論　文

多元LDPC符号に適したバースト誤り訂正アルゴリズム

木全　佑輔[†]　　和田山　正[†a)]

A Burst Error Correcting Algorithm for Nonbinary LDPC Codes

Yusuke KIMATA[†] and Tadashi WADAYAMA[†a)]

あらまし　本論文では，多元 LDPC 符号に適したバースト誤り訂正アルゴリズムを提案する．本論文で提案する復号アルゴリズムの復号プロセスにおいては，まず受信語から得られるシンドロームと検査行列の部分行列からなる連立方程式を解くことによりバースト誤りの候補が生成される．次に，得られた誤りベクトルの候補の中からバースト誤りの仮定に矛盾しないベクトルを推定語として選び出すことで復号を行う．更に本論文では，そのバースト誤り訂正アルゴリズムについて復号特性の解析を行い，復号誤り率の上界を導出する．本論文で提案する上界は，バースト誤り訂正アルゴリズムに用いる部分行列の列ベクトルによって張られる線形空間の構造に基づいて導出される．本論文で導く上界は，検査行列にガウス消去法を適用することにより効率的に数値評価することが可能であり，多元 LDPC 符号のバースト誤り訂正能力を評価する上で有用な指標となっている．

キーワード　多元 LDPC 符号，バースト誤り訂正，連立方程式，上界

1. まえがき

適切に設計された多元 LDPC 符号 [1] の復号性能は，二元 LDPC 符号の復号性能を上回ることが報告されており [2]，近年，多元 LDPC 符号に関する研究が盛んに行われている．

通信・記録等の分野において，多元 LDPC 符号の利用を考えた場合，ランダム性の誤りに対する復号性能だけでなく，バースト誤りに対する復号性能も重要である．ハードディスク等の磁気記録装置の場合，メディアの欠陥などによりバースト誤りが発生することが知られており，システムの信頼性向上のためにバースト誤りに関する強力な訂正アルゴリズムが求められている．

二元 LDPC 符号を用いた消失バースト誤り訂正については，文献 [3]～[6] などにおいて，訂正アルゴリズム，検査行列の構成，確率的解析の文脈から検討が行われている．また，Fossorier による文献 [7] は，一般の線形符号におけるバースト誤り訂正アルゴリズムについての議論を展開している．しかし，多元 LDPC 符号の性質に着目したバースト誤り訂正アルゴリズムについての研究はほとんどなされていない状況にある．

本論文では，多元 LDPC 符号に適したバースト誤り訂正アルゴリズム [8] を提案する．本論文で提案する復号アルゴリズムでは，受信語から得られるシンドロームと検査行列の部分行列からなる連立方程式を解くことによりバースト誤りの候補を生成する．次に，得られた誤りベクトルの候補の中からバースト誤りの仮定に矛盾しないベクトルを推定語として選ぶことで復号を行う．また，提案復号アルゴリズムについて復号特性の解析を行い，復号誤り率の上界を導出する [9]．この誤り率上界は，バースト誤り訂正アルゴリズムに用いる部分行列の列ベクトルによって張られる線形空間の構造に基づいて導出される．本論文で導く上界は，検査行列にガウス消去法を適用することにより，効率的に数値評価することが可能であり，多元 LDPC 符号のバースト誤り訂正能力を評価する上で有用な指標となっている．

本論文の構成は以下のとおりである．**2.** では，本論文で用いる表記や記号について説明する．**3.** では，多元 LDPC 符号に適したバースト誤り訂正アルゴリズムの提案を行う．**4.** では，提案バースト誤り訂正アルゴリズムについて復号特性の解析を行い，復号誤り率の上界を導出する．**5.** では，計算機実験により提案ア

[†] 名古屋工業大学大学院工学研究科，名古屋市
Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya-shi, 466–8555 Japan
a) E-mail: wadayama@nitech.ac.jp

ルゴリズムとその誤り率上界について評価を行う．

2. 準　　備

本章では，本論文で用いる表記の定義，並びに基礎事項の説明を行う．

2.1 表記・記号

ガロア体上の行列 $X \in \mathbb{F}_q^{m\times n}$ の第 i 列ベクトル $(i \in [0, n-1])$ を $\boldsymbol{x}_i^T$ とする．ここで，$\mathbb{F}_q$ は q 元（q は素数のべき）のガロア体である．また，m, n は自然数である．記法 $[a, b]$ $(1 \le a, b \le n)$ は整数集合 $\{a, a+1, a+2, \ldots, b\}$ を意味する．ベクトルはボールド体の英小文字で表し，特に指定がなければ行ベクトルを意味する．また，行列は英大文字で表す．なお，本論文において，行・列のインデックスは 0 から始まるものとする．

n を法として連続した添字をもつ X の列ベクトルからなる行列を X の部分行列と呼ぶ．行列 X の第 i $(i \in [0, n-1])$ 列ベクトルから第 $\langle i+l-1\rangle$ 列ベクトルまでの長さ l (>0) の部分行列を $X_i^{(l)}$ と表記する．すなわち，

$$X_i^{(l)} = (\boldsymbol{x}_{\langle i\rangle}^T, \boldsymbol{x}_{\langle i+1\rangle}^T, \ldots, \boldsymbol{x}_{\langle i+l-1\rangle}^T)$$

である．記法 $\langle a\rangle$ は $a \bmod n$ を表す．行列 X の列ベクトルが張る線形空間を

$$\mathrm{span}(X) = \left\{ \sum_{i=0}^{n-1} a_i \boldsymbol{x}_i \in \mathbb{F}_q^n : a_i \in \mathbb{F}_q, i \in [0, n-1] \right\}$$

