

(19) 日本国特許庁(JP)

## (12) 特 許 公 報(B2)

(11) 特許番号

特許第4635213号  
(P4635213)

(45) 発行日 平成23年2月23日(2011.2.23)

(24) 登録日 平成22年12月3日(2010.12.3)

(51) Int.Cl.

H03K 3/84 (2006.01)

F 1

H03K 3/84

A

請求項の数 10 (全 12 頁)

(21) 出願番号 特願2001-548538 (P2001-548538)  
 (86) (22) 出願日 平成12年12月22日 (2000.12.22)  
 (65) 公表番号 特表2003-527796 (P2003-527796A)  
 (43) 公表日 平成15年9月16日 (2003.9.16)  
 (86) 國際出願番号 PCT/EP2000/013364  
 (87) 國際公開番号 WO2001/048936  
 (87) 國際公開日 平成13年7月5日 (2001.7.5)  
 審査請求日 平成19年12月20日 (2007.12.20)  
 (31) 優先権主張番号 09/474,303  
 (32) 優先日 平成11年12月29日 (1999.12.29)  
 (33) 優先権主張国 米国(US)

(73) 特許権者 510000633  
 エスティー・エリクソン、ソシエテ、アノニム  
 スイス国プラン-レ-ズアト、シュマン、デュ、シャン-デ-フィーユ、39  
 (74) 代理人 100117787  
 弁理士 勝沼 宏仁  
 (72) 発明者 ダニエル、ジェイ、グリーンホー  
 オランダ国5656、アーアー、アンド  
 フェン、プロフ、ホルストラーン、6  
 審査官 栗栖 正和

最終頁に続く

(54) 【発明の名称】ガロアLFSR用ゼロ遅延マスク

## (57) 【特許請求の範囲】

## 【請求項 1】

複数の前段の出力に依存する出力を有する繰り返しシステムであって、前記前段の出力とは異なる処理された値を得るために前段の出力を処理し、この処理された値を格納し、処理され格納された値に応じて新たな出力を決定し、この新たな出力を提供する出力手段であって、前記出力手段は、回路ループ状に設けられ、このループの前段のレジスタの出力に各々の後段のレジスタの値入力が接続された一連のバイナリレジスタを含む、出力手段と、

前記前段の出力を得るために前記処理され格納された値を逆処理し、前記前段の出力を提供する逆処理手段と、

を備え、

前記逆処理手段は、

各々が第1及び第2の入力と、出力と、を有する一連の第1加算器であって、前記一連の加算器の各々の後段の加算器の各第1の入力は、前記一連の加算器の前段の加算器の前記出力に接続された、一連の第1加算器と、

前記一連の加算器における第1段の加算器の前記第1の入力に接続された出力を有する第1段のマスクスイッチと、前記一連の加算器における複数の前記後段の加算器の前記第2の入力にそれぞれ接続された出力を有する複数の後段のマスクスイッチと、を有する一連のマスクスイッチであって、各マスクスイッチは選択されたマスク値に基づく状態を有する一連のマスクスイッチと、

10

20

複数の前記レジスタの複数の前記出力を、複数の前記マスクスイッチの複数の入力に接続する接続ネットワークと、

前記一連の加算器における最終段の前記第1加算器の前記出力に接続された出力端子と、  
を含む繰り返しシステム。

**【請求項2】**

前記一連のレジスタの各レジスタのクロック入力に接続されたクロック信号線であって、クロック信号が前記クロック信号線を介して送信されたとき、各レジスタがそのときにそのレジスタの値入力で受信している値を出力し始めると共に、次のクロック信号までの前記入力値における何れのその後の変化にも関わりなくその値を出力し続けるためのクロック信号線をさらに備える請求項1に記載の繰り返しシステム。

10

**【請求項3】**

前記繰り返しシステムの少なくとも起動時に、各レジスタの前記値を初期化して、初期値を提供する、初期化手段をさらに備える請求項1に記載の繰り返しシステム。

**【請求項4】**

前記一連のレジスタにおける前段のレジスタの前記出力と後段のレジスタのそれぞれの値入力との間の接続における隣接するレジスタのペアの間に結合された1つ以上の第2加算器をさらに備え、各第2加算器は、前記各前段のレジスタに接続された第1の入力と、前記レジスタのペアの前記各後段のレジスタに接続された出力と、を有し、各第2加算器は、前記一連のレジスタの最終段のレジスタの前記出力と第1段のレジスタの前記入力とに接続された第2の入力を有し、前記ループを形成する、請求項1に記載の繰り返しシステム。

