

平成 13 年度
学士学位論文

符号分割多元接続に用いる時変 PN 系列

Code Division Multiple Access using Time Variant
PN Sequences

1041013 石坂 崇

指導教員 濱村 昌則

2002 年 2 月 8 日

高知工科大学 情報システム工学科

要旨

符号分割多元接続に用いる時変 PN 系列

石坂 崇

従来の符号分割多元接続 (CDMA) では、各ユーザに特定時不変の擬似雑音系列 (PN 系列) を割り当てて多元接続を実現している。CDMA は、FDMA や TDMA など他の多元接続方式に比べて秘話性が高いとはいえ、時不変 PN 系列を用いると、それが一旦他人に知れてしまうと、盗聴され続けるという問題が生じる。本論文では、この問題を解決するために時変 PN 系列を提案した。時変 PN 系列は、周期の長い M 系列、及び LMS アルゴリズムの考え方を応用して生成する。LMS アルゴリズムの考え方を応用した更新式によって、時変 PN 系列がランダムな数値で順次生成される。更新式における更新ゲイン μ の値によって、時変 PN 系列の変化に影響が及ぶため、秘話性能がかかわってくる。そこで μ の最適値について検討した結果、 $\mu \doteq 0.03$ が最適値という結果を得た。また、時変 PN 系列を用いた CDMA におけるビット誤り率においても検討した結果、ランダム系列を PN 系列に用いた場合とほぼ同じビット誤り率で多元接続を実現できることが明らかとなった。

キーワード スペクトル拡散, CDMA, 時変 PN 系列, M 系列

Abstract

Code Division Multiple Access using Time Variant PN Sequences

Takashi Ishisaka

In code division multiple access (CDMA) a specific and time invariant pseudo noise (PN) sequence is assigned to each user. Even though CDMA has low probability of intercept compared with other multiple access schemes such as FDMA and TDMA, once the assigned PN sequence is known to others, intercept continues until the end of communications. In order to solve this problem, in this research, time variant PN sequences will be proposed. Time variant PN sequences are generated by M-sequences with long period and a modified version of LMS algorithm. The value of the update gain μ in an updating formula will be used to attain the change of time variant PN sequences and will improve the performance against intercept. As a result of examining the optimal value of μ , $\mu \doteq 0.03$ was obtained. Moreover, performance of CDMA using time variant PN sequences is examined. As a result, it is shown that the almost same bit error rate as the case of random sequences is obtained.

key words spread spectrum, CDMA, time variant PN sequence, M-sequence

目次

第 1 章	はじめに	1
1.1	研究の背景と目的	1
第 2 章	従来方式	2
2.1	符号分割多元接続	2
2.1.1	符号分割多元接続とは	2
2.1.2	直接拡散方式	3
2.2	擬似雑音系列	6
2.2.1	M 系列の性質	6
2.2.2	M 系列の生成	6
2.3	ノイズとは	8
2.3.1	ノイズの導出	8
第 3 章	時変 PN 系列	11
3.1	時変 PN 系列とは	11
3.2	時変 PN 系列の生成	11
3.2.1	時変 PN 系列の正規化	13
3.2.2	考察	14
3.3	時変 PN 系列における最適な μ	14
3.3.1	最適な μ の条件	15
3.3.2	最適な μ	17
3.3.3	考察	18
3.4	ランダム性を高める M 系列 $\mathbf{R}_2(n)$ の役割	18
第 4 章	CDMA における性能	20

目次

4.1	ビット誤り率	20
4.2	ランダム系列を PN 系列に用いた場合の BER 特性	20
4.3	時変 PN 系列の BER 特性	21
4.4	ランダム系列と時変 PN 系列の BER 特性比較	22
第 5 章	まとめ	24
5.1	結果のまとめ	24
5.2	今後の課題	24
謝辞		25
参考文献		26
付録 A	アダマール行列	27
A.1	アダマール行列の利用	27
A.1.1	アダマール行列の生成	27
A.1.2	アダマール行列を PN 系列に用いた場合の BER 特性	28

目次

2.1	CDMA の構成	3
2.2	直接拡散 (DS) 方式	4
2.3	DS-CDMA (Data A を受信)	4
2.4	3 段のシフトレジスタ回路	7
2.5	白色雑音	9
2.6	ノイズの分布	10
3.1	時変 PN 系列生成のシステム構成	12
3.2	符号長分の時変 PN 系列 (左:1 回目の生成 右:2 回目の生成)	13
3.3	符号長分の時変 PN 系列 (左:100 回目の生成 右:1000 回目の生成)	13
3.4	符号長分の時変 PN 系列 (左:正規化 右:正規化なし)	14
3.5	$\mu=100$ (左:種となる M 系列 右:時変 PN 系列)	15
3.6	$\mu=10^{-5}$ (左:初期値に関するベクトル 右:時変 PN 系列)	16
3.7	更新式における μ と秘話性の関係	16
3.8	R_{min}^2 となる μ の値	17
4.1	ランダム系列を用いた場合の BER 特性	21
4.2	時変 PN 系列を用いた場合の BER 特性	22
4.3	BER 特性 (左:ランダム系列 右:時変 PN 系列)	22
A.1	アダマール行列の各行を PN 系列に用いた CDMA の BER 特性	29

表目次

2.1 M 系列に関する資料	8
--------------------------	---

第 1 章

はじめに

1.1 研究の背景と目的

現在，携帯電話のアクセス方式等に用いられている符号分割多元接続 (code division multiple access: CDMA) では，各ユーザに特定時不変の擬似雑音 (pseudo noise: PN) 系列を割り当てて多元接続を実現している [1]．CDMA 方式は，他の多元接続の方法に比べると秘話性は高いが，まだまだ秘話性の向上の余地はあると考えられる．そこで，本論文では直接拡散 (direct sequence: DS) 方式に用いる PN 系列に着目した．従来の PN 系列は，+1 か-1 の値で系列を生成している．その系列をユーザごとに割り当てて多元接続を実現しているが，第三者に系列を一度知られてしまうと，その後の通信をすべて盗聴されてしまうことになる．そこで，各ユーザに割り当てる PN 系列を，時間と共に変化していく時変 PN 系列とすることで，盗聴され続けるといった問題を解決しようと考えた．本論文では，この時変 PN 系列の生成に取り組むこととする．

第 2 章

従来方式

2.1 符号分割多元接続

現在，多元接続の主な方法として，周波数分割多元接続 (frequency division multiple access: FDMA)，時分割多元接続 (time division multiple access: TDMA)，符号分割多元接続 (CDMA) などが挙げられる．符号分割多元接続では，各ユーザに特定の擬似雑音 (PN) 系列を割り当てて多元接続を実現している．ここでは，今回提案した時変 PN 系列を用いるために，まず符号分割多元接続について述べる．

2.1.1 符号分割多元接続とは

CDMA では，スペクトル拡散の技術により，1 チャンネルの周波数帯の幅を TDMA や FDMA に比べて広くする代わりに，1 つのチャンネルを TDMA や FDMA よりさらに多くのユーザで利用することができる．スペクトル拡散方式には，直接拡散方式 (DS 方式) と周波数ホッピング方式 (frequency hopping: FH 方式) がある．本論文においては直接拡散方式を用いることにする．直接拡散方式は，情報信号にスペクトル拡散なる操作をしてから送信し，受信側では逆拡散という操作を施す．スペクトル拡散・逆拡散は，情報信号に PN 系列を掛け合わせるという動作である．つまり，PN 系列が違っていれば，同一周波数，同一時間にいくつもの信号を送ることができるのである．

