計算幾何を用いた1量子ビットの量子通信における Holevo 容量計算のアルゴリズム

大音真由美† 今井 浩†,†† 今井 桂子†††

† 東京大学大学院情報理工学系研究科　〒113-0033 東京都文京区本郷 7-3-1
†† ERATO 今井量子計算機構プロジェクト, JST　〒113-0033 東京都文京区本郷 5-28-3
††† 中央大学理工学部　〒112-8551 東京都文京区春日 1-13-27
E-mail: †{oto,imai}@is.s.u-tokyo.ac.jp, ††imai@ise.chuo-u.ac.jp

あらまし 量子ビットで表現されるパラメータ空間を量子空間と定義したとき，この量子空間における計算幾何では，量子ダイバージェンスは近傍関数として扱うことができ，量子計算幾何と呼ばれている．本研究は，大西と今井による古典情報幾何での計算幾何学的構造の研究成果を量子情報幾何に拡張したものであり，ここでは Kullback-Leibler ダイバージェンスは近傍関数として用いられており，ボロノイ図が導入されている．本稿ではまず，1量子ビットの量子空間における最小包含球問題について述べ，その応用として量子通信路でのホレボ容量を計算するアルゴリズムを提案する．次に，量子空間の離散化によって時間計算量が $O(1/\epsilon)$ で ϵ 近似解を持つことを述べる．

キーワード 量子通信路，最遠点ボロノイ図，最小包含球

An algorithm for computing the Holevo capacity of 1-qubit channel with using computational geometry

Mayumi OTO†, Hiroshi IMAI†,††, and Keiko IMAI†††

† Department of Information Science, University of Tokyo.　7–3–1 Hongo, Bunkyo-ku, Tokyo 113–0033, Japan
†† ERATO Quantum Computation and Information Project, JST.　Hongo White Building, 5–28–3 Hongo, Bunkyo-ku, Tokyo 113–0033, Japan
††† Department of Information and System Engineering, Chuo University.　1–13–27 Kasuga, Bunkyo-ku, Tokyo 112–8551, Japan
E-mail: †{oto,imai}@is.s.u-tokyo.ac.jp, ††imai@ise.chuo-u.ac.jp

Abstract Let a parameter space of qubits be a quantum space. In this space, computational-geometric problems can be treated for the quantum divergence as a proximity function, whose geometry is called quantum information geometry, and the quantum divergence is treated as a proximity function. By generalizing the result by Onishi and Imai on the computational-geometric structure in the classical information geometry, where the Kullback-Leibler divergence is used as a proximity function, Voronoi diagrams are introduced. In our paper, we describe the minimum enclosing sphere problem in the 1-qubit quantum space and propose the algorithm for computing the quantum channel capacity with respect to the quantum divergence and it produces ϵ-approximate solution in time $O(1/\epsilon)$.

Key words Quantum channel, the farthest Voronoi diagram, the minimum enclosing sphere

1. Introduction

The research field of the Voronoi diagram is available for various applications. Many of them are used with the Euclidean distance. In this report, considering another space which we call a quantum space, we analyze the Voronoi diagram in the space and show the different feature from Euclidean space. The quantum space is a key concept of quantum information. Quantum information has been attracting researchers in computer science and physics in recent years, since it can provide a new model of computation, Quantum Computer, and also a complete secure quantum key distribution. As for quantum fundamentals, see books [1], [2]. Quantum information theory is a basis of this new research field. It extends classical information theory to the quantum world. Many of classical information-geometric structure, especially structure related to the entropy and divergence, have been shown to carry over in quantum settings [1]. Computational-geometric analysis of information geometry is done by Onishi and Imai [3], [4]. The Voronoi diagram is defined with respect to the divergence, and these are shown to be extensions of the Euclidean counterparts with replacing the associated potential function from a paraboloid to the entropy function.

In section 2., we describe the preliminaries of computational geometry and propose an algorithm for computing the radius of the minimum enclosing sphere in the quantum space. In section 3., we show that the radius of the minimum enclosing sphere which gives an useful information for a capacity of a quantum channel and the capacity gives an useful information for a quantum coding theory.

