

様 式 C-19、F-19-1、Z-19 (共通)

科学研究費助成事業 研究成果報告書



平成 30 年 6 月 29 日現在

機関番号：17201

研究種目：基盤研究(C) (一般)

研究期間：2015～2017

課題番号：15K06071

研究課題名 (和文) シンボルペア符号の設計および復号法に関する研究

研究課題名 (英文) Study on Construction Method and Decoding Algorithm of Symbol-Pair Codes

研究代表者

廣友 雅徳 (HIROTOMO, Masanori)

佐賀大学・工学系研究科・准教授

研究者番号：00529795

交付決定額 (研究期間全体) : (直接経費) 3,800,000 円

研究成果の概要 (和文) : 2010年にシンボルペア符号と呼ばれる新しい誤り訂正符号が提案された。シンボルペア符号では、近年のハードウェア処理の高速化・高機能化に着目し、信号読み取りデバイスによって各信号がペアとして読み出される通信路 (シンボルペア通信路) を考えている。この通信路では、受信ベクトルをペアベクトルとして表現し、誤り訂正のためのメトリックにペア距離を、誤りのモデルとしてペア誤りを用いている。本研究では、ペア誤り訂正能力の高いシンボルペア符号の構成法、および、シンボルペア符号が有する訂正能力を十分に活用できる復号法の開発を行った。

研究成果の概要 (英文) : In 2010, new error correcting codes which are called symbol-pair codes have been proposed. They give a coding framework for channels whose outputs are overlapping pairs of symbols in storage applications. It is called symbol-pair read channel. The pair distance and pair error are used in this channel. In this research, we develop construction methods of symbol-pair codes and evaluate their pair error correcting capability. Furthermore, we develop decoding algorithms of symbol-pair codes.

研究分野：通信・ネットワーク工学

キーワード：誤り訂正符号 シンボルペア符号 シンボルペア通信路 シンドローム復号法 誤りトラップ復号法
代数的復号法 最小ペア距離 ペア誤り訂正能力

1. 研究開始当初の背景

今日の情報通信技術では、スマートフォンの普及によるモバイルブロードバンドサービスの拡大、ソーシャルネットワークサービス、クラウドコンピューティング、動画配信などのインターネットサービスの普及に対応するためにネットワークの高速化が急速に進んでいる。通信品質の保証（誤り率の低減）はサービスの信頼性にかかわるため、高速な通信基盤を構築するにあたり重要な課題になっている。

誤り訂正符号は、送信する側でデータに冗長を付加することによって、通信路で発生した誤りを受信側で訂正可能にする符号化技術である。2010年にシンボルペア符号と呼ばれる新しい誤り訂正符号が提案された。シンボルペア符号では、近年のハードウェア処理の高速化・高機能化に着目し、高速かつ高機能な信号読み取りデバイスによって各信号がペアとして読み出される通信路（シンボルペア通信路）を考えている。この通信路では、受信ベクトルをペアベクトルとして表現し、誤り訂正のためのメトリックにペア距離を、誤りのモデルとしてペア誤りを用いている。このような新しい誤り訂正のモデルによって、シンボルペア符号は、従来のハミング距離をメトリックとする符号（ハミングメトリック符号と呼ぶ）と比較して、次のような利点を持つ。

- ・シンボルペア通信路における誤り訂正の問題に対して、ペアベクトル、ペア距離、ペア誤りという新たな定義を用いることで、符号化／復号フレームワークを数学的に扱える。
- ・ハミングメトリック符号と比較して、誤り訂正能力の高い符号を設計できる。

しかしながら、シンボルペア符号が提案されているものの、符号設計、復号法、能力評価は巡回符号と呼ばれる一部の符号クラスに基づくもののみであり、シンボルペア符号として誤り訂正能力の高い符号の設計方法、また、その誤り訂正能力を引き出す復号法については研究がなされていない。

2. 研究の目的

シンボルペア符号では、高速かつ高機能な信号読み取り処理をモデル化した通信路（シンボルペア通信路）を扱い、その通信路で発生する誤り（ペア誤り）を訂正する符号を設計する。しかしながら、シンボルペア符号として、誤り訂正能力の高い符号の設計方法や、その誤り訂正能力を十分に引き出す復号法について研究がなされていない。本研究では、有限体理論などの性質を活用し、シンボルペア符号の符号設計法と復号法を開発する。

