Characterizing the entangling capacity of n-qubit computations

Stephen S. Bullock[a] and Gavin K. Brennen[b]

[a]National Institute of Standards and Technology, Gaithersburg, Maryland 20899-8910 USA
[b]National Institute of Standards and Technology, Gaithersburg, Maryland 20899-8420 USA

ABSTRACT

The state space $\mathcal{H}_n$ of n quantum bits of data is exponentially large, having dimension 2^n. The (pure) local states which correspond to each individual quantum bit being in an isolated one-qubit state, i.e. those which are tensor products, form a much smaller orbit of $\otimes_1^n U(2) \cdot |00\cdots 0\rangle$ of linear dimension within the state space. Hence most states are non-local, or *entangled.* The concurrence function on quantum data states is one measure of entanglement, intuitively capturing an exponentially small fraction of the phenomenon. This paper reports numerical tests of how concurrence changes as one applies a quantum computation u to a pure n quantum-bit data state $|\psi\rangle$. We make strong use of a mathematical tool for factoring $u = k_1\ a\ k_2$ into subcomputations, namely the CCD matrix decomposition. The *concurrence dynamics* of a computation $|\psi\rangle \mapsto u|\psi\rangle$ are in a certain sense localized to the a factor, and so our actual numerics concentrate on $|\psi\rangle \mapsto a|\psi\rangle$. This is a great simplification, since an arbitrary unitary evolution may vary over $4^n - 1$ real degrees of freedom, while the $a \in A$ of the appropriate form for the CCD matrix decomposition may vary over $2^n - 1$ or $2^{n/2} - 1$ as $n = 2p,\ 2p - 1$.

Keywords: concurrence, entanglement, concurrence canonical decomposition, quantum computation

1. INTRODUCTION

A great deal of interest has recently arisen in quantum computing, with two primary motivations. The most timely motivation is recent predictions[1] that current CMOS technologies will be insufficient to extend Moore's law into the 2020's. The second, optimistic motivation is Feynman's assertion[2] that a device in which a bit were replaced by a hypothetical two-state quantum system, the quantum-bit or qubit, could replace or perhaps outperform computers manipulating bits. Indeed, much theoretical work in the 1990's strengthened this assertion. One may show that a quantum computer with a quantum oracle outperforms a Turing machine equipped with a classical oracle in a few pages, and many examples of quantum algorithms which outperform their best known classical counterparts now exist. The most famous is Shor's algorithm, a quantum factoring algorithm capable of breaking the current widely-used RSA encryption protocol. Their are many others,[14] including the quantum Fourier transform and Hallgren's recently discovered (2002) algorithm[3, 4] for solving Pell's equation.

The most popular model for quantum computation is the quantum logic circuit. The precise statements of the above results are often theorems asserting the existence of a quantum logic circuit (various libraries; two-qubit gates) performing a given computation which is smaller than any known or possible classical (AND-OR-NOT) logic circuit. The computation realized in the quantum setting is some evolution of the n-qubit state space, usually taken to be a closed-system (unitary) evolution. Recalling this briefly, the one-qubit state space is the complex vector space $\mathcal{H}_1 = \mathbb{C}\{|0\rangle\} \oplus \mathbb{C}\{|1\rangle\}$ carrying the usual Hermitian inner product. The axioms of quantum mechanics then demand that the n-qubit state space should be $\mathcal{H}_n = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_1 = \otimes_1^n \mathcal{H}_1$, with the induced Hermitian inner product. Taking abbreviations such as $|1\rangle \otimes |0\rangle \otimes |1\rangle = |101\rangle$, we produce a basis of $\mathcal{H}_n$ over $\mathbb{C}$ as follows. Let $\vec{b} \in (\mathbb{F}_2)^n$ denote an n-bit string for $\mathbb{F}_2 = \{0, 1\}$ the field of two elements. Dropping set braces:

$$\mathcal{H}_n \ = \ \mathbb{C}|0\cdots 00\rangle \ \oplus \ \mathbb{C}|0\cdots 01\rangle \ \oplus \ \cdots \ \oplus \ \mathbb{C}|1\cdots 11\rangle \ = \ \bigoplus_{\vec{b}\in(\mathbb{F}_2)^n} \mathbb{C}|\vec{b}\rangle \tag{1}$$

Further author information: (Send correspondence to S.S.B.)
S.S.B.: E-mail: stephen.bullock@nist.gov, Telephone: (301) 975-4793
G.K.B.: E-mail: gavin.brennen@nist.gov, Telephone: (301) 975-3582

We further abbreviate a bit string inside a ket by the integer it denotes in binary, e.g. $|5\rangle$ for $|101\rangle$. Thus, for $N = 2^n$ a typical $|\psi\rangle \in \mathcal{H}_n$ may be written as $|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$, with the normalization condition being $\sum_{j=0}^{N-1} |\alpha_j|^2 = 1$. A local state $|\psi\rangle \in \mathcal{H}_n$ is any state which may be decomposed into one qubit local data as a tensor (Kronecker) product: $|\psi\rangle = \otimes_{j=1}^n |\psi_j\rangle$. A (pure) state $|\psi\rangle \in \mathcal{H}_n$ is *entangled* iff $|\psi\rangle$ is not local. Note that (i) the local states do not form a subvectorspace of $\mathcal{H}_n$, and (ii) nonetheless most states in some sense are not local. Indeed, one may check that all local states may be written as $\otimes_{j=1}^n u_j |0\cdots 00\rangle$ for some $u_1, u_2, \cdots, u_n$ each 2×2 unitary. We normalize phases to collect a $\mathrm{e}^{i\varphi}$, when each $u_j \in SU(2)$, $j = 1, 2, \cdots n$. Moreover, each $v \in SU(2)$ factors as

$$v = \mathrm{e}^{i\varphi} \begin{pmatrix} \mathrm{e}^{-i\phi_1/2} & 0 \\ 0 & \mathrm{e}^{i\phi_1/2} \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \begin{pmatrix} \mathrm{e}^{-i\phi_2/2} & 0 \\ 0 & \mathrm{e}^{i\phi_2/2} \end{pmatrix} \tag{2}$$

This *Euler angle decomposition* shows most states are not local. For the expression $\otimes_{j=1}^n u_j |0\cdots 00\rangle$ has no more than $4n$ real degrees of freedom. Many have suggested[6] that *entanglement*, i.e. nonlocality of quantum data, allows for a parallelism and ultimately outperformance of quantum logics *vis a vis* classical logics.

