カオス符号化変調方式の実現に関する研究

代表研究者　岡　本　英　二　名古屋工業大学大学院工学研究科准教授
共同研究者　岩　波　保　則　名古屋工業大学大学院工学研究科教授

1 まえがき

昨今の無線通信分野では，引き続きますますの高速通信の実現が必要となっている．また近年の携帯電話よる商取引サービスに代表されるように，生活の様々なシーンにおける無線通信サービスの比重は年々高まっており，金銭や個人情報のやり取りなど，ある個人にとって重要な情報の伝達に無線通信が用いられるようになって来た．そのため，無線における通信の秘匿性の確保は緊急の課題となっている．さらに現在特定の基地局を持たない端末間での情報伝送を行うアドホックネットワークやマルチホップネットワークの研究が盛んに行われている．送信端末－受信端末間の距離が大きい場合や障害物が存在している場合などは大電力が必要になったり，伝送が正常に行えなくなるが，中継端末がデータを受信・再送信することで受信端末への伝送が可能となる．これにより面的な通信容量の増大が期待でき，より高速かつロバストな通信が実現できる．携帯電話が生活の一部となった今では，何らかの携帯端末を用いたアドホックネットワークの構築により重要情報の伝送を行うことで，より快適・便利なシステムの構築を図るという方向も重要視されている．ここで問題となるのが輻輳と秘匿性である．既存の主な暗号化技術は低レイヤに対しては保護を行わないため，変調方式などの物理レイヤにおける信号のやり取りは基本的には秘匿されないままであった．通常無線通信システムにおける秘匿性の確保は，高レイヤにおける暗号化技術，例えばDESやAESの鍵技術に基づくものなどによってまかなわれているが，オーバーヘッド情報のやり取りが必要なため伝送効率の低下が免れなかった．一方，高効率伝送を実現する方式に符号化変調方式があるが，この方式自身には通信の秘匿性に対する能力は含まれていないため，秘匿性の向上には高レイヤの技術を追加適用せざるを得ず，結果的に伝送効率は低下していた．また高レイヤの暗号化技術はそのまま無線通信へ適用すると，無線伝搬環境の頻繁な変化により再送が必要になるなど著しい伝送能力の低下などを引き起こすことがあった．ところで，非線形カオス方程式に基づき通信信号を生成するカオス通信[1-6]は,通信の秘匿性を大きく向上させるため近年研究開発が進んでおり，著者らは符号化変調を構成するカオス符号化変調方式を検討してきた[7].

カオス変調によって生じる無相関系列を符号語間距離に用いるカオス符号化変調方式は，通信の秘匿性が高まり，かつ伝送品質を向上させることができる．符号化利得は復号計算量の増加と引き換えに獲得することができ，理想的には復号拘束長及び計算量の無制限下で，シャノン限界の範囲内において任意に復号誤り率を軽減させることができる.しかしながら本手法の有限処理量下での「所望パケット誤り」「受信SNR」「必要計算複雑度」の関係は明らかではなかった．そこで本研究では，復号方式として検討している準最尤系列推定復号手法について，その判定誤り率特性の解析的導出を行い，計算機シミュレーションにより得られた結果との比較検討を行った．カオス信号がガウス分布であることを前提とし，準最尤系列推定復号法における１ビットの判定誤り率の式を導出し，計算機シミュレーションによる誤り率と比較を行った．その結果，導出時に出てくる係数項が発散するため必要計算複雑度の指数は大きくできないが特性は比較的よく合致し，解析式の妥当性が確認できた．また本手法は大きな符号化利得を得るためには現在の基準では計算量が膨大になっていた．さらに符号長（１フレーム長）を長くすると潜在的な利得は増すが，誤り伝搬長も長くなることが課題であった.一方本方式は変調方式の一種であることから,変調以外の既存技術の適用を妨げない.そこで本手法に通信路符号化器としてターボ符号を外部に連接しLLRを媒介とし，計算量の発散を抑えて伝送特性を改善させる手法について検討し，計算量削減の効果を確認した．さらに本手法の応用として低レイヤーでの柔軟な伝送方式実現のため，符号化変調方式のマルチモード化の検討及び，移動通信への適用を前提にした高品質伝搬路ひずみ等化の手法について検討し，高い効果を得ることを確認した.

2 カオス符号化変調方式

2-1 符号化器

カオス符号化変調方式の利点は要約すれば，ランダム符号による符号化利得の拡大と，方程式による信号

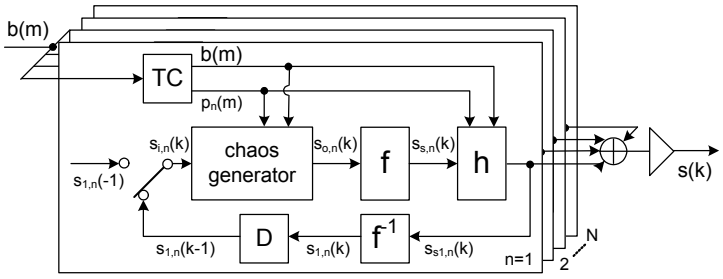


図１：符号化器の構成

点発生であるための信号点メモリの削減である．それを実現するための符号化器モデルを図１に示す．カオス系列を N 個発生させ加算平均することにより，伝送信号をガウス分布信号とし，各カオス生成器のランダム性の要件を緩和させる．カオス信号には次式の円環状カオスを用いた．

$$\begin{cases} x_{n,i+1} = y_{n,i} - (1.73 - 0.001b_1)x_{n,i} + \dfrac{5\left(-1+x_{n,i}^2\right)}{\left(1+x_{n,i}^2\right)} + \tan^{-1}\left(x_{n,i}+y_{n,i}\right) \\ y_{n,i+1} = (-0.98 + 0.001b_1)x_{n,i} \end{cases} \tag{1}$$

b_1 は後ほど述べる．(1)式から生成されたカオス信号を伝送信号の基本波形として成型する．送信側ではまず伝送ビット列 $b(m)\in\{0,1\}$ が連接された符号器により符号化される．符号化は利得増大のために行い，ここでは再帰的組織畳込み符号（RSC: recursive systematic convolutional code）$\left[1 \quad \left(D^M+1\right)\Big/\sum_{i=0}^{M} D^i\right]$ を適用した．ここで M はレジスタの数である．畳込み符号化によりパリティビット $p_n(m)\in\{0,1\}$ が得られるので，$b(m)$ と $p_n(m)$ を用いて変調操作が行われる．変調された信号は送信信号として伝送されるが，同時に送信機内で遅延後カオス生成器に帰還されカオス畳込みが行われる．このように符号化器は RSC によるものとカオスによるものの２つの畳込みを行っていることになる．変調された送信系列 $s(k)$ は通信路において，雑音 w(k) が加わった後，受信信号 r(k)

$$r(k) = s(k) + w(k) \tag{2}$$

が受信される．ここで w(k) は平均 0，分散 $\sigma_e{}^2$ のガウス雑音である．受信機では r(k) と推定系列 $\hat{r}(k)$ とのユークリッド距離が最小となる $\hat{b}(m)$ を復号結果とする．各カオス生成器における入出力は

$$s_{i,n}(k) = s_{1,n}(k-1) \tag{3}$$

$$\begin{aligned} &s_{s,n}(k) = \mathrm{f}\left(s_{o,n}\right) \\ &= \frac{\mathrm{Re}\left[s_{o,n}(k)\right] + \mathrm{Im}\left[s_{o,n}(k)\right]}{75} + j\frac{\mathrm{Re}\left[-s_{o,n}(k)\right] + \mathrm{Im}\left[s_{o,n}(k)\right]}{20} \end{aligned} \tag{4}$$

$$\begin{aligned} &s_{o,n}(k) = x_{l,m_1} + jy_{l,m_1} \\ &m_1 = 500 + 13b_1 + \mathrm{Rnd}(500) \end{aligned} \tag{5}$$

$$x_{n,0} = \mathrm{Re}\left[s_{i,n}(k)\right], \quad y_{n,0} = \mathrm{Im}\left[s_{i,n}(k)\right] \tag{6}$$

