On the homogeneous distance of negacyclic codes over Z_2^a

ZHU Shixin, KAI Xiaoshan
(School of Mathematics, Hefei University of Technology)

Abstract: In this paper, we investigate the homogeneous distance of negacyclic codes over Z_2^a of any length. We determine the torsion codes of a negacyclic code over Z_2^a for a given length. Using the higher torsion codes, we give a bound for the homogeneous distance of negacyclic codes over Z_2^a of any length. The exact homogeneous distance of some negacyclic codes over Z_2^a is also obtained.

Key words: cyclic code; negacyclic codes; homogeneous distance.

1 Introduction

Negacyclic codes over finite fields are a class of important codes that were initiated by Berlekamp in the early 1960s [1,2]. After successful applications of codes over Z_4 to good error-correcting codes [3] and unimodular lattices [4], codes over finite rings have received a lot of attention. In 1999, Wolfmann first introduced negacyclic codes over Z_4 of odd length and studied their binary images [5,6]. Later, Blackford [7] used a transform approach to classify negacyclic codes over Z_4 of even length. Recently, Dinh [8,9] computed various kinds of distances of all negacyclic codes of length 2^s over Z_{2^a}.

In the present work, we investigate the distances of negacyclic codes over Z_{2^a} for an arbitrary length. We consider the homogeneous distance of negacyclic codes over Z_{2^a} and the Euclidean distance of self-dual negacyclic codes over Z_{2^a}. It is well known that for a linear code C over Z_4, the Lee distance can be bounded by $\mathrm{Res}(C)$ and $Tor(C)$ [10]. We extend this bound to the homogeneous distance of negacyclic codes over Z_{2^a} in terms of the Hamming distances of torsion codes. To do this, we determine all torsion codes of a negacyclic code over Z_{2^a}. The material is organized as follows. In Section 2, we introduce some basic definitions and notations. We also review main results about negacyclic codes over Z_{2^a}. Section 3 determines all torsion codes of a negacyclic code Z_{2^a}. Bounds on the homogeneous distance of a negacyclic code Z_{2^a} are presented in Section 4.

2 Preliminaries

Let Z_{2^a} denote the finite commutative ring of integers modulo 2^a where $a \geq 2$ is a positive integer. Denote by $Z_{2^a}[x]$ the ring of polynomials in the indeterminate x with coefficients in Z_{2^a}. A polynomial in $Z_{2^a}[x]$ is called a basic irreducible polynomial if its reduction modulo 2,

---

Foundations: Specialized Research Fund for the Doctoral Pragram of High Education (No.200803590003) and the Foundamental Research Fund for the Central Universities (No.2011HGXJ1079)
Brief author introduction:1962 年生，男，教授，博导，主要研究领域：编码理论与密码. E-mail: zhushixin@hfut.edu.cn

denoted by $\overline{f}(x)$, is irreducible in $F_2[x]$. Each element $r \in Z_{2^a}$ can be written uniquely as

$$r = r_0 + 2r_1 + 2^2 r_2 + \cdots + 2^{a-1} r_{a-1},$$

where $r_i \in \{0,1\}$ for $0 \le i \le a-1$.

Two polynomials $f_1(x), f_2(x) \in Z_{2^a}[x]$ are said to be coprime if there exist $\lambda_1(x), \lambda_2(x) \in Z_{2^a}[x]$ such that $\lambda_1(x) f_1(x) + \lambda_2(x) f_2(x) = 1$. It is known that $f_1(x)$ and $f_2(x)$ are coprime in $Z_{2^a}[x]$ if and only if $\overline{f}_1(x)$ and $\overline{f}_2(x)$ are coprime in $F_2[x]$ (cf. [11]).