Hence, the study of how quantum computations or more generally unitary evolutions create and modify entanglement is timely and interesting. We attack part of this problem. Namely, we report numerical results on concurrence dynamics. Concurrence is an *entanglement montone*,[7] very loosely a function $f : \mathcal{H}_n \to [0, \infty)$ which vanishes on local states and fails to vanish on certain (but not all) entangled states. We seek to study how a unitary evolution u creates concurrence, i.e. maps the 0 level set of the monotone out into $\mathcal{H}_n$. The primary theoretical tool, greatly simplifying the numerics, is a recently introduced[8, 9] matrix decomposition tailored to this task, the *concurrence canonical decomposition.* The CCD generalizes the Euler angle decomposition above to n-qubit computations. Indeed, the above decomposition of Equation 2 is the one-qubit case.[8]

We next briefly recall the concurrence monotone and CCD; details may be found in the citations above and their references. First, we define the n-fold tensor power of the phased-Pauli matrix $-i\sigma^y = -|0\rangle\langle 1| + |1\rangle\langle 0|$:

$$(-i\sigma^y)^{\otimes n} = \sum_{j=0}^{N-1} (-1)^{\#j} |N-j-1\rangle\langle j| \tag{3}$$

where for $j = b_1 b_2 \cdots b_n$ in binary we have $\#j = b_1 \oplus b_2 \oplus \cdots \oplus b_n$ their XOR sum (i.e. sum in the field of two elements $\mathbb{F}_2$.) Then the concurrence $C_n(|\psi\rangle)$ of a data-state $|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle \in \mathcal{H}_n$ is given by

$$C_n(|\psi\rangle) = |\overline{\langle\psi|}(-i\sigma^y)^{\otimes n}|\psi\rangle| = \left| \sum_{j=0}^{N-1} (-1)^{\#j} \overline{\alpha}_j \alpha_{N-j-1} \right| \tag{4}$$

Computing directly, $C_{2p}(|00\cdots 0\rangle) = 0$. Then note that for any $v \in SU(2)$, we have $v^T(-i\sigma^y)v = \det(v)(-i\sigma^y) = (-i\sigma^y)$. Hence we also have $C_n(\otimes_{j=1}^n v_j |00\cdots 0\rangle) = \otimes_{j=1}^n \overline{\langle 0|} v_j^T (-i\sigma^y) v_j |0\rangle = \otimes_{j=1}^n \overline{\langle 0|}(-i\sigma^y)^{\otimes n}|0\rangle = 0$, which is consistent with $C_n(|\psi\rangle)$ being an entanglement measure. We also note that since $C_n(|\psi\rangle) \equiv 0$ for n odd, an algebraic fact due to $[(-i\sigma^y)^{\otimes n}]^T = -(-i\sigma^y)^{\otimes n}$.

We provide some more examples of the behavior of $C_n(-)$, for $n = 2p$. First, take $|\mathrm{GHZ}_n\rangle = \frac{1}{\sqrt{2}}(|00\cdots 0\rangle + |11\cdots 1\rangle)$, which is highly entangled. Then $C_n(|\mathrm{GHZ}_n\rangle) = 1$. The same is true for $|\mathrm{GHZ}_{n/2}\rangle \otimes |\mathrm{GHZ}_{n/2}\rangle$. On the other hand, for the entangled state $|W\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$, we have $C_4(|W\rangle) = 0$. Thus $C_n(-)$ only detects a small fraction of the total entanglement, as one might expect for any single function given the exponentially large codimension of local states.

The CCD then extends the Euler angle decomposition of Equation 2 to n-qubits. To begin, we label $K \subset SU(2^n)$ to be that subset of matrices defined by

$$K \;=\; \{\; v \in SU(2^n) \;;\; v^T(-i\sigma^y)^{\otimes n} v = (-i\sigma^y)^{\otimes n} \;\} \tag{5}$$

This matrix equation demands in particular that $C_n(k|\psi\rangle) = C_n(|\psi\rangle)$ for any $k \in K$, $|\psi\rangle \in \mathcal{H}_n$. For $n = 2p$, we take A to be the group of unitary matrices which are diagonal in the following entangled basis of $\mathcal{H}_n$:

$$\mathcal{B} \ = \ \{ \ |j\rangle + (-1)^{\#j}|N-j-1\rangle \ \} \sqcup \{ \ i|j\rangle + (-1)^{\#j+1} i|N-j-1\rangle \ \} \tag{6}$$

We further label a concurrence capacity of a unitary evolution v to be the amount of concurrence it may create from a concurrence 0 state:

$$\kappa_{2p}(v) \ = \ \max\{ \ C_n(v|\psi\rangle) \ ; \ C_n(|\psi\rangle) = 0, \ \langle\psi|\psi\rangle = 1 \ \} \tag{7}$$

Earlier theory papers[8, 9] then establish the following:

- Any $v \in SU(2^n)$ may be written as a matrix product $v = k_1 \ a \ k_2$ for $k_1, k_2 \in K$, $a \in A$.
- Label the concurrence spectrum $\lambda_c(v) = \mathrm{spec}(a^2)$, a subset of the complex circle $\{ \ z \in \mathbb{C} \ ; \ |z| = 1 \ \}$. Then put the convex hull of this set to be that polygon which has these points as vertices. Then the maximum possible value of $\kappa_{2p}(v)$ for any v is one, and this is attained if and only if said polygon contains $0 \in \mathbb{C}$.
- Intuitively, one then suspects most computations build maximal concurrence for $n >> 1$, in the sense that usually $\kappa_{2p}(v) = \kappa_{2p}(k_1 a k_2) = \kappa_{2p}(a) = 1$. For choosing many points on the circle makes it quite likely the polygon they span holds $0 \in \mathbb{C}$.

