The 27th Symposium on Information Theory
and Its Applications (SITA2004)
Gero, Gifu, Japan, Dec. 14-17, 2004

ソート・マッチング法に基づく軟判定復号アルゴリズムの修正
An Improved Soft-Decision Decoding Algorithm based on Sort-and-Match Technique

贄田 里詩[†] Satoshi NIEDA　細谷 剛[†] Gou HOSOYA　八木 秀樹[†] Hideki YAGI　平澤 茂一[†] Shigeichi HIRASAWA

Abstract— Several soft-decision decoding algorithms for linear block codes over the AWGN channel have been proposed. Especially, I. Dumer has proposed an efficient decoding algorithm based on Sort-and-Match Technique whose upper bound of the decoding error probability has been shown. The algorithm can be applied to arbitrary linear block codes. In this paper, we propose a new efficient decoding algorithm which reduces the time complexity of Dumer's decoding algorithm. The proposed decoding algorithm, which is formed from two methods based on Sort-and-Match Technique, generates Test-Patterns (or candidate codewords) efficiently. Consequently, the proposed decoding algorithm reduces the time complexity in total by the great reduction of the number of generated Test-Patterns, compared to Dumer's decoding algorithm with the negligible increase in the decoding error probability.
Keywords— maximum likelihood decoding, soft-decision decoding, binary linear block code, Sort-and-Match technique

1 はじめに

線形ブロック符号に対する軟判定復号は通信路から得られる情報を有効に利用することにより，通常用いられる硬判定復号より復号誤り確率を低減できる復号法である．特に最尤復号はそれぞれの符号語が等確率で送信されるときに最小の復号誤り確率を達成する．しかし，最尤復号は符号長が大きくなるにつれて，その計算量が莫大となり実行が困難となる．そのため，最尤復号と同等の復号誤り確率を効率的に達成する復号アルゴリズムの開発が求められており，従来より加法的白色ガウス雑音(AWGN) 通信路における効果的な軟判定復号について多くの研究がなされている．

D. Chase は硬判定受信系列に対して Test-Error-Pattern (TEP) を加え，代数的復号である限界距離復号を用いることによって優れた復号性能を達成しつつ時間計算量を削減する復号アルゴリズムを提案している [1]．また，Chase の手法と同様に，代数的復号を複数回繰り返す優れた復号アルゴリズムが T. Koumoto らや Y. Wu らなどによって提案されている [2], [3]．これらの復号アルゴリズムは，特に BCH 符号やゴッパ符号等といった代数的構造を持つ符号に対して，その効果を発揮する．

一方，I. Dumer は任意の q 元 (n,k) 線形ブロック符号に対し，$\frac{n}{2}$ 次元の Test-Pattern (TP) の集合を 2 組生成し，それらをソート・照会するソート・マッチング法を用いた軟判定復号アルゴリズムを提案している [4]．また，その復号誤り確率が最尤復号に近似できることを解析的に示している．しかし一方で，Dumer の手法では一定数の TP を生成しており，無駄な計算を行っている場合がある．

そこで本研究では，ソート・マッチング法を用いて，Dumer の手法に比べ生成する TP 数を平均的に削減できる新たな復号アルゴリズムを提案する．また，実際どの程度の TP 数が削減できるかを計算機シミュレーションにより評価する．その結果，提案手法は Dumer の手法に比べ平均時間計算量を大きく低減できることを示す．また，同時に復号誤り確率の劣化は無視できる程度であることも示す．

[†] 〒 169-8555 東京都新宿区大久保 3-4-1 早稲田大学理工学部経営システム工学科 School of Science and Engineering, Waseda University Okubo 3-4-1, Shinjuku-ku, Tokyo, 169-8555 Japan. E-mail: nieda@hirasa.mgmt.waseda.ac.jp

2 準備

符号長 n，情報記号数 k の 2 元線形ブロック符号 C を考える[1]．符号 C のパリティ検査行列を H とする．C の任意の符号語 $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1}) \in \{0,1\}^n$ は送信系列 $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1}) \in \{+1, -1\}^n$ に写像されて AWGN 通信路に入力される．受信側では受信した信号系列 $\boldsymbol{r} = (r_0, r_1, \ldots, r_{n-1}) \in R^n$ を系列 $\boldsymbol{\theta} = (\theta_0, \theta_1, \ldots, \theta_{n-1})$, $\theta_i = \ln \frac{P(r_i|c_i=0)}{P(r_i|c_i=1)}$, に写像し，復号器に入力する．ここで $P(r_i|c_i)$ はシンボル c_i の尤度を表すものとする．また，系列 $\boldsymbol{\theta}$ から硬判定系列 $\boldsymbol{z} = (z_0, z_1, \ldots, z_{n-1}) \in \{0,1\}^n$ を次式により得る．

$$z_i = \begin{cases} 0, & \text{if } \theta_i \geq 0; \\ 1, & \text{otherwise.} \end{cases} \tag{1}$$

