Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 14 (2008) 834–846

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k

Han Mao Kiah [a], Ka Hin Leung [a,*], San Ling [b,1]

[a] *Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore*

[b] *Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Block 5 Level 3, 1 Nanyang Walk, Singapore 637616, Republic of Singapore*

Received 13 March 2006; revised 14 December 2006

Available online 16 April 2008

Communicated by Gary L. Mullen

Abstract

We study cyclic codes of length p^k over $\mathrm{GR}(p^2, m)$, or equivalently, ideals of the ring $\mathrm{GR}(p^2, m)/\langle u^{p^k} - 1\rangle$. We derive a method of representing the ideals, and classify all ideals in the ring $\mathrm{GR}(p^2, m)/\langle u^{p^k} - 1\rangle$. We also analyse the duals, and identify the self-dual ideals.

Keywords: Cyclic codes; Galois ring

1. Introduction

Cyclic codes are an important class of codes from both a theoretical and a practical viewpoint. Traditionally, cyclic codes had been studied over finite fields. However, it was discovered that some good non-linear codes over $\mathbb{Z}_2$ can be viewed as binary images under a Gray map of linear cyclic codes over $\mathbb{Z}_4$, and this had motivated the study of cyclic codes over finite rings.

The key to describing cyclic codes of length N over a ring R, like in the case of a finite field, is to view them as ideals of the polynomial ring $R[X]/\langle X^N - 1\rangle$. Hence, to describe cyclic codes over $\mathbb{Z}_{p^e}$, we examine the ideals of the ring $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$. By the Chinese Remainder

[*] Corresponding author.

E-mail addresses: mao_zai@yahoo.com (H.M. Kiah), matlkh@nus.edu.sg (K.H. Leung), lingsan@ntu.edu.sg (S. Ling).

[1] The research of this author is partially supported by NTU Research Grant M58110003.

1071-5797/$ – see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2008.02.003

Theorem, it is therefore natural to look at the factorization of $X^N - 1$ over $\mathbb{Z}_{p^e}$. Unfortunately, polynomials in $\mathbb{Z}_{p^e}[X]$ do not necessarily have a unique factorisation. In particular, $X^N - 1$ does not factor uniquely when $p \mid N$.

In [2], Blackford circumvented this problem when he examined cyclic codes of length $2n$, where n is odd, over $\mathbb{Z}_4$. He considered the polynomial ring $\mathcal{R} = \mathbb{Z}_4[u]/\langle u^2 - 1\rangle$ and identified cyclic codes of length $2n$ over $\mathbb{Z}_4$ with constacyclic codes of length n over $\mathcal{R}$. Dougherty et al. [4] then generalised the results further. A key result in [4] (in our context) was that $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ is isomorphic to the direct sum of rings of the form $\mathrm{GR}(p^e, m)[u]/\langle u^{p^k} - 1\rangle$, where $\mathrm{GR}(p^e, m)$ denotes the Galois ring of characteristic p^e with $(p^e)^m$ elements, and k is the largest integer such that p^k divides N. Hence, it suffices to look at the ideals of the ring $\mathrm{GR}(p^e, m)[u]/\langle u^{p^k} - 1\rangle$.

Unfortunately, to account for all ideals in the ring $\mathrm{GR}(p^e, m)[u]/\langle u^{p^k} - 1\rangle$ is a tedious process. Hence, we examine only the case of characteristic p^2. In [1] and [3], the case of characteristic 4 is thoroughly examined. However, their methods are too cumbersome to our case. So, we introduce a new approach to this problem. In the next section, we define a new representation of ideals, and in Section 3, we account for all ideals in $\mathrm{GR}(p^2, m)[u]/\langle u^{p^k} - 1\rangle$ in the form of the new representation. Finally, in Section 4, we analyse the duals of the ideals in question.

2. A unique representation of ideals in $\mathbf{GR}(p^e, m)[u]/\langle u^{p^k} - 1\rangle$

In [4], Dougherty et al. derived a representation of any ideal in $\mathrm{GR}(p^e, m)[u]/\langle u^{p^k} - 1\rangle$ in terms of e polynomials in the ideal concerned. Unfortunately, the choice of those polynomials is not unique. Here, we make some refinements and obtain a unique representation for any such ideal in Theorem 2.5. This enables us to enumerate all ideals efficiently in $\mathrm{GR}(p^e, m)[u]/\langle u^{p^k} - 1\rangle$ when $e = 2$. Indeed, it should be possible to use our representation to enumerate all ideals when e is very small.

Let S be the finite ring $\mathrm{GR}(p^e, m)[u]/\langle u^{p^k} - 1\rangle$ and $\overline{S}$ be the ring $\mathbb{F}_{p^m}[u]/\langle u^{p^k} - 1\rangle$. We define a map

$$\mu : S \to \overline{S}$$
$$f(u) \mapsto f(u) \pmod{p}.$$

It can be easily verified μ is a surjective ring homomorphism. With this map, we define the following for any ideal C in S.

Definition 2.1. For $0 \leqslant i \leqslant e - 1$, we define

$$\mathrm{Tor}_i(C) = \mu\bigl(\bigl\{v \in S \bigm| p^i v \in C\bigr\}\bigr).$$

$\mathrm{Tor}_i(C)$ is called the ith *torsion code* of C. Usually, $\mathrm{Tor}_0(C) = \mu(C)$ is called the *residue code* and sometimes denoted by $\mathrm{Res}(C)$.

