The geometry of entanglement and Grover's algorithm

2008 J. Phys. A: Math. Theor. 41 105202

(http://iopscience.iop.org/1751-8121/41/10/105202)

J. Phys. A: Math. Theor. **41** (2008) 105202 (17pp) doi:10.1088/1751-8113/41/10/105202

The geometry of entanglement and Grover's algorithm

Toshihiro Iwai, Naoki Hayashi and Kimitake Mizobe

Department of Applied Mathematics and Physics, Kyoto University, Kyoto 606-8501, Japan

Received 20 November 2007, in final form 16 January 2008
Published 26 February 2008
Online at stacks.iop.org/JPhysA/41/105202

Abstract
A measure of entanglement with respect to a bipartite partition of n-qubit has been defined and studied from the viewpoint of Riemannian geometry (Iwai 2007 *J. Phys. A: Math. Theor.* **40** 12161). This paper has two aims. One is to study further the geometry of entanglement, and the other is to investigate Grover's search algorithms, both the original and the fixed-point ones, in reference with entanglement. As the distance between the maximally entangled states and the separable states is known already in the previous paper, this paper determines the set of maximally entangled states nearest to a typical separable state which is used as an initial state in Grover's search algorithms, and to find geodesic segments which realize the above-mentioned distance. As for Grover's algorithms, it is already known that while the initial and the target states are separable, the algorithms generate sequences of entangled states. This fact is confirmed also in the entanglement measure proposed in the previous paper, and then a split Grover algorithm is proposed which generates sequences of separable states only with respect to the bipartite partition.

PACS numbers: 02.40.Pc, 03.65.−w, 03.67.−a

1. Introduction

A measure of entanglement with respect to a bipartite partition of n-qubit has been defined and studied from the viewpoint of Riemannian geometry [1, 2]. While there are a number of candidates for measures of entanglement [3–10], the measure taken up in [2] is of the form $\det(I - \rho)$, where ρ is the reduced density matrix associated with the bipartite partition. This paper studies further the geometry of entanglement and investigates Grover's search algorithms in reference with entanglement.

As the distance between the maximally entangled states and the separable states is known already in the previous paper [2], this paper determines the set of maximally entangled states nearest to the typical separable state which is used as an initial state in Grover's search algorithms. Further, a geodesic segment is found, which has the length as large as the distance mentioned above.

Grover's search algorithm generates a sequence of states approaching a target state by iterative applications of the unitary operators determined in the algorithm. Grover gave two algorithms, one of which is the original algorithm [11] and the other the fixed-point algorithm [12]. To observe how the algorithm works, it is of help to measure the entanglement for Grover sequences. In this paper, a measure proposed in [2] is used to evaluate the entanglement for the Grover sequences. The measurement shows that though the initial and the target states in the algorithm are separable, the sequence generated by the algorithms are entangled. In view of this, a split Grover algorithm, which generates sequences of separable states only, will be proposed by a slight modification of the Grover algorithm.

This paper is organized as follows: section 2 is a brief review from [2], in which the sets of separable states and of maximally entangled states are identified, and the distance between those sets is described. In section 3, maximally entangled states are determined which are nearest from the state that is posed usually as an initial state in the Grover algorithm. Section 4 is concerned with 'horizontal' paths which join the initial state with maximally entangled target states. In particular, geodesic segments are found, which are as long as the distance stated in section 2. Section 5 contains a review of Grover's algorithms, the original one and the fixed-point one. In particular, the unitary operators for the fixed-point algorithm are represented in the matrix form. In section 6, the entanglement measure is evaluated along the sequence determined by both of the Grover algorithms. In section 7, a split Grover algorithm is proposed, which brings the initial state into a separable target state along a sequence of separable states only. Section 8 contains remarks on distances among states concerned. Further, an extension of the entanglement measure is touched upon.

2. Geometric setting up

This section is a review from [2]. Let $\mathcal{H} \cong \mathbb{C}^2$ be a Hilbert space for one-qubits with orthonormal basis vectors $|0\rangle, |1\rangle$. The Hilbert space for n-qubits is given by the tensor product $\mathcal{H}^{\otimes n}$. We consider the separability of n-qubits. There are a number of ways to partition the n-qubit system into subsystems. If an n-qubit state is separable, it is put in the form of a tensor product of p-qubit state and q-qubit state with $p + q = n$. Let

$$P = 2^p, \qquad Q = 2^q, \qquad N = 2^n = PQ. \tag{2.1}$$

Let y and z be the binary integers of the form $y = y_p y_{p-1} \cdots y_2 y_1$, $z = z_q z_{q-1} \cdots z_2 z_1$ with $y_j, z_k \in \{0, 1\}$, respectively. Then, with respect to the basis $|y\rangle \otimes |z\rangle$ of the total system $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q} \cong \mathcal{H}^{\otimes n}$, $|\phi\rangle \in \mathcal{H}^{\otimes n}$ is expressed as

$$|\phi\rangle = \sum_{y=0}^{P-1} \sum_{z=0}^{Q-1} c_{yz} |yz\rangle, \qquad c_{yz} \in \mathbb{C}. \tag{2.2}$$

We identify $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$ with $\mathbb{C}^{P\times Q}$, the set of $P \times Q$ complex matrices, through

$$|\phi\rangle \longmapsto C = (c_{yz}) \in \mathbb{C}^{P\times Q}. \tag{2.3}$$

The $\mathbb{C}^{P\times Q}$ is endowed with the Hermitian inner product,

$$\langle C_1|C_2\rangle = \mathrm{tr}\big(C_1 C_2^\dagger\big), \qquad C_1, C_2 \in \mathbb{C}^{P\times Q}. \tag{2.4}$$

For the reason of the probability measure, the state space is defined to be

$$M = \{C \in \mathbb{C}^{P\times Q} | \langle C|C\rangle = \mathrm{tr}(CC^\dagger) = 1\}. \tag{2.5}$$

In sections 3 and 4, we will treat M as a Riemannian manifold in the real category, and the real inner product

$$(C_1|C_2) := \mathrm{Re}\langle C_1|C_2\rangle \tag{2.6}$$

is used. The Riemannian metric is defined through the inner product $(X_1|X_2)$ for tangent vectors $X_1, X_2 \in T_C(M)$, where

$$T_C M = \{X \in \mathbb{C}^{P\times Q} | (C|X) = 0\}. \tag{2.7}$$

Further, the group $G := U(P) \times U(Q)$ acts on M in the manner

$$C \longmapsto gCh^\top, \qquad (g,h) \in U(P) \times U(Q), \tag{2.8}$$

where $h^\top$ denotes the transpose of $h \in U(Q)$. With respect to this action, the tangent space $T_C M$ is decomposed into a direct sum of the vertical subspace V_C and the horizontal subspace H_C; $T_C M = V_C \oplus H_C$, where V_C is defined to be the tangent space $T_C\mathcal{O}_C$ to the G-orbit $\mathcal{O}_C$ through C, and where $H_C = V_C^\perp$, the orthogonal complement to V_C. By definition, V_C and H_C are put in the form

$$V_C = \{\xi C + C\eta^\top | \xi \in u(P), \eta \in u(Q)\}, \tag{2.9}$$

$$H_C = \{X \in T_C M | CX^\dagger - XC^\dagger = 0, C^\dagger X - X^\dagger C = 0\}, \tag{2.10}$$

where $u(P)$ and $u(Q)$ are the Lie algebras of $U(P)$ and $U(Q)$, respectively.

We note here that the matrix $CC^\dagger$ is the partial trace of the density matrix $\rho = |\phi\rangle\langle\phi|$ with respect to the latter q-qubit of $\mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$. In view of this, we may call C maximally entangled, if all of eigenvalues of $CC^\dagger$ are equal to one another, where $P \leqslant Q$ is assumed.