3. 研究の方法

本研究では、シンボルペア符号による信頼性の高い通信を実現することを目的に、次の研究に取り組む。

(1) 誤り訂正能力の高いシンボルペア符号の設計法の開発

ペア距離をメトリックとして高い訂正能力が保障できる符号設計を目指し、有限体理論などの性質を活用したシンボルペア符号の設計法を検討する。

(2) シンボルペア符号の誤り訂正能力を活用可能な復号法の開発

シンボルペア符号に対して、その誤り訂正能力を十分に活用できる復号法を開発する。これまでに提案されている復号法は、巡回符号のハミング距離に基づく復号法を応用したものであり、ペア距離によって保障されるシンボルペア符号の誤り訂正能力を十分活用できない。シンボルペア符号のペア距離による構造的な特徴から復号問題に活用できる関係式を導出し、復号法の構築を目指す。

4. 研究成果

(1) シンボルペア符号のシンδροーム復号法
シンボルペア符号のパリティ検査行列（シンボルペアパリティ検査行列と呼ぶ）と、2種類のシンδροーム（シンボルペアシンδροーム、隣接シンボルシンδροーム）を新たに定義し、それらを用いるシンδροーム復号法を開発した。

$\mathbf{x} = [x_0, x_1, \dots, x_{n-1}]$ を n 次元空間におけるベクトルとする。 $\mathbf{x}$ のシンボルペアベクトルは $\pi(\mathbf{x})$

$= [(x_0, x_1), (x_1, x_2), \dots, (x_{n-2}, x_{n-1}), (x_{n-1}, x_0),]$ と定義される。 $\mathbf{x}$ の読み取り結果であるペアベクトルを

$\tilde{\mathbf{u}} = [(u_{L,0}, u_{R,0}), (u_{L,1}, u_{R,1}), \dots, (u_{L,n-1}, u_{R,n-1})]$ とする。元の符号のパリティ検査行列 $\mathbf{H}$ の各行をペアベクトルに変換した行列

$$\pi(\mathbf{H}) = \begin{bmatrix} \pi(h_0) \\ \pi(h_1) \\ \vdots \\ \pi(h_{n-k-1}) \end{bmatrix}$$

がシンボルペアパリティ検査行列である。シンボルペアシンδροームを次式で定義する。

$$\tilde{\mathbf{s}}^{(p)} = \tilde{\mathbf{u}} \cdot \pi(\mathbf{H})^T$$

また、隣接シンボルシンδροームを次式で定義する。

$$\mathbf{s}^{(n)} = [s_0^{(n)}, s_1^{(n)}, \dots, s_{n-1}^{(n)}]$$

$$s_i^{(n)} = \begin{cases} 0 & u_{L,i} = u_{R,i-1} \text{ のとき} \\ 1 & u_{L,i} \neq u_{R,i-1} \text{ のとき} \end{cases}$$

このとき、次の定理が成り立つ。

[定理 1] シンボルペア符号において、シンδροーム（シンボルペアシンδροームと隣接シンボルシンδροーム）と訂正能力の範囲内の誤りパターンは一对一対応する。

