그룹 G상의 일반화된 하다마드 행렬을 이용한 G^m상의 일반화된 하다마드 행렬의 확장

정회원 노 종 선*, 송 홍 엽**

Expanding Generalized Hadamard Matrices over G^m by Using Generalized Hadamard Matrices over G

Jong-Seon No*, Hong-Yeop Song** *Regular Members*

요 약

주어진 양의 정수 λ에 대해서 차수가 g인 가산 교환그룹 G상에서 $g\lambda \times g\lambda$ 일반화된 하다마드 행렬 $GH(g,\lambda)=[h(i,j)]$ $(1\le i\le g\lambda, 1\le j\le g\lambda)$가 정의될 수 있는데, 그러면 $h(i_1,1)-h(i_2,1)$, $h(i_1,2)-h(i_2,2)$, $\cdots$, $h(i_1,g\lambda)-h(i_2,g\lambda)$에서 G의 모든 요소는 정확히 λ번씩 나타난다. 이 논문에서는 주어진 행렬 $GH(g^m,\lambda_1)=B=[B_{ij}]$에서 각각의 m-튜플 B_{ij}를 $m=g\lambda_2$일 때, $B_{ij}\oplus GH(g,\lambda_2)$ 로 대치함으로써 행렬을 확장하는 새로운 방법을 제시한다. 여기서 $g^m\lambda_1$개의 $GH(g,\lambda_2)$를 사용하여 치환하며 생성되는 행렬은 차수가 g인 그룹에서 정의되는 것이다.

ABSTRACT

Over an additive abelian group G of order g and for a given positive integer λ, a generalized Hadamard matrix $GF(g,\lambda)$ is defined as a $g\lambda\times g\lambda$ matrix $[h(i,j)]$, where $1\le i\le g\lambda, 1\le j\le g\lambda$, such that every element of G appears exactly λ times in the list $h(i_1,1)-h(i_2,1), h(i_1,2)-h(i_2,2),\cdots,h(i_1,g\lambda)-h(i_2,g\lambda)$ for any $i\ne j$. In this paper, we propose a new method of expanding a $GH(g^m,\lambda_1)=B=[B_{ij}]$ over G by replacing each of its m-tuple B_{ij} with $B_{ij}\oplus GH(g,\lambda_2)$ where $m=g\lambda_2$. We may use $g^m\lambda_1$ (not necessarily all distinct) $GH(g,\lambda_2)$'s for the substitution and the resulting matrix is defined over the group of order g.

Ⅰ. 서 론

$\lambda\times\lambda$ 하다마드 행렬 H_λ는 I_λ가 $\lambda\times\lambda$ 항등원 행렬일 때, $H_\lambda\cdot H_\lambda^T=\lambda I_\lambda$가 되고 요소가 +1 또는 -1로 구성되는 행렬이다[5],[11],[16]. 이것은 H_λ의 각기 다른 두 개의 행이 서로 직교한다는 것을 의미한다. 이러한 이유로 인하여, 하다마드 행렬은 통신시스템, 부호이론 등의 많은 관련 분야에서 연구되어 왔다[1],[9],[15],[16],[17].

하다마드 행렬에서 심볼 부호(symbol alphabet)는 차수가 2 이상인 그룹으로 일반화될 수 있다. 이러한 경우에 직교성의 개념은 다음과 같은 정의에 의해서 표현될 수 있다[1],[3],[4],[6]. 본 논문에서는 그룹은 가산 교환그룹(additive abelian group)으로 국한한다.

정의 1: G를 가산 교환그룹이라 하고, $u_i, v_j\in G$일때, $u=(u_1,u_2,\cdots,u_{g\lambda})$와 $v=(v_1,v_2,\cdots,v_{g\lambda})$를 정의하자. u, v에 대해서 각 성분끼리의 차 u_1-v_1,

* 서울대학교 전기공학부 ** 연세대학교 전기전자공학과

논문번호 : 00318-0804, 접수일자 : 2000년 8월 4일

※ 본 연구는 한국과학재단의 특정기초연구사업(97-0100-0501-3)의 지원에 의해 수행되었습니다.

$u_2-v_2, \cdots, u_{g\lambda}-v_{g\lambda}$에서 G의 모든 원소가 정확히 λ번씩 나오는 경우에 차균형 (difference-balanced)이라고 한다.

정의 2: G가 가산 교환그룹일때, 양의 정수 λ에 대해서 행렬 $GH(g,\lambda)$의 서로 다른 어떠한 두 행도 차균형이면 $GH(g,\lambda)$는 G상의 $g\lambda \times g\lambda$ 일반화된 하다마드 행렬이라 정의한다.