2.1 符号分割多元接続

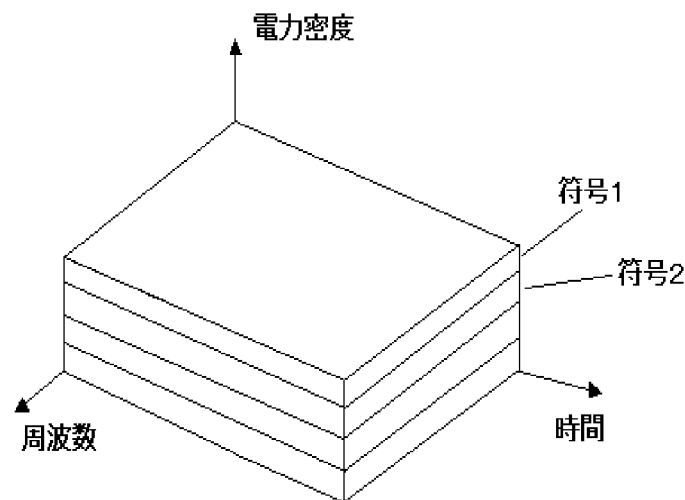


図 2.1 CDMA の構成

2.1.2 直接拡散方式

直接拡散方式 (DS 方式) とは、スペクトル拡散させるべき情報信号に、それより遥かに広帯域の信号を直接乗算させて、スペクトル拡散を実現する方式である。元の信号を復元させるには、スペクトル拡散を行った操作を逆に行えばよい。スペクトル拡散をするための信号は、広帯域信号でなければならないので、信号が変化する速度 (チップ速度) は、非常に高いことが要求される。更に、スペクトル拡散通信システムを構成するためには、多くのユーザ間で局認識ができる機能をもたなければならない。スペクトル拡散するための信号の条件としては、次のようなものがある [2]。

- 多くのユーザに信号が割り当てることができるように、信号の種類が多いこと
- 異なるユーザの信号とは区別がつくように相互相関が小さいこと
- 自局宛の信号を確実に捕えること (同期確立) ができるように、鋭い自己相関特性を持つこと
- 関係のない第三者に通信内容を傍受されないように、信号はできるだけランダムで周期が長く解読困難なこと

2.1 符号分割多元接続

このような条件を満足する符号として、最大周期 (maximum length: M) 系列や Gold 符号が利用される。直接拡散方式は、図 2.2 のように表現できる。

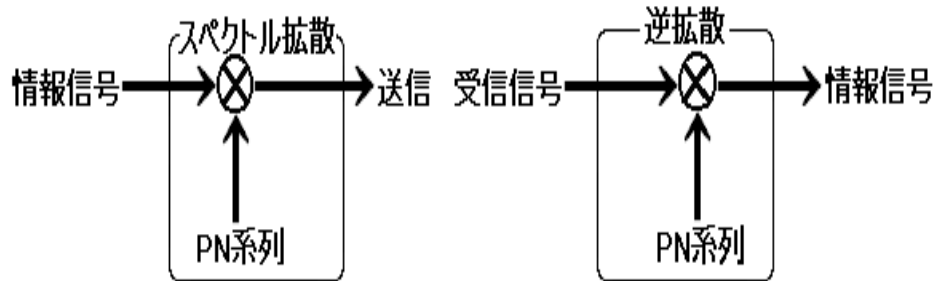


図 2.2 直接拡散 (DS) 方式

直接拡散方式において、例として 2 人で多元接続を行った場合、次のようなシステムになる。

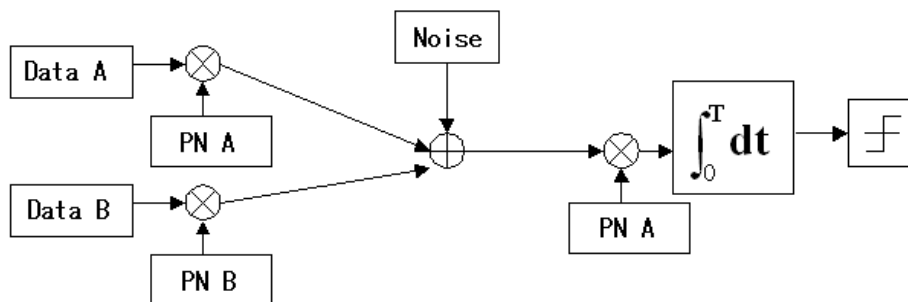


図 2.3 DS-SS-SSMA (Data A を受信)

図 2.3 は、DS-SS-SSMA 方式を用いた多元接続のシステムモデルである。このモデルではデータ A と B にスペクトル拡散を行い同時に送信し、スペクトル逆拡散をしてデータ A だけを取り出すシステムである。このモデルを数式で表す。今、図 2.3 におけるデータ A, B をそれぞれ d_1, d_2 と表し、PN 系列 A, B をそれぞれ $\mathbf{PN}_1(i), \mathbf{PN}_2(i)$ と表すことにする。DS-SS-SSMA において、 $\mathbf{PN}_1(i)$ を用いて多元接続を行ったユーザが、受信をする場合は次のような式になる。

2.1 符号分割多元接続

$$\sum_{i=1}^L (d_1 \mathbf{PN}_1(i) + d_2 \mathbf{PN}_2(i)) \times \mathbf{PN}_1(i) \quad (2.1)$$

ここで、 L は PN 系列の系列長である。式 (2.1) は多元接続によって送られてきた d_1 を求める式と言える。この式をさらに変形すると、式 (2.2) のようになる。

$$\sum_{i=1}^L (d_1 \mathbf{PN}_1(i) \mathbf{PN}_1(i) + d_2 \mathbf{PN}_2(i) \mathbf{PN}_1(i)) \quad (2.2)$$

また式 (2.2) は、

$$\sum_{i=1}^L d_1 \mathbf{PN}_1(i) \mathbf{PN}_1(i) + \sum_{i=1}^L d_2 \mathbf{PN}_2(i) \mathbf{PN}_1(i) \quad (2.3)$$

となる。ここで注目して欲しい点は、 $\sum_{i=1}^L \mathbf{PN}_1(i) \mathbf{PN}_1(i)$ と $\sum_{i=1}^L \mathbf{PN}_2(i) \mathbf{PN}_1(i)$ である。これらは、PN 系列同士の相関をとった形となっている。つまり、 $\sum_{i=1}^L \mathbf{PN}_1(i) \mathbf{PN}_1(i)$ の相関は同じ PN 系列同士の相関であるので、その相関値は得られる値の最高値でもある系列長 L となる。逆に、 $\sum_{i=1}^L \mathbf{PN}_2(i) \mathbf{PN}_1(i)$ は、それぞれの PN 系列によって、相関の値は変化してくるが、打ち消され合うため同じ PN 系列同士の相関値より大きくなることはない。つまり、直接拡散方式においては、異なった PN 系列で逆拡散した場合、PN 系列同士で打ち消し合いが生じ、逆拡散したデータは非常に小さい値となる。すなわち、適切な PN 系列を用いて逆拡散した場合のみ、大きな相関値が得られ、その値の正負によって、データを復元できることになる。つまりほとんど式 (2.4) になると考えられる。

$$\sum_{i=1}^L d_1 \mathbf{PN}_1(i) \mathbf{PN}_1(i) \quad (2.4)$$

ここで、得られた値の正負を判断し、データを復元することになる。

2.2 擬似雑音系列

PN 系列は、スペクトル拡散に使用される符号として重要である。この符号は、Pseudo-random Noise の頭文字をとって命名されたもので、その名が示すようにランダム雑音のような性質を持つ。PN 系列の発生過程は確定的であり、ランダムではない。PN 系列は、平衡性 (balance property), 連なり性 (run property), 相関性 (correlation) というランダム性の性質を満足する符号と、定義することができる。PN 系列には、M 系列, 平方剰余系列 (quadratic residue sequence), 双素数系列 (twin-prime sequence), そしてホール系列 (hall sequence) 等があることが知られている。この中で、M 系列は上記の性質を満足する。本論文においても、M 系列を用いた。