Next, we sum up some results from [4] and restate it as Theorems 2.2 and 2.4.

Theorem 2.2. *Let i be an integer such that $0 \leqslant i \leqslant e - 1$. Then $\mathrm{Tor}_i(C)$ is an ideal of $\overline{S}$ and $\mathrm{Tor}_i(C) = \langle (u - 1)^{T_i}\rangle$ for some $0 \leqslant T_i \leqslant p^k$. Moreover, we have the following*:

(i) $|\mathrm{Tor}_i(C)| = (p^m)^{p^k - T_i}$.
(ii) *If* $g(u) \in S$ *and* $p^i((u-1)^{t_i} + pg(u)) \in C$, *then* $t_i \geqslant T_i$.
(iii) $p^k \geqslant T_0 \geqslant T_1 \geqslant \cdots \geqslant T_{e-1} \geqslant 0$.
(iv) $|C| = (p^m)^{ep^k - (T_0 + T_1 + \cdots + T_{e-1})}$.

Definition 2.3. Let C be an ideal in S. For each $0 \leqslant i \leqslant e-1$, define $T_i(C)$ to be the T_i found in Theorem 2.2. We say $T_i(C)$ is the ith-*torsional degree* of C.

Note that T_i is the smallest degree amongst all the degrees of non-zero polynomials in $\mathrm{Tor}_i(C)$.

We have the following variation of Theorem 6.5 in [4].

Theorem 2.4. *Let C be a non-zero ideal of S. Then*

$$C = \langle F_0(u), F_1(u), \ldots, F_{e-1}(u) \rangle,$$

where $F_i(u) = p^i((u-1)^{T_i} + pg_i(u))$ *for some* $g_i(u) \in S$ *when* $T_i < p^k$ *and* $F_i(u) = 0$ *when* $T_i = p^k$.

As in [4], it is reasonable to choose the e polynomials $F_0(u), F_1(u), \ldots, F_{e-1}(u)$ to represent the ideal C. However, the choice for $F_i(u)$ is not unique. Moreover, the degree of the polynomial $F_i(u)$ is not necessarily T_i. Our aim is to impose extra conditions on $F_i(u)$ so as to make the choice of each $F_i(u)$ unique.

First, observe that we can rewrite $\sum_{j=0}^{N} a_j(u-1)^j$ as 0, or, $(u-1)^t h(u)$, where $h(u)$ is a unit with coefficients belonging to $\mathcal{T}_m$ and $t \leqslant N$. For convenience, we shall define the set of polynomials in u with coefficients belonging to $\mathcal{T}_m$ as $\mathcal{T}_m[u]$. Hence, we say that we can rewrite the expression $\sum_{j=0}^{N} a_j(u-1)^j$ as $(u-1)^t h(u)$, where $h(u) \in \mathcal{T}_m[u]$ and $h(u)$ is either zero or a unit, and vice versa.

Theorem 2.5. *Let C be an ideal of* $S = \mathrm{GR}(p^e, m)[u]/\langle u^{p^k} - 1 \rangle$. *Then C can be expressed as being generated by e polynomials, say* $f_0(u), f_1(u), \ldots, f_{e-1}(u)$, *where,*

(i) *when* $T_i(C) < p^k$,

$$f_i(u) = p^i(u-1)^{T_i} + p^{i+1}(u-1)^{t_{1,i}} h_{1,i}(u) + p^{i+2}(u-1)^{t_{2,i}} h_{2,i}(u) + \cdots + p^{e-1}(u-1)^{t_{e-1-i,i}} h_{e-1-i,i}(u),$$

where $h_{j,l}(u) \in \mathcal{T}_m[u]$, $h_{j,l}(u)$ *is either zero or a unit and* $t_{j,l} + \deg h_{j,l} < T_{j+l}$, *or,*

(ii) *when* $T_i(C) = p^k$,

$$f_i(u) = 0.$$

Moreover, the e-tuple $(f_0(u), f_1(u), \ldots, f_{e-1}(u))$ *is unique. In other words, if there is another e-tuple of polynomials satisfying the conditions in the theorem, say* $(f_0'(u), f_1'(u), \ldots, f_{e-1}'(u))$, *then the two e-tuples are equal.*

Proof. When $C = \{0\}$, the theorem holds trivially.

When C is non-zero, we rewrite the expression in (i) as:

$$f_i(u) = p^i(u-1)^{T_i} + p^{i+1}\sum_{j=0}^{T_{i+1}-1} b_{j,1,i}(u-1)^j + p^{i+2}\sum_{j=0}^{T_{i+2}-1} b_{j,2,i}(u-1)^j + \cdots + p^{e-1}\sum_{j=0}^{T_{e-1}-1} b_{j,e-1-i,i}(u-1)^j,$$

where $b_{j,l,i} \in \mathcal{T}_m$, and proceed to prove the theorem in this form.

Since C is non-zero, there exists a smallest r such that $T_r < p^k$. From Theorem 2.4, we can express C as $\langle F_0(u), F_1(u), \ldots, F_{e-1}(u)\rangle$ where $F_i(u) = p^i((u-1)^{T_i} + pg_i(u))$ for some $g_i(u) \in C$ for $r \leqslant i \leqslant e-1$ and $F_i(u) = 0$ for $0 \leqslant i \leqslant r-1$. Hence, for each $r \leqslant i \leqslant e-1$, we rewrite

$$F_i(u) = p^i(u-1)^{T_i} + p^{i+1}\sum_{j=0}^{p^k-1} a_{j,1,i}(u-1)^j + p^{i+2}\sum_{j=0}^{p^k-1} a_{j,2,i}(u-1)^j + \cdots + p^{e-1}\sum_{j=0}^{p^k-1} a_{j,e-1-i,i}(u-1)^j,$$

where $a_{j,l,i} \in \mathcal{T}_m$.

