連載講座

量子情報処理パラダイム
5. 量子計算と最適化

今井　浩

1. 量子情報処理の講座最終回にあたって

これまで4回，量子情報処理の基礎から先端の実験・組合せ構造との関係など多岐に渡って見てきた．量子コンピュータや量子暗号がはやっている研究分野ということでもあるので，地道な骨太の部分を取り上げて質実に書くことを目指した点もあり，研究の最先端の華やかさは押えぎみであったかもしれないが，オペレーションズ・リサーチでの最適化技法・統計技法・組合せ論などがいかにこの先端分野で新展開が図られてきたかを見て頂けたかと期待している．

最終回では，最適化技法の量子情報処理での展開の具体例を軸に述べてみたい．初回のはじめにで書き，またこの連載で繰り返し出てきたように，「量子状態は一般に複素行列でエルミート・非負定値・トレース1の行列で表される．このことだけからも，量子計算・情報での基礎的問題に，半定値計画問題が現れることは容易に想像頂けるだろう.」ということで，この点を詳しくみていく．本稿で，2-4節のより詳しい内容はImai, Hachimori, Hamada, Kobayashi, Matsumoto [6]にある．

2. 最適量子測定デバイス設計

量子状態の一般的な表現である密度行列と，測定の一般論であるPOVM測定について復習しておこう．量子状態は，対応する次元dをもってきて，次の条件を満す$d\times d$複素行列ρで数理的に表現できる: (1) $\rho=\rho^*$, (2) $\rho\geq 0$, (3) $\mathrm{Tr}\,\rho=1$. *は共役転置を表し，$\rho\geq 0$は，ρが非負定値であることをいい，$\mathrm{Tr}\,\rho$はρのトレースであり，対角要素の総和である．

量子状態から何らかの情報を得るには，測定をしないといけない．本稿でも得られる情報は有限でm個の事象であるとしよう．すると，測定の数理モデルは，m個のエルミート非負定値行列M_iの集合$\{M_1,\ldots,M_m\}$で，和が単位行列になるものとなる．

$$M_l=M_l^*\geq 0\ (l=1,\ldots,m),\quad \sum_{l=1}^{m}M_l=I.$$

そして，密度行列ρの量子状態に対してこの測定を行うと，測定から得られる確率変数Xとそのとる値$\{1,\ldots,m\}$に関して次が成立する．

$$\Pr(X=l)=\mathrm{Tr}\,\rho M_l\ \ (l=1,\ldots,m).$$

このような測定系をPOVM (Positive Operator Valued Measure)と呼んでいた．

量子情報処理では，量子状態の計算なり通信なりを行って最終的に測定を行うことによって情報を得る．この部分は，量子力学の測定デバイスによって実現される．POVMの行列がその測定デバイスを決定するパラメタになっている．実際に任意のPOVMに対して測定デバイスが作れる厳密な保証はないものの，数理的関連からはそれが最も一般的な形であると思われている

すると，与えられた一般の量子状態に対して，いくつかの候補を考え，そのどれが一番もっともらしいかを判断するためのPOVMを求める問題が考えられる．具体的には，m個の量子状態$\rho_1,\ldots,\rho_m$が，それぞれ$\xi_1,\ldots,\xi_m$の確率で起るとき，与えられた状態がそのm個のうちのどれであるかを判定することを考える．この問題は，ベイズ的に最適化問題として定式化できる．$c_{ij}(\geq 0)$を本当の状態がρ_iであるのに状態ρ_jであると判定してしまう費用(ペナルティ)とする．POVMを$M=\{M_1,\ldots,M_m\}$とすると，確率$P(j|i)=\mathrm{Tr}\,\rho_i M_j$で本当の状態$\rho_i$を状態$\rho_j$と測定してしまうことになる．このとき，平均費用は

$$C(M)=\sum_{i,j}\xi_i P(j|i)c_{ij}=\sum_j \mathrm{Tr}\left(\sum_i \xi_i\rho_i c_{ij}\right)M_j.$$

いまい ひろし　東京大学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 同文京区本郷5-28-3 本郷ホワイトビル

