様式 C-19

科学研究費補助金研究成果報告書

平成２１年６月２２日現在

研究種目：若手研究（Ｂ）
研究期間：2006～2009
課題番号：１８７０００１７
研究課題名（和文）　量子情報技術を頑強にする符号化技術の研究

研究課題名（英文）　Research on error-correcting codes that make quantum information technology stubborn

研究代表者
萩原　学　（HAGIWARA MANABU）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究員
研究者番号：80415728

研究成果の概要：ＣＳＳ符号（量子誤り訂正符号）を構成する古典符号の対をＱＣ－ＬＤＰＣ符号として実現する手法を提案した。ＱＣ－ＬＤＰＣ符号を特徴づけるモデル行列による、ＣＳＳ符号構成の必要十分条件を簡潔に与え、さらにその条件を満たす、具体的な構成方法を提示した。その発展として、ＱＣ－ＬＤＰＣ符号の組がＣＳＳ符号を構成する為の符号長とモデル行列構成要素である巡回行列のサイズに関する下限導出に成功した。また、量子誤り訂正シミュレータを古典計算機上で開発した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	1,100,000	0	1,100,000
2007 年度	1,100,000	0	1,100,000
2008 年度	800,000	240,000	1,040,000
総　計			3,240,000

研究分野：量子誤り訂正符号・組合せ論・情報セキュリティ
科研費の分科・細目：物理学・原子・分子・量子エレクトロニクス
キーワード：量子誤り訂正符号・ＣＳＳ符号・ＬＤＰＣ符号・組合せ論

１．研究開始当初の背景

量子情報理論研究の進展により、実用的な量子通信プロトコル理論開発、及び、装置開発は双方を互いに刺激し合い、今日も目覚しく進展し続けている。日本の量子暗号装置の研究・開発は、世界のトップクラス成果を挙げ、量子情報システムの基盤技術をリードし続けている。その一方、量子暗号装置における通信距離の増長、情報源・受信器の精度向上、通信路の雑音処理といった、改善の望まれる課題は山積していた。

本研究代表者の研究開始当初の成果では、自己双対含有性を持たないＣＳＳ型のＬＤＰＣ符号が提案されていた。この提案法は、Ａｒｒａｙ－Ｔｙｐｅと呼ばれる標準的な正則ＬＤＰＣ符号の構成技術を元に、シミュレーションによる誤判定を利用するといった、従来とは全く異なる符号構成法を生み出していた。

量子符号の代表格であるＣＳＳ符号には、

古典論的アナロジーがある。それは、線形符号２つの組でありそれらに包含関係を有するものを言う。この有用性としては、ＢＢ８４プロトコルの量子情報理論的無条件安全性証明に用いられたShor, Preskillの手法において、量子誤り訂正符号であるＣＳＳ符号の古典論的アナロジーが実現できれば秘匿性が高い誤り訂正手法が実現できることが指摘されている。それだけに留まらず、ＣＳＳ符号の古典論的アナロジーが開発されれば、直ちに量子符号としてのＣＳＳ符号の設計にも応用が効く。その為、そういった古典符号の開発は、現在の研究課題としても、未来の通信技術における基盤技術としても要請されるものである。以下、それら符号を単にＣＳＳ型古典符号と呼ぶことにする。

ＣＳＳ型古典符号に関しては、これまで代数的なアプローチをメインとして研究がなされてきている。Calderbankらは量子符号におけるＣＳＳ符号を提案した際、ＣＳＳ型線形符号の存在性を仮定し性能評価を行った。そこで、実際の構成が望まれ、Sarvepalliらによ りReed-Muller符号のＣＳＳ型符号への適用、Grasslによる量子Reed-Solomon符号が提案されている。これらの符号は代数的に構成されてきた。ＣＳＳ型の符号は含まれる側の符号の双対符号の性能が重要であるため、性能の評価を行うには代数的なアプローチが有用とされてきた。しかし、代数的符号では、符号長・符号化率に関しての自由度が高いとは言えない。

