Yu *et al. SpringerPlus (2016) 5:1325*
DOI 10.1186/s40064-016-2717-0

SpringerPlus

RESEARCH Open Access

$(1+u)$-Constacyclic codes over Z_4+uZ_4

Haifeng Yu[1], Yu Wang[1*] and Minjia Shi[2]

*Correspondence: wangyu351@hfuu.edu.cn
[1] Department of Mathematics and Physics, Hefei University, Hefei, China
Full list of author information is available at the end of the article

Abstract

Constacyclic codes are an important class of linear codes in coding theory. Many optimal linear codes are directly derived from constacyclic codes. In this paper, $(1+u)$-constacyclic codes over Z_4+uZ_4 of any length are studied. A new Gray map between Z_4+uZ_4 and Z_4^4 is defined. By means of this map, it is shown that the Z_4 Gray image of a $(1+u)$-constacyclic code of length n over Z_4+uZ_4 is a cyclic code over Z_4 of length $4n$. Furthermore, by combining the classical Gray map between Z_4 and F_2^2, it is shown that the binary image of a $(1+u)$-constacyclic code of length n over Z_4+uZ_4 is a distance invariant binary quasi-cyclic code of index 4 and length $8n$. Examples of good binary codes are constructed to illustrate the application of this class of codes.

Keywords: Cyclic code, Constacyclic code, Quasi-cyclic code, Gray map

Background

Recently, several new classes of rings have been studied in connection with coding theory. Many optimal binary linear codes have been obtained from codes over these rings via some Gray map. In Yildiz and Karadenniz (2010a, b), the authors introduced the ring $F_2+uF_2+vF_2+uvF_2$ and discussed linear and self-dual codes over $F_2+uF_2+vF_2+uvF_2$. Later, the structures of cyclic codes and $(1+u)$-constacyclic codes over $F_2+uF_2+vF_2+uvF_2$ were studied and many optimal binary linear codes were constructed from such codes in Yildiz and Karadenniz (2011a, b). More generally, cyclic codes over the ring R_k were investigated in Dougherty et al. (2012). Although the rings mentioned above are not finite chain rings, they have rich algebraic structures and produce binary codes with large automorphism groups and new binary self-dual codes. This demonstrates that linear codes over such non-chain rings have been received increasing attention (see Dougherty et al. 2012; Kai et al. 2012; Shi 2014; Shi et al. 2012; Siap et al. 2012; Zhu and Wang 2011). More recently, linear codes over the non-chain ring Z_4+uZ_4, where $u^2=0$, have been explored in Yildiz and Karadenniz (2014). The authors defined a linear Gray map from Z_4+uZ_4 to Z_4^2 and a non-linear Gray map from Z_4+uZ_4 to $(F_2+uF_2)^2$, and used them to successfully construct formally self-dual codes over Z_4 and good non-linear codes over F_2+uF_2. In Yildiz and Aydin (2014), the structure of cyclic codes over Z_4+uZ_4 was determined and many new linear codes over Z_4 were obtained from them. Motivated by the works in Yildiz and Aydin (2014) and Yildiz and Karadenniz (2014), we focus on constacyclic codes over Z_4+uZ_4 and intend to construct good binary codes from such codes.

Springer Open

The ring $Z_4 + uZ_4$ is a finite commutative ring with characteristic 4, where $u^2 = 0$. The purpose of this paper is to investigate a class of constacyclic codes over this ring, that is, $(1 + u)$-constacyclic codes over $Z_4 + uZ_4$. Constacyclic codes over finite commutative rings were first introduced by Wolfmann (1999), where it was proved that the binary image of a linear negacyclic code over Z_4 is a binary cyclic code (not necessarily linear). In Kai et al. (2012), the authors introduced a composite Gray map from $F_2 + uF_2 + vF_2 + uvF_2$ to F_2^4 and proved that the image of a $(1 + u)$-constacyclic code of length n over $F_2 + uF_2 + vF_2 + uvF_2$ under the Gray map is a distance invariant binary quasi-cyclic code of index 2 and length $4n$. It is known that the structure of $Z_4 + uZ_4$ is similar to that of $F_2 + uF_2 + vF_2 + uvF_2$. It is natural to ask if there exists a Gray map such that the Gray image of a linear code over $Z_4 + uZ_4$ has good structure. For this, we introduce a new Gray map from $Z_4 + uZ_4$ to Z_4, and explore the images of $(1 + u)$-constacyclic codes over $Z_4 + uZ_4$ under this Gray map.