とした．ここで $\mathrm{Rnd}(500)$ は 0 から 499 の整数乱数とし，$b_1 = 2b(m) + p_n(m) - 2$ であり，カオス信号の初期値 $s_{1,n}(-1)\in\mathbb{C}$ は予め乱数により送受信機で同一のものを与えるものとした．また(4)式の f は(1)式で生成されるカオス信号の整形を行うものであり，(5)式はランダム性を向上するための繰り返し演算である．これは生成される $s_{o,n}$ について $b(n)$ による信号の相関を低くするためである．

信号の変調とカオス畳込みのフィードバックは

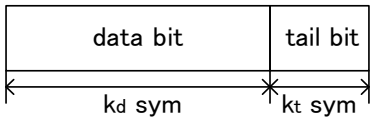


図２：フレーム構造

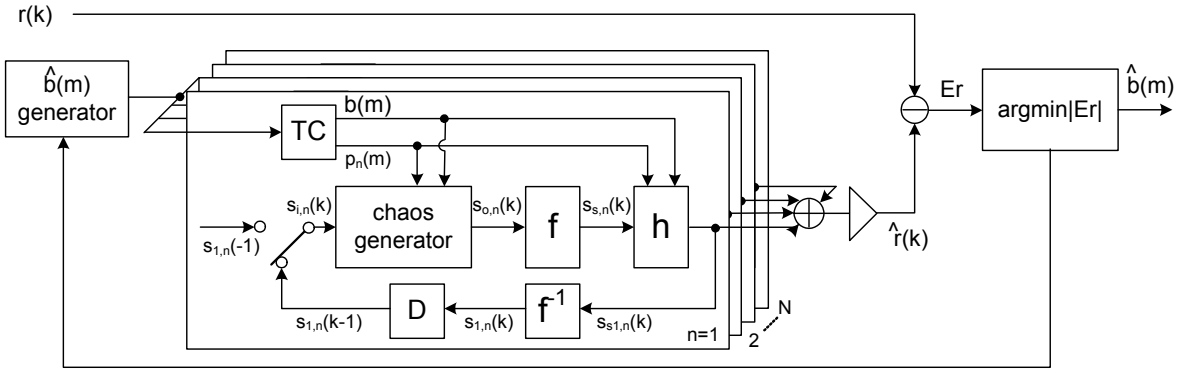


図３：復号器の構成

$$s_{s1,n}(k) = \mathrm{h}\left(k, b(m), p_n(m), s_{s,n}(k)\right) \tag{7}$$

$$s_{1,n}(k) = \mathrm{f}^{-1}\left(s_{s1,n}(k)\right) \tag{8}$$

$$\mathrm{h}\left(k, b(m), p_n(m), s_{s,n}(k)\right) = \begin{cases} s_{s,n}(k)\exp\{j\pi a/2\} : k = r_c n \\ s_{s,n}(k) \qquad\qquad\quad : k \neq r_c n \end{cases} \tag{9}$$

$$s(k) = \frac{1}{N}\sum_{n}^{N} s_{s1,n}(k) \tag{10}$$

とした．ここで $r_c(\geq 1)$ は１情報ビットあたりのカオス符号ビット数である．(1)(5)(9)式及び RSC の遅延素子数の違いより，各カオス系列を独立に変動させる．また(10)式により伝送信号 s(k)は N が大きい場合ガウス分布を持つことになる．

2-2 フレーム構成

本方式では復号誤りが生じたときに送受信機でのカオス同期が失われるが，カオス畳込みによって $b(m)$ を用いて変調された信号がカオス生成器にフィードバックされるため，2.1 の構成ではカオス同期は回復せず，１ビット誤ると BER が 1/2 に収束することになる．そこで図２に示すように送信機側でパケット化を行い，パケットの終端にテールビット $b(m)=0$ を挿入し，パケット終端でカオス生成器を初期値 $s_{1,n}(-1)$ に戻す．データ部を k_d シンボル，テール部を k_t シンボルとすると，伝送速度は $k_d/\{(k_d+k_t)r_c\}$ bit/symbol となる．今回は 2-3 で述べるように初めの１ビットの判定誤り率を導出することを目的とするため，フレーム長は短いものとした．

2-3 復号アルゴリズム

受信側では系列推定を行うが，最尤系列推定 (MLSE) を行うと状態数が指数関数的に増加してしまうため，準最尤の系列推定を行う．図３の受信側において，カオス生成器，演算 f，h，初期値 $s_{1,n}(-1)$ は送受信機で同じものを持つものとする．受信側ではまず推定系列 $\hat{\mathbf{b}}$ を作成し，それに対応する符号語 $\hat{\mathbf{r}}$ を作成する．符号語 $\mathbf{r}$ と $\hat{\mathbf{r}}$ の２乗ユークリッド距離

$$Er = \sum_{i=0}^{r_c l} \left| r(k+i) - \hat{r}(k+i) \right|^2 \tag{11}$$

が最小となる系列を探索する．ここで l は復号拘束長である．次に以下の２つの系列

$$\hat{\mathbf{b}}_0 = \left\{0, \hat{b}(m+1), \cdots, \hat{b}(m+l-1)\right\}$$
$$\hat{\mathbf{b}}_1 = \left\{1, \hat{b}(m+1), \cdots, \hat{b}(m+l-1)\right\} \quad (12)$$

について，(11)式の最小値をそれぞれ$\left\{\hat{b}(m+1), \cdots, \hat{b}(m+l-1)\right\}$の自由度に対して系列探索により算出する．これらを$d_0$，$d_1$とすると

$$d_0 = \min_{\hat{\mathbf{b}}_0} Er, \quad d_1 = \min_{\hat{\mathbf{b}}_1} Er \quad (13)$$

となるので，これらの差

$$d[b(n)] = d_0 - d_1 \quad (14)$$

に対し十分大きい閾値パラメータ sh を導入し，

$$\left|d\left[b(n)\right]\right| > sh \quad (15)$$

が満たされた場合，d[b(m)]>0 のとき$\hat{b}(m)$=1，d[b(m)]<0 のとき$\hat{b}(m)$=0 と１ビットずつ復号する．このとき l を伸ばすと(14)式の差が拡大することがわかる．つまり(11)式の探索のどちらかに必ず正しい送信系列が含まれていると仮定すると，系列を含む側の雑音電力が小さいためメトリック差が広がり，フレーム長が十分長く，正しい系列が含まれている限り(15)式はいつかは満たされ，$b(m)$は正しく復号できるといえる．しかし(12)式の系列数は2^lであるため，計算量は l の増大とともにすぐ発散してしまう．これを防ぐために探索状態数を削減する準最尤系列推定手法を用いる．最大状態数パラメータ K を用い$l \le K$の範囲では(13)式を全探索により求め，この範囲内で(15)式が満たされなければ，以降では$\hat{b}(m)$={0, 1}のそれぞれの領域で Er の大きい系列を 1/2 ずつ廃棄し，$l \to l+1$とする．これにより計算系列数を常に2^K個に保つ．3．ではこの近似値を導出する．

しかし実際には系列削減の際に送信系列を廃棄してしまうと l を増大させても(15)式が満たされなくなってしまうため，次のような計算量，復号拘束長可変の適応的復号アルゴリズムを用いる．

a) $K = K_0$，$l = K$とする．

b) (12)式の2^K個の系列に対し(13)式を算出する．

c) もし(15)式が満たされれば$\hat{b}(m)$を判定，復号し$m \to m+1$として探索終了．

d) $l \to l+1$とする．

e) もし$l < l_{\max}(K)$ならb)へ戻る．

f) もし$K < K_{\max}$なら$K \to K+1$，$l = K$とし，b)へ戻る．

g) この時点までの$\left|d\left[b(m)\right]\right|$の最大値に基づき$\hat{b}(m)$を復号する．$m \to m+1$として探索終了．

