Canonical Decompositions of n-qubit Quantum Computations and Concurrence

Stephen S. Bullock

Mathematical and Computer Sciences Division, National Institute of Standards and Technology, Gaithersburg, MD, 20089 [*]

Gavin K. Brennen

Quantum Processes Group, National Institute of Standards and Technology, Gaithersburg, MD, 20089[†]

The two-qubit canonical decomposition $SU(4) = [SU(2) \otimes SU(2)]\Delta[SU(2) \otimes SU(2)]$ writes any two-qubit unitary operator as a composition of a local unitary, a relative phasing of Bell states, and a second local unitary. Using Lie theory, we generalize this to an n-qubit decomposition, the concurrence canonical decomposition (CCD) $SU(2^n) = KAK$. The group K fixes a bilinear form related to the concurrence, and in particular any unitary in K preserves the tangle $|\overline{\langle\phi|}(-i\sigma_1^y)\cdots(-i\sigma_n^y)|\phi\rangle|^2$ for n even. Thus, the CCD shows that any n-qubit unitary is a composition of a unitary operator preserving this n-tangle, a unitary operator in A which applies relative phases to a set of GHZ states, and a second unitary operator which preserves the tangle.

As an application, we study the extent to which a large, random unitary may change concurrence. The result states that for a randomly chosen $a \in A \subset SU(2^{2p})$, the probability that a carries a state of tangle 0 to a state of maximum tangle approaches 1 as the even number of qubits approaches infinity. Any $v = k_1 a k_2$ for such an $a \in A$ has the same property. Finally, although $|\overline{\langle\phi|}(-i\sigma_1^y)\cdots(-i\sigma_n^y)|\phi\rangle|^2$ vanishes identically when the number of qubits is odd, we show that a more complicated CCD still exists in which K is a symplectic group.

I. INTRODUCTION

Entanglement is a unique feature of quantum systems that plays a key role in quantum information proccessing. Much effort has gone into describing the entanglement present in the state of a quantum system composed of two or more measurably distinct subsystems. Because different amounts of entanglement may be shared among the various partitions of the tensor factors of the Hilbert state space, there is no single measure of entanglement that captures all non-local correlations for many-particle systems. Rather, the number of partitions of the tensor factors grows exponentially with the number of factors themselves. Thus, it is reasonable to guess that same is true for the number of useful entanglement measures. In fact, the situation is yet more complicated. Many reasonable definitions create uncountably many entanglement types, which thus may not be associated to countable collections of partitions or monotones.

Nevertheless, it is interesting to consider how much entanglement is created by a given unitary evolution U of an n-qubit state space. To achieve this in a limited context, we focus on a single multi-qubit entanglement measure, the n-concurrence (1). Using Lie theory, we may decompose a unitary operator acting on n qubits into a form such that the entangling power of the unitary with respect to this measure is manifest.

The n-tangle and its square root, the n-concurrence, are two of several proposed multiqubit entanglement measures. Others include polynomial invariants which involve moments of the reduced state eigenvalues (2), the Schmidt measure (3) which is related to the minimum number of terms in the product state expansion of a state, the Q measure (4) which is related to the average purity each qubit's reduced state, and **GAVIN ADDS SOMETHING.** (5) A further measure makes use of hyperdeterminants (6); this powerful technique makes computation difficult in more than six qubits. The *concurrence* C_n is originally introduced in the two-qubit case (7). It is generalized to a measure on two systems of arbitrarily many dimensions in (8) and extends to n-qubits (1).

We now consider the quantitative expression for the concurrence. Suppose a quantum state space of data for

[*]Electronic address: stephen.bullock@nist.gov
[†]Electronic address: gavin.brennen@nist.gov

a quantum computer. Specifically, fix n as the number of qubits, $N = 2^n$. Throughout, we use $|j\rangle$ not to denote the state of a qudit but rather as an abbreviated multi-qubit state via binary form. For example, in three qubits $|5\rangle = |101\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle$. We write $\mathcal{H}_n = \mathrm{span}_{\mathbb{C}}\{|j\rangle\ ;\ 0 \le j \le N-1\}$ for the n-qubit Hilbert state space. Then the concurrence is a map $C_n : \mathcal{H}_n \to [0,\infty)$ given by $C_n(|\psi\rangle) = |\overline{\langle\psi|}(-i\sigma_1^y)\cdots(-i\sigma_n^y)|\psi\rangle|$. Note that the expression inside the complex norm is in general not real. A related entanglement measure $\tau_n = C_n^2$ is known as the *n-tangle* when n is even [1]. For $\langle\psi|\psi\rangle = 1$, the n-tangle of a state $|\psi\rangle$ assumes real values in the range $0 \le \tau_n \le 1$. It is moreover an entanglement monotone (9), as any good measure should be. This means in particular that $\tau_n : \mathcal{H}_n \to [0,\infty)$ vanishes on full tensor products of local states, and moreover that $\tau_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n|\psi\rangle) = \tau_n(|\psi\rangle)$ for any $v_1 \otimes v_2 \otimes \cdots \otimes v_n \in \otimes_1^n SU(2)$. We show in Appendix C that the n-concurrence is also an entanglement monotone.

The n-concurrence only detects certain kinds of entanglement. Specifically, while it returns zero on all separable states, it may also return zero on certain non-separable states. We illustrate the monotone's behavior by example. First, the n-partite Greenberger-Horne-Zeilinger (GHZ) state $|GHZ_n\rangle = (1/\sqrt{2})(|0_1 \ldots 0_n\rangle + |1_1 \ldots 1_n\rangle)$ has maximal n-concurrence while $C_n(|GHZ_{n-1}\rangle \otimes |0\rangle_n) = 0$. As a second example, the generalized $|W\rangle$ state given by $|W\rangle = (1/\sqrt{n})(|10\ldots0\rangle + |010\ldots0\rangle + \cdots + |0\ldots01\rangle)$ has zero n-concurrence despite being entangled. States with subglobal entanglement can also assume maximal n-concurrence; $C_n(|GHZ_n\rangle) = C_n(|GHZ_{n/2}\rangle \otimes |GHZ_{n/2}\rangle) = 1$. Generally, the n-concurrence seeks out superpositions between a state and its binary bit flip.

We extend these definitions by introducing a complex bilinear form, the *concurrence form* $\mathcal{C}_n : \mathcal{H}_n \times \mathcal{H}_n \to \mathbb{C}$. Here, complex bilinear means the function is linear when restricted to each variable. The antisymmetric concurrence form $\mathcal{C}_n(-,-)$ is nonzero even in the case n is odd, although of course $C_{2p-1} \equiv 0$ since $\mathcal{C}_{2p-1}(|\psi\rangle, |\psi\rangle) = -\mathcal{C}_{2p-1}(|\psi\rangle, |\psi\rangle) = 0$.

Definition I.1 The concurrence form $\mathcal{C}_n : \mathcal{H}_n \times \mathcal{H}_n \to \mathbb{C}$ is given by $\mathcal{C}_n(|\psi\rangle, |\phi\rangle) = \overline{\langle\psi|}(-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y)|\phi\rangle$. Note the complex conjugation of the lead bra is required for complex linearity (rather than antilinearity) in the first variable. The concurrence quadratic form is $Q_n^C(|\psi\rangle) = \mathcal{C}_n(|\psi\rangle, |\psi\rangle)$, so that $C_n(|\psi\rangle) = |Q_n^C(|\psi\rangle)| = \sqrt{\tau_n(|\psi\rangle)}$. Note that Q_n^C is a complex quadratic polynomial on the vector space $\mathcal{H}_n$.

The main technique of this paper is to build a new matrix decomposition of the Lie group of global phase normed quantum computations $SU(N)$. It is optimized for the study of the concurrence and n-tangle and generalizes the two-qubit canonical decomposition (10; 11; 12; 13; 14; 15)

$$SU(4) = [SU(2) \otimes SU(2)]\Delta[SU(2) \otimes SU(2)] \tag{1}$$

Here, the commutative group Δ applies relative phases to a "magic basis" (7; 12; 13; 14; 16) of phase-shifted Bell states. This two-qubit canonical decomposition is used to the study of the entanglement capacity of two-qubit operations (15), to building efficient (small) circuits in two qubits (14; 17; 18), and to classify which two-qubit unitary operators require fewer than average multiqubit interactions (17; 18).

The canonical decomposition is itself an example of the $G = KAK$ metadecomposition theorem of Lie theory (19, thm8.6,§VII.8). This theorem produces a decomposition of an input semisimple Lie group G given two further inputs:

- a Cartan involution (19, §X.6.3,pg.518) $\theta : \mathfrak{g} \to \mathfrak{g}$ for $\mathfrak{g} = \mathrm{Lie}(G)$. By definition, θ satisfies (i) $\theta^2 = \mathbf{1}$ and (ii) $\theta[X,Y] = [\theta X, \theta Y]$ for all $X, Y \in \mathfrak{g}$. We write $\mathfrak{g} = \mathfrak{p} \oplus \mathfrak{k}$ for the decomposition of $\mathfrak{g}$ into the $+1$ and -1 eigenspace of θ.
- a commutative subalgebra $\mathfrak{a} \subset \mathfrak{p}$ which is maximal commutative in $\mathfrak{p}$.

Then write $K = \exp \mathfrak{k}$, $A = \exp \mathfrak{a}$, where for linear $G \subset GL(n,\mathbb{C})$ the exponential coincides with the matrix power series on each of the Lie subalgebras $\mathfrak{k}$, $\mathfrak{a}$. The theorem asserts then that $G = KAK = \{k_1 a k_2\ ;\ k_1, k_2 \in K, a \in A\}$.

For example, the cononical decomposition of $SU(4)$ arises as follows. Take $\theta : \mathfrak{su}(4) \to \mathfrak{su}(4)$ by $\theta(X) = (-i\sigma_1^y)(-i\sigma_2^y)\bar{X}(-i\sigma_1^y)(-i\sigma_2^y)$ and

$$\mathfrak{a} = \mathrm{span}_{\mathbb{R}}\left\{\ i|0\rangle\langle 0| - i|1\rangle\langle 1| - i|2\rangle\langle 2| + i|3\rangle\langle 3|,\ i|0\rangle\langle 3| + i|3\rangle\langle 0|,\ i|1\rangle\langle 2| + i|2\rangle\langle 1|\ \right\} \tag{2}$$

[1] It is not clear how to recover the celebrated 3-tangle from this construction. By this definition we will see that $\tau_n \equiv 0$ for all odd n, so references to τ_n in the present paper will suppose that is not the case.

We extend this particular construction to n-qubits.

Definition I.2 Let $S = (-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y)$. Define $\theta : \mathfrak{su}(2^n) \to \mathfrak{su}(2^n)$ by $\theta(X) = S^{-1}\bar{X}S = (-1)^n S\bar{X}S$. Then $\mathfrak{k}$ denotes the $+1$-eigenspace of θ while $\mathfrak{p}$ denotes the -1-eigenspace. Finally, in case n is even we define

$$\begin{aligned}\mathfrak{a} \;=\; & \mathrm{span}_{\mathbb{R}}\big(\{\, i|j\rangle\langle j| + i|N-j-1\rangle\langle N-j-1| - i|j+1\rangle\langle j+1| - i|N-j-2\rangle\langle N-j-2|\,;\; 0 \le j \le 2^{n-1}-2 \,\} \\ & \sqcup \quad \{\, i|j\rangle\langle N-j-1| + i|N-j-1\rangle\langle j|\,;\; 0 \le j \le 2^{n-1}-1 \,\},\big) \text{ in case } n \text{ even}\end{aligned} \tag{3}$$

with $A = \exp \mathfrak{a}$. In case n odd, we drop the second set:

$$\begin{aligned}\mathfrak{a} \;=\; & \mathrm{span}_{\mathbb{R}}\big(\{\, i|j\rangle\langle j| + i|N-j-1\rangle\langle N-j-1| - i|j+1\rangle\langle j+1| - i|N-j-2\rangle\langle N-j-2|\,;\; 0 \le j \le 2^{n-1}-2 \,\}\big) \\ & \text{in case } n \text{ odd}\end{aligned} \tag{4}$$

Modulo checks reserved for the body, the *concurrence canonical decomposition (*`CCD`*)* in n-qubits is the resulting matrix decomposition $SU(2^n) = KAK$. Note that n may be even or odd.

