カオスダイナミクスの分離を利用したノンコヒーレントカオス通信のための多値変調方式

M-ary Modulation Method Using Separation of Chaotic Dynamics for Noncoherent Chaos Communications

荒井伸太郎 † 西尾芳文 ‡ 山里敬也 ††
† 香川高等専門学校
‡ 徳島大学
†† 名古屋大学

Shintaro ARAI† Yoshifumi NISHIO‡ Takaya YAMAZATO††
†Kagawa National College of Technology
‡Tokushima University
††Nagoya University

1 はじめに

カオスは非周期的であり，理論的には無限周期の系列を生成する事ができる．また，極めてシンプルなモデルからもカオス系列は生成可能であり，ダイナミクスと正確な初期値が与えられれば，指定した先の値を決定する事ができる．このような様々な特徴を活かして，現在，カオスを工学システムに応用する研究が盛んに行われている．特に，カオスを利用した通信システムは，その代表的な応用の 1 つである [1]– [6]．中でも，カオス系列によって変調された信号のみを用いて復調を行うノンコヒーレントカオス通信システムは，カオスの特徴を活かした独特の通信システムとして知られている．ノンコヒーレントシステムを用いた手法としては，Differential chaos shift keying (DCSK) [1] と Optimal receiver [2] が有名である．さらに，効率的なアルゴリズムを用いて，Optimal receiver と同等もしくはそれに近い特性を有する Suboptimal receiver の開発も重要視されている [3]．しかしながら，これらのシステムではカオスの特徴を用いての変復調という制限があるため，一般的な通信システムと比較すると，通信特性は劣ることが知られている．ゆえに，ノンコヒーレント通信の特性向上のためには，カオスの特徴を利用したさらなる工夫が必要である．

我々はこれまでの研究で，ノンコヒーレントカオス通信システムのための，カオスダイナミクスに基づく誤り訂正手法を提案した [7]．一般的なカオス通信システムでは，送信機で 2 値データ (1 bit) をある一定の長さのカオス系列で変調し，受信機でその長さごとに復調を行う．この時，受信機は，各データの変調に用いられたカオス系列のみを用いて復調を行っており，そのデータの前後のカオス系列は考慮していない．私達は，データの前後のカオス系列を同一のダイナミクスから生成された連続するカオス系列として捉え，これをデータを正確に復調するための受信機への付加情報として誤り訂正に利用した．さらに，これを発展させ，カオスダイナミクスの分離を利用した誤り訂正手法も提案した [8]．今，K 個の 2 値データを，K 個の信号ブロックとして伝送する場合を考える．本手法では，送信機側で信号ブロックの順序を故意に並び替え，信号ブロック間で連続するカオスダイナミクスを分離させる．ここで，各ブロックが持つカオス系列の順序は入れ替えないことに注意する．受信機側では，それを元に戻す動作 (再構成) を行い，再構成された系列のカオスダイナミクスを解析する事によって誤り訂正を行う．つまり，カオスダイナミクスの分離と再構成を信号復調の際の付加情報として利用した誤り訂正手法である．本手法を用いてコンピュータシミュレーションを行い，従来手法 (誤り訂正無し) と比較した結果，ビット誤り率 (BER) 特性において，2 ∼ 2.5 dB の利得を得ることができた．この結果から，カオスダイナ

ミクス及びその分離と再構成が，カオス通信システムの信号復調に多大な影響を与える事が分かった．

ここで，カオスダイナミクスの分離に再び注目する．上述した誤り訂正手法では，信号ブロックの順序のみを故意に並び替え，各ブロックが持つカオス系列の順序は入れ替えていない．これは，各ブロックで，1 bit のデータ復調が行えるようにするためである．もし，カオス系列の順序を並べ替えたとしたら，当然の事ながら 1 bit のデータ復調を行うことはできない．これは，先に述べた Optimal receiver や Suboptimal receiver でも同様である．つまり，カオスダイナミクスに基づく連続した系列でなければ，データの復調は不可能であることを意味する．しかしながら，分離させた系列を元に戻すことができれば，データの復調は可能である．この時重要となるのがその並べ替えのパターン数である．系列の並べ替えは系列長 N が長くなるほどそのパターン数も増加する ($N!$ で増加する)．ゆえに，故意に並べ替えた系列を総当たりで元に戻すのは困難である．

