代数的量子情報処理技術の研究
Study on Algebraic Quantum Information Processing

濵田　充
Mitsuru Hamada
玉川大学学術研究所
Tamagawa University

概要：量子計算においてデコヒーレンス等の量子雑音に抗する技術として，また量子暗号の中心的情報処理機構として，高性能な代数的量子誤り訂正符号が求められている．本研究では，符号の持つシンプレクティック幾何の構造に注目し，これまでに理論的・定量的に存在を証明してきた高性能な符号をもとに，様々の場面に利用可能な量子符号や同様の構造を持つ量子情報処理方式(量子エンタングルメント蒸留など)を実際に設計することを目指してきた．その狙いに即した成果をここに報告する．

【研究のねらい】 量子計算においてデコヒーレンス等の量子雑音に抗する技術，また量子暗号の中心的情報処理機構として，高性能な代数的量子誤り訂正符号が求められている．報告者はこれまでに代数的量子符号として定量的にどれだけ良いものが存在し得るかを理論的に明らかにした．本提案の研究では，これまで存在のみが知られていた高性能の量子符号や関連する量子情報処理方式を実際に設計あるいは発見することを第一の目標としている．

報告者は，本さきがけ研究開始以前から，上記の代数的符号の根底にある概念に Weyl の有限代数系の射影表現とその交換関係（これは正準交換関係に形式的に類似する）があること，その交換関係が背後にある代数の幾何的な性質で記述されること，その概念は量子符号以外にも，エンタングルメント(もつれ)蒸留，量子テレポーテイションなど多くの量子情報処理技術において陰に陽に使われていることなどを指摘し，これらの技術の理論的研究を進めてきた．

特に，本研究では冒頭に述べたように代数的量子誤り訂正符号に重点を置くが，これはシンプレクティック符号(ステイビライザ符号)のことを指す．シンプレクティック符号は古典の線形符号（線形誤り訂正符号，あるいは単に符号）に類似した構造を有する．

