J. Appl. Math. Comput. (2015) 49:433–445
DOI 10.1007/s12190-014-0847-5

ORIGINAL RESEARCH

The Gray images of $(1+u)$ constacyclic codes over $F_{2^m}[u]/\langle u^k \rangle$

Jian Ding · Hong-ju Li

Received: 29 August 2014 / Published online: 31 October 2014

Abstract Let R_k denote the polynomial residue ring $F_{2^m}[u]/\langle u^k \rangle$, where $2^{j-1}+1 \leq k \leq 2^j$ for some positive integer j. Motivated by the work in [1], we introduce a new Gray map from R_k to $F_{2^m}^{2^j}$. It is proved that the Gray image of a linear $(1+u)$ constacyclic code of an arbitrary length N over R_k is a distance invariant linear cyclic code of length $2^j N$ over F_{2^m}. Moreover, the generator polynomial of the Gray image of such a constacyclic code is determined, and some optimal linear cyclic codes over F_2 and F_4 are constructed under this Gray map.

Keywords Linear code · Cyclic code · Constacyclic code · Gray map

Mathematics Subject Classification 11T71 · 94B05 · 94B15

1 Introduction

Linear codes over finite rings have been studied since the early 1970s in [3,11], that study has regained attention by the works of Nechaev in [8] and Hammons et al in [4] on some efficient nonlinear binary codes. These works deal with nonlinear binary codes such as the Nordstrom-Robinson, Kerdock, Preparata, Goethals and Delsarte–Goethals codes which are considered as binary images under the Gray map of linear codes over the ring Z_4. Since then, many researchers have paid more and more attentions to study the codes over finite rings. In [15], Wolfmann showed that the Gray image of a

J. Ding (✉) · H. Li
Department of Common Course, Anhui Xinhua University, Hefei 230088, Anhui, People's Republic China
e-mail: dingjian_happy@163.com

H. Li
e-mail: zhenxidj.happy@163.com

linear single-root negacyclic code over Z_4 is a distance invariant binary cyclic code (not necessarily linear). This result was later generalized to a $(1+2^k)$ constacyclic code over $Z_{2^{k+1}}$ by Tapia-Recillas and Vega in [13], where the corresponding Gray image was a binary distance invariant quasi-cyclic code. In [7], Ling and Blackford generalized most of the results of [13,15] to the ring $Z_{p^{k+1}}$, where p is any prime and k is a positive integer.

$(1+u)$ constacyclic codes over F_2+uF_2 were first introduced by Qian et al in [9], where it was proved that the Gray image of a linear single-root $(1+u)$ constacyclic code over F_2+uF_2 is a binary distance invariant linear cyclic code. In [1], Abular and Siap extended the Gray map of [9] to an arbitrary length over F_2+uF_2 and the generator polynomial of the correspoding Gray image was obtained, some optimal binary codes were also constructed via the Gray map. Amarra et al in [2] discussed the Gray image of a single-root $(1-u)$ constacyclic code over $F_{p^k}+uF_{p^k}$, which was a quasi-cyclic code over F_p. Later, the result of [2] were extended to single-root $(1+u^t)$ constacyclic codes over $F_q[u]/\langle u^{t+1}\rangle$ and single-root $(1-u^m)$ constacyclic codes over $F_{p^k}[u]/\langle u^{m+1}\rangle$ in [12] and [14] respectively, where the Gray images were quasi-cyclic codes. Kai et al in [5] showed that the Gray image of a linear $(1+\lambda u)$ constacyclic code with an arbitrary length over F_p+uF_p was a distance invariant linear code over F_p. The Gray image of a single-root $(1+u+u^2)$ constacyclic code over the ring $F_2[u]/\langle u^3\rangle$ were proved to be a binary distance invariant linear cyclic code in [10], but the generator polynomials of the corresponding Gray images in [10] and [5] were not acquired. In this paper, we extend the result of [1] about the Gray map to the polynomial residue ring R_k, where the generator polynomials of the corresponding Gray images are obtained and some optimal linear cyclic code over F_2 and F_4 are constructed via the Gray map.