2.2.1 M 系列の性質

代表的な PN 系列として、今回は M 系列を取り上げる。M 系列は、0, 1 の数値を発生させる系列である。M 系列の性質を述べると、

- 2 値において 0 の数は 1 の数と 1 つだけ異なる。
- 0 または 1 がそれぞれ連続して現れる確率が乱数とほぼ同じ。
- 電力スペクトル分布が熱雑音と同じ。
- M 系列の自己相関の波形はインパルス関数によく似ている。

2.2.2 M 系列の生成

M 系列は、帰還シフトレジスタの出力を合成することによって発生される。帰還シフトレジスタは 2 値の状態メモリ、すなわち蓄積段とフィードバック演算からなる。例として、シフトレジスタの段数が 3 段の場合の M 系列の生成について述べる。

図 2.4 は 3 段シフトレジスタを表している。出力までの過程を述べると、

- x_1, x_2, x_3 のそれぞれのレジスタに初期値 1 が入っていると考える。

2.2 擬似雑音系列

- XOR は排他的論理和 (exclusive or) である. 排他的論理和は 2 値を比較し, 2 値が等しいならば 0 を返し, 等しくないならば 1 を返す. 矢印が 2 本 XOR 素子に向かっているが, ここでは x_1 と x_3 の値を比較し, x_1 に結果を送っている.
- XOR 素子から x_1 に値が送られる前に, x_1, x_2, x_3 は右シフトし, x_3 の値が出力される.

これが 3 段シフトレジスタの原理である. レジスタ長を大きくすることにより, 用いる帰還タップなど変わり, 生成できる M 系列の数や周期が増える性質をもつ.

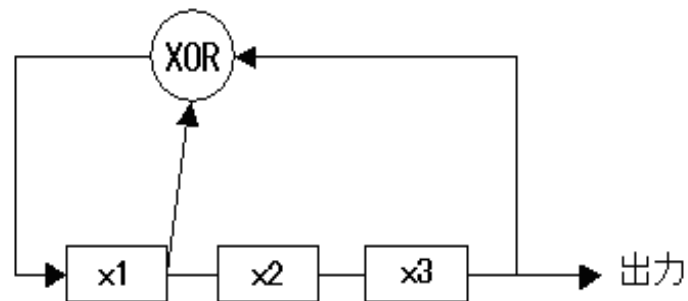


図 2.4 3 段のシフトレジスタ回路

表 2.1 は M 系列に関する資料である [2]. M 系列生成の一例として, シフトレジスタの段数と M 系列の周期, 周期の素因数分解, M 系列の数, そして, M 系列発生のためのシフトレジスタの帰還タップの位置を示す.

2.3 ノイズとは

表 2.1 M 系列に関する資料

次数	周期	周期の素因数分解	M 系列の数	代表的な帰還タップ
2	3		1	(1,2)
3	7		2	(1,3)
4	15	$3 \cdot 5$	2	(1,4)
5	31		6	(2,5)(2,3,4,5)(1,2,4,5)
6	63	$3^2 \cdot 7$	6	(1,6)(1,2,5,6)(2,3,5,6)
7	127		18	(3,7)(1,2,3,7)(1,2,4,5,6,7)(2,3,4,7)
8	255	$3 \cdot 5 \cdot 17$	16	(2,3,4,8)(3,5,6,8)(2,5,6,8)(1,3,5,8)
9	511	$7 \cdot 73$	48	(4,9)(3,4,6,9)(4,5,8,9)(1,4,8,9)
10	1023	$3 \cdot 11 \cdot 31$	60	(3,10)(2,3,8,10)(1,5,8,10)(1,3,4,10)
11	2047	$23 \cdot 89$	176	(1,11)(2,5,8,11)(2,3,7,11)(2,3,5,11)
12	4095	$3^2 \cdot 5 \cdot 7 \cdot 13$	144	(1,4,6,2)(2,3,9,12)(1,2,5,10,11,12)

2.3 ノイズとは

CDMA に限らず通信を行うにあたって、受信信号に雑音 (ノイズ) が混入してくる。雑音には、人工的に生成される人工雑音と、自然現象などにより生じる自然雑音がある。移動体通信において使用する帯域においては、人工雑音が最も主要な雑音である。通信における雑音は当然のように存在し雑音を除外する事は難しい。このことを踏まえ、本論文においても雑音の影響を考えるために、雑音電力について検討する。

2.3.1 ノイズの導出

今回、直接拡散方式を行った際に生じる雑音電力を次のように導出した。

生成する雑音は、 SN 比から求める。 SN 比とは信号電力 (Signal Power) と雑音電力

2.3 ノイズとは

(Noise Power) の比である. 雑音電力 N は電力密度 $N_0/2$ [W/Hz] をもつ白色ガウス雑音 (電力密度が一定値) とする [4].

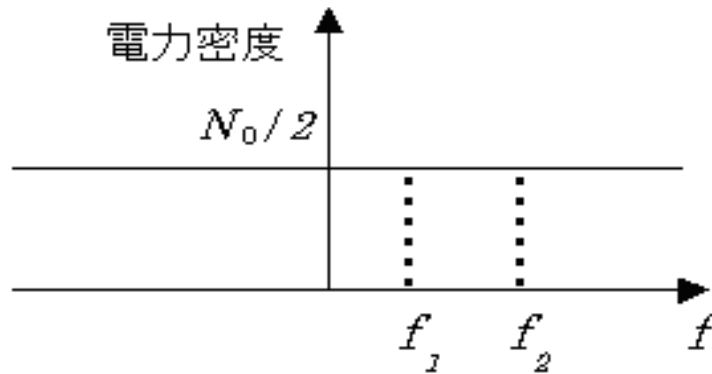


図 2.5 白色雑音

マッチドフィルタの理論を用いて E_c (1 チップあたりのエネルギー) [J] により SN 比を表現すると

$$\frac{S}{N} = \frac{2E_c}{N_0} \quad (2.5)$$

になる. さらに E_c は

$$E_c = \frac{E_b}{L} \quad (2.6)$$

と置き換えることができる. ここで

- E_b はビットあたりのエネルギー [J]
- L は PN 系列の系列長

また式 (2.6) を式 (2.5) に代入することにより

$$\frac{S}{N} = \frac{2E_b}{LN_0} \quad (2.7)$$

とする. 式 (2.7) を変形して N を求める.

$$N = \frac{SLN_0}{2E_b}$$

2.3 ノイズとは

$$N = \frac{S}{2 \frac{E_b}{LN_0}}$$

$$N = \frac{SL}{2 \frac{E_b}{N_0}} \quad (2.8)$$

式(2.8)から雑音電力 N を導くことができる。シミュレーションでは信号電力の大きさに1を用いる。そしてチップ長 L は、本論文においては8とした。

よって、 E_b/N_0 を決めることにより、雑音の大きさが決まる。

$$\frac{E_b}{N_0} [dB] = 10 \log(\alpha) \quad (2.9)$$

式(2.9)は対数なので、変形すると

$$\alpha = 10^{\frac{E_b/N_0}{10} [dB]} \quad (2.10)$$

となる。雑音には、平均が0で標準偏差が1の正規乱数を使用し、これに \sqrt{N} を掛けることで電力 N のガウス雑音とすることができる。

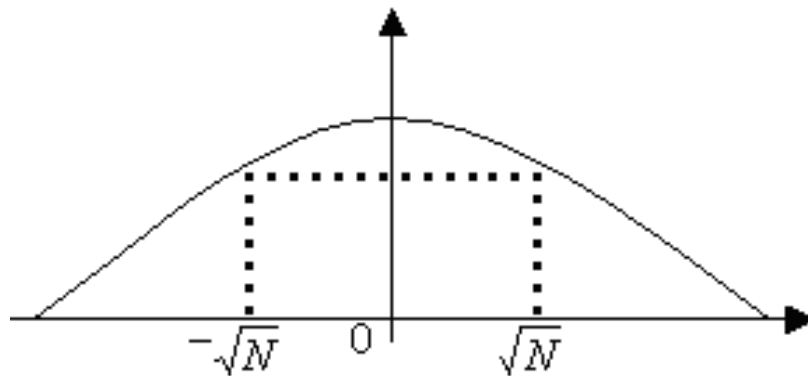


図 2.6 ノイズの分布

第 3 章

時変 PN 系列

3.1 時変 PN 系列とは

時変 PN 系列とは，直接拡散方式に用いられる PN 系列の秘話性をさらに向上させるために，PN 系列を時間的に変化させる方法である．時変 PN 系列を CDMA に用いることによって，拡散符号を他人に読み取られる可能性は大幅に減少させることが可能になる．

