非線形力学系としての大容量無線通信
～ その特性と性能改善 ～
(Nonlinear dynamics in high-capacity wireless communication systems)

2020 年 3 月

迫田 和之

目 次

第1章　序論

1.1　研究背景

一般に，自然科学や社会科学において考察する対象を系と呼ぶ．系の状態を表す物理量である状態変数が時間とともに変化するとき，系は動的で，その変化は数学モデルにより記述される．この数学モデルを力学系と呼ぶ．例えば，物体の運動では，独立変数が時間，状態変数が物体の位置や速度で，その時間変化は運動方程式に従う．また，力学系の解析では，状態変数で張られた空間（相空間）を用いて，状態変化を議論する．

力学系は線形の時間発展方程式で記述される線形力学系と，非線形の時間発展方程式で記述される非線形力学系に分けられる．線形力学系の時間変化は指数的（三角関数を含む）で，時間的に複雑な振る舞いを示さない．逆に言うと，複雑な振る舞いは非線形力学系から生じる．つまり，自然現象や社会現象の複雑な振る舞いは非線形力学系で記述される．例えば，電気回路の発振回路が示す挙動は van der Pol 方程式 [1–3] で記述され，ある条件下での生物の個体数変動はロジスティック写像 [1–3] で記述される．どちらも非線形力学系である．

理学の分野では，力学系を数理的 · 実験的に解析し，その特性を調べ，元の系で起こる現象を理解する研究がなされている．例えば先の van der Pol 方程式は非線形な抵抗特性を持つ発振回路であり，その強さを表すパラメータをもつ．その値が変化すると，系の動的振る舞いが変わる．このパラメータがある一定以下のとき，状態変数が時間発展とともに状態変数で張られた空間中で，ある点に収束する．このような点を安定固定点という．パラメータがある値より大きくなると，時間の経過とともにある周期的な軌道に近づいていく．この軌道をリミットサイクルという．このように安定固定点やリミットサイクルのような近傍の軌道を引きつける性質のある解をアトラクター（attractor）と呼ぶ [1]．非線形力学系には種々のアトラクターが存在し，時間の経過とともに状態変数がアトラクター上を運動するようになる．他にも，時間が離散的になるがロジスティック写像は，パラメータとして非線形性の強さを左右する繁殖率を持ち，その値に応じ個体数がある値（固定点）に収束，2 つの値を交互にとるような周期運動をするといった時間変動を示す．これらは，時間とともに個体数が一定数に落ち着く，周期的に個体数が増減するといった実際の系の振る舞い

と対応する．また，パラメータの値によっては，一見乱雑な振る舞いをすることも知られている．これはカオスと呼ばれており，決定論的力学系であるにもかかわらず非周期的な振る舞いをするものである [1–3]．カオスを示す場合，近接した 2 点の初期値から出発した軌道が時間経過に伴い指数関数的に離れる．これは初期値に対する鋭敏な依存性，すなわち軌道不安定性という．その乖離度の指標となるリアプノフ指数がカオスを特徴づける重要な量である．なお，このロジスティック写像を多数結合させた結合写像系は，同時に多くの異なるアトラクターを持つ．この系に限らず，大自由度非線形力学系はこのような振る舞いを示す．この場合，初期値によって至るアトラクターが変わる．それぞれのアトラクターに至る初期値の集合をベイスン（basin）と呼び，その構造を調べることや，アトラクターに至る時間を調べることなど多くの研究がなされている [4, 5]．このように現象を記述する力学系を調べることで，種々の振る舞いが起きる条件や特性を知ることができる．

工学の分野では，発振器やモーターなど人が利用するために作ったものが，結果的に非線形力学系に従うというだけでなく，意識的に非線形力学系を利用して有用な機能を実現するといった応用もなされている．例えば，ニューラルネットワークは，脳の神経回路網を数理モデル化した非線形力学系 [6–8] で，パターン認識などに用いられる．最近では物体認識による自動車の自動運転への応用や，画像の識別による医療診断技術への応用が検討されている [9, 10]．また，ノイズを含むデジタル画像の修復などの推定問題では，一定の規則による繰り返し計算を用いて徐々にノイズの少ない元の画像を推定する方法が用いられている [11–15]．この繰り返し計算過程は，繰り返し回数を独立変数（時間），画像データを状態変数とする非線形写像と見なすことができる．繰り返し計算（写像）により状態変数が固定点に至ることが，推定問題を解くこと（画像修復）にあたる．これは先に述べた，時間経過とともに状態変数がアトラクターに収束していくことにあたる．この種の繰り返し計算を用いた推定には EM（Expectation Maximization）アルゴリズム [11–13] や BP（Belief Proapgation）法 [14,15] などが用いられており，その手順は少し混み入っているが，多変数の大自由度非線形力学系と見なすことができる（ただし，このような繰り返し計算を非線形力学系と見なす研究は殆どなされていない）．このように工学の分野では，非線形力学系を応用することで大きな成果を上げている．

そこで本研究では非線形力学系としての無線通信に着目する．無線通信では受信信号から送信信号を推定する復号という過程があり，通信容量を増大させた大容量無線通信（大規模 MIMO，大規模 Multiple Input Multiple output）の復号法として BP 法を用いた繰り返し推定法（BP 復

号）が提案されつつある [16–23]．BP 復号を用いた大規模 MIMO は 3 章でみるように画像修復での例と同様，大自由度非線形力学系である．BP 復号は，従来の復号法では大きな問題となる計算量を大きく削減し，高い推定精度を示す可能性があると報告されている．本研究では，非線形力学系の立場から BP 復号を用いた大規模 MIMO を詳細に解析し，その問題点を明らかにし，その解消と性能向上の可能性を探る．

また無線通信分野において，通信容量に加えて重要なものは情報安全性である．そこで，BP 復号を用いた大規模 MIMO にも適切な情報安全性の仕組みを導入する必要がある．無線通信では既存のセキュリティと併用できるカオス通信（カオスを示す非線形写像を用いて，送信信号を暗号化する秘匿通信）が注目されている [24–31]．本研究では先の BP 復号にカオス通信を加えることを検討する．既にカオス通信を MIMO に導入したカオス MIMO [30, 31] も提案されているが，後に示すように，先に述べた BP 復号とうまく整合せず（推定することができない），大規模 MIMO では使えない．そこで本研究では，カオス MIMO の暗号方法を力学系の特性の視点から修正したカオス暗号を提案する．以上を通して，大規模 MIMO における，BP 復号とカオス暗号を導入することを提案し，力学系としての特性を明らかにするとともに工学的有用性を明らかにする．

1.2 論文の構成

本論文は，BP 復号を用いた大規模 MIMO を，非線形力学系としての特性と通信性能改善の面から研究したもので，主に以下の 2 つの研究をまとめたものである．

1. BP 復号が大自由度非線形写像系であることを示し，先行研究で不完全であった点を取り除き，その力学系としての性質を調べ，復号の問題点の解消と性能向上の可能性を探る．

2. カオス MIMO で提案されているカオス暗号が BP 復号に適合しない原因を，BP 復号とカオス暗号の力学系の挙動から明らかにし，それを基に，BP 復号に適合するカオス暗号を構築する．

1 章では，研究背景について述べる．

2 章では，本研究で取り扱う無線通信方式である MIMO の枠組みを説明し，本研究に関連の深いカオス MIMO と BP 復号について非線形力学系の視点から詳細に紹介する．

3 章では，BP 復号が大自由度非線形写像系であることを指摘し，先行研究での BP 復号で不完全であった点を取り除き，BP 復号での問題点の解決と，繰り返し計算による状態変数の振る舞いを詳細に調べる．BP 復

号の不完全な点は，繰り返し計算の際に評価する残留干渉成分の効果を見積もる方法が確立されていないことである．多くの研究では送信した信号すなわち正解の情報が用いられていて，実用できない形式である．そこで，力学系の安定固定点に至ることが復号にあたるように残留干渉成分を力学系の物理量で評価することで，実際の無線通信で実現できる方法を提案し，数値実験で性能を確認する．また，BP 復号の力学系を調べ，どのような種類の振る舞いがどの程度存在するかを把握し，性能との関係を探る．

4 章では，カオス MIMO でのカオス暗号が BP 復号で復号できないことを明らかにし，その解析に立脚して BP 復号に適合するカオス暗号（BP 適合カオス暗号）を構築する．しかし，その BP 適合カオス暗号では，BP 復号が機能するが，カオス暗号化を行わない場合と比べ推定精度がかなり低くなる．その原因を明らかにし，問題を回避する改良 BP 適合カオス暗号を提案する．それにより，無線通信で要求される推定精度の基準値を満たすことができ，BP 復号を用いた大規模 MIMO の情報安全性の向上が可能になると考えられる．

5 章では，本研究の結果をまとめ，今後の課題と展望を述べる．

第2章　先行研究

大自由度非線形力学系の立場から大容量無線通信を研究したものは，ほとんどない．この章では，力学系としての構造を整理しつつ，MIMO とカオス暗号および BP 復号を紹介する．

2.1　無線通信の変遷と現状

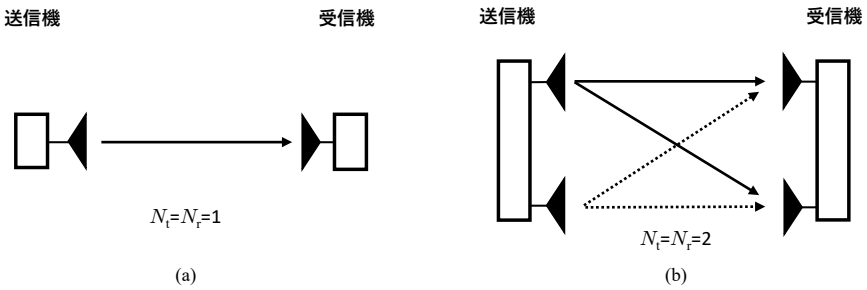


図 2.1: (a) SISO システム概要図．(b)MIMO システム概要図．
N_t，N_r はそれぞれ送信アンテナ数と受信アンテナ数．

携帯電話の第 3 世代（3G）以前の無線通信は，送受信アンテナを 1 本づつ用いた無線通信（Single Input Single Output，SISO）システム（図 2.1（a））で構成されていた（以下，送信アンテナ数を N_t，受信アンテナ数を N_r とする）．その後，携帯電話などの移動体通信が急速に普及するにつれ無線通信での通信量が増加し，通信容量を向上させる必要性が生じた．通信容量を向上させる方法として，使用する周波数帯域を増加させる方法があるが，使用可能な周波数資源は限られているので適切でない．他にも，送信電力を大きくする方法もある．しかしながら，送信電力を大きくすることにより得られる通信容量向上の恩恵は小さく，さらに，無線通信端末の小型化によりバッテリーの容量に限りがあるため，送信電力を大きくすることは難しい．そのため，周波数帯域や送信電力を大きくすること以外に通信容量を向上させる方法が求められている．そこで，複数の送受信アンテナを使用した MIMO が提案された（図 2.1（b））[32,33]．MIMO は，

携帯電話の第 4 世代（4G）や無線 LAN などの無線通信で広く実用化され，通信容量の向上に大きく寄与した．しかし，無線通信での高画質動画伝送に代表される大容量通信サービスの普及や IoT（Internet of Things）技術の発展に伴い多数の機器が無線通信で繋がることにより，今後，さらなる通信容量の向上が求められている．そのためには 2 – 4 本程度であった MIMO の送受信アンテナ数を 10 – 100 本程度に増加させ通信容量を向上させた大規模 MIMO の適用が考えられる [34–39]．これにより通信容量を向上させることが可能だが，単純な復号法である MLD（Maximum Likelihood Decoding）では，送信信号の全てのパターンの中から最も妥当なものを探索するため，$2^{N_{\mathrm{t}}}$ に比例する計算量が必要で現実的なものでない．そこで復号の計算量を削減するために，QR 分解を用いて MLD の計算量を削減する方法 [40,41] や繰り返し推定を用いる方法 [16–23,42–45] が提案されている．中でも BP 法を用いた繰り返し推定法が，現実的な計算量で高い推定精度を示す可能性がある [16–23]．

また，多数の機器が無線通信で繋がることにより電波盗聴の機会が増大するため，情報安全性の強化も重要である．無線通信で情報安全性を向上させる方法には，AES（Advanced Encryption Standard）や WEP（Wired Equivalent Privacy）などの通信プロトコルの上位レイヤを対象とし暗号化する技術が多かったが，近年下位レイヤである物理レイヤでの暗号化も重要視されはじめている．物理レイヤでの秘匿性向上法は，他のレイヤの暗号化を排他的に扱うことなく，既存セキュリティのさらなる強化が可能である．物理レイヤでの暗号化では，情報伝搬に用いる電磁波の位相や大きさを特定のルールに従い乱雑に置き換え情報の読み取りを防ぐ手法 [24–31] が多く報告されている．その中でも，カオスを示す写像（カオス写像）に基づき電磁波の位相や大きさを決定し送信信号を生成する，カオス通信が注目されている [24–31]．カオス通信をさらに発展させ MIMO と組み合わせたカオス MIMO という方式もあり，カオス写像と畳み込み符号を組み合わせ情報の秘匿性と高い伝送品質を備えたカオス通信として提案されている [30,31]．このような中で，本研究では BP 復号を用いた大規模 MIMO とカオス暗号化を非線形力学系の立場から研究する．

2.2 MIMO

ここでは本研究で無線通信として取り扱う MIMO の概略を紹介する．

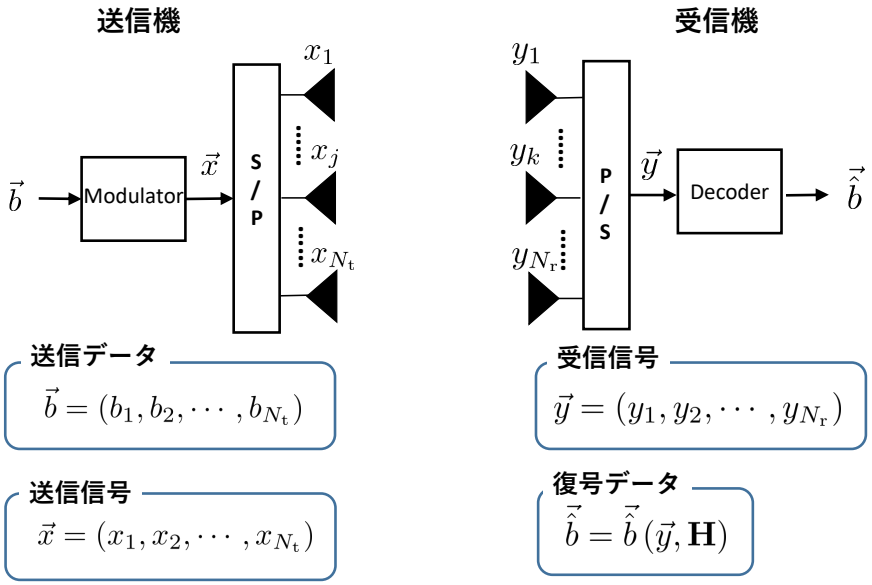


図 2.2: MIMO 概要図.
Modulator が変調器，S/P が直並列変換器，Decoder が復号器，P/S が並直列変換器で，N_t 本の送信アンテナと N_r 本の受信アンテナを持つ無線通信システム.

2.2.1 送信機

MIMO の送信機は，変調器，直並列変換器と N_t 本の送信アンテナで構成される（図 2.2）．送信データは，N_t 個のビット列

$$\begin{aligned} &\vec{b} = (b_1, b_2, \cdots, b_{N_t}), \\ &b_j \in \{0, 1\}, j = 1, 2, \cdots, N_t, \end{aligned} \tag{2.1}$$

で b_j を電磁波の位相 θ_j に

$$\theta_j = \begin{cases} 0, & (b_j = 1) \\ \pi, & (b_j = 0), \end{cases} \tag{2.2}$$

と変調させ，

$$\begin{aligned} &\vec{x}(\vec{b}) = (x_1, x_2, \cdots, x_{N_t}), \\ &x_j = \exp(i\theta_j), i = \sqrt{-1}, \end{aligned} \tag{2.3}$$

を送信する．この変調方法を BPSK（Binary Phase Shift Keying）と呼ぶ．なお，x_j を送信シンボルと呼び，直並列変換器により送信シンボルをそれぞれ送信アンテナに 1 つずつ割り当て，電磁波として同時刻同周波数で送信する．

2.2.2 通信路

送信された電磁波は空間中を伝搬し N_{r} 本の受信アンテナで受信され，受信信号は

$$\vec{y} = \mathbf{H}\vec{x} + \vec{n}, \tag{2.4}$$

と表せる．ここで

$$\mathbf{H} = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1N_{\mathrm{t}}} \\ h_{21} & h_{22} & \dots & h_{2N_{\mathrm{t}}} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N_{\mathrm{r}}1} & h_{N_{\mathrm{r}}2} & \dots & h_{N_{\mathrm{r}}N_{\mathrm{t}}} \end{pmatrix}, \tag{2.5}$$

は通信路行列である．$\mathbf{H}$ の要素 h_{kj} は送信シンボル x_j が k 番目の受信アンテナに届くまでの通信路情報（Channel State Information，CSI）で，本研究ではレイリーフェージングモデルを仮定し（詳細は補足 A を参照），通信路行列 $\mathbf{H}$ の要素 h_{kj} は平均値 0, 分散 1 の時間的 · 空間的に独立で複素ガウス分布に従う乱数とする [32, 33]．また，

$$\vec{n} = (n_1, n_2, \cdots, n_{N_{\mathrm{r}}}), \tag{2.6}$$

は雑音で，n_k は時間的にもアンテナ間でも相関のない平均 0，分散 σ_{n}^2 の複素ガウス分布 $\mathcal{CN}\left(0, \sigma_{\mathrm{n}}^2\right)$ に従う乱数とする．ここで $k = 1, 2, \cdots, N_{\mathrm{r}}$ である．

2.2.3 受信機

受信機では受信信号 $\vec{y}$ から送信データ $\vec{b}$ を推定する（これを復号という）．つまり復号したデータ $\hat{\vec{b}}$ は $\vec{y}$ と $\mathbf{H}$ の関数

$$\hat{\vec{b}} = \hat{\vec{b}}\,(\vec{y}, \mathbf{H}), \tag{2.7}$$

である．なお，ここで受信機側では $\mathbf{H}$ を既知（推定できている）とする[1]．MIMO で一般に用いられる復号法は MLD で，復号データ $\hat{\vec{b}}$ は

$$\hat{\vec{b}} = \arg\min_{\vec{b}} \|\vec{y} - \mathbf{H}\vec{x}(\vec{b})\|^2, \tag{2.8}$$

[1]本研究では，受信側で CSI を既知としているが，実際の通信環境では CSI を推定する過程がある．つまり，受信側でマルチパスによるフェージング現象に起因する受信信号の大きさと位相の変動を推定する．そのため一般的には送信信号を送る前に送信側からパイロット信号を送信し，受信側ではパイロット信号から CSI を推定する．このパイロット信号はあらかじめ送信側と受信側でどのような信号を使用するかを決めておく．

より定まる（詳細は補足 B を参照）．ここで $\|\vec{a}\|$ は複素ベクトルのノルム，$\arg\min_{\vec{b}}\{\cdot\}$ は全ての $\vec{b}$ の中で $\{\cdot\}$ を最小とする $\vec{b}$ である．MLD は MIMO での推定精度の面で優れており，一般的な手法として採用されている．しかし，起こりうる全ての送信ビットの候補を探索するため，2^{N_t} に比例する計算量が必要になり，大きな N_t では実用的でない．

2.2.4 MIMO での通信容量

通信容量とは，1 秒，1Hz 当りに送ることのできるビット数であり，SISO での通信容量はシャノンにより，

$$C_{\mathrm{SISO}} = \log_2\left(1 + \frac{P}{\sigma_\mathrm{n}^2}\right)\ [\mathrm{bit/sec/Hz}], \tag{2.9}$$

で定義される [32, 33]．ここで P は送信電力である．式（2.9）によると，通信容量を向上させる方法として送信電力を大きくする方法がある．しかしながら，式（2.9）で示されるように，送信電力を大きくすると通信容量は対数的にしか増加しない．送信電力の増加により通信容量を増加させるためには多大な電力が必要である．

そのため送信電力を大きくすること以外に通信容量を向上させる方法が必要になる．それに応えるのが複数の送受信アンテナを使用した MIMO である（図 2.1（b））．送受信アンテナ数 $N_\mathrm{t} = N_\mathrm{r}$ の MIMO の通信容量は次式で表される [32, 33]．

$$C_{\mathrm{MIMO}} = \log_2\left[\det\left(\mathbf{I} + \frac{P}{N_\mathrm{t}\sigma_\mathrm{n}^2}\mathbf{H}\mathbf{H}^H\right)\right]\ [\mathrm{bit/sec/Hz}], \tag{2.10}$$

ここで，$\mathbf{I}$ は単位行列，$\det(*)$ と $*^H$ はそれぞれ $*$ の行列式とエルミート転置とする．$\mathbf{H}$ について平均した通信容量はアンテナ数に比例して増加する [32, 33]．

2.3 カオス暗号

2.3.1 カオス写像

カオスとは周期外力の入った振子や熱対流のモデルであるローレンツ系など決定論的力学系から生じる非周期運動を指す．中でも昆虫の個体数変動のモデルであるロジスティック写像は最も有名なカオスを生成する写像力学系として，カオスに関する教科書には必ずといっていいほど紹介されている．本研究で用いるカオス暗号では，そのロジスティック写像を用い

るため，ここで簡単に紹介する．ロジスティック写像は，初期値 $x_0 \in [0,1]$ とし

$$\begin{aligned} x_{n+1} &= f(x_n) \\ &= a x_n (1 - x_n), \\ n &= 0, 1, 2, \cdots, \end{aligned} \tag{2.11}$$

で表される．パラメータ a は $0 \leq a \leq 4$ であり，この値によって周期運動やカオスを示す．特徴的な振る舞いをする $3 \leq a \leq 4$ の分岐図を図 2.3 に示す．

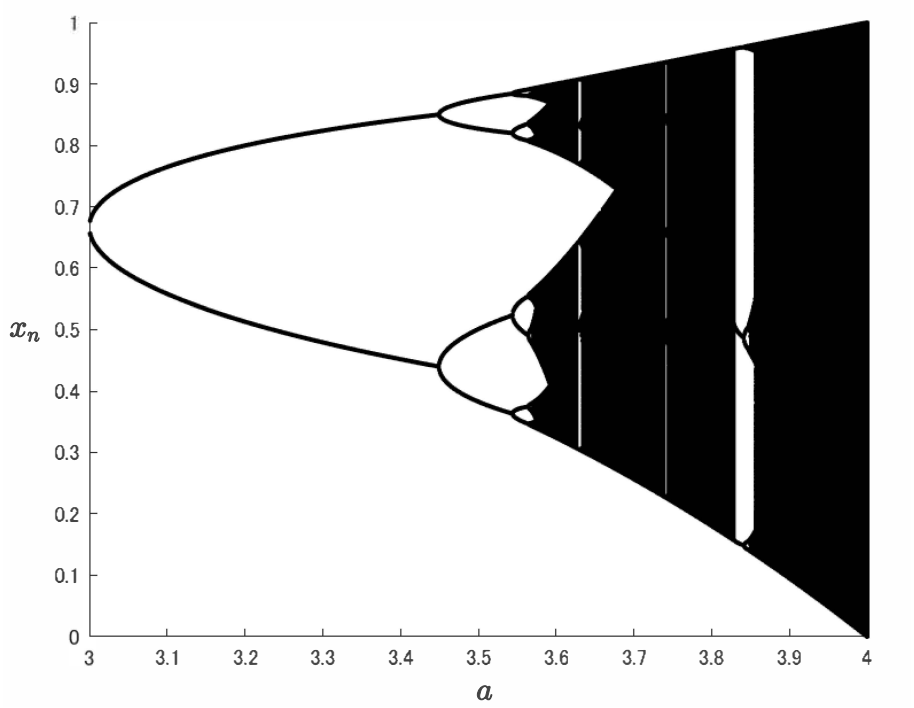


図 2.3: ロジスティック写像の分岐図．
各 a の値について，x_n,（$101 \leq n \leq 10000$）をプロットしたもの．a の刻み幅は 0.001 で $3 \leq a \leq 4$，初期値 x_0 は $[0,1]$ の中からランダムに選んだ．$a = 3.2$ では x_n は 0.5130，0.7995 を交互にとり，2 周期運動を示す．$a = 3.5$ では x_n は 0.5009，0.8750，0.3828，0.8269 を順にとり，4 周期運動を示す．$a = 4$ 付近のように点が連なっているように見えるところでは x_n が非周期運動を示す．$a = 3.83$ 付近では x_n は，3 つの値を順にとり，3 周期運動を示す．

