[UCI]I804:24011-200000280470

2020년 2월
교육학석사(수학교육)학위논문

행의 무게가 일정한 이진 (w, r)-중첩 부호 연구

조선대학교 교육대학원

수학교육전공

박 미 영

행의 무게가 일정한 이진 (w,r)-중첩 부호 연구

On the study of binary (w,r)-superimposed codes with constant row weight

2020년 2월

조선대학교 교육대학원

수학교육전공

박 미 영

행의 무게가 일정한 이진 (w, r)-중첩 부호 연구

지도교수 오 동 렬

이 논문을 교육학석사(수학교육)학위 청구논문으로 제출함.

2019년 10월

조선대학교 교육대학원

수학교육전공

박 미 영

박미영의 교육학 석사학위 논문을 인준함.

심사위원장 조선대학교 교수 안 영 준 인

심사위원 조선대학교 교수 이 관 규 인

심사위원 조선대학교 교수 오 동 렬 인

2019년 12월

조선대학교 교육대학원

CONTENTS

ABSTRACT

1. 소　　개 ····· 1

2. 중첩 부호 ····· 3

3. 행의 무게가 일정한
   이진 (w,r)-중첩 부호 ····· 12

참고문헌 ····· 18

ABSTRACT

On the study of binary $(w,r)-$superimposed codes with constant row weight

Park, Mi Young
Advisor : Prof. Dong Yeol Oh Ph.D.
Major in Mathematics Education
Graduate School of Education, Chosun University

Let X be a finite set with T elements and F be a family of subsets of X such that no intersection of w members of the family is covered by a union of r others, where $|F|=N$. The incidence matrix C of the family F is called a (binary) $(w,r)-$superimposed code of size $N\times T$. For a given $N\times T$ $(w,r)-$ superimposed code, resulting code obtained from the given $(w,r)-$superimposed code by inserting a new row or deleting any column is also a $(w,r)-$superimposed code. For a given T, w and r, we denote $N(T:w,r)$ by the minimal number of rows of $(w,r)-$superimposed code with T columns. An $N(T:w,r)\times T$ $(w,r)-$ superimposed code is called an optimal code. For a $(w,r)-$superimposed code C, C is called a $(w,r)-$superimposed code with constant weight k if the weight of rows of C is constant k. For a given T, w, r and k, we denote $N(T:w,r,k)$ by the minimal number of rows of $(w,r)-$superimposed code with T columns and constant weight k. In this thesis, we find the lower bound of $N(T:w,r,k)$ and study when the equality holds.

제 1 장 소 개

주어진 유한 집합에서, 서로 포함 관계가 없는 부분집합의 모임을 Sperner 족(Sperner family) 또는 덮개-자유 족(cover-free family)이라 한다. 1964년에 Kautz 와 Singleton[7]은 덮개-자유 족을 확장한 $(1,r)$ 덮개-자유 족을 소개하고 (주어진 유한 집합의 부분집합의 모임으로서 그 모임의 임의의 멤버가 r개의 멤버의 합집합에 포함되지 않는 모임을 $(1,r)$ 덮개-자유 족이라 한다.) 이 모임의 투사행렬(incidence matrix)을 $(1,r)-$중첩 부호라 하였다. 이후 D'yachikov 와 그 연구진[1,2]은 더욱 일반화 된 (w,r) 덮개-자유 족을 소개하고, 그 모임의 투사행렬을 $(w,r)-$중첩 부호라 하였다. 1988년 Michell 과 Piper[10]은 네트워크상에서 사용자들에게 키를 안전하게 분배하기 위한 방법으로 키 분배 패턴(key distribution pattern)을 제안하였다. 키 분배 패턴이 수학적으로 정확히 덮개-자유 족과 동일한 개념으로 밝혀짐으로 인해 중첩 부호는 부호이론, 조합이론 및 암호이론의 공통의 연구 대상이 되었다.

(w,r) 덮개-자유 족은 유한 집합의 부분집합의 모임으로서 임의의 w개의 부분집합의 교집합이 r개의 부분집합의 합집합에 포함되지 않는 모임을 의미하며, 이 모임의 투사 행렬을 $(w,r)-$중첩 부호라 한다. $w=r=1$인 경우 초기에 연구되어진 유명한 Sperner 족이 된다. 투사 행렬의 관점에서 보면, 성분이 0과 1로 이루어진 $N\times T$ 행렬 C 에 대하여 공통의 열이 없는 임의의 w개와 r개의 열에 대하여, w개의 열에 대한 좌표성분은 1이고 r개의 열에 대한 좌표성분은 0이 되는 행이 존재할 때 행렬 C를 $(w,r)-$중첩 부호라 한다.

주어진 w, r에 대하여, $N\times T$ 행렬 C를 $(w,r)-$중첩 부호라 하자. 행렬 C에서 새로운 행을 추가하거나, 임의의 열을 제거하여 얻은 행렬들 또한 $(w,r)-$중첩 부호가 됨을 쉽게 알 수 있다. 주어진 변수들에 대한 최소 행의 개수(또는 최대 열의 개수)를 $N(T,w,r)$(또는 $T(N,w,r)$)이라 하고, 이 때, $N(T,w,r)\times T$(또는 $N\times T(N,w,r)$)$(w,r)-$중첩 부호를 최상 중첩 부호라 한다.