3.2 時変 PN 系列の生成

本論文では，時変 PN 系列の生成に，最大周期系列 (M 系列) と LMS アルゴリズム [3] の考え方を応用する．まず周期の長い M 系列を用意し，想定する CDMA の符号長 L ごとに区切ったベクトル $\mathbf{r}_1(n)$ を生成する．これを種ベクトルとして時変 PN 系列の生成に用いる．LMS アルゴリズムの考えを応用した時変 PN 系列の更新 (update) 部において，種となる M 系列 $\mathbf{r}_1(n)$ が符号長分ずつ時変 PN 系列の各要素として変化していく．図 3.1 は時変 PN 系列生成のシステム構成である．時変 PN 系列の更新部における時変 PN 系列の生成には式 (3.1) の演算を行う．

$$\mathbf{c}'(n+1) = \mathbf{c}(n) \otimes \mathbf{r}_2(n) + \mu \mathbf{e}(n) \mathbf{r}_1(n) \quad (3.1)$$

ここで，図 3.1 や式 (3.1) 中の \otimes は，ベクトルの要素積を意味する． $\mathbf{r}_1(n)$ は種となる M 系列である． $\mathbf{r}_1(n)$ とは異なる別の M 系列で生成したベクトル $\mathbf{r}_2(n)$ を用意し，時変 PN 系列のランダム性を高めるために用いる． μ は本論文においては，更新ゲイン (Update Gain) と呼ぶ．また，式 (3.1) で生成された時変 PN 系列 $\mathbf{c}'(n+1)$ を二乗平均値が 1 と

3.2 時変 PN 系列の生成

なるよう正規化することによって、時変 PN 系列 $c(n+1)$ が生成される。時変 PN 系列の正規化については、次項で説明する。このようにして、時変 PN 系列が符号長分ずつ $c(n+1), c(n+2), c(n+3), \dots$ と順次生成されていく。

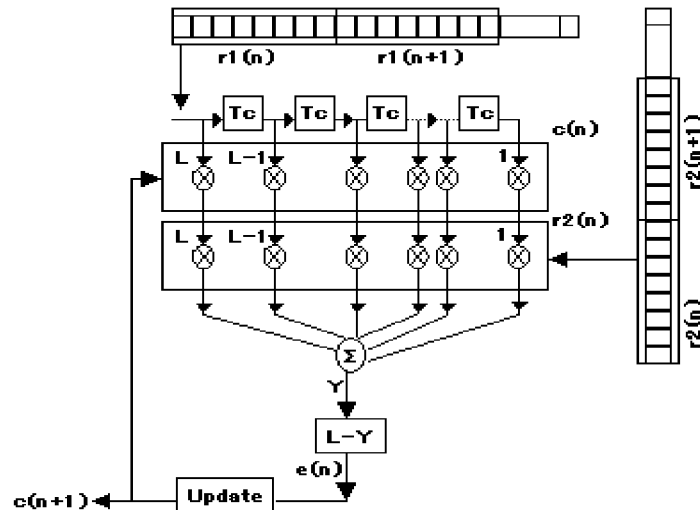


図 3.1 時変 PN 系列生成のシステム構成

符号長分ごとの時変 PN 系列を図 3.2, 図 3.3 に示した。図 3.1 のシステムによって、符号長分ずつ時変 PN 系列が生成され、その各要素値は、次々と変化しているのが分かる。これまでの CDMA のように、1 つの PN 系列を知るだけでは、盗聴は不可能である。また、変化する系列を、送信側と受信側が順次生成していくため、時変 PN 系列を盗聴したり生成することは限りなく不可能に近い。

今回、時変 PN 系列生成のために用いた 2 種類の M 系列の初期値と帰還タップ、時変 PN 系列の初期値、更新ゲイン μ には次のものを用いるとする。

- 種となる M 系列 r_1 の初期値: $[-1 \ 1 \ 1 \ 1 \ -1 \ -1 \ 1 \ 1 \ 1 \ 1]$
 使用した帰還タップ: (3,10)
- ランダム性を高める M 系列 r_2 の初期値: $[-1 \ -1 \ 1 \ -1 \ 1 \ 1 \ 1 \ -1 \ 1 \ 1]$
 使用した帰還タップ: (2,3,8,10)
- 使用した更新ゲイン: $\mu = 0.03$

3.2 時変 PN 系列の生成

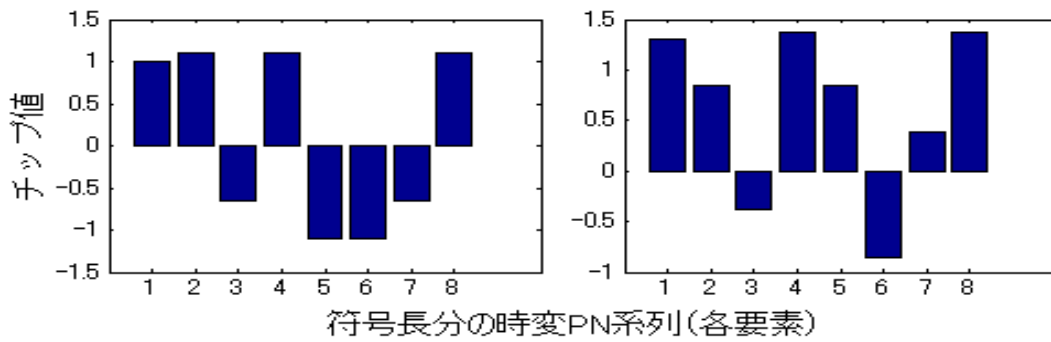


図 3.2 符号長分の時変 PN 系列 (左:1 回目の生成 右:2 回目の生成)

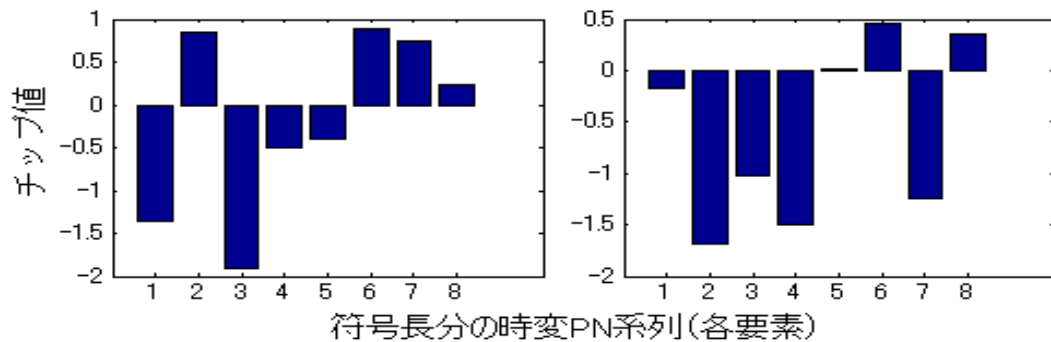


図 3.3 符号長分の時変 PN 系列 (左:100 回目の生成 右:1000 回目の生成)

3.2.1 時変 PN 系列の正規化

時変 PN 系列の正規化とは，時変 PN 系列生成のシステムによって生成された，符号長分ずつの時変 PN 系列の電力を 1 にするために行う．今回，更新部で生成された時変 PN 系列 $\mathbf{c}'(n+1)$ の 2 乗和が符号長の値になることを正規化とする．本論文においては，符号長を 8 とする．式 (3.2) は時変 PN 系列の正規化に用いる式である．

$$\mathbf{c}(n+1) = \frac{\sqrt{N}}{\sqrt{\sum_{i=1}^N \mathbf{c}_i'(n+1)^2}} \cdot \mathbf{c}'(n+1) \quad (3.2)$$

式 (3.2) における $\mathbf{c}_i'(n+1)$ は，式 (3.1) で生成された時変 PN 系列の各要素の i 番目を意味する．式 (3.2) によって，順次生成される時変 PN 系列 $\mathbf{c}(n+1), \mathbf{c}(n+2), \dots$ すべてにおいて，2 乗和が符号長 8 となる．したがって，電力は常に 1 である．図 3.4 は，正規化を行っている時変 PN 系列と正規化を行っていない時変 PN 系列の各要素のグラフを表したもの

3.3 時変 PN 系列における最適な μ

である.