Let $f_{e-1}(u) = F_{e-1}(u) = p^{e-1}(u-1)^{T_{e-1}}$.

Consider $F_{e-2}(u) = p^{e-2}(u-1)^{T_{e-2}} + p^{e-1}\sum_{j=0}^{p^k-1} a_{j,1,e-2}(u-1)^j$. Since $f_{e-1}(u) = p^{e-1}(u-1)^{T_{e-1}} \in C$, we see that by subtracting a suitable multiple of $f_{e-1}(u)$, we obtain $p^{e-2}(u-1)^{T_{e-2}} + p^{e-1}\sum_{j=0}^{T_{e-1}-1} b_{j,1,e-2}(u-1)^j$. This polynomial satisfies the condition in the theorem and hence let the polynomial be $f_{e-2}(u)$. Moreover, we can easily check that $C = \langle F_0(u), F_1(u), \ldots, F_{e-2}(u), f_{e-1}(u)\rangle = \langle F_0(u), F_1(u), \ldots, f_{e-2}(u), f_{e-1}(u)\rangle$.

Proceeding inductively, suppose we have chosen $f_{i+1}(u), \ldots, f_{e-1}(u)$ satisfying the conditions in the theorem and that $C = \langle F_0(u), F_1(u), \ldots, F_i(u), f_{i+1}(u), \ldots, f_{e-1}(u)\rangle$.

Again, by subtracting suitable multiples of $f_{i+1}(u), \ldots, f_{e-1}(u)$, we can obtain the polynomial $f_i(u)$ of the form

$$f_i(u) = p^i(u-1)^{T_i} + p^{i+1}\sum_{j=0}^{T_{i+1}-1} b_{j,1,i}(u-1)^j + p^{i+2}\sum_{j=0}^{T_{i+2}-1} b_{j,2,i}(u-1)^j + \cdots + p^{e-1}\sum_{j=0}^{T_{e-1}-1} b_{j,e-1-i,i}(u-1)^j.$$

We can also check that $C = \langle F_0(u), F_1(u), \ldots, F_i(u), f_{i+1}(u), \ldots, f_{e-1}(u)\rangle = \langle F_0(u), F_1(u), \ldots, F_{i-1}(u), f_i(u), \ldots, f_{e-1}(u)\rangle$.

Hence, we have obtained e polynomials $f_0(u), f_1(u), \ldots, f_{e-1}(u)$ such that $C = \langle f_0(u), f_1(u), \ldots, f_{e-1}(u)\rangle$.

To prove the uniqueness, we suppose that $C = \langle f_0'(u), f_1'(u), \ldots, f_{e-1}'(u)\rangle$ such that $f_0'(u), f_1'(u), \ldots, f_{e-1}'(u)$ satisfy the conditions in the theorem. From the definition of $f_{e-1}'(u)$ and $f_{e-1}(u)$, we can see that $f_{e-1}(u) = f_{e-1}'(u) = p^{e-1}(u-1)^{T_{e-1}}$.

Next, let $f_{e-2}'(u) = p^{e-2}(u-1)^{T_{e-2}} + p^{e-1}\sum_{j=0}^{T_{e-1}-1} c_{j,e-1-i,e-2}(u-1)^j$ where $c_{j,e-1-i,e-2} \in \mathcal{T}_m$. Consider

$$f_{e-2}(u) - f_{e-2}'(u) = p^{e-1}\sum_{j=0}^{T_{e-1}-1}(b_{j,e-1-i,e-2} - c_{j,e-1-i,e-2})(u-1)^j.$$

We rewrite the difference as $p^{e-1}(u-1)^K h(u)$ where $h(u)$ is a unit or zero, and $K \leqslant T_{e-1} - 1 < T_{e-1}$. If $h(u)$ is a unit, then $p^{e-1}(u-1)^K \in C$ implies that $K \geqslant T_{e-1}$, a contradiction. Therefore, $h(u) = 0$ and so $f_{e-2}(u) = f_{e-2}'(u)$. Proceeding inductively, we have that $f_i(u) = f_i'(u)$ for all i and so the expression is unique. □

Note that in Theorem 2.5, C is generated by the polynomials $f_0(u), \ldots, f_{e-1}(u)$ as an ideal, i.e. $C = \langle f_0(u), f_1(u), \ldots, f_{e-1}(u)\rangle$. However, as we would like to stress that these e-polynomials also satisfied conditions in Theorem 2.5, we define the following notation.

Definition 2.6. Let C be an ideal of S. We define the unique e-tuple obtained from Theorem 2.5 to be the *representation* of C. In that case, we also say that $C = \langle\langle f_0(u), f_1(u), \ldots, f_{e-1}(u)\rangle\rangle$.

Remark 2.7. We illustrate the differences between the representation given in Theorem 2.5 and those given in [4] and [3]. Let us consider the ideals in $\mathbb{Z}_4[X]/\langle X^4 - 1\rangle$.

