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 $C$, we define a mapping $w_C$ from $\text{PG}(k-1, q)$ to the set of weights of $C$ via a generator matrix of $C$. We give a geometric aspect derived from $w_C$ 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 $C$ 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 $x \in \mathbb{F}_q^n$, denoted by $\text{wt}(x)$, is the number of nonzero coordinate positions in $x$. The weight distribution of $C$ is the list of numbers $A_i$ which is the number of codewords of $C$ with weight $i$. The weight distribution with $(A_0, A_d, \ldots) = (1, \alpha, \ldots)$ is also expressed as $0^1 \alpha^d \cdot \ldots$. We only consider non-degenerate codes having no coordinate which is identically zero.

For an $[n, k, d]_q$ code $C$ with a generator matrix $G$, $C$ is called $(l, s)$-extendable (to $C'$) if there exist $l$ vectors $h_1, \ldots, h_l \in \mathbb{F}_q^k$ such that the extended matrix $[G, h_1^T, \ldots, h_l^T]$ generates an $[n+l, k, d+s]_q$ code $C'$ ([7]). Then $C'$ is called an $(l, s)$-extension of $C$. 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 $C$ and $C_0$ be an $[n, k, d]_q$ code and an $[n, k_0, d_0]_q$ code, respectively, such that $C \supset C_0$ and $d < d_0$. If there exists an $[l, k - k_0, d']_q$ code $C'$, then $C$ 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 $C$ 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 $C_0$ and that the remaining $k - k_0$ rows of $G$ form $G_1$. Let $G'$ be a generator matrix of $C'$. Then, the matrix $\begin{bmatrix} G_0 & O \\ G_1 & G' \end{bmatrix}$ generates an $(l, s)$-extension of $C$, 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 \(C_0\) of \(C\) when \(C\) is a BCH code, but it is not easy to find such a subcode for an arbitrary linear code \(C\) in general. We sometimes need to know the minimum \(l\) so that \(C\) 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 \(C\) be an \([n, k, d]_q\) code with a generator matrix \(G = [g_{ij}] = [g_1, \ldots, g_k]^T\). Put \(\Sigma = \text{PG}(k-1, q)\), the projective space of dimension \(k-1\) over \(\mathbb{F}_q\). We consider the mapping \(w_C\) from \(\Sigma\) to \(\{i \mid A_i > 0\}\), the set of weights of \(C\). For \(P = P(p_1, \ldots, p_k) \in \Sigma\) we define the weight of \(P\) with respect to \(C\), denoted by \(w_C(P)\), as

\[
 w_C(P) = |\{j \mid \sum_{i=1}^{k} g_{ij}p_i \neq 0\}| = \text{wt}\left(\sum_{i=1}^{k} p_i g_i\right).
\]

Let \(F_d = \{P \in \Sigma \mid w_C(P) = d\}\). Recall that a hyperplane \(H\) of \(\Sigma\) is defined by a non-zero vector \(h = (h_0, \ldots, h_{k-1}) \in \mathbb{F}_q^k\) as \(H = \{P = P(p_0, \ldots, p_{k-1}) \in \Sigma \mid h_0p_0 + \cdots + h_{k-1}p_{k-1} = 0\}\). \(h\) is called the defining vector of \(H\).

**Lemma 2.1.** \(C\) is extendable if and only if there exists a hyperplane \(H\) of \(\Sigma\) 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 \(C\).

**Proof.** For an \([n, k, d]_q\) code \(C\) with a generator matrix \(G\), there exists a vector \(h = (h_0, \ldots, h_{k-1}) \in \mathbb{F}_q^k\) such that \([G, h^T]\) generates an \([n+1, k, d+1]_q\) code if and only if \(\sum_{i=0}^{k-1} h_ip_i \neq 0\) holds for all \(P = P(p_0, \ldots, p_{k-1}) \in F_d\). 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.** \(C\) is \((l, 1)\)-extendable if and only if there exist \(l\) hyperplanes \(H_1, \ldots, H_l\) of \(\Sigma\) such that \(F_d \cap H_1 \cap \cdots \cap H_l = \emptyset\). Equivalently, there exists a \((k-1-l)\)-flat \(\Pi\) with \(F_d \cap \Pi = \emptyset\).
Lemma 2.3. [3] For two linearly independent vectors \( \mathbf{a}_1, \mathbf{a}_2 \in \mathbb{F}_q^n \), it holds that
\[
\sum_{\lambda \in \mathbb{F}_q} \text{wt}(\mathbf{a}_1 + \lambda \mathbf{a}_2) + \text{wt}(\mathbf{a}_2) \equiv 0 \pmod{q}.
\]

