"Horizontal" Grover's Search Algorithm

京都大学・情報学研究科
溝部 公威 (Kimitake Mizobe)
Graduate School of Informatics,
Kyoto University

1 Introduction

Quantum computation is a novel computing paradigm which is based on the quantum mechanics. The effects of superposition and entanglement provide quantum computers with the power to solve several problems more efficiently than classical computers. The most striking quantum algorithms are Shor's factoring algorithm and Grover's search algorithm. The former exploits quantum parallelism to offer an exponential speed-up over classical computers for prime factorization, suggesting the possibility of destroying the safety of the RSA cryptography system which is very widely used. The latter, to which this thesis is concerned, substantially speeds up the solution to the search problem.

If you are given an usual phone book, in which you wish to find the name whose telephone number is 012-345-6789, for instance, the only strategy you take is to look up the names one by one, so that before reaching the target name, you will read half of the names on average. Moreover, if you are completely out of luck, you will come to the name after having read all the names. Like this, we usually need $O(N)$ operations to find out an element from a database of size N without prior knowledge about its structure. Grover's algorithm, in contrast, provides a more efficient solution which needs only $O(\sqrt{N})$ operations by using power of quantum computer. Grover's algorithm attract great interest, since searching heuristics have wide range of applications such as quantum counting and speedup of solution to some NP-complete problems [1].

In 2001, Miyake and Wadati explored quantum search from the geometric viewpoint [8]. They claimed that Grover's algorithm skips along with the geodesic joining a target state and an initial state on a complex projective space $\mathbb{C}P^{N-1}$. Motivated by them, Uwano, Hino, and Ishiwatari studied an integrable dynamical system arising from Grover's quantum search algorithm extended for an ordered tuple of multi-qubit states [3, 4, 5].

They defined an action of unitary group $U(2^n)$ on the state space, making it into a fibre bundle over the space of regular 'relative configurations' of multi-qubit state.

In this article, further analysis is made on the fibre bundle structure to provide a new algorithm, "horizontal" Grover's search algorithm. This thesis is organized as follows: Section 2 is a review of quantum computation and Grover's search algorithm. We set up a Hilbert space for m-tuples of multi-qubit states, on which the extended Grover's algorithm is performed [4]. In Section 3, the fibre bundle structure is introduced. We also note that the tangent space at each point is decomposed into a direct sum of a vertical subspace and a horizontal subspace, and that the geodesic which the Grover's algorithm traces isn't horizontal. In Section 4, we define a connection on the principal stratum of the fibre bundle by extending the definition of connection of a principal fibre bundle. With the connection form taken into account, we can carry the search geodesic into a horizontal curve. Section 5 is a main part of this thesis. First, we assert that it would be easier to carry out operations on the states in the same orbit of the $U(2^n)$ action. It is to be noted that all the target states we are supposed to search are lying in the same orbit (target orbit). Second, we generalize the Grover operator. Finally, we propose a new algorithm which is broken up into two steps. In the first step, we reach the target orbit from the initial point by generalized Grover operator with less steps than the ordinary algorithm, and then, we proceed to carry out the search algorithm in the target orbit. Since the sequence of states generated in the first step traces a horizontal geodesic, we call this algorithm "horizontal" Grover's algorithm. Section 6 contains concluding remarks on the result obtained.

2 Quantum search algorithm

Suppose there is given an unsorted data array of size $N(=2^n)$ and one of the data is marked. According to Grover's quantum search algorithm [2], one can find out the marked datum with a success possibility almost 1 in only $O(\sqrt{N})$ queries, while the usual classical algorithm needs $O(N)$ queries in the worst case. The Grover algorithm can be extended so as to search an ordered m-tuple of data in the same $O(\sqrt{N})$ queries [4]. In this section, we make a review of the extended Grover algorithm together with some geometric aspects.

2.1 Setting up

Quantum computation is performed in a Hilbert space. The most basic Hilbert space $\mathcal{H}$ is that for a single qubit, which is a complex vector space of dimension two. Let $\{|0\rangle, |1\rangle\}$ denote an orthogonal basis of $\mathcal{H}$. We can then identify $\mathcal{H}$ with $\mathbb{C}^2$ by the relation

$$|\phi\rangle = c_0 |0\rangle + c_1 |1\rangle \quad \leftrightarrow \quad \phi = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}. \tag{2.1}$$

The Hilbert space V_n for n-qubits are constructed as the tensor product of 1-qubit Hilbert spaces, $\overbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}^{n}$. Elements of V_n are expressed as

$$|\phi\rangle = \sum_{i_1,\cdots,i_m} c_{i_1 \cdots i_m} |\phi_{i_1}\rangle \otimes |\phi_{i_2}\rangle \otimes \cdots \otimes |\phi_{i_m}\rangle, \quad |\phi_{i_k}\rangle \in \mathcal{H}. \tag{2.2}$$

The Hermitian inner product for $|\Psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_m\rangle$ and $|\Phi\rangle = |\phi_1\rangle \otimes \cdots \otimes |\phi_m\rangle$ is defined by

$$\langle \phi | \psi \rangle = \prod_{i=1}^{n} \langle \phi_i | \psi_i \rangle, \tag{2.3}$$

where inner product in the R.H.S. is that on 1-qubit space. By linearity, the Hermitean inner product is defined on the whole V_n. An orthonormal basis of V_n is formed from $|0\rangle$ and $|1\rangle$. We describe $x \in \{0, \cdots, 2^n - 1\}$ as a binary number like $x = x_1 x_2 \cdots x_n$ and define the elements $|x\rangle$ of V_n by

$$|x\rangle := |x_n\rangle \otimes |x_{n-1}\rangle \otimes \cdots \otimes |x_1\rangle, \quad |x_i\rangle = |0\rangle \, \text{or} \, |1\rangle. \tag{2.4}$$

The system $\{|x\rangle\}_{x=0,1,\ldots,2^n-1}$ forms an orthonormal basis of V_n, which is called the **computational basis of V_n**. Using this orthonormal basis, V_n is identified with $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$.

When the number of data to be searched is m, we need to use the direct product space of m n-qubit Hilbert spaces:

$$(V_n)^m := \underbrace{V_n \times \cdots \times V_n}_{m} = \{\, |\Phi\rangle = (|\phi_1\rangle, \cdots, |\phi_m\rangle) \mid |\phi_i\rangle \in V_n \,\} \tag{2.5}$$

in order to describe the data and to perform the search algorithm. The Hermitian inner product on $(V_n)^m$ is defined by

$$\langle \Phi | \Psi \rangle = \frac{1}{m} \sum_{i=1}^{m} \langle \phi_i | \psi_i \rangle. \tag{2.6}$$

The inner product in the R.H.S. is that on V_n. An orthonormal basis of $(V_n)^m$ is given in terms of the computational basis of V_n. Let

$$|\Phi(j;x)\rangle = \sqrt{m}(0, \cdots, 0, \underset{j\text{th}}{|x\rangle}, 0, \cdots, 0) \quad (j \in \{1, \cdots, m\}, x \in \{0, \cdots, 2^n - 1\}). \tag{2.7}$$

Then, the set $\{|\Phi(j;x)\rangle\}$ forms an orthonormal basis of $(V_n)^m$, which is called the **computational basis of** $(V_n)^m$.

$(V_n)^m$ is a $2^n \times m$ dimensional complex vector space and can be identified with $\mathbb{C}^{2^n \times m}$, the space of $2^n \times m$ complex matrices, through the correspondence:

$$|\Phi\rangle = \sum_{x=0}^{2^n-1} \sum_{j=1}^{m} c_{x+1,j} \, |\Phi(j;x)\rangle \quad \leftrightarrow \quad \Phi = \left(\sqrt{m} c_{xj}\right). \tag{2.8}$$

In the following, we deal with matrices $\Phi \in \mathbb{C}^{2^n \times m}$ rather than the Dirac notation $|\Phi\rangle$. The Hermitian inner product (2.6) is then given by

$$\langle \Phi, \Psi \rangle = \frac{1}{m} \mathrm{tr}(\Phi^\dagger \Psi), \quad \Phi, \Psi \in (V_n)^m. \tag{2.9}$$

The elements of the Hilbert space whose norm is 1 are called **state vectors**. The space of state vectors of $(V_n)^m$ is defined as

$$(V_n)_1^m = \{ \Phi \in (V_n)^m \mid \langle \Phi, \Phi \rangle = 1 \}. \tag{2.10}$$

The quantum computation is performed by applying a sequence of unitary operators to an initial state vector in $(V_n)_1^m$, so that an algorithm generates a sequence of points in $(V_n)_1^m$.

