Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 152-157*

New extension theorems for codes over $\mathbb{F}_q$ [1]

Tatsuya Maruta maruta@mi.s.osakafu-u.ac.jp
Taichiro Tanaka ta330cha@gmail.com
Hitoshi Kanda jinza80kirisame@gmail.com
Department of Mathematics and Information Sciences
Osaka Prefecture University, Sakai, Osaka 599-8531, Japan

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. Some generalized extension theorems for linear codes over $\mathbb{F}_q$ are presented.

1 Introduction

Let $\mathbb{F}_q^n$ denote the vector space of n-tuples over $\mathbb{F}_q$, the field of q elements. A q-ary linear code of length n and dimension k or an $[n,k]_q$ code is a k-dimensional subspace of $\mathbb{F}_q^n$. An $[n,k,d]_q$ code is an $[n,k]_q$ code with minimum (Hamming) distance d. The *weight* of a vector $\boldsymbol{x} \in \mathbb{F}_q^n$, denoted by $wt(\boldsymbol{x})$, is the number of nonzero coordinate positions in $\boldsymbol{x}$. The weight distribution of $\mathcal{C}$ is the list of numbers A_i which is the number of codewords of $\mathcal{C}$ with weight i. The weight distribution with $(A_0, A_d, ...) = (1, \alpha, ...)$ is expressed as $0^1 d^\alpha \cdots$ in this paper. A q-ary linear code $\mathcal{C}$ is *w-weight (mod q)* if $\mathcal{C}$ has exactly w kinds of weights under modulo q for codewords. We only consider linear codes over finite fields having no coordinate which is identically zero. For an $[n,k,d]_q$ code $\mathcal{C}$ with a generator matrix G, $\mathcal{C}$ is called *extendable* (to $\mathcal{C}'$) if there exists a vector $h \in \mathbb{F}_q^k$ such that the extended matrix $[G, h^{\mathrm{T}}]$ generates an $[n+1, k, d+1]_q$ code $\mathcal{C}'$. Then $\mathcal{C}'$ is called an *extension* of $\mathcal{C}$. The most well-known extension theorem is the following by Hill and Lizak (1995), see also [5].

Theorem 1 ([6])**.** *Every $[n,k,d]_q$ code with $gcd(d,q) = 1$, whose weights (of codewords) are congruent to* 0 *or* d (mod q)*, is extendable.*

For even $q \geq 8$, we give a stronger result:

Theorem 2. *For $q = 2^h$, $h \geq 3$, every $[n,k,d]_q$ code with d odd whose weights are congruent to* 0 *or* d (mod $q/2$) *is extendable.*

Theorem 2 is the first extension theorem for 4-weight (mod q) linear codes. As for the extension theorems for 3-weight (mod q) linear codes, see [12].

[1]This research is partially supported by Grant-in-Aid for Scientific Research of Japan Society for the Promotion of Science under Contract Number 24540138.

Theorem 3. *For $q = 2^h$, $h \geq 3$, every $[n, k, d]_q$ code with gcd$(d, q) = 2$ whose weights are congruent to* 0 *or* d (mod q) *is extendable.*

Simonis (2000) gave the following generalization of Theorem 1.

Theorem 4 ([13]). *Every $[n, k, d]_q$ code with gcd$(d, q) = 1$, $q = p^h$, p prime, is extendable if $\sum_{i \not\equiv d \pmod p} A_i = q^{k-1}$.*

We give a generalization of Theorem 4:

Theorem 5. *Let h, m, t be integers with $0 \leq m < t \leq h$. For $q = p^h$ with prime p, every $[n, k, d]_q$ code with gcd$(d, q) = p^m$ is extendable if*

$$\sum_{i \equiv d \pmod{p^t}} A_i > q^k - q^{k-1} - r(q)q^{k-3}(q-1), \tag{1}$$

where $q + r(q) + 1$ is the smallest size of a non-trivial blocking set in $PG(2, q)$.

It can be shown that (1) implies $\sum_{i \equiv d \pmod{p^t}} A_i = q^k - q^{k-1}$. Note that Theorem 4 is the case $m = 0$, $t = 1$ and $\sum_{i \equiv d \pmod{p^t}} A_i = q^k - q^{k-1}$ in Theorem 5.