軟判定復号器では系列 $\boldsymbol{\theta}$ と硬判定系列 $\boldsymbol{z}$ から送信された符号語を推定し，推定符号語 $\hat{\boldsymbol{c}}$ を出力する．

いま，任意の 2 元 n 次元ベクトル $\boldsymbol{a} \in \{0,1\}^n$ に対して，信頼度損失 $L(\boldsymbol{a}, \boldsymbol{z}, \boldsymbol{\theta})$ を次式により定義する．

$$L(\boldsymbol{a}, \boldsymbol{z}, \boldsymbol{\theta}) = \sum_{i=0}^{n-1} (a_i \oplus z_i)|\theta_i|. \tag{2}$$

ただし，$\oplus$ は排他的論理和を表す．また，以後簡単のため，$\boldsymbol{z}$ と $\boldsymbol{\theta}$ が固定されている間は $L(\boldsymbol{a}, \boldsymbol{z}, \boldsymbol{\theta})$ を $L(\boldsymbol{a})$ で表す．このとき，最尤の符号語 $\boldsymbol{c}_{\mathrm{ML}} \in C$ は $L(\boldsymbol{c}_{\mathrm{ML}}) = \min_{\boldsymbol{c} \in C} L(\boldsymbol{c})$ を満足する [2], [3].

3 固定サイズのリストを用いた軟判定復号アルゴリズム

本節では，Dumer により提案された固定サイズのリストを用いた軟判定復号アルゴリズムについて述べる．

3.1 固定サイズのリストを用いた準最尤復号アルゴリズム [5]

ある $\boldsymbol{\theta}, \boldsymbol{z}$ が与えられたもとで，全ての 2 元 n 次元ベクトルを信頼度損失の値順に並べたとき，ある系列 $\boldsymbol{a}$ の順位を $N(\boldsymbol{a})$ で表す．符号語を探索するための 2 元 s 次元ベクトルを s 次元 Test-Pattern (TP) と呼ぶ．

この復号アルゴリズムでは，n 次元 TP をサイズ N のリストに蓄える．以下に復号アルゴリズムを示す．

[復号アルゴリズム Φ_N]

a0) 復号器ではまず，n 次元 TP のリスト $A(\boldsymbol{r}, N) = \{\boldsymbol{a}_j \mid N(\boldsymbol{a}_j) \leq N\}$ を生成する．

[1] 本論文では簡単のため 2 元符号を扱うが q 元符号への拡張は容易である．

a1) $A(r,N)$ の要素である n 次元 TP $a_j,\ j=1,\ldots,N,$ について，それぞれシンドローム $h(a_j)=a_jH^{\mathrm{T}}$ を算出する[2].

a2) $h(a_j)=0$ となる a_j のうち $L(a_j)$ が最小の TP を推定符号語 $\hat{c}$ として出力し，アルゴリズムを終了する．$A(r,N)$ に符号語が一つも含まれていないときは復号失敗とする．

上記のアルゴリズムを復号アルゴリズム Φ_N と呼ぶ．復号アルゴリズム Φ_N の復号誤り確率 P_N は，最尤復号の復号誤り確率を P_{MLD} で表すとき，次式で表せる [5].

$$P_N \le P_{\mathrm{MLD}} \times \left(1+\frac{2^{n-k}}{N}\right). \tag{3}$$

上式より，リストのサイズ N を大きくすると P_N は P_{MLD} に近似されることがわかる．

3.2 ソート・マッチング法に基づく軟判定復号アルゴリズム [4]

復号アルゴリズム Φ_N が最尤復号を達成するためには，リストサイズ N は $N>2^{n-k}$ であるため莫大となる．そこで，Dumer によりリストサイズを大幅に低減できるソート・マッチング法に基づく軟判定復号法が提案された．

まず，スライド窓 $\mathcal{I}(p,s)$ を次式によって定義する．

$$\mathcal{I}(p,s)=\{p,p+1(\mathrm{mod}\ n),\ldots,p+s-1(\mathrm{mod}\ n)\}. \tag{4}$$