The paper is organized as follows. In §2, we study the concurrence dynamics of Grover's search algorithm numerically and analytically. This algorithm is well-known to provide a speedup in database search, when comparing a classical algorithm exploiting a classical oracle competing with a quantum algorithm using a quantum oracle. Our concurrence results track those obtained for another measure of entanglement, the Q-measure[10] of Meyer-Wallach. In §3, we describe the concurrence spectra of other well-known quantum algorithms. In §4, we study the main deficiency in the definition of a concurrence capacity. Specifically, we construct an explicit concurrence 0 state which maximizes the concurrence capacity of a Grover iteration in 4-qubits yet is highly nonlocal. An Appendix describes the procedure for constructing such states in detail.

2. COMPUTATION: CONCURRENCE DYNAMICS OF GROVER SEARCH

Grover's search is an example of a quantum algorithm which in conjunction with a quantum oracle allows for speedup. Suppose first one has a database of $N = 2^n$ classical elements and a classical oracle O_x which returns -1 on a target element $x \in \{0, 1, \cdots, N-1\}$ and 1 else. One expects in the worst case that $N-1$ calls to this oracle are required to classically identify x. On the other hand, suppose instead we have an oracle $\mathcal{O}_{|x\rangle}$ which acts on $\mathcal{H}_n$ by $\mathcal{O}_{|x\rangle} \sum_{j=0}^{N-1} \alpha_j |j\rangle = \sum_{j=0}^{x-1} \alpha_j |j\rangle - \alpha_x |x\rangle + \sum_{k=x+1}^{N-1} \alpha_k |k\rangle$. Grover's algorithm makes use of $O(\sqrt{N})$ oracle calls to create an output state $|\psi^{\text{out}}\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$ with a large amplitude in α_x, allowing one to identify x with high probability.

Grover's search algorithm[6] is iterative. Let $H = \frac{1}{\sqrt{2}} \sum_{j,k=0}^{1} (-1)^{jk} |j\rangle\langle k|$, so that $|\psi^0\rangle = H^{\otimes n}|00\cdots 0\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$ is a state in full superposition. For I_N the $N \times N$ identity matrix, label the Grover operator as

$$G \ = \ H^{\otimes n}(I_N - 2|00\cdots 0\rangle\langle 00\cdots 0|)H^{\otimes n}\mathcal{O}_{|x\rangle} \ = \ (I_N - 2|\psi^0\rangle\langle\psi^0|)\mathcal{O}_{|x\rangle} \tag{8}$$

with the last equation a change of basis. Then Grover's algorithm iterates through states $|\psi^k\rangle = G^k|\psi^0\rangle$. A central point of the construction is that these iterates always remain within the plane (in fact real span) of the kets $|x\rangle$ and $|\psi^0\rangle$, on which $\mathcal{O}_{|x\rangle}$ and $I_N - 2|\psi^0\rangle\langle\psi^0|$ act individually as reflections. Thus G acts as a rotation in this plane about some angle, in fact

$$\theta = 2\cos^{-1}\sqrt{\frac{N-1}{N}} \tag{9}$$

The output state $|\psi^{\text{out}}\rangle$ is the iterate $|\psi^\ell\rangle$ for ℓ some best possible integer approximation to $\frac{\cos^{-1} N^{-1/2}}{\theta}$; trigonometric approximations show this $\ell \leq \frac{\pi}{4}\sqrt{N}$. Hence, the asymptotic number of oracle calls is $O(\sqrt{N})$, improving upon $\Omega(N)$ classical oracle calls.

Computation of concurrences $C_{2p}(|\psi^k\rangle)$ for Grover states $|\psi^k\rangle$

We first consider how much entanglement (or at least entanglement in the sense of concurrence) is exploited by Grover's algorithm. To this end, we compute the concurrence of the Grover iterates. Since the iterates have a fairly simple form, remaining in the $\mathbb{R}$-span of two vectors, an analytic computation is most convenient.

To begin, suppose in binary $j = b_1 b_2 \cdots b_n$, and write $\#j = b_1 \oplus b_2 \oplus \cdots \oplus b_n$ the `XOR` sum, i.e. sum in the field of two elements. Given that $n = 2p$, we note that $\sum_{j=1}^{N-2}(-1)^{\#j} = -2$. For the Grey code[6] shows that there is an reordering of $0, 1, 2, \cdots, N-1$ so that the binary expansions of any two successive integers in this order differ at one bit. Hence, $\sum_{j=0}^{N-1}(-1)^{\#j} = 0$, while $\#0 = 0$ and $\#(N-1) = 0$ given $n = 2p$.

For simplicity, suppose henceforth that $x = N-1$. Then a standard analysis[6] shows that

$$|\psi^k\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle, \quad |\alpha\rangle = \frac{1}{\sqrt{N-1}}\sum_{j=0}^{N-2}|j\rangle, \quad |\beta\rangle = |x\rangle = |N-1\rangle \tag{10}$$

Now label the quadratic form $\mathcal{C}_n(|\phi\rangle, |\psi\rangle) = \overline{\langle\phi|}(-i\sigma^y)^{\otimes n}|\psi\rangle$, which is $\mathbb{C}$-linear in each variable. Then for all $|\psi\rangle \in \mathcal{H}_{2p}$, $C_{2p}(|\psi\rangle) = |\mathcal{C}_n(|\psi\rangle, |\psi\rangle)|$. Thus, we expand bilinearly and apply a trig identity to the cross-term for

$$\mathcal{C}_n(|\psi^k\rangle, |\psi^k\rangle) = \cos^2\left(\frac{2k+1}{2}\theta\right)\mathcal{C}_n(|\alpha\rangle, |\alpha\rangle) + \sin[(2k+1)\theta]\mathcal{C}_n(|\alpha\rangle, |\beta\rangle) + \sin^2\left(\frac{2k+1}{2}\theta\right)\mathcal{C}_n(|\beta\rangle, |\beta\rangle) \tag{11}$$

The last summand is zero, since $C_n(|\beta\rangle) = 0$ given $|\beta\rangle$ is local. The second summand may also be computed readily, recalling Equation 3. Then $(-i\sigma^y)^{\otimes n}|N-1\rangle = |0\rangle$, so that only the $\langle 0|$ term of $\overline{\langle\psi^0|}$ is relevant and $\mathcal{C}_n(|\alpha\rangle, |\beta\rangle) = \frac{1}{\sqrt{N-1}}$. Finally, a full expansion shows that

$$\mathcal{C}_n(|\alpha\rangle, |\alpha\rangle) \;=\; \frac{1}{N-1}\sum_{j=1}^{N-2}(-1)^{\#j} \;=\; \frac{-2}{N-1} \tag{12}$$

Thus we see that the concurrence of the Grover iterates is given by

$$C_{2p}(\;|\psi^k\rangle\;) \;=\; \left|\sin[(2k+1)\theta]\frac{1}{\sqrt{N-1}} - \cos^2\left(\frac{2k+1}{2}\theta\right)\frac{2}{N-1}\right| \tag{13}$$

See Figure 1 for the first hundred iterates in ten qubits. Note that the concurrence does not become large as the algorithm cycles; the maximum possible concurrence for normalized states is one.