この定理より次の復号法が得られる。

表 1: (3,2)符号のシンボルペア符号の標準配列

シンボルペア シンδροーム $\mathbf{s}^{(p)}$	隣接シンボル シンδροーム $\mathbf{s}^{(n)}$	コセット			
		誤りパターン コセットリーダー $\mathbf{e}$			
[(0,0)]	[000]	[(0,0),(0,0),(0,0)]	[(0,1),(1,1),(1,0)]	[(1,0),(0,1)(1,1)]	[(1,1),(1,1),(1,1)]
[(1,0)]	[100]	[(1,0),(0,0),(0,0)]	[(1,1),(1,1),(1,0)]	[(0,0),(0,1)(1,1)]	[(0,1),(1,1),(1,1)]
[(0,1)]	[010]	[(0,1),(0,0),(0,0)]	[(0,0),(1,1),(1,0)]	[(1,1),(0,1)(1,1)]	[(1,0),(1,1),(1,1)]
[(1,1)]	[110]	[(1,1),(0,0),(0,0)]	[(1,0),(1,1),(1,0)]	[(0,1),(0,1)(1,1)]	[(0,0),(1,1),(1,1)]
[(1,0)]	[010]	[(0,0),(1,0),(0,0)]	[(0,1),(0,1),(1,0)]	[(1,0),(1,1)(1,1)]	[(1,1),(0,1),(1,1)]
[(0,1)]	[001]	[(0,0),(0,1),(0,0)]	[(0,1),(1,0),(1,0)]	[(1,0),(0,0)(1,1)]	[(1,1),(1,0),(1,1)]
[(1,1)]	[011]	[(0,0),(1,1),(0,0)]	[(0,1),(0,0),(1,0)]	[(1,0),(1,0)(1,1)]	[(1,1),(0,0),(1,1)]
[(1,0)]	[001]	[(0,0),(0,0),(1,0)]	[(0,1),(1,1),(0,0)]	[(1,0),(0,1)(0,1)]	[(1,1),(1,1),(0,1)]
[(0,1)]	[100]	[(0,0),(0,0),(0,1)]	[(0,1),(1,1),(1,1)]	[(1,0),(0,1)(1,0)]	[(1,1),(1,1),(1,0)]
[(1,1)]	[101]	[(0,0),(0,0),(1,1)]	[(0,1),(1,1),(0,1)]	[(1,0),(0,1)(0,0)]	[(1,1),(1,1),(0,0)]

[シンボルペア符号のシンδροーム復号法]
復号器はシンδροーム $\mathbf{s}^{(p)}$, $\mathbf{s}^{(n)}$ と誤りパターン $\mathbf{e}$ の対応表を持っている。

Step1. 受信した $\mathbf{u}$ からシンδροーム $\mathbf{s}^{(p)}$, $\mathbf{s}^{(n)}$ を計算する。

Step2. 対応表を参照することで、シンδροーム $\mathbf{s}^{(p)}$, $\mathbf{s}^{(n)}$ から誤りパターン $\mathbf{e}$ を推定する。

Step3. 推定した誤りパターンと受信したペアベクトルの排他的論理和を取ることでペア誤りを訂正する。

$$\mathbf{w} = \mathbf{u} \oplus \mathbf{e}$$

Step4. ペア誤りを取り除かれたペアベクトル $\mathbf{w}$ を n 次元ベクトルに戻す。

$$\mathbf{w} = [w_{L,0}, w_{L,1}, \dots, w_{L,n-1}]$$

(3, 2) 符号のシンボルペア符号について考える。この符号は最小ペア距離 3 の単一ペア誤り訂正符号である。シンボルペアパリティ検査行列は

$$\pi(\mathbf{H}) = [(1,1), (1,1), (1,1)]$$

である。このとき、標準配列は表 1 のようになる。復号器は表 1 のような誤りパターン(コセットリーダー)とシンδροームの対応表を用い、シンδροームから誤りパターンを推定する。

(2) シンボルペア通信路上の巡回符号の復号法

ペア誤りのパターンと巡回符号の復号法で訂正可能な誤りの関係を利用し、効率的にペア誤りを訂正する復号法を開発した。従来のシンボルペア符号の復号法では、最小ペア距離の半分以下のペア誤りにもかかわらず、訂正不可能な場合が存在する。提案復号法では、距離の比較にペア距離を活用することで、巡回符号の復号器を用いて得られた誤りベクトルの推定失敗、成功を判断する。これにより従来法では訂正できないペア誤りを訂正可能にしている。

受信したペアベクトルを $\mathbf{u} =$

$[(u_{L,0}, u_{R,0}), (u_{L,1}, u_{R,1}), \dots, (u_{L,n-1}, u_{R,n-1})]$ とし、次のベクトルを定義する。

$$\mathbf{u}_L = [u_{L,0}, u_{L,1}, \dots, u_{L,n-1}]$$

$$\mathbf{u}_R = [u_{R,0}, u_{R,1}, \dots, u_{R,n-1}]$$

$$\mathbf{u}_S = [u_{L,0} \oplus u_{R,0}, \dots, u_{L,n-1} \oplus u_{R,n-1}]$$

ペア誤りベクトルと、その左シンボルと右シンボルを次のように表す。

$$\mathbf{e} = [(e_{L,0}, e_{R,0}), (e_{L,1}, e_{R,1}), \dots, (e_{L,n-1}, e_{R,n-1})]$$

$$= (\mathbf{e}_L, \mathbf{e}_R)$$

$$\mathbf{e}_L = [e_{L,0}, e_{L,1}, \dots, e_{L,n-1}]$$

$$\mathbf{e}_R = [e_{R,0}, e_{R,1}, \dots, e_{R,n-1}]$$

[シンボルペア通信路上の巡回符号の復号法]

