INTRODUCTION TO GRASSMANN MANIFOLDS AND QUANTUM COMPUTATION

KAZUYUKI FUJII

Received 18 October 2001 and in revised form 13 June 2002

Geometrical aspects of quantum computing are reviewed elementarily for nonexperts and/or graduate students who are interested in both geometry and quantum computation. We show how to treat Grassmann manifolds which are very important examples of manifolds in mathematics and physics. Some of their applications to quantum computation and its efficiency problems are shown. An interesting current topic of holonomic quantum computation is also covered. Also, some related advanced topics are discussed.

1. Introduction

This is a review article based on lectures given at several universities in Japan and a talk at Numazu meeting. (A meeting held by Yoshinori Machida at Numazu College of Technology to discuss recent results in geometry, mathematical physics, string theory, quantum computation, etc.) The aim is to show a somewhat unconventional, but fruitful, path connecting geometry and quantum computation, and the audience is graduate students and/or nonexperts who are interested in both of the disciplines.

The progress of quantum computation has become very remarkable after the excellent work of Shor [28] on prime factorization of integers and the work of Grover [12] on quantum database searching. These discoveries have had great impact on scientists. They drove not only theoreticians to find other quantum algorithms, but also experimentalists to build practical quantum computers. For standard introduction, see for example, [13, 17, 26, 29].

Journal of Applied Mathematics 2:8 (2002) 371–405
2000 Mathematics Subject Classification: 15A69, 15A90, 53C29, 53C30, 53C80, 81P68, 81Q70
URL: http://dx.doi.org/10.1155/S1110757X02110163

The conventional methods of quantum computation are more or less algebraic. On the other hand, we are interested in geometrical or topological methods. Geometry or topology are crucial to understanding mathematical or physical objects from the global point of view.

For general introduction of geometry and topology, [18] is strongly recommended. Although, the volume calculations of some important manifolds, like Grassmann ones or more generally symmetric spaces, are missing. They are important to the understanding of entanglements or entangled measures. In Sections 2, 3, and 4, we show in some detail the volume calculations of Grassmann manifolds. Here, we recall some basic concepts.

A homogeneous space is defined by

$$M \cong G/H, \tag{1.1}$$

where G is a Lie group and H is its subgroup. We are particularly interested in the case where G is a classical group (e.g., a unitary group $U(n)$ or an orthogonal group $O(n)$). The complex Grassmann manifold $G_{k,n}(\mathbb{C})$, which is our main concern in this paper, is written as

$$G_{k,n}(\mathbb{C}) \cong \frac{U(n)}{U(k)\times U(n-k)}. \tag{1.2}$$

The volume of $G_{k,n}$ is expressed in terms of the well-known volume of $U(n)$

$$\mathrm{Vol}\left(G_{k,n}(\mathbb{C})\right) = \frac{\mathrm{Vol}\left(U(n)\right)}{\mathrm{Vol}\left(U(k)\right)\times \mathrm{Vol}\left(U(n-k)\right)}. \tag{1.3}$$

This is the usual method to obtain the volume of homogeneous spaces.

On the other hand, the volume is obtained by integrating the volume form of Grassmann manifolds (: $dv(Z,Z^\dagger)$) that is expressed in terms of local coordinates (: Z)

$$\mathrm{Vol}\left(G_{k,n}(\mathbb{C})\right) = \int_{G_{k,n}(\mathbb{C})} dv(Z,Z^\dagger). \tag{1.4}$$

Is it really possible (practically) to carry out the integral on the right-hand side? As far as we know, such a calculation has not been performed except for $k = 1$ (the case of complex projective spaces). For $k \geq 2$, direct calculation seems to be very complicated. We would like to present this calculation as a challenging problem to the reader.

Now, we return to quantum computation (QC briefly).

Gauge theories are widely recognized as the basic ingredients of quantum field theories which have enjoyed remarkable progress recently, that is, String Theory, M-Theory, F-Theory, and so forth. Therefore, it is very natural to incorporate gauge theoretical ideas to QC; that is, the construction of *gauge theoretical* quantum computation and/or of *geometric* quantum computation in our terminology. The merit of geometric (or topological) method of QC may be the stability with respect to the influence from the environment.

In [22, 31], Zanardi and Rasetti proposed an attractive idea—*holonomic quantum computation*—using the non-abelian Berry phase (quantum holonomy in the mathematical terminology). We introduce this concept in the final section. See also [16, 24] for another interesting geometric model.

Quantum computation comprises many subjects. To give a comprehensive overview is beyond the scope of this paper, so we focus our attention on the construction and the efficiency of unitary operations, and give geometric interpretation to them. Here, we make a brief review.

For $n = 2^t$ $(t \in \mathbb{N})$ we set a unitary operation

$$U_f : (\mathbb{C}^2)^{\otimes t} \longrightarrow (\mathbb{C}^2)^{\otimes t}; \quad U_f(|a\rangle) = (-1)^{f(a)}|a\rangle, \tag{1.5}$$

where f is a signature function defined by

$$f : \{0,1,\dots,n-1\} \longrightarrow \mathbb{Z}_2 = \{0,1\}, \quad a \longmapsto f(a), \tag{1.6}$$

$$\begin{aligned} |a\rangle &\equiv |a_1\rangle \otimes |a_2\rangle \otimes \cdots |a_{t-1}\rangle \otimes |a_t\rangle, \quad a_k \in \mathbb{Z}_2, \\ a &= a_1 2^{t-1} + a_2 2^{t-2} + \cdots + a_{t-1}2 + a_t, \quad 0 \le a \le n-1. \end{aligned} \tag{1.7}$$

This operation plays a crucial role in the quantum database searching algorithm of Grover [12], and an important role in quantum computing in general. Our concern is to find out whether it is possible to construct this operator in an efficient manner (steps polynomial in t), and has such an algorithm been already given in quantum computation?

As far as we know, this point is rather unclear (see [1, 9, 11]). We will discuss this point in some detail.

We would like to construct a road connecting geometry and quantum computation, which is not an easy task. We will show one of such attempts as explicitly as possible. Though the results given in this paper are not new, we do hope our presentation offers new perspectives, not only to students and/or nonexperts but also to experts.

2. Grassmann manifolds

Let V be a k-dimensional subspace in $\mathbb{C}^n$ $(0 \le k \le n)$. Then it is well known in linear algebra that there is only one projection $P : \mathbb{C}^n \to \mathbb{C}^n$ with $V = P(\mathbb{C}^n)$. Here the projection means $P^2 = P$ and $P^\dagger = P$ in $M(n;\mathbb{C})$.

The Grassmann manifold is defined, in this case, by all the k-dimensional subspaces in $\mathbb{C}^n$, and it is identified with all the projections in $M(n;\mathbb{C})$ with the trace k or the rank k (corresponding to $V = P(\mathbb{C}^n)$). We note that the eigenvalues of a projection are either 0 or 1 (by $P^2 = P$), so the rank of P = trace of P. Therefore we arrive at

$$G_{k,n}(\mathbb{C}) = \{P \in M(n;\mathbb{C}) \mid P^2 = P,\ P^\dagger = P,\ \operatorname{tr} P = k\}. \tag{2.1}$$

In general, it is not easy to visualize all the k-dimensional subspaces in $\mathbb{C}^n$ except for experts in geometry. But it is easy to deal with (2.1) as will be shown in the following.

We note that $G_{0,n}(\mathbb{C}) = \{\mathbf{0}_n\}$ and $G_{n,n}(\mathbb{C}) = \{\mathbf{1}_n\}$. In particular, $G_{1,n}(\mathbb{C})$ is called a complex projective space and is written as $\mathbb{C}P^{n-1}$. In (2.1), we know a natural symmetry (isomorphism)

$$\kappa : G_{k,n}(\mathbb{C}) \longrightarrow G_{n-k,n}(\mathbb{C}), \quad \kappa(P) = \mathbf{1}_n - P, \tag{2.2}$$

so that we have $G_{k,n}(\mathbb{C}) \cong G_{n-k,n}(\mathbb{C})$.

Now it is easy to see that P can be written as

$$P = AE_kA^{-1} \quad \text{for some } A \in U(n), \tag{2.3}$$

where E_k is a special projection

$$E_k = \begin{pmatrix} \mathbf{1}_k & O \\ O & \mathbf{0}_{n-k} \end{pmatrix}. \tag{2.4}$$

Therefore, we have

$$G_{k,n}(\mathbb{C}) = \{AE_kA^{-1} \mid A \in U(n)\}, \tag{2.5}$$

which directly leads to

$$G_{k,n}(\mathbb{C}) \cong \frac{U(n)}{U(k) \times U(n-k)}. \tag{2.6}$$

In particular,

$$G_{1,n}(\mathbb{C}) = \mathbb{C}P^{n-1} \cong \frac{U(n)}{U(1)\times U(n-1)} \cong \frac{U(n)/U(n-1)}{U(1)} \cong \frac{S^{2n-1}}{S^1}, \tag{2.7}$$

see (3.2). Here S^k is the unit sphere in $\mathbb{R}^{k+1}$ and $U(1) = S^1$. We note that $G_{k,n}(\mathbb{C})$ is a complex manifold (moreover, a Kähler manifold) and its complex dimension is $k(n-k)$.

Next, we introduce local coordinates around P in (2.3). We denote by $M(n-k,k;\mathbb{C})$ the set of all $(n-k)\times k$-matrices over $\mathbb{C}$ and define a map

$$\mathcal{P} : M(n-k,k;\mathbb{C}) \longrightarrow G_{k,n}(\mathbb{C}) \tag{2.8}$$

as follows:

$$\mathcal{P}(Z) = A \begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix} \begin{pmatrix} \mathbf{1}_k & O \\ O & \mathbf{0}_{n-k} \end{pmatrix} \begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix}^{-1} A^{-1}. \tag{2.9}$$

Of course $\mathcal{P}(\mathbf{0}) = P$ in (2.3).

Here, a natural question arises. How many local coordinates do we have on $G_{k,n}(\mathbb{C})$? The number of them is just ${}_nC_k$.

We believe that this is the best choice of local coordinates on the Grassmann manifold, and this one is called the Oike coordinates in Japan. As far as the author knows, Oike is the first to write down (2.9) (see [19]).

