

機関番号：12608

研究種目：若手研究 (B)

研究期間：2009 ~ 2010

課題番号：21760276

研究課題名 (和文) 構造を有する LDPC 符号とその応用に関する研究

研究課題名 (英文) Structured LDPC codes and their applications

研究代表者

笠井 健太 (KASAI KENTA)

東京工業大学・大学院理工学研究科・助教

研究者番号：70431997

研究成果の概要 (和文)：

本研究では、量子計算および量子通信を実現するために必要な技術である量子誤り訂正符号を提案している。萩原・今井量子誤り訂正符号を有限体に拡張することで、従来最良の量子誤り訂正符号の誤り訂正能力を大きく凌ぐ量子誤り訂正符号を構成することに成功している。

研究成果の概要 (英文)：

We consider the quantum error correction over the depolarizing channels with non-binary low-density parity-check (LDPC) codes defined over Galois field of size  $2p$ . The proposed quantum error correcting codes are based on the binary quasi-cyclic CSS (Calderbank, Shor and Steane) codes. The resulting quantum codes outperform the best known quantum codes and surpass the performance limit of the bounded distance decoder.

交付決定額

(金額単位：円)

	直接経費	間接経費	合計
2009年度	1,000,000	300,000	1,300,000
2010年度	700,000	210,000	910,000
年度			
年度			
年度			
総計	1,700,000	510,000	2,210,000

研究分野：工学

科研費の分科・細目：電気電子工学・通信・ネットワーク工学

キーワード：LDPC 符号、誤り訂正、量子通信

## 1. 研究開始当初の背景

量子誤り訂正は、量子状態を確実に保存し高信頼度で通信すること、つまり量子計算および量子通信を実現するために必要な技術である。量子 LDPC 符号は、疎なパリティ検査方程式によって定義された、古典 LDPC 符号に対応する量子誤り訂正符号である。

CSS (Calderbank, Shor and Steane) 符号は、量子誤り訂正符号の重要な符号クラスである。CSS 符号  $CSS(C,D)$  は  $H_C(H_D)^T = 0$

となる 2 元パリティ検査行列  $H_C$  と  $H_D$  を有する、符号化率  $1/2$  以上の、2 つの 2 元古典符号  $C$  と  $D$  によって定義される量子誤り訂正符号である。

研究開始当初、無記憶通信路の通信路容量に接近する復号性能を有する、効率的に復号可能な誤り訂正符号は、すでに実現されていた。デジタル通信では 0 と 1 が表すビットを情報として扱うが、様々なノイズの影響によりビットが反転などして意図したものと異なる誤りが生じてしまうことがある。移動体通

