Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 203-209*

Extendability of linear codes over $\mathbb{F}_q$

Tatsuya Maruta maruta@mi.s.osakafu-u.ac.jp
Department of Mathematics and Information Sciences,
Osaka Prefecture University, Sakai, Osaka 599-8531, JAPAN

Abstract. For an $[n,k,d]_q$ code $\mathcal{C}$, we define a mapping $w_{\mathcal{C}}$ from $\mathrm{PG}(k-1,q)$ to the set of weights of $\mathcal{C}$ via a generator matrix of $\mathcal{C}$. We give a geometric aspect derived from $w_{\mathcal{C}}$ to investigate the extendability of linear codes. We survey known extension theorems and some recent results.

1 Introduction

Let $\mathbb{F}_q^n$ denote the vector space of n-tuples over $\mathbb{F}_q$, the field of q elements. A linear code $\mathcal{C}$ of length n, dimension k and minimum (Hamming) distance d over $\mathbb{F}_q$ is referred to as an $[n,k,d]_q$ code. 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 also expressed as $0^1 d^\alpha \cdots$. We only consider *non-degenerate* codes 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 (l,s)-*extendable* (to $\mathcal{C}'$) if there exist l vectors $h_1, \dots, h_l \in \mathbb{F}_q^k$ such that the extended matrix $[G, h_1^{\mathrm{T}}, \cdots, h_l^{\mathrm{T}}]$ generates an $[n+l, k, d+s]_q$ code $\mathcal{C}'$ ([7]). Then $\mathcal{C}'$ is called an (l,s)-*extension* of $\mathcal{C}$. A $(1,1)$-extendable code is simply called *extendable*. The following is well-known.

Theorem 1.1. [1] *Every $[n,k,d]_2$ code with d odd is extendable.*

As for the (l,s)-extendability, the next theorem is known as 'Construction X'.

Theorem 1.2. [1] *Let $\mathcal{C}$ and $\mathcal{C}_0$ be an $[n,k,d]_q$ code and an $[n,k_0,d_0]_q$ code, respectively, such that $\mathcal{C} \supset \mathcal{C}_0$ and $d < d_0$. If there exists an $[l, k-k_0, d']_q$ code $\mathcal{C}'$, then $\mathcal{C}$ is (l,s)-extendable, where $s = \min\{d', d_0 - d\}$.*

Proof. We give an elementary proof using generator matrices. Take a generator matrix G of $\mathcal{C}$ with two submatrices G_0 and G_1 so that G_0 consisting of the first k_0 rows of G is a generator matrix of $\mathcal{C}_0$ and that the remaining $k-k_0$ rows of G form G_1. Let G' be a generator matrix of $\mathcal{C}'$. Then, the matrix $\left[\begin{array}{c|c} G_0 & O \\ \hline G_1 & G' \end{array}\right]$ generates an (l,s)-extension of $\mathcal{C}$, where O is the zero matrix. □

For example, every $[n, k, d]_2$ code with odd d contains an $[n, k-1, d_0]_2$ code with $d_0 > d$ as a subcode. It might be possible to find a suitable subcode $\mathcal{C}_0$ of $\mathcal{C}$ when $\mathcal{C}$ is a BCH code, but It is not easy to find such a subcode for an arbitrary linear code $\mathcal{C}$ in general. We sometimes need to know the minimum l so that $\mathcal{C}$ is $(l, 1)$-extendable.

Problem 1. Find easily checkable conditions to see whether a given $[n, k, d]_q$ code is $(l, 1)$-extendable or not.

The aim of this paper is to give a geometric aspect to investigate the $(l, 1)$-extendability of linear codes and survey known extension theorems with some applications mainly for $l = 1$.

2 A geometric approach

We assume that $k \geq 3$, see [9] for $k = 1, 2$. Let $\mathcal{C}$ be an $[n, k, d]_q$ code with a generator matrix $G = [g_{ij}] = [g_1, \cdots, g_k]^{\mathrm{T}}$. Put $\Sigma =$PG$(k-1, q)$, the projective space of dimension $k-1$ over $\mathbb{F}_q$. We consider the mapping $w_{\mathcal{C}}$ from Σ to $\{i \mid A_i > 0\}$, the set of weights of $\mathcal{C}$. For $P = \mathbf{P}(p_1, \ldots, p_k) \in \Sigma$ we define *the weight of P with respect to $\mathcal{C}$*, denoted by $w_{\mathcal{C}}(P)$, as

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

Let $F_d = \{P \in \Sigma \mid w_{\mathcal{C}}(P) = d\}$. Recall that a hyperplane H of Σ is defined by a non-zero vector $h = (h_0, \ldots, h_{k-1}) \in \mathbb{F}_q^k$ as $H = \{P = \mathbf{P}(p_0, \ldots, p_{k-1}) \in \Sigma \mid h_0 p_0 + \cdots + h_{k-1} p_{k-1} = 0\}$. h is called the *defining vector of H*.