중첩 부호의 주요 연구 주제로 다음의 문제들이 있다.

(1) T가 주어진 경우 $N(T,w,r)$의 상계, 하계문제
(쌍대 문제로 N이 주어진 경우 $T(N,w,r)$의 상계, 하계 문제)
(2) 충분히 큰 T,N에 대한 $(w,r)-$중첩 부호의 점근적 행동(asymptotic behavior)문제
(3) 최적 중첩 부호(optimal superimposed code)의 구조 문제
(4) $(w,r)-$중첩 부호의 구성문제들이 있다.

$w=r=1$인 경우 위의 문제들은 극 집합 이론의 중요한 결과인 Sperner 정리에 의해 완벽히 해결되었으며, P. Erdős를 포함한 많은 연구자들에 의해 $(1,2)$, $(1,r)$ 중첩 부호에 대한 많은 연구가 이루어 졌다. ([2-6],[8],[9],[11],[12])

중첩 부호의 최적화와 관련하여 T,w,r이 주어진 경우, T개 원소를 가지는 집합에서 임의의 w개의 원소를 가지는 부분 집합의 모임은 항상 (w,r) 자유-덮개 족이 됨으로 크기가 $\binom{T}{w}\times T$ 인 (w,r)-중첩 부호는 항상 존재함을 알 수 있고, 이 부호를 자명 중첩 부호라 한다. 따라서 $N(T,w,r)$의 상계는 $N(T:w,r)\le\binom{T}{w}$이다.

본 학위 논문은 최상 중첩 부호의 상계문제와 관련하여 다른 조건 하나를 추가하여 공부하였다. 즉, $(w,r)-$중첩 부호 이면서 각 행에서 1의 개수가 일정한 중첩 부호에 대한 연구를 하였다. T가 주어진 경우 각 행에서 1의 개수가 k로 일정하게 갖는 $(w,r)-$중첩 부호의 행의 최대 개수를 $N(T:w,r,k)$라 하자. 이 논문에서는 $N(T:w,r,k)$의 하계를 구하였으며, 정확히 하계가 되는 구조를 밝혔다.

제 2 장 중첩 부호

이 장에서는 $(w,r)-$중첩 부호와 이진 선형 부호, $t-$디자인의 정의와 성질들을 소개하고, 이와 관련된 잘 알려진 결과들을 소개한다.
이 장의 대부분의 결과들은 참고문헌 [1],[5],[6],[7],[10],[12],[13]을 참고하였으며 증명은 가급적 생략하되 필요한 경우에만 간단하게 증명하도록 하겠다.

정의 2.1 집합 X를 n개의 원소를 갖는 집합이라 하자.
F는 X의 부분집합들의 모임으로 다음을 만족한다 :
임의의 $A_1, \cdots, A_w$, $B_1, \cdots, B_r \in F$에 대하여, $A_1 \cap \cdots \cap A_w \not\subseteq B_1 \cup \cdots \cup B_r$
이 때, F를 (w,r) 덮개-자유 족(cover-free family)이라 한다.

$w=r=1$인 경우, $(1,1)$ 덮개-자유 족은 유명한 Sperner 족(Sperner family)이 되며, (w,r) 덮개-자유 족의 투사 행렬(incidence matrix)을 $(w,r)-$중첩 부호라 한다.

정의 2.2 성분이 0과 1인 $N \times T$ 행렬 $C=[c_{ij}]$가 다음을 만족하면 행렬 C를 $(w,r)-$중첩 부호(superimposed codes)라고 한다.

집합 $[T]=\{1,2,\ldots,T\}$의 다음의 임의의 두 부분집합 I, J에 대하여,
$|I|=w$, $|J|=r, I \cap J=\varnothing$이면 $\begin{cases} c_{xp}=1, & \forall p \in I \\ c_{xq}=0, & \forall q \in J \end{cases}$ 을 만족하는 $x \in [N]$이 존재한다.

위의 정의에서 $[T]$의 원소를 행렬 C의 점(point)이라고 하며, 행렬 C의 점은 $p_1, p_2, \cdots$ 를 사용해서 표시하고 점들의 개수를 행렬 C의 기수(cardinality)라고 한다. 또한 $[N]$의 원소를 행렬 C의 블록(block)이라고 하며, 행렬 C의 블록을 $x_1, x_2, \cdots$ 를 사용해서 표시하고 블록의 개수를 행렬 C의 길이(length)라고 한다.

$N \times T$ 행렬 C를 $(w,r)-$중첩 부호라고 하자.
$p \in [T]$에 대하여 $S_p := \{x \in [T] \mid C_{xp}=1\}$라 할 때, S_p를 p번째 열의 특성집합(또는

고유집합)이라고 하며, $x \in [N]$에 대하여 $L_x := \{p \in [N] \mid C_{xp} = 1\}$라 할 때, L_x를 x 번째 행의 특성집합(또는 고유집합)이라고 한다.

예제 2.1 다음은 크기가 9×12인 $(1,2)-$중첩 부호이다.