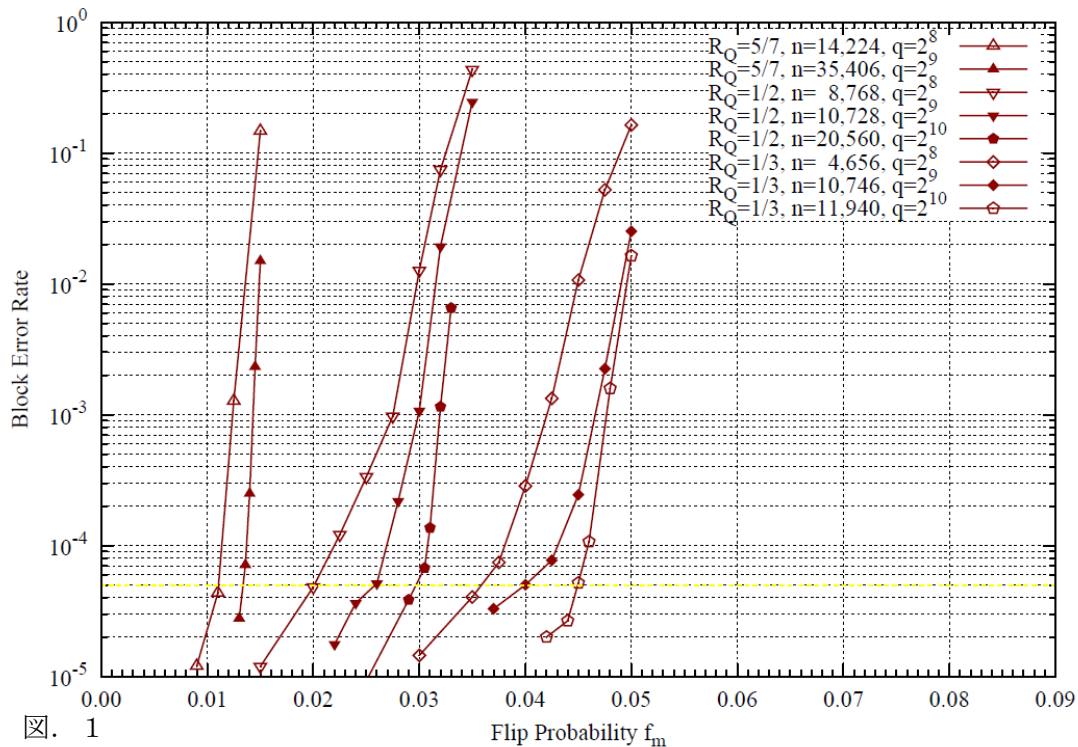


図. 1

信や記憶メディアの信頼性を高める誤り訂正技術は、Berrou らによるターボ符号の発明とその後の LDPC (Low-Density Parity-Check) 符号の再発見により、大きなブレークスルーが与えられた。しかし、効率的に復号可能な量子誤り訂正符号は、MacKay らによるヒューリスティクスを含んだ構成法しか知られておらず、誤り訂正能力も高くなかった。

## 2. 研究の目的

サイズが2より大きな有限体上で定義される LDPC 符号は、2元 LDPC 符号よりも優れた復号性能を有することが知られている。この誤り訂正技術を多元シンボルに拡張し、量子誤り訂正に応用することが本研究の目的である。

## 3. 研究の方法

当初の研究計画では、構造を有する LDPC 符号を用いた量子誤り訂正符号の設計を目指していたが計画通りの方法では、従来からある量子誤り訂正方式を上回る性能を引き出すことができなかった。そこで、申請書に書いた方法とは別の次のようなアプローチを試した。萩原と今井は、quasi-cyclic (QC) LDPC 符号を用いた LDPC-CSS 符号を提案している。この LDPC-CSS 符号のパリティ検査行列は任意の偶数の行重み  $L \geq 4$  と列重  $J (L/2 \geq J \geq 2)$  を有するように設計可能である。萩原と今井の LDPC-CSS 符号の構成法を次のように多元 LDPC 符号に拡張した。

この方法では、列重みが2であり行重みが  $L$  であり、直交するパリティ検査行列  $\Gamma$  と  $\Delta$  を、次の手順によって構成している。まず萩原と今井の方法により、列重みが2であり行重み

が  $L$  である2元  $M \times N$  パリティ検査行列  $C$  と  $D$  を構成する。 $C$  と  $D$  の非零成分を、 $GF(2^m)$  上の非零要素をとる変数と置き換えて、新たに列重み2、行重み  $L$  の  $GF(2^m)$  上の  $M \times N$  行列  $\Gamma$  と  $\Delta$  を考える。次に  $\Gamma$  と  $\Delta$  の非零成分を決定する。この問題は一般には極めて難しい問題として知られている  $GF(2^m)$  上の連立2次多変数方程式となってしまう。しかし、幸運なことに、 $L=2$  の萩原と今井の構成法から得られた  $C$  と  $D$  から作られた  $\Delta$  と  $\Gamma$  に対しては、この問題を整数上の線形連立方程式に帰着させることができる。

