

## カオス2値系列とその相関特性の評価に関する研究

常田, 明夫  
九州大学工学研究科情報工学専攻

<https://doi.org/10.11501/3099871>

---

出版情報：九州大学，1994，博士（工学），課程博士  
バージョン：  
権利関係：





カオス2値系列とその相関特性の評価に関する研究

常 田 明 夫



①

## カオス 2 値系列とその相関特性の評価に関する研究

常 田 明 夫

# 目次

主な記号	1
1 緒論	4
2 スペクトル拡散通信と符号分割多元接続	8
2.1 はじめに	8
2.2 スペクトル拡散通信（直接拡散方式）の基本原理	8
2.3 符号分割多元接続 (CDMA)	11
2.4 従来の拡散符号	15
2.4.1 $m$ 系列	15
2.4.2 Kasami 系列	18
2.4.3 Gold 系列	19
3 カオスの拡散符号への応用	21
3.1 はじめに	21
3.2 エルゴード写像によるカオスの生成法と不変密度	22
3.3 カオスの時系列解析法と相関関数	25
3.4 カオス 2 値系列	26
3.4.1 生成法と相関関数の評価	26
3.4.2 拡散符号としての性能評価	30
3.5 まとめ	42
4 チェビシェフ 2 値系列の相関関数の厳密評価	43
4.1 はじめに	43
4.2 統計量の経験値	44
4.3 Perron-Frobenius 作用素による相関関数の評価	45
4.3.1 数値例	51
4.4 偶および奇相関関数の評価	56
4.4.1 数値例	57
4.5 まとめ	70
5 有限周期カオス系列の統計量の揺らぎと高次相関関数	71
5.1 はじめに	71
5.2 分散による揺らぎの評価	71
5.3 分散の評価例	72
5.4 チェビシェフ 2 進系列の高次相関関数	73



5.5	数値例 . . . . .	74
5.6	まとめ . . . . .	78
6	画像データの SS 通信への応用 . . . . .	79
6.1	はじめに . . . . .	79
6.2	SS を用いたベースバンド画像伝送システム . . . . .	80
6.3	固定長および可変長 PN 符号による伝送モデル . . . . .	81
6.3.1	モデル 1 . . . . .	81
6.3.2	モデル 2 . . . . .	82
6.3.3	モデル 3 . . . . .	83
6.3.4	実験結果と検討 . . . . .	84
6.4	まとめ . . . . .	90
7	結論と今後の課題 . . . . .	91
	謝辞 . . . . .	94
	参考文献 . . . . .	95
	付録 A チェビシェフ写像より生成される実数値系列の自己相関関数の導出 . . . . .	101
	付録 B チェビシェフビット系列の相関関数の評価式 (3.30) の導出 . . . . .	104

## 主な記号

$d^{(k)}(t)$ :	ユーザー $k$ の情報データ信号
$c^{(k)}(t)$ :	ユーザー $k$ の擬似雑音 (PN) 信号
$d_p^{(k)}$ :	ユーザー $k$ の情報データ系列
$c_q^{(k)}$ :	ユーザー $k$ の PN 系列
$D_d$ :	情報データ信号の 1 シンボルの継続時間
$D_c$ :	PN 信号の 1 シンボルの継続時間 (チップ周期)
$s^{(k)}(t)$ :	ユーザー $k$ の拡散信号
$T$ :	PN 系列の周期
$r(t)$ :	CDMA における受信信号
$Z^{(i)}$ :	ユーザー $i$ の相関器の出力
$R_{ik}(\ell)$ :	PN 系列 $\{c_q^{(i)}\}_{q=0}^{T-1}$ と $\{c_q^{(k)}\}_{q=0}^{T-1}$ の間の偶相関関数
$\Theta_{ik}(\ell)$ :	PN 系列 $\{c_q^{(i)}\}_{q=0}^{T-1}$ と $\{c_q^{(k)}\}_{q=0}^{T-1}$ の間の奇相関関数
$A_{ik}(\ell)$ :	PN 系列 $\{c_q^{(i)}\}_{q=0}^{T-1}$ と $\{c_q^{(k)}\}_{q=0}^{T-1}$ の間の非周期相関関数
$\tau(x)$ :	非線形エルゴード写像
$x_n$ あるいは $\tau^n(x)$ :	初期値 $x_0$ あるいは $x$ の $\tau(x)$ による $n$ 回写像
$F(\tau^n(x))$ :	初期値 $x$ に対する時刻 $n$ の任意の観測値
$F_T(x)$ :	$F(\tau^n(x))$ の時間平均 (観測時間 $T$ )
$\langle F \rangle$ :	$F(\tau^n(x))$ の空間 (アンサンブル) 平均
$f^*(x)dx$ :	写像 $\tau$ の不変測度
$C_T(x, \ell; g, h)$ :	カオス系列 $\{g(\tau^n(x))\}_{n=0}^{T-1}$ と $\{h(\tau^n(x))\}_{n=0}^{T-1}$ の間の相関関数 (時間平均形)
$\langle C(\ell; g, h) \rangle$ :	カオス系列 $\{g(\tau^n(x))\}_{n=0}^{\infty}$ と $\{h(\tau^n(x))\}_{n=0}^{\infty}$ の間の相関関数 (空間平均形)



$\{\theta_c(\tau^n(x))\}_{n=0}^{\infty}$ :	カオス 2 進系列
$\{b_i(\tau^n(x))\}_{n=0}^{\infty}$ :	カオス第 $i$ ビット系列
$X$ :	初期値の集合
$L$ :	初期値の集合の大きさ
$\hat{F}_{T,L}$ :	$F_T(x)$ の $L$ 個の初期値に対する平均値 (経験値)
$P_{\tau}$ :	Perron-Frobenius (P-F) 積分作用素
$S_T(x, m; g, h)$ :	$C_T(x, \ell, g, h)$ の離散フーリエ変換
$\langle S(m; g, h) \rangle$ :	$\langle C(\ell, g, h) \rangle$ の離散フーリエ変換
$\hat{S}_{T,L}(m; g, h)$ :	$\hat{C}_{T,L}(\ell, g, h)$ の離散フーリエ変換
$B_T(x, \ell; g, h)$ :	カオス 2 値 $(-1, 1)$ 系列 $\{2g(\tau^n(x)) - 1\}_{n=0}^{T-1}$ と $\{2h(\tau^n(x)) - 1\}_{n=0}^{T-1}$ の間の相関関数 (時間平均形)
$\langle B(\ell; g, h) \rangle$ :	カオス 2 値 $(-1, 1)$ 系列 $\{2g(\tau^n(x)) - 1\}_{n=0}^{\infty}$ と $\{2h(\tau^n(x)) - 1\}_{n=0}^{\infty}$ の間の相関関数 (空間平均形)
$A_T(x, \ell; g, h)$ :	カオス 2 値 $(-1, 1)$ 系列 $\{2g(\tau^n(x)) - 1\}_{n=0}^{T-1}$ と $\{2h(\tau^n(x)) - 1\}_{n=0}^{T-1}$ の間の非周期相関関数 (時間平均形)
$\langle A(\ell; g, h) \rangle$ :	カオス 2 値 $(-1, 1)$ 系列 $\{2g(\tau^n(x)) - 1\}_{n=0}^{\infty}$ と $\{2h(\tau^n(x)) - 1\}_{n=0}^{\infty}$ の間の非周期相関関数 (空間平均形)
$R_T(x, \ell; g, h)$ :	カオス 2 値 $(-1, 1)$ 系列 $\{2g(\tau^n(x)) - 1\}_{n=0}^{T-1}$ と $\{2h(\tau^n(x)) - 1\}_{n=0}^{T-1}$ の間の偶相関関数 (時間平均形)
$\langle R(\ell; g, h) \rangle$ :	カオス 2 値 $(-1, 1)$ 系列 $\{2g(\tau^n(x)) - 1\}_{n=0}^{\infty}$ と $\{2h(\tau^n(x)) - 1\}_{n=0}^{\infty}$ の間の偶相関関数 (空間平均形)
$\hat{R}_{T,L}(\ell; g, h)$ :	カオス 2 値 $(-1, 1)$ 系列 $\{2g(\tau^n(x)) - 1\}_{n=0}^{T-1}$ と $\{2h(\tau^n(x)) - 1\}_{n=0}^{T-1}$ の間の偶相関関数の $L$ 個の初期値に対する経験値
$\Theta_T(x, \ell; g, h)$ :	カオス 2 値 $(-1, 1)$ 系列 $\{2g(\tau^n(x)) - 1\}_{n=0}^{T-1}$ と $\{2h(\tau^n(x)) - 1\}_{n=0}^{T-1}$ の間の奇相関関数 (時間平均形)
$\langle \Theta(\ell; g, h) \rangle$ :	カオス 2 値 $(-1, 1)$ 系列 $\{2g(\tau^n(x)) - 1\}_{n=0}^{\infty}$ と $\{2h(\tau^n(x)) - 1\}_{n=0}^{\infty}$ の間の奇相関関数 (空間平均形)
$\hat{\Theta}_{T,L}(\ell; g, h)$ :	カオス 2 値 $(-1, 1)$ 系列 $\{2g(\tau^n(x)) - 1\}_{n=0}^{T-1}$ と $\{2h(\tau^n(x)) - 1\}_{n=0}^{T-1}$ の間の奇相関関数の $L$ 個の初期値に対する経験値

$\sigma^2(F)$ :  $F_T(x)$  の分散の空間平均

$\langle C^{(d)}(\cdot) \rangle$ :  $d$  個の関数  $F^{(1)}, \dots, F^{(d)}$  に対する  $d$  次相関関数 (空間平均形)

$d(t_1, t_2)$ : 画像データの座標  $(t_1, t_2)$  における画素値

$\theta(k_1, k_2)$ :  $d(t_1, t_2)$  の 2 次元離散コサイン変換



## 第 1 章

### 緒論

乱数は、種々の確率統計現象を模擬する技法、いわゆるモンテカルロ法において大量に必要とされ、計算機の導入とともに、算術演算による擬似的にランダムな“擬似乱数”の生成法が求められるようになった。平方採中法や線形合同法およびシフトレジスタによる最大周期 (maximum length;  $m$ ) 系列は、代表的な擬似乱数系列として良く知られている。また、これらの擬似乱数の性質を調べるための統計的検定法も幾つか提案されており、利用目的に応じた検定が行なわれている<sup>[34],[35]</sup>。このように擬似乱数は、従来、モンテカルロ法において重要な役割を担ってきたが、近年、その応用範囲は、情報通信へと広がってきている。周知の通り、通信技術は、従来のアナログ方式から、デジタル方式に移行しており、デジタル通信技術の発展は目覚ましいものがある。擬似乱数の通信へ応用としては、まず暗号通信<sup>[38]</sup>が挙げられ、特に、情報データの  $\{0,1\}$  系列と  $\{0,1\}$  の擬似乱数と排他的論理和をとることで、暗号化および復号化を実現するバーナム暗号では、長周期の 2 値の擬似乱数が大量に必要である。また、最近では、画期的な技術として、スペクトル拡散 (spread spectrum; SS) 通信が特に注目されており、盛んに研究がなされている<sup>[39][40]</sup>。この技術は、情報信号に、これとは無関係な擬似乱数 (pseudo-noise; PN) 系列（あるいは拡散符号）を掛け合わせることで、送信信号の帯域を広げ、受信側ではその擬似乱数系列との相関を取ることで復調するものである。また、異なった擬似乱数系列によりチャネル識別を行なうことで、同一の周波数帯域で複数のユーザが同時に通信する符号分割多元接続 (code division multiple access; CDMA) を可能にする。その原理等については、本文第 2 章において概説する。このスペクトル拡散通信に基づいた CDMA 方式は、様々な利点を有することから、従来の周波数多元接続 (frequency division multiple access; FDMA) や時分割多元接続 (time division multiple access; TDMA) に代わる将来の通信技術として大いに期待されている。CDMA システムにおいては、完全同期状態での各ユーザー間の干渉の度合



に關係する“偶相互相関関数”，およびそれ以外の場合にはさらに“奇相互相関関数”を考慮した性質の良い擬似乱数系列が多数必要とされる<sup>[1]</sup>。また，同期確立のためには，デルタ関数的な自己相関特性が望まれるが，この場合もやはり，偶および奇自己相関関数を考慮しなければならない。CDMA 技術の成否は，用いる擬似乱数系列の相関特性に大きく依存するので，様々な系列の設計が盛んになされてきている<sup>[1]–[5]</sup>。

従来，SS 通信においては 2 値の擬似乱数系列が専ら用いられているが，中でも，最適な偶相関特性を有する Gold 系列や Kasami 系列等の， $m$  系列を基にしたシフトレジスタ系列の集合が良く知られている<sup>[1]</sup>。ただし，これらは，Welch<sup>[3]</sup>が理論的に与えた偶相関値の最大値の下界を満足するように有限体理論に基づいて設計されているが，奇相関に関する理論的解析は困難とされている。特に，平均誤り確率を評価する際には，偶および奇相関値の分布を知る必要があるが，無論，奇相関値の分布に関する理論的解析も困難とされている。

一方，最近，非線形写像より生成される“カオス”を擬似乱数として応用しようとする試みが見られる。この際，カオスが従来の擬似乱数と比べて乱雑さに関する性質の良い乱数であるかどうか問題となる。通常カオスの軌道は実数値系列であり，その乱雑さの度合の測定自身容易でないが，しばしば用いられる指標は，その実数値系列の自己相関関数である。すなわち，デルタ関数的な自己相関関数（従って一定のパワースペクトル）を有する実数値系列は，白色雑音とみなせるから，乱雑であるとするものである<sup>[18]</sup>。カオスを呈するエルゴード写像として良く知られているテント写像やロジスティック写像，チェビシェフ写像については，写像のエルゴード性を活用した“空間平均法”と呼ばれる方法によって，これらの写像より生成される実数値系列の自己相関関数がデルタ関数に等しいことが既に報告されている<sup>[18],[25]</sup>。また，実数値系列を種々の閾値関数により 2 値系列に変換し，これと，乱雑な 2 値系列の典型例であるベルヌイ試行との近さを測ることで，元の実数値系列の乱雑さを調べるという方法も提案されている<sup>[12]</sup>。

本論文では，従来 SS 通信で良く用いられているシフトレジスタ系列とは全く異なった擬似乱数系列として，上記の非線形写像より生成される“カオス”から得られる 2 値系列を応用することを試みる。カオスとは，常微分方程式や差分方程式で記述される確定系に見られる乱雑な統計確率的現象を総称したもので，非常に興味深い振舞いをするため，現在まで盛んに研究がなされてきており，工学的応用，特に通信への応用への試みも，近年少しずつ認識され始めている。しかしながら，その多くは，ある特定の回路において観測されるカオスの同期現象を利用した，アナログ的なスクランブル方式に基づく秘匿通信の実現例であり<sup>[27]–[32]</sup>，SS 通信への応用例では，その相関特性の評価についてほとんど議論さ



れていない<sup>[33]</sup>。これは、前述したようにカオスの実数値系列については、空間平均法によりその自己相関関数が理論的に評価出来るものの、SS通信において重要とされる相互相関関数という概念が容易に導入できないためであり、何らかの工夫が必要である。もちろん、偶および奇相関関数の理論的評価も容易ではない。従って、カオスをSS通信へ応用する場合は、このような点を克服する必要がある。

本論文は、非線形エルゴード写像に基づいたカオス2値系列の生成法とその相関特性の評価に関して、以下のような研究成果をまとめたもので、本文7章より成る。

第1章では、研究の背景、動機を述べた後、本論文の構成および主な成果を述べる。

第2章では、SS通信およびCDMAの基本原則を述べ、用いる擬似乱数系列の相関特性が重要な役割を担うこと、また、非同期通信においては、偶および奇の2種類の相関関数について考慮しなければならないこと等を概説する。

第3章では、まず、一次元非線形エルゴード写像を用いたカオスの生成法およびその時系列解析法を概説する。ある初期値に対して、一つの不規則で乱雑なカオス軌道が生成されるので、この軌道自身は一つの確率変数と見なすことが出来る。従って、その平均的振舞いを議論しなければならない。カオスの時系列解析法としては、二つの方法が挙げられる。一つは“時間平均法”と呼ばれるもので、ある初期値から得られる軌道を長時間観測し、その平均を求める方法である。他の一つは、“空間平均法”と呼ばれるもので、写像のエルゴード性を活用した方法である。バーコフ (Birchhoff) のエルゴード定理により、時間平均値は、その観測時間を無限に長くした時に、空間平均値に収束することが知られている。しかしながら、有限の観測時間による時間平均値は、初期値に依存した確率変数であるので、かなり揺らいだ値をもつ。一方、空間平均値は初期値の影響を受けないため、非常に有効な評価法である。このように、カオス系列は、確率論的符号の一種であると思なされるので、その統計量の評価法においても、従来のシフトレジスタ系列のそれとは全く異なる。次に、カオスの実数値系列を2値系列に変換する方法を2つ提案する。この方法は、ある一つの初期値より得られるカオスの実数値系列から、複数個の2値系列を生成するもので、実数値系列では導入できなかった相互相関関数の概念を導入出来、空間平均法によるその理論的評価が可能となる。ここでは、非線形エルゴード写像の一つであるチェビシェフ写像を例として取り上げ、これより得られる2値系列について、その自己および相互相関関数を空間平均法に基づいて評価するが、その厳密な評価は困難であるので、その上限をまず評価する。なお、チェビシェフ写像を選ぶ理由は、これより得られる実数値系列が良い性質を持つことが知られているからである。さらに、有限周期のカオス2値系列の集合を幾



つつくり，Gold 系列や Kasami 系列のそれらと比較するために，それぞれの系列の集合内でのあらゆる組合せにおいて，偶および奇相関関数を計算し，各ペアでの最大相関値の分布を調べる．その結果，偶相関特性は，Gold 系列や Kasami 系列に比べて悪いものの，奇相関特性に関してはそれほど差が無いことが示される．

第4章では，Perron-Frobenius(P-F) 積分作用素を用いることにより，第3章で上限しか与えられなかったカオス2値系列の相関関数の空間平均値を厳密に与える．その際，P-F 作用素に関して興味深い関係式が示される．また，チェビシェフ写像より得られる2値系列が良好な自己および相互相関特性をもつことも明らかになる．さらに，ここで得られた相関関数の空間平均値を基に，偶相関関数はもとより，従来，困難とされていた奇相関関数の理論的評価を行なう．

第5章では，有限周期のカオス系列の統計量の，空間平均値からの揺らぎについて議論する．実際にカオス系列を通信に応用する際には，有限周期の系列を使うので，その個々の系列の統計的振舞いを知ることは重要である．経験的にではあるが，いろいろな初期値に対する有限周期カオス系列の統計量の頻度分布が，初期値の集合の大きさを大きくした時，ガウス分布に近づくことを知ることが出来る．その平均値については，上述の空間平均値で与えられ，一方，分散については，その統計量の自己相関関数の空間平均値により事前に評価出来ることが示される．

第6章では，画像通信への応用例として，SS 方式による画像の伝送方法について，幾つかのモデルを提案する．SS 方式の実用化は，これまで主に音声データのみであり，画像に関しては，その膨大なデータ量のために，ほとんど検討されていなかった．ここでは，用いる擬似乱数系列の周期長を可変とすることにより，データ圧縮の点で，より効率的な符号化が可能であることを示す．その結果，周期長が任意に可変であるカオス2値系列の有用性が確認される．

第7章では，以上の研究のまとめと，今後の課題について述べる．



## 第2章

# スペクトル拡散通信と符号分割多元接続

## 2.1 はじめに

本章では、まず、スペクトル拡散(SS)通信の基本原則について述べ、これに基づいた符号分割多元接続(CDMA)の構成法を説明する。SS通信には、直接拡散(direct sequence; DS)方式および周波数ホッピング(frequency hopping; FH)方式の二種類があるが、ここでは、その構成の容易さから主流となっているDS方式を取り上げる。その原理から、用いる擬似乱数系列(拡散符号)の相関特性が重要となることがわかるが、その際、考えるべき相関関数として偶相関関数および奇相関関数の二種類があることが示される。

## 2.2 スペクトル拡散通信(直接拡散方式)の基本原則

図2.1に、スペクトル拡散(SS)通信の基本的な概念図を示す。

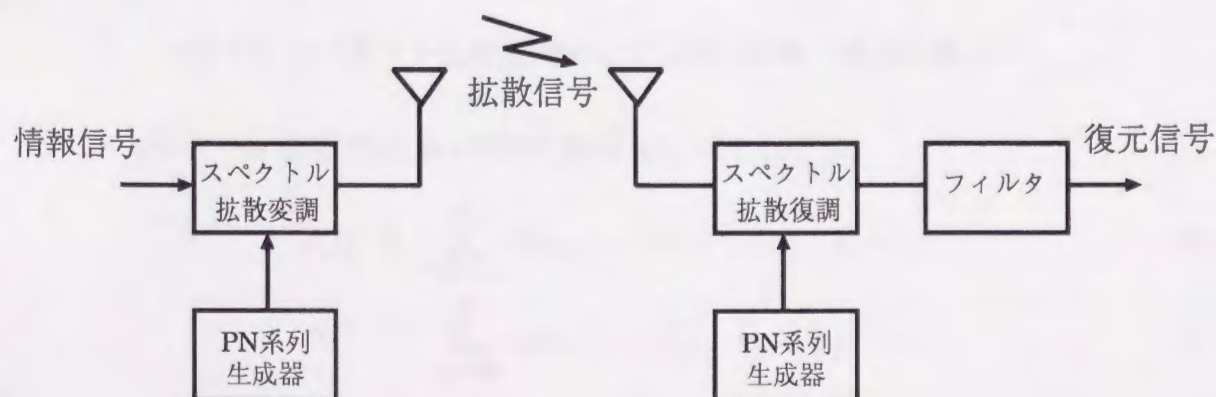


図 2.1: スペクトル拡散通信の基本的な概念図



DS 方式による SS 通信システムでは、送信側において、情報信号にこれとは独立な擬似乱数系列 (PN 系列) を掛け合わせ、情報信号の周波数を拡散し、受信側では、送信側で用いた PN 系列と全く同じ系列によって情報信号を復元する。ここでは、簡単のため、ベースバンド信号の場合について考えることとし、図 2.2 に基づいてその原理を説明する。

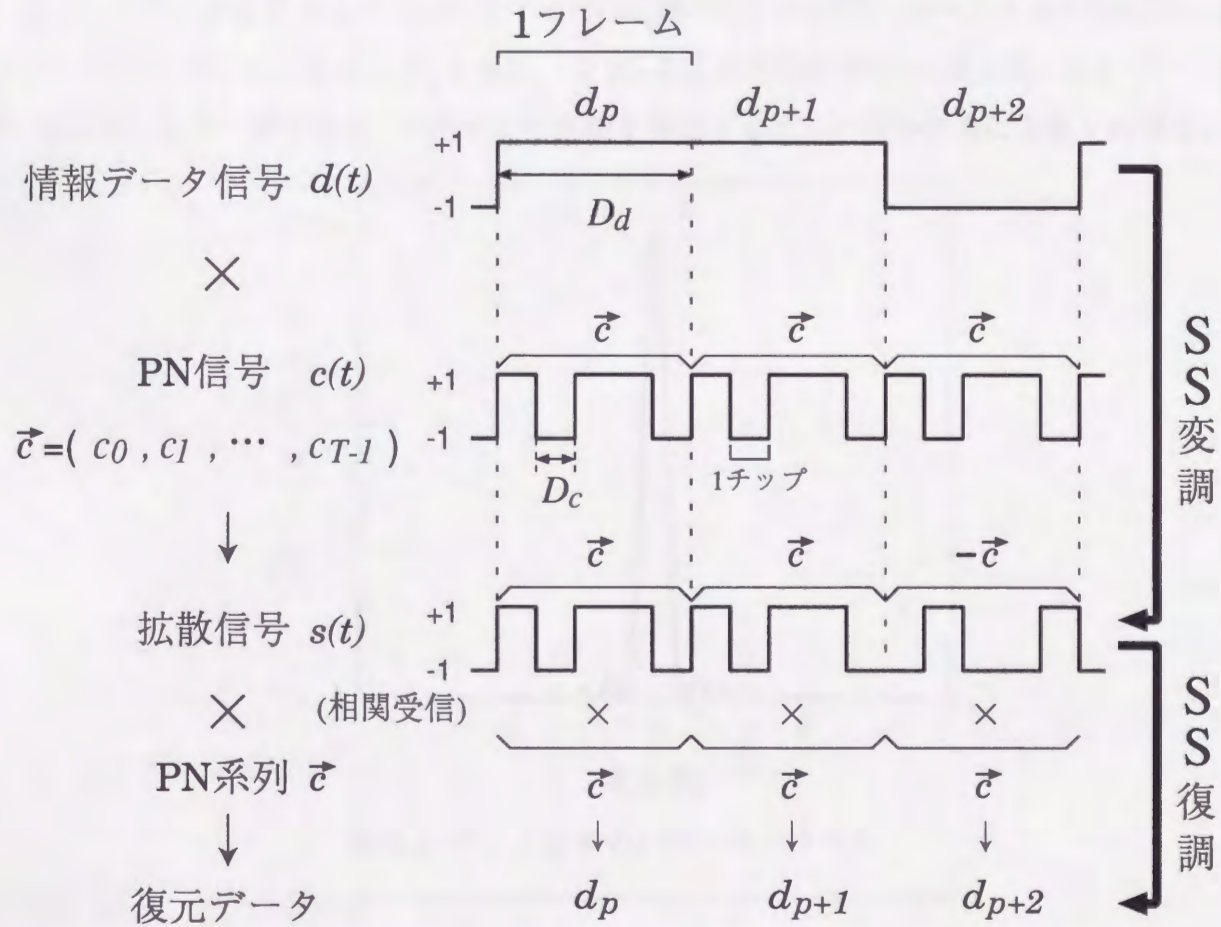


図 2.2: スペクトル拡散変調および復調の原理 (直接拡散方式)

まず、情報データ信号  $d(t)$  および PN 信号  $c(t)$  はそれぞれ、

$$d(t) = \sum_{p=-\infty}^{\infty} d_p u_{D_d}(t - pD_d) \quad d_p \in \{1, -1\} \quad (2.1)$$

$$c(t) = \sum_{q=-\infty}^{\infty} c_q u_{D_c}(t - qD_c) \quad c_q \in \{1, -1\} \quad (2.2)$$

と表すことが出来る。ここで、

$$u_D(t) = \begin{cases} 1 & (0 \leq t \leq D) \\ 0 & (\text{その他の場合}) \end{cases} \quad (2.3)$$



である。PN 系列は周期  $T = D_d/D_c$  の周期系列  $c_0, c_1, \dots, c_{T-1}$  であり、1 データシンボルに対して、1 周期分を掛け合わせる。よって  $D_d$  は、チップ周期  $D_c$  の整数倍にとられる。拡散信号  $s(t)$  は、

$$s(t) = d(t)c(t) \quad (2.4)$$

と書ける。データ信号および PN 信号（または拡散信号）のパワースペクトルの例を図 2.3、図 2.4 に示す ( $T = 5, D_d = 1, D_c = 0.2$ )。なお、PN 系列の周期  $T (= D_d/D_c)$  はスペクトルの“拡散率”を表す値であり、利用する周波数を考慮すると、 $T$  はむやみに大きく出来ない。

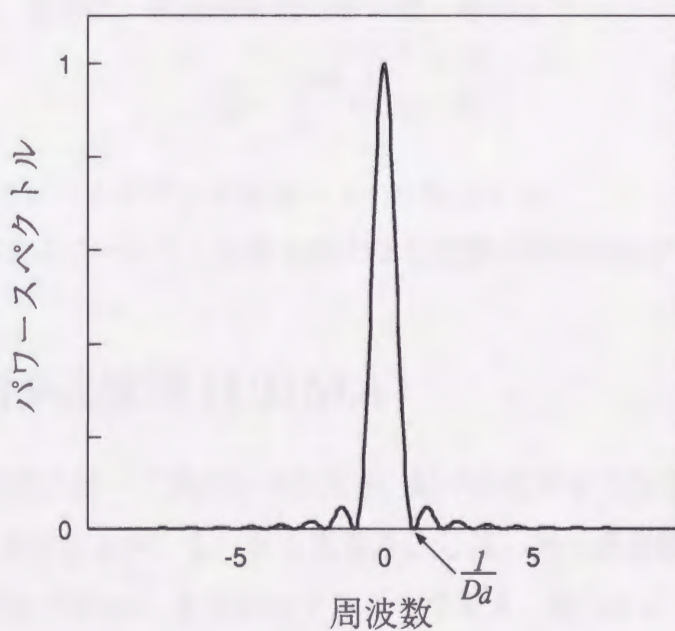


図 2.3: データ信号のパワースペクトル

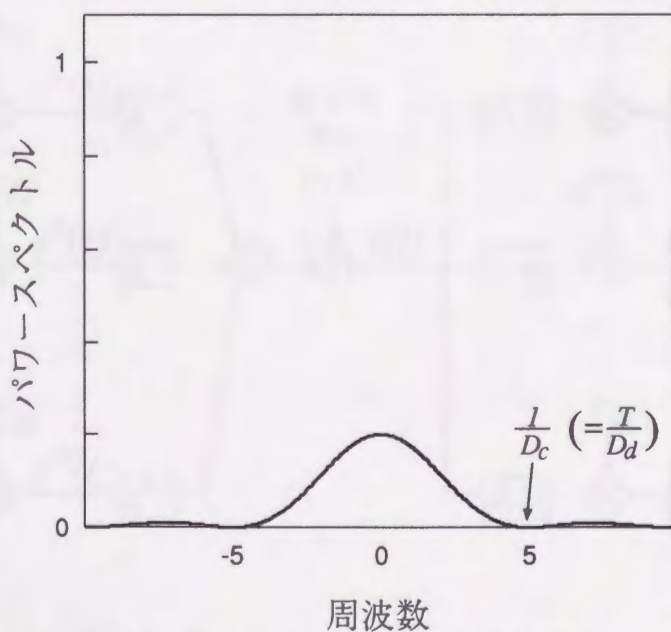


図 2.4: PN 信号（または拡散信号）の平均パワースペクトル ( $T = 5$ )



受信側では、所望の信号と同期を取った後、1フレーム毎に、相関受信を実行する。図2.2に示すようにベクトル  $\vec{c}$  を用いれば、情報データ  $d_p$  の復元は、拡散信号  $s(t)$  と  $\vec{c}$  との内積を取るような形で、

$$\frac{1}{T} \langle \underbrace{d_p \vec{c}}_{s(t)}, \vec{c} \rangle = d_p \quad (\langle \vec{a}, \vec{b} \rangle: \text{ベクトル } \vec{a} \text{ と } \vec{b} \text{ の内積}) \quad (2.5)$$

のように実行される。よって、一旦同期が確立した後は、フレーム毎にデータ信号を復元していくことになる。実際は、相関器を用いるので、その出力

$$Z_p = \int_0^{D_d} s(t)c(t)dt \quad (2.6)$$

の正負により、そのフレームのデータ信号の  $\pm 1$  を判定する。

以上が DS 方式によるスペクトル拡散変調および復調の基本原理である。

## 2.3 符号分割多元接続 (CDMA)

スペクトル拡散方式を用いて通信を行なうと、耐干渉性や耐妨害性、および秘匿通信の実現など多くの利点を有するが、もっとも重要なことは、同一周波数帯で同時に通信を行なう符号分割多元接続 (CDMA) を可能にすることである。図2.5にベースバンド CDMA システムのモデルを示す。

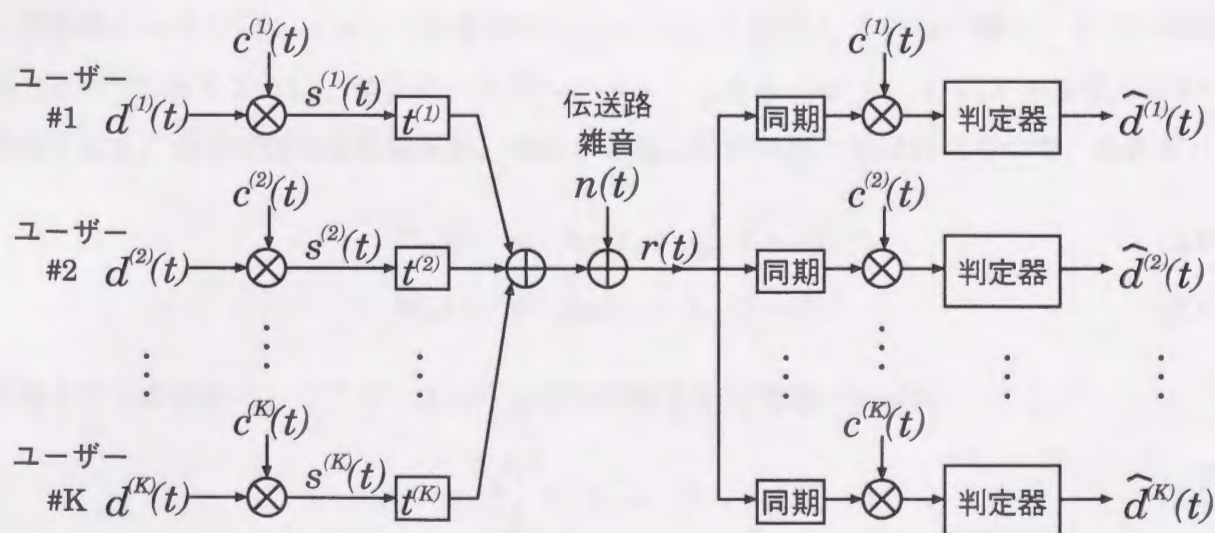


図 2.5: ベースバンド CDMA システム



$k$  番目のユーザーの信号  $d^{(k)}(t)$  および割り当てられた PN 信号  $c^{(k)}(t)$  はそれぞれ,

$$d^{(k)}(t) = \sum_{p=-\infty}^{\infty} d_p^{(k)} u_{D_d}(t - pD_d) \quad d_p^{(k)} \in \{1, -1\} \quad (2.7)$$

$$c^{(k)}(t) = \sum_{q=-\infty}^{\infty} c_q^{(k)} u_{D_c}(t - qD_c) \quad c_q^{(k)} \in \{1, -1\} \quad (2.8)$$