$(1 + u)$-Constacyclic codes over $Z_4 + uZ_4$

Throughout this paper, let R denote the ring $Z_4 + uZ_4$ with $u^2 = 0$. Any element in R can be written as $a + bu$, where $a, b \in Z_4$. The element $a + bu$ is a unit in R if and only if a is a unit in Z_4. The ring R is a local Frobenius ring, but not a finite chain ring. It has a total of 7 ideals given by $I_0 = \{0\} \subseteq I_{2u} = 2u(Z_4 + uZ_4) = \{0, 2u\} \subseteq I_u, I_2, I_{2+u} \subseteq I_{2,u} \subseteq I_1 = Z_4 + uZ_4$, where

$$\begin{aligned}
I_u &= u(Z_4 + uZ_4) = \{0, u, 2u, 3u\},\\
I_2 &= 2(Z_4 + uZ_4) = \{0, 2, 2u, 2 + 2u\},\\
I_{2+u} &= (2 + u)(Z_4 + uZ_4) = \{0, 2 + u, 2u, 2 + 3u\},\\
I_{2,u} &= \{0, 2, u, 2u, 3u, 2 + u, 2 + 2u, 2 + 3u\}.
\end{aligned}$$

A code over R of length n is a nonempty subset of R_n, and a code is linear over R of length n if it is an R-submodule of R_n. For some fixed unit $\lambda \in R$, the λ-constacyclic shift τ on R_n is the shift $\tau(c_0, c_1, \ldots, c_{n-1}) = (\lambda c_{n-1}, c_0, \ldots, c_{n-2})$. A linear code C of length n over R is λ-constacyclic if the code is invariant under the λ-constacyclic shift τ. We identify the code-word $c = (c_0, c_1, \ldots, c_{n-1})$ with its polynomial representation $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$. Then $xc(x)$ corresponds to a λ-constacyclic shift of $c(x)$ in the ring $R[x]/(x^n - \lambda)$. Thus, λ-constacyclic codes of length n over R can be identified as ideals in the ring $R[x]/(x^n - \lambda)$. From the above discuss, we have the following result.

Proposition 1 *A subset C of R_n is a linear cyclic code of length n if and only if C is an ideal of $A_n = R[x]/(x^n - 1)$. A subset C of R_n is a linear $(1 + u)$-constacyclic code of length n over R if and only if C is an ideal of $B_n = R[x]/(x^n - 1 - u)$.*

Now, we determine a set of generators of $(1 + u)$-constacyclic codes for an arbitrary length over R. We begin by recalling a unique set of generators for cyclic codes over Z_4.

Lemma 2 [cf. Abualrub and Siap (2006), Theorem 6] *Let C be a cyclic code of length n over Z_4. Then*

1. *If n is odd then* $C = \langle g(x), 2a(x)\rangle = \langle g(x) + 2a(x)\rangle$, *where* $g(x), a(x)$ *are binary polynomials with* $a(x)\big|g(x)\,|(x^n - 1) \mod 2$.
2. *If n is even then*
   - 2.1 *If* $g(x) = a(x)$, *then* $C = \langle g(x) + 2p(x)\rangle$, *where* $g(x), p(x)$ *are binary polynomials with* $g(x)|(x^n - 1) \mod 2$, *and* $g(x)\Big|p(x)\frac{(x^n-1)}{g(x)}$,
   - 2.2 $C = \langle g(x) + 2p(x), 2a(x)\rangle$, *where* $g(x), a(x)$ *and* $p(x)$ *are binary polynomials with* $a(x)\big|g(x)\,|(x^n - 1) \mod 2$, $a(x)\Big|p(x)\frac{(x^n-1)}{g(x)}$ *and* $\deg g(x) > \deg a(x) > \deg p(x)$.