From this we can show the curvature form $\mathcal{P}(Z)d\mathcal{P}(Z)\wedge d\mathcal{P}(Z)$:

$$\begin{aligned} d\mathcal{P}(Z) = A &\begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix} \begin{pmatrix} \mathbf{0}_k & {\Lambda_k}^{-1} dZ^\dagger \\ {M_{n-k}}^{-1} dZ & \mathbf{0}_{n-k} \end{pmatrix} \\ &\times \begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix}^{-1} A^{-1}, \end{aligned} \tag{2.10}$$

$$\begin{aligned} \mathcal{P}(Z)d\mathcal{P}(Z)\wedge d\mathcal{P}(Z) = A &\begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix} \begin{pmatrix} {\Lambda_k}^{-1} dZ^\dagger \wedge {M_{n-k}}^{-1} dZ & O \\ O & \mathbf{0}_{n-k} \end{pmatrix} \\ &\times \begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix}^{-1} A^{-1}, \end{aligned} \tag{2.11}$$

where

$$\Lambda_k = \mathbf{1}_k + Z^\dagger Z \in M(k;\mathbb{C}), \quad M_{n-k} = \mathbf{1}_{n-k} + ZZ^\dagger \in M(n-k;\mathbb{C}). \tag{2.12}$$

In the following we omit the symbol $\wedge$ and write, for example, $\mathcal{P}d\mathcal{P}d\mathcal{P}$ instead of $\mathcal{P}(Z)d\mathcal{P}(Z)\wedge d\mathcal{P}(Z)$ for simplicity. A (global) symplectic 2-form on $G_{k,n}(\mathbb{C})$ is given by

$$\omega = \operatorname{tr}\mathcal{P}d\mathcal{P}d\mathcal{P} \tag{2.13}$$

and its local form

$$\begin{aligned}\omega &= \operatorname{tr}\left(\Lambda_k^{-1}dZ^\dagger M_{n-k}^{-1}dZ\right)\\ &= \operatorname{tr}\left(\left(\mathbf{1}_k+Z^\dagger Z\right)^{-1}dZ^\dagger\left(\mathbf{1}_{n-k}+ZZ^\dagger\right)^{-1}dZ\right).\end{aligned} \tag{2.14}$$

We want to rewrite (2.14). Before doing this, we make some mathematical preliminaries. For $A\in M(m,\mathbb{C})$ and $B\in M(n,\mathbb{C})$, a tensor product $A\otimes B$ of A and B is defined as

$$A\otimes B=\left(a_{ij}B\right)\quad \text{for } A=\left(a_{ij}\right),\ B=\left(b_{pq}\right). \tag{2.15}$$

For example, for

$$A=\begin{pmatrix}a_{11}&a_{12}\\ a_{21}&a_{22}\end{pmatrix},\qquad B=\begin{pmatrix}b_{11}&b_{12}\\ b_{21}&b_{22}\end{pmatrix}, \tag{2.16}$$

we have

$$A\otimes B=\begin{pmatrix}a_{11}B&a_{12}B\\ a_{21}B&a_{22}B\end{pmatrix}=\begin{pmatrix}a_{11}b_{11}&a_{11}b_{12}&a_{12}b_{11}&a_{12}b_{12}\\ a_{11}b_{21}&a_{11}b_{22}&a_{12}b_{21}&a_{12}b_{22}\\ a_{21}b_{11}&a_{21}b_{12}&a_{22}b_{11}&a_{22}b_{12}\\ a_{21}b_{21}&a_{21}b_{22}&a_{22}b_{21}&a_{22}b_{22}\end{pmatrix}. \tag{2.17}$$

Therefore component-wise, we have $(A\otimes B)_{ip,jq}=A_{ij}B_{pq}$. Then it is not difficult to see

$$\operatorname{tr}(A\otimes B)=\operatorname{tr}(A)\operatorname{tr}(B),\qquad \det(A\otimes B)=\left\{\det(A)\right\}^n\left\{\det(B)\right\}^m. \tag{2.18}$$

We construct a column vector $\widehat{Z}$ in $\mathbb{C}^{k(n-k)}$ from Z in $M(n-k,k;\mathbb{C})$ in a usual manner

$$\widehat{Z}=\left(z_{11},\dots,z_{1k},\dots,z_{n-k,1},\dots,z_{n-k,k}\right)^T, \tag{2.19}$$

where T means a transpose. Now we rewrite (2.14) as follows:

$$\begin{aligned}
\omega &= \mathrm{tr}\,(\Lambda_k^{-1}\,dZ^\dagger M_{n-k}^{-1} dZ) \\
&= \mathrm{tr}\,(dZ^\dagger M_{n-k}^{-1} dZ \Lambda_k^{-1}) \\
&= \sum (dZ^\dagger)_{ij} (M_{n-k}^{-1})_{jp} (dZ)_{pq} (\Lambda_k^{-1})_{qi} \\
&= \sum d\bar{z}_{ji} (M_{n-k}^{-1})_{jp}\, dz_{pq} (\Lambda_k^{-1})_{qi} \\
&= \sum d\bar{z}_{ji} (M_{n-k}^{-1})_{jp} (\Lambda_k^{-1})_{qi} dz_{pq} \\
&= \sum d\bar{z}_{ji} (M_{n-k}^{-1})_{jp} (\Lambda_k^{-1})^T{}_{iq}\, dz_{pq} \\
&= \sum (d\hat{Z}^\dagger)_{ji} \left\{ M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T \right\}_{ji,pq} d\hat{Z}_{pq} \\
&= (d\hat{Z})^\dagger \left\{ M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T \right\} d\hat{Z}.
\end{aligned} \tag{2.20}$$

The symplectic volume on $G_{k,n}(\mathbb{C})$, which coincides with the usual volume, is given by

$$dv = \frac{1}{\{k(n-k)\}!} \left(\frac{\omega}{2\sqrt{-1}} \right)^{k(n-k)}. \tag{2.21}$$

Here, $1/(2\sqrt{-1})$ is a normalization factor. From (2.20) it is easy to see

$$\omega^{k(n-k)} = \{k(n-k)\}! \det \left\{ M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T \right\} \prod_{i,j} d\bar{z}_{ij} dz_{ij}. \tag{2.22}$$

Therefore, (2.21) becomes

$$dv = \det \left\{ M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T \right\} \prod_{i,j} \frac{d\bar{z}_{ij} dz_{ij}}{2\sqrt{-1}}. \tag{2.23}$$

On the other hand, by (2.18) we have

$$\begin{aligned}
\det \left\{ M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T \right\} &= (\det M_{n-k}^{-1})^k (\det (\Lambda_k^{-1}))^{n-k} \\
&= (\det M_{n-k})^{-k} (\det \Lambda_k)^{-(n-k)}.
\end{aligned} \tag{2.24}$$

Here we note $\det \Lambda_k = \det M_{n-k}$. For

$$X = \begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix}, \tag{2.25}$$

we have

$$\begin{aligned}\det X &= \det\begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix} = \det\begin{pmatrix} \mathbf{1}_k + Z^\dagger Z & -Z^\dagger \\ O & \mathbf{1}_{n-k} \end{pmatrix} \\ &= \det\left(\mathbf{1}_k + Z^\dagger Z\right) = \det \Lambda_k.\end{aligned} \tag{2.26}$$

On the other hand,

$$\begin{aligned}\det X &= \det\begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ Z & \mathbf{1}_{n-k} \end{pmatrix} = \det\begin{pmatrix} \mathbf{1}_k & -Z^\dagger \\ O & \mathbf{1}_{n-k} + ZZ^\dagger \end{pmatrix} \\ &= \det\left(\mathbf{1}_{n-k} + ZZ^\dagger\right) = \det M_{n-k},\end{aligned} \tag{2.27}$$

so that

$$\det \Lambda_k = \det M_{n-k}. \tag{2.28}$$

From (2.24), $\det\{M_{n-k}^{-1} \otimes (\Lambda_k^{-1})^T\} = (\det \Lambda_k)^{-n}$, so we arrive at

$$\begin{aligned}dv(Z, Z^\dagger) &= \left(\det \Lambda_k\right)^{-n} \prod_{i,j} \frac{d\bar{z}_{ij} dz_{ij}}{2\sqrt{-1}} \\ &= \left\{\det\left(\mathbf{1}_k + Z^\dagger Z\right)\right\}^{-n} \prod_{i,j} \frac{d\bar{z}_{ij} dz_{ij}}{2\sqrt{-1}}.\end{aligned} \tag{2.29}$$

From the above mentioned facts, the volume of Grassmann manifold $G_{k,n}(\mathbb{C})$ is given as

$$\mathrm{Vol}\left(G_{k,n}(\mathbb{C})\right) = \int_{M(n-k,k;\mathbb{C})} \frac{\prod_{i,j}\left(d\bar{z}_{ij} dz_{ij}/2\sqrt{-1}\right)}{\left\{\det\left(\mathbf{1}_k + Z^\dagger Z\right)\right\}^n}. \tag{2.30}$$

Problem 2.1. How can we calculate this integral?

3. Volume of unitary groups

Here we will show a heuristic method of evaluation of the volume of unitary group $U(n)$. Let S^{2k-1} be the $(2k-1)$-dimensional unit sphere

($k \geq 1$) over $\mathbb{R}$ and the volume be $\mathrm{Vol}(S^{2k-1})$. For example, $\mathrm{Vol}(S^1) = 2\pi$ and $\mathrm{Vol}(S^3) = 2\pi^2$. In general, we have

$$\mathrm{Vol}\left(S^{2k-1}\right) = \frac{2\pi^k}{(k-1)!}. \tag{3.1}$$

Since we know the fact

$$\frac{U(k)}{U(k-1)} \cong S^{2k-1}, \tag{3.2}$$

we have

$$\begin{aligned} U(n) &\doteq \frac{U(n)}{U(n-1)} \times \frac{U(n-1)}{U(n-2)} \times \cdots \times \frac{U(2)}{U(1)} \times U(1) \\ &\doteq S^{2n-1} \times S^{2n-3} \times \cdots \times S^3 \times S^1, \end{aligned} \tag{3.3}$$

where $\doteq$ means *almost equal*!

