On \((1 - u^m)\)-Cyclic Codes over
\[F_2 + uF_2 + u^2F_2 + u^3F_2 + \ldots + u^mF_2\]

Yasemin Cengellenmis

Department of Mathematics, Faculty of Science and Arts
Trakya University, 22030 Edirne, Turkey
ycengellenmis@yahoo.com

Abstract
A new Gray map between codes over \(F_2 + uF_2 + u^2F_2 + u^3F_2 + \ldots + u^mF_2\) and codes over \(F_2\) is defined. It is proved that the Gray image of a linear \((1 - u^m)\)-cyclic code over \(F_2 + uF_2 + u^2F_2 + u^3F_2 + \ldots + u^mF_2\) of length \(n\) is a binary distance invariant quasi-cyclic code of index \(2^{m-1}\) and length \(2^mn\). It is also proved that if \(n\) is odd, then every code of length \(2^mn\) over \(F_2\) which is the Gray image of a linear cyclic code of length \(n\) over \(F_2 + uF_2 + u^2F_2 + u^3F_2 + \ldots + u^mF_2\) is equivalent to a quasi-cyclic code of index \(2^{m-1}\).

Mathematics Subject Classification: 94B15, 94B60

Keywords: Gray map; Cyclic codes; Quasi-cyclic code

1. Introduction
It was introduced linear \((1 + u)\) constacyclic codes and cyclic codes over \(F_2 + uF_2\) and characterized codes over \(F_2\) which are the Gray images of \((1 + u)\) constacyclic codes or cyclic codes over \(F_2\), in [?]. In [?], they extended the result of [?] to codes over the commutative ring \(F_p^k + uF_p^k\) where \(p\) is a prime, \(k \in \mathbb{N}\) and \(u^2 = 0\). In [?], it was introduced \((1 - u^2)\)-cyclic codes over \(F_2 + uF_2 + u^2F_2\) and characterized codes over \(F_2\) which are the Gray images of \((1 - u^2)\)-cyclic codes or cyclic codes over \(F_2 + uF_2 + u^2F_2\). In this paper, it is defined a distance preserving map from \(F_2 + uF_2 + u^2F_2 + u^3F_2 + \ldots + u^mF_2\) to \(F_2\) and characterized codes over \(F_2\) which are the Gray images of \((1 - u^m)\)-cyclic codes or cyclic codes over \(F_2 + uF_2 + u^2F_2 + u^3F_2 + \ldots + u^mF_2\).
2. Preliminaries

Let $R$ be the commutative ring $F_2 + uF_2 + u^2F_2 + u^3F_2 + \ldots + u^mF_2$ where $m \in N$, $u^{m+1} = 0$. The ring is endowed with the obvious addition and multiplication with the property that $u^{m+1} = 0$. Then $R$ is a finite chain ring with maximal ideal $uR$ and residue field $F_2$.

Let the $C$ be a code of length $n$ over $R$ and $P(C)$ be its polynomial representation, i.e,

$$P(C) = \{ \sum_{i=0}^{n-1} r_i x^i | (r_0, \ldots, r_{n-1}) \in C \}$$

Let $\sigma$ and $\nu$ be maps from $R^n$ to $R^n$ given by

$$\sigma(r_0, \ldots, r_{n-1}) = (r_{n-1}, r_0, \ldots, r_{n-2})$$

and

$$\nu(r_0, \ldots, r_{n-1}) = ((1 - u^m)r_{n-1}, r_0, \ldots, r_{n-2})$$

Then $C$ is said to be cyclic if $\sigma(C) = C$ and $(1 - u^m)$ - cyclic if $\nu(C) = C$. A code $C$ of length $n$ over $R$ is cyclic if and only if $P(C)$ is an ideal of $R[x]/(x^n - 1)$.

A code $C$ of length $n$ over $R$ is $(1 - u^m)$ - cyclic if and only if $P(C)$ is an ideal of $R[x]/(x^n - (1 - u^m))$.

Let $a \in F_2^{2mn}$ with $a = (a_0, a_1, \ldots, a_{2^{2m-1}n-1}) = (a^{(0)} | \ldots | a^{(2^{2m-1}-1)})$, $a^{(i)} \in F_2^n$ for all $i = 0, 1, 2, \ldots, 2^{2m-1}-1$. Let $\sigma^{(2^{2m-1})}$ be the map from $F_2^{2mn}$ to $F_2^{2mn}$ given by $\sigma^{(2^{2m-1})}(a) = (\tilde{\sigma}(a^{(0)})) | \ldots | \tilde{\sigma}(a^{(2^{2m-1}-1)}))$ where $\tilde{\sigma}$ is the usual cyclic shift $(c_0, \ldots, c_{2n-1}) \mapsto (c_{2n-1}, c_0, \ldots, c_{2n-2})$ on $F_2^{2n}$. A code $\tilde{C}$ of length $2^{2m}n$ over $F_2$ is said to be quasi-cyclic of index $2^{2m-1}$ if $\sigma^{(2^{2m-1})}(\tilde{C}) = \tilde{C}$.