For a linear code C of length n over R, we can denote two linear codes of length n over Z_4 as follows:

1. The torsion code $Tor(C) = \{x \in Z_4^n | ux \in C\}$,
2. The residue code $\mathrm{Res}(C) = \{x \in Z_4^n \big| \exists y \in Z_4^n : x + uy \in C\}$.

Consider the homomorphism $\varphi : R \to Z_4$ defined by $\varphi(a + ub) = a$. The map φ extends naturally to a ring homomorphism $\varphi : R_n \to Z_4(n) = \frac{Z_4[x]}{(x^n-1)}$ defined by

$$\varphi(c_0 + c_1x + \cdots, c_{n-1}x^{n-1}) = \varphi(c_0) + \varphi(c_1)x + \cdots + \varphi(c_{n-1})x^{n-1}.$$

Acting φ on C over R, we define a ring homomorphism

$$\varphi : C \to \mathrm{Res}(C), \varphi(a + ub) = a \quad \text{where } a, b \in Z_4.$$

We can easily obtain that $Ker\varphi \cong Tor(C)$ and $\varphi(C) = Res(C)$. By the first isomorphism theorem of finite groups, we have $|C| = |Tor(C)||\mathrm{Res}(C)|$. It is obvious that the image of C under the map φ is a cyclic code of length n over Z_4. Combining the above discussion with Lemma 2, we can obtain the set of generators for cyclic codes of length n over R.

Theorem 3 *Let C be a* $(1 + u)$*-constacyclic code of length n over R. Then*

1. *If n is odd then* $C = \langle g_1(x) + 2a_1(x) + ub(x), u(g_2(x) + 2a_2(x))\rangle$, *where* $b(x)$ *is a polynomial in* $Z_4[x]$ *and* $g_i(x), a_i(x)$ *are binary polynomials with* $a_i(x)\big|g_i(x)\,|(x^n - 1) \mod 2$ *for* $i = 1, 2$.
2. *If n is even then*
   - 2.1 *If* $g_i(x) = a_i(x)$, *then* $C = \langle g_1(x) + 2p_1(x) + ud(x), u(g_2(x) + 2p_2(x))\rangle$, *where* $d(x)$ *is a polynomial in* $Z_4[x]$, $g_i(x), p_i(x)$ *are binary polynomials with* $g_i(x)|(x^n - 1) \mod 2$ *and* $g_i(x)\Big|p_i(x)\frac{(x^n-1)}{g_i(x)}$, *for* $i = 1, 2$;
   - 2.2 $C = \langle g_1(x) + 2p_1(x) + ue_1(x), 2a_1(x) + ue_2(x), ug_2(x) + 2up_2(x), 2a_2(x)\rangle$, *where* $e_i(x)$ *is a polynomial in* $Z_4[x]$, *and* $g_i(x), a_i(x), p_i(x)$ *are binary polynomials with* $a_i(x)\big|g_i(x)\,|(x^n - 1) \mod 2$, $a_i(x)\Big|p_i(x)\frac{(x^n-1)}{g_i(x)}$ *and* $\deg g_i(x) > \deg a_i(x) > \deg p_i(x)$, *for* $i = 1, 2$.

Proof We only give the proof of the part (1), and the proof of the part (2) is similar.

Assume that n is odd. Let C be a $(1 + u)$-constacyclic code of length n over R. Then the image of C under the map φ is $\mathrm{Res}(C)$, which is a cyclic code of length n over Z_4. By Lemma 2, we have $\varphi(C) = \langle g_1(x) + 2a_1(x)\rangle$, where $g_1(x)$, $a_1(x)$ are binary polynomials with $a_1(x)\big|g_1(x)\,|(x^n - 1) \mod 2$. Thus, there exists $b(x) \in Z_4[x]$ such that $g_1(x) + 2a_1(x) + ub(x) \in C$.

Furthermore, note that $Ker\varphi$ is a cyclic code of length n over $Z_4 + uZ_4$, so $Ker\varphi = u\ \langle g_2(x) + 2a_2(x)\rangle$, where $g_2(x)$, $a_2(x)$ are binary polynomials with $a_2(x)\big|g_2(x)\,|(x^n - 1)$ mod 2. Hence, $\langle g_1(x) + 2a_1(x) + ub(x), u(g_2(x) + 2a_2(x))\rangle \subseteq C$.

