様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　２６　日現在

機関番号：　３２６３９
研究種目：　基盤研究(C)（一般）
研究期間：　2010～2014
課題番号：　２２５４０１５０

研究課題名（和文）量子論に基づく符号理論の新展開と情報セキュリティへの応用

研究課題名（英文）Investigation on Error-Correcting Codes Based on Quantum Theory and Its Applications to Information Security Issues

研究代表者

浜田　充（Hamada, Mitsuru）

玉川大学・量子情報科学研究所・教授

研究者番号：１０４０７６７９

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：代数的誤り訂正符号の一般化と見なすことができ，量子誤り訂正に適用可能な剰余符号(quotient codes)を研究した．本研究は，自ら考案した連接の手法による剰余符号の構成法の具現化と性能解析の精緻化，またはその周辺に関するものである．例えば，申請と前後して，提案の多項式時間構成可能な符号が,盗聴通信路(wiretap channel)において漸近的に最適であることを証明したが，これに付随する結果を本研究期間中に発表した．また，研究期間の後半では，2次元系の任意の量子情報処理を構成する方法を提案した．これも建設的・具体的な情報処理方式であり，その最適性も自ら厳密に証明した．

研究成果の概要（英文）：Quotient codes, which generalize classical error-correcting codes and are applicable to quantum error correction, were studied. The present study was mainly aimed at embodiment of concatenated quotient codes, which are proposed by this researcher, refined performance analysis of them, and exploration into related issues. For instance, while this researcher had proved the asymptotic optimality of the proposed concatenated codes used on wiretap channels (a model due to Wyner) around the time of the application of this research, he obtained related results during the research period of the Kakenhi. In the latter half of the period, he proposed a construction method for arbitrary quantum information processing on single-qubit systems (specifically, arbitrary SU(2) elements). This is also a concrete constructive (algorithmic) method regarding information processing , and its optimality was also proved rigorously by himself.

研究分野：　応用数学

キーワード：　符号理論　誤り訂正符号　線形代数　アルゴリズム　量子論　量子コンピュータ　情報基礎　SU(2)

１．研究開始当初の背景

情報理論において，盗聴通信路 (wiretap channel) の問題が再び脚光を浴びていた．これは Wyner（1975）が定式化した盗聴下での安全な通信の問題であるが，この問題がふたたび注目を浴びることとなった学術的背景としては，量子鍵配送の研究の隆盛があった．報告者は，量子誤り訂正，量子鍵配送，（量子）盗聴通信路のいずれにも適用し得る「剰余符号 (quotient codes)」の研究を行ってきており，ある評価基準では知られるものの中で最良の結果を与えていた．自ら考案した連接の手法による剰余符号の構成法をはじめ，剰余符号には研究の余地があると考えた．

２．研究の目的

代数的誤り訂正符号の一般化と見なすことができる剰余符号を研究する．これは Wyner が定式化したような盗聴通信路の問題に有効である． 代数的量子誤り訂正符号 (シンプレクティック符号) はこの剰余符号の構造を有するのでこれも研究対象とする．これらの符号の設計規範の探求，構成，性能評価，理論的限界の解明などを主目的とする．

３．研究の方法

剰余符号は次を含む上位概念といえる：(i) 量子誤り訂正符号 (簡単に量子符号とも呼ぶ)，(ii) 盗聴通信路のための代数的符号．
また，申請者は (i), (ii) のいずれとしても意味のある共役符号対を中心として，建設的な成果をいくつか既に得ていたのでそれらを手がかりに理論の展開を図った．

４．研究成果

(1)　代数的誤り訂正符号の一般化と見なすことができ，量子誤り訂正に適用可能な剰余符号(quotient codes)を研究した．本研究は，自ら考案した連接の手法による剰余符号の構成法の具現化と性能解析の精緻化，またはその周辺に関するものである．例えば，申請と前後して，提案の多項式時間構成可能な符号が，盗聴通信路(wiretap channel)において漸近的に最適であることを証明したが，この研究の多くの部分を本研究期間中に発表した．具体的には，入出力のアルファベットサイズが 2 であるときに，漸近的に最適な符号を与え，紀要（下記５の雑誌論文④）に纏めた．この符号は当初の提案符号とは似て非なるものである（当初提案の符号は他機関の出版物に掲載する計画であったため同じ符号の利用は避けた）．アルファベットサイズが 2 というのは符号の構成において本質的ではない．この制限の主な理由は，当論文は専門外の者でも予備知識なしで読めることを意図して執筆したからである．より一般的なケイスの証明は，別途執筆した．特に，その本質的部分は IEEE International Symposium on Information Theory (ISIT) 2010 において発表している．その際用いた符号が，当初から提案していた多項式時間構成可能な符号である．なお，多項式時間構成可能な符号は，研究者自らが 2006 年に提案した連接の手法という方法で得られるものである．

