Geometric strategy for the optimal quantum search

Akimasa Miyake* and Miki Wadati†
Department of Physics, Graduate School of Science, University of Tokyo, Hongo 7-3-1, Bunkyo-ku, Tokyo 113-0033, Japan
(Received 4 April 2001; published 18 September 2001)

We explore quantum search from the geometric viewpoint of a complex projective space $\mathbb{CP}$, a space of rays. First, we show that the optimal quantum search can be geometrically identified with the shortest path along the geodesic joining a target state, an element of the computational basis, and such an initial state as overlaps equally, up to phases, with all the elements of the computational basis. Second, we calculate the entanglement through the algorithm for any number of qubits n as the minimum Fubini-Study distance to the submanifold formed by separable states in Segre embedding, and find that entanglement is used almost maximally for large n. The computational time seems to be optimized by the dynamics as the geodesic, running across entangled states away from the submanifold of separable states, rather than the amount of entanglement itself.

DOI: 10.1103/PhysRevA.64.042317 PACS number(s): 03.67.Lx, 03.65.−w, 89.70.+c

I. INTRODUCTION

Quantum computers would be more powerful than their classical counterparts [1,2]. Suppose an oracle function $f(x)$ with $x \in \{0,1\}^n$ is given such that $f(w)=1$ for an unknown single item w out of N ($:=2^n$) and $f(x)=0$ for $x \neq w$. Our purpose is to find the ''target'' w with the smallest possible number of the oracle evaluations, called the query complexity. As is often the case with computer science, the worst case of query complexity is concerned here. If we try with a classical computer, it is readily found that we need N queries in the worst case. On the other hand, we can obtain w with a success probability almost 1 in only $O(\sqrt{N})$ queries, regardless of w (i.e., for evaluation in not only the worst case but also the average case), by Grover's quantum search algorithm [3,4]. Furthermore, Zalka [5] proved that Grover's algorithm is exactly, and not only asymptotically, optimal for query complexity if quantum computation consists only of unitary transformations and the final measurement.

Grover's algorithm in the n-qubit case ($2^n=N$ states) is constructed as follows. We first introduce an initial ''average'' state $|a\rangle := (1/\sqrt{N})\Sigma_{x=0}^{N-1}|x\rangle$ where $|x\rangle$ ($x=0,\ldots,N-1$) forms the orthonormal computational basis. Writing the overlap between the average $|a\rangle$ and the target $|w\rangle$ by θ as

$$\sin\frac{\theta}{2} := \langle w|a\rangle = \frac{1}{\sqrt{N}}, \tag{1}$$

we have Grover's algorithm:

$$|a\rangle = \begin{bmatrix} \cos\dfrac{\theta}{2}|r\rangle \\ \sin\dfrac{\theta}{2}|w\rangle \end{bmatrix}, \tag{2}$$

$$G := -I_a I_w := -(\mathbf{1}-2|a\rangle\langle a|)(\mathbf{1}-2|w\rangle\langle w|) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \tag{3}$$

$$|\psi(k)\rangle := G^k|a\rangle = \begin{bmatrix} \cos\left(k+\dfrac{1}{2}\right)\theta|r\rangle \\ \sin\left(k+\dfrac{1}{2}\right)\theta|w\rangle \end{bmatrix}, \tag{4}$$

in the orthonormal basis of $|r\rangle$ ($:=[1/\sqrt{N-1}]\Sigma_{x\neq w}|x\rangle$) and $|w\rangle$, where $\mathbf{1}$ denotes the $2n\times 2n$ identity matrix. Note that as constructed from alternate inversions for the average $|a\rangle$ and the target $|w\rangle$ (i.e., I_a and I_w), the kernel G in Eq. (3) becomes a real two-dimensional rotation. We find in Eq. (4) that the target $|w\rangle$ is obtained with a success probability of 1 when $(k+\frac{1}{2})\theta=\pi/2$, i.e., $k\sim(\pi/4)\sqrt{N}$ by Eq. (1) in the case of $N\gg 1$. Because one query is used for every I_w [i.e., $I_w|x\rangle=(-1)^{f(x)}|x\rangle$] of G in Eq. (3), we can identify the query complexity with $k\sim O(\sqrt{N})$.

Our motivation is based on the two points below. First, while it is quite straightforward to verify Grover's algorithm [3,4] and Zalka's algebraic proof of its optimality [5], it has yet to be understood from the geometric aspects why Grover's algorithm works efficiently. Second, although it is often said that entanglement is useful to enhance quantum information processing, this remains obscure in theory [8] as well as in nuclear magnetic resonance (NMR) experiments [9], after, in particular, Lloyd's proposition of ''quantum search without entanglement'' [10,11]. Thus, in this paper, we characterize quantum search from the geometric viewpoint, which might shed light on the general strategy for constructing efficient quantum algorithms, and discuss how entanglement gives quantum computation its power.

The rest of the paper is organized as follows. In Sec. II, after we briefly review geometric aspects of quantum mechanics such as the complex projective space $\mathbb{CP}$ and the Fubini-Study metric on it, we show that Grover's algorithm corresponds to a geodesic of $\mathbb{CP}$. In Sec. III we discuss entanglement, which can be considered as the minimum Fubini-Study distance to the submanifold formed by sepa-

*Email address: miyake@monet.phys.s.u-tokyo.ac.jp
†Email address: wadati@phys.s.u-tokyo.ac.jp

rable states in $\mathbb{CP}$. Entanglement in Grover's algorithm is calculated for the general n-qubit case, and is found to be used almost maximally when n is large. In Sec. IV, we construct optimal quantum searches, including Grover's algorithm, by means of geodesics, and derive the geometric necessary and sufficient condition for the optimal quantum search. Finally, Sec. V is devoted to conclusions.

II. GEOMETRIC ASPECTS OF QUANTUM MECHANICS

In this section, we first consider, as a preliminary, the pure state space of a quantum mechanical system as a complex projective space $\mathbb{CP}$, a space of rays in the associated Hilbert space $\mathcal{H}$ [12–18]. Because we discuss the geometric characteristics of the efficient quantum algorithm itself, we can safely restrict our attention to the pure states. This implies that we never treat general mixed states (whole states given by the density matrix) which appear in some realistic situations. After that, we show that Grover's algorithm is the horizontal lift of a geodesic in $\mathbb{CP}$.

