様式 C-19

科学研究費補助金研究成果報告書

平成 23 年 5 月 27 日現在

機関番号：１６１０１
研究種目：若手研究(B)
研究期間：2009～2010
課題番号：21760295
研究課題名(和文)LT 符号を用いたシリアル連接符号化方式とその逐次型復号法に関する研究
研究課題名(英文)On a serial concatenated code using an LT code and its iterative decoding algorithm
研究代表者
得重　仁（TOKUSHIGE HITOSHI）
徳島大学・大学院ソシオテクノサイエンス研究部・講師
研究者番号：50336921

研究成果の概要（和文）：LT 符号は，符号長，情報シンボル数を任意に変更なレートレス符号であり，消失通信路に対してメッセージパッシング復号法を用いることで比較的少ない計算量で非常に良い性能を持つことが知られている．しかしながら，雑音通信路に対する耐性は非常に小さい．そこで，雑音通信路に対し，外部符号に LT 符号，内部符号に誤り訂正符号を用いる連接符号と内部復号に逐次型限界距離復号法を，外部復号に内部復号結果とその信頼度を用いるメッセージパッシング復号法を用いる連接復号法の提案を行った.提案連接符号化方式が，従来型連接符号化方式よりも優れた誤り制御特性を持つことを計算機模擬により示した.

研究成果の概要(英文)：LT codes are rate less codes whose code length and dimension can be arbitrarily chosen. It has been shown that they provide considerably better performance by using a message-passing decoding. However, they are not able to achieve good error performance for a noisy channel. Then we propose a concatenated code using outer LT and inner conventional error correcting codes, and its decoding algorithm in which an iterative bounded-distance decoding and soft-decision LT decoding are performed to the inner and outer codes, respectively. The simulation results have shown that the proposed scheme is more effective than a conventional concatenated coding scheme.

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	1,100,000	330,000	1,430,000
年度			
年度			
年度			
総　計	2,100,000	630,000	2,730,000

研究分野：通信・ネットワーク工学
科研費の分科・細目：情報理論
キーワード：LT 符号，レートレス符号，逐次型復号，限界距離復号，連接符号

1　研究開始当初の背景

GF(2^m) 上の Reed-Solomon(RS) 符号は，実用上非常に有用であり，その符号長 N は $N = 2^m - 1$ で与えられ，情報シンボル数を K とすると，訂正能力を決定する最小距離は $d_{\min} = N - K + 1$ により与えられる．したがって，すべての符号パラメータは，m と K により決定され，$1 \leq K < N = 2^m - 1$ の制約があり，パラメータの選択の自由度は然程，大きくない．RS 符号は，硬判定復号法の一つであり復号複雑度の小さい代数的復号法を用いることにより $s + 2t + 1 = d_{\min}$ を満たす s 個の消失と t 個までの誤りを訂正できる．また，通信路より得られた信頼度情報を入力として，代数的復号法を複数回用いることにより誤り制御特性の改善を目指した一般化最小距離 (GMD) 復号法や Chase-GMD(CG) 復号法等が提案されている．しかしながら，m の増大に伴い，代数的復号法の復号複雑度が増大することより，比較的 m の小さい RS 符号に対してのみへの適用が現実的である．ブロック誤り率を最適とする最尤復号法，ビット誤り率を最適とする最大事後確率復号法は，GMD 復号法や CG 復号法よりも尚更に適用が困難である．

RS 符号は雑音・消失通信路に対して用いることが可能であるが，消失通信路に対して，RS 符号に代わる符号として Luby Transform(LT) 符号が注目を集めている．LT 符号はレートレス符号であり，符号長 N と情報シンボル数 K を $N > K$ の下で任意に設定することが可能である．各符号化シンボルは，与えられた次数分布で発生した次数個分の異なる情報シンボルの排他的論理和により与えられることにより，情報シンボル長の選択も任意に設定できる．復号に於いては，約 $1.05 \times K$ 個の受信シンボルよりメッセージパッシング復号法により比較的少ない復号複雑度で復号が可能である．しかしながら，符号の性質上，雑音通信路への耐性は非常に低い．

2　研究の目的

LT 符号の利点を生かしつつ，雑音・消失通信路に対する耐性を高める為に，LT 符号と従来型誤り訂正符号を用いた連接符号とその復号法の開発を行う．RS 符号では実現が困難であったパラメータに於ける提案連接符号化方式が，比較的少ない復号複雑度で優れた誤り制御特性を持つことを示すのが目的である．

