Kangweon-Kyungki Math. Jour. **9** (2001), No. 2, pp. 129–131

ON SOME MDS-CODES OVER ARBITRARY ALPHABET

Gyu Whan Chang and Young Ho Park

Abstract. Let $q = p_1^{e_1} \cdots p_m^{e_m}$ be the product of distinct prime elements. In this short paper, we show that the largest value of M such that there exists an $(n, M, n-1)$ q-ary code is q^2 if $n - 1 \leq p_i^{e_i}$ for all i.

1. Introduction

Let F_q be a set of q distinct elements. A q-ary code C of length n over F_q is a subset of F_q^n. The Hamming distance $d(x, y)$ of $x, y \in C$ is defined to be the number of places in which they differ. The minimum distance $d(C)$ of C is the minimum of $d(x, y)$, where $x, y \in C$ and $x \neq y$. A q-ary (n, M, d) code is a code of length n over F_q, containing M codewords and having minimum distance d. We denote by $A_q(n,\ d)$ the largest value of M such that there exists an $(n,\ M,\ d)$-code. One of the main coding theory problem is to find the largest code of given length and given distance. An upper bound for $A_q(n, d)$ is given by Singleton.

Theorem 1 (The Singleton Bound).

$$A_q(n, d) \leq q^{n-d+1}.$$

An (n, q^{n-d+1}, d)-code is called a *maximum distance separable code* (MDS-code), which was first explicitly studied by Singleton [4]. The following theorem gives some MDS-codes [3].

Theorem 2. 1. $A_q(4,\ 3) = q^2$ *for all* $q \neq 2, 6$.
2. $A_q(n, n-1) = q^2$ *if* q *is a prime power and* $n - 1 \leq q$.

The purpose of this short paper is to generalize this result.

Received July 27, 2001.
2000 Mathematics Subject Classification: 94B65, 94B05.
Key words and phrases: Singleton bound, MDS-code, mutually orthogonal Latin squares.

2. Main Theorem

Let $q = p_1^{e_1} \cdots p_m^{e_m}$ be the prime factorization of q and let $R_i = GF(p_i^{e_i})$ be the Galois field of order $p_i^{e_i}$. Let $R = R_1 \times \cdots \times R_m$ be the direct product of the Galois fields R_i. Then R is a commutative ring with identity.

LEMMA 3. *If $d \leq p_i^{e_i}$ for all $i = 1, \cdots, m$, there exist unit elements $\alpha_1, \ldots, \alpha_{d-1}$ of R such that $\alpha_i - \alpha_j$ are also unit elements of R for all $i \neq j$.*

Proof. Choose any nonzero $d-1$ distinct elements $x_{i1}, \ldots, x_{id-1}$ of R_i and let $\alpha_j = (x_{1j}, x_{2j}, \ldots, x_{mj}) \in R$. Then each α_j is a unit element of R. Moreover, if $i \neq j$, then $\alpha_i - \alpha_j = (x_{1i} - x_{1j}, x_{2i} - x_{2j}, \ldots, x_{mi} - x_{mj})$ is a unit element of R because $x_{ki} - x_{kj} \neq 0$ for $k = 1, \ldots, m$. Thus $\{\alpha_1, \ldots, \alpha_{d-1}\}$ is a set of desired elements of R. □

A *Latin square* of order q is a $q \times q$ matrix whose entries are from R of q distinct elements such that each row and each column of the matrix contains each symbol exactly once. Let $A = (a_{ij})$ and $B = (b_{ij})$ be two Latin squares of order q. Then A and B are said to be *mutually orthogonal Latin squares* (MOLS) if the q^2 ordered pairs $(a_{ij},\ b_{ij})$ are all distinct. A set $\{A_1,\ \ldots,\ A_k\}$ of Latin squares is called a set of MOLS if each pairs $\{A_i,\ A_j\}$ is a pair of MOLS.