とする．集合 $[0, n-1]$ に含まれる a, b について，それらの間の Lee 距離 $\delta(a, b)$ を

$$\delta(a, b) = \min(|a-b|, n-|a-b|)$$

と定義する．

2.2 多元 LDPC 符号

本論文では，疎な検査行列によって定義される多元 LDPC 符号について議論する．ガロア体 $\mathbb{F}_q$ 上の疎な検査行列を $H \in \mathbb{F}_q^{m\times n}$ とする．ここで，m, n は自然数であり，$n > m$ であると仮定する．この検査行列 H に基づき，多元 LDPC 符号 $C(H)$ は $C(H) = \{\boldsymbol{x} \in \mathbb{F}_q^n : H\boldsymbol{x}^T = \boldsymbol{0}\}$ と定義される．

2.3 加法的バースト通信路

本節では，本論文で用いる通信路モデルである加法的バースト通信路を定義する．与えられた検査行列 H に対して，最大連続独立列数 η_{max} [8] は

$$\eta_{max} = \max_{\eta>0}\{\eta : \forall i \in [0, n-1], \mathrm{rank}(H_i^{(\eta)}) = \eta\}$$

と定義される．本論文で提案する復号法では，検査行列の部分行列を利用する．その部分行列の列数を η $(0 < \eta \le \eta_{max})$ とする．

送信者は送信したいメッセージに従い，符号語 $\boldsymbol{x} \in C(H)$ を選択し送信する．通信路では，バースト誤り $\boldsymbol{e} \in \mathbb{F}_q^n$ が生起する（その確率モデルは後述）．受信語を $\boldsymbol{y} \in \mathbb{F}_q^n$ とするとき，受信者は $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$ を受信する．この加法は $\mathbb{F}_q$ 上の加法に基づく．

バースト誤り $\boldsymbol{e}$ に関する確率モデルは次のとおりである．最大バースト長 β_{max} を $0 < \beta_{max} \le \eta$ を満たす整数とする．本モデルでは，誤りベクトル $\boldsymbol{e} \in \mathbb{F}_q^n$ は

$$\boldsymbol{e} = \mathrm{cyc}(\tilde{\boldsymbol{e}} \mid 0^{n-\beta_{max}}, s) \tag{1}$$

の形をしていると仮定する．ここで，

$$\tilde{\boldsymbol{e}} = (\tilde{e}_0, \tilde{e}_1, \ldots, \tilde{e}_{\beta_{max}-1}) \in \mathbb{F}_q^{\beta_{max}},\ \tilde{e}_0 \ne 0 \tag{2}$$

である．

ベクトル $\tilde{\boldsymbol{e}}$ は確率変数である．先頭要素 $\tilde{e}_0$ は $\mathbb{F}_q$ の非零元上の一様分布に従い実現値が定まる．その他の要素 $\tilde{e}_i$ $(i \in [1, \beta_{max}-1])$ は $\mathbb{F}_q$ の一様分布に従う．表記 $\mathrm{cyc}(\boldsymbol{z}, j)$ は，ベクトル $\boldsymbol{z} \in \mathbb{F}_q^n$ を右方向に $j \in [0, n-1]$ シンボル巡回置換させて得られるベクトルを意味している．記法 0^m は長さ m のゼロ行ベクトルである．演算子 | はベクトルの連接を表す．

式 (1) におけるシフト量 s はバースト開始位置を表す確率変数であり，その実現値は，$[0, n-1]$ 上の一様分布に従い定まると仮定する．バースト誤りベクトル $\boldsymbol{e} \in \mathbb{F}_q^n$ に対して，そのバースト開始位置を $\mu(\boldsymbol{e})$ と表記する．式 (1) で定義されるバースト誤り $\boldsymbol{e}$ については，$\mu(\boldsymbol{e}) = s$ となる．

上記で説明した本論文で仮定する誤りベクトルの概略図を図 1 に示す．

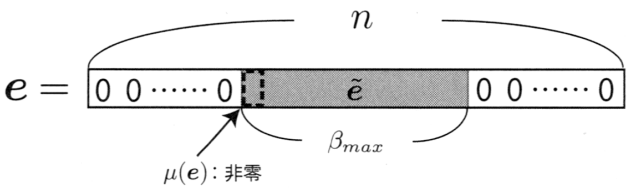


図 1　通信路で生起するバースト誤りベクトル $\boldsymbol{e}$ の概略図
Fig. 1　Outline drawing of burst error vector on channel.

3. バースト誤り訂正アルゴリズム

本論文では，多元LDPC符号に適したバースト誤り訂正アルゴリズムを提案する．本論文で提案するバースト誤り訂正アルゴリズムは，部分行列に基づく連立方程式系を解くことにより得られる推定解の中でバースト仮定に矛盾しないものを選び出す，という考え方に基づいている．本章では，提案法の概要から始めて，次にその詳細について述べる．

3.1 解候補集合

以下で説明する復号法では，検査行列 H からウィンドウ幅 η $(0 < \eta \leq \eta_{max})$ の部分行列を取り出し，対応する連立一次方程式を解くことにより誤りベクトルの候補を生成する．以下では，バースト誤り長 $\beta \leq \beta_{max}$ のバースト誤りベクトル $\boldsymbol{e}$ の生起を仮定する．ここで，β_{max} は $0 < \beta_{max} < \eta$ を満たす整数である．

受信器では，シンドローム $\boldsymbol{s}$ が $\boldsymbol{s} = H\boldsymbol{y}^T = H\boldsymbol{e}^T$ として最初に計算されるものとする．連立方程式 $H\boldsymbol{e}^T = \boldsymbol{s}$ が解ければ誤りベクトル $\boldsymbol{e}$ の特定が可能となるが，$n > m$ なのでこの問題は不良設定問題となり，一般には解を唯一に定めることができない．したがってバースト誤りの特性を生かした復号法が必要となる．