分岐図はパラメータ a によって変わる x_n のアトラクターを示している．図 2.3 の $3 \leq a \leq 3.57...$ の範囲では 2 周期の軌道から始まり a が大きくなるにつれて，周期が倍になっていく様子が見られる．これを周期倍分岐と

呼び，周期運動からカオスへ至る典型的な分岐現象である．$3.57... \leq a \leq 4$ はカオス領域と呼ばれており，カオスや様々な周期の安定な運動がある．非周期運動であるカオスは軌道が不安定で，近接する 2 つの軌道をみると，時刻 n での 2 つの差 δx_n は，初期のわずかな差 δx_0 が時間発展とともに急激に拡がる（図 2.4）．図 2.5 はその振る舞いを示し，写像を経るとその差が拡がっており

$$|\delta x_n| \sim |\delta x_0| \exp(\lambda n), |\delta x_0| \ll 1, \tag{2.12}$$

と振る舞う．図 2.5 の縦軸は，$|\delta x_n|$ の対数を取っているため，その傾きが λ である．ここで

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N} \log |f'(x_n)|, \tag{2.13}$$

で表され，リアプノフ指数と呼ばれる．カオスのとき，λ は正となり δx_n が指数関数的に拡がり，この性質を初期値鋭敏性と呼ぶ（λ が負のときは δx_n が小さくなり，x_n は安定なアトラクターに至ることを意味する）．つまり，リアプノフ指数は初期値鋭敏性の強さを表す量である．後に示すカオス暗号ではカオス領域の $a = 3.91, \lambda = 0.5498$ を使用し，カオスの初期値鋭敏性の特性を利用することで暗号を可能とする．なお，図 2.3 では，$a = 3.83$ 付近で 3 周期運動を示しており，カオス的な挙動はおきない（このようなパラメータ領域は周期窓と呼ばれる）．このような窓は大小無数にあり，ロジスティック写像をカオス暗号に使うためには周期窓を避ける必要がある．

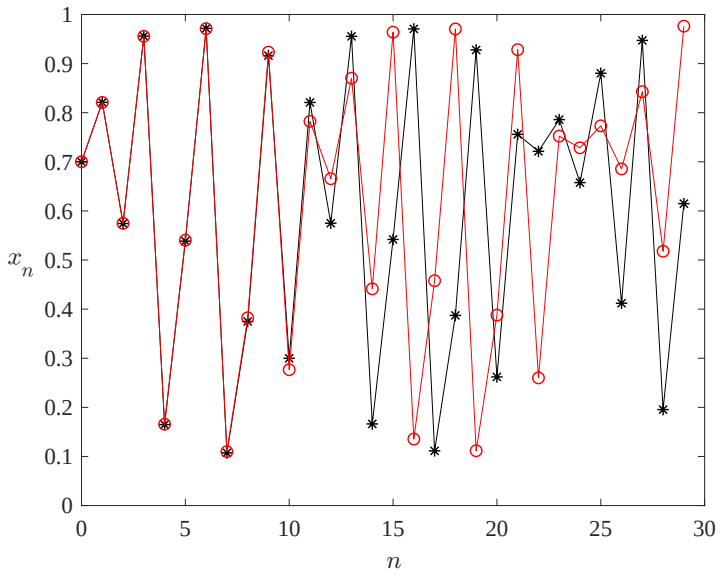


図 2.4: ロジスティック写像で初期値がわずかに異なる 2 軌道 x_n，x'_n の振る舞い．
$a = 3.91$，初期値 $x_0 = 0.7$（アスタリスク），$x'_0 = 0.7001$（丸）である．

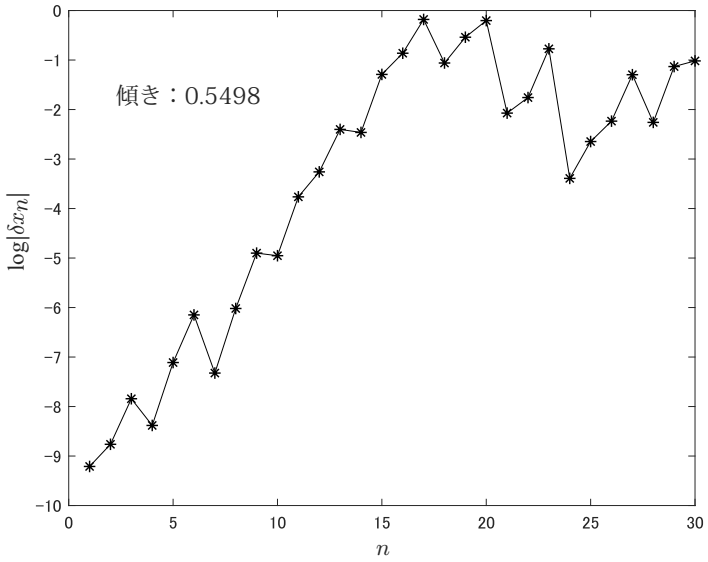


図 2.5: 図 2.4 の 2 軌道の差の拡がり．
$\delta x_n = x_n - x'_n$ である．

2.3.2　カオス通信

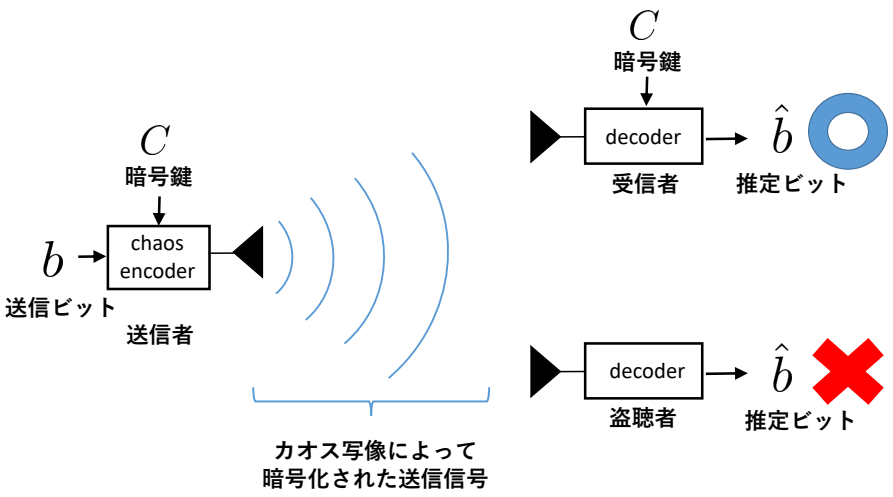


図 **2.6:** カオス通信概要図.

カオス通信とは，カオス写像を用いて送信信号を変調すること（カオス暗号）により，情報を暗号化する通信方法である（図 2.6）．送信側では送信ビットと暗号鍵を元に変調器でカオス写像を用いて変調し送信する．受信側では受信信号，暗号鍵とカオス写像を用いて送信ビットを推定する．このカオス通信は，暗号鍵と用いたカオス写像を知っている受信者でなければ送信ビットを得ることができない．変調規則すなわちカオス写像が公になっていても，正規の受信者のみが暗号鍵を所持していれば，送信者との間で秘匿通信が可能となる．

カオス通信の仕組み

ここでカオス通信の基本的な仕組みを紹介する．送信側では，送信ビット b と暗号鍵 C を用いて複素数の初期値

$$x_0 = x_0\left(b, C\right), \tag{2.14}$$

を生成する．そしてカオス写像 $f(\cdot)$ で l 回写像させた

$$x(b, C) = f^l\left(\mathrm{Re}[x_0(b, C)]\right) + i f^l\left(\mathrm{Im}[x_0(b, C)]\right), \tag{2.15}$$

を送信する．受信側での受信信号 y は，送信信号 x，通信路情報 h とノイズ n により

$$y = hx + n, \tag{2.16}$$

となる．復号データ $\hat{b}$ は MLD を用いて

$$\hat{b} = \arg\min_{\check{b}} \| y - hx\left(\check{b}, C\right) \|^2, \tag{2.17}$$

と得られる．この過程からわかるように，受信側で暗号鍵 C を持っていなければ受信信号を復号することができない．また，真の暗号鍵 C に近い鍵 C' を所持していたとしても，カオス写像の特性である初期値鋭敏性により $x(\check{b}, C)$ と $x(\check{b}, C')$ が全く異なるため，受信信号を正しく復号することができない．さらに，同様の性質により，異なる 2 つの送信ビット b, b' が十分に近くても，生成される送信信号 x，x' が全く異なるため，受信信号 y，y' を傍受しても，元の送信ビットが近いことがわからない．これらの性質を用いて，通信の秘匿性を高めている．

2.3.3 カオス MIMO

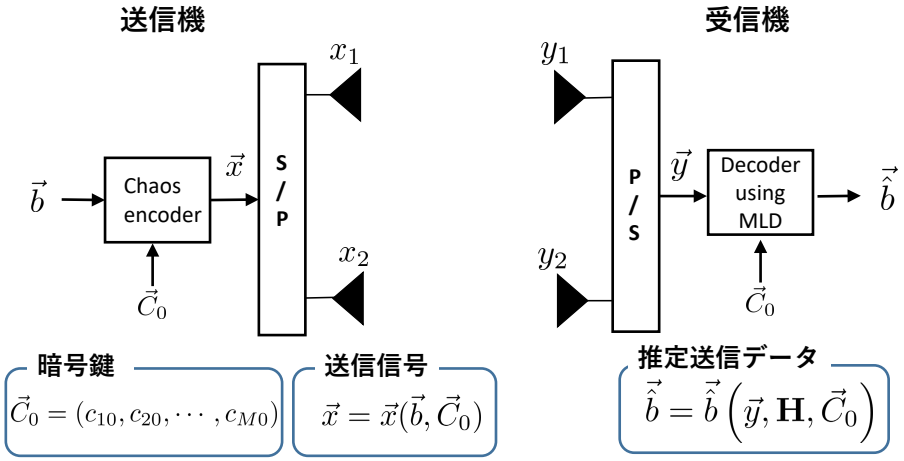


図 **2.7:** カオス MIMO 概要図.

カオス MIMO は，カオス暗号に畳み込み符号を組み込み，MIMO に導入したものである [30]．畳み込み符号は，電気通信の誤り訂正符号の一種である．1 つの送信シンボルに複数の送信ビット情報を含ませることで，送信シンボル間に相関を与え，その相関を利用して誤り訂正を行う．

図 2.7 は，その模式図で，暗号鍵 $\vec{C}_0$ を送受信側で共有する．受信側はこの鍵を用いて暗号化された信号を復号する．暗号鍵を保持していない第三者は受信信号を傍受しても復号することが困難となるため秘匿通信となる．カオス MIMO の詳細は以下の手順である．

M 個の暗号鍵を

$$\begin{aligned} \vec{C}_0 &= [c_{10}, c_{20}, \cdots, c_{M0}], \\ 0 \leq \mathrm{Re}\left[c_{m0}\right], \mathrm{Im}\left[c_{m0}\right] &\leq 1, \\ m &= 1, 2, \cdots, M, \end{aligned} \tag{2.18}$$

を，送信側と受信側が保持する．送信側では送信データ $\vec{b}$ と暗号鍵 $\vec{C}_0$ より

$$Z_{mj} = f\left(\mathrm{Re}[c_{m(j-1)}], b_j\right) + if\left(\mathrm{Im}[c_{m(j-1)}], b_j\right), \tag{2.19}$$

$$f(u,v) = \begin{cases} u, & (v=0) \\ u-0.5, & (v=1, u>0.5) \\ 1-u, & (v=1, u \leq 0.5), \end{cases} \tag{2.20}$$

$$c_{mj} = g^l\left(\mathrm{Re}[Z_{m(j-1)}]\right) + ig^l\left(\mathrm{Im}[Z_{m(j-1)}]\right), \tag{2.21}$$

$$g(z) = 3.91z(1-z), \tag{2.22}$$

とする．ここで $j = 1, 2, \cdots, N_\mathrm{t}$，$m = 1, 2, \cdots, M$ である．l は写像回数を決めるパラメータである．そして，暗号化した送信シンボル x_j を

$$s_j = \frac{1}{M}\sum_{m=1}^{M}\left(\mathrm{Re}[c_{mj}] + \mathrm{Im}[c_{mj}]\right)\exp\left[8\pi i\left(\mathrm{Re}[c_{mj}] - \mathrm{Im}[c_{mj}]\right)\right], \tag{2.23}$$

$$x_j = \exp\left[i\tan^{-1}\frac{\mathrm{Im}[s_j]}{\mathrm{Re}[s_j]}\right], \tag{2.24}$$

とする．x_j は複素単位円上に定義されるため，送信信号電力は BPSK と同じ一定値をとる．式（2.19）–（2.24）より，j 番目の送信シンボル x_j は $\vec{C}_j$ で定まるが，$\vec{C}_j$ すなわち式（2.21）は $\vec{C}_{j-1}$ と b_j より定まるので，結局

$$x_j = x_j\left(b_1, b_2, \cdots, b_j, \vec{C}_0\right), \tag{2.25}$$

である．このように，一つの送信シンボルに多数の送信ビットが含まれている．受信側の復号では，MLD を用いる．つまり，式（2.8）より，復号データ $\hat{\vec{b}}$ は

$$\hat{\vec{b}} = \arg\min_{\vec{b}} \|\vec{y} - \mathbf{H}\vec{x}\left(\vec{b}, \vec{C}_0\right)\|^2, \tag{2.26}$$

で得られる．すなわち，カオス MIMO では MLD で暗号に関する復号も同時に行う．

2.4 BP 復号

ここでは先行研究での BP 法を用いた復号法を紹介する [17]．しかしながら，BP 復号を用いた先行研究では，その復号過程を手順的にしか説明しておらず，未整理で，有効に働く機構や問題点も明確でない．そこで，本論文では著者の解釈を交えながら，BP 復号を多変数の力学系として整理し説明する．

一般的な BP 法の解説は [47, 48] に譲るが，BP 法とは，多数の確率変数（通信の場合は送信信号 $\vec{x}$ の各要素）を持つ確率分布を観測された情報（通信の場合は受信信号 $\vec{y}$）から効率的に求めるための手法で，人工知能分野で考案された [47, 48]．これはシステムサイズとともに指数関数的に計算量が増加していく大規模な確率モデルの統計量を繰り返し計算アルゴリズムに帰着させる手法で，人工知能分野や情報理論分野で広く用いられている．

MIMO の復号で用いられる MLD は，$\vec{y}$ を得た上で，N_{t} 個の確率変数を持つ確率分布を全ての確率変数のパターンで計算し，最も確度の高い $\vec{\hat{b}}$ を復号データとすることと等価である．そのため，計算量はシステムサイズ（N_{t}）とともに指数関数的（$2^{N_{\mathrm{t}}}$）に増加する．BP 復号では，ある一つの受信アンテナで得られた受信信号 y_k から見た送信ビット b_j の確率分布を計算できるようにし，その結果をアンテナ間で更新しながら，収束させることで復号データを得る．つまり，b_j を独立に計算できるようにすることで，$2^{N_{\mathrm{t}}}$ パターンの送信データを探索する必要がなく，y_k から見た b_j の 2 パターンを全ての k と j で探索することになる．それにより，計算量は $O(N_{\mathrm{t}}^2)$ 程度となり，大規模 MIMO でも現実的な計算量であるため注目されている．

2.4.1 BP 復号の手順と解釈

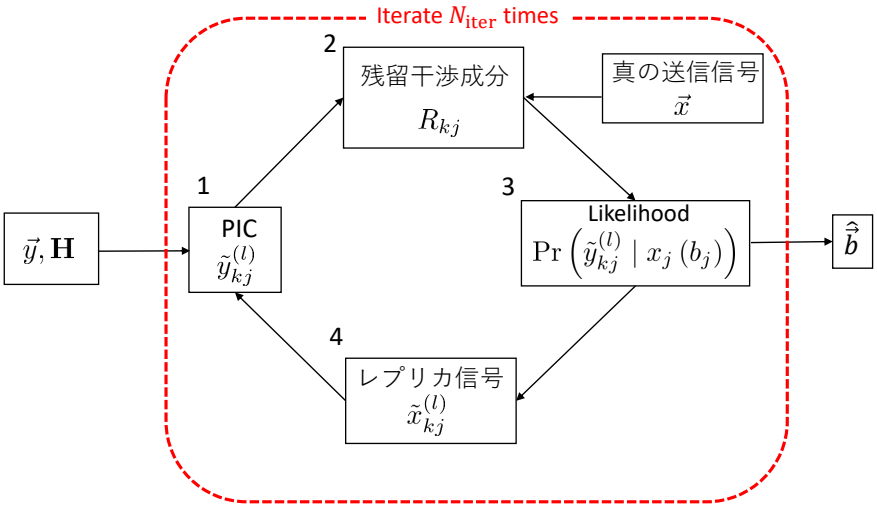


図 2.8: BP 復号のプロセスの概略図.

図 2.8 は大規模 MIMO での BP 復号の過程を整理したものである．以下で受信信号と CSI を得た後の BP 復号の手順を図 2.8 中の番号に沿って説明する．変調方法は式（2.3）で表せる BPSK とする．

1. PIC(Parallel Interference Canceller)

PIC は，N_{t} 個の送信シンボルに依存する受信信号 $\vec{y}$ から 1 つの送信シンボルのみの評価を可能にする操作である．k 番目の受信アンテナで得られる受信信号 y_k において j 番目の送信シンボルに着目すると，式（2.4）は

$$y_k = h_{kj}x_j + \sum_{m=1,m\neq j}^{N_{\mathrm{t}}} h_{km}x_m + n_k, \tag{2.27}$$

と書き直される．ここで，右辺第二項目の j 番目以外の送信シンボルからの寄与，これを干渉成分と呼ぶが，x_j に比べ大きく，x_j を全く評価できない．そこで右辺第二項を小さくし x_j を評価できるようにするため，前回の繰り返し計算で得られる暫定の推定値（k 番目の受信アンテナからみた m 番目の送信シンボルの暫定推定値のようなもので，その生成方法は

項 4 で説明する）$\tilde{x}_{km}^{(l)}$ を用いて，

$$\tilde{y}_{kj}^{(l)} = y_k - \sum_{m=1,m\neq j}^{N_\mathrm{t}} h_{km}\tilde{x}_{km}^{(l)} \tag{2.28}$$

$$= h_{kj}x_j - \sum_{m=1,m\neq j}^{N_\mathrm{t}} h_{km}\left(x_m - \tilde{x}_{km}^{(l)}\right) + n_k \tag{2.29}$$

$$= h_{kj}x_j + R_{kj}^{(l)} + n_k, \tag{2.30}$$

とする．ここで $l = 1, 2, \cdots$ は BP 復号での繰り返し回数（BP 繰り返し回数），$\tilde{x}_{km}^{(l)}$ はレプリカ信号，この操作を PIC と呼ぶ．式（2.30）の右辺第二項

$$R_{kj}^{(l)} = \sum_{m=1,m\neq j}^{N_\mathrm{t}} h_{km}\left(x_m - \tilde{x}_{km}^{(l)}\right), \tag{2.31}$$

は残留干渉成分と呼ばれ，この項が小さくなるようにレプリカ信号を作れば，結果として，x_j の評価を可能にする．

2. 残留干渉成分の評価

$R_{kj}^{(l)}$ が小さくとも 0 ではないので，次項 3 で計算する $\tilde{y}_{kj}^{(l)}$ の確率分布（尤度関数）にその効果を含める必要がある．ここでは，その効果をどのように評価するかを述べる．残留干渉成分は，受信信号では知りえない送信信号 $\vec{x}$ を含むので，この成分を平均 0，分散 $\sigma_{kj}^{(l)\,2}$ のノイズと独立な乱数と見なし，その効果を尤度関数に取り入れる．ここで $\sigma_{kj}^{(l)\,2}$ は

$$\sigma_{kj}^{(l)\,2} = \sum_{m=1,m\neq j}^{N_\mathrm{t}} |h_{km}|^2 \left(x_m - \tilde{x}_{km}^{(l)}\right)^2, \tag{2.32}$$

であるが，もちろん，受信者は真の送信シンボル x_m の値を知りえないので，何らかの方法でこれを評価する必要がある．先行研究 [16–23] では，送信信号を用いて式（2.32）に従って $\sigma_{kj}^{(l)\,2}$ を求めて BP 復号の振る舞いを調べている．

3. 尤度の計算

ここでは $\tilde{y}_{kj}^{(l)}$ の確率分布を計算し，k 番目の受信アンテナから見た j 番目の送信シンボルを対数尤度比を用いて評価する．送信ビット b_j が 0 ま

たは1の場合に $\tilde{y}_{kj}^{(l)}$ となり得る確率分布（尤度関数）は，前項2の $R_{kj}^{(l)}$ のモデルより

$$\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, x_j(b_j)\right) = \mathcal{CN}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, h_{kj}x_j(b_j), {\sigma_{kj}^{(l)}}^2 + \sigma_{\mathrm{n}}^2\right), \tag{2.33}$$

となる．ここで $\mathcal{CN}(*|\mu,\sigma^2)$ は $*$ を確率変数とし，平均 μ と分散 σ^2 の複素ガウス分布とする．すると，対数尤度比（Log Likelihood Ratio，LLR）

$$\alpha_{kj}^{(l)} = \log \frac{\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, x_j(b_j=1)\right)}{\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, x_j(b_j=0)\right)}, \tag{2.34}$$

で k 番目の受信アンテナからみた j 番目の送信シンボルを評価できる．つまり，$\alpha_{kj}^{(l)} \in (-\infty,\infty)$ であり，$\alpha_{kj}^{(l)}$ が正であれば，k 番目の受信アンテナから見た j 番目の送信シンボル（送信ビット）が $x_j = 1, (b_j = 1)$，負であれば $x_j = -1, (b_j = 0)$ の可能性を示し，$|\alpha_{kj}^{(l)}|$ の大きさでその信頼性を示していることになる．$\alpha_{kj}^{(l)}$ を全ての受信アンテナで足し合わせた $\gamma_j^{(l)}$ は

$$\gamma_j^{(l)} = \sum_{m=1}^{N_{\mathrm{r}}} \alpha_{mj}^{(l)}, \tag{2.35}$$

であり，全ての受信アンテナからみた j 番目の送信シンボルの推定値とその信頼性を評価する量となる．

4. レプリカ信号の生成

次の BP 繰り返し計算で PIC に用いるレプリカ信号を算出する．その算出に必要なパラメータ $\beta_{kj}^{(l+1)}$ を

$$\beta_{kj}^{(l+1)} = \gamma_j^{(l)} - \alpha_{kj}^{(l)}, \tag{2.36}$$

とする．$\beta_{kj}^{(l+1)}$ は $\alpha_{kj}^{(l)}$ と同様に，j 番目の送信シンボルを評価するためのものであるが，その違いは k 番目の受信アンテナ以外からみた j 番目の送信シンボルを評価する量である点である．それを用いてレプリカ信号を

$$\tilde{x}_{km}^{(l+1)} = \tanh\left(\frac{\beta_{km}^{(l+1)}}{2}\right), \tag{2.37}$$

