



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0110359
(43) 공개일자 2017년10월11일

(51) 국제특허분류(Int. Cl.)
G06F 7/58 (2006.01) G06F 17/18 (2006.01)
G06F 7/57 (2006.01)
(52) CPC특허분류
G06F 7/58 (2013.01)
G06F 17/18 (2013.01)
(21) 출원번호 10-2016-0034642
(22) 출원일자 2016년03월23일
심사청구일자 2016년03월23일

(71) 출원인
서울대학교산학협력단
서울특별시 관악구 관악로 1 (신림동)
울산과학기술원
울산광역시 울주군 언양읍 유니스트길 50
(72) 발명자
최기영
서울특별시 서초구 효령로 164, 1동 103호 (방배동, 신동아아파트)
이종은
울산광역시 남구 거마로 22, 102동 1203호 (옥동, 대륙1차현대아파트)
김경훈
경기도 수원시 영통구 동탄원천로881번길 35, 503동 1503호 (매탄동, 주공그린빌)
(74) 대리인
리엔목특허법인

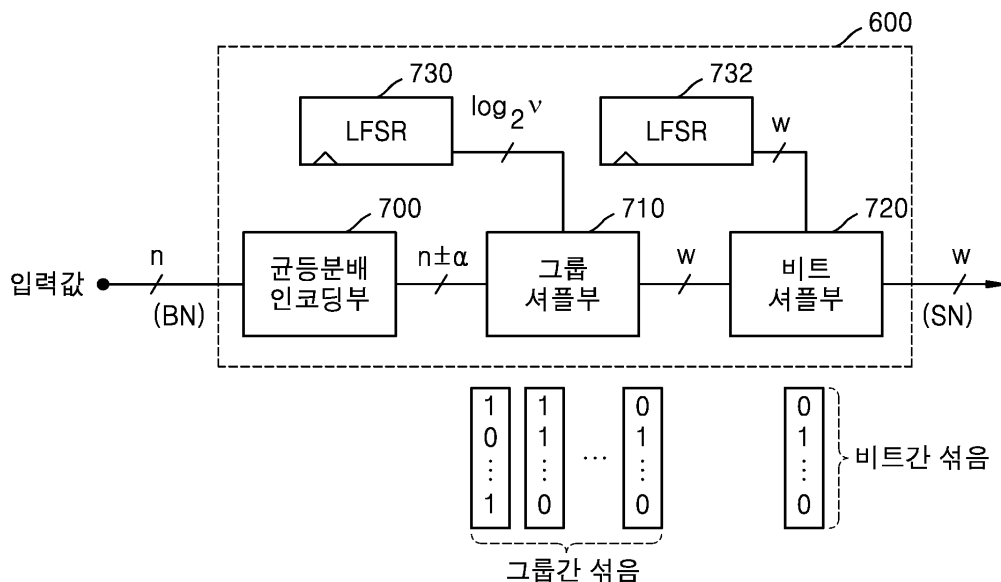
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 이진수를 난수로 변환 또는 난수를 이진수로 변환하는 방법 및 그 장치

(57) 요약

확률 컴퓨팅을 위하여 이진수를 난수로 변환 또는 난수를 이진수로 변환하는 방법 및 그 장치가 개시된다. 이진수-난수 변환 장치는 입력값을 복수 개의 비트로 구성된 복수 개의 그룹으로 균등분배 인코딩한 후 복수 개의 그룹의 그룹 순서를 섞고, 각 그룹 내 비트들의 비트 순서를 섞어 생성한 난수를 출력한다.

대표도 - 도7



(52) CPC특허분류
G06F 7/57 (2013.01)

명세서

청구범위

청구항 1

입력값을 복수 개의 비트로 구성된 복수 개의 그룹으로 인코딩하는 단계;

상기 복수 개의 그룹의 그룹 순서를 섞는 단계;

각 그룹 내 비트들의 비트 순서를 섞는 단계; 및

상기 그룹 순서 및 상기 비트 순서를 임의로 섞은 복수 개의 그룹을 상기 입력값에 대한 난수값으로 출력하는 단계;를 포함하는 것을 특징으로 하는 이진수-난수 변환 방법.

청구항 2

제 1항에 있어서, 상기 인코딩하는 단계는,

상기 복수 개의 그룹에 1 이상의 가중치를 부여하고, 그룹에 포함된 1의 개수의 최대값과 최소값의 차이가 상기 가중치 이하가 되도록 인코딩하는 단계;를 포함하는 것을 특징으로 하는 이진수-난수 변환 방법.

청구항 3

제 1항에 있어서, 상기 그룹 순서를 섞는 단계는,

상기 복수 개의 그룹을 비트 배열 형태에 따라 적어도 둘 이상의 서브영역으로 분할하는 단계;

상기 둘 이상의 서브영역 중 어느 하나를 선택하는 선택신호를 그룹의 개수만큼 생성하는 단계; 및

상기 선택신호에 해당하는 서브영역 내 그룹을 선택하여 출력하는 단계;를 포함하는 것을 특징으로 하는 이진수-난수 변환 방법.

청구항 4

제 1항에 있어서, 상기 비트 순서를 임의로 섞는 단계는,

각 그룹에 대해, 비트 위치와 가중치를 고려하여 각 비트를 복수 개 복제한 EP set을 각 비트별로 생성하고, 상기 가중치에 해당하는 개수의 초기 EP set을 생성하는 단계;

각 그룹에 대해, 서로 다른 EP set에 포함된 비트를 일대일 맵핑하는 단계; 및

각 그룹에 대해, 일대일 맵핑된 비트의 출력 순서를 임의로 섞는 단계;를 포함하는 것을 특징으로 하는 이진수-난수 변환 방법.

청구항 5

제 4항에 있어서,

입력값이 상기 가중치와 그룹 개수의 곱보다 크면, 상기 인코딩하는 단계의 입력값을 상기 기대값에서 상기 가중치와 그룹 개수의 곱을 차감한 값으로 조정하고, 상기 추가 값을 1로 설정하는 단계; 및

입력값이 상기 가중치와 그룹 개수의 곱보다 작으면, 상기 추가 값을 0으로 설정하는 단계;를 더 포함하는 것을 특징으로 하는 이진수-난수 변환 방법.

청구항 6

입력값을 복수 개의 비트로 구성된 복수 개의 그룹으로 인코딩하는 균등분배인코딩부;

상기 복수 개의 그룹의 그룹 순서를 섞는 그룹서플부; 및

각 그룹 내 비트들의 비트 순서를 섞어 출력하는 비트서플부;를 포함하는 것을 특징으로 하는 이진수-난수 변환

장치.

청구항 7

제 6항에 있어서, 상기 균등분배인코딩부는,

상기 복수 개의 그룹에 1 이상의 가중치를 부여하고, 그룹에 포함된 1의 개수의 최대값과 최소값의 차이가 상기 가중치 이하가 되도록 인코딩하는 것을 특징으로 하는 이진수-난수 변환 장치.

청구항 8

제 6항에 있어서, 상기 그룹서플부는,

비트 배열 형태에 따라 적어도 둘 이상의 서브영역으로 구분되는 복수 개의 그룹에 대해, 상기 둘 이상의 서브영역 중 어느 하나를 임의로 선택하는 선택신호에 따라 해당하는 서브영역의 그룹을 선택하여 출력하는 것을 특징으로 하는 이진수-난수 변환 장치.

청구항 9

제 6항에 있어서, 상기 비트서플부는,

각 그룹에 대해, 비트 위치와 가중치를 고려하여 각 비트의 값을 복수 개 복제하고, 상기 가중치에 해당하는 개수의 추가 값을 생성하고, 각 비트의 값과 하위 비트의 값의 일대일 맵핑관계를 형성하되, 최하위 비트의 값은 추가 값과 일대일 맵핑관계를 형성하고, 일대일 맵핑관계의 값들 중 기 설정된 확률로 어느 하나의 값을 출력하는 것을 특징으로 하는 이진수-난수 변환 장치.