In n-qubits, it is certainly *not* the case that K is the Lie group of local unitaries. Nonetheless, we prove momentarily by direct computation that the local unitary group $SU(2)\otimes SU(2)\otimes\cdots\otimes SU(2) \subset K$, with strict containment in $n \ge 3$ qubits by a dimension count. Moreover, for $n = 2p$ an even number of qubits the concurrence canonical decomposition is computable via an algorithm familiar from the two-qubit case (14), (see Appendix A). The following theorem provides the key to interpreting this extended canonical decomposition.

Theorem I.3 *Let $K = \exp \mathfrak{k}$ for $\mathfrak{k}$ the $+1$-eigenspace of the Cartan involution $\theta(X) = S^{-1}\bar{X}S$. Then K is the* symmetry group of the concurrence form $\mathcal{C}_n$. *Specifically, for $u \in SU(N)$,*

$$(u \in K) \Longleftrightarrow \big[\;\; \mathcal{C}_n(u|\phi\rangle, u|\psi\rangle) = \mathcal{C}_n(|\phi\rangle, |\psi\rangle) \quad \text{for every } |\phi\rangle, |\psi\rangle \in \mathcal{H}_n\big] \tag{5}$$

Moreover, for n even the concurrence form is symmetric. In the even case, it restricts to the usual dot product on the $\mathbb{R}$-span of a collection of n concurrence one states, and this $\mathbb{R}$ subspace of $\mathcal{H}_n$ is preserved by K. On the other hand, for n odd $\mathcal{C}_n$ is antisymmetric, i.e. a two-form. Thus,

- *$K \cong Sp(N/2)$, if n is an odd number of qubits*
- *$K \cong SO(N)$, if n is an even number of qubits*

Remark I.4 Bremner et al (20, thm5) observe symplectic Lie algebras independently in a context related to the above. We explore this in more detail in a sequel manuscript. $\diamond$

This interpretation allows for an extension of prior work on the entangling capacity of two-qubit unitaries (15). Here is the precise result:

Definition I.5 The *concurrence capacity* of a given n-qubit unitary operator $v \in SU(N)$ is defined by $\kappa(v) = \max\{C_n(v|\psi\rangle)\,;\, C_n(|\psi\rangle) = 0, \langle\psi|\psi\rangle = 1\}$.

Corollary I.6 (of I.3) *Let $u = k_1 a k_2$ be the n-qubit canonical decomposition of $u \in SU(N)$. Then $\kappa(u) = \kappa(a)$.*

Given the `CCD`, the function κ is properly viewed as a function on the A factor rather than on the entire group of phase-normalized unitaries $SU(N)$. Finally, a careful analysis of $\kappa(a)$ for randomly chosen a in A produces the following, perhaps surprising result.

Theorem I.7 *Suppose the number of qubits is even, i.e. $n = 2p$. Then for large p almost all $a \in A$ have maximal concurrence capacity. Specifically, suppose we choose $a \in A$ at random per the probability density function given by the unit normalized Haar measure da. Then*

$$lim_{p\to\infty} Probability[\kappa(a) = 1] \;=\; lim_{p\to\infty}\, da(\{a \in A\,;\, \kappa(a) = 1\}) \;=\; 1 \tag{6}$$

We rephrase this result colloquially. Suppose we think of those states $|\psi\rangle$ in even qubits with $\tau_n(|\psi\rangle) = 1$ as `GHZ`-like. Then as the even number of qubits grows large, almost every unitary evolution will be able to produce such a maximally concurrent `GHZ`-like state from some input state of 0 concurrence.

Notation and Contents

We provide some samples of our notation for the reader's convenience. Throughout, n is a number of qubits and $N = 2^n$. For $v = \sum_{j,k=0}^{N-1} v_{j,k}|k\rangle\langle j|$, we have the adjoint $v^\dagger = \sum_{j,k=0}^{N-1} \overline{v}_{k,j}|k\rangle\langle j|$. We also require the transpose operation, most easily visualized in matrix form as $(v_{j,k})^T = (v_{k,j})$. Equivalently, $v^T = \sum_{j,k=0}^{N-1} v_{j,k}|j\rangle\langle k|$. Thus $v^\dagger = \overline{v}^T$. Recall also the convention of collapsing the binary for an integer inside the ket of a computational basis state. We use lower rather than upper case letters for most operators to avoid confusing them with Lie groups denoted by capital letters. The older term *scholium* is used to refer to a corollary of the proof of a theorem or proposition rather than its formal statement. Besides these conventions, we follow the notations of either (21) or (19).

The paper is structured as follows. In §II, we verify that the conventions are Definition I.2 are appropriate for invoking the $G = KAK$ theorem. Having verified that the matrix decomposition exists, §II further describes *entanglers* and *finaglers*, loosely similarity matrices which rotate the `CCD` onto more standard KAK decompositions of $SU(N)$. In §III, we discuss the concurrence capacity and prove the properties of this capacity asserted above. The three appendices consecutively (i) provide an algorithm for computing the `CCD` given a matrix $v \in SU(N)$, exclusively in the case n is even, (ii) argue that any two normalized states $|\phi\rangle$, $|\psi\rangle$ with identical concurrence must have $k|\phi\rangle = |\psi\rangle$ for some k in the symmetry group K, and (iii) prove that the concurrence $C_n(-)$ is an entanglement monotone.

II. ENTANGLERS, FINAGLERS, AND CARTAN INVOLUTIONS OF $\mathfrak{su}(N)$

This section has two goals. First, we show our KAK decomposition is well-defined, by noting that θ is a Cartan involution, checking by direct computation that $\mathfrak{a}$ is abelian, and arguing that $\mathfrak{a}$ is maximal commutative. Second, we prove Theorem I.3. There are generally two approaches to the theorem. We could recall standard Cartan involutions and KAK decompositions from the literature. We will shortly construct similarity matrices E_0 and F_0 which rotate the standard $G = KAK$ decompositions of $SU(N)$ onto the `CCD`, and we could simply appeal to these matrices and the standard structures. Alternately, (many) intrinsic computations would suffice to check the required properties for $G = KAK$. The present approach is a compromise. The argument that the `CCD` $SU(N) = KAK$ is well-defined is intrinsic, except for a single appeal to classification. On the other hand, the classification of the K groups uses similarity matrices. As such, it is ultimately a change of basis in the n-qubit state space $\mathcal{H}_n$.

Properties of the `CCD` $SU(N) = KAK$

The following proposition is not used in the sequel. However, we include a direct proof due to its importance in guiding the choice of θ. It simplifies an older argument and arose from correspondence with P.Zanardi.

Proposition II.1 *Let K be as in Definition I.2. Then there is an inclusion $SU(2) \otimes SU(2) \otimes \cdots \otimes SU(2) \subset K$.*

Proof: Recall $i\sigma^x = i|0\rangle\langle 1| + i|1\rangle\langle 0|$, $i\sigma^y = |0\rangle\langle 1| - |1\rangle\langle 0|$, and $i\sigma^z = i|0\rangle\langle 0| - i|1\rangle\langle 1|$ forms a basis of $\mathfrak{su}(2^1)$. For the statement of the proposition, it suffices to check $\mathrm{Lie}[\otimes_1^n SU(2)] = \mathrm{span}\{i\sigma_j^x, i\sigma_j^y, i\sigma_j^z\ ;\ 1 \le j \le n\} \subset \mathfrak{k}$. We further recall the last item of Lemma II.2, as well as the fact that the complex conjugates of the Pauli matrices are $\overline{i\sigma^x} = -i\sigma^x$, $\overline{i\sigma^y} = i\sigma^y$, and $\overline{i\sigma^z} = -i\sigma^z$. Then we wish to show that θ fixes every σ_j^x, σ_j^y, and σ_j^z. For this,

$$\begin{array}{rclclcl}
(-1)^n\, S\, \overline{(i\sigma_j^x)}\, S &=& (-1)^n S\, (-i\sigma_j^x)\, S &=& (-1)^n S^2\, (i\sigma_j^x) &=& (i\sigma_j^x) \\
(-1)^n\, S\, \overline{(i\sigma_j^y)}\, S &=& (-1)^n S\, (i\sigma_j^y)\, S &=& (-1)^n S^2\, (i\sigma_j^y) &=& (i\sigma_j^y) \\
(-1)^n\, S\, \overline{(i\sigma_j^z)}\, S &=& (-1)^n S\, (-i\sigma_j^z)\, S &=& (-1)^n S^2 (i\sigma_j^z) &=& (i\sigma_j^z)
\end{array}$$

Hence each such infinitesimal unitary is in the $+1$ eigenspace of θ. This concludes the proof. □

We next note that θ is a Cartan involution. Indeed, direct computation shows that $\theta^2 = \mathbf{1}$. Moreover,

$$[\theta X, \theta Y] = (S^{-1}\overline{X}S)(S^{-1}\overline{Y}S) - (S^{-1}\overline{Y}S)(S^{-1}\overline{X}S) = S^{-1}\overline{(XY - YX)}S = \theta[X,Y]. \tag{7}$$

Thus we need the following to complete the argument that $SU(N) = KAK$ of Definition I.2 is well-defined: (i) $\mathfrak{a} \subset \mathfrak{p}$, (ii) $\mathfrak{a}$ is commutative, and (iii) no larger subalgebra of $\mathfrak{p}$ containing $\mathfrak{a}$ is commutative.

Lemma II.2 *Let $S = (-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y)$ be as in Definition I.2. Then (i) $S|j\rangle = (-1)^{\#j}|N-j-1\rangle$, (ii) $\langle j|S = (-1)^{n-\#j}\langle N-j-1|$, and (iii) $S\sigma_j^x = -\sigma_j^x S$, $S\sigma_j^y = \sigma_j^y S$, and $S\sigma_j^z = -\sigma_j^z S$. Note that (ii) refers to a composition of linear maps.*

Sketch: For (i), compute. For (ii), consider $\langle j|S|k\rangle$ for $|k\rangle$ varying over all computational basis states. Then apply (i) for (ii). For (iii), nonlike Pauli matrices anticommute, while S itself is a tensor. □

Lemma II.3 *Let $\mathfrak{a}$ be as in Definition I.2. Then $\mathfrak{a} \subset \mathfrak{p}$.*

Proof: There are two coordinate computations to complete in this case. For the first, momentarily extend the definition of θ to $\tilde{\theta}$ acting on $\mathfrak{u}(N)$ by the same formula. Then

$$\begin{aligned}
\tilde{\theta}[\, i|j\rangle\langle j| + i|N-j-1\rangle\langle N-j-1|\,] &= (-1)^n S(\,-i|j\rangle\langle j| - i|N-j-1\rangle\langle N-j-1|\,)S \\
&= (-1)^{n+1} i[\,(-1)^n|N-j-1\rangle\langle N-j-1| + (-1)^n|j\rangle\langle j|\,] \\
&= -i|j\rangle\langle j| - i|N-j-1\rangle\langle N-j-1|
\end{aligned}$$

Thus $i|j\rangle\langle j| + i|N-j-1\rangle\langle N-j-1|$ is in the -1-eigenspace of $\tilde{\theta}$, so that the elements of the first set of the definition of $\mathfrak{a}$ are contained in $\mathfrak{p}$. For the second basis set in case n even,

$$\begin{aligned}
\theta[\, i|j\rangle\langle N-j-1| + i|N-j-1\rangle\langle j|\,] &= S[\,(-i)|j\rangle\langle N-j-1| + (-i)|N-j-1\rangle\langle j|\,]S \\
&= [\,(-1)^{\#j+[n-(n-\#j)]}(-i)|N-j-1\rangle\langle j| \\
&\qquad + (-1)^{n-\#j+(n-\#j)}(-i)|j\rangle\langle N-j-1|\,] \\
&= (-i)|N-j-1\rangle\langle j| + (-i)|j\rangle\langle N-j-1|
\end{aligned}$$

Thus $i|j\rangle\langle N-j-1| + i|N-j-1\rangle\langle j| \in \mathfrak{p}$, in case n even. □

Proposition II.4 *Recall $\mathfrak{a}$ from Definition I.2. Then $\mathfrak{a}$ is commutative.*