符号長･符号化率の設計に自由度を持たせ、実用的であり高度な誤り訂正能力を持つ符号として、近年注目を集め続けてきた符号としてＬＤＰＣ（低密度パリティ検査）符号が知られている。ＬＤＰＣ符号は非常に高性能である一方、ＬＤＰＣ符号は符号の構造が読み取り難い。その為、ＣＳＳ型の符号構成に重要である、双対符号の性能評価が難しく、決定打といえる良い構成方法が実現されていなかった。

ＬＤＰＣ符号を利用したＣＳＳ型の符号構成では、自己双対含有性を持つ符号がMackayにより提案されている。この符号は符号長・符号化率も自由度がある。しかし、符号の誤り訂正能力に関して、改善の余地が非常に多く感じられるものであった。

２．研究の目的

本研究の目的は量子暗号装置で用いられる雑音処理の問題に対する、実用的で性能の高い符号化技術の開発である。

特に量子暗号プロトコルの中でも最も著名とされる、ＢＢ８４プロトコルに適した実用的符号化技術の開発を第一の目的とする。更に具体的には「ＣＳＳ符号の古典的アナロジーを実用的なＬＤＰＣ符号として実現すること」を、最大の目的として遂行する。

この研究成果は、非常に高度な安全性を保証する量子暗号方式の実用面にも、今後の量子通信理論研究にも幅広くインパクトを与えることが期待できる。

本研究代表者のこれまでの提案法を進展させることにより、研究期間を通じ、通信路のビット反転誤り率もしくは位相誤り率が0.03程度でも、フレーム誤り率が0.005未満とできるＣＳＳ型のＬＤＰＣ符号を実現する。

３．研究の方法

本研究では、量子情報理論の為の符号構成をＬＤＰＣ符号の観点から行うが、ＬＤＰＣ符号の評価には、理論的な解析のみならず、通信路をパーソナルコンピュータ上でシミュレートした評価結果が不可欠である。そこで、初年度は、シミュレーションを常時実行させる計算機を導入する。

ＳＩＴＡ，ＳＣＩＳ，ＱＩＴ、ＬＤＰＣワークショップと言った代表的な会議に積極的に参加し情報収集と発表を行う。

量子暗号における誤り訂正に有用として知られるＣＳＳ型の線形符号は包含関係にある二つの符号の組であるが、重要な性能はそれら二つの符号そのままではない。含むほうの線形符号のフレーム誤り率、そして、含まれるほうの双対符号のフレーム誤り率が重要である。含むほうの符号としてＬＤＰＣ符号を用いた場合、含まれる符号、つまり部分符号の構成自体が問題となる。それは、ＬＤＰＣ符号は性能の良い符号であるが、符号空間の構造が見えにくいことに起因する。

本研究の独創的かつ主要なアイデアは、一つのＬＤＰＣ符号を固定し、誤復号を利用して含まれる方の符号、つまり部分符号を構成することである。ＬＤＰＣ符号の性能解析ではシミュレーションを用いて行われる。シミュレーションの際に誤復号が発生すると期待でき、含むほうの符号空間自体を知らなくても、符号語を得ることが可能となる。そこで、それらを基底とした部分符号の構成が可能となる。

この手法を用いることで、得られる利点は別にある。誤復号により得られる符号語は、重みの小さな符号語が殆どである。つまり、部分符号の基底を並べた行列は、自動的に低密度となることが期待できる。そうして得た行列は、双対符号のパリティ検査行列である。つまり、含むほうの符号と、含まれるほうの双対符号の両方をＬＤＰＣ符号として実現・評価が可能となる。

今回はArray-Typeと呼ばれる種類の符号を含むほうのＬＤＰＣ符号として研究を進める。Array-TypeのＬＤＰＣ符号に着目した理由は、符号長・符号化率の設定が行いやすいことである。それらパラメータを幾つも試行錯誤しデータを召集する。また、正則ＬＤＰＣ符号であるので、誤復号で集まる符号語の重み分布の偏りが少ないと期待できる。

実用の面を考え、符号長は数千程度を考えている。この手法を用いるには、計算機を用いたシミュレーションによる十分な量のデータが必要であり、これらは多大な時間を要する。