提案連接符号では，情報シンボルに対して LT 外部符号化を行い，外部符号化シンボルを生成する．そして，得られた外部符号化シンボルそれぞれに対して誤り訂正内部符号化を行い，内部符号化シンボルを生成する．その内部符号化シンボルが，通信路へと送られる．復号では，通信路より得られた各受信シンボルに対し，内部復号法を行い，内部復号結果として内部復号シンボルとその信頼度を出力する．それらの得られた内部復号結果を入力とする軟判定 LT 外部復号法が行われ，推定情報シンボルが出力される．前出の目的の為に，

- ある程度の正復号率と誤復号率が非常に小さくなる様な Chase-like 内部復号法とその復号結果の信頼度の算出方法，
- 内部復号の信頼度を用いた LT 外部復号法

の開発をそれぞれ行い，最後に，両方法を組み合わせた提案連接符号化方式の計算機模擬による評価を行い，有効性を示す．

3　研究の方法

(1) 定義：$\mathcal{N}$ と $\mathcal{R}$ をそれぞれ正整数と実数の集合として定義する．p と $q \in \mathcal{N}$ に対して，V_p と V_p^q を次元 p の 2 元ベクトル集合と次元 q の V_p 上のベクトル集合とする．同様に $\mathcal{R}_p$ と $\mathcal{R}_p^q$ を次元 p の実ベクトル集合と次元 q の $\mathcal{R}_p$ 上のベクトル集合とする．$\boldsymbol{v} = (\boldsymbol{v}^{(1)}, \boldsymbol{v}^{(2)}, \ldots, \boldsymbol{v}^{(q)}) \in V_p^q$，$\boldsymbol{v}^{(q')} = (v_1^{(q')}, v_2^{(q')}, \ldots, v_p^{(q')}) \in V_p$，$v_{p'}^{(q')} \in \mathrm{GF}(2)$ (ここで，$1 \leq p' (\in \mathcal{N}) \leq p$，$1 \leq q' (\in \mathcal{N}) \leq q$) に対して，$\boldsymbol{v}$，$\boldsymbol{v}^{(q')}$，$v_{p'}^{(q')}$ を系列，$\boldsymbol{v}$ の q' 番目のシンボル，$\boldsymbol{v}^{(q')}$ の

p' 番目の要素と呼ぶ．同様に，$\boldsymbol{s} \in \mathcal{R}_p^q$, $\boldsymbol{s}^{(q')} \in \mathcal{R}_p$, $\boldsymbol{s}_{p'}^{(q')} \in \mathcal{R}$ も呼ぶ．V_m 上の符号長 N，情報シンボル数 K の LT(N, K) 符号を考える．$1 \leq n(\in \mathcal{N}) \leq N$ に対して，各符号化シンボル $\boldsymbol{c}^{(n)} \in V_m$ は次の様に与えられる．

1. $\boldsymbol{c}^{(n)}$ の次数 d_n が，与えられた次数分布に基づきランダムに選択され，
2. ランダムに選択された d_n 個の異なるメッセージシンボルの和が $\boldsymbol{c}^{(n)}$ となる．

符号化シンボルとメッセージシンボルを接続するグラフが，各符号化手順毎に定義され，復号に用いられる．復号手順は次の様になる．

1. 次数 1 の入力シンボル $\boldsymbol{i} \in V_m$ がグラフに存在するならば，
   (a) $\boldsymbol{i}$ が接続している推定メッセージシンボル $\boldsymbol{e}$ に $\boldsymbol{i}$ を代入し，
   (b) $\boldsymbol{e}$ に接続しているすべての入力シンボルに加える．そして，
   (c) $\boldsymbol{e}$ に接続しているすべての枝をグラフから削除する．
   そうでなければ，復号を終了する．
2. ステップ 1 は，すべての推定メッセージシンボルが決定するまで繰り返される．

Ideal soliton 分布と Robust soliton 分布が次数分布として提案されている．冗長性を除く為に各復号ステップでは，1 個の次数 1 の入力シンボルがあることが理想的である．Ideal soliton 分布は，

$$\rho(1) = 1/K, \tag{1}$$

$$\rho(d) = \frac{1}{d(d-1)} \text{ for } d = 2, 3, \ldots, K. \tag{2}$$

により与えられ，その理想を高い確率で実現しているが，実際には十分に機能していない．そこで，各復号ステップで次数 1 の入力シンボルが，約 $S \triangleq \theta \ln(K/\delta)\sqrt{K}$ 個存在し，設計パラメータとして δ と θ を持つ Robust soliton 分布が提案されている．その Robust soliton 分布は，

$$\mu(d) = \frac{\rho(d) + \tau(d)}{Z} \tag{3}$$

により与えられる．ここで，

$$\tau(d) \triangleq \begin{cases} \frac{S}{K}\frac{1}{d} & \text{for } d = 1, 2, \ldots, (K/S) - 1, \\ \frac{S}{K}\ln(S/\delta) & \text{for } d = K/S, \\ 0 & \text{for } d > K/S \end{cases} \tag{4}$$