2 Preliminaries

Let R_k denote the ring $F_{2^m}[u]/\langle u^k\rangle$, where $2^{j-1}+1 \leq k \leq 2^j$ for some positive integer j and $u^k=0$. If $x^n-1=f_1f_2\cdots f_q$ is the factorization of (x^n-1) into a product of monic basic irreducible pairwise coprime polynomials over R_k for an odd positive integer n, then this factorization is unique and can be directly carried over R_k from over F_{2^m}. Let C be a code of length $N=2^e n$ over R_k, where e is a non-negative integer. For some fixed unit α of R_k, the α constacyclic shift ν_α on R_k^N is the shift $\nu_\alpha(c_0,c_1,\cdots,c_{N-1})=(\alpha c_{N-1},c_0,c_1,\cdots,c_{N-2})$. The code C is said to be an α constacyclic code if $\nu(C)=C$. Now, we identify a codeword $c=(c_0,c_1,\cdots,c_{N-1})$ with its polynomial representation $c(x)=c_0+c_1x+\cdots+c_{N-1}x^{N-1}$, then $xc(x)$ corresponds to an α constacyclic shift of $c(x)$ in the ring $R_k[x]/\langle x^N-\alpha\rangle$. Thus α constacyclic codes of length N over R_k can be identified as ideals in the ring $R_k[x]/\langle x^N-\alpha\rangle$. In the following, we let j be a positive integer and $2^{j-1}+1 \leq k \leq 2^j$.

3 A class of matrices over F_{2^m}

Definition 3.1 If $j=1$, then $A_2=\begin{pmatrix}1&0\\1&1\end{pmatrix}$. If $j>1$, then $A_{2^j}=\begin{pmatrix}A_{2^{j-1}}&0\\A_{2^{j-1}}&A_{2^{j-1}}\end{pmatrix}$.

From the definition of matrix A_{2^j}, we see that there are 2^j rows and 2^j columns in A_{2^j}. Besides, the first row of A_{2^j} is $(1, \underbrace{0, \cdots, 0}_{(2^j-1)\ zeros})$, the first and 2^jth columns of A_{2^j} are $A_{2^j}(1)$ and $A_{2^j}(2^j)$ respectively, where $A_{2^j}(1) = (\underbrace{1, 1, \cdots, 1}_{2^j\ ones})^T$ and $A_{2^j}(2^j) = (\underbrace{0, \cdots, 0}_{(2^j-1)\ ones}, 1)^T$.

Lemma 3.1 *A_{2^j} is an invertible matrix over F_{2^m}.*

Proof From the definition of matrix A_{2^j}, we see that A_{2^j} is a lower triangular matrix and each element of its main diagonal is one. So A_{2^j} is invertible over F_{2^m}. □

Lemma 3.2 *Let* $B_{2^j} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix}$ *with 2^j rows and 2^j columns, then* $B_{2^j} A_{2^j} = (A_{2^j}(2^j), \underbrace{0, \cdots, 0}_{(2^j-1)\ zero\ vectors})$ *in F_{2^m}.*

Proof Since the first row of A_{2^j} is $(1, \underbrace{0, \cdots, 0}_{(2^j-1)\ zeros})$, then $B_{2^j} A_{2^j} = B_{2^j} = (A_{2^j}(2^j), \underbrace{0, \cdots, 0}_{(2^j-1)\ zero\ vectors})$ in F_{2^m}. □

Theorem 3.3 *Let* $H_{2^j} = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$ *and* $D_{2^j} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$, *where H_{2^j} and D_{2^j} are both square matrices with 2^j rows and 2^j columns, then $H_{2^j} A_{2^j} = A_{2^j} D_{2^j}$ in F_{2^m}.*

Proof We prove the result by induction on j. In F_{2^m}, if $j = 1$, then

$$H_2 A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = A_2 D_2.$$

Suppose $H_{2^{j_1}} A_{2^{j_1}} = A_{2^{j_1}} D_{2^{j_1}}$ for some positive integer j_1, then

$$H_{2^{j_1}} A_{2^{j_1}} = (A_{2^{j_1}}(2^{j_1}), A_{2^{j_1}}(1), \cdots, A_{2^{j_1}}(2^{j_1}-1)).$$

