JOURNAL OF MATHEMATICAL PHYSICS **46**, 062104 (2005)

Time reversal and *n*-qubit canonical decompositions

Stephen S. Bullock[a)]
Mathematical and Computational Sciences Division, National Institute of Standards and Technology, Gaithersburg, Maryland 20899

Gavin K. Brennen[b)]
Atomic Physics Division, National Institute of Standards and Technology, Gaithersburg, Maryland 20899

Dianne P. O'Leary[c)]
MCSD, National Institute of Standards and Technology, and Department of Computer Science, University of Maryland, College Park, Maryland 20742

(Received 19 March 2004; accepted 4 March 2005; published online 17 May 2005)

On pure states of n quantum bits, the *concurrence entanglement monotone* returns the norm of the inner product of a pure state with its spin-flip. The monotone vanishes for n odd, but for n even there is an explicit formula for its value on mixed states, i.e., a closed-form expression computes the minimum over all ensemble decompositions of a given density. For n even a matrix decomposition $\nu=k_1ak_2$ of the unitary group is explicitly computable and allows for study of the monotone's dynamics. The side factors k_1 and k_2 of this concurrence canonical decomposition (CCD) are concurrence symmetries, so the dynamics reduce to consideration of the a factor. This unitary a phases a basis of entangled states, and the concurrence dynamics of u are determined by these relative phases. In this work, we provide an explicit numerical algorithm computing $\nu=k_1ak_2$ for n odd. Further, in the odd case we lift the monotone to a two-argument function. The *concurrence capacity* of ν according to the double argument lift may be nontrivial for n odd and reduces to the usual concurrence capacity in the literature for n even. The generalization may also be studied using the CCD, leading again to maximal capacity for most unitaries. The capacity of $\nu\otimes I_2$ is at least that of ν, so odd-qubit capacities have implications for even-qubit entanglement. The generalizations require considering the spin-flip as a time reversal symmetry operator in Wigner's axiomatization, and the original Lie algebra homomorphism defining the CCD may be restated entirely in terms of this time reversal. The polar decomposition related to the CCD then writes any unitary evolution as the product of a time-symmetric and time-antisymmetric evolution with respect to the spin-flip. En route we observe a Kramers' nondegeneracy: the existence of a nondegenerate eigenstate of any *time reversal symmetric n*-qubit Hamiltonian demands (i) n even and (ii) maximal concurrence of said eigenstate. We provide examples of how to apply this work to study the kinematics and dynamics of entanglement in spin chain Hamiltonians. © *2005 American Institute of Physics.* [DOI: 10.1063/1.1900293]

I. INTRODUCTION

The entanglement theory of two quantum bits is now well understood. Let ρ be a mixed two-qubit quantum state, described by a 4×4 Hermitian density matrix. Hill and Wootters[22] describe all classes of ρ up to evolution by unitaries in terms of the concurrence. This concurrence

[a)]Electronic mail: stephen.bullock@nist.gov
[b)]Electronic mail: gavin.brennen@nist.gov
[c)]Electronic mail: oleary@cs.umd.edu

is explicitly a function of the eigenvalues of $\rho(\sigma^y)^{\otimes 2}\overline{\rho}(\sigma^y)^{\otimes 2}$, where the factor $\tilde{\rho}=(\sigma^y)^{\otimes 2}\overline{\rho}(\sigma^y)^{\otimes 2}$ may be interpreted as the spin-flip of ρ. Further, for pure states the entropy of the partial trace to either one-qubit subsystem is a one-to-one function of the concurrence, so that both measures agree as to which two-qubit states are more or less entangled. Local states (tensors) are unentangled, while states locally equivalent to Bell states have maximal entropy and concurrence.

For other systems, entanglement theory is more complicated. Even for two d-level systems (qudits) it is not typical to use a single function to quantify entanglement,[45] and research into generalized concurrences continues.[20] Instead we focus on the multi-partite qubit case. The key point is that it is not sensible in n-qubits to speak of a *unique* maximally entangled state. More precisely, suppose now ρ is a $2^n\times 2^n$ Hermitian density matrix describing a mixed n-qubit state. A unitary evolution is given by a $2^n\times 2^n$ unitary matrix, say ν, with the evolution being $\rho\mapsto\nu\rho\nu^\dagger$. A partial ordering of such ρ as more or less entangled follows by stipulating that (i) for $\nu=\otimes_{j=1}^n\nu_j$ local unitary, ρ and $\nu\rho\nu^\dagger$ are equally entangled, while (ii) the ρ becomes no more entangled on average after applying any sequence of local measurements and local unitaries, i.e., after applying local completely positive maps.[23] More entangled is a partial order which has distinct maximal elements for $n\geqslant 3$. For example, in three qubits, two states which are maximally entangled yet locally inequivalent are given as follows:[16]

$$|GHZ\rangle=(1/\sqrt{2})[|000\rangle+|111\rangle],\quad |W\rangle=(1/\sqrt{3})[|001\rangle+|010\rangle+|100\rangle]. \tag{1}$$

There are nine distinct maxima of the partial order in four qubits,[44] and strong theoretical evidence suggests that the number of such *entanglement types* grows quite rapidly with n (e.g., Ref. 33).

To quantify multi-partite entanglement, one often uses functions known as entanglement monotones.[3,45] All such monotones must vanish on any local state. A monotone might also vanish on certain entangled states but definitively reports that a state is not local should its value be nonzero. The value on a mixed state ρ is defined to be the minimum over all ensemble decompositions of ρ of the ensemble weighted-average. A monotone is convex on density matrices, since entanglement does not increase under mixing of states. Monotones are also nonincreasing *on average* under local quantum operations and classical communication. Among popular monotones are Meyer's Q-measure,[6,32] the Schmidt measure,[18] and certain polynomial invariants[3] of eigenvalues of density matrices representing stochastic mixtures of pure data states.

The n-qubit concurrence is an entanglement monotone. To define the monotone, we first note that *throughout* υ refers to the spin-flip of the n-qubit state space. Concurrence for a pure state[48] is the component on a pure state of its spin-flip:

$$C_n(|\psi\rangle)=|\langle\psi|\upsilon|\psi\rangle|/\langle\psi|\psi\rangle,$$

where

$$\upsilon|\psi\rangle=\overline{(-i\sigma^y)^{\otimes n}|\psi\rangle}=(-i\sigma^y)^{\otimes n}\overline{|\psi\rangle}. \tag{2}$$

The concurrence of an n qubit state with n odd vanishes identically. This monotone is noteworthy for two reasons. First, there is an explicit, computable closed-form expression for the minimum $C_n(\rho)$ which is again defined in terms of the eigenvalues of $\rho\tilde{\rho}=\rho(\sigma^y)^{\otimes n}\overline{\rho}(\sigma^y)^{\otimes n}$.[7,42] Second, in the context of concurrence dynamics we may study entanglement dynamics. This paper concerns itself with the latter topic, and we henceforth consider only pure states and unitary maps.

The primary mathematical tool used in this paper is the concurrence canonical decomposition (CCD). This is discussed in detail in Sec. II. Briefly, it is a way to decompose a unitary on n qubits into a factor that changes concurrence and factors that do not. Let $\nu:\mathcal{H}_n\to\mathcal{H}_n$ be a unitary evolution. Consider the CCD $\nu=k_1ak_2$.[8] Now k_1 and k_2 are symmetries of the concurrence, reducing concurrence dynamics to the second factor. This a factor applies relative phases to a basis of GHZ-like states. Such phases are not unique due to choices of diagonalization while computing the CCD, but the spectrum spec(a^2) is uniquely determined by ν. Moreover, the two-qubit test for maximal entanglement capacity[49] generalizes to n qubit concurrence capacities if n is even:

Let $\nu = k_1 a k_2$ be a CCD of ν. Consider spec(a^2) as a subset of the unit circle. Then for $n = 2p$, there is a $|\psi\rangle \in \mathcal{H}_n$ with $C_n(|\psi\rangle) = 0$ and $C_n(\nu|\psi\rangle) = 1$ if and only if 0 is within the convex hull of spec(a^2).[8,49]

Also, for even n there is an explicit numerical algorithm for computing the CCD and hence spec(a^2).[8]

This work presents three new results. The first is an extension of concurrence capacities to the case n odd. For n even, the concurrence symmetry group K to which k_1, k_2 belong is up to a similarity transform an orthogonal group. For n odd, K is not orthogonal but symplectic, a has repeat eigenvalues, and $C_{2p-1}(|\psi\rangle) = 0$ for all $|\psi\rangle$. Nonetheless, we define a two-argument lift of the usual concurrence, say $\mathcal{C}(|\phi\rangle, |\psi\rangle)$. [See Eq. (7).] Suppose we define the amount of concurrence an odd-qubit unitary ν creates to be

$$\kappa(\nu) = \max\{\mathcal{C}(\nu|\phi\rangle, \nu|\psi\rangle); \mathcal{C}(|\phi\rangle, |\psi\rangle) = 0\}. \tag{3}$$

This generalized capacity has the following properties:

- For n even, the one-argument concurrence capacity and the two-argument capacity of ν coincide.
- For n odd, often $\kappa_n(\nu) \neq 0$ for the pairwise capacity despite $C_n(|\psi\rangle) \equiv 0$. Further, $\kappa_n(\nu) = 1$ if and only if 0 lies within the convex hull of spec(a^2) for any CCD by $\nu = k_1 a k_2$.
- *Concurrence capacity monotonicity:* Using double argument capacities, the capacity of $\nu \otimes I_2$ is always at least that of ν.

Hence there exists a theory of odd-qubit concurrence dynamics, even though concurrence vanishes identically (on the diagonal) in odd qubits.

Second, we present an explicit numerical algorithm for computing the odd-qubit CCD. Various matrix logarithms must be computed, after which one invokes work in the numerical analysis literature[15] to diagonalize a time reversal symmetric Hamiltonian using symplectic matrices.

We close with the third observation, which we will refer to as *Kramers' nondegeneracy:*

On the n-quantum bit state space, suppose that a υ-time reversal symmetric Hamiltonian H has a nondegenerate eigenstate $|\lambda\rangle$. Then (i) n is even and (ii) $C_n(|\lambda\rangle) = 1$. In particular, $|\lambda\rangle$ is entangled, i.e. $|\lambda\rangle \neq \otimes_{j=1}^{n} |\psi_j\rangle$.

The proof follows from viewing υ as a time reversal symmetry operator in Wigner's axiomatization, a point of view which also simplifies the derivation of the CCD. Kramers' nondegeneracy leads one to wonder whether useful entangled states may be produced by cooling the system of qubits coupled to a υ-time reversal symmetric Hamiltonian. We consider the perturbative stability of this entanglement while breaking the time reversal symmetry here, while the thermal stability of the Kramers' nondegeneracy for the quantum XY model is considered elsewhere.[7]

II. BACKGROUND AND PRIOR WORK

Since our key tool is a generalized canonical decomposition,[8] we review the canonical decomposition literature. The two-qubit canonical decomposition (CD) states that any two-quantum bit unitary evolution ν, i.e., any 4×4 unitary matrix ν, may be written:

$$\nu = e^{i\varphi}(u_1 \otimes u_2) a (u_3 \otimes u_4). \tag{4}$$

Here u_1, u_2, u_3, u_4 are one-qubit (2×2) unitary matrices, which may be chosen to have determinant one. The unitary a is diagonal in the Bell basis and may be thought of as applying relative phases to this basis. However, it is better computationally to think of a as phasing the *magic basis*[4,29] instead:

$$|\mathrm{m}0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}, \quad |\mathrm{m}1\rangle = (|01\rangle - |10\rangle)/\sqrt{2},$$

$$|\mathrm{m}2\rangle = (i|00\rangle - i|11\rangle)/\sqrt{2}, \quad |\mathrm{m}3\rangle = (i|01\rangle + i|10\rangle)/\sqrt{2}. \tag{5}$$

Let E be defined by $E|j\rangle = |\mathrm{m}j\rangle$, and let $\mathrm{SU}(2^n)$ denote the Lie group of determinant one $2^n \times 2^n$ unitary matrices, $\mathrm{SO}(2^n)$ denotes determinant one orthogonal matrices, and $\mathrm{D}(2^n)$ denotes the diagonal $2^n \times 2^n$ unitary matrices. A diagonalization argument shows $\mathrm{SU}(4) = \mathrm{SO}(4)\mathrm{D}(4)\mathrm{SO}(4)$. Moreover, the magic basis has the property that $E^\dagger \mathrm{SU}(2) \otimes \mathrm{SU}(2) E = \mathrm{SO}(4)$, i.e., *determinant one* tensors have real matrix coefficients in the basis. Thus the canonical decomposition may be computed by transforming the diagonalization through E:

$$\mathrm{SU}(4) = [E\mathrm{SO}(4)E^\dagger][E\mathrm{D}(4)E^\dagger][E\mathrm{SO}(4)E^\dagger] = \mathrm{SU}(2) \otimes \mathrm{SU}(2)(E\mathrm{D}(4)E^\dagger)\mathrm{SU}(2) \otimes \mathrm{SU}(2). \tag{6}$$

We next provide a brief account and references for the best known applications and generalizations of the CD.