A code of length N over Z_{2^a} is a nonempty subset of $Z_{2^a}^N$, and a code of length N over Z_{2^a} is linear if it is a Z_{2^a}-submodule of $Z_{2^a}^N$. A linear code of length N over Z_{2^a} is negacyclic if C is invariant under the permutation of $Z_{2^a}^N$:

$$(c_0, c_1, \ldots, c_{N-1}) \to (-c_{N-1}, c_0, \ldots, c_{N-2}).$$

We identify a codeword $c = (c_0, c_1, \ldots, c_{N-1})$ with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{N-1} x^{N-1}$. Then $xc(x)$ corresponds to a negacyclic shift of $c(x)$ in the ring $Z_{2^a}[x]/\langle x^N + 1\rangle$. Thus negacyclic codes of length N over Z_{2^a} can be identified as ideals in the ring $Z_{2^a}[x]/\langle x^N + 1\rangle$. Let $N = 2^k n$, where k is a nonnegative integer and n is an odd number. Denote

$$\Re_a = Z_{2^a}[x]/\langle x^N + 1\rangle.$$

In particular, when $a = 1$, $\Re_1 = F_2[x]/\langle x^N + 1\rangle$. This means that a binary cyclic code of length $N = 2^k n$ $(n\ odd)$ is an ideal of $\Re_1$. It has been shown in [12,13] that negacyclic codes over Z_{2^a} of any length are principally generated. The following theorem gives the generators of negacyclic codes over Z_{2^a} for an arbitrary length.

Theorem 2.1 ([13]). Let $x^n - 1 = \prod_{i=1}^{r} f_i(x)$ be the unique factorization of $x^n - 1$ into a product of monic basic irreducible divisors in $Z_{2^a}[x]$. If C is a negacyclic code over Z_{2^a} of length $N = 2^k n$ $(n\ odd)$, then $C = \left\langle \prod_{i=1}^{r} f_i(x)^{k_i} \right\rangle$. Moreover

$$|C| = 2^{\sum_{i=0}^{r}(2^k a - i)\deg(f_i)}.$$

The homogeneous weight on Z_{2^a} is a weight function on Z_{2^a} defined by

$$w_{\hom}(r) = \begin{cases} 2^{a-2}, & if\ r \ne 2^{a-1} \\ 2^{a-1} & if\ r = 2^{a-1} \\ 0, & if\ r = 0. \end{cases}$$

The homogeneous weight of $c = (c_0, c_1, \ldots, c_{N-1})$ over Z_{2^a} is the rational sum of the homogeneous weights of components of C. The homogeneous distance $d_{\hom}(C)$ of a linear code C is the smallest homogeneous weight of nonzero codewords of C. The homogeneous weight on Z_4 coincides with the Lee weight. Carlet [14] introduced a generalized Gray isometry on Z_{2^a} with the above homogeneous weight to obtain the generalized Kerdock codes. Duursma et.al [15] used this Gray isometry on Z_8 to construct a nonlinear $(96, 2^{37}, 24)$ binary code.

3 Torsion codes

Let C be any code over Z_{2^a} of length N. We now associate C with some related codes. We define $\overline{C} = \{\overline{c} \mid c \in C\}$. For each i, $0 \le \gamma \le a-1$, we define the code $(C:2^\gamma) = \{c \in Z_{2^a}^N \mid 2^\gamma c \in C\}$.For a linear code C over Z_{2^a} of length N, it is easy to verify that $(C:2^j) \subseteq (C:2^{j+1})$ and $\overline{(C:2^j)} \subseteq \overline{(C:2^{j+1})}$, $0 \le j \le a-2$. In general, $\overline{C} = \overline{(C:2^0)}$ is called the residue code and is denoted by $\mathrm{Res}(C)$. Let γ be a fixed integer with $0 \le \gamma \le a-1$. Let C be a linear code of length N over Z_{2^a} , If C is negacyclic over Z_{2^a}, then it is easy to check that $(C:2^\gamma)$ is negacyclic over Z_{2^a} and $\overline{(C:2^\gamma)}$ is cyclic over F_2. Norton and Salagean introduced these codes [16] and used them to study the Hamming distance of linear codes over finite chain rings[17]. The code $(C:2^\gamma)$ is called the γth torsion code of C in [18]. The following is a special case of [18, Theorem 6.2].