本研究では，このカオスダイナミクスの分離と再構成及び並び替えパターン数に注目した，ノンコヒーレントカオス通信のための新たなデータ変復調方式を提案する．本手法では，送受信機間でカオス系列長を分離・再構成可能な複数の並び替えパターンを共有させ，各パターンとデータの対応付けを行う．送信機側では，送信データに対応したパターンを選び，それに従ってカオス系列の並べ替えを行うことでデータの変調を行う．受信機側では，共有しているパターンに従って受信した信号の系列を元に戻す．送受信機間ではデータと並び替えパターンは共有情報であるため，元に戻す際に用いたパターンに対応しているデータが復調されたデータとなる．さらに，本手法では，並び替えパターン数を複数用意することで，多値変調も行うことが可能である．本論文では，提案手法の動作について述べ，コンピュータシミュレーションによる BER 特性の評価を行う．

2　提案する多値変調方式

図 1 に提案する多値変調方式を用いた通信システムのブロック図を示す．本ブロックは送信機，伝送路，受信機と大きく 3 つに分かれている．提案手法では，カオスダイナミクスの分離と再構成にインターリーバとデインターリーバをそれぞれ用いる．今，b bit の多値情報を送信する場合を考えると，インターリーバとデインターリーバはそれぞれ $M = 2^b$ 個必要である．事前に任意のデータをインターリーバとデインターリーバに割り当てておき，m 番のインターリーバで並べ替えられた系列は，m 番のデインターリーバで元に戻るように，送受信機間で割り当てたデータと並べ替えパターンの情報を共有していると仮定する ($m : 0, 1, \cdots, M-1$)．また，各インターリーバの並べ替えパターンと同一のパターンは他のインターリーバで用いないように設定する．

送信機では，カオス写像によって生成されたカオス系列を，送信データに対応したインターリーバで順序を並べ替えることで変調を行う．本研究では，カオス写像に，式 (1) で表される Skew Tent Map を用いる．

$$x_{i+1} = \begin{cases} \dfrac{2x_i + 1 - a}{1 + a} & (-1 \le x_i \le a), \\ \dfrac{-2x_i + 1 + a}{1 - a} & (a < x_i \le 1). \end{cases} \tag{1}$$

ここで，$i = 0, 1, \cdots, N-1$，N はカオス系列長，a は Skew Tent Map の頂点を表すパラメータである．今，送信データが m だとすると，m 番のインターリーバが選択され，カオス系列の順序を並べ替える．カオス写像によって生成された系列のベクトルを $\mathbf{S}$，m 番のインターリーバで並べ替えられた系列のベクトルを $\mathbf{S_m}$ と定義すると以下のように表すことができる．

$$\mathbf{S} = x_0, x_1, \cdots, x_i, \cdots, x_{N-1}. \tag{2}$$

$$\mathbf{S_m} = x_{0,m}, x_{1,m}, \cdots, x_{i,m}, \cdots, x_{N-1,m}. \tag{3}$$

ここで，x_0 はカオス系列の初期値であり，本研究ではランダムに決定している．また，$x_{i,m}$ は m 番のインターリーバで順序を入れ替えられた系列の値を示している．この信号ベクトル $\mathbf{S_m}$ が送信信号系列となる．

送信された信号は伝送路を通って受信機に到達する．本研究では，伝送路でのノイズに相加性白色ガウス雑音 (additive white Gaussian noise: AWGN) を用いる．今，ノイズベクトルを $\mathbf{n}$ とすると，受信系列は，$\mathbf{R} = (r_0,\ r_1,\ \cdots, r_i,\ \cdots,\ r_{N-1}) = \mathbf{S_m} + \mathbf{n}$ と書く事ができる．

受信機では，受信系列をデインターリーバでカオスダイナミクスの再構成を行い，データの復調を行う．本研究では，ノンコヒーレントカオス通信システムを考えているため，受信機は送信機で用いたカオス写像を記録している．しかしながら，送信機側で生成したカオス系列の初期値は記録されていない．つまり，送受信機間で同一のカオス系列を生成する