Makhlin[31] anticipates the canonical decomposition by directly computing that the double cosets $[\mathrm{SU}(2)\otimes\mathrm{SU}(2)]\backslash\mathrm{SU}(4)/[\mathrm{SU}(2)\otimes\mathrm{SU}(2)]$ are parametrized by three real parameters, the number of parameters in a given $\det(a)=1$. The CD appears explicitly in Kraus and Cirac.[28] In an important paper, Khaneja, Brockett, and Glaser point out that one may view the CD as an example of the $G=KAK$ decomposition theorem for $G=\mathrm{SU}(4)$, $K=\mathrm{SU}(2)\otimes\mathrm{SU}(2)$, and $A=\Delta$ the commutative Lie group that phases the magic (or Bell) basis.[24] They also consider the matrix factorization from the point of view of control theory in order to compute minimum times for applying a given two-qubit unitary evolution. Zhang, Vala, Sastry, and Whaley made use of this observation to describe which 4×4 unitaries ν are equivalent up to tensors of one-qubit rotations. The factor $a \in \Delta$ is not unique but depends on choices of diagonalization, and these are described geometrically using Weyl chambers. Specifically, the Weyl group orbit of any a produces all possible a, and each orbit intersects the Weyl chamber once. For $G=\mathrm{SU}(4)$, the Weyl chamber is a tetrahedron.[49] The terms canonical decomposition and magic basis are by now standard, and there are published surveys (e.g., Ref. 13, Sec. II.B). Moreover, explicit control sequences for two-qubit unitary evolution have been mapped using the CD [Ref. 37, Eq. (B2)].[14] The timing arguments of Khaneja *et al.*[24] have been recently verified in liquid-state NMR.[35]

There are many applications of the two-qubit CD. In addition to timing as above, they include (i) studying the entanglement capacity of two-qubit operations,[49] (ii) building efficient (small) quantum circuits in two qubits,[10,41,43,46] and (iii) classifying which two-qubit computations require fewer than average multiqubit interactions.[41,46]

Besides the CCD,[8] there is another n-qubit generalization of the canonical decomposition due to Khaneja and Glaser.[25] It is also defined in terms of a $G=KAK$ decomposition. Label $N=2^n$ for the remainder. The type of a $G=KAK$ decomposition follows from a classification theorem of Cartan involutions and determines the groups K and A up to Lie isomorphism. [The classification appears in Helgason (Ref. 21, p. 518, see the same for details).] Given $G=\mathrm{SU}(N)$, the three possible types demand $K\cong\mathrm{SO}(N)$ (type **AI**), $K\cong\mathrm{Sp}(N/2)$ a symplectic group (type **AII**), or $K \cong \mathrm{S}[\mathrm{U}(p)\oplus\mathrm{U}(q)]$ for $p+q=N$ a block unitary (type **AIII**). In the **AII** case, the structure of the A group also demands any $a\in A$ has even-degenerate eigenvalues. The two-qubit canonical decomposition is type **AI**, and indeed the similarity transform by E shows $\mathrm{SU}(2)\otimes\mathrm{SU}(2)\cong\mathrm{SO}(4)$. The CCD alternates **AI** and **AII** as n is even or odd. The KGD of Khaneja and Glaser technically contains two $G=KAK$ decompositions, the first of which is type **AIII** for $n>2$. In fact, the KGD is similar to the cosine sine decomposition (CSD) of numerical linear algebra[11] and so may be computed numerically. Physically, the $K\cong\mathrm{S}[\mathrm{U}(N/2)\oplus\mathrm{U}(N/2)]$ group of the KGD may be viewed as those unitaries commuting with measurements in the z basis of the least significant qubit, i.e., commuting with $I_{N/2}\otimes\sigma^z$.

We next recall notation from quantum computing. The one-qubit state space is $\mathcal{H}_1=\mathbb{C}\{|0\rangle\}\oplus\mathbb{C}\{|1\rangle\}$. For n quantum bits, $\mathcal{H}_n=(\mathcal{H}_1)^{\otimes n}=\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_1$. (See Ref. 36.) A local state $|\psi\rangle$ is any state which may be written as $\otimes_{j=1}^n|\psi_j\rangle$ for $|\psi_j\rangle\in\mathcal{H}_1$, while an *entangled* state is any state which is not local. Notations such as, e.g., $|7\rangle$ refer not to the state of a qudit but rather to a multiqubit state, e.g., $|7\rangle = |1\rangle \otimes |1\rangle \otimes |1\rangle$. The n-concurrence of Eq. (2) is an entanglement monotone.[8] Besides the well-known two-qubit concurrence,[22] even qubit concurrences n-qubits [Ref. 48, Ref. 40—Eq. (62), Ref. 8] have also been studied. Since the single-argument concurrence vanishes for n odd, we introduce a two-argument generalization.

For υ per Eq. (2), the *concurrence bilinear form*[8] is the map $\mathcal{C}_n : \mathcal{H}_n \times \mathcal{H}_n \to \mathbb{C}$ given by

$$\mathcal{C}_n(|\phi\rangle, |\psi\rangle) = \overline{\langle \phi | \upsilon | \psi \rangle}. \tag{7}$$

The complex conjugate forces the two-argument function to be complex bilinear rather than complex bi-antilinear, and the concurrence monotone is the norm of the form on the diagonal: $\mathcal{C}_n(|\phi\rangle) = |\mathcal{C}_n(|\phi\rangle, |\phi\rangle)|$. The bilinear form $\mathcal{C}_n$ is symmetric for n even and antisymmetric for n odd, which causes vanishing of the monotone *but not the form* in the odd-qubit case.

The CD is an example of the $G=KAK$ decomposition theorem (Ref. 21, Theorem 8.6, Sec. VII.8) for $G=\mathrm{SU}(N)$. This theorem produces a decomposition of a reductive Lie group G for any θ, $\mathfrak{a}$ as follows:

- The map $\theta : \mathfrak{g} \to \mathfrak{g}$ for $\mathfrak{g} = \mathrm{Lie}(G)$ is a Cartan involution (Ref. 21, Sec. X.6.3, p. 518). By definition,[50] (i) $\theta^2 = \mathbf{1}_{\mathfrak{g}}$ and (ii) $\theta[X,Y] = [\theta X, \theta Y]$ for all $X, Y \in \mathfrak{g}$. As is standard, we write $\mathfrak{g} = \mathfrak{p} \oplus \mathfrak{k}$ for the decomposition of $\mathfrak{g}$ into the -1 and $+1$ eigenspace of θ.
- Given θ, $\mathfrak{a} \subset \mathfrak{p}$ is a commutative subalgebra which is maximal commutative in $\mathfrak{p}$.

Note that $\mathfrak{k}$ is closed under the Lie bracket, while this is trivially true for $\mathfrak{a}$. Thus the exponential of each is a group. Label $K = \exp \mathfrak{k}$, $A = \exp \mathfrak{a}$, where for linear $G \subset GL(n, \mathbb{C})$ the exponential may be interpreted as a matrix exponential. The theorem then asserts that $G = KAK = \{k_1 a k_2 ; k_1, k_2 \in K, a \in A\}$.

The CD is seen to be an example as follows, cf. Ref. 24. Take $\theta : \mathfrak{su}(4) \to \mathfrak{su}(4)$ by $\theta(X) = (-i\sigma^y)^{\otimes 2} \overline{X} (-i\sigma^y)^{\otimes 2}$ and $\mathfrak{a} = \mathrm{span}_{\mathbb{R}}\{ i|0\rangle\langle 0| - i|1\rangle\langle 1| - i|2\rangle\langle 2| + i|3\rangle\langle 3|, i|0\rangle\langle 3| + i|3\rangle\langle 0|, i|1\rangle\langle 2| + i|2\rangle \times \langle 1| \}$. Extending these choices to n qubits produces the CCD:

Definition II.1: [CCD, Ref. 8] Define $\theta : \mathfrak{su}(N) \to \mathfrak{su}(N)$ by $\theta(X) = [(-i\sigma^y)^{\otimes n}]^\dagger \overline{X} (-i\sigma^y)^{\otimes n}$. Then $\mathfrak{k}$ denotes the $+1$-eigenspace of θ while $\mathfrak{p}$ denotes the -1-eigenspace. Finally, in case n is even we define

$$\begin{aligned}\mathfrak{a} = \mathrm{span}_{\mathbb{R}}(\{ & i|j\rangle\langle j| + i|N-j-1\rangle\langle N-j-1| - i|j+1\rangle\langle j+1| - i|N-j-2\rangle\langle N-j-2|; \quad 0 \leqslant j \leqslant 2^{n-1} \\ & - 2\} \sqcup \{ i|j\rangle\langle N-j-1| + i|N-j-1\rangle\langle j| ; 0 \leqslant j \leqslant 2^{n-1}-1\},)\end{aligned} \tag{8}$$

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

$$\begin{aligned}\mathfrak{a} = \mathrm{span}_{\mathbb{R}}(\{ & i|j\rangle\langle j| + i|N-j-1\rangle\langle N-j-1| - i|j+1\rangle\langle j+1| - i|N-j-2\rangle\langle N-j-2|; \\ & 0 \leqslant j \leqslant 2^{n-1} - 2\}).\end{aligned} \tag{9}$$

The *concurrence canonical decomposition (CCD)* in n-qubits is the resulting matrix decomposition $\mathrm{SU}(N) = KAK$. Note that n may be even or odd.

In an earlier work,[8] computations in Dirac (bra-ket) notation show that $\theta(X)$ is a Cartan involution and $\mathfrak{a}$ is maximal-commutative in $\mathfrak{p}$. The $G=KAK$ theorem (Ref. 21, Theorem 8.6, Sec. VII.8) then shows that the CCD exists. Further, the CCD may be computed numerically in the even qubit case.[8]

The CCD is a useful tool for studying concurrence capacities since $K = \exp(\mathfrak{k})$ consists of symmetries of the concurrence form of Eq. (7), where $\mathfrak{k}$ is given per Definition II.1,[8]

$$(\nu \in K) \Leftrightarrow [\mathcal{C}_n(\nu|\phi\rangle, \nu|\psi\rangle) = \mathcal{C}_n(|\phi\rangle, |\psi\rangle) \text{ for all } |\phi\rangle, |\psi\rangle \in \mathcal{H}_n]. \tag{10}$$

In particular, the above may be used to verify that $\mathrm{SU}(2)^{\otimes n} \subseteq K$ as a subgroup of large codimension. One explanation for the fact that K alternates between orthogonal and symplectic groups is to note that the form $\mathcal{C}_n$ is symmetric or antisymmetric as n is even or odd.[8] Another outlook, illustrated in Sec. V, is that the spin-flip υ is a bosonic or fermionic time reversal symmetry operator as n is even or odd, i.e., $\upsilon^{-1}=(-1)^n\upsilon$.

III. ODD-QUBIT CONCURRENCE CAPACITIES

The main results of this section are summarized in Theorem III.11. Each is proven in turn.