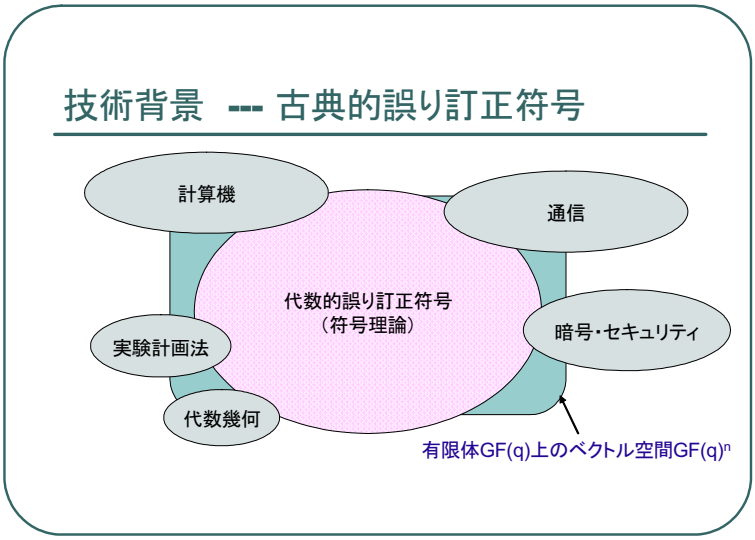

図 1　技術背景

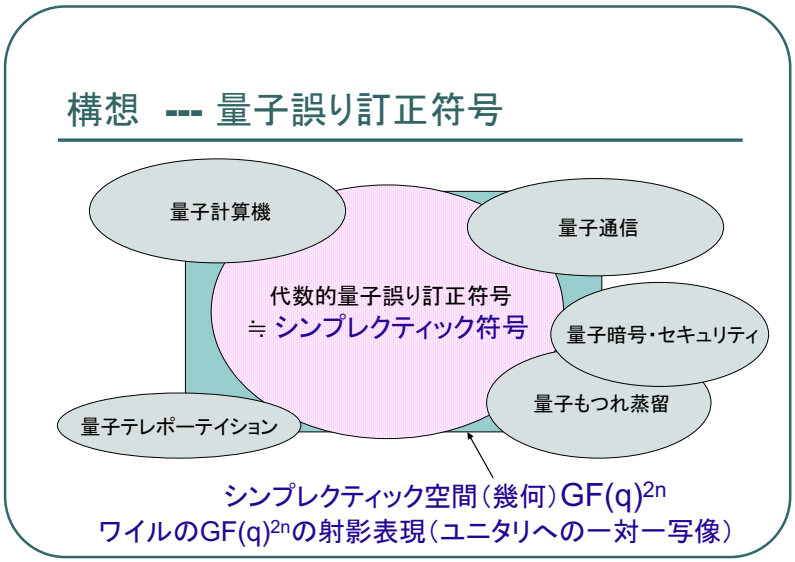

図２　研究構想

古典の符号の応用の広さは周知の通りであるが(図１)，このような技術の広がりを量子的な対応物であるシンプレクティック符号についても期待している(図２)．

より具体的に，研究提案時に掲げた研究目的は以下の通りである．

1)量子計算機の実現に向けた新しい量子誤り訂正符号の提案，設計，開発，性能解析．

2)量子暗号システムの実現に向けたより優れたCSS符号の提案，設計，開発，性能解析．

3)エンタングルメント蒸留など関連する代数的量子情報処理方式の提案，設計，開発，性能解析．

4)これらの技術の統一的な視点からの理論的整備，および更なる応用の探索．

5)通信路容量のような代数的量子情報処理方式に関連する理論的問題の探求．

【研究方法】 目的の 1），2），3）は具体的なもので，一括りに代数的量子誤り訂正符号の設計ということができる．これについては，「研究のねらい」で述べた古典符号とシンプレクティック符号の類似性を利用し，古典で知られている符号設計の方法論に根ざした方法でシンプレクティック符号の設計を行う．

また，次の2つを区別して研究を進めることが必要と考えた．

i)　一般のシンプレクティック符号，

ii) CSS符号．

i) はii) のクラスを含むのであるが，このように分けるのは，現状の技術でii) が量子暗号に用いることができるという事情からである．なお，原理的にはi)も暗号として使えるが，その実現には多粒子間のエンタングルメントを自由に操る高速の量子計算機が暗号プロトコルの参加者に必要となる．

また，符号の評価基準としては

(c1) 情報理論的基準：復号誤り確率

(c2) 符号理論的基準：符号の最小距離

が知られている．本研究では，(c1)が重要だが(c2)も扱う．これは，主に，本研究の文脈では(c1)が正統な基準なのだが，比較すべき従来結果の殆どが(c2)を用いているという事情からである．

目的の4),5)については主要テーマ1),2),3)に対して付随的なものという位置づけだが，結果的には主要結果の意義を裏付けるような形で4),5)に関する結果を得た（次節 (4)および (6)）．

【研究成果】 (1)代数的量子誤り訂正符号の一般的構成法．(2)前項の一般的構成法を用いた(c1)の意味で高性能な代数的量子誤り訂正符号の明示的構成．(3) 前々項の一般的構成法を用いた(c2)の意味で高性能な代数的量子誤

り訂正符号の明示的構成．(4) 構成した符号を含む代数的量子誤り訂正符号の情報セキュリティへの応用と解析．(5) 共役符号対の小さな集団の明示的構成．(6)その他．

以下，物理的背景および予備知識の整理の後これらの成果を順に説明する．

(0a) 物理的背景

本研究の大方は有限体とその上のベクトル空間を土俵として行われており，物理は然程必要としないが，物理との直接的な繋がりがあることを理解いただくため「研究のねらい」でも述べた本研究の根底にある本質的な概念を以下に説明する．これは物理的でもあり代数的あるいは幾何的でもある．