と表される．

ここで，$\sum_i \xi_i \rho_i c_{ij}$ を W_j $(j=1,\ldots,m)$ と表すと，W_j は生起確率などから定まる j にのみ依存する定数で，平均費用を最小にするPOVMを求める問題として

$$\begin{aligned} \min \quad & \sum_j \mathrm{Tr}\, W_j M_j \\ \text{s.t.} \quad & \sum_j M_j = I, \quad M_j^* = M_j \geq 0 \end{aligned}$$

として定式化される．この問題は，Yuen, Kennedy, Lax [14] によって1975年に考えられた．

この問題は，まさしく半定値問題である．今の言葉でいうと，その論文では，凸計画に対する双対定理を適用して，主問題のPOVMの制約が1次元の場合は単体の制約に対応するという基本的な形であることから最適性の条件で最適双対変数を代入操作で削除することができ，主結果として最適性の条件を最適主変数のみで書き下すということが行われている．

式で見ていくと，双対問題は

$$\begin{aligned} \max \quad & \sum_j \mathrm{Tr}\, L \\ \text{s.t.} \quad & L \leq W_j \end{aligned}$$

となり，相補性条件は

$$\sum_j \mathrm{Tr}\, M_j(L - W_j) = 0.$$

となる．条件 $M_j \geq 0$, $W_j - L \geq 0$ より，相補性条件は $M_j(L-W_j) = (L-W_j)M_j = 0$ に等価であることがいえ，$\sum_j M_j = I$ であることを用いると，最終的に最適性の条件として

$$\sum_j M_j W_j = \sum_j W_j M_j \geq W_k \quad (k=1,\ldots,m)$$

が得られる．

ただし，以上は有限次元で，候補の量子状態も有限の場合の話である．量子状態は無限次元Hilbert空間でのエルミート非負定値のトレース1の作用素として表せる場合もあり，その場合は無限次元半定値計画問題となって，無限次元凸解析でmin, maxとならずinf, supでしか成り立たない場合を適切に扱うことが必要となる．さらに，候補の量子状態が有限離散でない場合は，別の無限性も出てくる．このあたりをYuenらの論文では議論しているが，その議論自体は現代の理論で整理しておくといいのだろう．最近の論文Eldar, Megretski, Verghese [2] はこの方向を論じている．

量子状態の条件から，まさしく最適測定器を作ろうなどと思うと，半定値制約のもとの最適化問題にすぐなるのである．

3. 量子計算量理論での半定値計画の応用

前節では，POVMの条件そのものが半定値計画の制約式となる場合をみた．他に量子情報で半定値計画と密接に関係するものに，一般の量子状態を他の一般の量子状態に変換するもっとも汎用的な変換であるトレースを保存する完全正写像がある．次にこれを見ていこう．

急に計算量理論の話になって恐縮だが，1990年頃の計算量理論の一大成果の1つにIP=PSPACEがある (Shamir [13] など参照)．IP (Interactive Proof) とは，無限の計算能力をもつ証明者と多項式時間の計算能力をもつ検証者が，多項式回の対話を通して証明者の主張の正しさを検証者が確認できる計算量クラスである．PSPACEは多項式領域計算量で解ける問題のクラスで，NP完全よりも難しい問題クラスである．この2つが等しいということで，従来の計算モデルの代表的な計算量クラスであるPSPACEが，対話証明という新しい計算モデルのIPというクラスに等しいことが示されたわけだ．対話証明は応用面では認証にも発展するもので，この結果は計算量理論・現代暗号論での1つのマイルストーンになっている．

このように通常の計算モデルと，対話証明という新計算モデルに古典計算の枠組みでは対応がついているので，量子計算の観点からは，それぞれを量子計算に拡張したときに対応がどうなるのかということが知りたくなる．Kitaev, Watrous [7] は，Watrousが提案した量子対話証明のクラスQIP (Quantum Interactive Proof) と従来の古典計算量クラスのPSPACEの関係を調べ，

$$\mathrm{PSPACE} \subseteq \mathrm{QIP} \subseteq \mathrm{EXP}$$

を示している．ここで，EXPは指数時間計算量のクラスである．どうやらPSPACEよりQIPの方が真に大きそうな傍証もあるので，もしそうならこれで量子化することによって少なくとも古典の対話証明よりは強力になることがわかり，ただし上からは古典のEXPで押えられることになる．