$\mathcal{I}(p,s)$ は，$p\in\{0,\ldots,n-1\}$ シンボル目を始点として巡回的に連続する s シンボルの位置集合である．位置集合 $\mathcal{I}(p,s)$ 上での TP を $a_{\mathcal{I}}\in\{0,1\}^s$ と表す．また，$a_{\mathcal{I}}\in\{0,1\}^s$ の信頼度損失 $L_{\mathcal{I}}(a_{\mathcal{I}})$ を次式で定義する．

$$L_{\mathcal{I}}(a_{\mathcal{I}})=\sum_{i\in\mathcal{I}}(a_i\oplus z_i)|\theta_i|. \tag{5}$$

$\mathcal{I}(p,s)$ 上で定義される全ての TP を信頼度損失 $L_{\mathcal{I}}(a_{\mathcal{I}})$ の昇べき順に並べたとき，TP $a_{\mathcal{I}}$ の順位を $N(a_{\mathcal{I}})$ で表す．また，$N(a_{\mathcal{I}})\le M$ を満足する M 個の s 次元 TP のリストを次式で表す．

$$\begin{aligned}A(r_{\mathcal{I}},M)&=\{a_{\mathcal{I}}^{(1)},\ldots,a_{\mathcal{I}}^{(M)}\}\\&=\{a_{\mathcal{I}}\mid N(a_{\mathcal{I}})\le M\}.\end{aligned} \tag{6}$$

$\mathcal{I}(p,s)$ の要素 $p+s-1(\mathrm{mod}\ n)$ を除いたスライド窓を $\mathcal{I}'=\mathcal{I}\backslash\{p+s-1(\mathrm{mod}\ n)\}$ と表すとき，リスト $A(r_{\mathcal{I}'},M)$ に含まれる全ての $s-1$ 次元 TP $a_{\mathcal{I}'}$ に，$p+s-1(\mathrm{mod}\ n)$ シンボル目として $a_{p+s-1(\mathrm{mod}\ n)}\in\{0,1\}$ を付加した s 次元 TP のリストを $A'(r_{\mathcal{I}},2M)=\{a_{\mathcal{I}}\mid N(a_{\mathcal{I}'})\le M\}$ と表す．

ここで，符号長 n が偶数であると仮定し，$s=\frac{n}{2}$ とする．スライド窓 $\mathcal{L}=\mathcal{I}(p,\frac{n}{2})$ と，残りのシンボルでスライド窓 $\mathcal{R}=\mathcal{I}(p+\frac{n}{2},\frac{n}{2})$ を定義する．スライド窓 $\mathcal{L}$, $\mathcal{R}$ 上で定義される受信系列 r，および検査行列 H をそれぞれ $r_{\mathcal{L}}$, $r_{\mathcal{R}}$ および $H_{\mathcal{L}}$, $H_{\mathcal{R}}$ と表す．次に，これらに基づき $\mathcal{L}$ リスト $\{a_{\mathcal{L}}\}$ と $\mathcal{R}$ リスト $\{a_{\mathcal{R}}\}$ を以下のように定義する．

$$\{a_{\mathcal{L}}\}=A'(r_{\mathcal{L}},2M),\quad \{a_{\mathcal{R}}\}=A(r_{\mathcal{R}},M). \tag{7}$$

[復号アルゴリズム Φ_M]

b0) $p:=0$ とする．

b1) $\{a_{\mathcal{L}}\}$ と $\{a_{\mathcal{R}}\}$ を生成する．

b2) $a_{\mathcal{L}}^{(i)}\in\{a_{\mathcal{L}}\}$ と $a_{\mathcal{R}}^{(j)}\in\{a_{\mathcal{R}}\}$ について，それぞれのシンドローム $h(a_{\mathcal{L}}^{(i)})=a_{\mathcal{L}}^{(i)}\times H_{\mathcal{L}}^{\mathrm{T}}, h(a_{\mathcal{R}}^{(j)})=a_{\mathcal{R}}^{(j)}\times H_{\mathcal{R}}^{\mathrm{T}}$ を算出し，$\frac{n}{2}+1+n-k$ シンボルから成るレコード $\mathrm{b}_{\mathcal{L}}=(a_{\mathcal{L}}^{(i)},0,h(a_{\mathcal{L}}^{(i)}))$, $\mathrm{b}_{\mathcal{R}}=(a_{\mathcal{R}}^{(j)},1,h(a_{\mathcal{R}}^{(j)}))$ を構成する．ここで，$\frac{n}{2}+1$ シンボル目の 0 および 1 は $\mathcal{L}$ リストと $\mathcal{R}$ リストの識別子である．