と生成し，これが次の繰り返し，すなわち項1，式（2.28）で用いられる．$\tilde{x}_{kj}^{(l+1)}$ に k 番目以外の受信アンテナからの評価が入ることにより，j 番目の送信シンボルの評価の信頼性が向上し，各受信アンテナからの推定が整合すると考えられる．全ての j,k について $|\beta_{kj}^{(l+1)}|$ が大きくなると $\tilde{x}_{kj}^{(l+1)}$ は真の送信シンボルの大きさ $x_j = 1$ または -1 に近づく．

BP 繰り返し計算

前述の項 $1-4$ の一連の手順を BP 繰り返し計算と呼ぶ．BP 繰り返し計算により，$\tilde{x}_{kj}^{(l)}$ を更新することで，残留干渉成分 $R_{kj}^{(l)}$ が徐々に小さくなり，x_j を評価しやすくなることが期待される．そして，N_{iter} 回（BP 繰り返しの規定回数）の BP 繰り返し計算を行い，その際の $\gamma_j^{(N_{\mathrm{iter}})}$ を用いて復号ビット $\hat{b}_j$ を

$$\hat{b}_j = \begin{cases} 1, \ \gamma_j^{(N_{\mathrm{iter}})} \geq 0 \\ 0, \ \gamma_j^{(N_{\mathrm{iter}})} < 0, \end{cases} \tag{2.38}$$

で決定する．すなわち，式（2.35）より，全ての受信アンテナから見た j 番目の送信シンボルの評価を行い，最終的な復号ビットを決めていることにあたる．なお，BP 繰り返し計算の初回 $l=1$ では，項 4 の前なのでレプリカ信号 $\tilde{x}_{kj}^{(1)}$ を持たない．そこで [17] では全ての j と k で $\tilde{x}_{kj}^{(1)} = 0$ とする．

第3章　非線形力学系としてのBP復号とその問題点の解消

この章では，BP 復号を用いた大規模 MIMO を大自由度非線形写像として捉え，先行研究では不完全であった点を取り除き，BP 復号の問題点の解消と性能向上の可能性を探る．まず，3.1 節で BP 復号を用いた大規模 MIMO が非線形力学系として捉えられることを示す．無線通信の分野では BP 復号が提案されつつあるが，BP 繰り返し計算で残留干渉成分（式 (2.31)）の評価方法が確立されていない．そこで 3.2 節では，力学系の安定固定点に至ることが復号にあたるように残留干渉成分の評価を力学系内の物理量で行う方法を提案し，数値実験にて性能を確認する．また，3.3 節では，BP 復号の推定結果が BP 繰り返し回数 l に対し，一定値や周期運動に至ることを示し，その際の状態変数や推定精度などの力学系としての詳細な振る舞いを調べる．

3.1　大容量無線通信における非線形力学系

ここでは，本研究で取り扱う BP 復号を用いた大容量無線通信が大自由度非線形力学系であることを示し，その力学系がどのような構造をしているかを述べる．

従来の無線通信は，SISO（図 2.1（a））で構成されている．送信側では，送信ビット $b \in \{0,1\}$ を電磁波で送信するために BPSK を行い，送信信号は $x \in \{-1,1\}$ となる（図 3.1）．受信側では，受信信号 y として

$$y = hx + n, \tag{3.1}$$

を得る．ここで h は通信路情報，n は通信路のノイズ（何れも複素数）である．受信側では y と既知の h を用いて送信信号を推定する．それには $n = 0$ での $x = \pm 1$ に対応する受信信号 $\pm h$ より，図 3.2(a) の分類図を構成し，受信信号 y に応じて送信ビットを推定する．結果として推定送信信

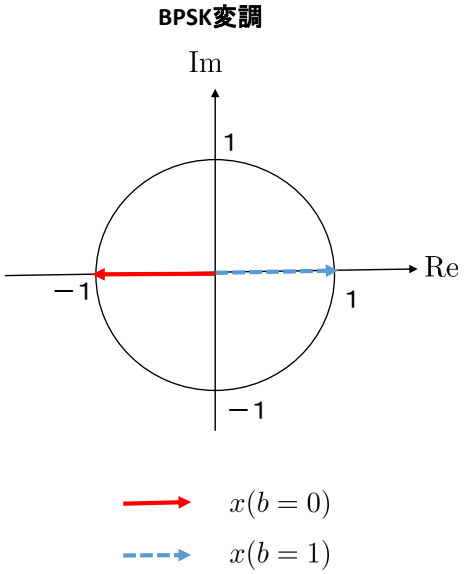


図 3.1: BPSK での送信信号 x を複素平面上に描いた信号空間図.
位相と振幅を表す.

号 $\hat{x}$ は非線形変換 $f(\cdot)$ により

$$\begin{aligned}\hat{x} &= f(y,h)\\ &= \frac{\mathrm{Re}[\frac{y}{h}]}{|\mathrm{Re}[\frac{y}{h}]|},\end{aligned} \tag{3.2}$$

と表される．このように無線通信での復号は非線形変換である．

次に MIMO での無線通信を見てみると，送信信号は BPSK にて変調を行い，受信信号 $\vec{y}$ は式（2.4）となる．この場合の復号も SISO と同様に非線形変換

$$\hat{\vec{x}} = \vec{f}(\vec{y}, \mathbf{H}), \tag{3.3}$$

により表される．$N_\mathrm{t} = N_\mathrm{r} = 2$ のとき，式（3.3）は図 3.2(b) で描かれる分類を各受信アンテナで行い，それを総合的に区分する非線形変換となる．大規模 MIMO の条件下では図 3.2(b) で描かれる分類図は複雑化し，式（3.3）の非線形変換にかかる計算量が膨大になる．これを回避する復号法の 1 つが 2.4 節で述べた BP 法を用いた繰り返し推定である．そこでは BP 復号のレプリカ信号 $\tilde{x}_{kj}^{(l)}$ が，BP 繰り返し回数毎に刻々と変化していく．つまり，$N_\mathrm{t} \times N_\mathrm{r}$ 個の $\tilde{x}_{kj}^{(l)}$ が状態変数で，それが時間を l とする決定論的時間発展に従う系，すなわち，大自由度非線形力学系である．

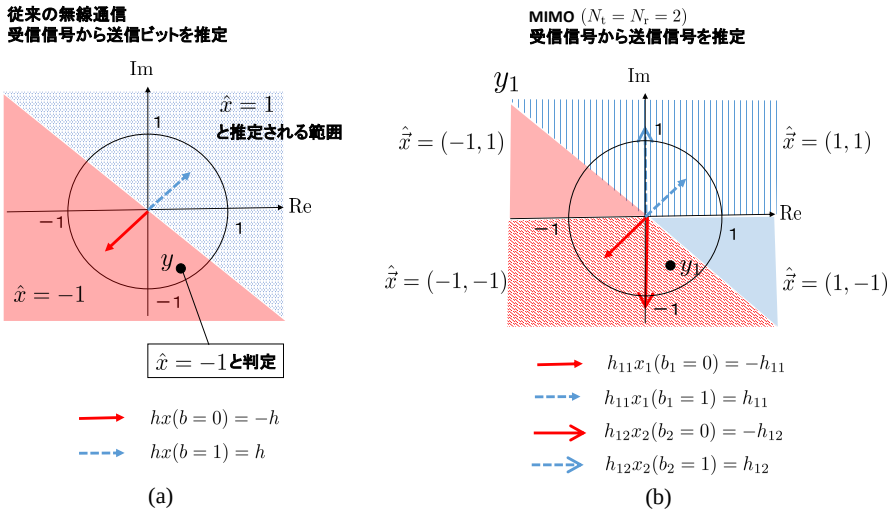


図 3.2: (a) SISO での推定送信信号の分類図．矢印が $n=0$ での受信信号で複素平面が 2 領域に分かれている．受信信号が y のとき，送信信号を $\hat{x}=-1$ と推定する． (b)MIMO での推定送信信号の分類図．矢印は $n_1=0$ で，ある $\mathbf{H}$ において $h_{1j}x_j$，$(j=1,2)$ を描いたもの．1 番目の受信アンテナは，$h_{11}x_1+h_{12}x_2$ を受信するので，複素平面が 4 つに分かれる．受信信号が，図の y_1 のとき，$\hat{\vec{x}}=(-1,-1)$ と推定される．y_2 についても同じ推定ができるが，2 つが一致するとは限らず，より複雑な分類が必要となる．

では BP 復号はどのような力学系なのだろうか．まず，k 番目の受信アンテナだけに注目した力学系を想定してみる．この場合，レプリカ信号は式（2.37）に変えて

$$\tilde{x}_{kj}^{(l)}=\tanh\left(\alpha_{kj}^{(l-1)}\right), \tag{3.4}$$

とする．このレプリカ信号を用いて PIC を行うと式（2.29）は

$$\tilde{y}_{kj}^{(l)}=h_{kj}x_j-\sum_{m=1,m\neq j}^{N_t}h_{km}\left(x_m-\tilde{x}_{km}^{(l)}\right)+n_k, \tag{3.5}$$

となる．当然であるが，$\tilde{x}_{km}^{(l)}$ に他のアンテナの受信信号が含まれることはなく，k 番目の受信アンテナだけで閉じた力学系である．このとき，$\tilde{x}_{kj}^{(l)}$ は，時間変化によって $\tilde{x}_{kj}^{(*)}$ に収束する（固定点に至る）．ただし，1 つの受信信号 y_k から N_t 個の送信シンボルが定まるため，N_t 個の初期状態 $\tilde{x}_{kj}^{(0)}$ によって異なる固定点に至る．従って，推定精度は高くない．

以上の考察の後，本来の BP 復号に立ち返ると，式（2.37）のレプリカ信号を生成する $\beta_{kj}^{(l)}$ は，式（2.36）のように，k 番目以外の受信アンテナ

から見た j 番目の送信シンボルの LLR（評価） $\alpha_{kj}^{(l-1)}$ の合計，すなわち平均となっていることがわかる．つまり，個々のアンテナでレプリカ信号が固定点に至ろうとする時間発展が，互いにレプリカ信号を交換させることで，共通の固定点に至ろうとする力学系になっている．これによって，正しく復号できることが期待される．

3.2 残留干渉成分の評価

3.2.1 疑似残留干渉成分による BP 復号の構築

2.4.1 節で述べたように BP 復号における残留干渉成分 $R_{kj}^{(l)}$ の評価には大きな問題がある．それは $R_{kj}^{(l)}$ の分散（式（2.32））に含まれる送信信号 x_m の評価方法が与えられていないことである．ここでは，その問題に取り組む．前節からもわかるように，BP 復号では，BP 繰り返し計算により，レプリカ信号 $\tilde{x}_{kj}^{(l)}$ が固定点に至り，真の送信シンボル x_j に近づき，$R_{kj}^{(l)}$ も 0 に近づくことが期待される．そこで，$\tilde{x}_{kj}^{(l)}$ が固定点に近づき，そのとき $R_{kj}^{(l)}$ も 0 に近づくことを要請する．そのためには，式（2.31）で不明な x_m に変えて $\tilde{x}_{km}^{(l-1)}$ を用い

$$\tilde{R}_{kj}^{(l)} = \sum_{m=1,i\neq j}^{N_{\mathrm{t}}} h_{km}\left(\tilde{x}_{km}^{(l-1)} - \tilde{x}_{km}^{(l)}\right), \tag{3.6}$$

として見積もることが自然であろう．このとき，この $\tilde{R}_{kj}^{(l)}$ を疑似残留干渉成分と呼ぶことにする．2 章の BP 復号において $R_{kj}^{(l)}$ を $\tilde{R}_{kj}^{(l)}$ に変えた系では，$\tilde{x}_{km}^{(l)}$ が $\tilde{x}_{km}^{(*)}$ に収束する，すなわち固定点に至ると $\tilde{R}_{kj}^{(l)} \to 0$ となる．もちろん，必ずしも $\tilde{x}_{kj}^{(*)} = x_j$ とは言えないが，送信シンボル以外の固定点はない，もしくはそのベイスンは狭いと考えれば，妥当と言える（これについては，3.2.3 節で数値的に確かめる）．ここで，ベイスンとは状態空間の中で，あるアトラクターに収束する初期値の集合のことである．なお，このとき $\tilde{R}_{kj}^{(l)}$ は平均，

$$\tilde{\mu}_{kj}^{(l)} = \tilde{R}_{kj}^{(l)}, \tag{3.7}$$

で分散

$$\tilde{\sigma}_{kj}^{(l)\,2} = \sum_{m=1,m\neq j}^{N_{\mathrm{t}}} |h_{km}|^2 \left(\tilde{x}_{km}^{(l-1)} - \tilde{x}_{km}^{(l)}\right)^2, \tag{3.8}$$

の乱数として BP 繰り返し計算を行う（これらも式（3.6）と同様，$\tilde{x}_{km}^{(l)}$ が固定点に至ることで 0 に近づく）．また，$l=1$ のとき，式（3.7），（3.8）の $\tilde{x}_{km}^{(0)}$ の項は力学系上に存在しないので，$\tilde{x}_{km}^{(0)}$ が 1 と -1 を等確率でとると考えて，$\tilde{\mu}_{kj}^{(1)}$ と $\tilde{\sigma}_{kj}^{(1)\,2}$ を，

$$\tilde{\mu}_{kj}^{(1)} = 0, \tag{3.9}$$

$$\tilde{\sigma}_{kj}^{(1)\,2} = \sum_{m=1, m\neq j}^{N_{\mathrm{t}}} |h_{km}|^2, \tag{3.10}$$

とする．

3.2.2 疑似残留干渉成分の尤度関数への効果

BP 復号を用いた先行研究では，残留干渉成分の効果を様々な方法で尤度関数に含めている．そのため，ここでは，疑似残留干渉成分の効果から妥当な尤度関数のモデルを考察する．前節で導入した疑似残留干渉成分は平均 $\tilde{\mu}_{kj}^{(l)}$，分散 $\tilde{\sigma}_{kj}^{(l)\,2}$ で，ノイズと独立な乱数と考えるので，送信ビット b_j が 0 か 1 である尤度関数は，

$$\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, x_j(b_j)\right) = \mathcal{CN}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, h_{kj}x_j(b_j) + \tilde{\mu}_{kj}^{(l)}, \tilde{\sigma}_{kj}^{(l)\,2} + \sigma_{\mathrm{n}}^2\right), \tag{3.11}$$

が妥当と考えられる．これを model-(a) とし，疑似残留干渉成分の平均と分散が BP 復号にどのような影響があるかを調べるため，平均のみを含める model-(b)，

$$\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, x_j(b_j)\right) = \mathcal{CN}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, h_{kj}x_j(b_j) + \tilde{\mu}_{kj}^{(l)}, \sigma_{\mathrm{n}}^2\right), \tag{3.12}$$

分散のみを含める model-(c)，

$$\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, x_j(b_j)\right) = \mathcal{CN}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, h_{kj}x_j(b_j), \tilde{\sigma}_{kj}^{(l)\,2} + \sigma_{\mathrm{n}}^2\right), \tag{3.13}$$

を考える．

以下では，これらの有効性，すなわち性能を数値実験で比較し検討する．なお，以降の数値実験は何も断らない限り次のように設定する．送信ビット b_j の値は $0, 1$ で出現する乱数とする．通信路行列 $\mathbf{H}$ はレイリーフェージングを仮定し，その要素 h_{kj} は平均 0，分散 1 の独立な複素ガウス分布に従う乱数とする．ノイズ $\vec{n}$ の要素 n_k は平均 0，分散 σ_{n}^2 の独立な複素ガウス分布に従う乱数とする．SNR（Signal to Noise Ratio）はノイズの分散 σ_{n}^2 と $\sigma_{\mathrm{n}}^2 = 10^{-\mathrm{SNR}/10}$ の関係である．また，それぞれの試行毎に，$\vec{b}$, $\mathbf{H}$，$\vec{n}$ を生成し，全てのモデルに用いる．数値実験は全て MATLAB® を用いる．

3.2.3 model-(a)，(b) 及び (c) の数値実験

復号にかかる計算時間

表 3.1: BP 繰り返しの規定回数 N_{iter} での復号にかかる計算時間．
全ての値は 100 試行分の合計時間を model-(a) の $N_{\mathrm{iter}} = 1$ の値で規格化している．送受信アンテナ数 $N_{\mathrm{r}} = N_{\mathrm{t}} = 12$，ノイズ $\vec{n}$ の分散 $\sigma_{\mathrm{n}}^2 = 10^{-2}$，（SNR=20 [dB]）とする．

model \ N_{iter}	1	5	10	20	30	40
model-(a)	1	5.0	12.8	27.0	43.0	56.0
model-(b)	0.7	3.6	9.4	21.0	33.2	45.5
model-(c)	0.8	4.6	10.2	20.0	34.8	46.9

表 3.1 に model-(a)，(b) および (c) の復号にかかる時間を BP 繰り返しの規定回数毎に比較する．当然，model-(a) は残留干渉成分の平均と分散のどちらも計算するため，他のモデルに比べ遅い．しかしながら，その影響はさほどではなく，復号にかかる計算時間は，3 つのモデル間で大きな差がない．そのため，3 つのモデル間で，復号にかかる計算量での性能差は殆どないと言える．

SNR に対する BER の比較

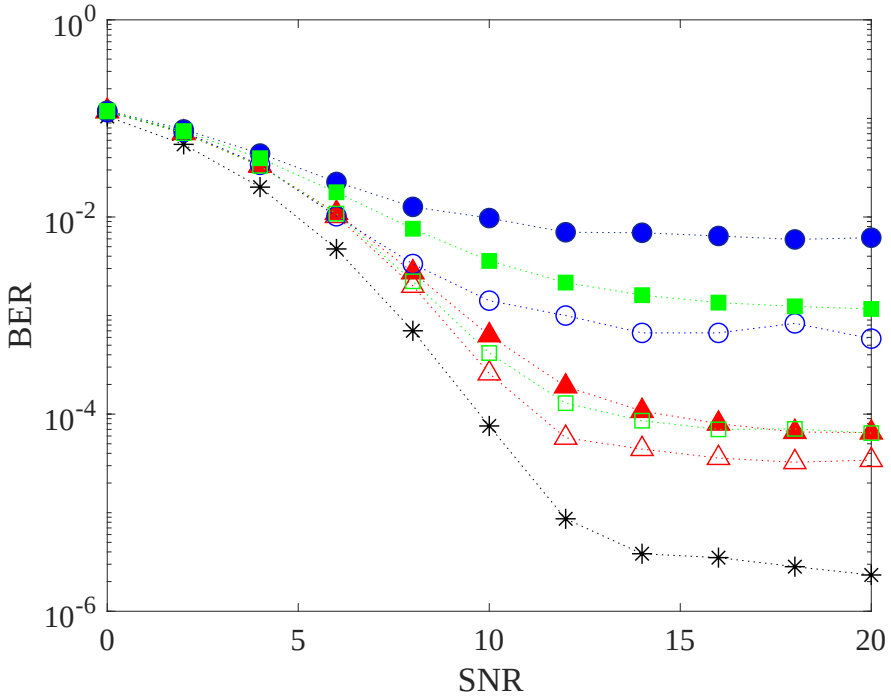


図 3.3: 各 SNR における model-(a)，model-(b) 及び model-(c) の BER の比較．四角，円，三角は，それぞれ model-(a)，model-(b)，model-(c) で，中塗り有と無しでそれぞれ $N_{\rm iter}=5$ と 20 を表す．なお，比較のために，式（2.32）のように残留干渉成分の評価で送信信号を用いたもの（$N_{\rm iter}=20$ のみ）を載せている．ノイズ $\vec{n}$ の分散は $\sigma_{\rm n}^2=10^{-{\rm SNR}/10}$ で，アンテナ数は $N_{\rm t}=N_{\rm r}=12$ とし，変調方式は BPSK とする．BER は 100000 試行の平均値とする．

図 3.3 は，異なる SNR での推定精度を 3 つのモデルで比較している（この SNR-BER の図は，無線通信の推定精度を評価する際に一般に用いられる）．縦軸は BER(Bit Error Ratio) であり，復号に失敗した信号の数の割合を表す．横軸の SNR は大きいほどノイズが小さく，縦軸の BER は小さいほど推定精度が高い．当然，SNR が大きいところで BER は低くなるが，SNR $\sim$ 15 程度から BER が収束しつつある．これは，SNR が大きくなると残留干渉成分の影響がノイズよりも大きくなるため，SNR を大きく（ノイズの影響を小さく）しても BER が低下しないためと考えられる．また，BP 復号では，$N_{\rm iter}$ が小さいうちは，レプリカ信号は BP 繰り返し計算の度に変化しており，固定点に至っておらず，当然，BER は大きいと考えられる．確かに本実験のどのモデルでも $N_{\rm iter}$ が小さいうちは

BER が大きく，増やすと BER が減少する．この結果から，どのモデルでも疑似残留干渉成分を用いて受信信号から復号できていることがわかり，3 つのモデルの中で，model-(c) が一番低い BER を示していることもわかる．しかしながら，図 3.3 に載せた残留干渉成分の評価で送信信号を用いたもの（式（2.32））と比較すると model-(c) でも BER に 10 倍程度の大きな差がある．

BP 繰り返し回数に対する BER の比較

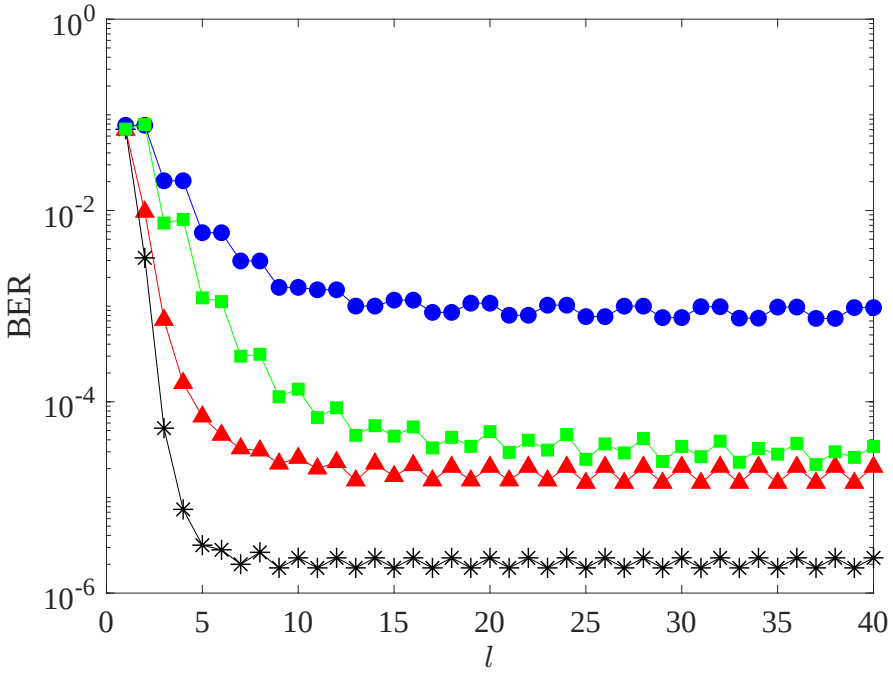


図 3.4: 各 l における model-(a)，model-(b) 及び model-(c) の BER の比較．シンボルや数値実験の条件は図 3.3 と同じ．ただし，ノイズ $\vec{n}$ の分散は $\sigma_{\mathrm{n}}^2 = 10^{-2}$,（SNR= 20[dB]）とする．

図 3.4 は BER と BP 繰り返し回数 l の関係を 3 つのモデルで比較している．BP 繰り返し規定回数を $N_{\mathrm{iter}} = 40$ とし，BP 繰り返し回数 l, $(l = 1, 2, \cdots, N_{\mathrm{iter}})$ での復号ビットを

$$\hat{b}_j^{(l)} = \begin{cases} 1, & \gamma_j^{(l)} \geq 0 \\ 0, & \gamma_j^{(l)} < 0, \end{cases} \tag{3.14}$$