ここでのQIP $\subseteq$ EXPの証明にKitaev, Watrousは半定値計画と，それが多項式時間で解けることを使っている．ここではその核となる部分のみ述べる．

N_1, N_2, M を正整数とし，$B_{1,1},\ldots,B_{1,k_1}$ を $M \times N_1$

複素行列，$B_{2,1},\ldots,B_{2,k_2}$ を $M\times N_2$ 複素行列とし，写像 $T_i:\mathbb{C}^{N_i\times N_i}\to\mathbb{C}^{M\times M}$ $(i=1,2)$ を

$$T_i(Y)=\sum_{j=1}^{k_i}B_{i,j}YB_{i,j}^*$$

とする．このとき，与えられた $\epsilon>0$ に対して，次の2つのうちのどちらか一方のみが成立するとする．

1. エルミート・非負定値・トレース1の複素行列 Y_1, Y_2 が存在して，$T_1(Y_1)=T_2(Y_2)$ を満す．
2. 任意のエルミート・非負定値・トレース1の複素行列 Y_1, Y_2 に対して，

$$\|T_1(Y_1)-T_2(Y_2)\|>\epsilon$$

が成立．ここで，$\|\cdot\|$ は

$$\|H\|=\sup_{x\neq 0}\frac{\|Hx\|}{\|x\|}$$

(右辺の $\|\cdot\|$ は L_2 ノルム)．

Kitaev, Watrous はこの問題が半定値計画問題を用いて多項式時間で解けることを示している．そして，量子対話証明の問題を入力の指数個のパラメタをもつこの問題として定式化できることを示し，したがって半定値計画アルゴリズムを用いて古典計算で指数時間で解けることを示した．

対話証明には証明者が多数いるバージョンがあり，その場合の クラスは MIP (Multi-prover Interactive Proof) と表される．このクラスは非決定性指数時間計算量クラス NEXP と等しいことがわかっている．Kobayashi, Matsumoto [8] は量子版を考えても能力が上がらないことを示している．

T_i という写像は，量子対話証明の問題として表すときには完全正写像に対応し，実際には一方が他方の情報はわからず自分だけの情報で量子状態を操作するという部分トレースを取ることに関係している．このように単に量子状態である密度行列や POVM で半定値性が出てくるだけでなく，完全正写像も半定値計画に関係してくるということで，量子情報は半定値計画の宝庫となっている．

4. 通信路容量

次に凸計画さらに半定値制約の全域的最適化問題の話をしよう．古典通信では通信路符号化定理によって，誤りがある通信路を用いてもうまく符号化すると誤りをいくらでも小さくできるための伝送レート，すなわち通信路容量を特徴づける理論が Shannon 以来確立されている．量子状態で伝送する量子通信路を用いると，さらに通信路容量を大きくすることが期待でき，今は量子通信路符号化定理も確立された．これらの通信路容量で凸計画・半定値制約の最適化問題となる．

4.1 古典通信路容量

離散・無記憶の古典通信路とは，入力記号 $A=\{a_1,\ldots,a_m\}$ と出力記号 $B=\{b_1,\ldots,b_n\}$, そしてその間の確率遷移行列

$$V=(V_{ij})\quad(\sum_{j=1}^{n}V_{ij}=1\ (i=1,\ldots,m))$$

からなる．$V_{ij}=P(b_j|a_i)$ は a_i を送信したときに b_j が受信される確率で，通信路のパラメタとなっている．

Shannon の通信路符号化定理は，このような通信路を使ってうまく符号化したとき送れる最大伝送レート $C(V)$ を与えており，次のように述べられる．

定理 1 (古典通信路符号化定理):

