONS

We have arrived at a view of local unitary invariants of qubit states which can be summarised as follows:

- Half of them (in the limit of large n) can be taken to be twirled cumulants. Thus for $n = 3$ the cumulants I_{100}, I_{110} and I_{111} correspond to A_{111}, B_{002} and C_{111}, respectively, in [17], which, together with permutations, account for 5 of the 6 invariants; and for $n = 4$, I_{1000}, I_{1100} and I_{1110} correspond to their A_{1111}, $\langle B_{0022}|B_{0022}\rangle$ and $\langle C_{1113}|C_{1113}\rangle$, respectively, which, with permutations, gives 11 of the total of 19.

- All the invariants come in families, related by a tracing operation (Proposition V.3) that I call a lift and indicate by a zero in the index string. The cumulant family is obtained this way, from I_1, I_{11}, I_{111}, etc., by lifting. A further example is the hyperdeterminant family: for $n = 3$, D_{000} in the notation in [17] is the 3-tangle (the modulus-squared of the hyperdeterminant), which I denote by H_{222}, and their $\langle D_{0004}|D_{0004}\rangle$ and its permutations are lifted 3-tangles, H_{2220} etc. in my notation. These families may overlap. For instance, I_{1111} is not included in the list of primary invariants in [17], and is therefore algebraically dependent on the lifted 3-tangles and others in their list.

- Many of the invariants are closely related to separability of states. Thus, the vanishing of members of the cumulant family can be used to characterise multipartite separability (see Theorem IV.2). The hyperdeterminant, in its guise as the 3-tangle, is of course also an entanglement measure. Unlike the cumulant invariants, the 3-tangle measures entanglement of mixed states, whereas the mixed state equivalent of cumulants, $\widehat{I}$, only measure correlation in mixed states.

We can add a number of conjectures to this list:

- I_{11} attains its maximum of 1/4 on Bell states, and I_{110} is maximised by $\Psi \otimes |0\rangle$, with Ψ a Bell state. We can regard this as an example of monogamy of entanglement [4, 12], with I_{110} detecting entanglement between the first two systems, which achieves its maximum when they are unentangled with the third system. I conjecture that I_{1^k0} is maximised by states of the form $|\mu\rangle \otimes |0\rangle$, where the k-qubit state $|\mu\rangle$ maximises I_{1^k}. Equivalently, $\widehat{I}_{1^k}(\rho)$ is maximised when ρ is pure.

- For 3 qubits, the highest degree invariant in [17, 23] is H_{222}, (equal to $\frac{1}{4}\tau^2$, where τ is the 3-tangle [4]) is derived from the covariant ι_{111} underlying I_{111} by applying what one could call the total transvectant operation $h_{222} = (f, \iota_{111})^{111}$, with an Ω operation at each index position. Can a highest degree invariant always be derived this way, by $h_{2^n} = (f, \iota_{1^n})^{1^n}$? In [17], the highest degree invariant for 4-qubits is defined by $(f, (f, \iota_{0111})^{1011})^{1100}$, but we can replace this by H_{2222} to obtain an algebraically independent set (though not necessarily a Hilbert basis). I therefore conjecture that H_{2^n} constitute another family.

How far can the ideas here can be generalised beyond pure qubit states? The cumulant-based invariants can be applied to mixed states via the map (44). However, they then constitute only an exponentially small fraction of the estimated $2^{2n} - 3n + 1$ invariants for mixed qubit states [24], and furthermore Theorem III.1 tells us only about correlation rather than mixed-state separability. The results also fail to generalise for pure states where the local dimension exceeds two. We can construct invariants, and Theorem III.1 holds, but the invariants are not algebraically independent. This is seen even for two qutrits, where we have four members of the cumulant family, namely I_{11}, I_{12}, I_{21} and I_{22}, whereas there are only two independent invariants [10]. Since four polynomial equations is the correct number to characterise separability, the simple relationship between invariants and separability cannot hold for $d > 2$. Nonetheless the basic concept of lifts and families still applies in all these wider contexts.

VII. ACKNOWLEDGEMENTS

I thank Johan Åberg and Tony Sudbery for comments on the emerging manuscript, and Graeme Segal for help with formulating the algebra of multi-partite states.

