

GPS L2C 신호의 Galois 및 Fibonacci 코드 생성기 구현

황용택, 김민수, 황지우, 유호영*
충남대학교 전자공학과

Implementation of Galois and Fibonacci code generators for GPS L2C signal

Yongtaek Hwang, Minsu Kim, Jiwoo Hwang, Hoyoung Yoo*
Electronics Engineering Department
Chungnam National University
E-mail : ythwang.cas@gmail.com, mskim.cas@gmail.com,
jwhwang.cas@gmail.com, *hyyoo@cnu.ac.kr.

Abstract

In this paper, we transform Galois structure into Fibonacci structure and compare which structure has better performance in terms of equivalent gate count, critical path delay, and total power. The GPS satellite transmits several signals, but the only one that generates PRN using the Galois structure is the L2C signal. Therefore, we changed the Galois structure to the Fibonacci structure and compared the difference between the two structures. Before comparing the differences, we converted an initial value to suit Fibonacci using equations to make the same output. As a result of the experiment, the two terms of equivalent gate count and total power are similar, but the critical path delay shows better performance of the fibonacci structure.

I. 서론

GPS(Global Positioning System) 위성이 송신한 신호로부터 위치와 시간 정보를 정확하게 얻기 위해서는 수신기에 서 현재 보이는 GPS 위성이 몇 번 위성인지를 알아야 한다.

This work was supported by National R&D Program through the National Research Foundation of Korea(NRF) funded by Ministry of Science and ICT(2020M3H2A1078119), and the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2022R1A5A8026986). The EDA tool was supported by the IC Design Education Center (IDEC), Korea.

GPS 신호에는 위성 번호에 따른 고유의 PRN(Pseudo-random noise) 코드가 포함되어 있으며, 수신기는 위성 번호 별 PRN 코드를 생성하여 가시 위성을 검색한다. PRN 코드를 생성하기 위해 LFSR(Linear feedback shift register)을 이용하는데 LFSR 구조에는 Fibonacci 구조와 Galois 구조가 있다. 대부분의 위성 신호들은 Fibonacci 구조의 LFSR 을 이용하여 코드를 생성하고 있지만 유일하게 GPS L2C 신호만 Galois 구조를 이용해 코드를 생성하고 있다[1].

따라서, 본 논문에서는 GPS L2C 코드 생성기의 Galois 구조를 Fibonacci 구조로 변환하는 방법을 살펴본다. 이후 변환한 Fibonacci 구조와 Galois 구조를 이용한 코드 생성기의 Equivalent gate count 와 Critical path delay, Total power 측면에서의 성능을 분석 및 비교한다.

II. Galois 및 Fibonacci 구조의 GPS L2C 코드 생성기

그림 1 은 기존 GPS L2C 신호에서 사용하는 Galois 구조의 코드 생성기이고 그림 2 는 Fibonacci 구조로 변환한 코드 생성기이다. 그림 1 의 Galois 구조는 XOR 연산을 각 레지스터의 출력에서 수행한다. 따라서, LFSR 의 출력과 레지스터 출력의 연산 결과가 다음 레지스터의 입력이 된다. 반