청구항 10

AND 게이트와 OR 게이트를 교대로 배치한 적어도 하나 이상의 레이어를 이용하여 난수를 입력받아 출력하는 단계; 및

상기 레이어의 출력값에 포함된 1의 개수를 병렬 카운터를 이용하여 세는 단계;를 포함하는 것을 특징으로 하는 난수-이진수 변환 방법.

청구항 11

AND 게이트와 OR 게이트를 교대로 배치한 레이어를 적어도 하나 이상 포함하는 근사유닛; 및

상기 근사유닛의 출력값에 포함된 1의 개수를 세는 병렬 카운터;를 포함하는 것을 특징으로 하는 난수-이진수 변환 장치.

청구항 12

제 1항 내지 제 5항 및 제10항 중 어느 한 항에 기재된 방법을 수행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체,

발명의 설명

기술 분야

[0001] 본 발명은 확률 컴퓨팅(stochastic computing)을 위하여 이진수를 난수로 변환하거나, 난수를 이진수로 변환하는 방법 및 그 장치에 관한 것이다.

배경 기술

[0002] 확률 컴퓨팅은 난수를 사용하여 산술 연산을 하는 계산 방법으로 종래의 고정 또는 부동 소수점의 이진수 연산보다 저전력 회로를 구현할 수 있는 장점이 있다.

[0003] 도 1은 종래 확률 컴퓨팅을 이용한 연산의 일 예를 도시한 도면이다.

- [0004] 도 1을 참조하면, 확률 컴퓨팅에서 곱셈은 AND 게이트로 구현되므로, 이는 종래 이진수 곱셈기에 비해 회로 면적과 소비전력이 적다. 확률 컴퓨팅에서 숫자는 전체 비트 수 중 1의 개수로 표현된다. 예를 들어, 6/8이라는 숫자는 전체 8개의 비트 중 1을 가진 6개의 비트로 표현한다. 마찬가지로 4/8이라는 숫자는 전체 8개의 비트 중 4개의 1로 표현된다. 이와 같이 확률 컴퓨팅은 전체 비트들 중 포함되는 1의 개수로 숫자를 표현한다. 다만, 확률 컴퓨팅에서는 전체 비트들 중 임의의 위치에 '1'를 배치시킨 난수를 활용하여 수를 계산하므로 기존의 이진수 계산 방법보다 정확도가 떨어질 수 있다.
- [0005] 도 2는 종래 확률 컴퓨팅을 위한 이진수-난수 변환기의 일 예를 도시한 도면이고, 도 3은 도 2의 LFSR의 상세 구성의 일 예를 도시한 도면이다.
- [0006] 도 2 및 도 3을 참조하면, 종래 이진수-난수 변환기(randomizer)는 LFSR(Linear Feedback Shift Register)의 입력과 이진수(binary number, BN)의 입력을 비교하여 0 또는 1을 출력함으로써 확률 컴퓨팅을 위한 난수를 생성한다. 그러나 종래 이진수-난수 변환기는 한 개의 비트를 생성하기 위하여 회로 전체가 구동되므로 에너지가 많이 소비된다. 많은 비트의 난수를 생성하는 LFSR 회로를 이용하여 적은 비트 수의 난수를 생성하는 것은 Progressive computing이라는 확률 컴퓨팅 방법에 매우 중요한 요소이다. 그러나, 종래 이진수-난수 변환기는 많은 비트의 난수를 생성하는 LFSR 회로를 사용하여 적은 비트의 난수를 생성하면 난수의 정확도가 떨어지는 문제점이 있다.
- [0007] 도 4는 종래 확률 컴퓨팅을 위한 난수-이진수 변환기의 일 예를 도시한 도면이다.
- [0008] 도 4를 참조하면, 종래 난수-이진수 변환기는 비트 스트림에서 1의 개수를 세는 것과 같으므로, 일반적인 직렬 카운터(serial counter)나 도 4와 같이 병렬 카운터(parallel counter)를 사용하여 구현된다. 직렬 카운터는 병렬 카운터에 비하여 효율이 상대적으로 좋지 않다.
- [0009] 도 5는 LFSR을 사용하는 종래 이진수-난수 변환기를 이용한 난수 생성에 대한 실험 결과의 일 예를 도시한 도면이다.
- [0010] 도 5를 참조하면, 종래 이진수-난수 변환기는 0.75에 대한 난수를 발생할 때, 2^{10} 에서는 정확한 값을 얻지만, 2^5 , 2^6 , 2^7 비트 난수 등에서는 값이 정확하지 않음을 알 수 있다.

선행기술문헌

특허문헌

- [0011] (특허문헌 0001) 등록특허공보 제10-1443575호

발명의 내용

해결하려는 과제

- [0012] 본 발명이 이루고자 하는 기술적 과제는, 난수의 정확도를 향상시킬 뿐만 아니라 작은 면적과 저전력으로 구현 가능한 이진수-난수 변환 또는 난수-이진수 변환 방법 및 그 장치를 제공하는 데 있다.

과제의 해결 수단

- [0013] 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 이진수-난수 변환 방법의 일 예는, 입력값을 복수 개의 비트로 구성된 복수 개의 그룹으로 인코딩하는 단계; 상기 복수 개의 그룹의 그룹 순서를 섞는 단계; 각 그룹 내 비트들의 비트 순서를 섞는 단계; 및 상기 그룹 순서 및 상기 비트 순서를 임의로 섞은 복수 개의 그룹을 상기 입력값에 대한 난수값으로 출력하는 단계;를 포함한다.
- [0014] 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 이진수-난수 변환 장치의 일 예는, 입력값을 복수 개의 비트로 구성된 복수 개의 그룹으로 인코딩하는 균등분배인코딩부; 상기 복수 개의 그룹의 그룹 순서를 섞는 그룹셔플러; 및 각 그룹 내 비트들의 비트 순서를 섞어 출력하는 비트셔플러;를 포함한다.
- [0015] 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 난수-이진수 변환 방법의 일 예는, AND 게이트와 OR 게이트를 교대로 배치한 적어도 하나 이상의 레이어를 이용하여 난수를 입력받아 출력하는 단계; 및 상기 레이어의

출력값에 포함된 1의 개수를 병렬 카운터를 이용하여 세는 단계;를 포함한다.

[0016] 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 난수-이진수 변환 장치의 일 예는, AND 게이트와 OR 게이트를 교대로 배치한 레이어를 적어도 하나 이상 포함하는 근사유닛; 및 상기 근사유닛의 출력값에 포함된 1의 개수를 세는 병렬 카운터;를 포함한다.

발명의 효과

[0017] 본 발명에 따르면, 난수 발생의 정확도를 향상시킬 수 있으며, 이진수-난수 변환기 및 난수-이진수 변환기를 작은 면적 및 저전력으로 구동가능한 회로로 구현할 수 있다.