Remark 3: $GH(2,\lambda/2)$는 차수가 λ인 이진 하다마드 행렬이라 한다.

$\lambda=1$일 때, $GH(g,1)$의 쉬운 예로 차수가 $g\geq 1$인 순회그룹의 그룹 표(group table)를 들 수 있다. 다른 다양한 g와 λ의 쌍에 대해서 하다마드 행렬을 생성할 수 있다[1],[3],[4],[6],[13].

이진 하다마드 행렬의 잘 알려진 생성 방법 중 하나로 Sylvester에 의해서 제안된 것이 있다[1],[5],[11]. 이 방법에 의하면, 먼저 각각 m, k의 차수를 갖는 하다마드 행렬 H_m과 $H_k=[h_{ij}]$가 있다고 할 때, $h_{ij}=\pm 1$를 $\pm H_m$으로 치환함으로써 mk의 차수를 갖는 새로운 하다마드 행렬을 생성할 수 있다. Sylvester 방법에 의해 생성된 차수 8인 하다마드 행렬의 한 예가 그림 1.에 나타나 있다.

+	+	+	+	+	+	+	+
+	−	+	−	+	−	+	−
+	+	−	−	+	+	−	−
+	−	−	+	+	−	−	+
+	+	+	+	−	−	−	−
+	−	+	−	−	+	−	+
+	+	−	−	−	−	+	+
+	−	−	+	−	+	+	−

그림 1. Sylvester 생성방법에 의한 차수 8인 하다마드 행렬

H_8은 16개의 차수 2인 블록들로 이루어져 있으며, 그 각각의 블록들은 모두 H_2이거나 $-H_2$임을 알 수 있다. 이와 유사하게, $B=[B_{ij}]=GH(g,\lambda_1)$과 $C=GH(g,\lambda_2)$가 G상에서 존재한다고 가정할 때, 차수 g를 갖는 G상의 일반화된 하다마드 행렬 $GH(g, g\lambda_1\lambda_2)$의 생성방법도 존재한다[4]. 이것은 B의 각각의 원소 B_{ij}를 $B_{ij}+C$로 치환함으로써, 블록들이 $a\in G$에 대해서 $a+C$의 형태를 갖도록 하는 방법이다. 이 방법은 일반화된 하다마드 행렬의 Sylvester 생성방법이라 한다.

본 논문에서는 행렬에서 각각의 m-튜플 B_{ij}를 $B_{ij}\oplus GH(g,\lambda_2)$로 치환하여 확장된 하다마드 행렬 $GH(g^m,\lambda_1)=B=[B_{ij}]$를 생성시키는 방법을 제안한다. 여기서, $m=g\lambda_2$이며, 연산 $\oplus$는 제2장에서 정의된다. 치환을 위하여, 서로 다르거나 또는 같은 $g^m\lambda_1$개의 $GH(g,\lambda_2)$이 사용되며, 생성되는 행렬은 차수 g인 그룹 상에서 정의된다.

새로운 일반화된 하다마드 행렬 생성방법의 증명은 제2장에서 기술될 것이며, 또한 몇몇의 예가 제시될 것이다. F_2상에서의 한 예가 길이 15인 4진 m 시퀀스를 이용하여 주어진다.

Ⅱ. 일반화된 하다마드 행렬의 생성

G를 차수 g인 그룹이라 하자. 주어진 일반화된 G상의 하다마드 행렬 $GH(g,\lambda)$는 (i) 각 행이나 열들끼리의 교환, (ii) 한 행이나 열의 모든 원소들에 $a\in G$를 가산함으로써, 다른 행렬로 변형시킬 수 있다. 위의 연산들의 조합에 의한 차이만을 갖는 두 개의 일반화된 하다마드 행렬은 등가라고 한다. 한 주어진 일반화된 하다마드 행렬에 대하여, 가장 위에 있는 첫 번째 행과 맨 왼쪽의 열이 모두 0으로만 이루어진 등가의 행렬을 찾을 수 있다. 그러한 일반화된 하다마드 행렬을 정규화 되었다고 한다. 그리고 나머지의 행들이 G의 모든 원소를 λ개씩 가지고 있다는 것은 자명하다. G가 차수가 g인 그룹이라 할 때, G의 모든 m-튜플 들은 차수 g^m인, 성분별 덧셈에 대한 그룹을 이룬다. 이 그룹을 앞으로는 G^m이라 할 것이다. $\oplus$는 G^m상에서의 연산으로 정의된 것이다. 또한 연산$\oplus$는 다음과 같이 정의된다.

