研 究 報 告 書

研 究 課 題 名

代数的量子情報処理技術の研究

（研究領域:「量子と情報」）

研究者氏名:　　濵田　充

（研究期間: 2004 年 10 月　1 日～　2008 年　3 月 31 日）

研究報告書

1. 研究課題名
　　代数的量子情報処理技術の研究

2. 氏名
　　濵田　充

3. 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ベースに，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(図1)．特に，代数的量子誤り訂正符号に重点を置いたが，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．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 Calderbank-Shor-Steane (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．

4. 研究成果①

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った．

　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

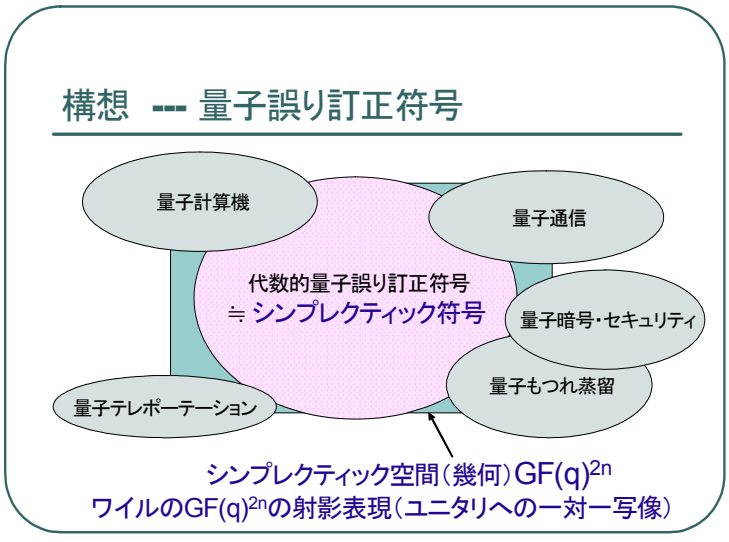

図1　研究構想

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．

このような方針に基づき研究を進め以下の主要成果を得た．
(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．

目的 1),2),3)に関して，中核となる結果(1),(2),(3)を得た．4),5)に関する主な結果は上記では(4)であるがその他に進行中のものもある．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最も本質的な概念を以下に説明する．

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 は素数と仮定する．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. 本節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もっとも近い 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 [3]

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 GF(q) 上の比較的小さい共役符号対(内符号と呼ぶ)とその拡大体 $GF(q^m)$ 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[1]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(物理に起因する)制約を満たさなければならないからである. なお, (C1,C2)を符号の集団 $(C1^{(i)},C2^{(i)})$, i=1,…,N で置き換えてもこの構成法は有効である.

(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 [4]

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. 理論的なレベルでは, 里程標といえるこの問題への有意な結果が 80 年代に得られている. すなわち, Shannon の通信路容量を達成する代数的符号が Delsarte と Piret [2]によって得られた.

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, [2]の構成法のアイディアが使えることは直ぐに予想できた. ただし, 内符号の集団は比較的

小さなものが必要なためこれを新たに設計した．すなわち，内符号の集団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．また，構成した符号は復号も多項式時間で行える．（c1)を扱った従来結果は，復号問題に限っても査読者の言葉を借りれば「試み」があった程度であるが，本研究では更に符号構成の問題にも解を与えた．

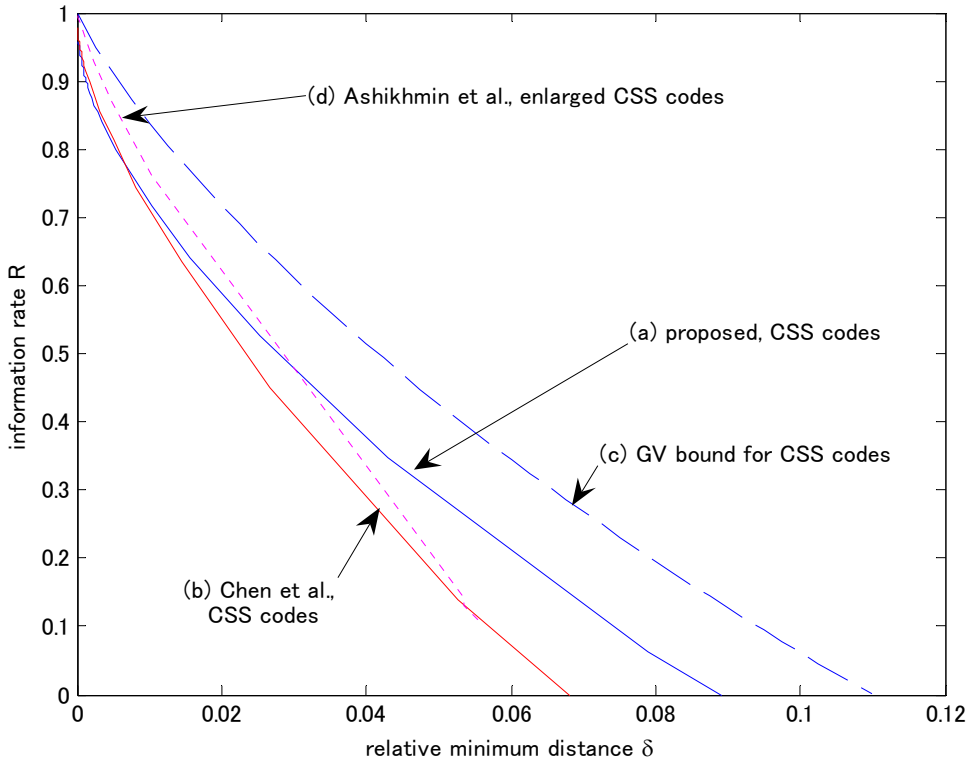

図2　最小距離の比較

(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 [5]
符号の構成問題を扱った従来結果は，(c1)より扱いの簡単な(c2)を評価基準としたものが殆どであった．提案の構成法(1)が従来より優れていることを示すためこの基準を用い，従来結果と比較した（図2）．

