이차 잉여를 이용한 최적에 가까운 부분 하다마드 부호책 생성 방법

홍석범, 박호성, 노종선
서울대학교 뉴미디어통신공동연구소

fousbyus@ccl.snu.ac.kr, {hpark1,jsno}@snu.ac.kr

Near-Optimal Partial Hadamard Codebook Construction Using Quadratic Residue

Seokbeom Hong, Hosung Park, Jong-Seon No
Seoul National University, INMC

요 약

본 논문에서는 p진 m-시퀀스를 이차 잉여 (quadratic residue) 맵핑을 적용하여 변환한 이진 시퀀스를 이용하여 최적에 가까운 부분 하다마드 부호책을 생성하는 기법을 제안하였다. 제안하는 기법은 모든 홀수인 소수 p에 대해 항상 적용 가능하며, p의 값이 무한히 증가함에 따라 웰치 하한의 등호 조건에 수렴하는 것을 확인하였다

Ⅰ. 서 론

정규화 (normalize)된 길이 M의 복소 벡터 N개로 이루어진 집합 $\mathcal{C}=\{\mathbf{c}_0,\mathbf{c}_1,\cdots\mathbf{c}_{N-1}\}$를 (N,M) 부호책이라 한다. 부호책 $\mathcal{C}$에 속하는 각 벡터 쌍의 상관값 가운데 최댓값을 $I_{\max}(\mathcal{C})$라 할 때, 주어진 M,N에 대하여 부호책이 달성할 수 있는 최소의 $I_{\max}(\mathcal{C})$는 다음의 웰치 하한 (Welch bound)[1]을 통해 알 수 있다.

$$I_{\max}(\mathcal{C})=\max_{0\le l\ne m\le N-1}\left|\mathbf{c}_l^H\mathbf{c}_m\right|\ge\sqrt{\frac{N-M}{M(N-1)}} \quad (1)$$

부호책 $\mathcal{C}$가 (1)의 등호 조건을 만족하는 경우, 이를 maximum-Welch-bound-equality (MWBE) 부호책이라 한다.[2] 일반적으로 $I_{\max}(\mathcal{C})$의 값이 작은 부호책이 여러 응용 분야에서 더 우수한 성능을 보이는 것으로 알려져 있기 때문에, MWBE 부호책을 설계하기 위한 연구가 지속적으로 진행되어 왔다.[2]-[4] 그러나 MWBE 부호책을 설계하는 것은 매우 어려운 일이며, 현재까지 알려져 있는 MWBE 부호책은 매우 제한적인 M,N에 대해서만 존재한다.

이에 따라 최근에는 최적의 (optimal) MWBE 부호책뿐 아니라, 보다 다양한 M,N 값에 대하여 최적에 가까운 (near-optimal) 부호책을 설계하고자 하는 많은 시도가 이루어지고 있다.[2],[5]-[7]

이와 같은 연구를 통해 알려진 우수한 특성을 가지는 부호책들 가운데 상당수는, $N\times N$ 하다마드 또는 푸리에 행렬로부터 M개의 행을 선택하여 생성된 부분 하다마드 (또는 푸리에) (N,M) 부호책이다. 하다마드 행렬과 푸리에 행렬은 행렬 내의 각 열 간의 상관값이 0이고, 일정한 구조를 가지고 있기 때문에 우수한 성능을 가지는 부호책 생성에 이용하기에 적합하다.

본 논문에서는 p진 m-시퀀스를 이차 잉여 (quadratic residue)를 이용하여 이진 시퀀스로 변환시키고, 이렇게 생성된 이진 시퀀스를 이용하여 최적에 가까운 부분 하다마드 부호책을 생성하는 기법을 제안하였다. 제안하는 기법은 하다마드 행렬의 알파벳 크기 p가 홀수인 소수인 경우 항상 적용 가능하며, p의 값이 무한히 증가함에 따라 웰치 하한의 등호 조건에 수렴하는 것을 확인하였다.

Ⅱ. 최적에 가까운 부분 하다마드 부호책 생성 방법

먼저, 홀수인 소수 p와 짝수 n에 대하여 $p^n\times p^n$ p진 하다마드 행렬과, 이로부터 부분 하다마드 부호책을 생성하는 데에 사용되는 행 선택 시퀀스를 다음과 같이 정의하겠다.

Definition 1: 트레이스 함수 $\mathrm{Tr}_l^k(\cdot):GF(p^k)\to GF(p^l)$를 $\mathrm{Tr}_l^k(x)=\sum_{i=0}^{k/l-1}x^{p^{ki}}$와 같이 정의하고, α를 $GF(p^n)$ 상의 원시근 (primitive root), ω를 1의 p중근 (p-th root of unity)이라 하자. 이 때, $p^n\times p^n$ p진 하다마드 행렬 $H=[h_{i,j}]$는 다음과 같이 정의된다.

$$h_{i,j}=\begin{cases}1, & i=0 \text{ or } j=0\\ \omega^{\mathrm{Tr}_1^n(\alpha^{i+j-2})}, & \text{otherwise}\end{cases}$$

Definition 2: $n=2m$, $T=p^m+1$이라 하고, $QR(p)$를 $GF(p)$ 상에서 이차 잉여들을 모아서 생성한 집합이라 하자. 또한 이진 맵핑 $q:GF(p)\to GF(2)$를 아래와 같이 정의하겠다.

$$q(x)=\begin{cases}1, & x\in QR(p)\\ 0, & x\notin QR(p)\end{cases}$$

이 때, 행 선택 시퀀스 $\mathbf{r}=\{r_0, r_1, \cdots, r_{p^n-1}\}$은 아래와 같이 정의된다.

$$r_l = \begin{cases} q\left(\mathrm{Tr}_1^m\left(\alpha^{T(l-1)}\right)\right), & 1 \le l \le p^n - 1 \\ 0, & l = 0 \end{cases}$$

위에 정의한 하다마드 행렬 및 행 선택 시퀀스를 이용하여, 이차 잉여를 이용한 최적에 가까운 부분 하다마드 부호책을 다음과 같이 설계할 수 있다.