From lemma 3.2, we can get

$$H_{2^{j_1+1}}A_{2^{j_1+1}} = \begin{pmatrix} H_{2^{j_1}} & B_{2^{j_1}} \\ 0 & H_{2^{j_1}} \end{pmatrix}\begin{pmatrix} A_{2^{j_1}} & 0 \\ A_{2^{j_1}} & A_{2^{j_1}} \end{pmatrix} = \begin{pmatrix} H_{2^{j_1}}A_{2^{j_1}} + B_{2^{j_1}}A_{2^{j_1}} & B_{2^{j_1}}A_{2^{j_1}} \\ H_{2^{j_1}}A_{2^{j_1}} & H_{2^{j_1}}A_{2^{j_1}} \end{pmatrix}$$

$$= \begin{pmatrix} (0, A_{2^{j_1}}(1), \cdots, A_{2^{j_1}}(2^{j_1}-1)) & (A_{2^{j_1}}(2^{j_1}), \underbrace{0, \cdots, 0}_{(2^{j_1}-1)\ zero\ vectors}) \\ (A_{2^{j_1}}(2^{j_1}), A_{2^{j_1}}(1), \cdots, A_{2^{j_1}}(2^{j_1}-1)) & (A_{2^{j_1}}(2^{j_1}), A_{2^{j_1}}(1), \cdots, A_{2^{j_1}}(2^{j_1}-1)) \end{pmatrix}.$$

so $H_{2^{j_1+1}}A_{2^{j_1+1}} = A_{2^{j_1+1}}D_{2^{j_1+1}}$, which gives the proof. □

4 A new Gray map and the structure of the corresponding Gray image

Let a, b be two elements in R_k, then a, b can be written as $a = \sum_{i=0}^{k-1} u^i r_i(a)$ and $b = \sum_{i=0}^{k-1} u^i r_i(b)$ respectively, where $r_i(a), r_i(b) \in F_{2^m}$ for $0 \le i \le k-1$. It is easy to check that $r_i(a+b) = r_i(a) + r_i(b)$ for $0 \le i \le k-1$.

Definition 4.1 For an arbitrary element a in R_k, a new Gray map Φ_k from R_k to $F_{2^m}^{2^j}$ is defined as follows:

$$\Phi_k(a) = (\underbrace{0, \cdots, 0}_{(2^j-k)\ zeros}, r_0(a), r_1(a), \cdots, r_{k-1}(a))A_{2^j}.$$

From the definition of Φ_k, we see that this Gray map is linear that because

$$\begin{aligned}\Phi_k(a+b) &= (\underbrace{0, \cdots, 0}_{(2^j-k)\ zeros}, r_0(a+b), r_1(a+b), \cdots, r_{k-1}(a+b))A_{2^j} \\ &= (\underbrace{0, \cdots, 0}_{(2^j-k)\ zeros}, r_0(a), r_1(a), \cdots, r_{k-1}(a))A_{2^j} \\ &\quad + (\underbrace{0, \cdots, 0}_{(2^j-k)\ zeros}, r_0(b), r_1(b), \cdots, r_{k-1}(b))A_{2^j} \\ &= \Phi_k(a) + \Phi_k(b).\end{aligned}$$

According to lemma 3.1, A_{2^j} is an invertible matrix over F_{2^m}, so Φ_k is a bijection from R_k to $F_{2^m}^{2^j}$. we identify a codeword $c = (c_0, c_1, \cdots, c_{N-1}) \in R_k^N$ with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{N-1}x^{N-1}$ and denote $P_i[c(x)] = \sum_{l=0}^{N-1} r_i(c_l)x^l$ for $0 \le i \le k-1$, then $c(x) = \sum_{i=0}^{k-1} u^i P_i[c(x)]$. Thus, the Gray map Φ_k can be extended to $R_k[x]$ in an obvious way.

Definition 4.2 For an arbitrary codeword $c = (c_0, c_1, \cdots, c_{N-1}) \in R_k^N$, its polynomial representation is $c(x) = c_0 + c_1x + \cdots + c_{N-1}x^{N-1}$. The polynomial Gray map

Φ_k from $R_k[x]$ to $F_{2^m}[x]$ is defined as follows:

$$\Phi_k[c(x)] = (\underbrace{0,\cdots,0}_{(2^j-k)\ zeros}, P_0[c(x)], P_1[c(x)], \cdots, P_{k-1}[c(x)])A_{2^j}\begin{pmatrix}1\\ x^N\\ \vdots\\ x^{(2^j-1)N}\end{pmatrix}.$$

Obviously, Φ_k is not only linear, but also a bijection from $R_k[x]$ to $F_{2^m}[x]$.

Definition 4.3 Let W_L be the Lee weight of the element of R_k and W_H be the Hamming weight of the element of $F_{2^m}^{2^j}$. We define that $W_L(a) = W_H[\Phi_k(a)]$ for an arbitrary element a in R_k. The Lee weight of a codeword in $R_k[x]$ is the rational integer sum of the Lee weight of its coefficients. The Lee distance between two codewords c and $\acute{c}$ is defined as the Lee weight of $(c-\acute{c})$.