Of course, the equality does not hold in (3.3) except for the cases of $n = 1, 2$. But, for the purpose of volume-counting or cohomology-counting, there is no problem to use (3.3) ("questionable equation" may be rather useful, see, e.g., [25]).

Combining (3.3) and (3.1), we obtain

$$\mathrm{Vol}\left(U(n)\right) = \prod_{j=1}^{n} \mathrm{Vol}\left(S^{2j-1}\right) = \prod_{j=1}^{n} \frac{2\pi^j}{(j-1)!} = \frac{2^n \pi^{n(n+1)/2}}{0!1!\cdots(n-1)!}. \tag{3.4}$$

We evaluate the volume of Grassmann manifold $G_{k,n}(\mathbb{C})$

$$\begin{aligned} &G_{k,n}(\mathbb{C}) \cong \frac{U(n)}{U(k) \times U(n-k)} \\ &\Longrightarrow \mathrm{Vol}\left(G_{k,n}(\mathbb{C})\right) = \frac{\mathrm{Vol}\left(U(n)\right)}{\mathrm{Vol}\left(U(k)\right) \times \mathrm{Vol}\left(U(n-k)\right)}. \end{aligned} \tag{3.5}$$

From (3.4) we obtain

$$\begin{aligned} \mathrm{Vol}\left(G_{k,n}(\mathbb{C})\right) &= \frac{0!1!\cdots(k-1)!\ 0!1!\cdots(n-k-1)!}{0!1!\cdots(n-1)!} \pi^{k(n-k)} \\ &= \frac{0!1!\cdots(k-1)!}{(n-k)!\cdots(n-2)!(n-1)!} \pi^{k(n-k)}. \end{aligned} \tag{3.6}$$

4. A question

Combining (2.30) with (3.6), we have the main result

$$\int_{M(n-k,k;\mathbb{C})} \frac{\prod_{i,j}\left(d\bar{z}_{ij}dz_{ij}/2\sqrt{-1}\right)}{\left\{\det\left(\mathbf{1}_k+Z^{\dagger}Z\right)\right\}^n} = \frac{0!1!\cdots(k-1)!}{(n-k)!\cdots(n-2)!(n-1)!}\pi^{k(n-k)}. \tag{4.1}$$

It has to be emphasized that the right-hand side has been obtained by an indirect path. Is it really easy (or practical) to carry out the integration to obtain the right-hand side? As far as we know, the integral has not been calculated except for the case $k=1$.

We review the case $k=1$

$$\int_{\mathbb{C}^{n-1}} \frac{1}{\left(1+\sum_{j=1}^{n-1}\left|z_j\right|^2\right)^n}\prod_{j=1}^{n-1}\frac{d\bar{z}_j dz_j}{2\sqrt{-1}} = \frac{\pi^{n-1}}{(n-1)!}. \tag{4.2}$$

The proof of (4.2) is as follows. First we make a change of variables:

$$z_j = \sqrt{r_j}e^{\sqrt{-1}\theta_j} \quad \text{for } 1\le j\le n-1. \tag{4.3}$$

Then we have, easily,

$$\frac{d\bar{z}_j dz_j}{2\sqrt{-1}} = \frac{1}{2}dr_j d\theta_j. \tag{4.4}$$

Under this change of variables, (4.2) becomes

$$\begin{aligned}\int_0^{2\pi}\int_0^{\infty} \frac{1}{\left(1+\sum_{j=1}^{n-1}r_j\right)^n}\prod_{j=1}^{n-1}\frac{d\theta_j}{2}\prod_{j=1}^{n-1}dr_j \\ = \pi^{n-1}\int_0^{\infty}\frac{1}{\left(1+\sum_{j=1}^{n-1}r_j\right)^n}\prod_{j=1}^{n-1}dr_j.\end{aligned} \tag{4.5}$$

Here, once more, we make a change of variables from $(r_1,\ldots,r_{n-1})$ to $(\xi_1,\ldots,\xi_{n-1})$:

$$\begin{aligned} r_1 &= \xi_1(1-\xi_2),\\ r_2 &= \xi_1\xi_2(1-\xi_3),\\ &\vdots\\ r_{n-2} &= \xi_1\xi_2\cdots\xi_{n-2}(1-\xi_{n-1}),\\ r_{n-1} &= \xi_1\xi_2\cdots\xi_{n-2}\xi_{n-1}. \end{aligned} \tag{4.6}$$

Conversely, we have

$$\begin{aligned}
\xi_1 &= r_1 + r_2 + \cdots + r_{n-2} + r_{n-1},\\
\xi_2 &= \frac{r_2 + \cdots + r_{n-2} + r_{n-1}}{r_1 + r_2 + \cdots + r_{n-2} + r_{n-1}},\\
&\vdots\\
\xi_{n-2} &= \frac{r_{n-2} + r_{n-1}}{r_{n-3} + r_{n-2} + r_{n-1}},\\
\xi_{n-1} &= \frac{r_{n-1}}{r_{n-2} + r_{n-1}}, \quad 0 \le \xi_1 < \infty,\ 0 \le \xi_2, \ldots, \xi_{n-1} \le 1,\\
\prod_{j=1}^{n-1} dr_j &= {\xi_1}^{n-2} {\xi_2}^{n-3} \cdots \xi_{n-2} \prod_{j=1}^{n-1} d\xi_j.
\end{aligned} \tag{4.7}$$

Under this change of variables, (4.2) becomes

$$\begin{aligned}
&\pi^{n-1} \int_0^\infty \frac{{\xi_1}^{n-2}}{(1+\xi_1)^n}\, d\xi_1 \int_0^1 {\xi_2}^{n-3}\, d\xi_2 \cdots \int_0^1 \xi_{n-2}\, d\xi_{n-2}\\
&= \pi^{n-1} \int_0^1 {\xi_1}^{n-2}\, d\xi_1 \int_0^1 {\xi_2}^{n-3}\, d\xi_2 \cdots \int_0^1 \xi_{n-2}\, d\xi_{n-2}\\
&= \pi^{n-1} \frac{1}{n-1} \frac{1}{n-2} \cdots \frac{1}{2} = \frac{\pi^{n-1}}{(n-1)!}.
\end{aligned} \tag{4.8}$$

The direct proof of (4.1) for $k = 1$ is relatively easy as shown above. But for $k \ge 2$, we do not know such a proof (a direct proof may be very complicated). Therefore, we present the following problem.

Problem 4.1. Give a direct proof to

$$\int_{M(n-k,k;\mathbb{C})} \frac{\prod_{i,j} \left(d\bar{z}_{ij} dz_{ij} / 2\sqrt{-1}\right)}{\left\{\det\left(\mathbf{1}_k + Z^\dagger Z\right)\right\}^n} = \frac{0!1! \cdots (k-1)!}{(n-k)! \cdots (n-2)!(n-1)!} \pi^{k(n-k)}. \tag{4.9}$$

As for another approach to the above problem, we refer to [10]. In this paper, coherent states based on Grassmann manifolds have been constructed.

5. Quantum computing

We move to the main subject of quantum computing. The typical examples of quantum algorithms up to now are as follows:

(i) factoring algorithm of integers by Shor [28],
(ii) quantum database searching algorithm by Grover [12].

(See [17, 26, 29] for general introduction, [14, 15] are also recommended.)

In quantum computing we, in general, expect an exponential speedup compared to classical ones, so we must construct necessarily unitary matrices in $U(n)$ in an efficient manner when n is a huge number like 2^{100}.

Problem 5.1. How can we construct unitary matrices in an efficient manner?

We return to (2.1). We denote the set of $n \times n$ projection operators by

$$G_n(\mathbb{C}) = \{P \in M(n;\mathbb{C}) \mid P^2 = P,\ P^\dagger = P\}. \tag{5.1}$$

The elements of $G_n(\mathbb{C})$ are classified by the trace, so $G_n(\mathbb{C})$ can be decomposed into a disjoint union

$$G_n(\mathbb{C}) = \bigcup_{k=0}^{n} G_{k,n}(\mathbb{C}). \tag{5.2}$$

For a k-dimensional subspace V in $\mathbb{C}^n$ $(0 \le k \le n)$, let $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ be an orthonormal basis (namely, $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \delta_{ij}$) and set

$$V = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k) \in M(n,k;\mathbb{C}). \tag{5.3}$$

We have identified a k-dimensional subspace V with a matrix V in (5.3) for simplicity (there maybe no confusion). Then we have an equivalence

$$\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k\} : \text{orthonormal} \iff V^\dagger V = \mathbf{1}_k. \tag{5.4}$$

Then it is easy to see that all orthonormal basis in V are given by

$$\{Va \mid a \in U(k)\}. \tag{5.5}$$

The projection corresponding to V is written by

$$P = VV^\dagger \in G_{k,n}(\mathbb{C}). \tag{5.6}$$

We remark that $(Va)(Va)^\dagger = Vaa^\dagger V^\dagger = VV^\dagger = P$, namely, P is of course independent of $a \in U(k)$. This P is also expressed as

$$P = \sum_{j=1}^{k} \mathbf{v}_j \mathbf{v}_j{}^\dagger. \tag{5.7}$$

If we use Dirac bracket notation $\mathbf{v}_j = |j\rangle$, then $P = \sum_{j=1}^{k} |j\rangle\langle j|$. This notation may be popular in physics rather than (5.7).

How can we construct an element of unitary group from an element of Grassmann manifolds? We have a canonical method, namely,

$$G_n(\mathbb{C}) \longrightarrow U(n) : P \longmapsto U = 1_n - 2P. \tag{5.8}$$

This U is called a uniton in the field of harmonic maps. Moreover, we can consider a product of some unitons, namely, for any $S \subset \{0,1,\dots,n-1,n\}$

$$U = \prod_{j \in S} (1_n - 2P_j) \quad \text{for } P_j \in G_{j,n}(\mathbb{C}). \tag{5.9}$$

In particular,

$$U = \prod_{j=1}^{n-1} (1_n - 2P_j) \quad \text{for } P_j \in G_{j,n}(\mathbb{C}) \tag{5.10}$$

is very important in the field of harmonic maps, see, for example, [4, 30].