ウィンドウ幅 η の H の部分行列に関して，連立一次方程式

$$H_i^{(\eta)}\boldsymbol{z}^T = \boldsymbol{s}, \quad i \in [0, n-1] \tag{3}$$

を考える．ここで，$\boldsymbol{s} = H\boldsymbol{e}^T$ はシンドローム，$H_i^{(\eta)} \in \mathbb{F}_q^{m\times\eta}$ は H の部分行列（**2.1** の定義参照）であり，$\boldsymbol{z} \in \mathbb{F}_q^{\eta}$ である．ウィンドウ幅 η に関する仮定 $\eta \leq \eta_{max}$ より，

$$\mathrm{rank}(H_i^{(\eta)}) = \eta, \quad \forall i \in [0, n-1]$$

が成り立つ．

今，$\boldsymbol{s} \in \mathrm{span}(H_i^{(\eta)})$ と仮定する．このとき，$\mathrm{rank}(A) = \eta$ を満たす任意の行列 $A \in \mathbb{F}_q^{\eta\times m}$ を考える．行列 A を式 (3) の両辺に左から乗じることにより

$$(AH_i^{(\eta)})\boldsymbol{z}^T = A\boldsymbol{s} \tag{4}$$

が得られる．A と $H_i^{(\eta)}$ の階数が共に η であることから，$AH_i^{(\eta)} \in \mathbb{F}_q^{\eta\times\eta}$ は正則行列となる．上式の両辺に $AH_i^{(\eta)}$ の逆行列を乗じることにより，解

$$\tilde{\boldsymbol{z}}_i^T = (AH_i^{(\eta)})^{-1}A\boldsymbol{s} \tag{5}$$

が得られる．仮定 $\boldsymbol{s} \in \mathrm{span}(H_i^{(\eta)})$ より，この解について，確かに $H_i^{(\eta)}\tilde{\boldsymbol{z}}_i^T = \boldsymbol{s}$ が成立する．なお，$\tilde{\boldsymbol{z}}_i^T = \boldsymbol{s}$ は A の取り方に依存しないことに注意したい．

一方，$\boldsymbol{s} \notin \mathrm{span}(H_i^{(\eta)})$ の場合，式 (5) により定まる $\tilde{\boldsymbol{z}}_i$ は $H_i^{(\eta)}\tilde{\boldsymbol{z}}_i^T = \boldsymbol{s}$ を満たさない．なぜならば，この等式を満たすとすると仮定に矛盾するからである．

式 (5) の計算は，ガウス消去法を利用して効率良く実行することができる．この場合，A はガウス消去法により定まる基本行操作に対応する行列となる．

このようにして求められる解に基づいて解候補集合を次のように定める．ここで，誤りベクトル $\boldsymbol{e} \in \mathbb{F}_q^n$ が $\boldsymbol{e} = \mathrm{cyc}(\tilde{\boldsymbol{e}} \mid 0^{n-\eta}, s)$，$s \in [0, n-1]$，$\tilde{\boldsymbol{e}} = (\tilde{e}_0, \tilde{e}_1, \ldots, \tilde{e}_\eta) \in \mathbb{F}_q^{\eta}$，$\tilde{e}_0 \neq 0$ の形に書けるとき，$\boldsymbol{e}$ のバースト長 $\ell(\boldsymbol{e})$ を $\ell(\boldsymbol{e}) = R(\tilde{\boldsymbol{e}}) + 1$ と定義する．ただし，$R(\boldsymbol{a})$ は，ベクトル $\boldsymbol{a} \in \mathbb{F}_q^k$ の最右非零位置を表し，長さ k のベクトル $\boldsymbol{a} = (a_0, a_1, \cdots, a_{k-1})$ に対して $R(\boldsymbol{a}) = \max\{i \in [0, k-1] : a_i \neq 0\}$ と定義される．

[定義 1]（解候補集合） 各 $i \in [0, n-1]$ について，式 (5) に基づき，$\tilde{\boldsymbol{z}}_i$ を求める．計算にはガウス消去法を利用する．推定バースト誤りベクトル $\boldsymbol{w}_i^* \in \mathbb{F}_q^n$ $(i \in [0, n-1])$ を

$$\boldsymbol{w}_i^* = \begin{cases} \mathrm{cyc}(\tilde{\boldsymbol{z}}_i \mid 0^{n-\eta}, i), & H_i^{(\eta)}\tilde{\boldsymbol{z}}_i^T = \boldsymbol{s} \\ \epsilon, & H_i^{(\eta)}\tilde{\boldsymbol{z}}_i^T \neq \boldsymbol{s} \end{cases} \tag{6}$$

とする．記号 ϵ は無効な解候補を表し，便宜上 $\ell(\epsilon) = \infty$ とする．それらをまとめた

$$W^* = \{\boldsymbol{w}_0^*, \boldsymbol{w}_1^*, \ldots, \boldsymbol{w}_{n-1}^*\}$$

を解候補集合と呼ぶ． □

以上の定義から解候補集合に含まれる ϵ を値にもたない任意の $\boldsymbol{w}_i^*$ について，

$$H\boldsymbol{w}_i^{*T} = \boldsymbol{s}, \quad \forall i \in [0, n-1] \tag{7}$$

が成り立つことが明らかである．値が ϵ でない解候補 $\boldsymbol{w}_i^*$ はいずれも式 (6) のとおりバースト誤り長がたかだか η のバースト誤りの形をしているため，バースト誤りベクトル $\boldsymbol{e}$ の推定候補となる．