ここでK_0は初期状態指数で，各 K における最大復号拘束長$l_{\max}(K)$と判定閾値 sh は許容計算量と所要性能などにより適切に選ぶ必要がある．現在のところ低 SNR において高品質を得ようとすると$K_{\max}$を大きくしなければならないという課題がある．

2 判定誤り率の導出

状態数2^K，復号拘束長 L における判定誤り率の近似値を導出する．ただし簡単のため，判定誤り率はフレーム内のある１ビットを判定する際の誤り率とする．以下ではその導出のため，１）時点 l で正解パスが生き残っていた場合に 0, 1 を正しく判定する確率，２）時点 K で正解パスのメトリックが最小から2^{K-2}位以内に存在する確率，３）時点 K 以降において，時点が１増加するときに生き残る確率（遷移確率），４）途中で破棄されたが正しく判定される確率，を順に求める．

まずカオス変調信号は$N(\mathbf{0}, \sigma_s^2)$なる複素ガウス分布信号とし，送受信信号間のメトリックd^2の確率分布はχ^2分布と仮定する．すると時点lにおける正解パスと時点 0 で分岐した誤りパスのメトリックの確率分布はそれぞれ

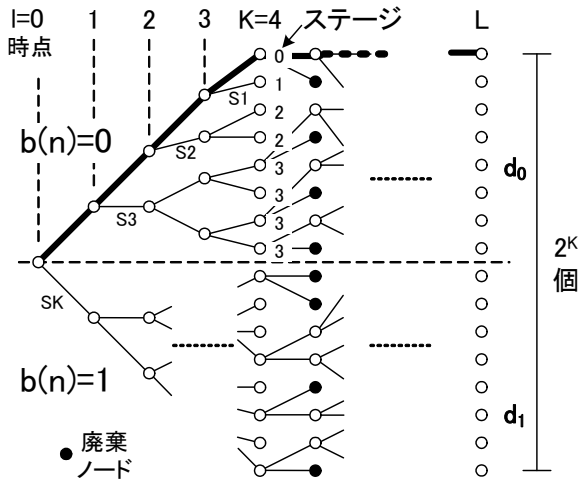


図４：準最尤系列探査手法

$$p_0(\gamma)=\frac{1}{(lr_c-1)!}\frac{\gamma^{(lr_c-1)}}{\sigma_e^{2lr_c}}\exp\left(-\frac{\gamma}{\sigma_e^2}\right) \tag{16}$$

$$p_1(\gamma)=\frac{1}{(lr_c-1)!}\frac{\gamma^{(lr_c-1)}}{\sigma_1^{2lr_c}}\exp\left(-\frac{\gamma}{\sigma_1^2}\right) \tag{17}$$

$$\sigma_1^2=2\lambda\sigma_s^2+\sigma_e^2 \tag{18}$$

となる[8]．ここでσ_e^2は通信路で受けるガウス雑音電力であり，λ（$0\le\lambda\le1$）は正解信号と誤り信号の無相関性を表すパラメータで理想的には$\lambda=1$であり，このとき i. i. d. となる．(16)（17）式より時点lで正解パスが生き残っていた場合に 0, 1 を正しく判定する確率は

$$\begin{aligned}P_c(l)&=\int_0^\infty p_0(\gamma)\int_\gamma^\infty p_1(\gamma)d\gamma\\&=\int_0^\infty\frac{1}{(lr_c-1)!}\frac{\gamma^{(lr_c-1)}}{\sigma_e^{2lr_c}}\exp\left(-\frac{\gamma}{\sigma_e^2}\right)\left[\exp\left(-\frac{\gamma}{\sigma_1^2}\right)\sum_{m=1}^{lr_c}\frac{(\gamma/\sigma_1^2)^{m-1}}{(m-1)!}\right]d\gamma\end{aligned} \tag{19}$$

となる．

次に有限状態数2^Kにおいて時点lで正解パスが生き残る確率，すなわちメトリックが上位2^{K-2}位以内に存在するを求める．図４に示すように復号アルゴリズムは時点Kまでは全探査を行い，各復号ビット領域での状態数は2^{K-1}となる．このとき正解パスとそれ以外のパスのメトリック差は，いつ分岐したかによりクラス分けを行うことができるので，これを図４のようにステージi（Si，$1\le i\le K-1$）と呼ぶことにする．ステージiのパス数は2^{i-1}であり，正解パスのメトリックがステージiのm_i個（$0\le m_i\le 2^{i-1}$）のパスメトリックより小さくなる確率p_{i,m_i}は

$$p_{i,m_i}=\int_0^\infty\frac{1}{(ir_c-1)!}\frac{\gamma^{(ir_c-1)}}{\sigma_e^{2ir_c}}\exp\left(-\frac{\gamma}{\sigma_e^2}\right)[a]^{m_i}\left[1-a\right]^{(2^{ir_c-1}-m_i)}dx \tag{20}$$

となる．ただし

$$a=\exp\left(-\frac{\gamma}{\sigma_1^2}\right)\sum_{m=1}^{ir_c}\frac{(\gamma/\sigma_1^2)^{m-1}}{(m-1)!} \tag{21}$$

である．p_{i,m_i}を用いると，時点Kで正解パスがステージk相当のメトリックになる確率が

$$p_{\mathrm{in},k}=\sum_{\mathbf{m}}\prod_{i=1}^{K-1}p_{i,m_i}{}^{2^{i-1}}C_{m_i} \tag{22}$$

となり，まとめると

$$\mathbf{p}_{\mathrm{init}}=\left[p_{\mathrm{in},0},p_{\mathrm{in},1},\cdots,p_{\mathrm{in},K-2}\right] \tag{23}$$

となる．ただし$\mathbf{m}=\left[m_1,\cdots,m_{K-1}\right]$であり，$k$と$m_i$の関係は

$$k = \left\lfloor \log_2(2^{K-1} - \sum_{i=1}^{K-1} m_i) \right\rfloor \tag{24}$$

で表される．(24)式では例えば正解パスのメトリックがすべてのパスより小さければ $m_i = 2^{i-1}$ となり $k = 0$ となる．なおステージ 0 は正解パス相当である．また m_i の範囲は以下のように表される．

$$2^{K-2} \le \sum_{i=1}^{K-1} m_i \le 2^{K-1} - 1 \tag{25}$$

すると，時点 K で正解パスのメトリックが最小から 2^{K-2} 位以内に存在する確率は

$$P_{s0} = \sum_{k=0}^{K-2} p_{\mathrm{in},k} \tag{26}$$

で与えられる．

そして，時点 K 以降において時点が 1 増加するときに正解パスが生き残る確率を求める．ここで仮定として，時点 $l > K$ においてステージ i のメトリックの期待値が

$$E[d_i^2] = (l-i)r_c\sigma_e^2 + ir_c(2\lambda\sigma_s^2 + \sigma_e^2) = (l\sigma_e^2 + 2i\lambda\sigma_s^2)r_c \tag{27}$$

であるとする．まず時点 l にステージ $s_{l,j}$ にいる正解パスが時点 $l+1$ で持つメトリックの確率密度は

$$p_{t1}(\gamma) = \frac{1}{(r_c-1)!} \frac{\left(\gamma - E\left[d_j^2\right]\right)^{(r_c-1)}}{\sigma_e^{2r_c}} \exp\left(-\frac{\gamma - E\left[d_j^2\right]}{\sigma_e^2}\right) U(\gamma - E\left[d_j^2\right]) \tag{28}$$

となる．ただし

$$U(x) = \begin{cases} 0 & ,x < 0 \\ 1 & ,x \ge 0 \end{cases} \tag{29}$$

である．同様に時点 l でステージ $s_{l,i}$ にいる誤りパスの時点 $l+1$ の確率密度は

$$p_{t2}(\gamma) = \frac{1}{(r_c-1)!} \frac{\left(\gamma - E\left[d_i^2\right]\right)^{(r_c-1)}}{\sigma_1^{2r_c}} \exp\left(-\frac{\gamma - E\left[d_i^2\right]}{\sigma_1^2}\right) U(\gamma - E\left[d_j^2\right]) \tag{30}$$