$$C(V)=\max_{p=(p_i):\sum_{i=1}^{m}p_i=1,\ p_i\geq 0}I(p,V),$$

ここで

$$I(p,V)=\sum_i\sum_j p_iV_{ij}\log\frac{V_{ij}}{\sum_k p_kV_{kj}}.$$

である． □

この定理の $I(p,V)$ は相互情報量であり，2つの確率分布 $q=(q_i)$, $r=(r_i)$ の間の Kullback-Leibler ダイバージェンス

$$D(q\|r)=\sum_j q_i\log\frac{q_i}{r_i}$$

を用いて

$$I(p,V)=\sum_i p_iD(V_{i\cdot}\|pV)$$

と表される ($q=pV$ は $q_j=\sum_i p_iV_{ij}$ で定義される確率分布)．

相互情報量 $I(p,V)$ は $p=(p_i)$ に関して凹であり，したがって古典通信路符号化定理の右辺による容量計算というのは単純な線形制約のもとでのその最大化となる．すなわち，凸計画問題の典型例となる．

この容量計算については，情報理論の方で EM アルゴリズムのような交代的極大化アルゴリズムが有名であるが (たとえば Cover, Thomas [1] の教科書参照)，今の数理計画ソフトなら単に式を上のように書いてパラメタを与えるだけで簡単にこの容量計算を行える．

4.2 量子通信路容量

量子無記憶通信路Γは，$\mathbb{C}^m$上の入力状態の集合S_1，すなわち$\mathbb{C}^{m\times m}$の密度行列の集合から，$\mathbb{C}^n$上の出力状態の集合S_2への完全正写像$\Gamma: S_1 \to S_2$として与えられる．ちなみに，完全正写像は確率遷移行列を表現できるのであったから，量子通信路は古典通信路の素直な拡張になっている．

この量子通信路の通信容量$C(\Gamma)$については，1973年頃にHolevoによって上界が示されて以降，それがタイトであるかどうかがずっと未解決であったが，量子情報・量子暗号・量子計算の進展に伴ってついに1990年代後半になって完全に証明された(Holevo [5], Schumacher, Westmoreland [12]).

定理 2 (量子通信路符号化定理):

$$C(\Gamma) = \sup_{\pi\in\Pi} I(\pi,\Gamma).$$

ここで，

$$\Pi = \{\pi = (\lambda_1,\ldots,\lambda_d;\sigma_1,\ldots,\sigma_d) \mid \lambda_i \geq 0,\ \textstyle\sum_i \lambda_i = 1,\ \sigma_i \in S_1\}$$

であり，$d = n^2$で，

$$I(\pi,\Gamma) = \sum_i \lambda_i \mathrm{Tr}\,\Gamma(\sigma_i)[\log\Gamma(\sigma_i) - \log\Gamma(\bar{\sigma})]$$

そして$\bar{\sigma}$は$\bar{\sigma} = \sum_i \lambda_i\sigma_i$のような確率的混合である．□

この場合は，量子相互情報量$I(\pi,\Gamma)$は，量子版のKullback-Leiblerダイバージェンスを用いて古典の場合と同様に記述される:

$$D(\sigma\|\rho) = \mathrm{Tr}\,\sigma[\log\sigma - \log\rho].$$

またここで，ρの固有値分解を

$$\rho = \sum_i \lambda_i \boldsymbol{v}_i\boldsymbol{v}_i^*,$$

としたとき，

$$\log\rho = \sum_i (\log\lambda_i)\boldsymbol{v}_i\boldsymbol{v}_i^*,$$

である．関連して，密度行列ρの量子状態のvon Neumannエントロピー$H(\rho)$は

$$H(\rho) = \mathrm{Tr}\,[-\rho\log\rho] = \sum_i -\lambda_i\log\lambda_i$$

である．密度行列固有値の和は1で非負なので，量子状態ρのvon Neumannエントロピーは，その固有値のShannonエントロピーとなっている．

混合パラメタ$\sigma = (\sigma_i)$を固定した場合，$I(\pi,\Gamma) = I((\lambda,\sigma),\Gamma)$は$\lambda = (\lambda_i)$に関して凹となる(古典の場合と同様)．従って，この固定された場合の量子通信路容量計算は凸計画問題となり，ただしその計算では行列の対数を上の意味で計算する必要がある．