2. Computational geometry in a quantum space

2.1 Quantum space

We describe a correspondence of the quantum space and the computational geometry. The quantum space has parameters of a quantum state. A possible region of the quantum state of 1-qubit is a sphere, which is called the Bloch spehre B and is shown in Fig.1. A density matrix ρ describes a quantum state. ρ is mapped to a point (x, y, z) in the Bloch sphere and can be expressed as

$$\rho = \begin{pmatrix} \frac{1+z}{2} & \frac{x-\mathrm{i}y}{2} \\ \frac{x+\mathrm{i}y}{2} & \frac{1-z}{2} \end{pmatrix}$$

$$B = \{(x,y,z) \mid x^2+y^2+z^2 \leq 1\}.$$

State ρ is called pure if it corresponds to a point on the boundary of the Bloch sphere. In such a case, the rank of ρ is 1. Otherwise, it is called mixed. Eigenvalues λ_1, λ_2 of $\rho = \rho(x, y, z)$ are given by

$$\frac{1 \pm \sqrt{1-x^2-y^2-z^2}}{2}.$$

Note that $\lambda_1 + \lambda_2 = 1$ as the trace of an original ρ is 1 and $\lambda_1, \lambda_2 \geq 0$. By the eigenvalue decomposition, ρ can be expressed as

$$\rho = \sum_i \lambda_i E_i, E_i E_j = \begin{cases} E_i & (i=j) \\ O & (i \neq j) \end{cases}, \mathrm{Tr}(E_i) = 1$$

Then, for a mixed state $\rho(x, y, z)$, $\log \rho$ is defined by

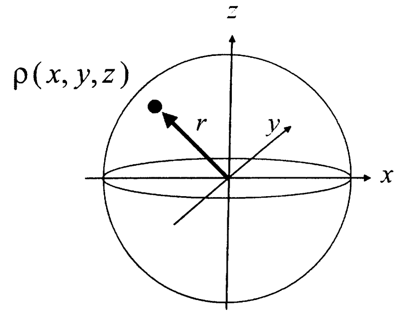

図 1 1 量子ビットのパラメータ空間を表すブロッホ球の内部の座標が量子状態を表している.

Fig. 1 The Bloch sphere: a point in a parameter space of 1-qubit represents a quantum state in the sphere.

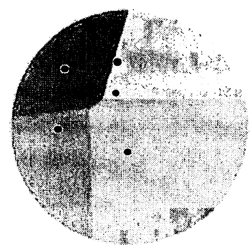

図 2 2 次元のブロッホ球での与えられた点に対する最遠点ボロノイ図.

Fig. 2 The farthest Voronoi diagram of given points in two dimensional Bloch sphere.

$$\log \rho = \sum_i (\log \lambda_i) E_i.$$

For a pure state, log is defined as an appropriate limit.

The farthest Voronoi diagram is defined as partitioning the plane into regions such that every point in the region around that site is farther to that site than to any of the other sites. The Voronoi edge is defined as a bisector of two sites whose regions are adjacent. It is different from the (nearest) Voronoi diagram, every site does not have its own region in the farthest one. Fig. 2 is an example of the farthest Voronoi diagram in a quantum space. Note that the Voronoi edge does not have Euclidean properties. The distance of two points denotes a quantum divergence which is described later.

Fig. 3 shows the geometric feature of a potential function and a distance-like divergence from θ to ρ in a general space. Note that the potential function is convex. Let given points be ρ, other points be θ and the θ-axis denote x, y, z dimensions. The divergence from θ to ρ is defined as the difference between the tangent hyperplane of θ and the potential function of ρ. For example, in a space of the classical information geometry, let the potential function be the Shannon entropy, a divergence is Kullbuck-Leibler divergence [3], [4].

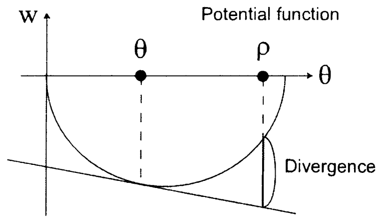

図 3 一般の空間におけるポテンシャル関数と接平面を用いて定義されたダイバージェンス.
Fig. 3 A divergence which is defined with using a potential function and a tangent plane in a general space.

表 1 空間とダイバージェンスの対応関係.
Table 1 The correspondence between a space and a divergence.

Space	Divergence
Information geometry	Kullbuck-Leibler divergence
Quantum	Quantum divergence

We expand the above result to a quantum space. Let the potential function be the von Neumann entropy, the divergence is defined as a quantum divergence. On the Bloch sphere, information-geometric structure can be induced by the von Neumann entropy as a potential function and the quantum divergence [5].