If $|\phi\rangle \in \mathcal{H}^{\otimes p} \otimes \mathcal{H}^{\otimes q}$ is separable, $|\phi\rangle$ is expressed as $|\psi_1\rangle \otimes |\psi_2\rangle$ with $|\psi_1\rangle \in \mathcal{H}^{\otimes p}$ and $|\psi_2\rangle \in \mathcal{H}^{\otimes q}$. Then, the corresponding matrix C is put in the form $C = \boldsymbol{c}_1\boldsymbol{c}_2^\top$, where $\boldsymbol{c}_1 = (c_k) \in \mathbb{C}^P$ and $\boldsymbol{c}_2 = (c'_j) \in \mathbb{C}^Q$ in correspondence with $|\psi_1\rangle = \sum c_k|k\rangle \in \mathcal{H}^{\otimes p}$ and $|\psi_2\rangle = \sum c'_j|j\rangle \in \mathcal{H}^{\otimes q}$, respectively. Hence, the C is of rank one. Conversely, if $\mathrm{rank}C = 1$, there exist vectors $\boldsymbol{c}_1 \in \mathbb{C}^P$ and $\boldsymbol{c}_2 \in \mathbb{C}^Q$ such that $C = \boldsymbol{c}_1\boldsymbol{c}_2^\top$, so that the corresponding state $|\phi\rangle$ is separable.

In [2], a function defined below is adopted as a measure of entanglement,

$$F(C) = \det(I_P - CC^\dagger), \qquad I_P : P \times P \text{ identify matrix}, \tag{2.11}$$

which has the properties (i) $F(C) = 0$ if and only if C is separable and (ii) $F(C)$ attains the maximal value, $((P-1)/P)^P$, if and only if C is maximally entangled. Further, $F(C)$ is invariant under the $U(P) \times U(Q)$ action.

According to [2], we describe the sets of separable states and of maximally entangled states, and the distance between them. If C is maximally entangled, one has $CC^\dagger = \frac{1}{P}I_P$, so that the set of maximally entangled states is described as

$$\mathcal{E} := \left\{C \in \mathbb{C}^{P\times Q} | CC^\dagger = \frac{1}{P}I_P\right\}, \tag{2.12}$$

which is identified with the Stiefel manifold of orthonormal P-frames in $\mathbb{C}^Q$, $V_P(\mathbb{C}^Q) \cong U(Q)/U(Q-P)$. If C is separable, C is singularly decomposed into $C = g[\boldsymbol{e}_1, 0]h^\dagger$, where $\boldsymbol{e}_1 = [1, 0, \ldots, 0]^\top \in \mathbb{C}^P$ and $(g,h) \in U(P) \times U(Q)$. Let $g = [\boldsymbol{u}_1, \ldots, \boldsymbol{u}_P]$ and $h = [\boldsymbol{v}_1, \ldots, \boldsymbol{v}_Q]$. Then, $C = \boldsymbol{u}_1\boldsymbol{v}_1^\dagger$. Since $\boldsymbol{u}_1\boldsymbol{v}_1^\dagger = \boldsymbol{u}_1\mathrm{e}^{\mathrm{i}\theta}(\boldsymbol{v}_1\mathrm{e}^{\mathrm{i}\theta})^\dagger$, and since $\|\boldsymbol{u}_1\| = 1$ in $\mathbb{C}^P$ and $\|\boldsymbol{v}_1\| = 1$ in $\mathbb{C}^Q$, an equivalence relation is defined on the set $S^{2P-1} \times S^{2Q-1}$ through $(\boldsymbol{u}_1, \boldsymbol{v}_1) \sim (\boldsymbol{u}_1\mathrm{e}^{\mathrm{i}\theta}, \boldsymbol{v}_1\mathrm{e}^{\mathrm{i}\theta})$, so that the set of separable states is described as $S^{2P-1} \times_{U(1)} S^{2Q-1}$, which is a fiber bundle over $S^{2P-1}/U(1) \cong \mathbb{C}P^{P-1}$ with fiber S^{2Q-1}.

Proposition 2.1 ([2]). *The sets of maximally entangled states and of separable states with respect to the isomorphism $\mathbb{C}^N \cong \mathbb{C}^{P\times Q}$ are diffeomorphic with the Stiefel manifold $V_P(\mathbb{C}^Q)$ of orthonormal P-frames in the space $\mathbb{C}^Q$ and with $S^{2P-1} \times_{U(1)} S^{2Q-1}$, a fiber bundle over $S^{2P-1}/U(1) \cong \mathbb{C}P^{P-1}$ with fiber S^{2Q-1}, respectively.*

Proposition 2.2 ([2])**.** *The distance between the set, $F^{-1}(0)$, of the separable states, and the level set $F^{-1}(k)$ with $0 \leqslant k \leqslant ((P-1)/P)^P$ is given by*

$$\arccos \sqrt{1-(P-1)(x_-(k))^2}, \tag{2.13}$$

where $x_-(k)$ denotes the smaller one of the solutions to

$$k = (P-1)x^2(1-x^2)^{P-1}. \tag{2.14}$$

In particular, the distance between the set, $F^{-1}((P-1)/P)^P)$, of maximally entangled states and the set, $F^{-1}(0)$, of separable states is given by $\arccos P^{-1/2}$.

3. Maximally entangled states nearest to a separable state

We take a typical separable state A given by

$$A = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & \cdots & 1 & \cdots & 1 \\ \vdots & \ddots & \vdots & & \vdots \\ 1 & \cdots & 1 & \cdots & 1 \end{bmatrix} \in \mathbb{C}^{P\times Q}, \tag{3.1}$$

which corresponds to a state $|a\rangle = \frac{1}{\sqrt{N}} \sum |i_1 i_2 \cdots i_n\rangle$ and is used as an initial state in the search algorithm. We know from the above proposition that the set of maximally entangled states is distant from A by $\arccos P^{-1/2}$. We now wish to know which states in $\mathcal{E}$ are distant from A by $\arccos P^{-1/2}$. The following theorem gives the answer to this question.

Theorem 3.1. *The maximally entangled states Φ_0 nearest to the separable state A are given by*

$$\Phi_0 = \frac{1}{\sqrt{P}}(A + HV^\dagger K^\dagger), \tag{3.2}$$

where the matrices K and H are defined, respectively, by

$$H = \begin{bmatrix} -\frac{P-1}{\sqrt{(P-1)P}} & 0 & \cdots & 0 \\ \frac{1}{\sqrt{(P-1)P}} & \ddots & \ddots & \vdots \\ \vdots & \ddots & -\frac{2}{\sqrt{2\cdot 3}} & 0 \\ \frac{1}{\sqrt{(P-1)P}} & \ddots & \frac{1}{\sqrt{2\cdot 3}} & -\frac{1}{\sqrt{1\cdot 2}} \\ \frac{1}{\sqrt{(P-1)P}} & \ddots & \frac{1}{\sqrt{2\cdot 3}} & \frac{1}{\sqrt{1\cdot 2}} \end{bmatrix} \in \mathbb{C}^{P\times(P-1)}, \tag{3.3}$$

$$K = \begin{bmatrix} -\frac{Q-1}{\sqrt{(Q-1)Q}} & 0 & \cdots & 0 \\ \frac{1}{\sqrt{(Q-1)Q}} & \ddots & \ddots & \vdots \\ \vdots & \ddots & -\frac{2}{\sqrt{2\cdot 3}} & 0 \\ \frac{1}{\sqrt{(Q-1)Q}} & \ddots & \frac{1}{\sqrt{2\cdot 3}} & -\frac{1}{\sqrt{1\cdot 2}} \\ \frac{1}{\sqrt{(Q-1)Q}} & \ddots & \frac{1}{\sqrt{2\cdot 3}} & \frac{1}{\sqrt{1\cdot 2}} \end{bmatrix} \in \mathbb{C}^{Q\times(Q-1)}, \tag{3.4}$$

and where $V \in \mathbb{C}^{(Q-1)\times(P-1)}$ is an arbitrary matrix satisfying

$$V^\dagger V = I_{P-1}, \tag{3.5}$$

which form a submanifold diffeomorphic with $V_{P-1}(\mathbb{C}^{Q-1})$ in $\mathcal{E} \cong V_P(\mathbb{C}^Q)$.