しかし，もっとも一般の問題である$\sup_{\pi\in\Pi} I(\pi,\Gamma)$を解こうとすると，$I(\pi,\Gamma)$は$\pi$に関して凹とも凸とも限らず，非常に難しくなる．量子情報理論の方から，古典の交代的極大化アルゴリズムを拡張したアルゴリズム(Nagaoka [10])も提案されているが，この容量計算は最適化問題にとってのチャレンジと思われる．

このように単なる半定値計画だけでなく，凸計画，さらには半定値制約のついた凸計画，もっとも一般の非凸計画まで量子情報処理の分野では様々な最適化問題が現れるのである．

5. 量子情報の組合せ論

通信路容量の節でエントロピーが出てきたが，古典のShannonエントロピーに関連して離散最適化で非常に重要な劣モジュラ関数が現れる．これが量子のvon Neumannエントロピーの場合でどうなるか見ていこう．

まずFujishige [4]により示されたShannonエントロピーから導かれるポリマトロイドについてまとめる．n個の確率変数Z_iで，各Z_iは1からk_iの整数の値をとるものからなる同時確率分布

$$\Pr(Z_1 = i_1,\ Z_2 = i_2,\ldots,\ Z_n = i_n) \quad (1 \leq i_j \leq k_j,\ j = 1,\ldots,n)$$

を固定する．これは$\prod_{i=1}^n k_i$次元の有限離散分布である．$E = \{1,2,\ldots,n\}$とし，$S \subseteq E$に対してSに入っていない添字についてすべて和をとると，$\prod_{i\in S} k_i$次元の有限離散分布が周辺分布として得られる．このSに関する周辺分布のShannonエントロピーを$h(S)$と定める．hは$h: 2^S \to \mathbb{R}$の集合関数である．

定理 3 (Fujishige [4]): (1) $h(\emptyset) = 0$

(2) $h(X) \leq h(Y)$ $(X \subseteq Y)$

(3) $h(X) + h(Y) \geq h(X\cup Y) + h(X\cap Y)$

(2)は集合関数としての単調非減少性であり，(3)は劣モジュラ性である．この定理の(1), (2), (3)の条件を満たす集合関数は，ポリマトロイドのランク関数であり，ポリマトロイドを定める．このように，同時分布を固定して得られる周辺分布のShannonエントロピーは，ポリマトロイドを構成する．Fujishige [4]で

は，ポリマトロイドの観点からみた情報理論展開がなされている．

量子の von Neumann エントロピーの場合はどうであろうか．まず，周辺分布に対応する操作であるが，それは部分トレースということであった (連載初回参照)．そこで，$\mathcal{H}_i = \mathbb{C}^{k_i}$ とし，$\mathcal{H} = \otimes_{i=1}^{n}\mathcal{H}_i$ とする．以下，$\mathcal{H}$ 上の密度行列 ρ を 1 つ固定する．$X \subseteq E = \{1,\ldots,n\}$ に対して，$\mathcal{H}(E-X) = \otimes_{i\in E-X}\mathcal{H}_i$ とし，

$$h_\rho(X) = H(\mathrm{Tr}_{\mathcal{H}(E-X)}\,\rho)$$

と定めると次の定理が成り立つ (本質的には Lieb, Ruskai [9] により示されている (この文献をご教示頂いた理化学研究所林正人氏に感謝します))．

定理 4: h_ρ は次の 3 つの条件を満たす．

(1) $h_\rho(\emptyset) = 0$

(2) $h_\rho(X) + h_\rho(Y) \geq h_\rho(X\cup Y) + h_\rho(X\cap Y)$

量子の世界では単調性は成立しない．たとえば，純粋状態では固有値は 1 と他は全て 0 ということで von Neumann エントロピーは 0 であるが，それの部分トレースをとってできる状態は一般に混合状態であり，正の値のエントロピーをもちえる．

一方，h_ρ が離散システム論の劣モジュラシステムを引き続き構成することは興味深い．h_ρ に関する基本分割などの量子情報理論的意味付けはまだ明確でない．また，基本分割を求めることなどは劣モジュラ関数最小化の応用例になるが，今のところ h_ρ の計算自体が定義通りに行うと指数時間かかる難点がある．

