Improvement on minimum distance of symbol-pair codes

Han Zhang
Northwest University, China

December 12, 2017
Outline

1. Section 1: Basic notations and some previous results

2. Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes

3. Section 3: Some specific MDS symbol-pair codes constructed by constacyclic codes

4. Section 4: Open Problems
Section 1: Basic notations and some previous results
symbol pair codes

- Σ – a symbol alphabet, each element in Σ is called a symbol.
symbol pair codes

- $\Sigma$ – a symbol alphabet, each element in $\Sigma$ is called a *symbol*.
- $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$ – a vector in $\Sigma^n$. 

\[ \pi(x) = [(x_0, x_1), (x_1, x_2), \cdots, (x_{n-1}, x_0)] \in (\Sigma \times \Sigma)^n, \text{ and for any } x, y \in \Sigma, \pi(x + y) = \pi(x) + \pi(y). \] 

$(a, b) \neq (c, d)$, if $a \neq c$ or $b \neq d$, or both.

The pair-distance between $x$ and $y$, $d_p(x, y) = d_H(\pi(x), \pi(y))$. 

Han Zhang (Northwest University, Cl)  
December 12, 2017 4 / 22
symbol pair codes

- $\Sigma$ – a symbol alphabet, each element in $\Sigma$ is called a symbol.
- $x = (x_0, x_1, \cdots, x_{n-1})$ – a vector in $\Sigma^n$.
- symbol-pair read vector of $x$,

$$\pi(x) = [(x_0, x_1), (x_1, x_2), \cdots, (x_{n-2}, x_{n-1}), (x_{n-1}, x_0)].$$
symbol pair codes

- $\Sigma$ – a symbol alphabet, each element in $\Sigma$ is called a symbol.
- $x = (x_0, x_1, \cdots, x_{n-1})$ – a vector in $\Sigma^n$.
- symbol-pair read vector of $x$,

$$\pi(x) = [(x_0, x_1), (x_1, x_2), \cdots, (x_{n-2}, x_{n-1}), (x_{n-1}, x_0)].$$

- $\pi(x) \in (\Sigma \times \Sigma)^n$, and for any $x, y \in \Sigma$,

$$\pi(x + y) = \pi(x) + \pi(y).$$
symbol pair codes

- $\Sigma$ – a symbol alphabet, each element in $\Sigma$ is called a symbol.
- $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$ – a vector in $\Sigma^n$.
- symbol-pair read vector of $\mathbf{x}$,

$$\pi(\mathbf{x}) = [(x_0, x_1), (x_1, x_2), \cdots, (x_{n-2}, x_{n-1}), (x_{n-1}, x_0)].$$

- $\pi(\mathbf{x}) \in (\Sigma \times \Sigma)^n$, and for any $\mathbf{x}, \mathbf{y} \in \Sigma$,

$$\pi(\mathbf{x} + \mathbf{y}) = \pi(\mathbf{x}) + \pi(\mathbf{y}).$$

- $(a, b) \neq (c, d)$, if $a \neq c$ or $b \neq d$, or both.
symbol pair codes

- $\Sigma$ – a symbol alphabet, each element in $\Sigma$ is called a symbol.
- $\bm{x} = (x_0, x_1, \cdots, x_{n-1})$ – a vector in $\Sigma^n$.
- symbol-pair read vector of $\bm{x}$,
  \[
  \pi(\bm{x}) = [(x_0, x_1), (x_1, x_2), \cdots, (x_{n-2}, x_{n-1}), (x_{n-1}, x_0)].
  \]
- $\pi(\bm{x}) \in (\Sigma \times \Sigma)^n$, and for any $\bm{x}, \bm{y} \in \Sigma$,
  \[
  \pi(\bm{x} + \bm{y}) = \pi(\bm{x}) + \pi(\bm{y}).
  \]
- $(a, b) \neq (c, d)$, if $a \neq c$ or $b \neq d$, or both.
- pair-distance between $\bm{x}$ and $\bm{y}$,
  \[
  d_p(\bm{x}, \bm{y}) = d_H(\pi(\bm{x}), \pi(\bm{y})).
  \]
For any vector $x \in \Sigma^n$, the pair weight of $x$,

$$\omega_p(x) = \omega_H(\pi(x)).$$
For any vector $\mathbf{x} \in \Sigma^n$, the pair weight of $\mathbf{x}$,

$$\omega_p(\mathbf{x}) = \omega_H(\pi(\mathbf{x})).$$

The minimum pair-distance of $\mathcal{C}$,

$$d_p(\mathcal{C}) = \min\{d_p(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}.$$ 

