p진 M-수열을 Decimation한 수열들 간의 상호상관도

*김지엽°, *최성태, *노종선, **정하봉
*서울대학교 전기컴퓨터공학부, 뉴미디어통신공동연구소
**홍익대학교 전기전자공학부

Cross-Correlation between Decimated p-ary M-Sequences

*Ji-Youp Kim°, *Sung-Tai Choi, *Jong-Seon No, **Habong Chung
*Department of EECS, INMC, Seoul National University
Department of Electronics and Electrical Engineering, Hongik University
{lakroforce, stchoi}@ccl.snu.ac.kr, jsno@snu.ac.kr, habchung@hongik.ac.kr

요 약

본 논문에서는 m-수열을 decimation하여 새로운 수열을 만들고, 이들 수열간의 상호상관도에 대한 시뮬레이션 결과를 소개한다. 본 논문에서 사용되는 m-수열은 F_{p^n}상의 수열로 p는 홀수인 소수이고 decimation한 수열들은 모두 주기가 $\frac{p^n-1}{2}$이다. 시뮬레이션 결과에 의하면 상호상관도의 값은 p=3 mod 4이고 n이 홀수일 때 $2\sqrt{N}$보다 낮은 것으로 나타났다.

1. 서론

CDMA통신 시스템에서는 TDMA나 FDMA와 달리 다중접속을 위해 사용자들에게 고유하게 부여되는 서명 수열(signature sequence)을 사용한다. 이 수열은 사용자들을 구별하는 역할을 할 뿐만 아니라 한 셀 안에서 많은 사용자들이 통신을 할 때 나타나는 간섭현상을 줄이는데도 사용된다. 또 통신시스템에서 필수적인 동기화(synchronization)를 위해서 서명 수열이 이용되기도 한다. 그러나 서명 수열이 이러한 역할을 제대로 이루어내기 위해서는 몇 가지 바람직한 특성을 가져야 한다. 그 중 가장 핵심적인 것으로 낮은 상호상관도가 고려된다.

그 동안 유사잡음수열의 상호상관도에 대한 연구와 관련하여 m-수열과 decimation한 m-수열 간의 상호상관값에 대한 연구가 많이 진행되어 왔다. Helleseth[1], Muller[2], Trachtenberg[3], Dobbertin[4]등은 각각 다른 decimation에 대해서 상호상관도의 값들을 구하였다. 본 논문에서는 우선 m-수열을 2로 decimation하여 반주기의 수열을 만들고, 이 수열을 다시 다양한 값으로 decimation하여 그 상호상관도의 값을 조사하였다.

2. 사전 지식

F_{p^n}을 원소의 수가 p^n인 유한체라고 하자. 여기서 p는 소수이고 n은 자연수이다. 이 때 트레이스 함수 tr_1^n : $F_{p^n} \rightarrow F_p$를 다음과 같이 정의한다.

$$tr_1^n(x) = \sum_{i=0}^{n-1} x^{p^i}$$

트레이스 함수는 F_p를 체로 가지는 벡터공간 F_{p^n}상에서의 선형함수가 된다. 이 트레이스 함수를 이용하여 m-수열 $s(t)$를 다음과 같이 정의한다.

$$m(t) = tr_1^n(\alpha^t)$$

여기서 α는 F_{p^n}의 원시근을 나타낸다.

위에서 정의된 m-수열을 이용해서 많은 의사잡음수열군들이 제시되었는데, 특히 m-수열과 m-수열을 decimation하여 얻어지는 수열을 shift하여 더하는 방식으로 많은 수열군들이 만들어져왔다. Kasami 수열군은 m-수열과 부분체의 m-수열을 더해서 만들어지는 방식이고 Gold 수열군은 m-수열과 m-수열을 decimation한 수열을 더해서 만드는 방식이다.

3. 수열의 상호상관도

본 논문에서는 p는 홀수인 소수이고 n은 자연수인 경우에 두 m-수열을 decimation한 수열들간의 상호상관도를 조사한다. 두 수열 $a(t)$와 $b(t)$사이의 상호상관함수 $R(\tau)$는 다음과 같이 정의된다.

$$R(\tau)=\sum_{t=0}^{N-1}\omega^{a(t+\tau)-b(t)}$$

또 최대 상호상관도 $R_{\max}$는 다음과 같이 정의한다.

$$R_{\max}=\max_{\tau\neq 0}R(\tau)$$

$m(t)$를 F_{p^n} 상에서의 m-수열이라고 하면 $m(2t)$는 p가 홀수이므로 $N=\frac{p^n-1}{2}$을 주기로 가지는 수열이 된다. 여기서 다시 자연수 d로 $m(2t)$을 decimation한 수열 $m(2dt)$는 주기가 $\gcd(d,\ N)$인 수열이다. d값을 변화시키면서 $m(2t)$와 $m(2dt)$, $m(2t)$와 $m(2dt+1)$, $m(2t+1)$와 $m(2dt)$, $m(2t+1)$와 $m(2dt+1)$사이의 상호상관도를 계산한 결과를 표로 정리하였다. 표에는 $\gcd(d,\ N)$=1이고 최대 상호상관도의 크기가 $2\sqrt{N}$보다 작은 경우만 표시하였다.