かつ $Z \triangleq \sum_{d=1}^{K}(\rho(d) + \tau(d))$ である．

(2) 提案連接符号：最小距離が $d_{\min}$ である 2 元内部誤り訂正 (N_1, K_1) 符号 C_1 と robust soliton 分布により生成された V_{K_1} 上の LT 外部 (N_2, K_2) 符号により構成される 2 元連接符号を考える．対象連接符号の符号長，情報ビット数は，それぞれ $N_1 \times N_2$, $K_1 \times K_2$ となる．$\boldsymbol{m} = (\boldsymbol{m}^{(1)}, \boldsymbol{m}^{(2)}, \ldots, \boldsymbol{m}^{(K_2)}) \in V_{K_1}^{K_2}$ をメッセージ系列とする．符号化は，内部・外部符号化の 2 ステップから構成され，外部符号化の後に内部符号化が行われる．最初の符号化ステップでは，メッセージ系列 $\boldsymbol{m}$ が，外部 LT 符号 C_2 により符号化され，外部符号語 $\boldsymbol{c}_2 = (\boldsymbol{c}_2^{(1)}, \boldsymbol{c}_2^{(2)}, \ldots, \boldsymbol{c}_2^{(N_2)}) \in V_{K_1}^{N_2}$ を得る．C_2 の生成行列は，robust soliton 分布を用いて予め生成されている．次の符号化ステップでは，$1 \leq i(\in \mathcal{N}) \leq N_2$ に対する各外部符号化シンボル $\boldsymbol{c}_2^{(i)}$ が，内部誤り訂正符号 C_1 によって符号化され，その得られた内部復号シンボルの系列を $\boldsymbol{c}_1 = (\boldsymbol{c}_1^{(1)}, \boldsymbol{c}_1^{(2)}, \ldots, \boldsymbol{c}_1^{(N_2)}) \in V_{N_1}^{N_2}$ で表す．$\boldsymbol{c}_1$ が，BPSK 変調方式を用いた AWGN 通信路へ等確率で送信される．

(3) 提案連接復号法：$\boldsymbol{r} = (\boldsymbol{r}^{(1)}, \boldsymbol{r}^{(2)}, \ldots, \boldsymbol{r}^{(N_2)}) \in \mathcal{R}_{N_1}^{N_2}$ を AWGN 通信路より得られた受信系列とする．また，$\boldsymbol{r}^{(i)} = (r_1^{(i)}, r_2^{(i)}, \ldots, r_{N_1}^{(i)}) \in \mathcal{R}_{N_1}$，$1 \leq j(\in \mathcal{N}) \leq N_1$ に対して $r_j^{(i)} \in \mathcal{R}_1$ を受信系列 $\boldsymbol{r}$ の第 i 番目の受信シンボル，その j 番目の受信要素とそれぞれ呼ぶ．$r_j^{(i)}$ の信頼度は，$r_j^{(i)}$ の絶対値により与えられる．簡単化の為に，$\boldsymbol{r}^{(i)}$ の受信要素は信頼度の昇順に並べられていると仮定する．硬判定関数を

$$z(r_j^{(i)}) \triangleq \begin{cases} 0 & r_j^{(i)} \leq 0 \text{ の場合}, \\ 1 & \text{その他の場合} \end{cases} \tag{5}$$

と定義し，$\boldsymbol{r}^{(i)}$ の硬判定シンボル $\boldsymbol{z}^{(i)}$ は，

$$\boldsymbol{z}^{(i)} \triangleq (z(r_1^{(i)}), z(r_2^{(i)}), \ldots, z(r_{N_1}^{(i)})) \in V_{N_1}. \tag{6}$$

により与えられる．$\boldsymbol{v} \in V_{N_1}$ に対して，BDD$(\boldsymbol{v})$ を $\boldsymbol{v}$ 中の $t_0(\triangleq \lfloor (d_{\min} - 1)/2 \rfloor)$ までの誤りを訂正する