On the other hand, for any $f(x) = f_1(x) + uf_2(x) \in C$, where $f_i(x) \in Z_4[x]$, *for* $i = 1, 2$, it is obvious that $f_1(x) \in \varphi(C)$. Hence,

$$\begin{aligned} f(x) &= f_1(x) + uf_2(x) \\ &= m(x)(g_1(x) + 2a_1(x)) + uf_2(x) \\ &= m(x)(g_1(x) + 2a_1(x) + ub(x)) + u(f_2(x) - m(x)b(x)) \end{aligned}$$

Since $u(f_2(x) - m(x)b(x)) \in Ker\varphi$, we have

$$f(x) \in \langle g_1(x) + 2a_1(x) + ub(x), u\big(g_2(x) + 2a_2(x)\big)\rangle.$$

This shows that $C \subseteq \langle g_1(x) + 2a_1(x) + ub(x), u(g_2(x) + 2a_2(x))\rangle$.

Thus, $C = \langle g_1(x) + 2a_1(x) + ub(x), u(g_2(x) + 2a_2(x))\rangle$. $\square$

Gray images of $(1 + u)$-constacyclic codes over R

A new Gray map

Recall that the Gray map ϕ_1 from Z_4 to F_2^2 is defined as $\phi_1(z) = (q, q + r)$ where $z = r + 2q$ with $r, q \in F_2$. The map ϕ_1 can be extended to Z_4^n as follows:

$$\begin{aligned} &\phi_1 : Z_4^n \to F_2^{2n} \\ &\quad (z_0, z_1, \ldots, z_{n-1}) \to (q_0, q_1, \ldots, q_{n-1}, q_0 + r_0, q_1 + r_1, \ldots, q_{n-1} + r_{n-1}) \end{aligned}$$

where $z_i = r_i + 2q_i$ with r_i, $q_i \in F_2$ *for* $0 \le i \le n - 1$. It is known that ϕ_1 is a distance-preserving map from Z_4^n (Lee distance) to F_2^{2n} (Hamming distance).

Now, we define a map ϕ_2 from R^n to Z_4^{4n}. First note that each element $c \in R$ can be expressed as $c = a + ub$, where $a, b \in Z_4$. The map ϕ_2 is defined as

$$\phi_2(c) = (b + 3a, b + 2a, b + a, b).$$

Clearly, this map can be also extended to R^n as follows:

$$\begin{aligned} &\phi_2 : R^n \to Z_4^{4n} \\ &\quad (c_0, c_1, \ldots, c_{n-1}) \to (b_0 + 3a_0, b_1 + 3a_1, \ldots, b_{n-1} + 3a_{n-1}, b_0 + 2a_0, b_1 \\ &\quad + 2a_1, \ldots, b_{n-1} + 2a_{n-1}, b_0 + a_0, b_1 + a_1, \ldots, b_{n-1} + a_{n-1}, b_0, b_1, \ldots, b_{n-1}) \end{aligned}$$

where $c_i = a_i + ub_i$ with a_i, $b_i \in Z_4$ *for* $0 \le i \le n - 1$.

It is well-known that the homogeneous weight has many applications for codes over finite rings and provides a good metric for the underlying ring in constructing superior codes. Next, we define a homogeneous weight on R. We first recall the definition of the homogeneous weight on a finite ring K.

Definition 4 *[cf.* Greferath and O'Sullivan (2004), *Definition 1.1]* A real-valued function w on the finite ring K is called a (left) homogeneous weight if w(0) = 0 and the following is true:

1. For all x, y ∈ K, Kx = Ky implies that w(x) = w(y) holds.
2. There exists a real number γ such that $\sum_{y \in Kx} w(y) = \gamma|Kx|$ for all $x \in K\backslash\{0\}$.

Right homogenous weight is defined accordingly. If a weight is both left homogenous and right homogeneous, we call it simply as a homogeneous weight.