To give another extension theorem, we introduce the diversity of a linear code. For an $[n, k, d]_q$ code $\mathcal{C}$ with gcd$(d, q) = 1$, let

$$\Phi_0 = \frac{1}{q-1} \sum_{q|i, i>0} A_i, \quad \Phi_1 = \frac{1}{q-1} \sum_{i \not\equiv 0, d \pmod q} A_i,$$

where the notation $q|i$ means that q is a divisor of i. The pair of integers (Φ_0, Φ_1) is called the *diversity* of $\mathcal{C}$ ([9], [10]). Theorem 1 shows that $\mathcal{C}$ is extendable if $\Phi_1 = 0$. We denote $\theta_j = (q^{j+1} - 1)/(q - 1)$ for $\mathbb{F}_q$. As for the extendability of ternary linear codes ($q = 3$), it is known that an $[n, k, d]_3$ code with gcd$(3, d) = 1$, $k \geq 3$, is extendable if

$$(\Phi_0, \Phi_1) \in \{(\theta_{k-2}, 0), (\theta_{k-3}, 2 \cdot 3^{k-2}), (\theta_{k-2}, 2 \cdot 3^{k-2}), (\theta_{k-2} + 3^{k-2}, 3^{k-2})\},$$

see [10]. For an $[n, k, d]_q$ code $\mathcal{C}$ with gcd$(d, q) = 1$, $k \geq 3$, it follows from Theorem 1 that $\mathcal{C}$ is extendable if $(\Phi_0, \Phi_1) = (\theta_{k-2}, 0)$. We generalize the case $(\Phi_0, \Phi_1) = (\theta_{k-2} + 3^{k-2}, 3^{k-2})$ for ternary linear codes to q-ary linear codes.

Theorem 6. *Let $\mathcal{C}$ be an $[n, k, d]_q$ code with diversity (Φ_0, Φ_1), gcd$(d, q) = 1$. Then $\mathcal{C}$ is extendable if $(\Phi_0, \Phi_1) = (\theta_{k-2}, 0)$ or $(\theta_{k-1} - 2q^{k-2}, q^{k-2})$.*

Example 1. (a) *Let $\mathcal{C}_1$ be a $[100, 3, 87]_8$ code. It can be proved that all possible weights of $\mathcal{C}_1$ are $87, 88, 91, 92, 95, 96$. Hence $\mathcal{C}_1$ is extendable by Theorem 2.*
(b) *There exists a $[30, 3, 22]_4$ code $\mathcal{C}_2$ with weight distribution $0^1 22^{45} 24^{15} 30^3$,*

see [3]. *$\mathcal{C}_2$ is extendable by Theorem 5 with $m = 1$, $t = 2$, $p = 2$.*
(c) *Let $\mathcal{C}_3$ be a $[15, 3, 11]_4$ code with generator matrix*

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & \bar{\omega} & \bar{\omega} & 1 & \omega & 1 & \bar{\omega} & \omega & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & \omega & 1 & 0 & 1 & 0 & 0 & \bar{\omega} & 1 \end{bmatrix},$$

where $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$. The weight distribution of $\mathcal{C}_3$ is $0^1 7^3 8^3 9^3 11^9 12^{36} 13^9$ with diversity $(13, 4)$. So, $\mathcal{C}_3$ is extendable by Theorem 6.

Problem. (i) Can the conditions "$q = 2^h$" and "$\pmod{q/2}$" in Theorem 2 be generalized to "$q = p^h$" and "$\pmod{q/p}$" for an odd prime p?
(ii) Is Theorem 6 valid for the case $\gcd(d, q) \geq 2$?
(iii) Find more diversities such that every code over $\mathbb{F}_q$ is extendable.

2 Proof of the new extension theorems

We first give the geometric method to investigate linear codes over $\mathbb{F}_q$ through the projective geometry. A *j-flat* of $\mathrm{PG}(r, q)$ is a projective subspace of dimension j in $\mathrm{PG}(r, q)$. The 0-flats, 1-flats, 2-flats and $(r-1)$-flats are called *points, lines, planes* and *hyperplanes*, respectively. The number of points in a j-flat is $|\mathrm{PG}(j, q)| = \theta_j = (q^{j+1} - 1)/(q - 1)$, where $|T|$ denotes the number of elements in the set T. We refer to [7] for geometric terminologies.