A. Double-argument capacities generalize single-argument capacities

To begin, we introduce a pairwise concurrence capacity $\kappa_n(\nu)$ and denote earlier concurrence capacities[8] with a tilde,

$$\begin{gathered}\tilde{\kappa}_n(\nu)=\max\{\mathcal{C}_n(\nu|\psi\rangle);\langle\psi|\psi\rangle=1,\mathcal{C}_n(|\psi\rangle)=0\},\\ \kappa_n(\nu)=\max\{|\mathcal{C}_n(\nu|\phi\rangle,\nu|\psi\rangle)|;\langle\phi|\phi\rangle=\langle\psi|\psi\rangle=1,\mathcal{C}_n(|\phi\rangle,|\psi\rangle)=0\}.\end{gathered} \tag{11}$$

Due to Eq. (10), any CCD of a unitary $\nu=k_1ak_2$ implies $\tilde{\kappa}_n(\nu)=\tilde{\kappa}_n(a)$[8] and $\kappa_n(\nu)=\kappa_n(a)$.

Proposition III.1: Suppose $n=2p$ is an even number of qubits. Then $\kappa_n(\nu)=\tilde{\kappa}_n(\nu)$.

The proof requires certain results from the literature.[8,49]

- There is an $n=2p$ qubit entangler E_0 so that for any $k\in K$, $E_0kE_0^\dagger$ is a real unitary matrix, i.e., orthogonal. The columns of E_0 resemble $|GHZ\rangle$ states.
- For this E_0, any CCD $\nu=k_1ak_2$ moreover has $d=E^\dagger aE$ for $d=\sum_{j=0}^{N-1}d_j|j\rangle\langle j|$ diagonal. As d is unitary diagonal, each d_j is on the unit circle within $\mathbb{C}$.
- The concurrence spectrum becomes $\lambda_c(\nu)=\{d_j^2\}_{j=0}^{N-1}$. Then $\tilde{\kappa}_{2n}(\nu)=1$ if and only if $0\in\mathbb{C}$ lies within the convex hull of $\lambda_c(\nu)$, a subset of the unit circle (Ref. 8, Lemma III.2).
- A corollary (Ref. 8, Scho. 2.18) of the symmetry group theorem shows that E_0 also translates between $\mathcal{C}_n(-,-)$ and a simpler bilinear form: $\mathcal{C}_n(E_0z_1,E_0z_2)=z_1^Tz_2$.

Example III.2: We use the CD to compute a two-qubit concurrence capacity. Consider a family of controlled-phase gates, e.g., $\nu(t)=e^{-it}|0\rangle\langle 0|+e^{-it}|1\rangle\langle 1|+e^{-it}|2\rangle\langle 2|+e^{3it}|3\rangle\langle 3|$ with $\det[\nu(t)]=1$. A possible CD is:

$$\nu(t)=(e^{-it\sigma^z}\otimes I_2)e^{it\sigma^z\otimes\sigma^z}(I_2\otimes e^{-it\sigma^z}). \tag{12}$$

The central factor is a valid choice for a in $\nu(t)=k_1ak_2$, since $e^{it\sigma^z\otimes\sigma^z}$ is also diagonal in the magic basis. Thus $\lambda_c[\nu(t)]=\mathrm{spec}(e^{2it\sigma^z\otimes\sigma^z})=\{e^{2it},e^{2it},e^{-2it},e^{-2it}\}$. Only for $t\in\pi/4\mathbb{Z}$ do we have 0 within the convex hull of $\lambda_c[\nu(t)]$, and the convex hull theorem asserts $\tilde{\kappa}_2[\nu(\pi/4)]=1$. Indeed, up to phase $\nu(\pi/4)=|0\rangle\langle 0|+|1\rangle\langle 1|+|2\rangle\langle 2|-|3\rangle\langle 3|$. Moreover, if

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

is the Hadamard gate,[36] a standard identity converts $\nu(\pi/4)$ into the quantum controlled-not:

$$\mathrm{CNOT}=|00\rangle\langle 00|+|01\rangle\langle 01|+|10\rangle\langle 11|+|11\rangle\langle 10|=(I_2\otimes H)\nu(\pi/4)(I_2\otimes H). \tag{13}$$

Thus $\nu(\pi/4)$ carries an unentangled state to a maximally entangled state, since $\mathrm{CNOT}(H\otimes I_2)|00\rangle=\mathrm{CNOT}(1/\sqrt{2})(|00\rangle+|10\rangle)=(1/\sqrt{2})(|00\rangle+|11\rangle)$. More intricate examples in two-qubits[41,49] and an even number of qubits[9] are available in the literature.

Lemma III.3: Suppose the number of qubits is even. Let $z_1=\sum_{j=0}^{N-1}a_j|j\rangle$, $z_2=\sum_{j=0}^{N-1}b_j|j\rangle$, and $z_3=\sum_{j=0}^{N-1}c_j|j\rangle$ throughout, and let $\lambda_c(\nu)=\{\lambda_j\}_{j=0}^{N-1}$. Then we have the following:

$$\tilde{\kappa}_n(\nu)=\max\left\{\left|\sum_{j=0}^{N-1}c_j^2\lambda_j\right|;z_3^\dagger z_3=1,z_3^Tz_3=0\right\},$$

$$\kappa_n(\nu) = \max\left\{ \left| \sum_{j=0}^{N-1} a_j b_j \lambda_j \right| ; z_1^\dagger z_1 = z_2^\dagger z_2 = 1, z_1^T z_2 = 0 \right\}. \tag{14}$$

Proof of Lemma III.3: The first equation appears in Ref. 8; cf. Ref. 49. For the second, take vectors z_1, z_2 and label $x=E_0 z_1$, $y=E_0 z_2$. Then

$$[\mathcal{C}_n(x,y) = 0] \Leftrightarrow [\mathcal{C}_n(E_0 z_1, E_0 z_2) = 0] \Leftrightarrow [z_1^T z_2 = 0]. \tag{15}$$

Moreover, without loss of generality by choice of z_1, z_2, and symmetry we may suppose $\nu = E_0 d E_0^\dagger$ for $d^2 = \Sigma_{j=0}^{N-1} \lambda_j |j\rangle\langle j|$. Then $\mathcal{C}_n(E_0 d E_0^\dagger x, E_0 d E_0^\dagger y) = \mathcal{C}_n(E_0 d z_1, E_0 d z_2) = (z_1^T d^T) d z_2 = \Sigma_{j=0}^{N-1} a_j b_j \lambda_j$.

Proof of Proposition III.1: Let a_j, b_j be chosen so as to maximize the expression for $\kappa_n(\nu)$ per Lemma III.3, i.e., $\kappa_n(\nu) = |\Sigma_{j=0}^{N-1} a_j b_j \lambda_j|$. Now choose complex numbers c_j so that $c_j^2 = a_j b_j$, and put $z_3 = \Sigma_{j=0}^{N-1} c_j |j\rangle$. We note that $z_3^T z_3 = 0$. Moreover, $z_3^\dagger z_3 \leqslant 1$, for

$$\sum_{j=0}^{N-1} |c_j|^2 = \sum_{j=0}^{N-1} |c_j^2| = \sum_{j=0}^{N-1} |a_j b_j| \leqslant \sum_{j=0}^{N-1} \frac{1}{2}|a_j|^2 + \frac{1}{2}|b_j|^2 = 1. \tag{16}$$

Label $t^2 = z_3^\dagger z_3$, noting $t^2 \leqslant 1$. Then $(t^{-1} z_3)^\dagger (t^{-1} z_3) = 1$, so by definition of $\tilde{\kappa}_{2p}(\nu)$ we have

$$\kappa_n(\nu) \geqslant \tilde{\kappa}_n(\nu) \geqslant \left| \sum_{j=0}^{N-1} t^{-2} c_j^2 \lambda_j \right| = t^{-2} \left| \sum_{j=0}^{N-1} a_j b_j \lambda_j \right| = t^{-2} \kappa_n(\nu). \tag{17}$$

Thus $t=1$ and hence $\kappa_n(\nu) = \tilde{\kappa}_n(\nu)$. □

B. Monotonicity

We next demonstrate concurrence capacity monotonicity, i.e., that $j \mapsto \kappa_{n+j}(\nu \otimes I_2^{\otimes j})$ is monotonic. It provides another justification for odd-qubit concurrence capacities, despite $\mathcal{C}_{2p-1} \equiv 0$. For if $\kappa_{2p-1}(\nu) > 0$, then there is a $2p$-qubit state $|\psi\rangle$ with $C_{2p}(|\psi\rangle) = 0$ while $C_{2p}[(\nu \otimes I_2)|\psi\rangle] \geqslant \kappa_{2p-1}(\nu)$.

Proposition III.4: Let n be either even or odd, $\nu \in \mathrm{SU}(N)$ an n-qubit computation, and let I_2 denote the trivial one-qubit computation. Then $\kappa_{n+1}(\nu \otimes I_2) \geqslant \kappa_n(\nu)$.

Proof: Choose $|\phi\rangle$, $|\psi\rangle$ such that $\kappa_n(\nu) = \mathcal{C}_n(\nu|\phi\rangle, \nu|\psi\rangle)$ while $\mathcal{C}_n(|\phi\rangle, |\psi\rangle) = 0$. Then $|\phi\rangle \otimes |0\rangle$ and $|\psi\rangle \otimes |1\rangle$ are a null-concurrent pair of $(n+1)$-qubit states:

$$\mathcal{C}_{n+1}(|\phi\rangle \otimes |0\rangle, |\psi\rangle \otimes |1\rangle) = \overline{(\langle\phi| \otimes \langle 0|)}(-i\sigma^y)^{\otimes n+1}(|\psi\rangle \otimes |1\rangle) = [\mathcal{C}_n(|\phi\rangle, |\psi\rangle)](\overline{\langle 0|}(-i\sigma^y)|1\rangle). \tag{18}$$

Now $\overline{\langle 0|}(-i\sigma^y)|1\rangle = 1$, so the above expression is $[0](1) = 0$. A similar argument demonstrates that

$$\mathcal{C}_{n+1}[(\nu \otimes I_2)(|\phi\rangle \otimes |0\rangle), (\nu \otimes I_2)(|\psi\rangle \otimes |1\rangle)] = [\mathcal{C}_n(\nu|\phi\rangle, \nu|\psi\rangle)][\mathcal{C}_1(|0\rangle, |1\rangle)]. \tag{19}$$

The second term of the product is one, while the first is $\kappa_n(\nu)$. Thus we have exhibited a pair for which $\nu \otimes I_2$ raises the pairwise concurrence by at least $\kappa_n(\nu)$. Since $\kappa_{n+1}(\nu \otimes I_2)$ is the maximum over all null-concurrent pairs, while $|\phi\rangle \otimes |0\rangle$, $|\psi\rangle \otimes |1\rangle$ is such, we see $\kappa_{n+1}(\nu \otimes I_2) \geqslant \kappa_n(\nu)$. □

C. Parity-independent concurrence spectra

We extend the maximal concurrence capacity condition of Zhang *et al.* and Bullock, Brennen[8] to odd-qubit systems. The first step is a definition valid in either parity.

Definition III.5: Let $\nu \in \mathrm{SU}(N)$, $N = 2^n$. For n of either parity, the concurrence spectrum $\lambda_c(\nu)$ is the set $\lambda_c(\nu) = \mathrm{spec}([(-i\sigma^y)^{\otimes n}]^\dagger \nu (-i\sigma^y)^{\otimes n} \nu^T)$. Viewing ν as an $\mathbb{R}$-linear map, equivalently $\lambda_c(\nu) = \mathrm{spec}(\nu \upsilon \nu^\dagger \upsilon^{-1})$.

We briefly show this coincides with the definition of the even-qubit concurrence spectrum of the literature.[8] The definition ibid. states that the concurrence spectrum is the spectrum of $(E_0^\dagger \nu E_0)(E_0^\dagger \nu E_0)^T$. Indeed, given $E_0 E_0^T = (-i\sigma^y)^{\otimes n}$ per the classification of E with $E\mathrm{SO}(N)E^\dagger = K$ ibid.,

$$\mathrm{spec}(E_0^\dagger \nu E_0)(E_0^\dagger \nu E_0)^T = \mathrm{spec}(E_0^\dagger \nu E_0 E_0^T \overline{E_0}) = \mathrm{spec}[(E_0 E_0^T)^\dagger \nu E_0 E_0^T \nu^T] = \mathrm{spec}[(-i\sigma^y)^{\otimes n}\nu(-i\sigma^y)^{\otimes n}\nu^T]. \tag{20}$$

In fact, the same argument shows that $\lambda_c(\nu)$ is the spectrum $(E^\dagger \nu E)(E^\dagger \nu E)^T$ for any E as above, cf. Ref. 31.