The following lemma 4.1 is straightforward from the definitions of the polynomial Gray map and Lee distance.

Lemma 4.1 *The polynomial Gray map Φ_k is not only a linear bijection from $R_k[x]$ to $F_{2^m}[x]$, but also a distance-preserving map from ($R_k[x]$, Lee distance) to ($F_{2^m}[x]$, Hamming distance).*

Theorem 4.2 *If C is a $(1+u)$ constacyclic code of length N over R_k, then $\Phi_k(C)$ is a linear cyclic code of length 2^jN over F_{2^m}.*

Proof It only needs to prove $\Phi_k[xc(x)] = x\Phi_k[c(x)]$. In fact, $x^N = 1+u$ in $R_k[x]/\langle x^N-(1+u)\rangle$, so $x^{2^jN} = 1$. For an arbitrary codeword $c(x) = c_0 + c_1x + \cdots + c_{N-1}x^{N-1} \in C$, it can be written in the form $c(x) = \sum_{i=0}^{k-1} u^i P_i[c(x)]$. Then, we have $xc(x) = (1+u)c_{N-1} + c_0x + c_1x^2 + \cdots + c_{N-2}x^{N-1} = \sum_{i=0}^{k-1} u^i P_i[xc(x)]$, where $P_0[xc(x)] = r_0[(c_{N-1})] + xP_0[c(x)] + x^N r_0(c_{N-1})$ and $P_i[xc(x)] = r_i[(1+u)c_{N-1}] + \sum_{l=0}^{k-2} r_i(c_l)x^{l+1} = [r_{i-1}(c_{N-1}) + r_i(c_{N-1})] + xP_i[c(x)] + x^N r_i(c_{N-1})$ for $1 \le i \le k-1$. Therefore

$$\Phi_k[xc(x)] = (\underbrace{0,\cdots,0}_{(2^j-k)\ zeros}, P_0[xc(x)], P_1[xc(x)], \cdots, P_{k-1}[xc(x)])A_{2^j}\begin{pmatrix}1\\ x^N\\ \vdots\\ x^{(2^j-1)N}\end{pmatrix}$$

$$= (\underbrace{0,\cdots,0}_{(2^j-k)\ zeros}, r_0(c_{N-1}), \sum_{i=0}^{1} r_i(c_{N-1}), \cdots, \sum_{i=k-2}^{k-1} r_i(c_{N-1}))A_{2^j}\begin{pmatrix}1\\ x^N\\ \vdots\\ x^{(2^j-1)N}\end{pmatrix}$$

$$+x^N(\underbrace{0,\cdots,0}_{(2^j-k)\ zeros}, r_0(c_{N-1}), r_1(c_{N-1}),\cdots, r_{k-1}(c_{N-1}))A_{2^j}\begin{pmatrix}1\\x^N\\\vdots\\x^{(2^j-1)N}\end{pmatrix}$$

$$+x(\underbrace{0,\cdots,0}_{(2^j-k)\ zeros}, P_0[c(x)], P_1[c(x)],\cdots, P_{k-1}[c(x)])A_{2^j}\begin{pmatrix}1\\x^N\\\vdots\\x^{(2^j-1)N}\end{pmatrix}$$

$$=(\underbrace{0,\cdots,0}_{(2^j-k)\ zeros}, r_0(c_{N-1}), r_1(c_{N-1}),\cdots, r_{k-1}(c_{N-1}))(H_{2^j}A_{2^j}+A_{2^j}D_{2^j})$$

$$\times\begin{pmatrix}1\\x^N\\\vdots\\x^{(2^j-1)N}\end{pmatrix}+x\Phi_k[c(x)].$$

By theorem 3.3, $\Phi_k[xc(x)] = x\Phi_k[c(x)]$. □

5 The generator polynomial of the Gray image

Lemma 5.1 *In* $F_{2^m}[x]$, $A_{2^j}\begin{pmatrix}1\\x^N\\\vdots\\x^{(2^j-1)N}\end{pmatrix}=\begin{pmatrix}1\\1+x^N\\\vdots\\(1+x^N)^{2^j-1}\end{pmatrix}$.

Proof We prove the result by induction on j. In $F_{2^m}[x]$, if $j=1$, then $A_2\begin{pmatrix}1\\x^N\end{pmatrix}=\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1\\x^N\end{pmatrix}=\begin{pmatrix}1\\1+x^N\end{pmatrix}$.