(2) Fano 不等式の改良を行った．上記 IEEE International Symposium on Information Theory (ISIT) 2010 における符号の安全性の証明中，Fano 不等式と呼ばれる情報理論における基本的な関係式を用いていた．この部分を改良することで安全性評価が改善するはずだという直観に基づき Fano 不等式の改良に着手し成功した．改良前と比べて数値例でも有意な差が出ることを確かめた．

(3)　研究期間の後半では，2 次元系の任意の量子情報処理を構成する方法を提案した．これも建設的・具体的な情報処理方式であり，その最適性も自ら厳密に証明した．具体的には任意の回転を「因子」の積に分解する（積として構成する）方法を与えたのだが，建設的な点を強調すると以下のように云える．回転を SU(2)の元とみなし，与えられた任意の回転をある制約のもと最小個数の回転の積に分解するアルゴリズムを与えた．制約は積を構成する因子の軸があらかじめ与えられた 2 軸のいずれかであることである．すなわち，2 軸 m,n を任意に固定し，任意の SU(2) の元 U にたいし U を構成するのに必要な m または n の周りの回転（因子）の最小の個数 $N_{m,n}(U)$ とそれを達成する具体的な因子の系列を与えた．建設的な本結果は量子計算回路のユニヴァーサルな構成に利用できる．なお，この結果は量子誤り訂正符号のエンコーダ（いわゆる量子状態を量子ノイズに強い部分空間に埋め込む仕組み）を含む一般的な量子情報処理方式に関する基本的な成果である．ここで SU(2)とは 2×2 のユニタリ行列で行列式が１のものからなる集合（積について閉じている）である．
上記のような分解は 2 軸が直交する場合についてはオイラー角の名のものとよく知られていたので，この直交ケイスに限定したのでは，上記問題は今更解く価値がない（少なくとも報告者には）．直交するとは限らない一般の 2 軸について最適解を与えたところが本研究の貢献である．
この問題は素朴に幾何学的興味を喚起するものではないかと思うが，本研究は量子物理に関連しているので物理的な意味合いについて述べる．このように一般的な 2 軸を考えることの物理的な意義は以下のような例から分かる．二次元系 $\mathbb{C}^2$ で表される量子物理系のハミルトニアン H を考える．この系の時間発展 $\exp(-itH)$の行列式の平方根を $c(t)$ とすると $\exp(-itH)$の「ノーマライズド版」$[c(t)]^{-1}\exp(-itH)$は SU(2)の元であり，その軸は H で定まる($t\in\mathbb{R}$)．いま，ハミルトニアン H がある 2 通りのインスタンス H_1, H_2 の間

で切り替えられるような状況を考える．それら H_1, H_2 の時間発展の作るユニタリ行列の系列でもって，与えられた（ターゲットとなる）回転 U を作るという問題に上記結果が適用できるわけであるが，H_1, H_2 の決める 2 軸が（もちろん平行は除き）どんな場合であっても本結果で最適解が得られる．ここで最適とは因子の個数が最小値 $Nm,n(U)$を達成することを意味する．従来のオイラー角の名のもと知られていた 3 つの因子への分解法では，H_1, H_2 の決める軸が直交する特殊ケイスしか扱えなかった．
本成果に該当する論文はopen access 形式で発表されており，広くアクセス可能である(DOI: 10.1098/rsos.140145).

(4) 上記(3)に関連する結果を述べ，付随する結果や経緯を説明する．成果(3)では，分解の最小個数 $Nm,n(U)$も最適解の一部として求まるが，その数は幾らでも大きくなり得る．一方，複数の量子計算の教科書の記述から，「m,n に依らず $Nm,n(U)\leqq 3$」と云うに等しい誤信が跋扈していたことが分かる．（したがって，多くの研究者が認識すらしていなかった量子回路構成の問題を解決したことになる．）今一度，成果(3)を振り返るが，成果(3)では，誤信を正すに止まらず，代わりに何が出来るか（ソルーション）を与え，しかもそれが最適なソルーションであることを証明している．既に成果(3)を得た今，上記誤信は取るに足らないものかも知れない．しかし，誤信が事実跋扈していたことを考えると，どちらが正しいか判断できない者達がいることが想像できる．この点に鑑み，上記誤信への直接の反証も与えてある（下記５の学会発表③ほか）．以下に反証と成果(3)を得るに至った経緯を述べる．$Nm,n(U)$は 2 軸 m と n とのなす角 δ と U で書けるので，以下 $Nm,n(U)$= N(U, δ)と置く．
成果(3)で扱った問題を考えるに至った経緯は以下の通りである．Nielsen-Chuang ①を初めとする複数の著名な研究者による量子計算の教科書では，「(δの値に依らず) N(U, δ)が常に３以下」ということに等価な記述があり，量子計算機の万能性をこれに帰着させている．報告者はこの「N(U, δ)が常に３以下」との主張に疑問を感じ，それが誤りであることを証明した（下記５の学会発表③）．ここでは，本成果との対応のため N(U, δ)を使って説明したが，量子計算の分野では N(U, δ)のような関数を求めるという問題意識すらなかった．（何故なら，その数が 3 以下だと思い込み，研究価値があることすら認識されなかったからである．）その後，報告者は，最適性の点で幾分弱い成果を経て，N(U, δ) とそれを達成する最適なユニタリ行列（回転）の系列構成法を発見し成果(3)に至った．より直接的な誤信の反証と，テクニカルなことを含めた，成果(3)を得るに至った経緯の説明は下記５の雑誌論文①に記した．