The concurrence of the Grover state $|\psi^k\rangle$ is simply related to another multipartite entanglement measure on pure states, the Q-measure of the state[10] which quantifies how entangled on average each qubit is with the rest of the system. It can be expressed as[12]

$$Q(\;|\psi\rangle\;) \;=\; 2\left(1 - \frac{1}{n}\sum_{j=1}^{n}\mathrm{Tr}[\rho_j^2]\right), \quad \rho = |\psi\rangle\langle\psi|, \quad \rho_j = \mathrm{Tr}_{k\neq j}(\rho) \tag{14}$$

Here, ρ_j is the *reduced state* of the jth qubit, generally a convex sum of pure states or *mixed* state.[6] Meyer calculates the explicit form of the Q-measure for the Grover state at any iteration. Using this result[10] and rewriting the angle $\theta = 2\sin^{-1}(1/\sqrt{N}) = 2\csc^{-1}(\sqrt{N})$, we find that the two quantities are related by:

$$Q(\;|\psi^k\rangle\;) \;=\; \left(\frac{N}{2} - 1\right)\Big[\;C_{2p}(|\psi^k\rangle)\;\Big]^2 \tag{15}$$

Recall from the literature that the square of the n-concurrence is itself an entanglement monotone, the n-tangle.[11] The fact that these two measures of entanglement of the Grover state are proportional is likely due to symmetries respected by Grover's algorithm. It is in some sense unsurprising that the concurrence would generically be smaller than Q, in that concurrence checks exclusively for a superposition within $|\psi\rangle$ of some state with its time-reversal[9] while Q as noted seeks out many pairwise entanglements.

Remark A standard variant of Grover's algorithm replaces the oracle $\mathcal{O}_{|x\rangle}$ with a multi-target oracle $\mathcal{O}_{\mathcal{S}}$, $\mathcal{S} \subset \{|j\rangle\;;\;0 \leq j \leq N-1\}$. For this variant, the concurrence $|\psi^k\rangle$ depends on the number and type of target states in the solution set $\mathcal{S}$. Indeed, $|\beta\rangle = \frac{1}{\sqrt{|\mathcal{S}|}}\sum_{j\in\mathcal{S}}|j\rangle$, which may have non-zero n-concurrence.

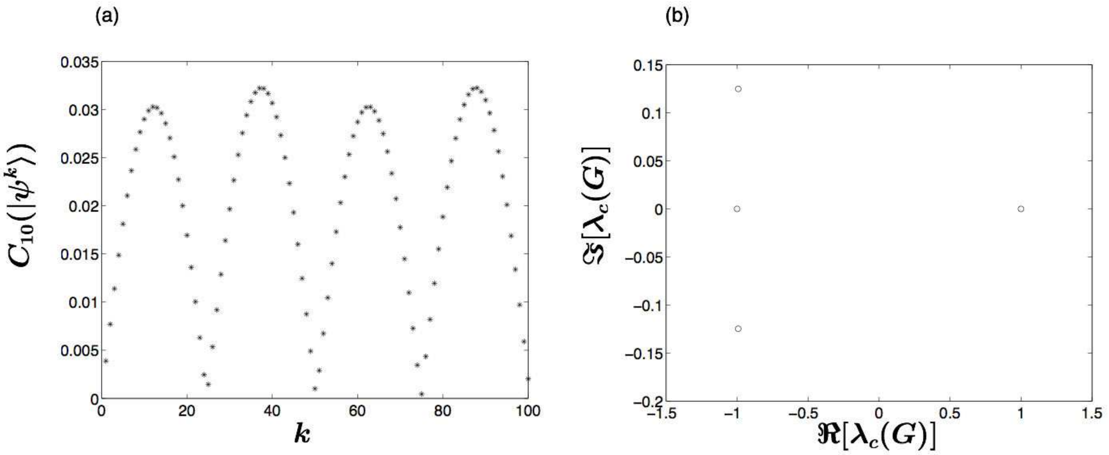

Figure 1. Entanglement properties of Grover's algorithm on $n = 10$ qubits. (a) The concurrence of the Grover state $|\psi^k\rangle$ as a function of iteration number k. Note that very little concurrence is created by the algorithm; the maximal allowed $C_n(|\psi\rangle)$ for $\langle\psi|\psi\rangle = 1$ is one. The highest concurrence shown is slightly larger than $C_n(\frac{1}{\sqrt{2}}|\alpha\rangle + \frac{1}{\sqrt{2}}|\beta\rangle) = \frac{1}{\sqrt{N-1}} - \frac{1}{N-1} \approx$ 0.3030. (b) The unimodular concurrence spectrum of a single Grover operator $G = H^{\otimes n}(I_N - 2|0\rangle\langle 0|)H^{\otimes n}\mathcal{O}$. Although the spectrum is sparse, 0 is a element of the convex hull of these eigenvalues. Hence, there is some, perhaps nonlocal state $|\phi\rangle$ with $C_n(|\phi\rangle) = 0$ yet $G|\phi\rangle = 1$.

Concurrence capacity of a Grover iterate

The above discussion shows that Grover's algorithm, even when considered over all iterates, never utilizes any maximally concurrent states, i.e. never $C_{2p}(|\psi^k\rangle) = 1$. This conclusion that the search algorithm only makes use of some of the entanglement resources available is consistent with earlier studies of Q-dynamics,[10] where the maximum Q is still roughly $0.5 < 1$.