Suppose $A_{2^{j_1}}\begin{pmatrix}1\\x^N\\\vdots\\x^{(2^{j_1}-1)N}\end{pmatrix}=\begin{pmatrix}1\\1+x^N\\\vdots\\(1+x^N)^{2^{j_1}-1}\end{pmatrix}$ for some positive integer j_1 in $F_{2^m}[x]$, then

$$A_{2^{j_1+1}}\begin{pmatrix}1\\x^N\\\vdots\\x^{(2^{j_1+1}-1)N}\end{pmatrix}=\begin{pmatrix}A_{2^{j_1}}&0\\A_{2^{j_1}}&A_{2^{j_1}}\end{pmatrix}\begin{pmatrix}1\\x^N\\\vdots\\x^{(2^{j_1+1}-1)N}\end{pmatrix}$$

$$= \begin{pmatrix} A_{2^{j_1}} \begin{pmatrix} 1 \\ x^N \\ \vdots \\ x^{(2^{j_1}-1)N} \end{pmatrix} \\ (1+x^{2^{j_1}N})A_{2^{j_1}} \begin{pmatrix} 1 \\ x^N \\ \vdots \\ x^{(2^{j_1}-1)N} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 1+x^N \\ \vdots \\ (1+x^N)^{2^{j_1+1}-1} \end{pmatrix}.$$

This gives the proof. □

Let n be an odd positive integer and let $x^n - 1 = f_1 f_2 \cdots f_q$ be the factorization of $(x^n - 1)$ into a product of monic basic irreducible pairwise coprime polynomials in $F_{2^m}[x]$, then the following lemma is straightforward from the theorem 4 and lemma 3 of [7].

Lemma 5.2 *Let C be a $(1+u)$ constacyclic code of length $N = 2^e n$ over R_k, then $C = \langle f_1^{k_1} f_2^{k_2} \cdots f_q^{k_q}\rangle$, where $0 \le k_i \le 2^e k$ for $i = 0, 1, \cdots, q$. Furthermore, $|C| = 2^{m(kN-\eta)}$, where $\eta = \sum_{i=1}^{q} k_i deg(f_i)$.*

Theorem 5.3 *Let $C = \langle f_1^{k_1} f_2^{k_2} \cdots f_q^{k_q}\rangle$ be a $(1+u)$ constacyclic code of length $N = 2^e n$ over R_k, where e is a non-negative integer and $0 \le k_i \le 2^e k$ for $i = 0, 1, \cdots, q$. Then the Gray image $\Phi_k(C)$ is a linear cyclic code of length $2^j N$ over F_{2^m} and $\Phi_k(C) = \langle f_1^{k_1+2^e(2^j-k)} f_2^{k_2+2^e(2^j-k)} \cdots f_q^{k_q+2^e(2^j-k)}\rangle$.*

Proof By theorem 4.2, $\Phi_k(C)$ is a linear cyclic code of length $2^j N$ over F_{2^m}. So, we only need to prove $\Phi_k(C) = \langle f_1^{k_1+2^e(2^j-k)} f_2^{k_2+2^e(2^j-k)} \cdots f_q^{k_q+2^e(2^j-k)}\rangle$. In fact, we denote $c(x) = f_1^{k_1} f_2^{k_2} \cdots f_q^{k_q} \in C$, then $c(x) = \sum_{i=0}^{k-1} u^i P_i[c(x)] = \sum_{i=0}^{k-1}(1 + x^N)^i P_i[c(x)]$. By lemma 5.1,

$$\Phi_k[c(x)] = (\underbrace{0, \cdots, 0}_{(2^j-k)\ zeros}, P_0[c(x)], P_1[c(x)], \cdots, P_{k-1}[c(x)])A_{2^j} \begin{pmatrix} 1 \\ x^N \\ \vdots \\ x^{(2^j-1)N} \end{pmatrix}$$

$$= (\underbrace{0, \cdots, 0}_{(2^j-k)\ zeros}, P_0[c(x)], P_1[c(x)], \cdots, P_{k-1}[c(x)]) \begin{pmatrix} 1 \\ 1+x^N \\ \vdots \\ (1+x^N)^{2^j-1} \end{pmatrix}$$

$$= (1+x^N)^{2^j-k} \sum_{i=0}^{k-1} (1+x^N)^i P_i[c(x)] = (1+x^N)^{2^j-k} c(x) \in \Phi_k(C).$$