Theorem 3.1 ([18]). For any linear code C over Z_{2^a}, we have $|C| = \prod_{\gamma=0}^{a-1} \left|\overline{(C:2^\gamma)}\right|$.

Next, we will determine the γth torsion code of C, for $0 \le \gamma \le m-1$. For this, we first give several helpful lemmas.

Lemma 3.2. In $\Re_a$, we have $\left\langle (x^n-1)^{2^k} \right\rangle = \langle 2 \rangle$.

Proof. The proof is similar to that for [7, Lemma 1]. By induction on n, it can be shown that $(x^n-1)^{2^k} = x^{2^k n} + 1 + 2\alpha_k(x^n)$, where $\alpha_k(x^n)$ is a unit in $\Re_a$. Therefore, $\left\langle (x^n-1)^{2^k} \right\rangle = \langle 2 \rangle$ in $\Re_a$.

Lemma 3.3. Let $f(x)$ be a divisor of x^n-1 in $F_2[x]$. Then, in $\Re_1$, $\left\langle f(x)^{2^k+l} \right\rangle = \left\langle f(x)^{2^k} \right\rangle$, for any positive integer l

Proof. Let $g(x) = (x^n-1)/f(x)$. Since $f(x)$and $g(x)$ are coprime in $F_2[x]$, it follows that $f(x)^l$ and $g(x)^{2^k}$ are coprime in $F_2[x]$,for any positive integer l. Hence, there exist $\theta(x), \vartheta(x) \in F_2[x]$ such that $\theta(x) f(x)^l + \vartheta(x) g(x)^{2^k} = 1$ in $F_2[x]$. Computing in

$\Re_1$, we have

$$\theta(x)f(x)^{2^k+l}=\left[1-\vartheta(x)g(x)^{2^k}\right]f(x)^{2^k}$$
$$=f(x)^{2^k}-\vartheta(x)(x^n-1)^{2^k}$$
$$=f(x)^{2^k}$$

Consequently, $\left\langle f(x)^{2^k+l}\right\rangle=\left\langle f(x)^{2^k}\right\rangle$ for any positive integer l.

Lemma 3.4. Let C be a negacyclic code over Z_{2^a} of length $N=2^k n$ (n odd) with generator polynomial $\prod_{i=1}^{r} f_i(x)^{k_i}$, where $f_i(x)(1\le i\le r)$ are monic basic irreducible divisors of x^n-1 in $Z_{2^a}[x]$ and $0\le k_i\le 2^k a$. Let γ be a fixed integer with $0\le\gamma\le a-1$. Then $(C:2^\gamma)$ contains the negacyclic code over Z_{2^a} of length $N=2^k n$ (n odd) with generator polynomial $\prod_{i=1}^{r} f_i(x)^{l_i^{(\gamma)}}$, where $l_i^{(\gamma)}=k_i-\min\{2^k\gamma,k_i\}$.

Proof. Let $D=\left\langle\prod_{i=1}^{r} f_i(x)^{l_i^{(\gamma)}}\right\rangle\subseteq\Re_a$ with $l_i^{(\gamma)}=k_i-\min\{2^k\gamma,k_i\}$. For any $f(x)\in D$, we have $f(x)=g(x)\prod_{i=1}^{r} f_i(x)^{l_i^{(\gamma)}}$, for some $g(x)\in\Re_a$. By Lemma 3.2, there exists an invertible element $\beta(x)$ in $\Re_a$ such that $\beta(x)(x^n-1)^{2^k}=2$. Hence,

$$2^\gamma f(x)=2^\gamma g(x)\prod_{i=1}^{r} f_i(x)^{l_i^{(\gamma)}}$$
$$=\beta(x)^\gamma(x^n-1)^{2^k\gamma}g(x)\prod_{i=1}^{r} f_i(x)^{l_i^{(\gamma)}}$$
$$=g(x)\beta(x)^\gamma\prod_{i=1}^{r} f_i(x)^{\tau_i^{(\gamma)}}$$

Where $\tau_i^{(\gamma)}=2^k\gamma+k_i-\min\{2^k\gamma,k_i\}$. Obviously, $2^\gamma f(x)\in C$, so $f(x)\in(C:2^\gamma)$. This gives that $D\subseteq(C:2^\gamma)$.

