Extendability of Linear Codes over $\mathbb{F}_q$

Tatsuya Maruta

Department of Mathematics
and Information Sciences
Osaka Prefecture University
Overview

- Known extension theorems and recent results are surveyed.
- A geometric method to investigate the $(l, 1)$-extendability of $[n, k, d]_q$ codes with $\gcd(d, q) = 1$ is presented.
Contents

1. Linear codes over $\mathbb{F}_q$
2. $(l, s)$-extendability of linear codes
3. Extension theorems
4. Geometric approach
1. Linear codes over $\mathbb{F}_q$

$\mathbb{F}_q^n = \{(a_1, a_2, ..., a_n) \mid a_1, ..., a_n \in \mathbb{F}_q\}$.

An $[n, k, d]_q$ code $C$ means a $k$-dimensional subspace of $\mathbb{F}_q^n$ with minimum distance $d$,

$$d = \min\{wt(a) \mid wt(a) \neq 0, \ a \in C\}.$$

We only consider non-degenerate codes (i.e. $\mathbb{F}_i \ ; \ c_i = 0$ for all $c = (c_1, ..., c_n) \in C$).
The weight distribution of $\mathcal{C}$ is the list of numbers $A_i = |\{c \in \mathcal{C} | \text{wt}(c) = i\}|$.

The weight distribution with

$$(A_0, A_d, \ldots, A_i, \ldots) = (1, \alpha, \ldots, w, \ldots)$$

is also expressed as

$$0^1 d^\alpha \ldots i^w \ldots.$$
A linear code $\mathcal{C}$ over $\mathbb{F}_q$ is $w$-weight (mod $q$) if

$\exists W = \{i_1, \cdots, i_w\} \subset \mathbb{Z}_q = \{0, 1, \cdots, q - 1\}$

s.t.

$A_i > 0 \implies i \equiv i_j \pmod{q}$ for some $i_j \in W$
Ex. The Golay $[11, 6, 5]_3$ code with a generator matrix

\[
G_1 = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 \\
0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 1 & 2 \\
0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 0 \\
\end{bmatrix}
\]

has weight distribution $0^{15}1^{32}2^61^{32}83^{30}91^{10}0^{11}2^{24}$, which is 2-weight (mod 3).
Ex. There exists a $[601, 5, 479]_5$ code with weight distribution

$0^1479^{10}40^480^520^481^{1000}484^{40}485^{100}489^{40}600^4$

which is 3-weight (mod 5) since

$A_i > 0 \Rightarrow i \equiv -1, 0, 1 \pmod{5}$. 
2. \((l, s)\)-extendability of linear codes

For an \([n, k, d]_q\) code \(C\) with a generator matrix \(G\), \(C\) is \((l, s)\)-extendable if \([G, h_1, \cdots, h_l]\) generates an \([n + l, k, d + s]_q\) code \(C'\) for some column vectors \(h_i, h_i^\top \in \mathbb{F}^k_q\). \(C'\) is an \((l, s)\)-extension of \(C\).

A \((1, 1)\)-extendable code is simply called extendable.
**Thm 1.** Every binary code with odd minimum distance is extendable.

**Note.** For an \([n, k, d]_q\) code \(C\), there is another type of extension called *extension up to dimension*, which is to find an \([n + l, k + s, d]_q\) code from \(C\). Here, we only consider *extension up to length* to find an \([n + l, k, d + s]_q\) code from \(C\).
As for the \((l, s)\)-extendability, the next is well known.

**Thm 2 (Construction X).**

\(C: [n, k, d]_q\) code, \(C_0: [n, k_0, d_0]_q\) code

\(C_0 \subset C, \ d < d_0,\)

\(C': [l, k - k_0, d']_q\) code, \(s = \min\{d', d_0 - d\}\)

\(\Rightarrow C\) is \((l, s)\)-extendable.
It is not easy to find a suitable subcode $C_0$ of a given $[n, k, d]_q$ code $C$ to apply Thm 2.

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

Theorems giving answers to this problem are called extension theorems.
The condition “$d$ is odd” for binary codes will be replaced by “gcd($d, q$) = 1” for $q$-ary linear codes.
But this is not sufficient for the extendability of $C$.
We assume $k \geq 3$ to avoid the trivial cases.
We also assume gcd($d, q$) = 1.
3. Extension theorems

**Thm 3** (Hill & Lizak 1995).
Let $C$ be an $[n, k, d]_q$ code with $\gcd(d, q) = 1$ s.t. $i \equiv 0$ or $d \pmod{q}$ for $\forall i$ with $A_i > 0$. Then $C$ is extendable.