도면의 간단한 설명

[0018] 도 1은 종래 확률 컴퓨팅을 이용한 연산의 일 예를 도시한 도면,
 도 2는 종래 확률 컴퓨팅을 위한 이진수-난수 변환기의 일 예를 도시한 도면,
 도 3은 도 2의 LFSR의 상세 구성의 일 예를 도시한 도면,
 도 4는 종래 확률 컴퓨팅을 위한 난수-이진수 변환기의 일 예를 도시한 도면,
 도 5는 LFSR을 사용하는 종래 이진수-난수 변환기를 이용한 난수 생성에 대한 실험 결과의 일 예를 도시한 도면,
 도 6은 본 발명에 따른 이진수-난수 변환장치의 입출력 구조의 일 예를 도시한 도면,
 도 7은 본 발명에 따른 이진수-난수 변환장치의 일 실시 예의 구성을 도시한 도면,
 도 8 및 도 9는 본 발명에 따른 균등분배 인코딩 방법의 일 예를 도시한 도면,
 도 10은 본 발명에 따른 복수 개의 그룹의 그룹순서를 섞는 방법의 일 예를 도시한 도면,
 도 11은 도 8의 각 그룹을 도 10의 그룹서플부를 이용하여 섞은 결과를 도시한 도면,
 도 12는 본 발명에 따른 그룹서플부를 논리회로로 구현한 일 예를 도시한 도면,
 도 13은 도 14에 도시된 본 발명에 따른 비트서플부의 기호를 정의한 도면,
 도 14는 본 발명에 따라 각 그룹 내 비트를 섞는 방법의 일 예를 도시한 도면,
 도 15는 본 발명에 따른 이진수-난수 변환 방법의 일 실시 예의 흐름을 도시한 도면,
 도 16은 본 발명에 따른 이진수-난수 변환 방법의 정확도 실험결과에 대한 일 예를 도시한 도면,
 도 17은 본 발명에 따른 이진수-난수 변환 장치를 회로로 구현한 경우의 성능실험 결과의 일 예를 도시한 도면,
 도 18은 본 발명에 따른 난수-이진수 변환 장치의 일 예를 개략적으로 도시한 도면,
 도 19는 본 발명에 따른 난수-이진수 변환 장치의 상세 구성의 일 예를 도시한 도면,
 도 20은 본 발명에 따른 난수-이진수 변환 장치를 회로로 구현한 경우의 성능 실험결과에 대한 일 예를 도시한 도면, 그리고,
 도 21은 본 발명에 따른 난수-이진수 변환 방법의 정확도 실험결과에 대한 일 예를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하에서, 첨부된 도면들을 참조하여 본 발명에 따른 이진수-난수 변환 방법 및 그 장치와, 난수-이진수 변환 방법 및 그 장치에 대해 살펴본다.

[0020] 도 6은 본 발명에 따른 이진수-난수 변환장치의 입출력 구조의 일 예를 도시한 도면이고, 도 7은 본 발명에 따른 이진수-난수 변환장치의 일 실시 예의 구성을 도시한 도면이다.

[0021] 도 6 및 도 7을 참조하면, 이진수-난수 변환장치(600)는 n (n 은 1 이상의 자연수) 비트의 이진수를 입력받으면, w (1 이상의 자연수) 개의 비트로 구성된 v (1 이상의 자연수) 개의 그룹으로 구성된 난수를 출력한다. 이하에서, 각 구성별로 상세히 살펴본다.

- [0022] 이진수-난수 변환장치(600)는 균등분배인코딩부(700), 그룹서플부(710) 및 비트서플부(720)를 포함한다.
- [0023] 균등분배인코딩부(700)는 입력값을 동일한 비트 개수를 포함하는 복수 개의 그룹으로 인코딩한다. 이때, 균등분배인코딩부(710)는 각 그룹이 가지고 있는 1의 개수가 가중치(b)와 같거나 이보다 작도록 인코딩한다. 예를 들어, i번째 그룹의 1의 개수가 g_i 라고 하면, g_i 가 가장 큰 그룹과 g_i 가 가장 작은 그룹은 다음과 같은 관계가 된다.

수학적 1

$$\max_{i \in v} g_i - \min_{i \in v} g_i \leq b$$

[0024]

- [0025] 여기서, 가중치(b)는 실시 예에 따라 다양하게 미리 설정되는 값이다. 도 8에는 가중치(b)가 3인 경우에 입력값 237을 균등분배 인코딩한 결과가 도시되어 있고, 도 9에는 가중치(b)가 1인 경우에 입력값 72를 균등분배 인코딩한 결과가 도시되어 있다. 도 8의 경우, 그룹 1의 비트열인 1100은 가중치 3을 고려할 때 $36(=2^3*3*1 + 2^2*3*1 + 2*3*0 + 1*3*0)$ 을 표현하고, 그룹 3의 비트열 1011은 33을 표현한다. 즉, 도 8과 같이, 입력값 237을 36, 36, 33, 33, 33, 33, 33을 각각 표현하는 비트열로 구성된 복수 개의 그룹으로 인코딩할 수 있다. 균등분배 인코딩 방법에 대해서는 도 8 및 도 9에서 다시 설명한다.

- [0026] 그룹서플부(710)는 균등분배인코딩부(700)에 의해 생성된 복수 개의 그룹의 그룹 순서를 임의로 섞는다. 본 실시 예는 LFSR(730)을 이용하여 복수 개의 그룹의 순서를 섞는 예를 도시하고 있으나 반드시 이에 한정되는 것은 아니며, 복수 개의 그룹의 순서를 다른 다양한 방법을 이용하여 섞을 수 있다. 작은 면적과 저전력의 회로로 구현 가능한 그룹서플부(710)의 일 예에 대해서는 도 10에서 설명한다.

- [0027] 비트서플부(720)는 각 그룹 내 비트들의 비트 순서를 임의로 섞는다. 본 실시 예는 LFSR(732)을 이용하여 각 그룹 내 비트의 순서를 섞는 예를 도시하고 있으나 반드시 이에 한정되는 것은 아니며, 각 그룹의 비트 순서를 다른 다양한 방법을 이용하여 섞을 수 있다. 작은 면적과 저전력의 회로로 구현 가능한 비트서플부(720)의 일 예에 대해서는 도 14에서 설명한다.

- [0028] 예를 들어, 도 14에 도시된 비트서플부(720)를 이용하여 비트 순서를 임의로 섞을 때, 가중치(b)에 따른 초기 비트 셋(1400)이 존재하므로, 균등분배인코딩부(700)에 입력되는 입력값의 조정이 필요하다. 예를 들어, 도 8과 같이, 가중치(b) 3을 이용하여 7개의 그룹으로 균등분배 인코딩할 때, 입력값 258을 그대로 균등분배인코딩부(700)에 입력하는 것이 아니라 조정된 입력값(= 입력값 - 가중치(b)*그룹개수 = $258 - 3*7 = 237$)을 균등분배인코딩부(700)에 입력한다.

- [0029] 도 8 및 도 9는 본 발명에 따른 균등분배 인코딩 방법의 일 예를 도시한 도면이다.

- [0030] 도 8을 참조하면, 균등분배인코딩부(700)는 입력값 237을 동일 개수의 비트로 구성된 복수 개의 그룹으로 인코딩한다. 즉, $237=36+36+33+33+33+33+33$ 이므로, 균등분배인코딩부는 가중치(b) 3(810)을 이용하여 237을 1100(36을 표현)의 비트 배열로 구성된 2개의 그룹과 1011(33을 표현)의 비트 배열로 구성된 5개의 그룹으로 인코딩한다.

- [0031] 입력값을 균등분배 인코딩하기 위한 그룹의 개수와 각 그룹 내 비트의 개수는 가중치에 따라 초기에 다양한 값으로 설정될 수 있다. 도 8은 가중치(b) 3인 경우이나, 가중치(b)가 2 또는 1이 되면, 237을 표현하기 위한 그룹의 개수와 그룹 내 비트의 개수가 변경될 수 있다. 또한, 도 8의 가중치(b)를 3으로 그대로 둔 상태에서, 그룹의 개수와 각 그룹 내 비트의 개수를 다르게 설정할 수 있다. 예를 들어, 각 그룹 내 비트의 개수를 5개로 설정하고, 최상위 비트를 모두 0으로 채울 수도 있다.

- [0032] 균등분배인코딩부(700)는 각 그룹 내 1의 개수의 최대값과 최소값의 차이가 가중치 이하가 되도록 인코딩하는데 도 8과 같이 기준점(α)(850)을 이용하여 용이하게 인코딩 할 수 있다.

- [0033] 먼저, 균등분배인코딩부(700)는 복수의 그룹이 세로로 배열된 행렬 형태(800)에서, 기준점(α)(850)을 기준으로 위쪽 행(802)은 모두 1 또는 0으로 채우고, 기준점(850)과 동일 행의 왼쪽(804)은 1, 오른쪽은 0으로 채운다. 그리고 기준점(850)의 아래 행들은 기준점(850)을 기준으로 왼쪽은 0으로 채우고, 기준점(850)을 포함한 오른쪽

(806)은 1로 채운다. 도 8의 행렬에서 빈 곳은 0을 나타낸다.