20

**【請求項5】**

前記接続ネットワークは、前記1つ以上の第2加算器にそれぞれ対応する1つ以上の第3加算器を含み、各第3加算器は、前記対応する第2加算器の後段の前記複数のレジスタのうちの1つの前記出力に結合された第1の入力と、前記対応する第2加算器の前段の前記複数のレジスタのうちの1つの前記出力に結合された第2の入力と、前記複数のマスクスイッチのうちの1つの入力に結合された出力と、を含む、請求項4に記載の繰り返しシステム。

30

**【請求項6】**

前記複数のマスクスイッチの各々は、前記複数のレジスタのうちの対応する1つの前記出力または前記1つ以上の第3加算器のうちの対応する1つの前記出力の何れかに結合されている入力を含む、請求項5に記載の繰り返しシステム。

**【請求項7】**

マスクされたガロア線形フィードバックシフトレジスタであって、回路ループ状に設けられ、このループの前段レジスタの出力に後段のレジスタの値を持つ入力が接続され、最終段のレジスタの出力が初段のレジスタの入力に接続されている一連のバイナリレジスタと；

前記一連レジスタにおける隣接するレジスタのペアのそれぞれの間に挿入されて、各々がそれぞれのレジスタのペアの前段のレジスタの出力に接続された第1の入力と、それぞれのレジスタのペアの後段の入力に接続された出力とを備え、各々が前記一連のレジスタの最終段のレジスタの出力に接続された第2の入力を備える1つまたはそれ以上のモジュロ2加算器と；

40

前記一連のレジスタの各レジスタのクロック入力に接続されたクロック信号線であって、クロック信号がこのクロック信号線を介して送信されたとき、各レジスタがそのときにそのレジスタの値を持つ入力で受信している値を出力し始めると共に、次のクロック信号までの前記入力値における何れかの連続する変化に関わりなくその値を出力し続けるためのクロック信号線と；

前記ガロア線形フィードバックシフトレジスタの少なくとも起動時に、初期値を提供して各レジスタの値を初期化する初期化手段と；

50

後段の加算器の第1の入力が前段の加算器の出力に接続された一連のモジュロ2加算器と；

前記一連の加算器における第1段の加算器の第1の入力に接続された出力を有する第1段のマスクスイッチと、前記一連の加算器における全加算器のそれぞれの第2の入力に接続された出力を有する後段のマスクスイッチと、を含む多数のマスクスイッチと；

選択されたマスク値に基づいて前記マスクスイッチの値を設定するための各マスクスイッチ用の個別のマスク値入力線と；

前記レジスタの入力または出力と、各マスクスイッチとの間に設けられ：レジスタの入力または出力と各マスクスイッチの入力との間の接続；および多数のレジスタの入力または出力とモジュロ2加算器の入力との間の接続および前記加算器の出力と各マスクスイッチとの間の接続；から各ネットワークが選択される接続ネットワークと；さらに

前記一連の加算器における最終段のモジュロ2加算器の出力に接続された出力端子と；を備えるガロア線形フィードバックシフトレジスタ。

#### 【請求項8】

送信機であって：

情報信号用の入力と；

電力供給源と；

前記電力供給源に接続されたマイクロコントローラと；

回路ループ状に設けられた一連のバイナリレジスタであって、前記ループの前段レジスタの出力に後段のレジスタの値を持つ入力が接続され、前記一連のレジスタの最終段のレジスタの出力が初段のレジスタの入力に接続されている一連のバイナリレジスタと；

前記一連レジスタにおける隣接するレジスタのペアのそれぞれの間に挿入されて、各々がそれぞれのレジスタのペアの前段のレジスタの出力に接続された第1の入力と、それぞれのレジスタのペアの後段の入力に接続された出力とを備え、各々が前記一連のレジスタの最終段のレジスタの出力に接続された第2の入力を備える1つまたはそれ以上のモジュロ2加算器と；

前記一連のレジスタの各レジスタのクロック入力に接続されたクロック信号線であって、クロック信号がこのクロック信号線を介して送信されたとき、各レジスタがそのときにそのレジスタの値を持つ入力で受信している値を出力し始める共に、次のクロック信号までの前記入力値における何れかの連続する変化に関わりなくその値を出力し続けるためのクロック信号線と；

前記ガロア線形フィードバックシフトレジスタの少なくとも起動時に、初期値を提供して各レジスタの値を初期化する初期化手段と；

後段の加算器の第1の入力が前段の加算器の出力に接続された一連のモジュロ2加算器と；

前記一連の加算器における第1段の加算器の第1の入力に接続された出力を有する第1段のマスクスイッチと、前記一連の加算器における全加算器のそれぞれの第2の入力に接続された出力を有する後段のマスクスイッチと、を含む多数のマスクスイッチと；

