The 24th Symposium on Information Theory
and Its Applications (SITA2001)
Kobe, Hyogo, Japan, Dec. 4 - 7, 2001

リスト復号アルゴリズムを用いた連接符号の復号法とその誤り訂正能力
Decoding algorithm for concatenated codes using list decoding algorithm and its error correcting capability

竹内 公二* Kouji TAKEUCHI　　小林 学* Manabu KOBAYASHI　　平澤 茂一* Shigeichi HIRASAWA

Abstract— Concanated codes composed of two codes are important because of their good erroor correcting capabilities. So many researchers have studied them. On the other hand, the list decoding algorithm corrects errors more than the number guaranteed by the minimum distance and generates condidate codewords. In this paper we propose a new decoding algorithm for concatenated codes using list decoding and discuss its error correcting capability.

Keywords—concatenated code, Reddy-Robinson algorithm, list decoding, Gurusuwami-Sudan algorithm

1 はじめに

連接符号は二つの符号を組み合わせた理論上，実用上両面において重要な符号であり，優れた誤り訂正能力をもつ．この符号の復号において，各構成符号に対しそれぞれ限界距離復号を行っただけでは，最小距離で保証された訂正能力以下の誤りさえ訂正できる保証はない．そこで，連接符号の復号法および誤り訂正能力について様々な研究がされてきた[1, 2, 4]．

一方，V.GurusuwamiとM.Sudanは，一般化Reed-Solomon符号，交代式符号および代数幾何符号に対して，それぞれの最小距離で保証される訂正能力を超える数の誤りを訂正し，候補となる符号語をリストとして出力する復号法(GS復号法)[3]を提案した．これは多項式オーダに収まる復号法として近年盛んに研究されている．

本研究では，連接符号の構成符号の復号に際し，GS復号法を適用することを考え，そのときに保証される誤り訂正能力と潜在的な誤り訂正能力について考察を行う．

2 準備

2.1 Reddy-Robinson(RR)復号法

以下では，二つの符号の組み合わせにより構成される符号として連接符号を考える．内部符号$\mathcal{C}_1$を2元(n,k,d)線形符号，外部符号$\mathcal{C}_2$を2^k元(N,K,D)符号とすると，2元$(n_0=nN, k_0=kK, d_0\geq Dd)$連接符号$\mathcal{C}$を構成することができる．

連接符号の復号では，内部符号・外部符号にそれぞれ限界距離復号法を用いただけでは最小距離で保証されるランダム誤り訂正能力$t_{RR}=\lfloor\frac{d_0-1}{2}\rfloor$を保証することはできない．RR復号法では，外部符号の復号に一般化最小距離(GMD)復号法を用いることによってその訂正能力を保証している．また，このRR復号法はある種のt_{RR}個以上の誤りに対しても潜在的な訂正能力を有している．以下にそのアルゴリズムを示す．

[RR復号アルゴリズム]

step0 $F=\phi$

step1 (内部符号の復号と信頼度の算出)
受信語$\boldsymbol{W}$の各行$\boldsymbol{w}_i=(w_{i,0},w_{i,1},\cdots,w_{i,n-1}), i=0,1,\cdots,N-1, w_{i,j}\in$GF(2)に対し，符号$\mathcal{C}_1$の限界距離復号を行う．このときの復号結果を$\hat{\boldsymbol{w}}_i=(\hat{w}_{i,0}, \hat{w}_{i,0},\cdots,\hat{w}_{i,n-1})$とする．第$i$行において訂正した個数を$a_i$個として，各行の信頼度を式(1)のように定義する．ただし，復号結果が誤り検出に終わったときは，$\hat{\boldsymbol{w}}_i=\boldsymbol{w}_i, \theta_i=0$とする．

$$\theta_i=\frac{d-2a_i}{d} \tag{1}$$

step2 各行$\hat{\boldsymbol{w}}_i$の長さkの情報ビットをGF(2^k)上のシンボルy_iに変換し，$\boldsymbol{y}=(y_0,y_1,\cdots,y_{N-1})$を生成する．