b3) $Z=\{\mathrm{b}_{\mathcal{L}}\}\cup\{\mathrm{b}_{\mathcal{R}}\}$ を構成する．Z に対しシンドロームの値に基づくソートを行い，値が一致し，かつ識別子が不一致となるレコードの組み合わせを探索する．このとき，$(a_{\mathcal{L}}^{(i)},a_{\mathcal{R}}^{(j)})$ は符号語を構成する．

b4) $L(c)$ が最小の符号語 $c=(a_{\mathcal{L}}^{(i)},a_{\mathcal{R}}^{(j)})$ を探索する．もし $p=n-1$ ならば b5) へ進み，それ以外ならば $p:=p+1$ と更新して b1) へ戻る．

b5) $p=0,\ldots,n-1$ の n 回の繰り返しの中で得られた符号語の中で $L(c)$ が最小の符号語を推定符号語として出力し，アルゴリズムを終了する． □

この復号アルゴリズム Φ_M におけるリストサイズの基準 M と，Φ_N におけるリストサイズ N が $M=\lfloor\sqrt{N}\rfloor$ を満足するとき，以下の定理 1 に基づき，復号アルゴリズム Φ_M においてもリスト $A(r,N)$ は全て探索される．このように 2 つのリストを生成し，ソートした後に照会（マッチング）するアルゴリズムをソート・マッチング法と呼ぶ．

定理 1 [4] $N(a)\le N$ を満たす n 次元 TP a には，次式を満たす $p\in\{0,\ldots,n-1\}$ が必ず存在する．

$$\max\{N(a_{\mathcal{L}'}),N(a_{\mathcal{R}})\}\le\lfloor\sqrt{N}\rfloor. \tag{8}$$

また，復号アルゴリズム Φ_M の復号誤り確率 P_M は次式で表すことができる．

$$P_M\le P_N. \tag{9}$$

□

4 可変サイズのリストを用いた軟判定復号アルゴリズム

信頼度損失 $L(a)$ の値に基づく順位が N 以内の n 次元 TP を探索する復号アルゴリズム Φ_N，およびソート・マッチング法に基づく復号アルゴリズム Φ_M は固定サイズのリストを用いて復号を行う．本節では，信頼度損失 $L(a)$ がある閾値 Θ 以内の n 次元 TP を探索する可変サイズのリストを用いた軟判定復号アルゴリズム $\Psi_{F(\Theta)}$ と，$\Psi_{F(\Theta)}$ のソート・マッチング法に基づく復号アルゴリズム $\Psi_{F_{\mathcal{I}}(\Omega)}$ を提案する．

全ての 2 元 n 次元 TP のうち，その信頼度損失が閾値 Θ 以下となる TP の数を $F(\Theta)$ とする．このとき，$F(\Theta)$ に基づくリストを $A(r,F(\Theta))=\{a_j\mid N(a_j)\le F(\Theta),j=1,\ldots,F(\Theta)\}$ と定義し，$A(r,F(\Theta))$ の中で信頼度損失が最小の符号語を推定符号語とする復号アルゴリズムを $\Psi_{F(\Theta)}$ と呼ぶ．以降では，$\Psi_{F(\Theta)}$ に対しソート・マッチング法を用いてリストサイズを低減できる軟判定復号アルゴリズム $\Psi_{F_{\mathcal{I}}(\Omega)}$ について述べる．ここで，Ω を信頼度損失 $L_{\mathcal{I}}(a_{\mathcal{I}})$ の閾値とする．

また，3.2 節と同様に，$\mathcal{L}=\mathcal{I}(p,\frac{n}{2})$, $\mathcal{R}=\mathcal{I}(p+\frac{n}{2},\frac{n}{2})$ を定義し，$r_{\mathcal{L}}$, $r_{\mathcal{R}}$ および $H_{\mathcal{L}}$, $H_{\mathcal{R}}$ を定義する．また，これらに基づき $\mathcal{L}$ リスト $\{a_{\mathcal{L}}\}$ と $\mathcal{R}$ リスト $\{a_{\mathcal{R}}\}$ を以下のように定義する．

$$\begin{aligned}\{a_{\mathcal{L}}\}&=A'(r_{\mathcal{L}},2F_{\mathcal{L}'}(\Omega)),\\ \{a_{\mathcal{R}}\}&=A(r_{\mathcal{R}},F_{\mathcal{R}}(\Omega)).\end{aligned} \tag{10}$$