シンプレクティック符号は古典の線形符号に類似していると書いたが，勿論シンプレクティック符号をシンプレクティック符号ならしめる本質差異もある．すなわち「シンプレクティックな内積」（正確には内積ではなく双線形形式）である．この根底にある概念は実は，量子力学において極めて基本的なもので，ある互いに共役な関係にある量の間に成り立つ交換関係である. これは, 大まかには, Weyl 型の正準交換関係の離散版ともいえる. より具体的には，情報処理を担う素子が q 準位系であるとして，整数 0,1,…,q－1 からなる集合 Zq に q を法とする演算を考える．本報告では q が素数と仮定する．特に，このとき Zq は有限体 GF(q)となる．GF(q)の元を n 個ならべてできる n 次元ベクトル x と z を組にして 2n 次元ベクトル(x,z)を考える．そして Weyl によるこのベクトル空間の射影ユニタリ表現 N(x,z)を考えると，その交換関係がシンプレクティックな内積で記述されるのである．すなわち，交換関係は N(x,z)N(x’,z’)＝exp(i2πf(x,z,x’,z’)/q)N(x’,z’)N(x,z)で f が「内積」である．これが意味する最も重要な事実は N(x,z)と N(x’,z’)が交換する必要十分条件は f(x,z,x’,z’)=0 であるということである. なお q=2 のとき N(x,z)は n 個のパウリ行列または単位行列のテンソル積の形で書ける．シンプレクティック符号とは互いに交換するいくつかの N(x,z)の同時固有空間のことであり（勿論復号操作は別に与える），交換する N(x,z)たちを取るというのは，N に通す前の(x,z)で言い直せば，互いに「内積」f に関して直交している 2n 次元ベクトルたちを取るということに他ならない.

このように, シンプレクティック符号の根底にあるのは GF(q)上のベクトル空間であるため，シンプレクティック符号の設計方針は古典の GF(q)上の線形符号にある程度類似することになる．しかし，古典の符号の設計では f に関する直交性の制約を課す必然性は無かったので，この制約のもと新たに符号を設計しなければならない．勿論，そのような方向の努力は既になされていたが，古典の符号理論（誤り訂正符号の理論）が Shannon の情報理論の誕生以降, 一研究分野として確立し, 半世紀を経た今もその発展が止まぬ状況と比べると量子情報理論における代数的符号の研究はその必要性にも関わらず，必ずしも十分に発展しているとは思われない. 換言すれば, 研究の余地が大きい．本提案の研究の主な内容は，この代数的構造を利用した情報処理技術の設計である．

(0b) 予備知識

有限体とは有限の元からなる体（四則演算が可能な代数系）のことである．元の個数が q 個の有限体を GF(q) で表す. 多くの応用では q=2 の場合を扱う．この場合，GF(q)={0,1}

である．この(0b)でも説明を簡単にするため暫く q=2 とする．誤り訂正符号とは，情報の伝達（あるいは保存）の際に， k ビットの情報の列（送るところの情報で，0,1 の列）をより長い n ビットの列（n>k）に符号化することで訂正の能力を実現する技術である．換言すれば，誤り訂正符号は情報に冗長を付加することで訂正を可能にしている．符号化した後の系列は GF(q) の元を n 個並べて出来るベクトル空間 $GF(q)^n$ の部分集合とみなせるが，この部分集合が線形空間となるとき，これを線形符号と呼ぶ．この際，「符号」はもはや符号化というプロセスではなく集合を指している．これは符号の設計論といえる符号理論の習慣であるが，空間 $GF(q)^n$ 内でうまく点（系列）を配置することを問題にしているためと理解できる．

なお，n を符号の長さ（符号長）と呼ぶ．また，前述評価基準(c2)の最小距離とはこれらの配置した複数の点のうち最も近い 2 点間の距離を指し，これが大きいことが望ましい．

(1) 代数的量子誤り訂正符号の一般的構成[6]

