유한체 상의 노름 함수를 이용한 복소 상관특성이 좋은 주기 p^2-1인 p진 수열군 생성

송민규, 송홍엽, 이장용

연세대학교

제26회 통신정보 합동학술대회

1. 표기법과 사전 지식

- α : 유한체 $\mathrm{GF}(p^2)$의 임의의 원시원소
- $\beta \triangleq \alpha^{p+1}$: α에 의해 결정되는 $\mathrm{GF}(p)$의 원시원소
- $\mathrm{N}_1^2(x) = x^{1+p}$: $\mathrm{GF}(p^2)$에서 $\mathrm{GF}(p)$로의 노름 함수
- $\mathrm{Tr}_1^2(x) = x + x^p$: $\mathrm{GF}(p^2)$에서 $\mathrm{GF}(p)$로의 대각합 함수
- 복소 상관 : 주기 p^2-1인 p진 수열 $a(t)$, $b(t)$의 임의의 순환지연 τ에서의 복소 상관 $\mathrm{C}_{a(t),b(t)}(\tau)$는

$$\mathrm{C}_{a(t),b(t)}(\tau) = \sum_{t=0}^{L-1} e^{j\frac{2\pi}{p}[a(t)-b(t+\tau)]}$$

와 같이 정의한다.[1]

- Welch bound[2]

주기 p^2-1인 p진 수열들의 집합 N의 크기가 $p-1$일 때, N의 비 자명 최대 상관의 절대값 $\mathrm{C}_{\max}(N)$은

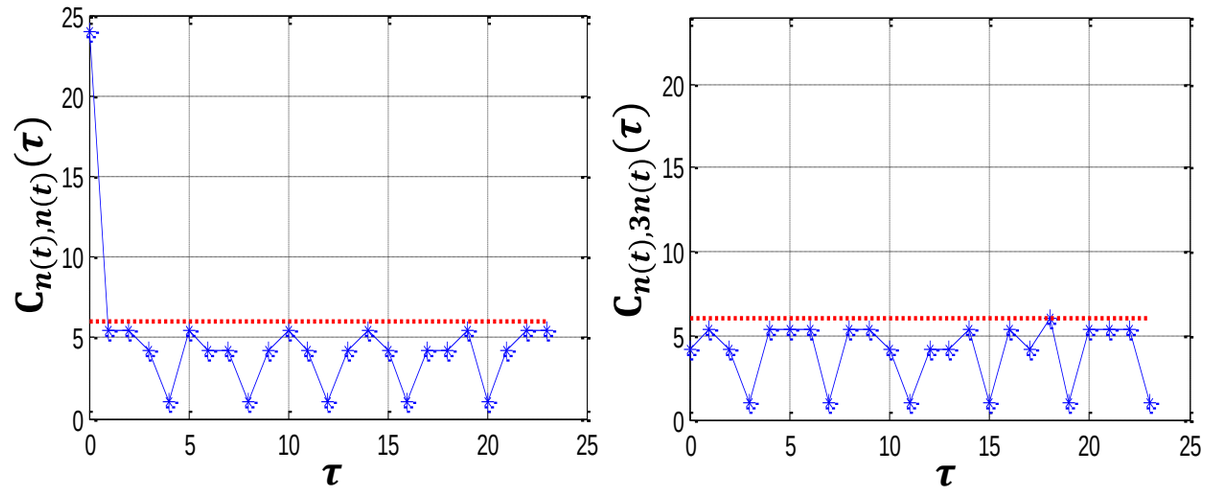
$$\mathrm{C}_{\max}(N) \geq \left(p^2-1\right)\sqrt{\frac{p-2}{(p-1)(p^2-1)-1}}$$

의 하계를 갖는다.

충분히 큰 p에 대해서 위의 부등식을 정리해 보면,

$$\mathrm{C}_{\max}(N) \geq p$$

와 같이 표현할 수 있다.