(i) Let C be the ideal generated by $(X-1)^2$. Theorem 2.5 gives the representation as $\langle\langle (X-1)^2, 2(X-1)^2\rangle\rangle$. However, Theorem 6.5 in [4] yields the following as possible representations $\langle (X-1)^2, 0\rangle$, $\langle (X-1)^2 + 2(X-1)^2, 0\rangle$, $\langle (X-1)^2 + 2(X-1)^3, 0\rangle$ and $\langle (X-1)^2 + 2(X-1)^3 + 2(X-1)^2, 0\rangle$. Thus, the representation obtained by using [4, Theorem 6.5] is not unique in general. However, it is interesting to note that [4, Theorem 6.5] gives explicitly the torsional degrees.

(ii) Let C be the ideal generated by $(X-1)^3$. Theorem 2.5 gives the representation as $\langle\langle (X-1)^3, 2(X-1)^2\rangle\rangle$, while the representation will be $\langle (X-1)^3\rangle$ in [3]. From the last representation, we see that the ideal is generated by one element. However, we cannot immediately know all the torsional degrees of the ideal from the representation. Whereas in our representation, we know all the torsional degrees.

Corollary 2.8. *If $\langle\langle f_0(u), f_1(u), \ldots, f_{e-1}(u)\rangle\rangle$ is the representation of C, then $T_i(C)$ is the degree of $f_i(u)$ when $f_i(u) \neq 0$, and $T_i(C) = p^k$ when $f_i(u) = 0$.*

Here, we state some results which can be easily be deduced from Theorem 2.5. These corollaries will describe the relation between T_i and polynomials with leading coefficient p^i. Analogous to the case over $\mathbb{Z}_p$, T_i is the lowest degree amongst the polynomials in C with leading coefficient p^i.

Corollary 2.9. *Suppose $T_i < p^k$ and let $f_i(u)$ be the polynomial constructed in Theorem* 2.5. *Then $f_i(u)$ is a polynomial of degree T_i with leading coefficient p^i.*

Proof. Clear from Theorem 2.5. □

Corollary 2.10. *Suppose $T_i < p^k$. Then the lowest degree amongst the polynomials in C with leading coefficient p^i is T_i.*

Proof. Let the lowest degree amongst the polynomials in C with leading coefficient p^i be t_i. From the above corollary, since $f_i(u)$ has degree T_i, it is clear that $T_i \geqslant t_i$.

Conversely, let $f(u)$ be the polynomial with leading coefficient p^i and degree t_i. Write $f(u) = p^i(u-1)^{t_i} + p^{i_{t_i-1}}\zeta_{t_i-1}(u-1)^{t_i-1} + \cdots + p^{i_0}\zeta_0$, where ζ_j is zero or a unit in S for $j = 0, 1, \ldots, t_i - 1$. In the case where $\zeta_j = 0$, we let $i_j = e$.

We claim that $i_j \geqslant i$ for all j. Suppose otherwise, then $\min\{i_j \mid j = 0, 1, \ldots, t_i - 1\} < i$. Then let r be the largest integer such that $i_r = \min\{i_j \mid j = 0, 1, \ldots, t_i - 1\}$. Hence, we can write $f(u) = p^{i_r}(g(u) + ph(u))$ where $g(u)$, $h(u)$ are polynomials in S and $g(u)$ is of degree r and has a leading coefficient not divisible by p. We note also that $r = \deg g < t_i$. Therefore, $\mu(g(u) + ph(u)) = \mu(g(u)) \in \mathrm{Tor}_{i_r}(C)$. Now, $\deg \mu(g) = \deg g$ and so $\deg g \geqslant T_{i_r}$. From above, we have $T_i \geqslant t_i$. Therefore,

$$T_{i_r} \leqslant \deg g < t_i \leqslant T_i,$$

which contradicts Theorem 2.2(ii). Hence, $\min\{i_j \mid j = 0, 1, \ldots, t_i - 1\} \geqslant i$.

Consequently, $i_j \geqslant i$ for all j and we can write $f(u)$ as $p^i((u-1)^{t_i} + z)$ for some $z \in S$. This means that $\mu((u-1)^{t_i} + z) = (u-1)^{t_i} + \mu(z) \in \mathrm{Tor}_i(C)$. We note that $\deg \mu(z) < t_i$ and hence $(u-1)^{t_i} + \mu(z)$ is non-zero. Therefore, $t_i \geqslant T_i$.

Combining both inequalities, we have the result. □

When $T_i = p^k$, it is not difficult to follow the above argument and conclude that there are no polynomials in C with leading coefficient p^i.

3. Ideals in $\mathrm{GR}(p^2, m)[u]/\langle u^{p^k} - 1\rangle$

In Section 2, we have found a way to represent an ideal uniquely by a set of e polynomials in it. In this section, we will apply those results to determine all ideals in the ring S when $e = 2$. In fact, the idea used in this section can be applied to the general case but the calculation involved is much more tedious.

From now on, we will restrict ourself to the case when $e = 2$. Let S be $\mathrm{GR}(p^2, m)[u]/\langle u^{p^k} - 1\rangle$ and let $\mathcal{I}$ be the set of all ideals in S. The objective of this section is to determine all ideals in the ring S by using their representations.

