CHARACTERIZATION OF MIN-HYPERS IN A FINITE PROJECTIVE GEOMETRY AND ITS APPLICATIONS TO ERROR-CORRECTING CODES

Noboru Hamada
Osaka Women's University

1. Introduction

Let V(n;q) be an n-dimensional vector space consisting of row vectors over a Galois field GF(q) of order q where n is a positive integer and q is a prime power. A k-dimensional subspace C of V(n;q) is said to be an (n,k,d;q)-code (or a q-ary linear code with code length n, dimension k, and minimum distance d) if the minimum distance of the code C is equal to d, that is, $\min\{ d(\underline{\alpha},\underline{\beta}) \mid \underline{\alpha}, \underline{\beta} \in C, \underline{\alpha} \neq \underline{\beta} \} = d$ where $d(\underline{\alpha},\underline{\beta})$ denotes the Hamming distance between two vectors $\underline{\alpha}$ and $\underline{\beta}$ in V(n;q).

It is well known (cf. MacWilliams and Sloane (1977) in detail) that if the elements of an (n,k,d;q)-code C are used as codewords over a q-ary symmetric channel, with q inputs, q outputs, a probability 1-p that no error occurs, and a probability p (< 0.5) that an error does occur, each of the q-1 possible errors being equally likely, the code C is capable of correcting all patterns of [(d-1)/2] or fewer errors by using a maximum likelihood decoding where [x] denotes the greatest integer not exceeding x. Hence in order to obtain a q-ary linear code which is capable of correcting most errors for given integers n, k and q, it is sufficient to obtain an (n,k,d;q)-code C (called an optimal linear

code) whose minimum distance d is maximum among (n,k,*;q)-codes for given integers n, k and q. It is also known that in order to obtain an optimal linear code, it is sufficient to solve the following problem for any prime power q and any integers k and d such that $k \geq 3$ and $d \geq 1$.

Problem A. Find an (n,k,d;q)-code C whose code length n is minimum among (*,k,d;q)-codes for given integers k, d and q.

Let q be any prime power and let k and d be any integers such that $k \ge 3$ and $d \ge 1$. Then d can be expressed uniquely as follows.

(1.1)
$$d = \omega q^{k-1} - \sum_{\alpha=0}^{k-2} \varepsilon_{\alpha} q^{\alpha}$$

using some integers ω and ε_{α} 's such that $\omega \geq 1$ and $0 \leq \varepsilon_{\alpha} \leq q-1$. Using (1.1), a lower bound for the code length n of Problem A, due to Griesmer (1960) for the case q=2 and to Solomon and Stiffler (1965) for the case $q \geq 3$, can be expressed as follows.

Theorem 1.1. If there exists an (n,k,d;q)-code, then

(1.2)
$$n \geq \sum_{k=0}^{k-1} \left(\frac{d}{q^k} \right) = \omega v_k - \sum_{\alpha=0}^{k-2} \varepsilon_{\alpha} v_{\alpha+1}$$

where ω and ϵ_{α} 's denote integers determined by (1.1) from three integers k, d and q and $v_{\mu}=(q^{\mu}-1)/(q-1)$ for any integer $\mu\geq 0$ and $x \in \mathbb{R}$ denotes the smallest integer $x \in \mathbb{R}$.

Theorem 1.1 shows that in order to obtain a solution of Problem A for given integers k, d and q, it is sufficient to obtain an (n,k,d;q)-code meeting the

Griesmer bound (1.2) in the case where there exists such a code for given integers k, d and q. Hence we shall consider the following

Problem B. (1) Find a necessary and sufficient condition for integers k, d and q that there exists an (n,k,d;q)-code meeting the Griesmer bound (1.2).

(2) Characterize all (n,k,d;q)-codes meeting the Griesmer bound (1.2) in the case where there exist such codes.

Remark 1.1. Since in the special case $(\epsilon_1, \epsilon_2, \cdots, \epsilon_{k-2}) = (0, 0, \cdots, 0)$, i.e., $d = \omega q^{k-1} - \epsilon_0$, Problem B has been already solved completely for any prime power q and any integers k, ω and ϵ_0 such that $k \geq 3$, $\omega \geq 1$ and $0 \leq \epsilon_0 \leq q-1$ (cf. Corollary 2.2 in Hamada (1985) for example), it is sufficient to solve Problem B for the case $(\epsilon_1, \epsilon_2, \cdots, \epsilon_{k-2}) \neq (0, 0, \cdots, 0)$.

Remark 1.2. In the case $(\epsilon_1, \epsilon_2, \dots, \epsilon_{k-2}) \neq (0, 0, \dots, 0)$, d can be also expressed as follows.

(1.1')
$$d = \omega q^{k-1} - (\varepsilon + \sum_{i=1}^{h} q^{i})$$

using some integers ω , ε and μ_i 's such that $\omega \ge 1$, $0 \le \varepsilon \le q-1$ and

(1.3)
$$(1,1,\dots,1,2,2,\dots,2,\dots,k-2) \equiv (\mu_1,\mu_2,\dots,\mu_h)$$

where $h = \sum_{\alpha = 1}^{k-2} \varepsilon_{\alpha}$. For example, (1.3) means that $\mu_1 = 1$, $\mu_2 = 1$ and $\mu_3 = 3$ in the case k = 5, $q \ge 3$ and $(\varepsilon_1, \varepsilon_2, \varepsilon_3) = (2,0,1)$. In this case, the Griesmer bound (1.2) can be expressed as follows.

(1.2')
$$n \geq \omega v_{k} - (\varepsilon + \sum_{i=1}^{h} v_{\mu_{i}+1})$$

where ω , ϵ , h and μ_i 's denote integers determined by (1.1').

It is well known (cf. Baumert and McEliece (1973) and Hamada and Tamari (1980)) that for any integers k and q, there exists some integer d_0 (depending on k and q) such that there exists an (n,k,d;q)-code meeting the Griesmer bound for any integer $d \geq d_0$. From the actual point of view, it is desirable to obtain a solution of Problem A (or B) for comparatively small integers k, d and q. Hence we shall confine ourself to the case $\omega = 1$ and $(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{k-2}) \neq (0,0,\cdots,0)$ in this paper. Problem B has been solved completely by Helleseth (1981) for the case $\omega = 1$ and q = 2 and by Hamada (1985) for the case $\omega = 1$, $q \geq 3$ and $\varepsilon_0 = 0$ or 1 ($\alpha = 0,1,\cdots,k-2$).