(1) $n(t)$의 자기상관 (2) $n(t)$와 $3n(t)$의 상호상관

그림1. 주기 24를 갖는 5진 수열군 N의 복소 상관 예

4. 비이진 Kasami 수열군 과의 관계

- 비이진 Kasami 수열[3]
  - 주기 p^2-1인 비이진 Kasami 수열군 S은

$$S = \left\{s_i(t) \middle| 0 \leq t \leq p^2-2\right\}$$

와 같이 정의된다. 여기서,

$$s_i(t) = \mathrm{Tr}_1^1\left\{\mathrm{Tr}_1^2(\alpha^t) + c_i\alpha^{(p+1)t}\right\}$$

이고, $c_i \in \mathrm{GF}(p)$이다.

  - 이 수열군 S의 비 자명 최대상관의 절대값은

$$|\mathrm{C}_{\max}(S)| \leq p+1$$

의 상계를 갖는다.

2. 노름 함수를 이용한 수열군의 생성

- 정의 1. p진 수열군 N을 다음과 같이 정의한다.

$$N = \{cn(t) | 1 \le c \le p-1\}.$$

여기서, $n(t)$는 $t = 0, 1, \ldots, p^2 - 1$ 에 대해 아래와 같이 정의한다.

$$n(t) = N_1^2(\alpha^t + 1).$$

3. 노름 함수로 생성한 수열군의 특성

- *보조정리 1.* 위에서 정의한 수열군 N에 속한 모든 수열의 주기는 $p^2 - 1$이다.
- *보조정리 2.* 수열 $a(t) = cn(t)$의 주기적 복소 자기상관의 절대값 $|C_{a(t),a(t)}(\tau)|$는, 임의의 순환지연 $\tau \not\equiv 0 \pmod{p^2-1}$에 대해,

$$|C_{a(t),a(t)}(\tau)| \le p + 1$$

의 상계를 갖는다.

- *보조정리 3.* 임의의 순환지연 $\tau \not\equiv 0 \pmod{p^2-1}$에 대해, 수열 $a(t) = c_1 n(t)$와 $b(t) = c_2 n(t)$의 주기적 복소 상호상관의 절대값 $|C_{a(t),b(t)}(\tau)|$는,

$$|C_{a(t),b(t)}(\tau)| \le p + 1$$

의 상계를 갖는다.

- *정리 1.* 보조정리 1, 2, 3으로 부터, 정의 1의 수열군 N은 주기가 $p^2 - 1$인 p진 수열군으로,

$$|C_{max}(N)| \le p + 1$$

의 상계를 만족함을 알 수 있다.
따라서, 이 수열군은 충분히 큰 p에 대해서, Welch bound와 1 만큼의 차이를 갖는다.

- 노름 함수를 이용하여 생성한 수열들과 $c_i \neq 0$ 인 비이진 Kasami 수열군과의 관계

$$\begin{aligned} s_i(t) &= \mathrm{Tr}_1^1\{\mathrm{Tr}_1^2(\alpha^t) + c_i\alpha^{(p+1)t}\} \\ &= \mathrm{Tr}_1^2(\alpha^t) + c_i\beta^t \\ &= \mathrm{Tr}_1^2(\alpha^t) + \beta^{t+\delta} \end{aligned}$$

$$\begin{aligned} cn(t) &= c\mathrm{N}_1^2(\alpha^t + 1) \\ &= c[\alpha^{t(p+1)} + \alpha^{tp} + \alpha^t + 1] \\ &= c[\beta^t + \mathrm{Tr}_1^2(\alpha^t) + 1] \\ &= \mathrm{Tr}_1^2(\alpha^t) + \beta^{t+\delta'} + c \end{aligned}$$

$\delta = \delta'$ 일 때, 상수 덧셈 관계

5. 결 론

- 노름 함수를 이용하여 정의 1과 같이

$$|C_{max}(N)| \le p + 1$$

을 만족하는 크기가 $p-1$인 주기 p^2-1의 p진 수열군을 생성할 수 있다.

- 허나, 이 수열군은 이미 잘 알려진 비이진 Kasami 수열군의 일부와 상수 덧셈 관계에 있다.

- 참고문헌

[1] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge University Press, 2005.

[2] L. R. Welch, "Lower bounds on the maximum crosscorrelation of signals (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397-399, 1974.

[3] S. C. Liu and J. J. Komo, "Nonbinary Kasami sequences over GF(p)," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1409-1412, 1992.