A code of length $n$ over $\Sigma$ is called an $(n, M, d_p)$-symbol-pair code if its size is $M$ and minimum pair distance is $d_p$. 

Proposition 1. *(Singleton Bound)* (Chee et al.)

Let \( q \geq 2 \) and \( 2 \leq d_H \leq n \). If \( C \) is an \((n, M, d_H)_q\)-symbol-pair code, then \( M \leq q^{n-d_H+2} \).
Proposition 1. (*Singleton Bound*)(Chee et al.)

Let \( q \geq 2 \) and \( 2 \leq d_H \leq n \). If \( C \) is an \((n, M, d_H)_q\)-symbol-pair code, then \( M \leq q^{n-d_H+2} \).

An \((n, M, d_H)_q\)-symbol-pair code attains the Singleton-type bound, i.e., \( M = q^{n-d_H+2} \), is said to be an maximum distance separable (MDS) symbol-pair code.
Cyclic codes and constacyclic codes

- $q$ – prime power, $\mathbb{F}_q$ is the finite field with $q$ elements.
Cyclic codes and constacyclic codes

- $q$ – prime power, $\mathbb{F}_q$ is the finite field with $q$ elements.
- If $C$ is a linear subspace over $\mathbb{F}_q$ of $\mathbb{F}_q^n$. 
- $q$ – prime power, $\mathbb{F}_q$ is the finite field with $q$ elements.
- If $C$ is a linear subspace over $\mathbb{F}_q$ of $\mathbb{F}_q^n$. 
Cyclic codes and constacyclic codes

- $q$ – prime power, $\mathbb{F}_q$ is the finite field with $q$ elements.
- If $C$ is a linear subspace over $\mathbb{F}_q$ of $\mathbb{F}_q^n$, $C$ is called a linear code.
Cyclic codes and constacyclic codes

- $q$ – prime power, $\mathbb{F}_q$ is the finite field with $q$ elements.
- If $C$ is a linear subspace over $\mathbb{F}_q$ of $\mathbb{F}_q^n$, $C$ is called a *linear code*.
- For a nonzero element $\eta$ in $\mathbb{F}_q$, the $\eta$-constacyclic shift $\tau_\eta$ on $\mathbb{F}_q^n$ is the shift

$$\tau_\eta(c_0, c_1, \ldots, c_{n-1}) = (\eta c_{n-1}, c_0, \ldots, c_{n-2}).$$
Cyclic codes and constacyclic codes

- $q$ - prime power, $\mathbb{F}_q$ is the finite field with $q$ elements.
- If $C$ is a linear subspace over $\mathbb{F}_q$ of $\mathbb{F}_q^n$. $C$ is called a linear code.
- For a nonzero element $\eta$ in $\mathbb{F}_q$, the $\eta$-constacyclic shift $\tau_\eta$ on $\mathbb{F}_q^n$ is the shift

$$\tau_\eta(c_0, c_1, \ldots, c_{n-1}) = (\eta c_{n-1}, c_0, \ldots, c_{n-2}).$$
- $q$ – prime power, $\mathbb{F}_q$ is the finite field with $q$ elements.
- If $C$ is a linear subspace over $\mathbb{F}_q$ of $\mathbb{F}_q^n$, $C$ is called a *linear code*.
- For a nonzero element $\eta$ in $\mathbb{F}_q$, the $\eta$-constacyclic shift $\tau_\eta$ on $\mathbb{F}_q^n$ is the shift
  \[
  \tau_\eta(c_0, c_1, \ldots, c_{n-1}) = (\eta c_{n-1}, c_0, \ldots, c_{n-2}).
  \]

