



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0046851  
(43) 공개일자 2011년05월06일

(51) Int. Cl.

H03M 13/15 (2006.01)

(21) 출원번호 10-2009-0103537

(22) 출원일자 2009년10월29일

심사청구일자 2009년10월29일

(71) 출원인

인하대학교 산학협력단

인천 남구 용현동 253 인하대학교

(72) 발명자

이한호

인천시 남구 용현3동 인하대학교 정보통신공학부

이기훈

인천시 부평구 부평1동 182-39

(74) 대리인

특허법인무한

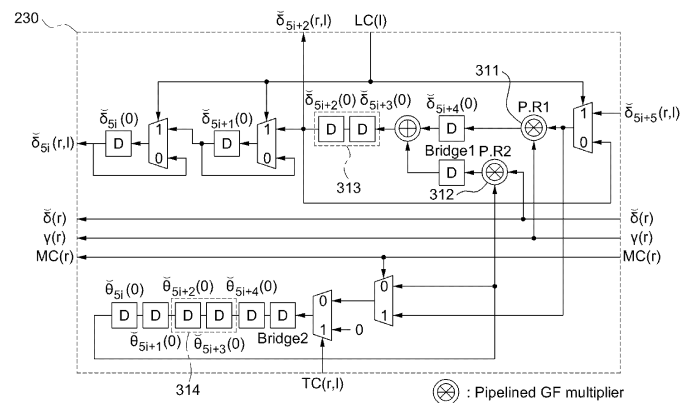
전체 청구항 수 : 총 5 항

(54) BCH 복호기를 위한 고속 소면적 파이프라인 폴딩 방식 벨르캄프-메시 알고리즘 연산 회로 및 그 방법

### (57) 요약

BCH 복호기를 위한 고속 소면적 파이프라인 폴딩 방식 벨르캄프-메시 알고리즘 연산 회로 및 그 방법이 개시된다. 고속 저복잡 BCH 복호기를 위한 파이프라인 폴딩 방식 간략화된 반전 없는 벨르캄프-메시 알고리즘을 이용한 오류 위치 다항식 연산 방법 및 오류위치 다항식 연산 회로는 고속 처리와 낮은 하드웨어 복잡도라는 특징을 갖고 있으며, 유연한 확장성을 가진 폴딩 구조로 인해 설계자가 특정 설계 요구 조건에 맞추어 자유롭게 최적화시킬 수 있는 특징을 가진다.

### 대표도



이 발명을 지원한 국가연구개발사업

과제고유번호 2009-F-010-01

부처명 지식경제부 한국산업기술평가관리원

연구관리전문기관

연구사업명 산업원천기술개발사업

연구과제명 차세대 광통신용디지털신호처리 기반 초고속 CMOS 회로 설계 기술

기여율

주관기관 인하대학교 산학협력단

연구기간 2009. 03. 01 ~ 2014. 02. 28

---

## 특허청구의 범위

### 청구항 1

신드롬 다항식 값으로부터 유한체 내에서 오류 위치 다항식의 반복 연산을 수행하여 근을 찾아내는 간략화된 반전없는 벨르캄프-메시 알고리즘(SiBM)을 이용한 오류위치 연산 방법에 있어서,

신드롬 다항식 값을  $(2 \times ff + 2)$  개의 D-플립플롭, 5 개의 멀티플렉서, 1 개의 갈로아체 덧셈기 및 2 개의 갈로아체 곱셈기를 포함하는 NoP개의 기본 셀의 래치에 초기화 저장하는 단계; 및

$t \times (ff + 1)$  번의 클럭 분주에 의해 반복 연산을 수행하여 오류 위치 다항식의 계수를 산출하는 단계를 포함하고,

상기 t는 부호화되는 전체 비트 수 중에 정정할 수 있는 비트 수를 의미하고,

상기 ff는 설정된 폴딩 인수를 의미하고,

$$NoP = \text{ceil}\left[\frac{2t+1}{ff}\right] NoP = \text{ceil}\left[\frac{2t+1}{ff}\right]$$

상기 NoP는 폴딩 인수에 따른 총 기본 셀의 개수를 의미( )하는, 오류 위치 연산 방법.

### 청구항 2

제1항에 있어서,

상기 오류 위치 다항식의 계수를 산출하는 단계는,

수학식( $\tilde{\delta}_i(r+1) = \gamma(r) \cdot \tilde{\delta}_{i+2}(r) - \tilde{\delta}_0(r) \cdot \tilde{\delta}_i(r)$ )을 적용하여 상기 오류 위치 다항식의 계수를 산출하는, 오류 위치 연산 방법.