---
[2] T は行列の転置を表す．

[復号アルゴリズム $\Psi_{F_{\mathcal{I}}(\Omega)}$]

c0) b0) と同様

c1) b1) ~ b3) と同様.

c2) $L(c)$ が最小の符号語 $\boldsymbol{c} = (\boldsymbol{a}_{\mathcal{L}}^{(i)}, \boldsymbol{a}_{\mathcal{R}}^{(j)})$ を探索する. もし, $p = n-1$ ならば c3) へ進み, それ以外ならば $\Omega := \frac{L(\boldsymbol{C})}{2}$, $p := p+1$ と更新して c1) へ戻る.

c3) b5) と同様. □

ここで復号アルゴリズム $\Psi_{F(\Theta)}$ と $\Psi_{F_{\mathcal{I}}(\Omega)}$ について, 以下の定理を示す.

定理 2 $L(\boldsymbol{a}) \leq \Theta$ を満たす TP 系列 $\boldsymbol{a}$ には, 次式を満たす $p \in \{0, \ldots, n-1\}$ が必ず存在する.

$$\max\{L_{\mathcal{L}'}(\boldsymbol{a}_{\mathcal{L}'}), L_{\mathcal{R}}(\boldsymbol{a}_{\mathcal{R}})\} \leq \frac{\Theta}{2}. \tag{11}$$

(証明) $e = p + \frac{n}{2} - 1 (\bmod n)$ と定義するとき, $L(\boldsymbol{a}) \leq \Theta$ を満たす n 次元 TP $\boldsymbol{a}$ の信頼度損失に関して, 以下の 3 式が任意の p で成り立つ.

$$L(\boldsymbol{a}) = L_{\mathcal{L}}(\boldsymbol{a}_{\mathcal{L}}) + L_{\mathcal{R}}(\boldsymbol{a}_{\mathcal{R}}). \tag{12}$$

$$L(\boldsymbol{a}_{\mathcal{L}}) = L(\boldsymbol{a}_{\mathcal{L}'}) + (z_e \oplus a_e)|\theta_e| \geq L(\boldsymbol{a}_{\mathcal{L}'}). \tag{13}$$

$$\min\{L_{\mathcal{L}}(\boldsymbol{a}_{\mathcal{L}}), L_{\mathcal{R}}(\boldsymbol{a}_{\mathcal{R}})\} \leq \frac{\Theta}{2}. \tag{14}$$

もし, $\max\{L_{\mathcal{L}}(\boldsymbol{a}_{\mathcal{L}}), L_{\mathcal{R}}(\boldsymbol{a}_{\mathcal{R}})\} \leq \frac{\Theta}{2}$ を満たす p が存在するならば, 式 (11) は成り立つ. それ以外ならば, p において $L_{\mathcal{L}}(\boldsymbol{a}_{\mathcal{L}}) \stackrel{def}{=} L^{(p)} < \frac{\Theta}{2}$ となり, $p+1$ において $L_{\mathcal{L}}(\boldsymbol{a}_{\mathcal{L}}) \stackrel{def}{=} L^{(p+1)} \geq \frac{\Theta}{2}$ となる p が必ず存在する. このとき, $p+1$ において, $L_{\mathcal{L}'}(\boldsymbol{a}_{\mathcal{L}'}) \leq L^{(p)}$ であるため式 (11) が成り立つ. □

復号アルゴリズム $\Psi_{F_{\mathcal{I}}(\Omega)}$ におけるリストの基準となる Ω と, 復号アルゴリズム $\Psi_{F(\Theta)}$ におけるリストの基準となる Θ が $\Omega = \frac{\Theta}{2}$ を満足するとき, 定理 2 に基づき, 復号アルゴリズム $\Psi_{F_{\mathcal{I}}(\Omega)}$ においてもリスト $A(\boldsymbol{r}, F(\Theta))$ は全て探索される.

5 ソートマッチング法に基づく軟判定復号アルゴリズムの修正

復号アルゴリズム Φ_M では M に基づき一定数の TP を生成する. また, 復号アルゴリズム $\Psi_{F_{\mathcal{I}}(\Omega)}$ の復号誤り確率 $P_{F_{\mathcal{I}}(\Omega)}$ は Ω の値によって変わることが予想されるが, その上界は容易には求められない. 本節では, ソート・マッチング法に基づく 2 つの復号アルゴリズム Φ_M と $\Psi_{F_{\mathcal{I}}(\Omega)}$ を組み合わせることで, 新たな復号アルゴリズム Υ_{V} を提案し, Φ_M に比べ 生成する $\frac{n}{2}$ 次元 TP 数を削減し平均計算量の低減を図る.