である．すると，時点 l のステージ $s_{l,j}$ の正解パスが時点 $l+1$ での m_i 個のステージ i （$0 \le i \le K-2$）に対しメトリックが小さくなる確率 $p_{s_{l,j},\mathbf{m}}$ は，

$$\begin{aligned} p_{s_{l,j},\mathbf{m}} &= \int_0^\infty p_{t1}(\gamma) \prod_{i=0}^{K-2} \left[\int_\gamma^\infty p_{t2}(u)du\right]^{m_i} \left[\int_0^\gamma p_{t2}(u)du\right]^{M_i - m_i} d\gamma \\ &= \int_0^\infty \frac{1}{(r_c-1)!} \frac{\left(\gamma - E\left[d_j^2\right]\right)^{(r_c-1)}}{\sigma_e^{2r_c}} \exp\left(-\frac{\gamma - E\left[d_j^2\right]}{\sigma_e^2}\right) \cdot \prod_{i=0}^{K-2} [b]^{m_i} [1-b]^{M_i - m_i} \, d\gamma \end{aligned} \tag{31}$$

となる．ここで

$$b = \begin{cases} 1 & \left(\gamma - E\left[d_i^2\right] < 0\right) \\ \left[\exp\left(-\dfrac{\gamma - E\left[d_i^2\right]}{\sigma_1^2}\right) \displaystyle\sum_{m=1}^{r_c} \frac{\left(\left\{\gamma - E\left[d_i^2\right]\right\}/\sigma_1^2\right)^{m-1}}{(m-1)!}\right] & \\ & \left(\gamma - E\left[d_i^2\right] \ge 0\right) \end{cases} \tag{32}$$

$$M_i = \begin{cases} 2^{i-1} & (s_{l,j} \ne i) \\ 2^{i-1} - 1 & (s_{l,j} = i) \end{cases} \tag{33}$$

である．これにより時点 l にステージ $s_{l,j}$ にいる正解パスが時点 $l+1$ で $s_{l+1,k}$ に遷移する確率が

$$p_{(l,j)(l+1,k)} = \sum_{\mathbf{m}} p_{s_{l,j},\mathbf{m}} \prod_{i=0}^{K-2} {}_{M_i}C_{m_i} \tag{34}$$

として求まる．これをまとめて行列表記すると，

$$\mathbf{P}_l = \begin{bmatrix} p_{(l,1)(l+1,1)} & \cdots & p_{(l,1)(l+1,K-2)} \\ \vdots & \ddots & \vdots \\ p_{(l,K-2)(l+1,1)} & \cdots & p_{(l,K-2)(l+1,K-2)} \end{bmatrix} \tag{35}$$

が構成される．これより，時点Lで正解パスが生き残る確率は

$$\mathbf{p}_1 = \left[p_{1,0}, \cdots, p_{1,K-2} \right] = \mathbf{p}_{\text{init}} \prod_{l=K}^{L-1} \mathbf{P}_l \tag{36}$$

で与えられ，時点Lで生き残りかつ正しく判定される確率は

$$P_o = P_c(L) \sum_{k=0}^{K-1} p_{1,k} \tag{37}$$

となる．

最後に時点lで正解パスが廃棄されたが正しく判定する確率を求める．復号判定は時点Lで行われるが，ここで仮定として，途中で正解パスが廃棄された場合その時点での正判定確率が時点Lまで変化しないとする．時点lで正解パスが廃棄される確率は，時点$l-1$まで生き残りlでメトリックが上位1/2以下となる確率なので，

$$p_d(l) = \mathbf{p}_{\text{init}} \prod_{m=K}^{l-2} \mathbf{P}_m \left[p_{(l-1,1)(l,K-1)}, \cdots, p_{(l-1,K-2),(l,K-1)} \right]^T \tag{38}$$

となり，このときの正判定確率は

$$P_{do}(l) = P_c(l) p_d(l) \tag{39}$$

となる．ただし$p_{(l,k)(l+1,K-1)}$は(34)式と同様に求める．

以上より，状態数2^K，時点Lにおける本復号手法の判定誤り率は

$$P_e = 1 - P_0 - \sum_{l=K+1}^{L} P_{d0}(l) \tag{40}$$

で与えられる．

4 シミュレーション結果

3．で導出した（40）式の判定誤り率を用いてカオス符号化変調方式の特性を検討した．以降では導出式による値を理論値と呼ぶ．まずEb/N0に対する特性を，2．1節の構成によるシミュレーション結果と比較する．ここで理論値，シミュレーション値とも$r_c = 1$，$\sigma_s^2 = 1.820$，$k_d = 12$，$k_t = 1$とした．またシミュレーションでは$K_0 = K_{\max} = K$として適応的復号アルゴリズムは用いなかった．$N = 5$，RSCは$M = 1 \sim 5$とした．ガウス信号の無相関性パラメータを$\lambda = 1/(2\sqrt{2})$としたときの結果を図5に示す．理論値とシミュレーション値はほぼ一致し，特に計算系列数$K = 4$のときによく合致した．両者の誤差は，主に解析式導出の際に用いた仮定に基づく（27）（38）式から生じていると予想される．しかしカオス系列は本来ならば$\lambda = 1$であるべきであるので，本結果からは2．1節の構成では相関を持つことが示されている．この検討とλの改善は今後の課題である．

また図からは当然ながらKの増加による特性の改善が現れており，ここから同じ送信系列においても受信側の計算量を増加させるだけで誤り率特性が改善されることが分かる．ただし本システムでは大きなKに対する理論特性を算出することが重要なのであるが，（22）（33）式の二項係数とその他の式の階乗が発散してしまうため導出できなかった．

次にEb/N0=5 dBのときのカオス信号の分散σ_s^2に対する誤り率特性を図6に示す．計算量Kの増加と相関性λの向上に従い特性が改善されることが分かるが，σ_s^2は特性に関係ないことが分かる．図7にはEb/N0=5 dBのときの伝送1ビットあたりのカオスシンボル数r_cに対する誤り率特性を示す．傾向は図6と同様であるが，λが小さい値の場合r_cの増加に伴い特性が劣化することが分かる．これは伝送シンボルに相関があるため符号語間のユークリッド距離の増加よりも，伝送効率の低下から来る雑音電力の増加の影響の方が大きいためである．$\lambda = 1$の場合はr_cの増加とともに特性が改善するが$r_c = 4$程度で飽和する．したがってそれ以上のr_cの増加は復号計算量削減にもほとんど寄与していない[9]ので意味が無いことが明らかになった．