### 청구항 3

제2항에 있어서,

상기 오류 위치 다항식  $\gamma(r)$ 의 계수를 산출하는 단계는,

상기 수학식을 ff+ps 클럭 주기동안 1회 계산하는 내부 루프 제 1 단계;

상기 제 1 단계가 종료될 때, 보조 변수  $\gamma(r)$ 과  $\tilde{\delta}(r)$  불합도를 갱신하는 외부 루프 제 2 단계; 및

상기 제 1 단계 및 상기 제 2 단계를 t회 반복 연산하여 오류 위치 다항식 산출을 완료하는 제 3단계를 포함하고,

상기 ps는 상기 갈로아체 곱셈기 내부에 존재하는 파이프라인 단계의 숫자를 의미하고,

상기  $\tilde{\delta}(r)$ 은 핵심 제어 장치 내부에 저장되는 불합도 값을 의미하고,

상기  $\gamma(r)$ 은 상기 핵심 제어 장치 내부에 저장되는 뉴턴 항등식에 의거한 보조 불합도 값을 의미하는, 오류 위치 연산 방법.

### 청구항 4

제3항에 있어서,

기본 셀(PE) 내부의  $\delta(r)$  과 상기 핵심 제어 장치 내부의  $\gamma(r)$  와 MC(r) 신호를 갱신하는 상기 제 2 단계 계산시 갱신되는 값을 선택하기 위해 SiBM에서 사용되던 제어 변수 k(r)을 사용하지 않는 구조인, 오류 위치 연산 방법.

## 청구항 5

제3항에 있어서,

상기 내부 루프 제1 단계를 수행하기 위해 상기 핵심 제어 장치 내부에 추가된 LC(r) 신호와 해당 신호를 제어하는 카운터와 비교기를 추가하고, 상기 외부 루프 제2 단계와 상기 내부 루프 제1 단계를 구분하기 위해 상기 핵심 제어 장치 내부에 2개의 멀티플렉서를 추가하는 구조인, 오류 위치 연산 방법.

## 명세서

### 발명의 상세한 설명

#### 기술 분야

[0001] 본 발명은 고속 소면적 BCH 복호기에 있어서, 파이프라인 폴딩 구조의 SiBM 알고리즘을 이용한 오류 위치 연산 방법 및 오류 위치 연산 회로에 관한 것으로 특히, 유연한 확장성을 가진 폴딩 구조로 인해 특정 설계 요구 조건에 맞추어 자유롭게 최적화시킬 수 있으며 종래의 연산 회로에 비교하여 아주 작은 임계 경로 지연(Critical path delay)과 면적-시간 복잡도(Area-Time Complexity)를 가지는 오류 위치 연산 회로에 관한 것이다.

#### 배경 기술

[0002] 최근 광통신, 디지털 비디오 방송 및 메모리, 데이터 저장 시스템의 데이터 전송에 있어서, 전송 중에 발생하는 다수의 오류를 찾고 정정할 수 있는 Bose-Chaudhuri-Hocquenghen (이하 'BCH'라 함) 복호기가 널리 사용되고 있다.

[0003] 일반적으로 BCH 복호기의 구조는 오류를 감지하고 정정하는 세 부분으로 구성되어 있다. 그 첫 번째 부분은 신드롬 다항식 계산(Syndrome Polynomial Computation, 이하 'SC'라 함) 블록으로 SC블록은 신드롬 다항식을 생성하고 수신된 코드워드(codeword)의 오류 패턴을 표현한다. SC블록에서 생성된 신드롬 다항식은 BCH 복호기의 두 번째 부분인 KES(Key Equation Solver) 블록에서 사용된다. KES 블록은 신드롬 다항식을 이용해 에러 위치 다항식을 구한다. 이 오류 위치 다항식을 이용하여 치엔 검색(Chine Search, 이하 'CS'라 함) 블록에서 오류를 수정해 출력한다.

[0004] KES 블록에서 해결 방정식(Key equation)을 해결하기 위한 방법에는 벨르캄프-메시(Berlekamp-Massey) 알고리즘, 유클리드(Euclidean) 알고리즘, 수정 유클리드(Modified Euclidean) 알고리즘 등이 오류 위치 다항식(error locator polynomial)을 구하기 위하여 사용될 수 있다. 또한 기존의 벨르캄프-메시 알고리즘을 구조적으로 개선한 재공식화된 반전 없는 벨르캄프-메시(Reformulation of inversionless Berlekamp-Massey, 이하 'RiBM'라 함) 알고리즘이 존재한다. 그리고 이를 간략화시킨 간략화된 반전 없는 벨르캄프-메시(Simplified inversionless Berlekamp-Massey, 이하 'SiBM'라 함) 알고리즘도 존재한다. 이러한 알고리즘을 사용하는 BCH 복호기 내부에서 q병렬 SC 블록과 CS 블록은 n/q 클럭 주기동안 동작하고 KES 블록은 t 클럭 주기동안 동작한다.

[0005] 일반적으로 BCH 복호기에서 t는 n에 비해 매우 작기 때문에 KES 블록의 동작시간(latency)은 SC 블록과 CS 블록에 비해 상당히 짧고 이런 동작시간의 차이는 KES 블록이 일정 시간 동안 유힬 상태로 존재하게 만든다. 이러한 유힬 상태를 이용해 복호기의 하드웨어 복잡도를 감소시키기 위해 싱글 채널 응용 분야를 위한 폴딩 구조 같은 기술이 소개되었다. 하지만 이는 고속에 적합하지 않고 짝수 폴딩 인수(folding factor, ff)만을 지원하는 문제점이 있다.