- [0034] 기준점(850)은 위와 같이 행렬에 1 또는 0을 채우는 과정을 통해서 용이하게 찾을 수 있다. 예를 들어, 행렬의 첫 번째 행을 모두 1로 채우는 경우, 가중치 3을 고려할 때, 첫 번째 행의 합은 $169(2^3 * 3 * 7)$ 가 되며, 이는 입력값 237보다 작다. 따라서 첫 번째 행을 모두 1로 채운다. 그리고 두 번째 행을 모두 1로 채우면, 두 번째 행의 합은 $84(2^2 * 3 * 7)$ 가 된다. 첫 번째 행의 169와 두 번째 행의 84를 더하면, 246이 되어 입력값 237보다 크다. 따라서 두 번째 행을 모두 1로 채울 수는 없다. 기준점(850)을 두 번째 행의 가장 왼쪽부터 순차적으로 오른쪽으로 옮기면서 왼쪽에 1, 좌하측에 1을 채우는 과정을 통해 각 그룹에 표현된 총합이 237이 되는 기준점(850)의 위치를 찾을 수 있다.
- [0035] 본 실시의 기준점(850)을 이용한 균등분배 인코딩하는 방법은 하나의 예일 뿐 본 발명이 반드시 이에 한정되는 것은 아니며, 각 그룹 내 1의 개수의 차이가 가중치 이하가 되도록 인코딩할 수 있는 다양한 방법이 존재할 수 있다.
- [0036] 기준점(850)이 파악되면, 기준점(850)의 위치를 이용하여 포화(saturation) 디지털(820), 디지털 인덱스(830), 그룹 인덱스(840) 등의 값을 파악한다. 포화 디지털(820)은 기준점(850)의 윗쪽 행렬이 0 또는 1로 채워졌는지를 나타내고, 디지털 인덱스(830)와 그룹 인덱스(840)는 각각 기준점(850)의 행렬 위치를 나타낸다. 도 8의 예에서, (포화 디지털)-(디지털 인덱스)-(그룹인덱스)로 구성된 균등분배 코드값(ED Code)은 1-10-010 (또는 100-10-010)이다. 그룹 인덱스(840) 등은 이후 그룹서플부(710) 등에서 사용된다.
- [0037] 도 9를 참조하면, 입력값 76을 가중치 1, 그룹 개수 15개, 각 그룹 내 비트 수 4개로 균등분배 인코딩한 결과가 도시되어 있다. 기준점(α)을 이용하여 파악된 입력값 76에 대한 ED Code는 01-01-0001 (또는 010-01-0001)이다.
- [0038] 도 10은 본 발명에 따른 복수 개의 그룹의 그룹순서를 섞는 방법의 일 예를 도시한 도면이다.
- [0039] 도 10을 참조하면, 그룹서플부(710)는 LFSR(730)과 선택신호 발생부(1000)를 이용하여 복수 개의 그룹 간 순서를 임의로 섞는다.
- [0040] 선택신호 발생부(1000)는 LFSR(730)의 값과 도 8 및 도 9에서 살펴본 그룹인덱스(840)를 입력받아, 복수 개의 그룹 중 어느 하나를 선택할 수 있는 선택신호(G)를 발생한다. 복수 개의 그룹은, 도 8 및 도 9와 같이 기준점(α)을 중심으로 두 서브영역으로 구분될 수 있다. 즉 기준점(α)의 앞쪽에 위치한 그룹과 기준점(α)을 포함한 뒤쪽 그룹으로 구분될 수 있다. 선택신호 발생부(1000)는 기준점(α)을 중심으로 구분되는 두 서브영역 중 어느 하나를 선택하는 선택신호(G)를 발생할 수 있는데, 일 예로, 선택신호 발생부(1000)의 값이 1이면 앞쪽 그룹을 선택하고, 0이면 뒤쪽 그룹을 선택할 수 있다. 앞쪽 그룹을 선택하기 위한 1의 개수는 그룹인덱스(840)에 따라 결정된다.
- [0041] 도 10의 (b)는 도 8의 그룹을 섞는 예로서, 그룹인덱스가 '010'이므로, 기준점(α)의 앞쪽에 위치한 두 개의 그룹(그룹 0,1)을 선택하기 위한 1의 신호(1010,1012)를 7 클락 중 임의의 위치에 두 번 출력한다.
- [0042] 도 11은 도 8의 각 그룹을 도 10의 그룹서플부를 이용하여 섞은 결과를 도시한 도면이다.
- [0043] 도 11을 참조하면, 도 10(b)의 그룹 선택신호(G)는 0010100이므로, 그룹서플부는 그룹 선택신호에 따라 그룹2-그룹3-그룹0-그룹4-그룹1-그룹5-그룹6을 순차적으로 선택한다. 순서가 섞인 그룹은 비트서플부(720)로 출력된다.
- [0044] 도 12는 본 발명에 따른 그룹서플부를 논리회로로 구현한 일 예를 도시한 도면이다.
- [0045] 도 12를 참조하면, 그룹서플부의 출력값은 디지털 인덱스, 포화 디지털, 그룹 선택신호에 의해 결정됨을 알 수 있다. 이를 이용하여 그룹의 최상위 비트(A3)의 출력값을 출력하는 논리회로가 도 12의 (b)와 같이 구현될 수 있다. 다른 비트의 출력값을 출력하는 논리회로 또한 이와 같은 논리를 이용하여 구현될 수 있다.
- [0046] 도 13은 도 14에 도시된 본 발명에 따른 비트서플부의 기호를 정의한 도면이고, 도 14는 본 발명에 따라 각 그룹 내 비트를 섞는 방법의 일 예를 도시한 도면이다.
- [0047] 먼저, 도 13을 참조하여, 기호 정의를 살펴보면, (a)는 입력신호 M과 N에 대해 출력신호 X,Y를 출력하는 회로로서, S가 1인 경우 출력신호 X,Y는 입력신호 M,N과 동일하고, S가 0인 경우 출력신호 X,Y는 입력신호 M,N이 뒤집어 출력된다. 이를 좀 더 간단한 기호로 표현하면 (b)와 같다. 만약 S가 0과 1을 출력할 확률이 50%로 동일하

다고 하면, 두 입력신호 M,N은 임의의 순서로 선택된다.

[0048] 도 14는 도 13의 (b)에 정의된 기호를 이용하여 표현한 비트서플부(720)의 일 예이다. 도 14를 참조하면, 비트서플부(720)는 그룹 내 각 비트를 가중치(b)를 고려하여 복제한 동등확률 셋(Equal Probability, EP set)(1410,1420,1430)을 생성한다. 예를 들어, 가중치(b)가 2이고, 그룹이 3비트로 구성된 경우, 최상위 비트를 $2^2 \times 2 = 8$ 개로 복제한 EP set(1430)을 생성하고, 그 다음 비트를 $2^1 \times 2 = 4$ 개로 복제한 EP set(1420)을 생성하고, 마지막 비트를 2개로 복제한 EP set(1410)을 생성한다. 즉 최상위 비트의 값이 1이면, 1이 8개로 복제된 EP set(1410)이 생성된다. 또한 비트서플부(720)는 가중치에 해당하는 초기 EP set(1400)을 포함한다. 도 14의 경우, 가중치가 2이므로, 초기 EP set(1400)은 2개의 값으로 구성된다.

[0049] 비트서플부(720)는 서로 다른 EP set의 비트를 일대일 맵핑한다. 일대일 맵핑하는 방법으로 최상위 비트의 EP set(1430)의 비트를 하위 비트들의 EP set(1420,1410) 및 초기 EP set(1400)의 각 비트와 일대일 맵핑하고, 두 번째 비트의 EP set(1420)의 비트를 그 다음 하위 비트의 EP set(1410) 및 초기 EP set(1400)의 각 비트와 일대일 맵핑한다. 이와 같은 방법으로 서로 다른 EP set들의 비트를 일대일 맵핑할 수 있으며, 이를 도 13의 기호를 이용하여 표현하면 도 14와 같다.