5.1 可変リストの概念を利用した修正

復号アルゴリズム $\Psi_{F_{\mathcal{I}}(\Omega)}$ では, 信頼度損失 $L_{\mathcal{I}}(\boldsymbol{a}_{\mathcal{I}})$ に対して閾値 Ω を決め, TP を生成するため, リストサイズが莫大になる可能性がある. そのため, 生成する最大 TP 数を制限する閾値 M_{V} を設定する.

[復号アルゴリズム Υ_{V}]

d0) b0) と同様.

d1) b1) ~ b3) と同様.

d2) $L(c)$ が最小である符号語 $\boldsymbol{c} = (\boldsymbol{a}_{\mathcal{L}}^{(i)}, \boldsymbol{a}_{\mathcal{R}}^{(j)})$ を探索する. もし符号語を探索したならば $\Omega := \frac{L(\boldsymbol{C})}{2}$, $p^{(V)} := p+1$, $u := 0$ とし d3) へ進む. 符号語を探索できなかった場合で, $p = n-1$ ならば復号失敗としてアルゴリズムを終了する. それ以外ならば $p := p+1$ と更新して d1) へ戻る.

d3) $p := p^{(V)} + u (\mathrm{mod}\ n)$ とし $\{\boldsymbol{a}_{\mathcal{L}}\} := A'(\boldsymbol{r}_{\mathcal{L}}, 2V_{\mathcal{L}'})$, $\{\boldsymbol{a}_{\mathcal{R}}\} = A(\boldsymbol{r}_{\mathcal{R}}, V_{\mathcal{R}})$ を生成する. ただし, $V_{\mathcal{L}'} = \min\{F_{\mathcal{L}'}(\Omega), M_{\mathrm{V}}\}$, $V_{\mathcal{R}} = \min\{F_{\mathcal{R}}(\Omega), M_{\mathrm{V}}\}$ である.

d4) b2), b3) と同様.

d5) $L(c)$ が最小の符号語 $\boldsymbol{c} = (\boldsymbol{a}_{\mathcal{L}}^{(i)}, \boldsymbol{a}_{\mathcal{R}}^{(j)})$ を探索する. もし, $u = n-1$ ならば d6) へ進み, それ以外ならば $\Omega := \frac{L(\boldsymbol{C})}{2}$, $u := u+1$ と更新し d3) へ戻る.

d6) 探索した符号語の中で $L(c)$ が最小の符号語を推定符号語として出力し, アルゴリズムを終了する. □

定理 3 復号アルゴリズム Υ_{V} における閾値 M_{V} に対し, 次式が成り立つと仮定する.

$$\forall u \in \{0, \ldots, n-1\},$$
$$M_{\mathrm{V}} \geq \max\{F_{\mathcal{L}'}(\Omega), F_{\mathcal{R}}(\Omega)\}. \tag{15}$$

このとき Υ_{V} の復号誤り確率 P_{V} は $P_{\mathrm{V}} = P_M$ を満足する. □

定理 3 より, 復号誤り確率 P_{V} は $M_{\mathrm{V}} \geq 2^{\frac{n}{2}}$ で $P_{\mathrm{V}} = P_M$ を満足するが, リストサイズを M_{V} で制限することによって, $M_{\mathrm{V}} < 2^{\frac{n}{2}}$ のとき $P_{\mathrm{V}} = P_M$ を必ずしも満足しなくなる. しかし, M_{V} を $M_{\mathrm{V}} \geq M$ とすることで, Φ_M に比べてその劣化が極めて小さく, 無視できる程度になることを次節で示す.

また, Υ_{V} は更に生成する TP 数を削減することが可能である. その一例を述べる.

d1) において, $\{\boldsymbol{a}_{\mathcal{L}}\} = A'(\boldsymbol{r}_{\mathcal{L}}, 2M)$, $\{\boldsymbol{a}_{\mathcal{R}}\} = A(\boldsymbol{r}_{\mathcal{R}}, M)$ を生成した際に $L_{\mathcal{L}}^{(p)} = L(\boldsymbol{a}_{\mathcal{L}'}^{(M)})$ および $L_{\mathcal{R}}^{(p)} = L(\boldsymbol{a}_{\mathcal{R}}^{(M)})$ を記憶しておく. そして, d3) において, もし $0 \leq p \leq p^{(V)} - 1$ かつ $\Omega < \min\{L_{\mathcal{L}}^{(p)}, L_{\mathcal{R}}^{(p)}\}$ ならば, 探索できる符号語は d1) において既に探索されているため, $\{\boldsymbol{a}_{\mathcal{L}}\} = A'(\boldsymbol{r}_{\mathcal{L}}, 2V_{\mathcal{L}'}(\Omega))$, $\{\boldsymbol{a}_{\mathcal{R}}\} = A(\boldsymbol{r}_{\mathcal{R}}, V_{\mathcal{R}}(\Omega))$ を生成せずに d5) に進むことができる.