2.2 Grover's Algorithm

Suppose that there are unsorted data arrays of size $N(=2^n)$ and m of them are labeled $d_1, \cdots, d_m$, $d_j \in \{1, \cdots, 2^n\}$. We assume the labels are different from one another. In other words, the label $d = \{d_1, \cdots, d_m\}$ is a permutation of m numbers from $\{1, \cdots, 2^n\}$. Let D be the set of all the possible labels, which has ${}_{2^n}P_m = \frac{2^n!}{m!}$ elements.

The purpose of the search algorithm is to find the labeled target data sequence out of the unsorted data arrays of size $N(=2^n)$.

Let the matrix

$$W = [e_{d_1}, \cdots e_{d_m}], \quad e_j = [0, \cdots, 0, \underset{j\text{th}}{1}, 0, \cdots, 0]^\top \tag{2.11}$$

describe the data sequence associated with the label $d_1, \cdots, d_m$, which we will search. We take up another element of $(V_n)_1^m$,

$$A = [a, \cdots, a], \quad a = \frac{1}{\sqrt{2^n}} [1, \cdots, 1]^\top \tag{2.12}$$

as an initial state in the algorithm. A is the superposition of all the computational basis at an equal weight. W and A are called the **target** and the **initial state**, respectively. It is easy to verify that W and A are in $(V_n)_1^m$.

We define a real inner product $(\cdot,\cdot)$ on $(V_n)_1^m$,

$$(\Phi,\Psi)=\mathrm{Re}\,\langle\Phi,\Psi\rangle=\frac{1}{m}\mathrm{Re}\left(\mathrm{tr}\Phi^{\mathrm{T}}\Psi\right),\quad \Phi,\Psi\in(V_n)^m. \tag{2.13}$$

We introduce two operators [1] on $(V_n)^m$ by

$$I_W:(V_n)_1^m\to(V_n)_1^m,\quad \Phi\mapsto\Phi-2\,(W,\Phi)\,W, \tag{2.14}$$
$$I_A:(V_n)_1^m\to(V_n)_1^m,\quad \Phi\mapsto\Phi-2\,(A,\Phi)\,A. \tag{2.15}$$

The I_W and I_A are shown to be unitary operators and to leave invariant the complex subspace $\mathrm{span}_{\mathbb{C}}\{\mathrm{W},\mathrm{A}\}$. In [4], the operators I_W and I_A are defined by using the Hermitian inner product instead of the real inner product. Two definitions are equivalent since the value of the Hermitian inner product is always real in this algorithm. The real inner product is essential for generalizing the algorithm in Section 5. Further, we are thinking of $(V_n)_1^m$ as a sphere $S^{2^n m-1}$ and of geometry in the real category.

Let us consider the dynamics of the algorithm. We define another state R by

$$R=\sqrt{\frac{2^n}{2^n-1}}A-\frac{1}{\sqrt{2^n-1}}W. \tag{2.16}$$

Then R and W form an orthonormal basis of $\mathrm{span}_{\mathbb{C}}\{\mathrm{W},\mathrm{A}\}=\mathrm{span}_{\mathbb{C}}\{\mathrm{R},\mathrm{W}\}$.

We define the **Grover operator** by $G=-I_A\circ I_W$. This operator acts on $\mathrm{span}_{\mathbb{C}}\{\mathrm{R},\mathrm{W}\}$ as

$$G(W)=\left(1-\frac{2}{2^n}\right)W-2\sqrt{\frac{1}{2^n}}\sqrt{\frac{2^n-1}{2^n}}R, \tag{2.17}$$
$$G(R)=\left(1-\frac{2}{2^n}\right)R+2\sqrt{\frac{1}{2^n}}\sqrt{\frac{2^n-1}{2^n}}W. \tag{2.18}$$

If we set

$$\sin\frac{\theta}{2}=\sqrt{\frac{1}{2^n}},\quad \cos\frac{\theta}{2}=\sqrt{\frac{2^n-1}{2^n}}, \tag{2.19}$$

the above transformation is expressed as

$$G\{R,W\}=\{R,W\}\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}, \tag{2.20}$$

[1] Operator I_W must be constructed using "oracle".

and A is put in the form

$$A=\sqrt{\frac{2^n-1}{2^n}}R+\sqrt{\frac{1}{2^n}}W=\left(\cos\frac{\theta}{2}\right)R+\left(\sin\frac{\theta}{2}\right)W. \tag{2.21}$$

A point to make here is that G is represented as a rotation operator in $\mathrm{span}_{\mathbb{C}}\{\mathrm{R},\mathrm{W}\}$. By carrying out successive G-operations on A, we obtain

$$G^k(A)=\left\{\cos\left(k+\frac{1}{2}\right)\theta\right\}R+\left\{\sin\left(k+\frac{1}{2}\right)\theta\right\}W. \tag{2.22}$$

On the assumption that the size of the data is big enough (i.e. $2^n\gg 1$), we have $\frac{\theta}{2}\simeq\sqrt{\frac{1}{2^n}}$ on account of (2.19). The amplitude of W of the state $G^k(A)$ becomes very closer to 1 when

$$k\simeq\frac{\pi}{4}\sqrt{2^n}-\frac{1}{2}, \tag{2.23}$$

so that $G^k(A)$ comes to W with a success possibility of almost 1.

In quantum computation, we can implement each unitary operator at the time of $O(1)$. We need to apply the Grover operator $O(\sqrt{2^n})$ times to find out the target state W and each application can be implemented at the time of $O(1)$, so that the total time of searching is $O(\sqrt{2^n})=O(\sqrt{N})$, where N is the size of the data array.

2.3 Searching sequence along a geodesic

The data space $(V_n)_1^m$ is endowed with a natural Riemannian metric defined by $(X_1,X_2)_\Phi=\frac{1}{m}\mathrm{Re}\left(\mathrm{tr}X_1^\dagger X_2\right)$, where X_1 and X_2 are tangent vectors to $(V_n)_1^m$ at $\Phi\in(V_n)_1^m$. Any geodesic $\Phi(t)$ in $(V_n)_1^m$ is expressed as

$$\Phi(t)=A\cos t+B\sin t, \tag{2.24}$$

where $A,B\in(V_n)_1^m$ satisfy the condition

$$(A,A)=(B,B)=1,\quad (A,B)=0. \tag{2.25}$$

As is shown in (2.22), the algorithm generates a sequence $G^k(A)$ on the data space $(V_n)_1^m$. The sequence moves on a curve

$$\Phi(t)=R\cos t+W\sin t. \tag{2.26}$$

This curve is shown to be a geodesic in the state space $(V_n)_1^m$.

3 Fibre bundle structure

We let $U(2^n)$ act on the state space $(V_n)_1^m$ to the left, and thereby endow $(V_n)_1^m$ with a natural fibre bundle structure. In the following, we assume that the number of the data to be searched is smaller than total data array, i.e. $2^n > m$.

3.1 Left $U(2^n)$ action

The unitary group $U(2^n) = \{ a \in \mathbb{C}^{2^n \times 2^n} \mid a^\dagger a = 1_{2^n} \}$ acts on $(V_n)_1^m$ to the left:

$$(a, \Phi) \in U(2^n) \times (V_n)_1^m \mapsto L_a(\Phi) = a\Phi, \tag{3.1}$$

where we note that $\langle L_a(\Phi), L_a(\Phi)\rangle = \langle \Phi, \Phi\rangle = 1$. The rank of Φ is invariant under the $U(2^n)$ action, *i.e.* $\mathrm{rank}(a\Phi) = \mathrm{rank}(\Phi)$. The orbit of $U(2^n)$ through Φ is defined to be $\mathcal{O}_\Phi = \{ a\Phi \in (V_n)_1^m \mid a \in U(2^n) \}$. The states in the orbit $\mathcal{O}_\Phi$ have the same relative-configuration as Φ, that is, the column vectors $\phi_1, \cdots, \phi_m$ of $\Phi = (\phi_1, \cdots, \phi_m)$ spread in a same shape in $\mathbb{C}^{2^n}$.

Let P be the space of positive semi-definite $m \times m$ Hermitian matrices of trace one,

$$P = \{ \rho \in \mathbb{C}^{m\times m} \mid \rho^\dagger = \rho, \mathrm{tr}\rho = 1, \rho \geq 0 \}. \tag{3.2}$$

The left quotient space $U(2^n)\backslash(V_n)_1^m$ associated with the left action is diffeomorphic with P [4]. The projection map is given by

$$\pi : \Phi \in (V_n)_1^m \to \frac{1}{m}\Phi^\dagger\Phi \in P. \tag{3.3}$$

If the action of $U(2^n)$ on $(V_n)_1^m$ were free, the $(V_n)_1^m$ would be made into a principle fibre bundle and the fibre $\pi^{-1}(\rho)$, $\rho \in P$ would be diffeomorphic to $U(2^n)$. But this is not the case. The isotropy subgroup of $U(2^n)$ at Φ, $G_\Phi = \{ g \in U(2^n) \mid g\Phi = \Phi \}$, is nontrivial and depends on the rank of Φ.