정의 4: (연산 $\oplus$) $X=(x_1,x_2,\cdots,x_m)$는 G상에서의 m-튜플이고, C는 G상의 $k\times m$행렬이라 하자. 그리고, C의 행들을 $\underline{C_1}, \underline{C_2}, \ldots, \underline{C_n}$라 하면 다음과 같이 정의된다.

$$X\oplus C = X\oplus\begin{bmatrix}\underline{C_1}\\ \underline{C_2}\\ \vdots\\ \underline{C_k}\end{bmatrix}=\begin{bmatrix}X\oplus\underline{C_1}\\ X\oplus\underline{C_2}\\ \vdots\\ X\oplus\underline{C_k}\end{bmatrix}$$

$$= \begin{bmatrix} x_1+c_{11}, & x_2+c_{12}, & \cdots & , x_m+c_{1m} \\ x_1+c_{21}, & x_2+c_{22}, & \cdots & , x_m+c_{2m} \\ & \vdots & & \\ x_1+c_{k1}, & x_2+c_{m2}, & \cdots & , x_m+c_{km} \end{bmatrix}$$

위의 연산은 본 논문의 일반화된 하다마드 행렬 생성방법의 중요한 역할을 한다. 연산 $X \oplus C$의 결과로, C의 각 행인 $\underline{C_i}$가 $X \oplus \underline{C_i}$으로 치환된다. 바꾸어 말하면, C의 모든 행, 예를 들어, j 번째 행의 원소 c_{ij}가(x_j가 X의 j 번째 원소일 때), x_j+c_{ij}로 치환되는 것이 있다. 그리고, 이것은 다음의 보조정리를 증명해 준다.

보조정리 5: G를 차수가 g인 그룹이라 하고, $m=g\lambda$ 라 하자. X가 G상의 m-튜플이고, C는 G상의 $GH(g,\lambda)$이면 $X \oplus C$는 G상의 $GH(g,\lambda)$이다.

정리 6: G가 차수 g인 그룹일 때, G^m상의 일반화된 하다마드 행렬 $B \triangleq [B_{ij}] \triangleq GH(g^m, \lambda_1)$가 존재한다고 가정하다. 또한, G상의 $GH(g,\lambda_2)$이며, 모두 각기 다를 필요는 없는 M개의 일반화된 하다마드 행렬 $C^{(1)}, C^{(2)}, \cdots, C^{(M)}$가 존재한다고 가정하다. 만약 $M=g^m\lambda_1$이고 $m=g\lambda_2$이면 G상에서 B_{ij}를 $B_{ij} \oplus C^{(i)}$로 대치하여 얻어지는 크기가 $mM \times mM$인 행렬 H는 G상에서 일반화된 하다마드 행렬 $GH(g, g^m\lambda_1\lambda_2)$가 된다.

증명 : 위의 생성방식에 의한 행렬 H는 다음과 같다.

$$H = \begin{bmatrix} B_{11} \oplus C^{(1)} & B_{12} \oplus C^{(1)} & \cdots & B_{1M} \oplus C^{(1)} \\ B_{21} \oplus C^{(2)} & B_{22} \oplus C^{(2)} & \cdots & B_{2M} \oplus C^{(2)} \\ B_{31} \oplus C^{(3)} & B_{32} \oplus C^{(3)} & \cdots & B_{3M} \oplus C^{(3)} \\ \vdots & \vdots & \cdots & \vdots \\ B_{M1} \oplus C^{(M)} & B_{M2} \oplus C^{(M)} & \cdots & B_{MM} \oplus C^{(M)} \end{bmatrix} \qquad (1)$$

행렬 H는 각각의 크기가 $m \times m$인 M^2개의 부분행렬들로 구성되어 있다. 여기서 H의 연속적인 m개의 행을 행블록이라 하자. 즉, H는 M개의 행블록을 가지고, 각각의 행블록은 크기가 $m \times m$인 M개의 부분행렬을 포함하고 있다. 여기서 증명해야 할 것은, G상에서 길이가 $L(\doteq mM)$인 H의 서로 다른 2개의 행은 첫번째 정의로부터 차균형(difference-balanced)이라는 것을 알 수 있다. 여기서는 (I) 두 개의 행이 같은 행블록에 있는 경우와 (II) 두 개의 행이 서로 다른 행블록에 있는 경우 등 두 가지로 나누어 생각한다.