[0006] 따라서, KES 블록 내의 유힬 상태 시간을 줄이는 동시에 높은 폴딩 확장성 구조를 지원하는 고속 소면적의 연산 회로가 절실히 요구된다.

#### 발명의 내용

### 해결 하고자하는 과제

- [0007] 본 발명은 간략화된 반전 없는 SiBM 알고리즘 연산 회로에 파이프라인화함으로써 고속화가 쉬운 오류 위치 연산 방법 및 연산 회로를 제공한다.
- [0008] 본 발명은 SiBM 알고리즘 연산회로의 짝수 폴딩 인수만을 지원하는 폴딩 구조를 해결하여 확장성을 높이고 하드웨어 복잡도를 감소시키는 오류 위치 연산 방법 및 연산 회로를 제공한다.

### 과제 해결수단

- [0009] 본 발명의 일실시예에 따른 오류 위치 연산 방법은 신드롬 값으로부터 유한 체 내에서 오류위치 다항식의 반복 연산을 수행하여 근을 찾아내는 간략화된 반전 없는 SiBM을 이용한 오류위치 연산 방법에 있어서, 다섯 개의 멀티플렉서, 한 개의 갈로아체 덧셈기, 및 두 개의 파이프라인된 갈로아체 곱셈기를 포함하는 복수개의 기본 셀의 래치(latch)에 초기화 저장하는 단계 및 (폴딩인수+1)\*t번의 클럭 분주에 의해 반복 연산을 수행하여 오류 위치 다항식의 계수를 산출하는 단계를 포함한다.
- [0010] 본 발명의 일측면에서 상기 오류 위치 다항식의 계수를 산출하는 단계는 수학적  $(\tilde{\delta}_i(r+1) = \gamma(r) \cdot \tilde{\delta}_{i+2}(r) - \tilde{\delta}_0(r) \cdot \tilde{\theta}_i(r))$ 을 적용하여 상기 오류 위치 다항식의 계수를 산출할 수 있다.
- [0011] 또한 본 발명의 일측면에서 상기 오류 위치 다항식  $\gamma(r)$ 의 계수를 산출하는 단계는 상기 수학적식 ff+ps 클럭 주기동안 1회 계산하는 내부 루프 제 1 단계와, 상기 제 1 단계가 종료될 때, 보조 변수  $\gamma(r)$ 과  $\tilde{\delta}(r)$  불합도를 갱신하는 외부 루프 제 2 단계 및 상기 제 1 단계 및 상기 제 2 단계를 t회 반복 연산하여 오류 위치 다항식 산출을 완료하는 제 3단계를 포함하고, 상기 ps는 상기 갈로아체 곱셈기 내부에 존재하는 파이프라인 단계의 숫자를 의미하고, 상기  $\tilde{\delta}(r)$ 은 핵심 제어 장치 내부에 저장되는 불합도 값을 의미하고, 상기  $\gamma(r)$ 은 상기 핵심 제어 장치 내부에 저장되는 뉴턴 항등식에 의거한 보조 불합도 값을 의미할 수 있다.
- [0012] 또한 본 발명의 일측면에서 기본 셀(PE) 내부의  $\tilde{\delta}(r)$ 과 핵심 제어 장치 내부의  $\gamma(r)$ 와 MC(r) 신호를 갱신하는 상기 제 2 단계 계산시 갱신되는 값을 선택하기 위해 SiBM에서 사용되던 제어 변수 k(r)을 사용하지 않는 구조일 수 있다.
- [0013] 또한 본 발명의 일측면에서 상기 내부 루프 제1 단계를 수행하기 위해 상기 핵심 제어 장치 내부에 추가된 LC(r) 신호와 해당 신호를 제어하는 카운터와 비교기를 추가하고, 상기 외부 루프 제2 단계와 상기 내부 루프 제1 단계를 구분하기 위해 상기 핵심 제어 장치 내부에 2개의 멀티플렉서를 추가하는 구조일 수 있다.

### 효과

- [0014] 본 발명의 일실시예에 따르면, SiBM 알고리즘 연산 회로를 파이프라인화함으로써 고속화가 쉬운 오류 위치 연산 방법 및 연산 회로를 제공할 수 있다.
- [0015] 또한 본 발명의 일실시예에 따르면, SiBM 알고리즘 연산회로의 짝수 폴딩 인수만을 지원하는 폴딩 구조를 해결하여 확장성을 높이고 하드웨어 복잡도를 감소시키는 오류 위치 연산 방법 및 연산 회로를 제공할 수 있다.