Combining the above lemmas with Theorem 3.1, we can determine the torsion codes of a negacyclic code over Z_{2^a} of length $N=2^k n$ (n odd) explicitly.

Theorem 3.5. Let C be a negacyclic code over Z_{2^a} of length $N=2^k n$ (n odd) with generator polynomial $\prod_{i=1}^{r} f_i(x)^{k_i}$, where $f_i(x)(1\le i\le r)$ are monic basic irreducible divisors of x^n-1 in $Z_{2^a}[x]$ and $0\le k_i\le 2^k a$. Let γ be a fixed integer with $0\le\gamma\le a-1$. Then $\overline{(C:2^\gamma)}$ is a binary cyclic code of length $N=2^k n$ (n odd) with generator polynomial $\prod_{i=1}^{r}\overline{f_i}(x)^{\tau_i^{(\gamma)}}$, where $\tau_i^{(\gamma)}=\min\{2^k(\gamma+1),k_i\}-\min\{2^k\gamma,k_i\}$

Proof. By Lemma 3.4, for each γ, $0\le\gamma\le a-1$, it is obvious that $\overline{(C:2^{\gamma})}\supseteq \left\langle \prod_{i=1}^{r}\overline{f}_i(x)^{l_i^{(\gamma)}}\right\rangle$,where $l_i^{(\gamma)}=k_i-\min\{2^k\gamma,k_i\}$. Let $\overline{D}=\left\langle \prod_{i=1}^{r}\overline{f}_i(x)^{l_i^{(\gamma)}}\right\rangle\subseteq\mathfrak{R}_1$. Applying Lemma 3.3, we get that

$$\overline{D}=\left\langle \prod_{i=1}^{r}\overline{f}_i(x)^{l_i^{(\gamma)}}\right\rangle=\left\langle \prod_{i=1}^{r}\overline{f}_i(x)^{\tau_i^{(\gamma)}}\right\rangle,$$

Where
$$\tau_i^{(\gamma)}=\min\{2^k,k_i-\min\{2^k\gamma,k_i\}\}$$
$$=\min\{2^k(\gamma+1),k_i\}-\min\{2^k\gamma,k_i\}.$$

This gives that $\left|\overline{(C:2^{\gamma})}\right|\ge 2^{t_\gamma}$ where

$$t_\gamma=N-\sum_{i=1}^{r}\tau_i^{(\gamma)}\cdot\deg(f_i).$$

Hence,
$$\prod_{\gamma=0}^{a-1}\left|\overline{(C:2^{\gamma})}\right|\ge 2^{t_0+t_1+\ldots+t_{a-1}}$$
$$=2^{aN-\sum_{i=1}^{r}\sum_{\gamma=0}^{a-1}\tau_i^{(\gamma)}\cdot\deg(f_i)}$$
$$=2^{aN-\sum_{i=1}^{r}k_i\cdot\deg(f_i)}.$$

From Theorem 3.1, we know that

$$|C|=\prod_{\gamma=0}^{a-1}\left|\overline{(C:2^{\gamma})}\right|=2^{aN-\sum_{i=1}^{r}k_i\cdot\deg(f_i)}.$$

Hence, for each γ, $0\le\gamma\le a-1$, it must have $\left|\overline{(C:2^{\gamma})}\right|=\left|\overline{D}\right|$ This shows that $\overline{(C:2^{\gamma})}=\overline{D}$. The desired result follows .

