링 위에서 수열의 선형복잡도

홍윤표* 은유창* 송홍엽* 이광억** 박성복**

yphong@eve.yonsei.ac.kr

2001. 7. 6

*연세대학교 전기전자공학과 부호 및 정보이론 연구실

**국방과학연구소

발표내용

1. 서론
2. Modified Berlekamp-Massey Algorithm 분석
3. Reeds & Sloane Algorithm 분석
4. 링 위에서 수열의 선형복잡도의 중요성
5. n-터플 드브루인 수열의 선형복잡도 실험결과
6. 결과 및 고찰
7. 참고문헌

1. 서 론(1)

♦선형복잡도 : 주어진 수열을 발생시키는 최소단수 LFSR의 단수

✓ 수열을 발생시키거나 분석함에 있어서 어려움의 측정 기준

♦필드 위에서의 선형복잡도 : 주어진 수열의 심볼들을 어떠한 필드의 원소로 간주

✓ 통상 Berlekamp-Massey 알고리즘[1] 으로 구함

✓ $m \neq p^n$ (m :주어진 수열의 심볼 개수, p :임의의 소수, n :임의의 자연수)

일 때는 $m \leq p^n$, $\min_{p,n}(p^n - m)$을 만족하는 필드($GF(p^n)$)위에서 구함

⇨ $GF(p^n)$의 원소중 $p^n - m$ 개의 원소는 수열에 나타나지 않는 원소

1. 서 론(2)

♦ 링 위에서의 선형복잡도 : 주어진 수열의 심볼들을 어떠한 링의 원소로 간주

✓ 수열의 심볼 개수(m)와 같은 수의 원소를 가지는 링(Z_m)위에서 구함

♦ 보안 측면에서의 선형복잡도

✓ 스트림 암호나 군용 주파수 도약 통신에서는 큰 선형복잡도를 가지는 수열 요구

➪ 필드 위에서의 선형복잡도와 링 위에서의 선형복잡도중 작은 값으로 선형복잡도를 보는 것이 보다 안전성을 가짐

♦ Modified Berlekamp-Massey Algorithm

✓ BM 알고리즘의 형태를 유지하면서 링 위에서의 선형복잡도를 구함

✓ 실제 구현상의 문제점

: $d_n \neq 0, l_{n+1} \neq \max(l_n, n+1-l_n)$인 경우 차수 l $(\max(l_n, n+1-l_n) \leq l < l_{n+1})$

을 하나씩 증가시키면서 모든 연결다항식을 탐색하여 새로운 해를 구함

⇨ 차수 l 에 대해 전영역 탐색의 계산량

⇨ 실제 구현상의 관점에서 비효율적인 알고리즘

3. Reeds & Sloan Algorithm[4] 분석(1)

♦ Reeds & Sloane Algorithm

✓ Chinese Remainder Theorem을 이용하여 링 위에서의 선형복잡도를 구함

✓ 주어진 수열 $S(s_1, s_2, \cdots, s_N)$ $(over\ Z_m)$ 의 심볼 개수 m 을 소인수 분해

$$m = \prod_{i=1}^{U} p_i^{e_i}, e_i \geq 1$$

✓ $i = 1, 2, \cdots, U$ 에 대해 $S(s_1, \cdots, s_N)$ $(\mathrm{mod}\, p_i^{e_i})$ 를 발생시키는 최소단수 LFSR의 연결다항식($a^{(i)}(x)$)과 선형복잡도($l^{(i)}$)를 구함

✓ Chinese Remainder Theorem을 이용하여 $S(s_1, s_2, \cdots, s_N)$ $(over\ Z_m)$ 를 발생시키는 최소단수 LFSR의 연결다항식($a(x)$)과 선형복잡도(l)를 다음과 같이 구함

$$a(x) \equiv a^{(i)}(x) \ (\mathrm{mod}\ p_i^{e_i}) \ \text{ for all } i \quad \& \quad l = \max_i(l^{(i)})$$

3. Reeds & Sloan Algorithm[4] 분석(2)

♦ Reeds & Sloane Algorithm의 실제 구현상의 효율성

✓ 대략적인 계산량 : $\sum_{i=1}^{U} e_i + (N-1)\sum_{i=1}^{U} 3e_i = (3N-2)\sum_{i=1}^{U} e_i$

⇨ 전영역 탐색보다 훨씬 적은 계산량

⇨ 실제 구현상의 관점에서 Modified BM 알고리즘 보다 효율적인 알고리즘

4. 링 위에서 선형복잡도의 중요성(1)

♦실험 내용

✓ 원시다항식 $1+x^3+x^{10}$ 을 이용한 이진 m-시퀀스 : $S=\{s(i)\}, i=1,2,\cdots,1023$

✓ m-시퀀스 S를 k-tuple씩 십진수로 읽어서 q 심볼을 갖는 1023주기 시퀀스 생성

: $S_q^k=\{s_q^k(i)\}, i=1,2,\cdots,1023$ $\quad s_q^k(i)=\sum_{j=i}^{i+k-1} s(j)\cdot 2^{i+k-1-j} \pmod q$