(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 [6]
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．具体的には量子鍵配送などへの応用を想定してきたが，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容易に推察できる．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3）．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

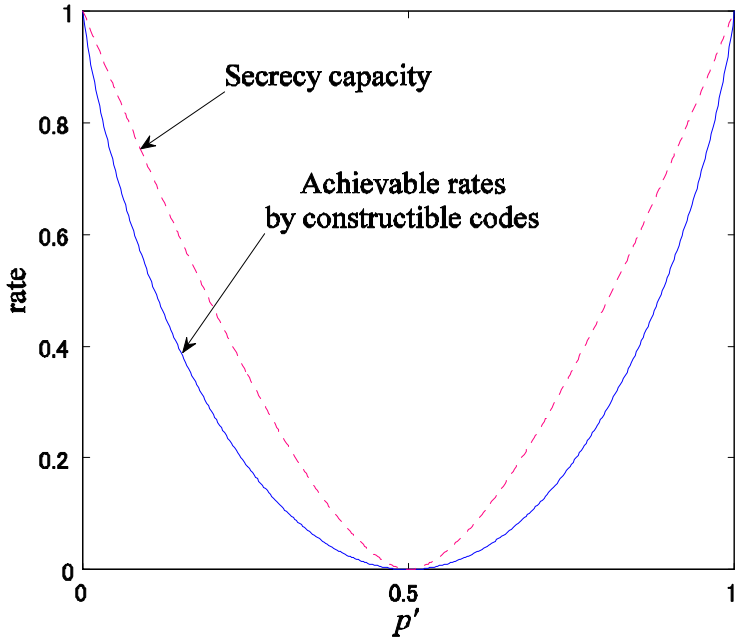

図3　盗聴通信路における本提案の符号による
達成可能レイトと理論的限界　Secrecy capacity

路がビット反転確率 $p_E=1/2\pm(p'(1-p'))^{1/2}$ の二元対称通信路からなる．正規通信路も二元対称通信路の場合は，このグラフを下に平行移動したものが得られる．

[1] G. D. Forney, Jr., *Concatenated Codes*. MA: MIT Press, 1966.
[2] 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.
[3] M. Hamada, "Concatenated conjugate codes," 2006, submitted to *IEEE Trans. Information Theory*. E-Print, arXiv: quant-ph/0610194.
[4] M. Hamada, "Constructive conjugate codes for quantum error correction and cryptography," 2006. E-Print, arXiv:cs/0703141 (cs.IT).
[5] 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.
[6] M. Hamada, "An algebraic and quantum theoretical approach to coding on wiretap channels," 日本応用数理学会 2007 年度年会予稿集, pp.166–167, 2007.

6．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．

なお，主要成果(1)を現実に用いる際には(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．

7．研究成果リスト

（1）論文（原著論文）発表　4件

1. Mitsuru Hamada,"Quotient Codes and Their Reliability," *IPSJ Digital Courier*, 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).

2. Mitsuru Hamada, “Conjugate Codes for Secure and Reliable Information Transmission,” Proc. IEEE Information Theory Workshop, pp.149–153, 2006.
3. Mitsuru Hamada, “Conjugate Codes and Applications to Cryptography,” Tamagawa University research review, no.12, pp. 19–25, 2006.
4. Mitsuru Hamada, “Algebraic and Quantum Theoretical Approach to Coding on Wiretap Channels,” Proc. The 3rd International Symposium on Communications, Control and Signal Processing (ISCCSP), 2008. In press.

（2）特許出願

研究期間累積件数：2 件(出願公開前[国内 1 件、国外 1 件])

（3）その他の成果

受賞

なし

著書 1 件

1. Mitsuru Hamada, Cryptography Research Perspectives（そのうちの一章）, Nova Science Publishers, Inc., 2008 出版予定.

学会発表 5 件

1. 濵田充, “An Upper Bound on the Decoding Error Probability of Additive Codes,” 第 11 回量子情報技術研究会 QIT2004-65, 2004.
2. 濵田充, “An Algebraic and Quantum Theoretical Approach to Coding on Wiretap Channels,” 日本応用数理学会 2007 年度年会
3. 濵田充, “Applications of Conjugate Codes to Wiretap Channels,” 電子情報通信学会研究会 (ISEC) , 2007.
4. 濵田充, “Quantum Coding as a Proof Technique for Secure and Reliable Information Transmission,” 電子情報通信学会研究会 (IT) , 2008.
5. Mitsuru Hamada, “Algebraic and Quantum Theoretical Approach to Coding on Wiretap Channels,” The 3rd International Symposium on Communications, Control and Signal Processing (ISCCSP), 2008.

招待講演 1 件

1. Mitsuru Hamada, “Conjugate Codes for Secure and Reliable Information Transmission,” IEEE Information Theory Workshop 2006.

国内・出版物 2 件

1. 濵田充, “Applications of Conjugate Codes to Wiretap Channels,” 信学技報, vol. 107, no. 346, ISEC2007-98, pp. 1–8, 2007.
2. 濵田充, “Quantum Coding as a Proof Technique for Secure and Reliable Information Transmission,” 信学技報, vol. 107, no. 422, IT2007-31, pp. 35–40, 2008.