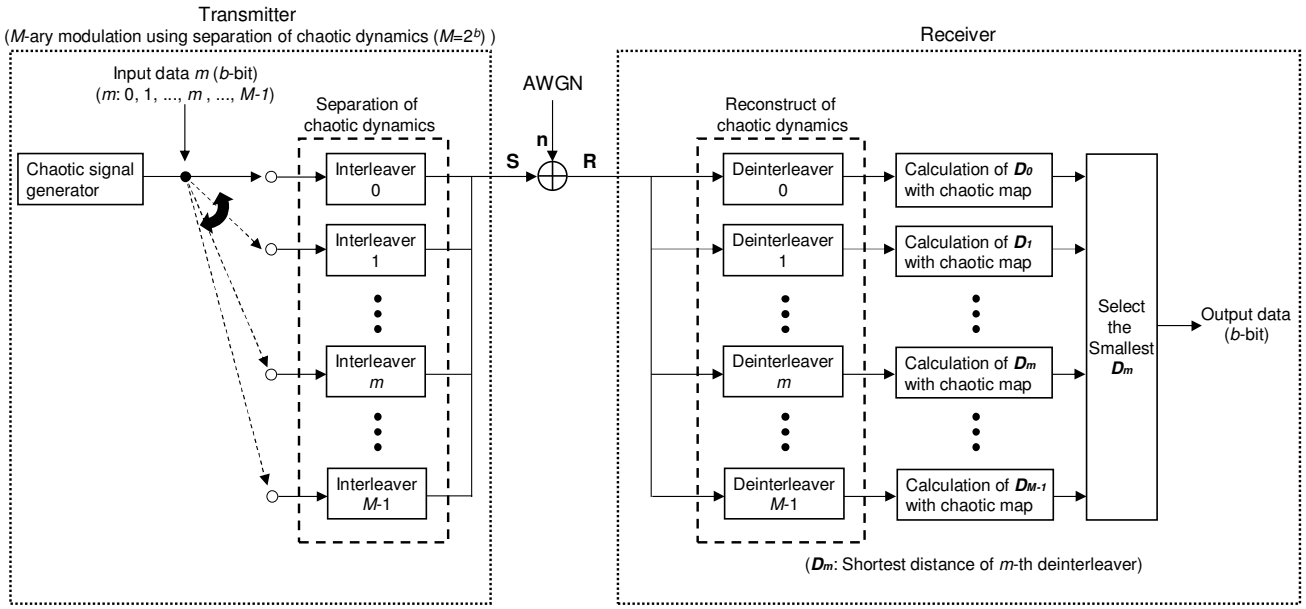


図 1: 提案する多値変調方式を用いた通信システム.

事はできないことを意味する.

データの復調方法について詳しく述べる. まず, 受信系列を受信機が持つ M 個のデインターリーバ全てに与え, M 個の再構成された系列を生成する. m 番のデインターリーバによって再構成された受信系列を以下のように定義する.

$$\mathbf{R_m} \quad = \quad (r_{0,m},\ r_{1,m},\ \cdots,\ r_{i,m},\ \cdots,\ r_{N-1,m}). \tag{4}$$