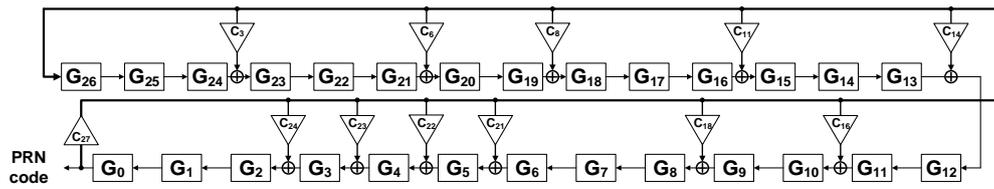


그림 1. Galois 구조의 GPS L2C 코드 생성기

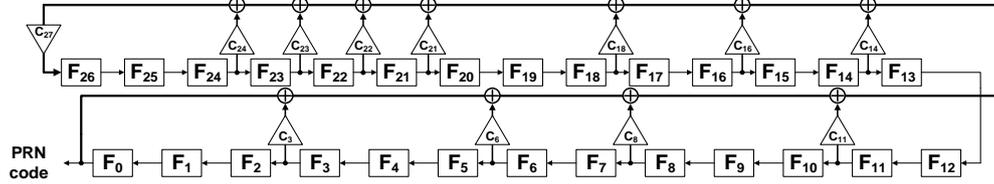


그림 2. Fibonacci 구조의 GPS L2C 코드 생성기

면, Fibonacci 구조는 LFSR의 출력과 레지스터의 출력이 더해져 가장 처음 레지스터의 입력으로 들어가게 된다. 그러므로 feedback 값이 직접적으로 다른 레지스터들에 영향을 미치지 않는다.

Galois 구조의 LFSR을 Fibonacci 구조의 LFSR로 변환시켰을 때 동일한 출력 시퀀스를 얻기 위해서는 먼저 Galois 구조의 레지스터 초깃값을 Fibonacci 구조의 초깃값으로 식 (1)을 이용하여 설정해야 한다[2].

$$G_i = \sum_{j=0}^i F_{i-j} c_{n-j} \quad (0 \leq i \leq n), \quad (1)$$

이때, G_i 는 Galois 구조의 i 번째 레지스터 초깃값이고 F_i 는 Fibonacci 구조의 i 번째 레지스터 초깃값을 의미한다. c_n 은 값이 0 또는 1인 가중치 계수로 레지스터 출력값을 feedback에 사용할지 결정하며 n 은 LFSR 레지스터의 개수이다. GPS L2C 코드 생성기의 피드백 다항식은 $f(x) = x^{27} + x^{24} + x^{23} + x^{22} + x^{21} + x^{18} + x^{16} + x^{14} + x^{11} + x^8 + x^6 + x^3 + 1$ 으로 c_n 은 그림 1과 같이 설정되며, Fibonacci 구조의 코드 생성기로 변환 시 그림 2와 같이 c_n 위치를 반전시켜주면 동일한 출력 시퀀스를 출력한다[2-3].

III. 실험 결과

실험은 CMOS 180nm 공정을 이용하여 합성을 진행하였다. 동작 주파수는 200MHz이고 Gate count에 이용할 2 입력 NAND의 면적은 9.97nm²이다. 두 LFSR의 초깃값을 수식 (1)을 이용해서 설정하였으며 출력 시퀀스는 모두 동일하다. 실험 결과, 표 1과 같이 Total power와 Equivalent gate count는 두 구조의 결과가 유사한 반면 Critical path delay는 Fibonacci 구조가 Galois 구조보다 13.33% 짧다.

표 1. Galois와 Fibonacci 구조의 코드 생성기 비교

	Galois	Fibonacci
Total power	0.7073mW	0.7108mW
Equivalent gate count	850.02	853.36
Critical path delay	4.50ns	3.90ns

IV. 결론

본 논문에서는 GPS L2C 신호의 PRN 코드 생성기를 기존의 Galois 구조에서 Fibonacci 구조로 변환하고 Equivalent gate count와 Critical path delay, Total power를 비교하였다. 실험 결과, Total power와 Equivalent gate count는 두 구조의 결과가 유사한 반면 Critical path delay는 Fibonacci 구조가 Galois 구조보다 13.33% 짧다. 따라서, GPS L2C 수신기에서 PRN 코드를 생성할 때 Fibonacci 구조의 코드 생성기를 설계하면 GPS 수신기의 동작 시간 측면에서 효율적이다.

참고문헌

- [1] M. Kim, et al., "Area-Efficient Universal Code Generator for Multi-GNSS Receivers," *MDPI Electronics*, vol.10, no.20, pp. 1-14, October, 2021.
- [2] A. Klein, "Stream Ciphers," Springer Publishing Company, Incorporated, 2013.
- [3] G. L. Puga, "Linear-feedback shift register seed determination for memory-constrained embedded systems," *2017 IEEE URUCON*, 2017, pp. 1-4.