Many important unitary matrices are made this way. (Those used in [2] for database searching algorithms are of this form with appropriate P_j.)

These unitary matrices also play an important role in quantum computing as shown in the following.

We consider a qubit (*qu*antum *bit*) space of quantum particles. The 1-qubit space is identified with $\mathbb{C}^2$ with basis $\{|0\rangle, |1\rangle\}$;

$$\mathbb{C}^2 = \mathrm{Vect}_{\mathbb{C}}\{|0\rangle, |1\rangle\}, \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{5.11}$$

The qubit space of t-particles is the *tensor product* (not direct sum!) of $\mathbb{C}^2$

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \equiv \left(\mathbb{C}^2\right)^{\otimes t}, \tag{5.12}$$

with basis

$$\left\{ \left| n_1, n_2, \dots, n_t \right\rangle = \left| n_1 \right\rangle \otimes \left| n_2 \right\rangle \otimes \cdots \otimes \left| n_t \right\rangle \mid n_j \in \mathbb{Z}_2 = \{0,1\} \right\}. \tag{5.13}$$

For example,

$$|0\rangle\otimes|0\rangle=\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\qquad |0\rangle\otimes|1\rangle=\begin{pmatrix}0\\1\\0\\0\end{pmatrix},$$
$$|1\rangle\otimes|0\rangle=\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\qquad |1\rangle\otimes|1\rangle=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}. \tag{5.14}$$

Now we take the Walsh-Hadamard transformation W defined by

$$W:|0\rangle\longrightarrow\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\qquad W:|1\rangle\longrightarrow\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle), \tag{5.15}$$

in matrix notation,

$$W=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\in O(2)\subset U(2). \tag{5.16}$$

This transformation (or matrix) is unitary and it plays a very important role in quantum computing. Moreover, it is easy to realize in quantum optics. We list some important properties of W

$$W^2=\mathbf{1}_2,\qquad W^\dagger=W=W^{-1},\qquad \sigma_1=W\sigma_3W^{-1}, \tag{5.17}$$

where $\{\sigma_1,\sigma_2,\sigma_3\}$ are the Pauli matrices

$$\sigma_1=\begin{pmatrix}&1\\1&\end{pmatrix},\qquad \sigma_2=\begin{pmatrix}&-\sqrt{-1}\\\sqrt{-1}&\end{pmatrix},\qquad \sigma_3=\begin{pmatrix}1&\\&-1\end{pmatrix}. \tag{5.18}$$

See Appendix B for a generalization of Pauli matrices. Next we consider t-tensor product of W ($t\in\mathbb{N}$)

$$W^{\otimes t}=W\otimes W\otimes\cdots\otimes W\ (t\text{-times}). \tag{5.19}$$

This matrix of course operates on the space (5.12). For example,

$$W \otimes W = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$W \otimes W \otimes W = \frac{1}{\sqrt{8}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}. \tag{5.20}$$

Hereafter, we set $n = 2^t$. Then (5.19) means $W^{\otimes t} \in U(n)$. The very important fact is that (5.19) can be constructed only by $t(= \log_2(n))$-steps in quantum computing. We show the matrix-component of (5.19) that is given by

$$\langle i_1, i_2, \ldots, i_t | W^{\otimes t} | j_1, j_2, \ldots, j_t \rangle = \frac{1}{\sqrt{n}}(-1)^{\sum_{k=1}^{t} i_k j_k}, \tag{5.21}$$

or, if we set

$$|i) = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_t\rangle, \quad i = i_1 2^{t-1} + i_2 2^{t-2} + \cdots + i_t,\ 0 \le i \le n-1, \tag{5.22}$$

we have

$$(i|W^{\otimes t}|j) = \frac{1}{\sqrt{n}}(-1)^{i \cdot j}, \tag{5.23}$$

where $i \cdot j$ means the sum of bit-wise products $\sum_{k=1}^{t} i_k j_k$.

The proof goes as follows. From (5.16) we know

$$W|i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^i |1\rangle\right) = \frac{1}{\sqrt{2}}\sum_{k=0}^{1}(-1)^{ik}|k\rangle, \tag{5.24}$$

which implies that

$$\begin{aligned} W^{\otimes t}|j) &= W|j_1\rangle \otimes W|j_2\rangle \otimes \cdots \otimes W|j_t\rangle \\ &= \frac{1}{\sqrt{2^t}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_t=0}^{1} (-1)^{k_1 j_1 + k_2 j_2 + \cdots + k_t j_t} |k_1\rangle \otimes |k_2\rangle \otimes \cdots |k_t\rangle \\ &= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} (-1)^{k \cdot j} |k). \end{aligned} \tag{5.25}$$

Therefore, we obtain

$$(i|W^{\otimes t}|j) = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} (-1)^{k \cdot j} (i|k) = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} (-1)^{k \cdot j} \delta_{ik} = \frac{1}{\sqrt{n}} (-1)^{i \cdot j}. \tag{5.26}$$

Moreover, (5.19) has an interesting property which we can guess from (5.20):

$$\sum_{j=0}^{n-1} (i|W^{\otimes t}|j) = \begin{cases} \sqrt{n}, & \text{if } i = 0, \\ 0, & \text{otherwise} \end{cases} \tag{5.27}$$

or

$$\sum_{i=0}^{n-1} (i|W^{\otimes t}|j) = \begin{cases} \sqrt{n}, & \text{if } j = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{5.28}$$

We clarify the meaning of (5.23) from the point of view of group theory.

We note that $\mathbb{Z}_2$ is an abelian group with operation $\oplus$

$$0 \oplus 0 = 0, \qquad 0 \oplus 1 = 1, \qquad 1 \oplus 0 = 1, \qquad 1 \oplus 1 = 0. \tag{5.29}$$

Then ${\mathbb{Z}_2}^t$ is a natural product group of $\mathbb{Z}_2$. We denote its element by

$$\mathbf{i} = (i_1, i_1, \ldots, i_t) \longleftrightarrow i = i_1 2^{t-1} + i_2 2^{t-2} + \cdots + i_t. \tag{5.30}$$

For $\mathbf{i} \in {\mathbb{Z}_2}^t$, we define

$$\chi_{\mathbf{i}} : {\mathbb{Z}_2}^t \longrightarrow \mathbb{C}^* = \mathbb{C} - \{0\}, \qquad \chi_{\mathbf{i}}(\mathbf{j}) = \sqrt{n}(i|W^{\otimes t}|j) = (-1)^{i \cdot j}. \tag{5.31}$$

Then we can show that

$$\chi_{\mathbf{i}}(\mathbf{j} \oplus \mathbf{k}) = \chi_{\mathbf{i}}(\mathbf{j})\chi_{\mathbf{i}}(\mathbf{k}). \tag{5.32}$$

That is, $\chi_{\mathbf{i}}$ is a character of the abelian group ${\mathbb{Z}_2}^t$.

The proof is as follows. From (5.29) we know

$$x \oplus y = x + y - 2xy \quad \text{for } x, y \in \mathbb{Z}_2. \tag{5.33}$$

Therefore, we obtain

$$\begin{aligned} \chi_{\mathbf{i}}(\mathbf{j} \oplus \mathbf{k}) &= (-1)^{\sum_{l=1}^t i_l(j_l \oplus k_l)} = (-1)^{\sum_{l=1}^t i_l(j_l + k_l - 2j_l k_l)} = (-1)^{\sum_{l=1}^t i_l(j_l + k_l)} \\ &= (-1)^{\sum_{l=1}^t i_l j_l}(-1)^{\sum_{l=1}^t i_l k_l} = (-1)^{i \cdot j}(-1)^{i \cdot k} = \chi_{\mathbf{i}}(\mathbf{j})\chi_{\mathbf{i}}(\mathbf{k}). \end{aligned} \tag{5.34}$$

These characters play an important role in discrete Fourier transform, see [14] or [15].

Now we consider a controlled-NOT operation (gate) which we will denote by C-NOT in the following. It is defined by

$$\begin{aligned} \text{C-NOT} : |0,0\rangle &\longrightarrow |0,0\rangle, \quad |0,1\rangle \longrightarrow |0,1\rangle, \\ |1,0\rangle &\longrightarrow |1,1\rangle, \quad |1,1\rangle \longrightarrow |1,0\rangle, \end{aligned} \tag{5.35}$$

or more compactly,

$$\text{C-NOT} : |a,b\rangle \longrightarrow |a, a \oplus b\rangle, \quad a, b \in \mathbb{Z}_2. \tag{5.36}$$

Graphically, it is expressed as

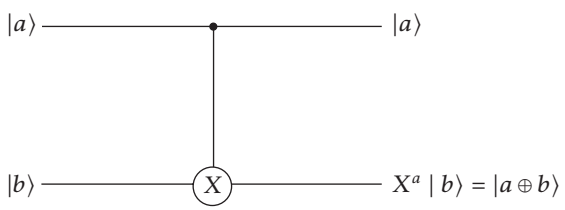

FIGURE 5.1

and the matrix representation is

$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{5.37}$$

Here $a \oplus b = a + b \pmod 2$ and we note the relation

$$X^a|b\rangle \equiv \sigma_1^a|b\rangle = |a \oplus b\rangle \quad \text{for } a,b \in \mathbb{Z}_2. \tag{5.38}$$

In this case, the first bit is called a control bit and the second a target bit.