Proposition 3.1. The isotropy subgroup G_Φ at $\Phi \in (V_n)_1^m$ is isomorphic to $U(2^n - r)$, where $r := \mathrm{rank}(\Phi)$.

Proof. To prove Proposition 3.1, we need to decompose the element $\Phi \in (V_n)_1^m$. With the singular decomposition, we decompose $\Phi \in (V_n)_1^m$ into

$$\Phi = \sqrt{m} g \begin{bmatrix} \Lambda \\ O_{2^n-m,m} \end{bmatrix} h^\dagger, \tag{3.4}$$

where $g \in U(2^n)$, $h \in U(m)$, and where

$$\Lambda = \mathrm{diag}\,[\lambda_1, \cdots, \lambda_r, 0, \cdots, 0] \in \mathbb{C}^{m\times m}, \quad \sum_{j=1}^{r} \lambda_j^2 = 1,\ \lambda_j > 0. \tag{3.5}$$

The numbers $\lambda_1, \cdots \lambda_m$ are singular values of Φ. By using (3.4), G_Φ is written as

$$G_\Phi = \left\{ g \begin{bmatrix} \mathbf{1}_r & 0 \\ 0 & b \end{bmatrix} g^{-1} \,\middle|\, b \in U(2^n - r) \right\} \cong U(2^n - r). \tag{3.6}$$

□

Proposition 3.1 implies the following theorem.

Theorem 3.2. The orbit $\mathcal{O}_\Phi$ through Φ is diffeomorphic to $U(2^n)/U(2^n - r)$, where $r = \mathrm{rank}(\Phi)$.

Proof. An equivalence relation is defined on $U(2^n)$ by

$$a_1 \sim a_2 \quad \Leftrightarrow \quad a_1\Phi = a_2\Phi, \tag{3.7}$$

where

$$a_1 \sim a_2 \Leftrightarrow {}^{\exists}b \in U(2^n - r),\ a_2 = a_1 g \begin{bmatrix} \mathbf{1}_r & 0 \\ 0 & b \end{bmatrix} g^\dagger. \tag{3.8}$$

We define a right action of H_Φ on $U(2^n)$ by

$$(a, a_b) \in U(2^n) \times G_\Phi \mapsto a \cdot a_b = ag \begin{bmatrix} \mathbf{1}_r & 0 \\ 0 & b \end{bmatrix} g^\dagger \in U(2^n). \tag{3.9}$$

The map

$$[a] \in U(2^n)/G_\Phi \mapsto a\Phi \tag{3.10}$$

is a diffeomorphism. This implies that the orbit $\mathcal{O}_\Phi$ is diffeomorphic with $U(2^n)/G_\Phi \cong U(2^n)/U(2^n - r)$. □

$(V_n)_1^m$ is then stratified into strata according to the rank of Φ:

$$(V_n)_1^m = \bigcup_{r=1}^{m} V_r, \quad V_r = \{\, \Phi \in (V_n)_1^m \mid \mathrm{rank}\Phi = r \,\}. \tag{3.11}$$

The image of V_r under the projection π is

$$P_r := \pi(V_r) = \{\, \rho \in P \mid \lambda_1^2 > \cdots > \lambda_r^2 > \lambda_{r+1}^2 = \cdots = \lambda_m^2 = 0 \,\}, \tag{3.12}$$

where $\lambda_1^2 > \cdots > \lambda_m^2$ are eigenvalues of $\rho = \pi(\Phi)$. Therefore we can make $(V_n)_1^m$ into a stratified fiber bundle with m strata [7]:

$$V_r \to P_r \cong U(2^n)\backslash V_r, \quad r = 1, \cdots, m, \tag{3.13}$$

whose fibre is diffeomorphic to $U(2^n)/U(2^n - r)$.

3.2 Decomposition of the tangent space $T_\Phi(V_n)_1^m$

The action $U(2^n)$ on $(V_n)_1^m$ induces a homomorphism $\sigma : \mathrm{u}(2^n) \to \mathfrak{X}((V_n)_1^m)$ through

$$\sigma : \xi \in \mathrm{u}(2^n) \mapsto \xi^* \in \mathfrak{X}((V_n)_1^m), \quad \xi^*_\Phi = \frac{d}{dt}\exp(t\xi)\Phi\bigg|_{t=0} = \xi\Phi. \tag{3.14}$$

The vertical subspace of $T_\Phi(V_n)_1^m$ is defined to be

$$\mathrm{Ver}(\Phi) = \{\, X = \xi\Phi \in T_\Phi(V_n)_1^m \mid \xi \in \mathrm{u}(2^n) \,\}, \tag{3.15}$$

while the horizontal subspace $\mathrm{Hor}(\Phi)$ of $T_\Phi(V_n)_1^m$ is defined as the orthogonal complement of $\mathrm{Ver}(\Phi)$ with respect to the Riemannian metric of $(V_n)_1^m$. Then, an easy calculation shows that the horizontal subspace is given by

$$\mathrm{Hor}(\Phi) = \{\, X \in T_\Phi(V_n)_1^m \mid \Phi X^\dagger - X\Phi^\dagger = 0 \,\}, \tag{3.16}$$

and the tangent space $T_\Phi(V_n)_1^m$ admits an orthogonal decomposition

$$T_\Phi(V_n)_1^m = \mathrm{Ver}(\Phi) \oplus \mathrm{Hor}(\Phi). \tag{3.17}$$

3.3 Horizontal geodesic

A C^∞ curve $\Phi(t)$ in $(V_n)_1^m$ is said to be a horizontal curve if and only if the tangent vector $\dot{\Phi}(t)$ belongs to horizontal subspace $\mathrm{Hor}(\Phi(t))$ at each $\Phi(t)$. Conditions for a geodesic of $(V_n)_1^m$ to be horizontal are given in the next proposition.

Proposition 3.3. A geodesic in $(V_n)_1^m$,

$$\Phi(t) = A\cos t + B\sin t, \quad (A, A) = (B, B) = 1,\ (A, B) = 0, \tag{3.18}$$

is horizontal, if and only if

$$BA^\dagger - AB^\dagger = 0, \tag{3.19}$$

that is, the matrix $AB^\dagger$ is Hermitian.

Since the geodesic which the searching sequence $G^k(\Phi)$ traces is expressed as in (2.26), it is horizontal if and only if $WR^\dagger$ is Hermitian. On account of

$$WR^\dagger = \sqrt{\frac{2^n}{2^n-1}}WA^\dagger - \frac{1}{\sqrt{2^n-1}}WW^\dagger, \tag{3.20}$$

$WR^\dagger$ is Hermitian, if and only if $WA^\dagger$ is Hermitian. However, from the definition (2.11) and (2.12), $WA^\dagger$ is written out as

$$WA^\dagger = \frac{1}{\sqrt{2^n}}[e_t, \cdots, e_t], \quad e_t = \sum_i e_{d_i}. \tag{3.21}$$

From this, it follows that $WA^\dagger$ is not Hermitian, since we have assumed that $2^n > m$, so that this geodesic is not horizontal.

4 Connection

In this section, we treat only the principal stratum V_m, which is made into a fibre bundle $V_m \to P_m$. We then give connection and a connection form on it.

4.1 Connection

For $r = m$, the space V_m is an open sub-manifold of $(V_n)_1^m$, and $T_\Phi V_m$ admits the decomposition $T_\Phi V_m = \mathrm{Ver}(\Phi) \oplus \mathrm{Hor}(\Phi)$ as given in Section 3.2. The dimension of $\mathrm{Hor}(\Phi)$ is constant on V_m, and a distribution $\Gamma : \Phi \mapsto \mathrm{Hor}(\Phi)$ is defined.

Theorem 4.1. The distribution defined above is a connection in V_m, that is, the subspace $\mathrm{Hor}(\Phi)$ of $T_\Phi V_m$ at each $\Phi \in V_m$ satisfies the following conditions:
(a) $T_\Phi V_m = \mathrm{Ver}(\Phi) \oplus \mathrm{Hor}(\Phi)$ (direct sum);
(b) $\mathrm{Hor}(a\Phi) = (L_a)_* \mathrm{Hor}(\Phi)$ for every $\Phi \in V_m$ and $a \in U(2^n)$;
(c) $\mathrm{Hor}(\Phi)$ depends differentiably on $\Phi$.
Condition (b) means that the distribution $\Gamma$ is invariant by $U(2^n)$.

This definition of the connection is an extension of the connection on a principal fibre bundle [6].