3.2 バースト誤り訂正アルゴリズムの詳細

次の補題は，推定語 $\hat{\boldsymbol{e}}$ を解候補集合から選び出すために有用である．

[補題 1] ベクトル $\boldsymbol{e}$ をバースト誤り長 β $(\leq \beta_{max})$

のバースト誤りとし，誤り開始インデックスを $t \in [0, n-1]$ とする．すなわち，$\ell(\boldsymbol{e}) = \beta$, $\mu(\boldsymbol{e}) = t$ であり，$\boldsymbol{e}$ は

$$\boldsymbol{e} = \mathrm{cyc}(\tilde{\boldsymbol{e}} \mid 0^{n-\beta}, t)$$

を満たすベクトルとなる．ここで，$\tilde{\boldsymbol{e}}$ は条件 (2) を満たす．また，シンドローム $\boldsymbol{s} = H\boldsymbol{e}^T$ とする．このとき，任意の a $(0 \le a \le \eta - \beta)$ について

$$\boldsymbol{w}^*_{\langle t-a \rangle} = \boldsymbol{e}$$

が成立する．

(証明) 仮定から任意の a $(0 \le a \le \eta - \beta)$ について

$$\boldsymbol{s} = H^{(\eta)}_{\langle t-a \rangle} \tilde{\boldsymbol{z}}^T_{\langle t-a \rangle}$$

と

$$\boldsymbol{s} = H^{(\eta)}_{\langle t-a \rangle} (0^a \mid \tilde{\boldsymbol{e}} \mid 0^{\eta-\beta-a})^T$$

が成立する．ただし，0^0 は空列を意味するものとする．仮定 $\eta \le \eta_{max}$ より $\mathrm{rank}(H^{(\eta)}_{\langle t-a \rangle}) = \eta$ であるため，等式

$$\tilde{\boldsymbol{z}}_{\langle t-a \rangle} = (0^a \mid \tilde{\boldsymbol{e}} \mid 0^{\eta-\beta-a})$$

が得られる．この関係を利用することにより，

$$\begin{aligned} \boldsymbol{w}^*_{\langle t-a \rangle} &= \mathrm{cyc}(\tilde{\boldsymbol{z}}_{\langle t-a \rangle} \mid 0^{n-\eta}, t-a) \\ &= \mathrm{cyc}(0^a \mid \tilde{\boldsymbol{e}} \mid 0^{\eta-\beta-a} \mid 0^{n-\eta}, t-a) \\ &= \mathrm{cyc}(\tilde{\boldsymbol{e}} \mid 0^{n-\beta}, t) \\ &= \boldsymbol{e} \end{aligned} \tag{8}$$

が得られる． □

この補題に基づくバースト誤り訂正アルゴリズムの詳細を以下に示す．

バースト誤り訂正アルゴリズム

入力 シンドローム $\boldsymbol{s}$

出力 推定語 $\hat{\boldsymbol{e}}$

Step 1 定義 1 に従い，解候補集合 W^* を構成する．

Step 2 インデックス集合

$$T = \{i \in [0, n-1] : \ell(\boldsymbol{w}^*_i) \le \beta_{max}\} \tag{9}$$

について，$\forall i \in T$, $\boldsymbol{w}^*_i = \boldsymbol{a} \in \mathbb{F}_q^n$ が成り立つ場合，$\hat{\boldsymbol{e}} = \boldsymbol{a}$ を出力して終了する．成り立たない場合は復号失敗としてアルゴリズムを終了する．

一つの解候補 $\boldsymbol{w}^*_i$ を得るために $m \times \eta$ $(\eta < m)$ の行列に対して，ガウス消去法を適用するものとすると，その計算量は $O(m^3)$ で上から抑えられる．なお，ここでは $\mathbb{F}_q$ の加減乗除が定数時間で実行可能であると仮定している．解候補は n 個あるので，提案アルゴリズムの計算量は $O(nm^3)$ となる．

文献 [8] では，LDPC 符号の疎性を生かした計算量削減手法が提案されている．この手法を用いることで，復号アルゴリズムにおけるガウス消去法の実行回数を 3 割程度減らすことができる．また，あらかじめガウス消去法における前進消去と後退代入の計算を行列として記憶しておくことでガウス消去法の計算処理を削減することもできる．この手法では，$m \times m$ の行列と長さ m の列ベクトルの積を n 回求める計算が必要となる．すなわち，$O(nm^2)$ となる．

4. バースト誤り訂正法の復号特性解析

本章では，前章で説明したバースト誤り訂正アルゴリズムの復号特性について解析を行い，復号誤り率の上界を導出する．

提案バースト誤り訂正法では，部分行列の列ベクトルにより構成される線形空間の重なりが復号性能に影響する．本章では，その点に着目し，復号誤り率の上界を導く．

4.1 復号失敗条件

バースト誤り訂正法の復号誤り率の上界を導出するために，復号失敗条件について考える．そのためにまず，バースト誤り訂正法の復号成功条件を表す定理 1 を示す．

[定理 1] $\eta < \eta_{max}$ とする．$\ell(\boldsymbol{e}) \le \beta_{max}$ を満足する誤りベクトル $\boldsymbol{e}$ について，$\mu(\boldsymbol{e}) = t$ $(t \in [0, n-1])$ とする．$\delta(t, j) > \eta - \beta_{max}$ を満たす任意の $j \in [0, n-1]$ について

$$\boldsymbol{s} \notin \mathrm{span}\left(H^{(\beta_{max})}_t\right) \cap \mathrm{span}\left(H^{(\beta_{max})}_j\right) \tag{10}$$

が成り立つならば，前章で示したバースト誤り訂正アルゴリズムの復号が成功する．また，その逆も成り立つ．

(証明) まず，上記の定理の順命題について証明を行う．$j \in [0, n-1]$ を $\delta(t, j) > \eta - \beta_{max}$ を満たすように任意に選ぶ．順命題の仮定 $\mu(\boldsymbol{e}) = t$ より，$\boldsymbol{s} \in \mathrm{span}\left(H^{(\beta_{max})}_t\right)$ である．もし，$\boldsymbol{s} \in \mathrm{span}\left(H^{(\beta_{max})}_j\right)$ を満たす j が存在するならば

$$\boldsymbol{s} \in \mathrm{span}\left(H^{(\beta_{max})}_t\right) \cap \mathrm{span}\left(H^{(\beta_{max})}_j\right)$$