Of course, we can consider the reverse case. Namely, the first bit is a target one and the second a control one, which is also called the controlled NOT operation

$$\text{C-NOT} : |a,b\rangle \longrightarrow |a \oplus b, b\rangle, \quad a,b \in \mathbb{Z}_2, \tag{5.39}$$

and the matrix representation is

$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{5.40}$$

In the 1-qubit case, we may assume that we can construct all unitary operations in $U(2)$ (we call the operation universal). In the 2-qubit case, how can we construct all unitary operations in $U(4)$? If we can construct the C-NOT (5.37), (5.40) in our system, then we can show that the operation is universal, see [1, 3]. This is a crucial point in quantum computing. Our comment here is that the C-NOT (5.37) can be written as a uniton (5.8)

$$\text{C-NOT} = \mathbf{1}_4 - 2P, \tag{5.41}$$

where

$$P = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \tag{5.42}$$

and this P can be diagonalized by making use of Walsh-Hadamard transformation (5.16) like

$$\begin{aligned} P &= (\mathbf{1}_2 \otimes W)\tilde{E}_1(\mathbf{1}_2 \otimes W)^{-1} \\ &= (\mathbf{1}_2 \otimes W)(\sigma_1 \otimes \sigma_1)E_1(\sigma_1 \otimes \sigma_1)^{-1}(\mathbf{1}_2 \otimes W)^{-1}, \end{aligned} \tag{5.43}$$

where

$$\widetilde{E}_1 = \begin{pmatrix} 0 & & & \\ & 0 & & \\ & & 0 & \\ & & & 1 \end{pmatrix}, \qquad E_1 = \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 0 & \\ & & & 0 \end{pmatrix}. \tag{5.44}$$

More generally, for the t-qubit case, we can construct $(t-1)$-repeated controlled-NOT operator and show it is a uniton.

The $(t-1)$-repeated controlled-NOT operation is defined by

$$\begin{aligned} \mathrm{C}^{(t-1)}\text{-NOT} : |a_1, a_2, \dots, a_{t-1}, a_t\rangle &\longrightarrow |a_1, a_2, \dots, a_{t-1}, a_1 a_2 \cdots a_{t-1} \oplus a_t\rangle, \\ & a_k \in \mathbb{Z}_2 \ (k = 1, 2, \dots, t), \end{aligned} \tag{5.45}$$

or in matrix form

$$\mathrm{C}^{(t-1)}\text{-NOT} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & 1 \\ & & & 1 & 0 \end{pmatrix} : 2^t \times 2^t\text{-matrix}. \tag{5.46}$$

As for the explicit construction of $(t-1)$-repeated controlled-NOT operator see [1, 9]. See also Appendix C. But unfortunately the construction is not *efficient*.

In [1] a rough estimation of the number of steps to construct the operator (5.45) is given and it is confirmed that an efficient construction is possible. But no explicit construction is given.

By the way, since

$$\mathbf{1}_2{}^{\otimes(t-1)} \otimes W \begin{pmatrix} W & & & \\ & \ddots & & \\ & & W & \\ & & & W \end{pmatrix}, \tag{5.47}$$

we have

$$
\begin{aligned}
&\left(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\right) \mathrm{C}^{(t-1)}\text{-NOT} \left(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\right) \\
&= \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & -1 \end{pmatrix} = \mathbf{1}_n - 2|n-1)(n-1|.
\end{aligned}
\tag{5.48}
$$

Therefore, the construction of $\mathrm{C}^{(t-1)}$-NOT and $\mathbf{1}_n - 2|n-1)(n-1|$ have almost the same number of steps. Is it possible to construct this operator efficiently?

As far as we know, an explicit and efficient construction of this operation has not yet been given.

Problem 5.2. Give an explicit and efficient algorithm to this operation.

We consider a set

$$
\left\{F_k \mid 1 \le k \le n\right\}, \tag{5.49}
$$

where

$$
F_k = \mathbf{1}_n - 2E_k = \begin{pmatrix} -\mathbf{1}_k & \\ & \mathbf{1}_{n-k} \end{pmatrix}. \tag{5.50}
$$

If F_1 can be constructed, then the other F's can be easily obtained. First, we show this with a simple example ($t = 2$)

$$
F_1 = \begin{pmatrix} -1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} = \mathbf{1}_4 - 2|0)(0|. \tag{5.51}
$$

Now we set

$$U_1 = \mathbf{1}_2 \otimes \sigma_1 = \begin{pmatrix} & 1 & & \\ 1 & & & \\ & & & 1 \\ & & 1 & \end{pmatrix},$$

$$U_2 = \sigma_1 \otimes \mathbf{1}_2 = \begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix}, \tag{5.52}$$

$$U_3 = \sigma_1 \otimes \sigma_1 = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix},$$

then we have

$$U_1 F_1 U_1 = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} = \mathbf{1}_4 - 2|1)(1|,$$

$$U_2 F_1 U_2 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & 1 \end{pmatrix} = \mathbf{1}_4 - 2|2)(2|, \tag{5.53}$$

$$U_3 F_1 U_3 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} = \mathbf{1}_4 - 2|3)(3|,$$

so that it is easy to check that

$$F_1(U_1 F_1 U_1) = F_2, \qquad F_2(U_2 F_1 U_2) = F_3, \qquad F_3(U_3 F_1 U_3) = -\mathbf{1}_4. \tag{5.54}$$

We prove the general case. For $i = i_1 2^{t-1} + i_2 2^{t-2} + \cdots + i_t$ $(0 \leq i \leq n-1)$, we set

$$U_i = \sigma_1^{i_1} \otimes \sigma_1^{i_2} \otimes \cdots \otimes \sigma_1^{i_t}, \quad (U_i^\dagger = U_i = U_i^{-1}). \tag{5.55}$$

Since

$$\begin{aligned} U_i|0) &= \sigma_1^{i_1} \otimes \sigma_1^{i_2} \otimes \cdots \otimes \sigma_1^{i_t} \big(|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle\big) \\ &= \sigma_1^{i_1}|0\rangle \otimes \sigma_1^{i_2}|0\rangle \otimes \cdots \otimes \sigma_1^{i_t}|0\rangle \\ &= \big|i_1\big\rangle \otimes \big|i_2\big\rangle \otimes \cdots \otimes \big|i_t\big\rangle \equiv |i), \end{aligned} \tag{5.56}$$

we have

$$\mathbf{1}_n - 2|i)(i| = U_i\big(\mathbf{1}_n - 2|0)(0|\big)U_i = U_i F_1 U_i. \tag{5.57}$$

Therefore, it is easy to see that

$$F_k\big(U_k F_1 U_k\big) = F_{k+1}, \quad (1 \le k \le n-1). \tag{5.58}$$

We note that this procedure is not efficient.

Now, we make a comment on Grover's database searching algorithm. In his algorithm, the following two unitary operations play an essential role

$$\mathbf{1}_n - 2|i)(i|, \qquad \mathbf{1}_n - 2|s)(s|, \tag{5.59}$$

in which the state $|s)$ (s stands for *sum*) is defined by

$$|s) \equiv \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i) = W^{\otimes t}|0). \tag{5.60}$$

We find via (5.25) that

$$\mathbf{1}_n - 2|s)(s| = W^{\otimes t}\big(\mathbf{1}_n - 2|0)(0|\big)W^{\otimes t} = W^{\otimes t} F_1 W^{\otimes t}. \tag{5.61}$$

Namely, the two operations (5.59) are both unitons and can be diagonalized by the efficient unitary operations U_i and $W^{\otimes t}$.

Finally, we mention the relation between $(t-1)$-repeated controlled-NOT operation and F_1. Since

$$\begin{aligned} &\big(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\big)\mathrm{C}^{(t-1)}\text{-NOT}\big(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\big) \\ &\qquad = \mathbf{1}_n - 2|n-1)(n-1| = U_{n-1} F_1 U_{n-1} \end{aligned} \tag{5.62}$$

by (5.48), we have

$$F_1 = U_{n-1}\big(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\big)\mathrm{C}^{(t-1)}\text{-NOT}\big(\mathbf{1}_2{}^{\otimes(t-1)} \otimes W\big)U_{n-1}. \tag{5.63}$$

Substituting $U_{n-1} = \sigma_1 \otimes \sigma_1 \otimes \cdots \otimes \sigma_1 \otimes \sigma_1$ into the equation above, we arrive at the desired relation

$$F_1 = \left({\sigma_1}^{\otimes(t-1)} \otimes \sigma_1 W\right) \mathrm{C}^{(t-1)}\text{-NOT} \left({\sigma_1}^{\otimes(t-1)} \otimes W \sigma_1\right). \tag{5.64}$$

6. Holonomic quantum computation

In this section, we briefly introduce a simplified version of holonomic quantum computation. The full story would require detailed knowledge of quantum mechanics, quantum optics, and global analysis, which are not discussed in this paper.

This model was proposed by Zanardi and Rasetti [22, 31], and it has been developed by Fujii [5, 6, 7, 8] and Pachos [20, 21].

This model uses the non-abelian Berry phase (quantum holonomy in the mathematical terminology [18]) in the process of quantum computing. In this model, a Hamiltonian (including some parameters) must have certain degeneracy because an adiabatic connection (the non-abelian Berry connection) is introduced in terms of the degeneracy, see [27]. In other words, a quantum computational bundle is introduced on some parameter space due to this degeneracy, and the canonical connection of this bundle is just the one mentioned above.

On this bundle, holonomic quantum computation is performed by making use of the holonomy operations. We note that our method is completely geometrical.

Here, we introduce *quantum computational bundles*, [5, 7, 8]. For this purpose, we need universal, principal, and vector bundles over infinite-dimensional Grassmann manifolds. We also need an infinite-dimensional vector space called a Hilbert (or Fock) space.

Let $\mathscr{H}$ be a separable Hilbert space over $\mathbb{C}$. For $m \in \mathbb{N}$, we set

$$\mathrm{St}_m(\mathscr{H}) \equiv \left\{ V = (v_1, \ldots, v_m) \in \mathscr{H} \times \cdots \times \mathscr{H} \mid V^\dagger V = \mathbf{1}_m \right\}, \tag{6.1}$$

where $\mathbf{1}_m$ is a unit matrix in $M(m, \mathbb{C})$. This is called a (universal) Stiefel manifold. Note that the unitary group $U(m)$ acts on $\mathrm{St}_m(\mathscr{H})$ from the right

$$\mathrm{St}_m(\mathscr{H}) \times U(m) \longrightarrow \mathrm{St}_m(\mathscr{H}) : (V, a) \longmapsto Va. \tag{6.2}$$

Next, we define a (universal) Grassmann manifold

$$\mathrm{Gr}_m(\mathscr{H}) \equiv \left\{ X \in M(\mathscr{H}) \mid X^2 = X,\ X^\dagger = X,\ \mathrm{tr}\, X = m \right\}, \tag{6.3}$$

where $M(\mathscr{H})$ denotes a space of all bounded linear operators on $\mathscr{H}$. Then we have a projection

$$\pi : \mathrm{St}_m(\mathscr{H}) \longrightarrow \mathrm{Gr}_m(\mathscr{H}), \quad \pi(V) \equiv VV^\dagger = \sum_{j=1}^{m} v_j v_j^\dagger, \tag{6.4}$$

compatible with the action (6.2) ($\pi(Va) = Va(Va)^\dagger = Vaa^\dagger V^\dagger = VV^\dagger = \pi(V)$).