A. Ray and complex projective Hilbert space $\mathbb{CP}$

Let $|\psi\rangle$ be a (not necessarily normalized) vector in a complex N-dimensional Hilbert space $\mathcal{H}(\mathbb{C}^N)$. The physical state of the quantum system in $\mathcal{H}(\mathbb{C}^N)$ is given by a ray, an equivalence class of vectors up to the overall normalization and phase. So the ray can be interpreted as a line in $\mathbb{C}^N$ passing through the origin. Note that universal quantum computation [6,7] is defined over rays. A set of rays forms the complex projective Hilbert space $\mathbb{CP}^{N-1}$ with the associated projection map Π,

$$\Pi: \quad \mathcal{H}(\mathbb{C}^N)\to\mathbb{CP}^{N-1},$$

$$|\psi\rangle\mapsto\{|\psi'\rangle \text{ such that } |\psi'\rangle=c|\psi\rangle, \ c\in\mathbb{C}-\{0\}\}. \quad (5)$$

Suppose $|\psi\rangle$ is given by N-tuples of complex amplitudes z_j $(j=0,\ldots,N-1)\in\mathbb{C}^N-\{0\}$ by choosing a basis in $\mathcal{H}$. According to Eq. (5), the ray $\Pi(|\psi\rangle)$ is represented as

$$\Pi(|\psi\rangle)=(z_0',z_1',\ldots,z_{N-1}'), \quad (6)$$

such that $z_j'=cz_j$ for all j with $c\in\mathbb{C}-\{0\}$. We find, however, that this representation (6), called the homogeneous coordinate representation in algebraic geometry, is not unique. To obtain a unique one, we also utilize, for any nonzero z_j (say z_0),

$$\zeta_l:=\frac{z_l'}{z_0'}=\frac{z_l}{z_0} \qquad (l=1,\ldots,N-1), \quad (7)$$

called the inhomogeneous coordinates.

B. Fubini-study metric and geodesics in $\mathbb{CP}$

Now we introduce the Fubini-Study metric, a natural Riemannian metric in $\mathbb{CP}^{N-1}$. Let $|\psi(s)\rangle$ be a normalized vector drawing a curve $\mathcal{C}$ in $\mathcal{H}$ and $|d\psi(s)\rangle$ the tangent vector along $\mathcal{C}$. Note that the normalization $\langle\psi(s)|\psi(s)\rangle\equiv 1$ implies $\mathrm{Re}\langle\psi(s)|d\psi(s)\rangle=0$. Under a global gauge transformation $|\psi\rangle\mapsto e^{i\gamma}|\psi\rangle$ with $\gamma\in\mathbb{R}$, the projection, orthogonal to the Hopf fibers, of $|d\psi(s)\rangle$,

$$|d\psi(s)_\perp\rangle:=|d\psi(s)\rangle-\langle\psi(s)|d\psi(s)\rangle|\psi(s)\rangle, \quad (8)$$

is gauge covariant (i.e., $|d\psi_\perp\rangle\mapsto e^{i\gamma}|d\psi_\perp\rangle$). Since $\langle d\psi(s)_\perp|d\psi(s)_\perp\rangle$ is gauge invariant, it can be used to define the metric in $\mathbb{CP}^{N-1}$, called the Fubini-Study metric, between two nearby rays $\Pi(|\psi(s)\rangle)$ and $\Pi(|\psi(s+ds)\rangle)$ as

$$\frac{1}{4}ds^2:=\langle d\psi(s)_\perp|d\psi(s)_\perp\rangle$$
$$=\langle d\psi(s)|d\psi(s)\rangle-[\mathrm{Im}\langle\psi(s)|d\psi(s)\rangle]^2. \quad (9)$$

By variation of the action $\int_{s_1}^{s_2}ds$ of the line element in Eq. (9), each extremal gives a geodesic $\mathcal{C}'$, which is found to be an arc of the great circle lying on some submanifold $\mathbb{CP}^1$ in $\mathbb{CP}^{N-1}$ [13,14]. Any lift of the geodesic $\mathcal{C}'$ becomes, by definition, a geodesic in $\mathcal{H}$. In particular, a horizontal lift of $\mathcal{C}'$, which implies the parallel transport $\mathrm{Im}\langle\psi(s)|d\psi(s)\rangle=0$, can be described simply as

$$|\psi(s)\rangle=\cos\frac{s}{2}|\psi_1\rangle+\sin\frac{s}{2}|\psi_2\rangle, \quad (10)$$

in terms of some orthonormal basis $|\psi_1\rangle,|\psi_2\rangle$ in $\mathcal{H}$. Thus the horizontal geodesic (10) is just a real two-dimensional rotation on the plane spanned by $|\psi_1\rangle$ and $|\psi_2\rangle$ in $\mathcal{H}$. Furthermore, according to Eq. (10), we can interpret the transition probability P as the distance $s(\in[0,\pi])$ along the geodesic joining $|\psi_1\rangle$ and $|\psi(s)\rangle$ [13–16]; i.e.,

$$P(|\psi(s)\rangle,|\psi_1\rangle):=|\langle\psi(s)|\psi_1\rangle|^2=\cos^2\frac{s}{2}. \quad (11)$$

We also find that the geodesic represents possible superpositions between $|\psi_1\rangle$ and $|\psi_2\rangle$.

C. Grover's algorithm as a geodesic

If we take $|\psi_1\rangle=|r\rangle,|\psi_2\rangle=|w\rangle$, and $s=2(k+\frac{1}{2})\theta$ in Eq. (10), we readily find that Grover's dynamics (4) satisfies the equation of a geodesic in Eq. (10), and in addition evolves along the shorter arc of the geodesic. This suggests that Grover's dynamics corresponds to the *shortest* path from the geometric viewpoint.

It is significant to note that the original Grover's algorithm evolves with discrete k, in other words, it skips along the geodesic. The interval of skip becomes shorter as N becomes larger, and it is almost continuous when N is sufficiently large. Here we can regard G in Eq. (3) as a one-step time evolution, because we are concerned with the computational complexity only in terms of the number of queries called. This might be called ''coarse graining,'' where the dynamics driven by the detailed physical operations is reduced to the effective dynamics (i.e., algorithm) of the query complexity.

III. ENTANGLEMENT IN GROVER'S ALGORITHM

In this section, we explore the geometry of $\mathbb{CP}$ in more detail to consider relationships between Grover's algorithm and entanglement. As mentioned in Sec. I, it is very interesting whether Grover's algorithm (and general quantum algorithms) takes advantage of entanglement to compute faster. It was shown in [8] that Grover's algorithm both in the ideal pure state case and in the pseudopure states in NMR does generate entanglement during the computation, by formally tracing out all but one qubit. Here we show from the geometric viewpoint that entanglement is used and calculate it explicitly.

A. Segre embedding and quadric of separable states

Some of the mysterious features of quantum mechanics, e.g., entanglement and so on, appear when we consider a composite system. In the bipartite case, by combining two systems with Hilbert space $\mathcal{H}(\mathbb{C}^m)$ and $\mathcal{H}(\mathbb{C}^{m'})$, the combined Hilbert space is taken as the tensor product $\mathcal{H}(\mathbb{C}^m)\otimes\mathcal{H}(\mathbb{C}^{m'})$ and the associated space of states is $\mathbb{CP}^{mm'-1}$, which has a much larger dimension than that of the mere Cartesian product $\mathbb{CP}^{m-1}\times\mathbb{CP}^{m'-1}$ (its dimension is only $m+m'-2$) of the two individual spaces of states. Thus the mystery seems to lie in the $(m-1)(m'-1)$ relative phases. Here we consider Segre embedding [15–17] in algebraic geometry, which enables products of projective spaces to be embedded into a projective space again. Then using the Segre embedding we may characterize entanglement geometrically.