step3 $\boldsymbol{y}$に対し，θ_iをもとに符号$\mathcal{C}_2$のGMD復号を以下のように行う．
(1)$|F|\geq D$なら誤り検出としてアルゴリズム終了．そうでないなら$y_i\in$GF$(2^k), i\in F$を消失とみなし，消失・誤り訂正を行い，復号結果を$\hat{\boldsymbol{y}}=(\hat{y}_0,\hat{y}_1,\cdots,\hat{y}_{N-1})$とする．訂正不可能の場合は，(3)へ．
(2)式(2)が成り立つなら，$\hat{\boldsymbol{y}}$を出力し，アルゴリズムを終了する．そうでない場合は，(3)へ．

$$\sum_{i=0}^{N-1}\theta_i\chi(y_i,\hat{y}_i)>N-D \tag{2}$$

ここで，$\chi(y_i,\hat{y}_i)$は，$y_i=\hat{y}_i$のとき1となり，$y_i\neq\hat{y}_i$のとき-1となる関数とする．
(3)$i\notin F$となる$i(=0,1,\cdots,N-1)$のうち，信頼度θ_iが最小のiをFに加え(1)へ．□

このとき次の定理が成り立つ．

定理 1 [1]　RR復号アルゴリズムは，t_{RR}個以下のすべての誤りを訂正することができる．□

RR復号法を拡張し，$t_{ERR}=\lfloor\frac{d(D+\delta)-1}{2}\rfloor,(\delta\geq 1)$個までのすべての誤りを訂正し，候補符号語をリストとして出力する復号法(ERR復号法)[4]も提案されている．

2.2 GS復号法

$(N,K,D=N-K+1)$一般化Reed-Solomom(GRS)符号に対し，GS復号法は最小距離で保証される誤り数を超える符号語を出力することが可能な復号法であり，消失・誤り訂正にも適用できる．この復号法に対し次の定理が成り立つ．

定理 2 [3] 誤り訂正個数をT, 消失個数をSとすると，次式を満足するとき消失・誤り訂正可能となる．

$$T+S<N-\sqrt{(N-S)(K-1)} \tag{3}$$

□

3 GS復号法を用いた連接符号の復号法

本節では，連接符号の復号において，外部符号の復号にGS復号法を用いる．そして，そのときに保証される誤り訂正能力について示す．

3.1 アルゴリズム

以下の2つの復号法を考える．

[復号法1]

step1 $0\leq t_{in}\leq\lfloor\frac{d-1}{2}\rfloor$となる$t_{in}$を選択し，各行$\boldsymbol{w}_i$に対し，内部符号$\mathcal{C}_1$で限界距離復号を行う．このとき，$t_{in}$個以下の誤りならば誤り訂正を行い，それ以外は，誤り検出．

* 早稲田大学理工学部経営システム工学科，〒169-8555 東京都新宿区大久保 3-4-1, School of Science and Engineering, Waseda University, 3-4-1 Ohkubo Shinjyuku-ku, Tokyo, 169-8555 Japan

step2 step1で誤り検出に終わった行を消失とし，外部符号$\mathcal{C}_2$に対しGS復号を行う．

[復号法2]

step0,step1 RR復号法と同様

step2 (1)$|F| \geq D$ならアルゴリズム終了．そうでないなら$y_i \in \mathrm{GF}(2^k), i \in F$を消失とみなし，GS復号を行い，復号結果をリストに加える．訂正不可能の場合は，(2)へ．
(2)$i \notin F$となる$i(=0,1,\cdots,N-1)$のうち，信頼度θ_iが最小のiをFに加え(1)へ．

3.2 保証される誤り訂正能力

復号法1，復号法2それぞれの場合に保証される誤り訂正能力について以下に示す．

3.2.1 復号法1の誤り訂正能力

復号法1で保証される誤り訂正能力をE_1とし，式(4)で定義される$E_1(t)$を考える．

$$E_1(t) = \min\Big\{(d-t)T + (t+1)S - 1 \;;T + S \geq N - \sqrt{(N-S)(K-1)}\Big\} \qquad (4)$$

E_1は，式(5)で定義される．

$$E_1 = \max\Big\{E_1(t); 0 \leq t \leq \Big\lfloor \frac{d-1}{2} \Big\rfloor\Big\} \qquad (5)$$