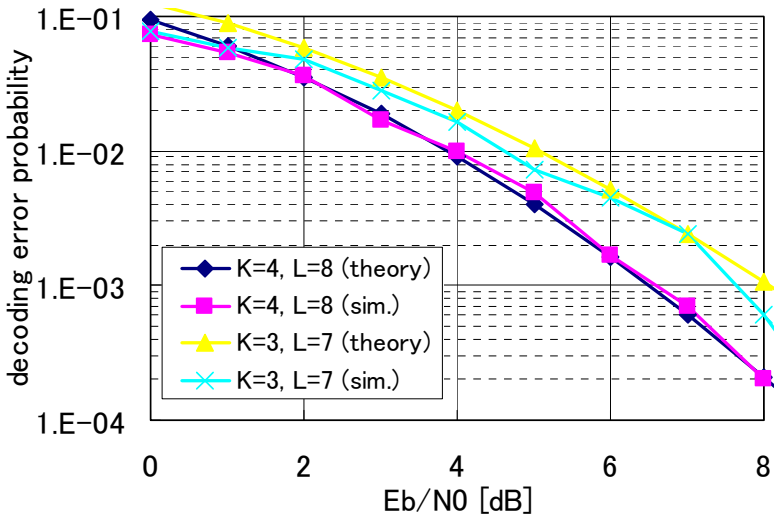


図５：判定誤り率特性

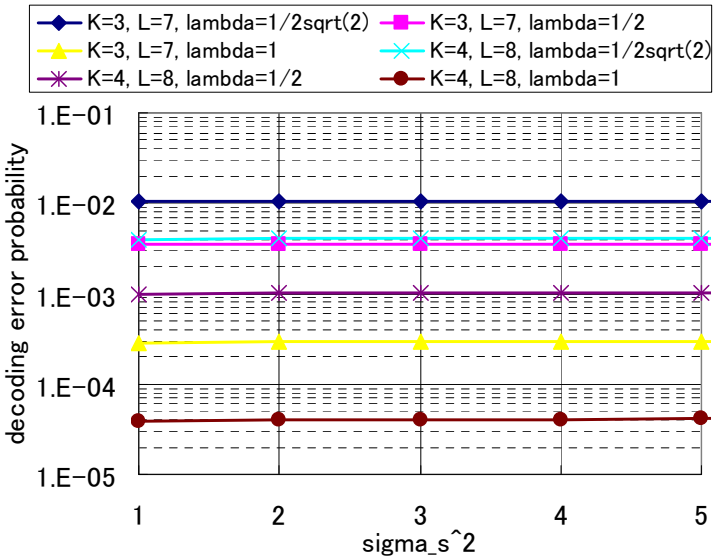


図６：カオス信号の分散 σ_s^2 に対する誤り率特性

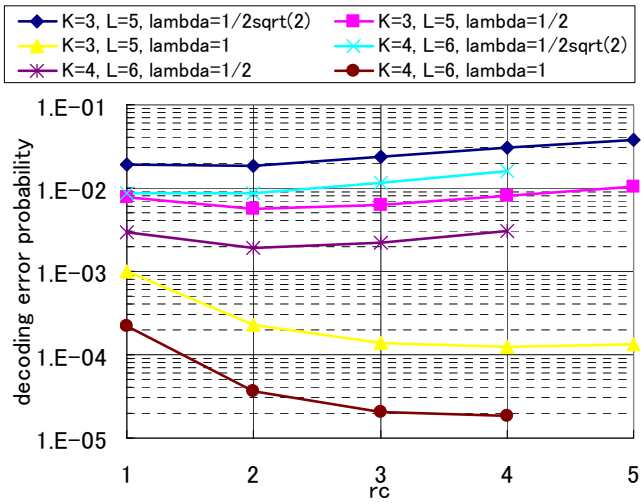


図７：カオスシンボル数 r_c に対する誤り率特性

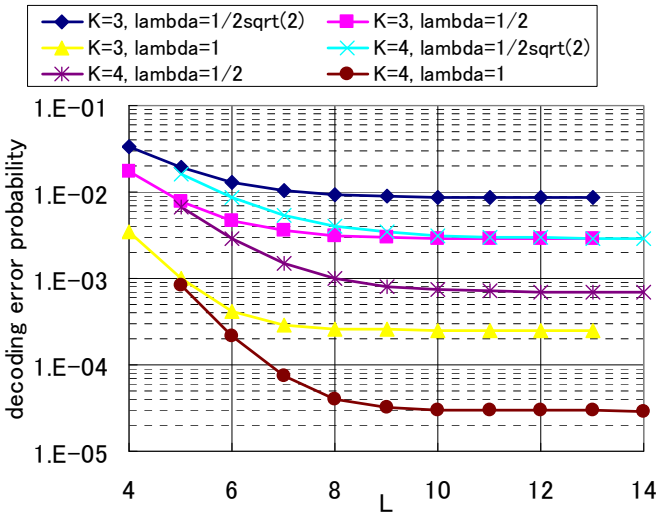


図８：復号拘束長 L に対する誤り率特性

最後に $r_c=1$，Eb/N0=5 dB のときの復号拘束長 L に対する誤り率特性を図８に示す．(38) 式導出の際の仮定により，本解析では L の増加に伴い特性が劣化することはありえないが，結果から $K=4$ のとき $L=10$ とある程度の L で飽和することが分かる．

以上の結果から，大きくない K に対しては 3. 節の式によりシミュレーションと比較的合致する特性解析が行えることがわかった．また復号誤り特性には，カオス系列の相関性 λ が大きく作用することが分かった．そして r_c と L は，$K=4$ までであればある程度の大きさを確保しておけばよいことも明らかとなった．

3 ターボ符号の連接による特性改善

3-1 システム構成

既に述べたようにカオス符号化変調方式は理想的には復号拘束長及び計算量の無制限下で，シャノンの限界の範囲内において任意に復号誤り率を軽減させることができる．しかし計算量の低減を目的とした場合は誤りの発生を許容し，誤り伝搬を抑えるために図２のフレーム長を短いものとする必要がある．これにより k_d シンボル長による符号化利得の限界が生じるが，これをターボ符号の連接により補うことを検討する．送信側では伝送ビット $b(m)$ をターボ符号化器に入力する．そして出力された符号語 $c(n)$（m, n は時間変数）をカオス符号化変調器に入力して伝送信号を生成する．受信側のブロック図を図９に示す．図２のフレームの各データシンボルに対して系列探査を行い，$\hat{\mathbf{c}}_0=\{0,\hat{c}(n+1),\cdots,\hat{c}(n+l_d-1)\}$，$\hat{\mathbf{c}}_1=\{1,\hat{c}(n+1),\cdots,\hat{c}(n+l_d-1)\}$ （$l_d \le k_d$）なる開始ビットの異なる推定語の伝送信号レプリカと受信信号 $\mathbf{r}$ との最小ユークリッド距離 $d_0=\min_{\hat{\mathbf{b}}_0} Er$，$d_1=\min_{\hat{\mathbf{b}}_1} Er$ を求め，LLR $L(n)=d_0-d_1$ なるソフト値を算出すると共に，$L(n)$ の符号により判定を行い時点 $n+1$ の系列探査へと移行する．このときの探査状態数を 2^4 と比較的低い値で固定しカオス復号の計算量を抑える．そして得られた LLR $\mathbf{L}$ を SOVA(soft output Viterbi algorithm)ターボ復号器に入力し，タ

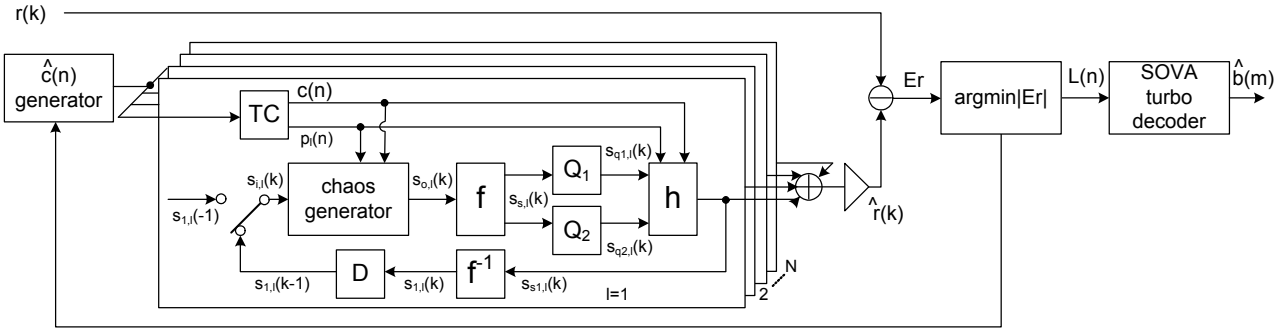


図９：ターボ符号連接復号器のブロック図

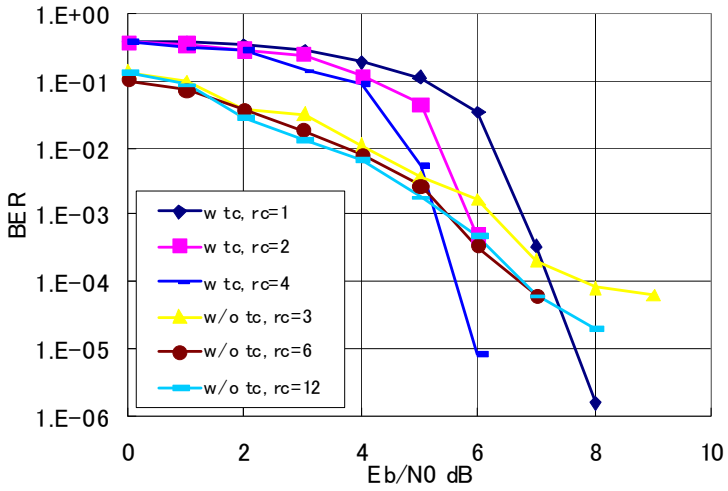


図１０：復号誤り率特性

ーボ復号器内で繰り返し演算を用い，最終的に復号ビット $\hat{b}(m)$ を得る．ただしターボ復号器での繰り返し演算の際の通信路値は 0 とし，SOVA のメトリック計算時にのみ $L(n)$ を用いた．これは信号点配置が固定でなく，カオス畳込みにより前方シンボルに依存したものとなるため通信路値としては不適であるためである．なお，本構成においてもカオスの符号化利得と計算量の関係は保持しており，状態数を 2^{k_d} まで増やすことにより復号特性が改善される．