4.2 Connection form

The connection defined in the previous subsection can be described in terms of a connection form $\omega$. We define the connection form as a 1-form with values in $\mathfrak{u}(2^n)/\mathfrak{u}(2^n - m)$ instead of $\mathfrak{u}(2^n)$. The quotient space $\mathfrak{u}(2^n)/\mathfrak{u}(2^n - m)$ is defined by the equivalence relation on $\mathrm{u}(2^n)$

$$\eta_1 \sim \eta_2 \quad \Leftrightarrow \quad {}^{\exists}\gamma \in \mathrm{u}(2^n - m),\ \eta_1 = \eta_2 + \begin{bmatrix} 0 & 0 \\ 0 & \gamma \end{bmatrix}. \tag{4.1}$$

It is to be noted that the linear map $\sigma_\Phi : \xi \in \mathrm{u}(2^n) \mapsto \xi^*_\Phi = \xi\Phi \in \mathrm{Ver}(\Phi)$ is not injective, where ξ^* is the vector field defined in (3.14). In contrast to this, σ is injective in the case of principal fibre bundles. Because of the non-injectivity, we cannot expect that the equation $\omega(\xi^*) = \xi$ holds, which is one of the defining equations for ω to be a connection form on a principal fibre bundle.

Factoring out the kernel of σ_Φ with Φ expressed as in (3.4),

$$\ker(\sigma_\Phi) = \left\{ \xi = g \begin{bmatrix} 0 & 0 \\ 0 & \gamma \end{bmatrix} g^\dagger \,\middle|\, \gamma \in \mathrm{u}(2^n - m) \right\}, \tag{4.2}$$

we can make the map σ_Φ into a bijection σ'_Φ,

$$\sigma'_\Phi : [\xi] \in \mathrm{u}(2^n)/\ker(\sigma_\Phi) \to \xi\Phi \in \mathrm{Ver}(\Phi), \tag{4.3}$$

where the quotient space $\mathrm{u}(2^n)/\ker(\sigma_\Phi)$ is of course defined by another equivalence relation on $\mathrm{u}(2^n)$,

$$\eta_1 \sim_\Phi \eta_1 \quad \Leftrightarrow \quad {}^{\exists}\xi \in \ker(\sigma_\Phi),\ \eta_1 = \eta_2 + \xi. \tag{4.4}$$

Proposition 4.2. The $\mathrm{u}(2^n)/\ker(\sigma_\Phi)$ is isomorphic with $\mathrm{u}(2^n)/\mathrm{u}(2^n - m)$ under the isomorphism [2] defined as

$$\mathrm{Ad}_g : [\xi] \in \mathrm{u}(2^n)/\mathrm{u}(2^n - m) \mapsto [g\xi g^\dagger] \in \mathrm{u}(2^n)/\ker(\sigma_\Phi). \tag{4.5}$$

We define a map $\tilde{\sigma}_\Phi$ from $\mathrm{u}(2^n)/\mathrm{u}(2^n - m)$ to $\mathrm{Ver}(\Phi)$ by

$$\tilde{\sigma}_\Phi = \sigma'_\Phi \circ \mathrm{Ad}_g. \tag{4.6}$$

Since both Ad_g and σ'_Φ are bijections, $\tilde{\sigma}_\Phi$ becomes a bijection, and thereby we can define a $\mathrm{u}(2^n)/\mathrm{u}(2^n - m)$ valued 1-form ω on V_m through

$$\omega_\Phi(X) = (\tilde{\sigma}_\Phi)^{-1}(X_{\mathrm{Ver}}), \tag{4.7}$$

where X_{Ver} denotes the vertical component of $X \in T_\Phi V_m$. The ω is the connection form for the connection defined in the previous subsection.

[2] This difformorphism is well-defined since $g\eta_1 g^\dagger = g\eta_2 g^\dagger + g \begin{bmatrix} 0 & 0 \\ 0 & \gamma \end{bmatrix} g^\dagger \Rightarrow g\eta_1 g^\dagger \sim_\Phi g\eta_2 g^\dagger$ if $\eta_1 \sim \eta_2 \in \mathrm{u}(2^n)$.

4.3 Explicit expression of the connection form

We define a linear map $\tilde{A}_\Phi$ of $\mathrm{u}(2^n)/\mathrm{u}(2^n-m)$ to $\mathrm{u}(2^n)$ by

$$\tilde{A}_\Phi([\xi]) = \mathrm{Ad}_g(\xi)\Phi\Phi^\dagger + \Phi\Phi^\dagger\mathrm{Ad}_g(\xi) = g\xi g^\dagger\Phi\Phi^\dagger + \Phi\Phi^\dagger g\xi g^\dagger, \tag{4.8}$$

where g is the matrix appearing in the singular decomposition of Φ. The $\tilde{A}_\Phi$ is an extension of the inertia tensor for a multi-body system. According to the singular decomposition, we have $\Phi\Phi^\dagger = mg\begin{bmatrix}\Lambda^2 & 0\\ 0 & 0\end{bmatrix}g^\dagger$ and further

$$\tilde{A}_\Phi([\xi]) = mg\begin{bmatrix}\Lambda^2\alpha + \alpha\Lambda^2 & -\Lambda^2\beta^\dagger\\ \beta\Lambda^2 & 0\end{bmatrix}g^\dagger, \tag{4.9}$$

where $[\xi] \in \mathrm{u}(2^n)/\mathrm{u}(2^n-m)$ is expressed as

$$[\xi] = \left\{\xi = \begin{bmatrix}\alpha & -\beta^\dagger\\ \beta & \gamma\end{bmatrix}\middle|\, \gamma \in \mathrm{u}(2^n-m)\right\}, \quad \alpha \in \mathrm{u}(m),\ \beta \in \mathbb{C}^{(2^n-m)\times m}. \tag{4.10}$$

$\tilde{A}_\Phi$ is well-defined since γ is not included in the R.H.S. of (4.9). Since $\ker(\tilde{A}_\Phi) = \{\,[0]\,\}$, there exists the inverse map $\tilde{A}_\Phi^{-1} : \mathrm{im}\tilde{A}_\Phi \to \mathrm{u}(2^n)/\mathrm{u}(2^n-m)$.

Theorem 4.3. The connection form ω defined by (4.7) is rewritten as

$$\omega_\Phi(X) = \tilde{A}_\Phi^{-1}\left(X\Phi^\dagger - \Phi X^\dagger\right), \quad X \in T_\Phi V_m. \tag{4.11}$$

Proof. For $X \in T_\Phi V_m$, we set $\omega_\Phi(X) = [\xi]$. The vertical component of X is written as $\tilde{\sigma}_\Phi([\xi]) = g\xi g^\dagger\Phi$, while the horizontal component X_{Hor} should satisfy $\Phi X_{\mathrm{Hor}}^\dagger - X_{\mathrm{Hor}}\Phi^\dagger = 0$. For $X = g\xi g^\dagger\Phi + X_{\mathrm{Hor}}$, we have

$$X\Phi^\dagger - \Phi X^\dagger = g\xi g^\dagger\Phi\Phi^\dagger + \Phi\Phi^\dagger g\xi g^\dagger + X_{\mathrm{Hor}}\Phi^\dagger - \Phi X_{\mathrm{Hor}}^\dagger = \tilde{A}_\Phi([\xi]). \tag{4.12}$$

Therefore, $X\Phi^\dagger - \Phi X^\dagger \in \mathrm{im}\tilde{A}_\Phi$ and $\tilde{A}_\Phi^{-1}\left(X\Phi^\dagger - \Phi X^\dagger\right) = [\xi] = \omega(X)$. □

We can write out the connection form explicitly by using (4.11). We put $X \in T_\Phi V_m$ in the form $X = \sqrt{m}g\begin{bmatrix}v\\ w\end{bmatrix}h^\dagger$, where $v \in \mathbb{C}^{m\times m}$ and $w \in \mathbb{C}^{(2^n-m)\times m}$. We then have

$$X\Phi^\dagger - \Phi X^\dagger = mg\begin{bmatrix}v\Lambda - \Lambda v^\dagger & -\Lambda w^\dagger\\ w\Lambda & 0\end{bmatrix}g^\dagger \in \mathrm{im}(\tilde{A}_\Phi). \tag{4.13}$$