We first illustrate the idea in the two-qubit case. (Segre embedding in the general case is given in Appendix A.) A state of a qubit is represented by the homogeneous coordinates $(z_0,z_1)\in\mathbb{CP}^1$. In particular, the spin-up and spin-down basis states $|0\rangle$ and $|1\rangle$ correspond to

$$|0\rangle\leftrightarrow(1,0),\quad |1\rangle\leftrightarrow(0,1), \tag{12}$$

respectively [precisely speaking, $\Pi(|0\rangle)=(1,0)$ and $\Pi(|1\rangle)=(0,1)$]. Then an arbitrary state (z_0,z_1) is a point on the complex projective line joining $\Pi(|0\rangle)$ and $\Pi(|1\rangle)$, interpreted as a superposition of $|0\rangle$ and $|1\rangle$ with the amplitudes proportional to z_0 and z_1, respectively, as seen in Sec. II.

We consider a mapping f (Segre embedding)

$$f:\quad \mathbb{CP}^1\times\mathbb{CP}^1\to\mathbb{CP}^3$$

$$((a_0,a_1),(b_0,b_1))\mapsto(a_0b_0,a_0b_1,a_1b_0,a_1b_1). \tag{13}$$

Note that although $(a_0,a_1)=(\alpha a_0,\alpha a_1)$, $(b_0,b_1)=(\beta b_0,\beta b_1)$ with $\alpha,\beta\in\mathbb{C}-\{0\}$, the above f in Eq. (13) maps them to the identical point in $\mathbb{CP}^3$, regardless of α and β. Now we discuss the condition for the image of f, $f(\mathbb{CP}^1\times\mathbb{CP}^1)$, to satisfy in $\mathbb{CP}^3$. By writing down the homogeneous coordinates in $\mathbb{CP}^3$ as (z_0,z_1,z_2,z_3), we define a polynomial of degree 2,

$$Q:=z_0z_3-z_1z_2, \tag{14}$$

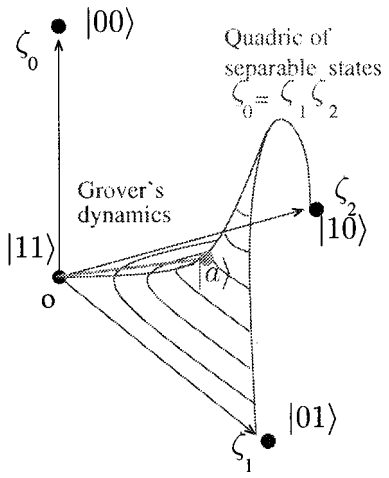

FIG. 1. The geometry of $\mathbb{CP}^3$ around $|11\rangle$, the assumed target $|w\rangle$. Note that because three axes of ζ_1,ζ_2, and ζ_3 represent complex numbers, this figure is written in the complex dimension 3 (real dimension 6). By extracting the real axes of ζ_1,ζ_2, and ζ_3, $|11\rangle$ is found to lie on a saddle point of the quadric. So is each of the other states of the computational basis.

which satisfies $Q(a_0b_0,a_0b_1,a_1b_0,a_1b_1)=0$. On the other hand, it is readily checked that arbitrary points on $Q=0$ are included in $f(\mathbb{CP}^1\times\mathbb{CP}^1)$. Thus we find

$$f(\mathbb{CP}^1\times\mathbb{CP}^1)=\{(z_0,z_1,z_2,z_3)|Q=0\}. \tag{15}$$

Because we can transform any nonsingular quadric into the "normal" quadric form $Q=z_0z_3-z_1z_2=0$ by a projective transformation g,

$$z_j\overset{g}{\mapsto}\sum_{l=0}^{N-1}A_{jl}z_l\quad(j=0,\ldots,N-1), \tag{16}$$

with an $N\times N$ matrix $A:=\{A_{jl}\in\mathbb{C}\}$ such that $\det A\neq0$, we can also identify the nonsingular quadric with $\mathbb{CP}^1\times\mathbb{CP}^1$. That is the reason why the algebraic submanifold of separable, or nonentangled, states $(\mathbb{CP}^1\times\mathbb{CP}^1)$ forms the quadric $Q=0$ in general state space for the two-qubit system $(\mathbb{CP}^3)$, and the states in $\mathbb{CP}^3$ off the quadric $Q=0$ are entangled states.

B. Usage of entanglement

Let us examine the geometry of $\mathbb{CP}^3$ in more detail. We suppose the case where the target state $|w\rangle$ is $|11\rangle$ without loss of generality. To draw the behavior around $|11\rangle$ $[\leftrightarrow(0,0,0,1)]$ as in Fig. 1, we introduce the inhomogeneous coordinates $\zeta_0=z_0/z_3$, $\zeta_1=z_1/z_3$, and $\zeta_2=z_2/z_3$ because of $z_3\neq0$. Then the quadric $Q=0$ in Eq. (14) is written as

$$\zeta_0=\zeta_1\zeta_2. \tag{17}$$

In particular, all the states orthogonal to $|11\rangle$, including $|00\rangle$, $|01\rangle$, $|10\rangle$, $(|01\rangle+|10\rangle)/\sqrt{2}$, etc., are located in points at infinity in Fig. 1. The evolution of Grover's algorithm in Eq. (4) is given by

$$|\psi\rangle \leftrightarrow \left(\frac{\cos\left(k+\frac{1}{2}\right)\theta}{\sqrt{3}}, \frac{\cos\left(k+\frac{1}{2}\right)\theta}{\sqrt{3}}, \frac{\cos\left(k+\frac{1}{2}\right)\theta}{\sqrt{3}}, \sin\left(k+\frac{1}{2}\right)\theta \right) \leftrightarrow (u,u,u,1), \tag{18}$$

or in terms of inhomogeneous coordinates

$$\zeta_0=\zeta_1=\zeta_2=u, \tag{19}$$

where $u:=\cot(k+\frac{1}{2})\theta/\sqrt{3}$ changes from 1 to 0. We find that Grover's algorithm starts from the average state $|a\rangle$ ($\zeta_0=\zeta_1=\zeta_2=1$) on the quadric, evolves away from the quadric along a (geodesic) line $0\leqslant\zeta_0=\zeta_1=\zeta_2\leqslant 1$, and finally reaches the target $|w\rangle$ at the origin on it. Hence Grover's algorithm uses entanglement in the two-qubit case.

Now we treat the general *n*-qubit case. Recalling Eq. (4), we now represent $|\psi(k)\rangle$ by the homogeneous coordinates in $\mathbb{C}\mathcal{P}^{N-1}$ $(N=2^n)$,

$$z_{j\neq w}(k)=\frac{\cos\left(k+\frac{1}{2}\right)\theta}{\sqrt{N-1}}, \quad z_w(k)=\sin\left(k+\frac{1}{2}\right)\theta. \tag{20}$$

We discuss whether the states of Grover's evolution in $\mathbb{C}\mathcal{P}^{2^n-1}$ are included in the algebraic submanifold of the completely separable states of $\mathbb{C}\mathcal{P}^1\times\cdots\times\mathbb{C}\mathcal{P}^1$ $[=:(\mathbb{C}\mathcal{P}^1)^{\times n}]$. As a first step, we consider the condition that Eqs. (20) are included in $\mathbb{C}\mathcal{P}^{2^{n-1}-1}\times\mathbb{C}\mathcal{P}^1$. This is just the necessary condition for the reduction $\mathbb{C}\mathcal{P}^{2^n-1}\rightarrow(\mathbb{C}\mathcal{P}^1)^{\times n}$ and, according to Eq. (A3) in Appendix A ($m=2^{n-1}-1$ and $m'=1$), is given by

$$\frac{\cos\left(k+\frac{1}{2}\right)\theta\sin\left(k+\frac{1}{2}\right)\theta}{\sqrt{N-1}}=\frac{\cos^2\left(k+\frac{1}{2}\right)\theta}{N-1}. \tag{21}$$