We assume $k \geq 3$. Let $\mathcal{C}$ be an $[n, k, d]_q$ code with diversity (Φ_0, Φ_1) and a generator matrix $G = [g_{ij}]$ with no all-zero column. Let g_i be the i-th row of G for $1 \leq i \leq k$. We consider the mapping w_G from $\Sigma :=\mathrm{PG}(k-1, q)$ to $\{i \mid A_i > 0\}$, the set of non-zero weights of $\mathcal{C}$. For $P = \mathbf{P}(p_1, \ldots, p_k) \in \Sigma$, *the weight of P with respect to G*, denoted by $w_G(P)$, is defined as

$$w_G(P) = |\{j \mid \sum_{i=1}^{k} g_{ij} p_i \neq 0\}| = wt(\sum_{i=1}^{k} p_i g_i).$$

Let $F_d = \{P \in \Sigma \mid w_G(P) = d\}$. Recall that a hyperplane H of Σ is defined by a non-zero vector $h = (h_1, \ldots, h_k) \in \mathbb{F}_q^k$ as $H = \{\mathbf{P}(p_1, \ldots, p_k) \in \Sigma \mid h_1 p_1 + \cdots + h_k p_k = 0\}$. The vector h is called a *defining vector of H*.

Lemma 7 ([11]). *$\mathcal{C}$ is extendable if and only if there exists a hyperplane H of Σ such that $F_d \cap H = \emptyset$. Moreover, the extended matrix of G by adding a defining vector of H as a column generates an extension of $\mathcal{C}$.*

Now, let

$$\begin{aligned} F_0 &= \{P \in \Sigma \mid w_G(P) \equiv 0 \pmod{q}\}, \\ F_1 &= \{P \in \Sigma \mid w_G(P) \not\equiv 0, d \pmod{q}\}, \\ F_2 &= \{P \in \Sigma \mid w_G(P) \equiv d \pmod{q}\} \supset F_d. \end{aligned}$$

Note that $(\Phi_0, \Phi_1) = (|F_0|, |F_1|)$. Since $(F_0 \cup F_1) \cap F_d = \emptyset$ if $\gcd(d, q) < q$, we get the following.

Lemma 8. *$\mathcal{C}$ is extendable if $gcd(d, q) < q$ and if there exists a hyperplane H of Σ such that $H \subset F_0 \cup F_1$.*

A set $\mathcal{B}$ in $\mathrm{PG}(r, q)$ is called a *blocking set with respect to s-flats* if every s-flat in $\mathrm{PG}(r, q)$ meets $\mathcal{B}$ in at least one point. A blocking set in $\mathrm{PG}(r, q)$ with respect to s-flats is called *non-trivial* if it contains no $(r - s)$-flat.

Theorem 9 ([1],[2],[4]). *Let $\mathcal{B}$ be a blocking set with respect to s-flats in $PG(r, q)$.*

(a) $|\mathcal{B}| \geq \theta_{r-s}$, *where the equality holds if and only if $\mathcal{B}$ is an $(r - s)$-flat.*

(b) $|\mathcal{B}| \geq \theta_{r-s} + q^{r-s-1}r(q)$ *if $\mathcal{B}$ is non-trivial, where $q + r(q) + 1$ is the smallest size of a non-trivial blocking set in $PG(2, q)$.*

Considering the $(q + 1) \times n$ matrix whose rows are the vectors in the set $\{\boldsymbol{a}_1 + \lambda \boldsymbol{a}_2 \mid \lambda \in \mathbb{F}_q\} \cup \{\boldsymbol{a}_2\}$, and counting the number of non-zero entries via rows and via columns, gives the following.

Lemma 10 ([5]). *For two linearly independent vectors $\boldsymbol{a}_1, \boldsymbol{a}_2 \in \mathbb{F}_q^n$, it holds that*

$$\sum_{\lambda \in \mathbb{F}_q} wt(\boldsymbol{a}_1 + \lambda \boldsymbol{a}_2) + wt(\boldsymbol{a}_2) \equiv 0 \pmod{q}.$$

As a consequence of Lemma 10, we get the following.

Lemma 11. *For a line $L = \{P_0, P_1, \cdots, P_q\}$ in Σ, it holds that*

$$w_G(L) := \sum_{i=0}^{q} w_G(P_i) \equiv 0 \pmod{q}. \tag{2}$$

Lemma 12 ([14]). *Let K be a set in $\Sigma = \mathrm{PG}(k - 1, q)$, $k \geq 3$, $q = 2^h$, $h \geq 3$, meeting every line in exactly 1, $q/2 + 1$, or $q + 1$ points. Then, K contains a hyperplane of Σ.*

Now, we are ready to prove our results.