Construction 1: $N=p^n, M=\frac{p-1}{2p}\left(N+\sqrt{N}\right)$ 이라 하고, 위에서 정의한 행 선택 시퀀스 $\mathbf{r}$에서 0 이 아닌 값을 가지는 인덱스들을 모은 집합을 $S=\{s_0, s_1, \cdots, s_{M-1}\}$ 라 하자. 이 때, 각각의

$$\mathbf{c}_l = \frac{1}{\sqrt{M}}\left(h_{s_0,l}, h_{s_1,l}, \cdots, h_{s_{M-1},l}\right)^T, \qquad 0 \le l \le N-1$$

에 대하여 $\mathcal{C}_{H,r}=\{\mathbf{c}_0, \mathbf{c}_1, \cdots, \mathbf{c}_{N-1}\}$은 (N, M) 부분 하다마드 부호책이 된다.

Ⅲ. 모의 실험 및 분석

Ⅱ 장의 Construction 1 에서 제안한 부분 하다마드 부호책 $\mathcal{C}_{H,r}$의 $I_{\max}$ 값을 모의 실험을 통해 확인해 본 결과는 다음의 표 1 과 같다. 표 1 의 I_{Welch}는 (1)의 웰치 하한의 등호 조건을 만족하는 값을 의미한다.

표 1 에서 확인할 수 있는 바와 같이, 제안하는 부분 하다마드 부호책의 최대 상관값은 웰치 하한과 비교적 근접한 값을 가지며, p의 값이 커질수록 웰치 하한에 더욱 근접하는 것을 확인할 수 있다.

이와 같은 실험 결과를 토대로, 제안하는 부분 하다마드 부호책의 최대 상관값 $I_{\max}$ 값을 다음의 Conjecture 1 과 같이 예측할 수 있다. 비록 이를 증명하지는 못하였으나, 다양한 p, n 값에 대하여 모의 실험을 수행한 결과 Conjecture 1 이 항상 성립하는 것을 확인하였다.

Conjecture 1: Construction 1 에서 제안한 부분 하다마드 부호책 $\mathcal{C}_{H,r}$의 최대 상관값 $I_{\max}(\mathcal{C}_{H,r})$ 값은 다음과 같다.

$$I_{\max} = \frac{1}{M}\cdot\frac{(p+1)\sqrt{N}}{2p} = \frac{p+1}{(p-1)(\sqrt{N}+1)}$$

또한, Conjecture 1 에서 예측한 $I_{\max}$ 에 대하여 $\frac{I_{\max}}{I_{\mathrm{Welch}}}$의 상한을 아래의 Theorem 1 을 통해 유도하였다. (증명은 간단하여 생략) 이를 통해 $I_{\max}$값이 p가 커질수

표 1. 제안하는 부분 하다마드 부호책의 최대 상관값

p	n	N	M	I_{Welch}	$I_{\max}$	$\frac{I_{\max}}{I_{\mathrm{Welch}}}$
3	4	81	30	1.46E-01	2.00E-01	1.372
3	6	729	252	5.10E-02	7.14E-02	1.401
3	8	6561	2214	1.73E-02	2.44E-02	1.410
5	2	25	12	2.13E-01	2.50E-01	1.176
5	4	625	260	4.74E-02	5.77E-02	1.216
7	2	49	24	1.47E-01	1.67E-01	1.131
7	4	2401	1050	2.32E-02	2.67E-02	1.152

록 웰치 하한에 근접하는 최적에 가까운 부분 하다마드 부호책임을 확인하였다.

Theorem 1: $I_{\max}$가 제안하는 부분 하다마드 부호책 $\mathcal{C}_{H,r}$의 최대 상관값이고 I_{Welch}는 웰치 하한의 등호 조건을 만족하는 값일 때, 다음의 식이 성립한다.

$$\frac{I_{\max}}{I_{\mathrm{Welch}}} < \sqrt{\frac{p+1}{p-1}}$$

ACKNOWLEDGMENT

이 논문은 2012 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2012-0000186).

참 고 문 헌

[1] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," IEEE Trans. Inf. Theory, vol. IT-20, no. 3, pp. 397-399, May 1974.

[2] D. V. Sarwate, "Meeting the Welch bound with equality," in Sequences and their Applications, C. Ding, T. Helleseth, and H. Niederreiter, Eds. New York: Springer-Verlag, 1999, DMTCS Series, pp. 79-102.

[3] T. Strohmer and R. Heath, "Grassmannian frames with applications to coding and communication," Appl. Comput. Harmon. Anal., vol. 14, no. 3, pp. 257-275, May 2003.

[4] C. Ding and T. Feng, "A generic construction of complex codebooks meeting the Welch bound," IEEE Trans. Inf. Theory, vol. 53, no. 11, pp. 4245-4250, Nov. 2007.

[5] N. Y. Yu, "A construction of codebooks associated with binary sequences," IEEE Trans. Inf. Theory, vol. 58, no. 8, pp. 5522-5533, Aug. 2012.

[6] C. Ding and T. Feng, "Codebooks from almost difference sets," Des. Codes Cryptogr., vol. 46, pp. 113-126, 2008.

[7] A. Zhang and K. Feng, "Two classes of codebooks nearly meeting the Welch bound," IEEE Trans. Inf. Theory, vol. 58, no. 4, pp. 2507-2511, Apr. 2012.