[7-9]

PBCA를 이용한 삼중 오류정정부호의 설계†

*조성진, **최언숙, ***허성훈, ***황윤희
*부경대학교 수리과학부, **영산대학교 자유전공학부, ***부경대학교 정보보호학과

Design of Triple-Error Correcting Code using PBCA†

*Sung-Jin Cho, **Un-Sook Choi, ***Seong-Hun-Heo and ***Yoon-Hee Hwang
*Division of Mathematical Sciences, Pukyong National Univ.
**University College of Undeclared Majors, Youngsan Univ.
***Dept. of Information Security, Pukyong National Univ.

요 약

오류정정부호는 메모리 시스템 설계, 다양한 디지털 데이터 통신 시스템 설계 등에 널리 이용된다. 특히 오늘날과 같이 통신망의 확대와 컴퓨터의 발전으로 인한 대용량 데이터의 교환과 처리가 요구되는 디지털 데이터 통신 시스템 설계에서는 통신 채널에서 발생하는 오류를 효율적으로 제어하기 위한 오류정정부호 장치가 필수불가결한 요소가 되었다. 본 논문에서는 기존의 셀룰라 오타마타 기반의 오류정정부호를 개선시킨 단일, 이중 및 삼중 오류정정부호의 효율적인 부호화 및 복호화 방법을 제안한다.

1. 서론

오늘날 많은 양의 데이터가 다양한 컴퓨터 시스템과 서브시스템 사이에서 디지털 논리 회로와 상호 연결선을 통하여 전송된다. 시스템의 신뢰성은 회로 모듈 사이에서 데이터 전송의 무오류성(error-free)에 의존한다[1]. 하지만 전자적 잡음, 장치 결함, 시간 오류 등으로 인하여 시스템에는 항상 언제 발생할지 모르는 잠재적 오류가 존재한다[1][2]. 따라서 시스템의 신뢰성을 향상시키기 위해서 오류정정부호 장치가 필수불가결한 요소가 되었다. 일반적으로 오류정정부호는 (n, k, d)부호로 나타내며, n은 부호어의 길이, k는 데이터(또는 정보어)의 길이, d는 최소거리를 나타낸다[2][3]. 기존의 오류정정부호는 k 값이 커짐에 따라 부호화 및 복호화 회로가 복잡해지는 단점이 있다.

Chowdhury 등[4]은 셀룰라 오토마타(Cellular Automata, 이하 CA)의 간단하고, 규칙적이며, 모듈화한 특성을 이용하여 처음으로 오류정정부호를 제안하였다. [4]에서 제안된 방법은 기존 선형부호에 비하여 복호법이 간단하다는 장점을 가지고 있으나 오류 정정부호의 설계에 있어 다소 복잡하며 T를 구성하는 알고리즘이 규칙적이지 못하다는 단점을 가지고 있다. Cho 등[8]은 PBCA를 이용하여 $(2k, k, 3)$ 부호를 제안하였다. 이 방법은 기존의 방법과 비교하여 간단한 알고리즘에 의하여 부호, 복호화가 가능하다. 그러나 부호어의 생성에 있어서 검사 비트의 수를 반드시 데이터의 양만큼 생성해야 한다. 이러한 점을 개선하기 위하여 본 논문에서는 주어진 데이터에 대하여 검사 비트를 효과적으로 줄이는 방법을 제안한다. 또한 단일 오류 뿐 아니라 이중 및 삼중 오류정정부호의 부호화 및 복호화 방법을 제안한다.

† 본 논문은 2004년도 부경대학교 기성회 학술연구비에 의한 것임.

2. 셀룰라 오토마타

CA는 동역학계(dynamical system)를 해석하는 하나의 방법으로 공간과 시간을 이산적으로 다루는 시스템이며, 셀룰라 공간(cellular space)의 기본 단위인 각 셀(cell)이 취할 수 있는 상태를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. 1차원 CA에서는 모든 셀들이 선형으로 배열되어 있고 국소적 상호작용이 세 개의 셀, 즉 자신과 인접한 두 셀에 의해 이루어지는 CA를 3-이웃(3-neighborhood) CA라 한다. 본 논문에서 다루는 CA는 3-이웃 1차원 CA에 국한시킨다. 세 개의 이웃을 가지는 CA에 대한 다음상태 전이함수(transition function)는 다음과 같이 나타낸다.

$$q_i(t+1) = f[\, q_{i-1}(t),\ q_i(t),\ q_{i+1}(t)\,]$$

여기서 i를 일차원으로 배열되어 있는 각 셀들의 위치라 하고, t 를 시간단계라 하면, $q_i(t)$는 시간 t에서 i번째 셀의 상태를 나타낸다. f는 결합논리를 가지는 국소 전이함수이다. f는 3개의 변수를 가지는 Boolean 함수이므로 2^{2^3}, 즉 256개의 다음 상태 전이함수들이 있으며 이것을 CA의 rule이라고 한다.

CA의 셀들의 상태를 0과 1의 두 가지 값으로 다루고 주어진 CA의 다음상태 전이함수를 아래와 같