### 발명의 실시를 위한 구체적인 내용

- [0016] 이하, 첨부된 도면들에 기재된 내용들을 참조하여 본 발명에 따른 실시예를 상세하게 설명한다. 다만, 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조부호는 동일한 부재를 나타낸다.
- [0017] 일반적으로 BCH 부호는 근래 통신 시스템에 가장 많이 쓰이고 있는 부호로서 국제 전기 통신 동맹(ITU)의 광통신 표준 및 유럽 전기 통신 표준 협회(ETSI)의 차세대 디지털 비디오 방송(DVB-S2)의 표준 등 다양한 표준 분야에 널리 쓰이는 순방향 오류 정정(Forward Error Correction, 이하 'FEC'라 함) 기술이다. BCH 부호를 나타내는 전형적인 형태는 BCH(n,k,t)이다. 여기서, n은 부호화되는 전체 비트(bit)의 수이고, t는 부호화되는 전체 비트 수 중에 정정할 수 있는 비트의 수를 의미하며, 이는  $n = 2^m - 1$ 로 표현되는 갈로아체(Galois Field)

의 지수인  $m$ 으로부터  $n - k = mt$ 의 수식에 의한 관계로 정의된다.  $k$ 는 실제 데이터의 비트 수를 의미하며,  $n - k = mt$ 에서  $mt$ 개의 패리티(parity) 비트로부터  $t$ 개의 데이터 전송상에서 생길 수 있는 오류를 정정할 수 있다.

[0018] 도 1은 본 발명의 일실시예에 있어서, BCH 복호기를 도시한 블록도이다.

[0019] 도 1을 참조하면, 일반적으로 사용되는 BCH 복호기(100)의 구조는 도 1과 같이 오류  $t$ 를 감지하고 정정하는 세 개의 주요한 부분(110, 120, 130)으로 구성되어 있다. 첫 번째 부분은 신드롬 계산부(110)이고, 신드롬 계산부(110)가 신드롬 다항식  $S(x)$ 를 생성하고 수신된 코드워드(codeword)의 오류 패턴을 표현한다. 신드롬 다항식  $S(x)$ 는 BCH 복호기의 두 번째 부분인 KES부(120)에서 사용된다. KES부(120)은 해결 방정식(Key equation)을 해결하기 위해 벨르캄프-메시(Berlecamp-Massay) 알고리즘, 유클리드(Euclidean) 알고리즘, 수정 유클리드(Modified Euclidean) 알고리즘 등이 오류 위치 다항식(error locator polynomial)  $A(x)$ 을 구하기 위하여 사용될 수 있다. 또한 기존의 벨르캄프-메시 알고리즘을 구조적으로 개선한 RiBM 알고리즘이 존재한다. 그리고 이를 보다 간략화시킨 SiBM 알고리즘이 존재한다.

[0020] 본 발명에 따른 PF-SiBM 구조는 고속화 저 복잡도 구조로 만들기 위해 위의 SiBM 알고리즘을 재공식화하였다. SiBM 알고리즘상에서  $\tilde{A}$  다항식의 계산은 수학식 1과 같다.

[0021] [수학식 1]

[0022] 
$$\tilde{\delta}_i(r+1) = \gamma(r) \cdot \tilde{\delta}_{i+2}(r) - \tilde{\delta}_0(r) \cdot \tilde{\theta}_{i+1}(r) \quad (i = 0, 1, \dots, 2t)$$

[0023] 하지만  $\tilde{\theta}_0(r)$ 의 값은 계산에 사용되어지지 않고 저장될 필요도 없으므로  $\tilde{\theta}$  다항식의 초기 입력 순서를 바꾸고  $\tilde{A}$  다항식의 갱신을 수학식 2와 같이 표현할 수 있다.

[0024] [수학식 2]

[0025] 
$$\tilde{\delta}_i(r+1) = \gamma(r) \cdot \tilde{\delta}_{i+2}(r) - \tilde{\delta}_0(r) \cdot \tilde{\theta}_i(r) \quad (i = 0, 1, \dots, 2t)$$

[0026] 또한 SiBM에 사용되는 조건문의 변수  $k$ 는 알고리즘 진행 중에 결코 음수가 되지 않고 이는 곧 데이터 처리에 영향을 끼치지 않는다는 것을 의미하므로 삭제하였다. PF-SiBM 알고리즘은 표 1과 같다.

[0027] [표 1]

[0028]

**The PF-SiBM Algorithm:**

[수학식 3] **Initialization:**

$$\delta_{2t}(0) = 1; \delta_{2t-1}(0) = 0;$$

$$\theta_{2t-1}(0) = 1; \theta_i(0) = 0, (i = 2t, 2t-2);$$

$$\gamma(0) = 1;$$

[수학식 4] **Input:**  $S_i, (i = 0, 1, \dots, 2t-2)$

$$\delta_i(0) = S_i, (i = 0, 1, \dots, 2t-2)$$

$$\theta_i(0) = S_{i+1}, (i = 0, 1, \dots, 2t-3)$$

for  $r = 0$  step 1 until  $t-1$  do  
begin  
Step PF-SiBM.1  
for  $l = 0$  step 1 until  $ff-1$  do  
begin