[0050] 비트서플부(720)는 일대일 맵핑된 비트들의 출력 순서를 임의로 섞는다. 즉, 도 13에서 살핀 바와 같이 일대일 맵핑된 비트들은 LFSR(732)에 의해 확률 50%로 비트의 순서를 그대로 출력할지 아니면 그 순서를 뒤집어 출력할지 결정한다. 따라서 각 맵핑된 비트들의 순서는 임의로 섞인다.

[0051] 각 그룹의 비트에 대한 EP set(1410,1420,1430) 외에 초기 EP set(1400)이 존재하고, 초기 EP set(1400)에 의해 비트서플부의 출력 비트열의 개수가 증가하므로, 균등분배인코딩부(700)에 입력되는 입력값을 조정할 필요가 있다. 본 실시 예에서, 가중치가 2에 의해 초기 EP set(1400)이 두 개의 비트로 구성되고, 만약 그룹 개수가 m 개이며, 총 $2m$ 개의 비트가 더 출력된다.

[0052] 따라서 균등분배인코딩부(700)에 입력되는 입력값을 초기 EP set(1400)을 고려하여 조정할 필요가 있으며, 이를 수학적식으로 표현하면 다음과 같다.

수학적식 2

$$\begin{cases} \text{if } L \geq (b \cdot v), \text{ then } L \leftarrow (L - b \cdot v), S \leftarrow 1 \\ \text{otherwise, } L \leftarrow L, S \leftarrow 0 \end{cases}$$

[0053]

[0054] 여기서, L은 입력값, b는 가중치, v는 그룹의 개수, S는 추가 신호선의 값을 나타낸다.

[0055] 예를 들어, 도 8과 같이, 가중치 3, 그룹 개수 7개로 균등분배 인코딩하는 경우에, 입력값이 258이면 입력값이 가중치와 그룹 개수의 곱($21=3 \times 7$)보다 크므로, 균등분배인코딩부(700)는 입력값 258을 그대로 이용하는 것이 아니라 $258-21=237$ 을 입력값으로 사용한다.

[0056] 도 15는 본 발명에 따른 이진수-난수 변환 방법의 일 실시 예의 흐름을 도시한 도면이다.

[0057] 도 15를 참조하면, 이진수-난수 변환 장치는 입력값을 복수 개의 비트로 구성된 복수 개의 그룹으로 인코딩한다(S1500). 이때 이진수-난수 변환 장치는 각 그룹 내 포함된 1의 개수의 최대 차이가 가중치 이하가 되도록 인코딩한다. 이러한 인코딩을 위하여 도 8 및 도 9에 도시된 기준점을 이용할 수 있다.

[0058] 이진수-난수 변환 장치는 각 그룹의 그룹 순서를 임의로 섞는다(S1510). 이때 이진수-난수 변환 장치는 도 10과 같이 LFSR(730)과 도 8에서 구한 그룹 인덱스를 이용하여 각 그룹을 임의로 선택하는 선택신호를 발생하여 그룹 순서를 섞을 수 있다.

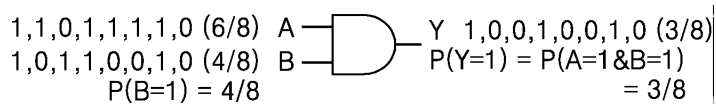
[0059] 그룹 순서를 섞은 후, 이진수-난수 변환 장치는 각 그룹 내 비트들의 순서를 임의로 섞는다(S1520). 보다 구체적으로, 이진수-난수 변환 장치는 각 그룹 내 비트에 대해 가중치를 고려하여 복제한 EP set을 생성하고, 서로 다른 EP set의 값들을 일대일 맵핑한 후, 맵핑된 비트들의 출력 순서를 임의로 결정하여 출력한다(S1530).

[0060] 도 16은 본 발명에 따른 이진수-난수 변환 방법의 정확도 실험결과에 대한 일 예를 도시한 도면이다.

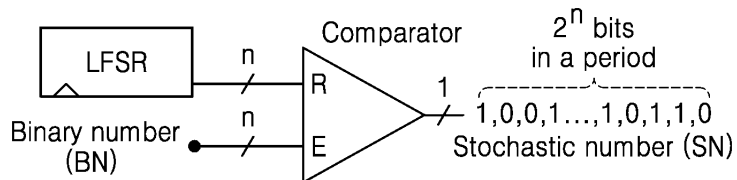
- [0061] 도 16을 참조하면, 입력값 0.6에 대하여 10비트 LFSR을 사용하고 $2^5 \sim 2^{10}$ 비트의 난수를 발생할 때의 정확도가 도시되어 있다. (a)의 종래 방법은 난수의 초대 최소 오차가 크지만, 본 발명에 따른 이진수-난수 변환 방법은 오차가 상대적으로 적은 것을 알 수 있다.
- [0062] 도 17은 본 발명에 따른 이진수-난수 변환 장치를 회로로 구현한 경우의 성능실험 결과의 일 예를 도시한 도면이다.
- [0063] 도 17을 참조하면, Conv.는 종래 방법, Shared는 종래 방법에 LFSR을 공유하는 방법, Prop.는 본 발명에 따른 방법을 나타낸다. 본 발명에 따른 이진수-난수 변환 장치가 회로면적, 소비전력 등에 있어서 종래에 비해 우함을 알 수 있다.
- [0064] 도 18은 본 발명에 따른 난수-이진수 변환 장치의 일 예를 개략적으로 도시한 도면이고, 도 19는 본 발명에 따른 난수-이진수 변환 장치의 상세 구성의 일 예를 도시한 도면이다.
- [0065] 난수-이진수 변환 장치는 비트열에서 1의 개수를 세는 역할을 수행한다. 예를 들어, 비트열이 11011110과 같이 구성된 경우, 난수-이진수 변환 장치는 1의 개수를 세어 6개임을 파악한다. 따라서 비트열의 총 비트 개수가 8개이므로, 6/8의 값을 얻을 수 있다.
- [0066] 확률 컴퓨팅은 근사적인 방법으로 계산을 수행하므로, 1의 개수를 세는 데에 기존의 카운터와 같이 정확할 필요가 없으므로, 본 발명에 따른 난수-이진수 변환 장치는 근사적인 방법을 사용한다. 특히 본 실시 예는 회로 면적, 소비전력 등의 효율성을 높이기 위한 구조를 제시한다.
- [0067] 도 18 및 도 19를 참조하면, 난수-이진수 변환 장치는 크게 근사유닛(Approximate Unit, AU)(1800)과 병렬 카운터(paralle counter, PC)(1810)로 구성된다. 근사유닛은 AND 게이트와 OR 게이트가 교대로 배치한 레이어(layer)를 적어도 하나 이상 포함하여 구성된다. 도 19의 (b)는 레이어가 하나인 경우, (c) 및 (d)는 각각 레이어가 두 개 및 세 개인 경우를 나타낸다. 레이어가 증가할 때마다 AND 및 OR 게이트의 계층이 증가한다. AND와 OR 게이트는 에러에 대해 상호보완적이므로 (c), (d), (e)와 같이 AND 및 OR 게이트를 교대로 배치하면 에러가 상쇄되는 효과가 있다. 병렬 카운터(1810)는 AU의 출력값에 대해 1의 개수를 계수한다.
- [0068] 도 20은 본 발명에 따른 난수-이진수 변환 장치를 회로로 구현한 경우의 성능 실험결과와 일 예를 도시한 도면이다.
- [0069] 도 20을 참조하면, 본 발명에 따른 난수-이진수 변환 장치(Prop)의 회로 면적, 회로지연시간(critical path delay) 및 소비 전력 등이 종래(Conv)에 비해 더 효율적임을 알 수 있다.
- [0070] 도 21은 본 발명에 따른 난수-이진수 변환 방법의 정확도 실험결과와 일 예를 도시한 도면이다.
- [0071] 도 21을 참조하면, 1024 비트열에서 1의 개수(x축)가 변화할 때 에러(y축)가 도시되어 있다. 도 21의 (a)를 참조하면, 각 시행에 대한 오차의 평균값은 0이고, 표준편차는 최대 12임을 알 수 있다. 도 21의 (b), (c)를 참조하면, 1의 개수가 각각 512, 128일 때 오차의 확률 분포가 도시되어 있는데, 표준 편차가 각각 11.32 및 9.40이다. 따라서 95%의 신뢰구간에서 오차가 2.2%이고, 70% 신뢰구간에서 오차가 1.1%이므로, 본 발명에 따른 방법은 비교적 정확한 1의 값을 카운팅하는 것을 알 수 있다.
- [0072] 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.
- [0073] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