Step1. 隣接シンボルシンδροーム $\mathbf{s}^{(n)}$ を計算する。

Step2. $\mathbf{u}_L$ に対して巡回符号の復号器 D_C を用いて左シンボルの誤りベクトル $\mathbf{e}_L$ を求める。

$$\mathbf{c}_L := D_C(\mathbf{u}_L)$$

$\mathbf{c}_L$ が復号不可能な場合 Step3 へ進む。そうでない場合は $\mathbf{e}_L := \mathbf{c}_L \oplus \mathbf{u}_L$ とし、 $\mathbf{e}_L$ と $\mathbf{s}^{(n)}$ から右シンボルの誤りベクトル $\mathbf{e}_R$ を求める。

$$\mathbf{e}_R := (\mathbf{e}_L \oplus \mathbf{s}^{(n)}) \ll 1$$

$\mathbf{e} = (\mathbf{e}_L, \mathbf{e}_R)$ のペア重みが訂正能力範囲ならば $\mathbf{c}_L$ を復号結果として出力しアルゴリズムを終了する。そうでなければ Step3 へ進む。

Step3. $\mathbf{u}_R$ に対して D_C を用いて左シンボルの誤りベクトル $\mathbf{e}_R$ を求める。

$$\mathbf{c}_R := D_C(\mathbf{u}_R)$$

$\mathbf{c}_R$ が復号不可能な場合 Step4 へ進む。そうでない場合は $\mathbf{e}_R := \mathbf{c}_R \oplus \mathbf{u}_R$ とし、 $\mathbf{e}_R$ と $\mathbf{s}^{(n)}$ から右シンボルの誤りベクトル $\mathbf{e}_L$ を求める。

$$\mathbf{e}_L := (\mathbf{e}_R \gg 1) \oplus \mathbf{s}^{(n)}$$

$\mathbf{e} = (\mathbf{e}_L, \mathbf{e}_R)$ のペア重みが訂正能力範囲な

表 2: 2 元 (n, k) BCH 符号から得られるシンボルペア符号のペア誤り訂正能力 t_p と従来法の訂正能力 t_0 , 提案復号法の訂正能力 t'_p

(n, k)	d_H	d_p	t_H	t_p	t_0	t'_p
(31, 21)	5	9	2	4	3	4
(127, 64)	21	34	10	16	15	16
(127, 85)	13	22	6	10	9	10
(127, 99)	9	15	4	7	6	7
(255, 223)	9	15	4	7	6	7

らば $\mathbf{c}_R \gg 1$ を復号結果として出力しアルゴリズムを終了する. そうでなければ Step4 へ進む.

Step4. $\mathbf{u}_S$ に対して D_C を用いて訂正を行う.

$$\mathbf{c}' := D_C(\mathbf{u}_S)$$

$\mathbf{c}'$ が復号不可能な場合は復号失敗になる. そうでない場合は

$$\tilde{c}_i = \sum_{j=0}^{i-1} c'_j$$

$$\mathbf{c} = \begin{cases} \tilde{\mathbf{c}} & d_h(\mathbf{u}_L, \tilde{\mathbf{c}}) < d_h(\mathbf{u}_L, \tilde{\mathbf{c}} + \mathbf{1}) \text{ のとき} \\ \tilde{\mathbf{c}} + \mathbf{1} & \text{その他のとき} \end{cases}$$

より, $\mathbf{c}'$ から $\mathbf{c}$ を求め, 復号結果として出力する.