このとき，$E_1(t)$を最大化する$t = t_{max}$を用いて，内部符号を限界距離復号し，その結果をもとに外部符号をGS復号すれば，E_1個の誤りは訂正することが保証される．内部符号の各パラメータ(n,k,d)と外部符号の各パラメータ(N,K,D)が与えられたときのt_{max}とそのとき保証される誤り訂正能力E_1の算出法を以下に示す．

誤り訂正能力の算出

式(4)に対し，TとSは非負の値をとることを考慮にいれると$T \geq N - S - \sqrt{(N-S)(K-1)} \geq 0$となり，$S$の範囲は$0 \leq S \leq N - K + 1 = D$で与えられる．

式(4)より，$(d-t)T + (t+1)S - 1$は式(6)のようになる．

$$(d-t)T + (t+1)S - 1 \geq \{2t - (d-1)\}S - (d-t)\sqrt{(N-S)(K-1)} + (d-t)N - 1 \qquad (6)$$

式(6)の右辺を$e(S,t)$と定義すると，$e(S,t)$は保証される誤り訂正能力の下界値となる．$e(S,t)$をSに関して偏微分すると，

$$\frac{\delta e_1(S,t)}{\delta S} = \{2t - (d-1)\} + \frac{d-t}{2}\sqrt{\frac{K-1}{N-S}} \qquad (7)$$

となる．以下の範囲に分けて考える．

1. $t_1 = \frac{d-1}{2}$と定義する．
   (a) t_1が整数のとき
   $e(S,t)$はSに関して単調増加となる．したがって$e(S,t)$を最小にするSは，$S = 0$のときである．$e(S,t)$に$S = 0$,$t = t_1$を代入し，$e_1 = e(0,t_1)$とし，$t_1 = t_1 - 1$とする．
   (b) t_1が整数ではないとき，2へ．
2. $0 \leq t \leq t_1$の範囲を考える．式(7)より，式(8)のように$S_1(t)$を定義すると，$e(S,t)$は，$S = S_1(t)$のとき極小値をとる．

$$S_1(t) = N - \frac{K-1}{4}\Big(\frac{d-t}{d-2t-1}\Big)^2 \qquad (8)$$

   (a) $0 \leq t \leq \lfloor \frac{d-2}{3} \rfloor$の範囲
   $e(S,t)$の極小値$S = S_1(t)$は$S_1(t) \geq D$となり，$0 \leq S \leq D$の範囲に存在しない．したがって$e(S,t)$を最小にするSは$S = D$のときとなる．$e_1(D,t) = (t+1)D - 1$となるので，この$e(D,t)$を最大化する$t = \lfloor \frac{d-2}{3} \rfloor = t_2$とし，$e_2 = e(D,t_2)$とする．
   (b) $\lfloor \frac{d+1}{3} \rfloor \leq t \leq t_1$の範囲
   $e(S,t)$の極小値$S = S_1(t)$は，$0 \leq S \leq D$の範囲に存在する．したがって$e(S,t)$に$S = S_1(t)$を代入すると式(9)のようになる．