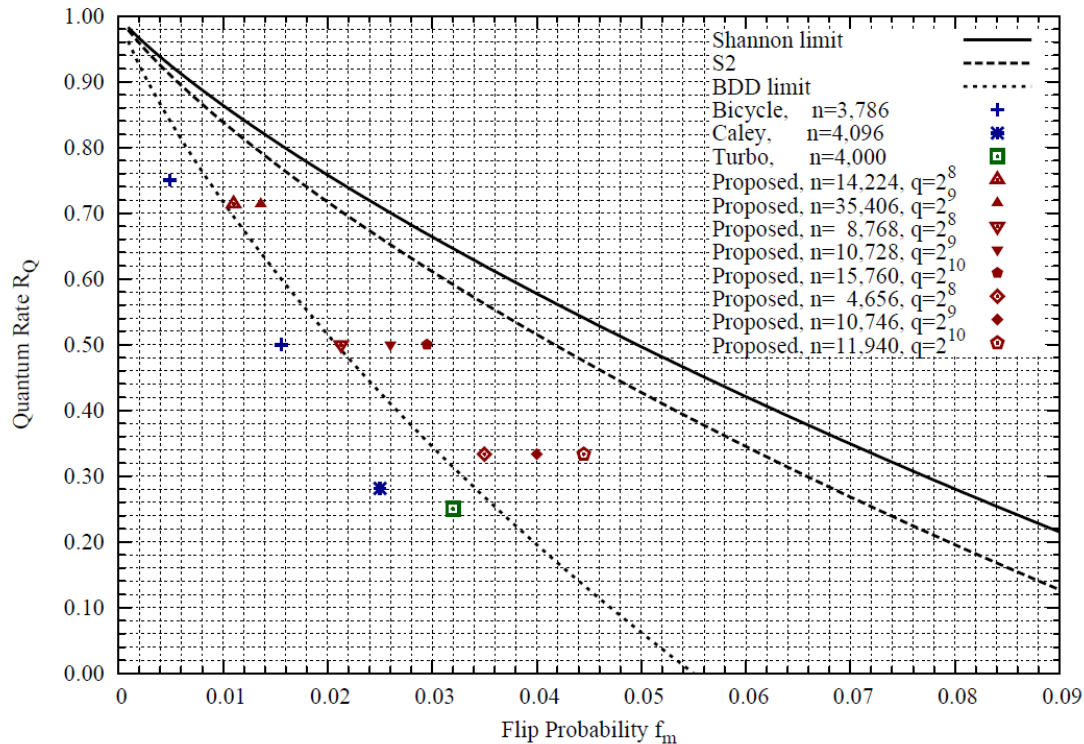
## 4. 研究成果

この方法で得られた、量子誤り訂正符号は従来の効率的に復号できる量子誤りの中で最も高い性能を有することを数値実験により確認した。

図1に量子符号化率  $R_Q$ 、符号長  $n$  [qubit] の  $GF(q)$  上で定義される提案符号の復号性能を描いた。横軸は反転確率、縦軸はブロック誤り率を表している。ブロック誤り率  $10^{-4}$  辺りまでエラーフロアがないことが確認できる。図2に、量子符号化率  $R_Q$  対ブロック誤り率  $5.0 \times 10^{-4}$  を達成する反転確率の性能評価を表した。赤で表した点が提案符号を表し、青と緑の点は、従来最良の量子誤り訂正符号を表している。

## 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 4 件)

(1) K. Kasai, D. Declercq, C. Poulliat and K. Sakaniwa, "Multiplicatively Repeated Non-Binary LDPC Codes," accepted, *IEEE Trans. on Information Theory*, Apr. 2011.

(2) K. Kasai, T. Awano, D. Declercq, C. Poulliat and K. Sakaniwa, "Weight Distribution of Non-binary LDPC Codes," *IEICE Trans. on Fundamentals*, vol. E94-A, no. 4, pp. 1106-1115, Apr. 2011.