と表せ, その拡散信号  $s^{(k)}(t)$  は,

$$s^{(k)}(t) = c^{(k)}(t)d^{(k)}(t) \quad (2.9)$$

で与えられる. 非同期システムにおいては, 受信信号  $r(t)$  は,

$$r(t) = \sum_{k=1}^K c^{(k)}(t - t^{(k)})d^{(k)}(t - t^{(k)}) + n(t) \quad (2.10)$$

のように表される. ここで,  $t^{(k)}$  は  $k$  番目のチャネルの時間遅れで,  $n(t)$  は伝送路雑音である. 受信信号  $r(t)$  が同期回路により, ユーザ  $i$  の拡散信号  $s^{(i)}(t)$  に同期している時, その相関器の出力は,

$$Z^{(i)} = \int_0^{D_d} r(t)c^{(i)}(t)dt \quad (2.11)$$

で与えられる. この時, 他のユーザーの拡散信号  $s^{(k)}(t)$  からの干渉が問題となる.  $k$  番目のユーザーからの干渉の度合は, ユーザー  $k$  が用いている拡散符号  $c^{(k)}(t)$  とユーザー  $i$  の拡散符号  $c^{(i)}(t)$  との間の相互相関特性で評価される. この場合, ユーザー  $k$  の情報信号によって, 2種類の相互相関関数が考えられる. 一つは, 図 2.6 (a) に示すように, ユーザー  $k$  の情報データが  $+1 \rightarrow +1$  (あるいは  $-1 \rightarrow -1$ ) と変化していない場合, もう一つは, 図 2.6 (b) に示すように, 情報データが  $+1 \rightarrow -1$  (あるいは  $-1 \rightarrow +1$ ) と変化している場合である. 前者が偶相互相関関数, 後者が奇相互相関関数と呼ばれるもので, それぞれ,

$$R_{ik}(\ell) = A_{ik}(\ell) + A_{ki}(T - \ell) \quad (2.12)$$

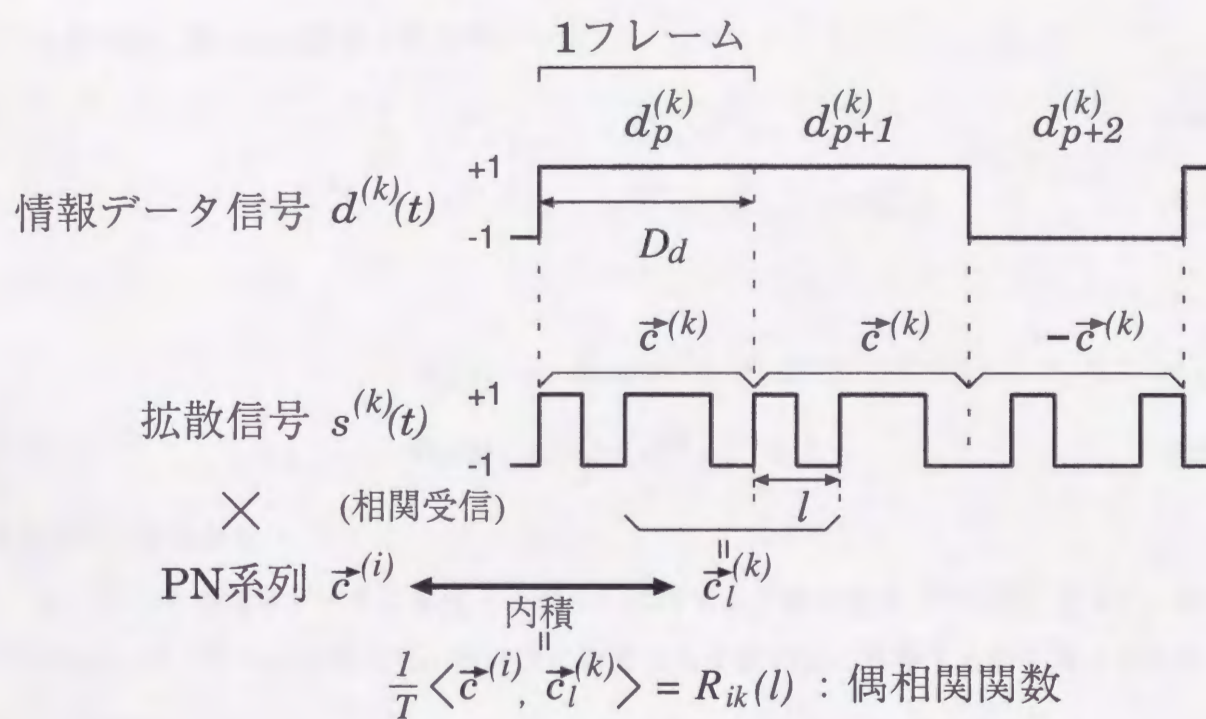
$$\Theta_{ik}(\ell) = A_{ik}(\ell) - A_{ki}(T - \ell) \quad (2.13)$$

と表すことが出来る. ここで,  $A_{ik}(\ell)$  は非周期相互相関関数と呼ばれ,

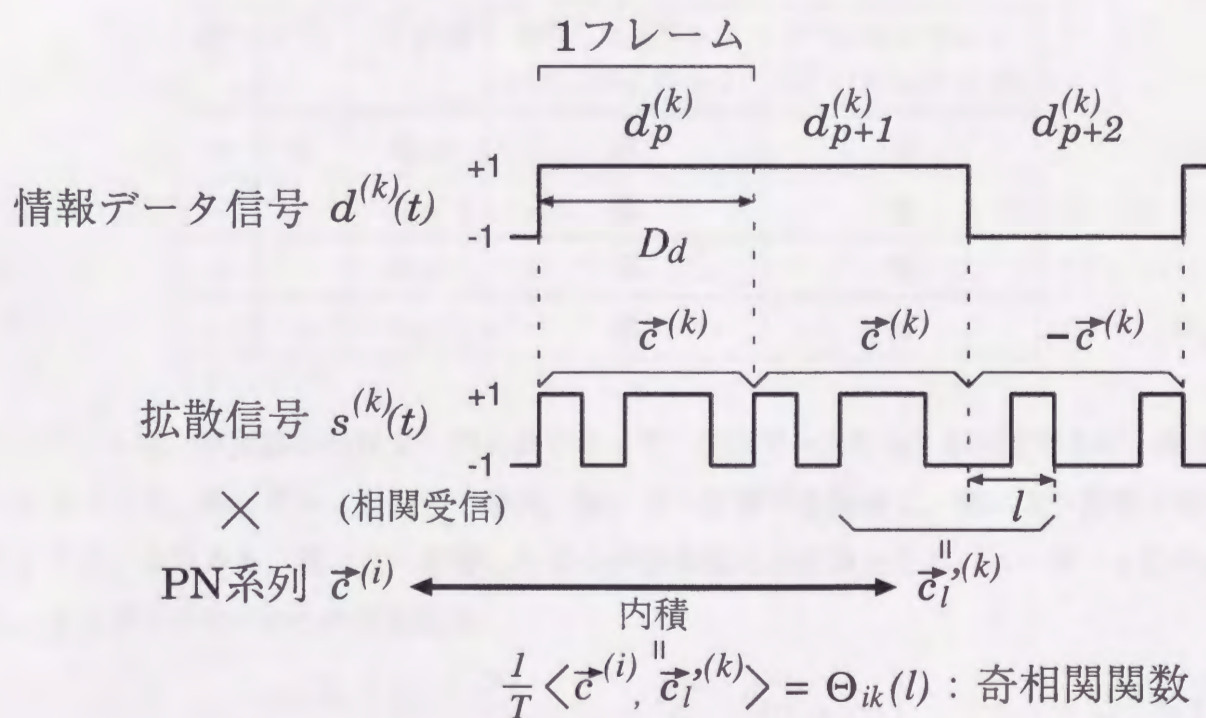
$$A_{ik}(\ell) = \sum_{j=0}^{T-1-\ell} c_j^{(i)} c_{j+\ell}^{(k)}, \quad 0 \leq \ell \leq T-1 \quad (2.14)$$

で定義される<sup>[1]</sup>.





(a)



(b)

図 2.6: (a) 偶相関関数を考慮する場合, (b) 奇相関関数を考慮する場合.



あるいは、図 2.6 に示すようなベクトル

$$\vec{c}_\ell^{(k)} = (c_\ell^{(k)}, c_{\ell+1}^{(k)}, \dots, c_{T-1}^{(k)}, c_0^{(k)}, \dots, c_{\ell-1}^{(k)}) \quad (2.15)$$

$$\vec{c}'_\ell^{(k)} = (c_\ell^{(k)}, c_{\ell+1}^{(k)}, \dots, c_{T-1}^{(k)}, -c_0^{(k)}, \dots, -c_{\ell-1}^{(k)}) \quad (2.16)$$

を用いると、

$$R_{ik}(\ell) = \frac{1}{T} \langle \vec{c}^{(i)}, \vec{c}_\ell^{(k)} \rangle \quad (2.17)$$

$$\Theta_{ik}(\ell) = \frac{1}{T} \langle \vec{c}^{(i)}, \vec{c}'_\ell^{(k)} \rangle \quad (2.18)$$

と表すことも出来る。

ユーザー  $k$  の情報データの変化（4通り）に対する干渉の度合（干渉値とする）、およびそれが、ユーザー  $i$  に対して、良い方に影響するか悪い方に影響するかを表 2.1 にまとめている。

表 2.1: ユーザー  $k$  からユーザー  $i$  への干渉値およびその影響

$d_p^{(k)}$	$d_{p+1}^{(k)}$	干渉値	$d^{(i)}(t)R_{ik}(\ell) > 0$ ( $d^{(i)}(t)\Theta_{ik}(\ell) > 0$ )	$d^{(i)}(t)R_{ik}(\ell) < 0$ ( $d^{(i)}(t)\Theta_{ik}(\ell) < 0$ )
+	+	$R_{ik}(\ell)$	良	悪
-	-	$-R_{ik}(\ell)$	悪	良
+	-	$\Theta_{ik}(\ell)$	良	悪
-	+	$-\Theta_{ik}(\ell)$	悪	良

ユーザー  $i$  は、相関器の出力  $Z^{(i)}$  の正負によって、情報データの  $\pm 1$  を判定するが、表 2.1 に示すように、ユーザー  $i$  からの干渉は、良い方へ影響する場合と、悪い方へ影響する場合がある。もちろん、悪い方へ影響した場合が復号誤りの原因となる。ユーザー  $i$  以外の  $K-1$  人のユーザーからの干渉値は、

$$\sum_{\substack{k=1 \\ k \neq i}}^K \left\{ \frac{d_p^{(k)} + d_{p+1}^{(k)}}{2} R_{ik}(\ell) + \frac{d_p^{(k)} - d_{p+1}^{(k)}}{2} \Theta_{ik}(\ell) \right\} \quad (2.19)$$

のように表すことが出来る。干渉が良い方へ働くか悪い方へ働くかは、各ユーザーの情報データや遅れ時間  $\ell$  によって変わるので、チャネル間干渉を小さくするためには、偶および奇相関値の絶対値が共に小さい系列が望まれる。また、所望の信号と同期を取るために



は、デルタ関数的な自己相関特性をもつような系列が望まれるが、その場合も、同様に、偶自己相関関数  $R_{ii}(\ell)$  および奇自己相関関数  $\Theta_{ii}(\ell)$  を考慮しなければならない。一般に、同期捕捉は、チャネル間干渉による復号誤りを抑えることよりも難しい問題である<sup>[41]</sup>。復号誤りについては、誤り訂正符号等の技術で補う事が可能であることを付記しておく。

以上のことからわかるように、CDMA を実現するための拡散符号としては、

- 同期確立およびチャネル間干渉低減のため、偶および奇相関特性が良いこと。
- より多くのユーザーに符号を割り当てるためには、種類数が多いこと。
- 第三者に容易に傍受されないために、ランダムであること。

等の性質が望まれる。

## 2.4 従来の拡散符号

従来の2値の擬似乱数系列としては、シフトレジスタにより生成される最大周期系列 ( $m$  系列) が、最適な偶の自己相関特性をもつ系列として有名である<sup>[1]</sup>。しかしながら、その相互相関特性は必ずしも良くなく、また、同じ周期の系列の数が非常に少ない。前述したように、CDMA においては、自己相関だけでなく、互いに相互相関の低い系列がより多く必要とされる。また、非同期の CDMA システムにおいては、偶と奇の2種類の相関関数について考慮しなければならない。Welch<sup>[3]</sup>は偶相関値の最大値の下界を理論的に与えたが、奇相関値の理論的解析は一般に困難とされている。よって、主に、Welch の下界を満足するような系列の設計がなされてきた。その代表的なものが、 $m$  系列を基にして得られる、Gold 系列や Kasami 系列であり、現在でも、拡散符号としてよく用いられている<sup>[1],[2]</sup>。以下にこれらの系列の生成法を簡単に紹介する。

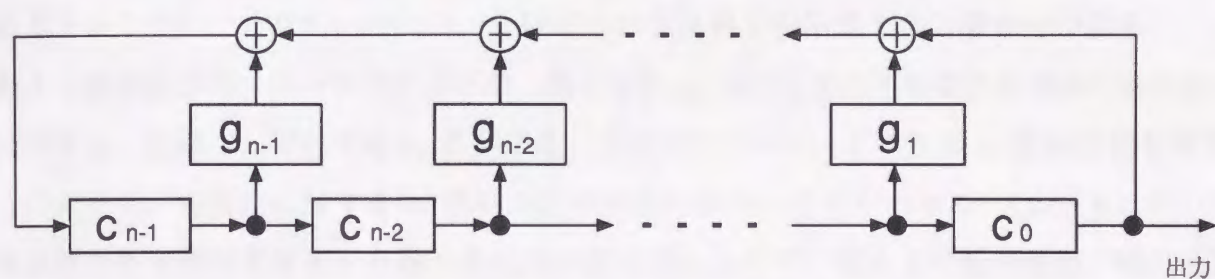
### 2.4.1 $m$ 系列

$m$  系列は、最大周期系列とも呼ばれるように、ある長さのシフトレジスタまたは遅延素子によって生成される符号系列の内、最長のものをいう。周期  $T = 2^n - 1$  の  $m$  系列は、ガロア体  $GF(2)$  上の  $n$  次の原始多項式

$$g(z) = z^n + g_{n-1}z^{n-1} + \cdots + g_1z + 1, \quad g_i \in \{0, 1\} \quad (2.20)$$



から構成される図 2.7 に示すような  $n$  段シフトレジスタを用いて発生出来る。ただし、 $\oplus$  は各要素の排他的論理和を表し、また、 $g_j = 0$  の場合は結線をしない。シフトレジスタは、全 0、すなわち  $(c_0, c_1, \dots, c_{n-1}) = (0, 0, \dots, 0)$  以外の全ての状態をとり、最大周期  $2^n - 1$  の  $m$  系列を生成する。その際、シフトレジスタの初期状態（もちろん全 0 以外）によって、位相シフトの異なる  $m$  系列が生成されるが、通常これらは一つの  $m$  系列とみなされる。よって、一つのシフトレジスタから一つの  $m$  系列が生成されることになる。表 2.2 には、 $m$  系列を生成する原始多項式の例を示す。

図 2.7:  $m$  系列を生成する  $n$  段シフトレジスタ回路表 2.2:  $m$  系列を生成する原始多項式の例

次数 $n$	周期 $T$	$g(z)$
3	7	$z^3 + z + 1$
4	15	$z^4 + z + 1$
5	31	$z^5 + z^2 + 1$ $z^5 + z^3 + 1$
6	63	$z^6 + z + 1$ $z^6 + z^4 + z^3 + z + 1$
7	127	$z^7 + z + 1$ $z^7 + z^3 + 1$
8	255	$z^8 + z^4 + z^3 + z^2 + 1$ $z^8 + z^5 + z^3 + z + 1$
9	511	$z^9 + z^4 + 1$ $z^9 + z^4 + z^3 + z + 1$
10	1023	$z^{10} + z^3 + 1$ $z^{10} + z^4 + z^3 + z + 1$
11	2047	$z^{11} + z^2 + 1$ $z^{11} + z^4 + z^2 + z + 1$



この  $m$  系列の主な特徴としては、1 周期内で 0 と 1 の出現する回数が高々 1 しか変わらないこと、および、図 2.8 に示すように偶の自己相関関数は遅れ時間 0 の時 1、それ以外は  $-1/(2^n - 1)$  となりデルタ関数的であること等が挙げられる。従って、平衡性および偶の自己相関特性は最適であり、また、先に述べたように、その段数のシフトレジスタに対して最大の周期を有することから、2 値の擬似乱数系列として広く用いられてきた。もちろん、SS 通信における拡散符号としての応用も例外ではない。しかしながら、 $m$  系列を生成するシフトレジスタの種類は非常に少なく、また、2 つの  $m$  系列の間の相互相関特性は一般にあまり良くない。ただし、中には、一様に小さな偶相互相関値をとる組合せが存在し、そのような組をプリファードペアと呼ぶ。表 2.3 に  $m$  系列を生成する原始多項式の各次数  $n$  に対する、周期  $T$ 、存在する  $m$  系列の数、およびプリファードペアの  $m$  系列の数を示す。この表から、各周期に対する  $m$  系列の数が非常に少ないことがわかる。CDMA においては良好な相関特性を有する多数の系列が必要とされるので、様々な拡散符号用の擬似乱数系列が提案されてきた。にもかかわらず、その生成法の容易さから、現在でも  $m$  系列はしばしば拡散符号として用いられている。その際、長周期の  $m$  系列を適当な長さに切り取って用いることが多い。

また、2 値系列としてだけでなく、これを実数値に変換して用いる方法も、Tausworthe<sup>[36]</sup> や Lewis & Payne<sup>[37]</sup> によって提案されている。

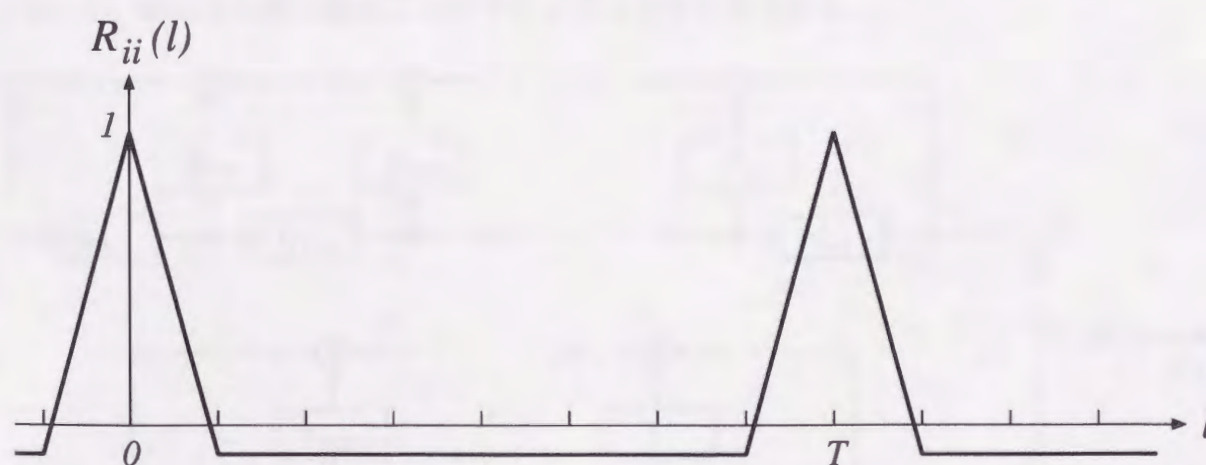


図 2.8:  $m$  系列の偶自己相関特性



表 2.3:  $m$  系列の数

次数 $n$	周期 $T$	$m$ 系列の数	プリファードペアの $m$ 系列の数
3	7	2	2
4	15	2	0
5	31	6	3
6	63	6	2
7	127	18	6
8	255	16	0
9	511	48	2
10	1023	60	3
11	2047	176	4

### 2.4.2 Kasami 系列

Kasami 系列は、 $m$  系列を生成する2つのシフトレジスタによって生成される。ただしこの場合、周期の異なる2つの  $m$  系列を用いる。すなわち、 $n$  次の原始多項式  $g(z)$  および次式で定義される  $n/2$  次の原始多項式（ただし  $n$  は偶数）

$$f(z) = z^{\frac{n}{2}} + f_{\frac{n}{2}-1}z^{\frac{n}{2}-1} + \cdots + f_1z + 1, \quad f_i \in \{0, 1\} \quad (2.21)$$

を用いて、図 2.9 の様に構成したシフトレジスタで生成される。

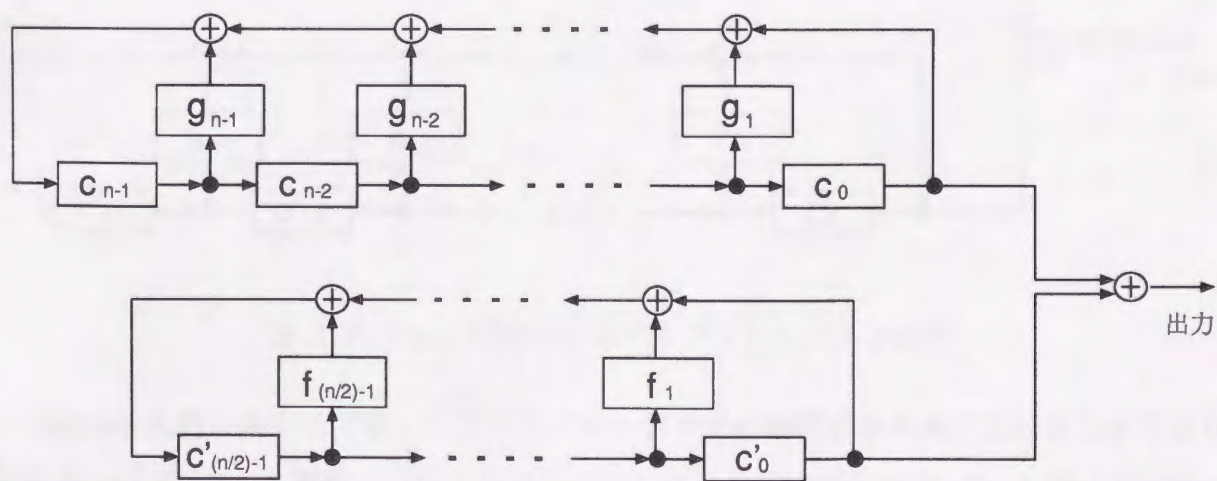


図 2.9: Kasami 系列を生成するシフトレジスタ回路

まず、各シフトレジスタに全0以外のある初期状態を与えると、これより一つの系列が生成される。この時、 $n/2$  段のシフトレジスタの初期状態を変化させることにより周期



$2^n - 1$  の  $2^{\frac{n}{2}} - 1$  種類の系列が生成される。こうして生成された  $2^{\frac{n}{2}} - 1$  個 ( $n$  段シフトレジスタから生成される  $m$  系列を加えると  $2^{\frac{n}{2}}$  個) の系列の集合を Kasami 系列の“ファミリー”と呼び、さらにその集合の要素数を“ファミリーサイズ”と呼ぶ。このファミリー内においては、あらゆる組合せでの偶相互相関関数は3値しか有しないようになっている。周期  $2^n - 1$  の2つの Kasami 系列間の偶相互相関関数は、各遅れ時間に対して

$$-\frac{1}{2^n - 1}, \quad \frac{2^{\frac{n}{2}} - 1}{2^n - 1}, \quad -\frac{2^{\frac{n}{2}} - 1}{2^n - 1}$$

の3値のいずれかをとる。偶自己相関関数についても遅れ時間0を除いては同様である。

### 2.4.3 Gold 系列

Gold 系列は、プリファードペアの  $m$  系列を用いて生成される。プリファードペアの  $m$  系列を生成する  $n$  次原始多項式をそれぞれ、 $g(z)$ ,  $h(z)$  とすると、Gold 系列は Kasami 系列と同様、図 2.10 のようにそれぞれのシフトレジスタを組み合わせることによって生成される。

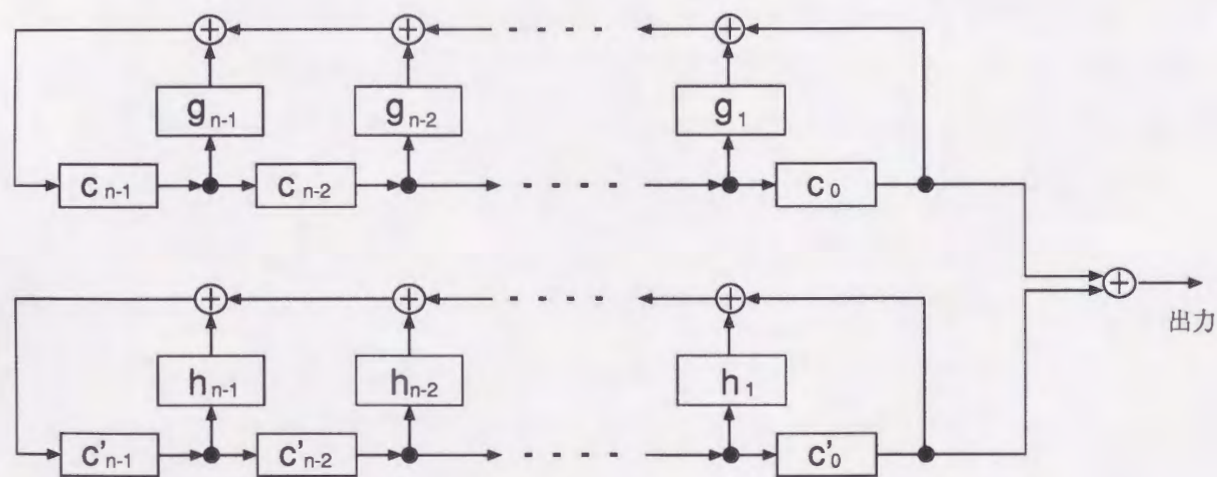


図 2.10: Gold 系列を生成するシフトレジスタ回路

Kasami 系列の場合と同様、片方のシフトレジスタの初期状態を変化させることにより、周期  $2^n - 1$  の  $2^n - 1$  種類の系列が生成される。こうして生成された  $2^n - 1$  個 (2つの  $m$  系列を加えると  $2^n + 1$  個) の系列の集合を Gold 系列のファミリーと呼ぶ。周期  $2^n - 1$  の2つの Gold 系列間の偶相互相関関数（および遅れ時間0以外の偶自己相関関数）は、各遅れ時間に対して

$$-\frac{1}{2^n - 1}, \quad \frac{2^{\lfloor \frac{n+2}{2} \rfloor} - 1}{2^n - 1}, \quad -\frac{2^{\lfloor \frac{n+2}{2} \rfloor} + 1}{2^n - 1}$$



の3値のいずれかをとる。ただし、 $[m]$  は  $m$  の整数部分を表す。また、Gold 系列の生成は  $n$  が4の倍数でない時に限られる。

この他、さらに1と0の出現頻度の平衡性を改善した Bent 系列等<sup>[4],[5]</sup>が提案されている。これらの系列は、偶相関特性や平衡性を最適にしようという立場で、有限体理論に基づいて設計された系列である。また、平均誤り確率を評価するためには、偶および奇相関値の分布を知る必要があるが、奇相関値の分布については、理論的評価が困難であるために、偶相関分布から近似的に求める方法等が提案されている<sup>[5]</sup>。また、その生成法からもわかるように、これらのシフトレジスタ系列は、周期長やファミリーサイズに制限があり、その種類数は必ずしも多くはない。

この他、以上のような2値系列だけでなく、多相あるいは多値の系列等の設計も盛んに行なわれている<sup>[5]</sup>。



## 第3章

### カオスの拡散符号への応用

#### 3.1 はじめに

スペクトル拡散通信技術の成否は、用いる拡散符号（擬似乱数系列）の相関特性に大いに依存する<sup>[1]</sup>。近年、拡散符号として、さまざまな系列が提案されているが、もっとも有名なのは、Gold 系列や Kasami 系列に代表される線形シフトレジスタ (linear feedback shift register; LFSR) 系列である<sup>[1],[2]</sup>。これらは、非常に良い偶相関特性を示すことで知られているが、その系列が形成する集合（ファミリー）の大きさ（ファミリーサイズ）や、異なったファミリーの数が限られている。このことは、その系列が容易に第三者に知られてしまう恐れが大きく、セキュリティ上好ましくない。また、将来増大と思われる利用者に対応できるか否かが疑問である。もちろん、通信者の情報を傍受者から守るための一つの方法は、周期  $T$  の場合、 $2^T$  種類の 2 値系列の中から、“ランダム” に選び出した系列を用いることであろう。しかしながら、簡単な“決定論的”アルゴリズムによる、そのような擬似乱数の選び方は容易でなく、系列の“ランダム性”を定義することや評価すること自体非常に難しい問題である<sup>[6],[7]</sup>。

本章では、非線形エルゴード写像より生成される“カオス”に基づいた 2 値の擬似乱数系列の簡便な方法を与える。この方法では、非線形写像から得られる非周期の実数値系列を 2 値系列に変換し、周期  $T$  で切り取って周期系列として用いる。そして、任意に初期値等のパラメータを選ぶことにより、異なった系列のファミリーを形成することが出来る。そこで、こうして得られる系列の有用性を調べるために、次のようにして相関特性の評価を行なう。まず第一に、カオス 2 値系列の相関関数が低い値を持つことを、カオスの時系列解析法の一つである“空間平均法”に基づいて理論的に示す。次に、周期  $T$  の系列が形成するそれぞれのファミリー内でのすべてのペアに対して、偶および奇相関関数を計算し、各々



のペアにおける最大相関値の分布の評価を行なう。さらに、それぞれのファミリーに独立な1つの妨害系列を加えた場合に付いても同様な評価を行なう。これらの数値結果は以下の通りである。カオスビット系列の偶相関特性は従来の Gold 系列や Kasami 系列に比べると劣っている。一方、奇相関特性については、あまり差が無いものの、ややカオスビット系列の方が劣っている。しかしながら、Gold 系列や Kasami 系列よりも大きい奇相関値をもつような系列のペアの出現確率は非常に小さい。また、Gold 系列や Kasami 系列のファミリーに1個の妨害系列を加えた場合、その相関特性がかなり劣化するのに対し、カオス系列の場合はそれほどの変化はない。カオス系列を生成する非線形写像は、幾つかのパラメータを持っており、これらを変えることによって、より多くの擬似乱数系列を生成できるので、カオス系列は符号分割多元接続 (CDMA) のための拡散符号として良い候補者であるといえる。

### 3.2 エルゴード写像によるカオスの生成法と不変密度

カオスを呈する最も単純な系は、一次元差分方程式

$$x_{n+1} = \tau(x_n) \quad (3.1)$$

である<sup>[8],[9]</sup>。ここで、 $x_n \in I, n = 0, 1, 2, \dots$  で  $\tau$  は区間  $I$  からそれ自身への非線形写像である。Ulam と von Neumann はロジスティック (Logistic) 写像  $\tau(x) = 4x(1-x)$  ( $0 \leq x \leq 1$ ) より生成される系列  $\{\tau^n(x)\}_{n=0}^{\infty}$  が良い乱数生成器の候補者であることを指摘し、テント写像  $\tau(x) = 2x, (0 \leq x \leq \frac{1}{2})$  および  $\tau(x) = 2(1-x), (\frac{1}{2} \leq x \leq 1)$  に対する共型変換  $h(x) = (2/\pi) \sin^{-1} x^{1/2}$  を与えた<sup>[8]</sup>。擬似乱数としてのカオス系列の応用については多くの研究がなされており<sup>[10]-[16]</sup>、さらに、カオス系列をスペクトル拡散 (SS) 通信や暗号通信などの通信システムに応用しようとする試みも幾つか見られる<sup>[27]-[33]</sup>。しかしながら、カオスが、従来の線形シフトレジスタ系列等に比べてより有効な擬似乱数生成器であるかどうかという基本的問題が残っている。また、これらの研究においては、区分線形写像により生成されるカオス軌道を用いようという試みが幾つか見られる。しかしながら、例えば  $m$  ビットの有限語長演算で区分線形写像によるカオス軌道を計算すると、その系列の周期が非常に短いことが容易にわかる。特に、テント写像の場合、 $m$  回写像した後、初期値  $x_0$  における情報はすべて消えてしまう。一方、ロジスティック写像の力学系の計算においては、たとえそれが“正確な”計算ではないとしても、適度にカオス的な系列が非常に長い時間継



続する。この性質は、擬軌道特性と呼ばれる<sup>[9]</sup>。従って、“有限語長演算”の影響は、ロジスティック写像とテント写像とでは全く異なることに注意しなければならない<sup>[9]</sup>。さらに、2つのセグメントからなる区分線形写像によるカオス軌道の自己相関関数は、写像がテントあるいはベルヌイ (Bernoulli) 写像である時のみデルタ関数に等しいことが知られている<sup>[19]</sup>。一方、 $k$  次のチェビシェフ (Chebyshev) 写像<sup>[17]</sup>

$$x_{n+1} = \cos(k \cos^{-1} x_n) \quad (-1 \leq x \leq 1) \quad (3.2)$$

はほとんどあらゆる初期値  $x_0$  に対してカオス軌道を生成し、その自己相関関数はデルタ関数である<sup>[18]</sup>。本論文では、主にチェビシェフ写像より生成されるカオス軌道の統計的性質を議論する。カオスを擬似乱数系列として通信に应用する場合、たとえカオス軌道が誤差を含んでいたとしても、符号化と復号化において同一の軌道が生成出来さえすれば良いことに注意しなければならない。また、暗号通信システムにおいては、統計的性質の良い、長周期の擬似乱数系列が必要である。

本論文では、一次元写像  $x_{n+1} = \tau(x_n)$  で生成される解軌道  $\{\tau^n(x)\}_{n=0}^{\infty}$  を考える。ここで、 $\tau^n(x) = x_n$ ,  $x = x_0$  である。解軌道  $\{\tau^n(x)\}_{n=0}^{\infty}$  の性質、すなわち写像  $\tau$  の性質を調べる場合、数学、(統計) 物理学、工学等の分野では、 $\{\tau^n(x)\}_{n=0}^{\infty}$  が区間  $I$  の部分集合  $S$  を訪れた頻度の長時間平均

$$\lim_{T \rightarrow \infty} \frac{1}{T} \sum_{n=0}^{T-1} \chi_S(\tau^n(x)) \quad (3.3)$$