6. 量子計算シミュレータ

最後に最適化ではないが，現在のコンピュータを用いた量子計算のシミュレーションについて触れる．

現在までに実現されている量子コンピュータは，NMR 量子コンピュータで数量子ビットまでで，Shor の量子素因数分解アルゴリズムを実現して $3\times 5 = 15$ の素因数分解をしたというところまでである．数十量子ビットはまだまだ見えていない．量子コンピュータの実現を待たずに数十量子ビットの量子アルゴリズムを動作させて，そのアルゴリズムの実際の挙動を知ることはできるだろうか．

今や何でも (とまではいかないかもしれないが) コンピュータで「作る」時代である．Computer-Aided ZZZ で ZZZ が昔は VLSI や機械 CAD だけであったが，今や Drug Design とか DNA Chip とか本当に多岐にわたってのものがコンピュータ上で仮想的にも実際的に

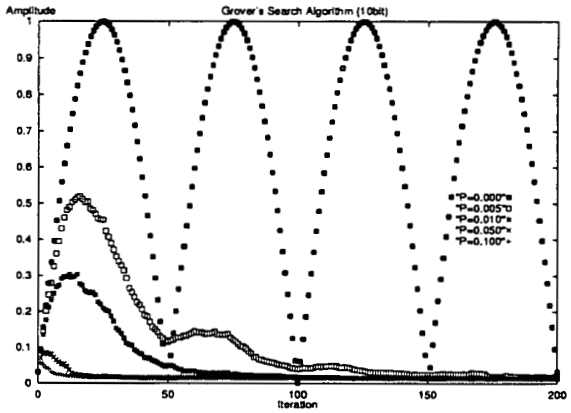

図 1: 10 量子ビットの Grover の量子探索アルゴリズムで，depolarizing channel モデルでデコヒーレンスが起こった場合のシミュレート結果．特定部位の振幅 (縦軸) が反復 (横軸) に従って変化するグラフ．理想的には完全に周期的な振る舞いをするが，デコヒーレンスによって減衰していく度合いが観測されている．

も設計されている．当然，量子コンピュータも今のコンピュータでシミュレートでき，かつ設計にも有用だと思われる．

もちろん，量子コンピュータが考えられたのは，今のコンピュータのモデルでは量子力学の計算をするのに指数時間の爆発的な時間がかかるのが，量子コンピュータなら効率よく実行できるということであったのだから，たとえ並列コンピュータを使おうとも限界があるのはその通りである．しかし，数十量子ビットのシミュレートが先にできていれば，実際に物理的実現ができた際の検証に用いることができるし，そこにいたる以前に物理的実現へのフィードバックが非常に期待できる．

Niwa, Matsumoto, Imai [11] は，30 量子ビット程度のサイズの量子計算シミュレータを開発して，すでに予備的な結果を得ている．それには大量のメモリでもって指数爆発する空間を表現するとともに，並列実行によって高速化を図っている．詳細はまた他の先の機会に譲るとして，ここではそのシミュレータを用いて計算した，Grover のアルゴリズムの中でデコヒーレンスという量子特有の誤りが起った場合の影響を示すシミュレーション結果のグラフを図 1 に示しておく．