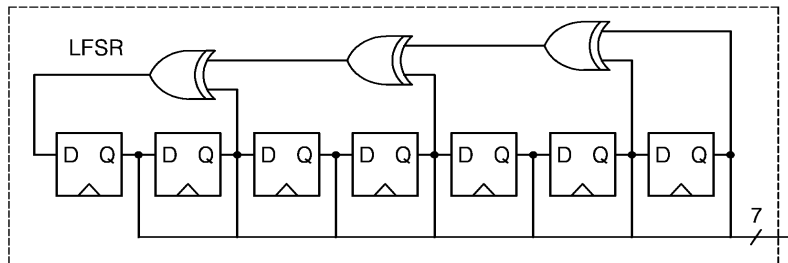
도면1



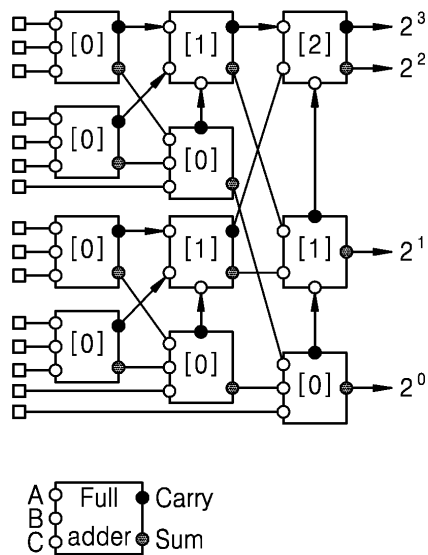
도면2



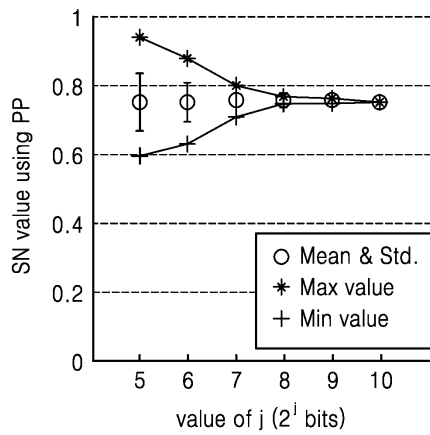
도면3



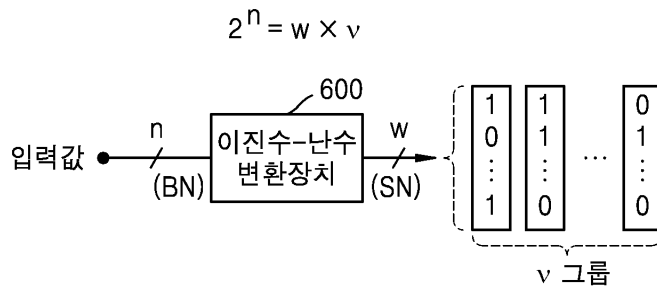
도면4



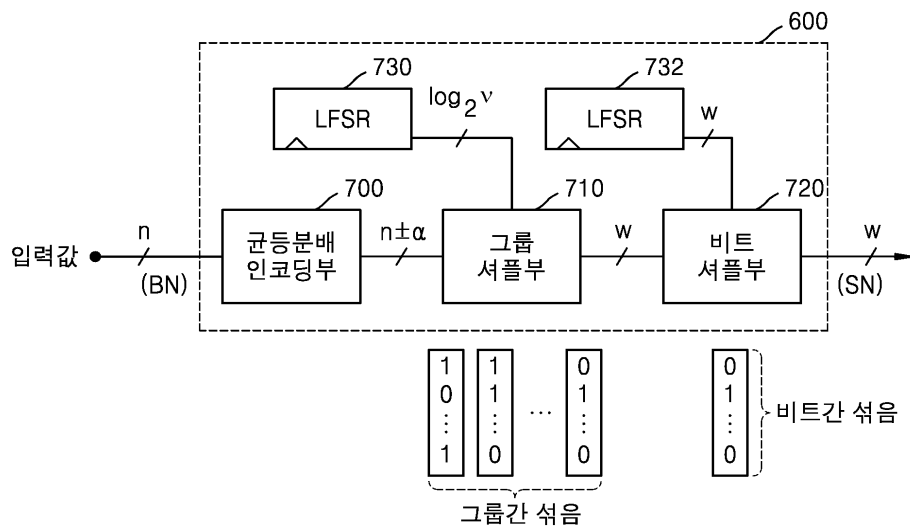
도면5



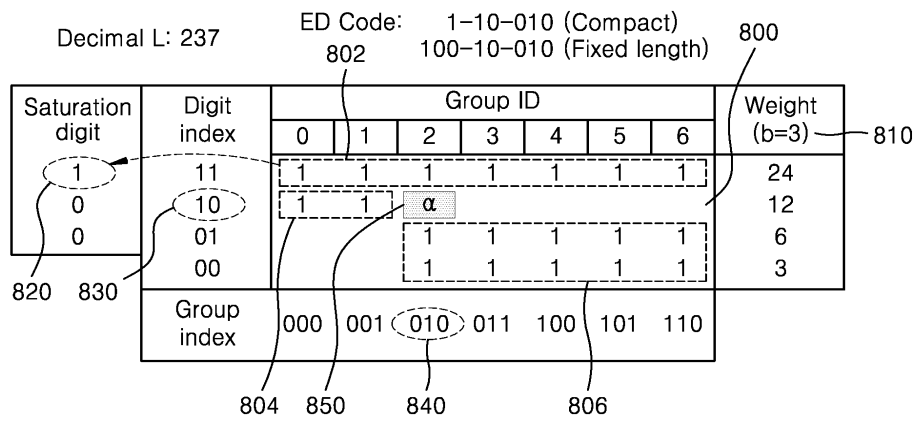
도면6