A linear code $C$ is said to be *$\eta$-constacyclic* if $C$ is a $\tau_\eta$-invariant subspace of $\mathbb{F}_q^n$, i.e., $\tau_\eta(C) = C$. 
Cyclic codes and constacyclic codes

- **q** – prime power, \( \mathbb{F}_q \) is the finite field with \( q \) elements.
- If \( C \) is a linear subspace over \( \mathbb{F}_q \) of \( \mathbb{F}_q^n \).
  \( C \) is called a **linear code**.
- For a nonzero element \( \eta \) in \( \mathbb{F}_q \), the \( \eta \)-constacyclic shift \( \tau_\eta \) on \( \mathbb{F}_q^n \) is the shift
  \[
  \tau_\eta(c_0, c_1, \ldots, c_{n-1}) = (\eta c_{n-1}, c_0, \ldots, c_{n-2}).
  \]
  A linear code \( C \) is said to be **\( \eta \)-constacyclic** if \( C \) is a \( \tau_\eta \)-invariant subspace of \( \mathbb{F}_q^n \), i.e., \( \tau_\eta(C) = C \).
- If \( \eta = 1 \), then \( C \) is just the usual **cyclic code**.
Cyclic codes and constacyclic codes

For \( \mathbf{x} = (x_0, x_1, \cdots, x_{n-1}) \), we define

\[
\mathbf{x}' = (x_0 + x_1, x_1 + x_2, \ldots, x_{n-1} + x_0).
\]
Cyclic codes and constacyclic codes

- For \( \mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \), we define

\[
\mathbf{x}' = (x_0 + x_1, x_1 + x_2, \ldots, x_{n-1} + x_0).
\]

**Lemma 1.**

For any \( \mathbf{x} \in \Sigma^n \), \( \omega_p(\mathbf{x}) = \omega_H(\mathbf{x}) + \omega_H(\mathbf{x}')/2 \).
For $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$, we define

$$\mathbf{x}' = (x_0 + x_1, x_1 + x_2, \ldots, x_{n-1} + x_0).$$

**Lemma 1.**

For any $\mathbf{x} \in \Sigma^n$, $\omega_p(\mathbf{x}) = \omega_H(\mathbf{x}) + \omega_H(\mathbf{x}')/2$.

**Lemma 2. (E. Yaakobi et al.)**

Let $C$ be a linear cyclic code of dimension greater than one. Then,

$$d_p(C) \geq d_H(C) + \left\lceil \frac{d_H(C)}{2} \right\rceil.$$
Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes
For \( \mathbf{x} = (x_0, x_1, \cdots, x_{n-1}) \), we define

\[
\mathbf{x}_\lambda = (x_0 + \lambda x_1, x_1 + \lambda x_2, \cdots, x_{n-1} + \lambda x_0), \lambda \in \mathbb{F}_q^*.
\]
Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes

For $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1})$, we define

$$\mathbf{x}_\lambda = (x_0 + \lambda x_1, x_1 + \lambda x_2, \cdots, x_{n-1} + \lambda x_0), \lambda \in \mathbb{F}_q^*.$$ 

Below are our main results.
Section 2: Lower bounds on the minimum pair distance of \( q \)-ary linear cyclic codes and constacyclic codes

For \( \mathbf{x} = (x_0, x_1, \cdots, x_{n-1}) \), we define

\[
\mathbf{x}_\lambda = (x_0 + \lambda x_1, x_1 + \lambda x_2, \cdots, x_{n-1} + \lambda x_0), \lambda \in \mathbb{F}_q^*.
\]

Below are our main results.