3-2 シミュレーション結果

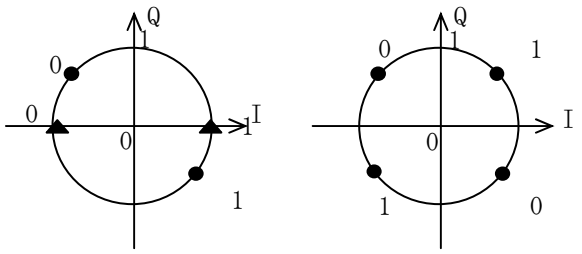
伝送誤り率特性を数値計算により算出した．連接するターボ符号は情報ビット数 $K=1998$，RSC[1 5/7]，符号化率 1/3 とした． $c(n)$ 1 ビットに対しカオス信号を r_c シンボル伝送する場合，全体の伝送効率は $k_d/\{3(k_d+k_t)r_c\}$ bit/sym となる．今回は $k_d=10, k_t=2$ とし， r_c をパラメータとしてターボ符号連接，同程度の伝送効率での連接無しの特性を算出した．結果を図１０に示すようにソフト値に基づく復号が有効に働いており，カオス復号の探査量が 2^4 でもターボ符号化の効果が現れていることが分かる．$r_c=1,2,4$ に対して，同程度の伝送速度の非連接系よりそれぞれ 7.1，6.0，5.2 dB 以降利得が得られている． カオス復号の状態数を増やすことで全体の特性がさらに改善すると予想される．

4 カオス符号化変調方式の応用に関する検討

本節ではカオス符号化変調方式の応用について検討を行った．符号化変調方式に対して，フェージング等による伝送路条件の変化に対応して誤り訂正の符号化率を可変とする適応変調方式が注目されている．そこで，カオス符号化変調方式に適用することを目的とし，その初期検討として LLR を導入しているマルチモードブロック符号化変調(マルチモード BCM：Block-Coded-Modulation)に対し，マルチパス環境においてマルチモード BCM へターボ等化を適用する手法について検討した．そして計算機シミュレーションによりその有効性を明らかにした．これにより伝送モードを複数持つことができ，品質や伝送速度についての更なる柔軟性を獲得することができるようになった．またさらに移動通信環境への適用について，その等化手法についての検討を行った．マルチパスフェージング通信路では，信号電力対雑音電力比を大きくしてもバースト的な誤りが起こり，信号速度を上げると受信信号自体に歪みが生じ，通信品質が得られにくい．これらの問題を解決する方法の一つとしてターボ等化方式が考えられる．上で述べたように本手法にターボ符号を適用する効果を確認しているため，ターボ符号を併用したターボ等化をマルチパス通信路に適応することを考えた．なおこれらの手法の検討は基礎段階のためカオス変調を用いていないが，手法においてカオス変調の適用を妨げる要因は存在しないため，カオス符号化変調への適用は比較的容易であると考えられる．

4-1 マルチモード BCM(BPSK/QPSK)のモード構成

BPSK と QPSK を用いたマルチモード BCM(block coded modulation: ブロック符号化変調)について検討する．マルチモード BCM は 1 ブロックの情報ビットの先頭部分にモード情報を付加し送信を行なう．受信側では，モード情報から BPSK モードか QPSK モードかを判別する．そのモード情報に関し 2 つのモード構成の検討を行なう．まずそれぞれの信号点配置の様子を図１１に示す．そして，図１２には符号化器マトリクスを示して



(a) BPSK　　(b) QPSK

図１１： 信号点配置

$$e_1:\ \overbrace{h_1}\ \overbrace{h_2}\ \cdots\ \overbrace{h_m}\ \overbrace{a_1}\ \overbrace{a_2}\ \cdots\ \overbrace{a_{b-m-1}}\ \overbrace{c_B}$$
$$\Downarrow\ \Downarrow\quad\Downarrow\ \Downarrow\ \Downarrow\quad\Downarrow\ \Downarrow$$
$$s_1\ s_2\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ s_b$$

(a) BPSK

$$e_1:\ \overbrace{h_1}\ \overbrace{h_2}\ \cdots\ \overbrace{h_m}\ \overbrace{a_1}\ \overbrace{a_1}\ \cdots\ \overbrace{a_1}\ \overbrace{a_1}$$
$$e_2:\ \underbrace{a_2}\ \underbrace{a_3}\ \cdots\ \underbrace{a_{m+1}}\ \underbrace{a_{m+2}}\ \underbrace{a_{m+3}}\ \cdots\ \underbrace{a_b}\ \underbrace{c_Q}$$
$$\Downarrow\ \Downarrow\quad\Downarrow\ \Downarrow\ \Downarrow\quad\Downarrow\ \Downarrow$$
$$s_1\ s_2\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ s_b$$

(b) QPSK

図１２：マルチモード BCM における符号化器マトリクス

いる．ここで，h はモードビット，m はモード長を示し，b はブロック長を示している．$a_j \in \{0,1\}$ は情報ビットを示し，$c \in \{0,1\}$ はパリティビットを示す．図１２より QPSK はモード部分に情報ビットを含んでいる．まずモード構成 1 に関しては単純にモードビットを BPSK は $h_i = 0\ (i = 1,2,\ldots,m)$，QPSK の場合は $h_i = 1 (i = 1,2,\ldots,\ m)$ とし，信号点配置は BPSK において図１１(a)の丸の点に配置する．この構成において，QPSK のモード部分における情報ビット(10, 11)のユークリッド距離は大きくできるが，モードビット(0 と 10, 11)の距離は大きくならない．従って，モード構成 2 においては BPSK の信号点配置を図１１の三角の点に配置し，モードビットを BPSK は $h_i = 0\ (i = 1,2,\ldots,m)$，QPSK の場合は $h_i = a_i (i = 2,3,\ldots,\ m+1)$ とする．これより QPSK のモードビットは 00 か 11 になるので，図１１よりモードビット(0 と 00, 11)のユークリッド距離は大きくなり，モードを誤る確率がモード構成 1 より改善される．しかし，モード部分の情報ビット(00, 11)の距離は小さくなるので，その影響による劣化が生じると考えられる．

4-2 マルチモード BCM のシミュレーション結果

AWGN 通信路において 2 つのモード構成におけるシミュレーションを行なった．ブロック長，モード長はそれぞれ b=20，m=4 とし，符号化器はマルチモード BCM，BPSK モード，QPSK モードの発生は簡単のため，生成確率 50%のランダムとする．復号には SOVA を用いている．シミュレーション結果を図１３に示す．

図１３の結果から，E_b/N_0 の低い部分ではモード構成 2 の方が良くなるものの，E_b/N_0 が高くなるにつれてモード構成 1 の特性が改善される結果となった．4-1 で述べたようにモード構成 2 はモード誤りを軽減できるので，低 E_b/N_0 領域では特性が良くなるが，モード誤りが両構成共に少なくなる高 E_b/N_0 領域では情報ビットのユークリッド距離の影響から特性が劣化する．

