Available online at www.sciencedirect.com
ScienceDirect
Applied Mathematics Letters 21 (2008) 1129–1133
Applied Mathematics Letters
www.elsevier.com/locate/aml

# On $(1-u)$-cyclic codes over $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$

Maria Carmen V. Amarra*, Fidel R. Nemenzo

*Institute of Mathematics, University of the Philippines, Diliman, Quezon City, Philippines*

Received 27 July 2007; accepted 27 July 2007

**Abstract**

We extend the results of [J.F. Qian, L.N. Zhang, S.X. Zhu, $(1+u)$-constacyclic and cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$, Appl. Math. Lett. 19 (2006) 820–823. [3]] to codes over the commutative ring $R=\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$, where $p$ is prime, $k\in\mathbb{N}$ and $u^2=0$. In particular, we prove that the Gray image of a linear $(1-u)$-cyclic code over $R$ of length $n$ is a distance-invariant quasicyclic code of index $p^{k-1}$ and length $p^kn$ over $\mathbb{F}_{p^k}$. We also prove that if $(n,p)=1$, then every code of length $p^kn$ over $\mathbb{F}_{p^k}$ which is the Gray image of a linear cyclic code of length $n$ over $R$ is permutation-equivalent to a quasicyclic code of index $p^{k-1}$.


*Keywords:* Cyclic and quasicyclic codes; Gray map; Finite rings

## 1. Preliminaries

Let $p$ be prime and $k\in\mathbb{N}$. Let $R$ be the ring $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$, where $u^2=0$ and $\mathbb{F}_{p^k}=GF(p^k)$. Then $R$ is a finite chain ring with maximal ideal $uR$ and residue field $\mathbb{F}_{p^k}$. Let $\mathcal{C}$ be a code of length $n$ over $R$, and $P(\mathcal{C})$ be its polynomial representation, i.e.,

$$P(\mathcal{C})=\left\{\sum_{i=0}^{n-1}r_ix^i \mid (r_0,\ldots,r_{n-1})\in\mathcal{C}\right\}.$$

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

$$\sigma(r_0,r_1,\ldots,r_{n-1})=(r_{n-1},r_0,\ldots,r_{n-2})$$

and

$$\nu(r_0,r_1,\ldots,r_{n-1})=((1-u)r_{n-1},r_0,\ldots,r_{n-2}).$$

Then $\mathcal{C}$ is said to be *cyclic* if $\sigma(\mathcal{C})=\mathcal{C}$, and $(1-u)$-*cyclic* if $\nu(\mathcal{C})=\mathcal{C}$. It is known that:

**Theorem 1.1.** *A code $\mathcal{C}$ of length $n$ over $R$ is cyclic if and only if $P(\mathcal{C})$ is an ideal of $R[x]/\langle x^n-1\rangle$.*

* Corresponding address: School of Mathematics and Statistics, The University of Western Australia, Perth, Australia.
*E-mail addresses:* mcamarra@maths.uwa.edu.au, carmen_amarra@yahoo.com (M.C.V. Amarra), fidel@math.upd.edu.ph (F.R. Nemenzo).

0893-9659/$ - see front matter 
doi:10.1016/j.aml.2007.07.035

**Theorem 1.2.** *A code $\mathcal{C}$ of length $n$ over $R$ is $(1-u)$-cyclic if and only if $P(\mathcal{C})$ is an ideal of $R[x]/\langle x^n-(1-u)\rangle$.*

Let $\mathbf{a} \in \mathbb{F}_{p^k}^{p^k n}$, with $\mathbf{a} = (a_0, \ldots, a_{p^k n-1}) = \left(a^{(0)} \mid \ldots \mid a^{(p^{k-1}-1)}\right)$, $a^{(i)} \in \mathbb{F}_{p^k}^{pn}$ for all $i = 0, \ldots, p^{k-1}-1$. Let $\sigma^{\otimes p^{k-1}}$ be the map from $\mathbb{F}_{p^k}^{p^k n}$ to $\mathbb{F}_{p^k}^{p^k n}$ given by

$$\sigma^{\otimes p^{k-1}}(\mathbf{a}) = \left(\tilde{\sigma}(a^{(0)}) \mid \ldots \mid \tilde{\sigma}(a^{(p^{k-1}-1)})\right),$$

where $\tilde{\sigma}$ is the usual cyclic shift $(c_0, c_1, \ldots c_{pn-1}) \mapsto (c_{pn-1}, c_0, \ldots, c_{pn-2})$ on $\mathbb{F}_{p^k}^{pn}$. A code $\tilde{\mathcal{C}}$ of length $p^k n$ over $\mathbb{F}_{p^k}$ is said to be *quasicyclic of index* $p^{k-1}$ if $\sigma^{\otimes p^{k-1}}(\tilde{\mathcal{C}}) = \tilde{\mathcal{C}}$.