[수학식 5]  $\delta_{i,ff+1}(r+1) =$

$$\gamma(r) \cdot \delta_{i,ff+1+2}(r) - \delta_0(r) \cdot \theta_{i,ff+1}(r), \quad (i = 0, 1, \dots, \text{NoP} - 1)$$

end  
Step PF-SiBM.2  
begin

if  $\delta_0(r) \neq 0$  then  
begin

for  $l = 0$  step 1 until  $ff-1$  do  
begin

[수학식 6]  $\theta_{i,ff+1}(r+1) = \delta_{i,ff+1+2}(r), \quad (i = 0, 1, \dots, \text{NoP} - 1)$

end

[수학식 7]  $\gamma(r+1) = \delta_0(r)$

end

else  
begin

for  $l = 0$  step 1 until  $ff-1$  do  
begin

[수학식 8]  $\theta_{i,ff+1}(r+1) = \theta_{i,ff+1}(r), \quad (i = 0, 1, \dots, \text{NoP} - 1) \quad (i = 0, 1, \dots, \text{NoP} - 1)$

end

[수학식 9]  $\gamma(r+1) = \gamma(r)$

end

Step PF-SiBM.3 if  $r \neq t-1$

[수학식 10]  $\theta_i(r+1) = 0, (i = 2t-2r-3, 2t-2r-4),$

end

[수학식 11] **Output :**  $\lambda_i(t) = \delta_i(t), (i = 0, 1, \dots, t)$

[0029] 도 2는 본 발명의 일실시예에 따른 PF-SiBM 구조를 나타내는 도면이다.

- [0030] BM 알고리즘의 구조는 피드백 구조 때문에 파이프라인 방법을 적용하기 어렵다고 알려져 있다. 본 발명에서 제안한 PF-SiBM 구조는 내부 루프를 실행하기 위해  $\tilde{\Delta}$ 와  $\tilde{\Theta}$ 의 다항식의 상수를 몇몇 그룹으로 나눈다. 내부 루프 안에 있는 각각의 상수는  $(ff+ps)$  클럭 주기동안 피드-포워드(feed-forward) 방식으로 연속적으로 계산된다. 그러므로 내부 루프 안의 파이프라인화는 내부 루프 안의 단일 파이프라인화 스테이지마다 하나의 클럭 주기만큼 동작 시간을 증가시킨다. 그 결과에 따라서 KES부(120)의 전체적인 동작 시간은  $t \times (ff + ps)$ 가 된다.  $ps$ 는 GF 곱셈기(multiplier)의 파이프라인화 스테이지의 깊이이다.
- [0031] 진술한대로, BCH 복호기는 주요 블록들 사이의 동작 시간이 불일치하기 때문에 KES부(120)에서 대기 상태로 길게 남아있게 되는데 이 대기 시간을 이용하여 KES부(120)에 파이프라인 구조와 폴딩 구조를 적용할 수 있다. 결과적으로 구현된 고속 낮은 복잡도의 PF-SiBM 구조는 도 3에 보여진다.
- [0032] 도 2, 도 3 내지 도 4를 참조하면, 시간 인덱스  $r$ 과  $l$ 이 모든 변수에 인덱스되어 있다.  $r$ 과  $l$ 이 인덱스 된 변수의 값은 각각 외부 루프와 내부 루프에 의해 바뀐다. 또한  $r$ 과  $l$ 이 모두 인덱스 된 변수의 값은 외/내부 모든 루프에 의해 바뀐다.
- [0033] 비록 기존 BM 구조의  $\tilde{\delta}(r)$ , 불합도는 시간 인덱스  $r$ 에 관계 없이 항상 0번째 레지스터에 고정되어 저장될 수 있지만 본 발명에서 제안하는 구조는 내부 루프가 실행되는 동안 핵심 제어 장치(Main Control Unit)(210)의 레지스터에 저장되어야 한다. 또한 다른 2개의 변수  $y(r)$ 와  $MC(r)$  역시 내부 루프가 실행되는 동안 고정될 필요성이 있다. 이러한 변수들을 고정하기 위해 몇몇 멀티플렉서와 레지스터들이 핵심 제어 장치(210)에 추가되었다. 내부 루프는  $(ff+ps)$  클럭 주기 동안 실행되고, 모듈러- $(ff+ps)$  카운터(410)와 비교기(420)를 사용하는 핵심 제어 장치(210)로부터 생성되는 LC신호에 의해 제어된다. 핵심 제어 장치(210)는 도 4에 보다 자세한 구성이 도시되어 있다.
- [0034] 세타 제어 장치(Theta Control Unit)(220)는 도 2의 점선안에 보여진다. 세타 제어 장치(220)는 기존의 RiBM 으로부터 오류 값 다항식을 계산하는 하드웨어 부분을 제거하기 위한 PF-SiBM의 스텝 3를 수행하는 구역이며 하드웨어로 구현하기 위해 모듈러-동작시간 카운터(240)와 비교기(250)를 사용한다. 핵심 제어 장치(210)와 세타 제어 장치(220)의 모든 출력은 임계 경로 지연(critical path delay)이 발생하지 않게 하기 위해 파이프라인화 하였다.
- [0035] 도 2에서 보여지는 PE(230)는 PF-SiBM 알고리즘의 모든 단계를 동시에 수행한다. 도 3에 폴딩 인수가 5일 때의 PE의 자세한 구조가 나타나 있다. 이 PE안에 존재하는 2개의 유한체 곱셈기(Finite Field Multiplier, 이하 'FFM')(311, 312)가 복호기의 면적과 동작 속도에 가장 큰 영향을 미치는 중요한 연산 장치이다. 본 발명에 따라 제안되는 PF-SiBM 구조의 FFM(311, 312)은  $GF(2^m)$ ,  $9 = m = 16$ 의 범위 하에서만 논의한다. 실용적으로 사용하기에  $m$ 이 9보다 작으면 너무 짧은 블록길이밖에 제공할 수 없고  $m$ 이 16이면 충분히 긴 블록길이(65,535비트)를 제공하기 때문이다. 이러한 제한하에서 FFM의 임계 경로 지연은 다음과 같다.