符号 C_1 の限界距離復号法とする．即ち，BDD($\boldsymbol{v}$) は，中心 $\boldsymbol{v}$ で半径 t_0 の超球中に存在するならば唯一の符号語を出力する．存在しなければ，何も出力せず復号失敗となる．Chase II 復号法では，その限界距離復号が，受信シンボルの硬判定シンボルと予め生成されているテスト系列集合の各系列の和を入力として繰り返し実行される．Chase II 復号法のテスト系列の集合は，

$$T = \{\boldsymbol{t} \circ \mathbf{0}_{N_1-\tau} : \forall \boldsymbol{t} = (t_1, t_2, \ldots, t_\tau) \in V_\tau\} \quad (7)$$

として与えられる．ここで，$\mathbf{0}_{N_1-\tau}$ は長さ $N_1-\tau$ の全 0 系列を，$\boldsymbol{t} \circ \mathbf{0}_{N_1-\tau}$ は

$$\boldsymbol{t} \circ \mathbf{0}_{N_1-\tau} \triangleq (t_1, t_2, \ldots, t_\tau, \underbrace{0, 0, \ldots, 0}_{N_1-\tau}) \in V_{N_1} \quad (8)$$

を表す．

Chase-like 内部復号法は，限界距離復号法の繰り返し回数を $\iota(\in \mathcal{N})$ とし，次の様に実行される．

1. $\boldsymbol{z}^{(i)}$ に対して，限界距離復号法への入力シンボル候補集合

$$S = \left\{\boldsymbol{z}^{(i)} + \boldsymbol{t} : \boldsymbol{t} \in T\right\} \quad (9)$$

を生成する．

2. $1 \leq k(\in \mathcal{N}) \leq \iota$ とし，$\boldsymbol{s}_k$ を集合 S の中で $\boldsymbol{r}^{(i)}$ に対して k 番目に尤度の高い系列

$$\boldsymbol{s}_k \triangleq \arg \max_{\boldsymbol{s} \in S \setminus \{\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_{k-1}\}} M(\boldsymbol{r}^{(i)}, \boldsymbol{s}) \quad (10)$$

として定義する．ここで，$M(\boldsymbol{r}^{(i)}, \boldsymbol{s})$ は，$\boldsymbol{r}^{(i)}$ に対する $\boldsymbol{s} = (s_1, s_2, \ldots, s_{N_1}) \in V_{N_1}$ の尤度

$$M(\boldsymbol{r}^{(i)}, \boldsymbol{s}) = \sum_{j=1}^{N_1} r_j^{(i)}(2s_j - 1) \quad (11)$$

として与えられる．

3. 入力シンボル集合 $\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_\iota$ の各系列に対して，限界距離復号を実行する．すべての入力シンボルに対して限界距離復号を行った後に，得られた候補復号シンボル中最も最尤のシンボルのメッセージシンボル $\boldsymbol{d}^{(i)} \in V_{K_1}$ とその添字 $\alpha^{(i)}$ を内部復号シンボルの信頼度として出力する．$1 \leq i'(\in \mathcal{N}) \leq N_2$ に対して，$\alpha^{(i)}$ が $\alpha^{(i')}$ よりも小さいならば，$\boldsymbol{d}^{(i)}$ の信頼度は，$\boldsymbol{d}^{(i')}$ よりも低いと言われる．

$D = \{\ldots, \boldsymbol{d}^{(i)}, \ldots, \boldsymbol{d}^{(i')}, \ldots\} \subseteq V_{K_1}$ を内部復号メッセージシンボル集合とする．$\boldsymbol{m}' = (\boldsymbol{m}'^{(1)}, \boldsymbol{m}'^{(2)}, \ldots, \boldsymbol{m}'^{(K_2)}) \in V_{K_1}^{K_2}$ を推定メッセージシンボル系列とする．外部復号法では，次数 1 の最信頼内部復号メッセージシンボルが各復号ステップで選ばれる LT 復号法が実行される．

1. 次数 1 の最信頼内部復号メッセージシンボル $\boldsymbol{d}^{(i)}$ を選択する．その様なシンボルが存在しないのならば終了する．
   (a) $\boldsymbol{d}^{(i)}$ が $1 \leq l(\in \mathcal{N}) \leq K_2$ である接続された $\boldsymbol{m}'^{(l)}$ に代入され，
   (b) $\boldsymbol{m}'^{(l)}$ が自身に接続している全ての内部復号メッセージシンボルに加えられ，
   (c) $\boldsymbol{m}'^{(l)}$ に接続している全ての枝がグラフから取り除かれる．
2. ステップ 1 は全ての推定メッセージシンボルが決定されるまで繰り返される．