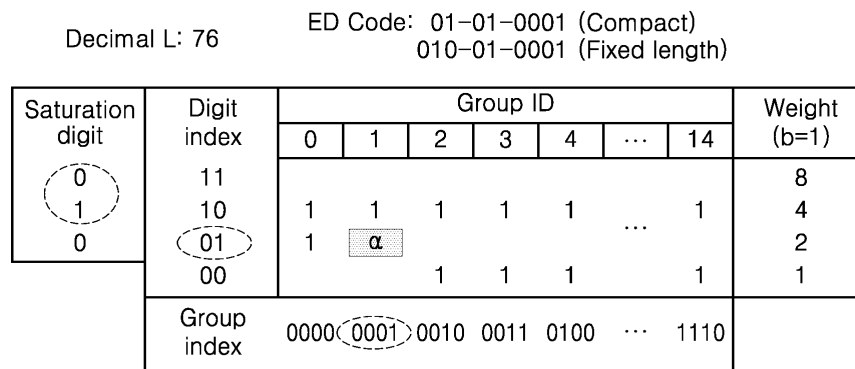
도면7



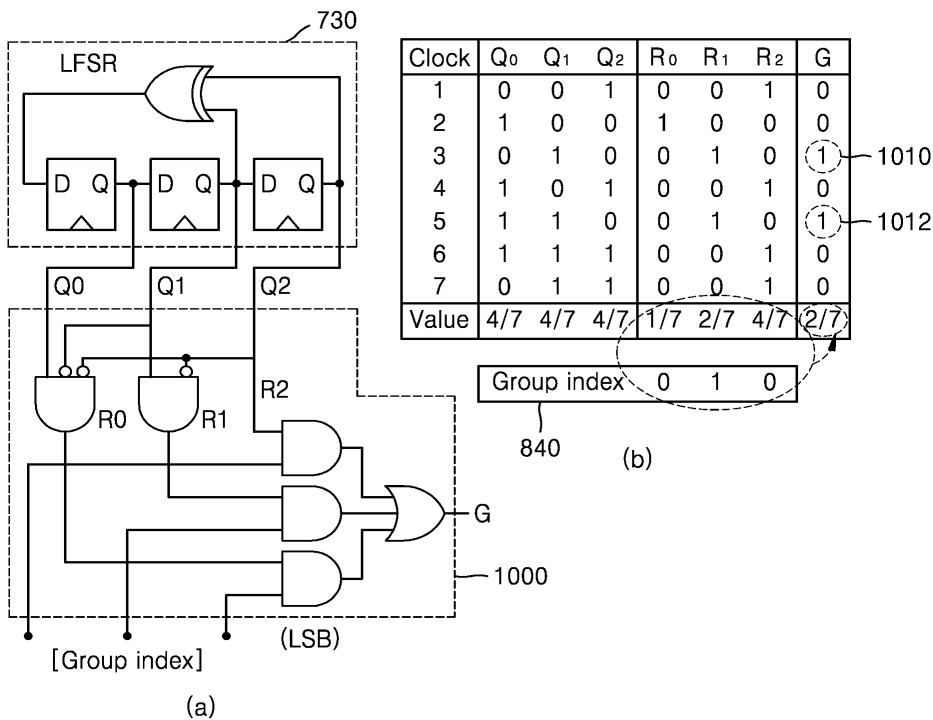
도면8



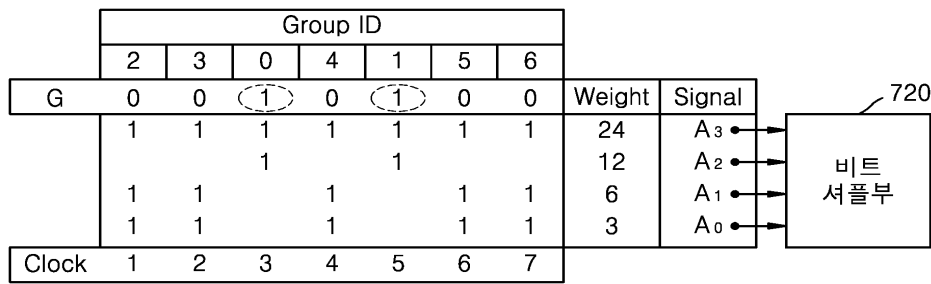
도면9



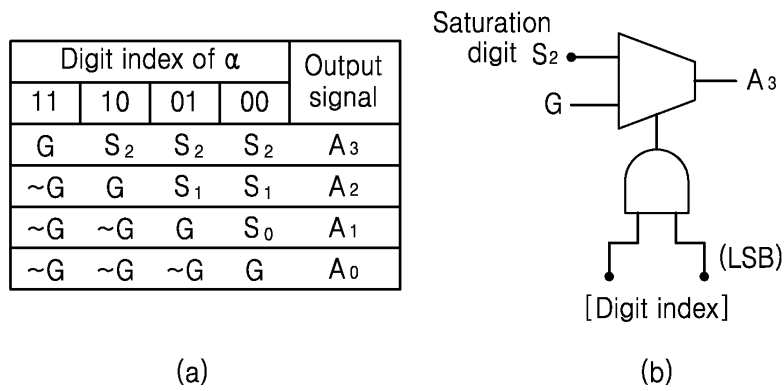
도면10



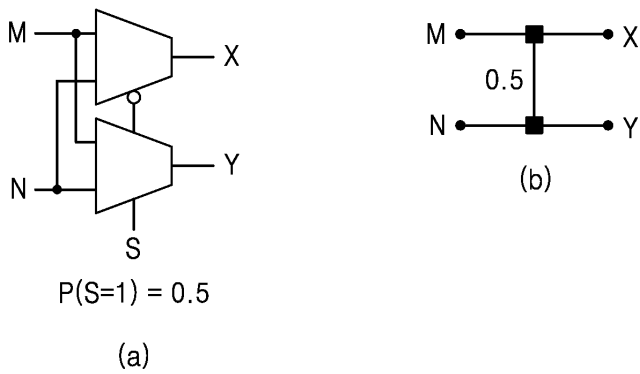
도면11



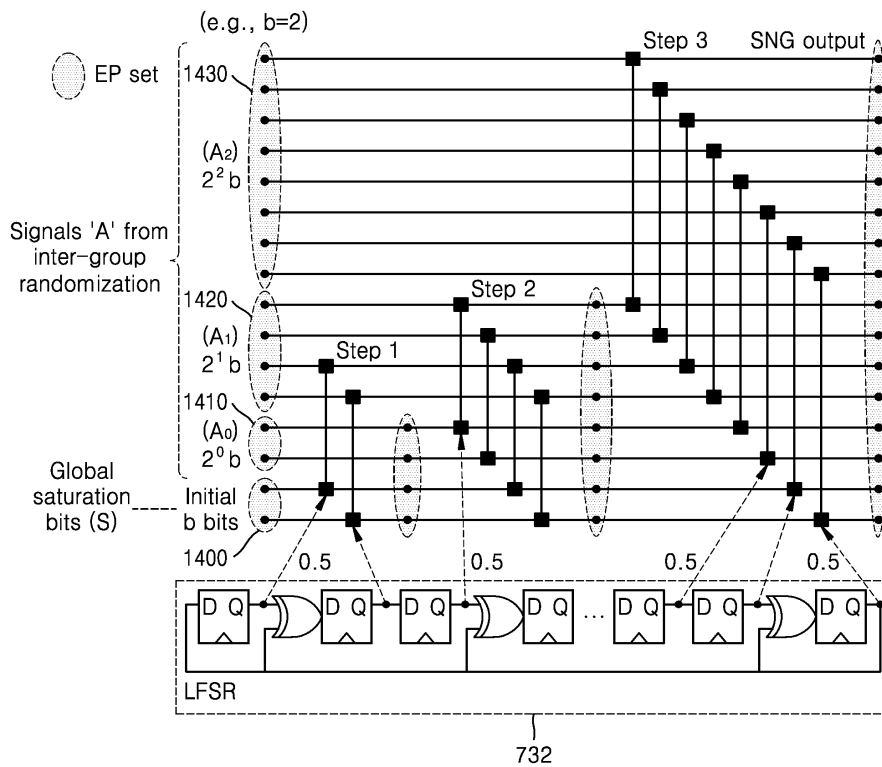
도면12