CSS 符号とは本質的に $C2^{\perp} \subseteq C1$ という制約を満たす線形符号の対 (C1,C2) のことである．このような符号対を共役符号対と名づけた．ここで $C^{\perp}$ は符号 C の双対符号で，C の全ての元に直交するベクトルからなる．有限体 F=GF(q) 上の比較的小さい共役符号対 (内符号と呼ぶ) と拡大体 $GF(q^k)$ 上の符号対 (外符号) が与えられたとき，それらを「連接 (concatenate)」しより大きな共役符号対を得る方法を発見した．連接するもとの符号はボルトとナットのサイズの一致の様な不可避なパラメータの制約を除き，無制約である．これは従来から知られ広く実用にも供されている連接符号の概念 (図３) を共役符号対 (CSS 符号) に拡張したものとみなせるが，それは非自明な拡張である．なぜなら，(C1,C2)と(D1,D2)を連接するには，C1 と D1 そして C2 と D2 を連接するのだが，連接して出来る符号対(L1,L2)も $L2^{\perp} \subseteq L1$ という(物理，具体的には上記交換関係に起因する)制約を満たさなければならないからである．従来は片側の連接のみ考えれば良かったのでこのような制約とは無縁であった．なお，本発見の特殊例は過去の文献に見られるが，一般的な構成法にまでは到達していなかった．具体的には，量子誤り訂正の文脈では文献 [2]にそのような特殊例が見られるが，本発見の構成法により [2]の構成法よりも良いものが得られた．これについては(3)に述べる．

(2) 代数的量子誤り訂正符号の具体的構成法と情報理論的基準(c1)を用いた評価 [8]

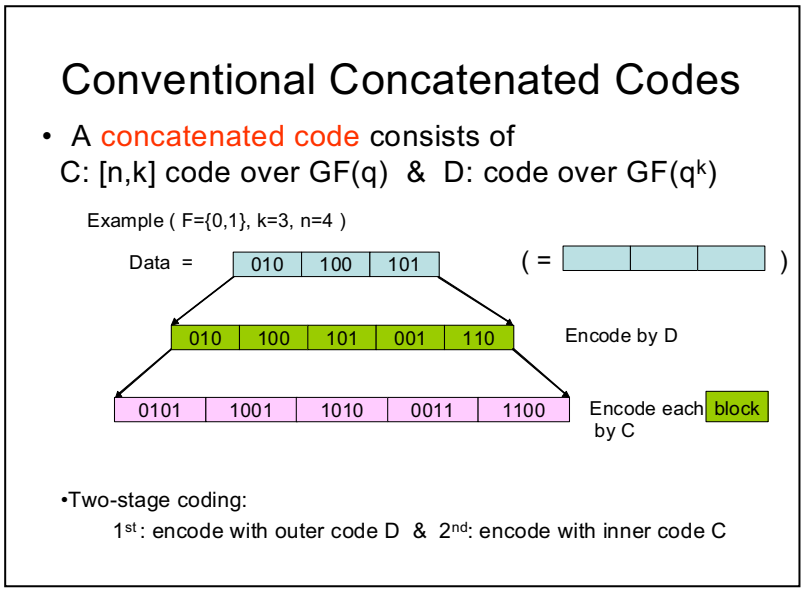

図３　従来の連接法（古典符号）

まず背景について述べる．古典の符号を扱う上で重要な指針であり続けてきたのは，Shannon の通信路容量なる概念あるいは通信路符号化定理であろう．これは，1948 年に彼が発表した論文「通信の数学的理論」の中心に位置付けされるが，この理論は今日情報理論と呼ばれるものの原型である．この通信路符号化定理は良い符号の存在を保証するものであったが，具体的な符号の構成法を与えるものではなかった．また，定理を証明するに当たって用いられた符号は，符号化・復号化の複雑さを度外視した非実用的なものであった．その後何十年にもわたる情報通信の発展を見透かしたようなこの画期的な論文の発表以来, Shannon の意味での良い符号を構成する努力が連綿と続けられている．余り注目されていないが, Shannon の通信路容量を達成する代数的符号が Delsarte と Piret [3]によって 80 年代に得られている．