PROPOSITION 4. *Suppose that $d \leq p_i^{e_i}$ for $i = 1, \ldots m$. Then there is a set $\{A_1, \ldots, A_{d-1}\}$ of mutually orthogonal $q \times q$ Latin squares whose entries are in R.*

Proof. Let $R = \{\lambda_1, \lambda_2, \ldots, \lambda_q\}$ and let $\{\alpha_1, \ldots, \alpha_{d-1}\}$ be a set of units in R such that $\alpha_i - \alpha_j$ is also a unit of R for $i \neq j$. Let $A_1, \ldots, A_{d-1}$ be $q \times q$ matrices, in which the (i,j)th entry of A_k is an element of R defined by

$$a_{ij}^{(k)} = \lambda_i + \alpha_k \lambda_j.$$

First, note that A_k is a Latin square. For if $a_{ij}^{(k)} = a_{it}^{(k)}$, then $\alpha_k \lambda_j = \alpha_k \lambda_t$ and hence $\lambda_j = \lambda_t$ (note that α_k is a unit in R). Similarly, if $a_{ij}^{(k)} = a_{tj}^{(k)}$, then $i = t$. Now we show that each pair A_k, A_t is mutually orthogonal. For $1 \leq k < t \leq d-1$, if

$$(a_{i_1 j_1}^{(k)},\ a_{i_1 j_1}^{(t)}) = (a_{i_2 j_2}^{(k)},\ a_{i_2 j_2}^{(t)}),$$

then

$$\lambda_{i_1} + \alpha_k \lambda_{j_1} = \lambda_{i_2} + \alpha_k \lambda_{j_2}, \quad \lambda_{i_1} + \alpha_t \lambda_{j_1} = \lambda_{i_2} + \alpha_t \lambda_{j_2},$$

and hence $(\alpha_k - \alpha_t)\lambda_{j_1} = (\alpha_k - \alpha_t)\lambda_{j_2}$. Recall that α_k, α_t, and $\alpha_k - \alpha_t$ are units in R. Thus $\lambda_{j_1} = \lambda_{j_2}$ and $\lambda_{i_1} = \lambda_{i_2}$, which implies that A_k and A_t are mutually orthogonal. □

THEOREM 5. *If* $n-1 \leq p_i^{e_i}$ *for all* $i = 1, \cdots, m$, *then* $A_q(n, n-1) = q^2$.

Proof. By the Singleton bound, it suffices to show that there exists a $(n, q^2, n-1)$-code. Let $\{A_1, \ldots, A_{n-2}\}$ be a set of mutually orthogonal $q \times q$ Latin squares over R as in Proposition 3. Let

$$C = \{(\lambda_i,\ \lambda_j,\ a_{ij}^{(1)},\ a_{ij}^{(2)}, \ldots,\ a_{ij}^{(n-2)}) \mid \lambda_i,\ \lambda_j \in R\}.$$

C has length n, and $|C| = q^2$. Next, since A_k are mutually orthogonal Latin squares, it follows that if $a_{i_1 j_1}^{(k)} = a_{i_2 j_2}^{(k)}$ for some k, then $i_1 \neq i_2$, $j_1 \neq j_2$ and $a_{i_1 j_1}^{(t)} \neq a_{i_2 j_2}^{(t)}$ for all $t \neq k$. On the other hand, if $a_{i_1 j_1}^{(k)} \neq a_{i_2 j_2}^{(k)}$ for all k, then clearly $i_1 \neq i_2$ or $j_1 \neq j_2$. Thus $d(C) \geq n-1$ and hence $d(C) = n-1$. Therefore C is a desired code by the construction of C. □

References

[1] R. Bose, S. Shrikhande and E. Parker, *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture*, Canad. J. Math. 12 (1960), 189-203.

[2] J. Deńes and A. Keedwell, *Latin squares and their applications*, Academic press, New York, 1974.

[3] R. Hill, *A first course in Coding Theory*, Oxford University press, 1986.

[4] R. Singleton, *Maximum distance q-nary codes*, IEEE Trans. Info. Theory 10 (1964), 116-118.

Department of Mathematics
Kangwon National University
Chunchon 200-701, KOREA