(경우 I) 보조정리 5에 의해 모든 i 와 j 에 대해 각각의 $m \times m$ 부분행렬 $B_{ij} \oplus C^{(i)}$는 G상에서 $GH(g,\lambda_2)$이다. 따라서 동일한 행블록에서 나온 H의 모든 서로 다른 두 개의 행은 차균형이다. 이 경우, 각각의 $C^{(i)}$가 일반화된 하다마드 행렬이라는 가정을 사용하였다.

(경우 II) $i \neq j$ 라 가정하고, $1 \leq x,\ y \leq m$인 $x,\ y$에 대해 i번째 행블록의 x번째 행과 j번째 행블록의 y번째 행을 생각해 보자. 만일 $C^{(i)}$의 x번째 행과 $C^{(j)}$의 y번째 행을 각각 $\underline{C_x^{(i)}}$와 $\underline{C_y^{(j)}}$로 나타내기로 하면, 두 개의 행은 다음과 같이 생각할 수 있다.

i 번째 행블록의 x 번째 행:

$$B_{i1} \oplus \underline{C_x^{(i)}}\ B_{i2} \oplus \underline{C_x^{(i)}}\ \cdots\ B_{iM} \oplus \underline{C_x^{(i)}}$$

j 번째 행블록의 y 번째 행:

$$B_{j1} \oplus \underline{C_x^{(j)}}\ B_{j2} \oplus \underline{C_x^{(j)}}\ \cdots\ B_{jM} \oplus \underline{C_x^{(j)}} \qquad (2)$$

위에서 B_{ik}, B_{jk}, $\underline{C_x^{(i)}}$, $\underline{C_y^{(j)}}$는 모두 G상에서 m-튜플이다. 만약 (2)의 두 행을 G^m상에서 길이가 M인 벡터로 간주하면, B의 i번째 행과 j번째 행이 차균형이므로 두 행은 G^m상에서 차균형이라 할 수 있다. 이러한 G^m상에서의 차들은 $\underline{C_x^{(i)}} \ominus \underline{C_y^{(j)}} \doteq D$가 성립하게 한다.

$$B_{ik} \ominus B_{jk} \oplus D, \quad \text{for} \quad k=1,\ 2,\ \cdots, M. \qquad (3)$$

위에서 D는 G상에서 m개의 성분을 갖는 벡터이고, k에 관계없이 $B_{ik} \ominus B_{jk}$는 일정한 편이(bias)를 갖는다. 다른 면에서, $B_{ik} \ominus B_{jk}$는 각 성분별로 계산되므로 (3)에서 정의된 차의 성분들에만 관심을 갖는다. 이와 유사하게 (2)의 두 행은 G상에서 길이가 mM인 벡터로 간주되고, G상에서 각 성분들의 차만을 고려한다. 그것들은 현재 찾는 성분들을 제외한 (3)에 열거한 차들과 정확히 일치한다. 또한 G^m의 모든 m개의 성분을 갖는 벡터들이 정확히 M/λ_1번씩 나타나는 G상의 M개의 m-튜플에서 G상의 모든 성분들이 정확히 mM/g번 나타나므로 (2)의 두 행은 G상에서 차균형이라 할 수 있다. 이 경우 B가 G^m상에서 일반화된 하다마드 행렬이라는 가정을 사용하였다.

Remark 7: 집합 상에서 일반화된 하다마드 행렬은 정방 행렬(square matrix)이다. 행렬에 있는 서로 다른 두 행의 차가 위와 같은 조건을 만족시키는 사각 배열을 차행렬(difference matrix)이라고 한다. 정리 6의 증명은 B나 C는 정방행렬이라는 사실을 사용하지 않았기 때문에 우리의 행렬 생성 방법은 차이행렬의 생성에 쉽게 적용될 수 있다[4]. 그러므로 우리의 생성방법은 G상에서 보다 큰 차이행렬을 구현하기 위해 G^m상에서의 차행렬 B와 G상에서의 C에 직접적으로 적용된다.

Remark 8: 하다마드 행렬의 생성에 있어, 모두 같은 $C^{(i)}$들 또는 다르지만 등가인 $C^{(i)}$들, 모두 등가가 아닌 $C^{(i)}$들을 사용할 수 있다. 그러나 $C^{(i)}$들이 모두 같은 경우에도 구현방법이 Sylvester 생성 방법과 다름에 주목해야 한다.