The von Neumann entropy $S(\theta)$ of a state θ is defined by

$$S(\theta) = \mathrm{Tr}(-\theta \log \theta).$$

Using the eigenvalues λ_1, λ_2 of ρ, it is expressed as

$$S(\rho) = \mathrm{Tr}(-(\sum_i \lambda_i E_i)(\sum_j (\log \lambda_j) E_j)) = -\sum_i \lambda_i \log \lambda_i$$

i.e., $S(\rho)$ is the Shannon entropy of eigenvalues. The quantum divergence $D(\theta||\rho)$ for two quantum states θ and ρ, where ρ is a mixed state, is defined by

$$D(\theta||\rho) = \mathrm{Tr}(\theta(\log \theta - \log \rho)).$$

It is known that $D(\theta||\rho) \geqq 0$, and $D(\theta||\rho) = 0$ iff $\theta = \rho$. The correspondence between a space and a divergence of Fig. 3 is shown in Table 1.

2.2 Dual coordinate systems

Note that the quantum divergence is non-commutative, namely $D(\theta||\rho) \neq D(\rho||\theta)$ in general. $D(\theta||\rho)$ is a distance from ρ to θ and similarly $D(\rho||\theta)$ is a distance from θ to ρ.

As easily seen in Fig. 3 and Table 1, making the distance from the given point ρ with using the von Neumann entropy, we obtain the quantum divergence $D(\theta||\rho)$. However, what we should analyze is $D(\rho||\theta)$. The reason is described in section 3.1. To solve the problem, the dual coordinate systems are introduced such that $D(\theta||\rho) = D^*(\rho||\theta)$, namely $D^*(\rho||\theta) \equiv D(\rho(\theta^*)||\theta^*)$. Here, we define the primal and the dual view as $D(\theta||\rho)$ and $D(\rho||\theta)$, and the primal and the dual

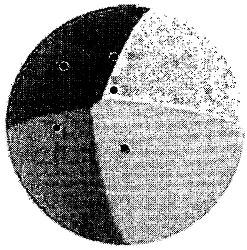

図 4 元の座標系での双対変換された最遠点ボロノイ図.
Fig. 4 The farthest Voronoi diagram from the dual view in the primal coordinate.

coordinate as D and D^*, respectively. That is to say, in Fig. 2, Fig. 4, and Fig. 5, the quantum divergence is denoted as $D(\rho||\theta)$, $D(\theta||\rho)$, and $D^*(\rho||\theta)$, respectively. The primal coordinate is transformed to the dual coordinate by the Legendre transformation. In the primal coordinate, let the potential function $-S(x,y,z)$ be $f(x,y,z)$. The distance r from the center of the sphere is $0 \leqq r = \sqrt{x^2+y^2+z^2} \leqq 1$. Then,

$$f = \frac{1+r}{2}\log\frac{1+r}{2} + \frac{1-r}{2}\log\frac{1-r}{2}.$$

The gradient of f is computed and is defined as (u,v,w).

$$\nabla f = \frac{1}{2}\left(\log\frac{1+r}{1-r}\right)\frac{1}{r}(x,y,z) \equiv (u,v,w).$$

(x,y,z) and (u,v,w) are in the primal and the dual coordinate, respectively. The function f in the dual coordinate is defined as

$$\begin{aligned} f^*(u,v,w) &\equiv (u,v,w)\cdot(x,y,z) - f(x,y,z) \\ &= -s + \log(2^{2s}+1), \end{aligned}$$

where $0 \leqq s \equiv \sqrt{u^2+v^2+w^2}$. Then, the gradient of f^* is

$$\nabla f^*(u,v,w) = \frac{2^{2s}-1}{2^{2s}+1}\frac{1}{s}(u,v,w) = (x,y,z).$$

Fig. 4 is the farthest Voronoi diagram $D(\rho||\theta)$ from the dual view in the primal coordinate. Since the Voronoi edge is curve, we transform Fig. 4 into Fig. 5 whose diagram is $D^*(\rho||\theta)$. Then, each Voronoi edge is mapped to the straight line in Fig. 5. We can define two farthest Voronoi regions $V_f(\rho_i)$ and $V_f^*(\rho_i)$ because of the asymmetry of the quantum divergence,

$$V_f(\rho_i) = \bigcap_{j\neq i}\{\theta \mid \rho(\theta) \in B, D(\rho_i||\theta) \geqq D(\rho_j||\theta)\} \quad (1)$$

$$V_f^*(\rho_i) = \bigcap_{j\neq i}\{\theta^* \mid \rho(\theta^*) \in B^*, D^*(\theta||\rho_i) \geqq D^*(\theta||\rho_j)\} (2)$$

Eq. (1) is from the dual view in the primal coordinate, that is Fig. 4, and Eq. (2) is from the dual view in the dual coordinate, that is Fig. 5.