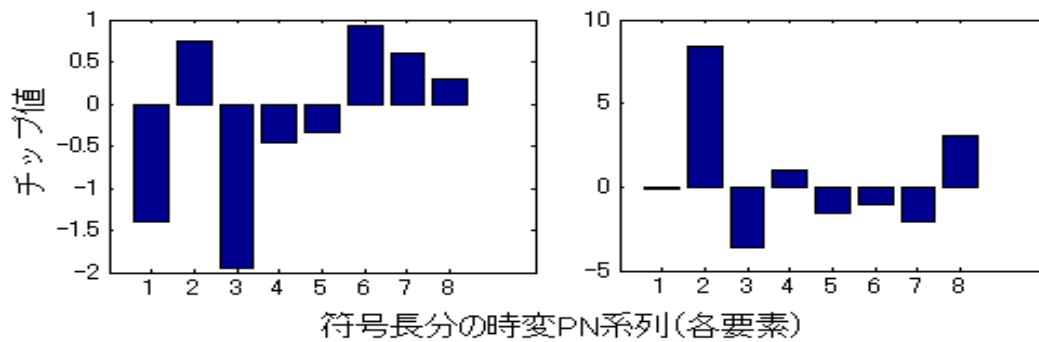


図 3.4 符号長分の時変 PN 系列 (左:正規化 右:正規化なし)

正規化を行っていない時変 PN 系列は, 系列のチップ値ごとにかんがりのばらつきがあり, 図 3.4 においては, 生成された時変 PN 系列の各チップ値の 2 乗和は 101.4571 となっている. また, それぞれの生成される時変 PN 系列によって, 各チップ値の 2 乗和の値が変化していつている. しかし, 正規化を行った時変 PN 系列であれば, 生成された時変 PN 系列の各チップ値の 2 乗和は常に符号長 8 となる.

3.2.2 考察

本論文で提案した生成法を用いて, 時変 PN 系列を生成した. また, 時変 PN 系列の 2 乗平均を 1 とするために正規化を行った. そこで, 生成される PN 系列がどのように変化していくのかを次項で考えたい.

3.3 時変 PN 系列における最適な μ

理想的な時変 PN 系列を生成するには, 更新式 (式 (3.1)) における更新ゲイン μ の値が重要になってくる. 時変 PN 系列の生成において種となる M 系列 $\mathbf{r}_1(n)$, 時変 PN 系列生成の初期値 $\mathbf{c}(0)$, 時変 PN 系列のランダム性を高めるために用いる M 系列 $\mathbf{r}_2(n)$ は, ユーザによって異なっている. また, 送信側と受信側が共有しなければならない情報でもある.

3.3 時変 PN 系列における最適な μ

この 3 種類の系列は，送信側と受信側の秘密情報でもあるので，なるべく他人に知られないようにしたい．すなわち，生成される時変 PN 系列の各要素の値が，できるだけこの 3 種類の系列からかけ離れている系列にすることが必要だと考えられる．そのために， μ の値を調整し，最適な時変 PN 系列を生成する．

3.3.1 最適な μ の条件

μ の最適値を決めるにあたっての条件を調べた．仮に μ が非常に小さい値ならば，生成される時変 PN 系列は $\mathbf{c}(0) \otimes \mathbf{r}_2(n)$ からなかなか変化しない．逆に， μ の値が非常に大きいならば，生成される時変 PN 系列は種となる M 系列 $\mathbf{r}_1(n)$ からなかなか変化しなくなる．すなわち，小さすぎず，かつ大きすぎない μ の値が存在すると予想できる．

例として， μ の値を非常に大きくした場合と，非常に小さくした場合に時変 PN 系列がどのような影響を受けるかを確認してみた．確認方法として，まず μ が非常に大きい場合を想定し， $\mu = 100$ を用いて時変 PN 系列の生成にあたる．時変 PN 系列はランダムな生成回数を選び (図 3.5 では 10 回目)，種となる M 系列と比較した．図 3.5 は生成時の種となる M 系列と時変 PN 系列のチップ値である．両方のグラフを比べると，チップ値には多少違いは見られるが，系列の正負は全く同じ特性を持っている．

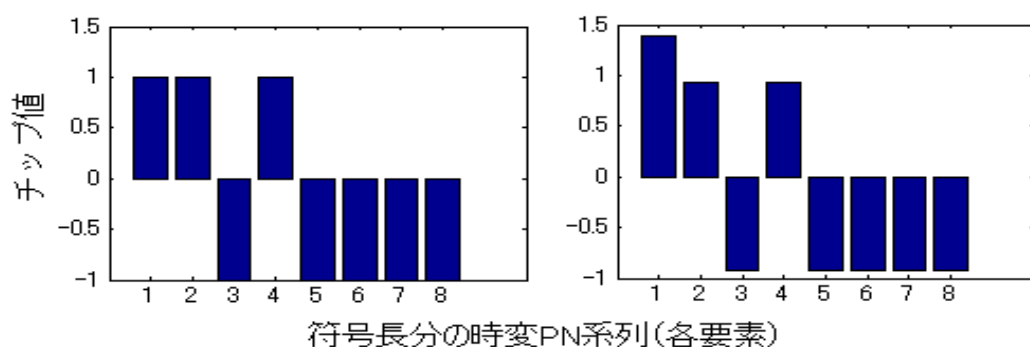


図 3.5 $\mu = 100$ (左:種となる M 系列 右:時変 PN 系列)

次に， μ が非常に小さい場合を想定し， $\mu = 10^{-5}$ を用いて時変 PN 系列の生成にあたった．図 3.6 は初期値に関するベクトルと時変 PN 系列のチップ値を比較したものである．両

3.3 時変 PN 系列における最適な μ

方のグラフを比べると、生成された時変 PN 系列は、初期値に関するベクトルと同じような系列になっていることがわかる。

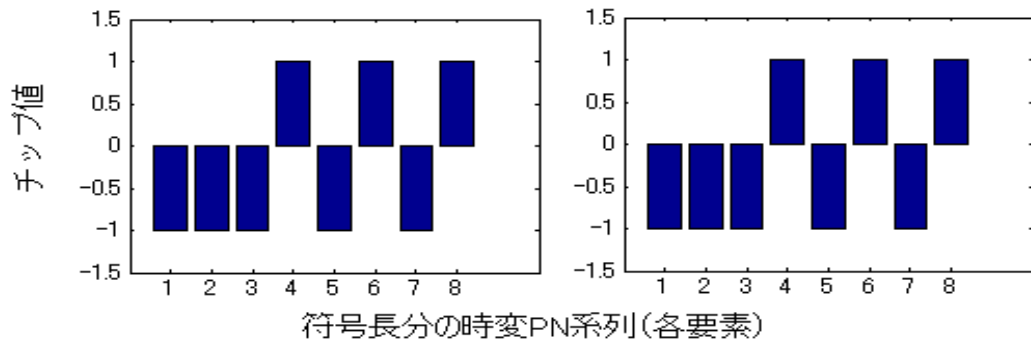


図 3.6 $\mu = 10^{-5}$ (左:初期値に関するベクトル 右:時変 PN 系列)