Now, the set

$$\{U(m), \mathrm{St}_m(\mathscr{H}), \pi, \mathrm{Gr}_m(\mathscr{H})\} \tag{6.5}$$

is called a (universal) principal $U(m)$ bundle, see [7, 18]. We set

$$E_m(\mathscr{H}) \equiv \{(X, v) \in \mathrm{Gr}_m(\mathscr{H}) \times \mathscr{H} \mid Xv = v\}. \tag{6.6}$$

Then we have also a projection

$$\pi : E_m(\mathscr{H}) \longrightarrow \mathrm{Gr}_m(\mathscr{H}), \quad \pi\big((X, v)\big) \equiv X. \tag{6.7}$$

The set

$$\{\mathbb{C}^m, E_m(\mathscr{H}), \pi, \mathrm{Gr}_m(\mathscr{H})\} \tag{6.8}$$

is called a (universal) mth vector bundle. This vector bundle is associated with the principal $U(m)$ bundle (6.5).

Next, let M be a finite or infinite dimensional differentiable manifold and the map $P : M \to \mathrm{Gr}_m(\mathscr{H})$ be given (called a projector). Using this P, we can define the pullback bundles over M from (6.5) and (6.8)

$$\{U(m), \tilde{\mathrm{St}}, \pi_{\tilde{\mathrm{St}}}, M\} \equiv P^*\{U(m), \mathrm{St}_m(\mathscr{H}), \pi, \mathrm{Gr}_m(\mathscr{H})\}, \tag{6.9}$$

$$\{\mathbb{C}^m, \tilde{E}, \pi_{\tilde{E}}, M\} \equiv P^*\{\mathbb{C}^m, E_m(\mathscr{H}), \pi, \mathrm{Gr}_m(\mathscr{H})\}, \tag{6.10}$$

see [18]. Of course, the second bundle (6.10) is a vector bundle associated with the first one (6.9):

$$\begin{array}{ccc} U(m) & & U(m) \\ \downarrow & & \downarrow \\ \tilde{\mathrm{St}} & \longrightarrow & \mathrm{St}_m(\mathscr{H}) \\ \downarrow & & \downarrow \\ M & \xrightarrow{P} & \mathrm{Gr}_m(\mathscr{H}) \end{array} \qquad \begin{array}{ccc} \mathbb{C}^m & & \mathbb{C}^m \\ \downarrow & & \downarrow \\ \tilde{E} & \longrightarrow & E_m(\mathscr{H}) \\ \downarrow & & \downarrow \\ M & \xrightarrow{P} & \mathrm{Gr}_m(\mathscr{H}) \end{array} \tag{6.11}$$

Let $\mathcal{M}$ be a parameter space (a complex manifold in general) and we denote by λ its element. Let λ_0 be a fixed reference point of $\mathcal{M}$. Let H_λ be a family of Hamiltonians parameterized by $\mathcal{M}$ acting on the Fock space $\mathcal{H}$. We set $H_0 = H_{\lambda_0}$ for simplicity and assume that this has an m-fold degenerate vacuum

$$H_0 v_j = \mathbf{0}, \quad j = 1, \dots, m. \tag{6.12}$$

These v_j's form an m-dimensional vector space. We may assume that $\langle v_i | v_j \rangle = \delta_{ij}$. Then $(v_1, \dots, v_m) \in \mathrm{St}_m(\mathcal{H})$ and

$$F_0 \equiv \left\{ \sum_{j=1}^{m} x_j v_j \mid x_j \in \mathbb{C} \right\} \cong \mathbb{C}^m. \tag{6.13}$$

Namely, F_0 is a vector space associated with the orthonormal (o.n.) basis $(v_1, \dots, v_m)$.

Next we assume, for simplicity, that a family of unitary operators parameterized by $\mathcal{M}$

$$W : \mathcal{M} \longrightarrow U(\mathcal{H}), \quad W(\lambda_0) = \text{identity}, \tag{6.14}$$

connects H_λ and H_0 isospectrally

$$H_\lambda \equiv W(\lambda) H_0 W(\lambda)^{-1}. \tag{6.15}$$

In this case, there is no level crossing of eigenvalues. Using $W(\lambda)$, we can define a projector

$$P : \mathcal{M} \longrightarrow \mathrm{Gr}_m(\mathcal{H}), \quad P(\lambda) \equiv W(\lambda) \left(\sum_{j=1}^{m} v_j v_j^\dagger \right) W(\lambda)^{-1}, \tag{6.16}$$

and the pullback bundles over $\mathcal{M}$

$$\{U(m), \tilde{\mathrm{St}}, \pi_{\tilde{\mathrm{St}}}, \mathcal{M}\}, \qquad \{\mathbb{C}^m, \tilde{E}, \pi_{\tilde{E}}, \mathcal{M}\}. \tag{6.17}$$

For the latter, we set

$$|\mathrm{vac}\rangle = (v_1, \dots, v_m). \tag{6.18}$$

In this case, a canonical connection form $\mathcal{A}$ of the principal bundle $\{U(m), \tilde{\mathrm{St}}, \pi_{\tilde{\mathrm{St}}}, \mathcal{M}\}$ is given by

$$\mathcal{A} = \langle \mathrm{vac} | W(\lambda)^{-1} dW(\lambda) | \mathrm{vac} \rangle, \tag{6.19}$$

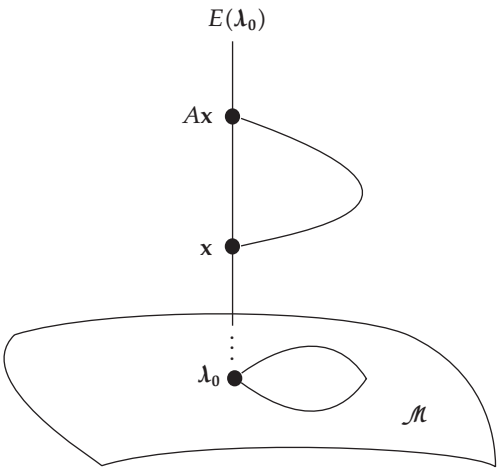

FIGURE 6.1

where d is a differential form on $\mathcal{M}$

$$d = \sum_k \left(d\lambda_k \frac{\partial}{\partial \lambda_k} + d\bar{\lambda}_k \frac{\partial}{\partial \bar{\lambda}_k} \right) \tag{6.20}$$

together with its curvature form (see [18, 27])

$$\mathcal{F} \equiv d\mathcal{A} + \mathcal{A} \wedge \mathcal{A}. \tag{6.21}$$

Let γ be a loop in $\mathcal{M}$ at λ_0, $\gamma : [0,1] \to \mathcal{M}$, $\gamma(0) = \gamma(1) = \lambda_0$. For this γ, a holonomy operator $\Gamma_{\mathcal{A}}$ is defined as

$$\Gamma_{\mathcal{A}}(\gamma) = \mathcal{P} \exp \left\{ \oint_\gamma \mathcal{A} \right\} \in U(m), \tag{6.22}$$

where $\mathcal{P}$ means path-ordering, see, for example, [21]. This acts on the fiber F_0 at λ_0 of the vector bundle $\{\mathbb{C}^m, \tilde{E}, \pi_{\tilde{E}}, M\}$ as follows: $\mathbf{x} \to \Gamma_{\mathcal{A}}(\gamma)\mathbf{x}$. The holonomy group $\mathrm{Hol}(\mathcal{A})$ is in general a subgroup of $U(m)$. In the case of $\mathrm{Hol}(\mathcal{A}) = U(m)$, $\mathcal{A}$ is called irreducible. The irreducibility of $\mathcal{A}$ is very important because it means the universality of quantum computation. To check whether $\mathcal{A}$ is irreducible or not, we need its curvature form (6.21), see [18].

In the holonomic quantum computation, we take

$$\begin{aligned} &\text{encoding of information} \Longrightarrow \mathbf{x} \in F_0, \\ &\text{processing of information} \Longrightarrow \Gamma_{\mathcal{A}}(\gamma) : \mathbf{x} \longrightarrow \Gamma_{\mathcal{A}}(\gamma)\mathbf{x} \equiv A\mathbf{x}. \end{aligned} \tag{6.23}$$

See Figure 6.1.

Our model is relatively complicated compared to the other geometric models and much more so than the usual spin models.

Appendices

A. A family of flag manifolds

We make a comment on an interesting relation between flag manifolds and the kernel of the exponential map defined on matrices. Here, a (generalized) flag manifold (which is a useful manifold as shown in the following) is a natural generalization of the Grassmann one.

First of all, we make a brief review. For

$$\exp : \mathbb{R} \longrightarrow S^1 \subset \mathbb{C}, \quad \exp(t) \equiv e^{2\pi\sqrt{-1}t}, \tag{A.1}$$

the kernel of this map is $\ker(\exp) = \mathbb{Z} \subset \mathbb{R}$.

By $H(n,\mathbb{C})$ we define the set of all hermitian matrices

$$H(n,\mathbb{C}) = \{X \in M(n,\mathbb{C}) \mid X^\dagger = X\}. \tag{A.2}$$

Of course, $H(1,\mathbb{C}) = \mathbb{R}$. Note that each element of $H(n,\mathbb{C})$ can be diagonalized by some unitary matrix.

The exponential map is now defined as

$$E : H(n,\mathbb{C}) \longrightarrow U(n), \quad E(X) = e^{2\pi\sqrt{-1}X}. \tag{A.3}$$

Here our target is $\ker(E)$.

Problem A.1. What is the structure of $\ker(E)$?