Setting $\omega_\Phi(X) = [\xi]$ and comparing (4.13) with (4.9), we can find that $\alpha \in \mathrm{u}(m)$ and $\beta \in \mathbb{C}^{(2^n-m)\times m}$ are determined as follows: Since $\Lambda^2\alpha + \alpha\Lambda^2 = v\Lambda - \Lambda v^\dagger$ and

$$(\alpha)_{ij} = \frac{1}{\lambda_i^2 + \lambda_j^2}\left(\lambda_j(v)_{ij} - \lambda_i\overline{(v)_{ji}}\right) \tag{4.14}$$

and since $\beta\Lambda^2 = w\Lambda$,

$$(\beta)_{ij} = \frac{1}{\lambda_j}(w)_{ij}. \tag{4.15}$$

Using these α and β, we express $\omega(X) \in \mathrm{u}(2^n)/\mathrm{u}(2^n - m)$ in an explicit manner:

$$\omega_\Phi(X) =$$

$$\left[\begin{pmatrix} \frac{i(\mathrm{Im} v_{11})}{\lambda_1} & \frac{\lambda_2 v_{12} - \lambda_1 \overline{v_{21}}}{\lambda_1^2+\lambda_2^2} & \cdots & \frac{\lambda_m v_{1m} - \lambda_1 \overline{v_{m1}}}{\lambda_1^2+\lambda_m^2} & -\frac{\overline{w_{11}}}{\lambda_1} & -\frac{\overline{w_{21}}}{\lambda_1} & \cdots & -\frac{\overline{w_{2^n-m,1}}}{\lambda_1} \\ \frac{\lambda_1 v_{21} - \lambda_2 \overline{v_{12}}}{\lambda_1^2+\lambda_2^2} & \frac{i(\mathrm{Im} v_{22})}{\lambda_2} & \cdots & \frac{\lambda_m v_{2m} - \lambda_1 \overline{v_{m2}}}{\lambda_2^2+\lambda_m^2} & -\frac{\overline{w_{12}}}{\lambda_2} & -\frac{\overline{w_{22}}}{\lambda_2} & \cdots & -\frac{\overline{w_{2^n-m,2}}}{\lambda_2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{\lambda_1 v_{m1} - \lambda_m \overline{v_{1m}}}{\lambda_1^2+\lambda_m^2} & \frac{\lambda_2 v_{m1} - \lambda_m \overline{v_{1m}}}{\lambda_2^2+\lambda_m^2} & \cdots & \frac{i(\mathrm{Im} v_{mm})}{\lambda_m} & -\frac{\overline{w_{1m}}}{\lambda_m} & -\frac{\overline{w_{2m}}}{\lambda_m} & \cdots & -\frac{\overline{w_{2^n-m,m}}}{\lambda_m} \\ \frac{w_{11}}{\lambda_1} & \frac{w_{12}}{\lambda_2} & \cdots & \frac{w_{1m}}{\lambda_m} & 0 & 0 & \cdots & 0 \\ \frac{w_{21}}{\lambda_1} & \frac{w_{22}}{\lambda_2} & \cdots & \frac{w_{2m}}{\lambda_m} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{w_{2^n-m,1}}{\lambda_1} & \frac{w_{2^n-m,2}}{\lambda_2} & \cdots & \frac{w_{2^n-m,m}}{\lambda_m} & 0 & 0 & \cdots & 0 \end{pmatrix}\right]. \tag{4.16}$$

4.4 Carrying a curve into a horizontal one

Let $\Phi(t)$ be a C^∞ curve on V_m. We would like to find a one-parameter group $a(t) \in U(2^n)$ which carries $\Phi(t)$ into a horizontal curve $\Psi(t) = a(t)\Phi(t)$. We assume that $\Phi(t)$ is decomposed as $\Phi(t) = \sqrt{m}\begin{bmatrix}\Lambda(t) \\ 0\end{bmatrix} h(t)^\dagger$ without loss of generality, because $g(t)$ can be incorporated in $a(t)$.

The horizontal subspace of $T_\Phi V_m$ is given by $\mathrm{Hor}(\Phi) = \{\, X \in T_\Phi V_m \,|X\Phi^\dagger - \Phi X^\dagger = 0 \,\}$. It then follows that $\Psi(t) = a(t)\Phi(t)$ is horizontal if and only if

$$\dot{\Psi} \in \mathrm{Hor}(\Psi) = (L_a)_* \mathrm{Hor}(\Phi), \tag{4.17}$$

that is,

$$a^\dagger \dot{\Psi} = a^\dagger \dot{a} \Phi + \dot{\Phi} \in \mathrm{Hor}(\Phi). \tag{4.18}$$

This implies that

$$\Phi\Phi^\dagger \left(a^\dagger \dot{a}\right) + \left(a^\dagger \dot{a}\right) \Phi\Phi^\dagger = \Phi\dot{\Phi}^\dagger - \dot{\Phi}\Phi^\dagger, \tag{4.19}$$

since $a^\dagger \dot{a}$ belongs to $\mathrm{u}(2^n)$. We note here that if $a(t) \in G_\Phi = U(2^n - m)$, the isotropy subgroup at $\Phi(t)$, $\Phi(t)$ is fixed, so that $\Psi(t)$ will not be expected to be horizontal. Thus, we may assume that $[a^\dagger \dot{a}]$ is non-trivial in general. Using the linear operator $\tilde{A}_\Phi$ defined by Eq. (4.8), we express this condition as $\tilde{A}_\Phi\left([a^\dagger \dot{a}]\right) = \Phi\dot{\Phi}^\dagger - \dot{\Phi}\Phi^\dagger$, so that

$$[a^\dagger \dot{a}] = -\tilde{A}_\Phi^{-1}\left(\dot{\Phi}\Phi^\dagger - \Phi\dot{\Phi}^\dagger\right). \tag{4.20}$$

Eventually, we have a differential equation on the quotient space $\mathrm{u}(2^n)/\mathrm{u}(2^n - m)$:

$$[a^\dagger \dot{a}] = -\omega(\dot{\Phi}). \tag{4.21}$$

It is possible to solve the equation on giving a certain representative element.

The tangent vector to the curve $\Phi(t)$ is put in the form $\dot{\Phi}(t) = \sqrt{m}\begin{bmatrix}\dot{\Lambda} + \Lambda\dot{h}^\dagger h \\ 0\end{bmatrix} h^\dagger$. Hence, if we set $\omega(\dot{\Phi}) = \begin{bmatrix}\alpha & -\beta^\dagger \\ \beta & \gamma\end{bmatrix}$, we have $\beta = 0 \in \mathbb{C}^{(2^n-m)\times m}$ from Eq. (4.15). Similarly, $\alpha \in \mathrm{u}(m)$ is determined by Eq. (4.14). If we assume that

$$\dot{h}^\dagger h = 0, \tag{4.22}$$

we have $\alpha = 0$. Then, (4.21) reduces to

$$[a^\dagger \dot{a}] = O \quad \Leftrightarrow \quad \dot{a} = a\begin{bmatrix}0 & 0 \\ 0 & \gamma\end{bmatrix}. \tag{4.23}$$

The solution is expressed as $a(t) = a(0)\begin{bmatrix}0 & 0 \\ 0 & c(t)\end{bmatrix}$. The curve $\Psi(t) = \sqrt{m}a\begin{bmatrix}\Lambda \\ 0\end{bmatrix}h^\dagger$ becomes horizontal for arbitrary constant $a \in U(2^n)$, since $\begin{bmatrix}0 & 0 \\ 0 & c(t)\end{bmatrix}$ gives no effect on $\Phi(t)$.

4.5 Horizontal curve from the search geodesic

We take up the geodesic (2.26) for the search algorithm to make it into a horizontal curve. We first make a singular decomposition of the geodesic.

Proposition 4.4. For $t \in [\frac{\theta}{2}, \frac{\theta}{2} + \pi]$, the geodesic (2.26) admits the singular decomposition:

$$\Phi(t) = \sqrt{m}g(t)\begin{bmatrix}\Lambda(t) \\ O_{2^n-m,m}\end{bmatrix}h^\dagger, \tag{4.24}$$

where $h \in [\boldsymbol{h}_1, \cdots, \boldsymbol{h}_m] \in U(m)$ is given by $\boldsymbol{h}_1 = \frac{1}{\sqrt{m}}[1, \cdots, 1]^{\mathsf{T}}$, and by a system $\{\boldsymbol{h}_2, \cdots, \boldsymbol{h}_m\}$ which forms an orthonormal basis of the $(m-1)$-dimensional subspace of $\mathbb{C}^m$ which is perpendicular to $\boldsymbol{h}_1$, and where $\Lambda(t)$ is expressed as

$$\begin{aligned} \Lambda(t) &= \operatorname{diag}[\lambda_1(t), \lambda_2(t), \cdots, \lambda_2(t)], \\ \lambda_1(t) &= \sqrt{\cos^2\left(t - \frac{\theta}{2}\right) + \frac{2^n - m}{m(2^n - 1)} \sin^2\left(t - \frac{\theta}{2}\right)}, \\ \lambda_2(t) &= \sqrt{\frac{2^n}{m(2^n - 1)}} \sin\left(t - \frac{\theta}{2}\right). \end{aligned} \tag{4.25}$$