なお，報告者の知る範囲では，上記誤信が見受けられる最も古い文献は Nielsen-Chuang ①である（同書十周年記念版でも訂正されなかった）．これは量子計算機分野の標準的な教科書であり邦訳もされ，また多くの量子計算機に関する教科書がこれの影響を受けている．文献①を含めそのような教科書の少なくとも 3 冊に誤信が明白に記されている(①, ②, ③)．
ところで，本研究期間の後半，理研において，従来の研究者の倫理感では理解し得ないような出来事が起き，国家の科学関連事業においても緊急に対策を講じ始めたことが直接的影響によって分かる．一度定説として定着したり，定着しないまでも権威ある学術誌に掲載されたりした科学的主張の誤りを正すことには殊更のエネルギーが必要であることが，この理研を舞台にした事件の報道で一般国民にも分かったのではないかと思う．本研究は，理論研究であり問題の理研の研究（もどき？）とは性格が異なるところがある．しかし，何か理研の事例と背景において無関係ではないと思わせるような事例が本研究分野でも見受けられる．本研究は数学分野での研究であり，本報告の研究成果も（応用寄り・学際的ではあるが）定理のような数学的な主張として記述してある．一方，それに矛盾する誤信も数学的主張として述べられていた（①，②，③）．この事例では，彼らの主張は 2×2 の行列である任意の回転 U が 3 つの 2×2 の行列で書けるという主張なので，そのたった 3 つの 2×2 の行列を具体的に求めようとすれば，その誤りに気付いたはずである（実際に問題に当たった感覚では）．あるいは，本成果(3)の論文（DOI: 10.1098/rsos.140145）に記述したように，$Nm,n(U)$を求めることよりも易しい max_U $Nm,n(U)$ (U の最大化は US(2)全体にわたる) を求める問題は max_U $Nm,n(U)$ =ceil(π/δ)+1 と 1970 年ころに Lowenthal によって解かれていたので，これを知っていれば上記主張は誤りと分かった．ここで，ceil(x)は x 以上の最小の整数.(ただし，上記の形 max_U $Nm,n(U)$ =ceil(π/δ)+1 は報告者が今回独立に再発見したときの形であり，Lowenthal はこのような簡潔な形では述べていなかった．したがって，見つけにくかったのも事実である．）この誤信の事例は，Lowenthal の公式に関する無知で片づけられる簡単なケイスかもしれない．しかしながら，本課題の研究を進める上で，誤りと思しき主張が正しい理論の発展を阻害しているのではないかと思わせるケイスが多々あった．これらの多くは，上記の誤信のケイスほど単純ではないし，程度の低い話に振り回されていては時間の浪費となるので，それらについては取捨選択も含めて今後の課題とした．ただ，今回のケイスで，誤りを正すだけでなく，誤っているならばそれを覆すべく正しく，かつ最適な（あるいはそれが出来ないまでも，定量的に従来

に優る）方式を提供するというスタンスが望ましいということが今一度確認出来た．実際，このスタンスは本研究以前から維持している．具体的には，本研究は報告者が 2000 年頃から続けている量子誤り訂正符号の研究の延長線上にあるが，本研究の提案後・採択前，やはり過去の「誤り」を正した上でそれを凌駕する方式，具体的には代数的符号を発明している（M. Hamada, "A polynomial-time construction of self-orthogonal codes and applications to quantum error correction", Proc. IEEE International Symposium on Information Theory (ISIT), pp.794—798, Seoul, Korea, 2009）．ただし，ここでの「誤り」は論理を積み上げる上で誤った inference を犯すといった通常の「誤り」ではない．「欺き」とでも云った方が正しいかもしれない．つまり，Ashkhimin et al. が多項式時間構成可能な符号の構成を問題として提起し，その下で彼らが提示し得るベストなものを提示したのにも拘わらず，問題をすり替えて（というより，はぐらかして）彼らの結果を改良したとする者がいる．具体的には，多項式時間構成可能であるとは証明されていない符号を主たる構成要素として用いた量子符号を提案し，それが Ashkhimin et al.らの結果を improve したとする論文を発表した者がいる．悲しいことにそれは本国からの発信であったが，本国の本報告者が「誤り」を正す（「誤り」を指摘し，元の問題設定を遵守した上で従来結果を凌駕する方式を与える）ことが出来たのは救いかも知れない．不思議だったのは，Ashkhimin et al.の後追い研究を行う者が一様に，本来の問題設定をはぐらかしたこの偽りの improvement を認めてしまっていたことである．小学校の理科で，何かを比較するときは，同じ条件下で比較しなければならないと習わなかったのであろうか．そういったことや他の研究に関するやり取りで，コミュニティの学術的健全さに疑問を感じることが多く，学術誌への投稿に消極的になっているところがあるが，一方で，文書の電子化が進み，会議録のページ制限が緩くなったお蔭で，会議録だけでも一昔前の correspondence くらいの長さの論文が書けるようになった．上記 ISIT2009 の報告者の成果などはその例である．