[1] J. Aberg and G. Mitchison, J. Math. Phys. **50**, 042103 (2009).
[2] H. A. Carteret, N. Linden, S. Popescu, A. Sudbery Found. Phys. **29**, 527, (1999).
[3] H. A. Carteret, A. Higuchi, A. Sudbery J. Math. Phys. **41**, 7932, (2000), quant-ph/0006125.
[4] V. Coffman, J. Kundu, W. K. Wootters Phys. Rev. A **61**, 2306 (2000), quant-ph/9907047.
[5] P. L. Dressel. Ann. Math. Stat. **11**, 33-57, (1940).
[6] R. A. Fisher, Proc. London Math. Soc. Ser. 2 **30**, 199 (1929).
[7] R. A. Fisher and J. Wishart, Proc. London Math. Soc. Ser. 2 **33**, 195 (1931).
[8] M. Grassl, M. Rötteler, T. Beth. Phys. Rev. A **58**, 1833 (1998).
[9] M. Grassl Transparencies of a talk. Joint work with T. Beth, M.Rötteler, Y. Makhlin. http://iaks-www.ira.uka.de/home/grassl/paper/MSRI_InvarTheory.pdf
[10] R.-J. Gu, F.-L. Zhang, S.-M. Fei, J.-L. Chen quant-ph/0912.1085 (2009).
[11] M. Kendall and A. Stuart, *The advanced theory of statistics, Volume 1* (Charles Griffin, London and High Wycombe, 1977).
[12] M. Koashi, A. Winter Phys. Rev. A **69**, 022309 (2004), quant-ph/0310037.
[13] B. Kraus, Phys. Rev. Lett. **104**, 020504 (2010), quant-ph/0909.5152.
[14] B. Kraus, quant-ph/1005.5995 (2010).
[15] M.S. Leifer, N. Linden, A. Winter. Phys. Rev. A **69**,052304 (2004), quant-ph/0308008.
[16] N, Linden and S. Popescu, Fortschritte Der Physik **46**, 567, (1998), quant-ph/9711016.
[17] J.-G. Luque, J.-Y. Thibon, F. Toumazet Math. Struct. in Comp. Science, **17**, 1133-1151, quant-ph/0604202.
[18] A. Miyake Phys. Rev. A (3) **67**, 012108 (2003), quant-ph/0206111.
[19] P. J. Olver, Classical Invariant Theory, CUP (1999).
[20] E.M. Rains. IEEE Trans. Inf. Theory **46**,54 (2000), quant-ph/9704042.
[21] A. Royer, J. Math. Phys. **24**, 897 (1983).
[22] A. Sawicki, M. Kuś, (2010) quant-ph/1009.0293.
[23] A. Sudbery J. Phys. A.: Math. Gen. **34**, 642-652 (2001), quant-ph/0001116.
[24] A. Sudbery Solution of R. Werner's Open Problem number 3 (2001). http://www.imaph.tu-bs.de/qi/problems/3.html
[25] T. N. Thiele *The Theory of Observations* (C & E Layton, London, 1903).
[26] T. N. Thiele, Ann. Math. Stat. Vol. 2, No. 2, p. 165-308 (1931).
[27] D. L. Zhou, B. Zeng, Z. Xu, L. You, Phys. Rev. A **74**, 052110 (2006) also quant-ph/0608240.

VIII. APPENDIX

A. An alternative cumulant-based invariant

There is a very different way of relating cumulants and invariants, due to Zhou et al. [27]. Given an n-party mixed state ρ, one defines its cumulant by analogy with (18) as

$$\rho_c = \sum_{\pi} (-1)^{|\pi|-1}(|\pi|-1)! \bigotimes_{i=1}^{|\pi|} \rho_{\pi_i}, \tag{59}$$

where ρ_{π_i} is the result of tracing out from ρ all systems apart from those with labels in π_i. For instance, for three systems

$$\rho_c = \rho - (\rho_1 \otimes \rho_{23} + \rho_2 \otimes \rho_{13} + \rho_3 \otimes \rho_{12}) + 2\rho_1 \otimes \rho_2 \otimes \rho_3.$$

The cumulant operator given by (59) is not in general a state, but Zhou et al. propose $M(\rho) = \frac{1}{2}\mathsf{tr}|\rho_c|$ as a measure of correlation of the mixed state ρ. It is manifestly invariant under local unitaries, and, because of the general property cumulants have of vanishing on products, $M(\rho) = 0$ whenever $\rho = \rho_S \otimes \rho_T$. For pure states, this means it vanishes when states are separable.

It therefore seems to have formal similarities to our cumulant-based invariants, and one can carry this further by defining, in line with Proposition V.3, the lift of M to be $M(\mathsf{tr}|\psi\rangle\langle\psi|)$. We can in fact adopt parallel notation to the I's, writing, for a 3-qubit state for example, $M_{111}(|\psi\rangle) = \frac{1}{2}\mathsf{tr}|\left(|\psi\rangle\langle\psi|\right)_c|$, $M_{110}(|\psi\rangle) = \frac{1}{2}\mathsf{tr}|\left(\mathsf{tr}_3|\psi\rangle\langle\psi|\right)_c|$, and so on. Then $M_{i_1\ldots i_n}(|\psi\rangle) = 0$ for any π-separable $|\psi\rangle$ where $\{i_1 \ldots i_n\}$ splits π. Furthermore, for 3-qubit states $M_{111}(|\psi\rangle) = 0$ is sufficient for separability of $|\psi\rangle$ ([27], Theorem 3), and the same is true if $I_{111}(|\psi\rangle) = 0$.

These similarities prompt the question of whether there is a functional connection. Can one write $M_{i_1\ldots i_n}(|\psi\rangle) = F(I_{i_1\ldots i_n}(|\psi\rangle))$, for some function F? For 2-qubit states, $M_{11} = I_{11} + \sqrt{I_{11}}$. However, there is only one 2-qubit invariant for normalised states, so a functional relationship here is unsurprising. For 3-qubit states of the form $|\psi\rangle = a|000\rangle + b|111\rangle$ one finds

$$M_{111} = 6I_{111}\sqrt{1 - 4I_{111}} + 2\sqrt{I_{111} + I_{111}^2 - 4I_{111}^3}, \tag{60}$$

whereas, for states of the form $|\phi\rangle = a|100\rangle + b|010\rangle + c|001\rangle$

$$(M_{111} - \frac{I_{111}}{2})^3 - \frac{1}{4}I_{111} = 0. \tag{61}$$

Since (60) and (61) do not define the same function of I_{111}, M_{111} must depend on other invariants besides I_{111}.