$$e(S_1(t),t) = (t+1)N - \frac{(K-1)(d-t)^2}{4(d-2t-1)} - 1 \qquad (9)$$

   式(9)をtに関して偏微分し，極大点$t_3 = \frac{d-1}{2} - \frac{d+1}{2}\sqrt{\frac{K-1}{8N+K-1}}$，極小点$t_4 = \frac{d-1}{2} + \frac{d+1}{2} \times \sqrt{\frac{K-1}{8N+K-1}}$が求まる．
   i. $\frac{d-1}{2} - \frac{d+1}{2}\sqrt{\frac{K-1}{8N+K-1}} \leq \lfloor \frac{d+1}{3} \rfloor$のとき
   $e(S,t)$を最大にする$t = \lfloor \frac{d+1}{3} \rfloor = t_5$とし，$S_2 = \lfloor S_1(t_5) \rfloor$，$S_3 = \lceil S_1(t_5) \rceil$と定義する．$S_2$，$S_3$のうち，値が$D$以下となるときにのみ$e(S,t)$に代入し$e(S,t)$の値が最小となるときの値を$e_3$とする．
   ii. $\lfloor \frac{d+1}{3} \rfloor < \frac{d-1}{2} - \frac{d+1}{2}\sqrt{\frac{K-1}{8N+K-1}} \leq t_1$のとき
   $e(S,t)$をtに関する関数とみたときに$e(S,t)$が最大の値をとるtは$t = t_3$のときである．$t_{31} = \lfloor t_3 \rfloor$，$t_{32} = \lceil t_3 \rceil$を定義し，それぞれを$S_1(t)$に代入した次のような$S_4 = \lceil S_1(t_{31}) \rceil$，$S_5 = \lfloor S_1(t_{31}) \rfloor$，$S_6 = \lceil S_1(t_{32}) \rceil$，$S_7 = \lfloor S_1(t_{32}) \rfloor$のうち値が$D$以下となるとき，そのときの$t$を$e(S,t)$に代入し，値が最小になる$e(S,t)$を$e_4$とする．
   iii. 符号のパラメータが(i)(ii)を満足しないとき
   $e(S,t)$を最大にするtは，$t = t_1$のときである．$S_8 = \lfloor S_1(t_1) \rfloor$，$S_9 = \lceil S_1(t_1) \rceil$と定義する．$S_8$，$S_9$のうち，値が$D$以下となるときにのみ$e(S,t)$に代入し値が最小となるときの値を$e_5$とする．

$e_1 \sim e_5$において最大の値が保証される誤り訂正能力の下界値と，その時のtがt_{max}でとなる．

3.2.2 復号法2の誤り訂正能力

連接符号において必ずE個までの誤りを訂正できる復号法が存在すると仮定する．次の補題が導かれる．

補題 1 連接符号において総誤り個数がE個以下なら，式(10)を満足する．

$$\sum_{i=0}^{N-1} \theta_i \chi(y_i, c_i) \geq N - \frac{2E}{d} \qquad (10)$$

[補題1の証明]

受信語$\boldsymbol{W}$の第i行における実際の誤り個数をe_i ,$i = 0,1,\cdots,N-1$とし，連接符号全体の誤り個数をeとすると$e = \sum_{i=0}^{N-1} e_i$が成り立つ．また補題の仮定より$e \leq E$が成り立つ．受信語の各行の復号に着目する．内部符号の復号において，第i行をa_i個訂正したとする．また，内部符号の誤り訂正能力を$t_{in} = \lfloor \frac{d-1}{2} \rfloor$とし，$i = 0,1,\cdots,N-1$

を2つの集合 $A = \{i|a_i \le t_{in}\}, B = \{0, 1, \cdots, N-1\} \setminus A$ に分ける．
(1)$i \in A$ のとき
第 i 行は正しく復号されるので式(11)が成り立つ．

$$\chi(y_i, c_i) = 1, e_i = a_i = \frac{(1-\theta_i)d}{2} \tag{11}$$

(2)$i \in B$ のとき
第 i 行は誤訂正または誤り検出となるので，$\chi(y_i, c_i) = \pm 1$ となる．ここで $d \le e_i + a_i$ であり，これと式(1)から $e_i \ge \frac{(1+\theta_i)d}{2}$ が成り立つ．これと式(11)の両辺を加え，$e \le E$ を考慮に入れると

$$E \ge \sum_{i \in A} \frac{(1-\theta_i)d}{2} + \sum_{i \in B} \frac{(1+\theta_i)d}{2} \tag{12}$$

が成り立つ．式(12)を展開すると式(13)のようになる．

$$2E \le Nd - \sum_{i \in A} \theta_i d + \sum_{i \in B} \theta_i d \tag{13}$$

式(13)より式(14)が成り立つ．

$$Nd - 2E \le \sum_{i \in A} \theta_i d - \sum_{i \in B} \theta_i d \le d \sum_{i=0}^{N-1} \theta_i \chi(y_i, c_i) \tag{14}$$