From the above theorem, we can express that the residue code $\mathrm{Res}(C)=\left\langle \prod_{i=1}^{r}\overline{f}_i(x)^{\tau_i^{(0)}}\right\rangle$, where $\tau_i^{(0)}=\min\{2^k,k_i\}$, and $\overline{(C:2^{a-1})}=\left\langle \prod_{i=1}^{r}\overline{f}_i(x)^{\tau_i^{(a-1)}}\right\rangle$ where $\tau_i^{(a-1)}=k_i-$. $\min\{2^k(a-1),k_i\}$

4 Homogeneous distance

Let $C=\left\langle \prod_{i=1}^{r}f_i(x)^{k_i}\right\rangle$ be a negacyclic code over $\mathbb{Z}_{2^a}$ of length $N=2^k n\ (n\ odd)$, where $f_i(x)\ (1\le i\le r)$ are monic basic irreducible divisors of x^n-1 in $\mathbb{Z}_{2^a}[x]$ and $0\le k_i\le 2^k a$. For each γ, $0\le\gamma\le a-1$, let d_γ denote the Hamming distance of the binary cyclic code $\overline{(C:2^{\gamma})}=\left\langle \prod_{i=1}^{r}f_i^{\tau_i^{(\gamma)}}\right\rangle$, where $\tau_i^{(\gamma)}=\min\{2^k(\gamma+1),k_i\}-\min\{2^k\gamma,k_i\}$. Clearly, $d_0\ge d_1\ge\cdots\ge d_{a-1}$. We first consider the Hamming distance of a negacyclic code over $\mathbb{Z}_{2^a}$ of length $N=2^k n\ (n\ odd)$. The Hamming distance is completely determined by the binary cyclic code $\overline{\left(C:2^{a-1}\right)}$.

Theorem 4.1. Let C be a negacyclic code over $\mathbb{Z}_{2^a}$ of length $N=2^k n\ (n\ odd)$ with generator polynomial $\prod_{i=1}^{r} f_i(x)^{k_i}$, where $f_i(x)(1\le i\le r)$ are monic basic irreducible divisors of x^n-1 in $\mathbb{Z}_{2^a}[x]$ and $0\le k_i\le 2^k a$. Then $d_H(C)=d_{a-1}$.

Proof. The result follows from [12, Theorem 4.2] and Theorem 3.5.

Theorem 4.2. Let C be a negacyclic code over $\mathbb{Z}_{2^a}$ of length $N=2^k n\ (n\ odd)$ with generator polynomial $\prod_{i=1}^{r} f_i(x)^{k_i}$, where $f_i(x)(1\le i\le r)$ are monic basic irreducible divisors of x^n-1 in $\mathbb{Z}_{2^a}[x]$ and $0\le k_i\le 2^k a$. Then

$$2^{a-2}\min\{d_{a-2},2d_{a-1}\}\le d_{\text{hom}}(C)\le 2^{a-1}d_{a-1}.$$

Proof. Let c be any nonzero codeword in C. Then there exists ν, $0\le\nu\le a-1$, such that c can be expressed in the form $2^{\nu}b$, where $b\in\mathbb{Z}_{2^a}^N$ is not divisible by 2. This gives that $0\ne\bar{b}\in\overline{\left(C:2^{\nu}\right)}$, which implies $w_H(\bar{b})\ge d_{\nu}$. If $0\le\nu\le a-2$, then $w_{\text{hom}}(c)\ge 2^{a-2}d_{\nu}$. Because $d_0\ge d_1\ge\cdots\ge d_{a-2}$, we have $w_{\text{hom}}(c)\ge 2^{a-2}d_{a-2}$, which means $d_{\text{hom}}(C)\ge 2^{a-2}d_{a-2}$. If $\nu=a-1$, then $d_{\text{hom}}(C)\ge 2^{a-1}d_{a-1}$. Hence, $d_{\text{hom}}(C)\ge\min\{2^{a-2}d_{a-2}, 2^{a-1}d_{a-1}\}$. On the other hand, note that $2^{a-1}\bar{b}=2^{a-1}b\in C$, so $d_{\text{hom}}(C)\le 2^{a-1}d_{a-1}$. Therefore, $2^{a-2}\min\{d_{a-2},2d_{a-1}\}\le d_{\text{hom}}(C)\le 2^{a-1}d_{a-1}$.