**Theorem 1.**

Let \( \mathcal{C} \) be a \( q \)-ary linear cyclic code of dimension greater than one. Then,

\[
d_p(\mathcal{C}) \geq d_H(\mathcal{C}) + \left\lceil \frac{d_H(\mathcal{C})}{2(q - 1)} \right\rceil.
\]
Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes

Theorem 2. Let $C$ be a $q$-ary $\eta$-constacyclic code of dimension greater than one. Then,

$$d_p(C) \geq d_H(C) + \left\lceil \frac{d_H(C)}{2(q - 1)} \right\rceil.$$
Section 2: Lower bounds on the minimum pair distance of \( q \)-ary linear cyclic codes and constacyclic codes

**Theorem 1.**

Let \( C \) be a \( q \)-ary linear cyclic code of dimension greater than one. Then,

\[
d_p(C) \geq d_H(C) + \left\lceil \frac{d_H(C)}{2(q-1)} \right\rceil.
\]

**Proof of Theorem 1.**

For any \( \mathbf{x} \in \Sigma^n \), let \( \mathbf{x} = (x_0, x_1, \cdots, x_{n-1}) \) be a codeword in \( C \). Assume that \( \mathbf{x} \neq \mathbf{\alpha}, \alpha \in \mathbb{F}_q^* \). Thus for any \( \lambda \in \mathbb{F}_q^* \),

\[
\mathbf{x}_\lambda' = (x_0, x_1, \cdots, x_{n-1}) + \lambda(x_1, \cdots, x_{n-1}, x_0) \in C.
\]
Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes

Theorem 1.

Let $C$ be a $q$-ary linear cyclic code of dimension greater than one. Then,

$$d_p(C) \geq d_H(C) + \left\lceil \frac{d_H(C)}{2(q-1)} \right\rceil.$$ 

Proof of Theorem 1.

For any $x \in \Sigma^n$, let $x = (x_0, x_1, \cdots, x_{n-1})$ be a codeword in $C$. Assume that $x \neq \alpha, \alpha \in \mathbb{F}_q^*$. Thus for any $\lambda \in \mathbb{F}_q^*$,

$$x'_\lambda = (x_0, x_1, \cdots, x_{n-1}) + \lambda(x_1, \cdots, x_{n-1}, x_0) \in C.$$ 

Now let

$$S_\alpha = \{i|(x_i, x_{i+1}) \neq (0, 0), x_i = \alpha\}, \alpha \in \mathbb{F}_q.$$
Section 2: Lower bounds on the minimum pair distance of \(q\)-ary linear cyclic codes and constacyclic codes

**Theorem 1.**

Let \(C\) be a \(q\)-ary linear cyclic code of dimension greater than one. Then,

\[
d_p(C) \geq d_H(C) + \left\lceil \frac{d_H(C)}{2(q - 1)} \right\rceil.
\]

**Proof of Theorem 1.**

For any \(x \in \Sigma^n\), let \(x = (x_0, x_1, \cdots, x_{n-1})\) be a codeword in \(C\). Assume that \(x \neq \alpha, \alpha \in \mathbb{F}_q^*\). Thus for any \(\lambda \in \mathbb{F}_q^*\),

\[
x'_{\lambda} = (x_0, x_1, \cdots, x_{n-1}) + \lambda(x_1, \cdots, x_{n-1}, x_0) \in C.
\]

Now let

\[
S_{\alpha} = \{i | (x_i, x_{i+1}) \neq (0, 0), x_i = \alpha\}, \alpha \in \mathbb{F}_q.
\]
Proof of Theorem 1.

For any $\alpha, \beta \in \mathbb{F}_q, \alpha \neq \beta$, one has $S_\alpha \cap S_\beta = \emptyset$ and $w_p(x) = \sum_{\alpha \in \mathbb{F}_q} |S_\alpha| = w_H(x) + |S_0|$. Thus, one has

$$
\sum_{\lambda \in \mathbb{F}_q^*} w_H(x'_\lambda) = 2(q-1)|S_0| + (q-2) \sum_{\alpha \in \mathbb{F}_q^*} |S_\alpha|
$$

$$
= 2(q-1)|S_0| + (q-2)w_H(x).
$$
Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes

Proof of Theorem 1.