提案復号法と従来法の誤り訂正能力の比較を表 2 に示す. 表 2 では, (n, k) 巡回符号は最小ペア距離 d_p の半分のペア誤り $t_p = \lfloor (d_p - 1)/2 \rfloor$ 個を訂正できる能力を持つ. 従来法はその全てのペア誤りを訂正できないのに対し, 提案復号法では全てのペア誤りを訂正できる.

(3) シンボルペア通信路上の巡回符号の誤りトラップ復号法

シンボルペア通信路上の巡回符号の誤りトラップ復号法を開発した. さらに, その復号法の回路実装として誤りトラップ復号回路を構成した.

受信したペアベクトル $\tilde{\mathbf{u}} = [(u_{L,0}, u_{R,0}), (u_{L,1}, u_{R,1}), \dots, (u_{L,n-1}, u_{R,n-1})]$ を次の多項式で表す.

$$\tilde{\mathbf{u}}(x) = \tilde{\mathbf{u}}_0 + \tilde{\mathbf{u}}_1 x + \dots + \tilde{\mathbf{u}}_{n-1} x^{n-1}$$

$$\mathbf{u}_L(x) = u_{L,0} + u_{L,1} x + \dots + u_{L,n-1} x^{n-1}$$

$$\mathbf{u}_R(x) = u_{R,0} + u_{R,1} x + \dots + u_{R,n-1} x^{n-1}$$

また, ペア誤り $\tilde{\mathbf{e}} = [(e_{L,0}, e_{R,0}), (e_{L,1}, e_{R,1}), \dots, (e_{L,n-1}, e_{R,n-1})]$ を次の多項式で表す.

$$\tilde{\mathbf{e}}(x) = \tilde{\mathbf{e}}_0 + \tilde{\mathbf{e}}_1 x + \dots + \tilde{\mathbf{e}}_{n-1} x^{n-1}$$

$$\mathbf{e}_L(x) = e_{L,0} + e_{L,1} x + \dots + e_{L,n-1} x^{n-1}$$

$$\mathbf{e}_R(x) = e_{R,0} + e_{R,1} x + \dots + e_{R,n-1} x^{n-1}$$

$\mathbf{u}_L(x)$ と $\mathbf{u}_R(x)$ を巡回符号の生成多項式 $g(x)$ で割った余りをシンボルペアシンδροーム多項

式 $\tilde{\mathbf{s}}(x) = (s_L(x), s_R(x))$ とする.

$$s_L(x) = u_L(x) \bmod g(x)$$

$$s_R(x) = u_R(x) \bmod g(x)$$

連続する $n - k$ ペアにペア誤りが限定される場合, ペア誤り多項式は次のように表される.

$$\tilde{\mathbf{e}}(x) = \tilde{\mathbf{e}}_i x^i + \tilde{\mathbf{e}}_{i+1} x^{i+1} + \dots + \tilde{\mathbf{e}}_{n-k+i-1} x^{n-k+i-1}$$

$$\mathbf{e}_L(x) = e_{L,i} x^i + e_{L,i+1} x^{i+1} + \dots$$

$$+ e_{L,n-k+i-1} x^{n-k+i-1}$$

$$\mathbf{e}_R(x) = e_{R,i} x^i + e_{R,i+1} x^{i+1} + \dots$$

$$+ e_{R,n-k+i-1} x^{n-k+i-1}$$

このペア誤りを右に $n - i$ 回巡回シフトを次のように表す.

$$\tilde{\mathbf{e}}^{(n-i)}(x) = \tilde{\mathbf{e}}_i + \tilde{\mathbf{e}}_{i+1} x + \dots + \tilde{\mathbf{e}}_{n-k+i-1} x^{n-k-1}$$

$$\mathbf{e}_L^{(n-i)}(x) = e_{L,i} + e_{L,i+1} x + \dots$$

$$+ e_{L,n-k+i-1} x^{n-k-1}$$

$$\mathbf{e}_R^{(n-i)}(x) = e_{R,i} + e_{R,i+1} x + \dots$$

$$+ e_{R,n-k+i-1} x^{n-k-1}$$

このとき, ペア誤りは受信ペアベクトルを右に $n - i$ 回巡回シフトした多項式 $\tilde{\mathbf{u}}^{(n-i)}(x)$ の下位 $n - k$ ビットに限定される. つまり, シンボルペアシンδροーム多項式 $\tilde{\mathbf{s}}^{(n-i)}(x) = (s_L^{(n-i)}(x), s_R^{(n-i)}(x))$ は次のようになる.