(3) K. Kasai, T. Awano, D. Declercq, C. Poulliat and K. Sakaniwa, "Weight Distributions of Multi-Edge type LDPC Codes," *IEICE Trans. on Fundamentals*, vol. E93-A, no. 11, pp. 1942-1948, Nov. 2010.

(4) K. Kasai and K. Sakaniwa, "Fourier Domain Decoding Algorithm of LDPC codes for Parallel Implementation," *IEICE Trans. on Fundamentals*, vol. E93-A, no. 11, pp. 1949-1957, Nov. 2010.

[学会発表] (計 17 件)

(1) K. Kasai, and K. Sakaniwa, Spatially-Coupled MacKay-Neal Codes and Hsu-Anastasopoulos Codes, Proc. IEEE Int. Symp. Inf. Theory (ISIT 2011), Saint-Petersburg, Russia, Jul. 31-Aug. 5 2011.

(2) K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, Non-Binary Quasi-Cyclic Quantum LDPC Codes, Proc. IEEE Int. Symp. Inf. Theory (ISIT 2011), Saint-Petersburg, Russia, Jul. 31-Aug. 5 2011.

(3) T. Nozaki, K. Kasai, and K. Sakaniwa, Analysis of Stopping Constellation Distribution for Irregular Non-binary LDPC code ensemble, Proc. IEEE Int. Symp. Inf. Theory (ISIT 2011), Saint-Petersburg, Russia, Jul. 31-Aug. 5 2011.

(4) H. Uchikawa, K. Kasai, and K. Sakaniwa, Spatially Coupled LDPC Codes for Decode-and-Forward in Erasure Relay Channel, Proc. IEEE Int. Symp. Inf. Theory (ISIT 2011), Saint-Petersburg, Russia, Jul. 31-Aug. 5 2011.

(5) S. Kudekar and K. Kasai, Threshold Saturation on Channels with Memory via Spatial Coupling, Proc. IEEE Int. Symp. Inf. Theory (ISIT 2011), Saint-Petersburg, Russia, Jul. 31-Aug. 5 2011.

(6) S. Kudekar and K. Kasai, Spatially Coupled Codes over the Multiple Access Channel, Proc. IEEE Int. Symp. Inf. Theory (ISIT 2011), Saint-Petersburg, Russia, Jul. 31-Aug. 5 2011.

(7) M. Hagiwara, K. Kasai, H. Imai, and K. Sakaniwa, Spatially Coupled Quasi-Cyclic Quantum LDPC Codes, Proc. IEEE Int. Symp. Inf. Theory (ISIT 2011), Saint-Petersburg, Russia, Jul. 31-Aug. 5 2011.

(8) T. Nozaki, K. Kasai, and K. Sakaniwa, Analysis of Error Floors of Non-Binary LDPC Codes over MBIOS Channel, Proc. of Int. Conf. on Comm. (ICC 2011), Kyoto, Japan, Jun. 5-9 2011.

(9)H. Uchikawa, K. Kasai, and K. Sakaniwa, "Terminated LDPC Convolutional Codes over  $GF(2^p)$ ", Forty-Eighth Annual Allerton Conference on Communication, Control, and Computing, Illinois 9.29-10.1. 2010.

(10)K. Kasai, R. Matsumoto and K. Sakaniwa, "Information Reconciliation for QKD with Rate-Compatible Non-Binary LDPC Codes," Proc. of International Symposium on Information Theory and its Applications (ISITA 2010), pp. 922-927, Taichung, Taiwan, Oct. 17-20,2010.

[その他]

ホームページ等

<http://www.comm.ss.titech.ac.jp/~kenta/index-e.html>

## 6. 研究組織

### (1) 研究代表者

笠井 健太 (KASAI KENTA)

東京工業大学・大学院理工学研究科・助教

研究者番号：70431997