さて[3]は連接符号を用いたもので，内符号を可変にすることで本来証明の手法であったランダム符号化の効果を具体的な(非確率的な)符号の構成に転用したともいえる巧妙なものであった．なお，ランダム符号化は Shannon の編み出したやはり巧妙な証明法で，符号をランダムに選ぶときの平均の符号性能を評価し，平均以上の性能が少なくとも１つの符号で達成されることから所望の符号の存在を帰結するという論法である. しかも，この論法で大方の符号の性能が良いことを示すことが出来る．Delsarte と Piret はランダム符号化に用い得るある符号集団の要素を全て内符号として列挙した連接符号を取り上げその連接符号の性能を解析した(図 3 では内符号 C を固定したがこれを可変とした)．直感的に，外符号および大方の内符号が良ければ全体としての性能も良いと予想できるが，彼らはその符号が Shannon の通信路容量を達成することを証明したのである.（符号構成のアイディア自体は Justesen によるが，彼の評価基準は最小距離だったため通信路容量にまでは達していなかった.）

本研究に戻る．(1)において連接符号の手法を共役符号対の構成に持ち込むことに成功したので，[3]の構成法が使えることは直ぐに予想できた．ただし，内符号の符号集団は比較的小さなものが必要でその構成は自明では無かった．これは(5)に述べる．これを明示的に与えることで明示的な（多項式時間で構成可能な）連接共役符号対を得ることが出来た．本提案の符号が達成するレイトは知られている共役符号対（CSS 符号）で達成可能なレイトの中で最大である．本研究以前には，その最大レイトを達成する CSS 符号の存在が知られているのみであった．なお，本研究では[3] 以降の符号理論の発展，具体的には代数幾何符号のそれを符号構成に盛り込んだ.

(3) 代数的量子誤り訂正符号の具体的構成法と符号理論的評価基準(c2)を用いた評価 [7]

本研究で用いた手法は多岐にわたる．前記(1),(2)に述べた符号構成そのものは符号理論の言葉で記述できるが，(2)の解析には情報理論の手法も用いた．このため，符号理論でよく用いられる最小距離の基準のみに慣らされ情報理論を出来れば避けたいものと思っている一部（残念ながら「大半」かも知れない）の符号理論家にとっては(2)の成果を理解するのは難しいと思われる．そのことは十分予想されたが，幸い(1)の方法を用い最小距離の基準(c2)でも優れた符号を構成することに成功した．すなわち，本提案の符号は前述の[2]などと比較して優れている（図 4）．また，本連接手法は共役符号対に類似したあるクラスのシンプレクティック符号(enlarged CSS

codes)についても有効である．このクラスにおいてもやはり従来より優れた符号をもたらすことを証明した(図４)．なお，内符号は(2)と異なり固定したもので評価している．また，図４で GV bound とは，これを達成する CSS 符号の存在のみが証明されているもので(c2)のもとでの符号構成の目標といえる．

(4) 代数的量子誤り訂正符号の情報セキュリティへの応用と解析 [9]

共役符号対（C1，C2）のセキュリティ問題への応用は研究提案書の段階から強調してきたが，その解析を進めた．

具体的には共役符号対の量子鍵配送への応用などを主に想定してきたが，本研究では符号の設計が問題であるから，量子鍵配送の中から本質的に関係する符号化の部分だけを抜き出したような問題の定式化を使った方が議論しやすい．そのような問題は情報理論で知られ盗聴通信路(wiretap channel)と呼ばれる．このモデル上で共役符号対の性能を解析した．量子版の盗聴通信路も既に提案されているが，このモデル上で，本研究で得られた共役符号対が有効性であるのは，過去の解析結果から明らかである．しかし，古典の盗聴通信路について本提案の符号がどの程度の性能を持つかは自明ではない．したがって，これを定量的に評価した．代表的な盗聴通信路について評価したところ，本研究成果(2)で得られた符号による達成可能レイトは理論的な限界に迫るものであった（図５）．この例では盗聴通信路は正規通信路が無雑音で盗聴者への通信路がビット反転確率 $p_E=1/2\pm(p'(1-p'))^{1/2}$ の二元対称通信路である．正規通信路も二元対称通信路の場合には，図５のグラフを下に平行移動したものが得られる．