Lemma 2.1. *$\mathcal{C}$ 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 the defining vector of H as a column generates an extension of $\mathcal{C}$.*

Proof. For an $[n, k, d]_q$ code $\mathcal{C}$ with a generator matrix G, there exists a vector $h = (h_0, \ldots, h_{k-1}) \in \mathbb{F}_q^k$ such that $[G, h^{\mathrm{T}}]$ generates an $[n+1, k, d+1]_q$ code if and only if $\sum_{i=0}^{k-1} h_i p_i \neq 0$ holds for all $P = \mathbf{P}(p_0, \ldots, p_{k-1}) \in F_d$. Equivalently, there exists a hyperplane H with defining vector h such that $F_d \cap H = \emptyset$. $\square$

The above lemma can be easily generalized to the $(l, 1)$-extendability.

Theorem 2.2. *$\mathcal{C}$ is $(l, 1)$-extendable if and only if there exist l hyperplanes $H_1, \ldots, H_l$ of Σ such that $F_d \cap H_1 \cap \cdots \cap H_l = \emptyset$. Equivalently, there exists a $(k-1-l)$-flat Π with $F_d \cap \Pi = \emptyset$.*

Lemma 2.3. [3] *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 2.3, we get the following.

Lemma 2.4. *For a line $L = \{P_0, P_1, \cdots, P_q\}$ in Σ, it holds that*

$$\sum_{i=0}^{q} w_{\mathcal{C}}(P_i) \equiv 0 \pmod{q}.$$

Now, let

$$\begin{aligned} F_0 &= \{P \in \Sigma \mid w_{\mathcal{C}}(P) \equiv 0 \pmod{q}\}, \\ \bar{F}_d &= \{P \in \Sigma \mid w_{\mathcal{C}}(P) \equiv d \pmod{q}\}, \quad F = \Sigma \setminus \bar{F}_d. \end{aligned}$$

The mapping $w_{\mathcal{C}}$ is *trivial* if $F = \emptyset$. For example, $w_{\mathcal{C}}$ is trivial if $\mathcal{C}$ attains the Griesmer bound and if $q|d$ when q is prime [17]. To avoid such cases we assume that $\gcd(d, q) = 1$. Then we have $F_0 \subset F$. If $\bar{F}_d$ contains a line L of Σ, then we have $d \equiv 0 \pmod{q}$ by Lemma 2.4, a contradiction. Hence we get the following.

Lemma 2.5. *F forms a blocking set with respect to lines in Σ if $\gcd(d, q) = 1$.*

Most of the known extension theorems presented in the next section can be proved by showing that F contains a hyperplane of Σ.

3 Extension theorems and their applications

A q-ary linear code $\mathcal{C}$ is w-*weight* (*mod* q) if there exists a w-set $W = \{i_1, \ldots, i_w\} \subset \mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ such that $A_i > 0$ implies $i \equiv i_j \pmod{q}$ for some $i_j \in W$. The condition 'd is odd' in Theorem 1.1 would be replaced by '$\gcd(d, q) = 1$' for general q. But this is not enough for $q > 2$. In this section, we assume that $\mathcal{C}$ is an $[n, k, d]_q$ code with $k \geq 3$ and $\gcd(d, q) = 1$. As a solution of Problem 1, Hill & Lizak showed the following for 2-weight (mod q) codes.

Theorem 3.1. [3],[4] *Every $[n, k, d]_q$ code with $\gcd(d, q) = 1$ whose weights (i's such that $A_i > 0$) are congruent to 0 or d $\pmod{q}$ is extendable.*

Most of the cases one can apply Theorem 3.1 for $q > 3$ are when $d \equiv -1 \pmod{q}$.

Corollary 3.2. *Every $[n, k, d]_q$ code with $d \equiv -1 \pmod{q}$ whose weights are congruent to 0 or -1 $\pmod{q}$ is extendable.*

The following is the first extension theorem for 3-weight (mod q) codes.