4 研究成果

最小距離が 21 である BCH(127, 64) 符号に対する Chase-like 内部復号法の復号失敗を含まない復号誤り率は然程大きくないことと LT 符号の特性を生かす為に LT 符号の符号長と情報シンボル数は小くないことが望ましいことより，BCH(127, 64) 内部符号と LT(1500, 1000) 外部符号を用いた提案連接符号を対象とする．PCCS(ι) を限界距離復号法の繰り返し回数が ι である Chase-like 内部復号法を用いた提案連接復号法とする．比較の為に，CCS(2^{10}) を限界距離復号法の繰り返し回数が 2^{10} である従来型の Chase II 内部復号法を用いた連接復号法とする．最初に，BPSK 変調方式を用いた AWGN 通信路に於て，パラメータ δ と θ を $0.01 \leq \delta, \theta \leq 3.0$ の間で 0.01 刻み，4.5dB で PCCS(2^6)，PCCS(2^7)，CCS(2^{10}) の誤り制御特性の評価を行なった．その結果，$\delta = 0.07$，$\theta = 0.02$ である PCCS(2^6) と

PCCS(2^7)，$\delta = 0.09$，$\theta = 0.03$ である CCS(2^{10}) が，最も優れた誤り率を持つことが示された．図 1 は，前出の δ と θ を持つ PCCS(2^6)，PCCS(2^7)，CCS(2^{10}) のビット誤り率を示している．図より，PCCS(2^7) は，PCCS(2^6) よりも優れた誤り率を持ち，PCCS(2^6) と PCCS(2^7) は，それぞれ 4.75dB 以上と 4.50dB 以上にて CCS(2^{10}) よりも優れた誤り率を持つことを示している．

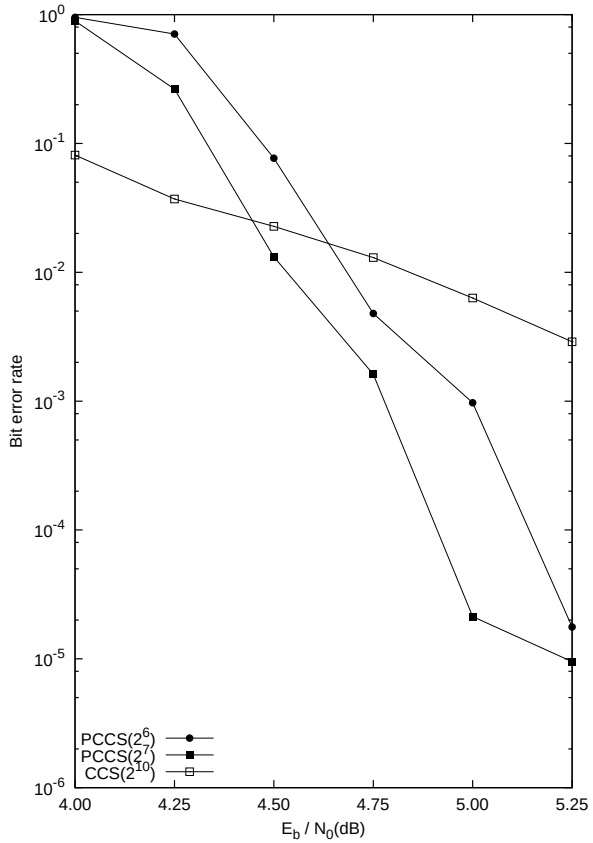

図 1　提案連接符号化方式の誤り率

5　主な発表論文等

[雑誌論文](計 9 件)

① Hitoshi Tokushige, Marc P. C. Fossorier and Tadao Kasami, “A Test Pattern Selection Method for a Joint Bounded-Distance and Encoding-Based Decoding Algorithm of Binary Codes,” *IEEE Transactions on Communications*, vol. 58, no. 6, pp. 1601–1604, Jun. 2010. 査読有

[学会発表](計 46 件)

① Hitoshi Tokushige and Jun Asatani, “On a soft-input decoding algorithm of concatenated LT codes,” *Technical Report of IEICE*, Vol.IT2009-64, pp.71-74, Jan. 2010. 査読無

② Yasunori Yanagida, Hitoshi Tokushige and Jun Asatani, “On an Iterative Bounded-distance Decoding Algorithm with a Learning Function for Binary Linear Block Codes,” *Proceedings of the 2010 International Workshop on Nonlinear Circuits, Communication and Signal Processing*, Waikiki, Hawaii, USA, pp. 385–388, Mar. 2010. 査読有

6　研究組織

(1) 研究代表者

得重 仁 (TOKUSHIGE HITOSHI)

徳島大学・大学院ソシオテクノサイエンス研究部・講師

研究者番号：50336921