Proof: Throughout, $0 \le j,k \le N/2-1$, $N = 2^n$. The following three computations of Lie brackets suffice.

$$\begin{aligned}
&[\ i|j\rangle\langle j| + i|N-j-1\rangle\langle N-j-1|\ ,\ i|k\rangle\langle k| + i|N-k-1\rangle\langle N-k-1|\ ] = \\
&\quad -|j\rangle\langle j|k\rangle\langle k| - |N-j-1\rangle\langle N-j-1|N-k-1\rangle\langle N-k-1| + \\
&\qquad |k\rangle\langle k|j\rangle\langle j| + |N-k-1\rangle\langle N-k-1|N-j-1\rangle\langle N-j-1|
\end{aligned}$$

$$\begin{aligned}
&[\ (-i)^{n+1}|j\rangle\langle N-j-1| + i^{n-1}|N-j-1\rangle\langle j|\ ,\ (-i)^{n+1}|k\rangle\langle N-k-1| + i^{n-1}|N-k-1\rangle\langle k|\ ] = \\
&\quad -|j\rangle\langle N-j-1|N-k-1\rangle\langle k|\ - |N-j-1\rangle\langle j|k\rangle\langle k| \\
&\qquad +|k\rangle\langle N-k-1|N-j-1\rangle\langle j|\ + |N-k-1\rangle\langle k|j\rangle\langle N-j-1|
\end{aligned}$$

$$\begin{aligned}
&[\ i|j\rangle\langle j| + i|N-j-1\rangle\langle N-j-1|\ ,\ (-i)^{n+1}|k\rangle\langle N-k-1| + i^{n-1}|N-k-1\rangle\langle k|\ ] = \\
&\quad (-i)^n|j\rangle\langle j|k\rangle\langle N-k-1|\ +\ i^n|N-j-1\rangle\langle N-j-1|N-k-1\rangle\langle k| \\
&\qquad -(-i)^n|k\rangle\langle N-k-1|N-j-1\rangle\langle N-j-1|\ -\ i^n|N-k-1\rangle\langle k|j\rangle\langle j|
\end{aligned}$$

Each of the final expressions is zero in case $j \neq k$ and also zero in case $j = k$. Thus, $\mathfrak{a}$ is commutative. □

The arguments above almost complete the proof that the CCD $SU(N) = KAK$ is well-defined. In the abstract, one also needs a fairly large coordinate computation which verifies $\mathfrak{a}$ is maximal commutative. This would verify that for any $X \in \mathfrak{p}$ with $[X,H] = 0$ for all $H \in \mathfrak{a}$, one must in fact have $X \in \mathfrak{a}$.

Rather than complete that task, we instead appeal to the Cartan classification (19, pg.518,tableV). Ostensibly a classification of globally symmetric spaces, this classification also describes all possible Cartan involutions of any real semisimple group G up to Lie isomorphism. For $G = SU(N)$, there are three overall possibilities grouped as type **AI**, **AII**, and **AIII**. For each, the *rank* refers to the dimension of any maximal commutative subalgebra $\mathfrak{a}$ of $\mathfrak{p}$. This dimension may not vary by subalgebra, since any two such $\mathfrak{a}_1$, $\mathfrak{a}_2$ must have $k\mathfrak{a}_1 k^{-1} = \mathfrak{a}_2$ for some $k \in K$. We now excerpt from the table the possibilities for $G = SU(N)$:

type	domain $\mathfrak{g}$ of $\theta : \mathfrak{g} \to \mathfrak{g}$	isomorphism representative of K	rank
AI	$\mathfrak{su}(N)$	$SO(N)$	$N-1$
AII	$\mathfrak{su}(N)$	$Sp(N/2)$	$N/2-1$
AIII	$\mathfrak{su}(N)$	$S[U(p)\oplus U(q)], p+q=N$	$\min(p,q)$

Suppose then for the moment that the number of qubits n is even. No type **AIII** Cartan involution admits an $\mathfrak{a}$ of dimension $N-1$. Indeed, if $p+q=N$, then $\min(p,q) \le N/2 < N-1$. The same is true of type **AII** involutions, i.e. $N-1 > N/2-1$. Hence we see that A must be maximal, and for n even the Cartan involution θ must have type **AI**.

What remains is to prove that $\mathfrak{a}$ is maximal in $\mathfrak{p}$ in case n odd. This follows by a dimension count *if* the Cartan involution is type **AII**. We thus postpone noting this point until after the proof of Theorem I.3. See Remark II.19.

As an aside, type **AIII** involutions do not appear in this work but have been used in quantum circuit design. Indeed, the CS-decomposition (22; 23) is an example of a KAK decomposition arising from a type **AIII** involution. Elements within the appropriate K group may be interpreted as products of computations on the last $n-1$ lines with computations on these lines controlled on the first qubit.

Entanglers

In the two-qubit case, the following computation E has the following property:

$$E = (1/\sqrt{2}) \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 0 & 1 & i \\ 0 & 0 & -1 & i \\ 1 & -i & 0 & 0 \end{pmatrix} \text{ satisfies } E^\dagger [SU(2)\otimes SU(2)] E = SO(4) \tag{8}$$

Using more Lie theory terminology, recall the adjoint representation of G on $\mathfrak{g}$ given by $\mathrm{Ad}(g)[X] = gXg^{-1}$. Then we may restate $\{\mathrm{Ad}(E^\dagger)\}[SU(2)\otimes SU(2)] = SO(4)$. This provides a physical interpretation for the low dimensional isomorphism $\mathfrak{su}(2)\oplus\mathfrak{su}(2) \cong \mathfrak{so}(4)$. We would like entanglers for the concurrence canonical decomposition.

Definition II.5 Let $\theta_{\mathbf{AI}} : \mathfrak{su}(2^n) \to \mathfrak{su}(2^n)$ denote the usual type **AI** Cartan involution $\theta_{\mathbf{AI}}(X) = \bar{X}$ associated to $SO(N) \subset SU(N)$. We say $E \in SU(2^n)$ is an entangler iff the following diagram commutes:

$$\begin{array}{ccccc} & \mathfrak{su}(N) & \xrightarrow{\theta_{\mathbf{AI}}} & \mathfrak{su}(N) & \\ \mathrm{Ad}(E) & \downarrow & & \downarrow & \mathrm{Ad}(E) \\ & \mathfrak{su}(N) & \xrightarrow{\theta} & \mathfrak{su}(N) & \end{array} \tag{9}$$

In particular as both groups are connected, we must have $\mathrm{Ad}(E)[SO(N)] = K$.

We next prove the surprising fact that there are no entanglers when n is odd. For this, we need to recall the central subgroup $\mathcal{Z}[SU(N)] = \{v \in SU(N)\ ;\ vuv^\dagger = u \text{ for all } u \in SU(N)\}$. The center is in fact the set of all phase computations corresponding to the N^{th} roots of unity:

$$\mathcal{Z}[SU(N)] = \{\xi\mathbf{1}\ ;\ \xi^N = 1\} \quad (19, \text{pg.310,516}) \tag{10}$$

With this fact recalled from the literature, we have the following lemma.

Lemma II.6 *Suppose that for $v \in SU(N)$, $[Ad(v)](X) = vXv^\dagger = X$ for every $X \in \mathfrak{su}(N)$. Then $v = \xi\mathbf{1}$ for some $\xi \in \mathbb{C}$ with $\xi^N = 1$. (Hence $\xi = e^{2\pi i k/N}, 0 \le k \le N-1$.)*

Proof: Recall that $\exp : \mathfrak{su}(N) \to SU(N)$ is onto. Thus each $u \in SU(N)$ may be written as $\exp X$ for some X. Thus, consider the one-parameter-subgroup (19, pg.104) $\gamma : \mathbb{R} \to SU(N)$ given by $t \mapsto v[\exp(tX)]v^\dagger$. This has derivative $\frac{d\gamma}{dt}|_{t=0} = vXv^\dagger = X$, and by uniqueness of one-parameter-subgroups (19, pg.103,Cor.1.5) $v\exp(tX)v^\dagger = \exp(tX)$ for all t. Taking $t=1$, we see $vuv^\dagger = u$ for a generic $u \in SU(N)$. $\square$

Proposition II.7 *If the number of qubits n is odd, then there does not exist an entangler $E \in U(N)$.*

Proof: Assume by way of contradiction that there does exist an entangler E for n odd. Then for all $X \in \mathfrak{su}(N)$, we have the following equation.

$$(EE^T)\bar{X}(EE^T)^\dagger \;=\; E\,\theta_{\mathbf{AI}}[E^\dagger X E]\,E^\dagger \;=\; \theta(X) \;=\; S\bar{X}S^{-1} \tag{11}$$

Since we may vary $Y = \bar{X}$ over $\mathfrak{su}(N)$ as well, this implies that $S^{-1}EE^T$ satisfies the hypothesis of Lemma II.6. Thus $S^{-1}EE^T = \xi\mathbf{1}$ for $\xi^N = 1$ or $EE^T = (\xi\mathbf{1})S$. Contradiction, for EE^T is always a complex symmetric matrix while $(\xi\mathbf{1})S$ is not a complex symmetric matrix when n is odd. □

Scholium II.8 *For an even number of qubits n, the matrix $E \in U(N)$ is an entangler iff $EE^T = (\xi\mathbf{1})S$, where $\xi^N = 1$.*

There are many possible entanglers. Indeed, even in two-qubits other choices have been used (10; 15). One possibility given n even is to take the $n/2$ fold tensor product $E \otimes E \otimes \cdots \otimes E$. However, we prefer the following choice as a standard instead, since it highlights the mapping of the computational basis to Greenberger-Horne-Zeilinger states.

Definition II.9 Suppose n is even, and write $S = (-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y) = \sum_{j=0}^{N/2-1} \varepsilon_j(|j\rangle\langle N-j-1| + |N-j-1\rangle\langle j|)$, with $\varepsilon_j = (-1)^{\#j}$, where $\#j$ is the number of 1's in the binary expression for j. The standard entangler E_0 in n-qubits is then given by

$$E_0 = \frac{1}{\sqrt{2}} \sum_{j=0}^{N/2-1} |j\rangle\langle 2j| + i|j\rangle\langle 2j+1| + \varepsilon_j(|N-j-1\rangle\langle 2j| - i|N-j-1\rangle\langle 2j+1|) \tag{12}$$

Proposition II.10 *The standard entangler E_0 is an entangler.*

Proof: First, we omit due to reasons of space a set of row operations which verifies that $\det(E_0) = 1$. Then we may write out an expression for E_0^T by reversing the indices in each bra-ket pair:

$$E_0^T = \frac{1}{\sqrt{2}} \sum_{k=0}^{N/2-1} |2k\rangle\langle k| + i|2k+1\rangle\langle k| + \varepsilon_k(|2k\rangle\langle N-k-1| - i|2k+1\rangle\langle N-k-1|) \tag{13}$$

Then Scholium II.8 shows that the following computation suffices to prove that E is an entangler.

$$\begin{aligned} E_0E_0^T \;&=\; \tfrac{1}{2}\textstyle\sum_{j=0}^{N/2-1} |j\rangle\langle j| \;+\; \varepsilon_j|j\rangle\langle N-j-1| \;+\; i^2|j\rangle\langle j| + \varepsilon_j|j\rangle\langle N-j-1| \\ &\quad + \varepsilon_j|N-j-1\rangle\langle j| + \varepsilon_j^2|N-j-1\rangle\langle N-j-1| \\ &\quad + \varepsilon_j(|N-j-1\rangle\langle j| + i^2\varepsilon_j^2|N-j-1\rangle\langle N-j-1|) \\ &=\; \textstyle\sum_{j=0}^{N/2-1} \varepsilon_j(|j\rangle\langle N-j-1| + |N-j-1\rangle\langle j|) \\ &=\; (-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y) \end{aligned} \tag{14}$$

This concludes the coordinate computation. □

In the next section, we will also make use of the following lemma. The computation is similar.