なお，共役符号対（C1, C2）あるいは（C2, C1)を量子暗号に使うときは，C1 の誤り訂正能力は通常の情報伝達のために必要とされ，C2 の誤り訂正能力は盗聴者に対する秘匿性に直結する．

(3)に書いた多岐な手法に関して言うと，本成果のためには，量子理論の枠組み，具体的には測定の概念や Holevo 限界を直接使った．ここでいう Holevo 限界とは，情報を担う量子状態の組が与えられたとき，測定を最適化することで（情報理論的な意味で）どれだけ情報が得られるかという問題に対し，その限界を定量的に示したものである．

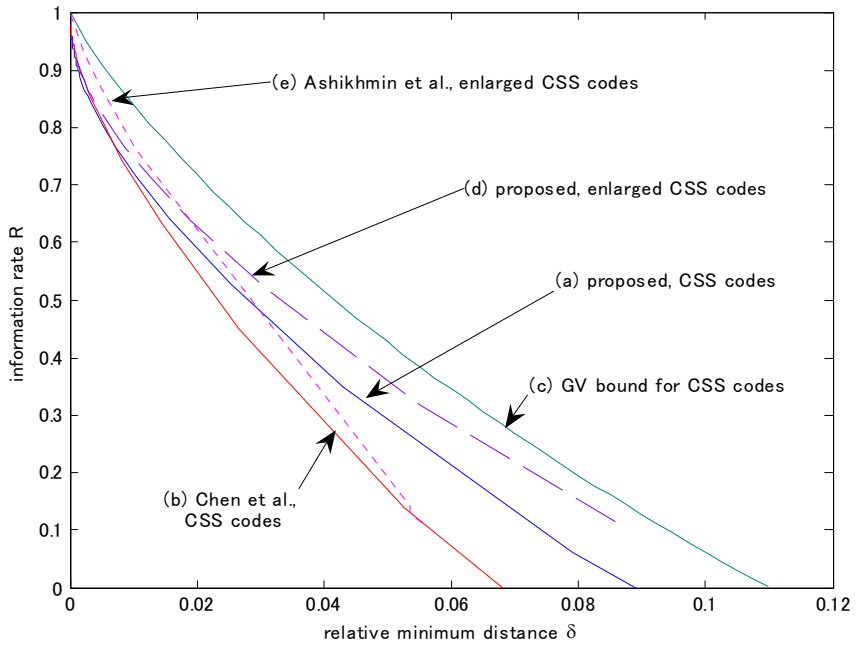

図４　最小距離の比較（q=2）

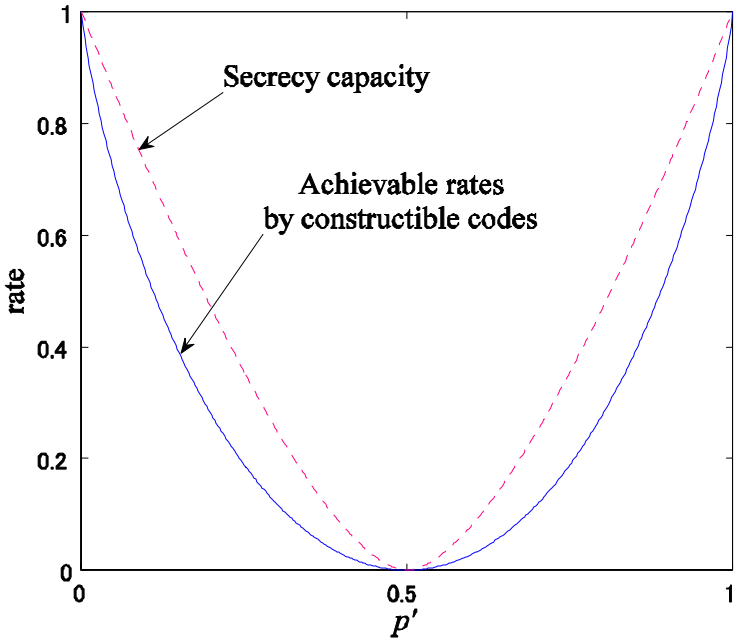

図５　盗聴通信路における本提案の符号による
達成可能レイトと理論的限界 Secrecy capacity

(5) 共役符号対の小さな集団（[8]の一部）
大きさ q^n 以下の共役符号対の集団で殆どが良い符号対からなるものを与えた．ここで n は符号長である．特に本構成法では，共役符号対(C1,C2)がこの集団を動くとき C1 および C2 にあらわれる非零のベクトルが一様に分布するという意味でバランスが良い. なお C1 と C2 の大きさ（古典の符号として送り得る情報の大きさ）は異なっていて良い．このような小さなバランスの良い符号集団は過去には知られていなかった.

この集団は(2)の符号構成に利用する目的で考案したものであり，独立した成果として発表したわけでは無いのだが，それ以前の関連する既知の結果と比べると，この部分だけ抜き出しても意義があるようなので説明する.

従来から知られていたランダム符号化は[1]や[11]に見られ，これらは[5]でも紹介した. 文献[1]では，ランダム符号化は，いわゆる CSS 符号の Gilbert-Varshamov (GV) 下界（つまりこの最小距離を達成する符号の存在；基準(c2)に関する）を証明するために用いられた．また，Mayers [11] に見られるランダム符号化もある．ただし，Mayers の主眼は量子鍵配送にあり, 当初から量子 CSS 符号(共役符号対)を意識したものでは無かったようである. しかし, 興味深いことに Mayers の補題はいわゆる CSS 符号の GV 下界を直接含意する.