前記マイクロコントローラにより自動的に選択されたマスク値に基づいて前記マスクスイッチの値を設定するための各マスクスイッチ用の個別のマスク値入力線と；

前記レジスタの入力または出力と、各マスクスイッチとの間に設けられ：レジスタの入力または出力と各マスクスイッチの入力との間の接続；および多数のレジスタの入力または出力とモジュロ2加算器の入力との間の接続および前記加算器の出力と各マスクスイッチとの間の接続；から各ネットワークが選択される接続ネットワークと；

前記一連の加算器の最終段のモジュロ2加算器の出力に基づいて情報信号を拡散させる拡散器と；さらに

媒体内に前記拡散された情報信号を送信する送信装置と；

を備える送信機。

#### 【請求項9】

受信機であって：

10

20

30

40

50

拡散された情報信号を媒体から受信する受信装置と；

電力供給源と；

前記電力供給源に接続されたマイクロコントローラと；

回路ループ状に設けられた一連のバイナリレジスタであって、前記ループの前段レジスタの出力に後段のレジスタの値を持つ入力が接続され、前記一連のレジスタの最終段のレジスタの出力が初段のレジスタの入力に接続されている一連のバイナリレジスタと；

前記一連レジスタにおける隣接するレジスタのペアのそれぞれの間に挿入されて、各々がそれぞれのレジスタのペアの前段のレジスタの出力に接続された第1の入力と、それぞれのレジスタのペアの後段の入力に接続された出力とを備え、各々が前記一連のレジスタの最終段のレジスタの出力に接続された第2の入力を備える1つまたはそれ以上のモジュロ2加算器と；

前記一連のレジスタの各レジスタのクロック入力に接続されたクロック信号線であって、クロック信号がこのクロック信号線を介して送信されたとき、各レジスタがそのときにそのレジスタの値を持つ入力で受信している値を出力し始める共に、次のクロック信号までの前記入力値における何れかの連続する変化に関わりなくその値を出力し続けるためのクロック信号線と；

前記ガロア線形フィードバックシフトレジスタの少なくとも起動時に、初期値を提供して各レジスタの値を初期化する初期化手段と；

後段の加算器の第1の入力が前段の加算器の出力に接続された一連のモジュロ2加算器と；

前記一連の加算器における第1段の加算器の第1の入力に接続された出力を有する第1段のマスクスイッチと、前記一連の加算器における全加算器のそれぞれの第2の入力に接続された出力を有する後段のマスクスイッチと、を含む多数のマスクスイッチと；

前記マイクロコントローラにより自動的に選択されたマスク値に基づいて前記マスクスイッチの値を設定するための各マスクスイッチ用の個別のマスク値入力線と；

前記レジスタの入力または出力と、各マスクスイッチとの間に設けられ：レジスタの入力または出力と各マスクスイッチの入力との間の接続；および多数のレジスタの入力または出力とモジュロ2加算器の入力との間の接続および前記加算器の出力と各マスクスイッチとの間の接続；から各ネットワークが選択される接続ネットワークと；

復元された情報信号を生成するために、前記一連の加算器の最終段のモジュロ2加算器の出力に基づいて前記拡散された情報信号を逆拡散させる逆拡散器と；さらに

前記復元された情報信号用の出力と；

を備える受信機。

#### 【請求項10】

複数の前段出力に応じた出力を有する繰り返しシステムを動作させる方法であって：

処理された値を得るために複数の前段出力を処理し、

前記処理された値を格納し、

前記格納するステップで格納された処理された値への接続を置くことにより、前記処理された値に応じて新たな出力を決定し、前記接続は前記処理された値を少なくとも1つの加算器に入力として提供し、

前記前段出力を得るために、前記処理された値を逆処理し、前記逆処理するステップは前記加算器からの出力を少なくとも1つのスイッチに供給することを更に有する、  
方法。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

この発明は、データを符号化したり復号化したりするための疑似雑音シーケンスを用いる、例えばCDMA-2000、UMTS、IS-95標準やこれと同様のセルラ電話システムなどを実現するための、直接シーケンススペクトラム拡散通信システムに関する。

##### 【0002】

10

20

30

40

50

### 【発明の背景】

スペクトラム拡散通信システムは、増加された用途と、双方向の空中の通信とを見出している。丁度AMおよびFMシステムが情報を運ぶために正弦波信号を用いているように、スペクトラム拡散システムは、情報を運ぶために雑音のような信号を用いている。送信機においては、デジタルデータストリームが、媒体を介してデータを送信するために、疑似雑音シーケンス(PNS)を用いて信号のスペクトルを拡散するために符号化される。受信機では、データが媒体から復元されて、その後、同じPNSを用いて信号のスペクトルを逆拡散し、最初のデジタルデータストリームを再生するために復号化されている。