The column vectors $\boldsymbol{h}_2, \cdots, \boldsymbol{h}_m$ are expressed with $V_1 \in U(m-1)$ as

$$[\boldsymbol{h}_2, \cdots, \boldsymbol{h}_m] = HV_1, \tag{4.26}$$

where H is the $m \times (m-1)$ matrix given by

$$H = \begin{bmatrix} -\frac{m-1}{\sqrt{(m-1)m}} & 0 & \cdots & 0 \\ \frac{1}{\sqrt{(m-1)m}} & \ddots & \ddots & \vdots \\ \vdots & \ddots & -\frac{2}{\sqrt{2\cdot3}} & 0 \\ \frac{1}{\sqrt{(m-1)m}} & \ddots & \frac{1}{\sqrt{2\cdot3}} & -\frac{1}{\sqrt{1\cdot2}} \\ \frac{1}{\sqrt{(m-1)m}} & \ddots & \frac{1}{\sqrt{2\cdot3}} & \frac{1}{\sqrt{1\cdot2}} \end{bmatrix}. \tag{4.27}$$

Since the assumption (4.22) is satisfied, $\Psi(t) = \sqrt{m}a \begin{bmatrix} \Lambda \\ 0 \end{bmatrix} h^\dagger$ becomes horizontal for arbitrary constant $a \in U(2^n)$. [3]

We request the horizontal curve $\Psi(t)$ to start with the same point as the original curve: $\Psi(\frac{\theta}{2}) = \Phi(\frac{\theta}{2}) = A$. The initial state A admits a singular decomposition:

$$A = \sqrt{m}g \begin{bmatrix} \Lambda_A \\ O_{2^n - m, m} \end{bmatrix} h^\dagger, \quad \Lambda_A = \operatorname{diag}[1, 0, \cdots, 0], \tag{4.28}$$

where $g = [\boldsymbol{g}_1, \cdots, \boldsymbol{g}_{2^n}]$ is given by

$$\boldsymbol{g}_1 = \frac{1}{\sqrt{2^n}}[1, \cdots, 1]^{\mathsf{T}}, \tag{4.29}$$

[3] The reason why $h \in U(m)$ is constant is that three matrix $W^\dagger W$, $A^\dagger A$ and $(A^\dagger W + W^\dagger A)$ are diagonalized by same unitary matrix.

and by $\{\boldsymbol{g}_2, \cdots, \boldsymbol{g}_{2^n}\}$ which forms an orthonormal basis of subspace which is perpendicular to $\boldsymbol{g}_1$ and is expressed as

$$[\boldsymbol{g}_2, \cdots, \boldsymbol{g}_m] = KV_2, \tag{4.30}$$

by using $V_2 \in U(2^n - 1)$ and where the $2^n \times (2^n - 1)$ matrix $K$ given by

$$K = \begin{bmatrix} -\frac{2^n-1}{\sqrt{(2^n-1)2^n}} & 0 & \cdots & 0 \\ \frac{1}{\sqrt{(2^n-1)2^n}} & \ddots & \ddots & \vdots \\ \vdots & \ddots & -\frac{2}{\sqrt{2\cdot 3}} & 0 \\ \frac{1}{\sqrt{(2^n-1)2^n}} & \ddots & \frac{1}{\sqrt{2\cdot 3}} & -\frac{1}{\sqrt{1\cdot 2}} \\ \frac{1}{\sqrt{(2^n-1)2^n}} & \ddots & \frac{1}{\sqrt{2\cdot 3}} & \frac{1}{\sqrt{1\cdot 2}} \end{bmatrix}. \tag{4.31}$$

Hence, the horizontal curve defined, by using this $g$, to be

$$\Psi(t) = \sqrt{m} g \begin{bmatrix} \Lambda(t) \\ O_{2^n - m, m} \end{bmatrix} h^\dagger, \quad t \in \left[\frac{\theta}{2}, \frac{\theta}{2} + \pi\right] \tag{4.32}$$

satisfies $\Psi(\frac{\theta}{2}) = A$. The horizontal curve $\Psi(t)$ is put in the form

$$\begin{aligned} \Psi(t) &= \sqrt{m} \begin{bmatrix} \boldsymbol{g}_1 & KV_2 \end{bmatrix} \begin{bmatrix} \mathrm{diag}\{\lambda_1, \lambda_2, \ldots, \lambda_2\} \\ O \end{bmatrix} \begin{bmatrix} \boldsymbol{h}_1 & HV_1 \end{bmatrix}^\dagger \\ &= \sqrt{m} \left(\lambda_1 \left(\boldsymbol{g}_1 \boldsymbol{h}_1^\dagger\right) + \lambda_2 KVH^\dagger\right) \\ &= \sqrt{m} \left(\lambda_1 \frac{1}{\sqrt{m}} A + \lambda_2 KVH^\dagger\right), \end{aligned} \tag{4.33}$$

where $V = \left(V_2 \begin{bmatrix} V_1^\dagger \\ O \end{bmatrix}\right)$. Since $V_1 \in U(m-1)$ and $V_2 \in U(2^n)$ are arbitrary, the matrix $V$ is an arbitrary $(2^n - 1) \times (m - 1)$ matrix satisfying $V^\dagger V = \mathbf{1}_{(m-1)}$.

5 Horizontalization of the algorithm

5.1 Purpose

One of problems in performing the search algorithm is that we have to control too much parameters. It would be preferable to reduce them for implementing the algorithm on the real quantum computer.

When we express the element of $(V_n)_1^m$ as

$$\Phi = [\phi_1, \cdots, \phi_m] \in (V_n)_1^m, \tag{5.1}$$

using m column vectors $\phi_i \, (i = 1, \cdots, m)$, the norm $||\phi_i||$ of each column vector is proved to be invariant under Grover's algorithm. Hence, it is reasonable to recognize that each column vector expresses a state of an n-qubit register. The operations given in Grover's algorithm are expressed as

$$\Phi \mapsto [a_1\phi_1, \cdots, a_m\phi_m], \quad a_i \in U(2^n), \tag{5.2}$$

which means that we control the registers one by one (Fig.5.1). Since each elements of $U(2^n)$ includes $(2^n)^2 = 4^n$ real parameters, We have to control at most $4^n \times m$ parameters, which seems too much from the viewpoint of implementation. Actually we don't use all the parameters, but the Grover operators should be designed to bring the initial state A to all the possible target states, W_d, $d \in D$, where D is the set of all the labels.

We here use the idea of the left $U(2^n)$ action,

$$L_a(\Phi) = a\Phi = [a\phi_1, \cdots, a\phi_m]. \tag{5.3}$$

The operation $\Phi \mapsto L_a(\Phi)$ means that all the n-qubit registers are controlled by the same unitary operator $a \in U(2^n)$ (Fig. 5.2). The operation L_a has only 4^n parameters, which is m times less than ordinary operations (5.2), so that it would be easy to move the state in the same orbit of left $U(2^n)$ action. It is to be noted that all the target states are lying in the same orbit. We shall refer to the orbit as the **target orbit**.

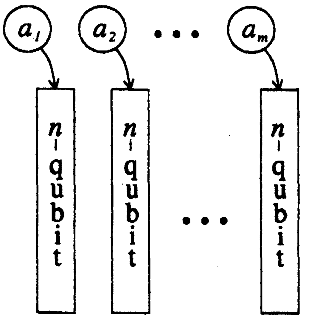

Fig. 5.1: Ordinary operations

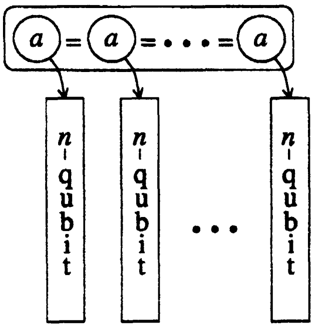

Fig. 5.2: Operations by same operator

We construct a new algorithm taking the above characteristics into account. Our algorithm is broken up into two parts. First, we reach the target orbit from the initial point A with less steps than the ordinary algorithm by a horizontalized Grover algorithm. The point A' of arrival in the target orbit is called the **relay state**, which is the nearest point from the initial point A. Then, we proceed to perform the search algorithm in the target orbit. The sketch of the original algorithm and that of the new algorithm are described as in Fig. 5.3, and Fig. 5.4, respectively.