The odd-qubit case requires different similarity matrices, say F,[8] which translate K not into an orthogonal group but rather a symplectic group per Eq. (22). For the concurrence form $\mathcal{C}_n(-,-)$ n-odd is antisymmetric, and symplectic rather than orthogonal groups are the appropriate symmetries of antisymmetric bilinear forms (i.e., two-forms). For a standard similarity matrix, we take

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

where

$$\{\iota_j\}_{j=0}^{N/2-1} \subset \{\pm 1\} \text{ by } (-i\sigma^y)^{\otimes n} = \sum_{j=0}^{N/2-1} \iota_j(|N-j-1\rangle\langle j| - |j\rangle\langle N-j-1|). \tag{21}$$

Also, label throughout $J_N = (-i\sigma^y)\otimes I_{N/2}$. Before showing that F_0 translates K into the standard symplectic group, we show that F_0 carries $\mathcal{C}(-,-)$ to the standard two-form $\mathcal{A}(-,-)$.

Lemma III.6: For $\mathcal{A}(|\phi\rangle,|\psi\rangle) = \overline{\langle\phi|} J_N |\psi\rangle$, $\mathcal{C}_n(F_0|\phi\rangle, F_0|\psi\rangle) = \mathcal{A}(|\phi\rangle,|\psi\rangle)$ *for all* $|\phi\rangle,|\psi\rangle \in \mathcal{H}_n$.

Proof: $\mathcal{C}_n(F_0|\phi\rangle, F_0|\psi\rangle) = \overline{\langle\phi|} F_0^T (-i\sigma^y)^{\otimes n} F_0 |\psi\rangle$. Now $F_0 J_N F_0^T = (-i\sigma^y)^{\otimes n}$ [Ref. 8, Proposition II.14], whence $F_0^T(-i\sigma^y)^{\otimes n} F_0 = J_N$. □

Now $\mathrm{Sp}(N/2)$ is that copy of the symplectic group which embeds within $\mathrm{SU}(N)$ as the symmetries of $\mathcal{A}(-,-)$, i.e., satisfying $\mathcal{A}(\nu|\phi\rangle, \nu|\psi\rangle) = \mathcal{A}(|\phi\rangle,|\psi\rangle)$ for all $|\phi\rangle,|\psi\rangle \in \mathcal{H}_n$. In block form:

$$\begin{aligned}\mathrm{Sp}(N/2) &= \{\nu \in \mathrm{SU}(N); \nu^T J_N \nu = J_N\} \\ &= \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{SU}(N); \begin{matrix} A^T C \text{ is symmetric}, B^T D \text{ is symmetric}, \\ A^T D - C^T B = I \end{matrix} \right\}\end{aligned} \tag{22}$$

As $E_0 \mathrm{SO}(N)\, E_0^\dagger = K_{2p}$, so too $F_0 \mathrm{Sp}(N/2)\, F_0^T = K_{2p-1}$.

We next associate $\lambda_c(\nu)$ to $\mathrm{spec}(a^2)$ for $\nu = k_1 a k_2$ in the odd-qubit case. Suppose we label D to be the following diagonal subalgebra of $\mathrm{SU}(N)$:

$$D = \left\{ \sum_{j=0}^{N/2-1} d_j(|j\rangle\langle j| + |N/2+j\rangle\langle N/2+j|);\ \prod_{j=0}^{N/2-1} d_j = \pm 1 \right\}. \tag{23}$$

Now there is a standard $\mathrm{SU}(N) = KAK$ decomposition which follows from $\theta_{\mathbf{AII}}(iH) = J_N(-iH^T)J_N^\dagger$ (Ref. 21, Sec. X.2, p. 452) and $\mathfrak{a} = \log D$ as above. Given a $\nu \in \mathrm{SU}(2^{2p-1})$, it writes $\nu = \omega_1 d \omega_2$, with $\omega_j \in \mathrm{Sp}(N/2)$, $j=1,2$ and $d \in D$.

Suppose given $\nu \in \mathrm{SU}(2^{2p-1})$, we then write $F_0^T \nu F_0 = \omega_1 d \omega_2$, with $\omega_j \in \mathrm{Sp}(N/2)$, $j=1,2$ and $d \in D$. The odd-qubit CCD again follows by a similarity transform: $\nu = (F_0\omega_1 F_0^T)(F_0 d F_0^T) \times (F_0 \omega_2 F_0^T)$ with $a = F_0 d F_0^T \in A$, $k_j = F_0 \omega_j F_0^T \in K$, $j=1,2$ is a CCD. Note that a is diagonal on the GHZ-like basis states $\{F_0|j\rangle\}$.

Lemma III.7: Let $n = 2p-1$. *Then for* $\nu = (F_0\omega_1F_0^T)(F_0dF_0^T)(F_0\omega_2F_0^T)$ *the CCD as above with* $d = \sum_{j=0}^{N/2-1} d_j(|j\rangle\langle j| + |N/2+j\rangle\langle N/2+j|)$ *diagonal and determinant one, we have* $\lambda_c(\nu) = \{d_j^2\}_{j=0}^{N/2-1} \sqcup \{d_j^2\}_{j=0}^{N/2-1}$ (*counted with multiplicity*.)

Proof: Given A, B, invertible, $\mathrm{spec}(AB)=\mathrm{spec}(BA)$. Also, Eq. (10) is equivalent to a matrix equation $k^T(-i\sigma^y)^{\otimes n}k=(-i\sigma^y)^{\otimes n}$ for all $k\in K$. Recall $F_0J_NF_0^T=(-i\sigma^y)^{\otimes n}$. Then

$$\begin{aligned}\lambda_c(\nu) &= \mathrm{spec}([(-i\sigma^y)^{\otimes n}]^\dagger \nu(-i\sigma^y)^{\otimes n}\nu^T) = \mathrm{spec}([(-i\sigma^y)^{\otimes n}]^\dagger k_1ak_2(-i\sigma^y)^{\otimes n}k_2^Ta^Tk_1^T)\\ &= \mathrm{spec}(k_1^T[(-i\sigma^y)^{\otimes n}]k_1ak_2[(-i\sigma^y)^{\otimes n}]^Tk_2^Ta^T) = \mathrm{spec}(k_1^T[(-i\sigma^y)^{\otimes n}]k_1a[k_2^T(-i\sigma^y)^{\otimes n}k_2]^Ta^T)\\ &= \mathrm{spec}([(-i\sigma^y)^{\otimes n}]a[(-i\sigma^y)^{\otimes n}]^Ta^T) = \mathrm{spec}(-[F_0J_NF_0^T]F_0dF_0^T[F_0J_NF_0^T]F_0d^TF_0^T)\\ &= \mathrm{spec}(-F_0J_NdJ_Nd^TF_0^T) = \mathrm{spec}(-J_NdJ_Nd) = \mathrm{spec}(d^2).\end{aligned} \tag{24}$$

The last equality makes use of $d\in D$ repeat diagonal. □

D. A convex hull argument in odd qubits

Definition III.8: Suppose $n=2p-1$. The *reduced concurrence spectrum* $\tilde{\lambda}_c(\nu)$ of $\nu\in SU(N)$ is the set $\{\lambda_j\}_{j=0}^{N/2-1}$ for $\nu=k_1(F_0dF_0^T)k_2$ a canonical decomposition of ν and $d=\Sigma_{j=0}^{N/2-1}\sqrt{\lambda_j}(|j\rangle\langle j|+|N/2+j\rangle\langle N/2+j|)$. The *convex hull* $\mathrm{CH}[\tilde{\lambda}_c(\nu)]$ of $\tilde{\lambda}_c(\nu)$ is the set of convex linear combinations of the points of $\tilde{\lambda}_c(\nu)$, i.e.,

$$\mathrm{CH}[\tilde{\lambda}_c(\nu)] = \left\{\sum_{j=0}^{N/2-1} t_j\lambda_j; 0\leqslant t_j\leqslant 1,\ \sum_{j=0}^{N/2-1} t_j = 1, \lambda_j\in\tilde{\lambda}_c(\nu)\right\}. \tag{25}$$

Proposition III.9: Suppose $n=2p-1$ is an odd number of qubits. Throughout, label $z_1=\Sigma_{j=0}^{N-1}a_j|j\rangle$, $z_2=\Sigma_{j=0}^{N-1}b_j|j\rangle$, and $\tilde{\lambda}_c(\nu)=\{\lambda_j\}_{j=0}^{N/2-1}$. Then the following hold:

- $\kappa_n(\nu)=\max\{|\Sigma_{j=0}^{N/2-1}\lambda_j(a_{N/2+j}b_j-a_jb_{N/2+j})|; z_1^TJ_Nz_2=0, z_1^\dagger z_1=z_2^\dagger z_2=1\}$,
- $(\kappa_n(\nu)=1)\Leftrightarrow(0\in\mathrm{CH}[\tilde{\lambda}_c(\nu)])$.

Proof: The first item follows from Lemma III.6, substituting $x=F_0z_1$, $y=F_0z_2$. We continue to the next item.

For the second item, we first prove ⇒. If $\kappa_n(\nu)=1$, then we may choose z_1, z_2 so that

$$\begin{aligned}1 &= \left|\sum_{j=0}^{N/2-1}\lambda_j(a_{N/2+j}b_j-a_jb_{N/2+j})\right| \leqslant \sum_{j=0}^{N/2-1}|a_{N/2+j}b_j-a_jb_{N/2+j}|\\ &\leqslant \sum_{j=0}^{N/2-1}\sqrt{|a_j|^2+|a_{N/2+j}|^2}\sqrt{|b_j|^2+|b_{N/2+j}|^2}\leqslant 1.\end{aligned} \tag{26}$$

Here, note that the second inequality is an iterate of $\mathcal{C}_1(|\phi\rangle,|\psi\rangle)\leqslant\sqrt{\langle\phi|\phi\rangle\langle\psi|\psi\rangle}$, for all $|\phi\rangle,|\psi\rangle\in\mathcal{H}_1$. The last inequality in Eq. (26) is the Schwarz inequality.

Now label $\alpha_j=a_{N/2+j}b_j-a_jb_{N/2+j}$, for $0\leqslant j\leqslant N/2-1$. Then by Eq. (26),

$$1 = \left|\sum_{j=0}^{N/2-1}\lambda_j\alpha_j\right| = \sum_{j=0}^{N/2-1}|\lambda_j\alpha_j| = \sum_{j=0}^{N/2-1}|\alpha_j|. \tag{27}$$

Thus there must exist some $z\in\mathbb{C}$, $z\overline{z}=1$, so that $\lambda_j\alpha_j=z|\alpha_j|$, and moreover $\Sigma_{j=0}^{N/2-1}|\alpha_j|=1$. On the other hand, $z_1^TJ_Nz_2=0$ demands that $0=\Sigma_{j=0}^{N/2-1}\alpha_j=z\Sigma_{j=0}^{N/2-1}|\alpha_j|\overline{\lambda_j}$. Multiplying by $\overline{z}$ and taking the complex conjugate, $0=\Sigma_{j=0}^{N/2-1}|\alpha_j|\lambda_j$ which given $\Sigma_{j=0}^{N/2-1}|\alpha_j|=1$ by Eq. (27) demands $0\in\mathrm{CH}[\tilde{\lambda}_c(\nu)]$.