예제 9: 3으로 나머지 연산을 취한 가산그룹 $G=\{0,1,2\}$을 생각해보자. 만약 $m=3\lambda_2$, $M=3^m\lambda_1$에 대해, G^m상에서 $B=GH(3^m,\lambda_1)$이고 G상에서 $GH(3,\lambda_2)$가 M (반드시 다를 필요는 없음)개가 있다면 G상에서 $GH(3,mM/3)$이 생성될 수 있다.

예제 10: 어떤 소수 p에 대해 G가 p개의 원소를 갖는 유한체 상의 가산그룹이라고 하자. 만약 $m=p\lambda_2$, $M=p^m\lambda_1$에 대해 F_{p^m}상에서 $B=GH(p^m,\lambda_1)$이고 F_p상에서 $GH(p,\lambda_2)$가 M(반드시 구별될 필요는 없는)개 있다면 F_p상에서 $GH(p,mM/p)$가 생성될 수 있다.

예를 들어 $p=2$인 경우를 생각해 보자. 만약 $\{b_t|t=0,\ 1,\ 2,\ \cdots,\ N-1\}$가 어떤 n에 대해 주기가 $N=2^{mn}-1$인 2^m진 m 시퀀스[2], [7], [8], [10], [12]라 하면, 아래와 같은 $(N+1)\times(N+1)$ 행렬은 가산그룹 F_{2^m}상에서 일반화된 하다마드 행렬 $GH(g^m,\lambda_1)=GH(2^m,2^{m(n-1)})$ 이 된다

$$B \triangleq \left[\begin{array}{c|ccccc} 0 & 0 & 0 & 0 & \cdots & 0 \\ \hline 0 & b_0 & b_1 & b_2 & \cdots & b_{N-1} \\ 0 & b_1 & b_2 & b_3 & \cdots & b_0 \\ 0 & b_2 & b_3 & b_4 & \cdots & b_1 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & b_{N-1} & b_0 & b_1 & \cdots & b_{N-2} \end{array}\right] \qquad (4)$$

위 행렬에서 0과 b_i는 F_2상에서 m-튜플 벡터로 나타낼 수 있다[10]. 이제 $M=N+1=2^{mn}$이라 하자. 만약 F_2상에서 M (반드시 다를 필요는 없음)개의 이진 하다마드 행렬 $GH(2,m/2)$가 있다면, F_2상에서 크기가 $m2^{mn}\times m2^{mn}$인 이진 하다마드 행렬 $GH(2,mM/2)=GH(2,m2^{mn-1})$을 생성 할 수 있다. 특별한 경우로 $m=2$이고 $n=2$를 생각해 보자. $F_4=\{0,\ 1,\ \beta,\ \beta^2\}$이다. 그러면 다음은 주기가 15인 4진 m 시퀀스가 된다.

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
b_t	0	1	1	β^2	1	0	β	β	1	β	0	β^2	β^2	β	β^2

위의 시퀀스로부터 다음과 같은 F_4상에서 $GH(4,4)$를 생성할 수 있다.

$$B=\left[\begin{array}{c|ccccccccc} 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & & \beta^2 & \beta^2 & \beta & \beta^2 \\ 0 & 1 & 1 & \beta^2 & & \beta^2 & \beta & \beta^2 & 0 \\ 0 & 1 & \beta^2 & 1 & \cdots & \beta & \beta^2 & 0 & 1 \\ 0 & \beta^2 & 1 & 0 & & \beta^2 & 0 & 1 & 1 \\ 0 & 1 & 0 & \beta & & 0 & 1 & 1 & \beta^2 \\ 0 & 0 & \beta & \beta & & 1 & 1 & \beta^2 & 1 \\ 0 & \beta & \beta & 1 & & 1 & \beta^2 & 1 & 0 \\ 0 & \beta & 1 & \beta & \cdots & \beta^2 & 1 & 0 & \beta \\ 0 & 1 & \beta & 0 & & 1 & 0 & \beta & \beta \\ 0 & \beta & 0 & \beta^2 & & 0 & \beta & \beta & 1 \\ 0 & 0 & \beta^2 & \beta^2 & & \beta & \beta & 1 & \beta \\ 0 & \beta^2 & \beta^2 & \beta & & \beta & 1 & \beta & 0 \\ 0 & \beta^2 & \beta & \beta^2 & \cdots & 1 & \beta & 0 & \beta^2 \\ 0 & \beta & \beta^2 & 0 & & \beta & 0 & \beta^2 & \beta^2 \\ 0 & \beta^2 & 0 & 1 & & 0 & \beta^2 & \beta^2 & \beta \end{array}\right]$$

이제 F_4의 $0,\ 1,\ \beta,\beta^2$을 F_2상에서 2개의 성분 00, 01, 10, 11로 나타내보자.