The purpose of this paper is to generalize those results using characterization of min-hypers in a finite projective geometry. In Section 2, a connection between a min-hyper and an (n,k,d;q)-code meeting the Griesmer bound (1.2) will be described and it will be shown that in order to solve Problem B for the case $\omega=1$ and $(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{k-2})\neq (0,0,\cdots,0)$, it is sufficient to solve Problem C, i.e., it is sufficient to find a necessary and sufficient condition for integers ε_0 , ε_1 , \cdots , ε_{t-1} , t and q that there exists an $\{f,m;t,q\}$ -min-hyper and to characterize all $\{f,m;t,q\}$ -min-hypers if there exist such min-hypers where t = k-1, $f=\sum_{\alpha=0}^{t-1}\varepsilon_{\alpha}v_{\alpha+1}$ and $f=\sum_{\alpha=1}^{t-1}\varepsilon_{\alpha}v_{\alpha}$. In Section 3, several constructive methods of min-hypers and a sufficient condition for the existence of a min-hyper will be given. In Section 4, we shall characterize certain min-hypers and using these characterizations, we shall obtain a necessary condition for the existence of some min-hyper. In detail, refer Hamada (1986a, 1986b and 1986c).

2. A connection between a min-hyper and an (n,k,d;q)-code meeting the bound (1.2)

In order to solve Problem B for the case $\omega=1$, we shall use a min·hyper which has been introduced by Hamada and Tamari (1978).

Definition 2.1. Let F be a set of f points in a finite projective geometry PG(t,q) of t dimensions where $t \ge 2$ and $f \ge 1$. If (a) $|F \cap H| \ge m$ for any hyperplane (i.e., (t-1)-flat) H in PG(t,q) and (b) $|F \cap H| = m$ for some hyperplane H in PG(t,q), then F is said to be an $\{f,m;t,q\}$ -min·hyper where $m \ge 0$ and |A| denotes the number of elements in the set A.

Example 2.1. (1) Let F be a μ -flat in PG(t,q) where $0 \le \mu < t$. Then F is a $\{v_{\mu+1}, v_{\mu}; t,q\}$ -min·hyper where $v_{\mu} = (q^{\mu}-1)/(q-1)$ for any integer $\mu \ge 0$. Because $|F| = v_{\mu+1}$, $|F \cap H| = v_{\mu}$ or $v_{\mu+1}$ for any hyperplane H in PG(t,q) and $|F \cap H| = v_{\mu}$ for some hyperplane H in PG(t,q).

(2) Let F be a set of ϵ_0 0-flats, ϵ_1 1-flats, \cdots , ϵ_{t-1} (t-1)-flats in PG(t,q) which are mutually disjoint where $0 \le \epsilon_{\alpha} \le q$ -1 for $\alpha = 0,1,\cdots,t-1$. Then F is a $\{\sum_{\alpha=0}^{t-1} \epsilon_{\alpha}v_{\alpha+1}, \sum_{\alpha=1}^{t} \epsilon_{\alpha}v_{\alpha};t,q\}$ -min·hyper.

Definition 2.2. Let $\mathcal{B}_{C}(\varepsilon_{1},\varepsilon_{2},\cdots,\varepsilon_{k-2};k-1,q)$ denote a set of all (n,k,d;q)-1 codes meeting the Griesmer bound (1.2) in the case $\omega=1$ and $d=q^{k-1}-\sum\limits_{\alpha=0}^{k-2}\varepsilon_{\alpha}q^{\alpha}$. Let $\mathcal{B}_{F}(\varepsilon_{0},\varepsilon_{1},\cdots,\varepsilon_{k-2};k-1,q)$ denote a set of all $\{\sum\limits_{\alpha=0}^{k-2}\varepsilon_{\alpha}v_{\alpha+1},\sum\limits_{\alpha=1}^{k-2}\varepsilon_{\alpha}v_{\alpha};k-1,q\}-1$ min hypers.

Definition 2.3. Two (n,k,d;q)-codes C_1 and C_2 are said to be congruent if there exists a $k \times n$ generator matrix G_2 of the code C_2 such that $G_2 = G_1^{PD}$ (or $G_2 = G_1^{DP}$) for some permutation matrix P and some nonsingular diagonal matrix D whose entries are elements of GF(q) where G_1 is a $k \times n$ generator matrix of C_1 .

The following theorem is due to the author (cf. Theorems I, 2.3 and 2.4 in Hamada (1985)).

Theorem 2.1. There is a one-to-one correspondence between a set $\mathcal{B}_{C}(\varepsilon_{0}, \varepsilon_{1}, \cdots, \varepsilon_{k-2}; k-1, q)$ and a set $\mathcal{B}_{F}(\varepsilon_{0}, \varepsilon_{1}, \cdots, \varepsilon_{k-2}; k-1, q)$ if we introduce an equivalence relation between two (n, k, d; q)-codes as Definition 2.3 where $(\varepsilon_{0}, \varepsilon_{1}, \cdots, \varepsilon_{k-2}) \neq (0, 0, \cdots, 0)$.