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \\ i \end{array} \begin{array}{c} \begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \end{array} \\ \begin{pmatrix} 1&1&1&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&1&1&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0&1&1&1&0&0 \\ 0&1&0&0&1&0&0&1&0&0&1&0 \\ 0&1&0&0&0&1&0&0&1&0&0&1 \\ 0&0&1&0&1&0&0&0&0&1&0&1 \\ 0&0&1&0&0&0&1&0&1&0&1&0 \\ 0&0&0&1&0&1&0&0&0&1&1&0 \\ 0&0&0&1&0&0&1&1&0&0&0&1 \end{pmatrix} \end{array}$$

위의 행렬을 보았을 때, 3번째 열의 특성집합 $S_3 = \{a, f, g\}$이고, 3번째 행의 특성집합 $L_3 = \{1, 8, 9, 10\}$이다. 또한, $I = \{2\}$이고 $J = \{5, 6\}$이면 $c_{a2} = 1$이고 $c_{a5} = c_{a6} = 0$인 a행이 존재하고, $I = \{7\}$이고 $J = \{2, 3\}$인 경우에도 $c_{b7} = 1$이고 $c_{b2} = c_{b3} = 0$인 b행이 존재한다. 따라서 모든 경우를 생각해보았을 때 위의 행렬은 $(1,2)-$중첩 부호임을 알 수 있다.

예제 2.2 다음은 대표적인 $(1,1)-$중첩 부호의 예들이다

$$\begin{pmatrix} 1&1&1&0&0&0 \\ 1&0&0&1&1&0 \\ 0&1&0&1&0&1 \\ 0&0&1&0&1&1 \end{pmatrix}, \quad \begin{pmatrix} 1&1&1&1&0&0&0&0&0&0 \\ 1&0&0&0&1&1&1&0&0&0 \\ 0&1&0&0&1&0&0&1&1&0 \\ 0&0&1&0&0&1&0&1&0&1 \\ 0&0&0&1&0&0&1&0&1&1 \end{pmatrix}, \quad \begin{pmatrix} 1&1&1&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&1&1&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0&1&1&1&0&0 \\ 0&1&0&0&1&0&0&1&0&0&1&0 \\ 0&1&0&0&0&1&0&0&1&0&0&1 \\ 0&0&1&0&1&0&0&0&0&1&0&1 \\ 0&0&1&0&0&0&1&0&1&0&1&0 \\ 0&0&0&1&0&1&0&0&0&1&1&0 \\ 0&0&0&1&0&0&1&1&0&0&0&1 \end{pmatrix}, \quad \begin{pmatrix} 1&1&1&1&1&1&1&0&0&0&0&0&0&0 \\ 1&1&1&0&0&0&0&0&0&0&1&1&1&1 \\ 1&0&0&1&1&0&0&0&1&1&0&0&1&1 \\ 1&0&0&0&0&1&1&0&1&1&1&1&0&0 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 0&1&0&0&1&0&1&1&0&1&1&0&1&0 \\ 0&0&1&1&0&0&1&1&1&0&0&1&1&0 \\ 0&0&1&0&1&1&0&1&1&0&1&0&0&1 \end{pmatrix}$$

예제 2.1에서 본 바와 같이 첫 번째 행렬은 크기가 4×6인 $(1,1)-$중첩 부호이고, 두 번째 행렬은 크기가 5×10인 $(1,1)-$중첩 부호, 세 번째 행렬은 크기가 9×12

인 $(1,2)-$중첩 부호, 네 번째 행렬은 크기가 14×8인 $(2,2)-$중첩 부호임을 알 수 있다.

다음은 $(w,r)-$중첩 부호의 기본적 성질로서, 증명은 생략하도록 한다.

보조 정리 2.3 $(w,r)-$중첩 부호 $N\times T$ 행렬 $C=[c_{ij}]$에 대하여 다음을 만족한다.

(1) $N\times T$ 행렬 $\overline{C}=[d_{ij}]$에 대하여 $d_{ij}=1-c_{ij}$를 만족하면 $\overline{C}$는 $(r,w)-$중첩 부호이다.
(2) $N\times T$ 행렬 C의 임의의 열을 제거하여 얻은 행렬 C'은 $(w,r)-$중첩 부호이다.
(3) $N\times T$ 행렬 C의 임의의 행을 추가하여 얻은 행렬 C'은 $(w,r)-$중첩 부호이다.

보조 정리 2.3의 (1)로부터 $(w,r)-$중첩 부호를 생각할 때, 항상 $w\le r$이라 가정하도록 한다.

다음은 중첩 부호를 구성하는데 필요한 이진 선형 부호의 정의와 간단한 성질에 대해 알아보도록 하자.

두 자연수 $n,k\in\mathbb{N}$가 주어졌다고 하자. 길이 n의 k차원 이진 선형 부호는 유한체 F_2위의 n차원 벡터 공간 F_2^n속의 k차원 F_2-부분 벡터 공간 $C\subseteq F_2^n$이다. 이 때, 선형 부호 C의 원소는 부호어라고 한다.