Consider now the converse case, i.e., $0\in\mathrm{CH}[\tilde{\lambda}_c(\nu)]$. Then there exist t_j real, non-negative so that $0=\Sigma_{j=0}^{N/2-1}t_j\lambda_j$. For $0\leqslant j\leqslant N/2-1$, label complex numbers $\alpha_j=t_j\overline{\lambda_j}$, so that we have $1=\Sigma_{j=0}^{N/2-1}|\alpha_j|$ and moreover $0=\overline{0}=\Sigma_{j=0}^{N/2-1}t_j\overline{\lambda_j}=\Sigma_{j=0}^{N/2-1}\alpha_j$. We are reduced to the following question: May we choose $\{a_j\}_{j=0}^{N-1}$, $\{b_j\}_{j=0}^{N-1}$ so that

$$\alpha_j = a_{N/2+j}b_j - a_j b_{N/2+j}, \quad \sum_{j=0}^{N-1} |a_j|^2 = \sum_{j=0}^{N/2-1} |b_j|^2 = 1. \tag{28}$$

To do this, write $\alpha_j = |\alpha_j| e^{i \arg \alpha_j}$, and take $a_j = \sqrt{|\alpha_j|}$, $a_{N/2+j}=0$, $b_j=0$, and $b_{N/2+j} = -e^{i \arg \alpha_j}\sqrt{|\alpha_j|}$. Then we see that $a_{N/2+j}b_j - a_j b_{N/2+j} = \alpha_j$. Moreover,

$$|a_j|^2 + |a_{N/2+j}|^2 = |\alpha_j|, \quad |b_j|^2 + |b_{N/2+j}|^2 = |\alpha_j|, \quad \sum_{j=0}^{N/2-1} |\alpha_j| = 1. \tag{29}$$

Thus the vectors z_1, z_2 per the statement of the proposition are normalized to be norm one. □

Hence, as in the even-qubit case, a convex hull criterion on the middle factor of the CCD determines which odd-qubit unitaries ν have concurrence capacity equal to the maximal possible capacity, i.e., one. The new feature, doubly degenerate eigenvalues in $\lambda_c(\nu)$ arising from the D above required for type **AII** will *a posteriori* be an instance of Kramers' degeneracy; see Sec. V.

Corollary III.10: For $n=2p-1$, $\lim_{p\mapsto\infty} da(\{a \in A; \kappa_n(a)=1\})=1$.

The proof of the Corollary follows by considering probability density functions on the unit circle,[8] given that the number of concurrence eigenvalues grows exponentially with n. Thus most unitary evolutions for large n (of either parity) are maximally entangling as measured by concurrence. It would be interesting but technically challenging to restate this in terms of Haar measure du on $\mathrm{SU}(N)$. The difficulty is that the pullback measure from the $K\times A\times K$ to $\mathrm{SU}(N)$ is singular, namely singular near the set where the A factor is an identity. For future reference, we summarize the concurrence capacity results of this section.

Theorem III.11: *Let* $\kappa_n(\nu)$, $\tilde{\kappa}_n(\nu)$ *be the pairwise concurrence capacity and concurrence capacity, respectively*.

1. *The pairwise capacity and the capacity are equal in any even number of qubits. Thus,*

$$\tilde{\kappa}_n(\nu) = \begin{cases} \kappa_n(\nu), & n = 2p \text{ even} \\ 0, & n = 2p-1 \text{ odd}. \end{cases} \tag{30}$$

2. *For n either even or odd, any CCD by* $\nu=k_1ak_2$ *satisfies* $\kappa_n(\nu=k_1ak_2)=\kappa_n(a)$.
3. *For any n, we must have* $\kappa_{n+1}(\nu\otimes I_2)\geqslant\kappa_n(\nu)$.
4. *Suppose* $n=2p-1$ *is odd. Then for da the Haar measure on A,*

$$\lim_{p\mapsto\infty} \mathrm{Prob}(\kappa_n(a)=1) = \lim_{p\mapsto\infty} da(\{a \in A; \kappa_n(a)=1\}) = 1. \tag{31}$$

IV. AN ALGORITHM COMPUTING THE ODD-QUBIT CCD

In this section, we close a gap in the literature. Specifically, we present an algorithm for computing the CCD when the number of qubits is odd. We make use of an algorithm[15] by Dongarra, Gabriel, Koelling, and Wilkinson cited in a survey[12] of diagonalization arguments. The algorithm,[15] which appears in the numerical matrix analysis literature, improves the numerical stability and computational efficiency of the earlier work on time reversal by Dyson.[17]

Recall from Sec. III C that it suffices to compute the standard type **AII** *KAK* decomposition given by $\mathrm{SU}(N)=\mathrm{Sp}(N/2)D\mathrm{Sp}(N/2)$ with D the repeat diagonal subgroup of $\mathrm{SU}(N)$. For given $\nu\in\mathrm{SU}(2^{2p-1})$ for which we wish to compute the CCD, suppose we obtain $F_0^T\nu F_0=\omega_1 d\omega_2$, with $\omega_j\in\mathrm{Sp}(N/2)$, $j=1,2$ and $d\in D$. Then ν will have CCD $\nu=k_1ak_2=(F_0\omega_1F_0^T)(F_0dF_0^T)(F_0\omega_2F_0^T)$. Before computing $\mathrm{SU}(N)=\mathrm{Sp}(N/2)D\mathrm{Sp}(N/2)$, we make one new definition.

Definition IV.1: Let $H\in\mathbb{C}^{N\times N}$ be Hermitian. Recall $J_N=(-i\sigma^y)\otimes I_{N/2}$. We say that the Hamiltonian H is J_N*-skew symmetric* iff $HJ_N-J_NH^T=0$.

Remark IV.2: In Ref. 15, the above is the definition of "H has a time reversal symmetry." Indeed, time reversal symmetry follows for the operator $\Theta=J_N\tau$, (τ complex conjugation) per the upcoming Definition V.1. Moreover, for the standard type **AII** Cartan involution (Ref. 21, p. 452)

$\theta_{\mathbf{AII}}(X)=J_N\overline{X}J_N^T$, let $\mathfrak{su}(N)=\mathfrak{p}_{\mathbf{AII}}\oplus\mathfrak{k}_{\mathbf{AII}}$ for the corresponding Cartan decomposition into $\underline{-1}$ and $+1$ eigenspaces. Then H is J_N skew-symmetric if and only if $iH\in\mathfrak{p}_{\mathbf{AII}}$. Indeed on $\mathfrak{su}(N)$, $\overline{X}=-X^T$. Hence $-iH=J_N\overline{iH}J_N^T=-J_NiH^TJ_N^T$ if and only if $HJ_N=J_NH^T$.

A. Algorithm for the standard AII *KAK* decomposition, SU(N)=Sp(N/2)DSp(N/2)

The outline below for computing the standard $\mathrm{SU}(N)=KAK$ decomposition of type **AII** (see Sec. III C) is similar to the **AI** case used in Ref. 8 to compute the even-qubit CCD. The added difficulties are (i) a more complicated formula for p^2 and (ii) a more delicate diagonalization argument for p^2 once computed. In fact, the latter requires the symplectic diagonalization argument referenced above.

Lemma IV.3: Suppose $\nu\in\mathrm{SU}(N)$ with $\nu=pk$ for $p=\exp(iH)$ with H a J_N skew-symmetric Hamiltonian and $k\in\mathrm{Sp}(N/2)$. Then $p^2=-\nu J_N\nu^TJ_N$.

Proof: We have $H^T=-J_NHJ_N$, given $J_N^\dagger=J_N^T=-J_N$. Thus for any $t\in\mathbb{R}$, $[\exp(iHt)]^T=J_N^\dagger\exp(iHt)J_N=-J_N\exp(iHt)J_N$. This holds in particular for p. Now put $w=\nu^\dagger$, so that $w=\widetilde{k}\widetilde{p}$ for $\widetilde{k}=k^\dagger$, $\widetilde{p}=p^\dagger$. Thus $\widetilde{p}^T=J_N^\dagger\widetilde{p}J_N$. Moreover, $k\in\mathrm{Sp}(N/2)$ demands $\widetilde{k}^TJ_N\widetilde{k}=J_N$, as $\mathrm{Sp}(N/2)$ is a group. Thus $-J_Nw^TJ_Nw=\widetilde{p}^2$. Taking the adjoint of each side produces the result. □

With this lemma, we now present the algorithm for computing the standard type **AII** decomposition.

1. Suppose $\nu=pk$ per Lemma IV.3. Compute $p^2=-\nu J_N\nu^TJ_N$.
2. We may write $p=\exp(iH)$ for some J_N skew-symmetric Hamiltonian H. Compute a logarithm of $p^2=\exp(2iH)$. The diagonalizing matrix implicit in computing the matrix log need not be symplectic, and generic logarithms will take the form $2iH$ for some $(2)H$ which is J_N skew-symmetric.
3. Compute a symplectic matrix $\omega_1\in\mathrm{Sp}(N/2)$ so that $iH_2=\omega_1^\dagger(iH)\omega_1$ is repeat diagonal, per Sec. IV B.
4. Label $p=\omega_1\exp(iH_2)\omega_1^\dagger$ and $d=\exp(iH_2)$. Compute $\omega_3=p^\dagger\nu$. Then $\omega_3\in\mathrm{Sp}(N/2)$.
5. Put $\omega_2=\omega_1^\dagger\omega_3\in\mathrm{Sp}(N/2)$. Note that $\omega_1d\omega_1^\dagger=p$. Thus the type **AII** decomposition is $\nu=[\omega_1]\times[d][\omega_1^\dagger\omega_3]=\omega_1d\omega_2$.

This concludes the overview of computing $\mathrm{SU}(N)=\mathrm{Sp}(N/2)D\mathrm{Sp}(N/2)$. The next section details step 3.

B. Symplectic diagonalization

In this section we address the problem of finding the eigendecomposition of a matrix H which is J_N skew-symmetric. Generically, these techniques work on any square matrix with an even number of rows and columns, and there are no simplifications when the size is a power of two. Thus we describe the generic case where

$$J_{2\ell}=\begin{pmatrix}\mathbf{0} & -I_\ell\\ I_\ell & \mathbf{0}\end{pmatrix}$$

and $H=H^\dagger$ is also $J_{2\ell}$ skew symmetric.

Explicitly, $J_{2\ell}$-skew symmetric means

$$H=\begin{pmatrix}A & B\\ -\overline{B} & \overline{A}\end{pmatrix},$$

where $A=A^\dagger$ and $B=-B^T$ are $\ell\times\ell$ matrices. We will construct a unitary skew-symmetric Hamiltonian matrix ω of the form

$$\omega = \begin{pmatrix} U & V \\ -\overline{V} & \overline{U} \end{pmatrix},$$

so that the columns of ω are the (right) eigenvectors of H. Each eigenvalue λ_k for $k=1,\ldots,\ell$ of H is real and of multiplicity 2. In particular, both the kth and the $(\ell+k)$th columns of ω are eigenvectors of H corresponding to λ_k. Also, given the block form, $\omega \in \mathrm{Sp}(N/2)$ up to global phase.

The algorithm of Dongarra *et al.*[15] proceeds in two major steps. First we reduce H to block diagonal form using a similarity transformation, and then we use the QR algorithm to find the eigenvalues of the blocks. We consider each of these phases in turn.

First, we construct a skew-symmetric Hamiltonian unitary matrix Q of the form

$$Q = \begin{pmatrix} Q_1 & Q_2 \\ -\overline{Q_2} & \overline{Q_1} \end{pmatrix}$$

so that

$$QHQ^{\dagger} = \begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix}$$

where T is real, symmetric, and tridiagonal. We initialize Q to be the $2\ell \times 2\ell$ identity matrix. In order to preserve the structure, we construct Q as the product of two simple types of matrices:

- The product of 2×2 skew-symmetric Hamiltonian matrices is also skew-symmetric Hamiltonian, and if we let $r^2=|a|^2+|b|^2$, then a matrix of the form

$$\begin{pmatrix} \overline{a}/r & -b/r \\ \overline{b}/r & a/r \end{pmatrix}$$

  is unitary. In addition,

$$\begin{pmatrix} \overline{a}/r & -b/r \\ \overline{b}/r & a/r \end{pmatrix}\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$$

  so the unitary matrix can be used to introduce zeros. Choose j between 1 and ℓ and construct a matrix R as the $2\ell \times 2\ell$ identity matrix except that entries $R_{\ell+j,\ell+j}=\overline{R_{j,j}}=a/r$ and $R_{j,\ell+j} =-\overline{R_{\ell+j,\ell+j}}=-b/r$. Then the product RH is equal to H except that the entries in rows j and $\ell+j$ become

$$\begin{pmatrix} (RH)_{j,k} & (RH)_{j,\ell+k} \\ (RH)_{\ell+j,k} & (RH)_{\ell+j,\ell+k} \end{pmatrix} = \begin{pmatrix} \overline{a}/r & -b/r \\ \overline{b}/r & a/r \end{pmatrix}\begin{pmatrix} A_{j,k} & B_{j,k} \\ -\overline{B_{j,k}} & \overline{A_{j,k}} \end{pmatrix}, \tag{32}$$

  $k=1,\ldots,\ell$. Since this product is skew-symmetric Hamiltonian, so is RH, and it can be shown in a similar way that $(RH)R^{\dagger}$ is skew-symmetric Hamiltonian. Thus we can use R as a similarity transformation that preserves the structure.
- Let S be a real orthogonal matrix of dimension $\ell \times \ell$. Then

$$\begin{pmatrix} S & 0 \\ 0 & S \end{pmatrix}\begin{pmatrix} A & B \\ -\overline{B} & \overline{A} \end{pmatrix}\begin{pmatrix} S^{\dagger} & 0 \\ 0 & S^{\dagger} \end{pmatrix} = \begin{pmatrix} SAS^{\dagger} & SBS^{\dagger} \\ -S\overline{B}S^{\dagger} & S\overline{A}S^{\dagger} \end{pmatrix} \tag{33}$$

  is skew-symmetric Hamiltonian.