In [1], a homogeneous weight on arbitrary finite chain rings is defined; we give it here for the case of the ring $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. The homogeneous weight $w_{\text{hom}}(r)$ of $r \in R$ is given by

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

This extends to a weight function in $R^n$: if $\mathbf{r} = (r_0, \ldots, r_{n-1}) \in R^n$, then

$$w_{\text{hom}}(\mathbf{r}) := \sum_{i=0}^{n-1} w_{\text{hom}}(r_i).$$

The homogeneous distance $d_{\text{hom}}(\mathbf{x}, \mathbf{y})$ between any distinct vectors $\mathbf{x}, \mathbf{y} \in R^n$ is defined to be $w_{\text{hom}}(\mathbf{x} - \mathbf{y})$.

## 2. Gray images of $(1-u)$-cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$

Any element $\epsilon \in \mathbb{Z}_{p^k}$ has $p$-adic representation

$$\gamma_{0,\epsilon} + \gamma_{1,\epsilon} p + \cdots + \gamma_{(k-1),\epsilon} p^{k-1},$$

where $\gamma_{i,\epsilon} \in \{0, 1, 2, \ldots, p-1\}$. If $\alpha$ is a fixed primitive element of $\mathbb{F}_{p^k}$, then corresponding to every $\epsilon \in \mathbb{Z}_{p^k}$ is an element $\alpha_\epsilon \in \mathbb{F}_{p^k}$, given by

$$\alpha_\epsilon := \gamma_{0,\epsilon} + \gamma_{1,\epsilon}\, \alpha + \cdots + \gamma_{(k-1),\epsilon}\, \alpha^{k-1}.$$

The *Gray map* $\Phi$ on $R$, which is a special case of the Gray map defined in [1], is given by

$$\begin{aligned} \Phi : R^n &\longrightarrow \mathbb{F}_{p^k}^{p^k n} \\ x + yu &\longmapsto (y, \alpha_1 x \oplus y, \ldots, \alpha_{p^k-1} x \oplus y), \end{aligned}$$

where $\oplus$ is componentwise addition in $\mathbb{F}_{p^k}$. The Gray map $\Phi$ is an isometry from $(R^n, d_{hom})$ to $\mathbb{F}_{p^k}^{p^k n}$ under the Hamming distance. It is also clear that $\Phi$ preserves linearity of codes.

From the above definitions, we have:

**Proposition 2.1.**

$$\Phi \circ \nu = \sigma^{\otimes p^{k-1}} \circ \Phi.$$

**Proof.** Let $\mathbf{r} = (r_0, \ldots, r_{n-1}) \in R^n$ and $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_{p^k}^n$ such that $\mathbf{r} = \mathbf{x} + \mathbf{y}u$. Let $\Phi(\mathbf{r}) = (a_0, \ldots, a_{p^k n-1})$. Then $\sigma^{\otimes p^{k-1}}(\Phi(\mathbf{r})) = (b_0, \ldots, b_{p^k n-1})$, where

$$b_{\epsilon n+j} = \begin{cases} a_{(\epsilon+p-1)n+(n-1)} & \text{if } j = 0, \gamma_{0,\epsilon} = 0 \\ a_{(\epsilon-1)n+(n-1)} & \text{if } j = 0, \gamma_{0,\epsilon} \neq 0 \\ a_{\epsilon n+j-1} & \text{if } j \neq 0. \end{cases}$$