4-3 SC/MMSE 連接によるターボ等化方式の特性改善

ターボ符号を用いた伝送系を移動通信に適用する場合，伝搬路の等化にターボ等化を用いることができる．このターボ等化の性能を向上させる手法について検討を行った．符号に並列連接畳み込み符号を用いたターボ等化器に SC/MMSE (Soft Canceller followed by Minimum Mean Square Error filter) を中間推定として

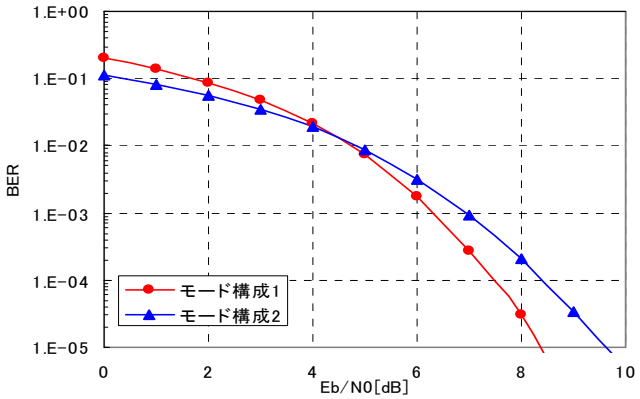


図１３：モード構成の違いによる BER 特性

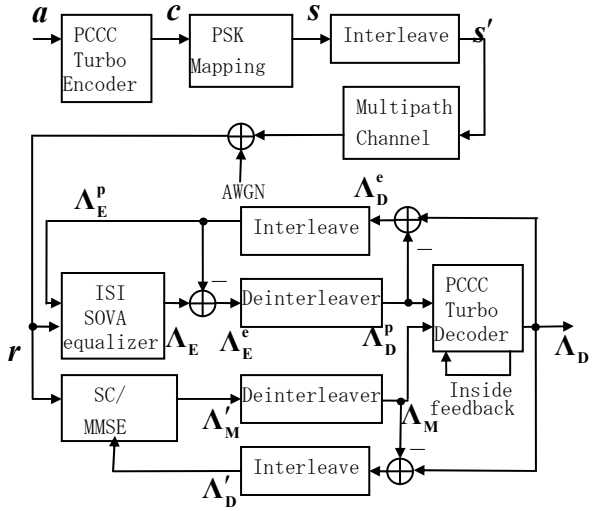


図１４：提案手法の受信機モデル

導入した提案手法のブロック図を図１４に示す．既存のターボ等化システムとの違いは ISI SOVA 等化器および SC/MMSE 等化器が復号器との間で相互に情報をやり取りすることが可能になる点である．以下に受信機の操作について示す．

（１）　既存のターボ等化と同様にターボ復号器と ISI SOVA 等化器の間で反復復号を行う．ISI 等化器に受信値 $\boldsymbol{r}$ と事前 LLR Λ_E^p（初期値は 0）を入力し，事後 LLR Λ_E を求める．$\Lambda_E^e = \Lambda_E - \Lambda_E^p$ により外部情報 Λ_E^e を求める．求めた外部情報 Λ_E^e は，デインタリーバにより並べ替えられ，復号器の事前 LLR Λ_D^p として復号器に入力される．このとき，SC/MMSE では演算を行わないので，SC/MMSE の出力である事後 LLR $\boldsymbol{\Lambda}_M = (\Lambda_M(s_1), \Lambda_M(s_2), \cdots, \Lambda_M(s_N))$ は復号器に入力されない．PCCC 復号器では複数回の繰り返し処理を行う．ここで得られた事後 LLR Λ_D と事前 LLR Λ_D^p を用いて，$\Lambda_D^e = \Lambda_D - \Lambda_D^p$ により外部情報 Λ_D^e を求める．求めた外部情報 Λ_D^e はインタリーバで並べ替え，ISI 等化器の事前 LLR Λ_E^p として再び ISI 等化器の入力とする．この操作を複数回繰り返し，事後 LLR Λ_D を求める．

（２）　得られた事後 LLR Λ_D をインタリーバで並べ替えた LLR $\boldsymbol{\Lambda}'_D$ を SC/MMSE に入力する．この LLR Λ'_D により生成したソフトレプリカと受信値 $\boldsymbol{r}$ を用いてソフトキャンセルを行い，LLR Λ'_M を求める．

（３）　(1)と同様に ISI 等化器と PCCC 復号器の間で反復復号を行うが，(2)で求めた LLR Λ'_M をデインタリーバで並べ替えた LLR Λ_M が PCCC 復号器に入力される．つまり，復号器に入力される値は ISI SOVA 等化器からの LLR Λ_D^p と SC/MMSE からの LLR Λ_M である．ここで，どちらか一方が誤っているときの影響を軽減するため Λ_D^p と Λ_M の平均をとって $(\Lambda_D^p + \Lambda_M)/2$ として PCCC 復号器へ入力する．ただし，この SC/MMSE からの LLR Λ_M の値は保持される．つまり，次の繰り返し等化処理の後に PCCC 復号器に入力される値は Λ_D^p のみ

が更新されることになる．また，ISI 等化器に入力される事前 LLR Λ_E^p は反復復号を行う前に初期化し **0** とする．反復復号を行った後 PCCC 復号器から事後 LLR Λ_D を求める．

（４） (2)，(3)を複数回繰り返し，ターボ復号器から最終的に得られる事後 LLR Λ_D によって符号を判定する．

4-4 ターボ等化方式の計算機シミュレーション

提案システムモデルの BER 特性を計算機シミュレーションにより,既存方式との比較を通して検討する.また，符号化器に LDPC（Low Density Parity Check）符号を用いた SC/MMSE 連接のターボ等化方式[10]の誤り率特性とも比較を行う．シミュレーション条件を表１に示す.

ターボ復号での繰り返し回数は２回と固定し，ターボ等化の繰り返し処理において ISI SOVA 等化器へのフィードバック２回毎に次のフィードバックを SC/MMSE に行うものとする．また，同じ演算量での比較を行うため AWGN 通信路でのターボ復号の回数をそれぞれ 6, 18 回とした．図１５の静的 5 パス等電力通信路において，遅延波がランダムに位相変化すると想定し位相平均をとった場合を図１６，位相変化なしとした場合を図１７にそれぞれ示す．図１７において，符号化に LDPC（1032，518）符号を用い，復号器で 10 回の繰り返し復号を行い，等化器へのフィードバック処理は提案手法と同じ方法を用いて SC/MMSE 等化器に計３回フィードバックを行った場合の BER 特性も示す．図１６，１７より，演算量が等しい PCCC ターボ等化#3 と提案手法「outside#2 SC/MMSE#1」および「PCCC ターボ等化#9」と提案手法「outside#2 SC/MMSE#3」をそれぞれ比べると，提案手法の BER 特性が BER10^{-4} において図１６では約 0.4dB，図１７では約 0.6dB の改善が見られる．特に図１７においては，既存手法のターボ等化が繰り返し 2 回以降で特性が改善されず特性限界となっているが，提案手法では特性が改善されていることがわかる．また「PCCC ターボ等化#9」に比べ提案手法の「outside#2 SC/MMSE#1」が特性を上回っていることがわかる．更には，図１７において 1 回目の feedback を ISI SOVA 等化器に 2 回目の feedback を SC/MMSE に行った「outside#1 SC/MMSE#1」の特性が「PCCC ターボ等化#9」の特性を上回っている．このことから，SC/MMSE を導入することによって演算量が削減されたと言える．更には，LDPC（1032，518）符号を用いた場合に比べると，この比較は符号長や符号化率といった点で公平な比較とは言えないが，提案手法の誤り率特性は大きく改善されていることがわかる．しかし，提案手法はいずれも AWGN での BER 特性には収束しておらず，更なる特性改善の余地があると言える．

表１． シミュレーション条件

符号化器	ターボ符号（並列連接RSC[7,5]符号化器）
送信ビット数	2000ビット
変調方式	BPSK
通信路	静的5パス等電力通信路 ＋ AWGN
等化器	ISI SOVA等化器 SC/MMSE 等化器
復号繰り返し回数	2回
等化繰り返し回数	3，9回
インタリーバ	S-ランダムインタリーバ