とする．全てのモデルで l を増加させると BER が低下し，概ね $l \geq 20$ で BER がほぼ収束している．また，model-(c) は BER の低下の速さと収束が他のモデルに比べ速いこともわかる．以上の結果から 3 つのモデルの中では model-(c) が優れていると言えよう．そこで以降の BP 復号は特に断らない限りこの model-(c) を用いる．

3.2.4 考察と議論

数値実験の結果，3.2 節で構成した疑似残留干渉成分を用いた BP 復号が期待したように機能していることがわかる．ただし，尤度関数の妥当なモデルとした model-(a) よりも model-(c) の方が優れていた．そこで 3 つのモデルにおける BER に差が生じる理由を考察する．まずは，平均のみを考慮する model-(b) と分散のみを考慮する model-(c) の差について考える．model-(b) の BER は SNR の高いところで model-(c) より，かなり大きい．これは model-(b) の尤度関数の分散が，残留干渉成分の分散を含まないため，小さすぎることが原因と考えられる．model-(b) の尤度関数の分散 σ_{n}^2 は SNR の高いところで非常に小さく，尤度関数の形状がデルタ関数に近づいていく．そのため，尤度関数の中心付近で尤度の変化が大きくなる．ノイズが小さい領域での BP 繰り返し計算では，主に残留干渉成分により $\tilde{y}_{kj}^{(l)}$ は決定され，それなりの大きさを持つのに，尤度関数の分散が小さいため，対数尤度比 $\alpha_{kj}^{(l)}$ が大きな値を示し，後の BP 繰り返し計算に大きく影響する．尤度関数に残留干渉成分の分散を考慮する model-(c) では，レプリカ信号が適切でなくとも，尤度関数の分散が大きいため，対数尤度比が大きくなりすぎることがなく，後の BP 繰り返し計算によってレプリカ信号を修正することができると考えられる．この差が，model-(b) と model-(c) の BER の差として表れていると考えられる．

一方で，どちらも考慮する model-(a) は一見，同じ原因で，model-(b) に比べ BER が増加しているとは考えにくい．しかし，model-(a) の尤度関数を詳しく見ると，

$$\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, x_j(b_j)\right) = \frac{1}{\sqrt{2\pi\left(\sigma_{\mathrm{n}}^2 + \tilde{\sigma}_{kj}^{(l)\,2}\right)}} \exp\left[-\frac{\left(\tilde{y}_{kj}^{(l)} - h_{kj}x_j(b_j) - \tilde{\mu}_{kj}^{(l)}\right)^2}{2\left(\sigma_{\mathrm{n}}^2 + \tilde{\sigma}_{kj}^{(l)\,2}\right)}\right], \tag{3.15}$$

である．この式の exp の中の分子部分を見ると，

$$\begin{aligned}\tilde{y}_{kj}^{(l)} - h_{kj}x_j(b_j) - \tilde{R}_{kj}^{(l)} &= R_{kj}^{(l)} - \tilde{R}_{kj}^{(l)} + n_k \\ &= \sum_{m=1,m\neq j}^{N_{\mathrm{t}}} h_{km}\left(x_m - \tilde{x}_{km}^{(l-1)}\right) + n_k, \qquad (3.16)\end{aligned}$$

となっており，model-(c) では

$$\tilde{y}_{kj}^{(l)} - h_{kj}x_j = \sum_{m=1,m\neq j}^{N_{\mathrm{t}}} h_{km}\left(x_m - \tilde{x}_{km}^{(l)}\right) + n_k, \qquad (3.17)$$

である．式（3.17）は l 回目の $\tilde{y}_{kj}^{(l)}$ の尤度に l 回目のレプリカ信号 $\tilde{x}_{km}^{(l)}$ を用いており，式（2.29）と見比べると自然である．しかし，式（3.16）では $l-1$ 回目のレプリカ信号 $\tilde{x}_{km}^{(l-1)}$ を用いることになっている．つまり，model-(a) の式（3.16）と尤度関数の分散は，BP 繰り返し計算により徐々に小さくなるが，分散部分のみが先に小さくなるモデルとなっている．そのため，前述の理由と同様，分散の小ささにより，model-(a) は model-(c) に比べ BER が増加したのではないかと考えられる．

なお，最もよい結果を示す model-(c) でも送信信号を用いたものより，BER に大きな差があるが，送信信号（正解の情報）を用いていないため当然と言えよう．

また，図 3.4 を見ると，$N_{\mathrm{iter}} \geq 15$ で BER が周期運動している．これが BER の大きさ，すなわち復号の失敗と関係する可能性があるが，その考察は，次節の BP 復号の力学系の調査と関連が深いため 3.3.3 節で行う．

3.3 BP 復号の力学系の調査

ここでは，BP 復号の推定結果が時間経過とともに，一定値や周期運動に至ることを示し，その際の状態変数 $\tilde{x}_{kj}^{(l)}$ と BER がどのような振る舞い（時間変化）をしているかを詳細に調べる．それらを把握することは，BP 復号の性能向上を求める上で重要なことと考えられる．

3.3.1 BP 復号における推定結果と状態変数の時間変化

ここでは，多数回の実験についての統計量である BER ではなく，力学系の挙動を詳細にみるために個々の復号について時刻 l の時点での推定値 $\vec{\hat{x}}^{(l)}$ の時間変化を数値的に調べ，その際の状態変数 $\tilde{x}_{kj}^{(l)}$ の変動を調べる．

$\vec{\hat{x}}^{(l)}$ の要素である $\hat{x}_j^{(l)}$ は，式（2.38）と同様に

$$\hat{x}_j^{(l)} = \begin{cases} 1, & \gamma_j^{(l)} \geq 0 \\ -1, & \gamma_j^{(l)} < 0, \end{cases} \tag{3.18}$$

とする．BP 復号は 3.2.2 節の model-(c) を用い，変調方法は BPSK とする．$N_{\mathrm{t}} = N_{\mathrm{r}} = 12$ とし，BP 繰り返し計算の純粋な振る舞いを見るためにノイズのない状況で数値実験を行う．

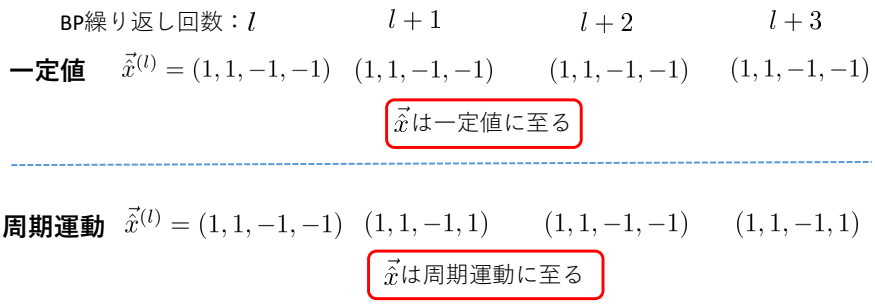


図 3.5: $\vec{\hat{x}}^{(l)}$ の時間変化の種類.

以下でその結果を述べるが，$\vec{\hat{x}}^{(l)}$ の時間変化に応じ図 3.5 のように，一定値に至る（固定点），周期運動に至るの 2 つに分類して示す．

一定値（固定点）に至る場合

ここでは，$l \gg 1$ で $\vec{\hat{x}}^{(l)}$ が一定値に至るケースを 2 つ分類して調査する．まず，case1 は，$\vec{\hat{x}}^{(l)}$ が一定値に至り，かつ送信信号に等しい（正しく復号できる）ケースである．図 3.6，3.7 で示される通り $\vec{\hat{x}}^{(l)}$ は一定値に至っている．$\hat{x}_1^{(l)}$ に注目し，それに関連する状態変数の一つである $\tilde{x}_{11}^{(l)}$ を調べると，$\tilde{x}_{11}^{(l)}$ は図 3.8 (a) で示される通り一定値に至っており（式（2.37）で $\tilde{x}_{11}^{(l)}$ を決定づける $|\beta_{11}^{(l)}|$ は ∞ に発散する），ここでは表示していないが他の $\tilde{x}_{kj}^{(l)}$ についても同様である．また，図 3.8 (b) の BER で示されるように，BP 繰り返し計算の 2 回目以降は BER が 0 であり，誤りが起きていない．つまり，状態変数 $\tilde{x}_{kj}^{(l)}$ が固定点に至り，復号データが送信データに等しくなる（正しく復号できる）ことがわかる．

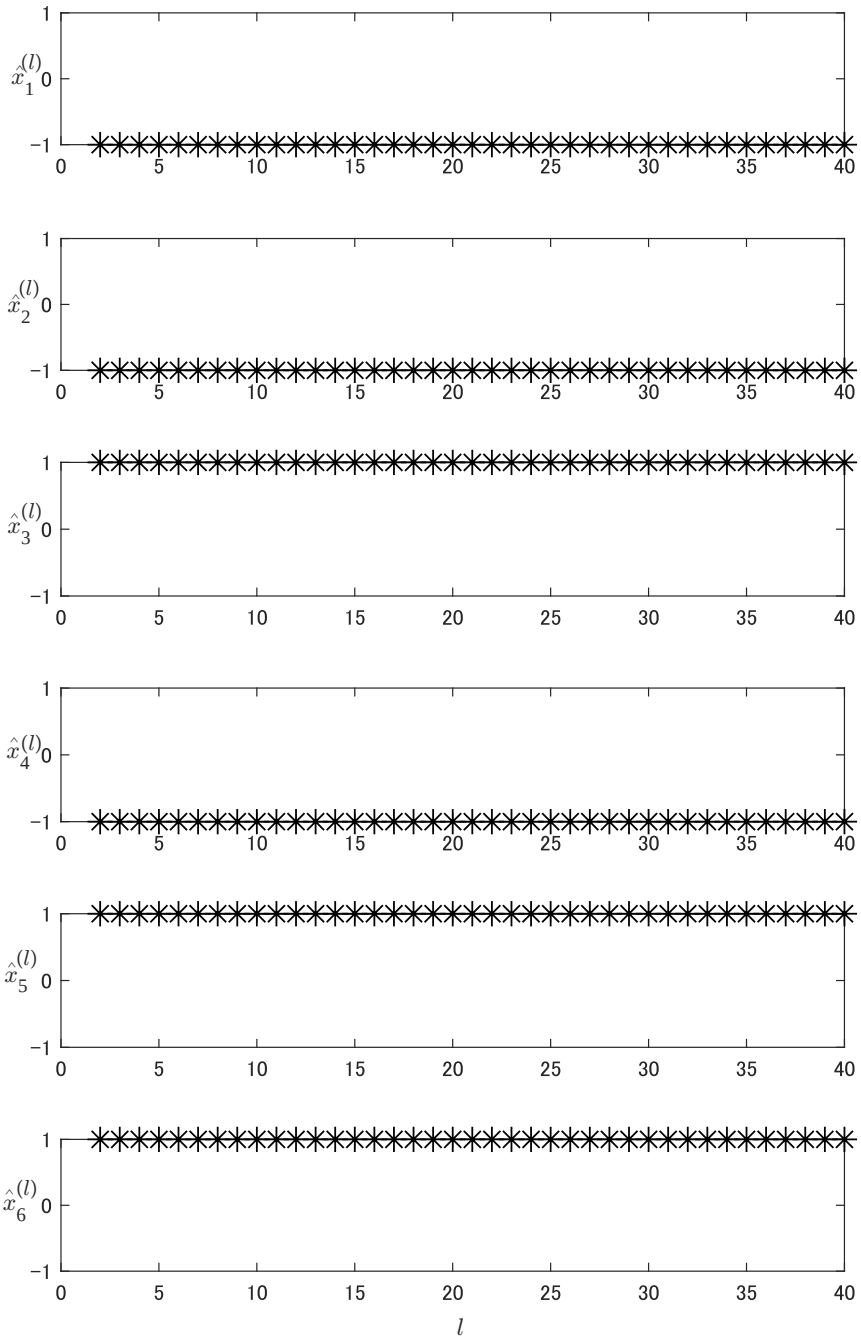


図 3.6: $\hat{x}_j^{(l)}$ の時間変化 $(j = 1, 2, \cdots, 12)$.
$N_{\mathrm{t}} = N_{\mathrm{r}} = 12$，ノイズ $\vec{n}$ の分散は $\sigma_{\mathrm{n}}^2 = 0$，(SNR=$\infty$[dB])（case1）.

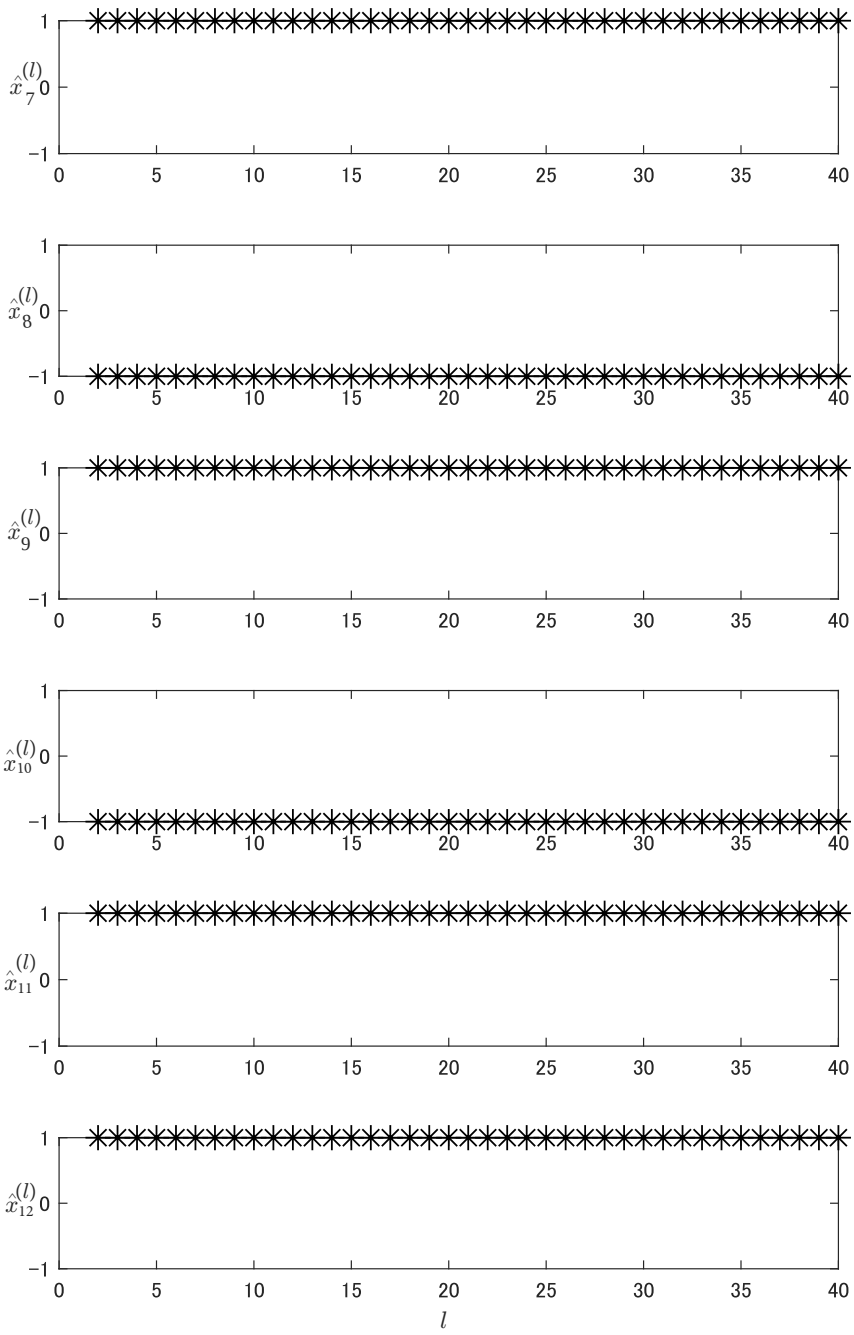
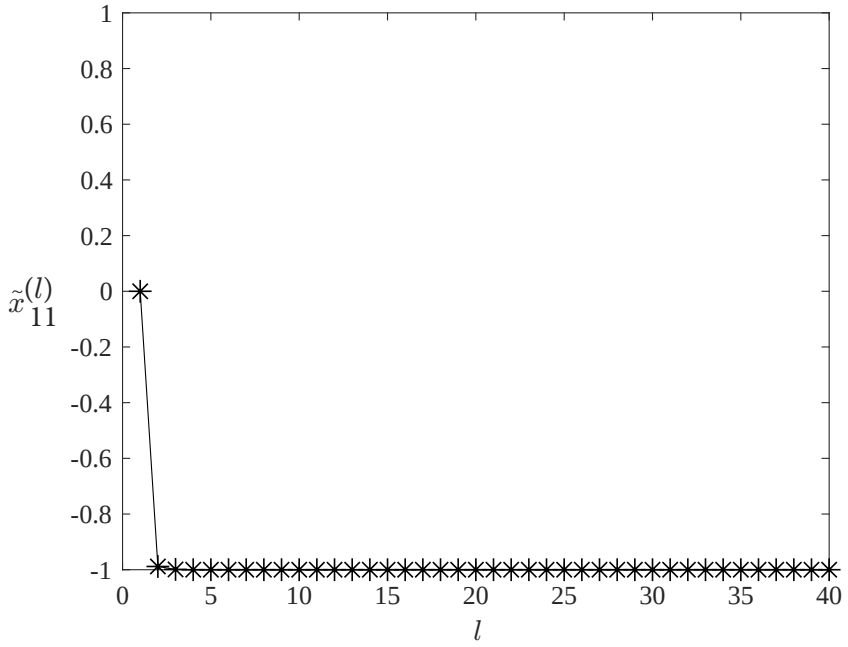
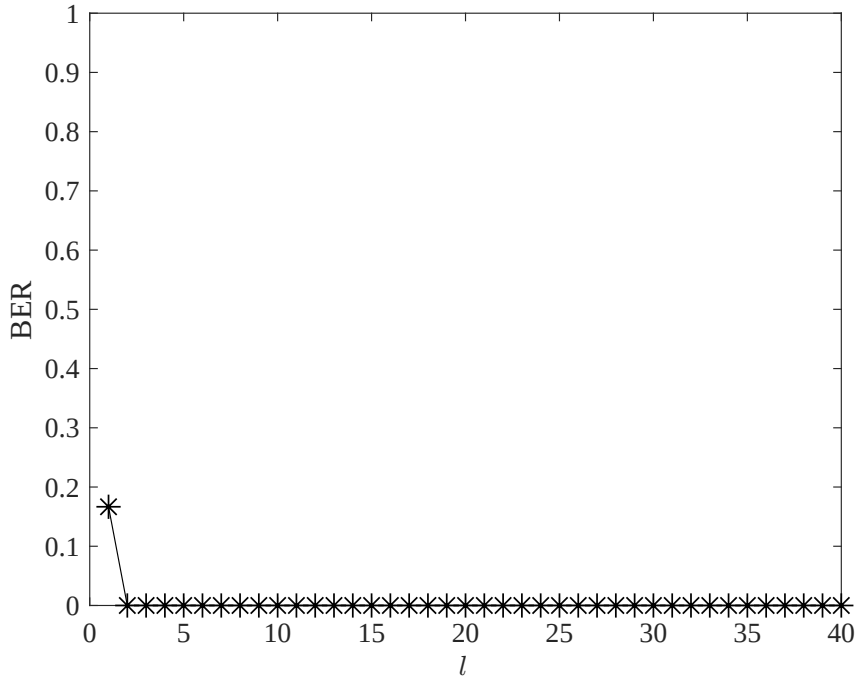

$\hat{x}_7^{(l)}$
$\hat{x}_8^{(l)}$
$\hat{x}_9^{(l)}$
$\hat{x}_{10}^{(l)}$
$\hat{x}_{11}^{(l)}$
$\hat{x}_{12}^{(l)}$
1
0
−1
0
5
10
15
20
25
30
35
40
l

図 3.7: 図 3.6 の続き.



(a) $\tilde{x}_{11}^{(l)}$ の時間変化.



(b) BER の時間変化.

図 3.8: 図 3.6 のときの $\tilde{x}_{11}^{(l)}$ と BER の時間変化.

case2 は，$\vec{\tilde{x}}^{(l)}$ が一定値に至り，かつ送信信号と異なる（つまり正しく復号できない）ケースである．case1 と同様に図 3.9，3.10 と図 3.11 (a) で示される通り，$\vec{\tilde{x}}^{(l)}$ と $\tilde{x}_{11}^{(l)}$ は一定値に至っている（$|\beta_{11}^{(l)}|$ は発散）．また，他の $\tilde{x}_{kj}^{(l)}$ についても同様でレプリカ信号が固定点に至っている．しかし，図 3.11 (b) で示される通り BER は 0 にならず，正しく復号できていない．つまり，状態変数 $\tilde{x}_{kj}^{(l)}$ が固定点に至る場合でも正しく復号できない場合もあることがわかる．

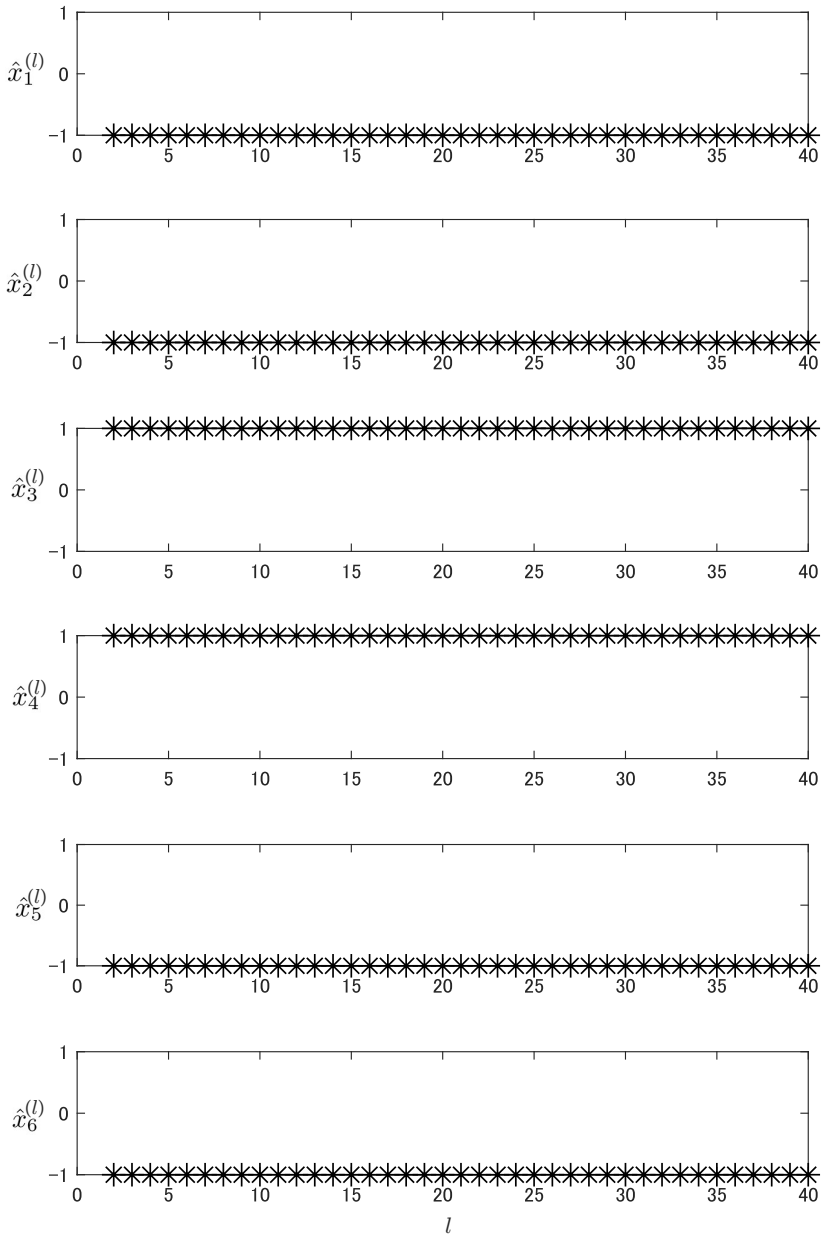


図 3.9: $\hat{x}_j^{(l)}$ の時間変化 $(j = 1, 2, \cdots, 12)$（case2）.