Theorem 3.3. [11] *Every* $[n,k,d]_q$ *code with odd* $q \geq 5$, $d \equiv -2 \pmod q$ *whose weights are congruent to* 0, -1 *or* $-2 \pmod q$ *is extendable.*

Throughout this section, we define the *diversity* of $\mathcal{C}$ as the pair (Φ_0, Φ_1) with

$$\Phi_0 = |F_0| = \frac{1}{q-1}\sum_{q|i, i>0} A_i, \quad \Phi_1 = |F \setminus F_0| = \frac{1}{q-1}\sum_{i \not\equiv 0, d \pmod q} A_i.$$

Theorem 3.4. [8] *Every* $[n,k,d]_q$ *code with* $gcd(d,q) = 1$ *is extendable if*

$$\Phi_1 \leq q^{k-3}(s(q) - q - 1)/(q-1)$$

where $s(q)$ *is the smallest size of a nontrivial blocking set in* $PG(2,q)$.

Theorem 3.5. [12] *Let* $\mathcal{C}$ *be an* $[n,k,d]_3$ *code with diversity* (Φ_0, Φ_1), $gcd(3,d) = 1$, $k \geq 3$. *Then* $\mathcal{C}$ *is extendable if one of the following conditions holds:*
(1) $\Phi_0 = \theta_{k-3}$, (2) $\Phi_1 = 0$, (3) $\Phi_0 + \Phi_1 < \theta_{k-2} + 3^{k-2}$,
(4) $\Phi_0 + \Phi_1 \geq \theta_{k-2} + 2 \cdot 3^{k-2}$, (5) $2\Phi_0 + \Phi_1 \leq 2\theta_{k-2}$,
where $\theta_j = (3^{j+1} - 1)/2$.

Theorem 3.6. [12] *Let* $\mathcal{C}$ *be an* $[n,k,d]_3$ *code with diversity* (Φ_0, Φ_1), $d \equiv 1 \pmod 3$, $k \geq 3$. *Then* $\mathcal{C}$ *is* $(2,2)$*-extendable if*

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

The condition (3) of Theorem 3.5 is generalized for other q as follows.

Theorem 3.7. [10] *Let* $\mathcal{C}$ *be an* $[n,k,d]_q$ *code with* $gcd(d,q) = 1$, $q = p^h$, p *prime. Then* $\mathcal{C}$ *is extendable if*

$$\sum_{i \not\equiv d \pmod p} A_i < q^{k-2}(2q-1)$$

and if one of the following conditions holds:
(1) $h = 1$ (*i.e.* q *is prime*),
(2) $q = 4$,
(3) $h = 2$ *with* $n \equiv 0 \pmod p$, $d \equiv -1 \pmod p$,
(4) $h = 2$ *with* $n \equiv d \equiv 1 \pmod p$ *and* $A_i = 0$ *for all* $i \equiv d \pmod p$ *with* $i \not\equiv n \pmod q$.

Theorem 3.7 for $q = 4$ was first found by Simonis [16]. When $h \geq 3$, the following result is known.

Theorem 3.8. [10] *Let $\mathcal{C}$ be an $[n,k,d]_q$ code with $gcd(d,q) = 1$, $q = p^h$, p prime, $h \geq 3$. Then $\mathcal{C}$ is extendable if*

$$\sum_{i \not\equiv d (\text{mod } p^{h-1})} A_i < q^{k-2}(2q-1).$$

Theorem 3.5 (except for the condition (4)) can be generalized as follows.

Theorem 3.9. [14] *Let $\mathcal{C}$ be an $[n,k,d]_q$ code with diversity (Φ_0, Φ_1), $k \geq 3$, $d \equiv -1 \pmod q$, q odd, whose weights are congruent to 0 or $\pm 1 \pmod q$. Then $\mathcal{C}$ is extendable if one of the following conditions holds:*
(1) $\Phi_0 = \theta_{k-3}$, (2) $\Phi_1 = 0$,
(3) $\Phi_0 + \Phi_1 \geq \theta_{k-2} + \alpha q^{k-2}$, (4) $\alpha\Phi_0 + \Phi_1 \leq \alpha\theta_{k-2}$,
where $\theta_j = (q^{j+1}-1)/(q-1)$, $\alpha = \theta_1/2$.

When (Φ_0, Φ_1) is none of the types in Theorem 3.9(1), we need more information about $\mathcal{C}$.

Theorem 3.10. [14] *Let $\mathcal{C}$ be an $[n,k,d]_q$ code with diversity (Φ_0, Φ_1), $k \geq 3$, $d \equiv -1 \pmod q$, q odd, whose weights are congruent to 0 or $\pm 1 \pmod q$. Then $\mathcal{C}$ is not extendable if (Φ_0, Φ_1) satisfies none of the criteria of Theorem 3.9 and if*

$$\sum_{d < i \equiv d \pmod q} A_i < \frac{(q-1)^2 q^{k-3}}{2}. \tag{3.1}$$

As for even q, the following theorem can be proved.