$$pp \cdot T_{xor2} + T_{and2} + [\log 2(m)] \cdot T_{xor2}$$

- [0036]
- [0037]  $pp$ 는 주어진 원시다항식에 의해 2 또는 3의 값을 가진다. 따라서 FFM의 총 경로 지연은  $T_{and2} + 6 \cdot T_{xor2}$  또는  $T_{and2} + 7 \cdot T_{xor2}$ 이다.
- [0038] FFM(311, 312) 내부에 파이프라인 위치를 선택할 때 신드롬 계산부(110)와 치옌 서치부(130)의 경로 지연을 고려하였다. 신드롬 계산부(110)와 치옌 서치부(130)는 모두 최악의 경로 지연 시간은  $T_{mult} + T_{add}$ 이며, 그 값은  $5T_{xor2}$ 이다. 이 값을 줄이기 위해 신드롬 계산부(110)와 치옌 서치부(130)를 파이프라인할 경우, 치옌 서치부(130)의 피드백(feedback) 구조와 긴 연산 주기 때문에 복호기의 총 동작 시간이 받아들일 수 없을 정도로 많이 증가될 것이다. 그러므로, FFM(311, 312) 내부의 AND-plane 위에 1개의 파이프라인을 넣었다. 이렇게 함으로서 FFM(311, 312)의 내부에는 새롭게  $m$ -비트(bit) 레지스터 4개가 추가되었고 임계 경로 지연은  $T_{and2} + 4 \cdot T_{xor2}$ 가 되었다. 이는 제안된 KSE부(120)가 신드롬 계산부(110), 치옌 서치부(130)와 거의 같은 클럭 속도에서 동작하게끔 만들어 준다.

- [0039] 도 3은 폴딩 인수가 5일 때의 구조를 보여준다.
- [0040] 도 3을 참조하면, PE(230) 내부에 존재하는  $\tilde{\theta}$  다항식과  $\tilde{\Delta}$  다항식의 계수를 저장하는 레지스터들 중, 점선 안의 레지스터(313, 314)는 폴딩 인수에 따라 자유롭게 조절이 가능하다. 이 레지스터의 수를 적절하게 조정함으로써 설계자는 3이상의 폴딩 인수를 자유롭게 선택이 가능하다. 폴딩 인수가 3일 경우 점선 안의 레지스터들은 존재하지 않게 된다. 그때는 최악의 경우로  $\tilde{\theta}$  다항식 안의 피드백 루프에서  $T_{add} + T_{mux2} + T_{pmult}$ , 즉  $T_{mux2} + 4T_{xor2}$ 를 가지는 새로운 임계 경로 지연이 생기게 된다.
- [0041] 이상의 결과, 본 발명에 따른 PF-SiBM 구조는 오류 위치 다항식을 계산하기 위해  $t \times (ff+1)+1$ 의 클럭 주기를 필요로 하며, 종래의 폴딩 구조와 비교하여 자유롭게 폴딩 인수를 선택할 수 있다.
- [0042] 또한 본 발명에 따른 PF-SiBM 구조는  $T_{and2}+4 \cdot T_{xor2}$ 의 임계 경로 지연을 갖고, 합성 결과는 종래의 BM 구조에 비해 62% 빨라진 클럭 속도인 625MHz를 가질 수 있음을 보였으며, 이는 파이프라인화 ME 구조와 비슷한 클럭 속도이다.
- [0043] 또한 본 발명에서 제안된 구조는 3이상의 어떠한 폴딩 인수로도 구현될 수 있고, 홀수의 폴딩 인수를 적용할 수 없었던 종래의 f-SiBM 구조와 비교하여 훌륭한 폴딩 확장성을 제공한다. 일례로 폴딩 인수가 25일 경우 본 발명에서 제안된 구조는 SiBM 구조에 비해 87.4%, 폴딩 인수 24를 가지는 f-SiBM 구조에 비해 26%의 면적-시간 복잡도의 향상을 가져온다.
- [0044] 상기와 같이 본 발명에 따른 PF-SiBM 기반의 고속 저 복잡도 VLSI 구조는 높은 클럭 속도를 제공하며 따라서 f-SiBM에 비교하여 짧은 경로 지연 시간을 가지게 된다.
- [0045] 또한 본 발명에 따른 오류 위치 연산 회로 및 연산 방법은 훌륭한 폴딩 확장성을 제공하며, 이는 설계자로 하여금 특정 설계 요구 조건에 맞추어 자유롭게 폴딩 인수를 적용할 수 있도록 한다.
- [0046] 또한 본 발명에서 제안한 PF-SiBM 구조는 광대역 통신 시스템을 위한 고속 저 복잡도의 BCH 복호기 응용 분야에 잠재 적용 실예를 가지고 있다.
- [0047] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명 사상은 아래에 기재된 특허청구범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