So $\langle(1+x^N)^{2^j-k} f_1^{k_1} f_2^{k_2} \cdots f_q^{k_q}\rangle \subseteq \Phi_k(C)$. Comparing the number of codewords, we have $\Phi_k(C) = \langle(1+x^N)^{2^j-k} f_1^{k_1} f_2^{k_2} \cdots f_q^{k_q}\rangle$. Since $1+x^N = (f_1 f_2 \cdots f_q)^{2^e}$ in $F_{2^m}[x]$, then we get the result. □

6 Examples

Let ω be a primitive element of F_4. In $F_2[x]$, $x^3-1 = Q_1 Q_2$, where $Q_1 = x+1$ and $Q_2 = x^2+x+1$. In $F_4[x]$, $x^3-1 = g_1 g_2 g_3$, where $g_1 = x+1$, $g_2 = x+\omega$ and $g_3 = x+\omega^2$. In $F_2[x]$ and $F_4[x]$, $x^7-1 = f_1 f_2 f_3$, where $f_1 = x+1$, $f_2 = x^3+x+1$ and $f_3 = x^3+x^2+1$.

Example 1 Let $k = 2$ and $m = 1$ in definition 4.2 and theorem 5.3, we get the result of Abularub et al about the Gray map in [1]. Now, we let $k = 2$ and $m = 2$, we can get some other optimal codes. For example, $C_1 = \langle g_1 g_2 g_3^3\rangle$ is a $(1+u)$ constacyclic code of length $N = 6$ over $F_4 + uF_4$. According to theorem 5.3, $\Phi_2(C_1) = \langle g_1 g_2 g_3^3\rangle$, which is a [4,7,12] linear cyclic code over F_4 and an optimal code. Table 1 presents

Table 1 Optimal linear codes over F_4 obtained from $(1+u)$ constacyclic codes over $F_4 + uF_4$

Length	Generator polynomial	Gray image
3	g_1	[6,5,2]
3	g_2	[6,5,2]
3	g_3	[6,5,2]
3	g_1^2	[6,4,2]
3	$g_1 g_2$	[6,4,2]
3	$g_1 g_3$	[6,4,2]
3	g_2^2	[6,4,2]
3	$g_2 g_3$	[6,4,2]
3	g_3^2	[6,4,2]
3	$g_1^2 g_2 g_3$	[6,2,4]
3	$g_1 g_2^2 g_3$	[6,2,4]
3	$g_1 g_2 g_3^2$	[6,2,4]
6	g_1	[12,11,2]
6	g_2	[12,11,2]
6	g_3	[12,11,2]
6	g_1^2	[12,10,2]
6	$g_1 g_2$	[12,10,2]
6	$g_1 g_3$	[12,10,2]
6	g_2^2	[12,10,2]
6	$g_2 g_3$	[12,10,2]
6	g_3^2	[12,10,2]
6	$g_1^3 g_2 g_3$	[12,7,4]

Table 1 continued

Length	Generator polynomial	Gray image
6	$g_1g_2^3g_3$	[12,7,4]
6	$g_1g_2g_3^3$	[12,7,4]
7	f_1	[14,13,2]
7	f_1^2	[14,12,2]
7	$f_1^2f_2$	[14,9,4]
7	$f_1^2f_3$	[14,9,4]

several optimal linear codes over F_4 obtained from $(1+u)$ constacyclic codes over $F_4 + uF_4$ of some lengths.

Tables 2, 3, 4, 5, 6 and 7 present some optimal codes obtained from $(1+u)$ constacyclic codes of some lengths over R_k under the Gray map.

Table 2 Optimal binary linear codes obtained from $(1+u)$ constacyclic codes over $F_2[u]/\langle u^3\rangle$

Length	Generator polynomial	Gray image
3	Q_1^2	[12,7,4]
3	Q_1^3	[12,6,4]
3	$Q_1^2Q_2$	[12,5,4]
3	Q_2^2	[12,5,4]
3	Q_2^3	[12,3,6]
3	$Q_1^3Q_2^2$	[12,2,8]
6	Q_1	[24,20,2]
6	Q_1^4	[24,17,4]
6	Q_1^5	[24,16,4]
6	$Q_1^4Q_2$	[24,15,4]
6	Q_1^6	[24,15,4]
7	$f_1^3f_2^2$	[28,12,8]
7	$f_1^3f_3^2$	[28,12,8]
7	$f_2^2f_3^3$	[28,6,12]
7	$f_2^3f_3^2$	[28,6,12]

Table 3 Optimal linear codes over F_4 obtained from $(1+u)$ constacyclic codes over $F_4[u]/\langle u^3\rangle$