임의의 $x=(a_1,\cdots,a_n)$, $y=(b_1,\cdots,b_n)\in F_2^n$에 대하여 $wt(x)$와 $d_H(x,y)$를 다음과 같이 정의하자.

$$wt(x):=|\{i\,|\,a_i\neq 0,\forall i=1,2,\cdots,n\}|$$
$$d_H(x,y):=|\{i\,|\,a_i\neq b_i,\forall i=1,2,\cdots,n\}|$$

$wt(x)$를 x의 해밍 무게, $d_H(x,y)$를 x와 y의 해밍 거리라 한다.
따라서 임의의 원소 x, y에 대하여, $d_H(x,y) = wt(x-y)$이다.

F_2^n의 선형부호 C에 대하여 $d := \min\{d_H(x,y) \mid \forall x \neq y \in C\}$라 정의하고, d를 C의 최소 해밍 거리라 한다. 또한, 최소 거리가 d이고 길이가 n인 k차원 이진 선형 부호를 $[n,k,d]-$선형 부호라고 표기한다.

예제 2.3 두 양의 정수 $1 \le k \le n$에 대하여,
$C := \{(a_1, a_2, \cdots, a_k, 0, 0, \cdots, 0) \mid a_i = 0, 1\} \subseteq F_2^n$는 자명하게 선형 부호이다. 또한 C는 F_2상의 k차원 부분 공간이고 최소 해밍 거리가 1이므로 $[n,k,1]-$선형 부호이다.

정의 2.4 임의의 $u = (u_1, \cdots, u_n) \in F_2^n$에 대하여, $\mathrm{supp}(u) := \{i \mid 1 \le i \le n,\ u_i \neq 0\}$라 하자. 이 때 $\mathrm{supp}(u)$를 벡터 u의 지지집합(support)라 한다.
따라서 $\mathrm{wt}(u) = |\mathrm{supp}(u)|$이다.

예제 2.4 $u = (1,0,1,0,0) \in F_2^5$의 경우 $\mathrm{supp}(u) = \{1,3\}$이고, $\mathrm{wt}(u) = 2$이다.

예제 2.5 다음은 자명한 $(w,r)-$중첩 부호의 예이다.
해밍 무게가 w이고 길이가 T인 모든 이진 벡터를 행으로 갖는 행렬은 크기가 $\binom{T}{w} \times T$인 $(w,r)-$중첩 부호이다.

이제 중첩 부호를 구성하는데 필요한 $t-$디자인에 대해 알아보자. $t-$디자인의 정의와 성질은 다음과 같다.

정의 2.5 $\varnothing \neq X$를 유한 집합이라 하고, $\mathscr{B}$를 X의 부분집합들의 모임이라 하자.
$(X, \mathscr{B})$가 다음을 만족하면 $(X, \mathscr{B})$를 $t-(v,k,\lambda)$디자인이라 한다.

(1) $|X| = v$

(2) 임의의 블록 $B \in \mathscr{B}$ 에 대하여 $|B| = k$이다.

(3) 임의의 서로 다른 t개의 점에 대하여, t개의 점을 동시에 포함하는 블록 $B \in \mathscr{B}$의 개수는 λ이다.

다음은 잘 알려진 $t-$디자인에서의 블록의 개수로 참고문헌 [13]을 참고하였으며 여기에서 증명을 다시 한 번 쓰도록 한다.

정리 2.6 $(X, \mathscr{B})$가 $t-(v,k,\lambda)$디자인이면 다음을 만족한다.

$$|\mathscr{B}| = \frac{\lambda \binom{v}{t}}{\binom{k}{t}}$$

증명 집합 $P = \{(A, B) \mid |A| = t, B \in \mathscr{B}, A \subseteq B\}$를 생각해 보자. 이 때, $|P|$를 두 가지 방법으로 계산하자.

(1) $|X| = v$ 이므로 집합 X 에서 서로 다른 t개의 점을 택하는 방법은 $\binom{v}{t}$가지가 있고 또 이와 같은 방법 하나하나에 대하여 t개의 점을 동시에 포함하는 블록의 개수는 λ이므로 $|P| = \binom{v}{t}\lambda$ 이다.

(2) $(X, \mathscr{B})$의 블록 전체의 개수는 $|\mathscr{B}|$이고 $B \in \mathscr{B}$ 에 대하여 B에서 서로 다른 t개의 점을 택하는 방법은 $\binom{k}{t}$가지가 있으므로 $|P| = |\mathscr{B}|\binom{k}{t}$이다.

(1), (2)에 의해 $\binom{v}{t}\lambda = |\mathscr{B}|\binom{k}{t}$이므로 $|\mathscr{B}| = \dfrac{\lambda \binom{v}{t}}{\binom{k}{t}}$ 이 성립한다.

예제 2.6 다음과 같은 결합구조 $(X, \mathscr{B})$는 $2-(4,2,1)$ 디자인이다.

$X = \{1, 2, 3, 4\}$, $\mathscr{B} = \{B_1, B_2, B_3, B_4, B_5, B_6\}$

$B_1 = \{1, 2\}$, $B_2 = \{2, 3\}$,

$B_3 = \{3, 4\}$, $B_4 = \{1, 4\}$,

$B_5 = \{1, 3\}, \quad B_6 = \{2, 4\}$

예제 2.7 다음과 같은 결합구조 $(X, \mathscr{B})$는 $2-(7, 4, 2)$ 디자인이다.