従って，$\theta_i \chi(y_i, c_i) \ge N - \frac{2E}{d}$ となり補題が証明された．
□

補題1を満足する符号語 c が存在すると仮定する．また，信頼度 θ_i が昇べきの順に並んでいると仮定する．ここで，$\lambda_i = \theta_i - \theta_{i-1}, (\theta_{-1} = 0)$ とすると式(15)が成り立つ．

$$\theta_i = \sum_{j=0}^{i} \lambda_j \le 1 \tag{15}$$

式(15)より，式(10)の左辺は式(16)のように展開できる．

$$\begin{aligned} \sum_{i=0}^{N-1} \theta_i \chi(y_i, c_i) &= \sum_{i=0}^{N-1} \sum_{j=0}^{i} \lambda_j \chi(y_i, c_i) \\ &= \sum_{j=0}^{N-1} \lambda_j \sum_{i=j}^{N-1} \chi(y_i, c_i) \end{aligned} \tag{16}$$

ここで，t_j を $\chi(y_j, c_j) \sim \chi(y_{N-1}, c_{N-1})$ のうち-1の値をとるものの数と定義すると，式(10)(16)より式(17)が成り立つ．

$$\sum_{i=0}^{N-1} \theta_i \chi(y_i, c_i) = \sum_{j=0}^{N-1} \lambda_j (N - 2t_j - j) \tag{17}$$

ここで，$\lambda_j \ne 0$ となる S のうち $N - 2t_j - j$ を最大にする j の値を S とすると，式(18)が成り立つ．

$$\sum_{j=0}^{N-1} \lambda_j (N - 2t_j - j) \le \sum_{j=0}^{N-1} \lambda_j (N - 2t_S - S) \le N - 2t_S - S \tag{18}$$

よって，式(10)(17)(18)より

$$N - \frac{2E}{d} \le \sum_{i=0}^{N-1} \theta_i \chi(y_i, c_i) \le N - 2t_S - S \tag{19}$$

が成り立つ．したがって，式(20)が成り立つ．

$$\frac{2E}{d} \ge 2t_S + S \tag{20}$$

これは，式(10)を満足する符号語 c が存在すれば，$\lambda_j \ne 0$ となる j のうち $N - 2t_j - j$ を最大にする j，つまり S は，必ず存在する．よって，式(10)を満足する符号語 c が誤り訂正能力 E の復号法で必ず得られるためには，この訂正能力 E は式(20)を満足する必要があるということを意味する．ここで、t_S は，$(y_j, \cdots, y_{N-1})$ と $(c_j, \cdots, c_{N-1})$ の Hamming 距離であるので，t_S を誤り数，つまり $t_S = T$, S を消失と考える．GS復号法を用いた場合，$2T + S$ は，式(21)の範囲をとる．

$$2T + S < 2N - S - 2\sqrt{(N-S)(K-1)} \tag{21}$$

ここで，この復号法で得られる符号語は必ずGS復号法で得られるとすると，式(20)(21)より，式(22)が成り立つ必要がある．

$$\frac{2E}{d} < 2N - S - 2\sqrt{(N-S)(K-1)} \tag{22}$$

$2N - S - 2\sqrt{(N-S)(K-1)}$ は $0 \le S \le D-1$ の範囲では単調減少．式(22)に $S = D - 1$ を代入すると式(23)のようになる．

$$E < \frac{d}{2} \times (N + K - 2\sqrt{K(K-1)}) \tag{23}$$

したがって，復号法において保証される誤り訂正能力の下界値は，$\lceil \frac{d}{2}(N + K - 2\sqrt{K(K-1)}) - 1 \rceil$ で示される．

3.3 訂正能力の比較および例

例として内部符号 $\mathcal{C}_1$ に2元(7,4,3)Hamming符号，外部符号 $\mathcal{C}_2$ に 2^4 元(15,6,10)RS符号を用いた(105, 24, 30)連接符号 $\mathcal{C}$ を考える．復号法1の誤り訂正能力は3.2.1節による算出法より，内部符号の復号において，$t_{in} = 1$ として限界距離復号おこなうことにより12となる．内部符号の限界距離復号の結果，誤り検出となった場所を消失として外部符号に対し消失・誤り訂正を1回行う復号法[2](Single-Trial-Decodingと呼ぶことにする．)と比較すると，文献[2]の解析結果より，この符号のパラメータのときはSingle-Trial-Decodingでは内部符号の復号において $t = 0$，$t = 1$ どちらを採用しても9個までの誤り訂正を保証している．

本節では，復号法1,2に関して次の定理が成り立つ．

定理 3 内部符号に対する復号法が同一の場合，復号法1により得られる符号語は，Single-Trial-Decodingにより得られる符号語を，復号法2により得られる符号語は，RR復号法により得られる符号語を必ず含む．