$$s_L^{(n-i)}(x) = u_L^{(n-i)}(x) \bmod g(x) = e_L^{(n-i)}(x)$$

$$s_R^{(n-i)}(x) = u_R^{(n-i)}(x) \bmod g(x) = e_R^{(n-i)}(x)$$

したがって, $\tilde{\mathbf{e}}^{(n-i)}(x) = (e_L^{(n-i)}(x), e_R^{(n-i)}(x)) = (s_L^{(n-i)}(x), s_R^{(n-i)}(x))$ が成り立つ. つまり, $\tilde{\mathbf{e}}(x) = x^i \cdot \tilde{\mathbf{s}}^{(n-i)}(x)$ となる.

この関係から次の定理が得られる.

[定理 2] 最小ペア距離 d_p のシンボルペア符号において, もし受信多項式 $\tilde{\mathbf{u}}(x)$ に生じているペア誤りが $t_p = \lfloor (d_p - 1)/2 \rfloor$ 個以下, かつその誤りが連続する $n - k$ ペアの範囲にあるならば, その誤りは次の条件を満たすときに限り, シンボルペアシンδροームとして現れる.

条件 1. シンボルペアシンδροームのペア重みが t_p 以下である.

条件 2. 受信多項式の隣接シンボルシンδροームとシンボルペアシンδροームの隣接シンボルシンδροームが一致する.

定理 2 に基づき, シンボルペア通信路上の誤りトラップ復号法が与えられる.

[シンボルペア通信路上の誤りトラップ復号法]

入力: 受信多項式 $\tilde{\mathbf{u}}(x) = (u_L(x), u_R(x))$

出力: 符号多項式 $\mathbf{c}(x)$ または復号失敗シンボル F

Step1. シンボルペアシンδροーム多項式 $\tilde{\mathbf{s}}(x) = (s_L(x), s_R(x))$, 隣接シンボルシン

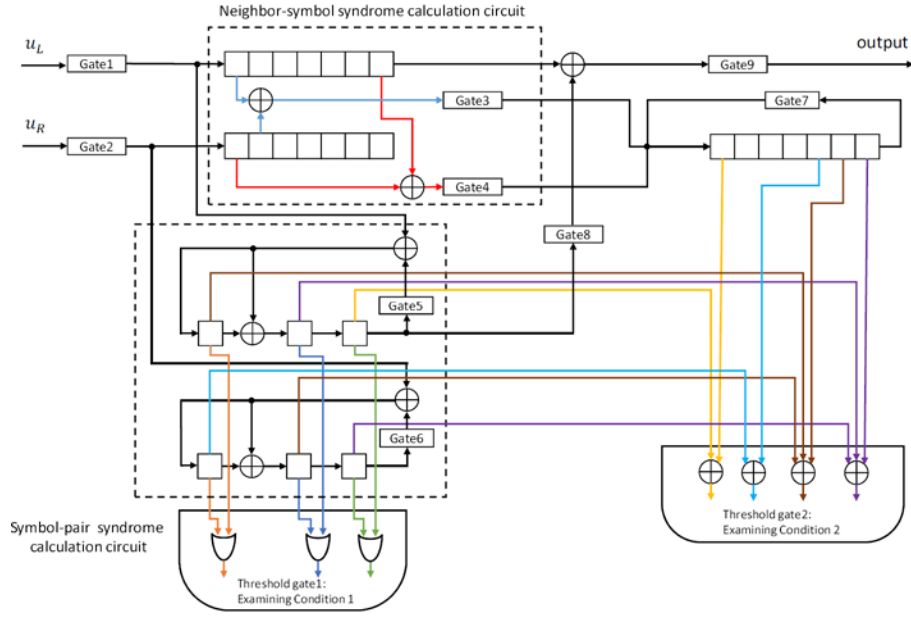


図 1: シンボルペア通信路上の(7,3)巡回ハミング符号の誤りトラップ復号器

ドローム多項式 $S(x)$ を計算する.

$$s_L(x) = u_L(x) \bmod g(x)$$

$$s_R(x) = u_R(x) \bmod g(x)$$

$$S(x) = u_L(x) + (x \cdot u_R(x) \bmod x^n - 1)$$

Step2. シンボルペアシンドローム多項式が条件 1, 条件 2 を満たすか調べる. 条件 1 と条件 2 を両方満たすならば Step5 へ進む. そうでなければ, $j = 0$ として Step3 へ進む.