上記より、 μ は大きすぎず、小さすぎない値を選ばなければいけないことを確認した。すなわち、時変 PN 系列の生成にあたっては、種となる M 系列 $\mathbf{r}_1(n)$ との相関 $\mathbf{R}_1(\mu)$ と初期値に関するベクトル $\mathbf{c}(0) \otimes \mathbf{r}_2(n)$ との相関 $\mathbf{R}_2(\mu)$ がバランスする μ を選べば、時変 PN 系列は、初期値に関するベクトルから離れ、なおかつ種となる M 系列からも離れた系列になっていると考える。したがって、更新式における μ の値と秘話性について次のような関係が成り立つ。

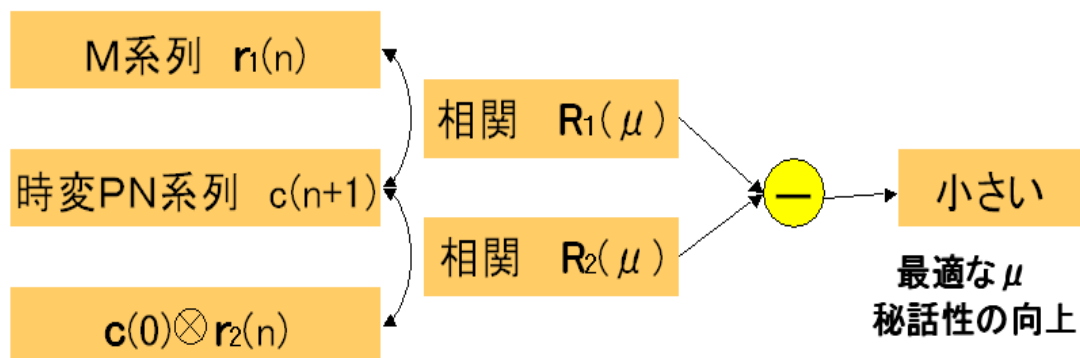


図 3.7 更新式における μ と秘話性の関係

3.3 時変 PN 系列における最適な μ

3.3.2 最適な μ

図 3.7 の考え方を式に表した. 式 (3.3) は相関の 2 乗値の差が最小になる場合の μ を求めるための式である. 式 (3.3) において, $\mathbf{R}^2(\mu)$ が最小値 R_{min}^2 となる μ が望ましい.

$$\mathbf{R}^2(\mu) = |\mathbf{R}_1^2(\mu) - \mathbf{R}_2^2(\mu)| \rightarrow R_{min}^2 \quad (3.3)$$

式 (3.3) によって, $\mathbf{R}^2(\mu)$ が最小値 R_{min}^2 となる μ を求め, 時変 PN 系列の繰り返し回数ごとにまとめたものが図 3.8 である.

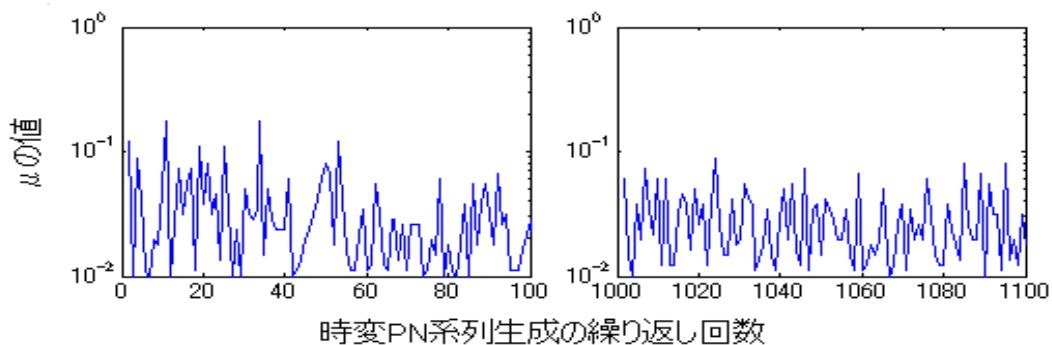


図 3.8 R_{min}^2 となる μ の値

図 3.8 より, 時変 PN 系列を生成するたびに, R_{min}^2 の得られる μ の値は変化していく結果を得た. つまり時変 PN 系列を生成するたびに, 望ましい時変 PN 系列を生成するための μ の値が変わっていくということになる. そこで, 本論文においては, これらの μ の平均値を μ の最適値とする. 平均値をとるために, 時変 PN 系列の生成を今回は 1000 回繰り返すことにした. 繰り返し回数ごとの R_{min}^2 となる μ を導出し, その平均を求めることにする. 結果として, $\mu \doteq 0.03$ が最適値となった.

時変 PN 系列の生成に最適な μ を求める理由は, 前にも述べたように, 時変 PN 系列を種となる M 系列やランダム性を高めるための M 系列, 時変 PN 系列の初期値から離れた系列に変化させるためである. しかし先程の結果より, 最適な μ の値は時変 PN 系列を生成するたびに変化していくという結果が得られた. それならば時変 PN 系列の生成を行うたびに, 変化していく μ の値を用いれば良いと考えられるが, 常に最適な μ の値を用いること

3.4 ランダム性を高める M 系列 $\mathbf{R}_2(n)$ の役割

も時変 PN 系列の秘話性を落としていることになってしまう。なぜならば、最適な μ を用いることで、生成される時変 PN 系列が、種となる M 系列と初期値に関するベクトルの中間をとる系列になってしまうからである。つまり、もし第三者に種となる M 系列と初期値に関するベクトルを知られてしまった場合、更新ゲイン μ の値に関わらず時変 PN 系列を生成することが可能となってしまうのである。このようなことを避けるために、最適な μ の平均をとって時変 PN 系列の生成に用いている。生成される時変 PN 系列は、種となる M 系列と初期値に関するベクトルの中間付近の値になるが、生成するたびに種となる M 系列に近づいたり、初期値に関するベクトルに近づいたりするので、盗聴の可能性は低くなる。

3.3.3 考察

時変 PN 系列生成における更新式の μ の重要性を確認した。最適な μ の値を求めることで、時変 PN 系列はそれぞれの初期値から離れた系列になる。しかし常に最適な μ を使い続けることは、種となる M 系列と初期値に関するベクトルの中間値となってしまう。すなわち μ の意味がなくなってしまう、系列の秘話性を落とすことになるので、最適な μ に近い値を用いることで通信の秘話性を上げている。 μ は時変 PN 系列の変化の度合いを定めるパラメータといえる。

3.4 ランダム性を高める M 系列 $\mathbf{R}_2(n)$ の役割

時変 PN 系列の生成や、生成に用いる更新式の最適な μ を求めるにあたって、時変 PN 系列のランダム性を高めるために用いている M 系列 $\mathbf{R}_2(n)$ は、大きな影響力を持つ。前項において、最適な μ の値を求めることができたが、この導出には M 系列 $\mathbf{R}_2(n)$ が関係している。本論文においても、当初は M 系列 $\mathbf{R}_2(n)$ を時変 PN 系列生成のシステム構成に用いていなかった。しかし、M 系列 $\mathbf{R}_2(n)$ を用いないと R_{min}^2 の得られる μ の値は、生成回数を増やすにつれて、だんだん小さくなっていく。つまり、 R_{min}^2 の得られる μ の値が 0 に収束していくことになる。 μ の値が 0 に収束していくということは、もし時変 PN 系列の生