(2) Let ε_{α} 's, k and q be any integers such that $\mathcal{B}_{F}(\varepsilon_{0},\varepsilon_{1},\cdots,\varepsilon_{k-2};k-1,q)$ $\neq \emptyset$ and let $F \equiv \{ (\underline{b}_{1}), (\underline{b}_{2}), \cdots, (\underline{b}_{f}) \}$ be any $\{f,m;k-1,q\}$ -min-hyper where k-2 $f = \sum_{\alpha = 0}^{K-2} \varepsilon_{\alpha} v_{\alpha+1}, m = \sum_{\alpha = 1}^{K-2} \varepsilon_{\alpha} v_{\alpha}, \underline{b}_{i}$'s being distinct nonzero vectors in a k-dimensional vector space over GF(q) consisting of column vectors and (\underline{b}) denotes a point in PG(k-1,q), i.e., $(\underline{v}_{1}) = (\underline{v}_{2})$ if and only if there exists some nonzero element σ in GF(q) such that $\underline{v}_{2} = \sigma \underline{v}_{1}$. Let $G = [\underline{b}_{1} \underline{b}_{2} \cdots \underline{b}_{f}]$. Then we can obtain an (n,k,d;q)-code meeting the Griesmer bound (1.2) for the case $\omega = 1$ and $d = q^{k-1} - \sum_{\alpha = 0}^{K-2} \varepsilon_{\alpha} q^{\alpha}$ from the matrix G which is a K K K generator matrix of a K-ary anticode with code length K, dimension K K, and maximum distance K-m (cf. Ch. 17-K6 in MacWilliams and Sloane (1977) in detail).

Definition 2.4. Let E(t,q) denote a set of all ordered sets $(\epsilon_0,\epsilon_1,\cdots,\epsilon_{t-1})$ of integers ϵ_α 's such that $(\epsilon_1,\epsilon_2,\cdots,\epsilon_{t-1}) \neq (0,0,\cdots,0)$ and $0 \leq \epsilon_\alpha \leq q-1$ for $\alpha=0,1,\cdots,t-1$. Let U(t,q) denote a set of all ordered sets $(\epsilon,\mu_1,\mu_2,\cdots,\mu_h)$ of integers ϵ , ϵ , ϵ , and ϵ such that ϵ is such that ϵ in ϵ integers ϵ , ϵ , ϵ and ϵ integers ϵ in ϵ integers ϵ , ϵ in ϵ in ϵ integers ϵ in ϵ in

number of integers i in { 1,2,...,h } such that μ_i = ℓ for the given integer ℓ .

Theorem 2.1 and Remark 1.2 show that in order to solve Problem B for the case $\omega=1$ and $(\epsilon_1,\epsilon_2,\cdots,\epsilon_{k-2})\neq (0,0,\cdots,0)$, it is sufficient to solve the

Problem C. Let t and q be a given integer \geq 2 and a given prime power.

- (1) Find a necessary and sufficient condition for an ordered set $(\epsilon_0, \epsilon_1, \cdots, \epsilon_{t-1})$ in E(t,q) ((or an ordered set $(\epsilon, \mu_1, \mu_2, \cdots, \mu_h)$ in U(t,q))) that there exists a $\{\sum_{\alpha = 0}^{\infty} \epsilon_{\alpha} v_{\alpha+1}, \sum_{\alpha = 1}^{\infty} \epsilon_{\alpha} v_{\alpha}; t,q\}$ -min·hyer ((or a $\{\sum_{i=1}^{\infty} v_{\mu_i} + 1\}$ + ϵ , i=1 i=1
- (2) Characterize all { $\Sigma \in_{\alpha} v_{\alpha+1}$, $\Sigma \in_{\alpha} v_{\alpha}$; t,q}-min·hyper\$((or all h h $\alpha=0$ $\alpha=1$) in the case where there exist such i=1 μ_{i} +1 μ_{i} +1 μ_{i} +2 μ_{i} +1 μ_{i} +2 μ_{i} +3 μ_{i} +4 μ_{i} +4 μ_{i} +5 μ_{i} +5 μ_{i} +6 μ_{i} +6 μ_{i} +7 μ_{i} +9 μ_{i} +9 μ_{i} +1 μ_{i} +9 μ_{i} +1 μ_{i} +1 μ_{i} +1 μ_{i} +1 μ_{i} +1 μ_{i} +2 μ_{i} +3 μ_{i} +4 μ_{i} +4 μ_{i} +4 μ_{i} +5 μ_{i} +6 μ_{i} +6 μ_{i} +6 μ_{i} +7 μ_{i} +7 μ_{i} +8 μ_{i} +9 μ_{i}

3. Construction of several min·hypers and a sufficient condition

Let $\Lambda(t,q)$ be a set of all ordered sets $(\lambda_1,\lambda_2,\cdots,\lambda_\eta)$ of integers η and λ_i 's such that $1 \leq \eta \leq (t+1)(q-1)$, $0 \leq \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_\eta \leq t-1$, $0 \leq m_0 \leq 2(q-1)$ and $0 \leq m_\alpha \leq q-1$ for $\alpha=1,2,\cdots,t-1$ where m_α denotes the number of integers i in $\{1,2,\cdots,\eta\}$ such that $\lambda_i=\alpha$ for the given integer α . Let $\widetilde{U}(t,q)$ be a set of all ordered sets $(\sigma,\mu_1,\mu_2,\cdots,\mu_h)$ such that $0 \leq \sigma \leq q$ and $(0,\mu_1,\mu_2,\cdots,\mu_h)$ ϵ U(t,q) where U(t,q) denotes a set defined in Definition 2.4.

Definition 3.1. For each ordered set $(\lambda_1, \lambda_2, \cdots, \lambda_\eta)$ in $\Lambda(t,q)$, let us denote by $\mathcal{F}(\lambda_1, \lambda_2, \cdots, \lambda_\eta; t, q)$, a family of all sets $\bigcup_{i=1}^{\eta} V_i$ of a λ_1 -flat V_1 , a λ_2 -flat V_2 , \cdots , a λ_η -flat V_η in PG(t,q) which are mutually disjoint. As occasion demands, we shall denote $\mathcal{F}(\lambda_1, \lambda_2, \cdots, \lambda_\eta; t, q)$ by $\mathcal{F}_U(\sigma, \mu_1, \mu_2, \cdots, \mu_h; t, q)$

where $\sigma=m_0$, $h=\eta-m_0$, $\mu_i=\lambda_{m_0+i}$ (i = 1,2,...,h) and m_0 denotes the number of integers i in { 1,2,..., η } such that $\lambda_i=0$.

Definition 3.2. Let V be a θ -flat in PG(t,q) where $2 \le \theta \le t$. A set S of m points in V is said to be an <u>m-arc in V</u> if $|S \cap H| \le \theta$ for any hyperplane H in PG(t,q) such that V \cap H is a $(\theta-1)$ -flat in the θ -flat V where $m \ge \theta$. In the special case θ = t, S is said to be an <u>m-arc in PG(t,q)</u>. Let m(t,q) denote the largest value of m for which there exists an m-arc in PG(t,q).