7. おわりに

本連載では，科学技術振興事業団の創造科学技術推進事業である ERATO 今井量子計算機構プロジェクト

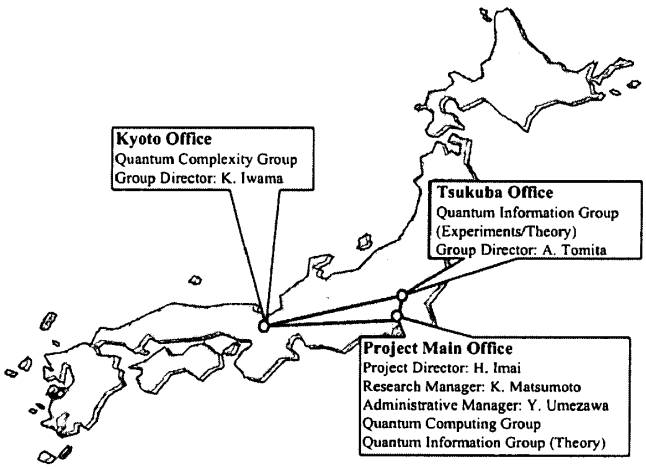

図 2: ERATO 量子計算機構プロジェクトの 3 オフィス

の関係者の方に解説を願った．そのプロジェクトでは，量子情報理論，量子推定，量子クローン限界，量子計算量理論，量子アルゴリズム論，量子オートマトン，位相的量子計算，量子回路理論，単一光子発生，光に基づく量子計算・量子暗号，量子通信など，幅広い研究活動を進めている．実験成果の方でもこの 5 月に光子検出器に関する新聞発表を行った．ERATO プロジェクトの組織としては，総勢20名を越える体制で，東京の事務所も併設されたオフィスを中心に，京都オフィスもかまえ，さらに筑波にも光を中心とした量子計算・量子暗号の研究を推進するオフィスも設置して研究を進めている (図 2)．色々な活動などはホームページ [3] に掲載されているので，そちらを参照頂ければ幸いである．

最後に，この連載の話を頂いた編集委員の皆様に感謝したい．この新しい量子情報処理の分野で，最適化からモデリング手法までのOR手法が広く適用されることを願っており，自分自身としてもこの方向をどんどん進めると同時に，本連載に興味を持って頂いて研究活動して頂ける方が出てこられる望みを最後に書いておわりとしたい．

参考文献

[1] T. M. Cover and J. A. Thomas: *Elements of Information Theory*, Wiley, 1991.

[2] Y. C. Eldar, A. Megretski and G. C. Verghese: Designing Optimal Quantum Detectors via Semidefinite Programming arXib:quant-ph/0205178, 2002.

[3] ERATO 今井量子計算機構プロジェクト, JST: `http://www.qci.jst.go.jp/`

[4] S. Fujishige: Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control*, Vol.39, No.1 (1978), pp.55–72.

[5] A. S. Holevo: The Capacity of Quantum Channel for General Signal States. *IEEE Transactions on Information Theory*, Vol.44 (1998), pp.269–273.

[6] H. Imai, M. Hachimori, M. Hamada, H. Kobayashi and K. Matsumoto: Optimization in Quantum Computation and Information. *Proceedings of the 2nd Japanese-Hungarian Symposium on Discrete Mathematics and Its Applications, Budapest*, April 2001,

[7] A. Kitaev and J. Watrous: Parallelization, Amplification, and Exponential Time Simulation of Quantum Interactive Proof Systems. *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, 2000, pp.608–617.

[8] H. Kobayashi and K. Matsumoto: On the Power of Quantum Multi-Prover Interactive Proof Systems. arXiv:cs.CC/0102013, 2001.

[9] E. H. Lieb and M. B. Ruskai: A Fundamental Property of Quantum-Mechanical Entropy. *Physical Review Letters*, Vol.30 (1973), pp.434–436.

[10] H. Nagaoka: Algorithms of Arimoto-Blahut Type for Computing Quantum Channel Capacity. *Proceedings of the International Symposium on Information Theory (ISIT)*, Cambridge, MA, USA, August 1998.

[11] J. Niwa, K. Matsumoto and H. Imai: General-Purpose Parallel Simulator for Quantum Computing. arXiv:quant-ph/0201042, 2002.

[12] B. Schumacher and M. D. Westmoreland: Sending Classical Information via Noisy Quantum Channels, *Physical Review A*, Vol.56 (1997), pp.131–138.

[13] A. Shamir: IP = PSPACE. *Journal of the Association for Computing Machinery*, Vol.39, No.4 (1992), pp.869–877.

[14] H. P. Yuen, R. S. Kennedy and M. Lax: Optimum Testing of Multiple Hypotheses in Quantum Detection Theory. *IEEE Transactions on Information Theory*, Vol.IT-21, No.2 (1975) pp.125–134.