**Cor.**

$C$: an $[n, k, d]_q$ code with $d \equiv -1 \pmod{q}$. Then $C$ is extendable if

$$A_i > 0 \Rightarrow i \equiv 0 \text{ or } -1 \pmod{q}$$
For 3-weight (mod $q$) codes, the following is known:

**Thm 4 (Maruta 2004).**

Let $C$ be an $[n, k, d]_q$ code with odd $q \geq 5$, $d \equiv -2 \pmod{q}$. Then $C$ is extendable if

$$A_i > 0 \Rightarrow i \equiv 0, -1, -2 \pmod{q}$$

Non-existence of $[205, 4, 163]_5$, $[105, 4, 83]_5$ was proved by Landjev et al. (2003) using Thm 4.
We define the diversity of $\mathcal{C}$ as the pair $(\Phi_0, \Phi_1)$ with

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

Note.

$\mathcal{C}$ is extendable if $\Phi_1 = 0$ by Thm 3.
**Thm 5** (Landjev & Rousseva, 2006).
Every $[n, k, d]_q$ code with $\gcd(d, q) = 1$ is extendable if

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

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

**Cor.** Every $[n, k, d]_3$ code with $d \equiv 1$ or $2 \pmod{3}$ is extendable if $\Phi_1 < 3^{k-3}$. 
Thm 6 (Maruta, 2001).

\( \mathcal{C} \): \([n, k, d]_3 \) code with diversity \((\Phi_0, \Phi_1)\), \(\gcd(3, d) = 1, k \geq 3\). 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 \( \theta_j = (3^{j+1} - 1)/2 \).
All possible diversities of \([n, k, d]_3\) codes are found by Maruta & Okamoto(2007), and the condition \(\Phi_1 < 3^{k-3}\) in Cor of Thm 5 can be improved as follows.

**Thm 7.** An \([n, k, d]_3\) code with diversity \((\Phi_0, \Phi_1)\), \(\gcd(3, d) = 1\), \(k \geq 3\), is extendable if \(\Phi_1 < 3^{k-2}\) or \(\Phi_1 > \theta_{k-2} + \theta_{k-4} + 1\).
**Thm 6** (Maruta, 2001).

\( \mathcal{C} : [n, k, d]_3 \) code with diversity \((\Phi_0, \Phi_1)\), \( \gcd(3, d) = 1, \ k \geq 3 \). 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 \( \theta_j = (3^{j+1} - 1)/2 \).
The condition (3) of Thm 6 is generalized for prime $q$ as follows.

**Thm 8** (Maruta, 2003).

$C$: $[n, k, d]_q$ code with $\gcd(d, q) = 1$, $q$ prime. Then $C$ is extendable if

$$\Phi_0 + \Phi_1 < \theta_{k-2} + q^{k-2}.$$ 

Similar results are known for non-prime $q$, see Theorems 3.7 and 3.8 in the Proceedings.
**Thm 6** (Maruta, 2001).

$\mathcal{C}$: $[n, k, d]_3$ code with diversity $(\Phi_0, \Phi_1)$, $\gcd(3, d) = 1$, $k \geq 3$. 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 $\theta_j = (3^{j+1} - 1)/2$. 
**Thm 9** (Maruta & Okamoto).

$C$: $[n, k, d]_q$ code with diversity $(\Phi_0, \Phi_1)$,

$k \geq 3$, $d \equiv -1 \pmod{q}$, $q$ odd, s.t.

$$A_i > 0 \Rightarrow i \equiv 0 \text{ or } \pm 1 \pmod{q}.$$

Then $C$ is extendable if one of (1)-(4) 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 $\theta_j = (q^{j+1} - 1)/(q - 1)$, $\alpha = \theta_1/2$. 
**Thm 10** (Maruta & Okamoto).

\( \mathcal{C} \): \([n, k, d]_q\) code with diversity \((\Phi_0, \Phi_1)\),

- \(k \geq 3\), \(d \equiv -1 \pmod{q}\), \(q\) odd, s.t.

  \[
  A_i > 0 \implies i \equiv 0 \text{ or } \pm 1 \pmod{q}.
  \]

Then \(\mathcal{C}\) is not extendable if \((\Phi_0, \Phi_1)\) satisfies none of the conditions of Thm 9 and if

\[
\sum_{d < i \equiv d \pmod{q}} A_i < \frac{(q - 1)^2q^{k-3}}{2}.
\]
Thm 11 (Maruta & Okamoto).