### 【0003】

PNSは、有限のパターンを伴うビットのストリームであるが、これはランダムなビットストリームであるように見える。PNSを生成する共通の装置は線形フィードバックシフトレジスタ(LFSR-linear feedback shift register-)である。LFSRの2つの普通のタイプは、フィボナッチ(Fibonacci)LFSRとガロア(Galois)LFSRである。両方のタイプとも、ループを介してビットがシフトされるビットレジスタとモジュロ2加算器を含む閉鎖されたループ回路を含んでいる。加算器はループの一部分である1つの入力と、ループの他の部分に接続された他の入力とを有し、それらがループを介してシフトされるように、ビットをランダム化するための複数のループを形成している。

10

### 【0004】

何れかのLFSR用のPNSの値は、大きな数のビットの後に繰り返されると共に、制限された量のハードウェアを使用することを繰り返すことなく、最長可能シーケンスを有するPNSを提供することが望まれている。これは、LFSRの加算器とレジスタとの構成と、この技術分野で公知の方法でのレジスタの初期値とを選択することにより実現されている。LFSRに含まれているm個のレジスタの所定の数のために、PNSの最長可能非反復部分は、 $2^m - 1$ ビットまでの長さに等しくなる。

20

### 【0005】

同じPNSを用いることに加えて、送信機と受信機はそれぞれ拡散および逆拡散するためのPNS内の同じ位置からの値を用いなければならない。PSN内の同一の位置での値を両者が用いるため送信機と受信機を同期させるために、オフセットマスク値が計算され、この技術分野で公知の方法によりPNS内の異なるシフトされた位置の値を生成するために(送信機または受信機内の)PNSの連続する位置の出力値と前記オフセットマスク値とが結合されている。

30

### 【0006】

この技術分野の熟練者たちは、以下の引用例に向けられている。シーデンバーグ(Siedenburg)に付与された合衆国特許第5,878,076号は、直接シーケンススペクトラム拡散通信システムを説明している。トーマス(Thomas)に付与された合衆国特許第5,754,603号は、PNSの同期について説明している。バロン(Barron)に付与された合衆国特許第5,926,070号は、オフセットマスクの生成を説明している。石田(Ishida)によるヨーロッパ特許出願第0660541号は、送信機と受信機のPNS位置を同期させる方法を説明している。メドロック(Medlock)によるPCT特許出願の国際公開WO99/45670号は、LFSR用のマスクを説明している。

40

### 【0007】

図1は、オフセットマスクを有するガロアLFSRの選択された部分を説明している。LFSR100は、ループ回路内で直列に接続された多数のバイナリレジスタ101-108を備えている。バイナリレジスタは、D型フリップフロップでも、または他の公知のビットレジスタ装置でも良い。一例として、レジスタ102を用いると、各々のレジスタ102は前段のレジスタ101の出力111に接続された値を持つ入力110を有し、各々のレジスタ102は後段のレジスタ103の値のある入力113に接続された出力112を有している。

### 【0008】

LFSR100はまた、ループ回路内で接続された1つまたはそれ以上のモジュロ2加算

50

器 115 - 117 を含んでいる。各々の加算器は、レジスタ列の異なるペアの連続するレジスタ 101 - 108 の間に挿入されている。加算器がその間に挿入されたレジスタのペアの選択は原始多項式の選択により決まっている。原始多項式は、素数の概念と同様のものである。原始多項式は、何れかのより簡単な多項式により分割されることができる多項式である。図 1 に示された LFSR の特別な例では、原始 2 値多項式は、 $D^8 + D^4 + D^3 + D^2 + 1$  である。この  $D^8$  は、LFSR に対して 8 つのレジスタを有することを要求しており、 $D^2$ ,  $D^3$  および  $D^4$  の項は、図示されているように、レジスタのペアにおける最後から 2 番目のペアの間、最後から 3 番目のペアの間および最後から 4 番目のペアの間にそれぞれ挿入された加算器を要求している。素数のような原始多項式は、この技術分野においては良く知られている。