Proof of Theorem 2. For $q = 2^h$, $h \geq 3$, let $\mathcal{C}$ be an $[n, k, d]_q$ code with d odd whose weights are congruent to 0 or $d \pmod{q/2}$. For a generator matrix G of $\mathcal{C}$ and a line L in $\Sigma = \mathrm{PG}(k - 1, q)$, we have $w_G(L) = \sum_{P \in L} w_G(P) \equiv 0 \pmod{q}$ by Lemma 11. Let $\tilde{F_0} := \{Q \in \Sigma \mid w_G(Q) \text{ is even}\}$. Then, $\tilde{F_0} \cap F_d = \emptyset$. Assume that the t points on L have odd weights and that the other have even weights. Then, from the condition, we have $td \equiv 0 \pmod{q/2}$, so, $t \equiv 0 \pmod{q/2}$, for d is odd. Hence $t = 0, q/2$ or q. Thus, $|\tilde{F_0} \cap L| = 1, q/2 + 1$ or $q + 1$, and $\tilde{F_0}$

contains a hyperplane of Σ by Lemma 12. Hence our assertion follows from Lemma 7. $\square$

Proof of Theorem 3. For $q = 2^h$, $h \geq 3$, let $\mathcal{C}$ be an $[n,k,d]_q$ code with $\gcd(d,q) = 2$ whose weights are congruent to 0 or $d \pmod q$. For a generator matrix G of $\mathcal{C}$ and a line L in $\Sigma = \mathrm{PG}(k-1,q)$, we have $w_G(L) = \sum_{P\in L} w_G(P) \equiv 0 \pmod q$ by Lemma 11. Note that $\Sigma = F_0 \cup F_2$, $F_0 \cap F_2 = \emptyset$. Assume $|L \cap F_2| = t$. Then, from the condition, we have $td \equiv 0 \pmod q$, so, $t \equiv 0 \pmod{q/2}$, for $\gcd(d,q) = 2$. Hence $t = 0, q/2$ or q. Thus, $|F_0 \cap L| = 1, q/2+1$ or $q+1$, and F_0 contains a hyperplane of Σ by Lemma 12. Hence $\mathcal{C}$ is extendable by Lemma 8. $\square$

Proof of Theorem 5. For integers h,m,t with $0 \leq m < t \leq h$ and for $q = p^h$ with prime p, let $\mathcal{C}$ be an $[n,k,d]_q$ code with $\gcd(d,q) = p^m$ and assume $\sum_{i\equiv d \pmod{p^t}} A_i > q^k - q^{k-1} - r(q)q^{k-3}(q-1)$. For a generator matrix G of $\mathcal{C}$ and a line L in $\Sigma = \mathrm{PG}(k-1,q)$, we have $w_G(L) = \sum_{P\in L} w_G(P) \equiv 0 \pmod q$ by Lemma 11. Let $\bar{F_0} = \{Q \in \Sigma \mid w_G(Q) \not\equiv d \pmod{p^t}\}$ and $\bar{F_2} = \{Q \in \Sigma \mid w_G(Q) \equiv d \pmod{p^t}\}$. Then, $\bar{F_0} \cap F_d = \emptyset$ and $|\bar{F_0}| < \theta_{k-2} + r(q)q^{k-3}$. Suppose $L \subset \bar{F_2}$. Then, we have $d \equiv 0 \pmod{p^t}$, a contradiction. Thus $\bar{F_0}$ forms a blocking set w.r.t. lines in Σ. Hence $\bar{F_0}$ contains a hyperplane of Σ by Theorem 9, and $\mathcal{C}$ is extendable by Lemma 7. $\square$

Lemma 13 ([8])**.** *Let K be a proper subset of a t-flat Π_t in $\mathrm{PG}(k-1,q)$. If every line meets K in either one or $q+1$ points, then K is a hyperplane of Π_t.*

A t-flat Π of Σ with $|\Pi \cap F_0| = i$, $|\Pi \cap F_1| = j$ is called an *$(i,j)_t$ flat.* An $(i,j)_1$ flat is called an *(i,j)-line.* An *(i,j)-hyperplane* is an $(i,j)_{k-2}$ flat. Note that a $(1,1)$-line and a $(0,1)$-line do not exist by Lemma 11.