Proof. The distance in the state space $M \cong S^{2N-1}$ is determined by using the length of geodesic segments. Since the geodesics on S^{2N-1} are great circles with radius one, the distance of two points (i.e., unit vectors) is equal to the angle between two unit vectors. Since the angle can be evaluated by the inner product of two unit vectors, our task is now to solve the problem

$$\begin{aligned} &\text{maximize} \quad (\Phi|A), \\ &\text{subject to} \quad \Phi\Phi^\dagger = \frac{1}{P} I_P, \end{aligned} \tag{3.6}$$

where $(|)$ denotes the real inner product and where the constraint condition means that $\Phi \in \mathcal{E}$. □

To solve the problem (3.6), we use the method of undetermined multipliers. Let $\mathcal{H}(P)$ denote the set of $P \times P$ Hermitian matrices. Since the constraint $\Phi\Phi^\dagger - I_P/P = 0$ is an equation for the Hermitian matrix $\Phi\Phi^\dagger$, we take a Lagrange multiplier Ω in $\mathcal{H}(P)$ to define the Lagrangian form,

$$L(\Phi, \Omega) = (\Phi|A) + \left(\Omega \middle| \left(\Phi\Phi^\dagger - \frac{1}{P} I_P\right)\right). \tag{3.7}$$

Necessary conditions for L to be extremal at (Φ, Ω) are that Φ and Ω satisfies

$$A^\dagger + 2\Phi^\dagger\Omega = 0, \tag{3.8a}$$

$$\Phi\Phi^\dagger - \frac{1}{P} I_P = 0. \tag{3.8b}$$

From these equations together with their Hermitian conjugates, we obtain

$$\Phi A^\dagger = -\frac{2}{P}\Omega, \qquad \Omega^2 = \frac{P}{4} A A^\dagger = \frac{1}{4} I, \tag{3.9}$$

where

$$I = \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix} \in \mathcal{H}(P), \tag{3.10}$$

so that the inner product $(\Phi|A)$ is expressed, in terms of Ω, as

$$(\Phi|A) = -\frac{2}{P}\operatorname{tr}(\Omega). \tag{3.11}$$

Hence, our problem is further reduced to the following:

$$\text{minimize} \quad \operatorname{tr}(\Omega), \tag{3.12a}$$

$$\text{subject to} \quad \Omega^2 = \frac{1}{4} I. \tag{3.12b}$$

Lemma 3.2. *The solution to the minimization problem (3.12) is expressed as*

$$\Omega = -\frac{1}{2\sqrt{P}} I, \tag{3.13}$$

where I is given in (3.10).

Proof. For the matrix in the right-hand side of (3.12b), there exists a unitary matrix $U \in U(P)$ such that

$$\frac{1}{4} I = U \operatorname{diag}\left[\frac{P}{4}, 0, \ldots, 0\right] U^\dagger. \tag{3.14}$$

On the other hand, the Hermitian matrix Ω is diagonalized by a unitary matrix $V \in U(P)$,

$$\Omega = V\,\mathrm{diag}[\omega_1, \ldots, \omega_P]V^\dagger, \tag{3.15}$$

where the eigenvalues $\omega_1, \ldots, \omega_P$ of Ω are real valued. Then, equations (3.12*b*), (3.14) and (3.15) are put together to give

$$\begin{aligned}\mathrm{diag}\big[\omega_1^2, \ldots, \omega_P^2\big] &= \frac{P}{4}(V^\dagger U)\mathrm{diag}[1, 0, \ldots, 0](V^\dagger U)^\dagger \\ &= \frac{P}{4}\boldsymbol{u}\boldsymbol{u}^\dagger = \frac{P}{4}(u_j\bar{u}_k),\end{aligned} \tag{3.16}$$

where $\boldsymbol{u} = [u_1, \ldots, u_P]^\top$ is the first column of the unitary matrix $V^\dagger U$ and where $\|\boldsymbol{u}\| = 1$. Therefore, equation (3.16) implies that there exists $m \in \{1, \ldots, P\}$ such that

$$\omega_m = \pm\frac{\sqrt{P}}{2}, \qquad \omega_j = 0, \qquad j \neq m, \tag{3.17}$$

so that

$$\mathrm{tr}(\Omega) = \mathrm{tr}(\mathrm{diag}[\omega_1, \ldots, \omega_P]) = \pm\frac{\sqrt{P}}{2}. \tag{3.18}$$

The minimum value of $\mathrm{tr}(\Omega)$ is then $-\frac{\sqrt{P}}{2}$, so that $\mathrm{tr}(\Omega) = \omega_m = -\frac{\sqrt{P}}{2}$. Hence equation (3.15) is brought into

$$\Omega = -\frac{\sqrt{P}}{2}\boldsymbol{v}\boldsymbol{v}^\dagger, \tag{3.19}$$

where $\boldsymbol{v}$ is the mth column vector of V. Let $\boldsymbol{v} = (v_j)$. Then, the above equation and the constraint (3.12*b*) are put together to show that $v_j = \mathrm{e}^{\mathrm{i}\theta}/\sqrt{P}$, $j = 1, \ldots, P$, so that Ω given in equation (3.13) proves to be the only solution to the minimization problem (3.12). This ends the proof of the lemma. □

We return to (3.8), which are now expressed as

$$A + 2\Omega\Phi = 0, \qquad \Omega = -\frac{1}{2\sqrt{P}}I, \qquad \Phi\Phi^\dagger = \frac{1}{P}I_P. \tag{3.20}$$

We wish to find the matrix Φ in the form

$$\Phi = sA + C, \tag{3.21}$$

where $s \in \mathbb{R}$ and where $C = (c_{k\ell}) \in \mathbb{C}^{P\times Q}$ is orthogonal to A, $(A|C) = 0$, that is,

$$\mathrm{Re}\sum_{k=1}^{P}\sum_{\ell=1}^{Q} c_{k\ell} = 0. \tag{3.22}$$

Since $\Omega A = -\frac{\sqrt{P}}{2}A$, as is easily verified, equations (3.20) and (3.21) are put together to give

$$(1 - s\sqrt{P})A + 2\Omega C = 0. \tag{3.23}$$

Written out componentwise, this equation provides

$$\sum_{k=1}^{P} c_{k\ell} = \frac{1}{\sqrt{Q}}(1 - s\sqrt{P}), \qquad \ell = 1, \ldots, Q. \tag{3.24}$$

Hence, from equation (3.22), we obtain

$$s = \frac{1}{\sqrt{P}}, \qquad \sum_{k=1}^{P} c_{k\ell} = 0, \qquad \ell = 1, \ldots, Q. \tag{3.25}$$

The second equation in equation (3.25) implies that the vector $\boldsymbol{h}_1 = \frac{1}{\sqrt{P}}[1, \ldots, 1]^\top \in \mathbb{C}^P$ is in the kernel of $C^\dagger$. Note that the column vectors of the matrix H given in (3.3) are perpendicular to $\boldsymbol{h}_1$. We set $B = C^\dagger H \in \mathbb{C}^{Q\times(P-1)}$. Since $HH^\dagger = I_P - \boldsymbol{h}_1\boldsymbol{h}_1^\dagger$, $C^\dagger$ can be put in the form

$$C^\dagger = BH^\dagger, \qquad B \in \mathbb{C}^{Q\times(P-1)}. \tag{3.26}$$

Thus, Φ turns out to take the form

$$\Phi = \frac{1}{\sqrt{P}}A + HB^\dagger. \tag{3.27}$$

We have a further look into B. We note that the matrix H satisfies

$$A^\dagger H = 0, \qquad H^\dagger H = I_{P-1}, \tag{3.28a}$$

$$HH^\dagger = I_P - AA^\dagger. \tag{3.28b}$$

Equations (3.8*b*) and (3.27) are put together and arranged by the use of (3.28) to provide

$$B^\dagger B = \frac{1}{P}I_{P-1}, \tag{3.29a}$$

$$AB = 0. \tag{3.29b}$$

Equations (3.29) imply that the column vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{P-1}$ of B are of magnitude $1/\sqrt{P}$ and form an orthogonal system in $\mathbb{C}^Q$, and further are perpendicular to $\boldsymbol{g}_1 = \frac{1}{\sqrt{Q}}[1, \ldots, 1]^\top \in \mathbb{C}^Q$. Hence, the matrix B can be expressed as

$$B = \frac{1}{\sqrt{P}}KV, \tag{3.30}$$

where K is defined in equation (3.4) and where V is a $(Q-1)\times(P-1)$ matrix satisfying

$$V^\dagger V = I_{P-1}. \tag{3.31}$$

Consequently, the matrix Φ given in (3.27) is put in the form

$$\Phi_0 := \frac{1}{\sqrt{P}}A + \frac{1}{\sqrt{P}}HV^\dagger K^\dagger. \tag{3.32}$$

Conversely, it is easy to verify that Φ_0 given in equation (3.32) satisfies equation (3.8) on account of $\Omega H = AK = 0$, $K^\dagger K = I_{Q-1}$ and (3.31). This ends the proof of the theorem.