### 도면의 간단한 설명

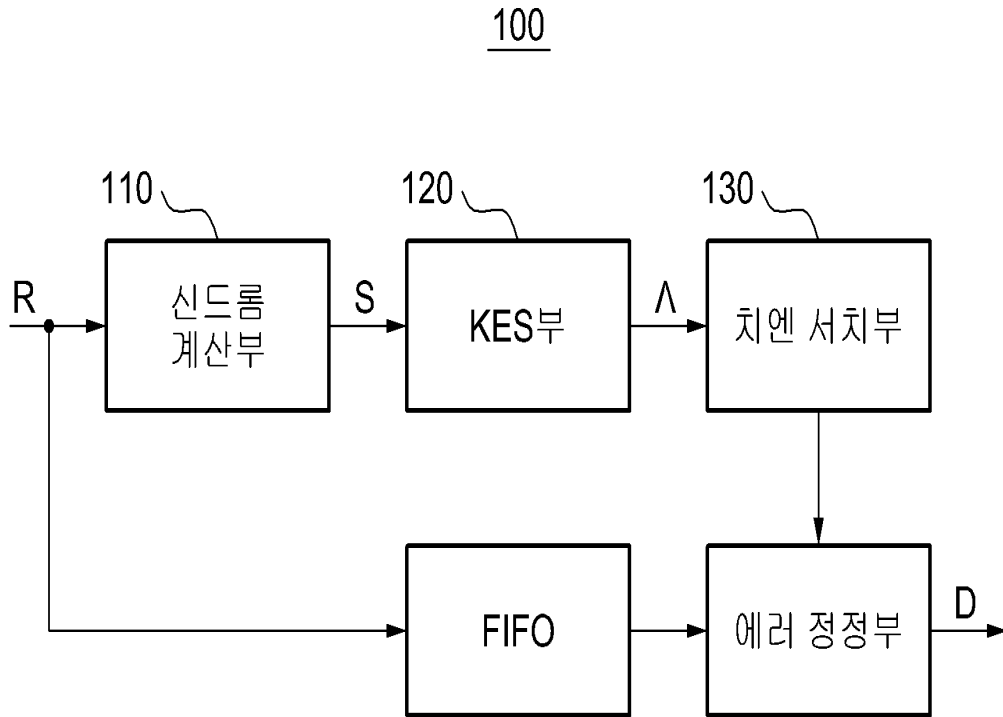
- [0048] 도 1은 본 발명의 일실시예에 있어서, BCH 복호기를 도시한 블록도이다.
- [0049] 도 2는 본 발명의 일실시예에 있어서, 파이프라인화 폴딩 구조 SiBM(PF-SiBM) 알고리즘 연산 회로를 도시한 도면이다.
- [0050] 도 3은 본 발명의 일실시예에 있어서, 폴딩 팩터가 5일 경우의 PE 회로를 도시한 도면이다.
- [0051] 도 4는 본 발명의 일실시예에 있어서, PF-SiBM 알고리즘 연산 회로의 핵심 제어 장치를 도시한 도면이다.
- [0052] <도면의 주요 부분에 대한 부호의 설명>
- [0053] 100: BCH 복호기
- [0054] 110: 신드롬 계산부
- [0055] 120: KES부
- [0056] 130: 치엔 서치부
- [0057] 210: 핵심 제어 장치
- [0058] 220: 세타 제어 장치
- [0059] 230: PE