✓ 주기 시퀀스 S_q^k 의 Z_q위에서의 선형복잡도와 $GF(p^n)$ 위에서의 선형복잡도를 구하여 서로의 크기를 비교

(p, n : $q \le p^n, \min_{p,n}(p^n-q)$ 를 만족하는 임의의 소수와 자연수)

4. 링 위에서 선형복잡도의 중요성(2)

♦실험 결과

✓ k=7, q =14

	Z_{14}	$GF(16)$
선형복잡도	1022	847

✓ k=7, q =62

	Z_{62}	$GF(64)$
선형복잡도	1023	847

✓ k=7, q =15

	Z_{15}	$GF(16)$
선형복잡도	1023	637

✓ k=7, q =63

	Z_{63}	$GF(64)$
선형복잡도	1023	967

4. 링 위에서 선형복잡도의 중요성(3)

♦실험 결과

✓ k=9, q =63

	Z_{63}	$GF(64)$
선형복잡도	1023	967

✓ k=9, q =62

	Z_{62}	$GF(64)$
선형복잡도	1023	847

✓ k=9, q =255

	Z_{255}	$GF(256)$
선형복잡도	1023	1022

✓ k=9, q =254

	Z_{254}	$GF(256)$
선형복잡도	1023	1012

✓ k=9, q =511

	Z_{511}	$GF(512)$
선형복잡도	1021	1022

✓ k=9, q =510

	Z_{510}	$GF(512)$
선형복잡도	1023	1012

4. 링 위에서 선형복잡도의 중요성(4)

➪주어진 수열의 링 위에서의 선형복잡도가 필드 위에서의 선형복잡도보다 작은 경우 존재

➪주어진 수열의 선형복잡도는 링 위에서의 선형복잡도와 필드 위에서의 선형복잡도중 작은 값으로 선택하는 것이 보다 일반적임

5. n-터플 드브루인 수열의 선형복잡도 실험결과(1)

♦실험 내용

✓주어진 n에 대하여 주기 2^n을 갖는 드부루인 수열 : $S = \{s(i)\}, i = 1,2,\cdots,2^n$

✓ 드부루인 수열 S를 n-tuple씩 십진수로 읽어서 2^n 심볼을 갖는 2^n주기 시퀀스 생성

: $S^n = \{s^n(i)\}, i = 1,2,\cdots,2^n$ $\quad$ $s^n(i) = \sum_{j=i}^{i+n-1} s(j) \cdot 2^{i+n-1-j}$

✓ $n = 4$ 부터 $n = 10$ 까지 각각 16, 2048, 100000, 10000, 10000, 1000, 1000개의 드부루인 수열에 대해 주기 수열 S^n의 Z_{2^n}와 $GF(2^n)$상에서의 선형복잡도를 구하여 서로의 크기를 비교

5. n-터플 드브루인 수열의 선형복잡도 실험결과(2)

♦실험 결과

✓ 조사한 모든 수열은 Z_{2^n} 의 선형복잡도가 $GF(2^n)$ 의 선형복잡도보다 크거나 같은 값을 가짐

선형복잡도	12	13	14	15
Over $GF(16)$	4	0	4	8
Over Z_{16}	0	4	4	8

< 4-터플 드브루인 수열의 선형복잡도 분포 >

선형복잡도	21	22	23	24	25	26	27	28	29	30	31
Over $GF(32)$	8	0	12	20	32	36	64	180	224	448	1024
Over Z_{32}	0	0	0	0	24	0	12	56	96	628	1232

< 5-터플 드브루인 수열의 선형복잡도 분포 >

6. 결과 및 고찰

- 실제 구현상의 관점에서 Reeds & Sloane Algorithm이 Modified Berlekamp-Massey Algorithm보다 효율적임

- 링 위에서의 선형복잡도가 필드 위에서의 선형복잡도보다 작은 경우 발생

  ⇨ 필드와 링 위에서의 선형복잡도를 동시에 고려해야함

- n-터플 드부루인 수열은 Z_{2^n} 의 선형복잡도가 $GF(2^n)$ 의 선형복잡도보다 항상 크거나 같은 값을 갖는가?

7. 참고문헌

[1] James L. Massey, “Shift-Register Synthesis and BCH Decoding,” IEEE Trans. on Information Theory, p122-127, vol.IT-15, No.1, Jan. 1969

[2] Jose Carmelo Interlando, Reginaldo Palazzo, Jr, “Modified Berlekamp-Massey Algorithm for Decoding BCH Codes Defined over Rings,” IEEE ISIT 1994. Proceedings, p94, 1994

[3] J. Carmelo Interlando, Reginaldo Palazzo, Jr, Michele Elia, “On the Decoding of Reed-Solomon and BCH Codes over Integer Residue Rings,” IEEE Trans. on Information Theory, p1013-1021, vol.43, No.3, May. 1997

[4] J. A. Reeds, N. J. A. Sloane, “Shift Register Synthesis (modulo m),” Siam J. Comp., vol. 14, No. 3, p505-513, Aug. 1985