Length	Generator polynomial	Gray image
3	g_1^2	[12,7,4]
3	g_2^2	[12,7,4]
3	g_3^2	[12,7,4]

Table 4 Optimal binary linear codes obtained from $(1+u)$ constacyclic codes over $F_2[u]/\langle u^4\rangle$

Length	Generator polynomial	Gray image
3	Q_1	[12,11,2]
3	Q_1^2	[12,10,2]
3	Q_2	[12,10,2]
3	Q_1^3	[12,9,2]
3	Q_1Q_2	[12,9,2]
3	$Q_1^3Q_2$	[12,7,4]
3	$Q_1^4Q_2$	[12,6,4]
3	$Q_1Q_2^3$	[12,5,4]
3	$Q_1^3Q_2^2$	[12,5,4]
3	$Q_1Q_2^4$	[12,3,6]
3	$Q_1^4Q_2^3$	[12,2,8]
6	Q_1	[24,23,2]
6	Q_1^2	[24,22,2]
6	Q_2	[24,22,2]
6	Q_1^3	[24,21,2]
6	Q_1Q_2	[24,21,2]
6	Q_1^4	[24,20,2]
6	$Q_1^2Q_2$	[24,20,2]
6	Q_2^2	[24,20,2]
6	$Q_1^5Q_2$	[24,17,4]
6	$Q_1^6Q_2$	[24,16,4]
6	$Q_1^5Q_2^2$	[24,15,4]
6	$Q_1^7Q_2$	[24,15,4]
7	$f_1^3f_2$	[28,22,4]
7	$f_1^3f_3$	[28,22,4]
7	$f_1^4f_2$	[28,21,4]
7	$f_1^4f_3$	[28,21,4]
7	$f_1^4f_2f_3^3$	[28,12,8]
7	$f_1^4f_2^3f_3$	[28,12,8]
7	$f_1f_2^4f_3^3$	[28,6,12]
7	$f_1f_2^3f_3^4$	[28,6,12]

Table 5 Optimal linear codes over F_4 obtained from $(1+u)$ constacyclic codes over $F_4[u]/\langle u^4\rangle$

Length	Generator polynomial	Gray image
3	g_1	[12,11,2]
3	g_2	[12,11,2]
3	g_3	[12,11,2]
3	g_1^2	[12,10,2]
3	g_2^2	[12,10,2]

Table 5 continued

Length	Generator polynomial	Gray image
3	g_3^2	[12,10,2]
3	$g_1 g_2$	[12,10,2]
3	$g_1 g_3$	[12,10,2]
3	$g_2 g_3$	[12,10,2]
3	$g_1 g_2 g_3^3$	[12,7,4]
3	$g_1 g_2^3 g_3$	[12,7,4]
3	$g_1^3 g_2 g_3$	[12,7,4]
7	f_1	[28,27,2]
7	f_1^2	[28,26,2]
7	f_2	[28,25,2]
7	f_3	[28,25,2]
7	f_1^3	[28,25,2]
7	$f_1^3 f_2$	[28,22,4]
7	$f_1^3 f_3$	[28,22,4]

Table 6 Optimal binary linear codes obtained from $(1+u)$ constacyclic codes over $F_2[u]/\langle u^8 \rangle$

Length	Generator polynomial	Gray image
7	f_1^2	[56,54,2]
7	f_1^3	[56,53,2]
7	f_2	[56,53,2]
7	f_3	[56,53,2]
7	$f_1 f_3$	[56,52,2]
7	$f_1 f_2$	[56,52,2]
7	f_1^4	[56,52,2]
7	$f_1^2 f_3$	[56,51,2]
7	$f_1^2 f_2$	[56,51,2]
7	$f_1^5 f_3$	[56,48,4]
7	$f_1^5 f_2$	[56,48,4]
7	$f_1^6 f_3$	[56,47,4]
7	$f_1^7 f_3$	[56,46,4]
7	$f_1^7 f_2$	[56,46,4]
7	$f_1^5 f_3^2$	[56,45,4]
7	$f_1^5 f_2^2$	[56,45,4]
7	$f_1^8 f_3$	[56,45,4]
7	$f_1^8 f_2$	[56,45,4]
7	$f_1^5 f_2 f_3$	[56,45,4]

Table 7 Optimal binary linear codes obtained from $(1+u)$ constacyclic codes over $F_2[u]/\langle u^{16}\rangle$