For any element $c = a + ub \in R$, we assign the weight, denoted by $w_{\text{hom}}(c)$, as $w_L(b + 3a, b + 2a, b + a, b)$, i.e., $w_{\text{hom}}(c) = w_L(b + 3a, b + 2a, b + a, b)$. By simple calculation, we can obtain the weight of any element $x = a + ub \in R$ as follows:

$$w_{\text{hom}}(x) = \begin{cases} 0, & x = 0 \\ 8, & x = 2u \\ 4, & \text{otherwise} \end{cases}$$

It is easy to verify that the weight defined above meets the conditions of Definition 4, hence it is actually a homogeneous weight on R. The homogeneous distance of a linear code over R, denoted by $d_{\text{hom}}(C)$, is defined as the minimum homogeneous weight of nonzero codewords of C. It can be checked that the map ϕ_2 is a distance-preserving map from R^n (homogeneous distance) to Z_4^{4n} (Lee distance). Using the maps ϕ_1 and ϕ_2, we can define a composite map $\phi : R \to F_2^8$ as $\phi = \phi_1\phi_2$. Thus, we have obtained three distance-preserving maps as follows:

$$\phi_1 : \left(Z_4^n, \text{ Lee distance}\right) \to \left(F_2^{2n}, \text{ Hamming distance}\right),$$
$$\phi_2 : \left(R^n, \text{homogeneous distance}\right) \to \left(Z_4^{4n}, \text{ Lee distance}\right),$$
$$\phi : \left(R^n, \text{ homogeneous distance}\right) \to \left(F_2^{8n}, \text{ Hamming distance}\right).$$

Gray images of (1 + u)-constacyclic codes

Lemma 5 *Let ϕ_2 be defined as above. Let τ be the $(1 + u)$-constacyclic shift on R^n and σ be the cyclic shift on Z_4^{4n}. Then $\phi_2\tau = \sigma\phi_2$.*

Proof Let $c = (c_0, c_1, \ldots, c_{n-1}) \in R^n$. Let $c_i = a_i + ub_i$ where $a_i, b_i \in Z_4$ *for* $0 \le i \le n - 1$. From definitions, we have

$$\begin{aligned}\phi_2(c) = (&\mathrm{b}_0 + 3a_0, \mathrm{b}_1 + 3a_1, \ldots, \mathrm{b}_{n-1} + 3a_{n-1}, \mathrm{b}_0 + 2a_0, \mathrm{b}_1 + 2a_1, \ldots, \mathrm{b}_{n-1} \\ &+ 2a_{n-1}, \mathrm{b}_0 + a_0, \mathrm{b}_1 + a_1, \ldots, \mathrm{b}_{n-1} + a_{n-1}, \mathrm{b}_0, \mathrm{b}_1, \ldots, \mathrm{b}_{n-1})\end{aligned}$$

Hence,

$$\begin{aligned}\sigma\phi_2(c) = (&\mathrm{b}_{n-1}, \mathrm{b}_0 + 3a_0, \mathrm{b}_1 + 3a_1, \ldots, \mathrm{b}_{n-1} + 3a_{n-1}, \mathrm{b}_0 + 2a_0, \mathrm{b}_1 + 2a_1, \ldots, \mathrm{b}_{n-1} \\ &+ 2a_{n-1}, \mathrm{b}_0 + a_0, \mathrm{b}_1 + a_1, \ldots, \mathrm{b}_{n-1} + a_{n-1}, \mathrm{b}_0, \mathrm{b}_1, \ldots, \mathrm{b}_{n-2})\end{aligned}$$

On the other hand,

$$\begin{aligned}\tau(c) &= ((1 + u)c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \\ &= (a_{n-1} + u(a_{n-1} + b_{n-1}), a_0 + ub_0, \ldots, a_{n-2} + ub_{n-2})\end{aligned}$$

Thus,

$$\begin{aligned}\phi_2\tau(c) = (&\mathrm{b}_{n-1}, \mathrm{b}_0 + 3a_0, \mathrm{b}_1 + 3a_1, \ldots, \mathrm{b}_{n-1} + 3a_{n-1}, \mathrm{b}_0 + 2a_0, \mathrm{b}_1 + 2a_1, \ldots, \mathrm{b}_{n-1} \\ &+ 2a_{n-1}, \mathrm{b}_0 + a_0, \mathrm{b}_1 + a_1, \ldots, \mathrm{b}_{n-1} + a_{n-1}, \mathrm{b}_0, \mathrm{b}_1, \ldots, \mathrm{b}_{n-2})\end{aligned}$$