Using these matrices, our construction takes $\ell-1$ steps. We describe the first step in detail.

The first step places zeros in the first column of the matrix in rows 3 through 2ℓ. To put a zero in position $(\ell+j,1)$ $(j=1,\ldots,n)$, we construct an R matrix involving rows j and $\overline{\ell+j}$. If $r_j^2 = |A_{j,1}|^2 + |B_{j,1}|^2$, then this matrix R_j is the identity matrix except that entries $R_{\ell+j,\ell+j} = \overline{R_{j,j}} = A_{j,1}/r_j$ and $R_{j,\ell+j} = -R_{\ell+j,\ell+j} = -B_{j,1}/r_j$. We replace H by $(RH)R^\dagger$ and update Q by premultiplying by R_j, repeating this for $j=1,\ldots,\ell$.

We complete the first step by putting zeros in rows 3 through ℓ of column 1. Note that these elements are now real, since elements 2 through ℓ are just the values r_j. Thus we can construct a real orthogonal reflection (Householder) matrix of the form $S=I-2ss^T$ where $\hat{s}=[0,r_2+\|r\|,r_3,\ldots,r_n]^T$ and $s=\hat{s}/\|\hat{s}\|$. A similarity transformation of H by

$$\begin{pmatrix} S & 0 \\ 0 & S \end{pmatrix}$$

produces the required zeros, and Q is updated by premultiplying by this matrix.

Steps 2 through $\ell-1$ are similar; in step k we first put zeros in the B portion of column k using R matrices and then zero elements $k+2$ through ℓ of the A portion using a reflection matrix. The final result is that the transformed H has a real tridiagonal matrix T in place of A and $\overline{A}$ and zeros elsewhere.

The QR algorithm is considered to be the algorithm of choice for determining all of the eigenvalues and eigenvectors of a real symmetric tridiagonal matrix. We use the algorithm to form X, the matrix of eigenvectors of T. Implementation of the algorithm requires care, and high quality implementations are available, for example, in LAPACK.[2] Other codes are available at http://www.netlib.org.

We construct the eigenvector matrices U and V as $U=Q_1^\dagger X$ and $V=Q_2{}^T X$. Note that most implementations of the QR algorithm do not guarantee that the eigenvalues are ordered, so a final sort of the eigenvalues and the columns of U and V should be done at the end if desired.

V. TIME REVERSAL, THE CCD, AND KRAMERS' NONDEGENERACY

The section presents three topics, all following from an interpretation of υ from Eq. (2) as a time reversal symmetry operator. First, the Cartan involution defining the CCD may be rewritten entirely in terms of the spin-flip, and the eigenspaces of $\theta(iH)$ are associated to time symmetric and antisymmetric Hamiltonians H in a natural way. Second, a well-known procedure exists to convert any $G=KAK$ decomposition into a polar decomposition, and the polar decomposition associated to the CCD writes a unitary $\nu \in \mathrm{SU}(N)$ as a product of two factors, one evolution by a time symmetric Hamiltonian and one evolution by a time anti-symmetric Hamiltonian. Third, we demonstrate the entangled eigenstates of Kramers' nondegeneracy as described in the introduction and consider the perturbative stability of this entanglement under time reversal symmetry breaking.

A. Spin-flips as time reversal symmetry operators

Recall the *Bloch sphere* (e.g., Ref. 36), which provides a picture of the data space of one qubit. As a remark, the Bloch sphere may be thought of as a parametrization of the complex projective line $\mathbb{CP}^1$ (e.g., Ref. 34, Sec. 40). Briefly, $\mathbb{CP}^1$ is the set of all equivalence classes of vectors in $\mathbb{C}^2$ up to multiple by a nonzero complex scalar. To associate such a class with a Bloch vector, normalize $|\psi\rangle$ as above so as to write $|\psi\rangle = re^{it}[\cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle]$. The Bloch sphere vector of $|\psi\rangle$, say $[|\psi\rangle]$, is given in spherical coordinates by $(1,\theta,\varphi)$ (Ref. 36, p. 15). Recall also that the north pole is $[|0\rangle]$ and $[|1\rangle]$ is the south pole.

Now let $\vec{b} \in (\mathbb{F}_2)^n$ be an n-bit string. The typical procedure when quantizing a classical computation is to extend the classical outputs linearly without phases. Thus, a reasonable interpretation of quantum bit-flip would be $(\sigma^x)^{\otimes n}$. This is the common interpretation, but note that in one qubit

σ^x is not reflection on the Bloch sphere and indeed has a fixed state, $(1/\sqrt{2})(|0\rangle+|1\rangle)$. Rather, the odd reflection of a single qubit under the Bloch parametrization of $\mathbb{CP}^1$ is the spin-flip $|\psi\rangle \mapsto \overline{(-i\sigma^y)|\psi\rangle}=(-i\sigma^y)\overline{|\psi\rangle}$.

The appropriate physical interpretation of the spin-flip is as a time reversal symmetry operator (Ref. 47, Chap. 26, Ref. 19, pp. 314–322, Refs. 27 and 39). Wigner defined a generic time reversal symmetry operator Θ as any $\mathbb{R}$-linear involutive map of the quantum Hilbert space which is antiunitary, i.e., complex anti-linear $(\Theta(\alpha|\psi_1\rangle+\beta|\psi_2\rangle)=\overline{\alpha}\Theta|\psi_1\rangle+\overline{\beta}\Theta|\psi_2\rangle)$, and orthogonal in the induced real inner-product on $\mathbb{R}^{2p}\cong\mathbb{C}^p$. Generic time reversal symmetry operators are usually denoted by a capital Θ; we ask the reader's forebearance in distinguishing this from the lower-case θ describing a Cartan involution.

Such a time reversal symmetry operator Θ maps the state of a system to its motion-reversed state, so that momentum eigenstates transform as $\Theta|\mathbf{p}\rangle=|-\mathbf{p}\rangle$. In particular, if our qubit is a spin $\frac{1}{2}$ particle, e.g., with $|0\rangle=|\uparrow\rangle$ and $|1\rangle=|\downarrow\rangle$, then υ per Eq. (2) reverses the one-qubit spin vector on the Bloch sphere and so is the natural quantum angular momentum reversal in n-qubits. Indeed, the total spin angular momentum, $\vec{S}=\Sigma_{j=1}^{n}\vec{\sigma}_j$, is inverted under time reversal: $\upsilon\vec{S}\upsilon^{-1}=-\vec{S}$. Spin-flip operators may be defined for d-level systems (qudits) but may not both preserve pure states and commute with local unitaries.[38]

We note in passing that the spin-flip picture also allows one to quickly rederive one of the monotone properties. Namely, antipodal points in the Bloch sphere parametrization of the complex projective line $\mathbb{CP}^1$ correspond to Hermitian-orthogonal states of $\mathcal{H}_1$. Hence, $C_n(|\psi\rangle)=|\langle\psi|\upsilon|\psi\rangle|=0$ if $|\psi\rangle=\otimes_{j=1}^{n}|\psi_j\rangle$ (the monotone property,) since in this event $\langle\psi|\upsilon|\psi\rangle$ has a factor $\langle\psi_j|\upsilon|\psi_j\rangle=0$. More generally $C_n(|\psi\rangle)=0$ whenever $|\psi\rangle=|\psi_1\rangle\otimes|\psi_2\rangle$ for $|\psi_1\rangle\in\mathcal{H}_{n-1}$ and $[|\psi_2\rangle]$ a point on the Bloch sphere. However, the latter is not an equivalence for n even. Consider $|\mathrm{W}_4\rangle=(1/2)\times(|0001\rangle+|0010\rangle+|0100\rangle+|1000\rangle)$.

B. Time reversal and the CCD Cartan involution

We next show that physically, the eigenspaces of the Cartan involution producing the CCD correspond to υ-time symmetric and υ-time antisymmetric Hamiltonians. They are then explicitly described in the Pauli-tensor basis of $\mathfrak{su}(N)$ in much more compact form than in Dirac notation.[8]

Definition V.1: Consider H a Hamiltonian on a finite dimensional Hilbert space $\mathcal{H}$, i.e., H is self-adjoint within $\mathrm{End}_{\mathbb{C}}(\mathcal{H})\subset\mathrm{End}_{\mathbb{R}}(\mathcal{H})$. Then H is time reversal symmetric with respect to Θ iff $H=\Theta H\Theta^{-1}$ as elements of $\mathrm{End}_{\mathbb{R}}(\mathcal{H})$. A Hamiltonian is time reversal anti-symmetric with respect to Θ iff $H=-\Theta H\Theta^{-1}$.

Proposition V.2: Let $\theta(X)$ per Definition II.1. Label $\mathfrak{su}(N)=\mathfrak{p}\oplus\mathfrak{k}$ as the -1 and $+1$-eigenspaces of θ. Let υ be the spin-flip. Then (i) for H a traceless Hamiltonian, so that $iH\in\mathfrak{su}(N)$, $\theta(iH)=\upsilon(iH)\upsilon^{-1}$, with the right-hand side viewed as a composition of $\mathbb{R}$-linear maps. Also (ii) (H has time reversal symmetry with respect to υ) $\Leftrightarrow(iH\in\mathfrak{p})$, and (iii) ($H$ has time reversal anti-symmetry with respect to υ) $\Leftrightarrow(iH\in\mathfrak{k})$.

Proof: Let τ denote the complex conjugation operator $|\psi\rangle\mapsto\overline{|\psi\rangle}$. Then $\upsilon=(-i\sigma^y)^{\otimes n}\tau=\tau(-i\sigma^y)^{\otimes n}$, given $-i\sigma^y$ real. So $\upsilon^{-1}=\tau[(-i\sigma^y)^{\otimes n}]^\dagger$. Moreover, $[(-i\sigma^y)^{\otimes n}]^\dagger=(-I_N)^n(-i\sigma^y)^{\otimes n}$. Finally, $\tau(iH)\tau=\overline{iH}$. Thus,

$$\upsilon(iH)\upsilon^{-1}=(-i\sigma^y)^{\otimes n}\tau(iH)\tau[(-i\sigma^y)^{\otimes n}]^\dagger=(-I_N)^n(-i\sigma^y)^{\otimes n}\overline{(iH)}[(-i\sigma^y)^{\otimes n}]=\theta(iH). \qquad (34)$$

The latter two items follow at once. □

With the above proposition, we may describe the infinitesimal Cartan decomposition $\mathfrak{su}(n)=\mathfrak{p}\oplus\mathfrak{k}$ directly in terms of tensors of Pauli operators. Let j denote either 0, x, y, or z, with $\sigma^j=I_2$ in case $j=0$ and Pauli matrices σ^x, σ^y, or σ^z as appropriate otherwise. A multi-index $J=j_1j_2\cdots j_k\cdots j_n$ denotes a string of length n, and J will be said to be nonzero if some $j_k\neq 0$. Finally, let $i\sigma^{\otimes J}$ denote $i\otimes_{k=1}^{n}(\sigma^{j_k})$. Then $\mathfrak{su}(N)=\oplus_{\text{all nonzero } J}\mathbb{R}\{i\sigma^{\otimes J}\}$. We have the following corollary, discovered independently by Bremner *et al.* (Ref. 5, Theorem 5) which has recently reappeared in a different context (Ref. 1, p. 243).