[0060] 240: 모듈러-동작시간 카운터

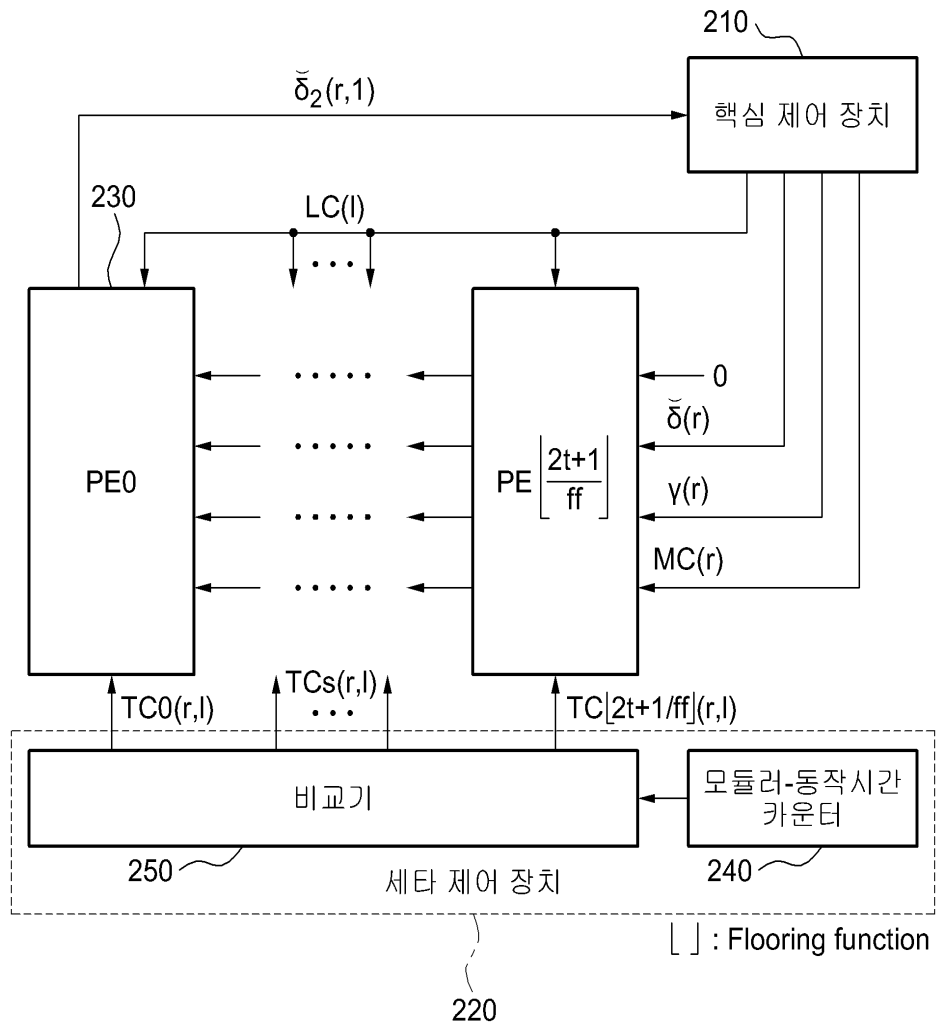
[0061] 250: 비교기

도면

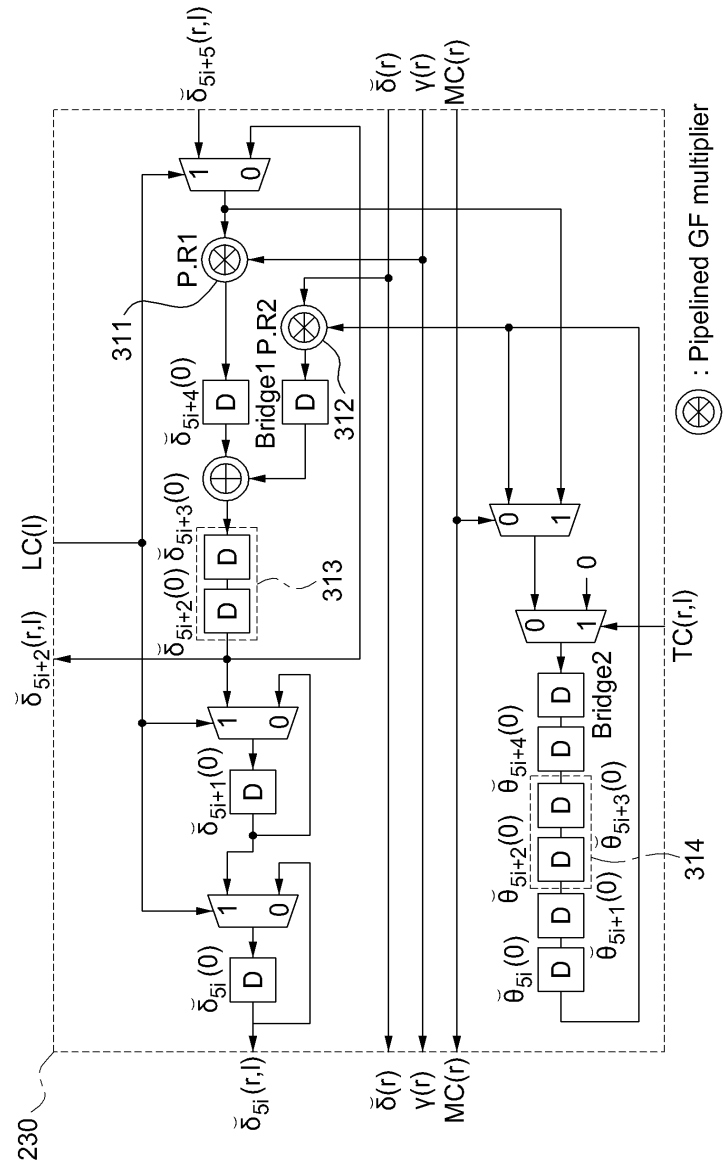
도면1



도면2



도면3



도면4