6 シミュレーションによる評価と考察

本節ではシミュレーションによる評価を行い, 提案手法の有効性を示す.

6.1 シミュレーション条件

符号長 $n = 31$, 情報記号数 $k = 21$ の 2 元 (31, 21) BCH 符号を用いて, 復号アルゴリズム Φ_M, Υ_{V} を行った. $N = 2^{(31-21)}$ とし, 復号アルゴリズム Υ_{V} の最大リストサイズの基準を $M_{\mathrm{V}} = vM$, $v \in \{1, 10, 100\}$, の 3 通りとする. また, 符号長が奇数のため $\mathcal{L}$ リスト, $\mathcal{R}$ リストの生成を行う際に仮想シンボルとして第 n シンボルを付加し, $|\theta_n| = \infty$ とし, 検査行列 H の第 n 列目として全 0 列を付加する. それぞれの復号アルゴリズムに対して 10^6 個の符号語を AWGN 通信路を介して送信する.

6.2 シミュレーション結果

表 1 に復号結果を示す. 復号誤り確率を各 SN 比 E_b/N_0 [dB] ごとに示す.

表 2 に, 1 回あたりの復号で生成された $\frac{n}{2}$ 次元 TP 数を各 E_b/N_0 [dB] ごとに示す. また, 表 3 では, 復号アルゴリズム Υ_{V} の d3) において $M_V < \max\{F_{\mathcal{L}'}(\Omega), F_{\mathcal{R}}(\Omega)\}$ となる割合を各 E_b/N_0 [dB] ごとに示す.

表 1. (31, 21) 符号に対する復号誤り確率

E_b/N_0 [dB]	最尤復号	Φ_M	Υ_V		
			$v=1$	$v=10$	$v=100$
1.0	0.273315	0.274533	0.274598	0.274529	0.274533
2.0	0.113918	0.113936	0.113979	0.113936	0.113936
3.0	0.031485	0.031688	0.031693	0.031689	0.031688
4.0	0.005196	0.005323	0.005322	0.005323	0.005323
5.0	0.000521	0.000535	0.000535	0.000535	0.000535
6.0	0.000021	0.000036	0.000036	0.000036	0.000036

表 2. $\frac{n}{2}$ 次元 TP の平均生成数

E_b/N_0 [dB]	Φ_M	Υ_V		
		$v=1$	$v=10$	$v=100$
1.0	3072	723.84	754.55	755.56
2.0	3072	509.76	522.10	522.60
3.0	3072	343.69	347.03	347.21
4.0	3072	245.24	245.81	245.86
5.0	3072	197.44	197.47	197.48
6.0	3072	176.44	176.44	176.44

表 3. 復号アルゴリズム Υ_V の d3) において $M_V < \max\{F_{\mathcal{L}'}(\Omega), F_{\mathcal{R}}(\Omega)\}$ となる割合

E_b/N_0 [dB]	Υ_V		
	$v=1$	$v=10$	$v=100$
1.0	6.12×10^{-2}	1.34×10^{-4}	6.25×10^{-8}
2.0	2.67×10^{-2}	6.62×10^{-5}	6.25×10^{-8}
3.0	8.18×10^{-3}	2.51×10^{-5}	0
4.0	1.61×10^{-3}	6.94×10^{-6}	0
5.0	1.99×10^{-4}	7.50×10^{-7}	0
6.0	1.19×10^{-5}	1.25×10^{-7}	0

表 1 から，各 E_b/N_0 で復号アルゴリズム Υ_V と Φ_M の復号誤り確率はほぼ同じであることが示されている．v の値にかかわらずほぼ同じであるが，特に $v=100$ では同値となった．

表 2 から，各 E_b/N_0 で復号アルゴリズム Υ_V が生成する $\frac{n}{2}$ 次元 TP 数は Φ_M が生成する $\frac{n}{2}$ 次元 TP 数に比べ，小さい値を示していることがわかる．特に E_b/N_0 [dB] が小さくなるにつれてその差が大きくなっている．