$C: [n, k, d]_q$ code with $q$ even, $k \geq 3$, $d \equiv -1 \pmod{q}$, s.t.

$$A_i > 0 \Rightarrow i \equiv 0 \text{ or } \pm 1 \pmod{q}.$$ 

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 yields that
$A_i > 0 \Rightarrow i \in \{0, 183, 184, 196, 228, 244, 245\}$
i.e. $A_i > 0 \Rightarrow i \equiv 0$ or $\pm 1 \pmod{4}$.
Applying Thm 11, $C_1$ is extendable, which
contradicts that a $[246, 5, 184]_4$ code does not exist.
Let $C_2$ be a $[q + 1, 3, q - 1]_q$ code, which is MDS and has the unique weight distribution

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

So, $A_i > 0 \Rightarrow i \equiv 0$ or $\pm 1$ (mod $q$), and its diversity $(\theta_1, q(q - 1)/2)$ satisfies none of the conditions of Thm 9. So, by Thms 10, 11, $C_2$ is not extendable when $q$ is odd, but $C_2$ is extendable when $q$ is even.
Recent results for another type of 3-weight \((\text{mod } q)\) codes by Cheon & Maruta:

**Thm 12.** Let \(C\) be an \([n, k, d]_q\) code with \(q \geq 4, d \equiv -1 \pmod{q}\) 
s.t. \(A_i > 0 \Rightarrow i \equiv 0 \text{ or } -1 \text{ or } -2 \pmod{q}\). 
Then \(C\) is extendable unless \(q\) is odd and 
\[
(\Phi_0, \Phi_1) = \left(\binom{q}{2}q^{k-3} + \theta_{k-3}, \binom{q}{2}q^{k-3}\right).
\]
5. Geometric approach

\( \mathcal{C}: [n, k, d]_q \) code, \( k \geq 3 \)

\( G = [g_1, \ldots, g_k]^T \): a generator matrix of \( \mathcal{C} \)

\( \Sigma := \text{PG}(k-1, q) \): the projective space of dimension \( k-1 \) over \( \mathbb{F}_q \)

For \( P = P(p_1, \ldots, p_k) \in \Sigma \) we define the weight of \( P \) with respect to \( \mathcal{C} \), denoted by \( w_{\mathcal{C}}(P) \), as

\[
w_{\mathcal{C}}(P) = \text{wt}(p_1g_1 + \cdots + p_kg_k).
\]
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

$$H = \{ P = P(p_0, \ldots, p_{k-1}) \in \Sigma \mid \quad h_0p_0 + \cdots + h_{k-1}p_{k-1} = 0 \}. $$

$h$ is called a defining vector of $H$.

Let $F_d = \{ P \in \Sigma \mid w_C(P) = d \}$. 

Lemma 13. \( C \) is extendable \( \iff \) there exists a hyperplane \( H \) of \( \Sigma \) s.t. \( F_d \cap H = \emptyset \).
Moreover, \([G, h]\) generates an extension of \( C \), where \( h^T \in \mathbb{F}_q^k \) is a defining vector of \( H \).
Lemma 13. \( C \) is extendable \( \iff \) there exists a hyperplane \( H \) of \( \Sigma \) s.t. \( F_d \cap H = \emptyset \).

Moreover, \([G, h]\) generates an extension of \( C \), where \( h^\top \in \mathbb{F}_q^k \) is a defining vector of \( H \).

Proof. \( C \) is extendable
\[
\Leftrightarrow \exists h = (h_0, \ldots, h_{k-1}) \in \mathbb{F}_q^k \text{ s.t. } [G, h^\top] \text{ generates an } [n+1, k, d+1]_q \text{ code}
\Leftrightarrow \sum_{i=0}^{k-1} h_i p_i \neq 0 \text{ for } \forall P = P(p_0, \ldots, p_{k-1}) \in F_d
\Leftrightarrow \exists H: \text{ a hyperplane with a defining vector } h \text{ s.t. } F_d \cap H = \emptyset.
\] \( \square \)
The above lemma can be easily generalized to the \((l, 1)\)-extendability.