Corollary V.3: Continue the convention of the previous paragraph, and write

$$\mathfrak{su}(N) = \Big(\bigoplus_{\#J=0 \bmod 2} \mathbb{R}\{i\sigma^{\otimes J}\}\Big) \oplus \Big(\bigoplus_{\#J=1 \bmod 2} \mathbb{R}\{i\sigma^{\otimes J}\}\Big). \tag{35}$$

The above is the infinitesimal Cartan decomposition of $\theta(iH)$, *i.e.*, $\mathfrak{p} = \oplus_{\#J=0 \bmod 2}\mathbb{R}\{i\sigma^{\otimes J}\}$, and $\mathfrak{k} = \oplus_{\#J=1 \bmod 2}\mathbb{R}\{i\sigma^{\otimes J}\}$. *In particular*, K *is the Lie group of those unitaries which are exponentials of Hamiltonians with time reversal anti-symmetry with respect to* υ.

Proof: Distinct Pauli matrices anti-commute, each has $(\sigma^j)^2 = I_2$, and σ^y is purely imaginary while σ^x, σ^z, and I_2 are real. Considering the tensors case by case completes the proof. □

C. A time reversal polar decomposition

We next consider the polar decomposition which may be derived from the CCD. In most treatments, the polar decomposition of a general Cartan involution is proven and then a $G = KAK$ theorem is derived from it. We next use the CCD to produce a polar decomposition for time reversal symmetry. This practical decision avoids rearguing the $G = KAK$ theorem for compact groups (Ref. 21, Theorem 8.6, Sec. VII.8).

Corollary V.4: Suppose $v \in \mathrm{SU}(N)$ *is a phase normalized quantum computation in n qubits. Then we may write* $v = \exp(iH_{\mathfrak{p}})\exp(iH_{\mathfrak{k}})$ *for some Hamiltonians* $H_{\mathfrak{p}}$, $H_{\mathfrak{k}}$ *such that* $H_{\mathfrak{p}}$ *has time reversal symmetry and* $H_{\mathfrak{k}}$ *has time reversal anti-symmetry with respect to the spin-flip* υ.

Proof: Let $v = k_1 a k_2$ be the CCD of $v \in \mathrm{SU}(N)$. Then in particular $v = (k_1 a k_1^\dagger)(k_1 k_2)$. Since K is a group, $k_1 k_2$ is a time antisymmetric evolution by Proposition V.2. Moreover, let $a = \exp iH$ for $iH \in \mathfrak{a} \subset \mathfrak{p}$ a time symmetric Hamiltonian. As $iH \in \mathfrak{p}$, we have $\theta(iH) = [(-i\sigma^y)^{\otimes n}]^\dagger \overline{(iH)}(-i\sigma^y)^{\otimes n} = -iH$. Moreover, $k \in K$ is a symmetry of the concurrence form [Eq. (10)] which as a matrix equation demands $k^T(-i\sigma^y)^{\otimes n}k = (-i\sigma^y)^{\otimes n}$. Hence $k_1^T(-i\sigma^y)^{\otimes n} = (-i\sigma^y)^{\otimes n}k_1^\dagger$, and for $k_1 iHk_1^\dagger \in \mathfrak{p}$:

$$\theta(k_1 iHk_1^\dagger) = [(-i\sigma^y)^{\otimes n}]^\dagger \overline{k_1}\,\overline{(iH)}k_1^T(-i\sigma^y)^{\otimes n} = k_1[(-i\sigma^y)^{\otimes n}]^\dagger \overline{(iH)}(-i\sigma^y)^{\otimes n}k_1^\dagger = -k_1(iH)k_1^\dagger. \tag{36}$$

Thus $k_1(iH)k_1^\dagger$ has time reversal symmetry, and the usual matrix exponential formula [valid since $\mathrm{SU}(N)$ is linear] shows $k_1 a k_1^\dagger = \exp[k_1(iH)k_1^\dagger]$. □

Remark V.5: Note that the vector space decomposition $\mathfrak{su}(N) = \mathfrak{p} \oplus \mathfrak{k}$ makes clear any such v may be approximated by rapid pulsing of the time symmetric and anti-symmetric factors, by applying the Trotter formula (e.g., Ref. 36, Sec. 4.7.2). However, the decomposition above requires no such pulsing of the time-symmetric and time-antisymmetric Hamiltonians.

D. Kramers' nondegeneracy

Finally, we rederive Kramers' degeneracy in the case of υ and note a further, υ-specific nondegeneracy property. Recall Kramers' degeneracy[26,27] proves that the eigenstates of a collection of an odd number of spin $\frac{1}{2}$ electrons become doubly degenerate in the exclusive presence of a time-reversal-symmetric interaction, such as an electric field. The degeneracy is broken with the introduction of a magnetic field. In terms of an energy Hamiltonian H of the system, the degeneracy corresponds to 2 or greater dimensional eigenspace for energy eigenstates.

Lemma V.6: Suppose that $|\psi\rangle \in \mathcal{H}_n$ *is an eigenstate of some traceless Hamiltonian* H *which has time reversal symmetry, with eigenvalue* $\lambda \in \mathbb{R}$. *Then the spin-flip* $\upsilon|\psi\rangle$ *is also an eigenstate of eigenvalue* λ.

Proof: Since iH has time reversal symmetry, $\theta(iH) = -iH$. Thus $(-i\sigma^y)^{\otimes n}(iH) + \overline{(iH)}(-i\sigma^y)^{\otimes n} = 0$, and taking a complex conjugate produces $(-i\sigma^y)^{\otimes n}\overline{(iH)} + (iH)(-i\sigma^y)^{\otimes n} = 0$. Now $(iH)|\psi\rangle = \lambda|\psi\rangle$, so that

$$(iH)\upsilon|\psi\rangle = (iH)(-i\sigma^y)^{\otimes n}\overline{|\psi\rangle} = -(-i\sigma^y)^{\otimes n}\overline{(iH)|\psi\rangle} = -(-i\sigma^y)^{\otimes n}\overline{i\lambda|\psi\rangle} = i\lambda\upsilon|\psi\rangle. \tag{37}$$

This concludes the proof. □

Theorem V.7 [cf. Kramers' degeneracy—Refs. 26, 27, and 39 (p. 281)]. *Let* H *be a traceless Hamiltonian on some number* n *of quantum-bits. Suppose* H *has time reversal symmetry with respect to* υ. *Let* λ *be a fixed eigenvalue of* H. *Then either (i)* λ *is degenerate with even multiplicity* *or (ii) the normalized eigenstate* $|\lambda\rangle$ *has* $C_n(|\lambda\rangle)=1$. *For n odd, case (i) holds: all* λ *are degenerate with even multiplicity*.

Proof: Let λ_j be some eigenvalue of H. By Lemma V.6, both $|\lambda_j\rangle$ and $\upsilon|\lambda_j\rangle$ are energy eigenstates. Should these two states be linearly independent, then λ_j is degenerate. If any eigenvalue is nondegenerate, say λ_k, then by antiunitarity of υ, we must have $\upsilon|\lambda_k\rangle=e^{i\varphi}|\lambda_k\rangle$ for some global phase φ. Using $C_n(|\lambda_k\rangle)=|\langle\lambda_k|\upsilon|\lambda_k\rangle|$ we see that this eigenstate must have concurrence one.

Suppose in particular $n=2p-1$. Then $\mathcal{C}_n(-,-)$ is antisymmetric and vanishes on the diagonal, implying $\langle\lambda_j|\upsilon|\lambda_j\rangle=0$ for all j. Consequently, $|\lambda_j\rangle$ and $\upsilon|\lambda_j\rangle$ are Hermitian orthogonal and may not be dependent, implying case (i). □

Thus, for the spin-flip υ there is in addition to the Kramers' degeneracy a Kramers' nondegeneracy. As always, if n is odd so that the total n-qubit system is a fermion, then a time reversal symmetric Hamiltonian implies that all energy eigenstates are degenerate. Yet moreover in the specific case of υ and *n even*, a nondegenerate eigenstate must also have maximal concurrence and hence be entangled.

We provide some illustrative examples. First note that there are many systems endowed with time reversal symmetric Hamiltonians. In particular, any system with (exclusively) pairwise nearest neighbor coupling between qubits has $iH\in\mathfrak{p}$, by Corollary V.3. An example of an interaction that occurs in many solid state systems is the quantum XYZ model:

$$H_{\mathrm{XYZ}}=\sum_{\langle j,k\rangle} J_x\sigma_j^x\sigma_k^x+J_y\sigma_j^y\sigma_k^y+J_z\sigma_j^z\sigma_k^z \tag{38}$$

with $J_{x,y,z}\in\mathbb{R}$ where the sum is taken over all nearest neighbor pairs and the boundaries may be fixed or periodic. In one dimension, these nearest neighbor coupled systems are known as spin chains. Spin chain Hamiltonians are of great theoretical interest, for under the appropriate parameter regime they exhibit long range classical correlations near a quantum phase transition.[30] We can characterize the dynamics of entanglement in spin chains using the concurrence capacity. With this goal in mind we observe the following useful fact:

Proposition V.8: Let $\mathfrak{p}$, $\mathfrak{k}$ *be as in Corollary V.3. If* $iH\in\mathfrak{p}$ *and* $H\in\mathbb{R}^{N\times N}$, *then* $\lambda_c(u=e^{-iHt})=\{e^{-2i\lambda_j t}\}$ *where* $t\in\mathbb{R}$ *parameterizes time and* $\lambda_j\in\mathbb{R}$ *are the eigenvalues of H*.

Proof: By Definition III.5 the concurrence spectrum of the unitary generated by iH, $u=e^{-iHt}$ is

$$\begin{aligned}\lambda_c(u)&=\mathrm{spec}[(-i\sigma^y)^{\otimes n\dagger}e^{iHt}(-i\sigma^y)^{\otimes n}(e^{-iHt})^T]=\mathrm{spec}(e^{-iHt}e^{-iH^Tt})\\&=\mathrm{spec}(e^{-2iHt})\qquad\qquad=\{e^{-2i\lambda_j t};\lambda_j\in\mathrm{spec}(H)\}.\end{aligned} \tag{39}$$

We have used $(-i\sigma^y)^{\otimes n\dagger}\overline{iH}(-i\sigma^y)^{\otimes n}=-iH$ and therefore $(-i\sigma^y)^{\otimes n\dagger}H(-i\sigma^y)^{\otimes n}=H$ because H is real. The third line is a consequence of H being Hermitian. □

The quantum XYZ Hamiltonian has time reversal symmetry with respect to the spin-flip υ. We next demonstrate how to build up entanglement with such a system. Consider a collection of n qubits laid out in a cyclic array interacting under the Ising class of Hamiltonians given by H_{XYZ} with $J_x=J_y=0$: $H_{Is}=\sum_{j=1}^n J_z\sigma_j^z\sigma_{j+1}^z$, where we identify $\sigma_{n+1}^z=\sigma_1^z$.

The eigenvalues are given by $\{\lambda_j\}=\{J_z(n-2\Sigma_k j_k\oplus j_{k+1});j=j_1j_2\ldots j_n\}$,[30] where the addition is done modulo 2 over the components j_k of the binary expansion of j. For n even, each eigenvalue λ_j is paired with another of opposite sign and in particular, $\lambda_0=-\lambda_{N-1}$ with $|\lambda_0|=n|J_z|=\lambda^{\max}$. The concurrence spectrum of $u=e^{-iH_{Is}t}$ is composed of complex conjugate pairs and the concurrence capacity $\tilde{\kappa}_n(u)$ may be computed explicitly. Then $\tilde{\kappa}_n(u)=\max\{|\sum_{j=0}^{N-1}a_j^2e^{-2i\lambda_j t}|;z^\dagger z=1,z^Tz=0\}$ where $z=\sum_{j=0}^{N-1}a_j|j\rangle$, per Eq. (14). Maximum capacity is obtained when the convex hull condition is satisfied which occurs precisely when the concurrence spectrum extends outside the right half of the complex plane. The minimum time at which this occurs is given by $e^{-2i\lambda^{\max}t_{\min}}=i$ or $t_{\min}=\pi/4|\lambda_0|=\pi/4n|J_z|$.