Definition 3.3. Let $\mathfrak{U}(\theta,\sigma;\mathfrak{t},\mathfrak{q})$ denote a family of all sets $V\setminus S$ of a θ -flat V in $PG(\mathfrak{t},\mathfrak{q})$ and a $(\mathfrak{q}+\theta-\sigma)$ -arc S in V where $2\leq\theta\leq\mathfrak{t}$ and $0\leq\sigma\leq\mathfrak{q}$. Let $\mathfrak{M}(\theta,\zeta;\xi,\pi_1,\pi_2,\cdots,\pi_\ell;\mathfrak{t},\mathfrak{q})$ denote a family of all sets $(V\setminus S)$ U A U B of a set $V\setminus S$ in $\mathfrak{U}(\theta,\zeta;\mathfrak{t},\mathfrak{q})$, a set A of ξ points in $PG(\mathfrak{t},\mathfrak{q})$ and a set B in $\mathfrak{F}_U(0,\pi_1,\pi_2,\cdots,\pi_\ell;\mathfrak{t},\mathfrak{q})$ such that $V\cap A=\emptyset$, $(V\setminus S)\cap B=\emptyset$ and $A\cap B=\emptyset$ where $0\leq\zeta$, $\xi\leq\mathfrak{q}$, $\zeta+\xi\leq\mathfrak{q}$, $2\leq\theta\leq\pi_1$, $0\leq\ell\leq(\mathfrak{t}-2)(\mathfrak{q}-1)$, $\mathfrak{F}_U(0,\pi_1,\pi_2,\cdots,\pi_\ell;\mathfrak{t},\mathfrak{q})=\emptyset$ in the case $\ell=0$, $(0,\pi_1,\pi_2,\cdots,\pi_\ell)\in U(\mathfrak{t},\mathfrak{q})$ in the case $\ell\geq 1$ and $\ell=\emptyset$ in the case $\ell=0$.

Theorem 3.1. (Hamada(1986a)) (1) In the case $(\sigma, \mu_1, \mu_2, \dots, \mu_h) \in \widetilde{U}(t,q)$, $\mathcal{F}_U(\sigma, \mu_1, \mu_2, \dots, \mu_h; t,q) \neq \emptyset$ if and only if either (a) h = 1 and $1 \leq \mu_1 \leq t-1$ or (b) $h \geq 2$ and $\mu_{h-1} + \mu_h \leq t-1$.

- (2) In the case $2 \le \theta \le t$, $U(\theta, \sigma; t, q) \ne \emptyset$ if and only if $q + \theta m(\theta, q) \le \sigma \le q$.
- (3) In the case $0 \le \zeta$, $\xi \le q$, $\zeta + \xi \le q$, $2 \le \theta \le \pi_1$, $1 \le \ell \le (t-2)(q-1)$ and $(0,\pi_1,\pi_2,\cdots,\pi_\ell)$ \in U(t,q), $\mathcal{M}(\theta,\zeta;\xi,\pi_1,\pi_2,\cdots,\pi_\ell;t,q) \ne \emptyset$ if and only if either (a) $\ell = 1$, $\theta + \Pi_1 \le t$ and $q+\theta-m(\theta,q) \le \zeta \le q$ or (b) $\ell \ge 2$, $\pi_{\ell-1} + \pi_{\ell} \le t-1$ and $q+\theta-m(\theta,q) \le \zeta \le q$.

The following theorem gives three methods of construction of min hypers.

Theorem 3.2. (Hamada(1986a)) Let $\mathcal{J}_{\mathbf{U}}(\sigma,\mu_1,\mu_2,\cdots,\mu_h;\mathbf{t},\mathbf{q})\neq\emptyset$, $\mathcal{U}(\theta,\sigma;\mathbf{t},\mathbf{q})\neq\emptyset$ and $\mathcal{M}(\theta,\zeta;\xi,\pi_1,\pi_2,\cdots,\pi_\ell;\mathbf{t},\mathbf{q})\neq\emptyset$ where $(\sigma,\mu_1,\mu_2,\cdots,\mu_h)\in\widetilde{\mathbf{U}}(\mathbf{t},\mathbf{q})$.

- (1) If $\mathbf{F} \in \mathcal{F}_{\mathbf{U}}(\sigma,\mu_1,\mu_2,\dots,\mu_h;t,q)$, then \mathbf{F} is a $\{\sum_{i=1}^{h} \mathbf{v}_{\mu_i+1} + \sigma, \sum_{i=1}^{h} \mathbf{v}_{\mu_i}, t,q\}$ -min-hyper.
- (2) If $\mathbf{F} \in \mathcal{U}(\theta,\sigma;t,q)$, then \mathbf{F} is a $\{ \begin{array}{ccc} \theta-1 & \theta-1 \\ \Sigma & (q-1)\mathbf{v}_{\alpha+1} + \sigma, & \Sigma \\ \alpha=1 & \alpha=1 \end{array} \right.$ $(\mathbf{q}-1)\mathbf{v}_{\alpha};$ $t,q\}$ -min·hyper.
- (3) If $\mathbf{F} \in \mathcal{M}(\theta,\zeta;\xi,\pi_1,\pi_2,\cdots,\pi_\ell;t,q)$, then \mathbf{F} is a $\{\sum_{\alpha=1}^{\theta-1}(q-1)v_{\alpha+1} + \sum_{\alpha=1}^{\theta-1}v_{\alpha+1} + \sum_{\alpha=1}^{\theta-1}v_{\alpha+1$

Remark 3.1. Theorem 3.2 shows that in the case $q+\theta-m(\theta,q) \leq \sigma \leq q$, $h \geq (\theta-1)(q-1) \geq 2$, $\mu_{(\alpha-1)(q-1)+1} = \mu_{(\alpha-1)(q-1)+2} = \cdots = \mu_{(\alpha-1)(q-1)+q-1} = \alpha$ $(\alpha = 1,2,\cdots,\theta-1) \text{ and } \mu_{h-1} + \mu_h \leq t-1 \text{ for some integer } \theta \text{ such that } 2 \leq \theta \leq t,$ there exist at least $\theta \in \Sigma$ $\nu_{h+1} + \sigma$, $\nu_{$