Lemma 3.1. *In S, $(u-1)^{p^l} = u^{p^l} - 1 - p(u-1)^{p^{l-1}} \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j}(u-1)^{p^{l-1}(j-1)}$ for all integers l.*

For convenience, we denote $\sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j}(u-1)^{p^{l-1}(j-1)}$ by $\Omega_{p,l}$. In case $k = l$, we have the following:

Lemma 3.2. *In S, for all integers k, $(u-1)^{p^k} = -p(u-1)^{p^{k-1}}\Omega_{p,k}$.*

Suppose $\langle f_0(u), f_1(u)\rangle$ is a representation of an ideal C in S. If $f_0(u)=0$ and $f_1(u)=p(u-1)^{i_1}$, it is not difficult to verify that $\langle\langle f_0(u), f_1(u)\rangle\rangle$ is indeed a representation of C. On the other hand, suppose $f_0(u)=(u-1)^{i_0}+p(u-1)^t h(u)$ and $f_1(u)=p(u-1)^{i_1}$, where $h(u)$ is either zero or a unit in S. From Corollary 2.8 and Definition 2.6, to check if $\langle\langle f_0(u), f_1(u)\rangle\rangle$ is indeed a representation of C, it suffices to show that $T_j(C)=i_j$ for $j=0,1$. Therefore, the crux of the problem is to compute the torsional degrees of the ideal C. To do so, we introduce the notion of the annihilator ideal.

Definition 3.3. Let C be an ideal of S. We define the *annihilator* of C, denoted by $\mathrm{Ann}(C)$, to be the set $\{f(u)\in S \mid f(u)g(u)=0 \text{ for all } g(u)\in C\}$.

Using standard argument, it is easy to verify the following:

Theorem 3.4. *Let C be an ideal of S. Then $\mathrm{Ann}(C)$ is an ideal of S.*

Theorem 3.5. *Let C be an ideal of S and $|C|=(p^m)^d$. Then $|\mathrm{Ann}(C)|=(p^m)^{(2\cdot p^k-d)}$.*

Theorem 3.6. *Let C be an ideal of S. Then $\mathrm{Ann}(\mathrm{Ann}(C))=C$. Furthermore, let $\mathcal{A}=\{C\in\mathcal{I} \mid T_0(C)+T_1(C)\leqslant p^k\}$ and $\mathcal{A}'=\{C\in\mathcal{I} \mid T_0(C)+T_1(C)\geqslant p^k\}$. Then the map $\phi:\mathcal{A}\to\mathcal{A}'; C\mapsto \mathrm{Ann}(C)$ is a bijection.*

Recall that our objective is to determine all ideals in S. In view of Theorem 3.6, it suffices to account for the ideals in the set $\mathcal{A}=\{C\in\mathcal{I} \mid T_0(C)+T_1(C)\leqslant p^k\}$.

As before, we assume $C=\langle\langle f_0(u), f_1(u)\rangle\rangle$ in $\mathcal{A}$. We note that if $f_0(u)=0$ then $T_0(C)=p^k$, and hence, $T_1(C)=0$. Therefore, the only ideal in $\mathcal{A}$ with $f_0(u)=0$ is of the form $\langle\langle 0, p\rangle\rangle$. Thus, from now on, we may assume $f_0(u)\neq 0$.

Theorem 3.7. $\langle\langle (u-1)^{i_0}+p(u-1)^t h(u), p(u-1)^{i_1}\rangle\rangle$ *is a representation of an ideal C in $\mathcal{A}$ if and only if i_0, i_1, t are integers and $h(u)\in\mathcal{T}_m[u]$ such that $0\leqslant i_0<p^k$, $0\leqslant i_1\leqslant\min\{p^{k-1}, i_0\}$, $t\geqslant 0$, $t+\deg h<i_1$ and $h(u)$ is either zero or a unit in S.*

Proof. Suppose $\langle\langle (u-1)^{i_0}+p(u-1)^t h(u), p(u-1)^{i_1}\rangle\rangle$ is a representation of C in $\mathcal{A}$. We shall first show that $i_1\leqslant p^{k-1}$.

Otherwise, we have $i_1>p^{k-1}$. Since $i_0+i_1\leqslant p^k$, we obtain $p^{k-1}<p^k-i_0$. As $(u-1)^{i_0}+p(u-1)^t h(u)\in C$, after multiplying it by $(u-1)^{p^k-i_0}$, we obtain

$$-p(u-1)^{p^{k-1}}\Omega_{p,k}+p(u-1)^{p^k-i_0+t}h(u)\in C.$$

Note that $p^k-i_0>p^{k-1}$. Hence,

$$\begin{aligned}&-p(u-1)^{p^{k-1}}\Omega_{p,k}+p(u-1)^{p^k-i_0+t}h(u)\\&\quad=p(u-1)^{p^{k-1}}\bigl(-\Omega_{p,k}+(u-1)^{p^k-i_0-p^{k-1}+t}h(u)\bigr).\end{aligned}$$

Now, $(-\Omega_{p,k}+(u-1)^{p^k-i_0-p^{k-1}+t}h(u))$, $-\Omega_{p,k}$ are units and $(u-1)^{p^k-i_0-p^{k-1}+t}h(u)$ is nilpotent. Hence, $p(u-1)^{p^{k-1}}\in C$. Therefore, $i_1\leqslant p^{k-1}$. This contradicts our assumption.

To finish our proof we only need to apply Theorem 2.5.