In conclusion of this section, we remark that the distance between A and Φ_0 is easy to calculate and satisfy

$$\arccos(A|\Phi_0) = \arccos\frac{1}{\sqrt{P}}. \tag{3.33}$$

4. Horizontal paths joining A and Φ_0

We now describe a geodesic which joins A and Φ_0 and is as long as the distance between A and Φ_0. Let

$$R_0 = \sqrt{\frac{P}{P-1}}A - \frac{1}{\sqrt{P-1}}\Phi_0. \tag{4.1}$$

Since R_0 and Φ_0 form an orthonormal two frame, the geodesic joining R_0 and Φ_0 is given by and written out as

$$\begin{aligned} C(t) &= \cos t R_0 + \sin t \Phi_0 \\ &= \cos(t-\psi)A + \frac{1}{\sqrt{P-1}}\sin(t-\psi)HV^{\dagger}K^{\dagger}, \end{aligned} \tag{4.2}$$

where

$$\sin\psi = \frac{1}{\sqrt{P}}, \qquad \cos\psi = \sqrt{\frac{P-1}{P}}. \tag{4.3}$$

This curve passes A and Φ_0 at $t=\psi$ and $t=\pi/2$, respectively. Let

$$h = [\boldsymbol{h}_1, HV_1] \in U(P), \qquad g = [\boldsymbol{g}_1, KV_2] \in U(Q), \tag{4.4}$$

where $\boldsymbol{h}_1 = \frac{1}{\sqrt{P}}[1,\ldots,1]^{\top} \in \mathbb{C}^P, \boldsymbol{g}_1 = \frac{1}{\sqrt{Q}}[1,\ldots,1]^{\top} \in \mathbb{C}^Q, V_1 \in U(P-1), V_2 \in U(Q-1)$, and where H and K are given in theorem 3.1. Then, the singular decomposition of $C(t)$ proves to take the form

$$C(t) = h[\Lambda_0(t), 0]g^{\dagger}, \tag{4.5}$$

where

$$\Lambda_0(t) = \begin{bmatrix} \cos(t-\psi) & \\ & \frac{1}{\sqrt{P-1}}\sin(t-\psi)I_{P-1} \end{bmatrix} \in \mathbb{C}^{P\times P}, \tag{4.6}$$

and where we have used the fact that $\boldsymbol{h}_1\boldsymbol{g}_1^{\dagger} = A$ and factorized $V^{\dagger}$ into $V^{\dagger} = [V_1, 0]V_2^{\dagger}$. As is easily verified, the curve $C(t)$ taking the form (4.5) is horizontal:

$$C\dot{C}^{\dagger} - \dot{C}C^{\dagger} = C^{\dagger}\dot{C} - \dot{C}^{\dagger}C = 0. \tag{4.7}$$

The length of the geodesic segment between $t=\psi$ and $t=\frac{\pi}{2}$ is $\frac{\pi}{2} - \psi = \arccos\frac{1}{\sqrt{P}}$, which is the same as the distance between A and Φ_0.

Proposition 4.1. *The length of the geodesic $C(t)$ joining A and Φ_0, which is given in (4.2), realizes the distance between A and the set of maximally entangled states.*

We here observe how the entanglement measure vary along curves between A and maximally entangled states. As for the curve $C(t)$, we obtain

$$F(C(t)) = \det(I_P - C(t)C(t)^{\dagger}) = (1-\cos^2(t-\psi))\left(1 - \frac{1}{P-1}\sin^2(t-\psi)\right)^{P-1}, \tag{4.8}$$

which takes minimum and maximum values at $t=\psi$ and $t=\pi/2$, respectively, where $C(\psi) = A$ and $C(\pi/2) = \Phi_0$.

Now we take a typical maximally entangled state

$$W = \frac{1}{\sqrt{P}}[I_P, 0] \in \mathbb{C}^{P\times Q}. \tag{4.9}$$

Note that W is the state that any maximally entangled state C is transformed by a local unitary transformation $(g,h) \in U(P)\times U(Q), gCh^{\top} = W$. We introduce a matrix R by

$$R = \sqrt{\frac{Q}{Q-1}}A - \sqrt{\frac{1}{Q-1}}W, \qquad Q \neq 1. \tag{4.10}$$

Note that W and R are orthogonal and that $(A|W) = 1/\sqrt{Q}$. Then, the geodesic joining R and W is given by

$$\Psi(t) = \cos t R + \sin t W, \tag{4.11}$$

which passes A and W at $t = \chi$ and $t = \pi/2$, respectively, where

$$\sin\chi = \frac{1}{\sqrt{Q}}, \qquad \cos\chi = \sqrt{\frac{Q-1}{Q}}. \tag{4.12}$$

In what follows, we calculate the entanglement measure $F(\Psi(t))$ along $\Psi(t)$. Note that R is written out as

$$R = \frac{1}{\sqrt{N-P}} \begin{bmatrix} 0 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ 1 & \ddots & \ddots & \vdots & \vdots & \cdots & \vdots \\ \vdots & \ddots & \ddots & 1 & \vdots & \cdots & \vdots \\ 1 & \cdots & 1 & 0 & 1 & \cdots & 1 \end{bmatrix}. \tag{4.13}$$

With the explicit expression of W and R, we carry out a straightforward calculation to obtain

$$\Psi(t)\Psi(t)^\dagger = \left(\frac{\cos^2 t}{N-P} - \frac{2\sin t\cos t}{\sqrt{P(N-P)}} + \frac{\sin^2 t}{P}\right) I_P + \left(\frac{(Q-2)\cos^2 t}{N-P} + \frac{2\sin t\cos t}{\sqrt{P(N-P)}}\right) I, \tag{4.14}$$

where I is the matrix given in (3.10). I is diagonalized by the unitary matrix $h \in U(P)$ given in (4.4),

$$h^\dagger I h = \mathrm{diag}[P, 0, \ldots, 0]. \tag{4.15}$$

On account of this, $\Psi(t)\Psi(t)^\dagger$ is written out as

$$\Psi(t)\Psi(t)^\dagger = h\,\mathrm{diag}\left[\lambda_1^2(t), \lambda_2^2(t), \ldots, \lambda_2^2(t)\right] h^\dagger, \tag{4.16}$$

where $\lambda_1^2(t)$ and $\lambda_2^2(t)$ are given by

$$\lambda_1^2(t) = \cos^2(t-\chi) + \frac{Q-P}{P(Q-1)}\sin^2(t-\chi), \tag{4.17a}$$

$$\lambda_2^2(t) = \frac{Q}{P(Q-1)}\sin^2(t-\chi), \tag{4.17b}$$

respectively, and where χ is given in (4.12). Hence, we have

$$F(\Psi(t)) = \det(I_P - \Psi(t)\Psi(t)^\dagger) = \left(1-\lambda_1^2(t)\right)\left(1-\lambda_2^2(t)\right)^{P-1}. \tag{4.18}$$

For $t = \chi$ and $t = \pi/2$, $F(\Psi(t))$ takes minimum and maximum values, respectively.