On the other hand,

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

where $(1-u)r_{n-1} = x_{n-1} + u(-x_{n-1} \oplus y_{n-1})$. Then $\Phi(\nu(\mathbf{r})) = (c_0, \ldots, c_{p^k n-1})$, where

$$c_{\epsilon n+j} = \begin{cases} \left(\sum_{i=0}^{k-1} \gamma_{i,\epsilon}\, \alpha^i - 1\right) x_{n-1} \oplus y_{n-1}, & \text{if } j = 0 \\ \left(\sum_{i=0}^{k-1} \gamma_{i,\epsilon}\, \alpha^i\right) x_{j-1} \oplus y_{j-1}, & \text{if } j \neq 0 \end{cases}$$

$$= \begin{cases} \left(\sum_{i=0}^{k-1} \gamma_{i,\epsilon}\, \alpha^i + p - 1\right) x_{n-1} \oplus y_{n-1}, & \text{if } j = 0, \gamma_{0,\epsilon} = 0 \\ \left(\sum_{i=0}^{k-1} \gamma_{i,\epsilon}\, \alpha^i - 1\right) x_{n-1} \oplus y_{n-1}, & \text{if } j = 0, \gamma_{0,\epsilon} \neq 0 \\ \left(\sum_{i=0}^{k-1} \gamma_{i,\epsilon}\, \alpha^i\right) x_{j-1} \oplus y_{j-1}, & \text{if } j \neq 0. \end{cases}$$

The conclusion follows. □

As a consequence:

**Theorem 2.2.** *A code $\mathcal{C}$ of length $n$ over $R$ is $(1-u)$-cyclic if and only if $\Phi(\mathcal{C})$ is quasicyclic of index $p^{k-1}$ and length $p^k n$ over $\mathbb{F}_{p^k}$.*

**Proof.** Suppose $\mathcal{C}$ is $(1-u)$-cyclic. Then

$$\sigma^{\otimes p^{k-1}}(\Phi(\mathcal{C})) = \Phi(\nu(\mathcal{C})) = \Phi(\mathcal{C}),$$

so $\Phi(\mathcal{C})$ is quasicyclic of index $p^{k-1}$. Conversely, if $\Phi(\mathcal{C})$ is quasicyclic of index $p^{k-1}$, then

$$\Phi(\nu(\mathcal{C})) = \sigma^{\otimes p^{k-1}}(\Phi(\mathcal{C})) = \Phi(\mathcal{C}).$$

Since $\Phi$ is injective, it follows that $\nu(\mathcal{C}) = \mathcal{C}$. □

## 3. Gray images of cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$

Suppose that $(n, p) = 1$. Following [2], let us have $n' \in \{0, 1, \ldots, p-1\}$ such that $nn' \equiv 1 (\mathrm{mod}\ p)$ and $\beta = 1 + n'u$. If $\mu$ is the map

$$\mu : R[x]/(x^n - 1) \longrightarrow R[x]/\left(x^n - (1-u)\right)$$
$$r(x) \longmapsto r(\beta x)$$

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 $R[x]/\langle x^n - (1-u)\rangle$. If $\overline{\mu}$ is the map

$$\overline{\mu} : R^n \longrightarrow R^n$$
$$r \longmapsto \left(r_0, \beta r_1, \beta^2 r_2, \ldots, \beta^{n-1} r_{n-1}\right)$$

then it also follows that:

**Proposition 3.1.** *The set $\mathcal{C} \subseteq R^n$ is a linear cyclic code if and only if $\overline{\mu}(\mathcal{C})$ is a linear $(1-u)$-cyclic code.*

We now define the permutation $\pi^{\otimes p^{k-1}}$, which is an extension of the Nechaev permutation introduced in [4], as follows:

For $\mathbf{c} = \left(c^{(p^0)} | \ldots | c^{(p^{k-1})}\right) \in \mathbb{F}_{p^k}^{p^k n}$,

$$\pi^{\otimes p^{k-1}}(\mathbf{c}) := \left(\pi\left(c^{(p^0)}\right) | \ldots | \pi\left(c^{(p^{k-1})}\right)\right),$$

where

$$\pi(\mathbf{a}) = \left(a_{\tau(0)}, \ldots, a_{\tau(pn-1)}\right)$$

for $\mathbf{a} = (a_0, \ldots, a_{pn-1}) \in \mathbb{F}_{p^k}^{pn}$, where

$$\tau(\gamma n + j) = (\gamma + jn')_p n + j,$$

$0 \leq \gamma \leq p-1$, $0 \leq j \leq n-1$, and $(\gamma + jn')_p$ is the least residue of $\gamma + jn'$ modulo $p$.