$X = \{0, 1, 2, 3, 4, 5, 6\}$, $\mathscr{B} = \{B_0, B_1, B_2, B_3, B_4, B_5, B_6\}$

$B_0 = \{0, 3, 5, 6\}, \quad B_1 = \{1, 4, 6, 0\},$

$B_2 = \{2, 5, 0, 1\}, \quad B_3 = \{3, 6, 1, 2\},$

$B_4 = \{4, 0, 2, 3\}, \quad B_5 = \{5, 1, 3, 4\},$

$B_6 = \{6, 2, 4, 5\}$

다음은 $t-$디자인으로부터 중첩 부호를 구성하는 결과로 잘 알려진 결과이나 여기에서 증명을 다시 하도록 한다. 자세한 것은 참고문헌 [13]을 참고하도록 한다.

정리 2.7 $(X, \mathscr{B})$가 $(t+1)-(v, k, \lambda)$ 디자인이라 하자. $(X, \mathscr{B})$의 투사 행렬은 다음을 만족하는 크기가 $N \times v$ 인 $(t, r)-$중첩 부호이다.

$$N = \frac{\lambda(v-t)\binom{v}{t}}{(k-t)\binom{k}{t}} \text{ 이고 } r < \frac{v-t}{k-t}$$

증명 집합 $P = \{(A, B) \mid |A| = t+1, B \in \mathscr{B}, A \subseteq B\}$를 생각해 보자.

정리 2.6의 증명과 같은 방법으로 $|P|$의 개수를 구하면 $N = \dfrac{\lambda(v-t)\binom{v}{t}}{(k-t)\binom{k}{t}}$을 얻을 수 있다.

다음으로 집합 $Q = \{(A, B) \mid |A| = t, B \in \mathscr{B}, A \subseteq B\}$를 생각해 보자. 이 때, $|Q|$를 두 가지 방법으로 계산하자. 여기에서 N_1을 서로 다른 t개의 점을 포함하는 블록의 개수라 하자.

(1) $|X| = v$ 이므로 집합 X에서 서로 다른 t개의 점을 택하는 방법은 $\binom{v}{t}$가지가 있고 또 이와 같은 방법 하나하나에 대하여 서로 다른 t개의 점을 동시에 포

함하는 블록의 개수는 N_1개 있으므로 $|Q| = \binom{v}{t} N_1$ 이다.

(2) $(X, \mathscr{B})$의 블록 전체의 개수는 N이고 $B \in \mathscr{B}$ 에 대하여 B에서 서로 다른 t개의 점을 택하는 방법은 $\binom{k}{t}$가지가 있으므로 $|Q| = N\binom{k}{t}$이다.

(1), (2)에 의해 $\binom{v}{t} N_1 = N\binom{k}{t}$이므로 $N_1 = \dfrac{\lambda(v-t)}{k-t}$ 이 성립한다.

이 때, 임의의 한 점을 지나는 블록의 개수를 r이라 하자. 그러면 임의의 서로 다른 $t+1$개의 점을 동시에 포함하는 블록의 개수는 λ이므로 $r\lambda < \dfrac{\lambda(v-t)}{k-t}$ 이 성립한다. 따라서 $r < \dfrac{v-t}{k-t}$이 성립한다.

예제 2.8 다음은 예제 2.6를 이용하여 $2-(4,2,1)$ 디자인으로부터 중첩 부호를 구성한 것으로 정리 2.7에 의해 크기가 6×4이고 $r < 3$인 $(1,r)-$중첩 부호임을 알 수 있다.

$$\begin{array}{c} \\ B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

예제 2.9 다음은 예제 2.7을 이용하여 $2-(7,4,2)$ 디자인으로부터 중첩 부호를 구성한 것으로 정리 2.7에 의해 크기가 7×7이고 $r < 2$인 $(1,r)-$중첩 부호임을 알 수 있다.

$$\begin{array}{c} \\ B_0 \\ B_1 \\ B_2 \\ B_3 \\ B_4 \\ B_5 \\ B_6 \end{array} \begin{array}{c} \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

정의 2.8 $(X,\mathscr{B})$를 $t-(v,k,\lambda)$디자인이라 하자.

(1) $t=2,\ k=3,\ \lambda=1$인 $2-(v,3,1)$ 디자인을 슈타이너 3중 시스템(Steiner triple system)라고 한다.
(2) $t=3,\ k=4,\ \lambda=1$인 $3-(v,4,1)$ 디자인을 슈타이너 4중 시스템(Steiner quadruple system)라고 한다.

다음은 슈타이너 3중 시스템과 슈타이너 4중 시스템의 존재성에 대해 잘 알려진 결과로 참고문헌 [8],[9]를 참고하였으며 증명은 생략하도록 한다.

정리 2.9 $t-(v,k,\lambda)$디자인 $(X,\mathscr{B})$에 대하여 다음 두 조건은 동치이다.

(1) $2-(v,3,1)$ 디자인이 존재한다.
(2) $v\equiv 1$ 또는 $3\ (\mathrm{mod}\ 6)$이다.

정리 2.10 $t-(v,k,\lambda)$디자인 $(X,\mathscr{B})$에 대하여 다음 두 조건은 동치이다.

(1) $3-(v,4,1)$ 디자인이 존재한다.
(2) $v\equiv 2$ 또는 $4\ (\mathrm{mod}\ 6)$이다.