In the computational geometry, the minimum enclosing

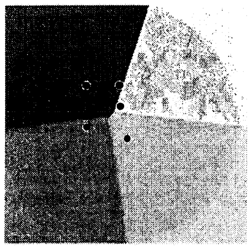

図 5 双対座標系での双対変換された最遠点ボロノイ図.
Fig. 5 The farthest Voronoi diagram of dual view in the dual coordinate.

sphere can be made from the farthest Voronoi diagram. The minimum enclosing sphere is defined as the smallest sphere which encloses all of a set of points in the sphere. In three dimensions, at most four points in the Bloch sphere determine the minimum enclosing sphere.

2.3 The minimum enclosing sphere

Let the given point be θ_i $(i = 1, \ldots, n)$. The following theorem holds.

[Theorem 1] Introducing the w-axis as the 4th one besides the 3-dimensional Bloch sphere, consider a graph of $w = -S(\theta)$ and its tangent plane h_i at $(\theta_i, -S(\theta_i))$. Then, a projection of the lower envelope, with respect to the w-axis, of h_i to the Bloch sphere is the farthest Voronoi diagram for n states θ_i in the Bloch sphere. A geometric feature is shown in Fig. 6.

Proof: On the interior of the Bloch sphere, $S(\theta)$ is differentiable and strictly convex, and hence there is a unique supporting hyperplane at $(\theta_i, -S(\theta_i))$, which is the tangent plane.

Consider a hyperplane $w = \mathrm{Tr}(\theta \log \theta_i)$ for variable θ and fixed θ_i. This is surely a hyperplane in θ. Since $D(\theta \| \theta_i)$ is nonnegative and is zero for $\theta = \theta_i$, it is a supporting hyperplane at $(\theta_i, -S(\theta_i))$. From the above discussion, this should be the tangent plane. Then, the theorem follows by similar arguments in the Euclidean Voronoi diagram with a paraboloid as its potential function and the Voronoi diagram in information geometry with respect to the Kullback-Leibler divergence [3], [4]. □

By applying standard algorithms for convex hulls (e.g., see [6]), we obtain the following.

[Corollary 1] The Voronoi diagram for n states θ_i in the Bloch sphere can be constructed in time $O(\min\{n^2, (n+F)(\log F)^2\})$ time where F is the number of faces of the diagram and $F = O(n^2)$ [7].

As its application, the minimum enclosing sphere of n points in the Bloch sphere, where the radius of the sphere is measured by the quantum divergence, can be computed within the same time. This minimum enclosing sphere problem for a finite set of points can be solved by changing the Euclidean distance to the divergence in standard algorithms for the minimum enclosing sphere in the Euclidean space, such as Megiddo [8]~[11], and we obtain the following.

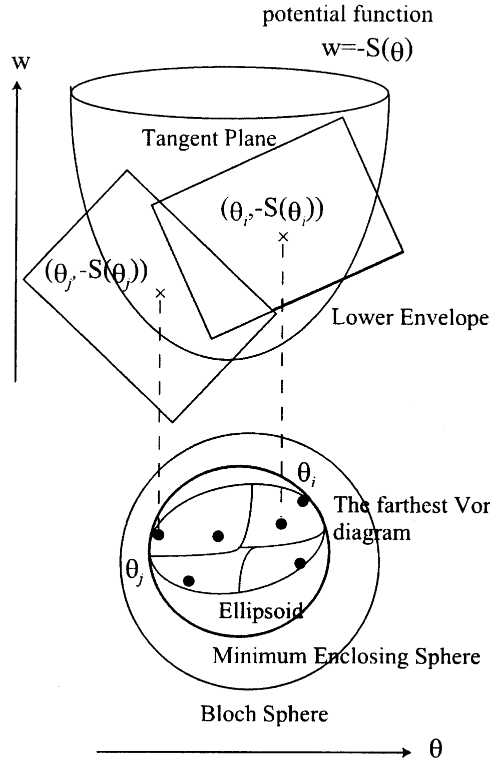

図 6 量子空間中の 1 量子ビットの状態と最小包含球問題.
Fig. 6 1-qubit states in the quantum space and minimum enclosing sphere problem.