3.4 ランダム性を高める M 系列 $\mathbf{r}_2(n)$ の役割

成に用いている μ の値が小さければ、生成される時変 PN 系列は、繰り返し回数を増やすにつれて、前回に生成した符号長分ずつの時変 PN 系列からあまり変化が見られなくなる。時変 PN 系列の変化が減少していくことは、長時間 CDMA において通信を行っていくにつれ、時変 PN 系列を用いた CDMA の秘話性が失われていくということになってしまう。また、時変 PN 系列の生成に、LMS アルゴリズムの考え方を利用しているということも時変 PN 系列のランダム性を失わせる原因となった。LMS アルゴリズムとは、本来は 2 乗平均誤差を最急降下法に基づいて最小にするための方法である。ランダム性を高めるための M 系列 $\mathbf{r}_2(n)$ を用いていなかった場合、時変 PN 系列の更新式は次のようになる。

$$\mathbf{c}'(n+1) = \mathbf{c}(n) + \mu \mathbf{e}(n) \mathbf{r}_1(n) \quad (3.4)$$

式 (3.4) においても、 μ の値が小さいと時変 PN 系列は、前回に生成した符号長分ずつの時変 PN 系列からあまり変化しなくなる。

この時変 PN 系列のランダム性を失わせる原因を解決するために、M 系列 $\mathbf{r}_2(n)$ を用いる。更新部によって生成され、正規化を行った時変 PN 系列が、次の時変 PN 系列生成時で更新部の重み $\mathbf{c}(n)$ となったときに、 $\mathbf{c}(n)$ と M 系列 $\mathbf{r}_2(n)$ の要素積を求めて、更新部における重みをランダム値にすることで、時変 PN 系列の生成を繰り返しても、生成される時変 PN 系列 $\mathbf{c}(n+1)$ は常に、ランダム性を失わない系列となる。

第 4 章

CDMA における性能

4.1 ビット誤り率

ビット誤り率 (bit error rate: BER) とは、送信データが受信されたときに、どのくらいの割合で誤っているかを示すものである。つまり、誤って受信した信号の全信号に対する割合である。ビット誤り率の求め方は、

$$\text{ビット誤り率} = \text{誤ったビット数} / \text{送信ビット数} \quad (4.1)$$

である。CDMA の 1 ユーザ時のビット誤り率は、ビットあたりのエネルギーに対する雑音電力密度比 (E_b/N_0) が 6.8dB の場合、 10^{-3} となる。ビット誤り率を求めるシミュレーションを次のように設定した。

- 直接拡散方式で、1 つのデータを拡散する PN 系列の系列長を 8 とする。
- ビット誤り率を求めるにあたって、送信データと受信データが 1000 回誤るまでシミュレーションを行う。
- 多元接続のビット誤り率を調べるために、ユーザ数を 1 ~ 3 人とする。

4.2 ランダム系列を PN 系列に用いた場合の BER 特性

従来の直接拡散方式における PN 系列を想定して、ランダム系列を PN 系列に用いて BER 特性を求めてみた。ランダム系列は、+1,-1 の値をランダムに並べた系列である。ランダム系列を PN 系列に用いることによって、実在する各 PN 系列を用いての BER 特性の平均値を求めることが可能となる。ランダム系列を PN 系列に用いた場合の CDMA におけ

4.3 時変 PN 系列の BER 特性

る BER 特性は次のようになった。

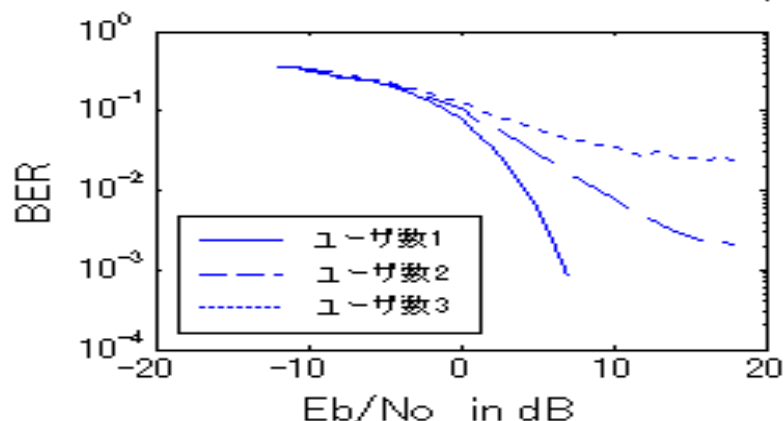


図 4.1 ランダム系列を用いた場合の BER 特性

4.3 時変 PN 系列の BER 特性

直接拡散方式における PN 系列に，本論文で提案した時変 PN 系列を用いて，BER 特性を求めた．時変 PN 系列生成における，2 種類の M 系列の初期値，時変 PN 系列生成の初期値，更新式における μ の値は次のように設定した．

- ユーザ 1 の種となる M 系列の初期値: [-1 1 1 1 -1 -1 1 1 1 1]
- ユーザ 2 の種となる M 系列の初期値: [1 1 -1 1 -1 -1 1 1 -1 -1]
- ユーザ 3 の種となる M 系列の初期値: [-1 1 -1 1 1 1 1 1 -1 1 1]
- ユーザ 1 の時変 PN 系列のランダム性を高める

M 系列の初期値: [-1 -1 1 -1 1 1 1 -1 1 1]

- ユーザ 2 の時変 PN 系列のランダム性を高める

M 系列の初期値: [-1 1 -1 1 -1 1 1 1 -1 1]

- ユーザ 3 の時変 PN 系列のランダム性を高める

M 系列の初期値: [1 -1 -1 -1 -1 1 1 1 1 -1]

- ユーザ 1 の時変 PN 系列生成の初期値: [1 1 -1 1 -1 -1 -1 1]

4.4 ランダム系列と時変 PN 系列の BER 特性比較

- ユーザ 2 の時変 PN 系列生成の初期値: [1 -1 -1 1 -1 1 -1 1]
- ユーザ 3 の時変 PN 系列生成の初期値: [-1 1 -1 -1 1 -1 1 1]
- 更新式における μ の値: $\mu=0.03$

上記の値を用いて、時変 PN 系列での多元接続による BER 特性を求めた。

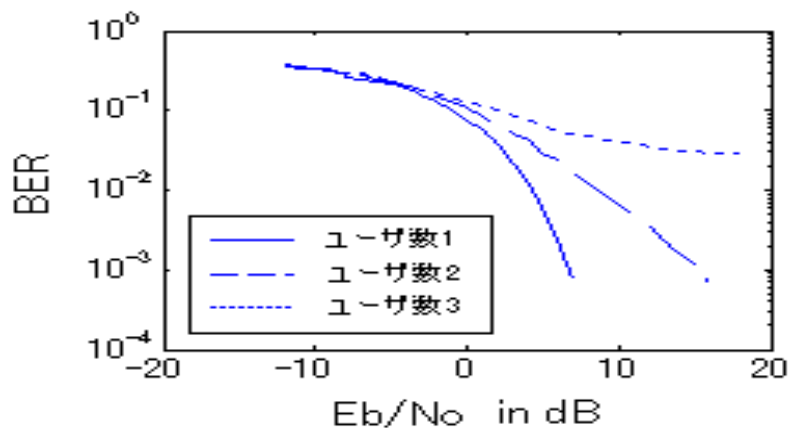


図 4.2 時変 PN 系列を用いた場合の BER 特性

4.4 ランダム系列と時変 PN 系列の BER 特性比較

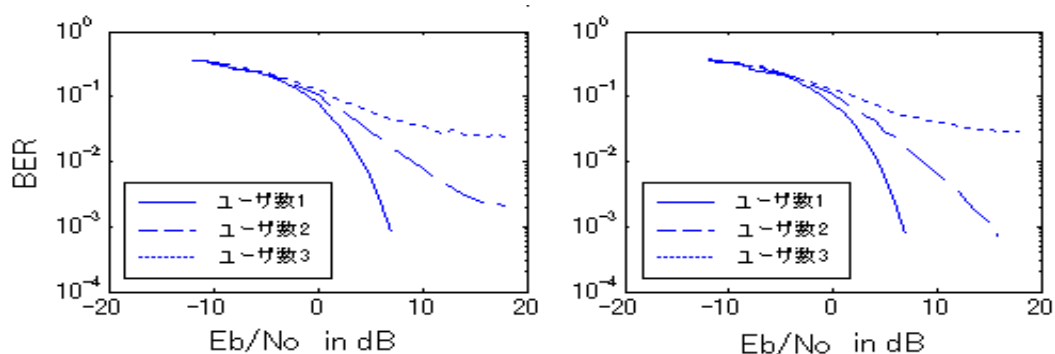


図 4.3 BER 特性 (左:ランダム系列 右:時変 PN 系列)