For the case $a=2$, the upper bound in the above theorem specializes to the bound given by Rains in [10, Lemma 4]. As special cases, we have the following two corollaries which provide the exact homogeneous distance of some negacyclic codes over $\mathbb{Z}_{2^a}$.

Corollary 4.3. Let C be a negacyclic code over $\mathbb{Z}_{2^a}$ of length $N=2^k n\ (n\ odd)$ with generator polynomial $\prod_{i=1}^{r} f_i(x)^{k_i}$, where $f_i(x)(1\le i\le r)$ are monic basic irreducible divisors of x^n-1 in $\mathbb{Z}_{2^a}[x]$ and $0\le k_i\le 2^k a$. If $d_{a-2}\ge 2d_{a-1}$ then $d_{\text{hom}}(C)=2^{a-1}d_{a-1}$.

Corollary 4.4. Let $C=\left\langle\prod_{i=1}^{r} f_i(x)^{k_i}\right\rangle$ be a negacyclic code over $\mathbb{Z}_{2^a}$ of length $N=2^k n\ (n\ odd)$, where $f_i(x)(1\le i\le r)$ are monic basic irreducible divisors of x^n-1 in $\mathbb{Z}_{2^a}$ and $0\le k_i\le 2^k a$. Let $\lambda=\max_{1\le i\le r}\{k_i\}$.

(1) If $1\le\lambda\le 2^k(a-2)$, then $d_{\text{hom}}(C)=2^{a-2}$.

(2) If $2^k(a-2)+1\le\lambda\le 2^k(a-1)$, then $d_{\text{hom}}(C)=2^{a-1}$.

Proof. (1) If $1\le\lambda\le 2^k(a-2)$, then, by Theorem 3.5, we get that $\overline{\left(C:2^{a-2}\right)}=\overline{\left(C:2^{a-1}\right)}=\langle 1\rangle$. From Theorem 4.2, it must be $2^{a-2}\le d_{\text{hom}}(C)\le 2^{a-1}$. Note that $\prod_{i=1}^{r} f_i(x)^{2^k(a-2)}=$

$\left(x^n-1\right)^{2^k(a-2)}=\left(2\beta\right)^{a-2}\in C$ for some unit β in R_a, which means $2^{a-2}\in C$. This implies that $d_{\text{hom}}\left(C\right)\le 2^{a-2}$. So, it must have $d_{\text{hom}}\left(C\right)=2^{a-2}$.

(2) if $2^k\left(a-2\right)+1\le\lambda\le 2^k\left(a-1\right)$, then $\overline{\left(C:2^{a-2}\right)}$ is not $\langle 0\rangle$ or $\langle 1\rangle$, but $\overline{\left(C:2^{a-1}\right)}=\langle 1\rangle$. Hence, $d_{a-2}\ge 2d_{a-1}$. From Theorem 4.2, we obtain that $d_{\text{hom}}\left(C\right)=2^{a-1}$.

Using torsion codes we can find the exact homogeneous distance of some negacyclic codes over $\mathbb{Z}_{2^a}$ of length $N=2^k n$ $(n\ odd)$. However, for the case when $\lambda=\max\limits_{1\le i\le r}\{k_i\}>2^k\left(a-1\right)$, it is difficult to determine the exact homogeneous distance for a negacyclic code over $\mathbb{Z}_{2^a}$ of length $N=2^k n$ $(n\ odd)$ in general. Thus, there are still a large number of negacyclic codes over $\mathbb{Z}_{2^a}$ of length $N=2^k n$ $(n\ odd)$ with homogeneous distance uncertain. Now we will give an upper bound for this case using simple-root binary cyclic code $C_0=\left\langle\overline{f}\left(x\right)\right\rangle$ of length n. Let C be a negacyclic code over $\mathbb{Z}_{2^a}$ of length $N=2^k n$ $(n\ odd)$ with generator polynomial $g\left(x\right)=\prod_{i=1}^{r}f_i(x)^{k_i}$, where $f_i\left(x\right)\left(1\le i\le r\right)$ are monic basic irreducible divisors of x^n-1 in $\mathbb{Z}_{2^a}[x]$ and $0\le k_i\le 2^k a$. Define $f\left(x\right)$ as the product of those basic irreducible polynomials $f_i\left(x\right)$ of $g\left(x\right)$ with multiplicity $k_i>2^k\left(a-1\right)$. The following lemma easily follows from [19, Theorem 1].