そうして得たデータから、通信路の誤り率が0.02程度でフレーム誤り率の低いＣＳＳ型ＬＤＰＣ符号を与えるパラメータに目星を付ける。性能向上や手法の確立は次年度以降の課題とする。

二年度目以降も、計算機と外付け記憶媒体を購入する。これは初年度に作成したＬＤＰＣ符号のシミュレーション環境を平行して動作させることで、研究の加速を期待できる為である。

また、負荷の高い計算を繰り返す中で、予期しないトラブルの対処策としても、複数の計算機を持つことが重要である。また、初年度同様、負荷の高い計算を常時行わせることと、多くのシミュレーション結果を扱うため、バックアップ用の記憶媒体が必要である。

消耗品費は、論文別刷り費に用いる。結果の成果を論文誌に投稿していくため、この予算も必要である。

初年度で検討するArray-TypeのＬＤＰＣ符号は内径が、基本的なデータを揃える現段階では十分であるが、６である為に、ＣＳＳ型の含む符号として、性能の頭打ちが予測される。そこで、別の正則ＬＤＰＣ符号の検討が必要であると予測される。Array-TypeのＬＤＰＣ符号に対し、マスク化と呼ばれる手法を用いて小さなループを取り除くことができる。この手法を利用し、正則ＬＤＰＣ符号の性能を向上させ、目標とする性能の良いＣＳＳ型のＬＤＰＣ符号を構成していく。必要に応じ、

array-Type以外のＬＤＰＣ符号も検討に入れる。

最終的な目標は通信路の誤り率0.01から0.03の範囲で、フレーム誤り率0.005を達成するＣＳＳ型ＬＤＰＣ符号の構成である。計画としては、前年度のうちにこれら誤り率の範囲で利用しやすい符号が選定されている。もし、有用な符号が見つからない場合は、若干符号長を大きくしたケースも検討する。その際、一万程度の符号長を用いることにする。本研究の手法は確定的な符号構成法ではない為、シミュレーションの結果により性能が左右される。シミュレーションにより得る結果は確率的であることは免れない。そこで、誤復号で得られた符号語から直接に部分符号を作り出さず、誤復号で得られた符号語を多く集めることで、部分符号を構成する符号語を選び出す手順を導入することが可能となる。データを多くすること、そして確定的な手順を導入することにより、性能の良いＣＳＳ型ＬＤＰＣ符号の構成を高い精度で構成できる手法が確立できる。

４．研究成果

２００６年度：本研究の目標は、量子誤り訂正符号の１つである CSS 符号を構成する古典符号の対を LDPC 符号として実現し、通信路の雑音率が 3%という大きな雑音環境の下でもブロック誤り率が 0.005 未満で済む高い誤り訂正パフォーマンスを達成することにある。問題は、古典符号の理論では想定されていなかった条件（本研究ではねじれ関係と呼んでいる）と、高い誤り訂正能力の両立にある。研究計画では Array-Type とよばれる LDPC 符号を１つ固定し、対となるもう一方の符号探索に計算機探索の手法を利用することで、そのような符号対を構成する予定であった。研究を通じ、Array-Type LDPC 符号では達成したいレベルの符号構築が困難であるとわかってきた。そこで、Array-Type の拡張である Quasi-Cyclic LDPC 符号を研究対象に加えるよう方向転換を行った。これが功を奏し、低い符号化率の符号では、３年間を通した目標である高い誤り訂正パフォーマンスを初年度で達成できた。さらに、計算機を用いる手法から得た知見をもとに、理論的考察が進められた。重要な理論成果として、QC LDPC 符号の組が量子符号の要素となる条件を、組合せ論的にシンプルな用語で与えることに成功した。結果、理論的手法と計算機を用いた手法を組み合わせることで、研究当初の想定を遥かに上回る効率良い構成方法を得ている。これらの成果は、ISIT2007 を初めとした査読のある国際学会等で採択されている。