Step3. $j < n$ ならば, 受信多項式を右に 1 回巡回シフトし, シンボルペアシンドローム多項式 $\tilde{s}^{(j+1)}(x) = (s_L^{(j+1)}(x), s_R^{(j+1)}(x))$ と隣接シンボルシンドローム多項式 $S^{(j+1)}(x)$ を求める.

$$\tilde{u}^{(j+1)}(x) = x \cdot \tilde{u}^{(j)}(x)$$

$$s_L^{(j+1)}(x) = u_L^{(j+1)}(x) \bmod g(x)$$

$$s_R^{(j+1)}(x) = u_R^{(j+1)}(x) \bmod g(x)$$

$$S^{(j+1)}(x) = u_L^{(j+1)}(x) + (x \cdot u_R^{(j+1)}(x) \bmod x^n - 1)$$

ただし, $j = 0$ のとき $\tilde{u}^{(0)}(x) = \tilde{u}(x)$ とする. $j = n$ ならば復号失敗シンボル F を出力し, アルゴリズムを終了する.

Step4. シンボルシンドローム多項式 $\tilde{s}^{(j+1)}(x)$ が条件 1, 条件 2 を満たすか調べる. 条件 1 と条件 2 の両方を満たすならば Step5 へ進む. そうでなければ $j = j + 1$ として Step3 へ戻る.

Step5. シンボルシンドローム多項式 $\tilde{s}^{(j)}(x)$ を用いて誤りを訂正し $\pi(c)(x)$ を求め, $c(x)$ を出力し, アルゴリズムを終了する.

$$\pi(c)(x) = \tilde{u}(x) + x^{n-j} \cdot \tilde{s}^{(j)}(x)$$

誤りトラップ復号法を実現する回路を図に

示す. 図はシンボルペア通信路における (7, 4) 巡回ハミング符号の誤りトラップ復号器である.

(4) シンボルペア通信路上における代数的復号法

シンボルペア通信路上で生じたペア誤りを代数的解法によって解く復号問題について検討した. ペア誤りが生じている位置を表す誤り位置多項式と, 受信したペアベクトルの矛盾する位置を表す矛盾位置多項式を新たに定義した. 2 ペア誤り訂正可能な 2 元 BCH 符号, および, 3 ペア誤り訂正可能な 2 元 BCH 符号に対して, シンドローム多項式と誤り位置多項式, 矛盾位置多項式の関係式を導出し, その関係式を解く代数的復号法を開発した.

(5) 巡回符号の最小ペア距離の評価

巡回符号から設計されるシンボルペア符号のペア誤り訂正能力を評価することを目的として, 巡回符号の最小ペア距離を高速に計算するアルゴリズムを開発した. そして, 代数的構成法によって設計される 2 元 BCH 符号の最小ペア距離を求め, 最小ペア距離の下界との比較を行った. その結果を表 3 に示す.

5. 主な発表論文等

[雑誌論文] (計 7 件)

- ① M. Takita, M. Hirotomo, and M. Morii, "Error-Trapping Decoding for Cyclic Codes over Symbol-Pair Read Channels," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E100-A, no.12, pp.2578-2584, Dec. 2017. (査読有)
- ② M. Takita, M. Hirotomo, and M. Morii, "Algebraic Decoding of BCH Codes over