Lemma 4.5. Let $C_1=\left\langle\overline{f}(x)^{2^k}\right\rangle$ be the binary cyclic code of length $N=2^k n$ $(n\ odd)$, and let $C_2=\left\langle\overline{f}(x)\right\rangle$ be the binary cyclic code of length n. Then $d_H\left(C_1\right)=d_H\left(C_2\right)$.

Corollary 4.6. Let C be a negacyclic code of length $N=2^k n$ $(n\ odd)$ with generator polynomial $g(x)=\prod_{i=1}^{r}f_i(x)^{k_i}$. Let C_0 be defined as above and d be the Hamming distance of C_0. Let $\lambda=\max\limits_{1\le i\le r}\{k_i\}>2^k(a-1)$ and l be the number of nonzero coefficients of the 2-adic expansion of $\lambda-2^k(a-1)$.

(1) If $\lambda=2^k a$, then $d_{\text{hom}}(C)\le 2^{a-1}d$.

(2) If $2^k(a-1)<\lambda<2^k a$, then

$$d_{\text{hom}}(C)\le\min\{2^{a+l-1},2^{a-1}d\}.$$

Proof. (1) Note that $f(x)$ is the product of those basic irreducible polynomials $f_i(x)$ of $g(x)$ with multiplicity $k_i>2^k(a-1)$, so $\overline{(C,2^{a-1})}\supseteq\left\langle\overline{f}(x)^{2^k}\right\rangle$. This implies that $d_{a-1}\le d_H(\left\langle\overline{f}(x)^{2^k}\right\rangle)$. Combining Lemma 4.5 yields $d_{\text{hom}}(C)\le 2^{a-1}d$.

(2) If $2^k(a-1)<\lambda<2^k a$, then

$$\begin{aligned}\prod_{i=1}^{r} f_i(x)^{\lambda} &= (x^n-1)^{\lambda} \\ &= (x^n-1)^{2^k(a-1)}(x^n-1)^{\lambda-2^k(a-1)} \\ &= 2^{a-1}u(x)(x^n-1)^{\lambda-2^k(a-1)} \in C,\end{aligned}$$

for some unit $u(x)\in \Re_a$. Hence, $2^{a-1}(x^n-1)^{\lambda-2^k(a-1)}$ be in C. This gives $d_{\hom}(C)\le 2^{a+l-1}$. Also, we have $d_{\hom}(C)\le 2^{a-1}d$ from (1). Thus, $d_{\hom}(C)\le \min\{2^{a+l-1},2^{a-1}d\}$.

Example 4.7. Let $C_i=\langle (x-1)^i\rangle$ be a negacyclic code of length 2^k over Z_{2^a} ,for some $i\in\{0,1,\ldots,2^k a\}$. Then by Corollary 4.4, we easily get that if $0\le i\le 2^k(a-2)$, then $d_{\hom}(C_i)=2^{a-2}$; if $2^k(a-2)+1\le i\le 2^k(a-1)$,then $d_{\hom}(C_i)=2^{a-1}$. If $2^k a-2^{s-m}+1 \le i\le 2^k a-2^{s-m-1}$ for $0\le m\le k-1$, then $\overline{(C:2^{a-1})}=\langle (x-1)^j\rangle$ with $2^k-2^{k-m}+1 \le j\le 2^k-2^{k-m-1}$ and $\overline{(C:2^{a-2})}=\langle 0\rangle$. By Corollary 4.3, $d_{\hom}(C_i)=2d_{a-1}=2^{a+m}$ .This in fact gives an alternative method of computing the homogeneous distance of negacyclic codes of length 2^k over Z_{2^a} [9].