From Eq. (21), we have two cases: (i) If $\cos(k+\frac{1}{2})\theta\neq 0$, the condition (21) becomes $\tan(k+\frac{1}{2})\theta=1/\sqrt{N-1}$. The solutions are given as $(k+\frac{1}{2})\theta=\theta/2,\theta/2+\pi(\mathrm{mod}\,2\pi)$ by use of Eq. (1). (ii) If $\cos(k+\frac{1}{2})\theta=0$, it means that $(k+\frac{1}{2})\theta=\pi/2,3\pi/2(\mathrm{mod}\,2\pi)$. These are also the solutions of Eq. (21). The solutions (i) and (ii) are also sufficient, i.e., completely separable to $(\mathbb{C}\mathcal{P}^1)^{\times n}$, and indeed correspond to the average and target state, respectively. For the states in Eq. (20) with other *k*, we cannot reduce them into $(\mathbb{C}\mathcal{P}^1)^{\times n}$ and thus they are entangled states. In brief, although the initial (average) state and the target state are separable, the intermediate states through which the system evolves are entangled.

C. Calculation of entanglement

For the Grover's evolution $|\psi\rangle$, let us calculate the amount of entanglement *E*. Entanglement *E* in our pure state space is naturally considered the *minimum* Fubini-Study distance *s* to the submanifold formed by completely separable states $(\mathbb{C}\mathcal{P}^1)^{\times n}$ in $\mathbb{C}\mathcal{P}^{N-1}$, i.e.,

$$E(|\psi\rangle):=\min_{\{|\phi\rangle|(\mathbb{C}\mathcal{P}^1)^{\times n}\}} s(|\psi\rangle,|\phi\rangle) \overset{\text{Eq. (11)}}{=} 2\arccos\sqrt{\max_{\{|\phi\rangle|(\mathbb{C}\mathcal{P}^1)^{\times n}\}} P(|\psi\rangle,|\phi\rangle)}. \tag{22}$$

Because the Fubini-Study distance in Eq. (22) can be reduced from Bures metric with the parallel transport connection in the case of pure states [19], it satisfies the requirements for a good measure of entanglement, i.e., (i) it is zero for any separable state; (ii) it is invariant under local unitary transformations; (iii) it has a nonincreasing expectation value under local operations, such as classical communication and subselection, as Vedral *et al.* suggested in [20].

It should be remarked that in the case of a *bipartite* (two-qubit) pure state system, the partial entropy (von Neumann entropy of the reduced density matrix associated with one of the parties) is widely supposed to be a good measure of entanglement [21]. However, we apply Eq. (22) as the geometric entanglement measure, because (i) the partial entropy has no apparent geometric meaning in $\mathbb{C}\mathcal{P}$; and (ii) an extension to the multipartite (*n*-qubit) case is nontrivial [22]. As a comparison, we calculate, in Appendix B, the entanglement by partial entropy in the two-qubit case. We find our measure of entanglement (22) almost corresponds to ''concurrence'' [23] so as to be consistent with the calculation using the partial entropy.

Let us first discuss the two-qubit case and then proceed to the general *n*-qubit case. To calculate the entanglement of the Grover's state $|\psi\rangle$ [in Eq. (18)] for the two-qubit case, we have to look for the point that gives the minimum of *s* (or maximum of *P*) in Eq. (22) on the submanifold of the quadric $Q=0$. Because this point must lie on the plane $\zeta_1=\zeta_2$ (i.e., $z_1=z_2$) as seen in Fig. 1, we can parametrize its candidates $|\phi\rangle$ as

$$|\phi\rangle\leftrightarrow(v^2,v,v,1), \tag{23}$$

with $v\in\mathbb{C}$ such that $0\leqslant|v|\leqslant 1$. Thus we consider

$$\max_v P(u,v) = \max_v \frac{[u(v+1)^2-u+1][u(v^*+1)^2-u+1]}{(3u^2+1)(|v|^2+1)^2} = \max_{(r,\chi)} \frac{(ur^2+2ur\cos\chi+1)^2+4u(u-1)r^2\sin^2\chi}{(3u^2+1)(r^2+1)^2}, \tag{24}$$

where v^* denotes the complex conjugate of v and we use $v=re^{i\chi}$ with $0\leqslant r\leqslant 1$. For fixed *r*, *P* in Eq. (24) is largest for the phase $\chi=0(\mathrm{mod}\,2\pi)$. This is solely because *u* in Eq. (18) is a real number. Since $(\partial/\partial r)P(u,r,\chi=0)=0$, we have, according to Eq. (22),

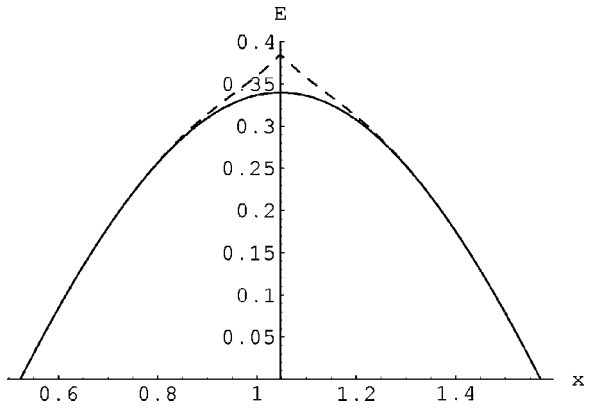

FIG. 2. Entanglement $E(\cot t/\sqrt{3})$ in Eq. (25) during Grover's evolution for two-qubit case (solid curve) is drawn, compared with the approximate estimate of the entanglement $E_2(\cot t/\sqrt{3})$ in Eq. (30) (two dashed curves). Note that the approximate (dashed) curve agrees well with the exact (solid) one except near the halfway state ($t=\pi/3$).

$$E(u)=2\arccos\sqrt{\frac{u^2}{3u^2+1}\left(\frac{v_M+1}{v_M}\right)^2}, \tag{25}$$

where $v_M:=[u-1+\sqrt{(u-1)^2+4u^2}]/(2u)$ gives the maximum of P in Eq. (24) with respect to r.

Changing the variable u into t by $u=\cot t/\sqrt{3}$, we find that the entanglement $E(\cot t/\sqrt{3})$ changes dynamically during evolution as shown in Fig. 2. It takes a value of 0 at the initial average state $|a\rangle$ ($t=\pi/6$), attains its maximum ~ 0.340 at the *halfway* state $u=1/3$ ($t=\pi/3$), and finally goes back to 0 at the target state $|w\rangle$ ($t=\pi/2$). Note that Grover's algorithm in the two-qubit case uses an entanglement at most ~ 0.340 although the available maximal entanglement is $\pi/2$. This implies that, for the halfway state ($t=\pi/3$), there is a closer state on the quadric than either $|a\rangle$ or $|w\rangle$ whose distance from the halfway state is $2(\pi/6)>0.34$. However, as seen in the following, Grover's algorithm comes to use the entanglement maximally when the number of qubits n becomes larger.