The result follows. $\square$

Theorem 6 *A linear code C of length n over R is a $(1+u)$-constacyclic code if and only if $\phi_2(C)$ is a cyclic code of length $4n$ over Z_4.*

Proof If C is a $(1+u)$-constacyclic code, then using Lemma 5 we have

$$\sigma(\phi_2(C)) = \phi_2(\tau(C)) = \phi_2(C).$$

Hence, $\phi_2(C)$ is a cyclic code of length $4n$ over Z_4.
Conversely, if $\phi_2(C)$ is a cyclic code of length $4n$ over Z_4, then using Lemma 5 again we get $\phi_2(\tau(C)) = \sigma(\phi_2(C)) = \phi_2(C)$.
Note that ϕ_2 is injection, so $\tau(C) = C$.
Thus, we immediately have the following result. □

Corollary 7 *The image of a $(1+u)$-constacyclic code of length n over R under the map ϕ_2 is a distance invariant cyclic code of length $4n$ over Z_4.*

Let σ be the cyclic shift. For any positive integer s, let σ_s be the quasi-shift given by

$$\sigma_s(a^{(1)}\left|a^{(2)}\right|\cdots\left|a^{(s)}\right.) = (\sigma(a^{(1)})\left|\sigma(a^{(2)})\right|\cdots\left|\sigma(a^{(s)})\right.)$$

where $a^{(1)}, a^{(2)}, \ldots, a^{(s)} \in F_2^{2n}$ and "|"denotes the usual vector concatenation. A binary quasi-cyclic code C of index s and length $2ns$ is a subset of $(F_2^{2n})^s$ such that $\sigma_s(C) = C$.

Lemma 8 *Let ϕ be defined as above and let τ be the $(1+u)$-constacyclic shift on R^n. Then $\phi\tau = \sigma_4\phi$.*

Proof Let $r = (r_0, r_1, \ldots, r_{n-1}) \in R^n$. Let $r_i = a_i + 2b_i + uc_i + 2ud_i$ where $a_i, b_i, c_i, d_i \in F_2$ *for* $0 \le i \le n-1$. Then we have

$$\begin{aligned}\phi(r) = (&a_0 + b_0 + d_0, \ldots, a_{n-1} + b_{n-1} + d_{n-1}, a_0 + d_0, \ldots, a_{n-1} + d_{n-1}, b_0 + d_0, \ldots, b_{n-1}\\ &+ d_{n-1}, d_0, \ldots, d_{n-1}, b_0 + c_0 + d_0, \ldots, b_{n-1} + c_{n-1} + d_{n-1}, a_0 + c_0 + d_0, \ldots, a_{n-1} + c_{n-1}\\ &+ d_{n-1}, a_0 + b_0 + c_0 + d_0, \ldots, a_{n-1} + b_{n-1} + c_{n-1} + d_{n-1}, c_0 + d_0, \ldots, c_{n-1} + d_{n-1})\end{aligned}$$

and so

$$\begin{aligned}\sigma_4\phi(r) = (&a_{n-1} + d_{n-1}, a_0 + b_0 + d_0, \ldots, a_{n-1} + b_{n-1} + d_{n-1}, a_0 + d_0, \ldots, a_{n-2}\\ &+ d_{n-2}, d_{n-1}, b_0 + d_0, \ldots, b_{n-1} + d_{n-1}, d_0, \ldots, d_{n-2}, a_{n-1} + c_{n-1} + d_{n-1}, b_0 + c_0\\ &+ d_0, \ldots, b_{n-1} + c_{n-1} + d_{n-1}, a_0 + c_0 + d_0, \ldots, a_{n-2} + c_{n-2} + d_{n-2}, c_{n-1}\\ &+ d_{n-1}, a_0 + b_0 + c_0 + d_0, \ldots, a_{n-1} + b_{n-1} + c_{n-1} + d_{n-1}, c_0 + d_0, \ldots, c_{n-2} + d_{n-2})\end{aligned}$$