Conversely, we assume $C = \langle (u-1)^{i_0} + p(u-1)^t h(u), p(u-1)^{i_1}\rangle$. To show $C = \langle\langle (u-1)^{i_0} + p(u-1)^t h(u), p(u-1)^{i_1}\rangle\rangle$ and it suffices to show $T_0(C) = i_0$ and $T_1(C) = i_1$. We note the following:

$$\begin{gathered}
\bigl((u-1)^{i_0} + p(u-1)^t h(u)\bigr)\bigl((u-1)^{p^k - i_1} + p(u-1)^{p^{k-1}-i_1}\Omega_{p,k} \\
- p(u-1)^{p^k - i_0 - i_1 + t} h(u)\bigr) = 0, \\
\bigl((u-1)^{i_0} + p(u-1)^t h(u)\bigr)\bigl(p(u-1)^{p^k - i_0}\bigr) = 0 \quad \text{and} \\
\bigl(p(u-1)^{i_1}\bigr)\bigl((u-1)^{p^k - i_1} + p(u-1)^{p^{k-1}-i_1}\Omega_{p,k} - p(u-1)^{p^k - i_0 - i_1 + t} h(u)\bigr) = 0.
\end{gathered}$$

Let D be the ideal $\langle (u-1)^{p^k - i_1} + p(u-1)^{p^{k-1}-i_1}\Omega_{p,k} - p(u-1)^{p^k - i_0 - i_1 + t} h(u), p(u-1)^{p^k - i_0}\rangle$. Clearly, $D \subseteq \operatorname{Ann}(C)$. By Theorem 2.2(i), we have $T_j(C) \leqslant i_j$ and $T_j(D) \leqslant p^k - i_{(1-j)}$. Hence, $|C| \geqslant (p^m)^{2\cdot p^k - i_0 - i_1}$ and $|\operatorname{Ann}(C)| \geqslant |D| \geqslant (p^m)^{i_0 + i_1}$. However, by Theorem 3.5, we have $|C| \cdot |\operatorname{Ann}(C)| = (p^m)^{2\cdot p^k}$. Combining all three inequalities, we have $T_0(C) = i_0$, $T_1(C) = i_1$ and $\operatorname{Ann}(C) = D$. □

For convenience, we sum up the above results as follows:

Theorem 3.8. *$\langle\langle (u-1)^{i_0} + p\sum_{j=0}^{i_1-1} h_j(u-1)^j, p(u-1)^{i_1}\rangle\rangle$ is a representation of an ideal in $\mathcal{A}$ if and only if i_0, i_1 are integers such that $0 \leqslant i_0 < p^k$, $0 \leqslant i_1 \leqslant \min\{p^{k-1}, i_0\}$, and $i_0 + i_1 \leqslant p^k$ and $h_j \in \mathcal{T}_m$ for all j.*

Next, we count the number of ideals in S.

Corollary 3.9. *In S, the number of distinct ideals with $T_0 + T_1 = d$, where $d \leqslant p^k$, is*

$$\frac{p^{m(K+1)} - 1}{p^m - 1}$$

where $K = \min\{\lfloor \frac{d}{2} \rfloor, p^{k-1}\}$.

Proof. We fix $T_1 = i_1$, so, $i_0 = T_0 = d - T_1$ is fixed.

We first assume $d < p^k$. Hence, $i_0 < p^k$. By Theorem 3.8, $\langle\langle (u-1)^{i_0} + p\sum_{j=0}^{i_1-1} h_j(u-1)^j, p(u-1)^{i_1}\rangle\rangle$ is a representation, and we have $(p^m)^{i_1}$ choices for $\sum_{j=0}^{i_1-1} h_j(u-1)^j$. By Theorem 3.8, we have $T_1 \leqslant \min\{p^{k-1}, T_0\}$. But $T_0 + T_1 = d$ means that $T_1 \leqslant \min\{p^{k-1}, \lfloor \frac{d}{2} \rfloor\} = K$. We vary T_1 from 0 to K, and we have $1 + (p^m) + \cdots + (p^m)^K = \frac{p^{m(K+1)}-1}{p^m - 1}$ ideals with $T_0 + T_1 = d$.

Next, let $d = p^k$. When $i_0 = p^k$, the only ideal with $T_0 + T_1 = p^k$ is the ideal represented by $\langle\langle 0, p\rangle\rangle$. When $i_0 < p^k$, we apply a similar argument as before. □

4. Duals in $\mathrm{GR}(p^2, m)[u]/\langle u^{p^k} - 1\rangle$

In $S = \mathrm{GR}(p^2, m)[u]/\langle u^{p^k} - 1\rangle$, we define the dot product such that for all $f(u) = \sum_{j=0}^{p^k-1} f_j u^j$, $g(u) = \sum_{j=0}^{p^k-1} g_j u^j \in S$,

$$f(u) \cdot g(u) = \sum_{j=0}^{p^k-1} f_j g_j.$$

With respect to the dot product, we define the dual of an ideal C, denoted by $C^\perp$ as

$$\{f(u) \in S \mid f(u) \cdot g(u) = 0 \text{ for all } g(u) \in C\}.$$

It can be shown that $C^\perp$ is an ideal of S.

Next, we define the conjugate map as $\bar{\ } : \mathrm{GR}(p^2, m)[u]/\langle u^{p^k} - 1\rangle \to \mathrm{GR}(p^2, m)[u]/\langle u^{p^k} - 1\rangle$, $\sum_{j=0}^{p^k-1} a_j u^j \mapsto \sum_{j=0}^{p^k-1} a_j u^{-j}$, and we write the image as $\overline{\sum_{j=0}^{p^k-1} a_j u^j}$. For any ideal C of S, we denote $\overline{C}$ to be the image of the conjugate map restricted to C. It can be shown that $\overline{C}$ is also an ideal of S. In particular, we have the following theorem which describes the relation between $\mathrm{Ann}(C)$ and $C^\perp$. The proof of which can be derived from a similar theorem, Theorem 7.37 in [5].