In [?], the homogeneous weight on arbitrary finite chain rings is defined. If it is given for the case of the ring $R$, the homogeneous weight of $r \in R$ is given by

$$w_{hom}(r) = \begin{cases} 2^{m-1} & \text{if } r \in R \setminus Ru \\ 2^{m} & \text{if } r \in Ru \setminus \{0\} \\ 0 & \text{otherwise} \end{cases}$$

This extends to a weight function in $R^n$. For $c = (c_0, c_1, \ldots, c_{n-1}) \in R^n$,

$$w_{hom}(c) = \sum_{i=0}^{n-1} w_{hom}(c_i)$$
The homogeneous distance $d_{\text{hom}}(x, y)$ between any distinct vectors $x, y \in R^n$ is defined to be $w_{\text{hom}}(x - y)$

3. The Gray images of $(1 - u^m)$-cyclic codes over $F_2 + uF_2 + u^2F_2 + u^3F_2 + \ldots + u^mF_2$

We define the Gray map $\phi$ on $R^n$ as follows

$$\phi : R^n \to F_2^{2n}$$

$$x_0 + ux_1 + u^2x_2 + \ldots + u^mx_m \mapsto (x_m, x_m \oplus x_0, x_m \oplus x_1, x_m \oplus x_1 \oplus x_0,$$

$$x_m \oplus x_2, x_m \oplus x_2 \oplus x_0, x_m \oplus x_2 \oplus x_1, x_m \oplus x_1 \oplus x_0, x_m \oplus x_3, x_m \oplus x_3 \oplus x_0, x_m \oplus x_3 \oplus x_1, x_m \oplus x_1 \oplus x_0, x_m \oplus x_3 \oplus x_2, x_m \oplus x_3 \oplus x_2 \oplus x_0, x_m \oplus x_3 \oplus x_2 \oplus x_1, x_m \oplus x_2 \oplus x_1 \oplus x_0,$$

$$x_m \oplus x_4, x_m \oplus x_4 \oplus x_0, x_m \oplus x_4 \oplus x_1, x_m \oplus x_1 \oplus x_0, x_m \oplus x_4 \oplus x_2, x_m \oplus x_4 \oplus x_2 \oplus x_0, x_m \oplus x_4 \oplus x_2 \oplus x_1, x_m \oplus x_2 \oplus x_1 \oplus x_0, x_m \oplus x_4 \oplus x_3, x_m \oplus x_4 \oplus x_3 \oplus x_0, x_m \oplus x_4 \oplus x_3 \oplus x_1, x_m \oplus x_3 \oplus x_1 \oplus x_0, x_m \oplus x_4 \oplus x_3 \oplus x_2, x_m \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_0, x_m \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1, x_m \oplus x_3 \oplus x_1 \oplus x_0, x_m \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1, x_m \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_0,$$

$\ldots, \ldots, \ldots, x_m \oplus x_{m-1} \oplus \ldots \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_0)$

where $\oplus$ is componentwise addition in $F_2$. The Gray map $\phi$ is an isometry from $(R^n, d_{\text{hom}})$ to $F_2^{2m}$ under the Hamming distance.

**Proposition 3.1** $\phi \nu = \sigma^{\otimes 2^{m-1}} \phi$.

**Proof:** Let $r = (r_0, r_1, \ldots, r_{n-1}) \in R^n$ and $x_i = (x^i_0, \ldots, x^i_{n-1}) \in F_2^n$, $i = 0, 1, 2, \ldots, m$ such that $r = x_0 + ux_1 + u^2x_2 + \ldots + u^mx_m$. Let $\phi(r) = (a_0, \ldots, a_{2^{m-1}})$.

Then $\sigma^{\otimes 2^{m-1}}(\phi(r)) = (b_0, \ldots, b_{2^{m-1}})$ where

$$b_{(2i+\varepsilon)n+j} = \begin{cases} a_{(2i+1)n+j} & j = 0, \varepsilon = 0 \\ a_{(2i+\varepsilon)n+j-1} & \text{otherwise} \end{cases}$$

for $0 \leq i \leq 2^{m-1} - 1$, $0 \leq \varepsilon \leq p - 1$, $0 \leq j \leq n - 1$. On the other hand

$$\nu(r) = ((1 - u^m)r_{n-1}, r_0, \ldots, r_{n-2})$$

where $(1 - u^m)r_{n-1} = x^0_{n-1} + u x^1_{n-1} + \ldots + u^m(-x^0_{n-1} \oplus x^m_{n-1})$. 