[証明]
Single-Trial-Decoding，RR復号法において用いられる限界距離復号法は，$2T + S < D = N - K + 1$ を満足する誤りは訂正可能である．これは，式(24)のように示すことができる．

$$T + S < N - \frac{(N-S)+K}{2} \tag{24}$$

一方，復号法1,2で用いられるGS復号法は，式(3)を満足する誤りは訂正可能である．式(3)，(24)の右辺を比較すると，式(3)の右辺の方が式(24)の右辺より常に等しいか大きい．つまり，Single-Trial-Decodingにおいて消失・誤り訂正される誤りと消失のパターンは，復号法1のGS復号法で，また，RR復号法において消失・誤り訂正される誤りと消失のパターンは，復号法2のGS復号法で必ず復号される．以上から定理が証明された． □

4 復号法の性能評価

3節では，復号法1，復号法2において保証される誤り訂正能力の下界値を示した．本節では，実際の連接符号において，訂正可能な誤り個数を評価するために，総誤り数を一定にしたもとで全ての誤りパターンを正復号，誤訂正に分類する評価法[4]を用いて評価した．復号法1，復号法2は，ともに保証される誤り訂正能力を越える誤りが生起しても復号可能な場合が存在する．本節ではこの評価方法でこの潜在的な誤り訂正能力についても評価する．

4.1 計算条件

符号2元(105,24,30)連接符号Cを用いて評価を行った．なお，符号Cの構成は次のとおりである．

C_1：2元(7,4,3)Haming符号

C_2：2^4元(15,6,10)RS符号

復号法1，復号法2それぞれにおいて送信語が復号結果のリスト中に含まれている場合(正復号)を成功とする．比較のためSingle-Trial-Decoding($t_{in} = 0, 1$)，RR復号法，ERR復号法($\delta = 1, 2$)も行った．

4.2 結果と考察

4.2.1 正復号数について

数値計算の結果，総誤り個数と正復号率の関係を図1に示す．RR復号法，ERR復号法($\delta = 1, 2$)，Single-Trial($t = 0, 1$)とも，保証される誤り訂正能力までは正復号率は100%の値をとることが確認できる．また，3.2.1より，復号法1の保証される誤り訂正能力の下界値は12であり，また3.2.2より復号法2の誤り訂正能力の下界値は15であるが，図1より，復号法1は13個まで，復号法2は16個までの誤りは必ず訂正できることが確認できる．

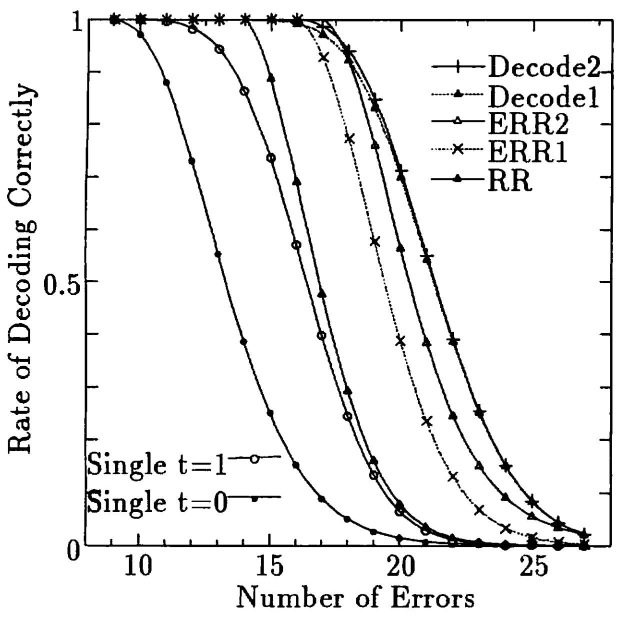

図 1: (105,24,30)連接符号に対する総誤り個数と正復号率の比較

4.2.2 正復号確率について

通信路を2元対称通信路(BSC)を仮定したときの通信路のビット誤り率と復号失敗確率との関係を図2に示す．

まず復号法1について考察する．図1では，RR復号法の方より保証される誤り訂正能力は小さいが，誤り数が保証される誤り訂正能力より大きいところでは，復号法1の方が正復号率が高くなっている．これより，復号法1の方が潜在的な誤り訂正能力が高いことが確認できる．また図2より，誤りの生起確率で重み付けした復号失敗確率は復号法1の方が減少していることがわかる．また，復号法2は，ERR($\delta = 1$)復号法よりも復号失敗確率が減少していることが確認できる．ERR($\delta = 2$)復号法と比較する