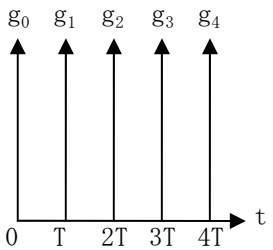


図１５：静的 5 パス等電力通信路の遅延プロファイル

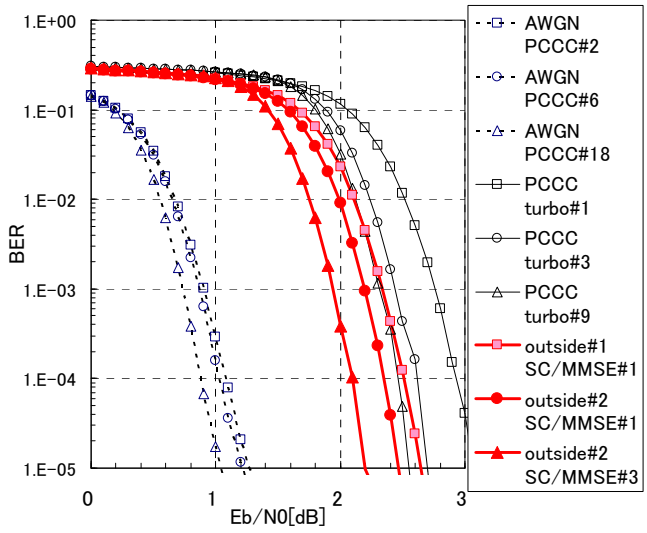


図１６：提案手法の誤り率特性(位相平均)

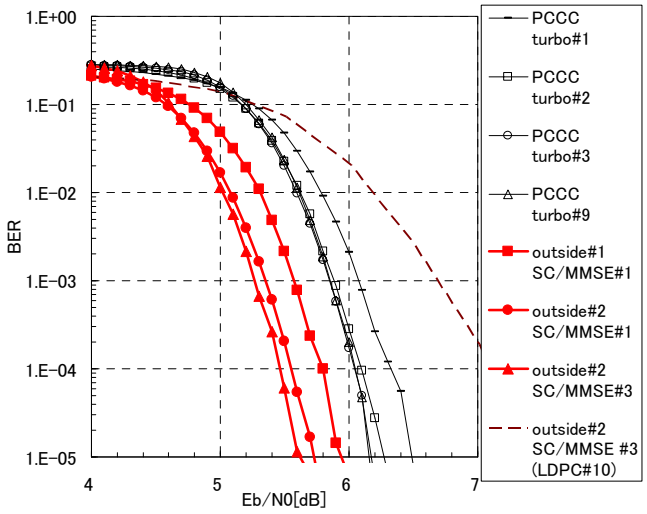


図１７：提案手法の誤り率特性(位相変化なし)

4-5 ターボ等化方式の考察

計算結果より，低い Eb/N0 で非常に優れた BER 特性を示すことが確認でき,既存の PCCC を用いたターボ等化に比べ,SC/MMSE を導入した提案手法は若干の BER 特性の改善が得られた．また同じ誤り率では,提案手法により繰り返し等化の収束特性が改善され,演算量の削減が行えた．これにより SC/MMSE および ISI SOVA 等化器とターボ復号器の間で相互に情報をやり取りすることで誤り率の改善を試みる提案手法の有効性が確認できた．しかし,AWGN 通信路での特性には収束していないため,より高い等化能力を持つ等化器の導入や，より LLR の相関が低い等化器同士の組み合わせなどによって更なる特性改善の検討及び理論解析必要であると考えられる．

5 まとめ

本研究ではカオス符号化変調方式の有限処理量下での「所望パケット誤り」「受信 SNR」「必要計算複雑度」の関係を明らかにするため，復号方式として検討している準最尤系列推定復号手法について，その判定誤り率特性の解析的導出を行い，計算機シミュレーションにより得られた結果との比較検討を行った．カオス信号がガウス分布であることを前提とし,準最尤系列推定復号法における 1 ビットの判定誤り率の式を導出し,計算機シミュレーションによる誤り率と比較を行った．その結果，導出時に出てくる係数項が発散するため必要計算複雑度の指数は大きくできないが特性は比較的よく合致し，解析式の妥当性が確認できた．また本

手法は大きな符号化利得を得るためには現在の基準では計算量が膨大になっていた．さらに符号長（１フレーム長）を長くすると潜在的な利得は増すが，誤り伝搬長も長くなることが課題であった．一方本方式は変調方式の一種であることから，変調以外の既存技術の適用を妨げない．そこで本手法に通信路符号化器としてターボ符号を外部に連接し LLR を媒介とし，計算量の発散を抑えて伝送特性を改善させる手法について検討し，計算量削減の効果を確認した．さらに本手法の応用として低レイヤーでの柔軟な伝送方式実現のため，符号化変調方式のマルチモード化の検討及び，移動通信への適用を前提にした高品質伝搬路ひずみ等化の手法について検討し，高い効果を得ることを確認した．

【参考文献】

[1] H. Dedieu, M. P. Kennedy and M. Hasler, “Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits,” IEEE Trans. Cir. Sys., vol. 40, no. 10, pp. 634–641, Oct. 1993.

[2] T. Ushio, T. Innami, and S. Kodama, “Chaos shift keying based on in-phase and anti-phase chaotic synchronization,"' IEICE Trans. Fundamentals., vol. E79-A, no. 10, pp. 1689–1693, Oct. 1996

[3] G. Kolumban and M.P. Kennedy, “Recent results for chaotic modulation schemes,” Proc. IEEE Intl. symp. on Cir. Sys., vol. 3, pp 141–144, May 2001.

[4] A.J. Lawrance and G. Ohama, “Exact calculation of bit error rates in communication systems with chaotic modulation,” IEEE Trans. Circuits and Systems I, vol. 50, no. 11, pp. 1391–1400, Nov. 2003.

[5] R. Bernardini and G.M. Cortelazzo, “A new efficient chaotic modulation scheme,” Proc. IEEE Intl. Conf. on Commun., vol.7 pp. 2236–2240, Jun. 2001.

[6] M. Ciftci and D.B. Williams, “Optimal estimation for chaotic sequences using the Viterbi algorithm,” Conf. Record of the 25th Asilomar Conf. on Sig., Sys. and Comp., vol. 2, pp. 1094–1097, Jun. 2001.

[7] E. Okamoto and Y. Iwanami, “A trellis-coded chaotic modulation scheme,” Proc. IEEE Int'l Conf. Commun. (ICC), WC32-2, 6 pages, Istanbul, Turkey, Jun. 2006.

[8] 唐沢好男, “ディジタル移動通信の電波伝搬特性, ”コロナ社, 2003.

[9] 岡本英二, 岩波保則, “カオス符号化変調方式の伝送効率と復号計算量に関する検討, ”2007 年信学会総合大会, B-5-106, Mar. 2007.

[10] 松岡克宏, 岡本英二, 岩波保則, “LDPC 符号を用いたターボ等化の特性改善に関する研究, ”信学論(B), Vol.J90-B No.4, pp.432-436,April.2007.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
カオス符号化変調方式のターボ符号連接に関する一検討	2008 年信学会総合大会	２００８年３月
カオス符号化変調方式の復号特性解析に関する一検討	電子情報通信学会技術研究報告	２００８年３月
Application of turbo equalization for multimode block-coded modulation	Proc. Int'l. Sym. Wireless Personal Multimedia Commun. (WPMC)	２００７年１２月
Performance Improvement of Turbo Equalization by Concatenating SC/MMSE Equalizer	Proc. Int'l. Sym. Wireless Personal Multimedia Commun. (WPMC)	２００７年１２月
マルチモードブロック符号化変調におけるモード構成の検討	2007 年電気関係学会東海支部連合大会	２００７年９月
カオス符号化変調方式の復号特性に関する検討	2007 年信学会ソサイエティ大会	２００７年９月