For any $\alpha, \beta \in \mathbb{F}_q, \alpha \neq \beta$, one has $S_\alpha \cap S_\beta = \emptyset$ and

$$w_p(x) = \sum_{\alpha \in \mathbb{F}_q} |S_\alpha| = w_H(x) + |S_0|.$$

Thus, one has

$$\sum_{\lambda \in \mathbb{F}_q^*} w_H(x'_\lambda) = 2(q - 1)|S_0| + (q - 2) \sum_{\alpha \in \mathbb{F}_q^*} |S_\alpha|$$

$$= 2(q - 1)|S_0| + (q - 2)w_H(x).$$

Then we can deduce that

$$|S_0| = \frac{1}{2(q - 1)} \sum_{\lambda \in \mathbb{F}_q^*} w_H(x'_\lambda) - \frac{q - 2}{2(q - 1)}w_H(x).$$
Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes

Proof of Theorem 1.

For any $\alpha, \beta \in \mathbb{F}_q, \alpha \neq \beta$, one has $S_\alpha \cap S_\beta = \emptyset$ and

$$w_p(x) = \sum_{\alpha \in \mathbb{F}_q} |S_\alpha| = w_H(x) + |S_0|.$$  Thus, one has

$$\sum_{\lambda \in \mathbb{F}_q^*} w_H(x'_\lambda) = 2(q - 1)|S_0| + (q - 2) \sum_{\alpha \in \mathbb{F}_q^*} |S_\alpha|$$

$$= 2(q - 1)|S_0| + (q - 2)w_H(x).$$

Then we can deduce that

$$|S_0| = \frac{1}{2(q - 1)} \sum_{\lambda \in \mathbb{F}_q^*} w_H(x'_\lambda) - \frac{q - 2}{2(q - 1)}w_H(x).$$

It follows that
Proof of Theorem 1.

\[ w_p(x) = w_H(x) + |S_0| \]
\[ = \frac{1}{2(q-1)} \sum_{\lambda \in \mathbb{F}_q^*} w_H(x') - \frac{q-2}{2(q-1)} w_H(x) + w_H(x) \]
\[ \geq \frac{d_H}{2} - \frac{q-2}{2(q-1)} d_H + d_H \]
\[ = \frac{d_H}{2(q-1)} + d_H. \]
Section 2: Lower bounds on the minimum pair distance of \(q\)-ary linear cyclic codes and constacyclic codes

Proof of Theorem 1.

\[
\begin{align*}
  w_p(\mathbf{x}) &= w_H(x) + |S_0| \\
  &= \frac{1}{2(q - 1)} \sum_{\lambda \in \mathbb{F}_q^*} w_H(x') - \frac{q - 2}{2(q - 1)} w_H(x) + w_H(x) \\
  &\geq \frac{d_H}{2} - \frac{q - 2}{2(q - 1)} d_H + d_H \\
  &= \frac{d_H}{2(q - 1)} + d_H.
\end{align*}
\]

Hence,

\[
  w_p(\mathbf{x}) \geq \left\lceil \frac{d_H}{2(q - 1)} \right\rceil + d_H.
\]
Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes

Proof of Theorem 2.
The proof of Theorem 2 implied by Theorem 1.
Lemma 2. (E. Yaakobi et al.)

Let $C$ be a linear cyclic code of dimension greater than one. Then,

$$d_p(C) \geq d_H(C) + \left\lceil \frac{d_H(C)}{2} \right\rceil.$$
Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes

Lemma 2. (E. Yaakobi et al.)

Let $C$ be a linear cyclic code of dimension greater than one. Then,

$$d_p(C) \geq d_H(C) + \left\lceil \frac{d_H(C)}{2} \right\rceil.$$  

Proof of Lemma 2.

Let $\mathbf{x} = (x_0, x_1, \cdots, x_{n-1}) \in \Sigma^n$. Our goal is to calculate $w_p(\mathbf{x})$, namely,

$$w_p(\mathbf{x}) = wt\{(x_0, x_1), (x_1, x_2), \cdots, (x_{n-1}, x_0)\}.$$
Section 2: Lower bounds on the minimum pair distance of \( q \)-ary linear cyclic codes and constacyclic codes

Lemma 2. (E. Yaakobi et al.)