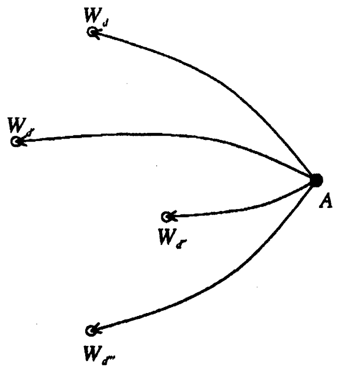

Fig. 5.3: The Original algorithm

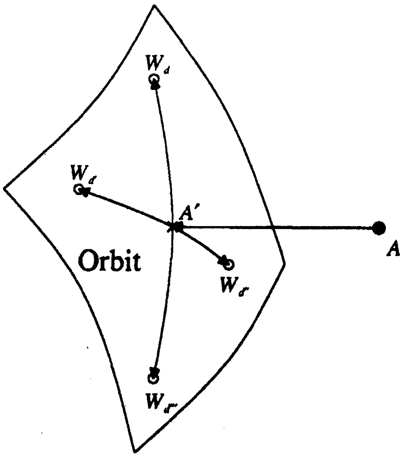

Fig. 5.4: The new algorithm

5.2 Generalization of the Grover operator

Grover's algorithm connects two states A and $W_d, d \in D$, by the Grover operator $G = -I_A \circ I_{W_d}$, where D is the set of all the labels. The operator G rotates quantum states on the plane $\mathrm{span}_{\mathbb{C}}\{A, W_d\}$. If we are given an arbitrary initial state Ψ_1 and an arbitrary target state Ψ_2 under the condition that $(\Psi_1, \Psi_2) \neq 0$, we can perform a rotation operation on $\mathrm{span}_{\mathbb{C}}\{\Psi_1, \Psi_2\}$.

The generalized Grover operator is given by

$$G = -I_{\Psi_1} \circ I_{\Psi_2}, \tag{5.4}$$

where $\Psi_1 \in (V_n)_1^m$, and where the unitary operators I_{Ψ_1} and I_{Ψ_2} are, respectively, defined by

$$I_{\Psi_i} : (V_n)_1^m \to (V_n)_1^m, \quad \Phi \mapsto \Phi - 2\,(\Psi_i, \Phi)\,\Psi_i \quad i = 1, 2. \tag{5.5}$$

Setting $c := (\Psi_1, \Psi_2)$, we define another state vector R by

$$R = \frac{1}{\sqrt{1-c^2}}\Psi_1 - \frac{c}{\sqrt{1-c^2}}\Psi_2. \tag{5.6}$$

We note that R and Ψ_2 form an orthonormal system. An easy calculation shows that

$$G(\Psi_2) = (1-2c^2)\Psi_2 - 2c\sqrt{1-c^2}R \tag{5.7}$$

$$G(R) = (1-2c^2)R + 2c\sqrt{1-c^2}\Psi_2. \tag{5.8}$$

On setting $\sin\frac{\theta}{2} := c$, Eqs. (5.7) and (5.8) is put in the form

$$G\{R, \Psi_2\} = \{R, \Psi_2\}\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \tag{5.9}$$

which shows that $G = -I_{\Psi_1} \circ I_{\Psi_2}$ acts as a rotation operator on $\mathrm{span}_{\mathbb{C}}\{\Psi_1, \Psi_2\}$. One applies the Grover operator G to the initial state Ψ_1 successively. Then, the sequence

$$G^k(\Psi_1) = \left\{\cos\left(k + \frac{1}{2}\right)\theta\right\} R + \left\{\sin\left(k + \frac{1}{2}\right)\theta\right\} \Psi_2 \tag{5.10}$$

is generated in $(V_n)_1^m$. If $c = (\Psi_1, \Psi_2)$ is small enough, *i.e.*, $\frac{\theta}{2} \sim c$, $G^k(\Psi_2)$ gets close to Ψ_2 when $k = \frac{\pi}{4c} - \frac{1}{2}$.

Once an initial state A' different from A is given, it is possible to construct a searching algorithm starting with A'. In choosing the initial point A', a condition must be satisfied, that is, $c = (A', W_d)$ should be independent of the label $d \in D$. This is because we must determine the number of operations k for any target state W_d before knowing where W_d is.

5.3 Relay state

Let $\mathcal{S}$ be the $U(2^n)$ orbit through the target state W_d, $d \in D$. As is easily seen, $\mathcal{S}$ is diffeomorphic to $U(2^n)/U(2^n - m)$, since the rank of the target state is m. The orbit $\mathcal{S}$ is identified with the Stiefel manifold: $\mathcal{S} = \left\{ \Phi \in \mathbb{C}^{2^n \times m} \mid \Phi^\dagger \Phi = \mathbf{1}_m \right\}$. It is to be noted that all the possible target states lie in the same orbit $\mathcal{S}$.

We wish to bring the initial state

$$A = \frac{1}{\sqrt{2^n}} \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix} \in (V_n)_1^m \tag{5.11}$$

into a state A' in the orbit $\mathcal{S}$ by using the generalized Grover operator. We will take $A' \in \mathcal{S}$ as the nearest point from A. We will prove father that A and A' are connected by a horizontal geodesic.

Our aim in this section is to prove the following theorem.

Theorem 5.1. Let $A' \in \mathcal{S} \subset (V_n)_1^m$ be

$$A' = \frac{1}{\sqrt{m}} A + KVH^\dagger, \tag{5.12}$$

where the matrices K and H are defined in Eqs. (4.31) and (4.27), respectively, and where V is an arbitrary $(2^n - 1) \times (m - 1)$ matrix which satisfies

$$V^\dagger V = \mathbf{1}_m. \tag{5.13}$$

Then, the following statements are true:

1. A' is the point in $\mathcal{S}$ nearest from the initial point A.
2. The geodesic through A' and A is horizontal.

In the final part of Section 4, we made the geodesic for the search algorithm into the horizontal curve $\Psi(t)$ given in Eq. (4.33). The curve $\Psi(t)$ reaches the target orbit at $t = \frac{\pi}{2}$, with the value A'.

The distance in the state space $(V_n)_1^m$ is defined to be the shorter length of those geodesic segments joining two unit vectors. Since the geodesic on $(V_n)_1^m$ is a great circle with radius 1, the distance is equal to the angle between two unit vectors. Therefore the distance can be evaluated by the inner product of two unit vectors.

Our task is now to find $A' \in (V_n)_1^m$ such that

$$\begin{aligned} &\text{maximize} \quad (A', A) = \frac{1}{m}\mathrm{Re}\left(\mathrm{tr}A'^{\dagger}A\right), \\ &\text{subject to} \quad A'^{\dagger}A' = \mathbf{1}_m. \end{aligned} \tag{5.14}$$

We note here that $A'^{\dagger}A' = \mathbf{1}_m \Leftrightarrow A' \in \mathcal{S}$.

We use the method of undetermined multipliers. Let Her(m) be the set of $m \times m$ Hermitian matrices. Since the constraint $A'^{\dagger}A' - \mathbf{1}_m = 0$ is an equation for the Hermitian matrix, we take a Lagrange multiplier Ω in Her(m). The Lagrangian form is defined as

$$\begin{aligned} L(A', \Omega) &= (A', A) + \left(\Omega, \left(A'^{\dagger}A' - \mathbf{1}_m\right)\right) \\ &= \frac{1}{m}\mathrm{Re}\left(\mathrm{tr}A'^{\dagger}A\right) + \frac{1}{m}\mathrm{Re}\left(\mathrm{tr}\Omega\left(A'^{\dagger}A' - \mathbf{1}_m\right)\right). \end{aligned} \tag{5.15}$$

An extremal point A' and Ω satisfy

$$\frac{\partial L}{\partial A'} = \frac{1}{m}(A + 2A'\Omega) = 0, \tag{5.16}$$

$$\frac{\partial L}{\partial \Omega} = A'^{\dagger}A' - \mathbf{1}_m = 0. \tag{5.17}$$

From these equations, we have

$$\Omega^2 = \frac{1}{4}A^{\dagger}A = \frac{1}{4}\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}. \tag{5.18}$$

Using these equations, we can reduce the problem to the following:

$$\begin{aligned}&\text{minimize} \quad \operatorname{tr}(\Omega), \\ &\text{subject to} \quad \Omega^2 = \frac{1}{4}\begin{bmatrix}1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1\end{bmatrix}.\end{aligned} \tag{5.19}$$

Lemma 5.2. The solution to the minimization problem (5.19) is given by

$$\Omega = -\frac{1}{2\sqrt{m}}\begin{bmatrix}1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1\end{bmatrix}. \tag{5.20}$$

Hereby, A and $A^\dagger$ satisfy

$$2A'\Omega + A = 0, \quad \Omega = -\frac{1}{2\sqrt{m}}\begin{bmatrix}1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1\end{bmatrix}, \tag{5.21}$$

and

$$A'^\dagger A' = \mathbf{1}_m. \tag{5.22}$$

We may put the element A' in the form $A' = sA + C$, where $s \in \mathbb{R}$ and where $C = (c_{kl}) \in \mathbb{C}^{2^n \times m}$ satisfies

$$(A, C) = 0 \quad \Leftrightarrow \quad \operatorname{Re}\sum_{k=1}^{2^n}\sum_{l=1}^{m} c_{kl} = 0. \tag{5.23}$$

Then, Eq. (5.21) implies $(1 - s\sqrt{m})\,A + 2C\Omega = 0$, so that

$$\sum_{l=1}^{m} c_{kl} = \sqrt{\frac{m}{2^n}}\left(1 - s\sqrt{m}\right). \tag{5.24}$$