Theorem 4.1. *Let C be an ideal of S. Then $C^\perp = \overline{\mathrm{Ann}(C)}$.*

From Theorem 3.8, we have the representation of an ideal C in $\mathcal{A}$ and from the proof, we have the description of $\mathrm{Ann}(C)$. Hence, it is not difficult to determine $\overline{\mathrm{Ann}(C)}$. We have the following theorem.

Theorem 4.2. *Let C be an ideal in $\mathcal{A}$ and $C = \langle\langle (u-1)^{i_0} + p\sum_{j=0}^{i_1-1} h_j (u-1)^j, p(u-1)^{i_1}\rangle\rangle$ where $h_j \in \mathcal{T}_m$. Then $C^\perp$ has the representation*

$$\left\langle\!\!\left\langle (u-1)^{p^k-i_1} - p(u-1)^{p^k-i_0-i_1} \sum_{r=0}^{i_1-1} \left(\sum_{j=0}^{r} h_j \binom{i_0-j}{r-j} \right) (u-1)^r \right.\right.$$
$$\left.\left. + \sum_{r=1}^{K} \left(\sum_{j=1}^{\min\{r, p-1\}} \binom{p}{j} \binom{p-j}{r-j} \right) (u-1)^{r \cdot p^{k-1} - i_1}, p(u-1)^{p^k - i_0} \right\rangle\!\!\right\rangle,$$

where $K = \lfloor \frac{p^k - i_0 + i_1 - 1}{p^{k-1}} \rfloor$. In the case where $K = 0$, we regard the sum as zero.

Proof. As shown in the proof of Theorem 3.8, we have

$$\mathrm{Ann}(C) = \left\langle (u-1)^{p^k-i_1} - p(u-1)^{p^k-i_0-i_1} \sum_{j=0}^{i_1-1} h_j (u-1)^j \right.$$
$$\left. + p(u-1)^{p^{k-1}-i_1} \Omega_{p,k}, p(u-1)^{p^k-i_0} \right\rangle.$$

Hence, $C^{\perp} = \overline{\mathrm{Ann}(C)}$ contains the elements, $p(u-1)^{p^k-i_0}$ and

$$(u-1)^{p^k-i_1} - p(u-1)^{p^k-i_0-i_1}\sum_{j=0}^{i_1-1} h_j(u-1)^j u^{i_0-j} + \sum_{j=1}^{p-1}\binom{p}{j}(u-1)^{j\cdot p^{k-1}-i_1}u^{p^k-j\cdot p^{k-1}}.$$

By using a similar argument as in the proof of Theorem 3.7 in calculating the number of elements in $C^{\perp}$ and $\overline{\mathrm{Ann}(C)}$, $C^{\perp}$ is indeed generated by the two elements. Hence, to obtain the desired representation, we write $u = (u-1)+1$ and remove all terms $p(u-1)^j$ with $j \geqslant p^k - i_0$. □

Next, we examine self-dual codes in S. Let C be an ideal of S. We say, C is *self-dual* if $C = C^{\perp}$. It is clear that if C is self-dual, then $|C| = (p^m)^{p^k}$. Therefore, if $C = \langle\langle (u-1)^{i_0} + p\sum_{j=0}^{i_1-1} h_j(u-1)^j, p(u-1)^{i_1}\rangle\rangle$, where $h_j \in \mathcal{T}_m$, then we have $i_0 + i_1 = p^k$. We rewrite the representation of C as

$$\left\langle\!\!\left\langle (u-1)^{p^k-i_1} + p\sum_{j=0}^{i_1-1} h_j(u-1)^j,\ p(u-1)^{i_1}\right\rangle\!\!\right\rangle.$$

By Theorem 4.2, $C^{\perp}$ has the representation,

$$\left\langle\!\!\left\langle (u-1)^{p^k-i_1} - p\sum_{r=0}^{i_1-1}\left(\sum_{j=0}^{r} h_j\binom{p^k-i_1-j}{r-j}\right)(u-1)^r,\ p(u-1)^{i_1}\right\rangle\!\!\right\rangle,$$

when $i_1 < \lfloor\frac{p^{k-1}+1}{2}\rfloor$, or,

$$\left\langle\!\!\left\langle (u-1)^{p^k-i_1} - p\sum_{r=0}^{i_1-1}\left(\sum_{j=0}^{r} h_j\binom{p^k-i_1-j}{r-j}\right)(u-1)^r + p(u-1)^{p^{k-1}-i_1},\ p(u-1)^{i_1}\right\rangle\!\!\right\rangle,$$

when $i_1 \geqslant \lfloor\frac{p^{k-1}+1}{2}\rfloor$.

By the uniqueness of the representation, if $C = C^{\perp}$, then for $r = 0, 1, \ldots, i_1 - 1$,

$$ph_r = p\left(-\left(\sum_{j=0}^{r} h_j\binom{p^k-i_1-j}{r-j}\right) + c_r\right),$$

where $c_r = 1$ when $r = p^{k-1} - i_1$ and $c_r = 0$ otherwise.