While $\Psi(t)$ is not a horizontal curve, we can bring it into a horizontal curve. Let

$$\Lambda(t) = \begin{bmatrix} \lambda_1(t) & \\ & \lambda_2(t) I_{P-1} \end{bmatrix} \in \mathbb{C}^{P\times P}, \tag{4.19}$$

where $\lambda_1(t)$ and $\lambda_2(t)$ are the non-negative functions determined by (4.17*a*) and (4.17*b*), respectively. Using this matrix, we define a curve $\Phi(t)$ to be

$$\Phi(t) = h[\Lambda(t), 0]g^\dagger, \tag{4.20}$$

where h and g are given in (4.4). The $\Phi(t)$ is written out as

$$\Phi(t) = \lambda_1(t)A + \lambda_2(t) H V^\dagger K^\dagger, \tag{4.21}$$

where $V^\dagger = [V_1, 0]V_2^\dagger$ with $0 \in \mathbb{C}^{P\times(Q-P)}$. As is easily seen, $\Phi(t)$ passes A and Φ_0 at $t = \chi$ and $t = \pi/2$, respectively, where Φ_0 is the matrix defined in (3.2). Like (4.5), the curve (4.20) is horizontal. Thus, the geodesic $\Psi(t)$ joining A and W is transformed into the horizontal curve $\Phi(t)$ joining A and Φ_0. However, the $\Phi(t)$ is not shortest among those horizontal curves joining A and Φ_0. The shortest one is $C(t)$ which we have already obtained.

Since $\Phi(t)\Phi(t)^\dagger = h\Lambda(t)^2 h^\dagger$, the entanglement measures for $\Phi(t)$ are put in the form

$$F(\Phi(t)) = \det(I_P - \Phi(t)\Phi(t)^\dagger) = \left(1-\lambda_1^2(t)\right)\left(1-\lambda_2^2(t)\right)^{P-1}, \tag{4.22}$$

which takes indeed minimum and maximum values at A and Φ_0, respectively.

5. A review of Grover's algorithms

5.1. Grover's original algorithm

We make a review of Grover's quantum search algorithm [11]. Suppose we are given initial and target states in $\mathbb{C}^N$, $|a\rangle = \frac{1}{\sqrt{N}}[1,\ldots,1]^\top$ and $|\phi\rangle$, respectively, where $\langle\phi|\phi\rangle = 1$, $\langle\phi|a\rangle \neq 0$. In Grover's search algorithm, the target state $|\phi\rangle$ is usually chosen to be one of computational basis vectors, but we have taken an arbitrary vector $|\phi\rangle$. We now define unitary operators I_a and I_ϕ to be

$$I_a := I - 2|a\rangle\langle a|, \tag{5.1a}$$

$$I_\phi := I - 2|\phi\rangle\langle\phi|, \tag{5.1b}$$

respectively, and thereby a Grover operator G to be

$$G := -I_a \circ I_\phi, \tag{5.2}$$

which generates a sequence $|a_k\rangle = G^k|a\rangle$. Defining a vector $|r\rangle$ to be

$$|r\rangle := \frac{1}{\sqrt{1-|c|^2}}|a\rangle - \frac{c}{\sqrt{1-|c|^2}}|\phi\rangle, \qquad c := \langle\phi|a\rangle, \tag{5.3}$$

one obtains an orthonormal frame $\{|r\rangle, |\phi\rangle\}$, with respect to which the Grover sequence is expressed as

$$G^k|a\rangle = \left(\cos\left(k+\tfrac{1}{2}\right)\theta\right)|r\rangle + \left(\mathrm{e}^{2\eta\mathrm{i}}\sin\left(k+\tfrac{1}{2}\right)\theta\right)|\phi\rangle, \tag{5.4}$$

where we have introduced real variables η and θ through

$$\mathrm{e}^{2\eta\mathrm{i}}\sin\frac{\theta}{2} = c, \qquad \cos\frac{\theta}{2} = \sqrt{1-|c|^2}. \tag{5.5}$$

5.2. Fixed-point algorithm

The original Grover's algorithm has a problem of optimal stopping. If the operation is not stopped, the sequence $G^k|a\rangle$ passes the target state. The fixed-point algorithm was invented to make the sequence converge monotonically to a target state [12]. We now make a review of the fixed-point algorithm with a bit of modification for our purpose. The initial and the target states are the same as in Grover's original algorithm. We define a series of unitary operators G_k by

$$G_k := R_{a_k} \circ R_\phi, \qquad k = 1, 2, \ldots, \tag{5.6}$$

where R_{a_k}, R_ϕ are the unitary operators given by

$$R_{a_k} := I - (1-\mathrm{e}^{\nu\mathrm{i}})|a_k\rangle\langle a_k|, \qquad \nu = \frac{\pi}{3}, \tag{5.7a}$$

$$R_\phi := I - (1-\mathrm{e}^{\nu\mathrm{i}})|\phi\rangle\langle\phi|, \tag{5.7b}$$

respectively. By iterative operations of G_k, we define a sequence $|a_k\rangle$ to be

$$|a_{k+1}\rangle = G_k|a_k\rangle, \qquad k = 1, 2, \ldots, \qquad |a_1\rangle = |a\rangle. \tag{5.8}$$

The sequence $|a_k\rangle$ is known to converge to the target state $|\phi\rangle$ with probability one. We now make a brief review of the proof. Let

$$c_k := \langle\phi|a_k\rangle, \qquad k = 1, 2, \ldots, \tag{5.9}$$

and introduce $0 < \epsilon_k < 1$ by

$$|c_k|^2 = 1 - \epsilon_k. \tag{5.10}$$

Then, one can show that $\epsilon_{k+1} = \epsilon_k^3$, so that

$$\epsilon_k = \epsilon_1^{3^{k-1}}, \qquad k = 1, 2, \ldots. \tag{5.11}$$

Since $|\epsilon_1| < 1$, ϵ_k tends to zero as $k \to \infty$. This and (5.10) are put together to imply that $|c_k|^2 \to 1$, which means that $|a_k\rangle$ converges to $|\phi\rangle$ within phase factors.

By using ϵ_k thus found, we can prove that

$$c_{k+1} = c_k \mathrm{e}^{\nu\mathrm{i}}(\mathrm{e}^{\nu\mathrm{i}} + \epsilon_k), \qquad \nu = \frac{\pi}{3}, \tag{5.12}$$

from which c_k turns out to be

$$c_{k+1} = \mathrm{e}^{k\nu\mathrm{i}}(\mathrm{e}^{\nu\mathrm{i}} + \epsilon_k)(\mathrm{e}^{\nu\mathrm{i}} + \epsilon_{k-1}) \cdots (\mathrm{e}^{\nu\mathrm{i}} + \epsilon_1)c_1. \tag{5.13}$$

This means that $\arg c_k$ does not converge, while we have shown that $|c_k| \to 1$.

We now write out the matrix representation of G_k. We define $|r_k\rangle$ to be

$$|r_k\rangle := \frac{1}{\sqrt{1-|c_k|^2}}|a_k\rangle - \frac{c_k}{\sqrt{1-|c_k|^2}}|\phi\rangle, \qquad k = 1, 2, \ldots. \tag{5.14}$$

Then, the matrix representation $\widetilde{G}_k^{(k)}$ of G_k with respect to $\{|r_k\rangle, |\phi\rangle\}$ proves to be

$$\widetilde{G}_k^{(k)} = \mathrm{e}^{\nu\mathrm{i}} \begin{bmatrix} 1-(1-\mathrm{e}^{-\nu\mathrm{i}})|c_k|^2 & -\bar{c}_k(1-\mathrm{e}^{\nu\mathrm{i}})\sqrt{1-|c_k|^2} \\ c_k(1-\mathrm{e}^{-\nu\mathrm{i}})\sqrt{1-|c_k|^2} & 1-(1-\mathrm{e}^{\nu\mathrm{i}})|c_k|^2 \end{bmatrix}. \tag{5.15}$$

Now, a straightforward calculation shows that

$$|r_{k+1}\rangle = \mathrm{e}^{\nu\mathrm{i}}|r_k\rangle, \qquad k = 1, 2, \ldots, \tag{5.16}$$

which gives rise to the transformation between frames $\{|r_{k+1}\rangle, |\phi\rangle\}$ and $\{|r_k\rangle, |\phi\rangle\}$. Then, we obtain