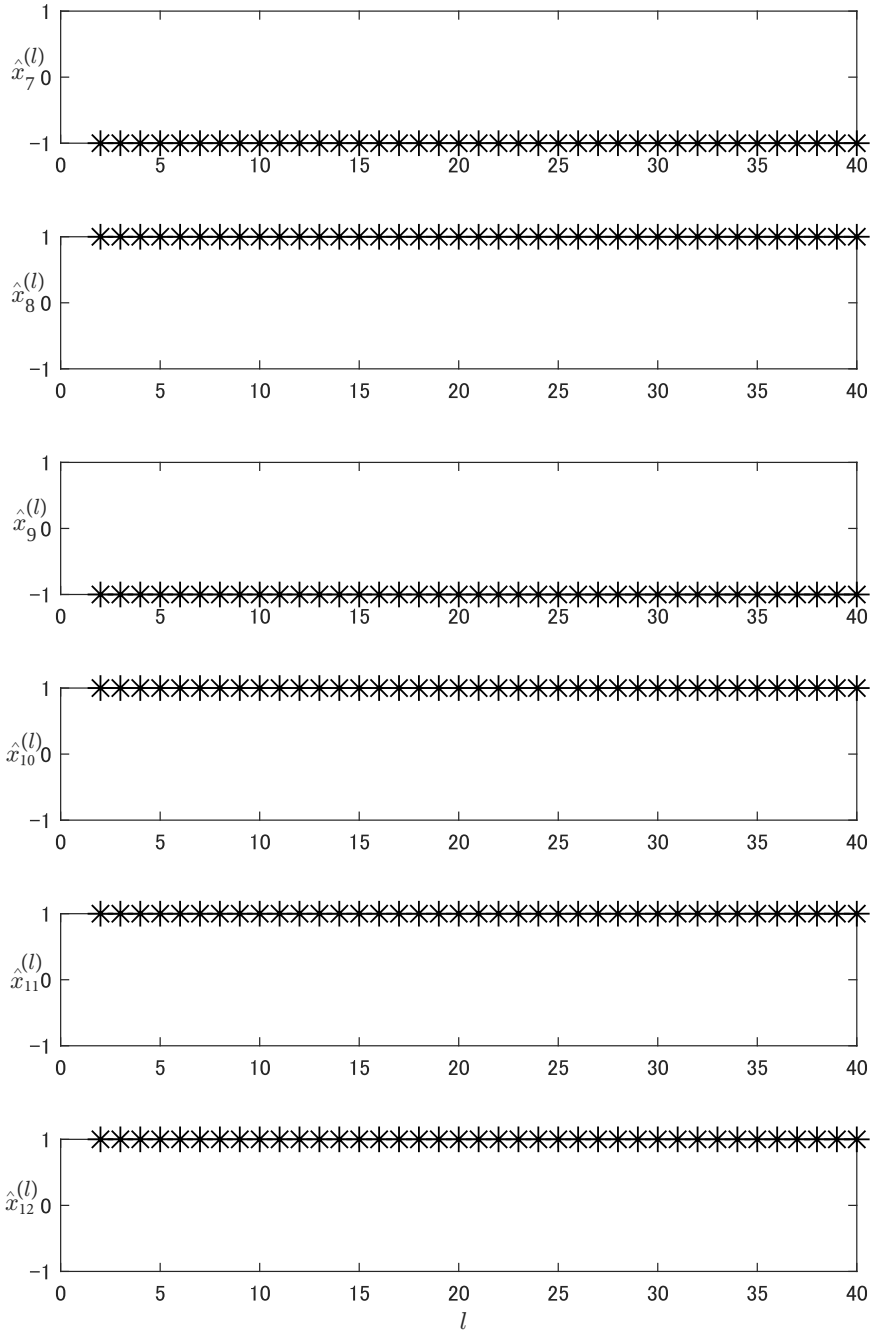
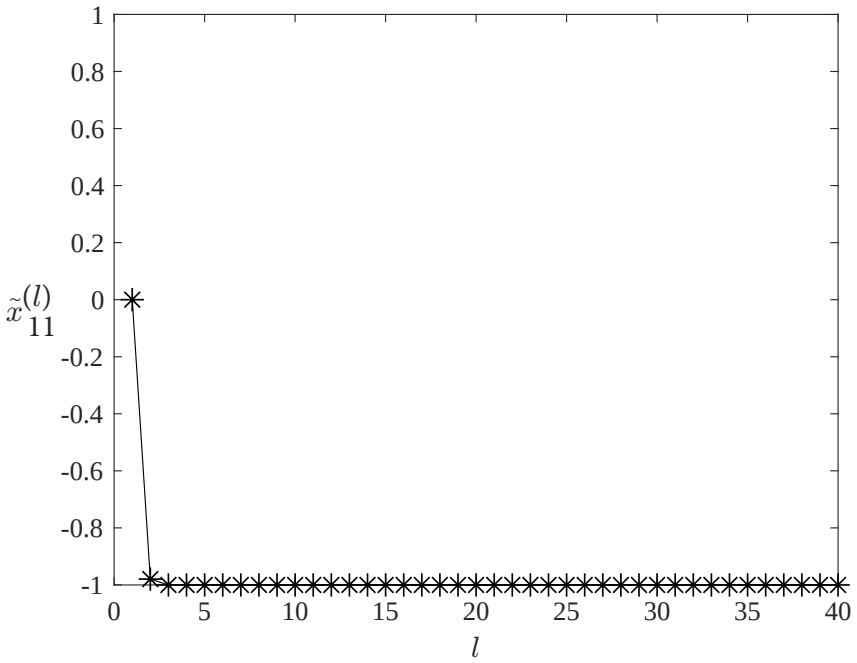
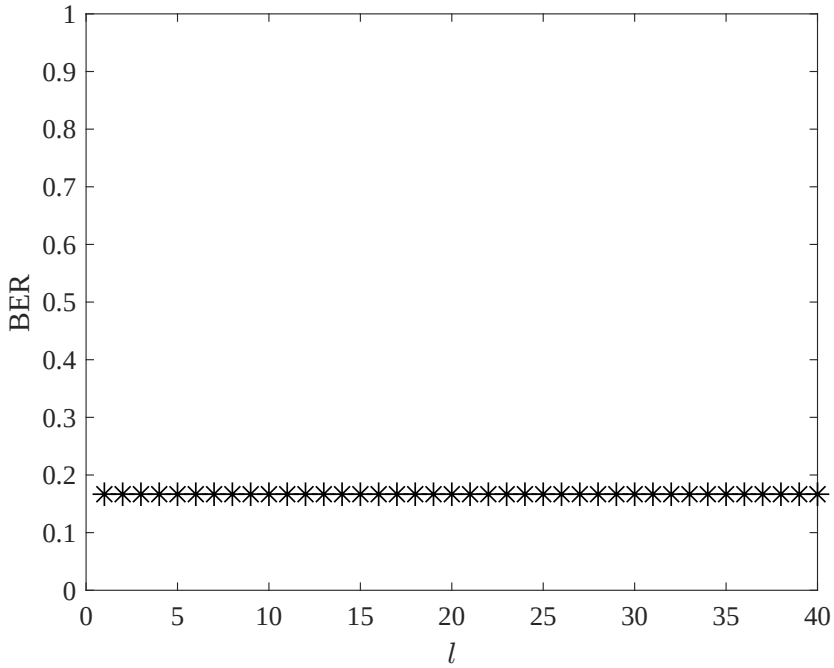

$\hat{x}_7^{(l)}$
$\hat{x}_8^{(l)}$
$\hat{x}_9^{(l)}$
$\hat{x}_{10}^{(l)}$
$\hat{x}_{11}^{(l)}$
$\hat{x}_{12}^{(l)}$
1
0
−1
0
5
10
15
20
25
30
35
40
l

図 3.10: 図 3.9 の続き.



(a) $\tilde{x}_{11}^{(l)}$ の時間変化.



(b) BER の時間変化.

図 3.11: 図 3.9 のときの $\tilde{x}_{11}^{(l)}$ と BER の時間変化.

周期運動に至る場合

$\vec{\hat{x}}^{(l)}$ の周期運動は 2 周期，3 周期，$\cdots$，と存在するが，ここでは 2 周期運動に至る場合を示す．図 3.12，3.13 で示される通り，$l \gg 1$ で $\hat{x}_j^{(l)}$ は j によって 2 周期運動に至るものと一定値に至るものが存在する．まず，2 周期運動に至る $\hat{x}_2^{(l)}$ の状態変数の一つである $\tilde{x}_{12}^{(l)}$ を調べる．図 3.14 より，l が大きくなると $\tilde{x}_{12}^{(l)}$ も 2 周期運動に至ることがわかる（$\beta_{12}^{(l)}$ も 2 周期運動）．次に，一定値に収束する $\hat{x}_1^{(l)}$ の状態変数の一つである $\tilde{x}_{11}^{(l)}$ を調べる．図 3.15 (a) をみると，$\tilde{x}_{11}^{(l)}$ は一定値に至っているようにみえるが，$\tilde{x}_{11}^{(l)}$ を決める $\beta_{11}^{(l)}$ は 2 周期運動に至っており（図 3.15（b)），$\tilde{x}_{11}^{(l)}$ も振幅は小さいが 2 周期運動している．この場合での $\tilde{x}_{kj}^{(l)}$ は，$N_{\mathrm{t}} \times N_{\mathrm{r}}$ 個あるため全てを図示することはできないが，全て 2 周期運動に至っている．BER の振る舞いをみると（図 3.16），当然ではあるが，正解の送信ビットは l に対して変化することはないので，正しく復号できていない．他の周期運動に至る場合も周期が異なるだけで上記と同様である．また，レプリカ信号は小さな振幅で変動しているが，推定送信信号は一定値で送信信号に等しい（または異なる）というケースはない．

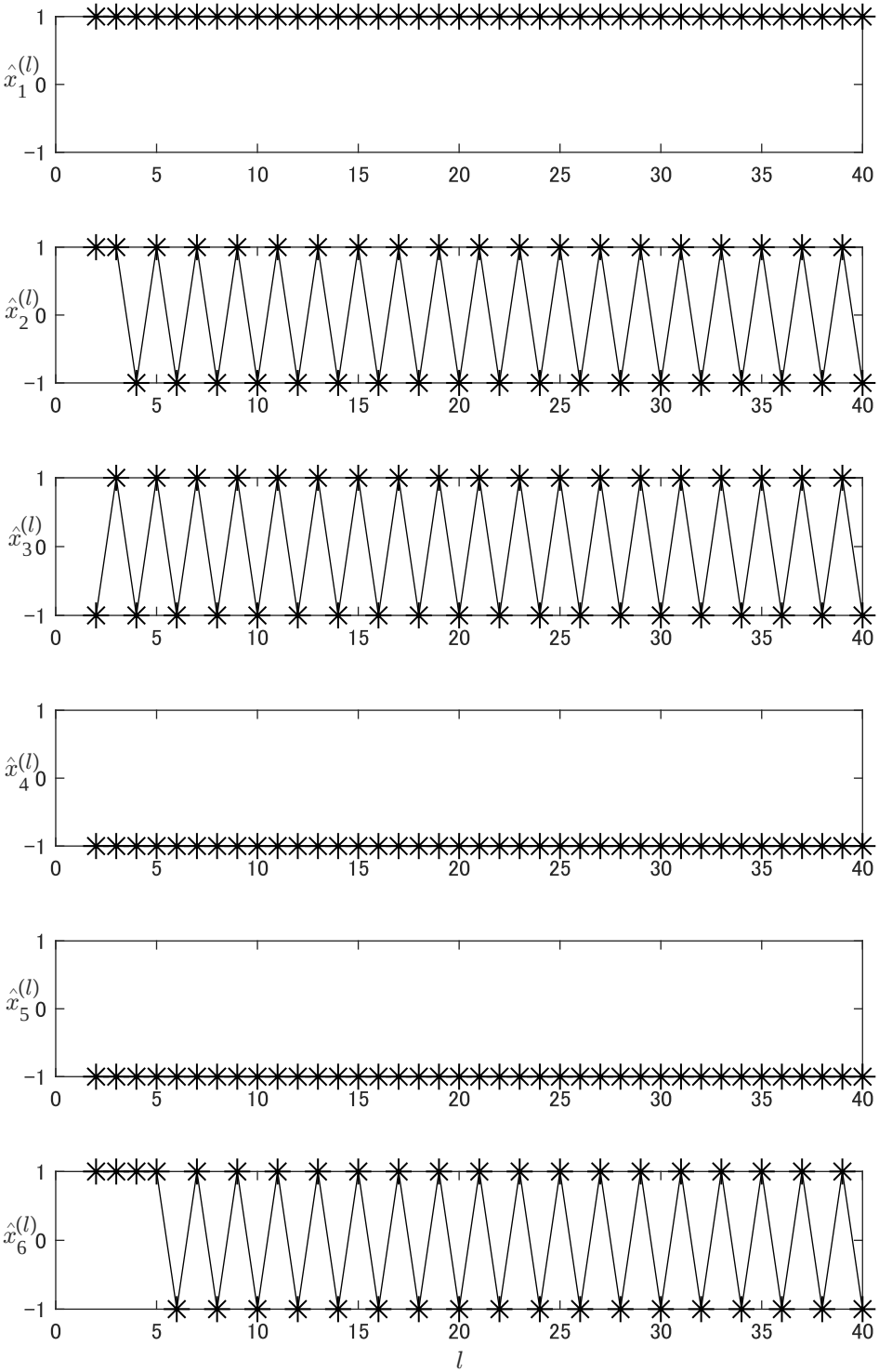


図 3.12: $\hat{x}_j^{(l)}$ の時間変化 $(j = 1, 2, \cdots, 12)$.

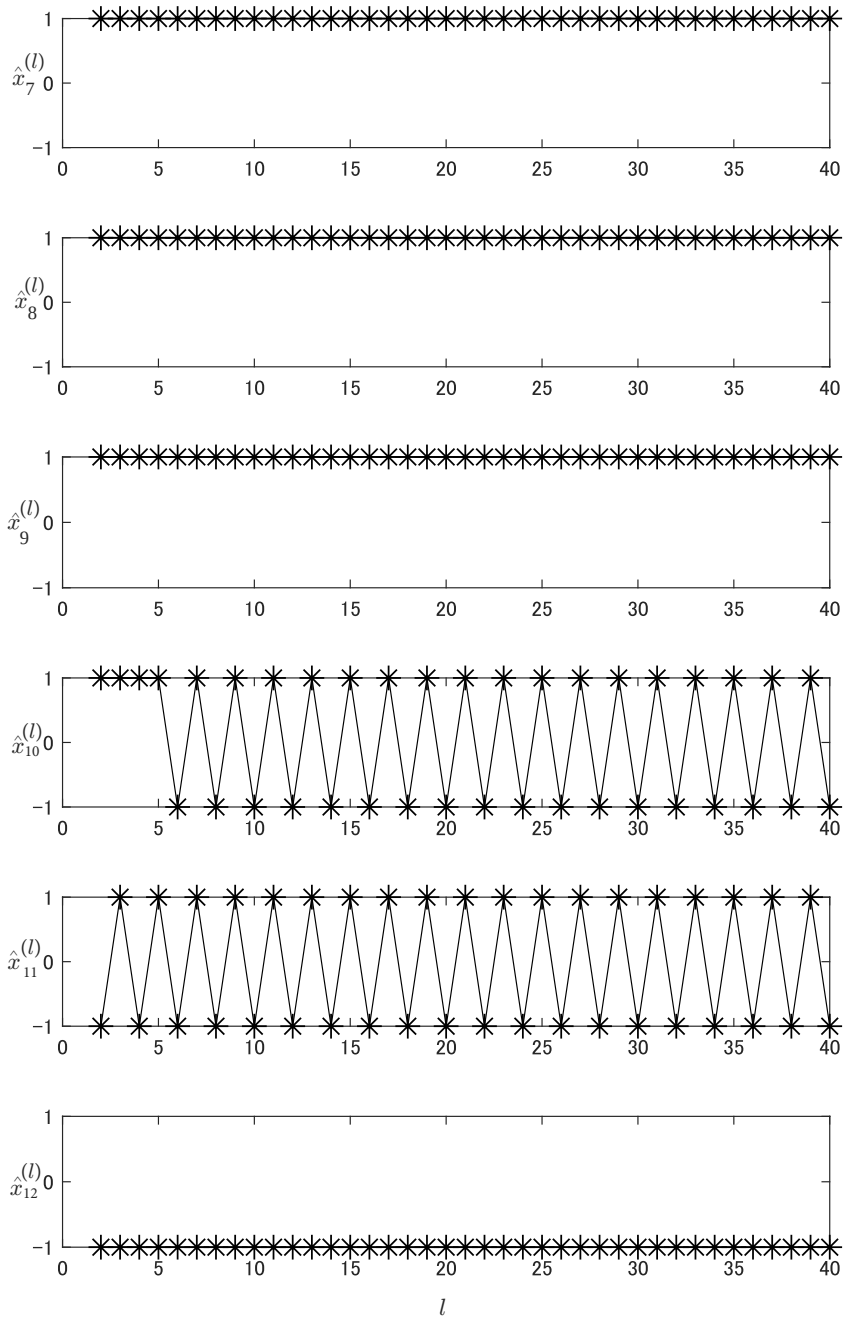


図 3.13: 図 3.12 の続き.

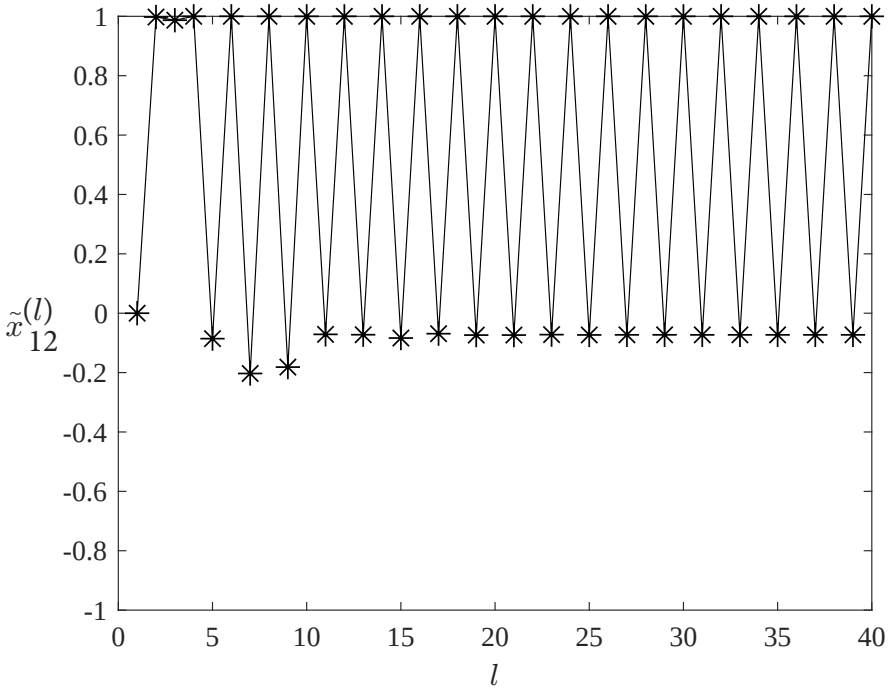
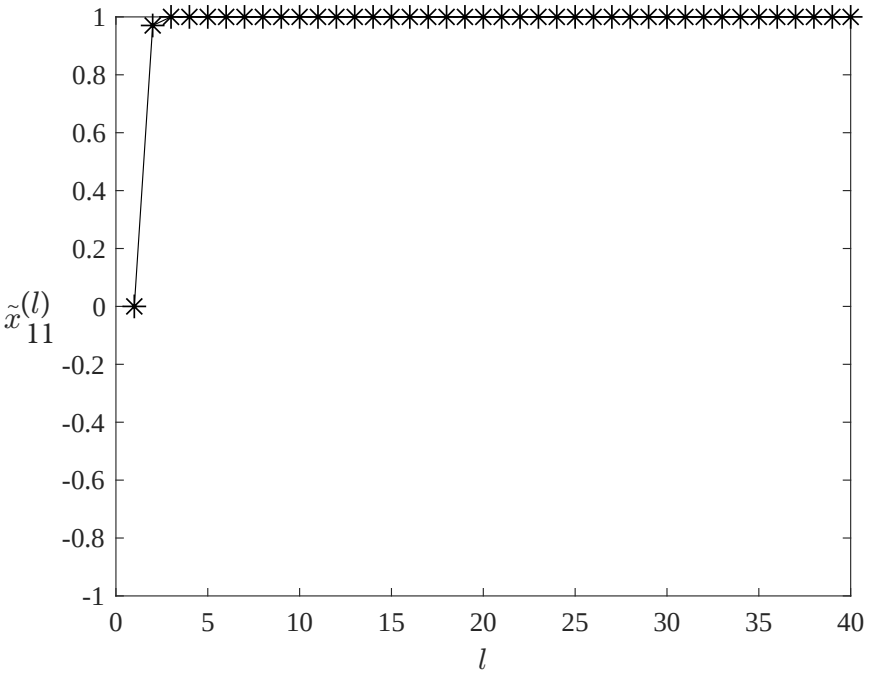
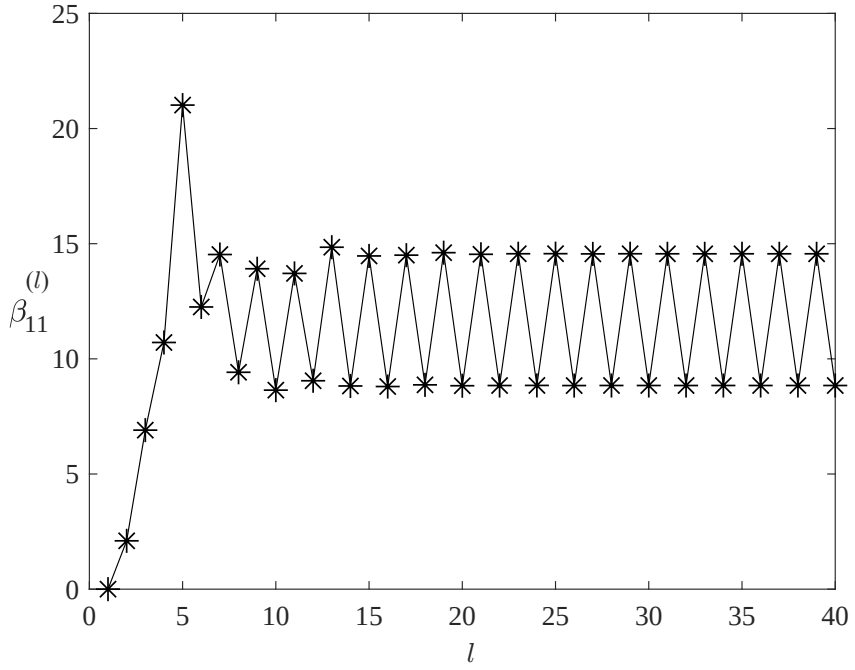


図 3.14: $\tilde{x}_{12}^{(l)}$ の時間変化.



(a) $\tilde{x}_{11}^{(l)}$ の時間変化.



(b) $\beta_{11}^{(l)}$ の時間変化.

図 3.15: 図 3.12 のときの $\tilde{x}_{11}^{(l)}$ と $\beta_{11}^{(l)}$ の時間変化.