다음 정리는 앞에서 본 정리 2.7, 정리 2.9, 정리 2.10에 의해 성립함을 쉽게 알 수 있다.

따름 정리 2.11 슈타이너 3중 시스템과 슈타이너 4중 시스템에 대하여 다음이 성립한다.

(1) $v\equiv 1$ 또는 $3\ (\mathrm{mod}\ 6)$이면 크기가 $\dfrac{v(v-1)}{6}\times v$이고 $r<\dfrac{v-1}{2}$인 $(1,r)-$중첩 부호가 존재한다.
(2) $v\equiv 2$ 또는 $4\ (\mathrm{mod}\ 6)$이면 크기가 $\dfrac{v(v-1)(v-2)}{24}\times v$이고 $r<\dfrac{v-2}{2}$인

$(2,r)-$중첩 부호가 존재한다.

예제 2.10 $v=7$이면 정리 2.9에 의해 $2-(v,3,1)$ 디자인이 존재한다. 따라서 크기가 7×7이고 $r<3$인 $(1,r)-$중첩 부호가 된다. 중첩 부호를 자세히 적으면 다음과 같다.

$$\begin{pmatrix} 0&1&1&0&1&0&0\\ 0&0&1&1&0&1&0\\ 0&0&0&1&1&0&1\\ 1&0&0&0&1&1&0\\ 1&0&0&0&0&1&1\\ 1&0&1&0&0&0&1\\ 1&1&0&1&0&0&0 \end{pmatrix}$$

예제 2.11 $v=8$이면 정리 2.10에 의해 $3-(v,4,1)$ 디자인이 존재한다. 따라서 크기가 14×8이고 $r<3$인 $(2,r)-$중첩 부호가 된다. 중첩 부호를 자세히 적으면 다음과 같다.

$$\begin{pmatrix} 1&0&0&1&0&1&1&0\\ 1&1&0&0&1&0&1&0\\ 1&1&1&0&0&1&0&0\\ 0&1&1&1&0&0&1&0\\ 1&0&1&1&1&0&0&0\\ 0&1&0&1&1&1&0&0\\ 0&0&1&0&1&1&1&0\\ 0&1&1&0&1&0&0&1\\ 0&0&1&1&0&1&0&1\\ 0&0&0&1&1&0&1&1\\ 1&0&0&0&1&1&0&1\\ 0&1&0&0&0&1&1&1\\ 1&0&1&0&0&0&1&1\\ 1&1&0&1&0&0&0&1 \end{pmatrix}$$

제 3 장 행의 무게가 일정한 이진 $(w,r)-$중첩 부호

이 장에서는 앞에서 다루었던 $(w,r)-$중첩 부호와 이진 선형 부호, $t-$디자인의 정의와 성질을 바탕으로 행의 무게가 일정한 이진 $(w,r)-$중첩 부호에 대해 살펴보도록 하겠다.

$(w,r)-$중첩 부호에서 T,w,r이 주어졌을 때 $(w,r)-$중첩 부호 $N\times T$ 행렬 $C=[c_{ij}]$인 N의 최솟값을 $N(T:w,r)$이라 하고, $N(T:w,r)\times T$의 중첩 부호를 최적 중첩 부호(또는 최상 중첩 부호)라고 한다. 이 때, 이를 만족하는 $N(T:w,r)$의 상계와 하계를 찾는 것이 중요한 문제이다. 이에 대한 쌍대 문제로 N,w,r이 주어졌을 때 (w,r)-중첩 부호 $N\times T$ 행렬 $C=[c_{ij}]$인 T의 최댓값을 $T(N:w,r)$이라 하고, $N\times T(N:w,r)$의 중첩 부호를 최적 중첩 부호(또는 최상 중첩 부호)라고 하며 이를 만족하는 $T(N:w,r)$의 상계와 하계를 찾는 것 또한 중요한 문제이다.

다음 정리는 $N(T:w,r)$에 대해 잘 알려진 결과로 [8]을 참고 하였으며 증명은 생략하도록 한다.

정리 3.1 $N(T:w,r)$에 대하여 다음을 만족한다.

(1) $T\le w+r+\dfrac{r}{w}$ 이면 $N(T:w,r)=\binom{T}{w}$

(2) $N(6:2,2)=\cdots=N(8:2,2)=14$

(3) $N(9:2,2)=18$

(4) $N(10:2,3)=30$

(5) $N(11:3,3)=66$

위의 문제를 해결하는 것은 일반적으로 어려운 문제이므로 이 장에서는 T,w,r이 주어진 경우 각 행의 해밍 무게가 k로 일정한 $(w,r)-$중첩 부호 $N(T:w,r)$의 상계와 하계를 구해보도록 하자. 여기에서 $k\ge w$이다.

정의 3.2 (w,r)-중첩 부호 $N\times T$ 행렬 $C=[c_{ij}]$에 대하여 모든 행의 무게를 k라 하자. T,w,r,k가 주어졌을 때, N의 최솟값을 $N(T:w,r,k)$라 한다.

예제 3.1 다음은 크기가 9×12인 $(1,2)$-중첩 부호이다.