5 Conclusion

In this paper, we give a bound for the homogenous distance of negacyclic codes over Z_{2^a} using their higher torsion codes. The bound of the homogenous distance enables us to determine the exact distance of some negacyclic codes over Z_{2^a}. A further work is to consider the Euclidean distance of negacyclic codes over Z_{2^a}.

References

[1] Berlekamp E R.Negacyclic codes for the Lee metric. In Proc. Conf. Combin. Math.and Its Appl.,Chapel Hill, NC, 1968: 298-316.

[2] Berlekamp E R. Algebric Coding Theory. Revised 1984 ed. Laguna Hills, CA: Aegean Park.

[3] Hammons Jr A R,Kumar P V. Calderbank A R, Sloane N J A, Sole P. The Z_4-linearity of Kerdock Preparata, Goethals, and related codes [J]. IEEE Trans. Inform. Theory, 1994, 40: 301-319.

[4] Bonnecaze A, Sole P, Calderbank A R. Quaternary quadratic residue codes and unimodular lattices [J]. IEEE Trans. Inform. Theory, 1995, 41: 366-377.

[5] Wolfmann J. Negacyclic and cyclic codes over Z_4 [J]. IEEE Trans. Inform. Theory, 1999, 45, 2527-2532.

[6] Wolfmann J. Binary images of cyclic codes over Z_4 [J]. IEEE Trans. Inform. Theory, 2001, 47: 1773-1779.

[7] Blackford T. Negacyclic codes over Z_4 of even length [J]. IEEE Trans. Inform. Theory, 2003, 49: 1417-1424.

[8] Dinh H Q. Negacyclic codes of length 2^s over Galois rings [J]. IEEE Trans. Inform. Theory, 2005, 51: 4252-4262.

[9] Dinh H Q. Complete distances of all negacyclic codes of length 2^s over Z_2^a [J]. IEEE Trans. Inform. Theory, 2007, 53: 147-161.

[10] Rains E. Optimal self-dual codes over Z_4 [J]. Discr. Math., 1999, 203: 215-288.

[11] McDonald B R. Finite Rings with Identity. Dekker, New York, 1974.

[12] Salagean A. Repeated-root cyclic and negacyclic codes over finite chain rings [J]. Discr. Appl. Math., 2006, 154: 413-419.

[13] Zhu S, Kai X. Dual and self-dual negacyclic codes of even length over Z_2^a [J]. Discr. Math., 2009, 309:2382-2391.

[14] Carlet C. Z_2^k-Linear codes [J]. IEEE Trans. Inform. Theory, 1998, 44: 1543-1547.

[15] Duursma I M, Greferath M, Litsyn S N, Schmidt S E. A Z_8-linear lift of the binary Golay code and a nonlinear binary (96,2^37,24)-code [J]. IEEE Trans. Inform. Theory, 2001, 47: 1596-1598.

[16] Norton G H, Salagean A, On the structure of linear and cyclic codes over a finite chain ring [J]. Appl. Algebra Engrg. Comm. Comput., 2000, 10: 489-506.

[17] Norton G H, Salagean A. On the Hamming distance of linear codes over a finite chain ring [J]. IEEE Trans. Inform. Theory, 2000, 46: 1060-1067.

[18] Dougherty S T, Park Y H. On modular cyclic codes [J].Finite Fields Appl., 2007, 13: 31-57.
[19] Castagnoli G, Massey J L, Schoeller P A, von Seemann N.On repeated-root cyclic codes [J]. IEEE Trans. Inform. Theory, 1991,37; 337-342.

关于 Z_2^a 上的负循环码的齐次距离

朱士信，开晓山
（合肥工业大学数学学院）

摘要：本文研究了 Z_2^a 上任意长度的负循环码的齐次距离。确立了 Z_2^a 上任意长度的负循环码的各阶挠码；利用高阶挠码给出了 Z_2^a 上任意长度的负循环码的齐次距离界，得到了 Z_2^a 上某些负循环码的确切的齐次距离。

关键词：循环码；负循环码；齐次距离
中图分类号：TN911.22