が成り立つ．しかし，順命題の仮定より上式の成立は否定されている．すなわち，$\boldsymbol{s} \notin \mathrm{span}\left(H_j^{(\beta_{max})}\right)$ である．したがって，$\delta(t,j) > \eta - \beta_{max}$ を満たす任意の $j \in [0, n-1]$ について $\ell(\boldsymbol{w}_j^*) > \beta_{max}$ が常に成り立つ．なお，$\delta(t,j) \leq \eta - \beta_{max}$ を満たす任意の $j \in [0, n-1]$ については，**3.** の補題 1 より，$\boldsymbol{w}_j^* = \boldsymbol{e}$ が成り立つ．すなわち，推定誤りベクトルが $\hat{\boldsymbol{e}} = \boldsymbol{e}$ と一意に定まり復号が成功する．

次に，逆命題について考える．バースト誤り訂正法が復号に成功するとき，解候補 $\boldsymbol{w}_j^*$ $(j \in [0, n-1])$ は

$$\boldsymbol{w}_j^* = \begin{cases} \boldsymbol{e}, & \delta(t,j) \leq \eta - \beta_{max} \\ \epsilon \text{ or } \mathrm{cyc}(\tilde{\boldsymbol{z}}_j \mid 0^{n-\eta}, j), & \delta(t,j) > \eta - \beta_{max} \end{cases}$$

となる．更に，$\delta(t,j) > \eta - \beta_{max}$ を満たす任意の j について

$$\ell(\boldsymbol{w}_j^*) > \beta_{max}$$

が成り立つ．以下では，$\delta(t,j) > \eta - \beta_{max}$ を満たす任意の j について考える．$\boldsymbol{w}_j^* = \epsilon$ となる場合，式 (6) より $\boldsymbol{s} \notin \mathrm{span}\left(H_j^{(\eta)}\right)$ である．$\eta > \beta_{max}$ であるため，$\boldsymbol{s} \notin \mathrm{span}\left(H_j^{(\beta_{max})}\right)$ となる．すなわち，式 (10) が成り立つ．また，$\boldsymbol{w}_j^* = \mathrm{cyc}(\tilde{\boldsymbol{z}}_j \mid 0^{n-\eta}, j)$ となる場合，$\ell(\boldsymbol{w}_j^*) > \beta_{max}$ であるため，$\boldsymbol{s} \notin \mathrm{span}\left(H_j^{(\beta_{max})}\right)$ である．したがって，式 (10) が成り立つ．以上の結果より，バースト誤り訂正法が復号に成功するとき，$\delta(t,j) > \eta - \beta_{max}$ を満たす任意の j について式 (10) が成り立つ． □

定理 1 より，復号失敗条件は次のとおりである．$\mu(\boldsymbol{e}) = t$ $(t \in [0, n-1])$ であるバースト誤りベクトル $\boldsymbol{e}$ について，

$$\boldsymbol{s} \in \mathrm{span}\left(H_t^{(\beta_{max})}\right) \cap \mathrm{span}\left(H_j^{(\beta_{max})}\right)$$

を満たし，$\delta(t,j) > \eta - \beta_{max}$ である $j \in [0, n-1]$ が存在するとき，またそのときに限り，バースト誤り訂正アルゴリズムは復号に失敗する．

4.2 復号誤り率の上界

前節で述べた復号失敗条件から，復号誤り率の導出を行う．まず，バースト誤り訂正アルゴリズムの復号誤り率 P_E は

$$P_E = \sum_{t=0}^{n-1} Pr[\mu(\boldsymbol{e}) = t] Pr[\mathit{failure} \mid \mu(\boldsymbol{e}) = t] \tag{11}$$

と表現することができる．ここで，$Pr[\cdot]$ は $[\cdot]$ 内のイベントが成立する確率を表しており，式 (11) の中の failure は，復号失敗イベントを表している．

次の定理はバースト誤り訂正アルゴリズムの復号誤り率 P_E の上界を与える．以降では，

$$S(i,j) = \mathrm{span}\left(H_i^{(\beta_{max})}\right) \cap \mathrm{span}\left(H_j^{(\beta_{max})}\right)$$

と置く．また，$S(i,j)$ を部分行列 $H_i^{(\beta_{max})}$ と $H_j^{(\beta_{max})}$ の共通部分空間と呼ぶ．

[定理 2] **2.** で仮定されたバースト通信路モデルと **3.** で示された復号アルゴリズムを考える．このとき，復号誤り率 P_E は

$$P_E \leq \frac{1}{n} \sum_{t=0}^{n-1} \sum_{j \in [0,n-1], \delta(t,j) > \eta - \beta_{max}} \frac{|S(t,j)| - 1}{(q-1) q^{\beta_{max}-1}} \tag{12}$$

と上から抑えられる．

（証明） 定理 1 に基づく復号失敗条件から，$Pr[\mathit{failure} \mid \mu(\boldsymbol{e}) = t]$ を評価すると

$$\begin{aligned} & Pr[\mathit{failure} \mid \mu(\boldsymbol{e}) = t] \\ &= Pr\left[\bigcup_{j \in [0,n-1], \delta(t,j) > \eta - \beta_{max}} [H\boldsymbol{e} \in S(t,j)] \,\middle|\, \mu(\boldsymbol{e}) = t \right] \\ &\leq \sum_{j \in [0,n-1], \delta(t,j) > \eta - \beta_{max}} Pr\left[H\boldsymbol{e} \in S(t,j) \mid \mu(\boldsymbol{e}) = t\right] \end{aligned} \tag{13}$$