10

#### 【0009】

挿入された加算器 115 - 117 はそれぞれ、2 つの入力と 1 つの出力を有しており、XOR ( 排他的論理和 ) ゲートとして簡単に実施されていても良い。一例として、加算器 115 は、前段のレジスタ 104 の出力 121 に接続された第 1 の入力 120 と、後段のレジスタ 105 の値を持つ入力 123 に接続された出力 122 を有している。さらに、加算器 115 は、最終段のレジスタ 108 の出力 125 と、連続するレジスタの最初のレジスタ 101 の入力 126 との間に接続された第 2 の入力 124 を有している。クロック信号線 130 は、連続するレジスタのうちの各々のレジスタのクロック入力に接続されており、クロック信号がこのクロック信号線を介して送信されたときに、各レジスタは、そのときにそれレジスタの値を持つ入力で受信されている値を出力し始める。例えばクロック信号線 130 は、レジスタ 101 のクロック入力 131 に接続されている。

20

#### 【0010】

制御線 135 は、レジスタの値を初期化するためにレジスタ 101 - 108 のそれぞれに接続された、少なくとも 1 つの初期化線 136 を含んでいる。例えば初期化線 136 は、レジスタ 108 の初期化入力 137 に接続されるように示されている。この初期化線は、レジスタにメモリ値を書き込むようにしても良いので、何れかの初期値を所望の何れかのレジスタに書き込むことができる。もう 1 つの方法として、制御線は、個々のレジスタのハードウェア内に設定された幾つかの所定の初期値を仮定するために、レジスタに簡単に信号を送るようにしても良い。もしもこのレジスタが D 型フリップフロップであるならば、初期化線は、“1 ( one )” に初期化されるべき全てのレジスタのセット入力に接続されると共に、“0 ( zero )” に初期化されるべき全てのレジスタのリセット入力に接続されており、初期化線がハイになるときに、レジスタの値はそれらの個別の初期値であると仮定している。個別の原始多項式のためのレジスタの初期値を選択する方法は公知のものであり、更なる議論はここでは求められていない。

30

#### 【0011】

図 1 に示されたガロア LFSR は、PNS に関するビット値を出力 138 から出力している。しかしながら、受信機に PNS における出力値の位置を同一の PNS を用いる送信機のための出力値の位置に同期させる（その逆の場合もまた同様である）ために、オフセットマスク値が PNS の以前に出力されていた箇所に結合させられるべきである。

40

#### 【0012】

マスク 140 は、図 1 に示されたようなガロア LFSR 100 の出力 138 に接続されている。このマスクは、LFSR からの PNS 出力の前段の 8 ビットをそれぞれ記憶する一連のレジスタ 141 - 148 を含んでいる。レジスタ 142 - 148 の出力は、それぞれのレジスタに続くレジスタ 141 - 147 の入力に接続されている。例えば、レジスタ 146 の入力 149 は、レジスタ 147 の出力 150 に接続されており、レジスタ 146 の出力 151 は、レジスタ 145 の入力 152 に接続されている。

#### 【0013】

マスクはさらに、一連のモジュロ 2 加算器 161 - 167 を含んでおり、連続する加算器 162 - 167 のそれぞれの第 1 の入力は加算器シリーズの個々の前段の加算器 161 - 166 のそれぞれの出力に接続されている。例えば、加算器 165 の入力 153 は、加算

50

器 164 の出力 154 に接続されており、この加算器 165 の出力 155 は、加算器 166 の入力 156 に接続されている。多くのマスクスイッチ 171 - 178 は、前記加算器シリーズの第 1 の加算器 161 の第 1 の入力 180 に接続された出力 179 を有する第 1 のマスクスイッチ 171 を含んでいる。さらに、それに続くマスクスイッチ 172 - 178 は、前記加算器シリーズにおける加算器 161 - 167 のそれぞれの第 2 の入力に接続された出力を有している。それぞれのレジスタ 141 - 148 の出力は、個々のスイッチ 171 - 178 の入力にそれぞれ接続されている。

#### 【 0014 】

制御線 135 のマスク値線 191 - 198 は、スイッチ 171 - 178 にそれぞれ接続されており、これは、個々のレジスタの値が個々のスイッチを介して加算器 161 - 167 の個々の加算器の入力へと供給されているか否かを制御する開放されたまたは閉鎖された位置に個々のスイッチ 171 - 178 をそれぞれセットするために接続されているものである。例えば、レジスタ 146 の出力 151 は、スイッチ 175 の入力 182 に接続されており、このスイッチ 175 の出力 183 は、加算器 165 の入力 184 に接続されている。したがって、スイッチ線 196 が “1” に設定されたときに、レジスタ 146 の値はその後、加算器 164 の出力 154 の出力値に加算されてモジュロ 2 となると共に、その結果は出力 155 から加算器 166 の入力 156 へと出力される。そうでなければ、スイッチ線 183 が “0” に設定されたときに、加算器 164 の出力 154 からの値はその後、加算器 165 を単純に通過して加算器 166 の入力 156 に供給されている。最後に、加算器シリーズの最終段のモジュロ 2 加算器 167 の出力に接続されている出力端子 199 は、マスクされた PNS の値を出力している。10