[Theorem 2] The minimum enclosing sphere of n points in the Bloch sphere can be found in $O(n)$ time.

3. Algorithm

3.1 Holevo capacity

Considering the situation of sending a qubit to a quantum channel Γ with noise and receiving it, input states ρ and σ are affine transformed to output states $\rho' = \Gamma(\rho)$ and $\sigma' = \Gamma(\sigma)$ in Fig. 7. By this transformation, the Bloch sphere is reduced to the ellipsoid.

Then, the Holevo capacity [12] of this quantum channel is known to be equal to the radius from the center to a given point of the minimum enclosing sphere of

$$\{(x', y', z') \mid \rho'(x', y', z') = \Gamma(\rho(x, y, z)), (x, y, z) \in B\}$$

[13] and the radius is equal to the quantum divergence.

Holevo capacity $C(\Gamma)$ of a 1-qubit quantum channel Γ is shown that

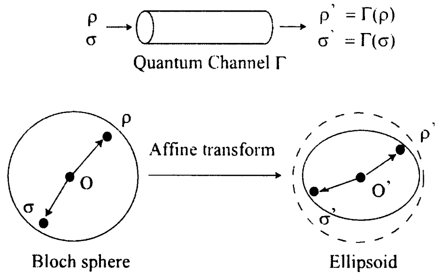

図 7　量子通信路を通った量子状態は雑音による影響を受ける．点 O と O' はそれぞれブロッホ球および楕円の中心．

Fig. 7　Quantum state is changed by noise of quantum channel. Points O and O' are the center of the Bloch sphere and the ellipsoid, respectively.

$$C(\Gamma) = \inf_{\theta} \sup_{\rho} D(\Gamma(\rho)||\Gamma(\theta)), \quad \theta, \rho \in B. \qquad (3)$$

As easily seen in Eq. (3), what we should analyze is $D(\rho||\theta)$, namely the distance from the center to a given point. How to compute the Holevo capacity of a 1-qubit quantum channel has been proposed [14], [15].

We extend the Voronoi diagram to a quantum space. A quantum state is continuum and the minimum enclosing sphere of given points is discrete quantity. Then, we consider quantization of quantum space and compute the complexity and an approximation error. The algorithm for computing the Holevo capacity of 1-qubit channel is as follows.

(1) Discretize the quantum space.
(2) Map all intersections to quantum states.
(3) Put them into a quantum channel.
(4) Obtain output states.
(5) Transform them to the dual coordinate.
(6) Compute the farthest Voronoi diagram of them.
(7) Obtain the radius of the minimum enclosing sphere.

3.2 Approximation error

An approximate solution to the minimum enclosing sphere is first found by discretizing the boundary of the Bloch sphere by a mesh of points, and then, using an obtained approximate solution as an initial solution, nonlinear optimization is further performed to obtain an optimal sphere. In this process, to guarantee the convergence in the nonlinear optimization process, it is better to solve the discretized problem for many points. In [15], the nonlinear programming package used in the latter step is applied also to the former step, and in Fig. 8, the approximation error is seen to be $O(1/n)$ for a regular mesh of n points in total.

Assuming the error for n points is $O(1/n)$, we obtain the following.

[Theorem 3]　Under the above-mentioned assumption, an n-approximation of the Holevo capacity of a 1-qubit quantum channel can be computed in $O(1/n)$ time.

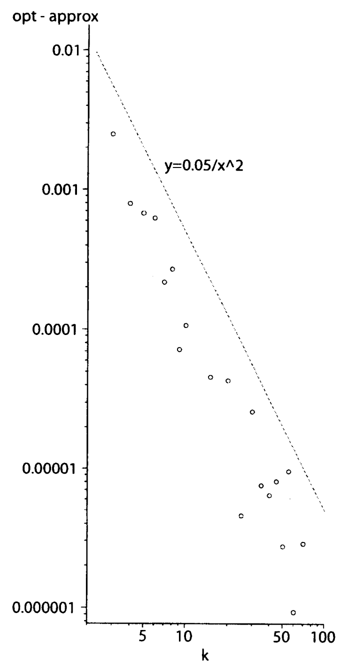

図 8　横軸 x はメッシュの数 $n(=x^2)$ で，縦軸は近似誤差である．

Fig. 8　Approximation values by $(k^2 - k + 2)$-point mesh. The horizontal x-axis is a log plot of k, and the vertical y-axis is a log plot of the difference to the optimum value in bit. A line $y = 0.05/x^2$ is drawn for reference. (from [15])