このような既知の符号集団を基に符号を設計する案を研究提案書に書いたが，結果的にはいずれでもないより優れたランダム符号化法を考案し更に明示的な符号構成をも与えた. 既知の符号集団の大きさは明らかに本発見の集団の大きさ q^n に比べ桁違いに肥大している．（なお，Shor と Preskill は符号構成については何も触れていないが，彼らが明示したプロトコルから考えて所望の符号の存在を証明 [1]，あるいは仮定したと解釈すべきであろう.）

このように，本考案の符号集団が得られた時点で従来結果より利点があったのだが，本研究では(2)に述べたように明示的な符号構成問題を解決している．これは，符号集団の

大きさで言うと究極である 1 にまで達したことを意味する.

(6) その他

上記情報セキュリティへの応用において高速な情報処理を実現する方法を提案した．これは実用上意義が大きいと判断し特許とした．研究目的 4)でいう「統一的な視点」からの理論整備については, 文献[5]を執筆した. なお, 本研究で構成した符号は量子エンタングルメント蒸留にも利用できる．これは一般のシンプレクティック符号について知られていることである．また，多くの研究者が 2 準位系に対する符号のみを考えているのに対し，本研究の符号は特殊例を除きそれに限らない q 準位系に適用可能である（q は素数あるいは素数の冪）.

【今後の展開】 基礎的な方式を考案できたと考えている．特に，成果(1)の応用範囲は少なくも理論上は広い．実際，量子情報処理のみならず，古典の情報処理機構としても従来に無い性能の良い符号を見出した[9].

なお, 主要成果(1)を実際に用いる際には(2)のように内符号を可変にするのは現実的ではない，すなわち，実際には良い内符号を固定して用いるのが良いと思われる．良い内符号を固定したときの性能評価は今後の課題である.

既に述べたように，本研究では符号理論，情報理論，量子論という極めて多岐にわたる議論を不可欠な要素として用いている．このことは，成果の発表における困難を予期させたが実際苦心している．これらの全てを理解できる研究者は，報告者の思いつく範囲では殆ど見当たらないのである．このことから成果を広めるために，報告者としては自明なことや，あるいは（必要な専門知識のレベルを下げるため）得られた結果を弱めたものなどを別の報告書などに纏めるかも知れない.