Proposition 5.1. *The kth unitary operator G_k in the fixed-point algorithm is represented, with respect to the frame $\{|r_1\rangle, |\phi\rangle\}$, as*

$$\widetilde{G}_k = \mathrm{e}^{\nu\mathrm{i}} \begin{bmatrix} 1-(1-\mathrm{e}^{-\nu\mathrm{i}})|c_k|^2 & -\bar{c}_k(1-\mathrm{e}^{\nu\mathrm{i}})\,\mathrm{e}^{(k-1)\nu\mathrm{i}}\sqrt{1-|c_k|^2} \\ c_k(1-\mathrm{e}^{-\nu\mathrm{i}})\,\mathrm{e}^{-(k-1)\nu\mathrm{i}}\sqrt{1-|c_k|^2} & 1-(1-\mathrm{e}^{\nu\mathrm{i}})|c_k|^2 \end{bmatrix}. \tag{5.17}$$

From (5.14) and (5.16), we can put the sequence $|a_k\rangle$ in the explicit form

$$|a_k\rangle = \sqrt{1-|c_k|^2}|r_k\rangle + c_k|\phi\rangle = \epsilon_k^{1/2}\,\mathrm{e}^{(k-1)\nu\mathrm{i}}|r_1\rangle + c_k|\phi\rangle, \tag{5.18}$$

where ϵ_k and c_k are given in (5.11) and (5.13), respectively.

6. Entanglement measurement

We look into how change occurs in the values of the entanglement measure along the sequences generated by Grover's original and the fixed-point algorithms. Let us be reminded of the fact that the basis vector $|r\rangle$ in Grover's original algorithm is the same as $|r_1\rangle$ in the fixed-point algorithm. Further, both algorithms share the same initial and target states. We can then deal with the sequences generated by respective algorithms in parallel. Further, we may introduce the same notation $|a_k\rangle$ for both the sequences. In fact, the sequences generated by Grover's original algorithm and by the fixed-point algorithm are expressed as

$$|a_k\rangle = G|a_{k-1}\rangle = \cdots = G^{k-1}|a_1\rangle, \tag{6.1}$$

$$|a_k\rangle = G_{k-1}|a_{k-1}\rangle = \cdots = G_{k-1}G_{k-2}\cdots G_1|a_1\rangle, \tag{6.2}$$

respectively.

On account of the isomorphism $\mathcal{H}^{\otimes n} \cong \mathbb{C}^{P\times Q}$, we carry the sequences $|a_k\rangle$ in $\mathcal{H}^{\otimes n}$ to those A_k in $\mathbb{C}^{P\times Q}$ to evaluate the entanglement measure $\det\left(I_P - A_k A_k^\dagger\right)$. In the quantum search algorithm, the target state is usually chosen to be one of computational basis vectors, a separable state. Take the target state $|t\rangle$ as $|t\rangle = [0,\ldots,0,1]^\top$. We denote the matrices corresponding to $|a\rangle$, $|t\rangle$ and $|r\rangle$ by A, T and R, respectively. Then, we have

$$A = \frac{1}{\sqrt{N}}\begin{bmatrix} 1 & \cdots & 1 & 1 & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 1 & \cdots & 1 & 1 & \cdots & 1 \\ 1 & \cdots & 1 & 1 & \cdots & 1 \end{bmatrix}, \qquad T = \begin{bmatrix} 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, \tag{6.3}$$

and

$$R = \frac{1}{\sqrt{N-1}}\begin{bmatrix} 1 & \cdots & 1 & 1 & \cdots & 1 & 1 \\ \vdots & \ddots & \vdots & \vdots & & \vdots & \vdots \\ 1 & \cdots & 1 & 1 & \cdots & 1 & 1 \\ 1 & \cdots & 1 & 1 & \cdots & 1 & 0 \end{bmatrix}, \tag{6.4}$$

where we have used (5.3) with $|\phi\rangle = |t\rangle$ and $c = (A|T) = \frac{1}{\sqrt{N}}$.

We denote the matrices corresponding to $|a_k\rangle$ by A_k and put them in the form

$$A_k = \alpha_k R + \beta_k T, \qquad \alpha_k, \beta_k \in \mathbb{C}. \tag{6.5}$$

After calculating $RR^\dagger$, $TR^\dagger$, $RT^\dagger$ and $TT^\dagger$ in the matrix form, $A_k A_k^\dagger$ proves to take the form

$$A_k A_k^\dagger = \begin{bmatrix} a_k & \cdots & a_k & b_k \\ \vdots & \ddots & \vdots & \vdots \\ a_k & \cdots & a_k & b_k \\ \bar{b}_k & \cdots & \bar{b}_k & d_k \end{bmatrix}, \tag{6.6}$$

where

$$a_k = \frac{Q}{N-1}|\alpha_k|^2, \qquad b_k = \frac{Q-1}{N-1}|\alpha_k|^2 + \frac{1}{\sqrt{N-1}}\alpha_k\bar{\beta}_k, \qquad d_k = \frac{Q-1}{N-1}|\alpha_k|^2 + |\beta_k|^2. \tag{6.7}$$

The characteristic polynomial of $A_k A_k^\dagger$ turns out to be given by

$$\det\left(\lambda I_P - A_k A_k^\dagger\right) = \lambda^{P-1}[\lambda^2 - \lambda + (P-1)(a_k d_k - |b_k|^2)], \tag{6.8}$$

and the eigenvalues are expressed, in terms of a_k, b_k, d_k given in (6.7), as

$$\begin{aligned}\lambda_1 &= \tfrac{1}{2}\bigl(1+\sqrt{1-4(P-1)(a_kd_k-|b_k|^2)}\bigr),\\ \lambda_2 &= \tfrac{1}{2}\bigl(1-\sqrt{1-4(P-1)(a_kd_k-|b_k|^2)}\bigr),\\ \lambda_3 &= 0((P-2)\text{-multiple}).\end{aligned} \tag{6.9}$$

The measure of entanglement $F(A_k)$ along the sequence is then expressed as

$$F(A_k) = \det\bigl(I_P - A_kA_k^\dagger\bigr) = (P-1)(a_kd_k-|b_k|^2). \tag{6.10}$$

For the sequence A_k generated by Grover's original algorithm, we have, from (5.4),

$$\alpha_k = \cos\bigl(k-\tfrac{1}{2}\bigr)\theta, \qquad \beta_k = \sin\bigl(k-\tfrac{1}{2}\bigr)\theta, \tag{6.11}$$

where

$$\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}}. \tag{6.12}$$

For the sequence A_k generated by the fixed-point algorithm, equation (5.18) provides

$$\alpha_k = \mathrm{e}^{(k-1)\nu\mathrm{i}}\sqrt{\epsilon_1^{3^{k-1}}}, \qquad \beta_k = c_k, \tag{6.13}$$

where c_k is given in (5.13) along with

$$\epsilon_1 = 1-\frac{1}{N}, \qquad c_1 = \frac{1}{\sqrt{N}}. \tag{6.14}$$

Substitution of (6.11) and (6.13) into (6.7) results in the explicit expression of a_k and b_k, the entries of $A_kA_k\dagger$, in the cases of original Grover's algorithm and of the fixed-point algorithm, respectively. Hence, in turn, one obtains the explicit expression of the eigenvalues (6.9) and of the entanglement measure (6.10) in respective cases.

Figure 1 provides the graphs of eigenvalues (6.9) and of entanglement measure (6.10) against the number of queries $q_k = \frac{1}{2}(3^k-1)$, where $P = 2^{10}$, $Q = 2^{20}$, $N = 2^{30}$.

We observe expectedly that as the difference between eigenvalues gets larger, the value of entanglement measure becomes smaller. The entanglement measure suggests that the sequence generated by the fixed-point algorithm converges to the target monotonically, if the number of iterations is large enough. In contrast with this, the sequence generated by Grover's original algorithm oscillates. The fact that $\det\bigl(I - A_kA_k^\dagger\bigr) \neq 0$ shows that the passing states are entangled, while the initial and the target states are separable. Another measure was proposed in [6], in which a figure similar to figure 1(*a*) was given.