Proof of Theorem 6. It suffices to prove for the case $(\Phi_0,\Phi_1) = (\theta_{k-1} - 2q^{k-2}, q^{k-2})$. Let $\mathcal{C}$ be an $[n,k,d]_q$ code with diversity $(\Phi_0,\Phi_1) = (\theta_{k-1} - 2q^{k-2}, q^{k-2})$, $\gcd(d,q) = 1$, $k \geq 3$. Then, we have $|F_1| = |F_2| = q^{k-2}$. For $R \in F_2$, there exist at least θ_{k-3} lines through R containing no point of F_1, for $|F_1| = q^{k-2}$. Such lines are $(1,0)$-lines, for $\gcd(d,q) = 1$. Let $l_1, \cdots, l_{\theta_{k-3}}$ be such lines and let $H = \bigcup_{i=1}^{\theta_{k-3}} l_i$. Since $|F_2 \cap H| = (q-1)\theta_{k-3} + 1 = |F_2|$, we have $F_2 \subset H$. Hence, every line through two points of F_2 is a $(1,0)$-line. For $R_i \in l_i$ and $R_j \in l_j$ with $i \neq j$ and $R_i, R_j \neq R$, the line $l = \langle R_i, R_j\rangle$ is a $(1,0)$-line. Let P be the point of F_0 on l. If there exists a point of F_1 on the line $l_P = \langle R, P\rangle$, then there exists a $(1,1)$-line or a $(0,1)$-line on the plane $\langle l_i, l_j\rangle$, a contradiction. Hence l_P is also a $(1,0)$-line, and l is contained in H. It follows that H forms a hyperplane of $\Sigma = \mathrm{PG}(k-1,q)$. Since H contains only $(1,0)$-lines or $(q+1,0)$-lines, $H_0 = F_0 \cap H$ is a hyperplane of H by Lemma 13. Now, take a hyperplane H_1 through H_0 with $H_1 \neq H$. Then, it holds that $H_1 \subset F_0 \cup F_1$ since $F_2 = H \setminus H_0$. Hence $\mathcal{C}$ is extendable by Lemma 8. $\square$

References

[1] A. Beutelspacher, Blocking sets and partial spreads in finite projective spaces, *Geom. Dedicata,* **9**, 1980, 425-449.

[2] R. C. Bose, R. C. Burton, A characterization of flat spaces in a finite projective geometry and the uniqueness of the Hamming and the MacDonald codes, *J. Combin. Theory,* **1**, 1966, 96-104.

[3] I. Bouyukliev, M. Grassl, Z. Varbanov, New bounds for $n_4(k, d)$ and classification of some optimal codes over GF(4), *Discrete Math.,* **281**, 2004, 43-66.

[4] U. Heim, Blockierende Mengen in endlichen projektiven Räumen, *Mitt. Math. Sem. Giessen,* **226**, 1996.

[5] R. Hill, An extension theorem for linear codes, *Des. Codes Cryptogr.,* **17**, 1999, 151-157.

[6] R. Hill, P. Lizak, Extensions of linear codes, *Proc. IEEE Int. Symposium on Inform. Theory*, Whistler, Canada, 1995, p. 345.

[7] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Second edition, Clarendon Press, Oxford, 1998.

[8] T. Maruta, On the extendability of linear codes, *Finite Fields Appl.,* **7**, 2001, 350-354.

[9] T. Maruta, A new extension theorem for linear codes, *Finite Fields Appl.,* **10**, 2004, 674-685.

[10] T. Maruta, Extendability of ternary linear codes, *Des. Codes Cryptogr.,* **35**, 2005, 175-190.

[11] T. Maruta, Extendability of linear codes over $\mathbb{F}_q$, *Proc. 11th International Workshop on Algebraic and Combinatorial Coding Theory*, Pamporovo, Bulgaria, 2008, 203-209.

[12] T. Maruta, Extension theorems for linear codes over finite fields, *J. Geom.,* **101**, 2011, 173-183.

[13] J. Simonis, Adding a parity check bit, *IEEE Trans. Inform. Theory,* **46**, 2000, 1544-1545.

[14] Y. Yoshida, T. Maruta, An extension theorem for $[n, k, d]_q$ codes with $\gcd(d, q) = 2$, *Australas. J. Combin.,* **48**, 2010, 117-131.