Lemma II.11 *$E_0^TE_0$ is diagonal and real. In fact, $E_0^TE_0 = |0\rangle\langle 0| - |1\rangle\langle 1| + |2\rangle\langle 2| - |3\rangle\langle 3| + \cdots$*

Proof: Computing the reversed product:

$$\begin{aligned} E_0^TE_0 \;&=\; \tfrac{1}{2}\textstyle\sum_{j=0}^{N/2-1} |2j\rangle\langle 2j| \;+\; i|2j+1\rangle\langle 2j| \;+\; i|2j\rangle\langle 2j+1| \;-\; |2j+1\rangle\langle 2j+1| \\ &\quad + \varepsilon_j^2|2j\rangle\langle 2j| - i\varepsilon_j^2|2j\rangle\langle 2j+1| - i\varepsilon_j^2|2j+1\rangle\langle 2j| + i^2\varepsilon_j^2|2j+1\rangle\langle 2j+1| \\ &=\; \textstyle\sum_{j=0}^{N/2-1} |2j\rangle\langle 2j| - |2j+1\rangle\langle 2j+1| \end{aligned} \tag{15}$$

This concludes the proof. □

Example II.12 Although this example is large, we explicitly describe the standard four-qubit entangler.

$$E_0 = (1/\sqrt{2}) \begin{pmatrix} 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & i \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & i & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{16}$$

Note that the antidiagonal pattern mirrors $S = (-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y)$ and that each computational basis state maps to a relative phase of a GHZ state. ◇

Finaglers

There do not exist entanglers when the number of qubits n is odd, because $\mathfrak{k} \cong \mathfrak{sp}(N/2)$ rather than $\mathfrak{so}(N)$. Cf. the as yet unproven Theorem I.3. Yet the fairly abstract embedding K of $Sp(N/2)$ into $SU(N)$ might be made more standard. This is indeed possible, and we call the any matrix which rotates K to the standard $Sp(N/2)$ a finagler.

Definition II.13 Let $\theta_{\mathbf{AII}} : \mathfrak{su}(N) \to \mathfrak{su}(N)$ be the standard Cartan involution (19, pg.445) fixing $\mathfrak{sp}(N/2)$, i.e. $\theta_{\mathbf{AII}}(X) = (-i\sigma^y \otimes \mathbf{1}_{N/2})X^T(-i\sigma^y \otimes \mathbf{1}_{N/2}) = (-i\sigma^y \otimes \mathbf{1}_{N/2})^{-1}\overline{X}(-i\sigma^y \otimes \mathbf{1}_{N/2})$. Then a finagler F is any $F \in SU(2^n)$ which causes the following diagram to commute:

$$\begin{array}{ccccc} & \mathfrak{su}(N) & \xrightarrow{\theta_{\mathbf{AII}}} & \mathfrak{su}(N) & \\ \mathrm{Ad}(F) & \downarrow & & \downarrow & \mathrm{Ad}(F) \\ & \mathfrak{su}(N) & \xrightarrow{\theta} & \mathfrak{su}(N) & \end{array} \tag{17}$$

If $F \in SU(N)$, then we say F finagles iff F is a finagler.

Proposition II.14 *F is a finagler iff $F(-i\sigma^y \otimes \mathbf{1}_{N/2})^T F^T = (\xi\mathbf{1})(-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y) = (\xi\mathbf{1})S$, $\xi^N = 1$.*

Proof: For convenience, label $\Sigma = -i\sigma^y \otimes \mathbf{1}_{N/2}$. ($F$ finagles) $\iff [F\Sigma^{-1}(\overline{F^\dagger X F})\Sigma F^\dagger = S^{-1}\overline{X}S \; \forall X \in \mathfrak{su}(N)]$ $\iff [F\Sigma^T F^T = (\xi\mathbf{1})S, \xi^N = 1]$. Note that the second equivalence uses Lemma II.6. □

Example II.15 In three qubits, we see the following computation is a finagler by direct computation.

$$F = (1/\sqrt{2}) \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix} \tag{18}$$

Unlike entanglers, it is possible for $F = \overline{F}$. The finagler maps computational basis states to GHZ states. $\diamond$

Definition II.16 Fix n an odd number of qubits. Let $S = (-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y) = \sum_{j=0}^{N/2-1} \iota_j (|N-j-1\rangle\langle j| - |j\rangle\langle N-j-1|)$ with $\iota_j = \pm 1$. The standard finagler F_0 is defined to be the following linear operator:

$$F_0 = \sum_{j=0}^{N/2-1} |j\rangle\langle j| + |N-j-1\rangle\langle j| \; + \; \iota_j(|j\rangle\langle N/2+j| - |N-j-1\rangle\langle N/2+j|) \tag{19}$$

Note that the standard finagler is real.

Proposition II.17 *The standard finagler F_0 finagles.*

Proof: We again omit the column operations verifying $\det(F_0) = 1$, as this would take several pages. Thus, let $\Sigma = -i\sigma^y \otimes \mathbf{1}_{N/2}$ be expanded as $\Sigma = \sum_{j=0}^{N/2-1} |j\rangle\langle N/2+j| - |N/2+j\rangle\langle j|$. We have the following equation:

$$F_0\Sigma = \frac{1}{\sqrt{2}} \sum_{j=0}^{N/2-1} |j\rangle\langle N/2+j| \; + \; |N-j-1\rangle\langle N/2+j| \; - \; \iota_j(|j\rangle\langle j| - |N-j-1\rangle\langle j|) \tag{20}$$

Moreover, $F_0^T = \frac{1}{\sqrt{2}} \sum_{j=0}^{N/2-1} |j\rangle\langle j| + |j\rangle\langle N-j-1| \; + \; \iota_j(|N/2+j\rangle\langle j| - |N/2+j\rangle\langle N-j-1|)$. Thus we see that

$$\begin{aligned} (F_0\Sigma)F_0^T \; &= \; \tfrac{1}{2}\textstyle\sum_{j=0}^{N/2-1} \iota_j(|j\rangle\langle j| - |j\rangle\langle N-j-1| + |N-j-1\rangle\langle j| - |N-j-1\rangle\langle N-j-1|) \\ &\qquad - \iota_j(|j\rangle\langle j| + |j\rangle\langle N-j-1| - |N-j-1\rangle\langle j| - |N-j-1\rangle\langle N-j-1|) \\ &= \; \textstyle\sum_{j=0}^{N/2-1} \iota_j(|N-j-1\rangle\langle j| - |j\rangle\langle N-j-1|) \end{aligned} \tag{21}$$

This concludes the proof. $\square$

We also briefly review how $Sp(N/2)$ embeds into $SU(N)$. By one standard definition of the group (19, pg.446),

$$\mathfrak{sp}(N/2) = \left\{ \begin{pmatrix} X_1 & X_2 \\ X_3 & -X_1^T \end{pmatrix} \; ; \; X_j = \overline{X}_j, X_{2,3} \text{ symmetric} \right\} \tag{22}$$

Another standard definition (24, pp.34-36) uses a symmetry in matrices of quaternions. Note that the matrices of Equation 22 are not elements of $\mathfrak{su}(N)$. Rather, the $+1$ eigenspace of $\theta_{\mathbf{AII}}(X) = \Sigma^{-1}\overline{X}\Sigma$ is:

$$\mathfrak{sp}(N/2) = \left\{ \begin{pmatrix} V & W \\ -W^\dagger & \overline{V} \end{pmatrix} \; ; \; V \in \mathfrak{u}(N/2), W = W^T \text{ is complex symmetric} \right\} \tag{23}$$

(For example, $Sp(4) \subset SU(8)$ this is 36 dimensional. For W includes two real symmetric matrices with 10 dimensions each, while $\mathfrak{u}(4)$ is 16 dimensional.) One may verify this is also a copy of $\mathfrak{sp}(N/2)$, so that $\mathfrak{k}$ is a copy of $\mathfrak{sp}(N/2)$ as well. Also, note that for $k \in K$, in particular $k \in \otimes_1^n SU(2)$, we expect $FkF^\dagger$ to be in the *copy of*

$Sp(N/2)$ *above* rather than to be a real matrix in an orthogonal subgroup of $SU(N)$. Finally, note that the exponentiating the Lie algebra above is not the best way to write out a closed form for elements of the global group $Sp(N/2)$. Rather, we have a block form:

$$Sp(N/2) = \{V \in SU(N)\ ;\ V^T \Sigma V = \Sigma\} = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SU(N)\ ;\ \begin{array}{l} A^T C \text{ is symmetric}, B^T D \text{ is symmetric}, \\ A^T D - C^T B = \mathbf{1} \end{array} \right\} \tag{24}$$

K is the symmetry group of the concurrence form

We are now in a position to provide the physical interpretation of K. Namely, K is the symmetry group of the concurrence bilinear form, as stated in Theorem I.3.

Proof of Theorem I.3: We first prove that $v \in K$ iff $\mathcal{C}_n(v|\phi\rangle, v|\psi\rangle) = \mathcal{C}_n(|\phi\rangle, |\psi\rangle)$ for all $|\phi\rangle$, $|\psi\rangle \in \mathcal{H}_n$. Let $X = \log v$. Since $X \in \mathfrak{su}(N)$, X is anti-Hermitian, i.e. $X = -X^\dagger = -\overline{X}^T$. Finally, recall $S = (-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y)$. Thus in mathematical notation, we have for $w, x \in \mathcal{H}_n$ the concurrence form given by $\mathcal{C}_n(w,x) = w^T S v$. Hence

$$(X = S^{-1}\overline{X}S) \iff (SX = \overline{X}S) \iff (SX = -X^T S) \iff (X^T S + SX = 0) \iff (v^T S v = S) \tag{25}$$

Now the first item is equivalent to $v \in K$ while the last is equivalent to $\mathcal{C}(vw, vx) = (w^T v^T)S(vx) = w^T(v^T S v)x = w^T S x = \mathcal{C}(w,x)$ for all $w, x \in \mathcal{H}_n$.

We next prove that for n odd, $K \cong Sp(N/2)$. To do so, it suffices to show n odd implies $\mathcal{C}_n$ is a nondegenerate two-form on $\mathcal{H}_n$. We first show $\mathcal{C}_n(x,w) = -\mathcal{C}_n(w,x)$ for any $w, x \in \mathcal{H}_n$. Noting that the transpose of a 1×1 matrix is again the same matrix, we realize that $\mathcal{C}_n$ is a two-form as follows:

$$\mathcal{C}_n(w,x) = w^T S x = [w^T S x]^T = x^T S^T w = -x^T S w = -\mathcal{C}_n(x,w) \tag{26}$$

Moreover, consider the tensor expression for S. We see that no eigenvalues of S are zero, and hence the form is nondegenerate. Thus, we must have $K \cong Sp(N/2)$.

Suppose now that n is even. We finally prove $K \cong SO(N)$. It suffices to construct a real vector space $V_{\mathbb{R}} \subset \mathcal{H}_n$ so that the following properties hold:

- $K \cdot V_{\mathbb{R}} \subseteq V_{\mathbb{R}}$
- The restriction of $\mathcal{C}_n$ to $V_{\mathbb{R}} \times V_{\mathbb{R}}$ is the usual dot product in the coordinates of a given basis.