$1\le i\le 8$에서 $C^{(i)}=\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$이라 가정하고, $9\le i\le 16$에 대해 그 전치행렬을 $C^{(i)}$로 취하고 B의

표 1. B가 F_4 상의 $GH(4,4)$ 일 때, $GH(2,16)$으로 바꾸는 치환 방법

B 의 윗 반쪽	*B*의 아래 반쪽
0를 $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ 로 치환	0를 $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ 로 치환
1을 $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ 로 치환	1을 $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ 로 치환
β를 $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ 로 치환	β를 $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ 로 치환
β^2을 $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ 로 치환	β^2을 $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ 로 치환

0, 1, β, β^2을 표 1.에 대치시켜주면 32×32 하다마드 행렬이 구해진다.

Ⅳ. 결 론

본 논문의 주 내용은 모든 i에 대해 B의 각각의 m개의 성분을 갖는 벡터 B_{ij}를 $B_{ij}\oplus C^{(i)}$로 바꾸어주는 것이다. 앞으로의 연구 방향은 $C^{(i)}$의 몇몇 다른 차집합으로부터 얻어지는 두 일반화된 하다마드 행렬의 등가성에 대한 연구이다.

참 고 문 헌

[1] S. S. Agaian, *Hadamard Matrices and Their Applications*, Lecture Notes in Mathematics, vol. 1168, Springer Berlag, New-York, 1980.

[2] L. D. Baumert, *Cyclic Differences Sets*, Lecture Notes in Mathematics, Springer-Verlag, 1971.

[3] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, London, 1986.

[4] C. J. Colbourn and W. De Launey "Difference matrices," Chapter IV.11, *CRC Handbook of Combinatorial Designs*, edited by C. J. Colbourn and J. H. Dinitz, CRC Press, New York, pp. 287-297, 1996.

[5] R. Craign, "Hadamard matrices and designs," Chapter IV .24, *CRC Handbook of Combinatorial Designs*, edited by C. J. Colbourn and J. H. Dinitz, CRC Press, New York, pp. 370-377, 1996.

[6] W. De Launey, "Generalized Hadamard matrices which are developed modulo a group," *Discrete Mathematics*, vol. 104, pp. 49-65, 1992.

[7] W. W. Golomb, *Shift-Register Sequences*, Holden-Day, San Francisco, CA, 1967; Aegean Park Press, Laguna Hills, CA 1982.

[8] D. Jungnickel, "Difference Sets," in book, *Contemporary design Theory: A Collection of Surveys*, edited by J. H. Dinitz and D. R. Stinson, John Wiley and Sons, pp. 241-324, 1992.

[9] J.-H. Kim and H.-Y. Song, "Existence of Cyclic Hadamard Difference Sets and its Relation to Binary Sequences with Ideal Autocorrelation," *Journal of Communications and Networks*, vol. 1, no. 1, pp. 14-18, March 1999.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*, Addison-Weseley, Reading, MA, 1983.

[11] J. H. van Ling and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, New York, 1992

[12] J. -S. No, H. -K. Lee, H. Chung, H, -Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Transactions of Information Theory*, vol 42, No. 6, pp. 2254-2255, Nov., 1996.

[13] J. -S. No and H. -Y. Song, "Generalized Sylvester-type Hadamard matrices," pre-print, 1999.

[14] J. -S. No, H. -Y. Song, H. Chung, and K. Yang, "Extension of Binary Sequences with Ideal Autocorrelation Property," preprint, 1999.

[15] H. Y. Song and W. W. Golomb, "On the existence of cyclic Hadamard difference sets," *IEEE Transactions on Information Theory*, vol. TI-40, pp. 1266-1268, July 1994.

[16] J. Severry and M. Yamada, "Hadamard Matrices, Sequences, and Block Design," in book, *Contemporary Design Theory: A*

Collection of Surveys, edited by J. H. Dinitz and D. R. Stinson, John Wiley and Sons, pp. 431-560, 1992

[17] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. 1, Computer Science Press, Rockville, MD, 1985; revised edition, McGraw-Hill, 1994.

노 종 선(Jong-Seon No) 종신회원
한국통신학회논문지 제25권 4A호 참조

송 홍 엽(Hong-Yeop Song) 종신회원
한국통신학회논문지 제25권 3A호 참조