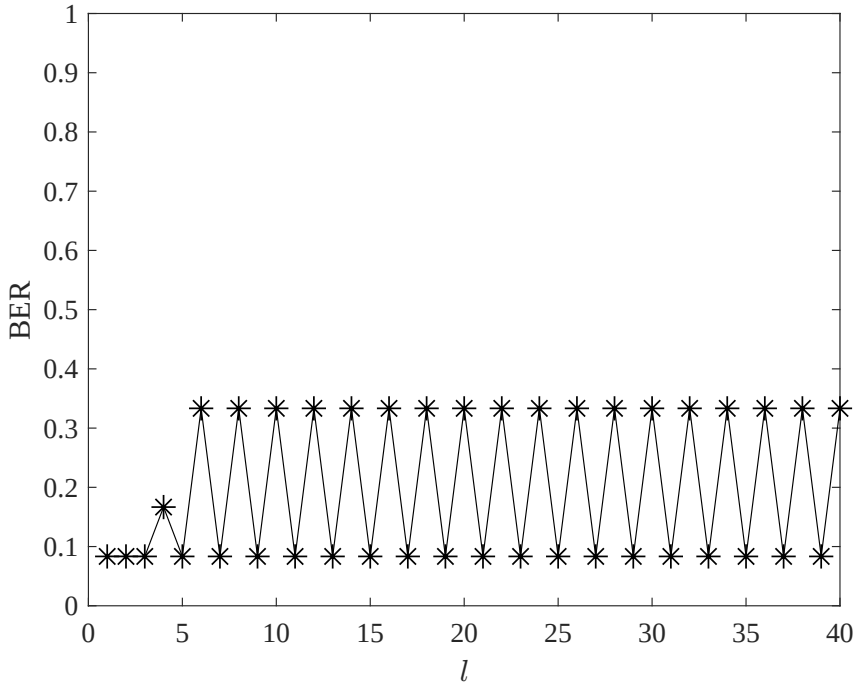


図 3.16: BER の時間変化.

3.3.2 時間変化の分類と BP 復号の誤り

状態変数であるレプリカ信号をみることで，BP 復号過程が幾つかの運動状態（アトラクター）に至ることがわかった．正しく復号できた場合は全て固定点（case1）に至るので，ここでは正しく復号できない場合（誤り）に，状態変数が各運動状態に至る割合を調べる．当然，無線通信では復号にかかる計算量が同等であれば，BER が低い方がよい．BER を悪くしている振る舞いを把握することは，今後の BP 復号の性能改善に大きな指針になる．

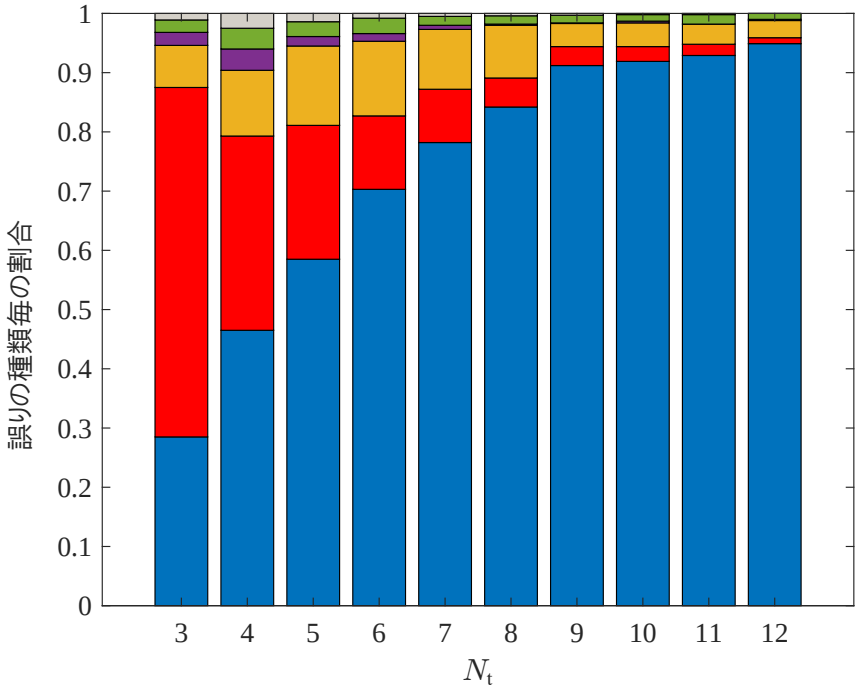


図 3.17: BP 復号における誤りの種類．横軸はアンテナ数 N_{t} で，縦軸は各誤りの割合．各アンテナ数毎に正しく復号できなかったものを 1000 ケース集めたもの．N_{iter} までに到達した運動状態を 2 周期（青），3 周期（紫），4 周期（緑），5 周期（灰色），固定点（赤）で表す．なお，アスタリスク（黄）は，$N_{\mathrm{iter}} = 20$ でも一定の運動状態に至っていないものである．BP 繰り返しの規定回数は $N_{\mathrm{iter}} = 20$，ノイズ $\vec{n}$ の分散は $\sigma_{\mathrm{n}}^2 = 0$（SNR=$\infty$[dB]），変調方式は BPSK とする．

図 3.17 は各アンテナ数での数値実験により正しく復号できなかったものを，誤りの種類（アトラクター）毎に分類し，その比率を表したものである．BP 繰り返しの規定回数 N_{iter} は 20 とする．$N_{\mathrm{t}} > 12$ では，BER が低く，誤りケースの収集に膨大な時間を要するため，$N_{\mathrm{t}} \leq 12$ で数値実験を行う．MIMO（$N_{\mathrm{t}} \leq 4$）ではレプリカ信号が固定点に至り，誤りに陥る割合が大きい．N_{t} が大きくなると，レプリカ信号が 2 周期運動に至り，誤りに陥る割合が大きくなる（その他の誤りの割合は小さくなる）．この傾向が $N_{\mathrm{t}} > 12$ でも続くと考えると，大規模 MIMO（$N_{\mathrm{t}} \geq 10$）での誤りは 2 周期運動に起因するものが多くを占めると予想される．

ここで，図 3.17 のアスタリスクで表される振る舞いは $N_{\mathrm{iter}} = 20$ までに周期運動にも固定点にも至っていないもので，次にこれが，どのようなものか調べてみる．まず，$\vec{\hat{x}}^{(l)}$ をみると（図 3.18，3.19），l に対し，最初カオス的に時間変化し，$l \geq 23$ である値に収束している．時間変化の激しい $\hat{x}_9^{(l)}$ に着目し，それと直接関係する $\tilde{x}_{19}^{(l)}$ の時間変化をみると（図 3.20

(a))，これも同様に不規則（カオス的）に動き，$l \geq 23$ である値に収束している．BER の時間変化をみると（図 3.20（b））$l < 23$ で正だが，それ以降は 0 となる．つまり，$\tilde{x}_{kj}^{(l)}$ がカオス的に動く中で，ある固定点に陥いると考えられる．多くのサンプルを調べると，カオス的に振る舞う場合には $N_{\mathrm{iter}} \geq 40$ で固定点に至り，それが正しく復号できる場合と正しく復号できない場合どちらも存在する．非線形力学系では，あるアトラクターに至る過程がカオス的な振る舞いを示すものをカオス的トランジェント（過渡現象）と呼ぶ [3]．これもその一つである．

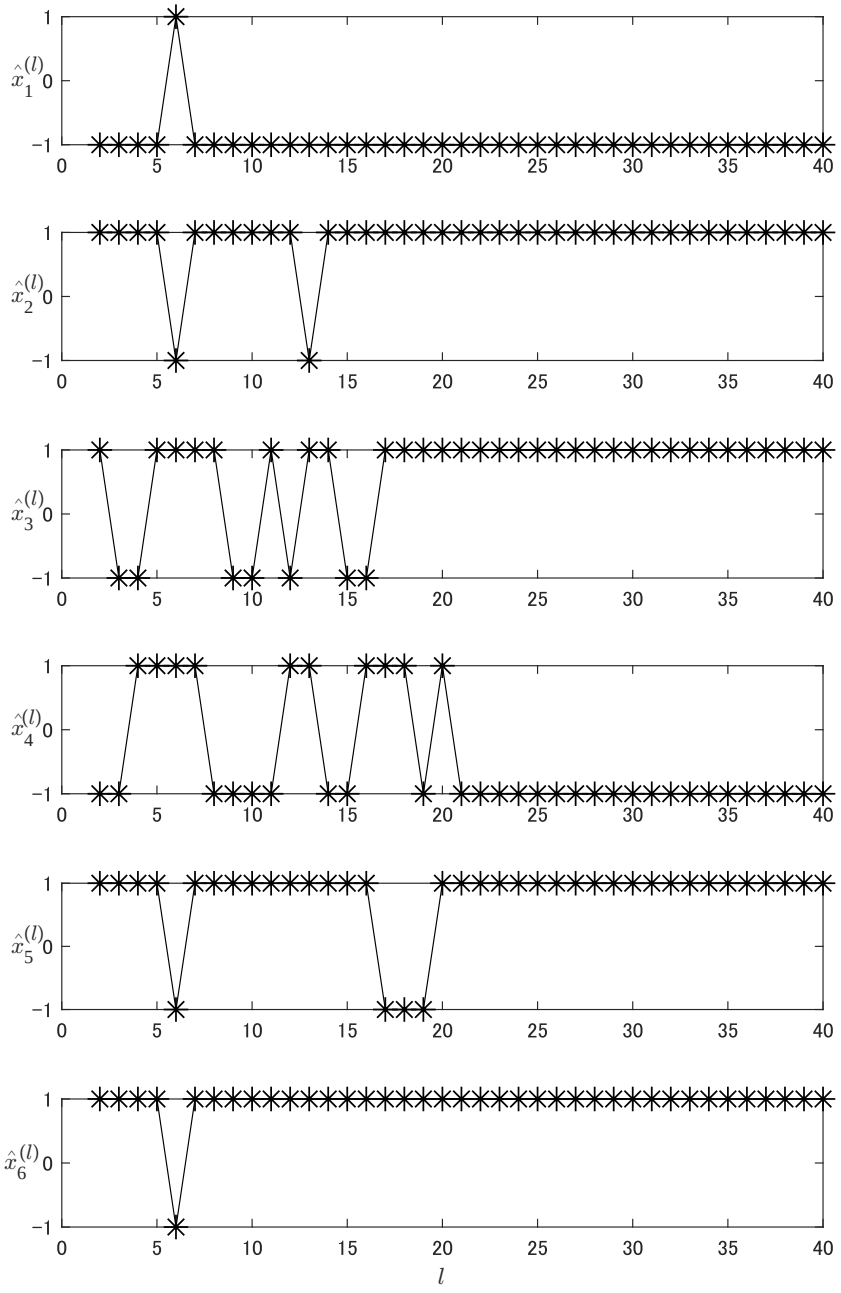


図 3.18: $\hat{x}_j^{(l)}$ の時間変化 $(j = 1, 2, \cdots, 12)$.
$N_{\mathrm{t}} = N_{\mathrm{r}} = 12$，ノイズ $\vec{n}$ の分散は $\sigma_{\mathrm{n}}^2 = 0$（SNR=$\infty$[dB]）.

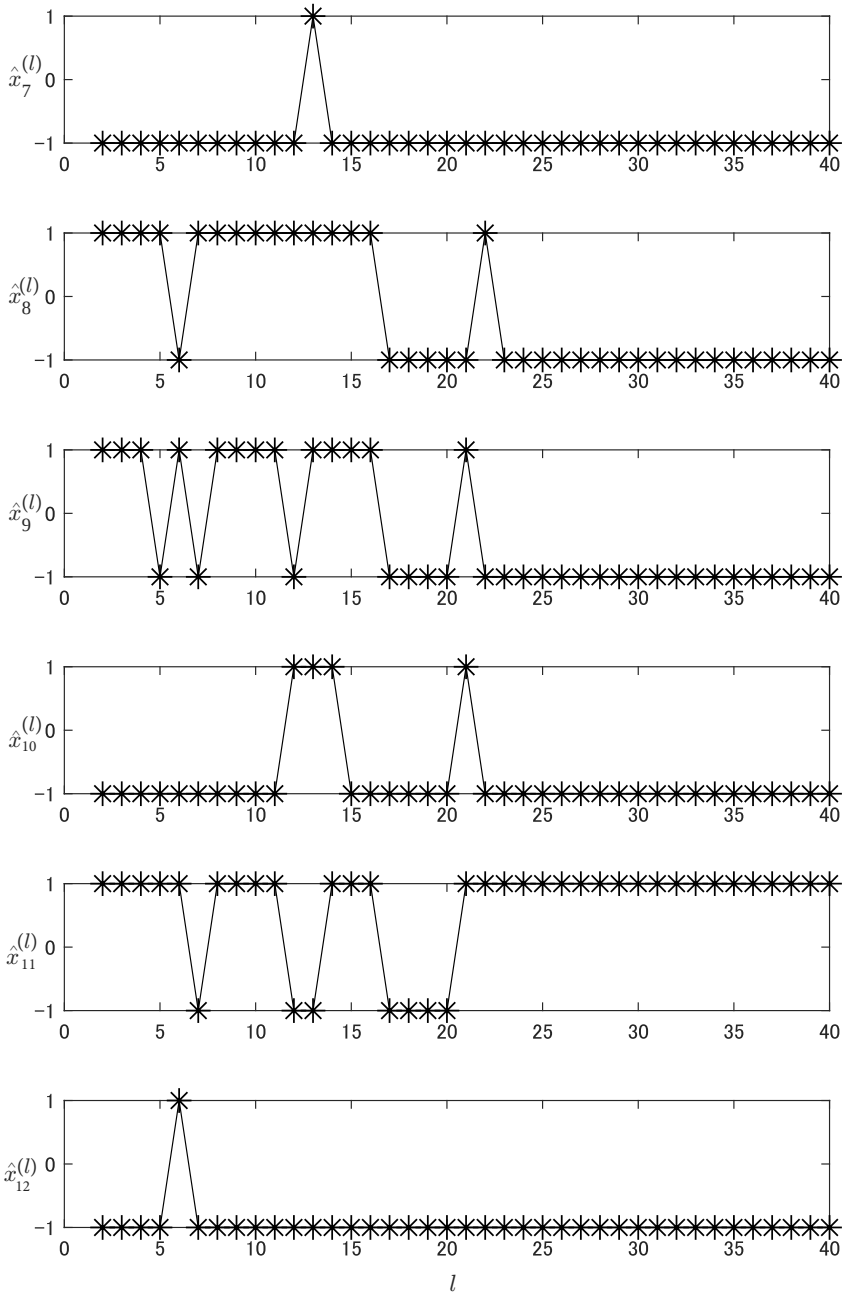
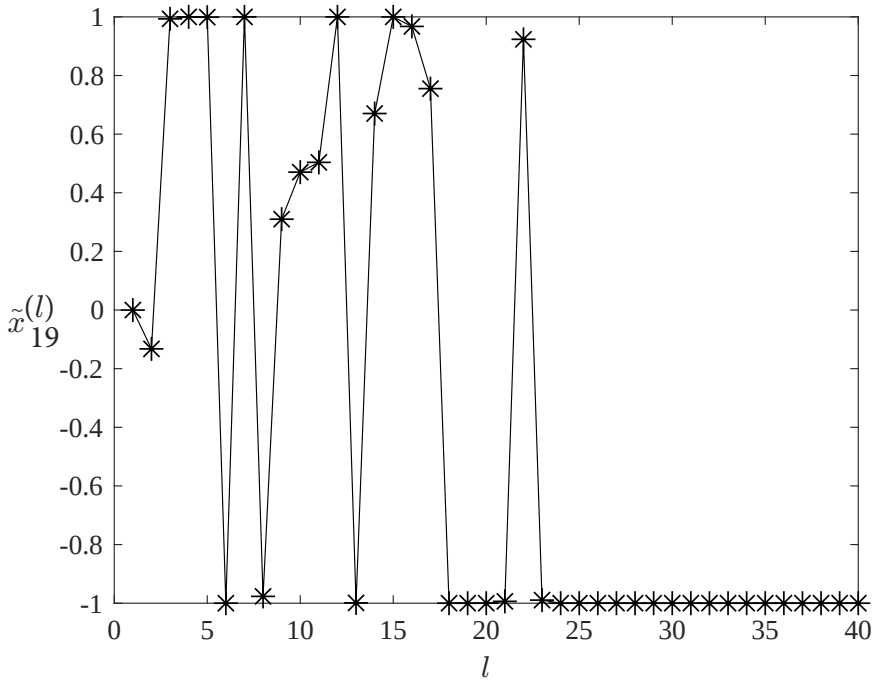
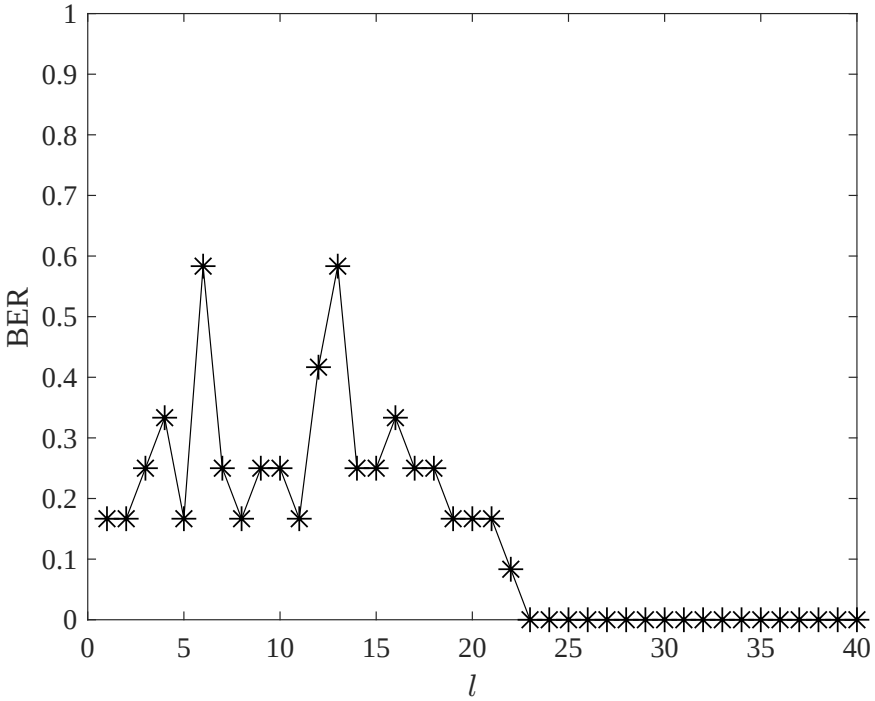


図 3.19: 図 3.18 の続き.



(a) $\tilde{x}_{19}^{(l)}$ の時間変化.



(b) BER の時間変化.

図 3.20: 図 3.18 のときの $\tilde{x}_{19}^{(l)}$ と BER の時間変化.

3.3.3 考察と議論

BP 復号の状態変数の時間変化は固定点に至る，周期運動に至るの 2 つの種類を示す．周期運動に至る場合は，当然，正しく復号できていないが，固定点に至る場合は，正しく復号できているケースとできていないケースがあり，その違いは運動状態を見てもわからない．しかし，大規模 MIMO（$N_{\mathrm{t}} \leq 10$）で正しく復号できない場合は，固定点に至るよりも 2 周期運動に至ることが圧倒的に多いため，2 周期運動を回避することで BER を大きく（1/10 程度）下げることができると予想される．また，図 3.4 が 2 周期的に振る舞う原因は，大規模 MIMO の誤りが 2 周期運動に至りやすく，その結果が反映されたためだと考えられる．

図 3.17 は，様々な $\mathbf{H}$ と $\vec{b}$ に対して，到達するアトラクターの分類を行い，その比率を表したものである．これは，結果的に固定した初期値でのベイスン構造の統計性を表していると考えられる．また，$\mathbf{H}$ と $\vec{b}$ を固定し初期値を変化させた場合のベイスン構造や，そのベイスン構造が $\mathbf{H}$ や $\vec{b}$ の変化でどのように変わるのかという点に非常に興味があるが，それは今後の課題としたい．

第4章　BP復号を用いた大規模MIMOへのカオス暗号の導入

この章では，大容量無線通信の情報安全性を向上させるため，カオスを示す非線形写像を用いたカオス暗号を導入する．まず，先行研究のカオスMIMOを大規模MIMO化し，BP復号を用いることを検討する．[1]しかし，それはカオス暗号とBP復号の不整合により上手くいかない．その原因を4.1節でBP復号の写像系とカオス暗号の写像系を詳しく調べることで明らかにする．4.2節では，その原因を取り除いたカオス暗号（BP適合カオス暗号）を構築する．さらに，BP適合カオス暗号を導入することによって，無暗号化時（BPSK）と比べて推定精度が低下する原因を明らかにし，それを回避した方法（改良BP適合カオス暗号）を見出す．

4.1　カオスMIMOとBP復号の不整合

2.3.3節で紹介したカオスMIMOは畳み込み符号により，1つの送信シンボルに複数の送信ビットが含んでおり（式（2.25））, これが原因でBP復号に適合できない．その理由をここで明らかにする．BP復号では，送信シンボルがとり得る2状態 $x_j = \mp 1,\ (b_j = 0, 1)$ を式（2.34）より評価する．カオスMIMOの場合，式（2.34）の $x_j(\cdot)$ の部分を式（2.25）で書き換えると

$$\alpha_{kj}^{(l)} = \log \frac{\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, x_j(b_1, b_2, \cdots, b_{j-1}, b_j = 1, \vec{C}_0) \right)}{\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)} \,\middle|\, x_j(b_1, b_2, \cdots, b_{j-1}, b_j = 0, \vec{C}_0) \right)}, \tag{4.1}$$

となる．これを評価するためには，$x_j(b_1, b_2, \cdots, b_{j-1}, b_j = 1, \vec{C}_0)$ で表されるカオス暗号化を要するが，これには $\{b_1, b_2, \cdots, b_{j-1}\}$ の送信ビットの情報が必要である．ここで，$\{b_1, b_2, \cdots, b_{j-1}\}$ には前回のBP繰り返し

[1] この検討は今まで行われておらず，著者の研究が初めての報告となる．

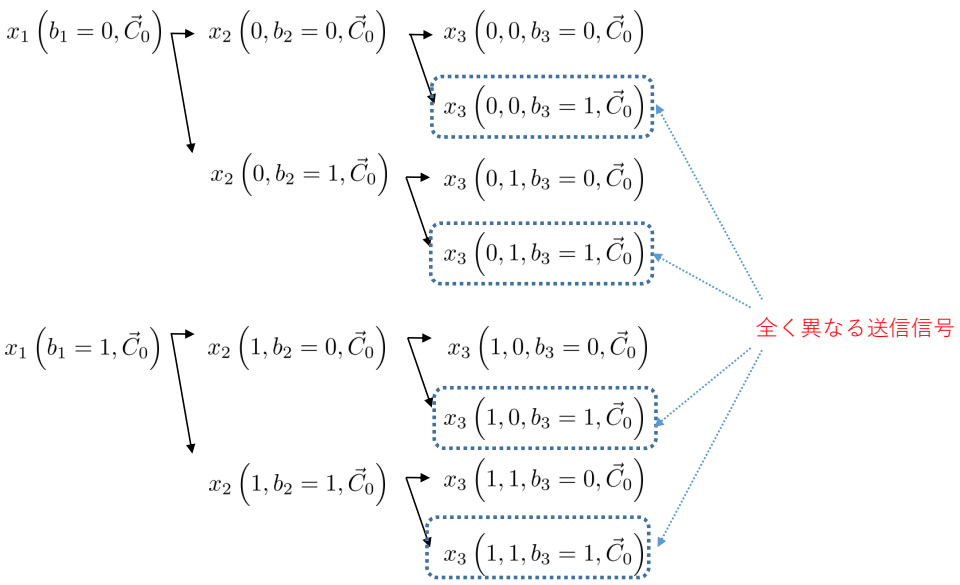


図 4.1: カオス MIMO でのカオス暗号を行った場合の送信シンボルの候補．$N_{\mathrm{t}}=3$ とし，$\vec{b}$ の全ての組み合わせを暗号化した場合の送信信号を表す．各送信シンボル生成にはカオスを用いているので，$(b_1,b_2,1)=(0,0,1)$，$(0,1,1)$，$(1,0,1)$，$(1,1,1)$ によって，$b_3=1$ から定まる x_3 が全く異なるものとなる．