Consider then $V_{\mathbb{R}} = \mathrm{span}_{\mathbb{R}}\{E_0|j\rangle\ ;\ 0 \leq j \leq N-1\}$, for E_0 the standard entangler of Definition II.9. Since E_0 is an entangler, certainly $K \cdot V_{\mathbb{R}} \subset V_{\mathbb{R}}$ since K acts on this real vector space by (real) orthogonal maps. Moreover, consider the concurrence on $V_{\mathbb{R}}$. For w, x in the $\mathbb{R}$ span of the computational basis, we have $E_0 w$, $E_0 x$ generic vectors in $V_{\mathbb{R}}$. Then

$$\mathcal{C}_n(E_0 w, E_0 x) = (E_0 w)^T S (E_0 x) = w^T E_0^T S E_0 x = w^T E_0^T E_0 E_0^T E_0 x = w^T \mathbf{1} x = w \cdot x \tag{27}$$

with the fourth equality by Lemma II.11. Hence in an even number of qubits, K fixes a real inner product on a real vector subspace of $\mathcal{H}_n$. Thus $K \cong SO(N)$. □

Scholium II.18 *For n even, for E_0 the standard entangler of Definition II.9, for any $|\phi\rangle$, $|\psi\rangle \in \mathcal{H}_n$, we have $\mathcal{C}_n(E_0|\phi\rangle, E_0|\psi\rangle) = \overline{\langle\phi|\psi\rangle}$.*

Remark II.19 Note that independent of any discussion of the algebra $\mathfrak{a}$ in n an odd number of qubits, we have shown that the Cartan involution θ has type **AII**. Hence any commutative $N/2-1$ dimensional subalgebra of $\mathfrak{p}$ must be maximal, and the concurrence canonical decomposition $SU(N) = KAK$ is well-defined for n odd. ◇

Remark II.20 Similar to Scholium II.18, note that the standard (real) finagler F_0 of Definition II.16 translates between the concurrence and the more standard two-form $(w,x) \mapsto w^T[(-i\sigma^y) \otimes \mathbf{1}_{N/2}]x$. Indeed, $F_0^{-1} = F_0^T$ since F_0 is orthogonal. Moreover, let w, x be in the real span of the computational basis states $\{|j\rangle\ ;\ 0 \leq j \leq N-1\}$. Then we may view $\{F_0|j\rangle\ ;\ 0 \leq j \leq N-1\}$ as a finagled basis, and the pullback of the concurrence from the finagled to the computational basis is the model two-form. Indeed, labelling $\Sigma = (-i\sigma^y) \otimes \mathbf{1}_{N/2}$, $F_0 \Sigma F_0^T = S$ and F_0 real imply $\Sigma = F_0^T S F_0$. Hence $\mathcal{C}_n(F_0 w, F_0 x) = (F_0 w)^T S (F_0 x) = w^T \Sigma x$. ◇

Cartan Involution in Coordinates

We finally present the Cartan involution in coordinates and provide some sample calculations. Let $X \in \mathfrak{su}(N)$, say with $X = \sum_{j,k=0}^{N-1} x_{j,k}|k\rangle\langle j|$. We now compute explicitly $\theta(X)$ so as to arrive at coefficient expressions for $\mathfrak{p}$, $\mathfrak{k}$.

$$\theta(X) \;=\; (-1)^n \sum_{j,k=0}^{N-1} \overline{x}_{j,k} S|k\rangle\langle j|S \;= (-1)^{n+n-\#k+\#j} \sum_{j,k=0}^{N-1} \overline{x}_{j,k} |N-k-1\rangle\langle N-j-1|$$

Consequently, we have the following characterizations:

- $X = \sum_{j,k=0}^{N-1} x_{j,k}|k\rangle\langle j| \in \mathfrak{p}$ iff $[(X \in \mathfrak{su}(N))$ and $(x_{N-1-k,N-1-j} = (-1)^{\#j+\#k+1}\overline{x}_{k,j})]$
- $X = \sum_{j,k=0}^{N-1} x_{j,k}|k\rangle\langle j| \in \mathfrak{k}$ iff $[(X \in \mathfrak{su}(N))$ and $(x_{N-1-k,N-1-j} = (-1)^{\#j+\#k}\overline{x}_{k,j})]$

This moreover produces the following description of $\mathfrak{k}$.

$$\begin{aligned}
\mathfrak{k} \;=\; \mathrm{span}_{\mathbb{R}} \; & \{|k\rangle\langle j| - |j\rangle\langle k| + (-1)^{\#j+\#k}|N-k-1\rangle\langle N-j-1| - (-1)^{\#j+\#k}|N-j-1\rangle\langle N-k-1|\} \\
& \sqcup \{i|k\rangle\langle j| + i|j\rangle\langle k| + (-1)^{\#k+\#j+1} i|N-j-1\rangle\langle N-k-1| + (-1)^{\#j+\#k+1} i|N-k-1\rangle\langle N-j-1|\} \\
& \sqcup \{i|j\rangle\langle j| - i|N-j-1\rangle\langle N-j-1|\}
\end{aligned} \tag{28}$$

Remark II.21 We *warn* the reader that the above expression does not allow one to count dimensions. Several repetitions occur from set to set, and moreover the expressions may vanish in case $j = N-k-1$. $\diamond$

Example in the two-qubit case

Recall the subalgebra $[\mathbf{1} \otimes \mathfrak{su}(2)] \oplus [\mathfrak{su}(2) \otimes \mathbf{1}]$ of infinitesimal transformations by $SU(2) \otimes SU(2) \subseteq SU(4)$. We show how the above Equation 28 recovers this subalgebra in the case of $n = 2$ qubits.

We begin by plugging $k = 0,\ j = 1$. Expanding into binary (or writing out the matrix) makes clear this is a tensor, and moreover a tensor by an identity matrix. Recall again that both are required to be in the Lie algebra of $SU(2) \otimes SU(2)$.

$$\begin{aligned}
& |0\rangle\langle 1| - |1\rangle\langle 0| - |3\rangle\langle 2| + |2\rangle\langle 3| && = \\
& |00\rangle\langle 01| - |01\rangle\langle 00| - |11\rangle\langle 10| + |10\rangle\langle 11| && = \\
& (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes (|0\rangle\langle 1| - |1\rangle\langle 0|)
\end{aligned} \tag{29}$$

One may similarly analyze the following matrices:

$$\begin{aligned}
& i|0\rangle\langle 1| + i|1\rangle\langle 0| + i|3\rangle\langle 2| + i|2\rangle\langle 3| \\
& |0\rangle\langle 2| - |2\rangle\langle 0| - |3\rangle\langle 1| + |1\rangle\langle 3| \\
& i|0\rangle\langle 2| + i|2\rangle\langle 0| + i|3\rangle\langle 1| + i|1\rangle\langle 3|
\end{aligned} \tag{30}$$

Note that for the next four expressions, substitution returns a 0 matrix:

$$\begin{aligned}
& |0\rangle\langle 3| - |3\rangle\langle 0| + |3\rangle\langle 0| - |0\rangle\langle 3| \\
& i|0\rangle\langle 3| + i|3\rangle\langle 0| - i|3\rangle\langle 0| - i|0\rangle\langle 3| \\
& |1\rangle\langle 2| - |2\rangle\langle 1| + |2\rangle\langle 1| - |1\rangle\langle 2| \\
& i|1\rangle\langle 2| + i|2\rangle\langle 1| - i|2\rangle\langle 1| - i|1\rangle\langle 2|
\end{aligned} \tag{31}$$

Further substitution yields the following:

$$\begin{aligned}
& |1\rangle\langle 3| - |3\rangle\langle 1| + |2\rangle\langle 0| - |0\rangle\langle 2| \\
& i|1\rangle\langle 3| + i|3\rangle\langle 1| + i|2\rangle\langle 0| + i|0\rangle\langle 2| \\
& |2\rangle\langle 3| - |3\rangle\langle 2| - |1\rangle\langle 0| + |0\rangle\langle 1| \\
& i|2\rangle\langle 3| + i|3\rangle\langle 2| + i|1\rangle\langle 0| + i|0\rangle\langle 1|
\end{aligned} \tag{32}$$

Finally, we consider the diagonal matrices in $\mathfrak{k}$:

$$\begin{array}{l} i|0\rangle\langle 0| - i|3\rangle\langle 3| \\ i|1\rangle\langle 1| - i|2\rangle\langle 2| \end{array} \tag{33}$$

Note that the $\mathbb{R}$ span of these two matrices coincides with $\mathbb{R}(i\sigma_z^1) \oplus \mathbb{R}(i\sigma_z^2)$.

The Cartan involution formalism thus works, although in a cumbersome way. We next explore the answer it returns in the three-qubit case.

Example in the three-qubit case, $K = Sp(4)$

We now describe explicitly the output of Equation 28 in three qubits. The corresponding real Lie algebra is thirty-six dimensional, which implies by the Cartan classification that K is an abstract copy of $Sp(4)$. A copy of $SO(8)$ would rather be twenty-eight dimensional.

The simplest way to organize the three qubit computation is to appeal to separation. We say a term $|k\rangle\langle j|$ has separation $|k-j|$ and extend linearly. In Equation 28, each matrix described has a well-defined separation.

$$\begin{array}{ll} \text{Separation 0} & i|0\rangle\langle 0| - i|7\rangle\langle 7| \\ \text{Total 4} & i|1\rangle\langle 1| - i|6\rangle\langle 6| \\ & i|2\rangle\langle 2| - i|5\rangle\langle 5| \\ & i|3\rangle\langle 3| - i|4\rangle\langle 4| \end{array} \tag{34}$$

$$\begin{array}{ll} \text{Separation 1} & |0\rangle\langle 1| - |1\rangle\langle 0| - |7\rangle\langle 6| + |6\rangle\langle 7| \\ \text{Total 8} & i|0\rangle\langle 1| + i|1\rangle\langle 0| + i|7\rangle\langle 6| + i|6\rangle\langle 7| \\ & |1\rangle\langle 2| - |2\rangle\langle 1| + |6\rangle\langle 5| - |5\rangle\langle 6| \\ & i|1\rangle\langle 2| + i|2\rangle\langle 1| - i|6\rangle\langle 5| - i|5\rangle\langle 6| \\ & |2\rangle\langle 3| - |3\rangle\langle 2| - |5\rangle\langle 4| + |4\rangle\langle 5| \\ & i|2\rangle\langle 3| + i|3\rangle\langle 2| + i|5\rangle\langle 4| + i|4\rangle\langle 5| \\ & |3\rangle\langle 4| - |4\rangle\langle 3| \\ & i|3\rangle\langle 4| + i|4\rangle\langle 3| \end{array} \tag{35}$$

$$\begin{array}{ll} \text{Separation 2} & |0\rangle\langle 2| - |2\rangle\langle 0| - |7\rangle\langle 5| + |5\rangle\langle 7| \\ \text{Total 6} & i|0\rangle\langle 2| + i|2\rangle\langle 0| + i|7\rangle\langle 5| + i|5\rangle\langle 7| \\ & |1\rangle\langle 3| - |3\rangle\langle 1| - |6\rangle\langle 4| + |4\rangle\langle 6| \\ & i|1\rangle\langle 3| + i|3\rangle\langle 1| + i|6\rangle\langle 4| + i|4\rangle\langle 6| \\ & |2\rangle\langle 4| - |4\rangle\langle 2| + |5\rangle\langle 3| - |3\rangle\langle 5| \\ & i|2\rangle\langle 4| + i|4\rangle\langle 2| - i|5\rangle\langle 3| - i|3\rangle\langle 5| \end{array} \tag{36}$$

$$\begin{array}{ll} \text{Separation 3} & |0\rangle\langle 3| - |3\rangle\langle 0| + |7\rangle\langle 4| - |4\rangle\langle 7| \\ \text{Total 6} & i|0\rangle\langle 3| + i|3\rangle\langle 0| - i|7\rangle\langle 4| - i|4\rangle\langle 7| \\ & |1\rangle\langle 4| - |4\rangle\langle 1| + |6\rangle\langle 3| - |3\rangle\langle 6| \\ & i|1\rangle\langle 4| + i|4\rangle\langle 1| - i|6\rangle\langle 3| - i|3\rangle\langle 6| \\ & |2\rangle\langle 5| - |5\rangle\langle 2| \\ & i|2\rangle\langle 5| + i|5\rangle\langle 2| \end{array} \tag{37}$$

$$
\begin{array}{ll}
\text{Separation 4} & |0\rangle\langle 4| - |4\rangle\langle 0| - |7\rangle\langle 3| + |3\rangle\langle 7| \\
\text{Total 4} & i|0\rangle\langle 4| + i|4\rangle\langle 0| + i|7\rangle\langle 3| + i|3\rangle\langle 7| \\
 & |1\rangle\langle 5| - |5\rangle\langle 1| - |6\rangle\langle 2| + |2\rangle\langle 6| \\
 & i|1\rangle\langle 5| + i|5\rangle\langle 1| + i|6\rangle\langle 2| + i|2\rangle\langle 6|
\end{array}
\tag{38}
$$

$$
\begin{array}{ll}
\text{Separation 5} & |0\rangle\langle 5| - |5\rangle\langle 0| + |7\rangle\langle 2| - |2\rangle\langle 7| \\
\text{Total 4} & i|0\rangle\langle 5| + i|5\rangle\langle 0| - i|7\rangle\langle 2| - i|2\rangle\langle 7| \\
 & |1\rangle\langle 6| - |6\rangle\langle 1| \\
 & i|1\rangle\langle 6| + i|6\rangle\langle 1|
\end{array}
\tag{39}
$$

$$
\begin{array}{ll}
\text{Separation 6} & |0\rangle\langle 6| - |6\rangle\langle 0| + |7\rangle\langle 1| - |1\rangle\langle 7| \\
\text{Total 2} & i|0\rangle\langle 6| + i|6\rangle\langle 0| - i|7\rangle\langle 1| - i|1\rangle\langle 7|
\end{array}
\tag{40}
$$

$$
\begin{array}{ll}
\text{Separation 7} & |0\rangle\langle 7| - |7\rangle\langle 0| \\
\text{Total 2} & i|0\rangle\langle 7| + i|7\rangle\langle 0|
\end{array}
\tag{41}
$$

Thus we see a total of $4+8+6+6+4+4+2+2 = 36$ real dimensions in $\mathfrak{k}$. Now by the Cartan classification (19, pg.518), the Cartan involution θ must be either type **AI** fixing an abstract copy of $SO(28)$, type **AIII** fixing some $S[U(p) \oplus U(q)]$ for $p+q = 2^n$, or else **type AII** fixing an abstract copy of $Sp(4)$. Since only $Sp(4)$ is thirty-six dimensional, we see $\mathfrak{k} \cong \mathfrak{sp}(4)$ and $K \cong Sp(4)$.