Our claim is that $\ker(E)$ is a family of flag manifolds. For that, we write $\ker(E)$ as

$$K_n(\mathbb{C}) = \{X \in H(n,\mathbb{C}) \mid e^{2\pi\sqrt{-1}X} = \mathbf{1}_n\}. \tag{A.4}$$

First, we prove

$$G_n(\mathbb{C}) \subset K_n(\mathbb{C}). \tag{A.5}$$

Since $P^2 = P$ from the definition, $P^k = P$ for $k \geq 1$, so that

$$\begin{aligned} e^{2\pi\sqrt{-1}P} &= \mathbf{1}_n + \sum_{k=1}^{\infty} \frac{\left(2\pi\sqrt{-1}\right)^k}{k!} P^k \\ &= \mathbf{1}_n + \sum_{k=1}^{\infty} \frac{\left(2\pi\sqrt{-1}\right)^k}{k!} P = \mathbf{1}_n + \left(e^{2\pi\sqrt{-1}} - 1\right) P = \mathbf{1}_n. \end{aligned} \tag{A.6}$$

We will prove that $G_n(\mathbb{C})$ becomes a kind of basis for $K_n(\mathbb{C})$.

For $X \in K_n(\mathbb{C})$, we write the set of all eigenvalues of X as $\mathrm{spec}(X)$. Then $\mathrm{spec}(X) = \{0,1\}$ for $X \in G_n(\mathbb{C})$.

It is clear that $\mathrm{spec}(X) \subset \mathbb{Z}$. For $X \in K_n(\mathbb{C})$, we have

$$\begin{gathered} \mathrm{spec}(X) = \left\{n_1(d_1), \ldots, n_k(d_k), \ldots, n_j(d_j)\right\} \quad \text{where } n_k \in \mathbb{Z}, \\ \sum_{k=1}^{j} d_k = n, \end{gathered} \tag{A.7}$$

in which (d_k) is the multiplicity of the eigenvalue n_k. Since X is diagonalized by some $U \in U(n)$,

$$X = UX_0U^{-1} = \sum_{k=1}^{j} n_k P_{d_k}, \tag{A.8}$$

where

$$\begin{aligned} X_0 &= \begin{pmatrix} n_1\mathbf{1}_{d_1} & & & \\ & n_2\mathbf{1}_{d_2} & & \\ & & \ddots & \\ & & & n_j\mathbf{1}_{d_j} \end{pmatrix}, \\ P_{d_k} &= U \begin{pmatrix} \mathbf{0}_{d_1} & & & & \\ & \ddots & & & \\ & & \mathbf{1}_{d_k} & & \\ & & & \ddots & \\ & & & & \mathbf{0}_{d_j} \end{pmatrix} U^{-1}. \end{aligned} \tag{A.9}$$

Here we list some properties of the set of projections $\{P_{d_k}\}$:

(1) $P_{d_k} \in G_{d_k,n}(\mathbb{C})$,
(2) $P_{d_k}P_{d_l} = \delta_{kl}P_{d_l}$,
(3) $P_{d_1} + P_{d_2} + \cdots + P_{d_j} = \mathbf{1}_n$.

Here, we prepare a terminology. For $X \in K_n(\mathbb{C})$, we call the set of eigenvalues together with multiplicities

$$\{(n_1,d_1),(n_2,d_2),\dots,(n_j,d_j)\} \tag{A.10}$$

the spectral type of X.

Then it is easy to see that X and $Y \in K_n(\mathbb{C})$ are of the same spectral type ($X \sim Y$) if and only if $Y = UXU^{-1}$ for some $U \in U(n)$. For $X \in K_n(\mathbb{C})$, we define

$$C(X) = \{Y \in K_n(\mathbb{C}) \mid Y \sim X\}. \tag{A.11}$$

We have clearly $C(X) = C(X_0)$. Then it is easy to see that $K_n(\mathbb{C})$ can be classified by the spectral type

$$K_n(\mathbb{C}) = \bigcup_X C(X) = \bigcup_{X_0} C(X_0), \tag{A.12}$$

and the unitary group $U(n)$ acts on $C(X)$ as follows:

$$U(n) \times C(X) \longrightarrow C(X) : (U,X) \longmapsto UXU^{-1}. \tag{A.13}$$

Since this action is free and transitive, the isotropy group at X_0 is

$$U(d_1) \times U(d_2) \times \cdots \times U(d_j), \tag{A.14}$$

so that we have

$$C(X) \cong \frac{U(n)}{U(d_1) \times U(d_2) \times \cdots \times U(d_j)}. \tag{A.15}$$

The right-hand side is called a generalized flag manifold. In particular, when $d_1 = d_2 = \cdots = d_n = 1$ (there is no overlapping in the eigenvalues of X), we have

$$C(X) \cong \frac{U(n)}{U(1) \times U(1) \times \cdots \times U(1)}. \tag{A.16}$$

This is called a flag manifold.

Namely, by (A.12) we know that $K_n(\mathbb{C})$ is a family of generalized flag manifolds.

For the Grassmann manifolds we have very good local coordinates like (2.9), while we do not know good local coordinates for generalized flag manifolds.

Problem A.2. Find a good local coordinate system.

For some applications of generalized flag manifolds, the paper [23] is recommended.

B. A generalization of Pauli matrices

Here, we introduce a generalization of Pauli matrices (5.18) that has been used in several situations in both quantum field theory and quantum computation.

First of all, we summarize the properties of Pauli matrices. By (5.18), $\sigma_2 = \sqrt{-1}\sigma_1\sigma_3$, so that the essential elements of Pauli matrices are $\{\sigma_1, \sigma_3\}$ and they satisfy

$$\sigma_1^2 = \sigma_3^2 = \mathbf{1}_2; \qquad \sigma_1^\dagger = \sigma_1, \qquad \sigma_3^\dagger = \sigma_3; \qquad \sigma_3\sigma_1 = -\sigma_1\sigma_3. \tag{B.1}$$

Let $\{\Sigma_1, \Sigma_3\}$ be the following matrices in $M(n, \mathbb{C})$:

$$\Sigma_1 = \begin{pmatrix} 0 & & & & & 1 \\ 1 & 0 & & & & \\ & 1 & 0 & & & \\ & & 1 & \ddots & & \\ & & & \ddots & & \\ & & & & 1 & 0 \end{pmatrix}, \qquad \Sigma_3 = \begin{pmatrix} 1 & & & & & \\ & \sigma & & & & \\ & & \sigma^2 & & & \\ & & & \ddots & & \\ & & & & \sigma^{n-1} & \end{pmatrix}, \tag{B.2}$$

where σ is a primitive root of unity $\sigma^n = 1$ ($\sigma = e^{2\pi\sqrt{-1}/n}$). We note that

$$\bar{\sigma} = \sigma^{n-1}, \quad 1 + \sigma + \cdots + \sigma^{n-1} = 0. \tag{B.3}$$

The two matrices $\{\Sigma_1, \Sigma_3\}$ are generalizations of Pauli matrices $\{\sigma_1, \sigma_3\}$, but they are not hermitian. Here we list some of their important properties:

$$\Sigma_1^n = \Sigma_3^n = \mathbf{1}_n; \qquad \Sigma_1^\dagger = \Sigma_1^{n-1}, \qquad \Sigma_3^\dagger = \Sigma_3^{n-1}; \qquad \Sigma_3\Sigma_1 = \sigma\Sigma_1\Sigma_3. \tag{B.4}$$

If we define a Vandermonde matrix W based on σ as

$$W = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \sigma^{n-1} & \sigma^{2(n-1)} & \cdots & \sigma^{(n-1)^2} \\ 1 & \sigma^{n-2} & \sigma^{2(n-2)} & \cdots & \sigma^{(n-1)(n-2)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \sigma^2 & \sigma^4 & \cdots & \sigma^{2(n-1)} \\ 1 & \sigma & \sigma^2 & \cdots & \sigma^{n-1} \end{pmatrix},$$

$$W^\dagger = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \sigma & \sigma^2 & \cdots & \sigma^{n-1} \\ 1 & \sigma^2 & \sigma^4 & \cdots & \sigma^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \sigma^{n-2} & \sigma^{2(n-2)} & \cdots & \sigma^{(n-1)(n-2)} \\ 1 & \sigma^{n-1} & \sigma^{2(n-1)} & \cdots & \sigma^{(n-1)^2} \end{pmatrix}, \tag{B.5}$$

then it is not difficult to see that

$$\Sigma_1 = W\Sigma_3 W^\dagger = W\Sigma_3 W^{-1}. \tag{B.6}$$

For example, for $n = 3$

$$\begin{aligned} W\Sigma_3 W^\dagger &= \frac{1}{3} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \sigma^2 & \sigma \\ 1 & \sigma & \sigma^2 \end{pmatrix} \begin{pmatrix} 1 & & \\ & \sigma & \\ & & \sigma^2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \sigma & \sigma^2 \\ 1 & \sigma^2 & \sigma \end{pmatrix} \\ &= \frac{1}{3} \begin{pmatrix} 1 & \sigma & \sigma^2 \\ 1 & 1 & 1 \\ 1 & \sigma^2 & \sigma \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \sigma & \sigma^2 \\ 1 & \sigma^2 & \sigma \end{pmatrix} \\ &= \frac{1}{3} \begin{pmatrix} 0 & 0 & 3 \\ 3 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} = \Sigma_1, \end{aligned} \tag{B.7}$$

where we have used that $\sigma^3 = 1$, $\bar{\sigma} = \sigma^2$, and $1 + \sigma + \sigma^2 = 0$.

That is, Σ_1 can be diagonalized by making use of W.

Since W corresponds to the Walsh-Hadamard matrix (5.16), so it may be possible to call W the generalized Walsh-Hadamard matrix.

C. General controlled unitary operations

Here, we introduce a usual construction of general controlled unitary operations to help in the understanding of general controlled-NOT one. In the following arguments, if we take $U = X = \sigma_1$, then they reduce to the arguments of a construction of general controlled-NOT operator.

First of all, we recall (5.33). For $x, y, z \in \mathbb{Z}_2$, we have identities

$$x + y - x \oplus y = 2xy, \tag{C.1}$$
$$x + y + z - x \oplus y - x \oplus z - y \oplus z + x \oplus y \oplus z = 4xyz, \tag{C.2}$$

where $x \oplus y = x + y (\mathrm{mod}\, 2)$. For the most general identities of the above mentioned type see [1, 9].