Length	Generator polynomial	Gray image
7	f_1	[112,111,2]
7	f_1^2	[112,110,2]
7	f_1^3	[112,109,2]
7	f_2	[112,109,2]
7	f_3	[112,109,2]
7	$f_1 f_2$	[112,108,2]
7	$f_1 f_3$	[112,108,2]
7	f_1^4	[112,108,2]
7	f_1^5	[112,107,2]
7	$f_1^2 f_2$	[112,107,2]
7	$f_1^2 f_3$	[112,107,2]
7	f_1^6	[112,106,2]
7	$f_1^3 f_2$	[112,106,2]
7	$f_1^3 f_3$	[112,106,2]
7	f_2^2	[112,106,2]
7	$f_2 f_3$	[112,106,2]
7	f_3^2	[112,106,2]
7	$f_1^9 f_2$	[112,100,4]
7	$f_1^9 f_3$	[112,100,4]
7	$f_1^{10} f_2$	[112,99,4]
7	$f_1^{10} f_3$	[112,99,4]
7	$f_1^{16} f_2^{16} f_3^{15}$	[112,3,64]
7	$f_1^{16} f_2^{15} f_3^{16}$	[112,3,64]

7 Conclusion

In this paper, we extend the result of [1] about the Gray map to the polynomial residue ring $R_k = F_{2^m}[u]/\langle u^k\rangle$, where $2^{j-1}+1 \le k \le 2^j$ for some positive integer j. Some optimal linear cyclic code over F_2 and F_4 have been constructed via the Gray map. A nature problem is to extend the results to the ring $F_q[u]/\langle u^k\rangle$.

Acknowledgments The research is supported by National Natural Science Foundation of China (61370089) and Anhui Province Natural Science Research (KJ2013B107).

References

1. Abular, T., Siap, I.: Constacyclic codes over $F_2 + uF_2$. J. Franklin Inst. **345**, 520–529 (2009)
2. Amarra, M.C.V., Nemenzo, F.R.: On $(1-u)$ cyclic codes over $F_{p^k} + uF_{p^k}$. Appl. Math. Lett. **21**(11), 1129–1133 (2008)

3. Blake, F.: Codes over integer residue rings. Inf. Control **29**(4), 295–300 (1975)
4. Hammons, A.R., Kumar, P.V., Calderbank, A.R., ASloane, N.J.: The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inf. Theory **40**(2), 301–319 (1994)
5. Kai, X., Zhu, S., Li, P.: $(1+\lambda u)$ Constacyclic codes over $F_p[u]/\langle u^k\rangle$. J. Franklin Inst. **347**, 751–762 (2010)
6. Ling, S., Blackford, T.: $Z_{p^{k+1}}$-Linear codes. IEEE Trans. Inf. Theory **48**(7), 2592–2605 (2002)
7. Li, Y., Zhu, S.: A class of constacyclic codes over the ring $F_{p^m}+uF_{p^m}+\cdots+u^{k-1}F_{p^m}$. J. Hefei Univ. Technol. **35**(3), 408–411 (2013). (in chinese)
8. Nechaev, A.: The Kerdock code in a cyclic form. Discret. Math. Appl. **1**(1), 123–139 (1989)
9. Qian, J.F., Zhang, L.N., Zhu, S.X.: $(1+u)$ Constacyclic and cyclic codes over F_2+uF_2. Appl. Math. Lett. **19**(8), 820–823 (2006)
10. Qian, J.F.: Cyclic codes over finite rings, wireless communications, networking and mobile computing (WiCOM). In: 7th international conference, 1–4 (2011)
11. Shankar, P.: On BCH codes over arbitrary integer rings. IEEE Trans. Inf. Theory **25**(4), 480–483 (1979)
12. Sobhani, R., Esmaeili, E.: Some constacyclic and cyclic codes over $F_q[u]/\langle u^{t+1}\rangle$. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **93**(4), 808–813 (2010)
13. Tapia-Recillas, H., Vega, G.: Some constacyclic codes over $Z_{2^{k+1}}$ and binary quasi-cyclic codes. Discret. Appl. Math. **128**(1), 305–316 (2003)
14. Udomkavanich, P., Jitman, S.: On the Gray image of $1+u^m$ cyclic codes over $F_{p^k}+uF_{p^k}+\cdots+u^mF_{p^k}$. Int. J. Contemp Math. Sci. **4**(26), 1265–1272 (2009)
15. Wolfmann, J.: Negacyclic and cyclic codes over Z_4. IEEE Trans. Inf. Theory **45**(7), 2527–2532 (1999)