#### 【 0015 】

マイクロコントローラ 200 は、プロセッサ 201 と、クロック 202 と、メモリ 203 とを含んでおり、これらはバス 204 により相互接続されている。電力供給源 205 は、プロセッサ、メモリおよびクロックを動作させるための電力を提供している。クロックは、動作を同期させるためにプロセッサおよびメモリにタイミング信号を提供している。マイクロプロセッサのメモリは、レジスタ 101 - 108 用の初期値を含むデータモジュール 206 と、初期化の際にこれらのレジスタに対して制御線 135 を介してその初期値を送信してプロセッサを制御するためのプログラムモジュール 207 と、を含んでいる。このメモリはまた、この技術分野における公知のやり方により、マスク値を演算するプログラムモジュール 208 をも含んでいるので、送信機のマスクされた PNS により提供される個々の値と受信機における対応する値とを同期させることができる。20

#### 【 0016 】

公知のマスクされたガロア LFSRにおいて、LFSR が初期化された後に、LFSR のマスクは、適正な PNS のビットがマスクの全てのレジスタの中に取り込まれるまで、無効なシーケンスを出力する。これは、送信機と受信機との間で同期をとっている間に LFSR を異なる初期値に初期化するようなシステムにおいては特に問題となる。

#### 【 0017 】

上述した引用例は、これによりこの明細書の全体にわたって、参考として組み入れられるものとする。40

#### 【 0018 】

##### 【発明の概要】

いくつかの応用を含むこの発明において、マスクされたガロア線形フィードバックシフトレジスタ (LFSR) は、この LFSR の初期化に直接基づいて、適正なマスクされた疑似雑音シーケンス (PNS) を出力することが可能である。これは、結合されたネットワークを介してガロア LFSR のマスクスイッチを LFSR のレジスタに相互接続することにより実現されている。この発明はまた、ガロア LFSR が実行する特定の原始多項式にもまた応じて LFSR のみにより決まるレジスタにスイッチをどのようにして相互接続するのかを決定するための単純な方法を提供している。

#### 【 0019 】

10

20

30

40

50

この技術分野における熟練者たちは、請求の範囲の特徴を表現した以下に添付する図面を参照しながら、以下に説明される好適な実施形態の詳細な説明を詳しく調べることにより、この発明およびこの発明の付加的目的および長所を理解することになる。

#### 【0020】

##### 【発明の実施の形態】

図においては、説明を簡略化するために、異なる図面に用いられた同一の構成要素は同一の符号を有するものとする。

#### 【0021】

図2は、この発明に係るマスクされたガロア線形フィードバックシフトレジスタ(LFSR)220を示している。レジスタ101-108および加算器115-117を含むLFSRの構成要素および動作は、上述した図1のものと同様である。また、マスクにおいても、一連の加算器161-167およびこの一連加算器のそれぞれの加算器の各入力に接続されたスイッチ171-178は、本質的には図1に示されたものと同様である。10

#### 【0022】

図2のマスクされたLFSRにおいて、各ネットワークは、1つまたはそれ以上のレジスタ101-108の出力と、マスクスイッチ171-178の各々の入力と、の間に接続されている。このネットワークは、レジスタ125, 101, 102, 103および104の出力と、各マスクスイッチ171, 172, 173, 174および175の入力と、の間の1対1接続221, 222, 223, 224および225を含んでいる。このネットワークは、レジスタ101および105の出力と、モジュロ2加算器231の入力との間の接続229および226と、モジュロ2加算器231の出力とマスクスイッチ176の入力との間の接続235と、を含んでいる。このネットワークは、レジスタ101, 102および106の出力と、モジュロ2加算器232の入力との間の接続230, 231および227と、モジュロ2加算器232の出力とマスクスイッチ177の入力との間の接続236と、を含んでいる。このネットワークはまた、レジスタ101, 102, 103および107の出力と、モジュロ2加算器233の入力との間の接続232, 233, 234および228と、モジュロ2加算器233の出力と、マスクスイッチ178の入力との間の接続237と、を含んでいる。20