計算で得られた推定値 $\{\hat{b}_1^{(l-1)},\hat{b}_2^{(l-1)},\cdots,\hat{b}_{j-1}^{(l-1)}\}$ を用いることになり，対数尤度比は

$$\alpha_{kj}^{(l)}=\log\frac{\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)}\,\middle|\,x_j(\hat{b}_1^{(l-1)},\hat{b}_2^{(l-1)},\cdots,\hat{b}_{j-1}^{(l-1)},b_j=1,\vec{C}_0)\right)}{\mathrm{Prob}\left(\tilde{y}_{kj}^{(l)}\,\middle|\,x_j(\hat{b}_1^{(l-1)},\hat{b}_2^{(l-1)},\cdots,\hat{b}_{j-1}^{(l-1)},b_j=0,\vec{C}_0)\right)},\quad(4.2)$$

となる．ここで，$b_{j-1}^{(l-1)}$ は式 (3.14) とする．これで形式的に BP 復号の力学系となり，レプリカ信号が送信信号に等しい場合が固定点となる．しかし，$\hat{b}_1^{(l-1)},\hat{b}_2^{(l-1)},\cdots,\hat{b}_{j-1}^{(l-1)}$ の 1 つでも送信ビットと異なっていると，$b_j=0,1$ に対する x_j はカオス暗号化されているので，2 章で説明した初期値鋭敏性により送信シンボルと全く異なるものとなる（図 4.1）．従って，その場合 $\alpha_{kj}^{(l)}$ は，分子分母ともに誤った送信シンボル候補で評価されるため，正しい推定とならない．さらに，レプリカ信号 $\tilde{x}_{kj}^{(l)}$ にも誤った送信シンボル候補を用いるため，次の BP 繰り返し計算で誤った送信シンボル候補により PIC を行う．それにより，全送信ビットの評価に影響を与え，送信ビットの推定に誤りを起こさせる可能性がある．つまり，推定値のうち 1

ビットでも異なるだけで，それ以降のビットの推定は全く異なる送信シンボル候補を用いることになり，繰り返し計算により全ての送信ビットの評価にその影響が波及してしまう．そのため，カオス MIMO のカオス暗号を用いた場合，BP 復号は推定が全くできなくなってしまう．

4.2 BP 適合カオス暗号の構築

前節の問題を解決するため，カオス暗号から畳み込みを除去し BP 復号に適合できるよう再構築を行う．具体的には，式（2.18）と同様に M 個の暗号鍵

$$\vec{C} = [C_1, C_2, \cdots, C_M], \tag{4.3}$$

を用意し，式（2.19），（2.21）を

$$Z_{mj} = f\left(\mathrm{Re}[C_m], b_j\right) + if\left(\mathrm{Im}[C_m], b_j\right), \tag{4.4}$$

$$c_{mj} = g^{j\times l}\left(\mathrm{Re}[Z_{mj}]\right) + ig^{j\times l}\left(\mathrm{Im}[Z_{mj}]\right), \tag{4.5}$$

と置き換える．ここで $f(\cdot)$，$g(\cdot)$ はそれぞれ式（2.20），式（2.22）である．このとき，Z_{mj} および c_{mj} は b_j と C_m のみで生成されるため，送信シンボル間に相関は無くなる．これにより式（2.25）を

$$x_j = x_j(b_j, \vec{C}), \tag{4.6}$$

に変える．1 つの送信シンボルに 1 つの送信ビットと $\vec{C}$ しか含まれていないため，1 回の BP 繰り返し計算の中で送信ビットを個別に推定する BP 復号においても適用できると予想される．この暗号手法を BP 適合カオス暗号とする．なお，$|\beta_{kj}^{(l)}| \to \infty$ の極限でレプリカ信号が真の送信シンボルに収束するように，式（2.37）を

$$\tilde{x}_{kj}^{(l)} = \begin{cases} \left|\tanh\left(\dfrac{\beta_{kj}^{(l)}}{2}\right)\right| \cdot x_j\left(1, \vec{C}\right), & \beta_{kj}^{(l)} \geq 0 \\ \left|\tanh\left(\dfrac{\beta_{kj}^{(l)}}{2}\right)\right| \cdot x_j\left(0, \vec{C}\right), & \beta_{kj}^{(l)} < 0, \end{cases} \tag{4.7}$$

と変更する．

4.2.1 BP 適合カオス暗号を用いた BP 復号の数値実験

BP 適合カオス暗号を BP 復号と合わせた際の性能を数値実験にて確認する．ただし，これ以降のカオス暗号で，カオス写像回数 $l = 10$，暗号鍵の要素数 $M = 10$ と設定する．暗号鍵の要素は複素数であり，実部と虚部をそれぞれ $[0, 1]$ の一様分布に従う乱数とし，要素間でも実部と虚部の間でも相関のないものとする．

復号にかかる計算時間

表 4.1: BP 適合カオス暗号の有無による復号にかかる計算時間．
全ての値は 100 試行分の合計時間を BPSK-MLD の $N_{\mathrm{t}} = 2$ の合計で規格化している．なお，受信アンテナ数は $N_{\mathrm{r}} = N_{\mathrm{t}}$, BP 繰り返しの規定回数を $N_{\mathrm{iter}} = 5$，ノイズ $\vec{n}$ の分散を $\sigma_{\mathrm{n}}^2 = 10^{-2}$（SNR=20 [dB]）とする．

model \ N_{t}	2	4	8	12	16	32	64
BP 適合カオス暗号-BP	1.8	4.9	13.5	30.1	55.1	226.0	1007.0
BPSK-BP	0.5	1.4	5.3	11.2	20.0	82.3	392.6
BPSK-MLD	1	5.6	131.3	3053.4	10000 以上		

表 4.1 では，復号にかかる計算時間を BP 適合カオス暗号に BP 復号用いた手法（BP 適合カオス暗号-BP），BPSK に BP 復号を用いた手法（BPSK-BP）および BPSK に MLD を用いた手法（BPSK-MLD）の 3 つを比較している．N_{t} が小さいときは，BP 復号と MLD の計算時間に大きな差はないが，N_{t} が増えると差は激しく増大し，MLD が大規模 MIMO に適さないことがわかる．一方，BP 適合カオス暗号-BP は，暗号を復号するための写像（式（4.4））の分だけ計算量が増え，BPSK-BP に比べ計算時間が大きいが，N_{t} の増加に対し計算時間の増加する速さは，MLD に比べ緩やかであり，BPSK-BP と同程度である（約 3 倍）．そのため，BP 適合カオス暗号は，大規模 MIMO において，現実的な計算時間で復号が可能であると言える．

SNR における BER の比較

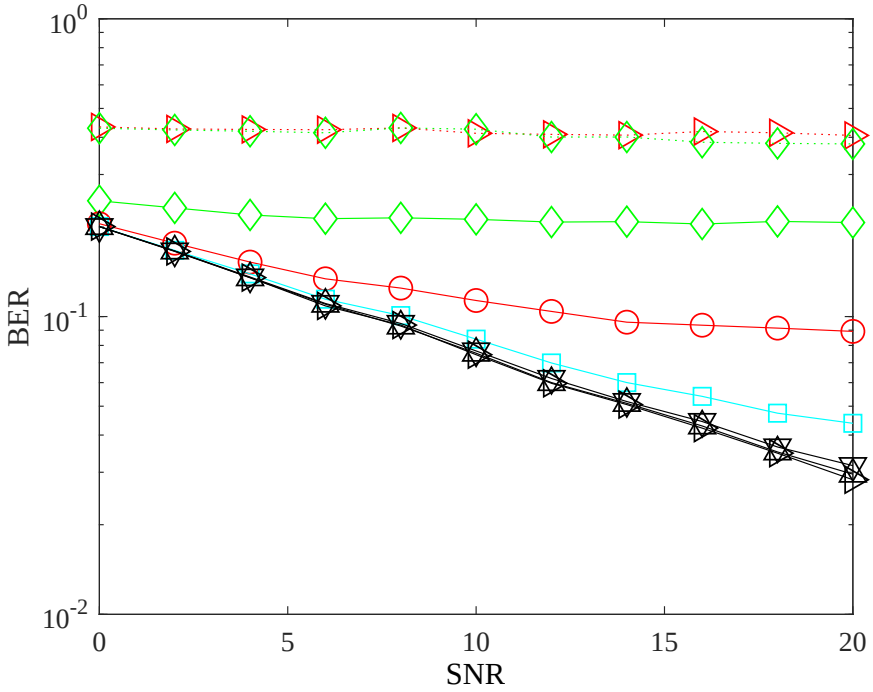


図 4.2: BP 適合カオス暗号-BP とカオス MIMO-BP の BER を SNR= 0 ∼ 20 について示したもの．
BER は 4000 試行の平均値である．なお，送受信アンテナ数 $N_{\mathrm{t}} = N_{\mathrm{r}} = 12$，ノイズ $\vec{n}$ の分散は ${\sigma_{\mathrm{n}}}^2 = 10^{-\mathrm{SNR}/10}$ とする．実線は BP 適合カオス暗号-BP，破線はカオス MIMO-BP を表す．BP 繰り返しの規定回数を $N_{\mathrm{iter}} = 1$（菱形），2（円），3（四角），4（下三角），5（三角）6（右三角）と表し，カオス MIMO-BP は $N_{\mathrm{iter}} = 1$（菱形），6（右三角）のみをプロットする．

図 4.2 では，BP 適合カオス暗号-BP とカオス MIMO に BP 復号を適用した手法（カオス MIMO-BP）の BER を SNR を変えて比較している．前節で予想したように，カオス MIMO-BP は SNR によらず BER がほぼ一定値 0.5 をとる（BER ∼ 0.5 は，推定したビットの半分が正解していることになるが，ビットは $b_i \in \{0, 1\}$ の 2 値しかとらないため，偶然正解していることにあたる）．一方，BP 適合カオス暗号-BP の結果は，SNR が大きくなると BER は低下し，SNR が大きい場合，N_{iter} を増やすと BER が低下している．この結果から BP 適合カオス暗号-BP は，BP 復号に適合したカオス暗号であることが示唆される．

BP 適合カオス暗号と BPSK の BER の比較

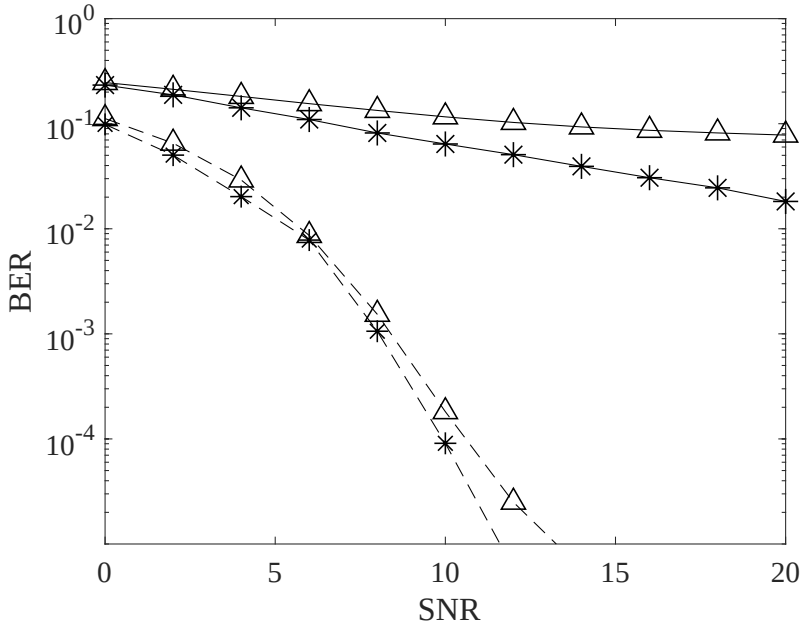


図 4.3: BP 適合カオス暗号-BP と BPSK-BP の SNR に対する BER.
BER は 10000 試行の平均値である．なお，送受信アンテナ数 $N_{\mathrm{t}} = N_{\mathrm{r}} = 12$，ノイズ $\vec{n}$ の分散は ${\sigma_{\mathrm{n}}}^2 = 10^{-\mathrm{SNR}/10}$ とする．BP 適合カオス暗号-BP は三角に実線，BPSK-BP は三角に破線，BP 繰り返しの規定回数は $N_{\mathrm{iter}} = 5$ とする．BP 適合カオス暗号-MLD はアスタリスクに実線，BPSK-MLD はアスタリスクに破線とする．BPSK の結果でシンボルが表示されていない領域は，試行中に誤りがなかったため．

一般に，暗号を導入することで，情報安全性の向上と引き換えに BER が増加する．そこで，ここでは BP 適合カオス暗号が推定精度に与える影響を調べる．図 4.3 に，BP 適合カオス暗号-BP，BPSK-BP，BP 適合カオス暗号-MLD，および BPSK-MLD の BER を示す．図より，復号方法に BP 復号と MLD のいずれを用いた場合も，BP 適合カオス暗号を導入することで BER が大幅に増加することがわかる．特に，復号法として BP 復号を用いた場合，無線通信における性能の基準値（SNR$\leq$ 20 において BER$\leq 10^{-3}$）を満たさないため，BP 適合カオス暗号はさらなる改善が求められる．そこで以下では，BP 適合カオス暗号の導入に伴って BER が増加する原因を考察し，これを取り除くことで提案手法の改良を行う．

4.2.2 BP 適合カオス暗号における BER 増加の考察

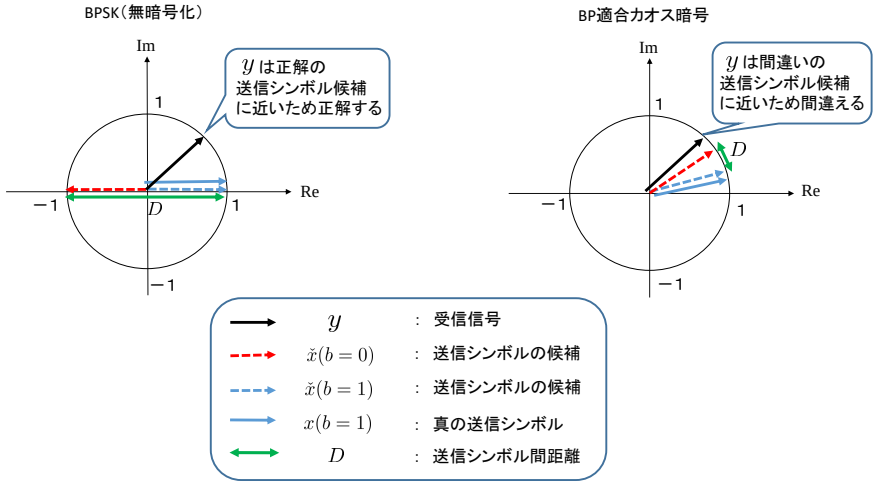


図 4.4: BPSK と BP 適合カオス暗号の送信シンボル間距離.
$N_{\mathrm{t}} = N_{\mathrm{r}} = 1$，通信路情報 $h = 1$ とした際の BPSK と BP 適合カオス暗号での送信シンボル間距離.

BP 適合カオス暗号での BER の増加の原因は，$b = 0, 1$ に対応する 2 つの送信シンボル間距離の減少にあると考えられる．簡単に考えるため，$N_{\mathrm{t}} = N_{\mathrm{r}} = 1$ とし，通信路情報 $h = 1$ とする．この場合の BPSK と BP 適合カオス暗号のときの送信シンボル間距離 D を表したものが図 4.4 である．D は，図 4.4 で表される複素平面上の 2 つの送信シンボル候補間の距離である．受信信号は

$$y = x + n, \tag{4.8}$$

であり，n は複素ガウス分布 $\mathcal{CN}(0, \sigma_{\mathrm{n}}^2)$ に従う乱数である．復号は，2 つの送信シンボル候補の内，受信信号から近い候補を推定結果とする．復号での誤りはノイズが大きくなると起こるが，これはノイズの大きさ σ_{n} だけでなく，送信シンボル間距離 D との大小関係に強く依存する．ノイズの大きさ σ_{n} が送信シンボル間距離 D の大きさより大きくなると，ノイズの効果により，受信信号と誤った送信シンボル候補の距離が小さくなり得るため，受信信号から送信ビットを推定することが困難となる．つまり，ノイズの大きさが同じでも，D が小さくなると誤りを起こしやすくなる．BP 適合カオス暗号では，BPSK で $D = 2$ であった送信シンボル間距離が，$0 \leq D \leq 2$ と小さくなるため，誤りを起こしやすくなり，BPSK に比べて BER が増加すると考えられる．

4.3 BP 適合カオス暗号の改良

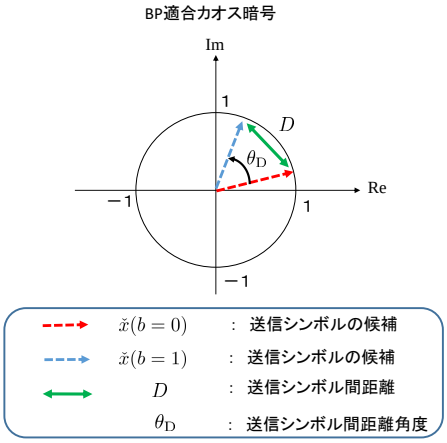


図 4.5: 送信シンボル間距離と送信シンボル間距離角度.

前節の問題を回避するためには，一定の送信シンボル間距離を保てばよい．そこで，その機構を備えた改良 BP 適合カオス暗号を構築する．信号間距離を一定に保つことで，送信シンボル間距離が減少することなく暗号化し，ノイズにおける誤りに強くなると考えられる．ここで，図 4.5 で表される送信シンボル間距離角度 θ_{D} は，送信電力を 1 とすると，D より

$$\theta_{\mathrm{D}} = 2\arcsin\left(\frac{D}{2}\right), \tag{4.9}$$

で表せる．本手法では，全ての送信シンボル間距離の角度を任意の設定角度 θ_{D} に設定できるカオス暗号とし，その詳細な手順は以下に示す．式（4.3）を暗号鍵とし，その要素である C_m を初期値としてカオス関数 $g(*)$ で $j \times l$ 回写像することで，複素変数

$$c_{mj} = g^{j\times l}\left(\mathrm{Re}[C_m]\right) + ig^{j\times l}\left(\mathrm{Im}[C_m]\right), \tag{4.10}$$

を得る．ただし，ここでカオス関数 $g(\cdot)$ は式（2.22）とする．暗号化された送信シンボル x_j は，式（2.23）を用いて c_{mj} から生成される s_j と設定角度 θ_{D} を用いて

$$x_k = \begin{cases} \exp\left[i\tan^{-1}\dfrac{\mathrm{Im}[s_j]}{\mathrm{Re}[s_j]}\right], & b_j = 0 \\ \exp\left[i\left(\tan^{-1}\dfrac{\mathrm{Im}[s_j]}{\mathrm{Re}[s_j]} + \theta_{\mathrm{D}}\right)\right], & b_j = 1, \end{cases} \tag{4.11}$$

とする．上記において，送信シンボル間距離が大きくなるように角度 θ_{D} を設定することで，推定精度が向上すると期待される．また，送信シンボ

ル間距離を最大にする $\theta_{\mathrm{D}} = \pi$ を採用することで，本提案手法における最高の推定精度を実現できると期待される．

4.3.1 改良 BP 適合カオス暗号の数値実験

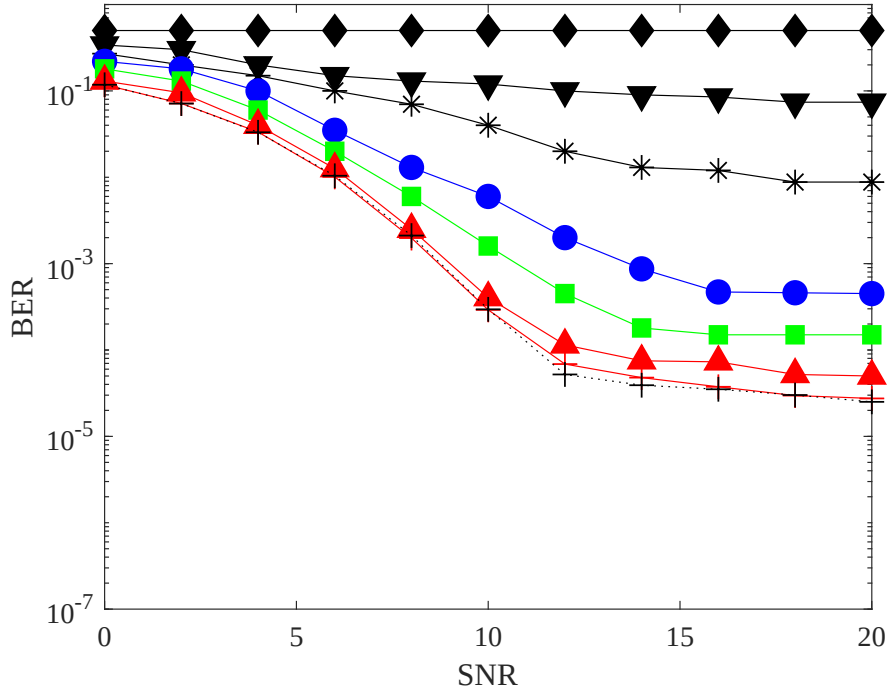


図 4.6: θ_{D} の変化に対する改良 BP 適合カオス暗号-BP の BER の変化．BER は 100000 試行の平均値である．なお，送受信アンテナ数 $N_{\mathrm{t}} = N_{\mathrm{r}} = 12$，ノイズ $\vec{n}$ の分散は ${\sigma_{\mathrm{n}}}^2 = 10^{-\mathrm{SNR}/10}$，BP 繰り返しの規定回数は $N_{\mathrm{iter}} = 20$ とする．送信シンボル間距離角度を $\theta_{\mathrm{D}} = \pi/18$（菱形），$3\pi/18$（下三角），$5\pi/18$（アスタリスク），$7\pi/18$（丸），$9\pi/18$（四角），$13\pi/18$（三角），$\pi$（十字）と表し，BPSK-BP の結果を破線（十字）で表す．

数値実験では，改良 BP 適合カオス暗号-BP の θ_{D} を様々な値に設定し，BER を評価する．前節で予想したように，θ_{D} を大きくしていくと BER が低下している（図 4.6）．また，BPSK-BP と改良 BP 適合カオス暗号-BP の $\theta_{\mathrm{D}} = \pi$ の BER の結果を比べると同等であることがわかる．

4.3.2 結果の考察

BPSK-BP と改良 BP 適合カオス暗号-BP の $\theta_{\mathrm{D}} = \pi$ の信号間距離はどちらも $D = 2$ であり，復号の際にノイズから受ける影響は同等であると

考えられる．そのため，その 2 つの手法の BER に差がなくなったと考えられる．これらの結果より，BP 適合カオス暗号の BER が高い原因はカオス暗号による送信シンボル間距離の減少だけにあることがわかる．

また，$\theta_{\mathrm{D}} \geq 7\pi/18$ で，無線通信における推定精度の基準値（SNR$\leq$ 20 において BER$\leq 10^{-3}$）を達成している．このため，本提案手法は情報安全性を向上させた大容量無線通信における基礎技術として，工学的応用の可能性が期待できる．

第5章　総括

5.1　本研究のまとめ

本論文では，BP 復号を用いた大規模 MIMO について，非線形力学系としての特性と通信性能改善の面から研究したもので，主に以下の 2 つの研究をまとめたものである．

1. BP 復号を大自由度非線形写像系であると捉え，実用性や性能などの視点から写像系を修正し，その力学系としての性質を調べ，復号性能との関係を議論した．

2. カオス MIMO で提案されているカオス暗号が BP 復号に適合しない原因を明らかにし，その上で，BP 復号に適合するカオス暗号を構築した．

これらの結果から，大規模 MIMO に，BP 復号とカオス暗号を導入する手法を見出し，情報安全性を向上させた大容量無線通信として工学的有用性を示した．

1 章では，研究背景を述べた．

2 章では，無線通信の変遷を述べ，本研究で取り扱う MIMO の枠組みを説明した．また，本研究に関連の深いカオス MIMO と BP 復号の研究を非線形力学系の視点から詳細に紹介し，著者の解釈を交えながらその枠組みを整理した．