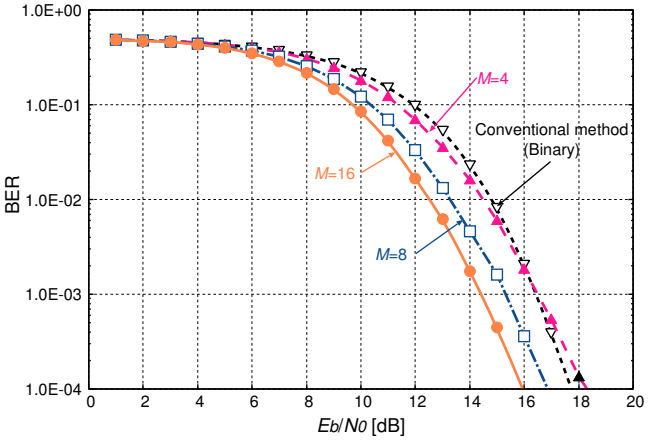
次に, 再構成された受信系列の解析を行い, M 個のデインターリーバの中から 1 つを選択する. ここでの解析とは, 再構成された受信系列の順序がカオスダイナミクスに従って連続した信号となっているかどうか調べることを意味する. デインターリーバには送信機側のインターリーバと同じデータが割り当てられているため, 選択されたデインターリーバに割り当てられているデータが復調データとなる. 本研究では, 系列の解析に私達がこれまでに提案した Suboptimal 検出アルゴリズムを用いる [7]. このアルゴリズムでは, 送信機側で用いたカオス写像と再構成された系列との最短距離を計算する. 最短距離の計算は, 再構成された系列が持つ N_d 個の連続する系列を取り出し, その系列とカオス写像を N_d 次元スペースで表したもので行う $(N_d : 2, 3, \cdots)$. ここで, N_d は系列長 N 以下の値である $(N \geq N_d)$. 本研究ではカオス写像に Skew Tent Map を用いており, これを N_d 次元スペースで表すと, そのスペース上に存在する直線の総数 l は以下の式で表すことができる.

$$l \quad = \quad 2^{N_d-1}. \tag{5}$$

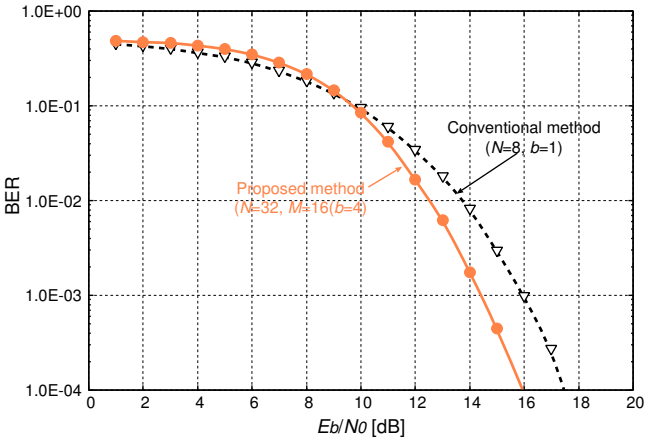
ゆえに, l 本全ての直線との距離を計算し, その中から最も小さい距離を最短距離 D_m とする. 受信系列の系列長 N が, N_d と等しい時 $(N = N_d)$, 最短距離は 1 つだけ計算される. N が N_d より大きい場合 $(N > N_d)$, 受信機は再構成された系列から取り出す位置をずらして, 再度最短距離を計算する. この動作を $N - N_d$ 回行い, 計算された全ての最短距離の総和を, m 番の再構成された系列の最短距離 $\sum D_m$ と決定する. 最後に, M 個の最短距離 $\sum D_m$ の中で, 最も小さい値を選択する. 先に述べた通り, 送受信機間はインターリーバとデインターリーバに関する情報を共有しており, 各インターリーバの並べ替えパターンと同一のパターンは他に存在しない. つまり, 受信系列を元のカオス系列の順序に戻すデインターリーバは 1 つしか存在しない. 解析に用いた最短距離の計算は, 系列の各値がカオスダイナミクスに従って連続する時に最も小さい値になる. ゆえに, 全ての $\sum D_m$ の中で最も小さい値になった時のデインターリーバに割り当てられたデータを復調データと決定する.

3 シミュレーション結果

提案した多値変調方式の性能を, コンピュータシミュレーションによって評価する. シミュレーション諸元を以下に記す. 送信機側において, Skew Tent Map の頂点 a を 0.05, 受信機側において, 最短距離 D_m の計算のために, カオス写像の 4 次元スペース $(N_d = 4)$ を用いる. カオス系列の初期値 x_0 は毎回ランダムに決める. 送受信機で用いるインターリーバとデインタリーバの数は, それぞれ $M = 2^b$ で決まり, 並び替えパターンはランダムに決める. 以上の諸



(a)



(b)

図 2: BER vs. E_b/N_0: (a) $N = 32$, (b) 1 bit あたりの送信エネルギーを等しくした時の比較.