#### 【0023】

レジスタおよびスイッチ間のネットワークの構成は、ガロアLFSRの構成より直接決定することができる。この場合、ガロアLFSRが第4, 第5および第6のレジスタの出力に接続された加算器を有しているので、これにより接続は、レジスタの出力から第4, 第5および第6のレジスタを越えてそれを行なうことができるスイッチへと延長すべきものである。接続229, 231および234のみは、レジスタの出力から4つのレジスタを介してそれぞれのスイッチへと延長することができる。接続230および233のみは、5つのレジスタを介してそれぞれのスイッチへと延長することができる。接続232のみは、6つのレジスタを介してスイッチへと延長することができる。好ましくは、接続の数は、第1項を除いて、幾つかのより低い順番の項のみを有する原始多項式を選択することにより最小化される。すなわち、もしも多項式がD<sup>7</sup>項を有するならば、加算器はレジスタ101および102間に1つ挿入されるであろうし、接続はそれを行なうことができる1つのレジスタを介して延長されることになるであろうので加算器はスイッチ173, 174および175のために求められるであろうし、さらに6つの接続が、レジスタ101, 102, 103, 104, 105および106からスイッチ173, 174, 175, 176, 177および178用の加算器にまでそれぞれ求められることになるであろう。3040

#### 【0024】

図3は、図2のマスクされたガロアLFSRを利用するこの発明の送信機300を示している。マイクロコントローラ200は、クロック、レジスタ初期化およびマスク信号をマスクされたガロアLFSR220に提供するために、図2に関連して上述したように、接続されている。情報信号は、入力301を介して符号化器302内に受信され、ここで情報を連続するビットストリームへと変換している。例えば、符号化器は、アナログ音声入50

力をビットストリームへと変換している。入力を介して受信された情報が既に連続するビットストリームであるならば、そのときは符号化器を必要としなくとも良い。拡散情報信号を提供するために、この発明に係るマスクされたガロアルフサル220のPNS出力に基づいて、拡散器303によりビットストリームが拡散される。送信機装置304は、拡散情報信号を媒体205内に送信する。送信機は、例えば、拡散情報信号を空中に放送するアンテナに接続された変調器；拡散情報信号をコンピュータ媒体に書き込むための媒体装置の書き込みヘッドに接続されたチャンネル符号化器；または光ファイバを介して送信するために接続されたレーザ装置またはその他の同等の情報送信システムであっても良い。

## 【0025】

10

図4は、図3の送信機により生成された拡散情報信号を受信し、送信機に最初に入力された情報信号を再生するための受信機320を示している。受信機装置321は、媒体305からの拡散情報信号を受信している。受信機の性質は、上述したように、媒体に基づいている。逆拡散器322は、上述したような符号化されたビットストリームを提供するために拡散情報を逆拡散している。復号化器323は、送信機300により最初に受信されていた情報信号を再生するために符号化されたビットストリームを復号化している。もしも符号化器が必要でなかったならば、状況によっては復号化器もまた必要でなくなるかもしれない。PNS発生器220は、図3のPNS発生器220と全く同じであり、好ましくは、図2のマスクされたガロアルフサル220である。PNS発生器220においては、疑似雑音シーケンス(PNS)の出力値は、PNSシーケンス内の異なる位置に対応する出力値を提供するために、この発明のマスクにより変形されてしまっているので、情報信号を拡散するため、および、拡散情報信号を逆拡散するために、同じ値を用いることができる。

## 【0026】

20

この発明は、この技術分野の熟練者たちにこの発明を想像し利用することを可能にするため、および、この発明を実施するために熟慮された最良の形態を説明するために、特別に好適な実施形態にしたがって説明されてきた。この技術分野の熟練者たちは、この発明の精神から逸脱することなく、これらの実施形態を変形したり、実施形態に付加したり、他の実施形態を提供したりしても良い。

## 【0027】

30

## 【発明の実施例】

出力手段が、レジスタ、D型フリップフロップ、およびワードメモリ：から選択されているメモリ内の処理された値を格納する、この発明の実施例によるシステム。

## 【0028】

逆処理が単純な動作の直ぐ内側で行なわれる、この発明の実施例によるシステム。

## 【0029】

前段の出力が新たな出力として同時に提供される、この発明の実施例によるシステム。

## 【0030】

初期化手段(135)が、所定の初期値を有するレジスタ；D型フリップフロップへセットラインまたはリセットラインを選択的に接続すること；初期値を何れかの演算された値に設定するために各々のレジスタに対してデータ線を提供することの中から：選択されている、この発明の実施例によるシフトレジスタ。

40

## 【0031】

モジュロ2加算器(160-167)がXORゲートである、この発明の実施例によるシフトレジスタ。

## 【0032】

レジスタがD型フリップフロップである、この発明の実施例によるシフトレジスタ。

## 【0033】

原始多項式の係数が：レジスタの間にモジュロ2加算器を有するレジスタのペアと、レジスタおよびマスクスイッチの間の接続ネットワークと、を決定する、この発明の実施例に

50

よるシフトレジスタ。

**【0034】**

原始多項式の係数が、レジスタの初期値を決定する、この発明の実施例によるシフトレジスタ。

**【0035】**

媒体が：送信機の媒体装置内のコンピュータ媒体、送信機に接続された広帯域ネットワーク、無線電波が搬送される開放空間と共に用いられるアンテナ、から選択される、この発明の実施例による送信機。