２００７年度：本年度の計画の軸は３つあり、それらは「１．ランダムに生成された符号の性能解析」、「２．その解析結果を受け、適切なパラメータを絞り込むための理論検討と計算機シミュレーション」、そして「３．高い誤り訂正能力をもつ符号のパラメータを、インターネット等を通じて公開」である。を達成するためには、ランダムな手法でＣＳＳ符号の条件であるねじれ関係を満たすＬＤＰＣ符号の組が構成する方法が必要となった。そこで、単純な構成方法を発見し、いくつかのランダムな符号構成を実現した。また、シミュレーションにより性能評価を行った。この成果は国際会議ＨＩＳＣにて講演している。

ＨＩＳＣで発表した構成方法をもとに、数多くのシミュレーションを実行した。また、ＨＩＳＣでのシンプルな構成方法を理論的に掘り下げ、古典ＱＣ－ＬＤＰＣ符号の理論

との融合に成功した。結果はＩＳＩＴ２００７にて発表している。

ＩＳＩＴ２００７で発表した符号のなかで、非常によい誤り訂正能力を示したパラメータを選定した。そして、研究代表者のＨＰにて、それらパラメータを公開した。

（ http://staff.aist.go.jp/hagiwara.hagiwara/qecc/qecc.html）

２００８年度：２００７年度までに構成された符号を中心に、「符号長」、「符号化率」、「ブロック誤り」、「符号化のしやすさ」、「復号のしやすさ」の視点で解析し、本研究で構成した符号は準巡回と呼ばれる性質が非常に有効と確認できた。「復号のしやすさ」について、LDPC 符号であることから、高速な復号が可能であることも確認できた。ブロック誤りについては、これまで同様にシミュレーションで確認を行っている。「符号長」、「符号化率」に関して、新たな理論解析手法が編み出せる状況になっている。これは今後、引き続き研究が必要である。

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　５　件）

１．Manabu Hagiwara, Marc Fossorier, Comment on “Quasi-Cyclic Low Density Parity Check Codes from Circulant Permutation Matrix”, IEEE Transactions on Information Theory, vol.55-3, 2009, pp.1430-1430, 査読有.

２．Hideki Imai, Manabu Hagiwara, Error-Correcting Codes and Cryptography, Applicable Algebra In Engineering Communication and Computing, vol.19-3, 2008, pp.213-228, 査読有.

３．Manabu Hagiwara, Hidaki Imai, A Simple Construction of Quantum Quasi-Cyclic LDPC Codes, Proc. of 2007 Hawaii and SITA Joint Conference on Information Theory, vol.1, 2007, pp.19-23, 査読無.

４．Manabu Hagiwara, Koji Nuida, Takashi Kitagawa, Marc Fossorier, Hideki Imai, On Minimal Length of Quasi Cyclic LDPC Codes with Girth Greater Than or Equal to 6, Proc. of The 2006 International Symposium on Information Theory and its Applications, vol.1, 2006, CD-ROM, 査読有.

５．Manabu Hagiwara, Hideki Imai, On a Construction of a Non-stabilizer Clifford Quantum Code for 2h(2j+1)-Level States, Electronics and Communications in Japan Part III-Fundamental Electronic Science, Apr-90, 2006, pp.63-68, 査読有.

〔学会発表〕（計　５ 件）

１．萩原学, 準巡回低密度パリティ検査符号にまつわる離散数学的側面と量子符号への拡張にまつわる問題, COS 08, 09/09/2008, 沖縄県

２．萩原学, 今井秀樹, ねじれ関係にあるＬＤＰＣ符号の組の構成, 情報理論とその応用シンポジウム, 11/27/2007, 三重県

３．萩原学, 非正則疑似巡回低密度パリティ検査符号の量子符号化にまつわる組合せ論的アプローチ

４．Manabu Hagiwara, Quantum Error-Correcting Codes, Summer School on Mathematical Aspects of Quantum Computing, 08/27/2007, Kinki University.

５．Manabu Hagiwara, Hideki Imai, Quantum Quasi-Cyclic LDPC Codes, 2007 IEEE International Symposium on Information Theory, 06/26/2007, Nice.

〔その他〕（計　１ 件）
１．研究成果ホームページ：
http://staff.aist.go.jp/hagiwara.hagiwara/qecc/qecc.html

６．研究組織
(1)研究代表者
萩原　学（HAGIWARA MANABU）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究員
研究者番号：80415728