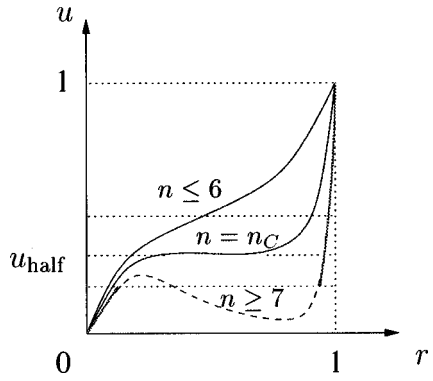

FIG. 3. Schematic pictures of the extremum condition (28) for $n\leqslant 6$, $n=n_C:=4+2\sqrt{2}$, and $n\geqslant 7$ are drawn. $u_{\mathrm{half}}:=\cot[(\pi+\theta)/4]/\sqrt{N-1}$ corresponds to the halfway state. When $n\geqslant 7$ ($>n_C$), the solid parts of the curve give the condition for the maximum of P_n.

Now it is straightforward to calculate the entanglement for the general n-qubit case. According to Eq. (20), the Grover's state $|\psi\rangle$ in the n-qubit case is given by $(u,\ldots,u,1)$, where u $[:=\cot(k+\frac{1}{2})\theta/\sqrt{N-1}]$ ranges from 0 to 1. The states $|\phi\rangle$, candidates closest to the state $|\psi\rangle$ on the submanifold $(\mathbb{C}\mathcal{P}^1)^{\times n}$, are "coherent" states [cf. Eq. (23)] parametrized as

$$|\phi\rangle\leftrightarrow\Big(\underbrace{v^n,v^{n-1},\ldots,v^{n-1}}_{n},\underbrace{v^{n-2},\ldots,v^{n-2}}_{n(n-1)/2},\ldots,\underbrace{v,\ldots,v}_{n},1\Big)$$

$$\leftrightarrow\underbrace{(v,1)\times\cdots\times(v,1)}_{n}, \tag{26}$$

with $v\in\mathbb{C}$ such that $0\leqslant|v|\leqslant 1$. Likewise, by use of $v=re^{i\chi}$ with $0\leqslant r\leqslant 1$, we have

$$E_n(u)=2\arccos\sqrt{\max_v P_n(u,v)}=2\arccos\sqrt{\max_{(r,\chi)}\frac{u^2(r^2+2r\cos\chi+1)^n+2u(1-u)\sum_{m=0}^{n}\binom{n}{m}r^m\cos m\chi+(1-u)^2}{[(N-1)u^2+1](r^2+1)^n}}. \tag{27}$$

For a fixed r, the maximum in Eq. (27) is attained at the phase $\chi=0(\mathrm{mod}\,2\pi)$ for the n-qubit case also. From $(\partial/\partial r)P_n(u,r,\chi=0)=0$, we have the extremum condition

$$u=\frac{r}{(1+r)^{n-1}(1-r)+r}. \tag{28}$$

It is hard to solve analytically the extremum condition (28) for r so as to seek the solution that gives the maximum of P_n. However, we readily find, as seen in Fig. 3, that Eq. (28) increases monotonically with r for $n\leqslant 6$; on the other hand, it has a relative maximum and a relative minimum for $n\geqslant 7$, i.e., for almost all n. When u has one-to-one correspondence with r in Fig. 3, it soon becomes the maximum condition of P_n. In contrast, when u has one-to-three correspondence to r, the point among the three that is included in the solid line in Fig. 3 indeed gives the maximum condition. Now it should be noted that because entanglement is symmetric for the halfway state as in the two-qubit case, all we

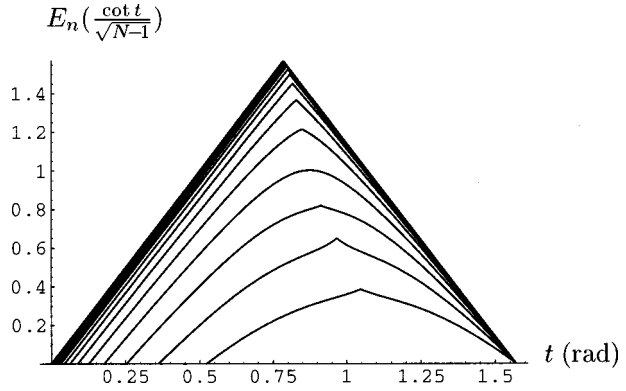

FIG. 4. Each entanglement $E_n(\cot t/\sqrt{N-1})$ in Eq. (30) for the $n=2$-,3-, . . . ,50-qubit case is drawn from the bottom to the top. Apparent singularities in the halfway states are just due to taking a mirror image of the approximate calculations (30) for the second half of the dynamics. While the true curves for small n should be smooth near the halfway states (cf. Fig. 2), an intrinsic singularity appears as the peak of an enveloping triangle $E=-2|t-\pi/4|+\pi/2$ when n goes to infinity.

need to consider is one-half of the whole dynamics, e.g., the second half here. By reparametrizing u as $u=\cot t/\sqrt{N-1}$, the second half, given by $t\in[(\pi+\theta)/4,\pi/2]$, corresponds to $u\in[\cot[(\pi+\theta)/4]/\sqrt{N-1},0]$. Thus when N is large the second half is almost $u\in[1/\sqrt{N-1},0]$ by Eq. (1), so that it can be treated as the realm of $u\ll 1$ and $r\ll 1$. Taking the first order of r in Eq. (28), we obtain an approximate maximum condition for $r,u\ll 1$: $u\sim r/[1+(n-1)r]$, or

$$r_M := \frac{u}{1-(n-1)u}. \tag{29}$$

Although Eq. (29) becomes a better approximation for larger N, it seems to remain valid for small N because, even in the two-qubit (worst approximation) case, the deviation from the exact result is limited near the halfway state and is small (see Fig. 2).

Substituting r_M of Eq. (29) and $\chi=0$ in Eq. (27), we have the entanglement of the n-qubit case:

$$E_n(u)\sim 2\arccos\sqrt{\frac{[u(r_M+1)^n+(1-u)]^2}{[(N-1)u^2+1](r_M^2+1)^n}}, \tag{30}$$

drawn in Fig. 4 with $u=\cot t/\sqrt{N-1}$. We find in Fig. 4 that $E_n(\cot t/\sqrt{N-1})$ almost converges to an enveloping triangle $E=-2|t-\pi/4|+\pi/2$ at $n\sim 15$. This suggests two points: first, entanglement is maximally used for large n. Second, the closest separable state during Grover's algorithm is either the initial average state $|a\rangle$ or the target state $|w\rangle$, which implies that the submanifold of completely separable states is sparse in the large-n-qubit state space.