From Theorems 3.1 and 3.2, we have the following corollary which gives a sufficient condition for integers t, ϵ , h, μ_1 , μ_2 , \cdots , μ_h and q ((or integers k, d and q)) that there exists a { $\sum_{i=1}^{L} v_{\mu_i} + 1 + \epsilon$, $\sum_{i=1}^{L} v_{\mu_i} + 1 + \epsilon$, and q ((or integers k, d and q)) that there exists a { $\sum_{i=1}^{L} v_{\mu_i} + 1 + \epsilon$, $\sum_{i=1}^{L} v_{\mu_i}$

Corollary 3.1. If either (a) $0 \le \varepsilon \le q-1$, h=1 and $1 \le \mu_1 \le t-1$ or (b) $0 \le \varepsilon \le q-1$, $h \ge 2$ and $\mu_{h-1} + \mu_h \le t-1$ or (c) $q+\theta-m(\theta,q) \le \varepsilon \le q-1$, $h=(\theta-1)(q-1)$ and $\mu_{(\alpha-1)(q-1)+1} = \mu_{(\alpha-1)(q-1)+2} = \cdots = \mu_{(\alpha-1)(q-1)+q-1} = \alpha$ ($\alpha=1,2,\cdots,\theta-1$) for some integer θ such that $2 \le \theta \le t$, there exist a $\{\sum_{i=1}^{n} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{n} v_{\mu_i} + \varepsilon,$

In the special case q = 2, we have the following corollary since $m(\theta,2)$ = $\theta+2$ for any integer $\theta \geq 2$.

Corollary 3.2. If either (a) ϵ ϵ {0,1}, h = 1 and 1 \leq $\mu_1 \leq$ t-1 or (b) ϵ ϵ {0,1}, $h \geq$ 2 and μ_{h-1} + $\mu_h \leq$ t-1 or (c) ϵ ϵ {0,1}, $2 \leq h \leq$ t-1 and $(\mu_1, \mu_2, \dots, \mu_h)$ = (1,2,...,h), there exist a { $\sum_{i=1}^{L} \nu_{i} + 1 + \epsilon$, $\sum_{i=1}^{L} \nu_{i}$; t,2}-min hyper and an (n,k,d;2)-code meeting the Griesmer bound (1.2') where k = t+1, ω = 1, d = 2^{k-1} - (ϵ + $\sum_{i=1}^{L} 2^{i}$) and ν_{μ} = 2^{μ} - 1 for any integer $\mu \geq$ 0.

Helleseth (1981) showed that (1) a sufficient condition in Corollary 3.2 is also a necessary condition in the case q=2 and (2) there is no (n,k,d;2)-code meeting the Griesmer bound (1.2') except for (n,k,d;2)-codes constructed by Theorem 3.2, Remarks 3.1 and 2.1 in the case q=2, k=t+1, $\omega=1$ and $d=2^{k-1}$ - ($\epsilon+\sum_{i=1}^{k}2^{i}$). In terms of a min-hyper, his result can be expressed i=1 as follows.

Theorem 3.3. Let $(\epsilon, \mu_1, \mu_2, \cdots, \mu_h)$ be an ordered set in U(t,2) and let $v_{\mu} = 2^{\mu} - 1$ for any integer $\mu \geq 0$ where $t \geq 2$.

(1) In the case h = 1, F is a $\{v_{\mu_1}^{\dagger}+1+\epsilon, v_{\mu_1}^{\dagger}; t, 2\}$ -min hyper if and only if

F **ϵ** $\mathcal{F}_{_{11}}(\epsilon,\mu,;t,2)$

- (2) In the case $h \ge 2$, $\mu_{h-1} + \mu_h \le t-1$ and $(\mu_1, \mu_2) \ne (1, 2)$, F is a $\{\sum_{i=1}^{h} v_{\mu_i} + 1\}$ $+\epsilon$, $\sum_{i=1}^{h} v_{\mu_i} + 1$ $+\epsilon$, $\sum_{i=1}^{$
- (3) In the case $t \geq 3$, $(\mu_1, \mu_2, \cdots, \mu_h) = (1, 2, \cdots, h)$ and $t/2 < h \leq t-1$ (i.e., $\mu_{h-1} + \mu_h > t-1)$, F is a $\{\sum_{i=1}^{L} v_{\mu_i} + 1 + \epsilon, \sum_{i=1}^{L} v_{\mu_i}; t, 2\}$ -min hyper if and only if $i=1 \quad i=1 \quad i=1$ F $\in \mathcal{U}(h+1,\epsilon;t,2)$.
- (4) In the case $t \geq 4$, $(\mu_1, \mu_2, \cdots, \mu_h) = (1, 2, \cdots, h)$ and $2 \leq h \leq t/2$ (i.e., $\mu_{h-1} + \mu_h \leq t-1$), F is a $\{\sum_{i=1}^{L} v_{\mu_i+1} + \epsilon, \sum_{i=1}^{L} v_{\mu_i}; t, 2\}$ -min hyper if and only if either F $\in \mathcal{F}_U(\epsilon, 1, 2, \cdots, h; t, 2)$ or F $\in \mathcal{U}(h+1, \epsilon; t, 2)$ or F $\in \mathcal{M}(\alpha, \zeta_\alpha; \xi_\alpha, \alpha, \alpha+1, \cdots, h; t, 2)$ for some integer α in $\{2, 3, \cdots, h\}$ where ζ_α and ξ_α are any nonnegative integers such that $\zeta_\alpha + \xi_\alpha = \epsilon$.
- (5) In the case $h \ge \theta$, $(\mu_1, \mu_2, \cdots, \mu_{\theta-1}) = (1, 2, \cdots, \theta-1)$, $\mu_{\theta} > \theta$ and $\mu_{h-1} + \mu_h \le t-1$ for some integer $\theta \ge 3$, F is a $\{\sum_{i=1}^{\infty} v_{\mu_i+1} + \epsilon, \sum_{i=1}^{\infty} v_{\mu_i}; t, 2\}$ -min-hyper if and only if either F $\in \mathcal{F}_U(\epsilon, \mu_1, \mu_2, \cdots, \mu_h; t, 2)$ or F $\in \mathcal{M}(\alpha, \zeta_{\alpha}; \xi_{\alpha}, \mu_{\alpha}, \mu_{\alpha+1}, \cdots, \mu_h; t, 2)$ for some integer α in $\{2, 3, \cdots, \theta\}$ where ζ_{α} and ξ_{α} are any nonnegative integers such that $\zeta_{\alpha} + \xi_{\alpha} = \epsilon$.