On the other hand,

$$\begin{aligned}\tau(r) &= ((1+u)r_{n-1}, r_0, r_1, \ldots, r_{n-2})\\ &= ((a_{n-1} + 2b_{n-1}) + u(a_{n-1} + c_{n-1}) + 2u(b_{n-1} + d_{n-1}), a_0\\ &\quad + 2b_0 + uc_0 + 2ud_0, \ldots, a_{n-2} + 2b_{n-2} + uc_{n-2} + 2ud_{n-2})\end{aligned}$$

Hence,

$$\phi\tau(r) = (a_{n-1} + d_{n-1}, a_0 + b_0 + d_0, \ldots, a_{n-1} + b_{n-1} + d_{n-1}, a_0 + d_0, \ldots, a_{n-2} + d_{n-2}, d_{n-1}, b_0 + d_0, \ldots, b_{n-1} + d_{n-1}, d_0, \ldots, d_{n-2}, a_{n-1} + c_{n-1} + d_{n-1}, b_0 + c_0 + d_0, \ldots, b_{n-1} + c_{n-1} + d_{n-1}, a_0 + c_0 + d_0, \ldots, a_{n-2} + c_{n-2} + d_{n-2}, c_{n-1} + d_{n-1}, a_0 + b_0 + c_0 + d_0, \ldots, a_{n-1} + b_{n-1} + c_{n-1} + d_{n-1}, c_0 + d_0, \ldots, c_{n-2} + d_{n-2})$$

This completes the proof. □

Theorem 9 *A linear code C of length n over R is a $(1+u)$-constacyclic code if and only if $\phi(C)$ is a binary quasi-cyclic code of index 4 and length $8n$.*

Proof If C is $(1+u)$-constacyclic, then using Lemma 8 we have

$$\sigma_4(\phi(C)) = \phi(\tau(C)) = \phi(C).$$

Hence, $\phi(C)$ is a binary quasi-cyclic code of index 4 and length $8n$. Conversely, if $\phi(C)$ is a binary quasi-cyclic code of index 4 and length $8n$, then using Lemma 8 again we get $\phi(\tau(C)) = \sigma_4(\phi(C)) = \phi(C)$.

Also, ϕ is injection, hence $\tau(C) = C$. □

From Theorem 9 and the definition of the map ϕ, we immediately have the following result.

Corollary 10 *The image of a $(1+u)$-constacyclic code of length n over R under the map $\phi$is a distance invariant binary quasi-cyclic code of index 4 and length $8n$.*

Now, we can construct some binary codes with good parameters based on the new Gray map.

Example 11 Consider $(1+u)$-constacyclic codes over $Z_4 + uZ_4$ of length 3. In $F_2[x]$, $x^3 - 1$=$(x-1)(x^2+x+1)$.

1. In Theorem 3, we take $g_1(x) = x$−1, $a_1(x) = 1$, $b(x) = 3x$, and $g_2(x) = a_2(x) = x^3 - 1$. Then, we obtain the $(1+u)$-constacyclic code C_1 over R of length 3 with generator polynomial $(1+u)x+1$. That is $\langle(1-u)x+1\rangle = \langle x+(1+u)\rangle$, It is easy to see that both $\mathrm{Res}(C_1)$ and $Tor(C_1)$ have size 16. Moreover, $d_{\mathrm{hom}}(C_1) = 8$. By Corollary 7, $\phi_2(C_1)$ is a Z_4-linear code of length 12 with size 256 and Lee distance 8. By Theorem 9, $\phi(C_1)$ is a binary quasi-cyclic code of index 4 and length 24. We find that $\phi(C_1)$ is a non-linear binary code with parameters (24, 256, 8). The code $\phi(C_1)$ attains the performance of the best-known binary linear code with the same parameters based on Grassl's codetables (Grassl 2007).
2. In Theorem 3, $g_1(x) = x^3 + 1, a_1(x) = 1, b(x) = 3, g_2(x) = x + 1,$ and $a_2(x) = x + 1$. Then, we obtain the code $C_2 = \langle 3u(x+1)\rangle = \langle u(x+1)\rangle$. Obviously, $\mathrm{Res}(C_2) = \{0\}$ and $Tor(C_2)$ has size 4. By Corollary 7, $\phi(C_2)$ is a Z_4-linear code of length 12 with size 4 and Lee distance 16. By Theorem 9, $\phi(C_2)$ is a binary quasi-cyclic code of index 4

and length 24. The code $\phi(C_2)$ is a linear binary code with parameters [24, 2, 16], which is optimal based on Grassl's codetables (Grassl 2007).