7. A split Grover algorithm

As was observed in the previous section, the initial and the target states are separable, but the sequences generated by both of the Grover algorithms are entangled. We wish to find an algorithm which generates a sequence of separable states approaching the target separable state. We first note that the initial and the target states are expressed, respectively, as

$$A = \boldsymbol{a}_P\boldsymbol{a}_Q^\dagger, \qquad \boldsymbol{a}_P = \frac{1}{\sqrt{P}}[1,\ldots,1]^\top \in \mathbb{C}^P, \qquad \boldsymbol{a}_Q = \frac{1}{\sqrt{Q}}[1,\ldots,1]^\top \in \mathbb{C}^Q, \tag{7.1}$$

$$T = \boldsymbol{e}_P\boldsymbol{e}_Q^\dagger, \qquad \boldsymbol{e}_P = [0,\ldots,0,1]^\top \in \mathbb{C}^P, \qquad \boldsymbol{e}_Q = [0,\ldots,0,1]^\top \in \mathbb{C}^Q. \tag{7.2}$$

According to the Grover algorithm, as was done in section 5, we define sequences $\boldsymbol{a}_k \in \mathbb{C}^P$ and $\boldsymbol{b}_k \in \mathbb{C}^Q$ with initial states $\boldsymbol{a}_1 = \boldsymbol{a}_P$ and $\boldsymbol{b}_1 = \boldsymbol{a}_Q$ by setting $\boldsymbol{a}_k = U_{k-1}^{(P)}\boldsymbol{a}_P$ and $\boldsymbol{b}_k = U_{k-1}^{(Q)}\boldsymbol{a}_Q$,

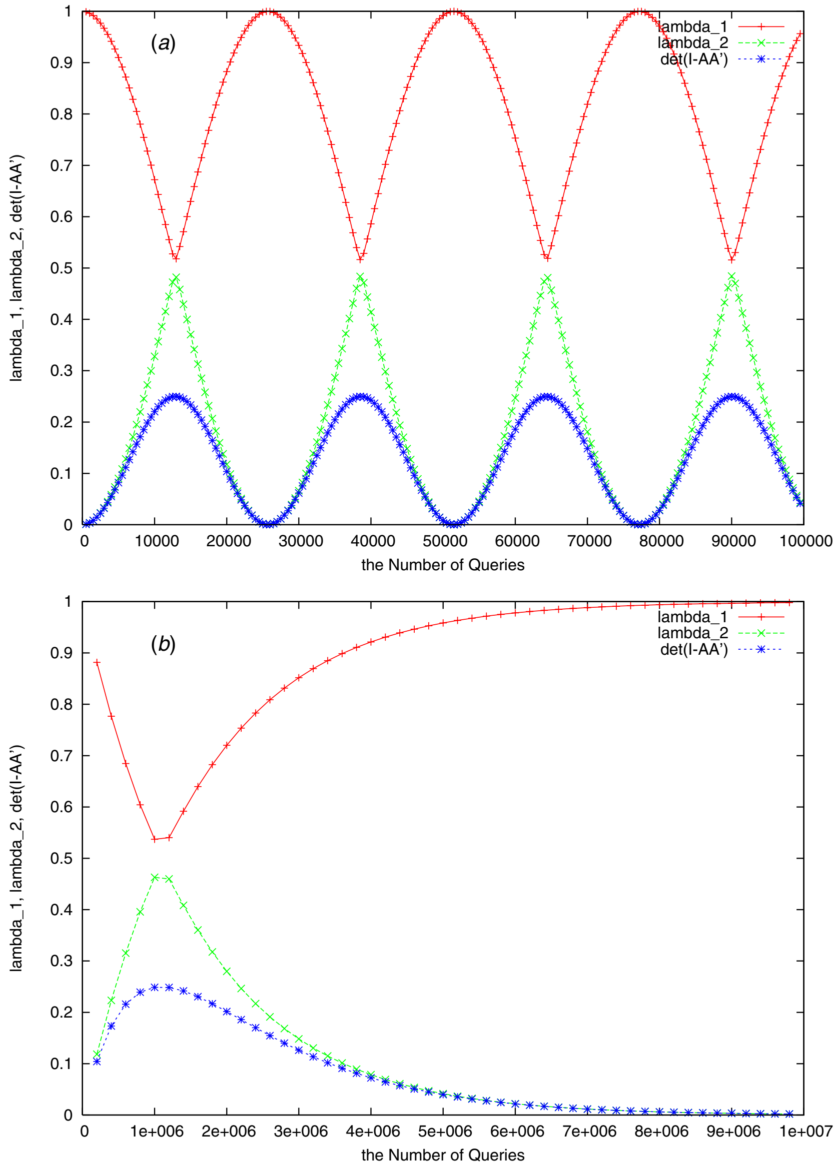

Figure 1. Eigenvalues and the measure of entanglement along the sequence approaching a separable state with $P = 2^{10}$, $Q = 2^{20}$ and $N = 2^{30}$.

(This figure is in colour only in the electronic version)

where $U_{k-1} = G_{k-1} \cdots G_1$ or $U_{k-1} = G^{k-1}$ according to whether the fixed point algorithm or the original algorithm is concerned, and where the superscript (P) or (Q) is attached to U_{k-1} according to whether the algorithm is performed in $\mathbb{C}^P$ or in $\mathbb{C}^Q$. In the fixed-point algorithm, the sequences $\boldsymbol{a}_k$ and $\boldsymbol{b}_k$ converge to the respective target states, $\boldsymbol{e}_P$ and $\boldsymbol{e}_Q$, within phase factors. Then, the sequence of matrices

$$A_k = \boldsymbol{a}_k \boldsymbol{b}_k^\dagger \in \mathbb{C}^{P\times Q} \tag{7.3}$$

converge to the target state T within phase factors. Since the A_k are of rank one and invariant under the $U(1)$ action, $(\boldsymbol{a}_k, \boldsymbol{b}_k) \mapsto (\mathrm{e}^{\mathrm{i}\theta}\boldsymbol{a}_k, \mathrm{e}^{\mathrm{i}\theta}\boldsymbol{b}_k)$, on $S^{2P-1} \times S^{2Q-1}$, the sequence (7.3) moves in the set, $S^{2P-1} \times_{U(1)} S^{2Q-1}$, of separable states. We call the algorithm that generates the sequence A_k a split Grover algorithm.

In conclusion of this section, we compute the distance between A and T with respect to a naturally defined Riemannian metric on $S^{2P-1} \times_{U(1)} S^{2Q-1}$. The product space $S^{2P-1} \times S^{2Q-1}$ has a natural Riemannian metric, which we denote by $\mathrm{d}s_P^2 + \mathrm{d}s_Q^2$, where $\mathrm{d}s_P^2$ and $\mathrm{d}s_Q^2$ denote the canonical metrics on S^{2P-1} and S^{2Q-1}, respectively. The metric projects to a metric on $S^{2P-1} \times_{U(1)} S^{2Q-1}$, as it is invariant under the $U(1)$ action; $(\boldsymbol{u}, \boldsymbol{v}) \mapsto (\mathrm{e}^{\mathrm{i}\theta}\boldsymbol{u}, \mathrm{e}^{\mathrm{i}\theta}\boldsymbol{v})$. Let $\boldsymbol{r}_P \in \mathbb{C}^P$ and $\boldsymbol{r}_Q \in \mathbb{C}^Q$ be

$$\boldsymbol{r}_P = \sqrt{\frac{P}{P-1}}\boldsymbol{a}_P - \frac{1}{\sqrt{P-1}}\boldsymbol{e}_P, \tag{7.4}$$

$$\boldsymbol{r}_Q = \sqrt{\frac{Q}{Q-1}}\boldsymbol{a}_Q - \frac{1}{\sqrt{Q-1}}\boldsymbol{e}_Q, \tag{7.5}$$

respectively. Then, the geodesics joining $\boldsymbol{r}_P$ and $\boldsymbol{e}_P$ and joining $\boldsymbol{r}_Q$ and $\boldsymbol{e}_Q$ are given, respectively, by

$$\boldsymbol{c}_P(t_P) = \cos t_P \boldsymbol{r}_P + \sin t_P \boldsymbol{e}_P, \tag{7.6}$$

$$\boldsymbol{c}_Q(t_Q) = \cos t_Q \boldsymbol{r}_Q + \sin t_Q \boldsymbol{e}_Q. \tag{7.7}$$