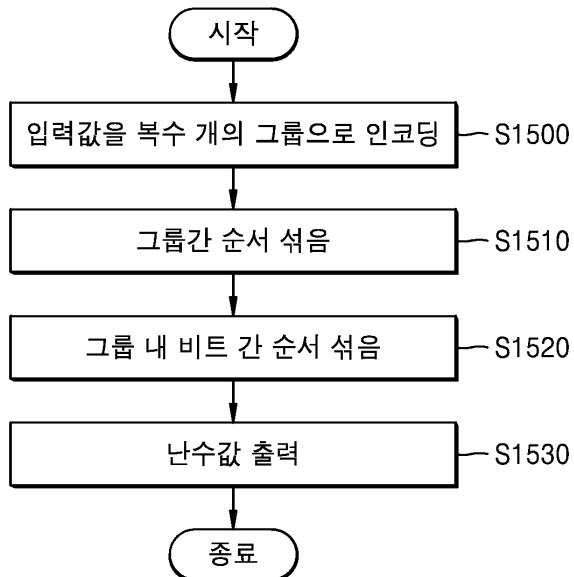
도면13



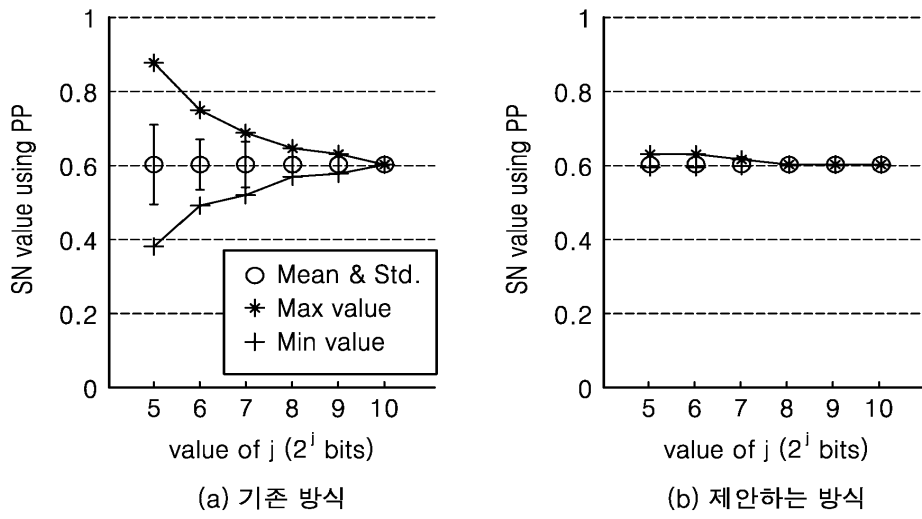
도면14



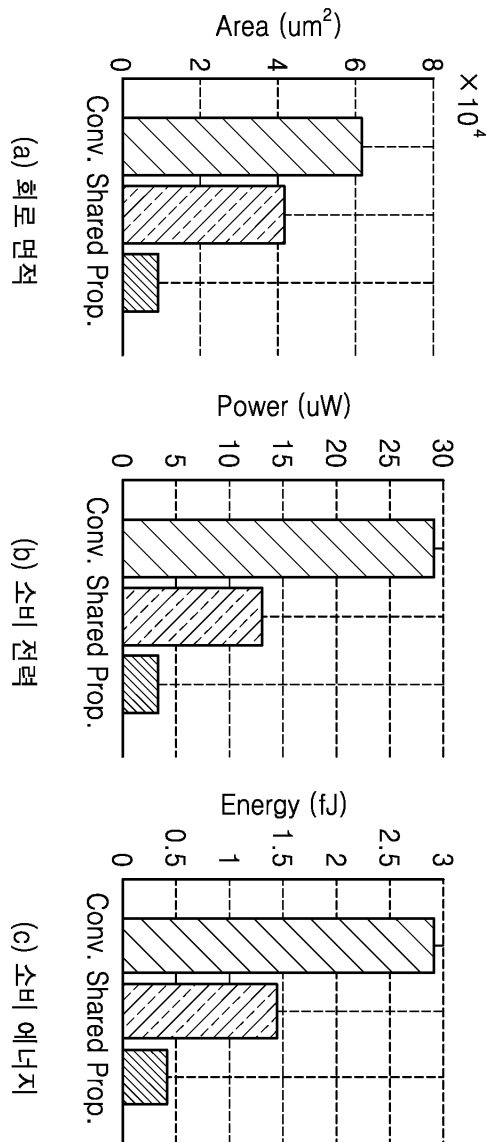
도면15



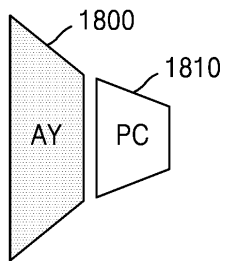
도면16



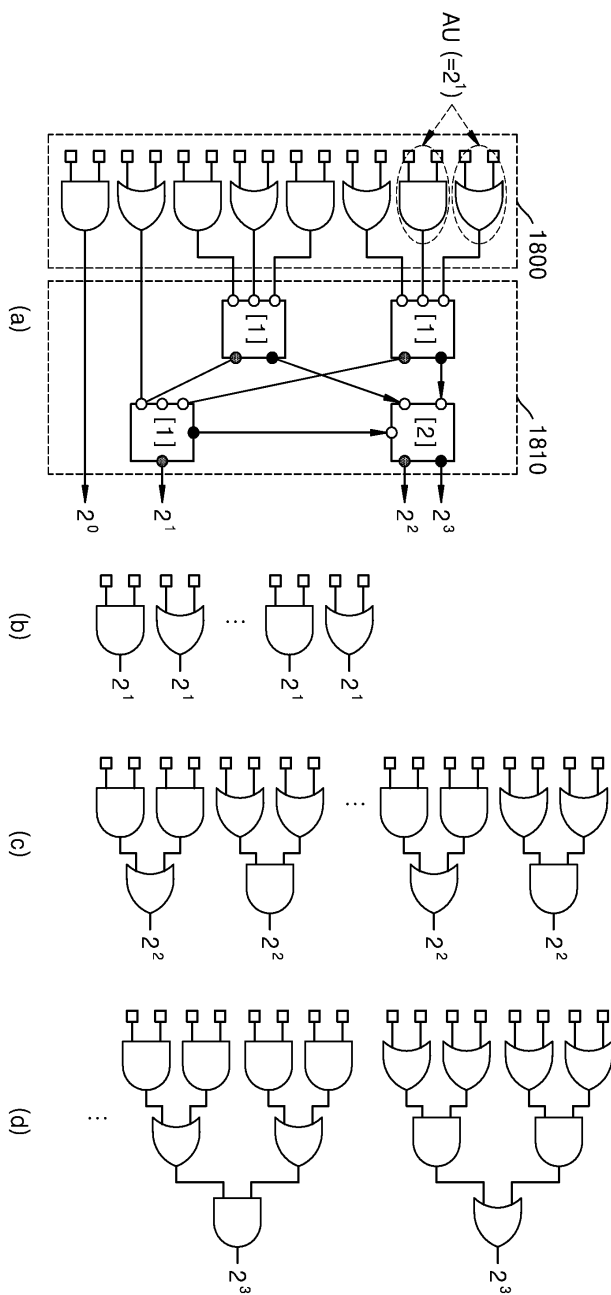
도면17



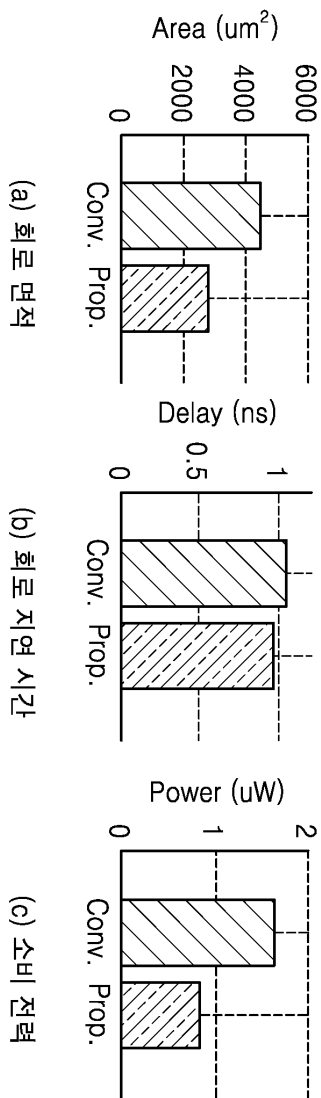
도면18



도면19



도면20



도면21