が成り立つ．不等号はユニオン上界に基づく．以下では $Pr\left[H\boldsymbol{e} \in S(t,j) \mid \mu(\boldsymbol{e}) = t\right]$ を評価する．本論文で仮定するバースト通信路モデルでは，$\mu(\boldsymbol{e}) = t$ とするとき，バースト長 $\ell(\boldsymbol{e})$ 以下のバースト誤り系列が等確率で生起すると仮定している．バーストパターンの総数が $(q-1)q^{\beta_{max}-1}$ であり，それらのバーストパターンに対するシンドロームが全て相異なる（$\eta \leq \eta_{max}$ より）ことから

$$\begin{aligned} & \sum_{j \in [0,n-1], \delta(t,j) > \eta - \beta_{max}} Pr\left[H\boldsymbol{e} \in S(t,j) | \mu(\boldsymbol{e}) = t\right] \\ &\leq \sum_{j \in [0,n-1], \delta(t,j) > \eta - \beta_{max}} \frac{|S(t,j)| - 1}{(q-1) q^{\beta_{max}-1}} \end{aligned} \tag{14}$$

が得られる．式 (14) の右辺は共通部分空間に含まれる零ベクトル以外のベクトルの総数である．式 (14) を

式 (13) に代入し，それを式 (11) に適用することにより，定理 2 が得られる． □

次節に示される，二つの部分行列の共通部分空間の次元計算法を利用することにより，この定理の上界は符号長に対して多項式時間で評価が可能である．

4.3 部分行列対の共通部分空間の次元

定理 2 で示された誤り率の上界を計算するには，二つの部分行列の共通部分空間に含まれる元の個数を求める必要がある．この量は，式 (12) における分子部分に必要とされる．以下では，式 (12) の計算方法について説明する．

まず，各部分行列 $H_i^{(\beta_{max})}, H_j^{(\beta_{max})}$ を

$$H_i^{(\beta_{max})} = (\boldsymbol{a}_0^T, \boldsymbol{a}_1^T, \cdots, \boldsymbol{a}_{\beta_{max}-1}^T) \tag{15}$$

$$H_j^{(\beta_{max})} = (\boldsymbol{b}_0^T, \boldsymbol{b}_1^T, \cdots, \boldsymbol{b}_{\beta_{max}-1}^T) \tag{16}$$

と置く．このとき，二つの部分行列の共通部分空間に含まれる任意の $\boldsymbol{c}^T \in \mathbb{F}_q^m$ に対して

$$\boldsymbol{c}^T = \sum_{k=0}^{\beta_{max}-1} x_k \boldsymbol{a}_k^T = \sum_{k=0}^{\beta_{max}-1} y_k \boldsymbol{b}_k^T, \quad x_k, y_k \in \mathbb{F}_q \tag{17}$$

を満たす x_k, y_k $(k = 0, 1, \cdots, \beta_{max} - 1)$ が存在する．ここで，$\mathbb{F}_q$ の標数を 2 と仮定すると式 (17) より

$$\sum_{k=0}^{\beta_{max}-1} x_k \boldsymbol{a}_k^T + \sum_{k=0}^{\beta_{max}-1} y_k \boldsymbol{b}_k^T = \boldsymbol{0} \tag{18}$$

が成り立つ．すなわち，式 (18) の連立方程式を満たす解の個数が部分行列間の共通部分空間に含まれる元の個数となる．

式 (18) を満たす解の個数は，その連立方程式の自由度により決定される．ここで，$\boldsymbol{x} = (x_0, x_1, \cdots, x_{\beta_{max}-1})$, $\boldsymbol{y} = (y_0, y_1, \cdots, y_{\beta_{max}-1})$ と置くと式 (18) は

$$\left(H_i^{(\beta_{max})} H_j^{(\beta_{max})}\right) (\boldsymbol{x} \mid \boldsymbol{y})^T = \boldsymbol{0} \tag{19}$$

と書き直すことができる．自由度は式 (19) の左辺の連結した行列（連結行列と呼ぶ）のランクにより決定される．

連結行列に行基本操作またはガウス消去法を適用することにより，容易にそのランクを求めることが可能である．連結行列のランクが r の場合，式 (18) の自由度は $2\beta_{max} - r$ となり，解の個数は $q^{(2\beta_{max}-r)}$ となる．すなわち，

$$\left|\mathrm{span}\left(H_i^{(\beta_{max})}\right) \cap \mathrm{span}\left(H_j^{(\beta_{max})}\right)\right| = q^{(2\beta_{max}-r)} \tag{20}$$

となる．

本章で導出した復号誤り率の上界は，与えられた検査行列の部分行列対の連結行列のランクを求めることで計算可能であり，ガウス消去法等の単純な演算により効率的に求めることができる．

5. 計算機実験による提案法の性能評価

本章では，提案バースト誤り訂正法の復号性能を計算機実験により評価する．また，定理 2 の式 (12) の上界の精度や性質についても評価を行う．

5.1 計算機実験の概要

計算機実験に用いた検査行列を表 1 に示す．表 1 に示した検査行列は，Gallager の手法に基づいて構成した正則 LDPC 符号の検査行列である．検査行列の非零要素にはガロア体 $\mathbb{F}_q$ 上の非零元を一様分布に従って割り当てている．また，本章の実験においては，検査行列上の非零要素の位置は符号を定義するガロア体のサイズ q にかかわらず一定である．

5.2 計算機実験の結果

検査行列 H_1 により定義された多元 LDPC 符号について，復号誤り率の上界と符号の復号誤り率の真値を図 2 に示す．ここで真値とは，**2.** で定義したバースト誤りベクトルの条件を満たす全てのバースト誤りを生成し，その全ての誤りに対して復号を行うことで求めた誤り率のことである．復号に用いる部分行列のサイズは $\eta = 8$ とした．図 2 の横軸は通信路で生起する誤りベクトルの最大バースト長 β_{max} を表しており，縦軸は復号誤り率を表している．また，図中のラベル Upper Bound($\mathbb{F}_4$) は符号を定義するガロア体のサイズ $q = 4$ のときの上界を表し，True Value($\mathbb{F}_4$) はガロア体のサイズ $q = 4$ のときの真値を表す．Upper Bound($\mathbb{F}_{16}$) と True Value($\mathbb{F}_{16}$) についても同様である．

表 1 計算機実験に用いる検査行列のパラメータ
Table 1 Parameter of parity check matrix for computation simulation.

