Trace 함수를 이용한 부호계열 발생

박선광, 이정재

동의대학교

jjlee@deu.ac.kr

A Review of Code Sequence Generation using Trace Functions

Park Sun Kwang, Lee Jeong Jae

Dongeui Univ.

요 약

본 논문에서는 Trace 함수의 특성과 유한장 그리고 m-계열과의 관계를 검토한다. 또한 Trace 함수를 이용한 통상적인 Gold 계열과 유사 Gold 계열 그리고 큰 선형스팬을 갖는 유사 Gold 계열의 발생알고리즘과 발생된 부호계열간의 자기상관함수와 상호상관함수를 비교 분석 한 결과를 소개한다.

1. 서 론

대역확산을 이용한 통신방식은 CDMA를 포함하여 GPS, 거리측정 기술 등 다양하게 이용되고 있다. 또한 핵심기술 중의 하나는 대역을 확산하기위한 확산부호계열이며 대표적인 계열로 m-계열이 있다. m-계열은 쉬프트레지스터를 이용하여 쉽게 발생시킬 수 있고 자기상관함수 특성이 매우 우수하여 가장 많이 사용되는 계열이다. 그러나 상호상관함수특성은 그다지 좋지 못하다. 그리고 GPS에 사용되는 Gold 계열은 두 종류의 m-계열을 조합하여 발생되는 선형 계열이며 상자기상관함수와 상호상관함수 특성이 우수하다. 그러나 구조적인 간편함에도 불구하고 단순한 선형성으로 인하여 선형스팬이 매우 적어 대략 쉬프트레지스터 길이의 2배정도만을 확인하면 복사가 가능하여 보안성에 취약하다 [1-7].

본 논문에서는 Gold 계열과 유사한 특성을 갖고 큰 선형스팬을 갖는 유사 Gold 계열의 Trace 함수를 이용 한 발생알고리즘을 분석하고 발생된 부호계열의 특성을 분석하기 위하여 제 2절에서는 Trace 함수와 유한장 그리고 m-계열과의 관계를 살펴본다. 제 3절에서는 Trace 함수를 이용한 통상적인 Gold 계열과 유사 Gold 계열 그리고 큰 선형스팬을 갖는 유사 Gold 계열의 발생알고리즘을 분석한다. 그리고 제 4절에서는 부호계열을 발생시키고 그 상관함수 특성을 검토한다. 마지막으로 제 5절에서 결론을 맺는다.

2. Trace 함수의 특성

α를 $GF[(p^s)^r]$의 원소라면 Trace 함수는 부분장 $GF(p^s)$와 관련하여 다음 식(1)과 같이 정의된다[1,2].

$$Tr_s^{rs}(\alpha)=\alpha+\alpha^{p^s}+\cdots+\alpha^{p^{(r-1)s}}=\sum_{i=0}^{r-1}\alpha^{p^{is}} \quad (1)$$

그리고 Trace 함수는 다음과 같은 특성을 갖는다.

1) 원소 $b\in GF(p^s)$가 $x^{p^s}-x=0$의 근이면 $b^{p^s}-b=0$ 이며 원소 $\alpha\in GF[(p^s)^r]$에 대하여 $Tr_s^{rs}(\alpha)$은 $GF(p^s)$에 포함된다. 따라서 Trace 함수는 $GF[(p^s)^r]$의 원소 α를 부분장 $GF(p^s)$의 원소 b로 사상한다.

2) 모든 $\alpha\in GF[(p^s)^r]$에 대하여 $\alpha^{p^{ks}}=\alpha$이므로

$Tr_s^{rs}(\alpha)=Tr_s^{rs}(\alpha^{p^{ks}})$이다.

3) 모 든 $\alpha,\ \beta\in GF[(p^s)^r]$와 정수 k에 대하여

$(\alpha+\beta)^{p^{ks}}=\alpha^{p^{ks}}+\beta^{p^{ks}}$

$Tr_s^{rs}(\alpha+\beta)=Tr_s^{rs}(\alpha)+Tr_s^{rs}(\beta)$.

4) $b\in GF(p^s)$이면 $b^{p^s}=b$이고 $b^{p^{ks}}=b$이며 임의의 $\alpha\in GF[(p^s)^r]$에 대하여

$Tr_s^{rs}(b\alpha)=Tr_s^{rs}(\alpha)$.

5) 만약 s=1이면 $Tr_1^r(\alpha)$는 $\alpha\in GF(p^r)$를 GF(p)로 사상한다. 만약 m=rs, $\alpha\in GF(p^m)$이면

$Tr_1^m(\alpha)=Tr_1^s(Tr_s^m(\alpha))$

그리고 Trace 함수와 m-계열과의 관계를 알아보면

$$Tr_s^m(\alpha)=\sum_{i=0}^{m/s-1}\alpha^{2^{si}},\ \alpha\in GF(2^m),\ m=rs$$

이는 $\alpha\in GF(2^m)$를 부분장 $GF(2^s)$로 사상한다. GF(2)에 원소를 갖는 이진 m-계열 $\{a_n\}$은 선형회귀의 영이 아닌 해로 정의된다.

$$a_n+\sum_{i=1}^{m}h_i a_{n-i}=0$$

이것은 다음의 원시 다항식에 대응된다.

여기서 $h_i\in GF(2)$이고 원시원 $\alpha\in GF(2^m)$에 대하여