このように，提案・採択と前後する成果も含め，本研究では，跋扈する「誤り」を見抜きそれらに屈せず，正しい理論・成果・方式を提供することができた．しかも，それらは，自ら最適性を厳密に証明することに成功しているか，少なくとも，従来結果を凌駕するものである．また，本研究提案の土台とした提案方式も（盗聴通信路の問題への適用において）最適な符号化方式であることを自ら証明しているが，これも報告者の研究を特徴づける点であろう．

<引用文献>

① M.Nielsen and I.Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000

② K. R. Parthasarathy, Lectures on Quantum Computation, Quantum Error Correcting Codes and Information Theory, Narosa Publishing House, 2006

③ Kaye, R. Laflamme, and M. Mosca, An Introduction to Quantum Computing, Oxford University Press, 2007

５．主な発表論文等

（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 6 件）

① Mitsuru Hamada, A Simple Demonstration of a Fallacy in Implementability Arguments on Quantum Computation, Tamagawa University Quantum ICT Research Institute Bulletin, 査読有, vol. 4, 2014, 31—32

② Mitsuru Hamada, The minimum number of rotations about two axes for constructing an arbitrarily fixed rotation, Royal Society Open Science, 査読有, vol.1, 2014, 1--18, DOI: 10.1098/rsos.140145

③ Mitsuru Hamada, Simple Method for Obtaining Expansions of Simplectic Codes Over An Extension Field for Quantum Error Correction, Tamagawa University Quantum ICT Research Institute Bulletin, 査読有, vol. 2, 2012, 1—4

④ Mitsuru Hamada, Constructive Codes for Communication Over Channels Subject to Eavesdropping, Tamagawa University Research Review, 査読有, 2010, 巻の標記なし, 19--49

〔学会発表〕（計 14 件）

① Mitsuru Hamada, Toward Implementation of Algebraic Coding for Wiretap Channels, 電子情報通信学会 IT・ISEC・WBS 合同研究会, 北九州市立大学（福岡県北九州市）, 2015 年 3 月 3 日

② Mitsuru Hamada, The Minimum Number of Rotations About Two Axes for Constructing an Arbitrary Rotation, 5th Nagoya Winter Workshop on Quantum Information, Measurement, and Foundations, 名古屋大学（愛知県名古屋市）, 2014 年 3 月 7 日

③ Mitsuru Hamada, Overlooked restrictions on Euler angles in quantum computation, American Physical Society March Meeting, ボルチモア(米国), 2013 年 3 月 19 日

④ Mitsuru Hamada, Security of Concatenated Encoders for Wiretap Channels, IEEE International Symposium on Information Theory (ISIT), **オースチン(米国),** 2010 **年** 6 **月** 16 **日**

〔図書〕（計　0　件）

〔産業財産権〕

○出願状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　2　件）

名 称 ： ENCODING DEVICE FOR ERROR CORRECTION, ENCODING METHOD FOR ERROR CORRECTION AND ENCODING PROGRAM FOR ERROR CORRECTION
発明者：浜田充
権利者：玉川学園
種類：特許
番号：US 8,365,052
出願年月日：2012 **年** 4 **月** 3 **日**
取得年月日：2013 **年** 1 **月** 29 **日**
国内外の別： 国外

名称：誤り訂正符号化装置, 誤り訂正符号化方法及びプログラム
発明者：浜田充
権利者：学校法人玉川学園
種類：特許
番号：特許第 5062643 **号**
出願年月日：2011 **年** 5 **月** 13 **日**
取得年月日：2012 **年** 8 **月** 17 **日**
国内外の別： 国内

〔その他〕
ホームページ等

６．研究組織

(1)**研究代表者**

浜田 充　　（HAMADA, Mitsuru）
玉川大学・量子情報科学研究所・教授
研究者番号：１０４０７６７９