The curve $(\boldsymbol{c}_P(t_P), \boldsymbol{c}_Q(t_Q))$ becomes a geodesic in $S^{2P-1} \times S^{2Q-1}$, if the parameters t_P and t_Q are adjusted. We take t_P and t_Q as functions of another parameter τ

$$t_P(\tau) = \frac{1}{L}\left(\frac{\pi}{2} - \theta_P\right)\tau + \theta_P, \qquad t_Q(\tau) = \frac{1}{L}\left(\frac{\pi}{2} - \theta_Q\right)\tau + \theta_Q, \tag{7.8}$$

where θ_P and θ_Q are defined through $\sin\theta_P = \frac{1}{\sqrt{P}}$ and $\sin\theta_P = \frac{1}{\sqrt{Q}}$, respectively, and where L is a positive real number. Then, the curve segment $(\boldsymbol{c}_P(t_P), \boldsymbol{c}_Q(t_Q))$ starting with $(\boldsymbol{a}_P, \boldsymbol{a}_Q)$ at $\tau = 0$ and ending with $(\boldsymbol{e}_P, \boldsymbol{e}_Q)$ at $\tau = L$ has the length, with respect to the metric $\mathrm{d}s_P^2 + \mathrm{d}s_Q^2$, given by

$$\int_0^L \sqrt{\left|\frac{\mathrm{d}\boldsymbol{c}_P}{\mathrm{d}\tau}\right|^2 + \left|\frac{\mathrm{d}\boldsymbol{c}_Q}{\mathrm{d}\tau}\right|^2}\,\mathrm{d}\tau = \sqrt{\left(\frac{\pi}{2} - \theta_P\right)^2 + \left(\frac{\pi}{2} - \theta_Q\right)^2}. \tag{7.9}$$

We here note that the curve $(\boldsymbol{c}_P(t_P), \boldsymbol{c}_Q(t_Q))$ is horizontal in the sense that the tangent vector $\left(\frac{\mathrm{d}\boldsymbol{c}_P(t_P)}{\mathrm{d}\tau}, \frac{\mathrm{d}\boldsymbol{c}_Q(t_Q)}{\mathrm{d}\tau}\right)$ to the curve is orthogonal to the vertical vector $(\mathrm{i}\boldsymbol{c}_P(t_P), \mathrm{i}\boldsymbol{c}_Q(t_Q))$, a tangent vector to the $U(1)$ orbit through $(\boldsymbol{c}_P(t_P), \boldsymbol{c}_Q(t_Q))$, with respect to the Riemannian metric on $S^{2P-1} \times S^{2Q-1}$. Hence, the length (7.9) provides the distance between $A = \boldsymbol{a}_P\boldsymbol{a}_P^\dagger$ and $T = \boldsymbol{e}_P\boldsymbol{e}_P^\dagger$ with respect to the metric on $S^{2P-1} \times_{U(1)} S^{2Q-1}$.

8. Concluding remarks

The distance between A and T is given by $d(A, T) = \arccos\frac{1}{\sqrt{N}}$, which is larger than the distance $d(A, W) = \arccos\frac{1}{\sqrt{Q}}$ between A and W, and than the distance $d(A, \Phi_0) = \arccos\frac{1}{\sqrt{P}}$ between A and Φ_0. Put another way, the separable state T is much more distant than the maximally entangled states W and Φ_0. With respect to the Riemannian metric on the set of separable states, the distance $d_S(A, T)$ between A and T, which is given by (7.9), is still larger than or equal to $d(A, W)$ and $d(A, \Phi_0)$. From the viewpoint of Riemannian geometry of the state space, this fact sounds strange. However, from the viewpoint of quantum mechanics, the separable states would be easily accessible from the initial state A by means of local unitary transformations by $U(P) \times U(Q)$. This is because the group $U(P) \times U(Q)$ of smaller size is easier to treat than the group $U(N)$ of full size. Hence, the above fact would be acceptable.

The split Grover algorithm can be extended to be applicable in multipartite partitions. In fact, each sequence generated by the Grover algorithm in each party is combined to form a sequence in the total space.

A number of entanglement measures with respect to multi-partite partitions have been proposed, some of which are, for example, the n-concurrence [7], polynomial invariants [8], the Schmidt measure [9], the Q measure [6] and hyperdeterminants [10]. However, as long as bipartite partition is concerned, our measure is in keeping with geometric study of entanglement.

In conclusion, we make a comment on an extension of the entanglement measure. Though we have considered only one bipartite partition, we may take several bipartite partitions into account. Let $|\phi\rangle = \sum c_{i_1\cdots i_n}|i_1\cdots i_n\rangle$, and let integers p and q be fixed with $p+q=n$ and $p \leqslant q$. Denote by $K = (k_1, k_2, \ldots, k_p)$ the loci of p qubits in $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ with $k_1 < k_2 < \cdots < k_p$. Let $J = j_1 j_2 \cdots j_p$ be a binary integer formed from coefficient's indices with respect to K, and $L = \ell_1 \ell_2 \cdots \ell_q$ a binary integer formed from coefficient's indices with respect to the loci other than K, where $j_a, \ell_b \in \{0, 1\}, a = 1, \ldots, p$, and $b = 1, \ldots, q$. Then, the coefficients of the state $|\phi\rangle$ are mapped to a matrix $C^{(K)} \in \mathbb{C}^{P\times Q}$,

$$(c_{i_1 i_2\cdots i_n}) \mapsto C^{(K)} = \left(C^{(K)}_{JL}\right) \in \mathbb{C}^{P\times Q}. \tag{8.1}$$

The p-particle density matrix is then written as

$$\rho_K = C^{(K)} C^{(K)\dagger}. \tag{8.2}$$

We may define an entanglement measure to be

$$\prod_K \det(I_P - \rho_K), \tag{8.3}$$

where K ranges over all bipartite partitions with p fixed. If (8.3) vanishes for $|\phi\rangle$, there exists a bipartite partition with respect to which $|\phi\rangle$ is separable. It is to be noted that this measure is invariant under the local unitary transformation $U(2) \times U(2) \times \cdots \times U(2)$. In particular, for a three-qubit, one has $(p, q) = (1, 2)$, and (8.3) reduces to $\det \rho_A \det \rho_B \det \rho_C$, where A, B and C are symbols attached to respective particles. For the GHZ state $|\phi\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |111\rangle)$, one has $\rho_A = \rho_B = \rho_C = \frac{1}{2} I_2$, so that $\det \rho_A \det \rho_B \det \rho_C = (1/4)^3$, which means that the GHZ state is maximally entangled with respect to any bipartite partition. If we wish, we may vary p and q under the condition $p + q = n$, $p \leqslant q$, and extend the measure (8.3) to

$$\prod_{p=1}^{[n/2]} \prod_{K(p)} \det(I - \rho_{K(p)}), \tag{8.4}$$

where $[n/2]$ denotes the integer part of $n/2$.

References

[1] Iwai T 2007 *J. Phys. A: Math. Theor.* **40** 1361
[2] Iwai T 2007 *J. Phys. A: Math. Theor.* **40** 12161

[3] Witte C and Trucks M 1999 *Phys. Lett.* A **257** 14
[4] Ozawa M 2000 *Phys. Lett.* A **268** 158
[5] Bertlmann R A, Narnhofer H and Thirring W 2002 *Phys. Rev.* A **66** 032319
[6] Meyer D A and Wallach N R 2002 *J. Math. Phys.* **43** 4273
[7] Bullock S S and Brennen G K 2004 *J. Math. Phys.* **45** 2447
[8] Barnum H and Linden N 2001 *J. Phys. A: Math. Gen.* **34** 6787
[9] Eisert J and Briegel H J 2001 *Phys. Rev.* A **64** 022306
[10] Miyake A and Wadati M 2002 *Quantum Inf. Comput.* **2** 540
[11] Grover Lov K 1997 *Phys. Rev. Lett.* **79** 325
[12] Grover Lov K 2005 *Phys. Rev. Lett.* **95** 150501