表 3 から，復号アルゴリズム Υ_V の d3) において $M_V < \max\{F_{\mathcal{L}'}(\Omega), F_{\mathcal{R}}(\Omega)\}$ となる割合は小さい値を示していることがわかる．1.0 ~ 4.0 [dB] において，$v=1$ では，その割合が 7 %未満であるが，それ以外ならば 0.02 %未満となっている．このとき，定理 3 より $M_V < \max\{F_{\mathcal{L}'}(\Omega), F_{\mathcal{R}}(\Omega)\}$ を満たさなければ，復号アルゴリズム Υ_V の復号誤り確率 P_V は Φ_M の復号誤り確率 P_M と同じになることに注意されたい．

6.3 評価と考察

本節では，シミュレーション結果より，復号アルゴリズム Υ_V の平均計算量，復号誤り確率，およびリストサイズに対する評価と考察を行う．

(1) 平均計算量

復号アルゴリズム Φ_M は b1) における TP のリスト生成を n 回行う．これに対し，復号アルゴリズム Υ_V は d1), d3) 合わせて n 回以上のリスト生成行うが，d3) における n 回のリスト生成では Ω の値が更新されることによって，リストサイズ $F_{\mathcal{I}}(\Omega)$ が平均的に小さい値となり，生成する TP 数を削減できていると考えられる．

生成する TP 数が削減されることによって，TP 生成の際の信頼度損失算出にかかる計算量，およびシンドローム算出にかかる計算量等が低減される．生成する TP 数の差分を g と表すと，低減できる計算量はそれぞれ $O(gn\log n)$ 回の実数演算，$O(gn^2)$ 回の 2 進演算となり，平均計算量が大きく低減できている．

(2) 復号誤り確率とリストサイズ

表 3 の，復号アルゴリズム Υ_V の d3) において $M_V < \max\{F_{\mathcal{L}'}(\Omega), F_{\mathcal{R}}(\Omega)\}$ となる割合が小さい値を示していることから，最大リストサイズの基準 M_V を適切に設定すれば，ほぼ全ての復号で式 (15) が成り立つといえる．さらに，式 (15) が，ある位置 $u=\rho\in\{0,\ldots,n-1\}$ において成り立たず，アルゴリズム Φ_M では探索される $\hat{c}=a_j,\ j=\arg\min_j\{N(a_j)\mid N(a_j)\le N, h(a_j)=0\}$，が探索されなかったとしても，他の位置 $u\in\{0,\ldots,n-1\}\backslash\rho$ において $\hat{c}$ を探索できる可能性がある．これらのことから，復号アルゴリズム Υ_V と Φ_M の復号誤り確率がほぼ同じになったと考えられる．

7 まとめと今後の課題

本研究では，Dumer によって提案された固定サイズの TP リストを用いたソート・マッチング法に基づく軟判定復号に対して，リストサイズを可変としたソート・マッチング法に基づく軟判定復号を提案した．また，ソート・マッチング法に基づく 2 つの復号アルゴリズムを組み合わせることによって，Dumer による手法に比べ生成する TP 数を大幅に削減できる手法を提案した．さらに，計算機シミュレーションによって，復号誤り確率の劣化とリストサイズの増加は無視できるほど小さいことを示した．

今後の課題としては，q 元符号についても評価を行うこと，および Dumer の手法に比べ復号誤り確率を理論的に保証しつつリストサイズを低減する手法の開発が挙げられる．

謝辞

著者の一人である鶯田は，本研究を進めるにあたり，数多くのご助言，ご支援を賜りました早稲田大学平澤研究室の各位に感謝いたします．

参考文献

[1] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inform. Theory*, Vol.IT-18, No.1, pp.170–182, Nov. 1972.

[2] T. Koumoto, T. Kasami, and S. Lin, "A sufficient condition for ruling out some useless test error patterns in iterative decoding algorithms," *IEICE Trans. Fundamentals*, Vol.E81-A, No.2, pp.321–326, Feb. 1998.

[3] Y. Wu and D. A. Pados, "An adaptive two-stage algorithm for ML and sub-ML decoding of binary linear block codes," *IEEE Trans. Inform. Theory*, Vol.49, No.1, pp.261–269, JAN. 2003.

[4] I. Dumer, "Sort-and-match algorithm for doft-decision decoding," *IEEE Trans. Inform. Theory*, Vol.45, No.7, pp.2333–2338, Nov. 1999.

[5] I. Dumer, "Suboptimal decoding of linear codes: partition technique," *IEEE Trans. Inform. Theory*, Vol.42, No.6, pp.1971–1986, Nov. 1996.