**【0036】**

マイクロコントローラが、バス（204）により相互接続されたプロセッサ（201）、メモリ（203）、およびクロック（202）を含む、この発明の実施例による送信機。 10

**【0037】**

したがって、この発明の範囲は、上述した特許請求の範囲によって制限されるのみである。

**【図面の簡単な説明】**

**【図1】** 従前のマスクされたガロア線形フィードバックシフトレジスタ（LFSR）の具体的な特徴を示す回路図である。

**【図2】** この発明に係るLFSRを示す回路図である。

**【図3】** 図2のLFSRを用いる送信機を示すブロック図である。

**【図4】** 図2のLFSRを用いる受信機を示すブロック図である。

20

**【符号の説明】**

101 - 108 レジスタ

101 - 138 出力手段

115 - 117 モジュロ2加算器

121 - 137 接続ネットワーク

130 クロック信号線

135 初期化手段

161 - 167 一連のモジュロ2加算器

161 - 198 処理手段

171 - 178 多数のマスクスイッチ

30

179 第1のマスクスイッチ

191 - 198 マスク値入力線

199 出力端子

200 マイクロコンピュータ

201 プロセッサ

202 クロック

203 メモリ

204 バス

205 電力供給源

206 初期化手段

40

207 初期化手段（コンピュータプログラム）

221 - 237 逆処理手段（接続ネットワーク）

241 - 243 モジュロ2加算器

301 入力

303 拡散器

322 逆拡散器

324 出力

【 図 1 】

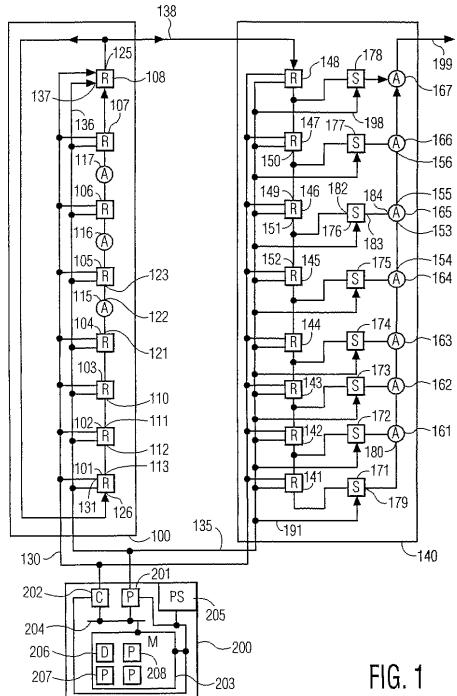


FIG. 1

【 図 2 】

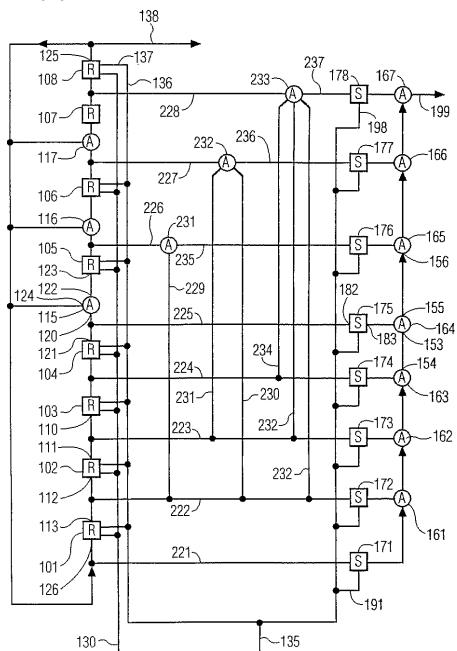


FIG. 2

【図3】

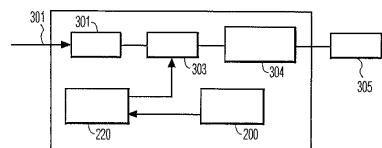


FIG. 3

【 図 4 】

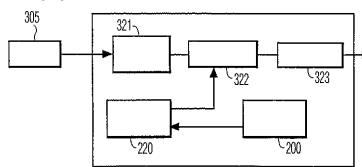


FIG. 4

---

フロントページの続き

(56)参考文献 米国特許第05926070(US,A)  
国際公開第99/035564(WO,A1)  
国際公開第99/045670(WO,A1)

(58)調査した分野(Int.Cl., DB名)

H03K 3/64-3/86