の存在がまず問題とされる。ただし、 $\chi_S$  は  $S$  の定義関数であり、

$$\chi_S(x) = \begin{cases} 1 & (x \in S \text{ の時}) \\ 0 & (\text{その他の場合}) \end{cases} \quad (3.4)$$

である。エルゴード定理によれば、写像  $\tau$  がルベーグ測度に関して絶対連続な不変測度  $\mu$  をもつとき、任意の可測集合  $S$  に対し、上記の長時間平均が存在し、ほとんど全ての初期値  $x$  に対し

$$\lim_{T \rightarrow \infty} \frac{1}{T} \sum_{n=0}^{T-1} \chi_S(\tau^n(x)) = \mu(S) \quad (3.5)$$

となる。ただし、測度  $\mu$  が不変であるとは、任意の可測集合  $S$  に対し

$$\mu(S) = \mu(\tau^{-1}(S)) \quad (3.6)$$

が成立することであり、 $\mu$  ルベーグ測度に対し絶対連続である時、積分可能な関数  $f$  が存在し

$$\mu(S) = \int_S f(x) dx \quad (3.7)$$



と書くことが出来る。また、不変測度をもつ写像  $\tau$  がエルゴード的であるとは、 $\tau^{-1}(S) = S$  を満たす集合が  $\mu = 0$  と  $1$  との自明な場合に限る時をいう。絶対連続な不変測度 (absolutely continuous invariant measure) を略して ACI 測度と呼び、それに対応する式 (3.7) の関数  $f$  を不変密度と呼ぶ。写像  $\tau$  の不変密度  $f(x)$  が存在する時、式 (3.6) の集合  $S$  として  $x$  の近傍  $dx$  をとれば、式 (3.6), (3.7) より  $f(x)$  は、ペロンフロベニウス (Perron-Frobenius; P-F) 方程式

$$P_{\tau}f(x) = f(x) \quad (3.8)$$

を満たすことがわかる (図 3.1 参照)。ただし、 $P_{\tau}$  は

$$P_{\tau}h(x) = \frac{d}{dx} \int_{\tau^{-1}([a,x])} h(y) dy \quad (3.9)$$

$$= \sum_{y_m(x) \in \tau^{-1}(x)} \frac{h(y_m(x))}{|\tau'(y_m(x))|} \quad (3.10)$$

で定義される可積分関数の集合  $L_1$  から  $L_1$  への演算子であり、 $y_m(x)$  は写像  $\tau$  の下での  $x$  の  $m$  番目の逆像を示す。従って、不変密度  $f$  は式 (3.8) を満足する  $P_{\tau}$  の不動点と理解され、これを  $f^*(x)$  と表すことにする。この不変密度  $f^*(x)$  は、次節に示すように、カオスの統計量の空間平均を求める際に不可欠な基本量である。

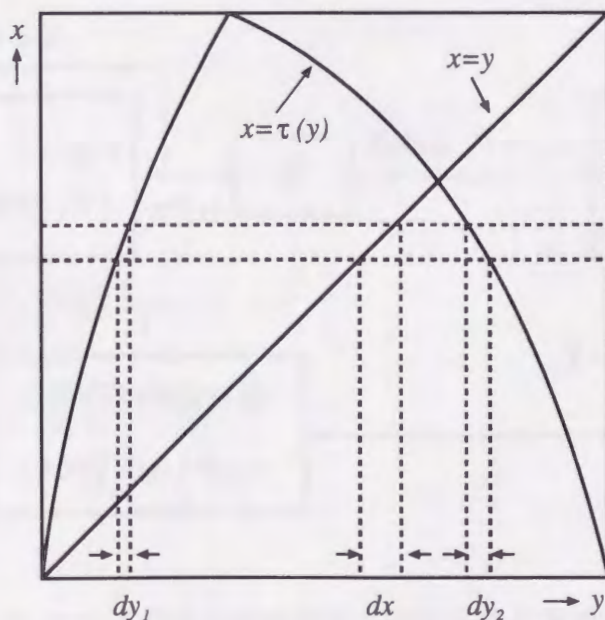


図 3.1: 式 (3.8) の説明図。本図では、 $\tau^{-1}(x) = \{y_1, y_2\}$  である。  $f(x)dx = \sum_m f(y_m)dy_m$  に  $dy_m = dx/|\tau'(y_m)|$  ( $m = 1, 2$ ) を代入すると  $f(x) = \sum_m f(y_m)/|\tau'(y_m)|$  を得る。



### 3.3 カオスの時系列解析法と相関関数

初期値  $x$  に対する時刻  $n$  の任意の観測値  $F(\tau^n(x))$  は軌道  $\{\tau^n(x)\}_{n=0}^{\infty}$  と同様、一種の確率変数であり、その時間平均  $F_T(x)$  および空間（アンサンブル）平均  $\langle F \rangle$  は、それぞれ

$$F_T(x) = \frac{1}{T} \sum_{n=0}^{T-1} F(\tau^n(x)) \quad (3.11)$$

$$\langle F \rangle = \int_I F(x) f^*(x) dx \quad (3.12)$$

で定義される。ここで  $f^*(x)$  前節で述べた不変密度であるが、チェビシエフ写像の場合、

$$f^*(x) = \frac{1}{\pi \sqrt{1-x^2}} \quad (3.13)$$

である。バーコフ (Birchoff) のエルゴード定理によれば、エルゴード写像  $\tau(x)$  に対して

$$\lim_{T \rightarrow \infty} F_T(x) = \langle F \rangle \quad \text{a.e.} \quad (3.14)$$

となる。(図 3.2 参照.) 時間平均  $F_T(x)$  は、カオスの鋭敏な初期値依存性のために、それ自身が確率的な振舞いをするので、カオスの統計量の理論的評価法としては、初期値に依存しない空間平均法が有力である。

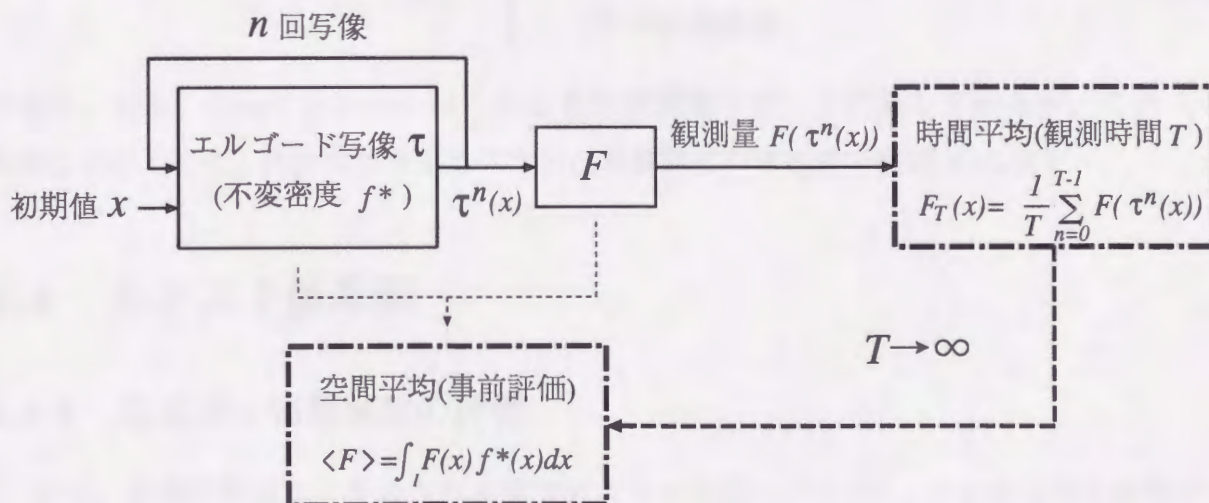


図 3.2: カオスの時系列解析法 (時間平均と空間平均)

次にカオス系列の相関関数を定義する。関数  $g(x)$  および  $h(x)$  より得られるカオス系列  $\{g(\tau^n(x))\}_{n=0}^{\infty}$  と  $\{h(\tau^n(x))\}_{n=0}^{\infty}$  に関し

$$C(x, \ell; g, h) = (g(x) - \langle g \rangle)(h(\tau^\ell(x)) - \langle h \rangle) \quad (3.15)$$



とすると,  $C_T(x, \ell; g, h)$  および  $\langle C(\ell; g, h) \rangle$  は2つの系列の間の, それぞれ, 時間平均形および空間平均形の相互相関関数を表す. ただし,  $g = h$  の時は自己相関関数を表す. 本論文では, 非線形エルゴード写像として, 主にチェビシェフ写像を用いるが, その理由は, これより生成される実数値系列  $\{\tau^n(x)\}_{n=0}^{\infty}$  の空間平均形の自己相関関数  $\langle C(\ell; x, x) \rangle$  はデルタ関数に等しい<sup>[18]</sup>ことが知られており, さらに, 以下に示すように, Geisel & Fairen<sup>[25]</sup>によって, 高次の自己相関関数もデルタ関数的であることが知られているからである. 3次および4次の自己相関関数は, それぞれ,

$$\begin{aligned} \langle C^{(3)}(\ell, m; x, x, x) \rangle &= \int_I x \tau^\ell(x) \tau^{\ell+m}(x) f^*(x) dx \\ &= \frac{1}{4} \delta_{k,2} \delta_{\ell,0} \delta_{m,1}, \end{aligned} \quad (3.16)$$

$$\begin{aligned} \langle C^{(4)}(\ell, m, n; x, x, x, x) \rangle &= \int_I x \tau^\ell(x) \tau^{\ell+m}(x) \tau^{\ell+m+n}(x) f^*(x) dx \\ &= \frac{1}{4} \delta_{\ell,0} \delta_{m,0} + \frac{1}{8} \delta_{\ell,0} \delta_{m,0} \delta_{n,0} \\ &\quad + \frac{1}{8} \delta_{k,2} \delta_{\ell,0} \delta_{m,1} \delta_{n,1} + \frac{1}{8} \delta_{k,3} \delta_{\ell,0} \delta_{m,0} \delta_{n,1}. \end{aligned} \quad (3.17)$$

のように計算されている. ここで,

$$\delta_{\ell,m} = \begin{cases} 0 & (\ell = m \text{ の時}) \\ 1 & (\text{その他の場合}) \end{cases} \quad (3.18)$$

である. なお, Geisei & Fairen はこれらを特性関数を使って計算しているが, これより, 簡単な方法として, P-F 作用素を用いた自己相関関数の導出法を付録 A に示す.

## 3.4 カオス 2 値系列

### 3.4.1 生成法と相関関数の評価

まず, 非線形写像より生成される実数値カオス系列  $\{\tau^n(x)\}_{n=0}^{\infty}$  を 2 値系列に変換する簡単な方法を 2 つ提案する.

[方法 1] 閾値関数

$$\theta_c(x) = \begin{cases} 0 & (x < c) \\ 1 & (x \geq c) \end{cases} \quad (3.19)$$



を用いることにより, 2 値系列  $\{\theta_c(\tau^n(x))\}_{n=0}^{\infty}$  が得られる. この系列を “カオス 2 進系列” あるいは “チェビシェフ 2 進系列” と呼ぶ.

[方法 2]  $x$  の絶対値を次のように 2 進ビットに展開する.

$$|x| = 0.b_1(x)b_2(x)\cdots b_i(x)\cdots, \quad b_i(x) \in \{0, 1\} \quad (3.20)$$

第  $i$  番目のビットを取り出す関数  $b_i(x)$  は

$$b_i(x) = \sum_{r=1}^{2^i-1} (-1)^{r-1} \hat{\theta}_{\frac{r}{2^i}}(x) \quad (3.21)$$

で表される. ここで  $\hat{\theta}_c(x)$  は,

$$\hat{\theta}_c(x) = \begin{cases} 0 & (|x| < c) \\ 1 & (|x| \geq c) \end{cases}, \quad (c \geq 0) \quad (3.22)$$

である. すると, 図 3.3 に示すように, 2 値系列  $\{b_i(\tau^n(x))\}_{n=0}^{\infty}$  を得ることが出来る. この系列は, “カオスビット系列” あるいは “チェビシェフビット系列” と呼ばれる.

$$\begin{array}{ccccccc} & & & & & \text{i-th bit seq.} & \\ |x_0| & = & b_1(x_0) & b_2(x_0) & \cdots & b_i(x_0) & \cdots \\ |x_1| & = & b_1(x_1) & b_2(x_1) & \cdots & b_i(x_1) & \cdots \\ |x_2| & = & b_1(x_2) & b_2(x_2) & \cdots & b_i(x_2) & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \\ |x_n| & = & b_1(x_n) & b_2(x_n) & \cdots & b_i(x_n) & \cdots \\ \vdots & & \vdots & \vdots & & \vdots & \end{array}$$

図 3.3: カオスビット系列

このようにして生成される 2 値系列は, 適当な長さに切ることにより周期系列として用いられる. 従って, 生成法は異なるものの, 一旦生成された後は, 従来のシフトレジスタを用いたシステムがそのまま流用出来る. この点において, カオスの同期現象を利用した通信システム<sup>[27]–[32]</sup>とは大きく異なることに注意されたい. また, 一つの初期値より複数の



2値系列を生成することで、従来困難とされていた空間平均法による相互相関関数の概念を導入することができ、その事前評価が可能となる。

次に、上記の2つの方法により生成されるチェビシエフ2進およびビット系列の相関関数を考える。

方法1により得られるチェビシエフ2進系列  $\{\theta_c(\tau^n(x))\}_{n=0}^{\infty}$  については、その正規化自己相関関数は

$$\left| \frac{\langle C(\ell; \theta_c, \theta_c) \rangle}{\langle C(0; \theta_c, \theta_c) \rangle} \right| \leq \frac{1}{k^\ell} \quad (3.23)$$

のように計算されており<sup>[20]</sup>、チェビシエフ写像の次数  $k$  が大きい時、閾値  $c$  に無関係にデルタ関数的であることがわかる。一方、ある1つの初期値  $x$  から得られる2つの系列  $\{\theta_c(\tau^n(x))\}_{n=0}^{\infty}$  および  $\{\theta_{c'}(\tau^n(x))\}_{n=0}^{\infty}$  の間の相互相関関数は

$$\langle C(0; \theta_c, \theta_{c'}) \rangle = \begin{cases} \langle \theta_c \rangle (1 - \langle \theta_{c'} \rangle) & (c > c') \\ \langle \theta_{c'} \rangle (1 - \langle \theta_c \rangle) & (c < c') \end{cases} \quad (3.24)$$

$$|\langle C(\ell; \theta_c, \theta_{c'}) \rangle| \leq \frac{\langle \theta_{c'} \rangle (1 - \langle \theta_{c'} \rangle)}{k^\ell} \quad (3.25)$$

$$\langle \theta_c \rangle = \frac{1}{\pi} \cos^{-1} c \quad (3.26)$$

のように評価される。

方法2により得られるチェビシエフビット系列  $\{b_i(\tau^n(x))\}_{n=0}^{\infty}$  の自己相関関数は

$$\langle C(0; b_i, b_i) \rangle = \langle b_i \rangle - \langle b_i \rangle^2 \quad (3.27)$$

$$\left| \frac{\langle C(\ell; b_i, b_i) \rangle}{\langle C(0; b_i, b_i) \rangle} \right| < \frac{1}{1 - \langle b_i \rangle} \cdot \frac{1}{k^\ell} \quad (3.28)$$

のように評価できる。

一方、ある1つの初期値  $x$  より生成される2つの系列  $\{b_i(\tau^n(x))\}_{n=0}^{\infty}$  および  $\{b_j(\tau^n(x))\}_{n=0}^{\infty}$  の相互相関関数は、

$$\langle C(0; b_i, b_j) \rangle = Q_{ij} - \langle b_i \rangle \langle b_j \rangle \quad (3.29)$$

$$|\langle C(\ell; b_i, b_j) \rangle| < \frac{\langle b_j \rangle}{k^\ell}, \quad (i < j) \quad (3.30)$$

となる。ここで、

$$Q_{ij} = \int_I b_i(x) b_j(x) f^*(x) dx = 2 \int_{I_{ij}} dx \quad (3.31)$$

$$I_{ij} = \left( \bigcup_{\alpha=1}^{2^{i-1}} I_i(\alpha) \right) \cap \left( \bigcup_{\beta=1}^{2^{j-1}} I_j(\beta) \right) \quad (3.32)$$

$$I_i(\alpha) = \left[ \frac{1}{\pi} \cos^{-1} \frac{2\alpha}{2^i}, \frac{1}{\pi} \cos^{-1} \frac{2\alpha-1}{2^i} \right] \quad (3.33)$$



である。(導出は付録B参照。) 以上の評価から、チェビシェフ写像の次数  $k$  を大きくした時、良い相関特性を有する2値系列が得られることがわかる。

また、 $\{b_i(\tau^n(x))\}_{n=0}^{\infty}$  の空間平均値  $\langle b_i \rangle$  は、

$$\langle b_i \rangle = \frac{2}{\pi} \sum_{m=1}^{2^{i-1}} \left( \cos^{-1} \frac{2m-1}{2^i} - \cos^{-1} \frac{2m}{2^i} \right) \quad (3.34)$$

で与えられ、 $i$  が増加するにつれて

$$\langle b_i \rangle \rightarrow \frac{1}{2} \quad (3.35)$$

のような性質をもつ。

ここで、チェビシェフビット系列の相関関数の具体的な評価例を幾つか示す。

[例1] 第1ビットと第2ビットの自己相関関数はそれぞれ、

$$\begin{cases} \langle C(0; b_1, b_1) \rangle = \langle b_1 \rangle - \langle b_1 \rangle^2 = \frac{2}{9} \\ \left| \frac{\langle C(\ell; b_1, b_1) \rangle}{\langle C(0; b_1, b_1) \rangle} \right| < \frac{1}{1 - \langle b_1 \rangle} \cdot \frac{1}{k^\ell} = \frac{3}{k^\ell}, \\ \langle C(0; b_2, b_2) \rangle = \langle b_2 \rangle - \langle b_2 \rangle^2 \simeq 0.232 \\ \left| \frac{\langle C(\ell; b_2, b_2) \rangle}{\langle C(0; b_2, b_2) \rangle} \right| < \frac{1}{1 - \langle b_2 \rangle} \cdot \frac{1}{k^\ell} \simeq \frac{2.72}{k^\ell} \end{cases}$$

のように評価される。

[例2] 第1ビットと第2ビット間および第1ビットと第3ビット間の相互相関関数は、それぞれ、

$$\begin{cases} \langle C(0; b_1, b_2) \rangle = Q_{12} - \langle b_1 \rangle \langle b_2 \rangle \simeq 0.0384 \\ \left| \frac{\langle C(\ell; b_1, b_2) \rangle}{\langle C(0; b_1, b_2) \rangle} \right| < \frac{\langle b_2 \rangle}{k^\ell} \simeq \frac{0.633}{k^\ell}, \\ \langle C(0; b_1, b_3) \rangle = Q_{13} - \langle b_1 \rangle \langle b_3 \rangle \simeq 0.0308 \\ \left| \frac{\langle C(\ell; b_1, b_3) \rangle}{\langle C(0; b_1, b_3) \rangle} \right| < \frac{\langle b_3 \rangle}{k^\ell} \simeq \frac{0.602}{k^\ell} \end{cases}$$

のように評価される。

なお、ここでは、相関関数の上限を評価したに過ぎないが、第4章においてその厳密な評価を行なう。



### 3.4.2 拡散符号としての性能評価

相関特性の理論的評価から、チェビシェフビット系列の方がチェビシェフ2進系列よりも良い相関特性をもつことがわかるので、前者の拡散符号としての性能評価を行なうことにする。周期  $T$  の周期系列  $\{b_i(\tau^n(x))\}_{n=0}^{T-1}$  は、非周期系列  $\{b_i(\tau^n(x))\}_{n=0}^{\infty}$  を長さ  $T$  で打ち切ることによって容易に得られる。そのような周期系列は初期値  $x$  の関数となるので、その系列自身や相関関数は一種の確率変数となる。ここで、 $X$  を初期値  $x$  の集合とすると、集合  $\{\{b_i(\tau^n(x))\}_{n=0}^{T-1} | x \in X\}$  は周期  $T$  のチェビシェフビット系列の“ファミリー”と呼ばれる集合を表す。また、その集合の要素数  $L$  は“ファミリーサイズ”と呼ばれる。

まず、チェビシェフビット系列における“1”および“0”の出現頻度の平衡性を調べる。系列の平衡性は、直流成分の除去や耐妨害電波の点で望まれているものである。 $p$  および  $q$  をそれぞれ、周期  $T$  の系列中の“1”および“0”の出現回数とすると、 $(p - q)/T$  は“1”および“0”の出現確率の“非平衡度”を示す。図 3.4 は、各々のビットにおけるこの非平衡度の値を周期  $T = 63$  およびチェビシェフ写像の次数  $k = 2^{16}$  の場合に対し、100 個の初期値について計算したものである。これより、より大きいビット番号が良い平衡性を示していることがわかる。この平衡性は、Gold 系列や Kasami 系列より悪いが、図 3.5 に示すように、系列の周期を  $T = 256$  と長くした場合には、改善されていることがわかる。よって、十分大きいビット番号の系列を用いた方が良いといえる。



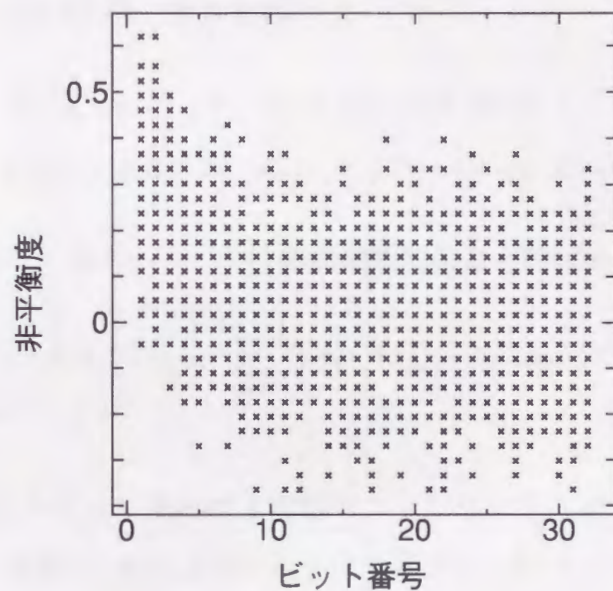


図 3.4: 100 個の初期値に対する周期 63 のチェビシェフビット系列の“1”および“0”の出現確率の非平衡度

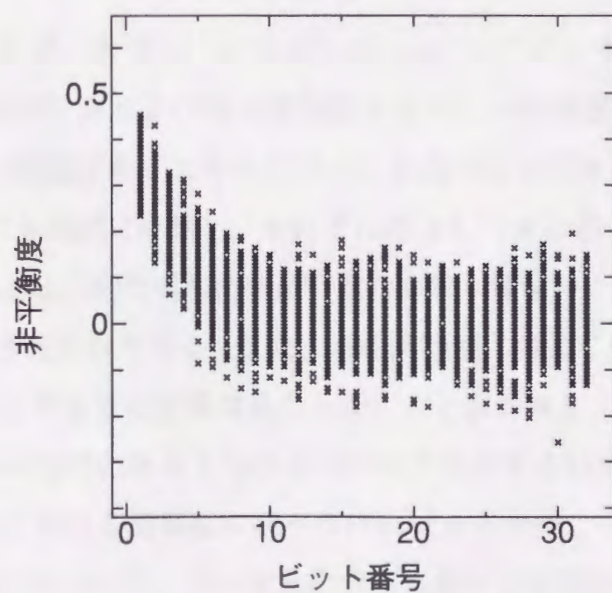


図 3.5: 100 個の初期値に対する周期 256 のチェビシェフビット系列の“1”および“0”の出現確率の非平衡度



2つの  $\{0, 1\}$ -系列  $\{g(\tau^n(x))\}_{n=0}^{T-1}$  と  $\{h(\tau^n(x))\}_{n=0}^{T-1}$  の間の偶相関関数  $R_T(x, \ell; g, h)$  および奇相関関数  $\Theta_T(x, \ell; g, h)$  は、それぞれ、

$$R_T(x, \ell; g, h) = A_T(x, \ell; g, h) + A_T(x, T - \ell; h, g) \quad (3.36)$$

$$\Theta_T(x, \ell; g, h) = A_T(x, \ell; g, h) - A_T(x, T - \ell; h, g) \quad (3.37)$$

と定義される。ここで、 $A_T(x, \ell; g, h)$  は非周期相関関数と呼ばれ、

$$A_T(x, \ell; g, h) = \frac{1}{T} \sum_{n=0}^{T-1-\ell} (2g(\tau^n(x)) - 1)(2h(\tau^{n+\ell}(x)) - 1) \quad (3.38)$$

で与えられる<sup>[1]</sup>。

次に、チェビシェフビット系列の4種類のファミリーを、ビット番号や初期値を変えて構成する。ここで、周期  $T$  およびファミリーサイズ  $L$  はともに63である。4つのファミリーはそれぞれ、C.B.(1), C.B.(2), C.B.(3), そしてC.B.(4)と表され、

$$\begin{aligned} \text{C.B.}(1) &= \{\{b_{15}(\tau^n(x))\}_{n=0}^{62} | x \in X = \{0.003 \times r\}_{r=1}^{63}\} \\ \text{C.B.}(2) &= \{\{b_{15}(\tau^n(x))\}_{n=0}^{62} | x \in X = \{0.009 \times r\}_{r=1}^{63}\} \\ \text{C.B.}(3) &= \{\{b_{14}(\tau^n(x))\}_{n=0}^{62} | x \in X = \{0.003 \times r\}_{r=1}^{63}\} \\ \text{C.B.}(4) &= \{\{b_{16}(\tau^n(x))\}_{n=0}^{62} | x \in X = \{0.003 \times r\}_{r=1}^{63}\} \end{aligned} \quad (3.39)$$

で与えられる。まず、ある2つのチェビシェフビット系列  $\{b_{15}(\tau^n(0.03))\}_{n=0}^{62}$  と  $\{b_{15}(\tau^n(0.06))\}_{n=0}^{62}$  の間の偶および奇相関関数をすべての時間遅れ  $\ell = 0 \sim 62$  に対して計算し、その相関値の頻度分布（ヒストグラム）を図3.6に示す。また、Gold系列およびKasami系列についても同様に計算し、それぞれ図3.7, 3.8に示す。良く知られているように、Gold系列やKasami系列の偶相関値は3値しか取り得ない。一方、チェビシェフビット系列は、偶奇ともに多値を取り得る。また、奇相関特性に関してだけ見ると、これらの3種類の系列の間にはあまり大きな差異は見られないことがわかる。しかしながら、これらは、それぞれのファミリー内でのある1つの系列のペアに対する結果であるので、当然、その他のあらゆる組合せにおける相関値を調べなければならない。それらすべてのヒストグラムを示すことは困難であるので、それぞれの分布における相関値の絶対値の最大値を調べ、その最大値の分布（パーセント値）および最大値の中の最大値を表3.1にまとめている。



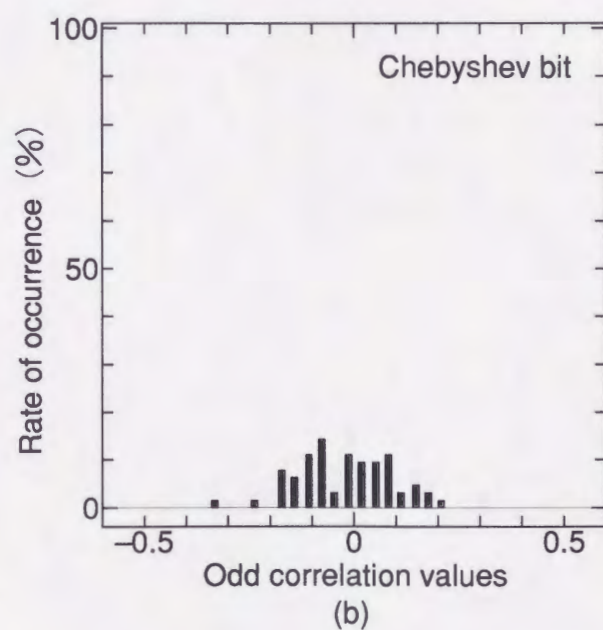
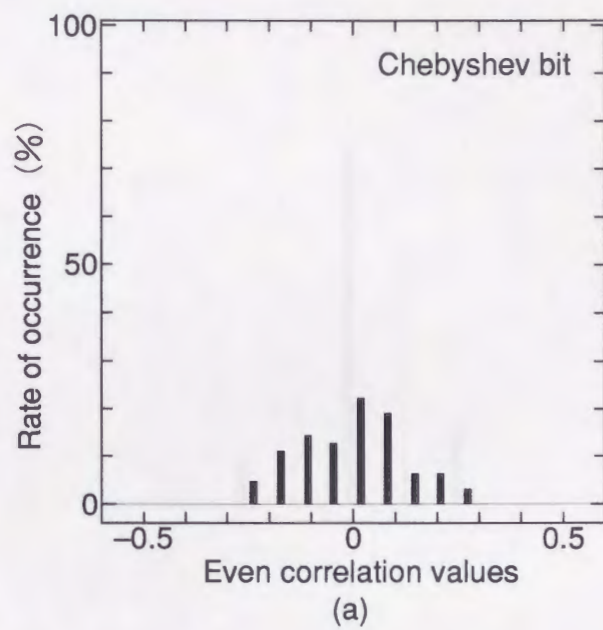


図 3.6: チェビシェフビット系列のあるペアの (a) 偶および (b) 奇相関値のヒストグラム (周期 63)



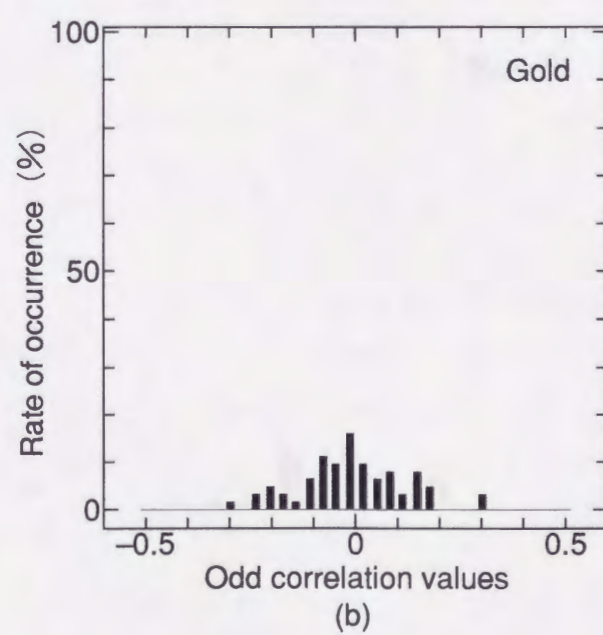
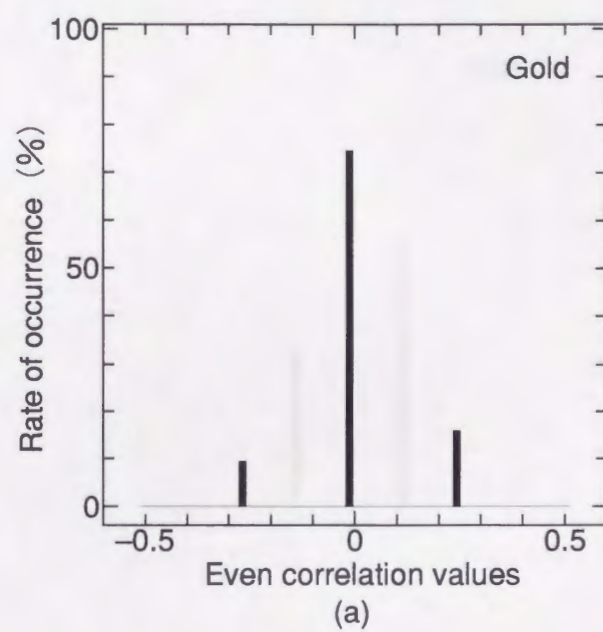


図 3.7: Gold 系列のあるペアの (a) 偶および (b) 奇相関値のヒストグラム (周期 63)



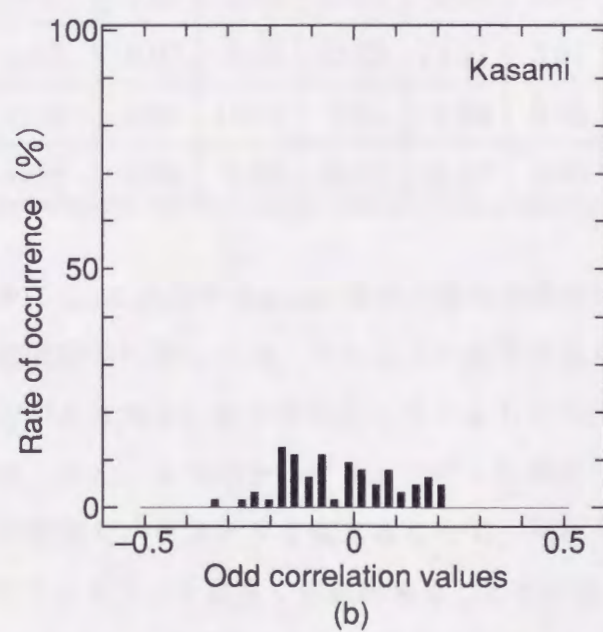
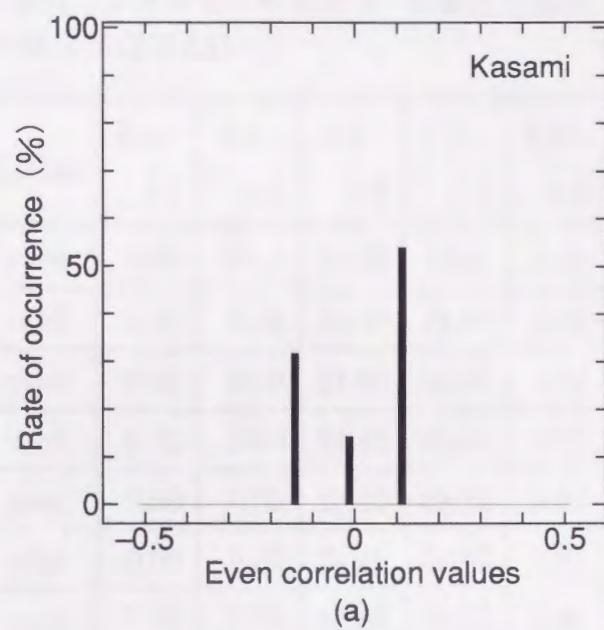


図 3.8: Kasami 系列のあるペアの (a) 偶および (b) 奇相関値のヒストグラム (周期 63)



表 3.1: チェビシェフビット系列 (ファミリーサイズ 63), Gold 系列 (ファミリーサイズ 63), および Kasami 系列 (ファミリーサイズ 7) の最大相関値の分布 (パーセント値) および最大値の中の最大値. (周期長 63)

Kinds of Families		0.0~ 0.1	0.1~ 0.2	0.2~ 0.3	0.3~ 0.4	0.4~ 0.5	0.5~	Max of Maxima
C.B.(1)	even	0.00	0.10	24.25	70.29	5.31	0.05	0.524
	odd	0.00	0.15	22.52	72.02	5.06	0.25	0.524
C.B.(2)	even	0.00	0.10	24.80	69.94	4.76	0.40	0.556
	odd	0.00	0.10	24.45	70.04	5.21	0.20	0.556
C.B.(3)	even	0.00	0.05	25.35	69.39	5.01	0.20	0.556
	odd	0.00	0.20	24.85	69.69	4.91	0.35	0.556
C.B.(4)	even	0.00	0.20	23.86	70.33	5.31	0.30	0.587
	odd	0.00	0.10	25.15	69.19	5.21	0.35	0.556
Gold	even	0.00	0.00	100.0	0.00	0.00	0.00	0.270
	odd	0.00	0.10	22.72	74.11	3.07	0.00	0.429
Kasami	even	0.00	100.0	0.00	0.00	0.00	0.00	0.143
	odd	0.00	0.00	46.43	53.57	0.00	0.00	0.397

この表を見ると, 確かに Gold 系列や Kasami 系列の偶相関特性は非常に優れていることがわかる. しかし, 奇相関特性に関しては, それほどの差異は見られない. さらに, チェビシェフビット系列の方がより大きい最大値を有しているものの, その値の出現確率は非常に小さいことがわかる. また, 4つのチェビシェフビット系列の間にもあまり差は見られない. このことは, 初期値やパラメータを変えることで, 同程度の相関特性を有するチェビシェフビット系列のファミリーを数多く形成出来ることを示唆している.