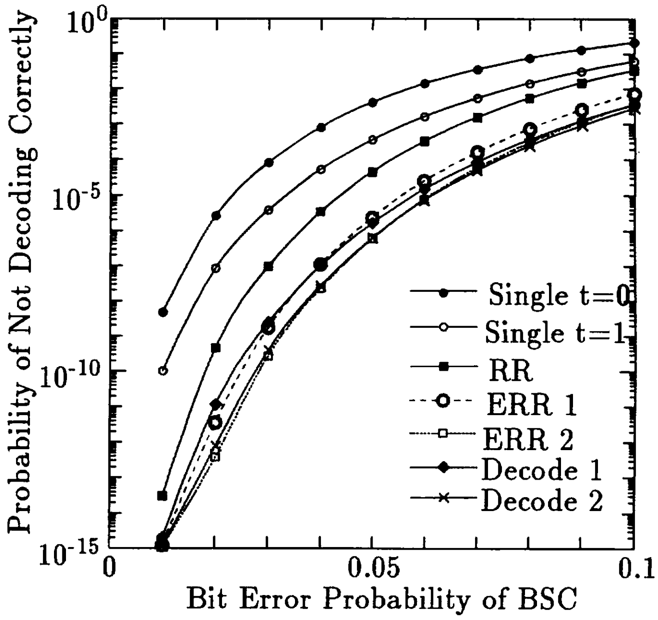

図 2: (105,24,30)連接符号に対するビット誤り率と各復号法の復号誤り率の比較

と，ビット誤り率が0.06より大きいとき，復号法2の復号誤り確率の方がわずかであるが減少していることがわかる．

今回の数値計算に用いた符号のパラメータのように，RR復号法やERR($\delta = 1, 2$)復号法よりも本復号法のほうが有利に働く場合があるが，これらは用いる符号のパラメータによるところが大きいものと思われる．

5 まとめと今後の課題

本稿では，連接符号における外部符号の復号に際しGS復号法を適用し，リスト形式として出力する復号法とそのとき保証される誤り訂正能力について考察した．また，数値計算により実際に保証できる誤り訂正能力，潜在的な誤り訂正能力について評価し，従来提案されているRR復号法やERR復号法との比較を行った．結果的に復号法2は，ERR($\delta = 1, 2$)よりも保証される誤り訂正能力や正復号確率について有利な場合が多く存在するが，これらは選ぶパラメータによる．

今後の課題としては，まず，リスト中から符号語を選ぶための判定方式の提案があげられるが，同じ判定条件で符号語を1つ選ぶとき，定理3より復号法2はRR復号法よりも復号誤り率は悪くなることはない．他には符号のパラメータをどのように選択すれば本復号法が有利に働くかということの理論的解析，リスト復号へ拡張したことによる計算量の増大対策等があげられる．

謝辞： 本研究の一部は文部科学省平成12・13年度科学研究費補助金（課題番号12875072）の助成による．

参考文献

[1] S.M.Reddy, J.P.Robinson, "Random Error and Burst Correction by Iterated Codes," *IEEE Trans. Inform. Theory*, vol.IT-18, No.1, pp.182-185, Jan. 1972.

[2] J. H. Weber and K. A. S. Abbel-Ghaffar, "Guaranteed Error Correction Rate for a Simple Concatenated Coding Scheme with Single-Trial Decoding," *IEEE Trans. Inform. Theory* Vol. IT-46, No.4, pp.1590-1597, July. 2000.

[3] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon codes and algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol.IT-45, pp.1757-1767, Sept. 1999.

[4] 岩下将人，小林学，平澤茂一，"Reddy-Robinson復号法のリスト復号への拡張とその誤り訂正能力，" 信学技報，IT2000-41，pp.1-7，2001.