$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \\ i \end{array} \begin{array}{c} \begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \end{array} \\ \begin{pmatrix} 1&1&1&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&1&1&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0&1&1&1&0&0 \\ 0&1&0&0&1&0&0&1&0&0&1&0 \\ 0&1&0&0&0&1&0&0&1&0&0&1 \\ 0&0&1&0&1&0&0&0&0&1&0&1 \\ 0&0&1&0&0&0&1&0&1&0&1&0 \\ 0&0&0&1&0&1&0&0&0&1&1&0 \\ 0&0&0&1&0&0&1&1&0&0&0&1 \end{pmatrix} \end{array}$$

위의 행렬은 모든 행의 무게가 4로 일정하므로 $N(12:1,2,4)\le 12$이다.

다음 정리는 잘 알려진 결과로 참고문헌 [9]에 잘 나와 있으며 여기에서 다시 한 번 증명하도록 한다.

정리 3.3 $(w,r)-$중첩 부호 $N\times T$ 행렬 $C=[c_{ij}]$에 대하여 임의의 w개의 점을 $p_1,\cdots,p_w$라 하였을 때, $x\in S_{p_1}\cap\cdots\cap S_{p_w}$을 만족하는 모든 x에 대하여 $|L_x|>w$ 이면 $|S_{p_1}\cap\cdots\cap S_{p_w}|\ge r+1$이다.

증명 $|S_{p_1}\cap\cdots\cap S_{p_w}|\le r$라 가정하고, $S_{p_1}\cap\cdots\cap S_{p_w}=\{x_1,\cdots,x_l\}$, $l\le r$로 두자.
임의의 $i=1,2,\cdots,r$에 대하여 $|L_{x_i}|>w$이므로 다음의 행렬이 존재한다.

$$
\begin{array}{c}
\\ x_1 \\ x_2 \\ \cdot \\ \cdot \\ \cdot \\ x_l \\ \cdot \\ \cdot \\ \cdot
\end{array}
\begin{array}{c}
p_1\ p_2 \cdots p_w\ q_1\ q_2 \cdots q_l \\
\begin{pmatrix}
1&1&1&1&1&1&1&\cdot&\cdot&\cdot&\cdot&\cdot \\
1&1&1&1&1&1&\cdot&1&\cdot&\cdot&\cdot&\cdot \\
1&1&1&1&1&1&\cdot&\cdot&1&\cdot&\cdot&\cdot \\
1&1&1&1&1&1&\cdot&\cdot&\cdot&1&\cdot&\cdot \\
1&1&1&1&1&1&\cdot&\cdot&\cdot&\cdot&1&\cdot \\
1&1&1&1&1&1&\cdot&\cdot&\cdot&\cdot&\cdot&1 \\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot \\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot \\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot
\end{pmatrix}
\end{array}
$$

C가 $(w,r)-$중첩 부호이므로 $(w,l)-$중첩 부호임이 자명하다.
따라서 $p_1, p_2, \cdots, p_w$와 $q_1, q_2, \cdots, q_l$에 대하여 $C_{xp_i}=1(i=1,\cdots,w)$을 만족하는 C의 행 $x \in S_{p_1} \cap \cdots \cap S_{p_w}$가 존재한다. 그러나 $C_{xp_1}= \cdots = C_{xp_w}=1$ 이고 $C_{xq_1}= \cdots = C_{xq_l}=0$을 만족하는 C의 x 행이 존재하지 않으므로 이는 모순이다.

다음은 자명한 결과로 증명은 생략하도록 한다.

정리 3.4 T, w, r, k가 주어졌을 때, N의 최솟값 $N(T: w, r, k)$에 대하여 다음을 만족한다.

$$N(T: w, r, k) \le \binom{T}{k}$$

2장에서 살펴본 바에 의하면 $t-(v,k,\lambda)$디자인으로부터 중첩 부호를 구성할 수 있으며 이 중첩 부호는 모두 행의 개수가 일정한 중첩 부호이다. 정리 2.7과 슈타이너 3중 시스템, 슈타이너 4중 시스템에 의해 다음이 성립한다.

보조 정리 3.5 $(X,\mathscr{B})$를 $(t+1)-(v,k,\lambda)$ 디자인이라 하자.

$$N(v: t, r, k) \le \frac{\lambda(v-t)\binom{v}{t}}{(k-t)\binom{k}{t}}, \quad r < \frac{v-t}{k-t}$$

보조 정리 3.6 $(X,\mathscr{B})$를 $t-(v,k,\lambda)$디자인이라 하자.

(1) $v \equiv 1$ 또는 $3 \pmod 6$이면, $N(v:1,r,3) \le \dfrac{v(v-1)}{6}$, $r < \dfrac{v-1}{2}$ 이다.

(2) $v \equiv 2$ 또는 $4 \pmod 6$이면, $N(v:2,r,4) \le \dfrac{v(v-1)(v-2)}{24}$, $r < \dfrac{v-2}{2}$ 이다.

정리 3.7 $N(T:w,r,k)$에 대하여 $k > w$이면 다음을 만족한다.

$$\frac{\binom{T}{w}(r+1)}{\binom{k}{w}} \le N(T:w,r,k)$$

증명 $N \times T$ 행렬 C를 (w,r)-중첩 부호라 하고 행렬 C의 모든 행의 무게를 k라 하자. 다음의 집합 $\{(A,B) \mid A \subseteq B,\ |A| = w,\ B = L_x,\ x \in [N]\}$을 편의 상 S라고 표기하도록 하며 $|S|$를 두 가지 방법으로 계산하자.