次に, 各々のファミリーに1個の独立な妨害系列が加わった場合を考え, 同様な計算を行なった結果を表 3.2 に示す.



表 3.2: 1 個の妨害系列を加えた場合の, チェビシェフビット系列 (ファミリーサイズ 63+1), Gold 系列 (ファミリーサイズ 63+1), および Kasami 系列 (ファミリーサイズ 7+1) の最大相関値の分布 (パーセント値) および最大値の中の最大値. (周期長 63)

Kinds of Families		0.0~ 0.1	0.1~ 0.2	0.2~ 0.3	0.3~ 0.4	0.4~ 0.5	0.5~	Max of Maxima
C.B.(1)+1	even	0.00	0.10	24.34	70.22	5.29	0.05	0.524
	odd	0.00	0.14	22.56	72.01	5.05	0.24	0.524
C.B.(2)+1	even	0.00	0.10	24.92	69.74	4.86	0.38	0.556
	odd	0.00	0.10	24.53	70.03	5.15	0.19	0.556
C.B.(3)+1	even	0.00	0.05	25.25	69.55	4.96	0.19	0.556
	odd	0.00	0.19	24.58	69.94	4.95	0.34	0.556
C.B.(4)+1	even	0.00	0.19	23.67	70.56	5.29	0.29	0.587
	odd	0.00	0.10	24.91	69.46	5.19	0.34	0.556
Gold+1	even	0.00	0.00	97.50	2.02	0.43	0.05	0.556
	odd	0.00	0.09	22.61	74.17	3.13	0.00	0.460
Kasami+1	even	0.00	80.00	8.57	11.43	0.00	0.00	0.397
	odd	0.00	0.00	37.14	57.14	5.72	0.00	0.429

これを見ると, Gold 系列や Kasami 系列の相関特性は劣化しており, 特に偶相関特性の劣化が著しいことがわかる. Gold 系列や Kasami 系列は, 低い偶相関値を有するように設計されているため, 全く別の妨害系列が加わった時に, 高い相関値が出現することは当然といえる. 一方, チェビシェフビット系列は, 元来“ランダム”な系列であるために, 妨害系列が加わっても, 相関特性はあまり変化しない. また, 表 3.3 に見られるように, ファミリーサイズを大きくした場合についても, やはり相関特性にあまり変化は見られない. このことは, より多くのユーザーに系列を割り当てることが出来ることを示唆している. さらに, 表 3.4 には, 周期を長くした場合についての結果を示しており, 周期が短い時よりも相関値が小さくなっていることがわかる. ただし, 先に述べたように, 拡散符号の周期を長くすると, それに応じて帯域も広がるので, あまりに長い周期の系列は拡散符号として実用的ではないことに注意しなければならない. 表 3.3 および表 3.4 における C.B.(5)-(12) はそれぞれ,

$$\text{C.B.}(5) = \{ \{ b_{15}(\tau^n(x)) \}_{n=0}^{62} | x \in X = \{ 0.003 \times r \}_{r=1}^{100} \}$$



$$\begin{aligned}
\text{C.B.}(6) &= \{ \{b_{15}(\tau^n(x))\}_{n=0}^{62} | x \in X = \{0.009 \times r\}_{r=1}^{100} \} \\
\text{C.B.}(7) &= \{ \{b_{14}(\tau^n(x))\}_{n=0}^{62} | x \in X = \{0.003 \times r\}_{r=1}^{100} \} \\
\text{C.B.}(8) &= \{ \{b_{16}(\tau^n(x))\}_{n=0}^{62} | x \in X = \{0.003 \times r\}_{r=1}^{100} \} \\
\text{C.B.}(9) &= \{ \{b_{15}(\tau^n(x))\}_{n=0}^{1022} | x \in X = \{0.003 \times r\}_{r=1}^{31} \} \\
\text{C.B.}(10) &= \{ \{b_{15}(\tau^n(x))\}_{n=0}^{1022} | x \in X = \{0.009 \times r\}_{r=1}^{31} \} \\
\text{C.B.}(11) &= \{ \{b_{14}(\tau^n(x))\}_{n=0}^{1022} | x \in X = \{0.003 \times r\}_{r=1}^{31} \} \\
\text{C.B.}(12) &= \{ \{b_{16}(\tau^n(x))\}_{n=0}^{1022} | x \in X = \{0.003 \times r\}_{r=1}^{31} \}
\end{aligned} \tag{3.40}$$

とした。

表 3.3: チェビシェフビット系列の最大相関値の分布（パーセント値）および最大値の中の最大値。（周期長 63, ファミリーサイズ 100）

Kinds of Families		0.0~ 0.1	0.1~ 0.2	0.2~ 0.3	0.3~ 0.4	0.4~ 0.5	0.5~	Max of Maxima
C.B.(5)	even	0.00	0.04	23.72	70.59	5.47	0.18	0.587
	odd	0.00	0.10	24.04	70.35	5.29	0.22	0.556
C.B.(6)	even	0.00	0.04	23.64	70.89	5.15	0.28	0.587
	odd	0.00	0.08	24.14	70.26	5.28	0.24	0.587
C.B.(7)	even	0.00	0.08	23.56	70.53	5.43	0.40	0.587
	odd	0.00	0.06	25.19	68.85	5.62	0.28	0.587
C.B.(8)	even	0.00	0.08	24.30	70.55	4.79	0.28	0.556
	odd	0.00	0.10	24.73	69.64	5.21	0.32	0.556



表 3.4: チェビシェフビット系列および Kasami 系列の最大相関値の分布 (パーセント値) および最大値の中の最大値. (周期長 1023, ファミリーサイズ 31)

Kinds of Families		0.0~ 0.08	0.08~ 0.09	0.09~ 0.10	0.10~ 0.11	0.11~ 0.12	0.12~ 0.13	0.13~	Max of Maxima
C.B.(9)	even	0.00	1.81	21.37	44.36	20.77	8.67	3.02	0.152
	odd	0.20	1.41	21.37	39.92	22.99	9.88	4.23	0.155
C.B.(10)	even	0.00	2.22	25.40	41.53	20.77	6.85	3.23	0.146
	odd	0.20	2.42	22.38	38.51	25.40	7.46	3.63	0.144
C.B.(11)	even	0.00	2.42	24.59	36.49	23.39	9.68	3.43	0.150
	odd	0.00	2.82	20.56	41.13	23.79	7.06	4.64	0.155
C.B.(12)	even	0.00	1.81	23.19	41.13	22.18	7.66	4.03	0.144
	odd	0.00	1.82	22.58	39.92	22.38	10.48	2.82	0.161
Kasami	even	100.0	0.00	0.00	0.00	0.00	0.00	0.00	0.032
	odd	0.60	37.10	56.25	6.05	0.00	0.00	0.00	0.103

カオス 2 値系列は、ランダムな系列として設計しているが、もちろん、他にもランダムな系列を生成する方法が幾つかある。その中で、従来、擬似乱数として良く知られている線形合同系列および部分  $m$  系列を取り上げ、同様にして相関特性を調べる。

#### [線形合同法を用いる方法]

線形合同法による擬似乱数列  $\{x'_n\}_{n=0}^{\infty}$  ( $x'_0$ : 初期値) の生成法は、

$$x'_{n+1} = (a \cdot x'_n + d) \bmod M \quad (3.41)$$

$$x'_n \in [0, M-1]$$

で与えられる。これを正規化した系列

$$x_n = \frac{x'_n}{M-1} \quad (3.42)$$

$$x_n \in [0, 1]$$

を用いることにより、2 値系列  $\{\theta_c(x_n)\}_{n=0}^{\infty}$  (式 (3.19) 参照) が得られる。ただし、“良い” 乱数を生成するパラメータ  $a, d, M$  の組は限られている<sup>[34],[35]</sup>。ここでは、



$a = 65539, d = 0, M = 2^{31}$  を用いる.

[部分  $m$  系列を用いる方法]

十分長い  $m$  系列から，短い周期の系列を適当に切り取ることにより，多くの 2 値系列を得ることが出来る．ここでは，周期  $2^{20} - 1$  の  $m$  系列を生成する 3 項原始多項式

$$g(z) = z^{20} + z^3 + 1 \quad (3.43)$$

による 20 段シフトレジスタを用いる.

表 3.5 に、上記 2 つの方法により得られる 2 値系列の、幾つかのファミリーについての  
 相関特性を示す。ただし、表中の L.C. は線形合同系列を、T.M. は部分  $m$  系列を示す。



表 3.5: 線形合同系列および部分  $m$  系列の最大相関値の分布 (パーセント値) および最大値の中の最大値. (周期長 63, ファミリーサイズ=63)

Kinds of Families		0.0~ 0.1	0.1~ 0.2	0.2~ 0.3	0.3~ 0.4	0.4~ 0.5	0.5~ 0.6	0.6~	Max of Maxima
L.C.1 ( $c = 0.5$ )	even	0.00	0.00	23.46	70.93	5.36	0.25	0.00	0.556
	odd	0.00	0.05	21.63	72.27	5.70	0.35	0.00	0.556
L.C.2 ( $c = 0.5$ )	even	0.00	0.15	23.76	70.73	5.21	0.15	0.00	0.524
	odd	0.00	0.15	23.12	70.83	5.65	0.25	0.00	0.587
L.C.3 ( $c = 0.5$ )	even	0.00	0.05	25.55	69.39	4.81	0.15	0.05	0.619
	odd	0.00	0.20	24.50	70.49	4.66	0.15	0.00	0.556
L.C.4 ( $c = 0.5$ )	even	0.00	0.35	23.81	70.48	4.96	0.40	0.00	0.556
	odd	0.00	0.10	24.21	69.89	5.80	0.00	0.00	0.492
L.C.5 ( $c = 0.3$ )	even	0.00	0.00	5.31	57.24	30.41	6.35	0.69	0.746
	odd	0.00	0.00	6.15	70.29	20.29	2.92	0.35	0.683
L.C.6 ( $c = 0.6$ )	even	0.00	0.05	21.58	69.94	7.74	0.69	0.00	0.587
	odd	0.00	0.10	22.72	71.77	5.11	0.20	0.10	0.619
T.M.1	even	0.00	0.05	16.42	70.04	11.85	1.59	0.05	0.619
	odd	0.00	0.00	14.14	75.00	9.77	1.09	0.00	0.587
T.M.2	even	0.00	0.10	14.23	72.07	11.71	1.69	0.20	0.683
	odd	0.00	0.00	14.39	72.32	12.40	0.84	0.05	0.619
T.M.3	even	0.00	0.00	15.57	70.19	12.60	1.49	0.15	0.683
	odd	0.00	0.00	13.34	73.91	12.05	0.65	0.05	0.619
T.M.4	even	0.00	0.00	15.47	71.08	11.71	1.49	0.25	0.683
	odd	0.00	0.00	15.03	72.42	11.61	0.84	0.10	0.651

この表から、最大値の最大値に関して見た場合、部分  $m$  系列がチェビシェフビット系列より劣っていることがわかる。一方、線形合同法を用いた方法では、閾値  $c = 0.5$  の時が最も相関特性が良く、チェビシェフビット系列とほぼ変わらない特性を示している。しかしながら、先に述べたように、線形合同法を用いた場合、良い乱数を生成できるパラメータの組  $(a, d, M)$  は限られており、また、その周期が短いという点では、チェビシェフビット系列より劣っているといえる。



### 3.5 まとめ

本章では、非線形エルゴード写像より得られるカオスに基づいた、簡単な、2値系列の生成法を示した。まず、空間平均法による、それらの相関関数の理論的評価を与えた。次に、有限周期の場合のカオス系列の相関特性を数値実験により評価したところ、最大相関値に関して見た場合、従来の Gold 系列や Kasami 系列より劣ることがわかった。しかしながら、奇相関値に関しては、Gold 系列や Kasami 系列よりも大きい相関値の出現する確率は非常に小さい。さらに、カオス系列は以下のような利点を有する。

- 生成法が簡単であること。
- 周期長を任意に選べること。
- 初期値やビット番号、チェビシェフ写像の次数などパラメータを有し、多種類の符号が生成可能であること。
- ランダムな系列であるため、パラメータを鍵とすることにより、セキュリティが確保されること。

また、別のランダムな系列の生成法として、線形合同法や部分  $m$  系列を用いた方法との比較も行なった。部分  $m$  系列については、相関値が相対的に大きく、良好な相関特性を有する初期値の組合せは得られなかった。一方、線形合同法については、チェビシェフビット系列とほぼ同様の相関特性が得られたが、事前の理論的評価が容易でないこと、また、パラメータ数が少ないこと等が欠点として挙げられる。

従って、カオス系列は、CDMA のための拡散符号としての良い候補者であるといえる。



## 第4章

### チェビシェフ2値系列の相関関数の厳密評価

#### 4.1 はじめに

性質の良い擬似乱数は、計算機科学や通信などのさまざまな工学的応用分野において大量に必要とされている。特に、2値系列は、スペクトル拡散(SS)通信や暗号通信などのような、今日のデジタル通信システムにおいて重要な役割を担う。既に述べたように、そのような2値系列の中で、最も良く知られているのは、 $m$ 系列やKasami系列、Gold系列等のシフトレジスタ系列のクラスである。近年、全く異なった2値系列の生成法としてテント写像やロジスティック(logistic)写像、チェビシェフ(Chebyshev)写像<sup>[17]</sup>などのような、非線形エルゴード写像より生成されるカオスを利用しようとする試みが幾つか見られる。写像 $\tau$ にある初期値 $x$ を与えると、周期 $T$ の軌道 $\{\tau^n(x)\}_{n=0}^{T-1}$ を観測することが出来る。この軌道は、 $T$ 次元の確率変数 $\vec{x} = (x, \tau(x), \dots, \tau^{T-1}(x))$ と見なすことが出来る。すなわち、軌道 $\{\tau^n(x)\}_{n=0}^{T-1}$ は $T$ 次元空間の1点に写像される。従って、そのような確率変数の関数 $g(\vec{x})$ もまた、確率変数と見なされる。例えば、幾つかの初期値 $\{x, y, z, \dots\}$ に対する確率変数 $\{g(\vec{x}), g(\vec{y}), g(\vec{z}), \dots\}$ の算術平均は、そのような確率変数の典型的な統計量の一つである。よって、初期値の個数や、周期 $T$ が大きくなった時の、そのような統計量の漸近的振舞いを評価することは重要な課題である。良く知られているように、相関関数は最も重要な統計量の一つであり<sup>[18]</sup>、特に通信システムにおいて重要であることは、第2章で述べた通りである。実数値のカオス系列の相関関数については、広く研究がなされているが、カオス2値系列についてはほとんど議論がなされていない。前章において、カオス2値系列の生成法、およびチェビシェフ2進およびビット系列の相関関数の空間平均値の上限を与えたが、本章では、Perron-Frobenius作用素と呼ばれる積分作用素を用いて、その厳密な評価を行なう。特に、チェビシェフ写像を取り上げ、その統計的性質を議論する理由は、こ



れより得られる実数値系列について、通常の2次の相関特性だけでなく、高次の相関特性も良いことが知られているからである<sup>[25]</sup>。評価された自己および相互相関関数は、“時間平均法”によって得られた“経験値”と良く一致し、“空間平均法”の有用性が確かめられる。また、チェビシェフビット系列が良好な相関特性をもつことが示される。さらに、得られた相関関数の空間平均値を基に、SS通信において考慮されるべき偶および奇相関関数の理論的評価を行なう。

## 4.2 統計量の経験値

第3章で述べたように、一次元差分方程式  $x_{n+1} = \tau(x_n)$  から得られる軌道  $\{\tau^n(x)\}_{n=0}^{T-1}$  に対する、任意の  $L_1$  関数  $F(x)$  の時間平均  $F_T(x)$  および空間（アンサンブル）平均  $\langle F \rangle$  は、それぞれ

$$F_T(x) = \frac{1}{T} \sum_{n=0}^{T-1} F(\tau^n(x)) \quad (4.1)$$

$$\langle F \rangle = \int_I F(x) f^*(x) dx \quad (4.2)$$

で与えられる。ここで、注意すべきことは、有限の  $T$  に対する時間平均  $F_T(x)$  は、初期値  $x$  に依存した確率変数であるということである。カオス系列を実際に通信等に応用する際には、この  $F_T(x)$  の振舞いが問題となり、その統計的性質を議論することが重要となる。空間平均  $\langle F \rangle$  はあらゆる初期値に対する平均値と見なすことも出来るので、 $L$  個の初期値に対する  $F_T(x)$  の平均

$$\hat{F}_{T,L} = \frac{1}{L} \sum_{i=1}^L F_T(x_i) \quad (4.3)$$

は、 $T$  および  $L$  が十分大きい時、空間平均  $\langle F \rangle$  に近づく。そこで、この  $\hat{F}_{T,L}$  を“経験値”と呼ぶことにする。もちろん、この経験値は初期値の集合  $\{x_i\}_{i=1}^L$  に依存するが、 $T$  および  $L$  が十分大きい場合は、異なる初期値の集合から得られる経験値の間の差は非常に小さいので、その平均的な振舞いを評価すべきである。従って、確率変数  $F_T(x)$  の統計的性質を理解する上で、空間平均  $\langle F \rangle$  を評価することは重要となる。



### 4.3 Perron-Frobenius 作用素による相関関数の評価

式(3.10)で定義されたP-F作用素  $P_\tau$  は重要な性質

$$\int_I g(x) P_\tau h(x) dx = \int_I g(\tau(x)) h(x) dx \quad (4.4)$$

をもつので、後で示されるように相関関数の空間平均値の評価に非常に有効である。

$$C(x, \ell; x, x) = (x - \langle x \rangle)(\tau^\ell(x) - \langle x \rangle) \quad (4.5)$$

とすると、 $\langle C(\ell; x, x) \rangle$  は、通常の実数値系列の自己相関関数を表す。テント写像やロジスティック写像、およびチェビシェフ写像等の良く知られている幾つかの写像については、その自己相関関数  $\langle C(\ell; x, x) \rangle$  は既に評価されている<sup>[18]</sup>。しかしながら、一般の写像の解析的な不変密度を得ることは困難であるので、“ガレルキン (Galerkin) 法” に基づいた ACI 測度の近似アルゴリズムが提案されている<sup>[22],[23]</sup>。

一方、近年、実数値の擬似乱数生成器のランダム性の検定や<sup>[12]</sup>、SS 通信や暗号通信などの工学的応用のために、実数値のカオス軌道から2値系列を生成しようとする試みが幾つか見られる<sup>[27],[28]</sup>。既に第3章において、実数値系列を2値系列に変換する方法を与えた。その2値系列の相関関数の空間平均値についての厳密評価をP-F作用素を用いて行なう。

チェビシェフ2進系列  $\{\theta_c(\tau^n(x))\}_{n=0}^\infty$  と  $\{\theta_{c'}(\tau^n(x))\}_{n=0}^\infty$  との間の相関関数、およびチェビシェフビット系列  $\{b_i(\tau^n(x))\}_{n=0}^\infty$  と  $\{b_j(\tau^n(x))\}_{n=0}^\infty$  との間の相関関数は、それぞれ、

$$\langle C(\ell; \theta_c, \theta_{c'}) \rangle = \int_I (\theta_c(x) - \langle \theta_c \rangle)(\theta_{c'}(\tau^\ell(x)) - \langle \theta_{c'} \rangle) f^*(x) dx \quad (4.6)$$

$$\langle C(\ell; b_i, b_j) \rangle = \int_I (b_i(x) - \langle b_i \rangle)(b_j(\tau^\ell(x)) - \langle b_j \rangle) f^*(x) dx \quad (4.7)$$

で与えられる。ここで、 $P_\tau$  の性質 (式(4.4)) を用いると、

$$\langle C(\ell; \theta_c, \theta_{c'}) \rangle = \int_I P_\tau^\ell \{(\theta_c(x) - \langle \theta_c \rangle) f^*(x)\} (\theta_{c'}(x) - \langle \theta_{c'} \rangle) dx, \quad (4.8)$$

$$\langle C(\ell; b_i, b_j) \rangle = \int_I P_\tau^\ell \{(b_i(x) - \langle b_i \rangle) f^*(x)\} (b_j(x) - \langle b_j \rangle) dx \quad (4.9)$$

が得られる。

次に重要な定理を与える。

[定理]  $\tau'(c) \neq 0$  であるような  $c \in I$  に対して、

$$P_\tau \{(\theta_c(x) - \langle \theta_c \rangle) f^*(x)\} = \frac{1}{k} s(\tau'(c)) (\theta_{\tau(c)}(x) - \langle \theta_{\tau(c)} \rangle) f^*(x) \quad (4.10)$$



が成り立つ。ただし,

$$\langle \theta_c \rangle = \frac{1}{\pi} \cos^{-1} c \quad (4.11)$$

$$s(x) = \begin{cases} -1 & (x < 0) \\ 1 & (x \geq 0) \end{cases} \quad (4.12)$$

である.

[証明]  $\tau(x)$  の導関数は,

$$\tau'(x) = \frac{k}{\sqrt{1-x^2}} \sin(k \cos^{-1} x) \quad (4.13)$$

である. また, チェビシェフ写像  $\tau$  の下での  $x$  の  $m$  番目の逆像 (図 4.1 参照) は,

$$y_m(x) = \cos \left( \frac{m\pi + \cos^{-1}(-1)^m x}{k} \right) \quad 0 \leq m \leq k-1 \quad (4.14)$$

で与えられる. 式 (3.10) を用いると,

$$P_\tau \{(\theta_c(x) - \langle \theta_c \rangle) f^*(x)\} = \frac{1}{k} f^*(x) \sum_{m=0}^{k-1} (\theta_c(y_m(x)) - \langle \theta_c \rangle) \quad (4.15)$$

が得られるので,  $\sum \theta_c(y_m(x))$ , すなわち, 領域  $y \geq c$  における  $y_m$  の個数を考えなければならない. その個数が  $x = \tau(c)$  を境界に変化することは容易にわかる. ここで,  $N$  を  $y_N(\tau(c)) = c$  を満足する整数とすると,  $N$  は式 (4.14) に  $x = \tau(c)$  を代入することによって,

$$N = \frac{k}{\pi} \cos^{-1} c - \frac{1}{\pi} \cos^{-1}((-1)^N \tau(c)) \quad (4.16)$$

のように得られる.

(i)  $\tau'(c) > 0$  を満たすような  $c$  に対して,  $N$  が偶数になることは, 図 4.1 から明らかである. この場合, 式 (4.16) は

$$N = \frac{k}{\pi} \cos^{-1} c - \frac{1}{\pi} \cos^{-1} \tau(c) \quad (4.17)$$

となる. 図 4.2(a) から,

$$\sum_m \theta_c(y_m(x)) = N + \theta_{\tau(c)}(x) \quad (4.18)$$

が得られ, さらに, 式 (4.11) および式 (4.17) を用いると,

$$\sum_m \theta_c(y_m(x)) = k \langle \theta_c \rangle - \langle \theta_{\tau(c)} \rangle + \theta_{\tau(c)}(x) \quad (4.19)$$



と表される。従って,

$$\sum_m (\theta_c(y_m(x)) - \langle \theta_c \rangle) = \theta_{\tau(c)}(x) - \langle \theta_{\tau(c)} \rangle \quad (4.20)$$

となる。

(ii)  $\tau'(c) < 0$  を満たすような  $c$  に対しては, 図 4.1 から  $N$  は偶数となる。この場合, 式 (4.16) は

$$N = \frac{k}{\pi} \cos^{-1} c - \frac{1}{\pi} (\pi - \cos^{-1} \tau(c)) \quad (4.21)$$

となり, また, 図 4.2(b) から (i) と同様にして

$$\sum_m \theta_c(y_m(x)) = N + 1 - \theta_{\tau(c)}(x) \quad (4.22)$$

$$= k \langle \theta_c \rangle + \langle \theta_{\tau(c)} \rangle - \theta_{\tau(c)}(x) \quad (4.23)$$

が得られる。よって,

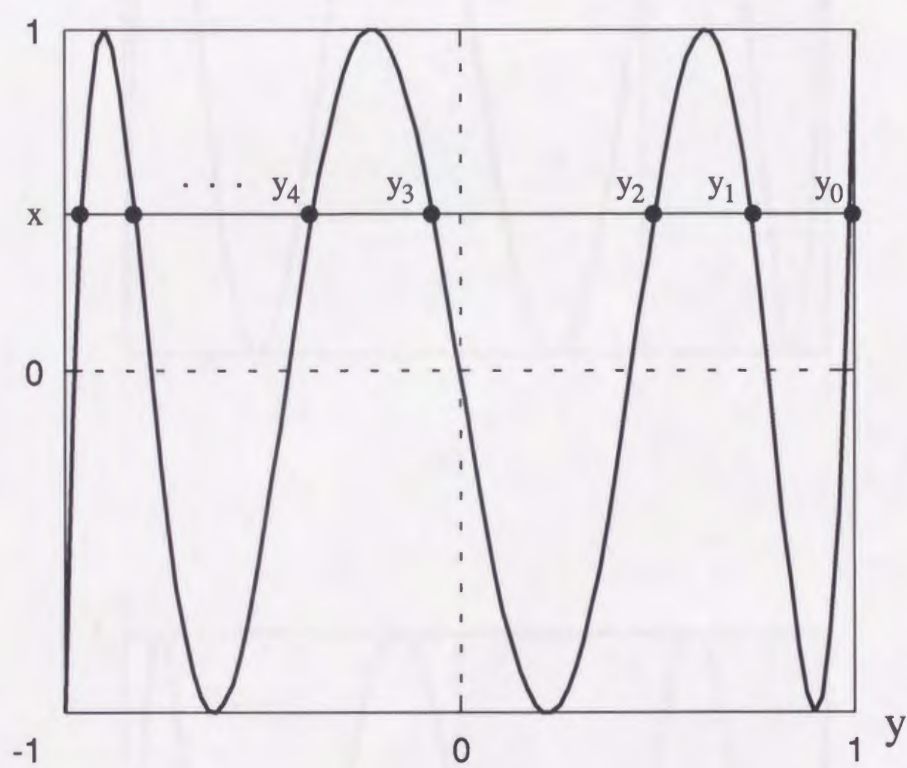
$$\sum_m (\theta_c(y_m(x)) - \langle \theta_c \rangle) = -\theta_{\tau(c)}(x) + \langle \theta_{\tau(c)} \rangle \quad (4.24)$$

となる。

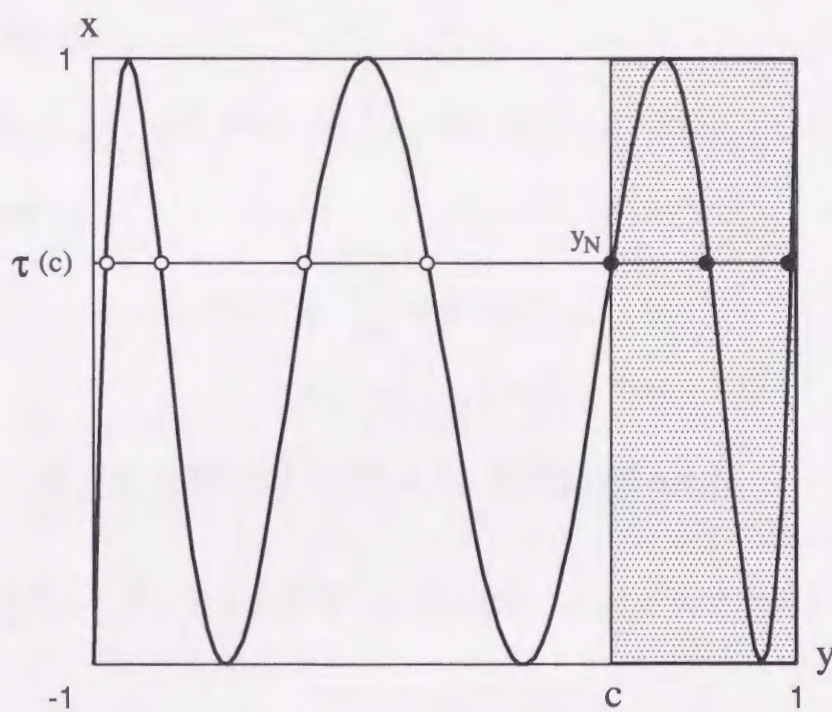
ゆえに (i) および (ii) から, 式 (4.10) を得る。(証明終)

**[Remark 1]**  $P_\tau\{(\theta_c(x) - \langle \theta_c \rangle)f^*(x)\}$  の評価は, 領域  $y \geq c$  における逆像  $y_m(x)$  の個数の数え上げの問題に帰着する。

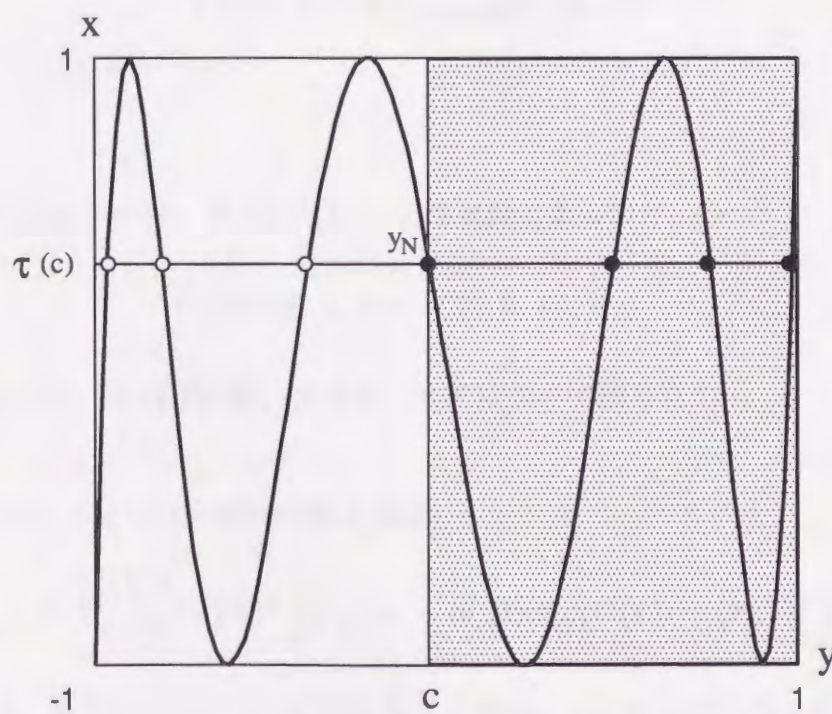


図 4.1: チェビシェフ写像における  $x$  の逆像





(a)



(b)

図 4.2: (a)  $\tau'(c) > 0$  の場合, (b)  $\tau'(c) < 0$  の場合.