図 4.3 は CDMA に用いる PN 系列として、ランダム系列及び時変 PN 系列をそれぞれ用いた場合の BER 特性の比較である。ランダム系列の BER 特性は、それぞれの系列に対す

4.4 ランダム系列と時変 PN 系列の BER 特性比較

る平均であるが、時変 PN 系列の BER 特性は、2 種類の M 系列、時変 PN 系列生成の初期値、更新ゲインに特定の初期値を用いた場合の特性となっている。実際のところ、何回か初期値を変更して BER 特性の導出を試みてみたところ、多少のずれはあるものの図 4.3 の右図とほぼ同じ特性を持つ結果を得た。すなわち、時変 PN 系列を用いた CDMA は、ランダム系列を用いた CDMA と、ほぼ同じビット誤り率特性を持つことが確認できる。この結果を得ることにより、時変 PN 系列を CDMA に用いることによる、CDMA の BER 特性に与える影響はほぼないと考えられる。つまり、BER 特性を保ったまま PN 系列の秘話性を向上させることが可能になった。

第 5 章

まとめ

5.1 結果のまとめ

本論文では，時変 PN 系列を提案し，系列生成過程における μ の最適値，多元接続をした際の CDMA の性能を調べた．その結果，時変 PN 系列生成に用いる最適な μ を $\mu \doteq 0.03$ と得た．また時変 PN 系列を用いることで，ランダム系列とほぼ等しい BER 特性を持ちながら，秘話性を向上させることが可能になった．

5.2 今後の課題

従来の PN 系列においても，CDMA による多元接続を行った際に，ユーザ数 1 の BER 特性と同じ特性を持たせることは難しいと言われている．原理的には，ユーザごとに割り当てられる PN 系列に直交性を持たせることによって，互いの PN 系列が干渉なくなり，BER 特性の向上は可能ではある．しかし，移動局から基地局への上りチャンネルにおいては，各ユーザが発信するタイミングが異なるため，PN 系列の同期がずれる．たとえ PN 系列が直交していたとしても，系列同期が失われると直交性を持つことはできない．そこで，今後の課題としては，このような直交性の問題を解決できる PN 系列の生成を考案し，その考えを時変 PN 系列に取り入れることで，時変 PN 系列のビット誤り率特性をさらに向上させていきたい．

謝辞

本論文の作成にあたり、一年間ご指導をしてくださいました濱村昌則講師に深く感謝いたします。また、一年間共に研究を進めてきた濱村研究室のみなさんお世話になりました。研究室のPCの面倒をいつも見てくれたネットワーク担当の三好君。PCの設定など環境設定を助けてくれてありがとうございました。また、研究室でご飯を食べてばかりの遠藤君。研究が行き詰まった時にあなたとご飯を食べる事でやる気を起こさせてもらった気がします。また、3年生なのに、私より研究室の滞在時間が多かったのではないのでしょうか？高橋君。いつも喋ってばかりでごめんなさい。渋い声を響かせていた山川君、研究等手伝ってくれてありがとう。隣の席の仙頭君、質問にまともに答えてあげられなくてごめんなさい。あと枝広君、佐藤君、室津君、ゼミの時間にわたしのわけのわからない講義を聞いてくれてありがとう。3年生のみなさん、これからがんばって研究を進めてください。最後に、同じ部屋で共に研究を進めてきた任研究室のみなさん、一年間ありがとうございました。

参考文献

- [1] ガルグスマリックウィルクス, “CDMA セルラー移動体通信システム”, 科学技術出版, 2001
- [2] 横山光雄, “スペクトル拡散通信システム”, 科学技術出版社, 1988
- [3] サイモン ハイキン, “適応フィルタ入門”, 現代工学社, 1987
- [4] ラシイ著, “通信方式”, マグロウヒルブック株式会社, 1977

付録 A

アダマール行列

A.1 アダマール行列の利用

今後の課題として PN 系列の直交性を取り上げたが，CDMA における各ユーザが同じタイミングで通信を行った場合に限ると，アダマール行列 (Hadamard matrix) の各行を PN 系列として利用することにより，PN 系列に直交性を持たせることが可能になる．この PN 系列を用いて多元接続を行えば，理想的なビット誤り率を持った通信を行うことができる．一例として，アダマール行列の各行を PN 系列として用いた場合の CDMA 性能を調べる．

A.1.1 アダマール行列の生成

アダマール行列は以下のように定義される．要素は+1 と-1 で表す．

$$\mathbf{H}_k = \begin{bmatrix} \mathbf{H}_{k-1} & \mathbf{H}_{k-1} \\ \mathbf{H}_{k-1} & \overline{\mathbf{H}_{k-1}} \end{bmatrix} = \begin{bmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \vdots \\ \mathbf{c}_n \end{bmatrix} \quad (\text{A.1})$$

上の表現で， $\overline{\mathbf{H}_{k-1}}$ は \mathbf{H}_{k-1} の補数で，各要素を反転 ($1 \rightarrow -1$, $-1 \rightarrow 1$) した行列を意味する．具体例を示すと次のようになる．

$$\mathbf{H}_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (\text{A.2})$$

A.1 アダマール行列の利用

$$\mathbf{H}_2 = \begin{bmatrix} \mathbf{H}_1 & \mathbf{H}_1 \\ \mathbf{H}_1 & \overline{\mathbf{H}_1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \mathbf{c}_3 \\ \mathbf{c}_4 \end{bmatrix} \quad (\text{A.3})$$

$$\mathbf{H}_3 = \begin{bmatrix} \mathbf{H}_2 & \mathbf{H}_2 \\ \mathbf{H}_2 & \overline{\mathbf{H}_2} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} = \begin{bmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \mathbf{c}_3 \\ \mathbf{c}_4 \\ \mathbf{c}_5 \\ \mathbf{c}_6 \\ \mathbf{c}_7 \\ \mathbf{c}_8 \end{bmatrix} \quad (\text{A.4})$$

このようにして、生成されたアダマール行列の各行成分 $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n$ を直交符号に利用することで、良好なビット誤り率で多元接続を実現できる。

A.1.2 アダマール行列を PN 系列に用いた場合の BER 特性

図 A.1 は直接拡散方式における PN 系列に、アダマール行列を用いた場合のビット誤り率特性を表している。前にも述べているが、アダマール行列の各行は直交しているので、ユーザ数を増やした場合でも PN 系列同士が互いに干渉しあうことはない。つまり、図 A.1 はノイズの影響しか受けていないことになる。本論文で用いる時変 PN 系列においても、アダマール行列を用いた CDMA の BER 特性のように、時変 PN 系列同士が干渉し合わない系列にしたいと考えている。

A.1 アダマール行列の利用

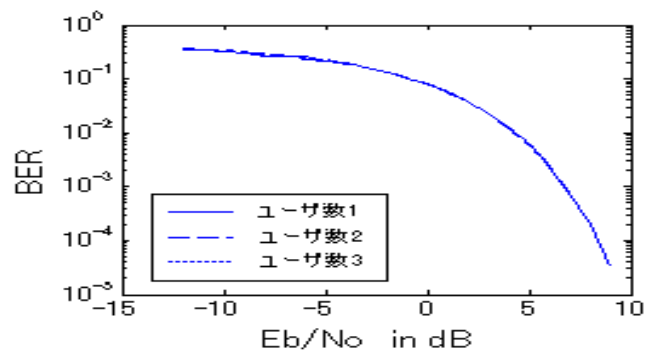


図 A.1 アダマール行列の各行を PN 系列に用いた CDMA の BER 特性