We next consider the concurrence dynamics of the Grover computation itself,

$$G = H^{\otimes n}(I_N - 2|00\cdots 0\rangle\langle 00\cdots 0|)H^{\otimes n}\mathcal{O}_{|x\rangle} = (I_N - 2|\psi^0\rangle\langle\psi^0|)\mathcal{O}_{|x\rangle}$$

One might wonder if the reason the $|\psi^k\rangle$ do not become highly concurrent is that G may not build large concurrences. In fact, this is not the case. Earlier work[8, 9] has shown the following:

> Fix $v \in SU(N)$, with any CCD by $v = k_1\ a\ k_2$. If 0 is contained within the polygon spanned by $\lambda_c(v) = \text{spec}(a^2)$ then there exists some normalized $|\phi\rangle \in \mathcal{H}_n$ with $C_n(|\phi\rangle) = 0$ yet $C_n(v|\phi\rangle) = 1$.

Using numerical methods, we compute these eigenvalues as the number of qubits is $n = 2, 4, 6, 8, 10$. (See Figure 1, right for case $n = 10$.) In each case, the concurrence spectrum holds 1 with high multiplicity yet also contains four sporadic eigenvalues: -1 with multiplicity two, and for some small, decreasing $\delta = \delta(n)$ both $\mathrm{e}^{i\pi\pm\delta}$, each with multiplicity one. Thus the numerics show that 0 lies within the convex hull of $\text{spec}(a^2)$ in each case. Hence, there exists some $|\phi\rangle$, perhaps nonlocal yet with $C_n(|\phi\rangle) = 0$, so that $C_n(\ G|\phi\rangle\ ) = 1$.

We finally remark that the concentration of the concurrence spectrum of $G = k_1 a k_2$ heuristically decreases the number of degrees of freedom when computing such $|\phi\rangle$. See Appendix A. The first step is to choose a weighting of the eigenvalues which places 0 explicitly within the convex hull of $\lambda_c(G) = \text{spec}(a^2)$. For $n = 10$, this forces nonzero weights on the leftmost four eigenvalues, while on a widely distributed concurrence spectrum there would be myriad possibilities of which eigenvalues to weight. In §4, we explicitly construct such states $|\phi\rangle$.

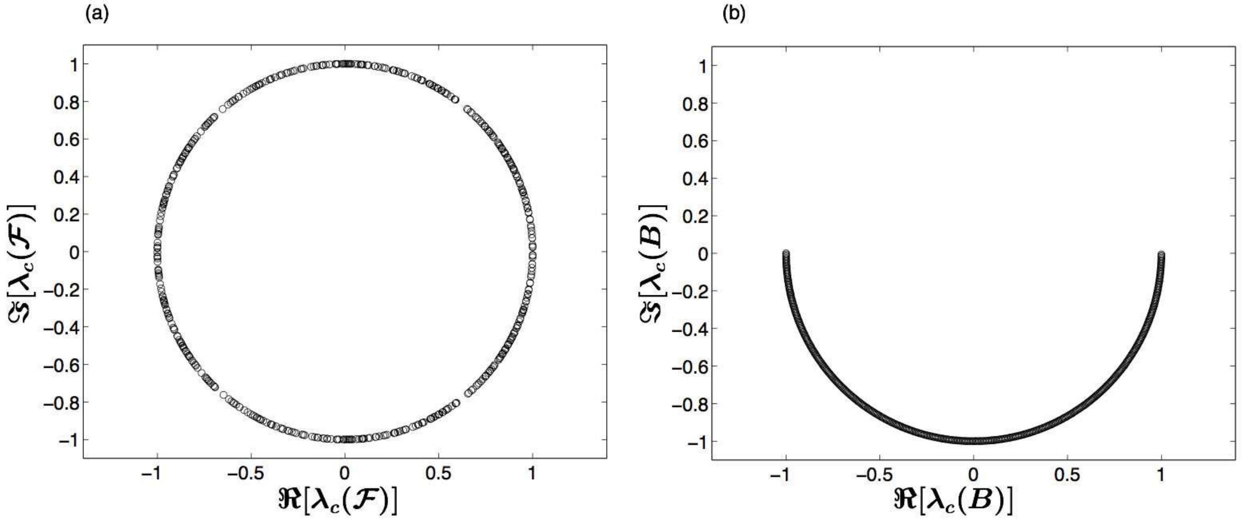

Figure 2. Concurrence spectra of two ten-qubit unitaries: (a) the Fourier transform and (b) the quantum baker's map. In case (a) 0 is contained in the convex hull meaning that a single Fourier transform can map a zero concurrence state to a maximally concurrence one. In contrast, a single iteration of the baker's map cannot do so because its spectrum is limited to a single halfplane within $\mathbb{C}$.

3. NUMERICAL OBSERVATIONS: CONCURRENCE SPECTRA OF OTHER COMPUTATIONS

Generically, most $v \in SU(N)$ will have evenly spread concurrence spectra and hence concurrence capacity of one.[8, 9] However, most quantum computations are far from generic unitary evolutions of $\mathcal{H}_n$. Indeed, admitting a small quantum circuit is an exceptional property. Intuitively, since there are $4^n - 1$ real degrees of freedom in the group of all unitary evolutions $SU(2^n)$, most evolutions require exponentially large circuits. Thus, it is interesting to consider the concurrence spectra of well-known algorithms and seek structure, similar to the structure already found in the Grover computation.