The existence of a time reversal symmetry in the interaction between qubits gives us important information about the nature of quantum correlations in the energy eigenstates. Applying Theorem V.7, we immediately find that the ground state of a Hamiltonian H with time reversal symmetry has maximum n-concurrence if it is unique. Examples of interactions satisfying these conditions are the XYZ Hamiltonian with $(J_x=J_y=J_z=J>0)$, denoted the XXX Hamiltonian, and the XY Hamiltonian $(J_x=J_y, J_z=0)$.[30] In particular, the XXX Hamiltonian with $J>0$ has been shown to have nondegenerate ground states in any number of dimensions, with or without periodic boundary conditions, provided the underlying lattice has a reflection symmetry about some plane (ibid.).

To illustrate this phenomenon we consider what happens when the time reversal symmetry is broken by adding a time-antisymmetric term to the XY Hamiltonian:

$$H=\sum_{j=1}^{n} J\left(\frac{1+g}{4}\sigma_j^x\sigma_{j+1}^x+\frac{1-g}{4}\sigma_j^y\sigma_{j+1}^y\right)+\frac{h_z}{2}\sigma_j^z, \tag{40}$$

where $\sigma_{n+1}^{\alpha}\equiv\sigma_1^{\alpha}$. The presence of the linear term proportional to the total spin projection operator $S_z=\Sigma_{j=1}^{n}\sigma_j^z$, breaks the time reversal symmetry so that $iH\notin\mathfrak{p}$ when $h_z\neq 0$. For zero magnetic field and $0\leqslant g<1$, the Hamiltonian is time reversal symmetric and the ground state is nondegenerate meaning the concurrence is maximal. In the isotropic case $(g=0)$, the Hamiltonian commutes with S_z and eigenstates are independent of h_z. For magnetic field strengths below some critical value, $|h|<h_{\mathrm{crit}}$ the ground state corresponds to an eigenstate with eigenvalue $s_z=0$ of the operator S_z. This ground state has maximal concurrence. For $|h_z|>h_{\mathrm{crit}}$, the ground state corresponds to an eigenvalue $s_z\neq 0$ and the concurrence is zero.[7]

VI. CONCLUSIONS

We show that the odd-qubit concurrence canonical decomposition admits generalizations of all constructions studied on the even qubit CCD. In particular, a generalized pairwise concurrence capacity may be defined, and the operators for which this is maximal are characterized by a convex hull condition on the concurrence spectrum. Again for an odd number of qubits, we find that for large odd n most unitaries have maximal concurrence capacities. Moreover, we provide an explicit algorithm for computing the odd-qubit CCD.

These advances are complemented by new interpretation of the original inputs to the $G=KAK$ theorem which define the CCD. Specifically, they may be rewritten in terms of time reversal symmetry υ which is the spin-flip in n quantum bits, and the CCD is best understood in terms of such symmetries. For example, the odd-qubit CCD is a type **AII** *KAK* decomposition, and as such must have degenerate eigenvalues. In fact, this recaptures Kramers' degeneracy for the odd-qubit spin-flip, and a more careful study of the arguments reveals a Kramers' nondegeneracy: Nondegenerate eigenstates of υ time reversal symmetric Hamiltonians only exist when the number of quantum bits is even and *moreover* must be highly entangled. Specifically, such $|\lambda\rangle$ are highly entangled in the sense that the concurrence $C_n(|\lambda\rangle)=|\langle\lambda|\upsilon|\lambda\rangle|=1$. Finally, the polar decomposition extracted from the CCD in the usual way accomplishes the following: any unitary n-qubit evolution is a product of precisely one time reversal symmetric and one time reversal antisymmetric evolution.

ACKNOWLEDGMENTS

S.S.B. acknowledges a National Research Council postdoctoral fellowship, G.K.B. acknowledges support through DARPA QuIST, and DPO acknowledges NSF Grant No. CCR-0204084.

NIST disclaimer. Certain commercial equipment or instruments may be identified in this paper to specify experimental procedures. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology.

[1] Albertini, F. and D'Alessandro, D., "Model identification for spin networks," Linear Algebr. Appl. **394**, 237 (2005).
[2] Anderson, E., Bai, Z., Bischof, C., Blackford, S., Demmel, J., Dongarra, J., Du Croz, J., Greenbaum, A., Hammarling, S., McKenney, A., and Sorensen, D., *LAPACK Users' Guide*, 3rd ed. (SIAM, Philadelphia, 1999).
[3] Barnum, H. and Linden, N., "Monotones and invariants for 'multi-particle quantum states,' " J. Phys. A **34**, 6787 (2001).
[4] Bennett, C., DiVincenzo, D., Smolin, J., and Wootters, W., "Mixed-state entanglement and quantum error correction," Phys. Rev. A **54**, 3824 (1996).
[5] Bremner, M., Dodd, J., Nielsen, M., and Bacon, D., "Fungible dynamics: There are only two types of entangling

multi-qubit interactions," Phys. Rev. A **69**, 012313 (2004).
[6] Brennen, G. K., "An observable measure of entanglement for pure states of multi-qubit systems," Quantum Inf. Comput. **3**, 619 (2003).
[7] Brennen, G. K. and Bullock, S. S., "Stability of global entanglement in thermal states of spin chains," Phys. Rev. A **70**, 052303 (2004).
[8] Bullock, S. and Brennen, G., "Canonical decompositions of *n*-qubit quantum computations and concurrence," J. Math. Phys. **45**, 2447 (2004).
[9] Bullock, S. and Brennen, G., "Characterizing the entangling capacity of *n*-qubit computations," Proc. SPIE **5436**, 127 (2004) (see http://math.nist.gov/SBullock).
[10] Bullock, S. and Markov, I., "An elementary two-qubit quantum computation in twenty-three elementary gates," Phys. Rev. A **68**, 012318 (2003).
[11] Bullock, S. S., "Note on the Khaneja Glaser decomposition," Quantum Inf. Comput. **5**, 396 (2004).
[12] Bunse-Gerstner, A., Byers, R., and Mehrmann, V., "A chart of numerical methods for structured eigenvalue problems," SIAM J. Matrix Anal. Appl. **13**, 419 (1992).
[13] Childs, A., Haselgrove, H., and Nielsen, M., "Lower bounds on the complexity of simulating quantum gates," Phys. Rev. A **68**, 052311 (2003).
[14] D'Alessandro, D., "Constructive controllability of one and two spin 1/2 particles," Proceedings of the 2001 American Control Conference, Arlington, VA, June 2001 (see http:/http://www.public.iastate.edu/~daless/QC3.html/).
[15] Dongarra, J., Gabriel, J., Koelling, D., and Wilkinson, J., "The eigenvalue problem for Hermitian matrices with time reversal symmetry," Linear Algebr. Appl. **60**, 27 (1984).
[16] Dür, W., Vidal, G., and Cirac, J. I., "Three qubits can be entangled in two inequivalent ways," Phys. Rev. A **62**, 062314 (2000).
[17] Dyson, F., "Statistical theory of energy levels of complex system, I.," J. Math. Phys. **3**, 140 (1961).
[18] Eisert, J. and Briegel, H., "The Schmidt measure as a tool for quantifying multi-particle entanglement," Phys. Rev. A **64**, 022306 (2001).
[19] Gottfried, K., *Quantum Mechanics* (Benjamin, 1966).
[20] Gour, G., "A family of concurrence monotones and its applications," http://www.arxiv.org/abs/quant-ph/0410148.
[21] Helgason, S., *Differential Geometry, Lie Groups, and Symmetric Spaces* (American Mathematical Society, Providence, RI, 2001), vol. 34, graduate studies in mathematics, (corrected reprint of the 1978 original edition).
[22] Hill, S. and Wootters, W., "Entanglement of a pair of quantum bits," Phys. Rev. Lett. **78**, 5022 (1997).
[23] Horodecki, M., Horodecki, P., and Horodecki, R., "Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments," Springer Tracts in Modern Physics (2001), quant-ph/0109124.
[24] Khaneja, N., Brockett, R., and Glaser, S. J., "Time optimal control in spin systems," Phys. Rev. A **63**, 032308 (2001).
[25] Khaneja, N. and Glaser, S., "Cartan decomposition of $SU(2^n)$ and control of spin systems," Chem. Phys. **267**, 11 (2001) (see http://www.sciencedirect.com/science/journal/03010104).
[26] Kramers, H. A., "Theorie generale de la rotation paramagnetique dans les cristaux," Proc. R. Acad. Sci. Amsterdam **33**, 959 (1930).
[27] Kramers, H. A., *Quantum Mechanics* (Dover, Phoenix, 2004), ISBN 0486495337.
[28] Kraus, B. and Cirac, J. I., "Optimal creation of entanglement using a two-qubit gate," Phys. Rev. A **63**, 062309 (2001).
[29] Lewenstein, M., Kraus, B., Horodecki, P., and Cirac, I., "Characterization of separable states and entanglement witnesses," Phys. Rev. A **63**, 044304 (2001).
[30] Lieb, E., Schultz, T., and Mattis, D., "Two soluble models of an antiferromagnetic chain," Ann. Phys. **16**, 407 (1961).
[31] Makhlin, Y., "Nonlocal properties of two-qubit gates and mixed states and optimization of quantum computations," Quantum Inf. Process. **1**, 243–252 (2002).
[32] Meyer, D. and Wallach, N., "Global entanglement in multi-partite systems," J. Math. Phys. **43**, 4273 (2002).
[33] Miyake, A. and Wadati, M., "Multi-partite entanglement and hyperdeterminants," Quantum Inf. Comput. **2**, 540 (2002).
[34] Munkres, J., *Elements of Algebraic Topology* (Addison-Wesley, New York, 1984).
[35] Nakahara, N., Vartiainen, J., Kondo, Y., and Tanimura, K., "Warp-drive quantum computation," http://www.arxiv.org/abs/quant-ph/0308006.
[36] Nielsen, M. and Chuang, I., *Quantum Information and Computation* (Cambridge University Press, Cambridge, 2000).
[37] Ramakrishna, V., Ober, R. J., Flores, K. L., and Rabitz, H., "Control of a coupled two-spin system without hard pulses," Phys. Rev. A **65**, 063405 (2002).
[38] 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).
[39] Sakurai, J. J., *Modern Quantum Mechanics*, revised Ed. (Addison–Wesley, New York, 1985).
[40] Scott, A. and Caves, C., "Entangling power of the quantum baker's map," J. Phys. A **36**, 9553–9576 (2003).
[41] Shende, V., Bullock, S., and Markov, I., "Recognizing small-circuit structure in two-qubit operators," Phys. Rev. A **70**, 012310 (2004).
[42] Uhlmann, A., "Fidelity and concurrence of conjugated states," Phys. Rev. A **62**, 032307 (2000).
[43] Vatan, F. and Williams, C., "Optimal realization of an arbitrary two-Qubit quantum gate," Phys. Rev. A **69**, 032315 (2004).
[44] Verstraete, F., Dehaene, J., De Moor, B., and Verschelde, H., "Four qubits can be entangled in nine different ways," Phys. Rev. A **65**, 052112 (2002).
[45] Vidal, G., "Entanglement monotones," J. Mod. Opt. **47**, 355 (2000).
[46] Vidal, G. and Dawson, C., "A universal quantum circuit for two-qubit transformations with three CNOT gates," Phys. Rev. A **69**, 010301 (2004).
[47] Wigner, E., *Group Theory and Its Application to the Quantum Mechanics of Atomic Spectra* (Academic, New York,

1959).
[48] Wong, A. and Christensen, N., "A potential multiparticle entanglement measure," Phys. Rev. A **63**, 044301 (2001).
[49] Zhang, J., Vala, J., Sastry, S., and Whaley, K., "Geometric theory of nonlocal two-qubit operations," Phys. Rev. A **67**, 042313 (2003).
[50] Some authors only use the term Cartan involution in the case that $\mathfrak{g}$ is a noncompact Lie algebra. In their terminology, this definition of a Cartan involution on the Lie algebra of a compact group, e.g., $\mathfrak{su}(N)$, is the image of a Cartan involution of a noncompact Lie algebra through symmetric duality $(\mathfrak{g}=\mathfrak{k}\oplus\mathfrak{p})\leftrightarrow(\mathfrak{g}^{\text{dual}}=\mathfrak{k}\oplus i\mathfrak{p})$.