Remark 3.2. Theorem 3.3 can be proved directly using the inductive structure of a min-hyper such as Proposition 3.1 in Hamada (1985).

Remark 3.3. In the case $q \ge 3$, there exists a $\begin{cases} \Sigma & v_{\mu_i+1} + \epsilon, \Sigma & v_i; \\ h & h \\ t,q$ -min-hyper except for $\begin{cases} \Sigma & v_{\mu_i+1} + \epsilon, \Sigma & v_i; \\ 1 = 1 & i \end{cases}$ by Theorem 3.2 and Remark 3.1.

Example 3.1. (1) In the case q = 3, h =1, μ_1 = 1, ϵ = 2 and t \geq 2, let (ν_0) , (ν_1) and (ν_2) be any non-collinear points in PG(t,3) and let F = $\{(\nu_1)$, $(\nu_0+\nu_1)$, $(2\nu_0+\nu_1)$, (ν_2) , $(\nu_1+\nu_2)$, $(\nu_0+2\nu_1+\nu_2)$. Then F is a $\{v_2+2,1;t,3\}$ -min hyper which contains no 1-flat (i.e., F $\not\in \mathcal{F}_U(2,1;t,3)$) where v_2 = $(3^2-1)/(3-1)$.

- (2) In the case q = 4, h = 1, μ_1 = 1, ϵ = 2 and t \geq 2, let (ν_0) , (ν_1) and (ν_2) be any noncollinear points in PG(t,4) and let F = { $(\nu_0 + \nu_1)$, $(\alpha \nu_0 + \nu_1)$, $(\alpha^2 \nu_0 + \nu_1)$, (ν_2) , $(\nu_0 + \nu_1 + \nu_2)$, $(\alpha^2 \nu_0 + \alpha \nu_1 + \nu_2)$, $(\alpha \nu_0 + \alpha^2 \nu_1 + \nu_2)$ } where α is a primitive element of GF(2²) such that $\alpha^2 = \alpha + 1$ and $\alpha^3 = 1$. Then F is a { $\nu_2 + 2$,1; t,4}-min·hyper which contains no 1-flat where $\nu_2 = (4^2 1)/(4 1)$.
- (3) In the case $q \ge 4$, h = 2, $\mu_1 = \mu_2 = 1$, $\epsilon = q-2$ and $t \ge 2$, let V be any 2-flat in PG(t,q) and let L_i ($i = 1,2,\cdots,q+1$) be q+1 1-flats in V passing through one point Q in V and let $F = L_1 \cup L_2 \cup \{P_3,P_4,\cdots,P_{q+1}\}$ where P_i ($3 \le i \le q+1$) denotes any point in $L_i \setminus \{Q\}$. Then F is a $\{2v_2+(q-2),2;t,q\}$ -min·hyper such that $F \not\in \mathcal{F}_{U}(q-2,1,1;t,q)$.

From Theorem 2.6 in Hamada (1985), we have the

Theorem 3.4. If there exists a $\{\sum_{\alpha=0}^{\infty} \epsilon_{\alpha} v_{\alpha+1}, \sum_{\alpha=0}^{\infty} \epsilon_{\alpha} v_{\alpha}; t,q\}$ -min·hyper, there exists a $\{\sum_{\alpha=0}^{\infty} \epsilon_{\alpha} v_{\alpha+1-n}, \sum_{\alpha=n}^{\infty} \epsilon_{\alpha} v_{\alpha-n}; t,q\}$ -min·hyper for any positive integer $n \leq t-2$.

From Theorem 3.4, we have the following corollary which is very useful in proving the nonexistence of a min-hyper.

 such that $1 \le m \le n$ and $0 \le \varepsilon_1^* \le q-1$.

(2) If there is no $\{\sum\limits_{i=1}^{h}v_{\mu_{i}}^{}+1+\epsilon,\sum\limits_{i=1}^{h}v_{\mu_{i}}^{};t,q\}$ -min·hyper for some ordered $\sum\limits_{i=1}^{h}v_{\mu_{i}}^{}+1+\epsilon,\sum\limits_{i=1}^{h}v_{\mu_{i}}^{};t,q\}$ -min·hyper for some ordered set $(\epsilon,\mu_{1},\mu_{2},\cdots,\mu_{h})$ in U(t,q) such that $\mu_{h}\leq t-2$, there is no $\{\sum\limits_{i=1}^{L}v_{\mu_{i}}^{}+m+1+\epsilon v_{\mu_{i}}^{}+\epsilon v_{\mu_{i}}^{}+m+1+\epsilon v_{\mu_{i}}^{}+\epsilon v_{\mu_{i}}$

4. Characterization of certain min hypers and a necessary condition

Recently, the author proved the following theorem using Propositions 3.1 and 3.2 in Hamada (1985).

Theorem 4.1. (Hamada(1985)) Let t and q be any integer \geq 2 and any prime power \geq 3 respectively and let $(\epsilon,\mu_1,\mu_2,\cdots,\mu_h)$ be any ordered set in U(t,q) such that ϵ \in {0,1} and $1 \leq \mu_1 < \mu_2 < \cdots < \mu_h \leq$ t-1 where $1 \leq h \leq$ t-1.