【結言】 共役符号対の一般的な連接法を与え, それを用いて明示的な符号構成を与えた．これは CSS 符号で達成可能な既知の最大レイトを達成する．また，最小距離の意味でも本連接法を用いて従来よりも高い性能を持つ符号を明示的に構成した．これらの符号が量子盗聴通信路において適用可能なことは従来結果より明らかだが，量子通信路のみならず古典の盗聴通信路においても高い性能を持つことを定量的に示した.

本研究の成果の鍵となったものの一つは報告者が，東工大で符号設計の研究に当たった学生の頃から親しんできた道具コンパニオン行列であるが，符号を専門とする研究者でも実用を狙った符号を設計した経験のある一部の者を除いては, これを知らないようである. 本研究の提案書には, (研究内容として挙げたもののうち多くは) 「問題として既にある程度認識されているものであり，問題提起のレベルでの独創性は比較的小さく，むしろ，良い符号を作った時点で新規性が生まれる．このような事情から現段階で考慮頂きたい事実は，申請者は古典の計算機に使用する目的で代数的誤り訂正符号を考案した実績があるということである」と書いた．体面が保たれた格好である.

「研究のねらい」に書いたように，本研究で扱った代数的構造，あるいはより具体的にシンプレクティック符号は極めて応用の裾野が広く発展の可能性を秘めていると考えている(図２)．そういった発展のほんの一部においてでも，本研究が「さきがけ」であったと

後に振り返られるようなことがあれば報告者の望外の喜びである.

本研究を支援下さる研究総括細谷曉夫教授を初めとする科学技術振興機構「量子と情報」研究領域関係者の皆様に深謝する.

参考文献

[1] A. R. Calderbank and P. W. Shor, “Good quantum error correcting codes exist,” *Phys. Rev. A*, vol. 54, pp. 1098-1105, 1996.

[2] H. Chen, S. Ling, and C. Xing, “Asymptotically good quantum codes exceeding the Ashikhimin-Litsyn-Tsfasman bound,” *IEEE Trans. Information Theory*, vol. 47, pp. 2055-2058, July 2001.

[3] P. Delsarte and P. Piret, “Algebraic construction of Shannon codes for regular channels,” *IEEE Trans. Information Theory*, vol. 28, no. 4, pp. 593-599, Jul. 1982.

[4] G. D. Forney, Jr., *Concatenated Codes*. MA: MIT Press, 1966.

[5] M. Hamada, ``Quotient codes and their reliability,'' *IPSJ Digital Courie*r, vol. 1, no. 0, pp. 450--460, Oct. 2005 [招待論文]
http://www.jstage.jst.go.jp/article/ipsjdc/1/0/1_450/_article. Also appeared in *IPSJ Journal*, vol. 46, pp. 2428-2438, no. 10, Oct., 2005.

[6] M. Hamada, ``Concatenated conjugate codes,'' 2006, submitted to *IEEE Trans. Information Theory*. E-Print, arXiv: quant-ph/0610194,

[7] M. Hamada, “Minimum distance of concatenated conjugate codes for cryptography and quantum error correction,” 2006, submitted to *IEEE Trans. Information Theory*. E-Print, arXiv:quant-ph/0610195, LANL.

[8] M. Hamada, ``Constructive conjugate codes for quantum error correction and cryptography,'' 2007. E-Print, arXiv:cs/0703141 (cs.IT).

[9] M. Hamada, “An algebraic and quantum theoretical approach to coding on wiretap channels,” manuscript, Oct. 2007.

[10] M. Hamada, “Conjugate codes for secure and reliable information transmission,” *Proc. of IEEE Information Theory Workshop, Chengdu, China*, pp. 149-153, Oct. 2006. [招待講演]

[11] D. Mayers, “Unconditional security in quantum cryptography,” *J. Assoc. Comp. Mach.*, vol. 48, pp.351-406, 2001.