The controlled-controlled unitary operations are constructed by using both several controlled unitary operations and controlled-NOT operations: let U be an arbitrarily unitary matrix in $U(2)$, and V a unitary one in $U(2)$ satisfying $V^2 = U$. Then by (C.1), we have

$$\begin{aligned} V^{x+y-x\oplus y} &= V^{2xy} = \left(V^2\right)^{xy} = U^{xy}, \\ V^{x+y-x\oplus y} &= V^x V^y V^{-x\oplus y} = V^x V^y \left(V^{-1}\right)^{x\oplus y} = V^x V^y \left(V^\dagger\right)^{x\oplus y}, \end{aligned} \tag{C.3}$$

so a controlled-controlled U operation is graphically represented as Figure C.1.

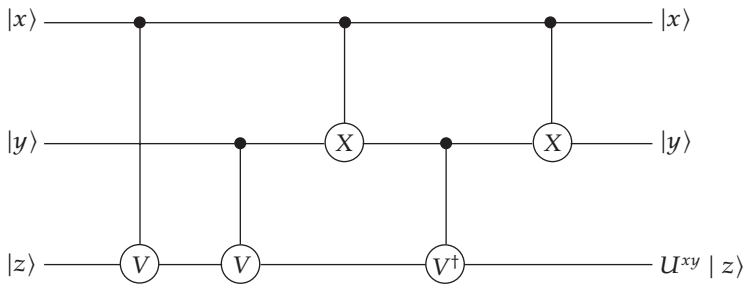

FIGURE C.1

This figure should be read from left to right as follows:

$$|x\rangle \otimes |y\rangle \otimes |z\rangle \longrightarrow |x\rangle \otimes |y\rangle \otimes U^{xy}|z\rangle. \tag{C.4}$$

The controlled-controlled-controlled unitary operations are constructed as follows: let U be an arbitrarily unitary matrix in $U(2)$, and let V be a unitary one in $U(2)$ satisfying $V^4 = U$. Then by (C.1)

$$\begin{aligned} V^{x+y+z-(x\oplus y+x\oplus z+y\oplus z)+x\oplus y\oplus z} &= V^{4xyx} = U^{xyz}, \\ V^{x+y+z-(x\oplus y+x\oplus z+y\oplus z)+x\oplus y\oplus z} &= V^x V^y V^z \left(V^\dagger\right)^{x\oplus y} \left(V^\dagger\right)^{x\oplus z} \left(V^\dagger\right)^{y\oplus z} V^{x\oplus y\oplus z}, \end{aligned} \tag{C.5}$$

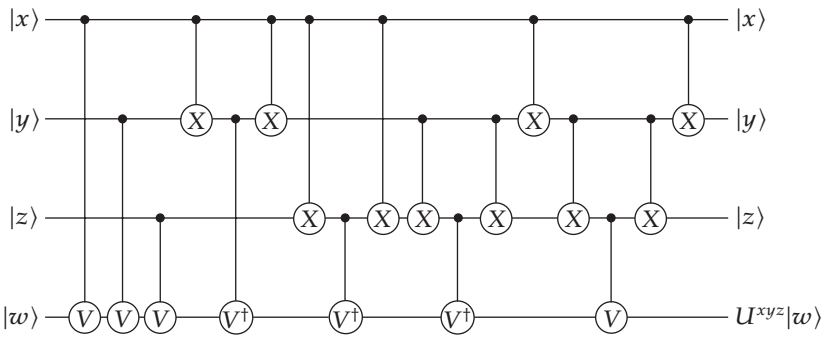

FIGURE C.2

so a controlled-controlled-controlled U operation is graphically represented as Figure C.2.
This figure means that

$$|x\rangle \otimes |y\rangle \otimes |z\rangle \otimes |w\rangle \longrightarrow |x\rangle \otimes |y\rangle \otimes |z\rangle \otimes U^{xyz}|w\rangle. \tag{C.6}$$

For the case $U = X = \sigma_1$, we have from (5.45)

$$\begin{aligned} \big|a_1, a_2, \ldots, a_{n-1}, a_n\big\rangle &\longrightarrow \big|a_1, a_2, \ldots, a_{n-1}, a_1 a_2 \cdots a_{n-1} \oplus a_n\big\rangle \\ &\equiv \big|a_1\big\rangle \otimes \big|a_2\big\rangle \otimes \cdots \big|a_{n-1}\big\rangle \otimes \big|a_1 a_2 \cdots a_{n-1} \oplus a_n\big\rangle \\ &= \big|a_1\big\rangle \otimes \big|a_2\big\rangle \otimes \cdots \big|a_{n-1}\big\rangle \otimes X^{a_1 a_2 \cdots a_{n-1}} \big|a_n\big\rangle. \end{aligned} \tag{C.7}$$

As can be seen from the figures, the well-known construction of general controlled unitary operations needs exponential steps. Namely, it is not efficient. For more details see [1, 9].

Acknowledgments

The author wishes to thank Yoshinori Machida for his warm hospitality at Numazu College of Technology. He also wishes to thank Akira Asada, Ryu Sasaki, and Tatsuo Suzuki for reading this manuscript and making some useful comments.

References

[1] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. H. Margolus, P. W. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, *Elementary gates for quantum computation*, Phys. Rev. A **52** (1995), no. 5, 3457–3467.

[2] G. Chen and Z. Diao, *Exponentially fast quantum search algorithm*, http://arxiv.org/abs/math/quant-ph/0011109.

[3] D. Deutsch, A. Barenco, and A. Ekert, *Universality in quantum computation*, Proc. Roy. Soc. London Ser. A **449** (1995), no. 1937, 669–677.
[4] G. Dunne, *Self-Dual Chern-Simons Theories*, Lecture Notes in Physics, vol. M36, Springer, Berlin, 1995.
[5] K. Fujii, *Mathematical foundations of holonomic quantum computer II*, http://arxiv.org/abs/quant-ph/0101102.
[6] ———, *More on optical holonomic quantum computer*, http://arxiv.org/abs/math/quant-ph/0005129.
[7] ———, *Note on coherent states and adiabatic connections, curvatures*, J. Math. Phys. **41** (2000), no. 7, 4406–4412.
[8] ———, *Mathematical foundations of holonomic quantum computer*, Rep. Math. Phys. **48** (2001), no. 1-2, 75–82.
[9] ———, *A lecture on quantum logic gates*, The Bulletin of Yokohama City University **53** (2002), 1–10.
[10] K. Fujii, T. Kashiwa, and S. Sakoda, *Coherent states over Grassmann manifolds and the WKB exactness in path integral*, J. Math. Phys. **37** (1996), no. 2, 567–602.
[11] K. Funahashi, private communication.
[12] L. K. Grover, *A framework for fast quantum mechanical algorithms*, STOC '98 (Dallas, TX), ACM, New York, 1999, pp. 53–62.
[13] A. Hosoya, *Lectures on Quantum Computation*, Science Publishing, Peking, 1999.
[14] R. Jozsa, *Quantum algorithms and the Fourier transform*, R. Soc. Lond. Proc. Ser. A Math. Phys. Eng. Sci. **454** (1998), no. 1969, 323–337.
[15] ———, *Quantum factoring, discrete logarithms and the hidden subgroup problem*, IEEE Computing in Science and Engineering **3** (2001), no. 2, 34–43.
[16] A. Yu. Kitaev, *Fault-tolerant quantum computation by anyons*, http://arxiv.org/abs/quant-ph/9707021.
[17] H.-K. Lo, S. Popescu, and T. Spiller (eds.), *Introduction to Quantum Computation and Information*, World Scientific Publishing, New Jersey, 1998.
[18] M. Nakahara, *Geometry, Topology and Physics*, Graduate Student Series in Physics, Adam Hilger, Bristol, 1990.
[19] H. Oike, *Geometry of Grassmann Manifolds*, Yamagata University, Japan, 1979.
[20] J. Pachos and S. Chountasis, *Optical holonomic quantum computer*, Phys. Rev. A **62** (2000), 1–9, 052318.
[21] J. Pachos and P. Zanardi, *Quantum holonomies for quantum computing*, Internat. J. Modern Phys. B **15** (2001), no. 9, 1257–1285.
[22] J. Pachos, P. Zanardi, and M. Rasetti, *Non-Abelian Berry connections for quantum computation*, Phys. Rev. A (3) **61** (2000), no. 1, 1–4, 010305.
[23] R. F. Picken, *The Duistermaat-Heckman integration formula on flag manifolds*, J. Math. Phys. **31** (1990), no. 3, 616–638.
[24] J. Preskill, *Fault-tolerant quantum computation*, Introduction to Quantum Computation and Information (H.-K. Lo, S. Popescu, and T. Spiller, eds.), World Scientific Publishing, New Jersey, 1998, pp. 213–269.
[25] S. G. Rajeev, S. K. Rama, and S. Sen, *Symplectic manifolds, coherent states, and semiclassical approximation*, J. Math. Phys. **35** (1994), no. 5, 2259–2269.
[26] E. G. Rieffel and W. Polak, *An introduction to quantum computing for non-physicists*, ACM Comput. Surveys **32** (2000), no. 3, 300–335.

[27] A. Shapere and F. Wilczek (eds.), *Geometric Phases in Physics*, Advanced Series in Mathematical Physics, vol. 5, World Scientific Publishing, New Jersey, 1989.
[28] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26** (1997), no. 5, 1484–1509.
[29] A. Steane, *Quantum computing*, Rep. Progr. Phys. **61** (1998), no. 2, 117–173.
[30] W. J. Zakrzewski, *Low-Dimensional Sigma Models*, Adam Hilger, Bristol, 1989.
[31] P. Zanardi and M. Rasetti, *Holonomic quantum computation*, Phys. Lett. A **264** (1999), no. 2-3, 94–99.

Kazuyuki Fujii: Department of Mathematical Sciences, Yokohama City University, Yokohama 236-0027, Japan
E-mail address: fujii@yokohama-cu.ac.jp