III. APPLICATIONS TO CONCURRENCE CAPACITY

This section focuses on an application of the concurrence canonical decomposition $SU(N) = KAK$ of Definition I.2 when the number of qubits n is even. Namely, we study how a given computation $v \in SU(N)$ may change the concurrence of the quantum data state. Since we have the concurrence $C_n(|\psi\rangle) = |\overline{\langle\psi|}(-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y)|\psi\rangle|$ with the n-tangle $\tau_n = C_n^2$ for n even, there are immediate applications to the n-tangle as well.

Let $v \in SU(N)$. Recall from Definition I.5 that the concurrence capacity is defined as

$$
\kappa(v) = \max\{C_n(v|\psi\rangle)\ ;\ C_n(|\psi\rangle) = 0, \langle\psi|\psi\rangle = 1\}
\tag{42}
$$

Since we vary over all $C_n(|\psi\rangle) = 0$, we see that for $k \in K$ we have $\kappa(vk) = \kappa(v)$ by symmetry. Immediately $\kappa(kv) = \kappa(v)$. Thus, for $v = k_1 a k_2$ the $\texttt{C.C.}$ decomposition of any $v \in SU(N)$, we have $\kappa(v) = \kappa(k_1 a k_2) = \kappa(a)$.

We next describe the concurrence capacity of any $a \in A$. The formalism makes strong use of entanglers to translate between $\mathcal{C}_n$ and $(w,x) \mapsto w^T x$.

Definition III.1 The *concurrence spectrum* $\lambda_c(v)$ of $v \in SU(N)$ is the spectrum of $E_0^\dagger v E_0 (E_0^\dagger v E_0)^T$, for E_0 the standard entangler of Definition II.9. Note that the spectrum is the set of eigenvalues since $\mathcal{H}_n$ is finite dimensional. The *convex hull* $\texttt{CH}[\lambda_c(v)]$ of $\lambda_c(v)$ is the set of all line segments joining all points of $\lambda_c(v)$, i.e.

$$
\texttt{CH}[\lambda_c(v)] = \left\{ \sum_{z_j \in \lambda_c(v)} t_j z_j\ ;\ 0 \le t_j \le 1, \sum_{j=0}^{\#\lambda_c(v)} t_j = 1 \right\}
\tag{43}
$$

These definitions allow us then to prove the following general results regarding concurrence capacity. The techniques closely follow those in prior work (15).

Lemma III.2 *Let $v \in SU(N)$, with* $\texttt{CCD}$ *$v = k_1 a k_2$ for $a = E_0 d E_0^\dagger$ for d diagonal in $SU(N)$.*

- $\lambda_c(v) = \lambda_c(a) = \Big\{ d_j^2 \,;\, d = \sum_{j=0}^{N-1} d_j |j\rangle\langle j| \Big\}$.
- $\kappa(v) = \kappa(a) = max\Big\{ |\sum_{j=0}^{N-1} a_j^2 d_j^2| \,;\, |\psi\rangle = \sum_{j=0}^{N-1} a_j|j\rangle, \langle\psi|\psi\rangle = 1, \overline{\langle\psi|}\psi\rangle = 0 \Big\}$.
- $(\kappa(v) = \kappa(a) = 1) \Longleftrightarrow \big(0 \in \mathtt{CH}[\lambda_c(v)] = \mathtt{CH}[\lambda_c(a)]\big)$.

Proof: For the first item, recall $v = k_1 a k_2$. Thus the following expression results from expanding Definition III.1.

$$E_0^\dagger v E_0 (E_0^\dagger v E_0)^T = [(E_0^\dagger k_1 E_0)(E_0^\dagger a E_0)(E_0^\dagger k_2 E_0)][(E_0^\dagger k_2 E_0)^T (E_0^\dagger a E_0)^T (E_0^\dagger k_1 E_0)^T] \tag{44}$$

Label the elements of $SO(N)$ by $o_1 = (E_0^\dagger k_1 E_0)$, $o_2 = (E_0^\dagger k_2 E_0)$, and put $d = E_0^\dagger a E_0$ diagonal. Then the above reduces to $o_1 d o_2 o_2^T d^T o_1^T = o_1 d^2 o_1^{-1}$, with spectrum identical to d.

For the next item, compare the two-qubit case (15, Eq.(41)) and recall Scholium II.18. Suppose $C_n(|\varphi\rangle) = 0$. Then per Scholium II.18, for $|\psi\rangle = E_0^\dagger|\varphi\rangle$ we have we see $0 = \mathcal{C}_n(E_0E_0^\dagger|\varphi\rangle, E_0E_0^\dagger|\varphi\rangle) = \overline{\langle\psi|}\psi\rangle$. Now for $\kappa(a)$, take $|\psi\rangle = E_0^\dagger|\varphi\rangle$. We then maximize over expressions $\mathcal{C}_n(a|\varphi\rangle, a|\varphi\rangle) = \mathcal{C}_n(E_0E_0^\dagger aE_0|\psi\rangle, E_0E_0^\dagger aE_0|\psi\rangle) = \mathcal{C}_n(E_0 d|\psi\rangle, E_0 d|\psi\rangle) = \overline{\langle\psi|} d^2|\psi\rangle$.

The final item makes use of the Schwarz inequality. For should the concurrence capacity be maximal, there is by compactness of the set of normalized kets some normalized $|\psi\rangle$ with $C_n(|\phi\rangle) = 1$. For $|\psi\rangle = \sum_{j=0}^{N-1} a_j|j\rangle$,

$$1 = |\sum_{j=0}^{N-1} a_j^2 d_j^2| \le \sum_{j=0}^{N-1} |a_j^2 d_j^2| = \sum_{j=0}^{N-1} |a_j|^2 = 1 \tag{45}$$

The Schwarz *equality* further requires some $z \in \mathbb{C}$, $z\overline{z} = 1$, so that $a_j^2 d_j^2 = |a_j|^2 z, \forall j$. Now since $\overline{\langle\psi|}\psi\rangle = 0$,

$$0 = \sum_{j=0}^{N-1} a_j^2 = \sum_{j=0}^{N-1} |a_j|^2 \overline{d_j^2} z \tag{46}$$

Multiplying through by $\overline{z}$ and taking the complex conjugate, we see $0 \in \mathtt{CH}[\lambda_c(v)]$. □

As already noted in the introduction, the concurrence capacity κ is properly thought of as a function of A rather than a function of $SU(N)$. This is advantageous from a computational standpoint, because in order to calculate $\kappa(v)$ one need minimize over a function involving $N-1$ real parameters in A versus N^2-1 parameters describing a general $v \in SU(N)$. We next consider typical values for a large number of qubits. To do so, we need to be able to randomly choose an element of A.

Definition III.3 Consider the following coordinate map on the commutative group A:

$$[0,2\pi]^{N-1} \to A \text{ by } (t_0, t_2, \cdots, t_{N-2}) \mapsto \exp E_0\big(\sum_{j=0}^{N-2} it_j|j\rangle\langle j| - it_j|j+1\rangle\langle j+1|\big)E_0^\dagger \tag{47}$$

The Haar measure on da is the group multiplication invariant measure $da = (2\pi)^{-N+1} dt_0\, dt_2 \,\cdots\, dt_{N-2}$. This is the pushforward of the independent product of uniform measures $dt_j/(2\pi)$ on each $[0,2\pi]$.

Recall that for $p = 2n$, Theorem I.7 asserts that according to da, almost all $a \in A$ have $\kappa(a) = 1$ for p large. Specifically, we assert

$$\lim_{p\to\infty} da(\{a \in A \,;\, \kappa(a) = 1\}) = 1 \tag{48}$$

We prove this assertion shortly, but we first need a lemma.

Lemma III.4 *Label as uniform distribution on the circle a distribution whose pullback to $[0,2\pi]$ under $t \mapsto e^{2\pi i t}$ is uniform, and similarly say two random variables Z_1, Z_2 on $\{z\overline{z} = 1\}$ are independent iff their pullbacks to $[0,2\pi] \times [0,2\pi]$ are. Then suppose Z_1 is any random variable on the circle, and let Z_2 be independent to Z_1 and uniform. Then $Z_1 Z_2$ is uniform.*

Proof: Consider the random variable $T = -i \log Z_1 - i \log Z_2 \mathrm{mod}\, 2\pi$ on $[0, 2\pi]$. Let $f_1(t)$ be the pullback probability density function of the nonuniform random variable Z_1 to $[0, 2\pi]$. We let $F_T(t) = \mathrm{Prob}(T \le t)$ be the cumulative density function. Then

$$F_T(t) = \frac{1}{2\pi} \int_0^{2\pi} \mathrm{Prob}(-i \log Z_2 \in [s, s+t]) f_1(s) ds = \frac{1}{2\pi} \int_0^{2\pi} t f_1(s) ds = t/(2\pi) \tag{49}$$

Since $F_T(t) = t/(2\pi)$, we see that T is uniform. Hence $Z_1 Z_2$ is uniform. □

Proof of Theorem I.7: First, let us check that $\{\kappa(a) = 1\}$ is da-measurable. To see this, note that the concurrence spectrum $\lambda_c(a)$ may be expressed in terms of the coordinates t_j as follows:

$$d_0^2 = \mathrm{e}^{2it_0}, d_1 = \mathrm{e}^{2it_1 - 2it_0}, d_2^2 = \mathrm{e}^{2it_2 - 2it_1}, \cdots d_j^2 = \mathrm{e}^{2it_j - 2it_{j-1}}, \cdots, d_{N-1}^2 = \mathrm{e}^{-2it_{N-2}} \tag{50}$$

Thus Lemma III.2 induces a measurable condition on the t_j.

Continuing the proof, by direct calculation Z^2 is a uniform random variable on the circle $\{z\bar{z} = 1\}$ given that Z is such. Thus note that d_0^2, d_2^2, d_4^2, $\cdots$, d_{N-1}^2 are $p = N/2$ independent, uniform random variables by Lemma III.4. It suffices to show that $\ell + 1 = p$ independent, random variables on the circle have 0 in their convex hull as $\ell \mapsto \infty$. Relabel $d_0^2 = Z_0$, $d_2^2 = Z_1$, $\cdots$ $d_{N-1}^2 = Z_\ell$.