IV. GEOMETRIC CONSTRUCTION OF OPTIMAL QUANTUM SEARCH

In Secs. II and III, we found that Grover's algorithm is a horizontal lift of a geodesic lying away from the submanifold of the separable states in $\mathbb{C}\mathcal{P}$, which can be interpreted as the geometric necessary condition for the optimal quantum search. In this section, let us consider, on the contrary, whether all the geodesics toward the target state $|w\rangle$ become the optimal quantum search. That is to say, we discuss the geometric sufficient condition for the optimal quantum search, from which the bound of the computational time is also derived naturally.

A. Geometric strategy by means of geodesics

Let us consider a set of all the geodesics through the target state $|w\rangle$ in $\mathbb{C}\mathcal{P}^{N-1}$. As seen in Sec. II, its horizontal geodesic in $\mathcal{H}$ is just a real two-dimensional rotation on the plane spanned by $|w\rangle$ and some arbitrary state $|y\rangle$ (denoted for brevity as the w-y plane). We can restrict $|y\rangle$ such that q $(:=\langle w|y\rangle\in\mathbb{R})$ ranges from 0 to 1, by choosing the preferable overall phase of $|y\rangle$ for each ray $\Pi(|y\rangle)$. $|w\rangle$ and $|y\rangle$ are said to be "in phase" in terms of the Pancharatnan connection [14]. By a consequence of an elementary theorem of real Euclidean geometry, a two-dimensional rotation on the w-y plane is constructed by two successive reflections,

$$U_{y'} := -I_{y'}I_w, \tag{31}$$

where $I_{y'}:=\mathbf{1}-2|y'\rangle\langle y'|$ and $I_w:=\mathbf{1}-2|w\rangle\langle w|$ denote a reflection for the line orthogonal to $|y'\rangle$ and $|w\rangle$ in the w-y plane, respectively. We take an overall -1 in Eq. (31) for convenience, which simply means that $-I_{y'}=I_{y'_\perp}$ [24]. Although in general $|y'\rangle$ can be any state on the w-y plane, we put $|y'\rangle=|y\rangle$ without loss of generality because $|y\rangle$ itself is any state. By using $\eta\in[0,\pi]$ such that $\sin(\eta/2):=q=\langle w|y\rangle$, Eq. (31) is represented by

$$U_y(\eta) := -I_yI_w=\begin{bmatrix}\cos\eta & -\sin\eta\\ \sin\eta & \cos\eta\end{bmatrix}, \tag{32}$$

in the basis of $|r'\rangle$ $[:=(|y\rangle-q|w\rangle)/\sqrt{1-q^2}]$, orthogonal to $|w\rangle$, and $|w\rangle$. Two remarks are in order: First, the angle of the rotation in Eq. (32), which corresponds to the speed of a single query, is determined just by η (or q). This means that the speed is faster for larger η (or q). Second, the direction of the rotation in Eq. (32) is determined by the order of I_w and I_y. Alternate applications of I_w and I_y cause successive rotations in the same direction, as can be seen in Fig. 5.

Thus the candidate for the algorithm that gives the *optimal* quantum search toward the target $|w\rangle$ is constructed in terms of the geodesics as

$$|\Psi(k)\rangle=U_{y_k}(\eta_k)\cdots U_{y_2}(\eta_2)U_{y_1}(\eta_1)|y_0\rangle, \tag{33}$$

such that $|y_0\rangle,|y_1\rangle,\ldots,|y_k\rangle$ must lie on the *same* two-dimensional plane including $|w\rangle$ with $\eta_0\leqslant\eta_1\leqslant\cdots\leqslant\eta_k$, where $\sin(\eta_j/2):=\langle w|y_j\rangle$. We find, however, that only the case of $|y_0\rangle=|y_1\rangle=\cdots=|y_k\rangle$ (i.e., $\eta_0=\eta_1=\cdots=\eta_k$) is possible.

The reason is the following. Suppose the algorithm begins from a fixed $|y_0\rangle$, then $|\Psi(1)\rangle=U_{y_1}(\eta_1)|y_0\rangle$ is determined by selecting $|y_1\rangle$ on the w-y_0 plane. However, because we

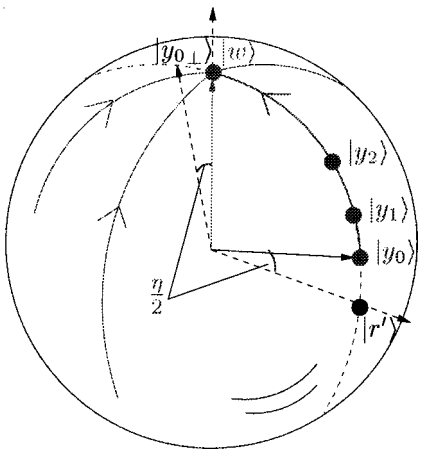

FIG. 5. Each horizontal geodesic toward the target $|w\rangle$ consists of two-dimensional successive rotations in the plane including $|w\rangle$.

never know (only the oracle knows) which is the target $|w\rangle$, the only state we are able to utilize on the w-y_0 plane is $|y_0\rangle$. So $|y_1\rangle=|y_0\rangle$. Then to get $|\Psi(2)\rangle$ by the choice of $U_{y_2}(\eta_2)$, it might seem possible to apply $|\Psi(1)\rangle$ as well as $|y_0\rangle$ to $|y_2\rangle$ on the w-y_0 plane. Yet, we must call another oracle as a subroutine to take advantage of $|\Psi(1)\rangle$ in case no measurements are done during the computation. This case is just the situation where Zalka [5] showed the optimality of Grover's algorithm. We restrict our attention here to an algorithm including no subroutines that require another oracle, because, if needed, we can always embed a no-subroutine algorithm into a certain larger algorithm as a subroutine [25]. Hence all we can do is $|y_2\rangle=|y_0\rangle$, again. In the same way, we finally obtain $|y_0\rangle=\cdots=|y_k\rangle$ (i.e., $\eta_0=\cdots=\eta_k$) which can be denoted simply by $|y\rangle$ and η, respectively.

Accordingly, Eq. (33) turns out to be an extension of Grover's algorithm where the average state $|a\rangle$ is replaced with the arbitrary state $|y\rangle$ [26]. That is, our algorithm is written as

$$|y\rangle := \begin{bmatrix} \cos\frac{\eta}{2}|r'\rangle \\ \sin\frac{\eta}{2}|w\rangle \end{bmatrix}, \tag{34}$$

$$|\Psi(k)\rangle := U_y(\eta)^k|y\rangle = \begin{bmatrix} \cos\left(k+\frac{1}{2}\right)\eta|r'\rangle \\ \sin\left(k+\frac{1}{2}\right)\eta|w\rangle \end{bmatrix}.$$

The speed of the algorithm (34), considered as the traveling (Fubini-Study) distance of a single query along the geodesic, is given by

$$V(k) := \frac{\Delta s}{\Delta k} = 2\arccos|\langle\Psi(k+1)|\Psi(k)\rangle| = 2\eta = 4\arcsin q, \tag{35}$$

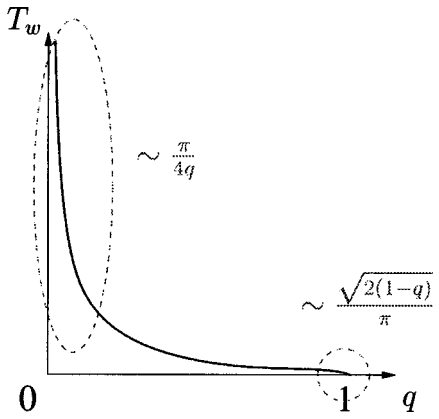

FIG. 6. The computational time T_w in Eq. (37).