従って、定理より、

$$P_{\tau}^{\ell}\{(\theta_c(x) - \langle \theta_c \rangle)f^*(x)\} = \frac{1}{k^{\ell}} s((\tau^{\ell})'(c))(\theta_{\tau^{\ell}(c)}(x) - \langle \theta_{\tau^{\ell}(c)} \rangle)f^*(x) \quad (4.25)$$

が得られる。ただし、

$$(\tau^{\ell})'(x) = \frac{d}{dx} \cos(k^{\ell} \cos^{-1} x) \quad (4.26)$$

$$= \frac{k^{\ell}}{\sqrt{1-x^2}} \sin(k^{\ell} \cos^{-1} x) \quad (4.27)$$

である。これを、式(4.8)に適用することにより、次の系が得られる。

[系1] 次数  $k$  のチェビシェフ2進系列の相関関数は、 $\tau'(c) \neq 0$  であるような  $c \in I$  に対して、

$$\langle C(\ell; \theta_c, \theta_{c'}) \rangle = \frac{1}{k^{\ell}} s((\tau^{\ell})'(c)) \langle C(0; \theta_{\tau^{\ell}(c)}, \theta_{c'}) \rangle \quad (4.28)$$

のように評価される。ここで、 $a, b \in I$  に対して、

$$\langle C(0; \theta_a, \theta_b) \rangle = \langle \theta_{\max[a,b]} \rangle - \langle \theta_a \rangle \langle \theta_b \rangle \quad (4.29)$$

である。

[Remark 2]  $\tau'(c) = 0$  の時、 $P_{\tau}\{\theta_c(x)f^*(x)\}$  は定数となるので、

$$\langle C(\ell; \theta_c, \theta_{c'}) \rangle = \langle C(0; \theta_c, \theta_{c'}) \rangle \delta_{\ell,0} \quad (4.30)$$

が得られる。よって、式(4.28)は、任意の  $c \in I$  について成り立つ。

次に、チェビシェフビット系列の相関関数

$$\langle C(\ell; b_i, b_j) \rangle = \sum_{r=1}^{2^i-1} \sum_{s=1}^{2^j-1} (-1)^{r+s} \int_I (\hat{\theta}_{\frac{r}{2^i}}(x) - \langle \hat{\theta}_{\frac{r}{2^i}} \rangle) (\hat{\theta}_{\frac{s}{2^j}}(\tau^{\ell}(x)) - \langle \hat{\theta}_{\frac{s}{2^j}} \rangle) f^*(x) dx \quad (4.31)$$

について考える。区間が  $I = [-1, 1]$  であることから、 $c \geq 0$  に対して、 $\hat{\theta}_c(x)$  および  $\langle \hat{\theta}_c \rangle$  は、それぞれ、

$$\hat{\theta}_c(x) = \theta_c(x) + 1 - \theta_{-c}(x), \quad (4.32)$$

$$\langle \hat{\theta}_c \rangle = \langle \theta_c \rangle + 1 - \langle \theta_{-c} \rangle \quad (4.33)$$



と表せる。従って、式(4.31)は、

$$\begin{aligned} \langle C(\ell; b_i, b_j) \rangle &= \sum_{r=1}^{2^i-1} \sum_{s=1}^{2^j-1} (-1)^{r+s} \{ \langle C(\ell; \theta_{\frac{r}{2^i}}, \theta_{\frac{s}{2^j}}) \rangle - \langle C(\ell; \theta_{\frac{r}{2^i}}, \theta_{-\frac{s}{2^j}}) \rangle \\ &\quad - \langle C(\ell; \theta_{-\frac{r}{2^i}}, \theta_{\frac{s}{2^j}}) \rangle + \langle C(\ell; \theta_{-\frac{r}{2^i}}, \theta_{-\frac{s}{2^j}}) \rangle \} \end{aligned} \quad (4.34)$$

と書き直すことが出来る。従って、次の系を得る。

[系2] 次数  $k$  のチェビシェフビット系列の相関関数は、

$$\begin{aligned} \langle C(\ell; b_i, b_j) \rangle &= \frac{1}{k^\ell} \sum_{r=1}^{2^i-1} \sum_{s=1}^{2^j-1} (-1)^{r+s} \\ &\quad \cdot \left\{ s((\tau^\ell)'(\frac{r}{2^i})) (\langle C(0; \theta_{\tau^\ell(\frac{r}{2^i})}, \theta_{\frac{s}{2^j}}) \rangle - \langle C(0; \theta_{\tau^\ell(\frac{r}{2^i})}, \theta_{-\frac{s}{2^j}}) \rangle) \right. \\ &\quad \left. - s((\tau^\ell)'(-\frac{r}{2^i})) (\langle C(0; \theta_{\tau^\ell(-\frac{r}{2^i})}, \theta_{\frac{s}{2^j}}) \rangle - \langle C(0; \theta_{\tau^\ell(-\frac{r}{2^i})}, \theta_{-\frac{s}{2^j}}) \rangle) \right\} \end{aligned} \quad (4.35)$$

のように評価される。

以上、チェビシェフ写像より得られる2値系列の相関関数の空間平均値を P-F 作用素に基づいて評価したが、他の写像についても同様な評価が可能であることを付記しておく。

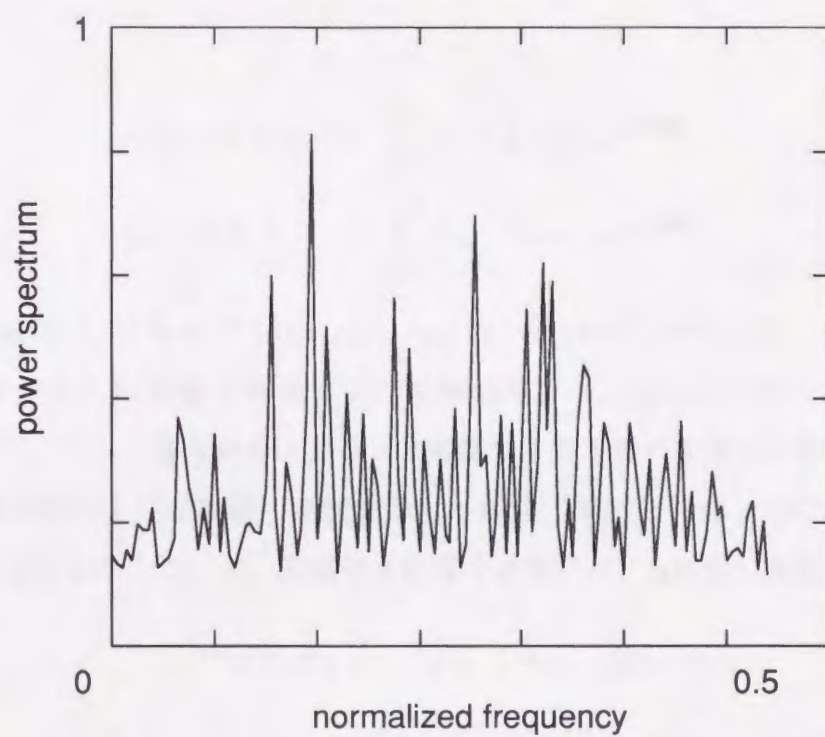
#### 4.3.1 数値例

本節では、チェビシェフビット系列の相関関数について、幾つか数値例を示す。まず、

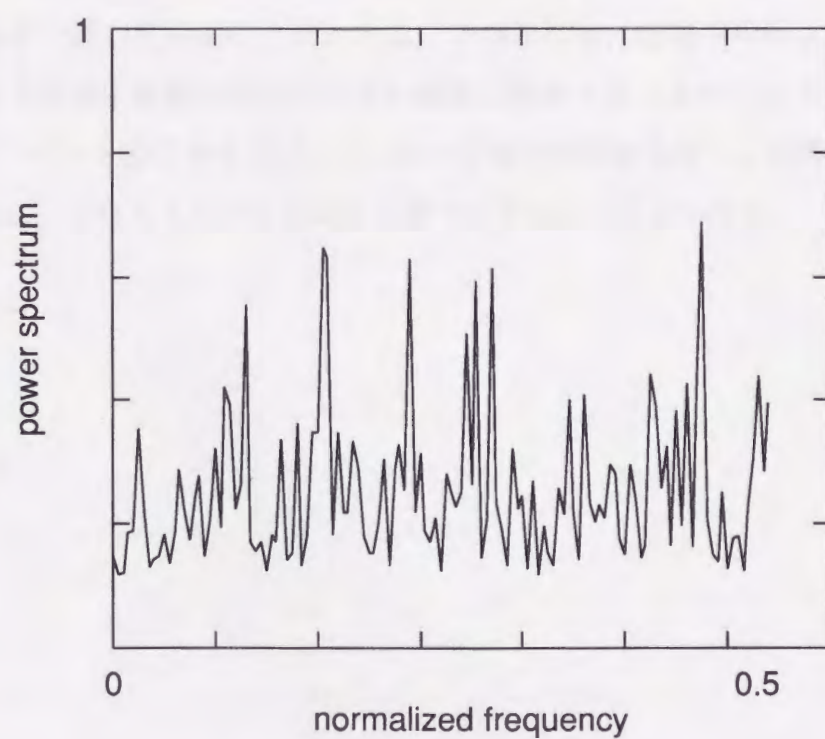
$$S_T(x, m; b_i, b_i) = \sum_{\ell=0}^{T-1} C_T(x, \ell; b_i, b_i) e^{-j \frac{2\pi \ell m}{T}} \quad (4.36)$$

とおく。すると、 $|S_T(x, m; b_i, b_i)|$  は第  $i$  ビットのチェビシェフビット系列のパワースペクトルを表す。図 4.3 は、ある初期値  $x$  から得られる周期  $T = 256$  の系列のパワースペクトルの例を示したものである。 $S_T(x, m; b_i, b_i)$  (あるいは  $C_T(x, m; b_i, b_i)$ ) は確率変数であるので、かなり大きく揺らいでいる。従って、そのようなカオスの振舞いの統計的性質を調べるためには“空間平均法”を用いるのが有効である。





(a)



(b)

図 4.3: チェビシェフビット系列のパワースペクトル  $|S_T(x, m; b_i, b_i)|$  ( $k = 2, T = 256, i = 2$ ).(a)  $x = 0.3$ , (b)  $x = 0.7$ .



次に,

$$\langle S(m, b_i, b_j) \rangle = \sum_{\ell=0}^{T-1} \langle C(\ell; b_i, b_j) \rangle e^{-j \frac{2\pi \ell m}{T}} \quad (4.37)$$

$$\hat{S}_{T,L}(m, b_i, b_j) = \sum_{\ell=0}^{T-1} \hat{C}_{T,L}(\ell; b_i, b_j) e^{-j \frac{2\pi \ell m}{T}} \quad (4.38)$$

とおくと,  $|\langle S(m, b_i, b_j) \rangle|$  および  $|\hat{S}_{T,L}(m, b_i, b_j)|$  は, それぞれパワースペクトル (あるいはクロススペクトル) の空間平均値および経験値を示す. 図 4.4 には,  $T = 256$  および  $L = 300$  に対して, ビット番号やチェビシェフ写像の次数を幾つか変えた時の, パワースペクトルの空間平均値および経験値の比較を示してある. 同様に, 図 4.5 にはクロススペクトルの場合の結果を示す. ここで, 経験値を計算する際には, 300 個の初期値  $\{x^{(r)}\}_{r=1}^{300}$  は

$$x^{(r)} = 0.003 \times r, \quad r = 1, 2, \dots, 300 \quad (4.39)$$

のように選んだ. もちろん, これらの初期値は任意に選んでも良い. 経験値は, 初期値の集合  $\{x^{(r)}\}_{r=1}^{300}$  に依存し, ある程度の揺らぎをもつ. 前述したように, その揺らぎは比較的小さく, むしろ, 経験値の平均的振舞いが重要である. 図 4.4 および図 4.5 から, 空間平均値と経験値が良く一致していることがわかる. このことは, 空間平均法により, ここで取り扱っているような確率変数の統計的性質を厳密に評価することが可能であることを示している. さらに, ビット番号およびチェビシェフ写像の次数を大きくした時に, パワースペクトルは一定値に, クロススペクトルは 0 に近づいていることがわかる.



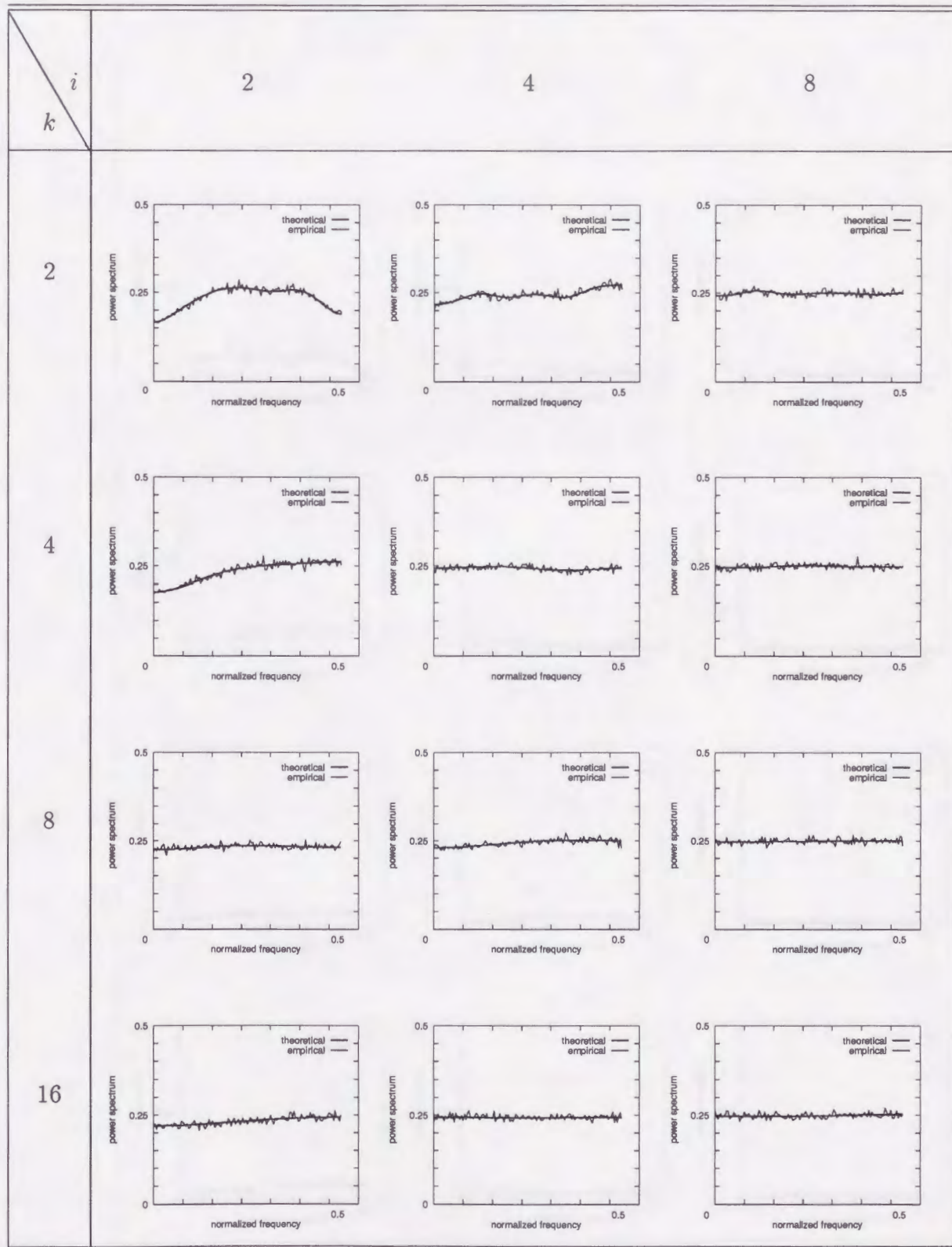


図 4.4: チェビシェフビット系列のパワースペクトルの空間平均値  $|\langle S(m, b_i, b_i) \rangle|$  および経験値  $|\hat{S}_{T,L}(m, b_i, b_i)|$ . ( $T = 256, L = 300$ )



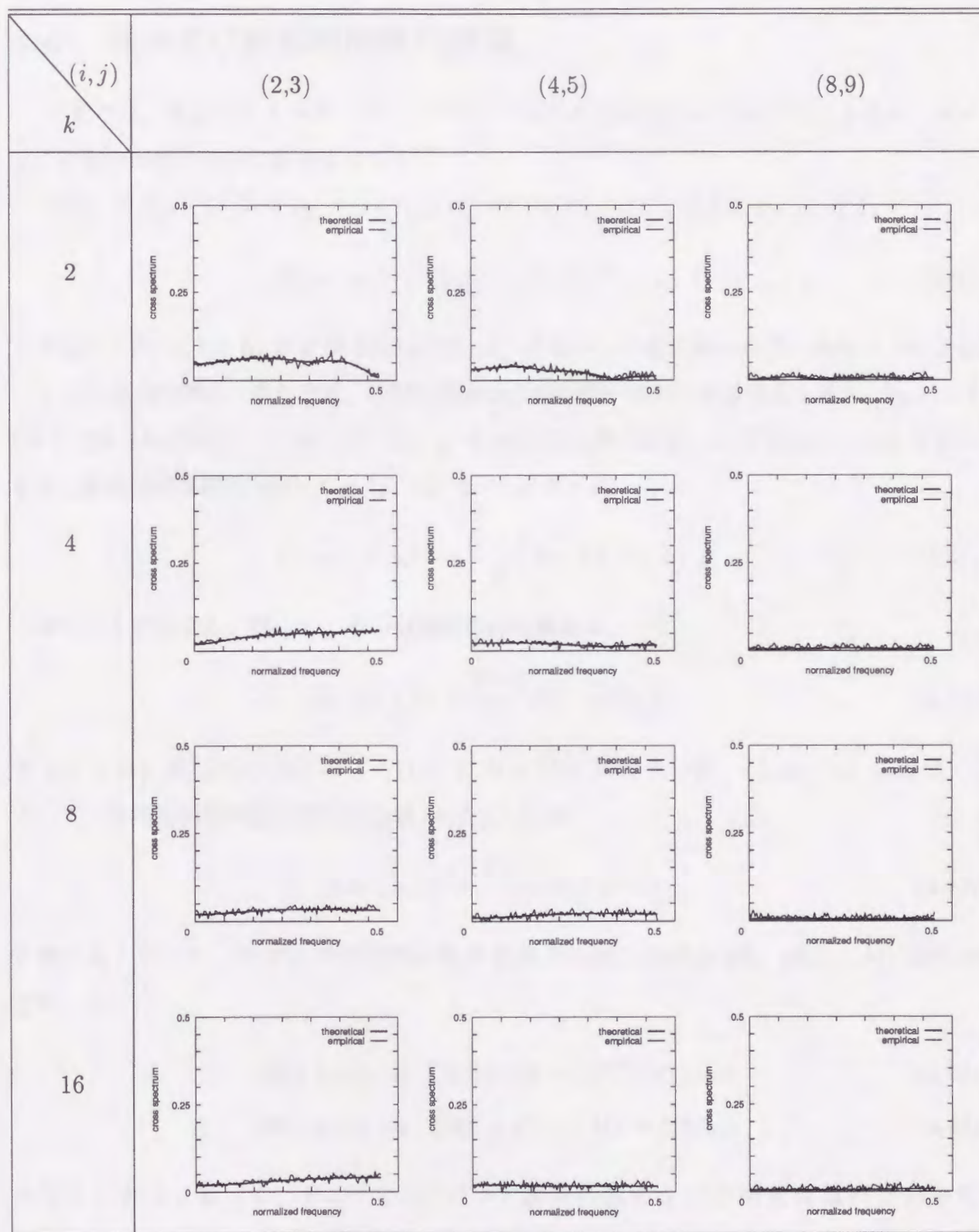


図 4.5: チェビシェフビット系列のクロススペクトルの空間平均値  $|\langle S(m, b_i, b_j) \rangle|$  および経験値  $|\hat{S}_{T,L}(m, b_i, b_j)|$ . ( $T = 256, L = 300$ )



#### 4.4 偶および奇相関関数の評価

本節では、前節で与えたチェビシェフビット系列の相関関数の空間平均値を基に、偶および奇相関関数の理論的評価を行なう。

まず、2値  $(0, 1)$  系列  $\{g(\tau^n(x))\}_{n=0}^{\infty}$  および  $\{h(\tau^n(x))\}_{n=0}^{\infty}$  を考える。ここで、

$$B(x, \ell; g, h) = (2g(x) - 1)(2h(\tau^\ell(x)) - 1) \quad (4.40)$$

とおくと、 $B_T(x, \ell; g, h)$  および  $\langle B(\ell; g, h) \rangle$  は、ある一つの初期値から得られる2つの2値  $(-1, +1)$  系列の間の、それぞれ、時間平均形および空間平均形の相関関数を表す。 $2g(x) - 1$  (あるいは  $2h(\tau^\ell(x)) - 1$ ) は、 $\{0, 1\} \rightarrow \{-1, +1\}$  の変換を表す。この  $B_T(x, \ell; g, h)$  を用いると、非周期相関関数  $A_T(x, \ell; g, h)$  (式(3.38)参照) は、

$$A_T(x, \ell; g, h) = \frac{T - \ell}{T} B_{T-\ell}(x, \ell; g, h) \quad (4.41)$$

と表すことが出来る。従って、その相関関数の経験値は、

$$\hat{A}_{T,L}(\ell; g, h) = \frac{T - \ell}{T} \hat{B}_{T-\ell,L}(\ell; g, h) \quad (4.42)$$

で与えられ、 $\hat{B}_{T-\ell,L}(\ell; g, h)$  は、やはり  $T$  および  $L$  が大きい時、 $\langle C(\ell; g, h) \rangle$  に近づく。よって、非周期相関関数の空間平均値  $\langle A(\ell; g, h) \rangle$  は、

$$\langle A(\ell; g, h) \rangle = \frac{T - \ell}{T} \langle B(\ell; g, h) \rangle \quad (4.43)$$

と書ける。従って、偶および奇相関関数の空間平均値、 $\langle R(\ell; g, h) \rangle$ 、 $\langle \Theta(\ell; g, h) \rangle$  はそれぞれ、

$$\langle R(\ell; g, h) \rangle = \langle A(\ell; g, h) \rangle + \langle A(T - \ell; h, g) \rangle \quad (4.44)$$

$$\langle \Theta(\ell; g, h) \rangle = \langle A(\ell; g, h) \rangle - \langle A(T - \ell; h, g) \rangle \quad (4.45)$$

で与えられる。従って、チェビシェフビット系列の偶および奇相関関数の空間平均値  $\langle R(\ell; b_i, b_j) \rangle$ 、 $\langle \Theta(\ell; b_i, b_j) \rangle$  は、 $\langle B(\ell; b_i, b_j) \rangle$  を評価することにより得ることが出来る。 $\langle B(\ell; b_i, b_j) \rangle$  は、4.3節において評価された  $\langle C(\ell; b_i, b_j) \rangle$  を用いると、

$$\langle B(\ell; b_i, b_j) \rangle = 4\langle C(\ell; b_i, b_j) \rangle + (2\langle b_i \rangle - 1)(2\langle b_j \rangle - 1) \quad (4.46)$$

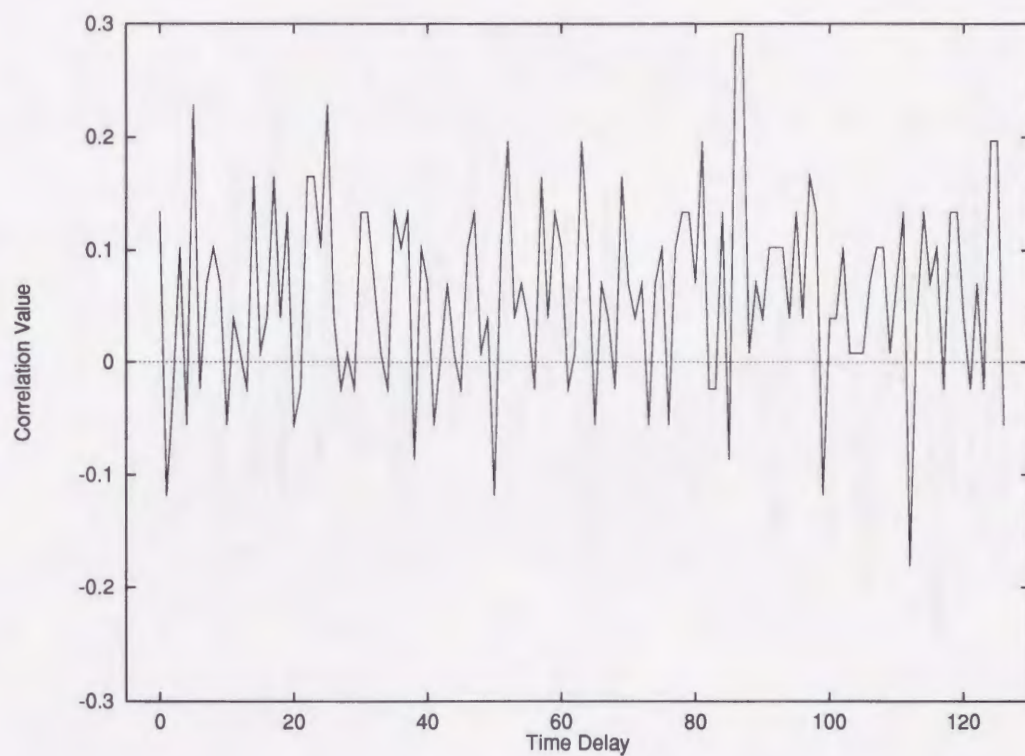
と表されるので、 $\langle R(\ell; b_i, b_j) \rangle$  および  $\langle \Theta(\ell; b_i, b_j) \rangle$  の陽な評価式を得ることが出来る。



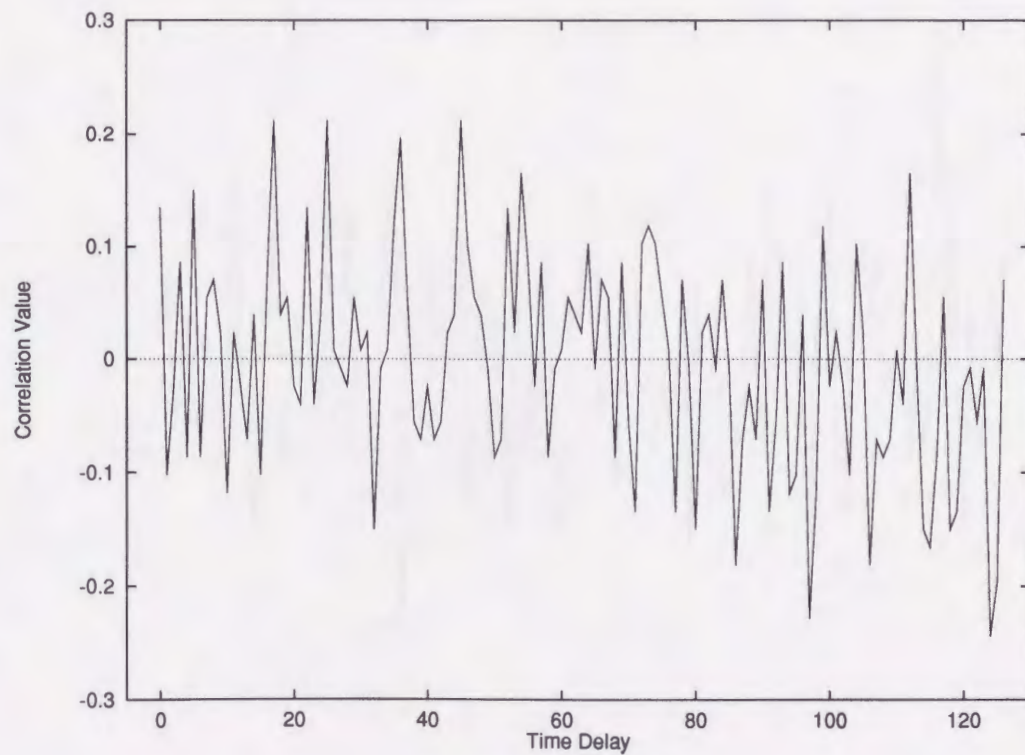
#### 4.4.1 数値例

次に、チェビシェフビット系列の偶および奇相関関数の数値例を示す。まず、図 4.6 および図 4.7 には、ある一つの初期値から得られた系列間の偶相関関数  $R_T(x, \ell; b_i, b_j)$  および  $\Theta_T(x, \ell; b_i, b_j)$  を示す。ここで、 $T = 127$  である。ビット番号およびチェビシェフ写像の次数は図中に示す。これらは、確率変数であるため、かなり揺らいでいることがわかる。





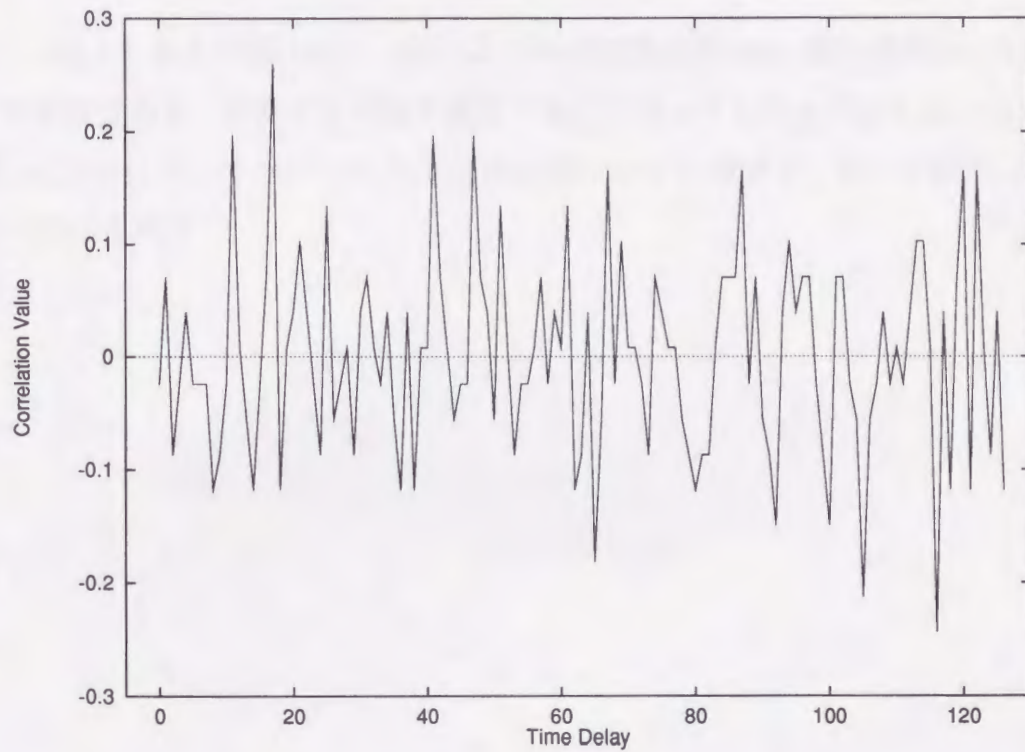
(a) 偶相関関数



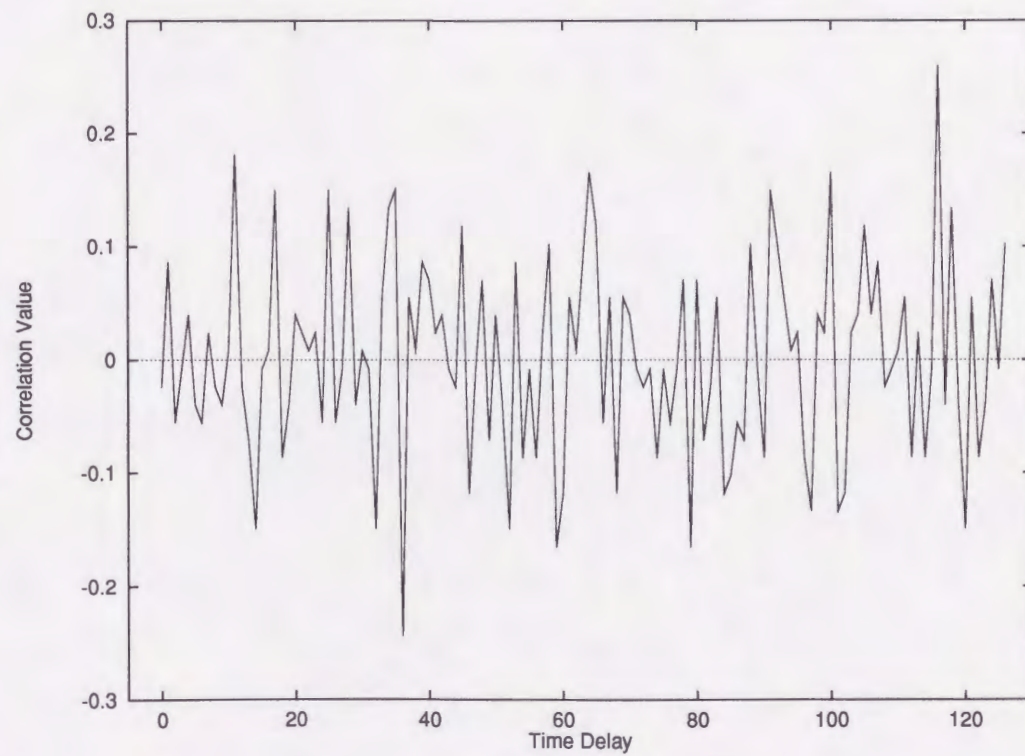
(b) 奇相関関数

図 4.6: ある一つの初期値  $x$  より得られた系列間の相関関数. (a)  $R_T(x, \ell; b_2, b_3)$ , (b)  $\Theta_T(x, \ell; b_2, b_3)$ . ( $k = 2$ )





(a) 偶相関関数



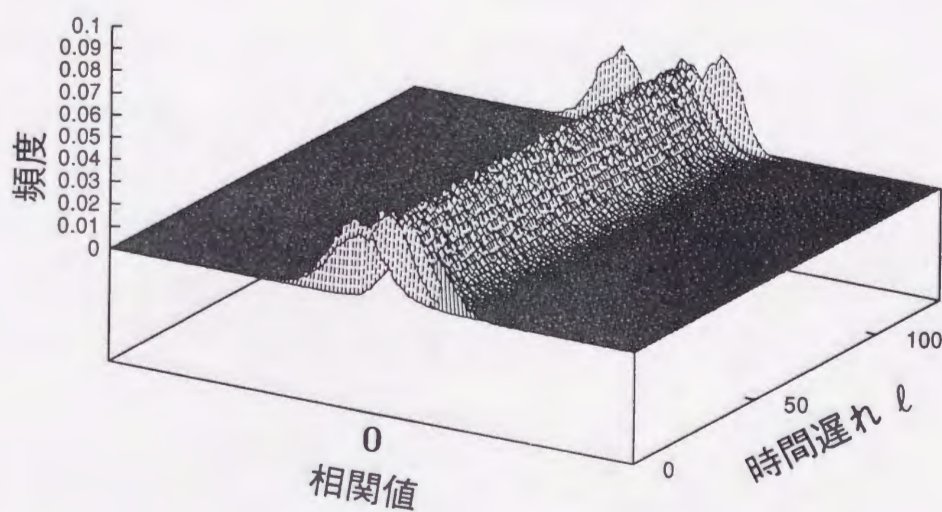
(b) 奇相関関数

図 4.7: ある一つの初期値  $x$  より得られた系列間の相関関数. (a)  $R_T(x, \ell; b_8, b_9)$ , (b)  $\Theta_T(x, \ell; b_8, b_9)$ . ( $k = 16$ )