Without loss of generality, say $Z_0 = 1$. Let C_2 be the event that no Z_1, Z_2, $\cdots$ Z_ℓ is in the second quadrant $\{z = x + iy\,;\, x < 0, y > 0\}$, with C_3 similar for the third quadrant $\{x < 0, y < 0\}$. Let D be the event that 0 is in the convex hull of Z_0, Z_1, $\cdots$, Z_ℓ. Then (NOT $C_2 \cap$ NOT C_3) $\subset D$. Then Prob(NOT $C_2 \cap$ NOT C_3) $\le$ Prob(D), and

$$1 - \mathrm{Prob}(D) \le 1 - \mathrm{Prob}(\text{NOT } C_2 \text{ and NOT } C_3) = \mathrm{Prob}(C_2 \text{ or } C_3) = (1/2)^\ell \tag{51}$$

Hence as $\ell \to \infty$, Prob(D) goes to 1. Hence the probability $\mathtt{CH}[\lambda_c(v)]$ contains 0 limits to 1. □

IV. CONCLUSIONS AND ONGOING WORK

We have shown that there exists a generalized canonical decomposition of unitary operators on n qubits which may be used to study changes in the concurrence entanglement monotone. This decomposition closely resembles the older two-qubit decomposition when n is even, and it may be used to study the concurrence-entanglement capacity of generic unitary operators. The main result is that such a generic unitary operator is almost always perfectly entangling with respect to the concurrence monotone when the number of qubits is large and even.

Ongoing work would attempt to extend the dynamical viewpoint taken in this paper. Specifically, the unitary operator describes the dynamics of a quantum data state, and the present techniques allow us to quantitatively study the dynamics of the concurrence entanglement measure. Similarly, we would wish to study the dynamics of this concurrence capacity of quantum computations in naturally defined families or sequences of such computations. As a separate topic, we might also study the failure of the concurrence function itself by quantifying how entangled a quantum state with zero concurrence may be.

APPENDIX A: Computing the CCD When the Number of Qubits Is Even

This appendix recalls how to compute the canonical decomposition in an even number $n = 2p$ of qubits. Note that other arguments in the case $n = 2$ (12; 13) may be found in the literature, and that the present treatment is a straightforward genearlization of a matrix-oriented treament in the two-qubit case (14, App.A). It is included for completeness.

The overall structure of the algorithm is contains two steps.

1. Produce an algorithm for computing the decomposition $SU(N) = SO(N)\, D\, SO(N)$ for D the diagonal subgroup of $SU(N)$. We will refer to this decomposition as the *unitary* SVD *decomposition* henceforth.

2. Recall E_0 the standard entangler of Definition II.9. Given a $v \in SU(N)$ for which we wish to compute the CCD, compute first the unitary SVD $E_0^\dagger v E_0 = o_1 d o_2$. Then we have a CCD given by

$$v \;=\; (E_0 o_1 E_0^\dagger)(E_0 d E_0^\dagger)(E_0 o_2 E_0^\dagger) \;=\; k_1 a k_2 \tag{A1}$$

since $k_1 = E_0 o_1 E_0^\dagger \in K$, $k_2 = E_0 o_2 E_0^\dagger \in K$, and $a = E_0 d E_0^\dagger \in A$.

Note that the unitary SVD decomposition exists due to KAK metadecomposition theorem, taking as inputs $G = SU(N)$, $\theta_{\mathbf{AI}}(X) = \bar{X}$, and $\mathfrak{a}$ the diagonal subalgebra of $\mathfrak{su}(N)$.

Before continuing to Step 1, we first prove a lemma. It is useful in computing particular instances of the unitary SVD.

Lemma A.1 *For any $p \in SU(N)$ with $p = p^T$, there is some $o \in SO(N)$ such that $p = odo^T$ with d a diagonal, determinant one matrix.*

Proof: We first show the following.

$\forall\, a, b$, symmetric real $N \times N$ matrices with $ab = ba$, there is some $o \in SO(N)$ such that oao^T and obo^T are diagonal.

It suffices to construct a basis which is simultaneously a basis of eigenvectors for both a and b. Thus, say V_λ is the λ eigenspace of b. For $x \in V_\lambda$, $b(ax) = a(bx) = \lambda ax$, i.e. $x \mapsto ax$ preserves the eigenspace. Now find eigenvectors for a restricted to V_λ, which remains symmetric. Thus we may find the desired $o \in SO(N)$, making choices of orderings and signs on an eigenbasis as appropriate for determinant one.

Given the above, write $p = a + ib$. Now $\mathbf{1} = pp^\dagger = p\bar{p} = (a+ib)(a-ib) = (a^2+b^2) + i(ba - ab)$. Since the imaginary part of $\mathbf{1}$ is $\mathbf{0}$, we conclude that $ab = ba$. Hence a single o exists per the last paragraph which diagonalizes the real and imaginary parts. □

Suppose then that $v = o_1 d o_2$ is the unitary SVD of some $v \in SU(N)$. For convenience, we also label $v = po_3$ the type **AI** Cartan decomposition (19, thm1.1.iii,pg.252) (24, thm6.31.c). This is a generalized polar decomposition in which $p = p^T$, $k \in SO(N)$. Note that it is equivalent via Lemma A.1 to compute $v = pk$, as the unitary SVD follows by $v = (o_1 d o_1^T)k = o_1 d o_2$. Continuing to the algorithm for Step 1,

- Compute p^2 as follows: $p^2 = pp^T = po_3 o_3^T p^T = vv^T$.
- Apply Lemma A.1 to p^2. Thus $p^2 = o_1 d^2 o_1^T$ for $o_1 \in SO(N)$.
- Choose square roots entrywise in d^2 to form d. Be careful to ensure $\det d = 1$.
- Compute $p = o_1 d o_1^T$.
- Thus $o_3 = p^\dagger v$, and $v = p(o_3) = o_1 d o_1^T o_3 = o_1 d o_2$.

This concludes the algorithm for computing the unitary SVD of Step 1.

Step 2 is almost follows given the inline description. The reader may produce algorithms outputting E_0.

Another question is computational efficiency. This is ongoing work, but we note immediately that an implementation of the spectral theorem of Lemma A.1 is required. This will be difficult with current technologies in 16+ qubits. Moreover, in the range of 50 to 60 qubits an even spread of the concurrence spectrum $\lambda_c(v)$ of Definition III.1 would make certain elements indistinguishable at 16-digit precision.

APPENDIX B: Concurrence level sets and K orbits

Mathematically, related measures are often easier to use than C_n. For example, the concurrence quadratic form $Q_n^C(|\psi\rangle) = \mathcal{C}_n(|\psi\rangle, |\psi\rangle)$ with $C_n(|\psi\rangle) = |Q_n^C(|\psi\rangle)|$ has smaller level sets than C_n itself. Moreover, it turns out that the normalized states within these level sets $[Q_n^C]^{-1}(\{z\}) = \{|\psi\rangle\ ;\ Q_n^C(|\psi\rangle) = z\}$ are naturally orbits of the group K, which must then be false for C_n.

Suppose throughout $n = 2p$ is an even number of qubits. For a vector $v \in \mathbb{C}^N$, put $Q_{\mathbf{AI}}(v) = v^T v$, noting that $Q_{\mathcal{C}}(E_0 v) = Q_{\mathbf{AI}}(v)$. Moreover, for $O \in SO(N)$, we have the following:

$$Q_{\mathbf{AI}}(O \cdot v) = Q_{\mathcal{C}}[E_0 O E_0^\dagger \cdot (E_0 v)] \tag{B1}$$

Thus we may study level sets of $Q_{\mathbf{AI}}$ under $SO(N)$ rather than study level sets of $Q_{\mathcal{C}}$ under K. Now if $v = v_1 + iv_2$ is a decomposition into real and imaginary parts of a complex vector, note that $Q_{\mathbf{AI}}(v_1 + iv_2) = v^T v = (|v_1|^2 - |v_2|^2) + 2i(v_1 \cdot v_2)$.

Lemma B.1 *Label $S^{2N-1} = \{|\psi\rangle\ ;\ \langle\psi|\psi\rangle = 1\}$. We have the following orbit decompositions of the level sets $Q_{\mathbf{AI}}^{-1}(\alpha) \cap S^{2N-1}$ for any fixed $\alpha \in \mathbb{C}$.*

1. *Let t be real, and let $v \in Q_{\mathbf{AI}}^{-1}(t) \cap S^{2N-1}$. Then $Q_{\mathbf{AI}}^{-1}(t) \cap S^{2N-1} = [SO(N) \cdot v]$.*

2. *Let α be complex, and let $v \in Q_{\mathbf{AI}}^{-1}(\alpha) \cap S^{2N-1}$. Then $Q_{\mathbf{AI}}^{-1}(\alpha) \cap S^{2N-1} = [SO(N) \cdot v]$.*

Proof: For the first item, write $v = v_1 + iv_2$. Then $v_1 \cdot v_2$ is zero as a set of real vectors. Consider the subset of $\mathbb{R}^{2N}$ given by $|v_1|^2 - |v_2|^2 = t$. Suppose now we have another pair of orthogonal vectors w_1, w_2 with $|w_1|^2 - |w_2|^2 = t$ and $|w_1|^2 + |w_2|^2 = 1$. Then $|w_1|^2 = |v_1|^2 = (1-t)/2$, thus $|v_2|^2 = |w_2|^2$ so that there is some $O \in SO(N)$ with $O \cdot v_1 = w_1$, $O \cdot v_2 = w_2$.

For the second item, suppose $\alpha = \mathrm{e}^{i\phi} t$ for some $t \in \mathbb{R}$. Now if $v \in Q_{\mathbf{AI}}^{-1}(\alpha)$, then note that we have $Q_{\mathbf{AI}}(\mathrm{e}^{-i\phi/2} v) = \mathrm{e}^{-i\phi} Q_{\mathbf{AI}}(v) = \mathrm{e}^{-i\phi}\alpha = t$. Conversely, if $w \in Q_{\mathbf{AI}}^{-1}(t)$ we have $\mathrm{e}^{i\phi/2} w \in Q_{\mathbf{AI}}^{-1}(\alpha)$. Having established bijective phase maps between the two level sets, it must also be the case that the level set of α forms a single $SO(N)$ orbit. □

Corollary B.2 *The restricted action of K to the normalized kets in any concurrence level set is transitive. Specifically, suppose $\alpha \in \mathbb{C}$, with $|\psi\rangle$ normalized with $Q_C(|\psi\rangle) = \alpha$. Then label $S^{2N-1} = \{\langle\phi|\phi\rangle = 1\}$ the set of normalized kets. Per Equation B1, we have $K \cdot |\psi\rangle = Q_C^{-1}(\alpha) \cap S^{2N-1}$.*

We restate the result colloquailly. Should any two normalized states $|\phi\rangle$, $|\psi\rangle$ have the same concurrence, then there is some global phase $\mathrm{e}^{i\theta}$ so that $|\phi\rangle = \mathrm{e}^{i\theta} k|\psi\rangle$ for $k \in K = E_0\ SO(N)\ E_0^\dagger$.

APPENDIX C: Concurrence is an entanglement monotone

The $n-$tangle, defined to be $\tau_n(|\psi\rangle) = C_n(|\psi\rangle)^2$ has been proposed (1) as a measure of n qubit entanglement for n even. The n-tangle of a state $|\psi\rangle$, like the n-concurrence, assumes real values in the range $0 \le \tau_n \le 1$ and has been shown to be an entanglement monotone, meaning τ_n is a convex function on states and is non-increasing under local operations and classical communication (LOCC). Most of our arguments focus on constructions more directly related to the concurrence C_n rather than the n-tangle $\tau_n = (C_n)^2$. Therefore, for completeness, we show that the n-concurrence is, in fact, a good measure of entanglement. The monotonicity property of a function is established by considering its action on mixtures of quantum states encoded within Hermitian density matrices ρ with tr $\rho = 1$. See, e.g., (21).

Definition C.1 The n-concurrence can be defined on mixed states ρ using the convex roof extension:

$$C_n(\rho) = \min\left\{\sum_k \lambda_k C_n(|\psi^k\rangle)\ ;\quad \rho = \sum_k \lambda_k |\psi^k\rangle\langle\psi^k|,\ \ |\psi\rangle^k \in \mathcal{H}_n,\ \ \langle\psi^k|\psi^k\rangle = 1\right\} \tag{C1}$$

This minimization is over all pure state ensemble decompositions of the state $\rho = \sum_k \lambda_k |\psi^k\rangle\langle\psi^k|$.

This definition is quite intricate. We point out the following remarkable result, not used in the sequel.

Theorem C.2 (Uhlmann, (1; 25)) *We may express $C_n(\rho)$ in closed form as follows:*

$$C_n(\rho) = \max\{0, \lambda_0 - \lambda_1 \ldots - \lambda_{N-1}\} \tag{C2}$$

Here, the λ_k are the square roots of the eigenvalues (in non-increasing order) of the product $\rho\tilde{\rho}$ where $\tilde{\rho} = S\overline{\rho}S^{-1}$.