元に基づき，本研究では 2 種類のシミュレーションを行う．1 つ目は，データを 10^4 ビット送信し，$N = 32$ 一定，$M = 4, 8, 16$ に変化させた時の E_b/N_0(1 bit あたりの SNR) に対する BER を求める．2 つ目は，同じくデータを 10^4 ビット送信し，$M = 16E_b/N_0$ 一定にした時の N に対する BER を求める．

1 つ目のシミュレーションの結果を図 2(a) と (b) に示す．図 2(a) は，$N = 32$ 一定にした時の E_b/N_0 に対する BER 特性の結果である．M は $4, 8, 16$ の 3 つを選び，それぞれを提案手法の結果として表示している．また，同図には比較のため，Suboptimal receiver の結果を従来手法の 2 値データ (Binary) として表示している．結果から分かる通り，M の値が増加するにしたがって，BER 特性が向上しているのが分かる．今，BER$= 1 \times 10^{-4}$ に注目すると，従来手法ではこの値を達成するのに必要とする 1 bit あたりの SNR は 18 dB である．一方，提案手法では $M = 16$ の時，この値を達成するのに必要とする 1 bit あたりの SNR は 16 dB である．すなわち，提案手法は $M = 16$ の時，送信エネルギーを 2 dB 節約することができると言える．

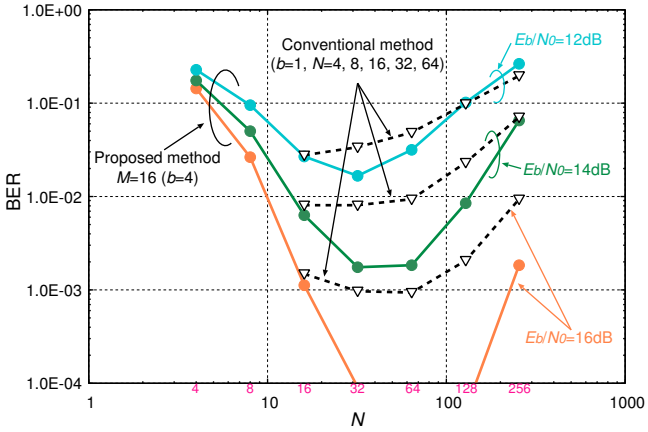


図 3: BER vs. N ($M = 16$).

図 2(b) は，1 bit あたりの送信エネルギーを提案手法と従来手法とで等しくした時の E_b/N_0 に対する BER 特性の結果である．提案手法が $N = 32, M = 16$ ($b = 4$) の場合，従来手法は $N = 8$ の時，両者の 1 bit あたりの送信エネルギーは等しくなる．結果より，提案手法では従来手法と比較して，最大で約 1.4 dB の利得が得られることが確認できる．特性が向上した理由として，デインターリーバでのカオスダイナミクスの再構成の効果が働いたためであると考える．カオスダイナミクスの再構成において，元のカオス系列に戻すことができるデインターリーバは 1 種類のみであり，それ以外は系列の順序をさらに掻き乱すこととなる．送信系列は元々インターリーバによって順序が並べ替えられている．それを受信機側でさらに順序を並び替えたことにより，元のカオス系列が持っていたカオスダイナミクスの特性がほとんど失われてしまったためだと推測する．これにより，正しい順序に戻ったカオス系列との差異が強く表れ，復調特性の向上につながったと考える．

次に，図 3 に，2 つ目のシミュレーション結果の $M = 16$ 及び E_b/N_0 を一定にした時の N に対する BER 特性を示す．一定にする E_b/N_0 は，12，14，16 dB の 3 つを用い，系列長 N は 4 ～ 256 まで変化させて BER を計測した．比較のため，従来手法である Suboptimal receiver の結果を，1 bit あたりの N を等しくして表示している．例えば，提案手法の N が 16 の場合，$M = 16$ では 1 bit あたりの N は 4 であるため，$N = 4$ の従来手法の結果と比較する．結果から，$N = 32, 64, 128$ の時，提案手法の BER 特性が従来手法と比較して明らかに向上している事