Hence, from Eq.(5.23), we have

$$s = \frac{1}{\sqrt{m}}, \quad \sum_{l=1}^{m} c_{kl} = 0. \tag{5.25}$$

The second equation in Eq. (5.25) implies that C is put in the form $C = BH^\dagger$, where the matrix H defined in Eq. (4.27) and an arbitrary matrix $B \in \mathbb{C}^{2^n \times (m-1)}$. Hence, we can express the A' as

$$A' = \frac{1}{\sqrt{m}}A + BH^\dagger \tag{5.26}$$

We note here that the matrix H satisfy:

$$AH = 0, \tag{5.27}$$

$$H^\dagger H = \mathbf{1}_{m-1}, \quad HH^\dagger = \mathbf{1}_m - \frac{1}{m}\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}. \tag{5.28}$$

From Eqs. (5.17) and (5.26), we have

$$A'^\dagger A' = \frac{1}{m}A^\dagger A + \frac{1}{\sqrt{m}}\left(A^\dagger BH^\dagger + HB^\dagger A\right) + HB^\dagger BH^\dagger = \mathbf{1}_m, \tag{5.29}$$

and further

$$B^\dagger B = \mathbf{1}_{m-1} \tag{5.30}$$

by multiplying (5.29) by $H^\dagger$ and H from the left and the right, respectively. Then, we have $A^\dagger BH^\dagger + HB^\dagger A = 0$ from Eq. (5.29), and further $A^\dagger B = 0$ by multiplying $H^\dagger$ from the left. The matrix B satisfying Eq. (5.30) and $A^\dagger B = 0$ proves to be expressed as $B = KV$, where K is defined in Eq. (4.31), and where V is a $(2^n - 1) \times (m-1)$ matrix satisfying

$$V^\dagger V = \mathbf{1}_{m-1}. \tag{5.31}$$

Consequently, the matrix A' is put in the form

$$A' = \frac{1}{\sqrt{m}}A + KVH^\dagger. \tag{5.32}$$

It is easy to verify that Eq. (5.32) satisfies Eqs. (5.16) and (5.17) for any $V \in \mathbb{C}^{(2^n-1)\times(m-1)}$ subject to Eq. (5.31).

We shall prove the following proposition.

Proposition 5.3. The geodesic connecting the initial point A and the extremal point A' is horizontal, which is expressed as

$$\Phi(t) = R\cos t + A'\sin t, \tag{5.33}$$

where R is defined to be $R = \frac{1}{\sqrt{1-c^2}}A - \frac{c}{\sqrt{1-c^2}}A'$ with $c = (A, A')$.

Proof. The geodesic is horizontal if and only if $RA'^\dagger = A'R^\dagger$ on account of Eq. (3.19). This condition is equivalent to $A'A^\dagger = AA'^\dagger$. Since A is expressed as Eq. (5.12), we have

$$A'A^\dagger = \frac{1}{\sqrt{m}}AA^\dagger + KV(AH)^\dagger = \frac{1}{\sqrt{m}}AA^\dagger, \tag{5.34}$$

where we have used Eq. (5.27). In the same manner we have $AA'^\dagger = \frac{1}{\sqrt{m}}AA^\dagger$. Hence, $A'A^\dagger = AA'^\dagger$ holds. □

5.4 Horizontalization

As for the ordinary Grover's algorithm, we need $O(\sqrt{2^n})$ steps to reach the target orbit $\mathcal{S}$, because the sequence don't reach the target orbit until it reaches a target point. Hence, all the $O(\sqrt{2^n})$ steps should be implemented to the set of m registers.

The horizontal Grover's algorithm is performed by operating a generalized Grover operator,

$$G = -I_{A'} \circ I_A, \tag{5.35}$$

to the initial state A successively, where the state A' is the relay state defined in Eq. (5.12). Since we have

$$c = (A', A) = \frac{1}{\sqrt{m}}, \tag{5.36}$$

the number of operations G needed for reaching A' is equal to

$$k = \frac{\pi}{4c} - \frac{1}{2} = \frac{\pi\sqrt{m}}{2} - \frac{1}{2} = O(\sqrt{m}). \tag{5.37}$$

Since we have assumed that $2^n > m$, we can reach the target orbit $\mathcal{S}$ by less operations than the original algorithm.

5.5 Algorithm in the target orbit

The horizontal Grover's algorithm carries the initial state A into the relay state A' in the $U(2^n)$ orbit $\mathcal{S}$ through the target state W_d, $d \in D$. Now, we would like to perform the algorithm in the target orbit $\mathcal{S}$ to bring the relay state A' to the target state $W_d = [\boldsymbol{e}_{d_1}, \cdots, \boldsymbol{e}_{d_m}]$.

Our first trial is to apply the generalized Grover's search algorithm illustrated in Section 5.2 with initial state A'. A condition should be satisfied, that is, $c = (A', W_d)$ has to be independent of the label $d \in D$. For a matrix V in Eq. (5.12) such that $\mathrm{Re}(V) = O_{2^n-1,m-1}$, the condition is satisfied. However, the sequences generated by this algorithm don't run in the target orbit, so that we need to push the sequences into the target orbit somehow or other.

Our second attempt is to apply a unitary operation to the state A'. Let the state A' be put in the form $A' = [\boldsymbol{A}'_1, \cdots, \boldsymbol{A}'_m]$. Since A' and W_d are sitting in the same orbit, there exists a unitary operator a_d such that $A' = a_d W_d$. Let $a_d = [\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m]$. Then, one has $\boldsymbol{a}_{d_j} = \boldsymbol{A}'_j$. Since $A'^\dagger A' = \mathbf{1}_m$, we can form an element a in $U(2^n)$ by adding certain column vectors $\boldsymbol{A}'_{m+1}, \cdots, \boldsymbol{A}'_{2^n}$ to $\boldsymbol{A}'_1, \cdots, \boldsymbol{A}'_m$, $a' = [\boldsymbol{A}'_1, \cdots, \boldsymbol{A}'_{2^n}]$. Once a' is fixed, a_d is expressed as

$$a_d = a' P_d, \tag{5.38}$$

where $P_d \in U(2^n)$ is a matrix which represents the permutation of the column vectors of a' such that $\boldsymbol{a}_{d_j} = \boldsymbol{A}'_j$ holds. Then, we have

$$(a_d)^\dagger A' = W_d, \tag{5.39}$$

which shows that we can approach W_d by applying the unitary operator $a_d^\dagger$ to the relay state A'.

6 Conclusions

In this article, we analyzed the fibre bundle structure related to Grover's search algorithm with proposing the horizontal version of the algorithm. After a review of quantum computation and Grover's search algorithm in Section 2, we illustrated the fibre bundle structure and its connection in Section 3 and 4. Though the geodesic which the searching sequence $G^k(A)$ traces is not horizontal, we succeeded in carrying it into a horizontal curve by means of the connection form, which gave us the idea of horizontalizing the algorithm.

In Section 5, the main part of this article, we explained the meaning of the left $U(2^n)$ action from the viewpoint of control, claiming that it is easier to perform operations on the states in the same orbit. In view of this, we tried to reach the target orbit with as a few steps as possible. We found the nearest point, the relay point, in the target orbit and reached it by applying the generalized Grover operator successively, which we named "horizontal" Grover's search algorithm. Our new algorithm needs only $O(m)$ steps to reach the target orbit, while the ordinary algorithm needs $O(N)$ steps.

We here make a concluding remark on a future work. In the final part of Section 5, the unitary operation was expressed which carries the relay state to the target state. It should be implemented by a sequence of some elementary quantum gates, which was not easy to accomplish. However, it must be possible, since all the unitary operation can be implemented by the set of universal gates [1].

References

[1] M. A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information”, Cambrige University Press (2000).

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

[3] Y.Uwano, H, Hino and Y.Ishiwatari “Certain integrable system on a space associated with a quantum search algorithm”, nlin.SI/0512004.

[4] 石渡康恵, “順序付きデータの量子探索”, 京都大学大学院情報学研究科数理工学専攻 2003年度修士論文.

[5] 日野英逸, “量子探索アルゴリズムの幾何学”, 京都大学大学院情報学研究科数理工学専攻 2004年度修士論文.

[6] S. Kobayashi and K. Nomizu, “Foundations of Differntial Geometry”, Interscience Publishers (1963).

[7] T. Iwai and H. Yamaoka “Stratified reduction of many-body kinetic energy operators”, J. Math. Phys. **44**, 10 (2003).

[8] A. Miyake and M. Wadati “Geometric strategy for the optimal quantum search”, Phys. Rev. A. **64**, 042317 (2001).

[9] S. Tanimura, M. Nakahara, D. Hayashi “Exact solutions of the isoholonomic problem and the optimal control problem in holonomic quantum computation“, J. Math. Phys. **46**, 022101 (2005).