3 章は，大規模 MIMO での BP 復号が大自由度非線形力学系であることを指摘し，その力学系の特徴を述べた．そして，それに立脚することで BP 復号の問題点を解消し，繰り返し計算による状態変数の振る舞いを詳細に調べた．

BP 復号の先行研究では，繰り返し計算における残留干渉成分の評価が確立されておらず，送信信号（正解の情報）を用いて評価することで BP 復号の可能性を調べていた（無線通信として実現できる形ではない）．本研究では，力学系の安定固定点に至ることが復号にあたるように疑似残留干渉成分 $\tilde{R}_{kj}^{(l)}$ を定め，その効果を尤度関数の分散に含める方法（本論文では model-（c））が有効であることを，数値実験の結果と考察により明

らかにした．そこでは送信信号ではなく，力学系内で得られる前回のレプリカ信号 $\tilde{x}_{kj}^{(l-1)}$ を用いるので，実際の無線通信で実現できる．

また，BP 復号の力学系を調べ，どのような種類の振る舞いがどの程度存在するかを調べた．そのために状態変数であるレプリカ信号 $\tilde{x}_{kj}^{(l)}$ の時間変化を調べ，それが固定点に至る，周期運動に至るの 2 つに分類されることを明らかにした．同時に，大規模 MIMO では，正しく復号できない場合，誤った固定点ではなく 2 周期運動に至る誤りが多いことを明らかにし，さらなる改善の可能性を示した．

4 章では，BP 復号を用いた大規模 MIMO に適合できるカオス暗号を構成した．まず，カオス MIMO のカオス暗号は送信シンボル間に相関のある暗号であるため，BP 復号の各回では送信信号を独立に推定する BP 復号は機能しない（復号できない）ことを力学系的な視点から明らかにした．そこで，送信シンボル間の相関を無くした暗号化を検討し，暗号化に伴う送信シンボル間距離の減少を回避することが可能であることを示した（改良 BP 適合カオス暗号）．その数値実験により，改良 BP 適合カオス暗号に BP 復号を適用することで，暗号化しているにもかかわらず無暗号化（BPSK）時に BP 復号を適用した場合と同等の推定精度であること，無線通信での推定精度の基準値を達成することを示した．以上の研究結果より，BP 復号を用いた大規模 MIMO に改良 BP 適合カオス暗号を用いる手法は，情報安全性を向上させた大容量無線通信として期待できることを明らかにした．

5.2 課題と展望

本研究の課題として，以下の 4 つを挙げる．

1 つ目は，BP 復号の力学系のベイスン構造の調査である．ベイスン構造の把握は初期値によりどのようなアトラクターに至るかを知ることができるため，BP 復号において重要である．今回の研究では，3.3.2 節で述べたように，一部のベイスン構造の調査のみとなってしまっている．そのため，広範囲のベイスンがどのような構造になっているかを調べられていない．この構造を把握し，適切な初期値に変更する方法を見出すことで，より正しく復号でき，推定精度をさらに向上させる方法を構築できる可能性がある．

2 つ目は，BP 復号におけるアトラクター周りでの安定性解析である．今回の研究では，BP 復号における推定結果の時間変化を分類しただけで，それらの運動状態の安定性の強さなどを調べていない．安定性解析により，アトラクター周辺の安定性の詳細な構造を知ることで，どのような摂動を加えると，正しく復号できる他のアトラクターに移るのかを知ること

ができる．これにより，正しく復号できない場合の固定点や周期運動に摂動を加えることで，さらに推定精度が向上すると予想される．

3 つ目は，BP 復号における疑似残留干渉成分の評価方法をさらに調べることである．先行研究における送信信号（正解の情報）を用いた場合に比べると，まだ推定精度が高くなる余地がある．そのため，疑似残留干渉成分の振る舞いがより残留干渉成分に近くなる方法を模索する必要がある．今回は，送信信号の代わりに過去のレプリカ信号 $\tilde{x}_{kj}^{(l)}$ を用いたが，推定シンボル $\hat{x}_{j}^{(l)}$ などの代替方法も考えられる．

4 つ目は，情報安全性の評価である．カオス暗号での情報安全性の評価は国内外の研究で課題となっており定まった方法がない．カオス暗号以外の暗号方法の情報安全性の評価指標を調査し，カオス暗号の情報安全性の強度を正しく測れる方法を探る必要がある．これらにより，本研究で行えなかった性能評価や特性把握および更なる性能向上を期待できる．

今後の展望として，BP 法の他の推定への応用や，BP 法が用いられている枠組みでの非線形力学系からのアプローチが考えられる．MIMO では，送信信号の推定以外にも，通信路行列 $\mathbf{H}$ を推定する過程がある．大規模 MIMO になると $\mathbf{H}$ のサイズも大きくなるため，その推定にかかる計算量も当然大きくなる．推定にかかる計算量が大きくなると，1 秒あたりに送信できる情報量が減ってしまうため（通信容量が低下するため），大規模 MIMO 化した利点が小さくなる．そこで BP 法を用いた繰り返し推定を応用し，$\mathbf{H}$ の推定にかかる計算量を低減できるのではないかと考えられる．送信信号の推定において，BP 復号は推定精度と計算量で高水準であるため，$\mathbf{H}$ の推定にも期待できる．本研究では，$\mathbf{H}$ を完全に推定できている状態（知っている状態）で，送信信号を推定しているが，実際の無線通信では，$\mathbf{H}$ の推定精度が送信信号の推定精度に大きく影響する．つまり，BP 法を用いて $\mathbf{H}$ を高精度かつ少ない計算量で推定できれば，送信信号の推定精度と通信容量の向上にも期待でき，大容量無線通信の性能の底上げになると言える．また，序論で紹介した画像修復では BP 法が用いられている．この例でも，BP 法における繰り返し計算を非線形写像系として捉えた研究は殆どなされていない．本研究で，BP 復号を非線形力学系として捉え，その結果から，性能向上の可能性を見出したように，画像修復でも同じことが行えると考えられる．性能向上だけでなく，その力学系のベイスン構造や状態変数の時間変化を把握するなどの理学的な興味も尽きない．これらは，画像修復での BP 法だけでなく，一定の規則による繰り返し計算を行うものであれば同様であるため，幅広い研究対象があると言える．

謝辞

本研究を行うにあたり，多忙な中，ご指導，ご助言を頂きました，指導教員の秦浩起准教授，同研究室の秦重史准教授に深く感謝いたします．社会人であり，修士課程まで他大学である私を受け入れてくださっただけでなく，丁寧かつ熱心な指導，また，公私ともに様々な配慮をしてくださり，誠にありがとうございました．今現在の私に対する指導だけでなく，今後の私に必要になることを見据えて指導してくださっていると深く感じました．お二人の指導により経験したことを糧にし，今後さらに精進していく所存でございます．

3 年間の専攻ゼミナールを通じて，藤井伸平教授は様々な助言をくださり，本研究を客観的に見ることができました．半田利弘教授は，本論文をまとめるにあたり，的確な助言をしてくださりました．また，修士課程のときの指導教員である東京工業大学情報理工学院の樺島祥介教授は，論文の内容や投稿に関して助言をしてくださりました．深く感謝いたします．同研究室の学生には，暖かく接していただき，また支援していただき感謝いたします．

参考文献

[1] 合原一幸, 'カオス' (サイエンス社, 1990)

[2] 桑村雅隆, 'パターン形成と分岐理論' (共立出版, 2015)

[3] Ott, E., 'Chaos in Dynamical Systems' (Cambrige University Press, Second edition, 2002)

[4] Kaneko, K., 'Clustering, coding, switching, hierarchical ordering, and control in a network of chaotic ekements,' *Physica D*, 1990, **41**, pp. 137–172

[5] Kaneko, K and Egami, K, 'Glassy dynamics in a spatially distributed dynamical system,' *Phys. Lett. A*, 1993, **174**, pp. 103–110

[6] 甘利俊一, '神経回路網の数理' (産業図書，1978)

[7] Roth, M. W., 'Survey of neural network technology for automatic target recognition,' *IEEE Trans. Neural Netw.*, 1990, **1**, pp. 28–43

[8] Liu, W., Wang, Z., Liu, X., et al. 'A survey of deep neural network architectures and their applications,' *Neurocomputing*, 2017, **234**, pp. 11–26

[9] Chen, C., Seff, A., Kornhauser and A., Xiao, J., 'DeepDriving: Learning Affordance for Direct Perception in Autonomous Driving,' *Proc. IEEE International Conference on Computer Vision(ICCV)*, 2015, pp. 2722–2730

[10] Litjens, G., Kooi, T., Bejnordi, B. E., et al., 'A survey on deep learning in medical image analysis,' *Proc. IEEE International Conference on Computer Vision(ICCV)*, 2017, **42**, pp. 60–88

[11] Katsaggelos, K., Lay, K. 'Maximum Likelihood Blur Identication and Image Restoration Using the EM Algorithm,' *IEEE Trans. Signal Process.*, 1991, **39**, pp. 729–733

[12] Figueiredo, M., Nowak, R. 'An EM algorithm for wavelet-based image restoration,' *IEEE Trans. Image Processing*, 2003, **12**, pp. 906–916

[13] Figueiredo, M., Nowak, R. 'Wavelet-based EM algorithm for multispectral-image restoration,' *IEEE Trans. Geosci. Remote Sens.*, 2009, **47**, pp. 3892–3898

[14] Hasegawa, R., Okada, M. and Miyoshi, S. 'Image Segmentation Using Region-Based Latent Variables and Belief Propagation,' *J. Phys. Soc. Jpn*, 2011, **80**, 093802

[15] Tanaka, K., Kataoka, S., Yasuda, M., et al. 'Bayesian Image Segmentations by Potts Prior and Loopy Belief Propagation,' *J. Phys. Soc. Jpn*, 2014, **83**, 124002

[16] Som, P., Datta, T., Chockalingam, A., Rajan, B.S., et al. 'Improved large-MIMO detection based on damped belief propagation,' *Proc. IEEE Trans. inf. Theory*, Jan. 2010, pp. 1–5

[17] Fukuda, W., Abiko, T., Nishimura, T., et al. 'Low-complexity detection based on belief propagation in a massive MIMO system,' *Proc. IEEE Vehicular Technology Conf. (VTC)* June 2013

[18] Usami, T., Nishimura, T., Ohgane, T., et al. 'BP-based detection of spatially multiplexed 16-QAM signals in a fully massive MIMO system,' *Proc. International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2016

[19] Yang, J., Zhang, C., Liang, X., et al.: 'Improved symbol-based belief propagation detection for large-scale MIMO,' *Proc. IEEE Workshop on Signal Processing Systems (SiPS)* , Oct. 2015

[20] Takahashi, T., Ibi, S., Sampei, S., et al. 'On normalization of matched filter belief in GaBP for large MIMO detection,' *Proc. IEEE Vehicular Technology Conf. (VTC)* , Sept. 2016

[21] F. Long, T. Lv, 'Relaxed belief propagation for MIMO detection,' *Proc. IEEE International Symposium on Information Theory (ISIT)2011*, July 2011

[22] Tano, S., Nishimura, T., Takeo, O., et al., 'A Comparison of Serial and Parallel LLR Updates for LDPC Coded Massive MIMO Detec-

tion with Belief Propagation,' *Proc. IEEE International Symposium on Information Theory and Its Applications (ISITA)* , Oct. 2016

[23] Pretti, M., 'A message passing algorithm with damping,' *Jl. Stat. Mech.: Theory and Practice*, 2005, p11008

[24] Bloch, M., Barros, J. 'Physical-Layer Security' (Cambridge University Press, 2011)

[25] Shiu, Y., Chang, S., Wu, H., et al. 'Physical layer security in wireless networks: a tutorial,' *IEEE Wireless Commun.*, 2011, **18**, pp. 66–74

[26] Carroll, T.L., Pecora, L.M. 'Synchronizing chaotic circuits,' *IEEE Trans. Cir. Sys.*, 1991, **38**, pp. 453–456

[27] Dedieu, H. 'Chaos shift keying : modukation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits,' *IEEE Trans. Cir. Sys.*, 1993, **40**, pp. 634–641

[28] Kaddoum, G., Vu, M., Gagnon, F. 'Performance analysis of differential chaotic shift keying communications in MIMO systems,' *Proc. IEEE International Symposium of Circuits and Systems (ISCAS)*, May 2011

[29] Lu, H., Zhang, L., Jiang, M. 'High-security chaotic cognitive radio system with subcarrier shifting,' *IEEE Commun. Letters*, 2015, **19**, pp. 1726–1729

[30] Okamoto, E. 'A chaos MIMO transmission scheme for channel coding and physical-layer security,' *IEICE Trans. Commun.*, 2012, E**95**-B, pp. 1384–1392

[31] Okamoto, E., Horiike, N. 'Performance improvement of chaos MIMO scheme using advanced stochastic characteristics,' *IEICE Commun. Express*, 2016, **5**, pp. 371–377

[32] 大鐘武雄, 小川恭孝, 'わかりやすい MIMO システム技術' (オーム社, 2009)

[33] Proakis, J.G. 'Digital Communications' (McGraw-Hill Education, 2001, Fourth edition)

[34] Marzetta, T.L. 'Noncooperative cellular wireless with unlimited numbers of base station antennas,' *IEEE Trans. Wireless Commun.*, 2010, **9**, pp. 3590–3600

[35] Rusek, F., Persson, D., Lau B.K., et al. 'Scaling Up MIMO: Opportunities and challenges with very large arrays,' *IEEE Signal Process. Mag.*, 2013, **30**, pp. 40–60

[36] Telatar, E. 'Capacity of multi-antenna gaussian channels,' *European transactions on telecommunications*, 1999, **10**, pp. 585–595

[37] Lu, L., Li, G.Y., Swindlehurst, A.L., et al. 'An overview of massive MIMO: benefits and challenges,' *IEEE J. Sel. Topics Signal Process.*, 2014, **8**, pp. 742–758

[38] Yang, S., Hanzo, L. 'Fifty years of MIMO detection: the road to large-scale MIMOs,' *IEEE Commun. Surveys Tuts.*, 2015, **17**, pp. 1941–1988

[39] Araújo D., Maksymyuk, T., Almeida, A.L.F., et al. 'Massive MIMO: survey and future research topics,' *IET Commun.*, 2016, **10**, pp. 1938–1946

[40] Im, T.H., Kim, J., Cho, Y.S. 'A low complexity QRM-MLD for MIMO systems,' *Proc. IEEE Vehicular Technology Conf. (VTC)*, Apr. 2007, pp. 2243–2247

[41] Kawai, H., Higuchi, K., Maeda, N., et al. 'Likelihood function for QRM-MLD suitable for soft-decision turbo decoding and its performance for OFCDM MIMO multiplexing in multipath fading channel,' *IEICE Trans. Commun.*, 2005, E**88**-B, pp. 47–57

[42] Wu, M., Dick, C., Cavallaro, J.R., et al. 'Iterative detection and decoding in 3GPP LTE-based massive MIMO systems,' *Proc. European Signal Processing Conf. (EUSIPCO)*, Sept. 2014

[43] Ahmed, S., Kim, S. 'Efficient soft bit estimation for joint iterative multiple input multiple output detection,' *IET Commun.*, 2015, **9**, pp. 2107–2113

[44] Yoon, S. 'Iterative detection and decoding of MIMO signals usingl low-complexity soft-in/soft-out detector,' *IEICE Trans. Commun.*, 2015, E**98**-B, pp. 890–896

[45] Wo, T. and Hoeher, P. A. 'Low-Complexity Gaussian Detection for MIMO Systems,' *Journal of Electrical and Computer Engineering*, 2010, Article ID 609509, 12 pages doi:10.1155/2010/609509.

[46] Dong, L., Han, Z., Petropulu, A.P., et al. ‘Improving wireless physical layer security via cooperating relays,’ *IEEE Trans. on Signal Process.*, 2009, **58**, pp. 1875–1888

[47] 田中和之, ‘ベイジアンネットワークの統計的推論の数理’ (コロナ社, 2009)

[48] 渡辺有祐, ‘グラフィカルモデル’ (講談社, 2016)

補足

A　通信路モデル

通信路行列の代表的なモデルは自由空間モデル，レイリーフェージングモデル，仲上ライスモデルの 3 つがある（図 1）．自由空間モデルは，通信路に電磁波を反射 · 散乱させる物体がなく，送信された電磁波が直接受信アンテナで受信される状況を仮定している．この状況は，従来の無線通信システムである $N_{\mathrm{t}} = N_{\mathrm{r}} = 1$ で構成された SISO では理想的な状況だが，MIMO では複数の送信シンボルが同振幅同位相であるため混信してしまい，無線通信として成立しない．一方，レイリーフェージングモデルは，通信路に電磁波を反射 · 散乱させる物体が多数存在することを仮定している．それにより全ての電磁波は複数経路（マルチパス）を経て受信アンテナに届き，多数の電磁波が重なり合うフェージング現象が起きる．仲上ライスモデルは，一部の通信路はマルチパスを通るレイリーフェージングモデル，その他の通信路はマルチパスのない自由空間モデルである．MIMO は，送信シンボルがマルチパスを通って受信アンテナで受信される際に生じるフェージング現象を利用している．フェージング現象とは，受信信号が送信シンボルに比べ大きさや位相が大きく変動する現象である．例えば，長距離の無線通信は空間を伝送媒体としているため，周囲の地形や建物の壁などによって電磁波が反射 · 散乱され，マルチパスを通って電磁波が受信アンテナに到来する．それらの電磁波が重なり合うことによって干渉波ができる．MIMO は，フェージング現象によりおきる位相や振幅の変化（CSI）を正確に把握することで，N_{t} 個の送信アンテナから送信された送信信号を混信することなく受信することができる．

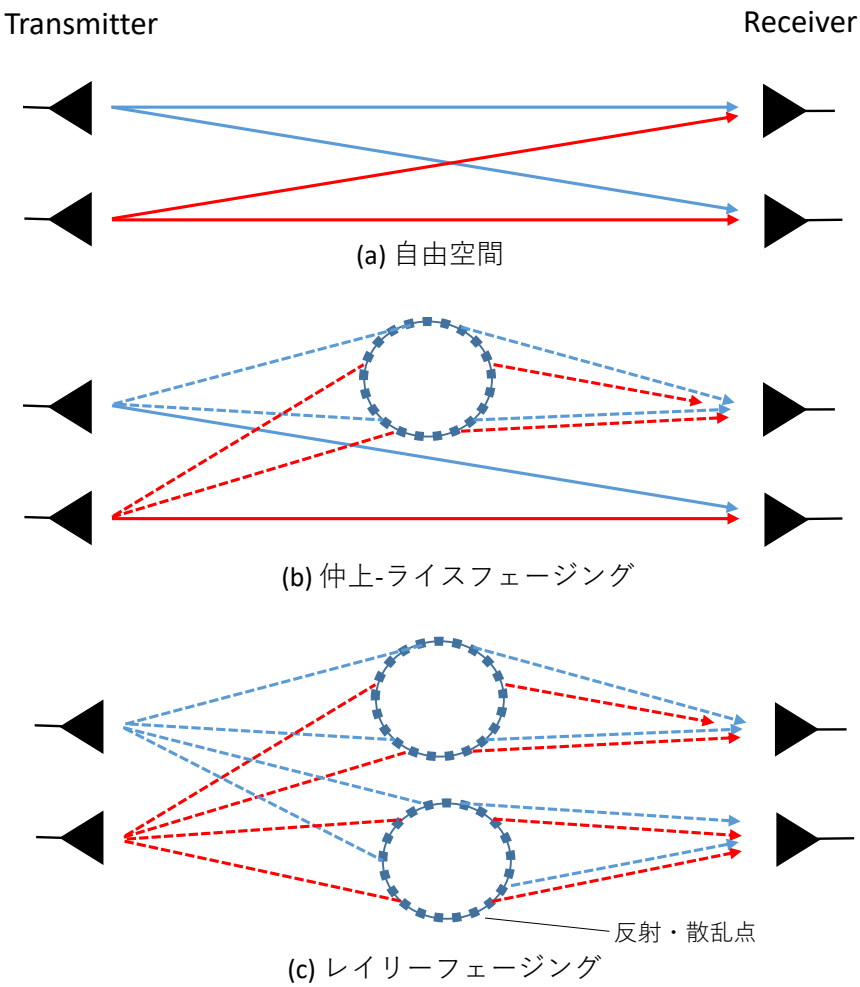


図 1: 無線通信での通信路モデル．
(a) 自由空間モデル (b) 仲上-ライスフェージングモデル (c) レイリーフェージングモデルを表す．実線は送受信アンテナ間を反射 · 散乱することなく届く直接波を表す．破線は反射 · 散乱して届く電磁波を表す．

B MLD

ここでは，MLD の復号計算式である式（2.8）の導出を行う．MLD は，$2^{N_{\mathrm{t}}}$ 個の送信データ候補 $\vec{b}$ の中から，事後確率（受信信号 $\vec{y}$ の下で，送信データが $\vec{b}$ である確率）$P\left(\vec{x}(\vec{b})|\vec{y}\right)$ を最大にする $\vec{b}$ を探す方法である．こ

こでベイズの定理により，この事後確率は，

$$P\left(\vec{x}(\vec{b}) \mid \vec{y}\right) = \frac{P\left(\vec{y} \mid \vec{x}(\vec{b})\right) P\left(\vec{x}(\vec{b})\right)}{P\left(\vec{y}\right)}, \tag{1}$$

と変形できる．このとき，$P\left(\vec{y}\right)$ は送信信号候補によらず一定と考え，事前確率 $P\left(\vec{x}(\vec{b})\right)$ に関する情報がなく，全ての候補で等しいとすると，$P\left(\vec{x}(\vec{b}) \mid \vec{y}\right)$ を最大にすることは，$P\left(\vec{y} \mid \vec{x}(\vec{b})\right)$ を最大にすることに等しい．ここで，通信路行列 $\mathbf{H}$ と送信信号候補 $\vec{x}(\vec{b})$ から生成した受信信号レプリカを

$$\vec{y} = \mathbf{H}\vec{x}(\vec{b}), \tag{2}$$

で与える．実際に受信された受信信号 $\vec{y}$ と $\vec{y}$ との差は，送信信号候補 $\vec{x}(\vec{b})$ が送信されたときの雑音ベクトル $\vec{n}$ となる．送信信号候補 $\vec{x}(\vec{b})$ のときに，$\vec{n} = \vec{y} - \mathbf{H}\vec{x}(\vec{b})$ の確率密度関数は，雑音ベクトル $\vec{n}$ が N_{r} 次元の複素ガウス分布に従うとし，

$$p\left(\vec{y} \mid \vec{x}(\vec{b})\right) = \frac{1}{\left(2\pi\sigma_{\mathrm{n}}^2\right)^{N_{\mathrm{r}}}} \exp\left[-\frac{\left(\vec{n}^H\vec{n}\right)}{2\sigma_{\mathrm{n}}^2}\right], \tag{3}$$

で表される．ここで，$*^H$ はエルミート転置である．送信信号候補に依存する部分は指数の分子部分のみで，

$$\begin{aligned}\left(\vec{n}^H\vec{n}\right) &= \left(\vec{y} - \mathbf{H}\vec{x}(\vec{b})\right)^H \left(\vec{y} - \mathbf{H}\vec{x}(\vec{b})\right) \\ &= \|\vec{y} - \mathbf{H}\vec{x}(\vec{b})\|^2,\end{aligned} \tag{4}$$

と与えられる．従って，式（4）を最小化する $\vec{b}$ が最適な復号データ $\hat{\vec{b}}$ で，つまり，式（2.8）

$$\hat{\vec{b}} = \arg\min_{\vec{b}} \|\vec{y} - \mathbf{H}\vec{x}(\vec{b})\|^2,$$

である．