We first consider the Fourier transform $\mathcal{F}_n = \frac{1}{\sqrt{N}} \sum_{j,k=0}^{N-1} \omega^{jk} |k\rangle\langle j|$, $\omega = \mathrm{e}^{2\pi i/N}$. Using algebra,[9] we note that for any decomposition $\mathcal{F}_n = k_1 a k_2$, the spectrum of a^2 does not depend on the choice of decomposition. Indeed, the concurrence spectrum of any v, say $\lambda_c(v)$, may also be computed as spec($[(-i\sigma^y)^{\otimes n}]^\dagger v (-i\sigma^y)^{\otimes n} v^T$). Hence, a computation shows that the concurrence spectrum of the Fourier transform is given as the spectrum of the following operator:

$$[(-i\sigma^y)^{\otimes n}]^\dagger \mathcal{F}_n (-i\sigma^y)^{\otimes n} \mathcal{F}_n^T \quad = \quad \frac{1}{N} \sum_{j,q=0}^{N-1} (-1)^{\#j} \left(\sum_{\ell=0}^{N-1} (-1)^{\#N-\ell-1} [\overline{\omega}^{j+q}]^{\ell} \right) |j\rangle\langle q| \qquad (16)$$

Here, $\#p$ for an integer p is the number of 1's within its binary expansion. Numerical tests show that the expression within the parentheses sometimes vanishes, although it is not clear how analytically compute the eigenvalues of this operator. The two-qubit Fourier transform does not have capacity one, while the concurrence spectrum becomes progressively more spread for $n = 4, 6$. The quantum Fourier transform also has a well-spread concurrence spectrum for $n = 8, 10$. We also note that even in 10-qubits, the concurrence spectrum of $\mathcal{F}_n$ is not evenly dispersed about $\{|z| = 1\}$ but rather contains noticeable gaps; see Figure 2.

Another example of an iterated quantum algorithm besides Grover's algorithm is the quantum baker's map. This map describes the symbolic dynamics of a quantum system whose behavior is chaotic in the sense of showing hypersensitivity to perturbations. The Balazs-Voros quantum baker's map acting on n qubits is defined by

$$B_n \;=\; \mathcal{F}_n(I_2 \otimes \mathcal{F}_{n-1}^\dagger) \qquad (17)$$

The entangling power of this map was studied extensively by Scott and Caves.[13] They show that multiple iterations of the map tend to map (pure) product states to highly entangled states. In particular, suppose for a given k we compute the value of the n-tangle $C_n(B_n^k|\psi\rangle)^2$ and average over all $|\psi\rangle = \otimes_{j=1}^n |\psi_j\rangle$. Then as $k \mapsto \infty$, this average seems to converge to a value slightly larger than the average n-tangle over all (generically nonlocal) pure states of n qubits.

We now use our techniques to investigate the entanglement created by a single iteration of the quantum baker's map B_n. The results provide a contrast to earlier work, as they indicate that a single application of B_n is not generically entangling. In Figure 2, we plot the concurrence spectrum of a single iteration of B_n on $n = 10$ qubits contrasted to that of the quantum Fourier transform. Notice that zero is not contained in the convex hull of $\lambda_c(B_n) = \mathrm{spec}(\ [(-i\sigma^y)^{\otimes n}]^\dagger B_n (-i\sigma^y)^{\otimes n} B^T\ )$. Therefore, a single iteration of B_n will not create a concurrence one state from a concurrence zero state. Numerical evidence also suggests that the concurrence spectrum of B_n is doubly-degenerate for any n, and that $\lambda_c(B_n)$ is restricted to the lower half circle in the complex plane. Specifically, if we restrict $(-i\log) : \{|z| = 1\} \to [-\pi, \pi]$, then numerically one observes $-i\log[\lambda_c(B_n)] \subset [-\pi, 0)$. Moreover, the angle of separation between the largest such argument and 0 appears to decrease as $\pi/2^{n-1}$. As with the Fourier transform, it would be interesting to carry-out the eigenvalue analysis analytically.

n, # qubits	$\max\{\ -i\log(\lambda)\ ;\ \lambda \in \lambda_c(B_n)\ \}$	$\pi/2^{n-1}$
4	−0.392 699 081	0.392 699 081
6	−0.098 174 770	0.098 174 770
8	−0.024 543 693	0.024 543 693
10	−0.006 135 923	0.006 135 923

4. STATES REALIZING THE CONCURRENCE CAPACITY OF THE GROVER MAP

Recall Equation 7, the definition of the concurrence capacity of a unitary evolution $v \in SU(N)$, in case $n = 2p$:

$$\kappa_{2p}(v) \ = \ \max\{\ C_{2p}(v|\psi\rangle)\ ;\ C_{2p}(|\psi\rangle) = 0,\ \langle\psi|\psi\rangle = 1\ \}$$

This definition has been the focus of much theoretical work, as the `CCD` makes it convenient to consider states $|\psi\rangle$ with $C_{2p}(\ |\psi\rangle\ ) = 0$. Indeed, such states are classified[8]; each such normalized state satisfies $|\psi\rangle = k \cdot |000\cdots 0\rangle$ for some $k \in K$. However, the definition is limited, in that $C_{2p}(\ |\psi\rangle\ ) = 0$ is a much weaker condition than $|\psi\rangle = \otimes_{j=1}^n |\psi_j\rangle$ for $p > 1$. We recall the basic four-qubit example that $C_{2p}(|W\rangle) = 0$, although $|W\rangle = \frac{1}{2}(\ |0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle\ )$ is (quite) entangled. Hence, it is of interest to consider the definition of $\kappa_{2p}(-)$ more carefully, by considering entanglement of the null-concurrent $|\psi\rangle$ returned by the theory.

Computing such $|\psi\rangle$ is the topic of Appendix A. We note that the construction requires auxilliary machinery for computing a *fixed* choice of `CCD` for the given unitary v, as well as the requisite similarity matrices E_0. There are many degrees of freedom which may be exploited in constructing such states as well, particularly (i) the choice of `CCD` and (ii) the choice of weights within $0 = \sum_{j=0}^{N-1} t_j \lambda_j$ for $\lambda_c(v) = \{\lambda_j\}_{j=0}^{N-1}$, $0 \le t_j \le 1$, $\sum_{j=0}^{N-1} t_j = 1$.

We here report three such output states for the Grover's map G which is iterated in the course of applying Grover's algorithm. We take $n = 4$ qubits and choose the target state $|x\rangle = |15\rangle$. Thus, to apply the appendix one requires a `CCD` of $G = H^{\otimes 4}(I_{16} - 2|00\cdots 0\rangle\langle 00\cdots 0|)H^{\otimes 4}\mathcal{O}_{|15\rangle}$, which is determinant one. The most convenient choice in our `MatLab` implementation orders the diagonal matrix $E_0 a^2 E_0^\dagger$ so that the first four eigenvalues are $\lambda_0 = -1$, $\lambda_1 = -1$, $\lambda_2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, and $\lambda_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ respectively, with $\lambda_4 = \lambda_6 = \cdots = \lambda_{15} = 1$. We next report three explicitly constructed $|\psi\rangle$ which are null-concurrent with $C_4(G|\psi\rangle) = 1$. For each, we also provide the Q-measure in order to quantify how entangled $|\psi\rangle$ may be despite $C_{2p}(|\psi\rangle) = 0$.