The necessary and sufficient conditions for a function on quantum states to be a entanglement monotone are delineated in (9). For the n-concurrence, they can be summarized as follows:

- $C_n \ge 0$, and $C_n(\rho) = 0$ if ρ is fully separable.
- C_n is a convex function, i.e. $C_n(p\rho_1 + (1-p)\rho_2) \le pC_n(\rho_1) + (1-p)C_n(\rho_2), \forall p \in [0,1]$ and ρ_1, ρ_2 Hermitian matrices of trace one

- C_n is non increasing under LOCC. Specifically, $C_n(\rho) \geq \sum_j p_j C_n(\rho_j)$, where $\rho_j = A_j \rho A_j^\dagger / p_j$ are the states conditioned on the outcome j of a positive operator valued measurement (POVM) which occurs with probability $p_j = tr[A_j^\dagger A_j \rho]$.

Before proving this, we first establish the useful fact that the n-concurrence is invariant under permutations of the qubits. Defining Π_n to be the set of unitary operators corresponding to permutations on n qubits, we have:

Proposition C.3 *For n even, $C_n(P|\psi\rangle) = C_n(|\psi\rangle)$ $\forall P \in \Pi_n$.*

Proof: Any permutation P on n elements can be written as a finite composition of transpositions on pairs of elements. Hence it suffices to show invariance under a single swap operation. Writing the swap operator between qubits j and k as

$$S_{jk} = \frac{\mathbf{1}_j \otimes \mathbf{1}_k + \sigma_j^x \otimes \sigma_k^x + \sigma_j^y \otimes \sigma_k^y + \sigma_j^z \otimes \sigma_k^z}{2}, \tag{C3}$$

we have for any state $|\psi\rangle$,

$$\begin{aligned} C_n(S_{jk}|\psi\rangle) &= |\overline{\langle\psi|S_{jk}^\dagger} S S_{jk}|\psi\rangle| = |\overline{\langle\psi|} S_{jk} S S_{jk}|\psi\rangle| \\ &= |\overline{\langle\psi|} S S_{jk}^2|\psi\rangle| = C_n(|\psi\rangle). \end{aligned} \tag{C4}$$

Here we have used the fact that S_{jk} is real symmetric and unitary, and in the third equality we use the fact that $[\sigma_j^y \otimes \sigma_k^y, \sigma_j^l \otimes \sigma_k^l] = 0$ for $\sigma^l \in \{\sigma^x, \sigma^y, \sigma^z\}$. This proposition necessarily implies that $\Pi_n^+ \subsetneq K$, where Π_n^+ is the set of unitary permutation matrices on n objects with $+1$ determinant, i.e. permutations composed of an even number of transpositions. $\square$

Lemma C.4 *$C_n(\rho)$ is an entanglement monotone.*

Sketch: For the first condition, one first checks that $0 \leq C_n \leq 1$ using the eigenvalue decomposition of the matrix $S = (-i\sigma_1^y)(-i\sigma_2^y)\cdots(-i\sigma_n^y)$. Then any separable state can be realized by stochastic local unitaries acting on the fiducial separable state $|0\rangle_n = |0_1 \ldots 0_n\rangle$. Now, $C_n(|0\rangle_n) = 0$ and C_n is invariant under local unitaries per Proposition II.1 and Theorem I.3. To generalize from pure states to density matrices, recall Definition C.1.

The second condition is shown by writing the minimal ensemble decompositions for ρ_1 and ρ_2 separately as

$$p \min_{\{\lambda_k, |\psi^k\rangle\} | \sum \lambda_k |\psi^k\rangle\langle\psi^k| = \rho_1} \sum_k \lambda_k C_n(|\psi^k\rangle) + (1-p) \min_{\{\beta_k, |\phi^k\rangle\} | \sum \beta_k |\phi^k\rangle\langle\phi^k| = \rho_2} \sum_k \beta_k C_n(|\phi^k\rangle). \tag{C5}$$

These are not necessarily the minimal decompositions for the composite state $\rho = p\rho_1 + (1-p)\rho_2$, therefore, $C_n(p\rho_1 + (1-p)\rho_2) \leq pC_n(\rho_1) + (1-p)C_n(\rho_2)$.

Finally, we show that the n-concurrence is on average non-increasing under LOCC. First, because of permutation symmetry of the concurrence we can consider operations on one particular qubit of the n qubit system, say the first. An arbitrary, trace perserving, completely positive map on a quantum system can written in the Krauss decompostion (26) as $S(\rho) = \sum_j A_j \rho A_j^\dagger$ where the positive Krauss operators satisfy the sum rule $\sum_j A_j^\dagger A_j = \mathbf{1}$. The map can be composed of multiple operations with two operators at a time so we consider only two operators A_0 and A_1 acting on the first qubit. By the polar decomposition theorem, the operators can be written as $A_j = u_j b_j$, where $b_j = \sqrt{A_j^\dagger A_j}$ is positive and u_j is defined to be $\mathbf{1}$ on the kernel $\mathcal{K}$ of A_j and $A_j|A_j|^{-1}$ on $\mathcal{K}^\perp$. Physically, the map $S(\rho)$ corresponds to a generalized measurement on ρ followed by a unitary operation conditioned on the measurement. Because of the sum rule, which corresponds to trace preservation, we can write $A_0 = w_o \cos gX$ and $A_1 = w_1 \sin gX$ for $g \in \mathbb{R}$ and X a positive operator with unit trace. These operators are expressed in simpler form by diagonalizing X, viz. $A_0 = u_o d_o v$ and $A_1 = u_1 d_1 v$, where $u_j, v \in SU(2)$ and d_j are real diagonal matrices with elements (q,r) and $(\sqrt{1-q^2}, \sqrt{1-r^2})$. The average concurrence of a state ρ after the 2 outcome POVM is

$$\begin{aligned} p_0 C_n(\rho_0) + p_1 C_n(\rho_1) &= p_0 \min_{\{\lambda_k, |\psi^k\rangle\} | \sum \lambda_k |\psi^k\rangle\langle\psi^k| = \rho} \sum_k \lambda_k C_n(A_0|\psi^k\rangle / \sqrt{p_0}) \\ &\quad + p_1 \min_{\{\beta_k, |\phi^k\rangle\} | \sum \beta_k |\phi^k\rangle\langle\phi^k| = \rho} \sum_k \beta_k C_n(A_1|\phi^k\rangle / \sqrt{p_1}). \end{aligned} \tag{C6}$$

States conditioned on the first outcome satisfy:

$$\begin{aligned} C_n(A_0|\psi\rangle/\sqrt{p_0}) &= |\overline{\langle\psi|}v^T d_0^T u_0^T S u_0 d_0 v|\psi\rangle|/p_0 \\ &= qrC_n(v|\psi\rangle)/p_0 \\ &= qrC_n(|\psi\rangle)/p_0, \end{aligned} \tag{C7}$$

where in the second equality we have used $u_0^T(-i\sigma^y)u_0 = -i\sigma^y$, and the third equality follows by invariance of concurrence under local unitaries. Similarly, $C_n(A_1|\phi\rangle/\sqrt{p_1}) = \sqrt{(1-q^2)(1-r^2)}C_n(|\phi\rangle)/p_1$. The result is,

$$\begin{aligned} p_0C_n(\rho_0)+p_1C_n(\rho_1) &= qr\min_{\{\lambda_k,|\psi^k\rangle\}|\sum\lambda_k|\psi^k\rangle\langle\psi^k|=\rho}\sum_k\lambda_kC_n(|\psi^k\rangle) \\ &\quad +\sqrt{(1-q^2)(1-r^2)}\min_{\{\beta_k,|\phi^k\rangle\}|\sum\beta_k|\phi^k\rangle\langle\phi^k|=\rho}\sum_k\beta_kC_n(|\phi^k\rangle) \\ &= (qr+\sqrt{(1-q^2)(1-r^2)})C_n(\rho) \\ &\leq C_n(\rho), \end{aligned} \tag{C8}$$

with equality iff $q=r$, i.e. the A_j are stochastic unitaries. □

References

[1] Wong, A. and Christensen, N. Potential Multiparticle Entanglement Measure. *Phys. Rev. A* **63**, 044301 (2001).
[2] Barnum, H. and Linden, N. Monotones and Invariants for Multi-particle Quantum States. *J. Phys. A* **34**, 6787 (2001).
[3] Eisert, J. and Briegel, H. The Schmidt Measure as a Tool for Quantifying Multi-Particle Entanglement. *Phys. Rev. A* **64**, 022306 (2001).
[4] Meyer, D. A. and Wallach, N. R. Global Entanglement in Multi-partite Systems. *J. of Math. Phys.* **43**, 4273 (2002).
[5] Eggeling, T. and Werner, R. F. Separability properties of tripartite states with UxUxU symmetry, *Phys. Rev. A* **63**, 042111 (2001).
[6] Miyake, A. and Wadati, M. Multi-partite Entanglement and Hyperdeterminants. *Q. Inf. and Comp.* **2** (2002).
[7] Hill, S. and Wootters, W. Entanglement of a Pair of Quantum Bits. *Phys. Rev. Lett.* **78**, 5022 (1997).
[8] Rungta, P., Buzek, V., Caves, C., Hillery, M., and Milburn, G. Universal State Inversion and Concurrence in Arbitrary Dimensions. *Phys. Rev. A* **64**, 042315 (2001).
[9] Vidal, G. Entanglement Monotones. *J. Mod. Opt.* **47**, 355 (2000).
[10] Makhlin, Y. Nonlocal Properties of Two-qubit Gates and Mixed States and Optimization of Quantum Computations. *quant-ph/0002045* (2000).
[11] Kraus, B. and Cirac, J. I. Optimal Creation of Entanglement using a Two-Qubit Gate. *Phys. Rev. A* **63**, 062309 (2001).
[12] Khaneja, N., Brockett, R., and Glaser, S. J. Time Optimal Control in Spin Systems. *Phys. Rev. A* **63**, 032308 (2001).
[13] Lewenstein, M., Krauss, B., Horodecki, P., and Cirac, I. Characterization of Separable States and Entanglement. *Phys. Rev. A* **63**, 044304 (2001).
[14] Bullock, S. and Markov, I. An Elementary Two-Qubit Quantum Computation in Twenty-Three Elementary Gates. *Phys. Rev. A* **68**, 012318 (2003).
[15] Zhang, J., Vala, J., Sastry, S., and Whaley, K. Geometric Theory of Nonlocal Two-Qubit Operations. *Phys. Rev. A* **67**, 042313 (2003).
[16] Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., and Wooters, W. K. Mixed State Entanglement and Quantum Error Correction. *Phys. Rev. A* **54**, 3824 (1996).
[17] Vidal, G. and Dawson, C. A Universal Quantum Circuit for Two-Qubit Transformations with Three CNOT Gates. *quant-ph/0307177* (2003).
[18] Shende, V., Bullock, S., and Markov, I. Recongnizing Small-Circuit Structure in Two-Qubit Operators. *quant-ph/0308045* (2003).
[19] Helgason, S. *Differential geometry, Lie groups, and symmetric spaces*, volume 34. American Mathematical Society, Providence, RI, graduate studies in mathematics, (corrected reprint of the 1978 original) edition, (2001).
[20] Bremner, M., Dodd, J., Nielsen, M., and Bacon, D. Fungible Dynamics: there are only two types of entangling multi-qubit interactions, *quant-ph/0307148* (2003).
[21] Nielsen, M. and Chuang, I. *Quantum Information and Computation*. Cambridge Univ. Press, (2000).
[22] Tucci, R. A Rudimentary Quantum Compiler. *quant-ph/9902062* (1999).
[23] Golub, G. and Loan, C. V. *Matrix Computations*. Johns Hopkins Press, Baltimore, (1996).
[24] Knapp, A. *Lie Groups Beyond an Introduction*, volume 140. Progress in Mathematics, Birkhäuser, (1996).
[25] Uhlmann, A. Fidelity and Concurrence of Conjugated States. *Phys. Rev. A* **62**, 032307 (2000).
[26] Krauss, K. *States, Effects, and Operations*. Springer, Berlin, (1983).