Conclusion

We study the structure of $(1 + u)$-constacyclic codes over $Z_4 + uZ_4$ of an arbitrary length, and obtain the examples of good binary codes from them. Our results show that a $(1 + u)$-constacyclic code of length n over $Z_4 + uZ_4$ under certain map is equivalent to a cyclic code of length $4n$ over Z_4. Furthermore, we discuss the relation between $(1 + u)$-constacyclic codes of length n over $Z_4 + uZ_4$ and their binary Gray images. It would be interesting to study other constacyclic codes over $Z_4 + uZ_4$ and use them to construct more good codes over Z_4 or F_2.

Authors' contributions

HFY prepared the manuscript, YW participated in its design, and helped to draft the manuscript, MJS revised the manuscript. All authors read and approved the final manuscript.

Author details

[1] Department of Mathematics and Physics, Hefei University, Hefei, China. [2] School of Mathematical Sciences, Anhui University, Hefei, China.

Acknowledgements

This work was supported by the Natural Science Fund of Education Department of Anhui province under Grant Nos. KJ2015A226, KJ2015B1105916, and Key Projects of Support Program for Outstanding Young Talents in Colleges and Universities under Grant No. gxyqZD2016270.

Competing interests

The authors declare that they have no competing interests.

Received: 9 January 2016 Accepted: 29 June 2016
Published online: 11 August 2016

References

Abualrub T, Siap I (2006) Reversible quaternary cyclic codes. In: Proceedings of the 9th WSEAS international conference on applied mathematics, pp 441–446

Dougherty ST, Karadeniz S, Yildiz B (2012) Cyclic codes over R_k. Des Codes Cryptogr 63:113–126

Grassl M (2007) Bounds on the minimum distance of linear codes and quantum codes. http://www.codetables.de

Greferath M, O'Sullivan ME (2004) On bounds for codes over Frobenius rings under homogeneous weights. Discrete Math 289:11–24

Kai XS, Zhu SX, Wang L (2012) A family of constacyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$. J Syst Sci Complex 25:1032–1040

Shi MJ (2014) Optimal p-ary codes from constacyclic codes over a non-chain ring R. Chin J Electron 23:773–777

Shi MJ, Yang SL, Zhu SX (2012) Good p-ary quasi-cyclic codes from cyclic codes over $F_p + vF_p$. J Syst Sci Complex 25:375–384

Siap I, Abualrub T, Yildiz B (2012) One generator quasi-cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$. J Frankl Inst 349:284–292

Wolfmann J (1999) Negacyclic and cyclic codes over Z_4. IEEE Trans Inf Theory 45:2527–2532

Yildiz B, Aydin N (2014) On cyclic codes over $Z_4 + uZ_4$ and their Z_4-images. Int J Inf Coding Theory 2:226–237

Yildiz B, Karadenniz S (2010a) Linear codes over $F_2 + uF_2 + vF_2 + uvF_2$. Des Codes Cryptogr 54:61–81

Yildiz B, Karadenniz S (2010b) Self-dual codes over $F_2 + uF_2 + vF_2 + uvF_2$. J Frankl Inst 347:1888–1894

Yildiz B, Karadenniz S (2011a) Cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$. Des Codes Cryptogr 58:221–234

Yildiz B, Karadenniz S (2011b) $(1 + v)$-constacyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$. J Frankl Inst 348:2625–2632

Yildiz B, Karadenniz S (2014) Linear codes over $Z_4 + uZ_4$: MacWilliams identities, pro-jections, and formally self-dual codes. Finite Fields Appl 27:24–40

Zhu SX, Wang L (2011) A class of constacyclic codes over $F_p + vF_p$ and its Gray image. Discrete Math 311:2377–2682