$\|\psi\rangle$	choice of weights	$Q(\ \|\psi\rangle\ )$
$0.50000000000000\|0\rangle - 0.03624195588241\|1\rangle$ $+0.10560461176979\|2\rangle - 0.41308351052014\|3\rangle$ $-0.06936265588739\|4\rangle + 0.06596124263797\|5\rangle$ $-0.24027928828975\|6\rangle + 0.24027928828975\|9\rangle$ $-0.06596124263797\|10\rangle - 0.06936265588739\|11\rangle$ $+0.41308351052014\|12\rangle + 0.10560461176979\|13\rangle$ $-0.03624195588241\|14\rangle + 0.50000000000000\|15\rangle$	$\frac{1}{2}\lambda_0 + \frac{1}{2}\lambda_4 = 0$	0.982723
$-0.28867513459481\|0\rangle - 0.02959143306412\|1\rangle$ $+0.08622580444024\|2\rangle - 0.62595640857213\|3\rangle$ $-0.05663437137612\|4\rangle - 0.23481800550717\|5\rangle$ $-0.48486235195114\|6\rangle - 0.09248791723849\|9\rangle$ $-0.34253226368246\|10\rangle - 0.05663437137612\|11\rangle$ $+0.04860613938250\|12\rangle + 0.08622580444024\|13\rangle$ $-0.02959143306412\|14\rangle + 0.28867513459481\|15\rangle$	$\frac{1}{3}\lambda_2 + \frac{1}{3}\lambda_3 + \frac{1}{3}\lambda_4 = 0$	0.789296
$-0.28867513459481\|0\rangle + 0.13307838607972\|1\rangle$ $-0.04327252689545\|2\rangle - 0.10174037401628\|3\rangle$ $-0.08980585918427\|4\rangle - 0.20327318462360\|5\rangle$ $-0.59977175644388\|6\rangle + 0.02242148725426\|9\rangle$ $-0.37407708456602\|10\rangle - 0.08980585918427\|11\rangle$ $-0.47560989517334\|12\rangle - 0.04327252689545\|13\rangle$ $+0.13307838607972\|14\rangle + 0.28867513459481\|15\rangle$	$\frac{1}{3}\lambda_2 + \frac{1}{3}\lambda_3 + \frac{1}{3}\lambda_5 = 0$	0.805425

Notice the entanglement of the concurrence zero states with respect to the Q measure is large. Although these states have no overlap with their time-reversed state, the average entanglement of each qubit with the other qubits is relatively large. It would be interesting to know which weights on the concurrence spectrum correspond to the state of this type with minimum Q. Note that there are $N - 1$ real degrees of freedom in choosing weights.

5. CONCLUSIONS

We have presented a technique to quantify how entangling a given unitary operator is with respect to one measure of entanglement: the n-concurrence. Our approach to studying entangling dynamics is novel in that we show how to explicitly compute the states with zero initial concurrence that are mapped to maximally concurrent states by the unitary computation. In this sense, we study the entangling power of the evolution on the entire state space. This is distinct from other approaches which focus on how the entanglement of the data state evolves under a quantum computation beginning with a pure product state.

Earlier theoretical work on the entanglement dynamics of the entire state space focuses on a concurrence capacity (or entanglement capacity in two-qubits,) i.e. the quantity of new concurrence which may be created by a given evolution v starting with *any* concurrence zero state. This may be studied efficiently using a matrix decomposition, the `CCD` by $v = k_1 a k_2$. For in fact the capacity depends only on the central factor a, indeed only on the concurrence spectrum $\lambda_c(v) = \text{spec}(a^2)$. However, numerical investigations using Meyer's Q measure show that sample concurrence zero states which a computation maps to maximally concurrent states may yet be highly entangled. Nonetheless, quantum computations such as Grover's algorithm or the Fourier transform still possess structured concurrence spectra. This perhaps indicates more structure in their concurrence dynamics than is predicted by the capacity alone. In particular, these constructions might be useful for identifying underlying symmetries in entanglement dynamics of evolutions and computations.

APPENDIX A. COMPUTING STATES REALIZING CONCURRENCE CAPACITIES

The theoretical analysis allows for descriptions of concurrence capacity of $v = k_1 a k_2 \in SU(2^n)$ in terms of $\text{spec}(a^2)$. The most intuitive result is this capacity must be one, i.e. there must exist some normalized $|\psi\rangle$ with $C_{2p}(|\psi\rangle) = 0$ and $C_{2p}(v|\psi\rangle) = 1$, if and only if 0 lies within the polygon spanned by $\text{spec}(a^2)$. However, as states with $C_{2p}(|\psi\rangle) = 0$ may be highly entangled according to other quantifications of entanglement, one would like in the abstract to classify such $|\psi\rangle$ and study how close they may be to local. As a first step, we consider how to construct any $|\psi\rangle$ satisfying this property.

Suppose first we have weights which place 0 within the convex hull of the concurrence spectrum $\{\lambda_j\}_{j=0}^{N-1}$. Many of these weights t_j may be zero; note however that indexing is important.

$$\sum_{j=0}^{N-1} t_j \lambda_j = 0 \quad \text{where} \sum_{j=0}^{N-1} t_j = 1, 0 \leq t_j \leq 1 \tag{18}$$