(1) S에 속하는 (A,B)에서 먼저 A의 개수를 구하고 그 다음 B의 개수를 구하자. $(A,B) \in S$인 A는 $|A| = w$이므로 $\binom{T}{w}$개만큼 존재하고 B는 $(r+1)$개만큼 존재한다. 따라서 정리 3.3에 의해 $\binom{T}{w}(r+1) \le |S|$이 성립한다.

(2) S에 속하는 (A,B)에서 먼저 B의 개수를 구하고 그 다음 A의 개수를 구하자. $(A,B) \in S$인 B는 $N(T:w,r,k)$개만큼 존재하고 A는 $\binom{k}{w}$개만큼 존재한다. 따라서 $|S| \ge N(T:w,r,k)\binom{k}{w}$이 성립한다.

(1), (2)에 의해 $\dfrac{\binom{T}{w}(r+1)}{\binom{k}{w}} \le N(T:w,r,k)$이 성립한다.

예제 3.2 다음은 크기가 9×12인 $(1,2)$-중첩 부호이다.

$$\begin{pmatrix} 1&1&1&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&1&1&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0&1&1&1&0&0 \\ 0&1&0&0&1&0&0&1&0&0&1&0 \\ 0&1&0&0&0&1&0&0&1&0&0&1 \\ 0&0&1&0&1&0&0&0&0&1&0&1 \\ 0&0&1&0&0&0&1&0&1&0&1&0 \\ 0&0&0&1&0&1&0&0&0&1&1&0 \\ 0&0&0&1&0&0&1&1&0&0&0&1 \end{pmatrix}$$

보조 정리 3.5에 의해 $N(12:1,2,4) \le 9$ 이고, 정리 3.7에 의해 $9 \le N(12:1,2,4)$ 이므로 $N(12:1,2,4) = 9$이다. 따라서 이는 최적화된 중첩 부호이다.

예제 3.3 다음은 예제 2.10으로부터 구성한 크기가 7×7인 $(1,2)-$중첩 부호이다.

$$\begin{pmatrix} 0&1&1&0&1&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&1&1&0&1 \\ 1&0&0&0&1&1&0 \\ 1&0&0&0&0&1&1 \\ 1&0&1&0&0&0&1 \\ 1&1&0&1&0&0&0 \end{pmatrix}$$

보조 정리 3.5에 의해 $N(7:1,2,3) \le 7$ 이고, 정리 3.7에 의해 $7 \le N(7:1,2,3)$ 이므로 $N(7:1,2,3) = 7$이다. 따라서 이는 최적화된 중첩 부호이다.

예제 3.4 다음은 예제 2.11로부터 구성한 크기가 14×8인 $(2,2)-$중첩 부호이다.

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

보조 정리 3.5에 의해 $N(8:2,2,4) \le 14$ 이고, 정리 3.7에 의해 $14 \le N(8:2,2,4)$ 이므로 $N(8:2,2,4) = 14$이다. 따라서 이는 최적화된 중첩 부호이다.

참고문헌

[1] A. D'yachkov, A. Macula, and V. Rykov, New superimposed code, IEEE Trans. Inform. Theory 46 (2000).

[2] A. D'yachkov, A. Macula, D. Torney and P. Vilenkin, Families of finite sets in which no intersection of l sets is covered by the union of others, J. Combin. Theory, Ser. A 99 (2002) 195-218.

[3] P. Erdős, P. Frankl, and Z. Furedi, Families of finite sets in which no set is covered by the union of two others, J. Combin. Theory Ser. A 33 (1982) 158-166.

[4] P. Erdős, P. Frankl, and Z. Furedi, Families of finite sets in which no set is covered by the union of others, Israel J. math. 51 (1985) 75-89.

[5] P.L. Erdos, P. Frankl, and G.O.H. Katona, Two-part and k-Sperner families-new proofs using permutations, SIAM J. Discrete Math. 19 (2005) 489-500.

[6] S. Hong, S. Kapralov, H.K. Kim and D.Y. Oh, Uniqueness of some superimposed codes, Probl. Inform. Transm. 43 (2007) 113-123.

[7] W.H. Kautz and R.C. Singleton, Nonrandom binary superimposed codes, IEEE. Trans. Inform. Theory IT-10 (1964) 363-377.

[8] H.K. Kim and V. Lebedev, On optimal superimposed codes, J. Combin. Designs 12 (2004) 79-91.

[9] H.K. Kim, V. Lebedev, and D.Y. Oh, Some new results on superimposed codes, J. Combin. Designs 13 (2005) 276-285.

[10] C.J. Mitchell and F.C. Piper, Key storage in secure networks, Discr. Appl. Math. 21 (1988) 215-228.

[11] D.Y. Oh, A classification of the structures of some Sperner families and superimposed codes, Discr. Math. 306 (2006) 1722-1731.

[12] E. Sperner, Ein Satz uber Untermegen einer endilchen Menge, Math. Z. 27 (1928) 544-548.

[13] 박승안, 이산수학 제3판, 경문사 (2012).