**Proposition 3.2.**

$$\Phi \circ \overline{\mu} = \pi^{\otimes p^{k-1}} \circ \Phi.$$

**Proof.** Let $\mathbf{r} = (r_0, \ldots, r_{n-1}) \in R^n$. If $\Phi(\mathbf{r}) = (a_0, \ldots, a_{p^k n-1})$, then $\pi^{\otimes p^{k-1}}(\Phi(\mathbf{r})) = (b_0, \ldots, b_{p^k n-1})$, where

$$\begin{aligned} b_{\epsilon n+j} &= a_{[\gamma^{(\epsilon)} + (\gamma_{0,\epsilon} + jn')_p]n+j} \\ &= \left[\sum_{i=1}^{k-1} \gamma_{i,\epsilon}\alpha^i + (\gamma_{0,\epsilon} + jn')_p\right] x_j \oplus y_j. \end{aligned}$$

On the other hand, $\overline{\mu}(\mathbf{r}) = \left(r_0, \beta r_1, \ldots, \beta^{n-1} r_{n-1}\right)$, where

$$\begin{aligned} \beta^j r_j &= (1 + n'u)^j r_j \\ &= x_j + u(jn' x_j \oplus y_j). \end{aligned}$$

Hence $\Phi(\overline{\mu}(\mathbf{r})) = (c_0, c_1, \ldots, c_{p^k n-1})$, where

$$\begin{aligned} c_{\epsilon n+j} &= \left(\sum_{i=0}^{k-1} \gamma_{i,\epsilon}\alpha^i\right) x_j \oplus (jn' x_j \oplus y_j) \\ &= \left[\sum_{i=1}^{k-1} \gamma_{i,\epsilon}\alpha^i + (\gamma_{0,\epsilon} + jn')_p\right] x_j \oplus y_j. \end{aligned}$$

The conclusion follows. □

**Corollary 3.3.** *If $\tilde{C}$ is the Gray image of a linear cyclic code of length $n$ over $R$, then $\tilde{C}$ is equivalent to a quasicyclic code of index $p^{k-1}$ and length $p^k n$ over $\mathbb{F}_{p^k}$.*

**Proof.** From Proposition 3.1, a code $\mathcal{C}$ of length $n$ over $R$ is linear cyclic if and only if $\overline{\mu}(\mathcal{C})$ is linear $(1-u)$-cyclic. From Theorem 2.2, this is so if and only if $\Phi(\overline{\mu}(\mathcal{C}))$ is a linear quasicyclic code of index $p^{k-1}$ over $\mathbb{F}_{p^k}$, that is, if and only if $\pi^{\otimes p^{k-1}}(\Phi(\mathcal{C}))$ is linear quasicyclic of index $p^{k-1}$ over $\mathbb{F}_{p^k}$. □

The following example illustrates the above results. Computations were done using MAGMA.

**Example.** Let $\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega = \omega^2\}$. Consider $x^3 - 1$. In $\mathbb{F}_4 + u\mathbb{F}_4$,

$$x^3 - 1 = (x+1)(x+\omega)(x+\omega^2).$$

Applying the map $\mu : x \mapsto (1+u)x$, we obtain

$$x^3 - (1-u) = [x + (u+1)][x + (\omega u + \omega)][x + (\omega^2 u + \omega^2)] = f_1(x) f_2(x) f_3(x).$$

1. Let $\mathcal{C}_1$ be the $(1-u)$-cyclic code generated by $a$, where
$$a(x) = f_1(x)f_2(x) = x^2 + (\omega^2 u + \omega^2)x + 1.$$
The code $\Phi(\mathcal{C}_1)$ is a [12, 2, 9] quaternary code, which is an optimal code.
2. Let $a(x)$ be as in the above,
$$b(x) = uf_1(x) = ux + u,$$
and $\mathcal{C}_2$ be the $(1-u)$-cyclic code over $\mathbb{F}_4 + u\mathbb{F}_4$ generated by $a$ and $b$. The code $\Phi(\mathcal{C}_2)$ is a [12, 3, 8] quaternary code, which is an optimal code.

## References

[1] M. Greferath, S.E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, IEEE Trans. Inform. Theory 45 (1999) 2522–2524.
[2] S. Ling, J. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, IEEE Trans. Inform. Theory 48 (2002) 2592–2605.
[3] J.F. Qian, L.N. Zhang, S.X. Zhu, $(1+u)$-constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, Appl. Math. Lett. 19 (2006) 820–823.
[4] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 45 (1999) 2527–2532.