where, in the third equality, we use $\langle\Psi(k)|U_y(\eta)|\Psi(k)\rangle=\cos\eta$ from Eqs. (32) and (34). This corresponds to the Anandan-Aharonov relation [13] $ds/dt=2\Delta H/\hbar$, which means that the speed in $\mathbb{CP}$ is determined by the energy uncertainty ΔH. Note that $V(k)$ in Eq. (35) is constant, independent of k, through the algorithm so that it depends only on η (or q). The total traveling distance is naturally thought to be the statistical distance [27] between the initial state $\Pi(|y\rangle)$ and the goal state $\Pi(|w\rangle)$:

$$s_w := \pi-\eta=\pi-2\arcsin q. \tag{36}$$

Consequently, we obtain the time required to reach the target $|w\rangle$:

$$T_w := \frac{s_w}{V}=\frac{\pi-\eta}{2\eta}=\frac{\pi-2\arcsin q}{4\arcsin q}. \tag{37}$$

As seen in Fig. 6, T_w is shorter for larger q. We also find that $T_w\sim\pi/(4q)$ for $q\ll 1$, while $T_w\sim\sqrt{2(1-q)}/\pi$ for $q\sim 1$.

B. Bound for the computational time

We may ask where the bound of the computational time T_w comes from. Remember that we want to extract $|w\rangle$ with probability 1 in an optimal computational time for the worst case evaluation. However, because we do not know *a priori* (only the oracle knows) which is the target $|w\rangle$, we have to select $|y\rangle$ independently of $|w\rangle$. When $|y\rangle$ is selected as $|y\rangle=\Sigma_{x=0}^{N-1}z_x|x\rangle$ $(\Sigma_{x=0}^{N-1}|z_x|^2=1)$ in the computational basis $|x\rangle$ $(\ni|w\rangle)$, its smallest overlap $q_s(:=|z_s|)$ gives the computational time T_w for the worst case. We find

$$\frac{\pi-2\arcsin q_s}{4\arcsin q_s}\geqslant\frac{\pi-2\arcsin(1/\sqrt{N})}{4\arcsin(1/\sqrt{N})}\sim\frac{\pi}{4}\sqrt{N}, \tag{38}$$

where because of $q_s\leqslant 1/\sqrt{N}$, the equality in Eq. (38) is attained for the $|y\rangle$ such that $q_s=1/\sqrt{N}$, i.e, all $q_x:=|z_x|=1/\sqrt{N}$. This implies that the "mixedness" of the searching state space (in part) bounds the efficiency of the quantum search as Bose *et al.* [28] mentioned. Thus, regardless of which is the target, the optimal computational time is $(\pi/4)\sqrt{N}$. This result of course coincides with Grover's result [3], first proved optimal by Zalka [5].

It should be commented that there remains room for relative phases in $|y\rangle$. $|y\rangle=|a\rangle$ in the original Grover's algorithm is only a choice. In general, any element of the Fourier basis

$$|p\rangle := \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{(2\pi i/N)px}|x\rangle \quad (p=0,1,\ldots,N-1) \tag{39}$$

can be taken as a $|y\rangle$ among the completely separable states. This implies that the quantum search takes advantage of dual bases $|x\rangle$ and $|p\rangle$ to run in the optimal computational time because its kernel takes the form $U=-I_pI_x$ by Eq. (32).

V. CONCLUSIONS

In this paper, we have shown two geometric characteristics of quantum search: one is related to the geodesic in $\mathbb{CP}$, the other related to entanglement. First, the geometric necessary and sufficient condition for the optimal quantum search is given by the horizontal geodesic joining the target $|w\rangle$ and a preferable selected initial state $|y\rangle$ such that it overlaps equally, up to relative phases, with all the elements of the computational basis $|x\rangle$ $(\ni|w\rangle)$. Second, Grover's quantum search uses entanglement for an arbitrary number of the qubits n, in particular, almost maximally for large n. However, there seems to be no direct relationship between the amount of entanglement (how far the dynamics is away from the submanifold of separable states) and the optimal, i.e., shortest, computational time. This is because (i) the amount of entanglement is different for each n although Grover's algorithm is exactly optimal regardless of n [5]; (ii) the computational time is rather determined by the overlap $q=\langle w|y\rangle$ as seen in Sec. IV. It is significant that the algorithm consists of the shortest path by means of the geodesic; as a result it runs across entangled states away from the submanifold of the separable states.

It is readily found that the multiple target case [4] is also characterized in completely the same manner. Moreover, our geometric strategy would be useful to construct other efficient quantum algorithms, as some efficient classical algorithms are widely known to be geodesics in their parameter spaces. Exploring the geometric viewpoint also seems appealing toward the realization of quantum computers. For instance, (i) the holonomic approach to quantum computation [29], where loops by horizontal lifts of the path in $\mathbb{CP}$ construct the logic gates to compute quantum algorithms, is supposed to have built-in fault-tolerant features against local perturbations; and (ii) time optimal pulse sequences in NMR quantum computing [30], given by geodesics on certain coset spaces, would minimize the effect of relaxation and optimize the sensitivity of the experiments.

ACKNOWLEDGMENT

One of the authors (A.M.) would like to thank I. Tsutsui for kind interest in this work.

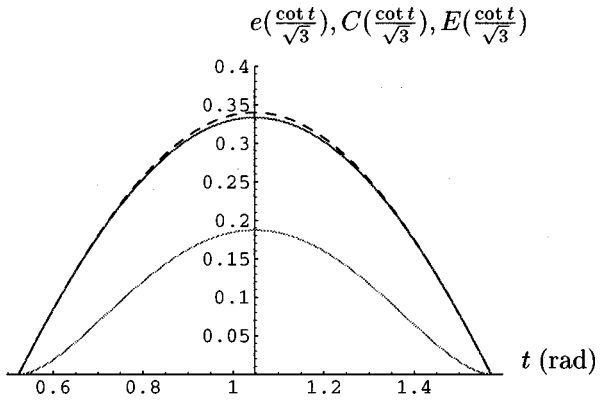

FIG. 7. Three entanglement measures: (i) the partial entropy $e(\cot t/\sqrt{3})$ in Eq. (B2) (the lower solid curve); (ii) the concurrence $C(\cot t/\sqrt{3})$ in Eq. (B4) (the upper solid curve); and (iii) the minimum Fubini-Study distance to separable states $E(\cot t/\sqrt{3})$ in Eq. (25) (the upper dashed curve).