p	n	$R_{\max}/\sqrt{N}$	d	$\gcd(d,\ N)$
7	5	1.41359	6002	1
11	3	1.40526	544	1
19	3	1.40181	3068	1
23	3	1.40347	5554	1

표 1 $m(2t)$**와** $m(2dt)$**사이의 상호상관함수값**

p	n	$R_{\max}/\sqrt{N}$	d	$\gcd(d,\ N)$
5	4	1.81164	157	1
5	4	1.37915	187	1
5	5	1.59404	21, 149, 967, 1063	1
5	5	1.40901	937	1
5	6	1.40159	4687	1
7	4	1.39335	857	1
7	5	1.99573	6002	1
11	3	1.94748	2	1
11	3	1.9671	87, 153, 292, 558	1
11	3	1.94748	333, 338	1
11	3	1.95559	544	1
11	4	1.41009	5989	1
13	3	1.40297	929	1
17	3	1.98972	1229	1
17	3	1.41396	2167	1
19	3	1.96178	3068	1
23	3	1.99746	5554	1

표 2 $m(2t+1)$**와** $m(2dt)$**사이의 상호상관함수값**

p	n	$R_{\max}/\sqrt{N}$	d	$\gcd(d,\ N)$
7	5	1.8764	43, 391, 6058, 6346	1
7	5	1.41359	6002	1
11	3	1.97275	136, 181	1
11	3	1.96303	179	1
19	3	1.40181	3068	1
23	3	1.40349	5554	1

표 3 $m(2t+1)$**와** $m(2dt+1)$**사이의 상호상관함수값**

p	n	$R_{\max}/\sqrt{N}$	d	$\gcd(d,\ N)$
5	4	1.81164	157	1
5	4	1.37915	187	1
5	5	1.59405	21, 149, 967, 1063	1
5	5	1.40901	937	1
5	6	1.40159	4687	1
7	4	1.39335	857	1
7	5	1.99573	6002	1
11	3	1.94748	2, 333, 338	1
11	3	1.96871	87, 153, 292, 558	1
11	3	1.95559	544	1
11	4	1.41009	5989	1
13	3	1.40297	929	1
17	3	1.98972	1229	1
17	3	1.41395	2167	1
19	3	1.96178	3068	1

표 4 $m(2t)$**와** $m(2dt+1)$**사이의 상호상관함수값**

시뮬레이션은 $p^n=5^4, 5^5, 5^6, 7^4, 7^5, 11^3, 13^3, 17^3, 19^3$인 경우에 대해 수행하였고 $m(2t)$와 $m(2dt+1)$의 경우를 제외하고는 23^3의 경우도 계산하였다. 위 결과를 보면 네 가지 경우 모두에 대해 $R_{\max}/\sqrt{N}$이 2이하로 상한되는 경우는 p^n=7^3, 7^5, 11^3, 19^3, 23^3이고 $d=N-p^{n-1}$인 경우이다. 이는 p=3 mod 4이고 n이 홀수인 경우이므로 다음 추론을 생각해볼 수 있다.

추론 1: p=3 mod 4인 소수이고 n이 홀수라고 하자. F_{p^n} 상의 m-수열 $m(t)$에 대해 주기 $N=\frac{p^n-1}{2}$인 수열

$m(2t)$를 생각하자. 만약 $d = N - p^{n-1}$이면 수열 $m(2t)$와 $m(2dt)$사이의 상호상관함수의 절대값은 $2\sqrt{N}$으로 상한된다.

마찬가지로 나머지 3가지 경우에 대해서도 비슷한 추론을 생각해볼 수 있다.

4. 결론

시뮬레이션을 통해 m-수열을 decimation한 수열 $m(2t)$와 $m(2dt)$사이의 상호상관값의 절대값이 $2\sqrt{N}$보다 낮은 경우의 p, n, d에 대한 조건을 조사하였다. 그 조건은 p=3 mod 4, n은 홀수, $d = N - p^{n-1}$이 될 것으로 추측된다.

5. 감사의 글

본 연구는 2009년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원 [No. 2009-0081441]과 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업의 일환으로 수행하였음 [2008-F-007-02, 3차원 환경에서의 지능형 무선통신 시스템].

6. 참고 문헌

[1] T.Helleseth, Some results about the cross correlation function between two maximal linear sequences, Discr. Math., vol. 16, pp.209-232, 1976

[2] E.N.Muller, On the cross-correlation of sequences over GF(p) with short periods, IEEE Trans. Inf. Theory, vol. 45, no. 1, pp.289-295, Jan. 1999.

[3] H.M.Trachtenberg, On the Cross-Correlation Functions of Maximal Recurring Sequences, Ph.D. dissertation, Univ. of Southern California, Los Angeles, 1970.

[4] H.Dobbertin, T.Helleseth, P.V.Kumar, and H.Martinsen, Ternary m-sequences with three-valued cross-correlation functions: New decimations of Welch and Niho type, IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1473-1481, May 2001.