**Thm 14.** \(\mathcal{C}\) is \((l, 1)\)-extendable

\(\iff\) there exist \(l\) hyperplanes \(H_1, \ldots, H_l\) of \(\Sigma\) s.t. \(F_d \cap H_1 \cap \cdots \cap H_l = \emptyset\).

\(\iff\) \(\exists (k - 1 - l)\)-flat \(\mathcal{\Pi}\) with \(F_d \cap \mathcal{\Pi} = \emptyset\).

E.g. \(\mathcal{C}\) is \((2, 1)\)-extendable

\(\iff\) \(\exists (k - 3)\)-flat \(\mathcal{\Pi}\) with \(F_d \cap \mathcal{\Pi} = \emptyset\).
Now, let

\[
F_0 = \{ P \in \Sigma \mid w_c(P) \equiv 0 \pmod{q} \}, \\
F_1 = \{ P \in \Sigma \mid w_c(P) \not\equiv 0, d \pmod{q} \}, \\
F = F_0 \cup F_1.
\]

**Note.** \((\Phi_0, \Phi_1) = (|F_0|, |F_1|)\).

**Lemma 15.** \(F\) forms a blocking set with respect to lines in \(\Sigma\) if \(\gcd(d, q) = 1\).
Note. If $C$ is divisible by $q$, then $F_0 = \Sigma$. There is no way to deal with theoretically for such codes except computer search, e.g. Q-extension. So, we assume $\gcd(d, q) = 1$.

Lemma 16. $C$ is $(l, 1)$-extendable if 
$\exists (k - 1 - l)$-flat $\Pi$ in $\Sigma$ with $\Pi \subset F$.

Most of the known extension theorems can be proved geometrically using this lemma.
Problem 2. Find a new extension theorem for 4-weight (mod $q$) codes.

Question. Is any $[n, k, d]_5$ code with $d \equiv -3 \pmod{5}$ extendable?
Answer. Not always. A \([16, 3, 12]_5\) code \(C\) with generator matrix

\[
\begin{bmatrix}
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 2 & 2 & 3 & 3 & 4 & 4 & 1 & 1 \\
0 & 0 & 1 & 1 & 3 & 4 & 0 & 4 & 3 & 4 & 1 & 3 & 0 & 1 & 1 & 2
\end{bmatrix}
\]

has weight distribution \(0^{11}2^{60}3^{40}4^{15}24\). But \(C\) is not extendable.
Question.

Let $\mathcal{C}$ be an $[n, k, d]_q$ code with $q \geq 7$, $d \equiv -3 \pmod{q}$, $\gcd(d, q) = 1$, satisfying

$$A_i > 0 \implies i \equiv 0, -1, -2, -3 \pmod{q}.$$ 

Then, is $\mathcal{C}$ always extendable?
Question.

Let $\mathcal{C}$ be an $[n, k, d]_q$ code with $q \geq 7$, $d \equiv -3 \pmod{q}$, $\gcd(d, q) = 1$, satisfying $A_i > 0 \Rightarrow i \equiv 0, -1, -2, -3 \pmod{q}$. Then, is $\mathcal{C}$ always extendable?

The answer is unknown. Let’s try!
Thank you for your attention!
Let $q = 4$.

$C$: an $[n, k, d]_4$ code with $k \geq 3$, $d$ odd.

We define the diversity of $C$ as the 3-tuple $(\Phi_0, \Phi_1, \Phi_2)$ with

$$\Phi_0 = \frac{1}{3} \sum_{4|i,i>0} A_i,$$

$$\Phi_j = \frac{1}{3} \sum_{i \equiv -j \pmod{4}} A_i \quad \text{for } j = 1, 2$$

when $d \equiv 1 \pmod{4}$,

$$\Phi_j = \frac{1}{3} \sum_{i \equiv j \pmod{4}} A_i \quad \text{for } j = 1, 2$$

when $d \equiv 3 \pmod{4}$. 
Thm 17. (Simonis 2000, Maruta et al.)
An $[n, k, d]_4$ code $C$ with div. $(\Phi_0, \Phi_1, \Phi_2)$, $d$ odd, is extendable if one of the following conditions holds:

1. $\Phi_0 = \theta_{k-4}$
2. $\Phi_1 = 0$
3. $\Phi_2 = 0$
4. $\Phi_0 + \Phi_2 < \theta_{k-2} + 4^{k-2}$
5. $\Phi_0 + \Phi_2 = \theta_{k-2} + 2 \times 4^{k-2}$. 