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 \( \Sigma \), it holds that
\[
\sum_{i=0}^{q} w_C(P_i) \equiv 0 \pmod{q}.
\]

Now, let
\[
F_0 = \{ P \in \Sigma \mid w_C(P) \equiv 0 \pmod{q}\},
\]
\[
F_d = \{ P \in \Sigma \mid w_C(P) \equiv d \pmod{q}\}, \quad F = \Sigma \setminus F_d.
\]
The mapping \( w_C \) is trivial if \( F = \emptyset \). For example, \( w_C \) is trivial if \( C \) attains the Griesmer bound and if \( q \mid d \) when \( q \) is prime [17]. To avoid such cases we assume that \( \gcd(d, q) = 1 \). Then we have \( F_0 \subset F \). If \( F_d \) contains a line \( L \) of \( \Sigma \), 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 \( \Sigma \) 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 \( \Sigma \).

3 Extension theorems and their applications

A \( q \)-ary linear code \( C \) is \( w \)-weight \( (\pmod q) \) 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 \( C \) 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 \( (\pmod{q}) \) codes.

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

Throughout this section, we define the diversity of \(C\) as the pair \((\Phi_0, \Phi_1)\) with

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

**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 \(C\) be an \([n, k, d]_3\) code with diversity \((\Phi_0, \Phi_1)\), \(\gcd(3, d) = 1, k \geq 3\). Then \(C\) 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 \(C\) be an \([n, k, d]_3\) code with diversity \((\Phi_0, \Phi_1)\), \(d \equiv 1 \pmod 3, k \geq 3\). Then \(C\) 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 \(C\) be an \([n, k, d]_q\) code with \(\gcd(d, q) = 1, q = p^h, p\) prime. Then \(C\) 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 $C$ be an $[n, k, d]_q$ code with $\gcd(d, q) = 1$, $q = p^h$, $p$ prime, $h \geq 3$. Then $C$ is extendable if

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

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

Theorem 3.9. [14] Let $C$ be an $[n, k, d]_q$ code with diversity $(\Phi_0, \Phi_1)$, $k \geq 3$, $d \equiv -1 \pmod{q}$, $q$ odd, whose weights are congruent to $0$ or $\pm 1 \pmod{q}$. Then $C$ 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 $(\Phi_0, \Phi_1)$ is none of the types in Theorem 3.9(1), we need more information about $C$.

Theorem 3.10. [14] Let $C$ be an $[n, k, d]_q$ code with diversity $(\Phi_0, \Phi_1)$, $k \geq 3$, $d \equiv -1 \pmod{q}$, $q$ odd, whose weights are congruent to $0$ or $\pm 1 \pmod{q}$. Then $C$ is not extendable if $(\Phi_0, \Phi_1)$ satisfies none of the criteria of Theorem 3.9 and if

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

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

Theorem 3.11. [14] Let $C$ 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 $C$ 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 $C_1$, 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, $C_1$ 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 $C_2$ be a $[q + 1, 3, q - 1]_q$ code, which is MDS (see [6]) and has the unique weight distribution

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

So, the weights of $C_2$ 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, $C_2$ 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 \(C_2\) 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 \(C\) be an \([n,k,d]_q\) code with even \(q \geq 4\), \(k \geq 3\), whose weights are congruent to 0, \(-1\) or \(-2\) (mod \(q\)) and \(d \equiv -1\) (mod \(q\)). Then \(C\) is extendable.

**Theorem 3.13.** [2] Let \(C\) be an \([n,k,d]_q\) code with odd \(q \geq 5\), \(k \geq 3\), whose weights are congruent to 0, \(-1\) or \(-2\) (mod \(q\)) and \(d \equiv -1\) (mod \(q\)). Then \(C\) 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**