が分かる．特に，$E_b/N_0 = 16$ dB の時，提案手法の BER 特性は 1×10^{-4} を下回っており，従来手法よりも BER は一桁以上改善している．この結果からも，提案手法が用いているカオスダイナミクスの分離・再構成の有効性が確認できる．

しかしながら，N が小さい領域及び大きい領域 ($N = 256$) で提案手法の BER 特性が劣化しているのが分かる．この原因については以下のように考察する．まず，N が小さい領域での特性劣化の原因として，N が小さくなったことによる，インターリーバの並べ替えパターン数の減少が考えられる．例えば，$N = 4$ ではパターン数は $4! = 24$ しかない．パターン数が少ない場合，カオス系列のカオスダイナミクスの分離が十分に行われないため，再構成された系列の解析において判定誤りが増加したと考えられる．次に，N が大きい領域での特性劣化は，1 bit あたりの系列が長くなったことが，再構成された系列の解析で行う最短距離の計算に影響したためと考えられる．受信系列は伝送路でノイズが加えられるため，正しいデインターリーバによって元の順序に戻ったカオス系列でも，最短距離はゼロにはならず，誤差が生じてしまう．また，先に述べたとおり，$N > N_d$ の場合，受信機は再構成された系列から取り出す位置をずらしながら最短距離を計算し，最終的に $N - N_d$ 個の最短距離の総和を判定に用いる．N が大きいほど最短距離の計算数も多いため，最短距離の計算誤差がこの計算過程で蓄積されてしまったと推測する．ゆえに，計算誤差の蓄積が判定誤りに影響したと考える．以上の結果から，提案手法には，系列の並び替えパターン数と 1 bit あたりの系列長の最適値が存在し，これらを正しく設定する必要があることが分かった．

4 まとめ

本研究では，カオスが持つ特徴の 1 つであるカオスダイナミクスに着目し，カオスダイナミクスの分離を利用した多値変調方式を提案した．シミュレーションを行い，提案手法と従来手法と比較した結果，M を増加させることによって，送信エネルギーの節約が可能であることが確認できた．さらに，1 bit あたりの送信エネルギーを等しくして比較した結果，$N = 32, M = 16$ の時，最大で約 1.4 dB の利得を提案手法は得ることができた．ゆえに，カオスダイナミクスの分離と再構成は，多値変調方式に用いるのに有効な手段であると言える．

参考文献

[1] G. Kolumbán, B. Vizvári, W. Schwarz, and A. Abel, “Differential chaos shift keying: A robust coding for chaos communication,” *Proc. NDES’96*, pp. 87-92, Jun. 1996.

[2] M. Hasler and T. Schimming, “Chaos communication over noisy channels,” *Int. J. Bifurcation and Chaos*, vol. 10, no. 4, pp. 719-736, Apr. 2000.

[3] M. Hasler and T. Schimming, “Optimal and suboptimal chaos receivers,” *Proc. IEEE*, vol. 90, Issue 5, pp. 733-746, May 2002.

[4] W. M. Tam, F. C. M. Lau and C. K. Tse, *Digital Communications with Chaos*, Elsevier Science & Technology, 2006.

[5] J. C. Fang and C. K. Tse, *Reconstruction of Chaotic Signals with Applications to Chaos-Based Communications*, Tsinghua University Press and World Scientific Publishing Co. Pte. Ltd., 2008.

[6] G. Kaddoum and F. Gagnon, “Error correction codes for secure chaos-based communication system,” *Proc. QBSC’10*, pp. 193-196, May 2010.

[7] S. Arai, Y. Nishio and T. Yamazato, “Error-Correcting Scheme Based on Chaotic Dynamics and its Performance for Noncoherent Chaos Communications,” *NOLTA, IEICE*, vol. 1, no. 1, pp. 196-206, Oct. 2010.

[8] S. Arai, Y. Nishio and T. Yamazato, “Improvement of Error-Correcting Method Based on Chaotic Dynamics for Noncoherent Chaos Communications,” *Proc. NOLTA’12*, pp. 801-804, Oct. 2012.