検査行列	m	n	列重み	行重み	η
H_1	14	28	2	4	8
H_2	53	105	2	4	41
H_3	26	105	2	4	16

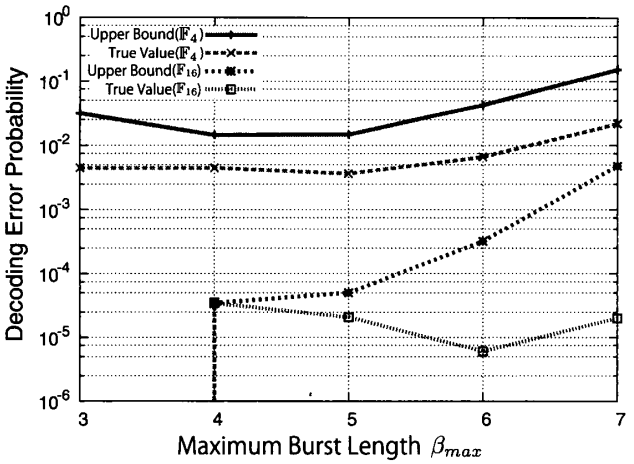


図 2 復号誤り率の真値と上界の関係（$m = 14$, $n = 28$, $\eta = 8$, 検査行列 H_1）

Fig. 2 Relation between true value of decoding error probability and upper bound. ($m = 14$, $n = 28$, $\eta = 8$, parity check matrix H_1)

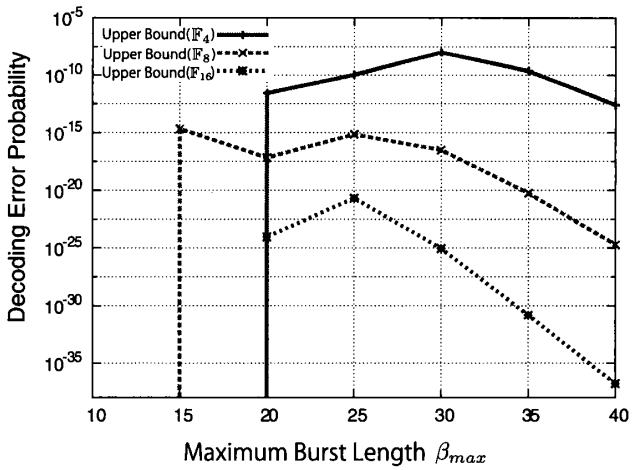


図 3 体のサイズと復号誤り率上界の関係（$m = 53$, $n = 105$, $\eta = 41$, 検査行列 H_2）

Fig. 3 Relation between size of Galois field and upper bound of decoding error probability. ($m = 53$, $n = 105$, $\eta = 41$, parity check matrix H_2)

図 2 より，通信路で発生する最大バースト誤り長 β_{max} が 3 から 7 の範囲において，本論文で導出した上界が，復号誤り率の真値を確かに上から抑えていることが分かる．また，符号 $C(H_1)$ を定義するガロア体が $\mathbb{F}_4$ の場合，復号誤り率上界に対する真値の比は $\beta_{max} = 3$ から $\beta_{max} = 7$ の範囲において，10^{-1} 程度となっている．

また，符号 $C(H_1)$ を定義するガロア体のサイズ $q = 4$ と $q = 16$ を比較した場合，復号誤り率の上界も真値も $q = 16$ のときの方が小さくなっていることが分かる．符号を定義するガロア体 $\mathbb{F}_q$ のサイズ q が大きくなると符号のバースト誤り訂正能力が向上することが確認できる．符号を定義するガロア体のサイズが大きくなると，部分行列が存在する線形空間が広がり，共通部分空間にシンドロームが存在する確率が低くなる．その結果，バースト誤り訂正アルゴリズムの復号失敗条件が満たされる確率が下がり，復号誤り率が低下すると考えられる．

次に，多元 LDPC 符号を定義するガロア体 $\mathbb{F}_q$ のサイズ q の変化による復号誤り率の上界の変化を図 3 に示す．対象とする検査行列は表 1 の H_2 である．復号に用いる部分行列のサイズは $\eta = 41$ とした．

図 3 より，符号 $C(H_2)$ を定義するガロア体 $\mathbb{F}_q$ のサイズ q が大きくなると復号誤り率の上界の値が小さくなることが確認できる．この結果は，図 2 と同様に，ガロア体のサイズと復号誤り率の間でトレードオフの関係があることを示している．

また，表 1 の検査行列 H_3 を用いた場合の復号誤り率の上界を図 4 に示す．復号に用いる部分行列のサイズは $\eta = 16$ とした．

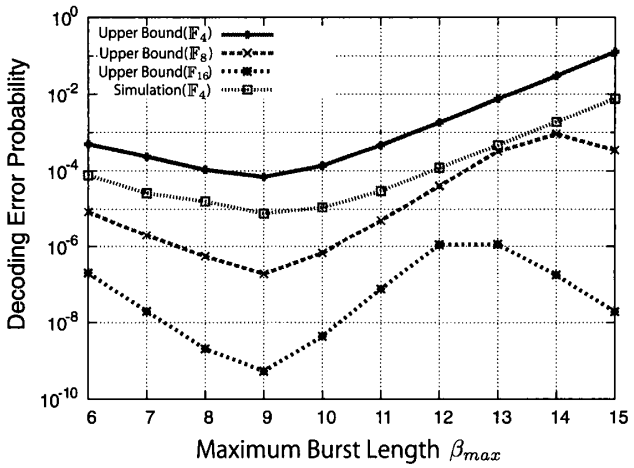


図 4 体のサイズと復号誤り率上界の関係（$m = 26$, $n = 105$, $\eta = 16$, 検査行列 H_3）

Fig. 4 Relation between size of Galois field and upper bound of decoding error probability. ($m = 26$, $n = 105$, $\eta = 16$, parity check matrix H_3)