Theorem 3.11. [14] *Let $\mathcal{C}$ be an $[n,k,d]_q$ code with q even, $d \equiv -1 \pmod q$, whose weights are congruent to 0 or $\pm 1 \pmod q$, $k \geq 3$. Then $\mathcal{C}$ is extendable.*

Extension theorems can be applied to find new codes from old ones or to prove the nonexistence of codes with certain parameters. For example, we demonstrate the nonexistence of $[245,5,183]_4$ codes. For a putative $[245,5,183]_4$ code $\mathcal{C}_1$, considering the residual codes (see Theorem 2.7.1 in [6]) yields that $A_i = 0$ for all $i \notin \{0,183,184,196,228,244,245\}$. Applying Theorem 3.11, $\mathcal{C}_1$ is extendable, which contradicts that a $[246,5,184]_4$ code does not exist. See also [15] for the extendability of quaternary linear codes.

Next, we give a typical example one can apply Theorems 3.10 and 3.11. Let $\mathcal{C}_2$ be a $[q+1,3,q-1]_q$ code, which is MDS (see [6]) and has the unique weight distribution

$$0^1(q-1)^{(q+1)q(q-1)/2}q^{q^2-1}(q+1)^{q(q-1)^2/2}.$$

So, the weights of $\mathcal{C}_2$ are congruent to 0 or $\pm 1 \pmod q$ and its diversity $(\theta_1, q(q-1)/2)$ satisfies none of the conditions of Theorem 3.9. When q is odd, $\mathcal{C}_2$ is not extendable by Theorem 3.10 since the left hand side of (3.1) is 0. This fact is known as the completeness of $(q+1)$-arcs in PG(2,q) for q odd, see [5]. On the other hand, it is also known that $\mathcal{C}_2$ is extendable when q is even, as guaranteed by Theorem 3.11. The inequality (3.1) could be slightly improved according to diversities just as for the case when $q = 3$ ([12],[13]).

As for other types of 3-weight (mod q) codes, Cheon and Maruta recently proved the following.

Theorem 3.12. [2] *Let $\mathcal{C}$ be an $[n,k,d]_q$ code with even $q \geq 4$, $k \geq 3$, whose weights are congruent to $0, -1$ or $-2 \pmod q$ and $d \equiv -1 \pmod q$. Then $\mathcal{C}$ is extendable.*

Theorem 3.13. [2] *Let $\mathcal{C}$ be an $[n,k,d]_q$ code with odd $q \geq 5$, $k \geq 3$, whose weights are congruent to $0, -1$ or $-2 \pmod q$ and $d \equiv -1 \pmod q$. Then $\mathcal{C}$ is extendable if $(\Phi_0, \Phi_1) \neq (\binom{q}{2}q^{k-3} + \theta_{k-3}, \binom{q}{2}q^{k-3})$.*

Problem 2. Find a new extension theorem for 4-weight (mod q) codes.

References

[1] J. Bierbrauer, *Introduction to Coding Theory*, Chapman & Hall/CRC, 2005.

[2] E.J. Cheon, T. Maruta, A new extension theorem for 3-weight modulo q linear codes over $\mathbb{F}_q$, in preparation.

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

[4] R. Hill, P. Lizak, Extensions of linear codes, *Proc. IEEE Intern. Symp. Inform. Theory*, Whistler, Canada, 1995.

[5] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed., Clarendon Press, Oxford, 1998.

[6] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[7] A. Kohnert, (l,s)-extension of linear codes, *Discr. Math.*, to appear.

[8] I. Landjev, A. Rousseva, An extension theorem for arcs and linear codes, *Probl. Inform. Transm.* 42, 2006, 319-329.

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

[10] T. Maruta, Extendability of linear codes over GF(q) with minimum distance d, $\gcd(d,q) = 1$, *Discr. Math.* 266, 2003, 377-385.

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

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

[13] T. Maruta, K. Okamoto, Some improvements to the extendability of ternary linear codes, *Fin. Fields Their Appl.* 13, 2007, 259-280.

[14] T. Maruta, K. Okamoto, Extendability of 3-weight (mod q) linear codes over $\mathbb{F}_q$, submitted.

[15] T. Maruta, M. Takeda, K. Kawakami, New sufficient conditions for the extendability of quaternary linear codes, *Fin. Fields Their Appl.*, to appear.

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

[17] H.N. Ward, Divisibility of codes meeting the Griesmer bound, —it J. Combin. Theory Ser. A 83, 1998, 79-93.