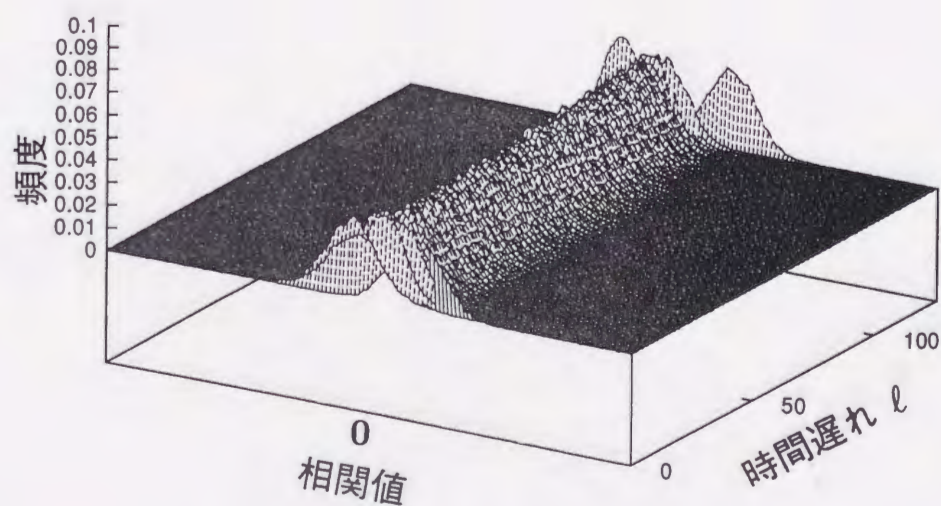


次に、図 4.8 および図 4.9 に、偶および奇相関関数を 8001 個の初期値に対して計算し、その頻度分布を、それぞれの時間遅れ  $l$  毎にプロットしたものである。図 4.8 はビット番号  $(i, j) = (2, 3)$ 、チェビシェフ写像の次数  $k = 2$  の場合を、図 4.9 は  $(i, j) = (8, 9)$ 、 $k = 16$  の場合を示す。





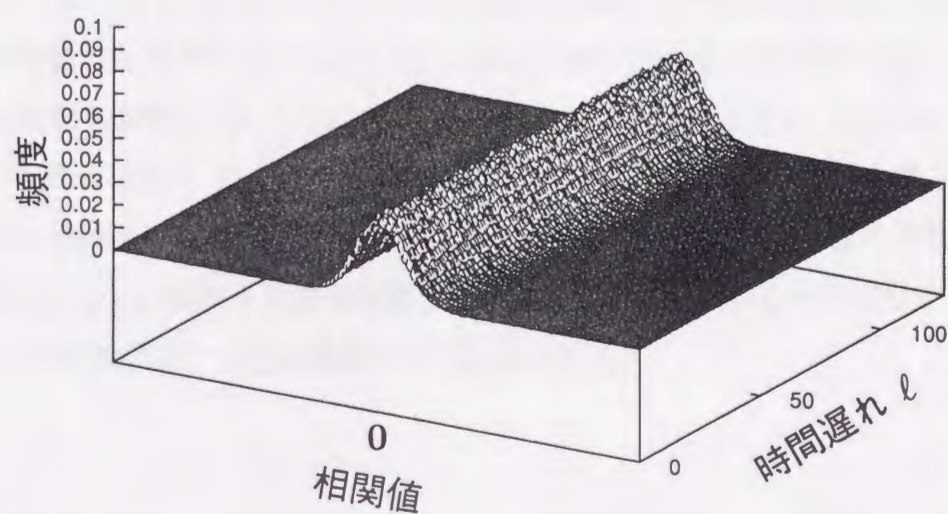
(a) 偶相関関数



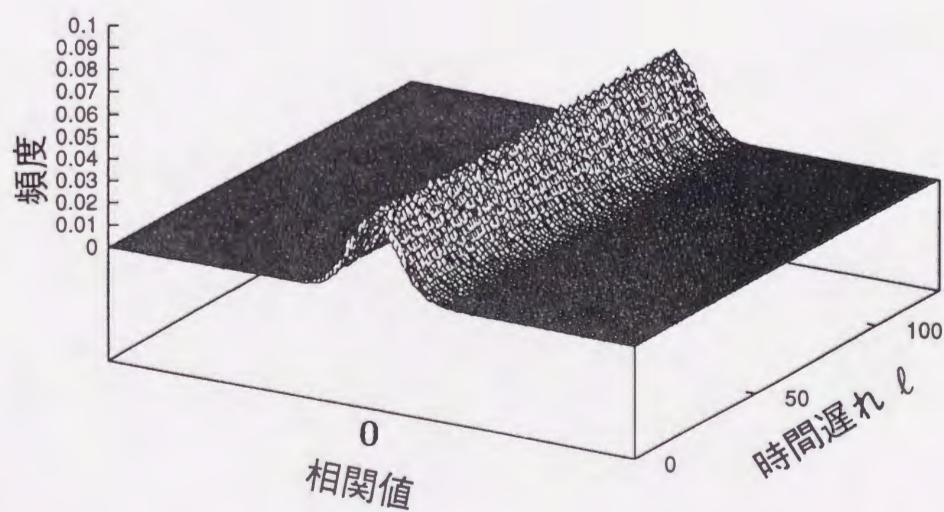
(b) 奇相関関数

図 4.8: チェビシェフビット系列の相関値の分布  $((i, j) = (2, 3), k = 2)$





(a) 偶相関関数



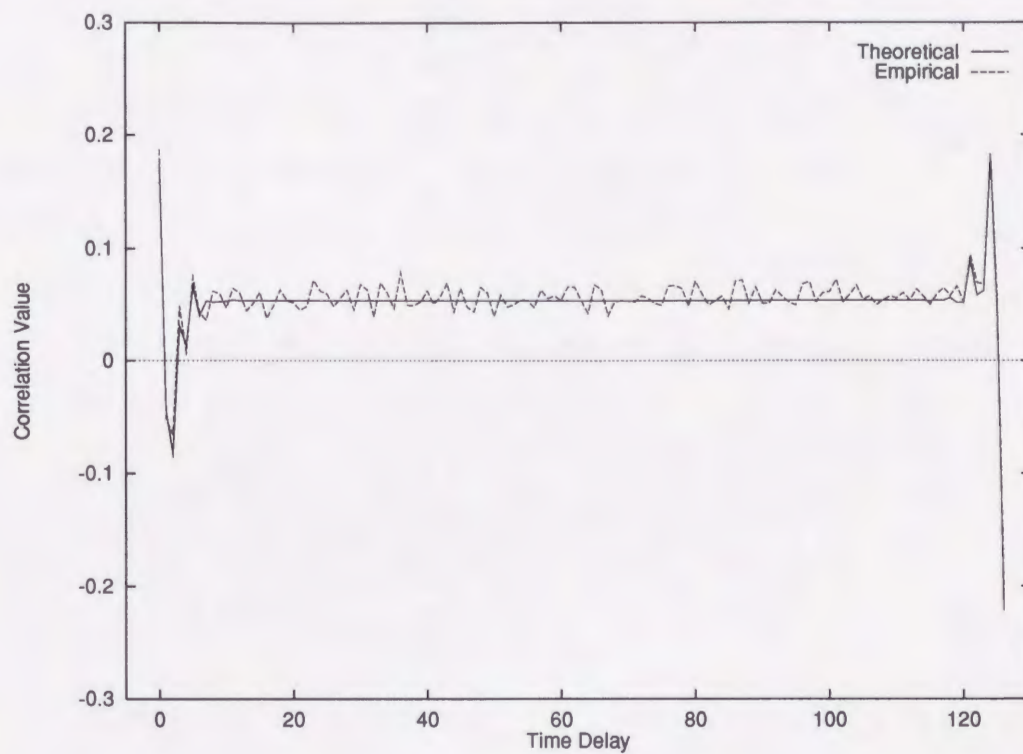
(b) 奇相関関数

図 4.9: チェビシェフビット系列の相関値の分布 ( $(i, j) = (8, 9), k = 16$ )

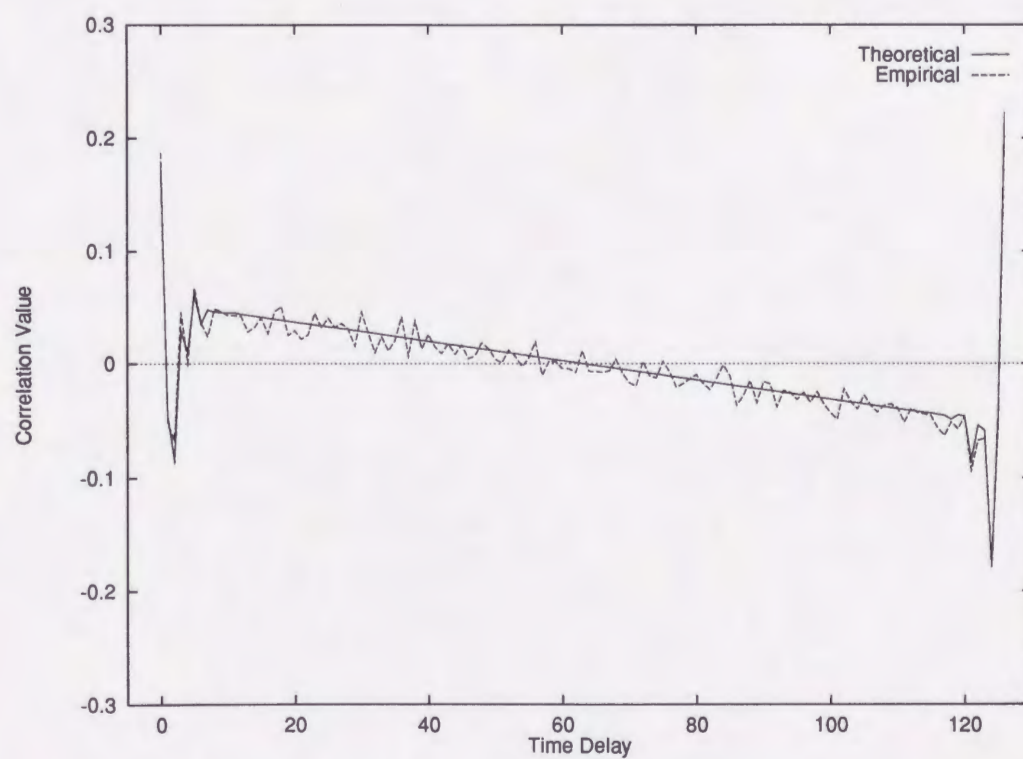


これらの図からわかるように、チェビシェフビット系列の相関値の頻度分布は、ほぼガウス分布を形成していることがわかる。ここでは、その平均値（すなわち“経験値”）が本節で与えた空間平均値で評価されることを示す。（なお、分散については、次章で議論する。）そこで、図 4.10 および 図 4.11 に、偶相関関数の空間平均値  $\langle R(\ell; b_i, b_j) \rangle$ （あるいは奇相関関数の空間平均値  $\langle \Theta(\ell; b_i, b_j) \rangle$ ）および偶相関関数の経験値  $\hat{R}_{T,L}(\ell; b_i, b_j)$ （あるいは奇相関関数経験値  $\hat{\Theta}_{T,L}(\ell; b_i, b_j)$ ）を示す。ここで、 $T = 127$ 、 $L = 100$  である。チェビシェフ写像の次数  $k$  およびビット番号は図中に示してある。これらの図より、やはり空間平均値と経験値が良く一致していること、また、チェビシェフ写像の次数およびビット番号が大きい時に、偶および奇相関値とも小さい値をとっていることがわかる。このことは、 $\ell = 0$  の時を除けば、自己相関関数でも同様である。





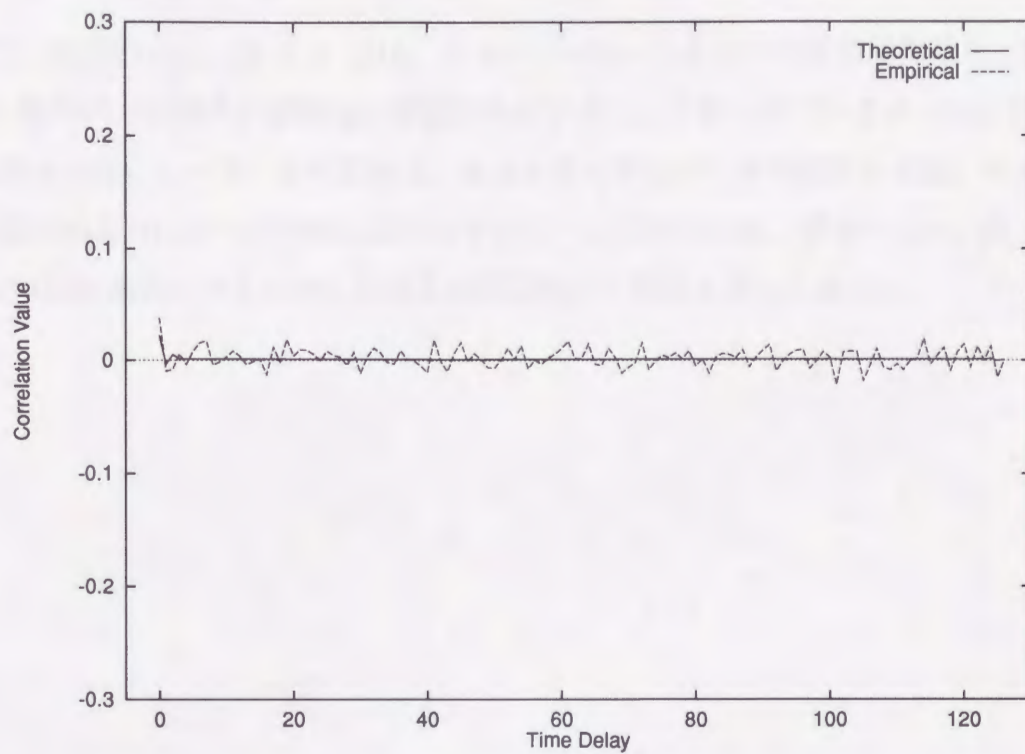
(a) 偶相関関数



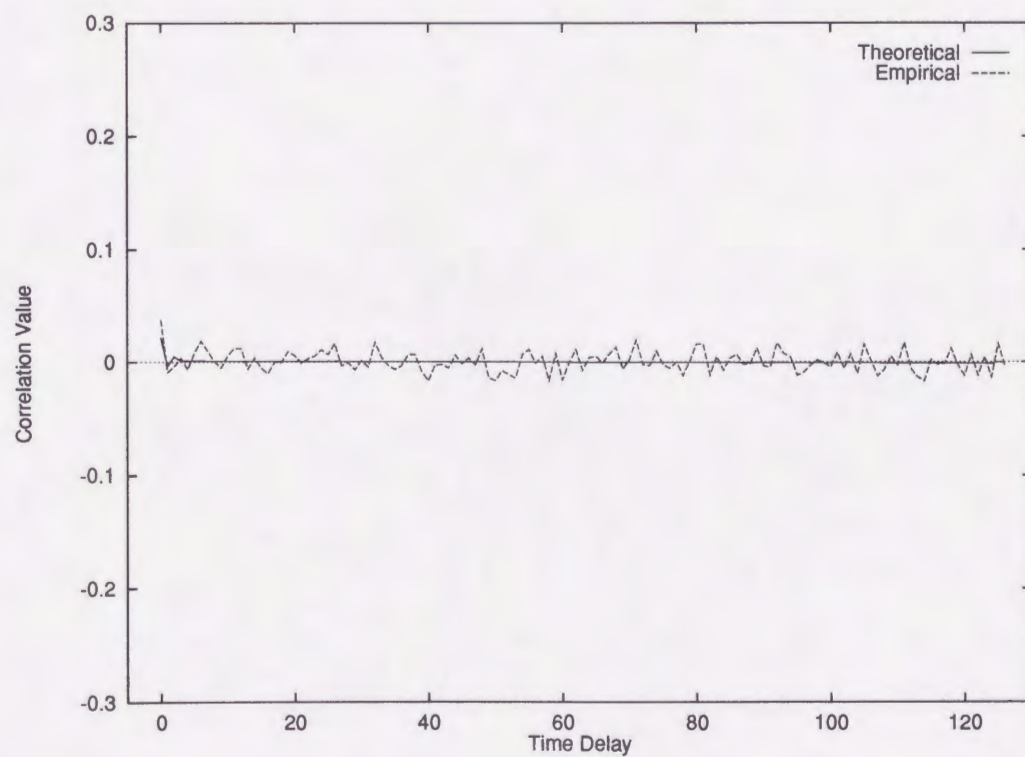
(b) 奇相関関数

図 4.10: (a)  $\langle R(\ell; b_2, b_3) \rangle$  および  $\hat{R}_{T,L}(\ell; b_2, b_3)$ , (b)  $\langle \Theta(\ell; b_2, b_3) \rangle$  および  $\hat{\Theta}_{T,L}(\ell; b_2, b_3)$ . ( $k = 2$ ,  $L = 100$ )





(a) 偶相関関数



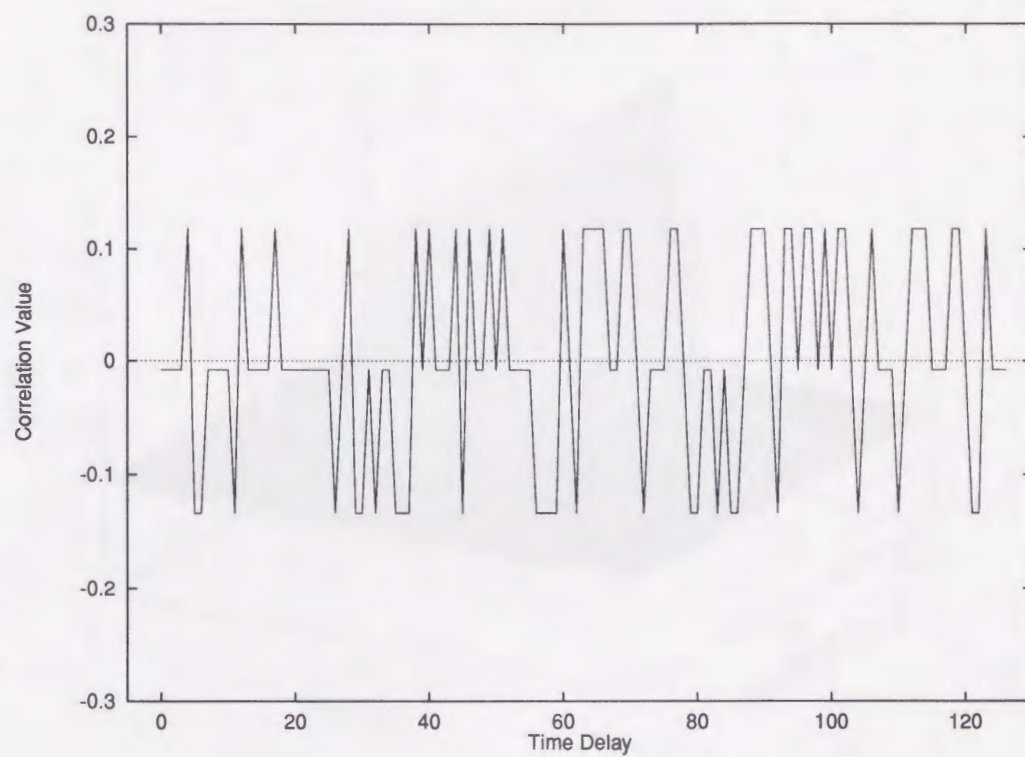
(b) 奇相関関数

図 4.11: (a)  $\langle R(\ell; b_8, b_9) \rangle$  および  $\hat{R}_{T,L}(\ell; b_8, b_9)$ , (b)  $\langle \Theta(\ell; b_8, b_9) \rangle$  および  $\hat{\Theta}_{T,L}(\ell; b_8, b_9)$ . ( $k = 16$ ,  $L = 100$ )

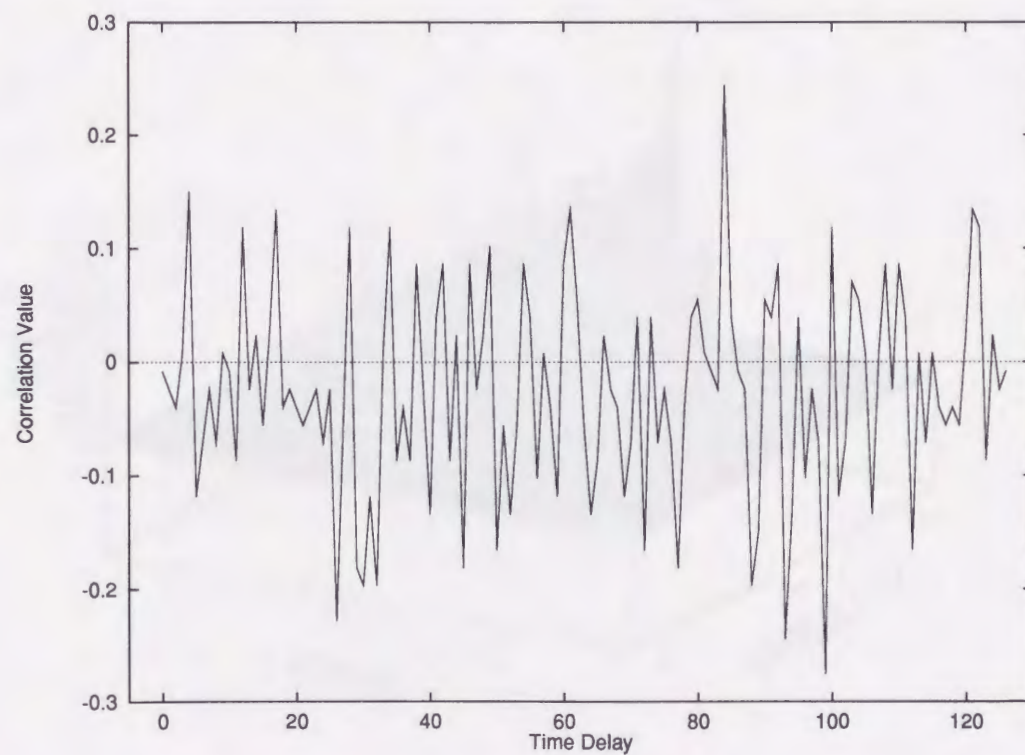


また、比較のため、図 4.12 には、あるペアの Gold 系列の相互相関関数を、図 4.13 には 8001 組のペアに対する相関値の頻度分布を示す。よく知られているように、偶相関値は 3 値しかとらない。一方、奇相関値は、多値を取り得るが、その頻度分布は、チェビシェフビット系列のようにガウス分布にはなっていないことがわかる。参考のため、図 4.14 には、100 組の Gold 系列のペアに対する相互相関関数の平均値を示しておく。





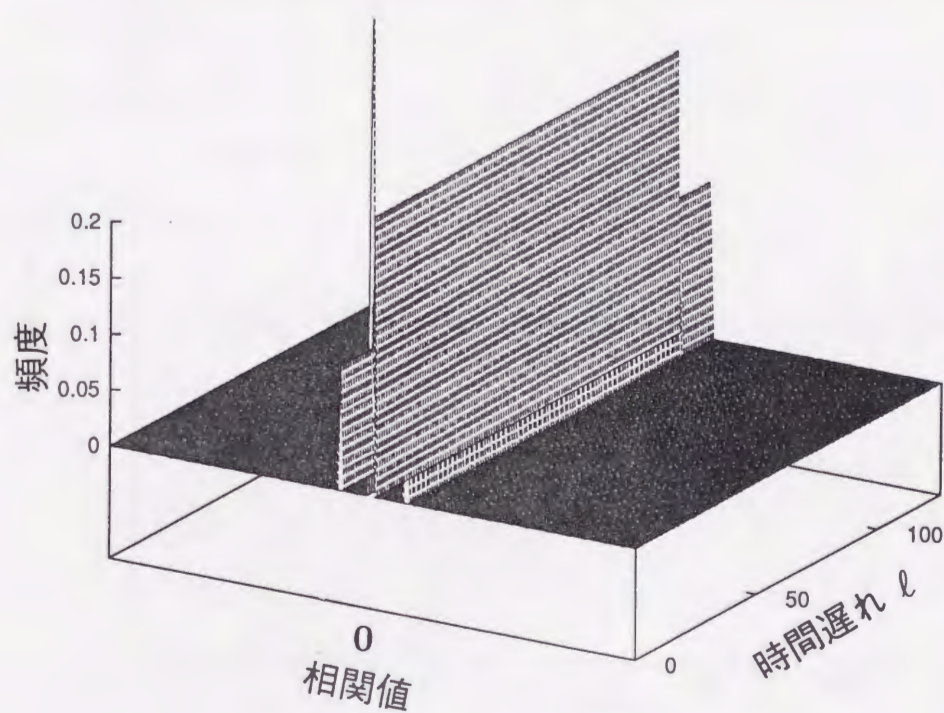
(a) 偶相関関数



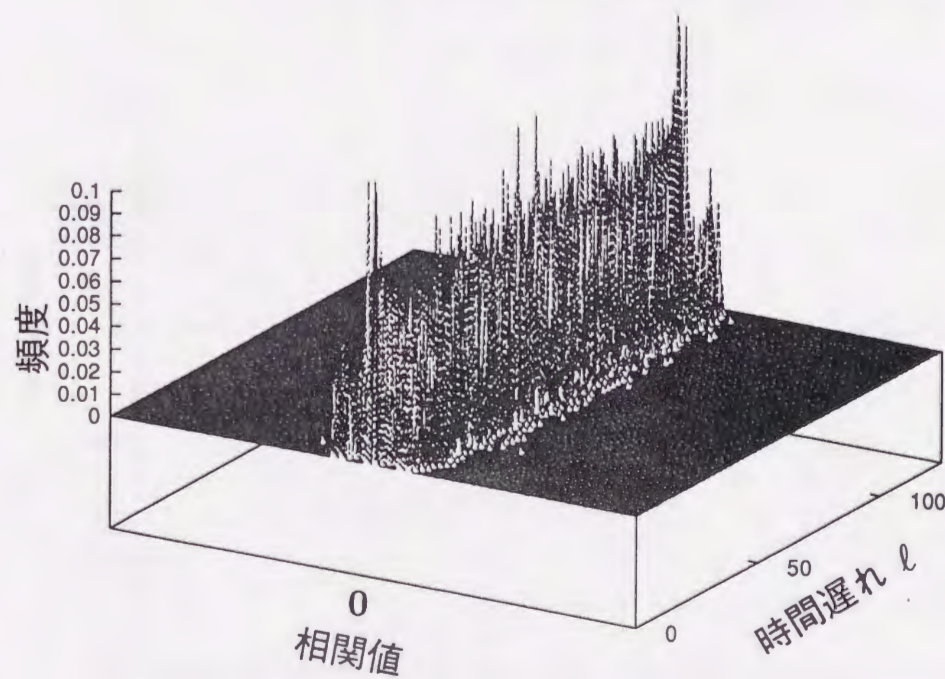
(b) 奇相関関数

図 4.12: あるペアの Gold 系列の相互相関関数.





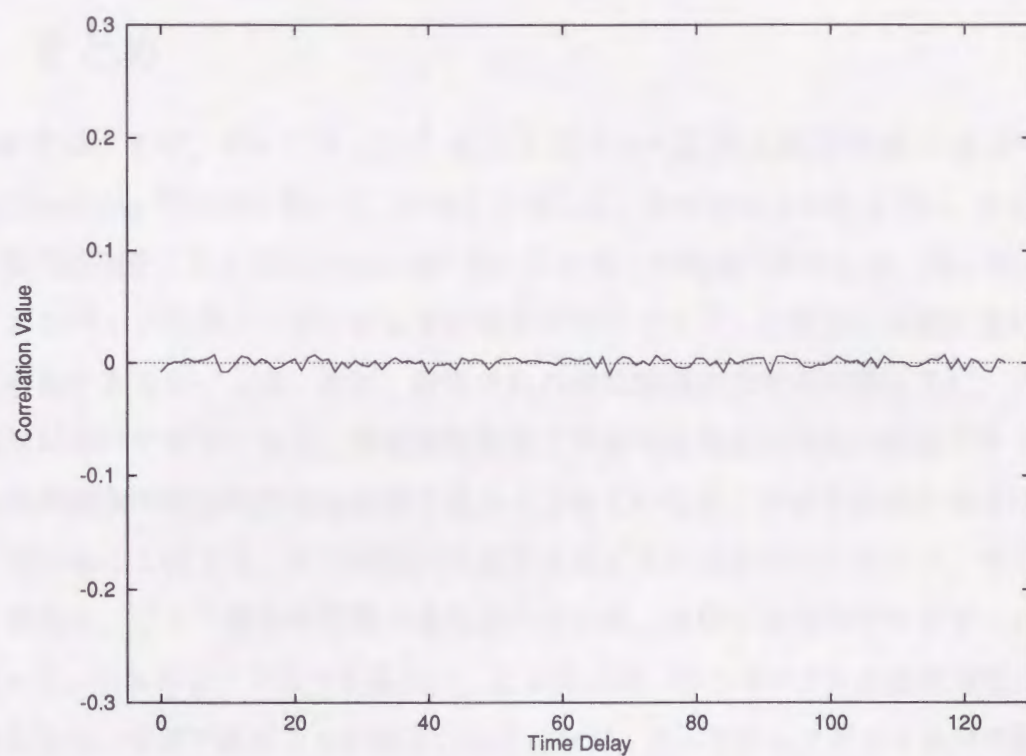
(a) 偶相関関数



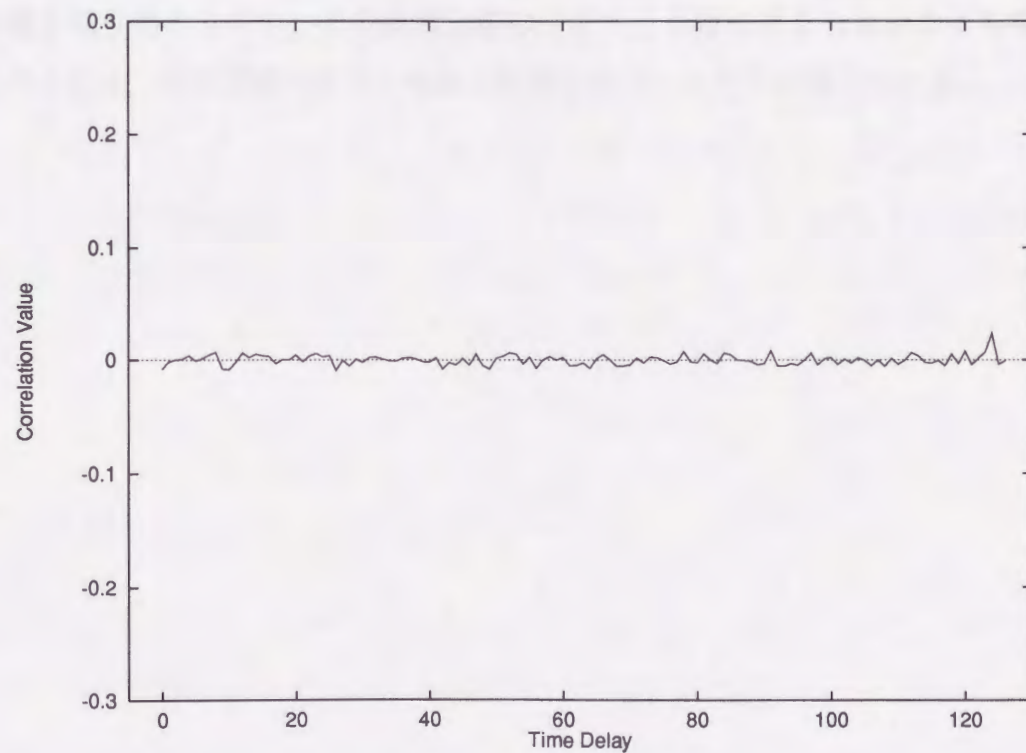
(b) 奇相関関数

図 4.13: Gold 系列の相関値の分布





(a) 偶相関関数



(b) 奇相関関数

図 4.14: 100 組の Gold 系列のペアに対する相互相関関数の平均値.