図 4 より，符号化率が異なる場合においても他の結果と同様に，符号 $C(H_3)$ を定義するガロア体 $\mathbb{F}_q$ のサイズ q が大きくなると復号誤り率の上界の値が小さくなることが確認できる．

また，図 4 の Simulation($\mathbb{F}_4$) は計算機シミュレーションによって求めたバースト誤り訂正アルゴリズムの復号誤り率である．この誤り率は，**2.** の定義を満たすバースト誤りベクトルを一様分布に従い生成し，バースト誤り訂正アルゴリズムにより復号を行うことで求めた．試行回数は 10^7 回である．このように求め

たバースト誤り訂正法の誤り率が，本論文で求めた上界によって上から抑えられていることが確認できる．ガロア体 $\mathbb{F}_4$ 上で定義される符号の復号誤り率上界に対する復号誤り率の比は，$\beta_{max}=6$ から $\beta_{max}=15$ の範囲において 10^{-1} 程度となっている．

6. むすび

本論文では，多元 LDPC 符号に適したバースト誤り訂正アルゴリズムの提案を行った．提案法は，ガウス消去法を複数回実行することにより解候補集合を構成し，その中からバースト仮定を満たす推定誤りベクトルを選択するという考えに基づいた復号アルゴリズムである．また，提案バースト誤り訂正アルゴリズムの復号特性について解析を行い，復号誤り率の上界を導出した．提案した上界は，バースト誤り訂正アルゴリズムに用いる部分行列の共通部分空間に着目し，ペアワイズ復号失敗イベントに対してユニオン上界を考えることで得られた．この上界はガウス消去法等を用いることで効率的に求めることが可能である．なお，本論文で議論されたバースト誤り訂正アルゴリズムとその復号誤り率の上界は多元 LDPC 符号だけでなく，一般の線形符号について適用可能である．

文献 [7] に示される復号手法と誤り率の解析手法も一般の線形符号に適用可能な手法である．ただし，文献 [7] で示された手法は，検査行列に含まれる連続する $m\times m$ 部分行列が全て正則であるという条件に基づいている．この条件は，検査行列が疎な場合には成立しない場合が多く（疎行列により定義される符号の最小距離は m に対して小さく，また最小距離付近の符号語数も多い），LDPC 符号の場合には必ずしも文献 [7] で示された手法が利用できるとは限らないことを注意しておきたい．更に本研究で示された手法は，[8] で論じられているように検査行列の疎性に基づいた高速化が可能な点も，本論文の復号手法・性能解析手法が多元 LDPC 符号に適している点である．

計算機実験の結果，バースト誤り訂正アルゴリズムは符号を定義するガロア体のサイズ q が大きくなるにつれて，ブロック誤り率が低下することが確認できた．また，提案の上界は実際の復号誤り率の振舞いをよく反映していることが確認された．

今後の課題として，部分行列の共通部分空間を考慮した上で，検査行列の列ベクトル置換を行う，検査行列改善アルゴリズムの開発が挙げられる．

文　献

[1] R.G. Gallager, Low-Density Parity-Check Codes, in Research Monograph Series, MIT Press, Cambridge, 1963.

[2] M.C. Davey and D.J.C. Mackay, "Low-density parity check codes over $GF(q)$," IEEE Commun. Lett., vol.2, no.6, pp.165–167, 1998.

[3] G. Hosoya, H. Yagi, T. Matsushima, and S. Hirasawa, "Performance of low-density parity-check codes for burst erasures," Proc. 2006 International Symposium on Information Theory and Its Applications (ISITA2006), pp.491–496, Seoul, Korea, Oct. 2006.

[4] E. Paolini and M. Chiani, "Improved low-density parity-check codes for burst erasure channels," Proc. 2006 IEEE International Conference on Commun. (ICC06), Istanbul, Turkey, June 2006.

[5] T. Wadayama, "Ensemble analysis on minimum span of stopping sets," Proc. Information Theory and Its Applications Workshop, UCSD, Feb. 2006.

[6] M. Yang and W.E. Ryan, "Performance of efficiently encodable LDPC codes in noise bursts on the EPR4 channel," IEEE Trans. Magn., vol.40, no.2, pp.507–512, March 2004.

[7] M.P.C. Fossorier, "Universal burst error correction," International Symposium on Information Theory, ISIT '2006, pp.1969–1973, Seattle, USA, July 2006.

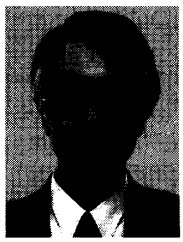
[8] 木全佑輔，和田山正，"多元 LDPC 符号に適したバースト誤り訂正アルゴリズム，" 第 33 回情報理論とその応用シンポジウム，2010.

[9] 木全佑輔，和田山正，"多元 LDPC 符号に適したバースト誤り訂正アルゴリズムに関する復号誤り率の上界，" 第 34 回情報理論とその応用シンポジウム，2011.

（平成 24 年 3 月 23 日受付，11 月 3 日再受付）

木全　佑輔

2010 名工大・工・情報工学卒．2012 同大大学院博士前期課程了．



和田山　正　（正員）

1993 京都工芸繊維大学大学院了．1997 京都工芸繊維大学工博．1995 岡山県立大学情報工学部助手．2004 名古屋工業大学大学院工学研究科助教授．2007 名古屋工業大学大学院工学研究科准教授．2010 名古屋工業大学大学院工学研究科教授．符号理論，情報理論，ディジタル通信方式の研究に従事．IEEE 会員．