- (1) In the case h = 1 and 1 $\leq \mu_1 \leq$ t-1, F is a $\{v_{\mu_1+1} + \epsilon, v_{\mu_1}; t, q\}$ -min·hyper if and only if F $\in \mathcal{F}_U(\epsilon, \mu_1; t, q)$.
- (2) In the case $h \ge 2$ and $\mu_{h-1} + \mu_h \le t-1$, F is a $\begin{cases} \Sigma & v_{\mu_1+1} + \varepsilon, & \Sigma & v_{\mu_1}; \\ i=1 & i=1 \end{cases}$ t,q}-min·hyper if and only if F $\in \mathcal{F}_{\mu_1}(\varepsilon,\mu_1,\mu_2,\cdots,\mu_h;t,q)$.
- t,q}-min·hyper if and only if F $\in \mathcal{J}_U(\varepsilon,\mu_1,\mu_2,\cdots,\mu_h;t,q)$. (3) In the case $h \geq 2$ and $\mu_{h-1} + \mu_h > t-1$, there is no $\{\sum_{i=1}^h v_{\mu_i} + 1 + \epsilon, \sum_{i=1}^h v_{\mu_i}; t,q\}$ -min·hyper F.

In order to generalize Theorem 4.1, it is necessary to characterize all $\{\varepsilon_1 v_2 + \varepsilon_0, \varepsilon_1; t, q\}$ -min-hypers for any ordered set $(\varepsilon_0, \varepsilon_1)$ in E(t, q) and to generalize Propositions 3.1 and 3.2 in Hamada (1985). In this section, we shall try to characterize all $\{\varepsilon_1 v_2 + \varepsilon_0, \varepsilon_1; t, q\}$ -min-hypers for any ordered set $(\varepsilon_0, \varepsilon_1)$ in E(t, q) such that $\varepsilon_1 \in \{1, 2\}$, $\varepsilon_0 \in \{0, 1, 2\}$, $t \ge 2$ and $q \ge 3$ and to generalize

Proposition 3.1 in Hamada (1985). In the case $\mu_1 \geq 2$ and $0 \leq \epsilon \leq q-1$, we have the following theorem from the proof of Proposition 3.1 in Hamada (1985) since $v_{\mu-1} + (q-1) < v_{\mu} \text{ for any integer } \mu \geq 2.$

Theorem 4.2. Let $(\varepsilon,\mu_1,\mu_2,\cdots,\mu_h)$ be any ordered set in U(t,q) such that $\mu_1 \geq 2$ and $\mathcal{F}_U(\varepsilon,\mu_1-1,\mu_2-1,\cdots,\mu_h-1;t-1,q) \neq \emptyset$ and let δ_j 's be any nonnegative integers such that $\sum_{j=1}^K \delta_j = \varepsilon$. If there exists a $\{\sum_{j=1}^K v_{\mu_j+1} + \varepsilon, \sum_{j=1}^K v_{\mu_j};t,q\}$ -min-hyper F such that (a) F \bigcap G \in $\mathcal{F}_U(\mu_1-2,\mu_2-2,\cdots,\mu_h-2;t,q)$ for some (t-2)-flat G in PG(t,q) and (b) F \bigcap H \in $\mathcal{F}_U(\delta_j,\mu_1-1,\mu_2-1,\cdots,\mu_h-1;t,q)$ for any hyperplane H \in $\mathcal{F}_U(\varepsilon,\mu_1,\mu_2,\cdots,\mu_h;t,q)$.

Remark 4.1. Let $(\varepsilon,\mu_1,\mu_2,\cdots,\mu_h)$ be an ordered set in U(t,q) such that $h \geq 2$ and $\mu_1 \geq 2$. Then it follows from Theorem 3.1 that (1) $\mathcal{F}_U(\varepsilon,\mu_1^{-1},\mu_2^{-1},\cdots,\mu_h^{-1};t^{-1},q) \neq \emptyset$ if and only if $\mu_{h-1} + \mu_h \leq t$ and (2) $\mathcal{F}_U(\varepsilon,\mu_1,\mu_2,\cdots,\mu_h^{-1};t,q) \neq \emptyset$ if and only if $\mu_{h-1} + \mu_h \leq t^{-1}$. Hence in the case $\mu_{h-1} + \mu_h = t$, there is $\mu_{h-1} + \mu_h = t$, $\mu_{h-1} + \mu_h = t$, $\mu_{h-1} + \mu_h = t$, $\mu_{h-1} + \mu_h = t$, it is sufficient to show that (a) and (b) $\mu_{h-1} + \mu_h = t$, it is sufficient to show that $\mu_{h-1} + \mu_h = t$, it is sufficient to show that $\mu_{h-1} + \mu_h = t$, $\mu_{h-1} + \mu_h = t$, it is sufficient to show that $\mu_{h-1} + \mu_h = t$, $\mu_{h-1} + \mu_{h-1} + \mu_{h-1}$

From Theorem 4.2, Remark 4.1 and Corollary 3.3, we have the

 $0 \le \varepsilon \le q-1$ and $2 \le \mu_1 \le t-1$.

(2) Let $(0, \mu_1, \mu_2, \cdots, \mu_h)$ be an ordered set in U(t,q) such that $h \geq 2$, $\mu_1 = 2$ and $\mu_{h-1} + \mu_h \leq t$. If $(\alpha) \in \mathcal{F} \in \mathcal{F}(\mu_1-2,\mu_2-2,\cdots,\mu_h-2;t,q)$ for any $\{\sum_{i=1}^{n} v_{\mu_i-1}, \sum_{i=1}^{n} v_{\mu_i-1}, \cdots, \sum_$

In the case $h \ge 2$, $\mu_1 = 1$ and $\mu_h \ge 3$, we can prove the following theorem using a method similar to the proof of Proposition 3.1 in Hamada (1985).

Theorem 4.3. Let $(\epsilon,\mu_1,\mu_2,\cdots,\mu_h)$ and θ be an ordered set in U(t,q) and an integer respectively such that $h \geq \theta \geq 2$, $\mu_1 = 1$, $\mu_\theta \geq 3$ and $\mu_{h-1} + \mu_h \leq t$ and let τ be the number of integers i in $\{1,2,\cdots,h\}$ such that $\mu_i = 1$ and let δ_j 's be nonnegative integers such that $\sum_{j=1}^{q+1} \delta_j = \epsilon$. If there exists a $\{\sum_{j=1}^{q} v_{\mu_j+1} + \epsilon, j=1\}$ is $\sum_{j=1}^{q} v_{\mu_j+1} + \sum_{j=1}^{q} v_{\mu_j+1} + \sum_{j=1}^{$

Remark 4.2. A set X in Theorem 4.3 is not necessarily unique. For example, either X \in $\mathcal{F}(1,2;t,2)$ or X \in $\mathcal{U}(3,0;t,2)$ in the case q=2, $\epsilon=0$, $h\geq 3$, $\mu_1=1$, $\mu_2=2$ and $\mu_3\geq 3$.