## 4.5 まとめ

本章では、まず、チェビシェフ2進およびビット系列の相関関数の空間平均値を、Perron-Frobenius作用素を用いて、厳密に評価した。定理で示されたように、P-F作用素は相関関数の評価を、ある領域内の逆像の数の数え上げの問題に帰着した。従って、P-F作用素は、エルゴード写像より得られる実数値系列だけでなく、2値系列の統計量の評価にも非常に有用であるといえる。次に、評価された相関関数の空間平均値を基に、スペクトル拡散通信において重要である、偶相関関数および奇相関関数の理論的評価式を与えた。従来、奇相関関数の理論的評価は困難であるとされていたが、カオス系列の場合は、空間平均法を用いることにより、その評価が可能であることが示された。さらに、チェビシェフビット系列は、ビット番号や写像の次数が大きい時、良好な相関特性を示すことがわかった。よって、チェビシェフビット系列は、工学的応用、特にスペクトル拡散通信における拡散符号として、有用であることが確認された。なお、チェビシェフビット系列の相関値の頻度分布がガウス分布になることを経験的に知ることができ、その平均値は、空間平均値で評価されることが示された。また、Gold系列の奇相関値は、チェビシェフビット系列と同様、多値を取り得るものの、その頻度分布は、ガウス分布にはならないことも確かめられた。このことは、奇相関値の分布が容易に評価できないことを示唆している。



## 第5章

# 有限周期カオス系列の統計量の揺らぎと高次相関関数

### 5.1 はじめに

第4章において、エルゴード写像より生成されるカオス2値系列の相関関数の理論的評価を、空間平均法によって行なった。ただし、この空間平均値は、系列の周期が無限長である場合の値であり、また、有限周期系列の統計量のあらゆる初期値に対する平均値と見なすことも出来た。カオス系列を通信等に実際に応用する際は、有限周期の系列を使うので、その振舞いを知ることは重要である。個々の初期値に対する有限周期長のカオス系列の統計量はそれ自身が確率変数となり、空間平均値からの揺らぎを生じるが、第4章で示したように、その頻度分布は、初期値の個数が大きい時、ガウス分布に近づき、その平均値（すなわち経験値）は空間平均値で評価される。従って、本章では、その分散についての議論を行なう。

### 5.2 分散による揺らぎの評価

経験的にではあるが、 $L$  個の初期値  $\{x_i\}_{i=1}^L$  に対する  $F_T(x_i)$  の頻度分布が、 $L$  を大きくするに従って、ガウス分布に近づくことを知ることが出来る。周知の通り、ガウス分布は平均値と分散によって定まる分布であり、

$$\phi(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{(x-\mu)^2}{2\sigma^2}\right] \quad (-\infty \leq x \leq \infty) \quad (5.1)$$

で表される<sup>[47]</sup>。ここで、 $\mu$  は平均値、 $\sigma^2$  は分散である。平均値  $\mu$  は、空間平均値  $\langle F \rangle$  で与えられるので、分散の評価が出来れば、時間平均  $F_T(x)$  がいろいろな初期値に対してどの



ように分布するかを事前に知ることが可能となる。そこで、 $F_T(x)$  の分散を

$$\sigma^2(F) = \langle (F_T(x) - \langle F \rangle)^2 \rangle \quad (5.2)$$

で定義し、平均値  $\langle F \rangle$ 、分散  $\sigma^2(F)$  のガウス分布を、 $\{F_T(x_i)\}_{i=1}^L$  の“推定分布”と呼ぶことにする。

### 5.3 分散の評価例

第3章で定義した  $\langle C(\ell; g, h) \rangle$  を用いると、式(5.2)は、

$$\sigma^2(F) = \frac{1}{T^2} \sum_{n=0}^{T-1} \sum_{m=0}^{T-1} \langle C(|n-m|, F, F) \rangle \quad (5.3)$$

のように表される。以下に  $F(x)$  として幾つかの統計量を選んだ場合の例を示す。

[例1]  $F(x) = x$  を式(5.3)に代入すると、実数値系列  $\{\tau^n(x)\}_{n=0}^{T-1}$  の平均値の分散は、

$$\sigma^2(x) = \frac{1}{T^2} \sum_{n=0}^{T-1} \sum_{m=0}^{T-1} \langle C(|n-m|, x, x) \rangle \quad (5.4)$$

となる。

次にカオス2進系列  $\{\theta_c(\tau^n(x))\}_{n=0}^{\infty}$  を考える。

[例2]  $F(x) = \theta_c(x)$  を式(5.3)に代入すると

$$\sigma^2(\theta_c) = \frac{1}{T^2} \sum_{n=0}^{T-1} \sum_{m=0}^{T-1} \langle C(|n-m|, \theta_c, \theta_c) \rangle \quad (5.5)$$

が得られる。

[例1] および [例2] の評価式の  $\langle C(\ell, x, x) \rangle$  や  $\langle C(\ell, \theta_c, \theta_c) \rangle$  については、既に陽な評価式が得られているので、具体的に計算が可能である。

次にカオス2進系列の2次の相関関数について考える。

[例3]  $F(x) = C(x; \ell, \theta_c, \theta_{c'})$  を式(5.3)に代入すると

$$\sigma^2(C(\ell, \theta_c, \theta_{c'})) = \frac{1}{T^2} \sum_{n=0}^{T-1} \sum_{m=0}^{T-1} \langle C(|n-m|, C(\ell; \theta_c, \theta_{c'}), C(\ell; \theta_c, \theta_{c'})) \rangle \quad (5.6)$$



を得る.

[例3] の  $\langle C(|n-m|, C(\ell; \theta_c, \theta_{c'}), C(\ell; \theta_c, \theta_{c'})) \rangle$  は4次の相関関数となる. 一般に  $d$  次の相関関数の分散の評価には  $2d$  次の相関関数の評価が必要となる.

## 5.4 チェビシェフ2進系列の高次相関関数

まず,  $d$  個の関数  $F^{(1)}(x), F^{(2)}(x), \dots, F^{(d)}(x)$  に対する  $d$  次相関関数を次式で定義する.

$$\begin{aligned} \langle C^{(d)}(\ell_{d-1}, \ell_{d-2}, \dots, \ell_1; F^{(d)}, F^{(d-1)}, \dots, F^{(1)}) \rangle = \\ \int_I (F^{(d)}(x) - \langle F^{(d)} \rangle) (F^{(d-1)}(\tau^{\ell_{d-1}}(x)) - \langle F^{(d-1)} \rangle) (F^{(d-2)}(\tau^{\ell_{d-1} + \ell_{d-2}}(x)) - \langle F^{(d-2)} \rangle) \cdot \\ \dots (F^{(1)}(\tau^{\ell_{d-1} + \ell_{d-2} + \dots + \ell_1}(x)) - \langle F^{(1)} \rangle) f^*(x) dx \end{aligned} \quad (5.7)$$

チェビシェフ2進系列に関しては, 既に, 第4章において (式(4.25)),

$$P_\tau^\ell \{ (\theta_c(x) - \langle \theta_c \rangle) f^*(x) \} = \frac{1}{k^\ell} s((\tau^\ell)'(c)) (\theta_{\tau^\ell(c)}(x) - \langle \theta_{\tau^\ell(c)} \rangle) f^*(x) \quad (5.8)$$

のような結果が得られている. よって, チェビシェフ2進系列の  $d$  次の相関関数は,

$$\begin{aligned} \langle C^{(d)}(\ell_{d-1}, \ell_{d-2}, \dots, \ell_1; \theta_{c_d}, \theta_{c_{d-1}}, \dots, \theta_{c_1}) \rangle = \\ \frac{1}{k^{\ell_{d-1}}} s((\tau^{\ell_{d-1}})'(c_d)) \{ \langle C^{(d-1)}(\ell_{d-2}, \dots, \ell_1; \theta_{\max[\tau^{\ell_{d-1}}(c_d), c_{d-1}], \theta_{c_{d-2}}, \dots, \theta_{c_1}) \rangle \\ - \langle \theta_{c_{d-1}} \rangle \langle C^{(d-1)}(\ell_{d-2}, \dots, \ell_1; \theta_{\tau^{\ell_{d-1}}(c_d)}, \theta_{c_{d-2}}, \dots, \theta_{c_1}) \rangle \\ - \langle \theta_{\tau^{\ell_{d-1}}(c_d)} \rangle \langle C^{(d-1)}(\ell_{d-2}, \dots, \ell_1; \theta_{c_{d-1}}, \theta_{c_{d-2}}, \dots, \theta_{c_1}) \rangle \\ + (\langle \theta_{\max[\tau^{\ell_{d-1}}(c_d), c_{d-1}]} \rangle - \langle \theta_{\tau^{\ell_{d-1}}(c_d)} \rangle \langle \theta_{c_{d-1}} \rangle) \langle C^{(d-2)}(\ell_{d-3}, \dots, \ell_1; \theta_{c_{d-2}}, \dots, \theta_{c_1}) \rangle \} \end{aligned} \quad (5.9)$$

のように  $d-1$  次以下の相関関数の形で書き表される. ここで,

$$\langle C^{(1)}(\theta_{c_1}) \rangle = \int_I (\theta_{c_1}(x) - \langle \theta_{c_1} \rangle) f^*(x) dx = 0 \quad (5.10)$$

$$\langle C^{(0)} \rangle = \int_I f^*(x) dx = 1 \quad (5.11)$$

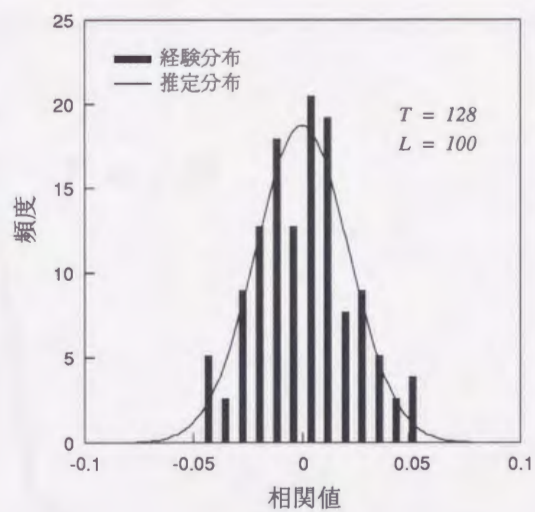
である. よって, 式(5.9)を再帰的に用いることにより,  $d$  次の相関関数の計算が可能である.



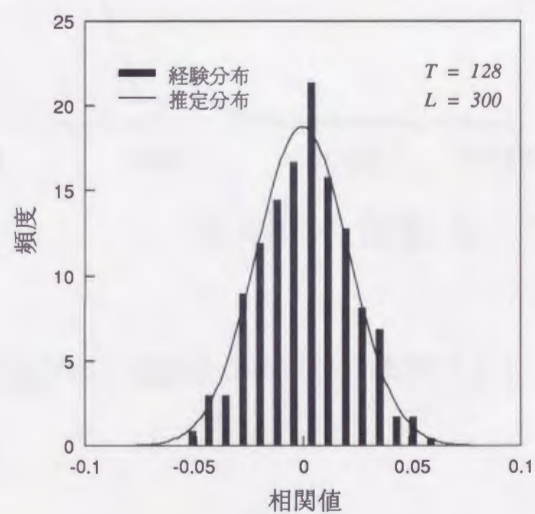
## 5.5 数値例

図 5.1 は、チェビシェフ 2 進系列の 2 次の相関値  $C_T^{(2)}(x; 30; \theta_{0.3}, \theta_{0.7})$  の経験分布および推定分布を初期値の個数  $L$  を変えて計算した結果であり、図 5.2 には、経験分布と推定分布との差の自乗和の  $L$  に対する特性を示す。これらの図から、 $L$  を大きくした時、経験分布が推定分布に近づくことがわかる。また、図 5.3 には、周期  $T$  を変えて計算した結果を示す。さらに、図 5.4 は、分散の  $T$  に対する特性である。これらの図から、 $T$  を大きくした時には分散が小さくなっていることがわかる。

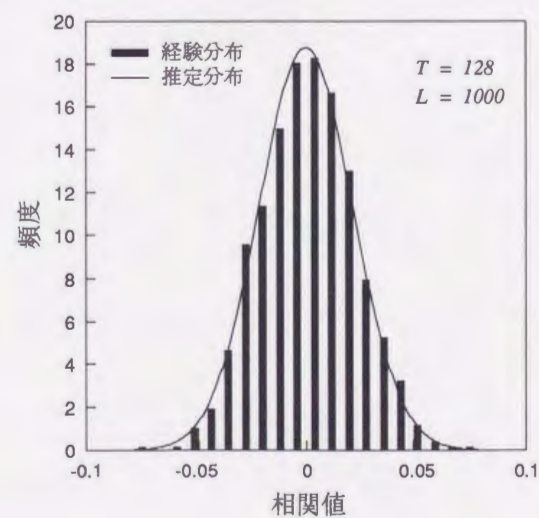




(a)



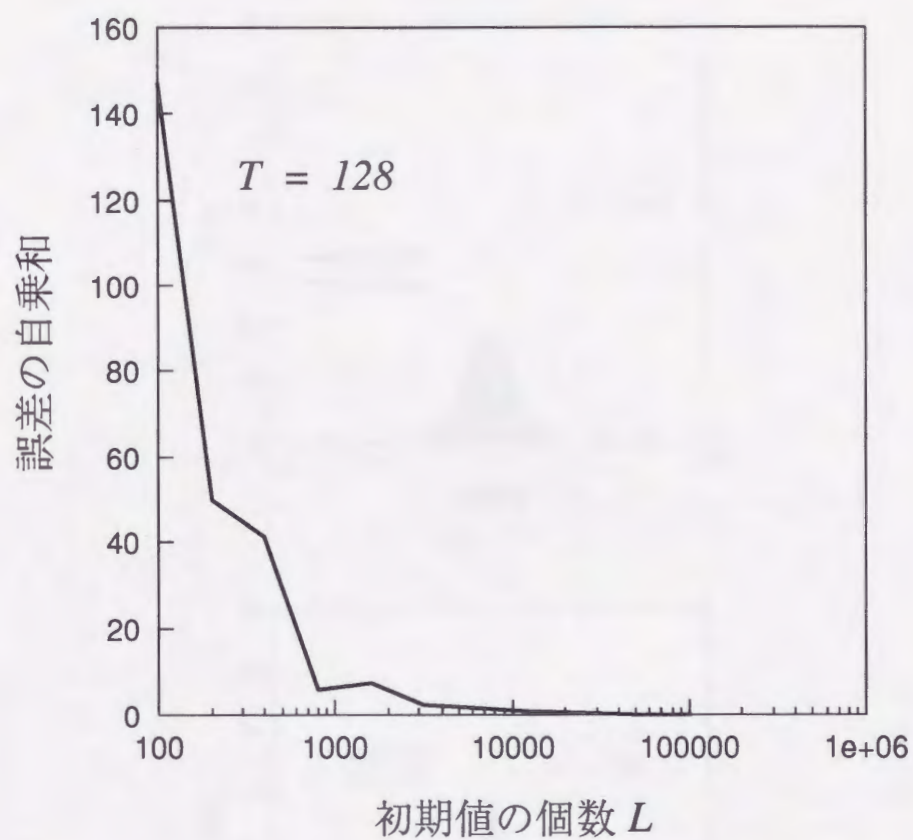
(b)



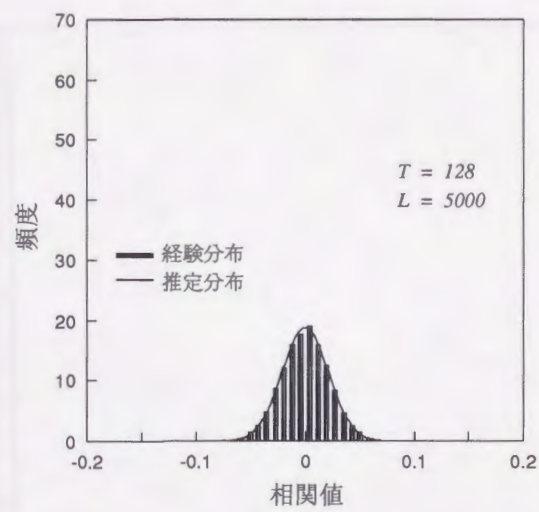
(c)

図 5.1:  $C_{128}^{(2)}(x_i; 30; \theta_{0.3}, \theta_{0.7})\}_{i=1}^L$  の分布. (a)  $L = 100$ , (b)  $L = 300$ , (c)  $L = 1000$ .

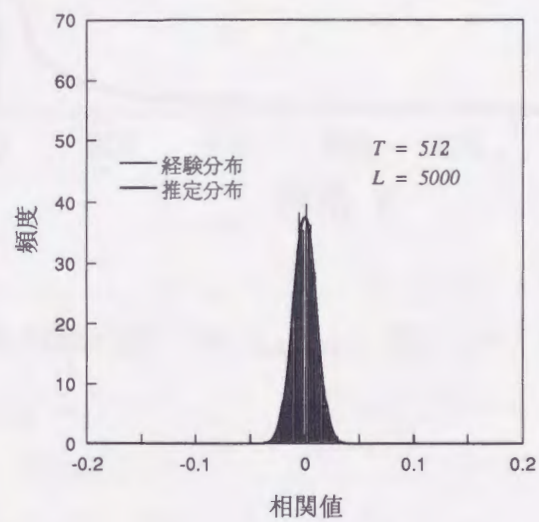


図 5.2: 推定分布と経験分布の差の自乗和の  $L$  に対する特性

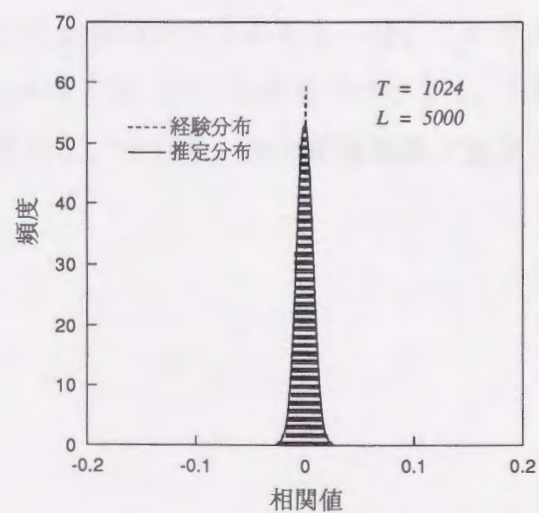




(a)



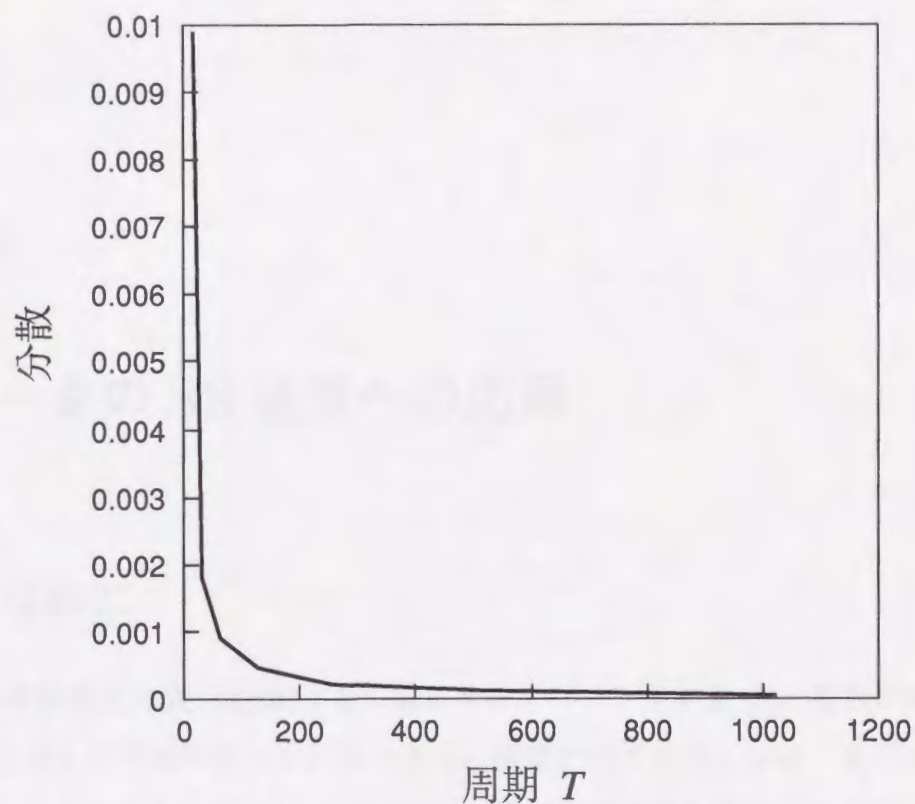
(b)



(c)

図 5.3:  $C_T^{(2)}(x_i; 30; \theta_{0.3}, \theta_{0.7})\}_{i=1}^{5000}$  の分布. (a)  $T = 120$ , (b)  $T = 512$ , (c)  $T = 1024$ .



図 5.4: 分散 $\sigma^2(C^{(2)}(30; \theta_{0.3}, \theta_{0.7}))$  の  $T$  に対する特性

## 5.6 まとめ

有限周期長のカオス系列の統計量の揺らぎについての評価を行なった。この統計量の頻度分布を調べると、初期値の集合の大きさが大きい時、これがガウス分布に近づくことが経験的に確かめられるが、本章では、その平均値だけでなく、分散もまた、空間平均法により評価が可能であることを示し、その際、高次相関関数が重要となることも併せて明らかにした。



## 第 6 章

### 画像データの SS 通信への応用

#### 6.1 はじめに

符号分割多重接続方式 (CDMA) を可能にするスペクトル拡散 (SS) 技術が実用化されているのは現在のところ音声データのみであり、画像データに関しては、まだほとんど検討されていない。その最大の理由は、画像データ量が音声のそれに比べて遥かに大きいため、高能率符号化が実現できないことに起因する。画像の符号化に際しては、離散コサイン変換 (DCT) が広く用いられているので、この DCT 係数を CDMA 伝送路を通して伝送することを考える。この場合、どのように DCT 係数を各チャネルに振り分けるか、あるいは、各チャネルに割り当てる拡散符号長をどのようにするか等で、幾つかのモデルが考えられるが、ここでは、3つのモデルを提案し、各モデルについての予備的検討を行なう。その結果、カオス系列のような可変長の擬似乱数 (PN) 系列がスペクトル拡散 (SS) 変調方式を用いた画像伝送に有効であることを示す。



## 6.2 SS を用いたベースバンド画像伝送システム

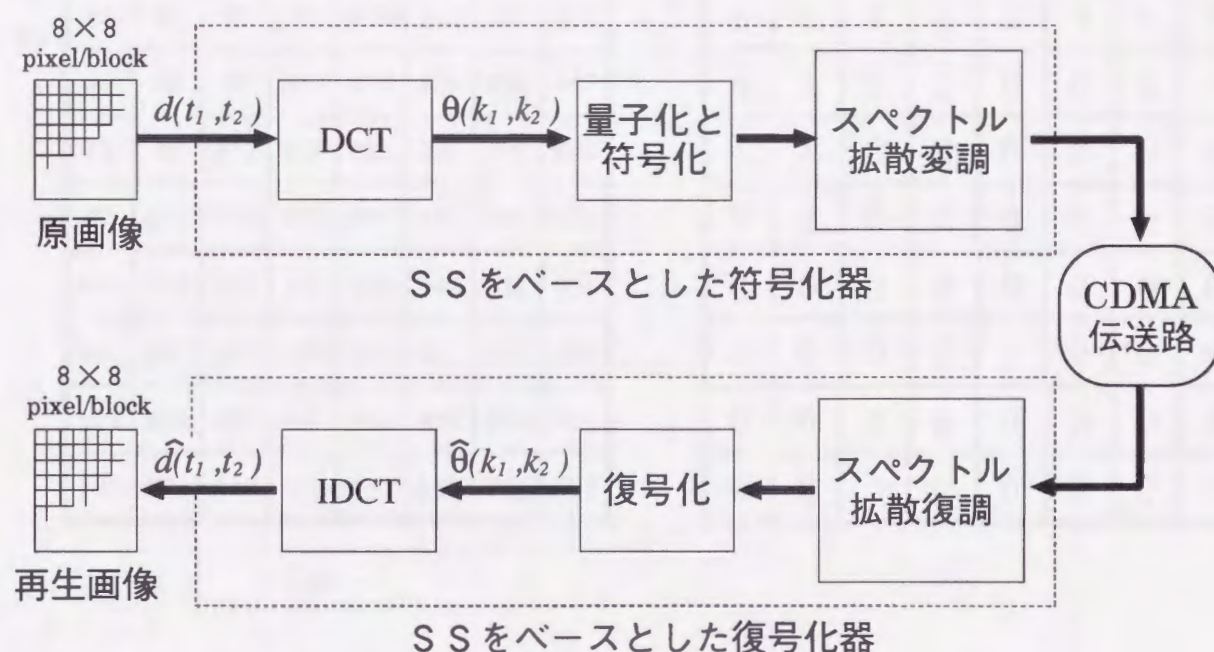


図 6.1: SS 技術を用いた画像伝送システム

SS を用いたベースバンド画像伝送システムは、送信側では基本的に画像の符号化、量子化、SS 変調等の3つの処理単位からなり、受信側ではその逆の処理が逆の順番で行われる。図 6.1 にそのような SS 技術を用いた基本的な画像伝送システムを示す。

ここでは、送信側でまず画像を  $8 \times 8$  画素からなるブロックに分割し、後の処理をブロック単位で行うものとする。画像の符号化としては、画像信号  $d(t_1, t_2)$  の2次元(2-D)離散コサイン変換(DCT)を用いる。ここで DCT 係数には、図 6.2 (a) に示されるような番号付けをしておく。そのあと量子化器で 2-DDCT 係数  $\theta(k_1, k_2)$  を量子化し、画像において重要である低周波数の係数には、高周波数の係数より多くのビット数を割り当てて伝送することとする。具体的にはビット数は図 6.2 (b) に示すように割り当てるものとする。ここでは1ブロックにつき低周波の方から15個の DCT 係数(54ビット/ブロック, 0.84ビット/画素)を伝送することにする。この後、SS 処理を行い、信号を CDMA 伝送路へと送信する。なお、誤り訂正機能を追加する際には、誤り訂正用の符号化器および復号化器は、それぞれ、SS 変調器の入力側、SS 逆変調器の出力側につければよい。ただし、ここでは、簡単のため、誤り訂正機能を付加しないで考える。



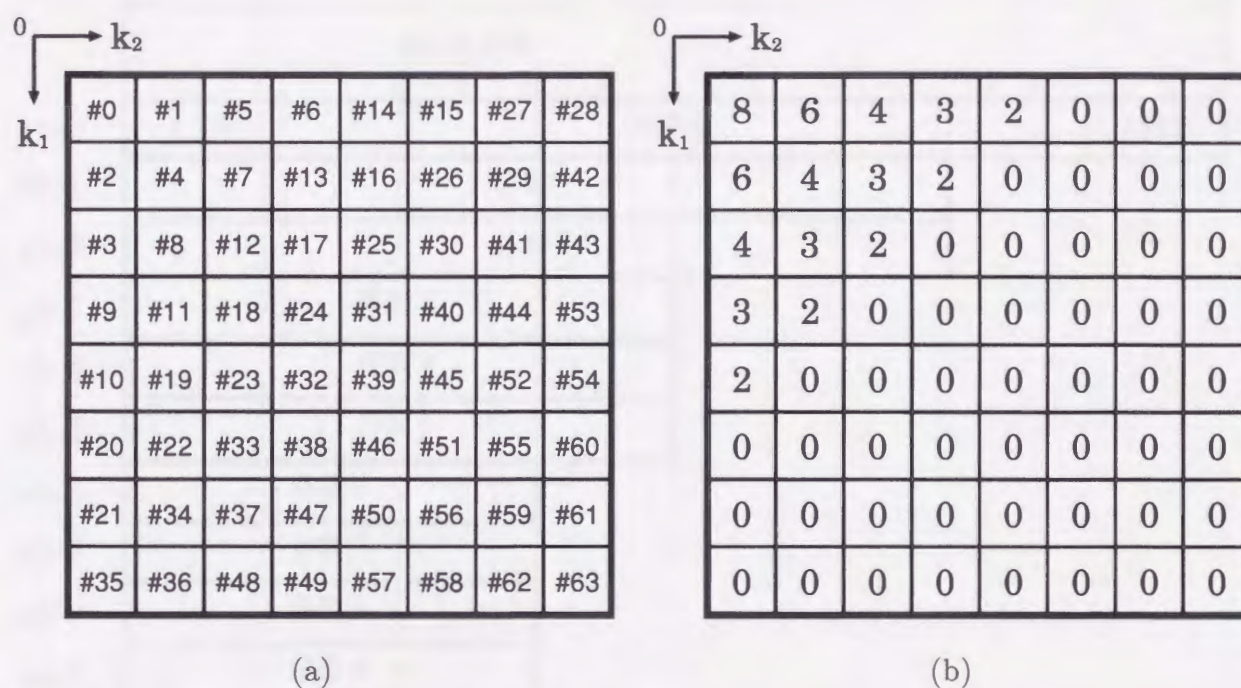


図 6.2: (a) 係数番号, (b) ビット割り当て.

### 6.3 固定長および可変長 PN 符号による伝送モデル

CDMA システムに基づいた DCT 係数の伝送に対し, 次の3つのモデルを提案する.

#### 6.3.1 モデル 1

第1のモデルは図 6.3 に示すように簡単なモデルで, 各係数には, 固定長のそれぞれ異なる拡散符号が掛けられ伝送される. このモデルでは, 重要な情報をもつ低周波の係数の上位ビットほど高周波の係数の下位ビットより多重度を低くすることで, 低周波の係数の上位ビットの誤り確率を抑えて(重みをつけて)伝送することになる. ブロック長は図中においてそれぞれのチャンネルのうちチップ(拡散符号のビットの最小単位)数の総和の最大の値で定義される. このシステムには15チャンネルが必要であるが, チャンネルを有効に使用しているとは言えない.





図 6.3: モデル 1

### 6.3.2 モデル 2

第 2 のモデルでは、図 6.4 に示すように拡散符号としては可変長のものが用いられ、幾つかの係数には共通の拡散符号が掛けられて同じチャネルを通して伝送される。ここで重要なのは、可変長の拡散符号を用いることにより、CDMA システムが普通望ましくないとされる非同期になってしまうことである。しかし、低周波の係数には高周波の係数より周期長の長い拡散符号が掛けられることになり、低周波の係数のビット誤り率が抑えられることになる。ただし、係数 10 から 14 については、チャネル利用効率の都合上、かえって周期長が長くなっている。また、各チャネルのデータ長はそれぞれ等しくなり、各係数について上位ビットと下位ビットはほぼ同じ多重度で伝送されることになる。このモデルでは、



チャンネル数も5に減少しており、チャンネルの利用効率は改善されている。



図 6.4: モデル 2

### 6.3.3 モデル 3

第3のモデルも図 6.5 に示すように、可変長の拡散符号が用いられ非同期のシステムとなっている。図中で、1対の  $(n, m)$  は  $n$  番目の係数の最上位から数えて  $m$  位のビットを表す。例えば、 $(0, 1)$  は係数 0 の最上位ビット (MSB) を、 $(0, 8)$  は係数 0 の最下位ビット (LSB) を表す。このモデルでは、より低周波、より上位のビットにはより長い周期長をもつ拡散符号が掛けられることになり、低周波の上位のビットほど誤り率が抑えられることになる。各チャンネルのデータ長はそれぞれ等しくなり、チャンネル数もさらに減少していて、チャンネルの利用効率はさらに改善されている。



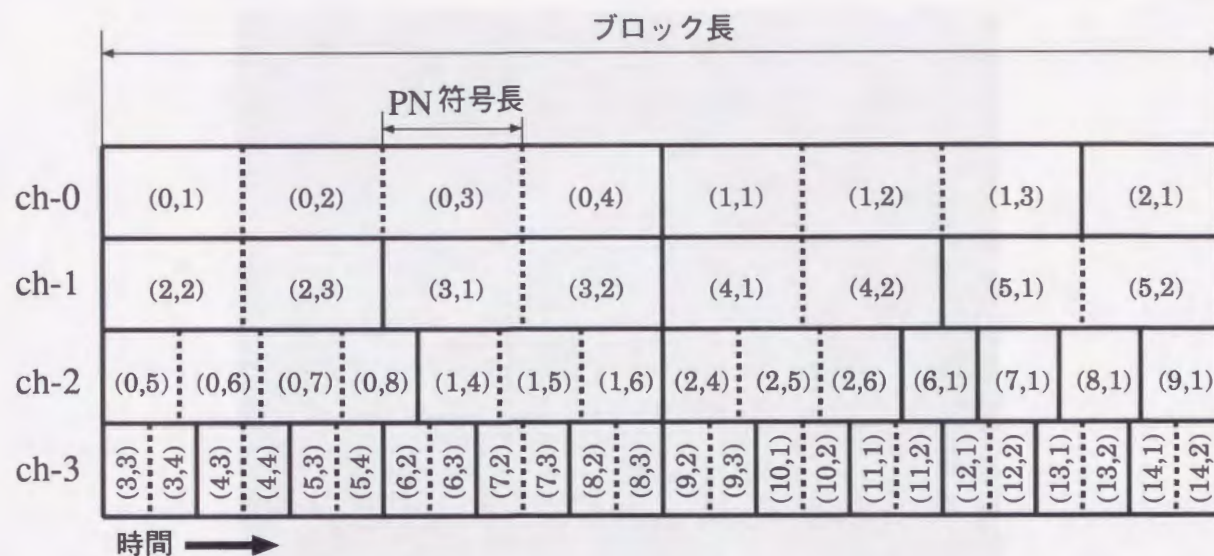


図 6.5: モデル 3

### 6.3.4 実験結果と検討

上記の3つのモデルについて、実験を行った。これらの実験においては、PN符号としては任意の符号長を選べるチェビシェフビット系列を用いた(モデル1の場合PN符号長が固定されていて、SR系列もこのシステムに利用できるので、比較のためGold系列を用いた場合の実験結果も示す。ただしこのシステムでは同期式にできるが、モデル2やモデル3のような他の非同期式のシステムと比較するため、あえてここでは非同期式にしている)。サンプル画像(図6.6)は、モノクロ画像(720×576画素、256階調)を用いた。簡単のため、チャネル雑音はないものとし、誤り訂正技術は取り入れずに実験した。図6.7には、量子化誤差およびデータ圧縮による誤差のみを含んだ画像を示す。すなわち、伝送路において誤りがなければ、この程度まで復元できることを示す。図6.8～図6.10に、それぞれのモデルでの復元画像を示す。(ブロック長は図中に示す。)





図 6.6: 原画像 (Barbara)



図 6.7: 量子化誤差等を含んだ画像





(a) チェビシェフピット系列 (ブロック長 240)



(b) Gold 系列 (ブロック長 248)

図 6.8: モデル 1 での復元画像



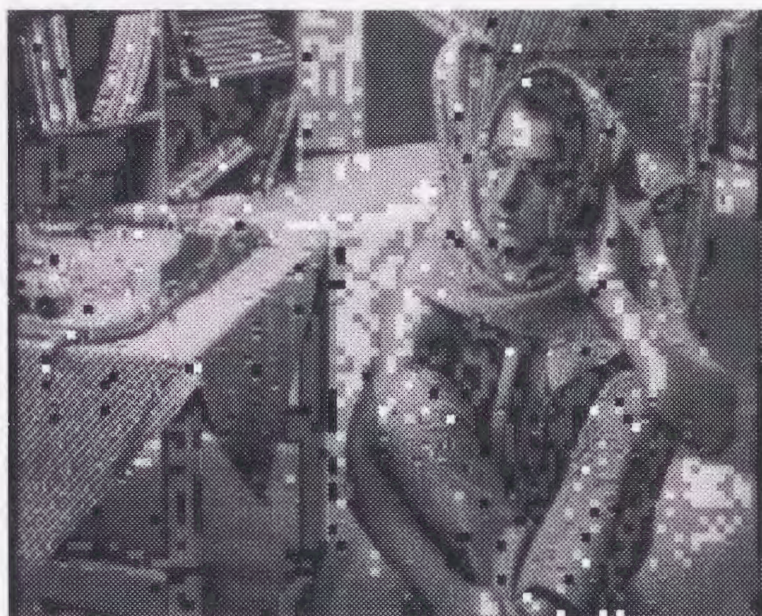


図 6.9: モデル 2 での復元画像 (チェビシェフビット系列, ブロック長 240)