Let \( C \) be a linear cyclic code of dimension greater than one. Then,

\[
\text{d}_p(C) \geq d_H(C) + \left\lceil \frac{d_H(C)}{2} \right\rceil.
\]

Proof of Lemma 2.

Let \( \mathbf{x} = (x_0, x_1, \cdots, x_{n-1}) \in \Sigma^n \). Our goal is to calculate \( w_p(\mathbf{x}) \), namely,

\[
w_p(\mathbf{x}) = \text{wt}\{(x_0, x_1), (x_1, x_2), \cdots, (x_{n-1}, x_0)\}.
\]

Now we let

\[ S_0 = \{i : (x_i, x_{i+1}) \neq (0, 0) \text{ and } x_i = 1\} , \]
\[ S_1 = \{i : (x_i, x_{i+1}) = (0, 1)\} . \]
Proof of Lemma 2.

Hence, $|S_0| = \omega_H(x)$, $S_0 \cap S_1 = \emptyset$, and $\omega_p(x) = |S_0| + |S_1|$. 

Han Zhang (Northwest University, Cl) 

December 12, 2017 17 / 22
Proof of Lemma 2.

Hence, $|S_0| = \omega_H(x), S_0 \cap S_1 = \emptyset$, and $\omega_p(x) = |S_0| + |S_1|$. For all $0 \leq i \leq n - 1$, $i \in S_1$, we get

$$|S_1| = |\{i : x_{i+1} = 1 \text{ and } x_i = 0\}|.$$
Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes

Proof of Lemma 2.

Hence, $|S_0| = \omega_H(x)$, $S_0 \cap S_1 = \emptyset$, and $\omega_p(x) = |S_0| + |S_1|$.

For all $0 \leq i \leq n - 1$, $i \in S_1$, we get

$$|S_1| = |\{i : x_{i+1} = 1 \text{ and } x_i = 0\}|.$$

Note that for any $x \in \Sigma^n$,

$$|\{i : x_{i+1} = 1 \text{ and } x_i = 0\}| = |\{i : x_{i+1} = 0 \text{ and } x_i = 1\}|.$$
Section 2: Lower bounds on the minimum pair distance of $q$-ary linear cyclic codes and constacyclic codes

**Proof of Lemma 2.**

Hence, $|S_0| = \omega_H(x)$, $S_0 \cap S_1 = \emptyset$, and $\omega_p(x) = |S_0| + |S_1|$. For all $0 \leq i \leq n - 1$, $i \in S_1$, we get

$$|S_1| = |\{i : x_{i+1} = 1 \text{ and } x_i = 0\}|.$$

Note that for any $x \in \Sigma^n$,

$$|\{i : x_{i+1} = 1 \text{ and } x_i = 0\}| = |\{i : x_{i+1} = 0 \text{ and } x_i = 1\}|,$$

and the sum of the cardinality of the two sets is $\omega_H(x')$. Hence, $|S_1| = \frac{\omega_H(x')}{2}$ and

$$\omega_p(x) = |S_0| + |S_1| = \omega_H(x) + \frac{\omega_H(x')}{2}.$$
Section 3: Some specific MDS symbol-pair codes constructed by constacyclic codes
Example

(1) Let $C$ be a $[23, 3, 19]_5$ $\eta$-constacyclic code, there exists an MDS $[23, 22]_5$-symbol-pair code. (2) Let $C$ be a $[11, 5, 6]$ $\eta$-constacyclic code over $\mathbb{F}_3$, there exists an MDS $(11, 8)_3$-symbol-pair code.
Section 4: Open Problems
Section 4: Open Problems

- Is the lower bound on the minimum pair-distance of a constacyclic code can be improved?
Section 4: Open Problems

- Is the lower bound on the minimum pair-distance of a constacyclic code can be improved?
- Is there any optimal code constructions by using constacyclic codes?
Thanks for your attention!