APPENDIX A: SEGRE EMBEDDING IN THE GENERAL CASE

It is straightforward to extend the mapping f of the Segre embedding into the general case:

$$f:\mathbb{CP}^m\times\mathbb{CP}^{m'}\to\mathbb{CP}^{(m+1)(m'+1)-1}$$

$$((a_0,\ldots,a_m),(b_0,\ldots,b_{m'})) \mapsto (a_0b_0,\ldots,a_0b_{m'},a_1b_0,\ldots,a_mb_0,\ldots,a_mb_{m'}). \tag{A1}$$

We find, in the same way as in the text, that the algebraic submanifold given by the image of f is the zero locus of all the homogeneous polynomials of degree 2:

$$Q_{(i,j),(k,l)} := z_{(m'+1)i+k}z_{(m'+1)j+l} - z_{(m'+1)i+l}z_{(m'+1)j+k}, \tag{A2}$$

where $0\leqslant i<j\leqslant m$, $0\leqslant k<l\leqslant m'$. Hence we have

$$f(\mathbb{CP}^m\times\mathbb{CP}^{m'})=\{Q_{(i,j),(k,l)}=0\}, \tag{A3}$$

where a set of quadratic constraints $\{Q_{(i,j),(k,l)}=0\}$ consists of $m(m+1)m'(m'+1)/4$ simultaneous equations.

APPENDIX B: CALCULATION OF ENTANGLEMENT BY PARTIAL ENTROPY IN TWO-QUBIT CASE

In this Appendix, the entanglement of the two-qubit case is calculated in terms of the partial entropy, so as to be compared with the results in Sec. III. For the Grover's state $|\psi\rangle=(u|00\rangle+u|01\rangle+u|10\rangle+|11\rangle)/\sqrt{3u^2+1}$ in Eq. (18), we obtain a reduced density matrix by tracing out, e.g., the second qubit,

$$\rho_{\mathrm{red}} := \mathrm{tr}_{2\mathrm{nd}}(|\psi\rangle\langle\psi|) = \frac{1}{3u^2+1}\begin{pmatrix} 2u^2 & u(u+1) \\ u(u+1) & u^2+1 \end{pmatrix}. \tag{B1}$$

We calculate entanglement as the partial entropy of the reduced density matrix (B1):

$$e(u) := -\mathrm{tr}(\rho_{\mathrm{red}} \log \rho_{\mathrm{red}}) = -\lambda_+ \log \lambda_+ - \lambda_- \log \lambda_- , \tag{B2}$$

where $\lambda_\pm$, the eigenvalues of the reduced density matrix ρ_{red} in Eq. (B1), are given by

$$\lambda_\pm := \frac{1 \pm \sqrt{1-C(u)^2}}{2}, \tag{B3}$$

$$C(u) := 2\left|\det \frac{1}{\sqrt{3u^2+1}} \begin{pmatrix} u & u \\ u & 1 \end{pmatrix}\right| = \frac{2u(1-u)}{3u^2+1}. \tag{B4}$$

As $C(u)$ in Eq. (B4), called ''concurrence'' [23], goes from 0 to 1, the entanglement $e(u)$ in Eq. (B2) increases monotonically from 0 to 1. So $C(u)$ as well as $e(u)$ can be regarded as a measure of entanglement.

The partial entropy $e(\cot t/\sqrt{3})$ as well as the concurrence $C(\cot t/\sqrt{3})$, compared with our entanglement $E(\cot t/\sqrt{3})$ in Eq. (25), are drawn in Fig. 7. We note two points in Fig. 7: First, all three entanglement measures are convex upward and are maximized at the halfway state $t=\pi/3$ $(u=1/3)$. Second, surprisingly enough, our entanglement measure E almost coincides with the concurrence C, characterized also as $C=2|z_0z_3-z_1z_2|=2|Q|$ [in Eq. (14)] with normalized homogeneous coordinates z_j. It should be noted, however, that their normalizations are different, i.e., E is normalized to $\pi/2$, while C is normalized to 1. In summary, our calculation of entanglement by Eq. (22) is consistent with that by partial entropy.

[1] R.P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[2] P. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 124.

[3] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[4] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Fortschr. Phys. **46**, 493 (1998).

[5] C. Zalka, Phys. Rev. A **60**, 2746 (1999).

[6] D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London, Ser. A **449**, 669 (1995).

[7] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[8] S.L. Braunstein and A.K. Pati, e-print quant-ph/0008018.

[9] S.L. Braunstein, C.M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).

[10] S. Lloyd, Phys. Rev. A **61**, 010301 (1999).

[11] D.A. Meyer, Phys. Rev. Lett. **85**, 2014 (2000).

[12] D.N. Page, Phys. Rev. A **36**, 3479 (1987).

[13] J. Anandan and Y. Aharonov, Phys. Rev. D **38**, 1863 (1988); Phys. Rev. Lett. **65**, 1697 (1990).

[14] N. Mukunda and R. Simon, Ann. Phys. (N.Y.) **228**, 205 (1993).

[15] G.W. Gibbons, J. Geom. Phys. **8**, 147 (1992).

[16] D.C. Brody and L.P. Hughston, J. Geom. Phys. **38**, 19 (2001).

[17] J.-L. Brylinski, e-print quant-ph/0008031.

[18] M. Kuś and K. Życzkowski, Phys. Rev. A **63**, 032307 (2001).

[19] D. Petz and C. Sudár, J. Math. Phys. **37**, 2662 (1996).

[20] V. Vedral, M.B. Plenio, M.A. Rippin, and P.L. Knight, Phys. Rev. Lett. **78**, 2275 (1997); V. Vedral and M.B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[21] C.H. Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996); C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, *ibid.* **54**, 3824 (1996).

[22] To characterize fully the multipartite system, we would need several kinds of entanglement related to arbitrary partitions of the composite system into subsystems as proposed by W. Dür, J.I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999); J. Eisert and H.J. Briegel, Phys. Rev. A **64**, 022306 (2001), etc. This corresponds in our scheme to taking into consideration minimum distances to other submanifolds like, e.g., $\mathbb{C}\mathcal{P}^3 \times (\mathbb{C}\mathcal{P}^1)^{\times n-2}$ as well as Eq. (22). In the text, we consider only the *principal* one (22) among them because we are interested here in how entanglement is useful for quantum computation rather than in the classification of entangled states.

[23] S. Hill and W.K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997); W.K. Wootters, *ibid.* **80**, 2245 (1998).

[24] R. Jozsa, e-print quant-ph/9901021.

[25] The dynamical improvement of $|y_j\rangle$ in which η_j became larger would make the algorithm faster if another oracle were not required. In fact, because using other oracles in a subroutine can be found to result in an equivalent algorithm to the original Grover's one for the computational time, it does not lead to a speed-up.

[26] The generalized quantum search for an arbitrary initial state has already been discussed by L.K. Grover, Phys. Rev. Lett. **80**, 4329 (1998); E. Biham, O. Biham, D. Biron, M. Grassl, and D.A. Lidar, Phys. Rev. A **60**, 2742 (1999). It should be emphasized that, in this paper, we consider it as the geometric sufficient condition.

[27] S.L. Braunstein and C.M. Caves, Phys. Rev. Lett. **72**, 3439 (1994).

[28] S. Bose, L. Rallan, and V. Vedral, Phys. Rev. Lett. **85**, 5448 (2000).

[29] J. Pachos and P. Zanardi, Int. J. Mod. Phys. B **15**, 1257 (2001), and references therein.

[30] N. Khaneja, R. Brockett, and S.J. Glaser, Phys. Rev. A **63**, 032308 (2001).