図 6.10: モデル 3 での復元画像 (チェビシェフビット系列, ブロック長 168)



また、3つのモデルそれぞれについて、ビット誤り率と輝度の平均自乗誤差 (MSE)

$$\text{MSE} = E \left[ \frac{|d(t_1, t_2) - \hat{d}(t_1, t_2)|^2}{|d(t_1, t_2)|^2} \right] \quad (6.1)$$

を求めた。ただし  $E$  は、 $t_1, t_2$ , ブロックについて平均をとるものとする。図 6.11 および図 6.12 にそれぞれの結果を示す。



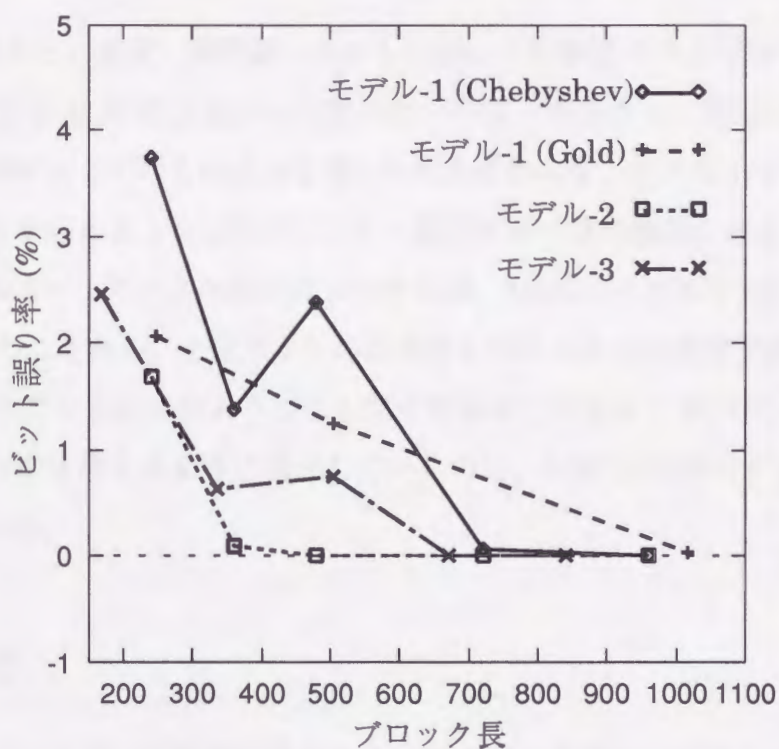


図 6.11: ビット誤り率 対 ブロック長

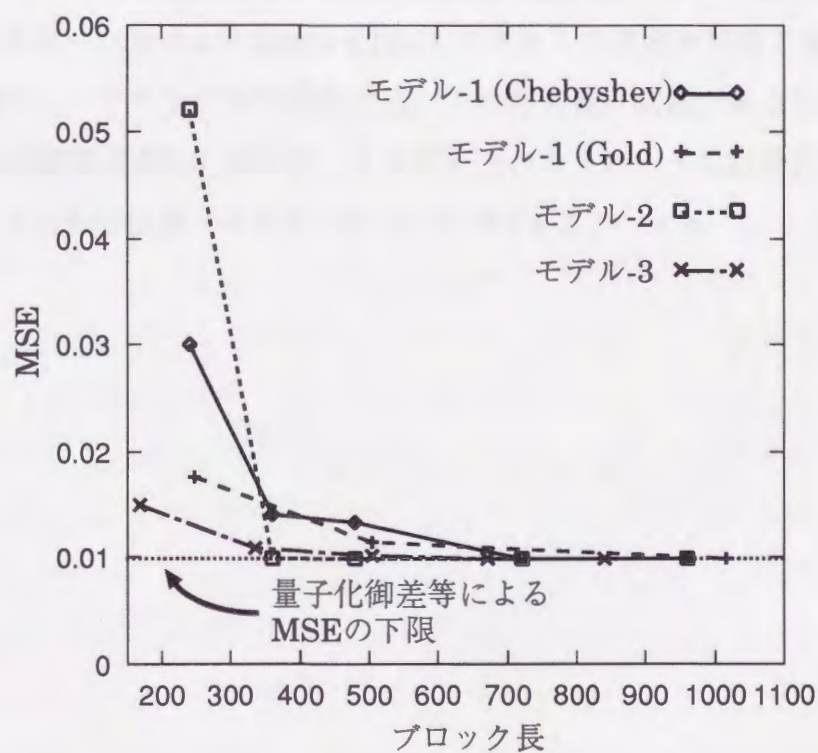


図 6.12: MSE 対 ブロック長



上の実験結果から、まず、非同期システムにおいては特性のうえではチェビシェフビット系列はそれほどGold系列と変わりはないということが分かる。第2に、モデル1でのビット誤り率はモデル2でのそれよりも高いにもかかわらず、モデル1で各DCT係数の上位ビットの誤り率を抑えるように設計した分、復元画像の質の指標となるMSEはそれぞれそんなに変わりはない(ブロック長が短いときには、MSEはモデル1の方がモデル2のそれより良い)。このことから、上位ビットの誤り率を抑えることは重要であることが分かる。モデル3では、モデル2の場合よりビット誤り率は等しいかより悪いが、低周波の係数の上位ビットの誤り率を抑えるように構成しているので、MSEは他のモデルと比較してもかなり改善されている。

## 6.4 まとめ

SSに基づくベースバンド画像伝送システムのモデルを幾つか提案した。幾つかのモデルの実験結果により、多重度を落としたり割り当てるPN符号の周期長を変えることで、重要なビットに重みづけをして伝送することが出来ることが示された。低周波係数の上位ビットの誤り率を抑えるような設計をすることで、復元画像の質がさらに改善される。その際、可変長PN系列を用いた方がより柔軟なCDMAシステムの構成が可能であり、有用であるといえる。従来の、シフトレジスタ系列では、その符号長に制限があるために、このような柔軟な符号化が容易でない。よって、カオス系列のように、その符号長が可変であることは、このような効率的伝送システムの構成に有効であるといえる。



## 第7章

### 結論と今後の課題

本論文では、カオス2値系列を情報通信の分野へ応用するために、主に、その重要な統計量である相関特性に関して議論を行なった。

第1章では、本研究の背景および動機について述べた。

第2章では、スペクトル拡散通信および符号分割多元接続(CDMA)の基本原理を述べた。ここで、拡散符号の相関特性が重要な役割を担うこと、また、非同期通信においては、偶および奇の2種類の相関関数について考慮しなければならないこと等を示した。

第3章では、まず、一次元非線形エルゴード写像を用いたカオスの生成法およびその時系列解析法を概説し、カオス系列が確率論的符号であること、従って、その統計量を評価することが重要であり、その際、空間平均法が有力であることを述べた。次に、実数値のカオス系列を2値系列に変換する方法を2つ提案した。カオスを2値系列として用いることは、従来のシフトレジスタ系列を用いたシステムがそのまま使えるということ、また、実数値系列では導入できなかった相互相関関数の概念が導入可能となり、空間平均法によるその理論的評価も可能となること等の利点を有する。本論文では、非線形エルゴード写像として、チェビシェフ写像を取り上げ、これより得られる2値系列について、その自己および相互相関関数の空間平均値の上限を評価した。さらに、有限周期のカオス2値系列のファミリーを幾つかつくり、Gold系列やKasami系列のそれと比較するために、それぞれのファミリー内でのあらゆる組合せでの偶および奇相関値を計算し、各ペアでの最大値の分布を調べた。その結果、偶相関特性は、Gold系列やKasami系列に比べて悪いものの、奇相関特性に関してはそれほど差が無いことが示された。このことは、非同期通信においては、カオス2値系列を用いた場合とシフトレジスタ系列を用いた場合とで、ビット誤り確率等の通信の品質は、あまり変わらないことを示唆している。また、シフトレジスタ系列が、その周期長やファミリーサイズに制限があるのに対して、カオス2値系列に対しては、



任意に周期長を選べること、また、幾つかのパラメータを変えることでより多くの系列が生成可能であるなどの利点を有するので、将来の拡散符号として有用であるといえる。

第4章では、第3章で上限しか与えられなかったカオス2値系列の相関関数の空間平均値を、Perron-Frobenius(P-F)作用素と呼ばれる積分作用素を用いることにより、厳密に与えた。その際、P-F作用素に関して興味深い関係式が示され、相関関数の評価は、数え上げの問題に帰着された。その結果、相関関数の空間平均値の陽な評価式を与えることが出来た。さらに、ここで得られた理論的評価式を基に、偶相関関数はもとより、従来、困難とされていた奇相関関数の理論的評価式も与えることが可能となった。また、チェビシェフビット系列は、チェビシェフ写像の次数およびビット番号が大きい時に、良好な（偶および奇）相関特性を示すことも明らかになった。

第5章では、有限周期のカオス系列の統計量の、空間平均値からの揺らぎについて議論を行なった。実際にカオス系列を通信に応用する際には、有限周期の系列の振舞いが重要である。いろいろな初期値に対する有限周期カオス系列の統計量の頻度分布が、初期値の集合の大きさを大きくした時、ガウス分布に近づくことを、経験的に知ることが出来るが、そのガウス分布の平均値だけでなく、分散も、やはり空間平均法により評価が可能であることが示される。その際、(2次あるいは高次)相関関数が重要な役割を果たすことも示された。

第6章では、画像通信への応用例として、SS方式による効率的な画像の伝送方法について、幾つかのモデルを提案した。膨大なデータ量の画像を効率の良い圧縮率で伝送するための方法として、用いる拡散符号の符号長を可変とすることが有用であることが示された。その結果、周期長が任意に可変であるカオス系列の有用性が確かめられた。

今後の課題としては、まず、SS通信への応用に関しては、本論文において、既に、有限周期カオス系列の統計量の分布が理論的に評価されたので、これを利用した、ビット誤り確率等の理論的評価を行なうこと、また、SS通信において重要な問題である同期捕捉についての、カオス2値系列の性能評価および従来の系列との比較をする必要がある。その他、誤り訂正符号を用いた場合の実験的検討や、周波数ホッピング法への応用に関する検討等が挙げられる。

また、本論文ではSS通信への応用を中心に議論してきたが、カオス系列は暗号通信への応用も期待されており、これに関しては、擬似乱数系列としての各種検定や、鍵系列として暗号通信に応用した場合の暗号強度等の性能評価および既存のシステムとの比較等が必要である。

その他、従来のモンテカルロシミュレーションでの応用や、情報理論でしばしば仮定さ



れる i.i.d. の実現例として、情報源や雑音源の具体的構成法としても、非常に有用であることが考えられる。



## 謝辞

本研究を進めるにあたり、懇切丁寧な御指導・御助言を頂きました九州大学工学部情報工学科 香田 徹 教授に深く感謝の意を表します。

本論文をまとめるにあたっては、九州大学工学部情報工学科 西 哲生 教授，電子工学科 二宮 保 教授に多くの御助言を賜りました。ここに厚く感謝致します。

また、九州大学名誉教授（現久留米工業大学教授）の 古賀 利郎 先生には、著者が学部および修士課程在学中に直接の指導者として、大変お世話になりました。ここに厚く感謝の意を表します。

さらに、本研究を行なう過程で、御指導・御助言を頂きました佐賀大学理工学部の松藤 信哉 博士に深く感謝致します。

最後に、本研究を行なうにあたり、多大な御助言・御協力を頂きました回路研究室および情報工学科の方々に深く感謝致します。



## 参考文献

- [1] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," Proc. IEEE, vol. 68, no. 3, pp.593-619, 1980.
  - [2] R. Kohno, "Pseudo-noise sequences and interference cancellation technique for spread spectrum systems-spread spectrum theory and technique in Japan," IEICE, Trans., vol. E74, pp.1083-1092, 1991.
  - [3] L. R. Welch, "Lower Bounds on the Maximum Cross Correlation of Signals", IEEE Trans. Information Theory, vol. 20, no. 3, pp.397-399, 1974.
  - [4] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-Function Sequences", IEEE Trans. Information Theory, vol. 28, No. 6, pp.858-864.
  - [5] S. Matsufuji, "Design of Balanced Sequences with Optimal Correlation Properties", 学位论文 (九州大学), 1993.
  - [6] S. K. Park, K. W. Miller, "Random Number Generators : Good Ones Are Hard to Find", Commun. ACM, vol. 31, no. 10, pp.1192-1201, 1988.
  - [7] D. S. Ornstein, "Ergodic Theory, Randomness, and "Chaos", Science, vol. 243, pp.182-186, 1989.
  - [8] S. L. Ulam and J. von Neumann, "On combination of stochastic and deterministic processes, Bull. Math. Soc., vol. 53, p.1120, 1947.
  - [9] E. A. Jackson, *Perspective nonlinear dynamics*, Cambridge Univ. Press, 1989.
  - [10] T. Y. Li and J. A. Yorke, "Ergodic transformations from an interval into itself", Trans. Am. Math. Soc., vol. 235, pp.183-192, 1978.
-



- [11] S. Oishi and H. Inoue, "Pseudo-random number generators and chaos", Trans. IEICE Japan, vol. E65, pp.534-541, 1982.
- [12] 香田, 柿本, "擬似乱数とカオス", 情報処理学会論文誌, vol. 27, No. 3, pp.289-296, 1986.
- [13] M. Casdagli, "Nonlinear prediction of chaotic time series", Physica D, vol. 35, pp.335-356, 1989.
- [14] L. O. Chua, Y. Yao and Q. Yang, "Generating randomness from chaos and constructing chaos with desired randomness", Int. J. Circuit and Applications, vol. 18, pp.215-240, 1990.
- [15] A. R. Murch and R. H. T. Bates, "Colored noise generation through deterministic chaos", IEEE Trans. on Circuit and Systems, vol. 37, no. 5, pp.608-613, 1990.
- [16] G. M. Bernstein and M. A. Lieberman, "Secure Random Generation Using Chaotic Circuits", IEEE Trans. Circuits and Systems, vol. 37, no. 9, pp.1157-1164, 1990.
- [17] R. L. Adler, and T. J. Rivlin, "Ergodic and mixing properties of Chebyshev polynomials," Proc. Amer.Math.Soc., vol. 15, pp. 794-796, 1964.
- [18] S. Grossmann and S. Thomae, "Invariant distributions and stationary correlation functions of one-dimensional discrete processes," Z. Naturforsch., vol. 32a, pp.1353-1363, 1977.
- [19] 香田, 村尾, 四反田, "区分的線形差分方程式の不規則解の相関関数", 電子通信学会論文誌, vol. J66-A, pp.725-732, 1983.
- [20] 香田, 梶原, "チェビシェフ乱数列の理論的検定", 電子情報通信学会技術研究報告, vol. NLP88-53, pp.35-40, 1988.
- [21] A. Lasota, and M. C. Mackey, *Probabilistic properties of deterministic systems*, Cambridge University Press, 1985.
- [22] 香田, 村尾, "一次元非線型差分方程式の不変密度の有限要素法的解法", 電子通信学会誌, vol. J65-A, no. 6, pp.505-512, 1982.



- [23] T. Kohda and K. Murao, "Approach to Time Series Analysis for One-Dimensional Chaos Based on Frobenius-Perron Operator," *Trans. IEICE*, vol. E73, no. 6, pp. 793-800, 1990.
  - [24] A. Boyarsky and M. Scarowsky, "On A Class of Transformations Which Have Unique Absolutely Continuous Invariant Measures," *Trans. Am. Math. Soc.*, vol. 255, pp. 243-262, 1979.
  - [25] T. Geisel and V. Fairen, "Statistical Properties of Chaos in Chebyshev Maps," *Physics Letters*, vol. 105A, no. 6, pp. 263-266, 1984.
  - [26] T. Y. Li and J. A. Yorke, "Ergodic maps on  $[0, 1]$  and nonlinear pseudo-random number generators", *Nonlinear Analysis Theory, Methods and Applications*, vol. 2, pp.473-481, 1978.
  - [27] 小原, 谷古宇, 藤村, 斉藤, 笹瀬, "カオスを用いた拡散スペクトル通信", 電子情報通信学会技術研究報告, vol. NLP89-85, pp.19-23, 1989.
  - [28] T. Habutsu, Y. Nishio, I. Sasase, and S Mori, "A secret key crypto system using a chaotic map," *Trans. IEICE*, vol. E73, pp.1041-1044, 1990.
  - [29] G. Heidari-Bateni, C.D. McGillem, M.F. Tenorio, "A Novel Multiple-Address Digital Communication System Using Chaotic Signals", *Proc. 1992 IEEE International Conference on Communications (ICC '92)*, pp.1232-1236, 1992.
  - [30] P. C. J. Hill, A. M. S. Haisan, "Statistical Reference Chip-Code Designs for LPI Enhancement in DS/SS Communication Systems", *Proc. IEEE Second International Symposium on Spread Spectrum Techniques and Applications (ISSSTA'92)*, pp.151-154, 1992.
  - [31] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications", *IEEE Trans. Circuit and Systems—II*, vol. 40, no. 10, pp.626-633, 1993.
  - [32] Hervé 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. Circuit and Systems—II*, vol. 40, no. 10, pp.634-642, 1993.
-



- [33] U. Parlitz and S. Ergezinger, "Robust Communication Based on Chaotic Spreading Sequences", *Physics Letters A*, vol. 188, pp.146-150, 1994.
  - [34] D. Knuth, *The art of Computer Programming*, vol. 2, Seminumerical Algorithms, 2nd ed. Addison-Wesley, Reading, Mass, 1981.
  - [35] 津田, モンテカルロ法とシミュレーション, 培風館, 1977.
  - [36] R. C. Tausworthe, "Random numbers generated by linear recurrence modulo two", *Mathematics of Computation*, vol. 19, pp.201-209, 1965.
  - [37] T. G. Lewis and W. H. Payne, "Generalized feedback shift register pseudorandom number algorithm", *J. ACM*, vol. 20, pp.456-468, 1973,
  - [38] J. L. Massey, "An Introduction to Contemporary Cryptology", *Proc. IEEE*, vol. 76, no. 5, May 1988.
  - [39] A. J. Viterbi, "Spread Spectrum Communications — Myths and Realities," *IEEE Communications Magazine*, pp.11-18, May, 1979.
  - [40] 横山, スペクトル拡散通信システム, 科学技術出版社, 1988.
  - [41] U. Madhow and M. B. Pursley, "Acquisition in Direct-Sequence Spread-Spectrum Communication Networks: An Asymptotic Analysis", *IEEE Trans. Information Theory*, vol. 39, no.3, pp.903-912, 1993.
  - [42] K. S. Gilhousen, et al., "On the Capacity of a Cellular CDMA System," *IEEE, Trans., Veh. Technol.*, vol. 40, pp.303-312, 1991.
  - [43] D. Schilling, et al., "Broadband CDMA for Personal Communications Systems," *IEEE Communications Magazine*, vol. 29, no. 11, pp.86-93, 1991.
  - [44] N. MacDonald, "Transmission of compressed video over radio link," *Visual Communication and Image Processing '92*, no. 1818-149, 1992.
  - [45] W. F. Schreiber, "Spread-Spectrum Television Broadcasting," *SMPTE Journal*, pp.538-549, August, 1992.
-



- [46] N. Doi, T. Yano, N. Kobayashi, H. Kishida, and M. Ohnishi, "Development of Wireless TV-phones using Spread-Spectrum Communication," Proc. The 16th Symposium on Information Theory and Its Applications (SITA '93), pp.121-124, 1993.
  - [47] W. Feller, *An Introduction to Probability Theory and Its Applications*, vol. 1, Charles E. Tuttle Company, 1967.
  - [48] T. Kohda, A. Tsuneda, and T. Sakae, "Chaotic Binary Sequences by Chebyshev Maps and Their Correlation Properties", Proc. IEEE Second International Symposium on Spread Spectrum Techniques and Applications (ISSSTA'92), pp.63-66, 1992.
  - [49] T. Kohda and A. Tsuneda, "Pseudonoise Sequences by Chaotic Nonlinear Maps and Their Correlation Properties," IEICE Trans. Communications vol. E76-B, no. 8, pp. 855-862, 1993.
  - [50] T. Kohda and A. Tsuneda, "Correlation Properties of PN Sequences for CDMA: Chaotic Binary Sequences, Gold Sequences, and Kasami Sequences," Proc. General Assembly of the International Union of Radio Science, p.127, 1993.
  - [51] T. Kohda and A. Tsuneda, "Correlation Properties of Chebyshev Binary/Bit Sequences", Proc. of 1994 IEEE International Symposium on Information Theory (ISIT'94), p.76, 1994.
  - [52] T. Kohda and A. Tsuneda, "Even- and Odd-Correlation Functions of Chaotic Chebyshev Bit Sequences for CDMA", Proc. of the IEEE Third International Symposium on Spread Spectrum Techniques & Applications (ISSSTA'94), pp.391-395, 1994.
  - [53] T. Kohda, A. Oshiumi, A. Tsuneda, and K. Ishii, "A Study on Pseudonoise-Coded Image Communicaitons", Proc. of SPIE's Visual Communications and Image Processing '94 (VCIP'94), pp.874-884, 1994.
  - [54] T. Kohda, Y. Sugisawa, and A. Tsuneda, "A Study on Statistics of Chaotic Sequences of Finite Period", Proc. of 1994 Symposium on Nonlinear Theory and its Applications (NOLTA'94), pp.121-124, 1994.
-



- [55] T. Kohda, and A. Tsuneda, "Explicit Evaluations of Correlation Functions of Chebyshev Binary and Bit Sequences Based on Perron-Frobenius Operator", IEICE Trans., vol. E77-A, no.11, pp.1794-1800, 1994.



## 付録 A

### チェビシェフ写像より生成される実数値系列の自己相関関数の導出

2 次および 3 次の自己相関関数  $\langle C(\ell; x, x) \rangle$ ,  $\langle C^{(3)}(\ell, m; x, x, x) \rangle$  はそれぞれ

$$\langle C(\ell; x, x) \rangle = \int_I (x - \langle x \rangle)(\tau^\ell(x) - \langle x \rangle)f^*(x)dx \quad (\text{A.1})$$

$$\langle C^{(3)}(\ell, m; x, x, x) \rangle = \int_I (x - \langle x \rangle)(\tau^\ell(x) - \langle x \rangle)(\tau^{\ell+m}(x) - \langle x \rangle)f^*(x)dx \quad (\text{A.2})$$

のように表される。ここで、

$$\langle x \rangle = \int_I x f^*(x)dx = 0 \quad (\text{A.3})$$

である。よって、

$$\langle C(\ell; x, x) \rangle = \int_I x \tau^\ell(x) f^*(x)dx, \quad (\text{A.4})$$

$$\langle C^{(3)}(\ell, m; x, x, x) \rangle = \int_I x \tau^\ell(x) \tau^{\ell+m}(x) f^*(x)dx. \quad (\text{A.5})$$

式 (3.10) の  $P_\tau$  の定義に従うと

$$P_\tau\{x f^*(x)\} = \frac{1}{k} f^*(x) \sum_{i=0}^{k-1} g_{k-i}(x) \quad (\text{A.6})$$

が得られる。

(1i)  $k$  が偶数の時,  $\tau(x)$  は偶関数となるので, 明らかに

$$\sum_{i=0}^{k-1} g_{k-i}(x) = 0$$

である。



(1ii)  $k$  が奇数の時, すなわち,  $k = 2r + 1$  の時

$$\begin{aligned}
 \sum_{i=0}^{k-1} g_{k-i}(x) &= \sum_{\text{even}} \cos\left(\frac{i\pi + \cos^{-1} x}{k}\right) + \sum_{\text{odd}} \cos\left(\frac{(i+1)\pi - \cos^{-1} x}{k}\right) \\
 &= \sum_{j=0}^r \cos\left(\frac{2j\pi + \cos^{-1} x}{2r+1}\right) + \sum_{j=1}^r \cos\left(\frac{2j\pi - \cos^{-1} x}{2r+1}\right) \\
 &= \sum_{j=0}^r \cos\left(\frac{2j\pi + \cos^{-1} x}{2r+1}\right) \\
 &\quad + \sum_{j=0}^r \cos\left(\frac{2j\pi - \cos^{-1} x}{2r+1}\right) - \cos\left(\frac{-\cos^{-1} x}{2r+1}\right) \\
 &= \cos\left(\frac{\cos^{-1} x}{2r+1}\right) \left\{ 2 \sum_{j=0}^r \cos\left(\frac{2j\pi}{2r+1}\right) - 1 \right\} \\
 &= 0.
 \end{aligned}$$

となる.

(1i) および (1ii) より

$$P_{\tau}\{xf^*(x)\} = 0 \quad (\text{A.7})$$

を得る. 同様にして,

$$P_{\tau}\{x^2 f^*(x)\} = \begin{cases} \frac{1}{2} f^*(x) & \text{for } k \neq 2 \\ \frac{1}{2} (1+x) f^*(x) & \text{for } k = 2 \end{cases} \quad (\text{A.8})$$

が得られる. よって, 2 次の自己相関関数  $\langle C(\ell; x, x) \rangle$  は

$$\langle r(\ell) \rangle = \int_I P_{\tau}\{xf^*(x)\} \tau^{\ell-1}(x) dx = 0 \quad \text{for } \ell \geq 1 \quad (\text{A.9})$$

と書ける. また,  $\ell = 0$  の時

$$\langle r(0) \rangle = \int_I x^2 f^*(x) dx = \frac{1}{2} \quad (\text{A.10})$$

である.

次に, 3 次の自己相関関数  $\langle C^{(3)}(\ell, m, x, x, x) \rangle$  を考える.

(2i)  $\ell \neq 0$  の時

$$\langle r(\ell, m) \rangle = \int_I P_{\tau}\{xf^*(x)\} \tau^{\ell-1}(x) \tau^{\ell+m-1}(x) dx = 0. \quad (\text{A.11})$$



(2ii)  $\ell = 0$  かつ  $m = 0$  の時

$$\langle r(0, 0) \rangle = \int_I x^3 f^*(x) dx = 0 \quad (\text{A.12})$$

(2iii)  $\ell = 0$  かつ  $m = 1$  の時

$$\begin{aligned} \langle r(0, 1) \rangle &= \int_I x^2 \tau(x) f^*(x) dx = \int_I P_\tau\{x^2 f^*(x)\} x dx \\ &= \begin{cases} \frac{1}{2} \int_I x f^*(x) dx = 0 & \text{for } k \neq 2 \\ \frac{1}{2} \int_I (x + x^2) f^*(x) dx = \frac{1}{4} & \text{for } k = 2 \end{cases} \end{aligned} \quad (\text{A.13})$$

(2iv)  $\ell = 0$  かつ  $m \geq 2$  の時

$$\begin{aligned} \langle r(0, m) \rangle &= \int_I P_\tau\{x^2 f^*(x)\} \tau^{m-1}(x) dx \\ &= \begin{cases} \frac{1}{2} \int_I \tau^{m-1}(x) f^*(x) dx & \text{for } k \neq 2 \\ \frac{1}{2} \int_I (1 + x) \tau^{m-1}(x) f^*(x) dx & \text{for } k = 2 \end{cases} \\ &= 0 \end{aligned} \quad (\text{A.14})$$

(2i)–(2iv) より, 式 (3.16) を得る. 同様にしてさらに高次の自己相関関数が計算できる.



## 付録 B

### チェビシェフビット系列の相関関数の評価式 (3.30) の導出

$\langle C(\ell; b_i, b_j) \rangle$  は、次のようにも表せる.

$$\langle C(\ell; b_i, b_j) \rangle = \int_I b_i(x) b_j(\tau^\ell(x)) f^*(x) dx - \langle b_i \rangle \langle b_j \rangle \quad (\text{B.1})$$

ここで,

$$Q_{ij}(\ell) = \int_I b_i(x) b_j(\tau^\ell(x)) f^*(x) dx \quad (\text{B.2})$$

とおく. また,  $b_i(x)$  および  $f^*(x)$  の偶関数性を用いると,

$$Q_{ij}(\ell) = 2 \int_0^1 b_i(x) b_j(\tau^\ell(x)) f^*(x) dx \quad (\text{B.3})$$

と書ける. ここで,

$$\tau^\ell(x) = \cos(k^\ell \cos^{-1} x) \quad (\text{B.4})$$

$$f^*(x) = \frac{1}{\pi \sqrt{1-x^2}} \quad (\text{B.5})$$

を考慮し, 変数変換

$$k^\ell \cos^{-1} x = y \quad (\text{B.6})$$

を施すと,

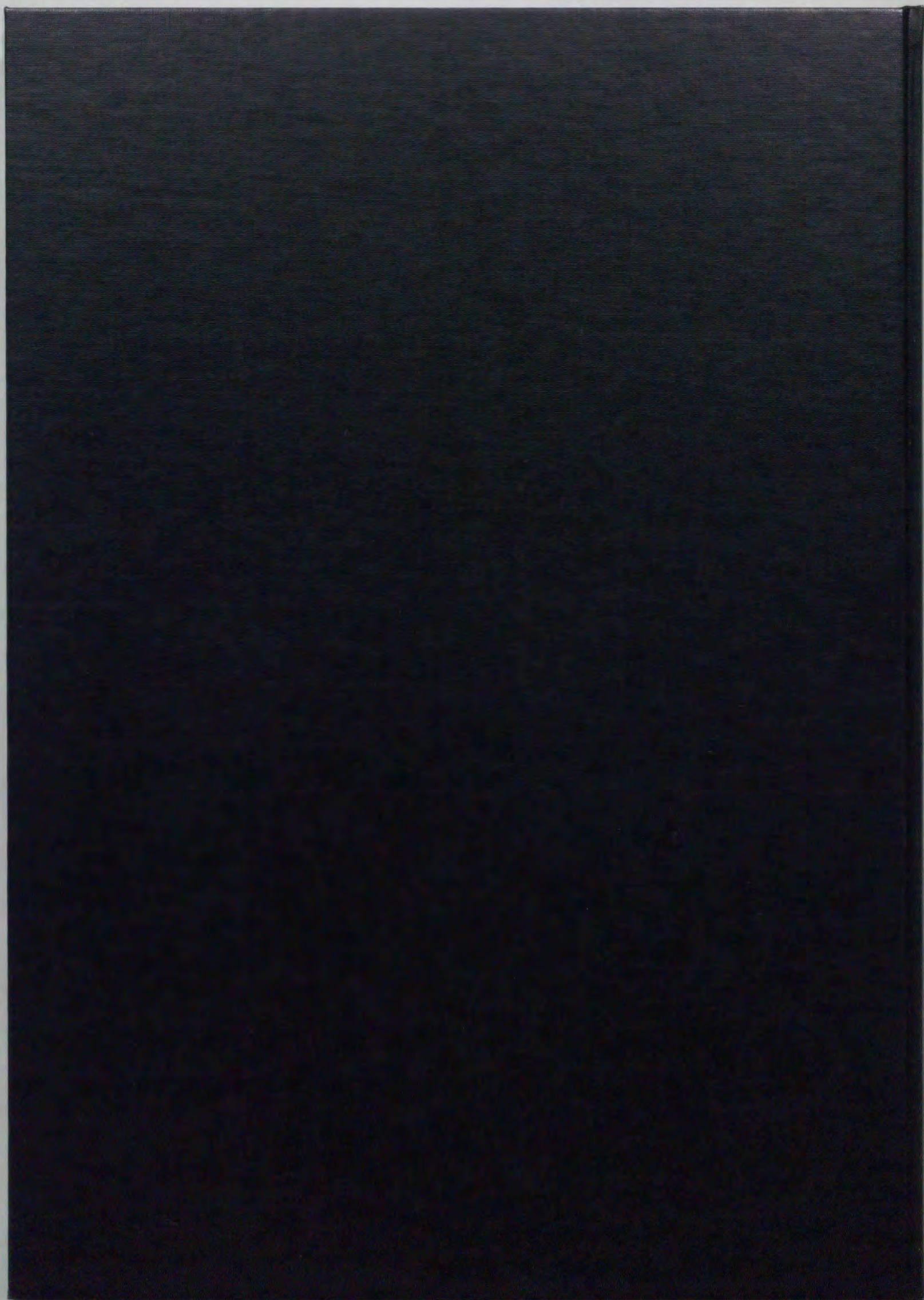
$$Q_{ij}(\ell) = 2 \int_0^{\pi k^\ell / 2} b_i(\cos \frac{y}{k^\ell}) b_j(\cos y) dy \quad (\text{B.7})$$

が得られる.  $b_i(\cos \frac{y}{k^\ell})$  および  $b_j(\cos y)$  が 1 になる区間を考慮すると,

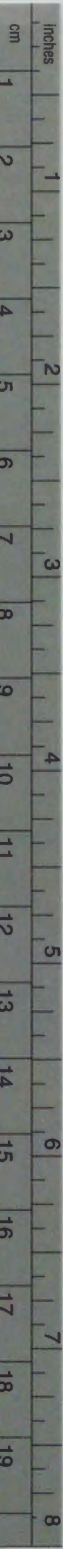
$$\frac{1}{k^\ell} (k \langle b_i \rangle \langle b_j \rangle - \langle b_j \rangle) < Q_{ij}(\ell) < \frac{1}{k^\ell} (k \langle b_i \rangle \langle b_j \rangle + \langle b_j \rangle) \quad (\text{B.8})$$

となる. よって, 式 (3.30) を得る. また,  $i = j$  とすれば, 式 (3.28) が得られる.









# Kodak Color Control Patches

© Kodak, 2007 TM: Kodak

Blue	Cyan	Green	Yellow	Red	Magenta	White	3/Color	Black

## Kodak Gray Scale



© Kodak, 2007 TM: Kodak

- |          |   |   |   |   |   |   |          |   |   |    |    |    |    |    |    |          |    |    |    |
|----------|---|---|---|---|---|---|----------|---|---|----|----|----|----|----|----|----------|----|----|----|
| <b>A</b> | 1 | 2 | 3 | 4 | 5 | 6 | <b>M</b> | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | <b>B</b> | 17 | 18 | 19 |
|----------|---|---|---|---|---|---|----------|---|---|----|----|----|----|----|----|----------|----|----|----|