表 3: 2 元 (n, k) BCH 符号 (最小ハミング距離 d_H) から構成されるシンボルペア符号のおよび最小ペア距離 d_p と下界との比較

(n, k)	Minimum distance d_H	Minimum pair distance d_p	Lower bound on d_p		
			Thm. 3 [2]	Thm. 4 [2]	Thm. 5 [4]
(7,4)	3	5	5	—	5
(15,5)	7	11	9	10	11
(15,7)	5	8	7	—	8
(15,11)	3	5	5	—	5
(31,6)	15	23	17	18	23
(31,11)	11	17	13	14	17
(31,16)	7	11	9	—	11
(31,21)	5	9	7	—	8
(31,26)	3	5	5	—	5
(63,7)	31	47	33	34	47
(63,10)	27	41	29	30	41
(63,16)	23	35	25	26	35
(63,18)	21	32	23	24	32
(63,24)	15	23	17	18	23
(63,30)	13	20	15	—	20
(63,36)	11	17	13	—	17
(63,39)	9	14	11	—	14
(63,45)	7	11	9	—	11
(63,51)	5	8	7	—	8
(63,57)	3	5	5	—	5
(127,8)	63	95	65	66	95
(127,15)	55	83	57	58	83
(127,22)	47	71	49	50	71
(127,29)	43	65	45	46	65
(127,36)	31	47	33	34	47
(127,43)	31	47	33	34	47
(127,50)	27	43	29	30	41
(127,57)	23	37	25	—	35
(127,64)	21	34	23	—	32
(127,71)	19	30	21	—	29
(127,78)	15	23	17	—	23
(127,85)	13	22	15	—	20
(127,92)	11	18	13	—	17
(127,99)	9	15	11	—	14
(127,106)	7	11	9	—	11
(127,113)	5	8	7	—	8
(127,120)	3	5	5	—	5

Symbol-Pair Read Channels: Cases of Two-Pair Error and Three-Pair Error Correction," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E99-A, no.12, pp.2179-2191, Dec. 2016. (査読有)

- ③ M. Takita, M. Hirotomo, and M. Morii, "Error-Trapping Decoding for Cyclic Codes over Symbol-Pair Read Channels," Proc. 2016 International Symposium on Information Theory and its Applications (ISITA2016), pp.717-721, Monterey, California, USA, Nov. 2016. (査読有)
- ④ M. Hirotomo, H. Tamiya, and M. Morii, "Error Correction Capability of Irregular LDPC Codes under the Gallager A Algorithm," Proc. 2016 International Symposium on Information Theory and its Applications (ISITA2016), pp.617-621, Monterey, California, USA, Nov. 2016. (査読有)
- ⑤ K. Kasai, M. Hirotomo, and M. Morii "LDPC Codes and Iterative Decoding over Symbol-Tuple Error Channels," Proc. 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC 2016), pp.276-279, Brest, France, Sept. 2016. (査読有)

- ⑥ M. Takita, M. Hirotomo, and M. Morii, "A Decoding Algorithm for Cyclic Codes over Symbol-Pair Read Channels," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E98-A, no.12, pp.2415-2422, Dec. 2015. (査読有)
- ⑦ M. Takita, M. Hirotomo, and M. Morii, "Syndrome Decoding of Symbol-Pair Codes," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E98-A, no.12, pp.2423-2428, Dec. 2015. (査読有)

〔学会発表〕(計 4 件)

- ① 笠井健太, 廣友雅徳, 森井昌克, "シンボルタプル誤り通信路の入出力相互情報量に接近する空間結合符号," 第 39 回情報理論とその応用シンポジウム (SITA2016), 2016 年 12 月, 岐阜県.
- ② 瀧田慎, 廣友雅徳, 森井昌克, "シンボルペア通信路における代数的符号の復号問題について (II)," 第 38 回情報理論とその応用シンポジウム (SITA2015), 2015 年 11 月, 岡山県.
- ③ 笠井健太, 廣友雅徳, 森井昌克, "シンボルタプル誤り通信路の LDPC 符号による符号化," 第 38 回情報理論とその応用シンポジウム (SITA2015), 2015 年 11 月, 岡山県.
- ④ 瀧田慎, 廣友雅徳, 森井昌克, "シンボルペア符号の復号問題と代数的解法について," 電子情報通信学会情報理論研究会, 2015 年 9 月. 石川県

〔図書〕(計 0 件)

〔産業財産権〕

- 出願状況 (計 0 件)
- 取得状況 (計 0 件)

〔その他〕

なし

6. 研究組織

(1) 研究代表者

廣友 雅徳 (HIROTOMO, Masanori)
佐賀大学・大学院工学系研究科・准教授
研究者番号：00529795

(2) 研究分担者

なし

(3) 連携研究者

なし

(4) 研究協力者

なし