$(1 - u^m)$-Cyclic codes
Let $\phi(\nu(r)) = (c_0, \ldots, c_{2^m n - 1}) = (-x_{n-1}^0 \oplus x_{n-1}^m, x_0^m, x_1^m, \ldots, x_{n-2}^m)$

So we have the following theorem.

**Theorem 3.2** A code $C$ of length $n$ over $R$ is $(1-u^m)$-cyclic if and only if $\phi(C)$ is quasi-cyclic of index $2^{m-1}$ and length $2^m n$ over $F_2$.

**Proof:** Suppose $C$ is $(1-u^m)$-cyclic. As $\sigma \otimes 2^{m-1} (\phi(C)) = \phi(\nu(C))$, $\phi(C)$ is a quasi-cyclic of index $2^{m-1}$. Conversely, if $\phi(C)$ is quasi-cyclic of index $2^{m-1}$, then $\phi(\nu(C)) = \sigma \otimes 2^{m-1} (\phi(C)) = \phi(C)$ Since $\phi$ is isometry, so $\nu(C) = C$, that is $C$ is $(1-u^m)$-cyclic code. $ullet$

Note that $(1-u^m)^n = 1 - u^m$ if $n$ is odd, $(1-u^m)^n = 1$ if $n$ is even. In here, it is studied the properties of $(1-u^m)$ cyclic codes of odd length in this section.

Let $\mu$ be the map of $R[x]/\langle x^n - 1 \rangle$ into $R[x]/\langle x^n - (1-u^m) \rangle$ defined by $\mu(c(x)) = c((1-u^m)x)$. If $n$ is odd, then $\mu$ is a ring isomorphism. Hence $I$ is an ideal of $R[x]/\langle x^n - 1 \rangle$ if and only if $\mu(I)$ is an ideal of $R[x]/\langle x^n - (1-u^m) \rangle$. If $\bar{\mu}$ is the map

$$\bar{\mu} : R^n \rightarrow R^n$$

$$r \mapsto (r_0, (1-u^m)r_1, (1-u^m)^2r_2, \ldots, (1-u^m)^{n-1}r_{n-1})$$

then it also follows that:

**Proposition 3.3** The set $C \subseteq R^n$ is a linear cyclic code if and only if $\bar{\mu}(C)$ is a linear $(1-u^m)$-cyclic code.

**Definition 3.4** Let $\tau$ be the following permutation of $\{0, 1, 2, \ldots, 2n-1\}$ with $n$ odd:

$$\tau = (1, n+1)(3, n+3) \ldots (n-2, 2n-2)$$

The Nechaev permutation is the permutation $\pi$ of $F_2^{2n}$ defined by
We defined the permutation $\pi \otimes 2^{m-1}$ as follows: For $c = (c^{(1)}| \ldots |c^{(2^m-1)}) \in F_2^{2^m n}$,

$$\pi \otimes 2^{m-1}(c) = (\pi(c^{(1)})| \ldots |\pi(c^{(2^m-1)})$$

where $c^{(i)} \in F_2^{2n}, i = 1, 2, 3, \ldots, 2^m - 1$.

**Proposition 3.5** Assume $n$ odd, let $\bar{\mu}$ be the permutation of $R^n$ such that $\bar{\mu}(c_0, \ldots, c_{n-1}) = (c_0, (1 - u^m)c_1, \ldots, (1 - u^m)^{n-1}c_{n-1})$. If $\pi$ is the Nechaev permutation and if $\phi$ is the Gray map $R^n$ into $F_2^{2^m n}$, then $\phi \bar{\mu} = \pi \otimes 2^{m-1} \phi$.

**Corollary 3.6** If $\tilde{C}$ is the Gray image of a linear cyclic code of length $n$ over $R$, then $\tilde{C}$ is equivalent to a quasi-cyclic code of index $2^m - 1$ and length $2^m n$ over $F_2$.

**Proof:** From Proposition 3.3, a code $C$ of length $n$ over $R$ is linear cyclic code if and only if $\bar{\mu}(C)$ is linear $(1 - u^m)$-cyclic. From Theorem 3.2, this is also so if and only if $\phi(\bar{\mu}(C))$ is a linear quasi-cyclic code of index $2^m - 1$ over $F_2$, that is, if and only if $\pi \otimes 2^{m-1}(\phi(C))$ is linear quasi cyclic of index $2^m - 1$ over $F_2$.

**References**


Received: November, 2008