Remark 4.3. Theorem 4.3 shows that in the case h > 0 \geq 2, μ_1 = 1, $\mu_0 \geq$ 3 and μ_{h-1} + μ_h = t, there is no { $\sum_{i=1}^{h} v_{\mu_i+1} + \epsilon$, $\sum_{i=1}^{r} v_{\mu_i}$; t,q}-min·hyper which satisfies two conditions (a) and (b) in Theorem 4.3 since there exist a μ_{h-1} -flat and a μ_h -flat in PG(t,q) which are mutually disjoint if and only if μ_{h-1} + $\mu_h \leq$ t-

Since there is no space to give the proof of the following theorem, we shall describe only results. In detail, refer Hamada (1986a, 1986b and 1986c) in which the proofs of theorems in Sections 3 and 4 and more general results are give

Theorem 4.4. (Hamada(1986b and 1986c)) Let t and q be an integer \geq 2 and a prime power \geq 3 respectively and let $v_2 = q+1$.

- (1) In the case $0 \le \varepsilon < \sqrt{q}$, F is a $\{v_2+\varepsilon,1;t,q\}$ -min·hyper if and only if F $\in \mathcal{F}_U(\varepsilon,1;t,q)$.
- (2) In the case where either (a) q=3 and $\epsilon=2$ or (b) $q=p^{2r}$ and $\sqrt{q} \leq \epsilon \leq q-1$ for a prime p and a positive integer r, there exists a $\{v_2+\epsilon,1;t,q\}$ -minhyper F such that $f \notin \mathcal{F}_U(\epsilon,1;t,q)$.
- (3) In the case where q is a prime and (q+1)/2 $\leq \epsilon \leq$ q-1, there exists a $\{v_2+\epsilon,l;t,q\}$ -min·hyper F such that F $\notin \mathcal{F}_U(\epsilon,l;t,q)$.
- (4) In the case t = 2, (a) there is no $\{2v_2, 2; t, q\}$ -min·hyper for any prime power $q \ge 3$ and (b) there is no $\{2v_2+1, 2; t, q\}$ -min·hyper for any prime power $q \ge 4$ and (c) there is no $\{2v_2+2, 2; t, q\}$ -min·hyper for any prime power $q \ge 5$.
- (5) In the case $t \ge 3$ and $q \ge 3$, F is a $\{2v_2, 2; t, q\}$ -min-hyper if and only if $f \in \mathcal{F}(1,1;t,q)$.
- (6) In the case $t \ge 3$ and q = 3, F is a $\{2v_2+1,2;t,3\}$ -min·hyper if and only if either F $\in \mathcal{F}(0,1,1;t,3)$ or F $\in \mathcal{U}(2,1;t,3)$. In the case $t \ge 3$ and $q \ge 4$, F is a $\{2v_2+1,2;t,3\}$ -min·hyper if and only if F $\in \mathcal{F}(0,1,1;t,q)$.

(7) In the case $t \ge 3$ and $q \ge 5$, F is a $\{2v_2+2,2;t,q\}$ -min-hyper if and only if $F \in \mathcal{F}(0,0,1,1;t,q)$. In the case $t \ge 3$ and q = 3 or 4, there exists a $\{2v_2+2,2;t,q\}$ -min-hyper F such that $F \notin \mathcal{F}(0,0,1,1;t,q)$.

References

- 1. L. D. Baumert and R. J. McEliece, A note on the Griesmer bound, Trans. Information Theory 19 (1973), 134-135.
- 2. J. H. Griesmer, A bound for error-correcting codes, IBM J. Res. Develop. 4 (1960), 532-542.
- 3. N. Hamada and F. Tamari, On a geometrical method of construction of maximal t-linearly independent sets, J. Combinatorial Theory (A) 25 (1978), 14-28.
- 4. N. Hamada and F. Tamari, Construction of optimal codes and optimal fractional factorial designs using linear programming, Annals of Discrete Mathematics 6 (1980), 175-188.
- 5. N. Hamada and F. Tamari, Construction of optimal linear codes using flats and spreads in a finite projective geometry, European J. Combinatorics 3 (1982), 129-141.
- N. Hamada, Characterization resp. nonexistence of certain q-ary linear codes attaining the Griesmer bound, Bulletin of Osaka Women's University 22 (1985), 1-47.
- 7. N. Hamada, Characterization of min hypers in a finite projective geometry and its applications to error-correcting codes, Submitted for publication (1986a).
- 8. N. Hamada, Characterization of {2(q+1),2;t,q}-min·hypers and {2(q+1)+1,2;t,q}-min·hypers in a finite projective geometry, Submitted for publication (1986b).
- 9. N. Hamada, Characterization of {(q+1)+2,1;t,q}-min·hypers and {2(q+1)+2,2;t,q}-min·hypers in a finite projective geometry, Submitted for publication (1986c).
- 10. T. Helleseth, A characterization of codes meeting the Griesmer bound, Information and Control 50 (1981), 128-159.
- 11. F. J. MacWilliams and N. J. A. Sloane, The theory of error-correting codes, North-Holland Mathematical Library, 16 (1977), Amsterdam.
- 12 G. Solomon and J. J. Stiffler, Algebraically puncture cyclic codes, Information and Control 8 (1965), (1965), 170-179.

- 13. F. Tamari, On an {f,m;t,s}-max.hyper and a {k,m;t,s}-min.hyper in a finite projective geometry PG(t,s), Bulletin of Fukuoka University of Education 31 (III) (1981), 35-43.
- 14. F. Tamari, On linear codes which attain the Solomon-Stiffler bound, Discrete Mathematics 49 (1984), 179-191.