The t_j and λ_j may be used directly to produce a sample $|\psi\rangle$, as follows. First, we recall the similarity matrix[8] E_0 which rotates an even-qubit CCD onto the decomposition $SU(N) = SO(N)\ D\ SO(N)$, for the group of diagonal determinant-one unitaries. The columns of E_0 are all either of the form $|j\rangle + (-1)^{\#j}|N-j-1\rangle$ or $i|j\rangle - (-1)^{\#j} i|N-j-1\rangle$. The similarity relation for which E_0 is constructed is that $E_0 K E_0^\dagger = SO(N)$, i.e. the determinant one (real) orthogonal matrices. Thus, for $v = k_1 a k_2$, we have in particular that $o_2 = E_0^\dagger k_2 E_0$ is some real matrix, $o_2 o_2^T = I_N$, $\det(o_2) = 1$. Since $SO(N)$ is a group, o_2^T is again orthogonal and $o_2 o_2^T = I_N$. We show momentarily that a possible choice of $|\psi\rangle$ is then

$$|\psi\rangle = k_2^\dagger E_0 \left(\sum_{j=0}^{N-1} \sqrt{t_j} {\lambda_j}^{-1/2} \right) |j\rangle = E_0 o_2^T \left(\sum_{j=0}^{N-1} \sqrt{t_j} {\lambda_j}^{-1/2} \right) |j\rangle \tag{19}$$

The further significance of a fixed choice of E_0 is that $E_0 d E_0^\dagger = \sum_{j=0}^{N-1} \lambda_j^{1/2} |j\rangle\langle j|$. Thus, although the eigenstates of a are given by the form above and resemble GHZ states, the *particular choice* of j and possible complex multiple corresponds to a single eigenvalue of a. In the above equation, $\sqrt{\lambda_j}$ should be chosen to coincide with this diagonalization of a.

We now justify this assertion briefly. Put $|\eta\rangle = E_0^\dagger |\psi\rangle = o_2^T \sum_{j=0}^{\ell} (t_j/\lambda)^{1/2} |j\rangle$. We recall[8] that generically $\mathcal{C}_{2p}(E_0|\phi\rangle, E_0|\psi\rangle) = \overline{\langle\phi|\psi\rangle}$. We also label $d = \sum_{j=0}^{\ell} \lambda_j |j\rangle\langle j|$. We next note the following:

$$\overline{\langle\eta|\eta\rangle} = \left(\sum_{j=0}^{N-1} (t_j/\lambda_j)^{1/2} \langle j| \right) o_2 o_2^T \left(\sum_{k=0}^{N-1} (t_\ell/\lambda_\ell)^{1/2} |\ell\rangle \right) = \sum_{j=0}^{N-1} t_j \overline{\lambda}_j = 0 \tag{20}$$

using the conjugate of Equation 18. Thus $\mathcal{C}_{2p}(|\psi\rangle, |\psi\rangle) = \mathcal{C}_{2p}(E_0|\eta\rangle, E_0|\eta\rangle) = \overline{\langle\eta|\eta\rangle} = 0$, i.e. $C_{2p}(|\psi\rangle) = 0$. On the other hand, by symmetry $\mathcal{C}_{2p}(v|\psi\rangle, v|\psi\rangle) = \mathcal{C}_{2p}(k_1 a k_2|\psi\rangle, k_1 a k_2|\psi\rangle) = \mathcal{C}_{2p}(a k_2|\psi\rangle, a k_2|\psi\rangle)$. Now $a = E_0 d E_0^\dagger$ while $k_2|\psi\rangle = E_0 \left(\sum_{j=0}^{N-1} \sqrt{t_j} {\lambda_j}^{-1/2} \right) |j\rangle$. Thus

$$a k_2 |\psi\rangle = E_0 d \left(\sum_{j=0}^{N-1} \sqrt{t_j} {\lambda_j}^{-1/2} \right) |j\rangle \tag{21}$$

This yields the following computation, verifying that $C_{2p}(v|\psi\rangle) = 1$:

$$\begin{array}{rcl} \mathcal{C}_{2p}\Bigg(E_0 d \sum_{j=0}^{N-1} (t_j/\lambda_j)^{1/2} |j\rangle, E_0 d \sum_{j=0}^{N-1} (t_j/\lambda_j)^{1/2} |j\rangle \Bigg) & = & \\ \sum_{j=0}^{N-1} (t_j/\lambda_j)^{1/2} \langle j|\ \left(\sum_{k=0}^{N-1} \lambda_k |k\rangle\langle k|\right)\ \sum_{\ell=0}^{N-1} (t_\ell/\lambda_\ell)^{1/2} |\ell\rangle & = & \sum_{j=0}^{N-1} t_j \\ & = & 1 \end{array} \tag{22}$$

REFERENCES

1. V.Zhirnov, R. Cavin III, J. Hutchby, Limits to Binary Logic Switch Scaling–A Gedanken Model, *Proc. of the* IEEE, vol 91, no. 11, 1934 (2003).
2. Feynman, R., Simulating physics with computers, *Int. J. Theor. Phys*, **21**, 467 (1982).

3. Hallgren, S. Polynomial time quantum algorithms for Pell's equation and the principal ideal problem, *Symposium on the Theory of Computation*, (2002).
4. Jozsa, R. Notes on Hallgren's efficient quantum algorithm for solving Pell's equation, `http://arXiv.org/abs/quant-ph/0302134` (2003).
5. Knapp, A. *Lie Groups Beyond an Introduction*, volume 140. Progress in Mathematics, Birkhäuser, (1996).
6. Nielsen, M. and Chuang, I. *Quantum Information and Computation*. Cambridge Univ. Press, (2000).
7. Vidal, G.: Entanglement monotones. J. Mod. Opt. **47**, 355 (2000).
8. Bullock, S. and Brennen, G. Canonical decompositions of n-qubit quantum computations and concurrence, J. of Math. Phys. in press, `http://arXiv.org/abs/quant-ph/0309104` (2003).
9. Bullock, S., Brennen, G., and O'Leary, D. Time reversal and n-qubit canonical decompositions, `http://arXiv.org/abs/quant-ph/0402051` (2004).
10. Meyer, D. and Wallach, N.: Global entanglement in multi-partite systems. J. of Math. Phys. **43**, 4273 (2002).
11. Wong, A. and Christensen, N.: Potential multiparticle entanglement measure. Phys. Rev. A **63**, 044301 (2001).
12. Brennen, G.: An observable measure of entanglement for pure states of multi-qubit systems, Q. Inf. and Comp. **3**, no. 6 619 (2003).
13. Scott, A.J. and Caves, C.M. Entangling power of the quantum baker's map. J. Phys. A **36**, 9553 (2003).
14. See the theory section of the `QIST` roadmap, `http://qist.lanl.gov`