Therefore, our objective is to find the number of i_1-tuples $(ph_0, ph_1, \ldots, ph_{i_1-1})^t$ such that

$$p\begin{pmatrix} 2 & 0 & 0 & \cdots & 0 \\ \binom{p^k-i_1}{1} & 2 & 0 & \cdots & 0 \\ \binom{p^k-i_1}{2} & \binom{p^k-i_1-1}{1} & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{p^k-i_1}{i_1-1} & \binom{p^k-i_1-1}{i_1-2} & \binom{p^k-i_1-2}{i_1-3} & \cdots & 2 \end{pmatrix}\begin{pmatrix} h_0 \\ h_1 \\ h_2 \\ \vdots \\ h_{i_1-1}\end{pmatrix} = p\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{i_1-1}\end{pmatrix}.$$

We denote the $i_1 \times i_1$ matrix to be $M(p^k, i_1)$, and the last column $\vec{c}$. For convenience, we regard the first column as the 0th column, the first row as the 0th row, and so on and so forth.

As all h_i are in $\mathcal{T}_m$, solutions exist if and only if

$$M\big(p^k, i_1\big)(x_0, \dots, x_{i_1-1})^t = (c_0, \dots, c_{i_1-1})^t$$

in $\mathbb{F}_{p^m}$. Let κ be the nullity of $M(p^k, i_1)$ over $\mathbb{F}_{p^m}$. Then the number of solutions $(h_0, \dots, h_{i_1-1}) \bmod p$ is $(p^m)^\kappa$.

Since we are only interested in the i_1-tuples $(ph_0, \dots, ph_{i_1-1})^t$, the number of such i_1-tuples is still $(p^m)^\kappa$. We thus obtain the following result.

Theorem 4.3. *Let $N(p^k, i_1)$ denote the number of self-dual ideals in S with $T_1 = i_1$. Then,*

$$N\big(p^k, i_1\big) = \begin{cases} (p^m)^\kappa, & \text{when there is a solution for } (x_0, \dots, x_{i_1-1})^t, \\ 0, & \text{otherwise.} \end{cases}$$

In particular, when p is odd, $M(p^k, i_1)$ is an upper triangular matrix with non-zero diagonal entries in $\mathbb{F}_{p^m}$. Therefore, $M(p^k, i_1)$ is invertible and hence the nullity is zero and the solution for the matrix equation is always unique.

Therefore, we have the following corollary.

Corollary 4.4. *Let p be odd. Then the number of self-dual ideals in S is $p^{k-1} + 1$. Furthermore, let C be a self-dual ideal in S, and fix $T_1(C) = i_1$. Then C has the representation,*

$$\big\langle\!\big\langle (u-1)^{p^k - i_1}, p(u-1)^{i_1} \big\rangle\!\big\rangle, \quad \text{when } i_1 < \left\lfloor \frac{p^{k-1}+1}{2} \right\rfloor, \quad \text{or,}$$

$$\big\langle\!\big\langle (u-1)^{p^k - i_1} + pa(u-1)^{p^{k-1} - i_1}, p(u-1)^{i_1} \big\rangle\!\big\rangle, \quad \text{when } i_1 \geqslant \left\lfloor \frac{p^{k-1}+1}{2} \right\rfloor,$$

where a is the inverse of 2 in $\mathcal{T}_m$ (identifying $p\mathcal{T}_m$ with $\mathbb{F}_{p^m}$).

Proof. We note that when p is odd, 2 is a unit in $\mathbb{F}_{p^m}$. Hence, $M(p^k, i_1)$ is an invertible matrix and its nullity is zero. So for each $i_1 = 0, 1, \dots, p^{k-1}$, the matrix equation has a unique solution.

When $i_1 < \lfloor \frac{p^{k-1}+1}{2} \rfloor$, $\vec{c}$ is a zero column vector, and hence $h_0 = h_1 = \cdots = h_{i_1-1} = 0$.

When $i_1 \geqslant \lfloor \frac{p^{k-1}+1}{2} \rfloor$, $\vec{c}$ is a column vector with 1 at the $(p^{k-1} - i_1)$th coordinate with zeros elsewhere. We note that, the $(p^{k-1} - i_1)$th column consists of 2 at the $(p^{k-1} - i_1)$th coordinate. The $(p^{k-1} - i_1 + j)$th coordinate is $\binom{p^k - p^{k-1}}{j}$ when $1 \leqslant j \leqslant 2i_1 - p^{k-1} - 1$. Moreover, $\binom{p^k - p^{k-1}}{j} = 0$ when $1 \leqslant j \leqslant 2i_1 - p^{k-1} - 1$. Hence, we check that $h_{p^{k-1} - i_1} = a$ and $h_j = 0$, when $j \neq p^{k-1} - i_1$, is indeed the unique solution. We thus obtain the above representations. □

Unfortunately, when $p = 2$, $M(2^k, i_1)$ is a lower triangular matrix with the leading coefficient 0. Hence, the calculation is more involved, and so we restrict our analysis to small k. We have the following corollary.

Corollary 4.5. *For $k \in \{1,2,3,4\}$ and C is a self-dual ideal in S if and only if C is one of the following*:

(i) $(k=1)$ $\langle\langle 0,2\rangle\rangle$;
(ii) $(k=2)$ $\langle\langle 0,2\rangle\rangle$, *or*, $\langle\langle (u-1)^3+2h_0, 2(u-1)\rangle\rangle$;
(iii) $(k=3)$ $\langle\langle 0,2\rangle\rangle$, $\langle\langle (u-1)^7+2h_0, 2(u-1)\rangle\rangle$, *or*, $\langle\langle (u-1)^6+2(h_1(u-1)+h_0), 2(u-1)^2\rangle\rangle$;
(iv) $(k=4)$ $\langle\langle 0,2\rangle\rangle$, $\langle\langle (u-1)^{15}+2h_0, 2(u-1)\rangle\rangle$, $\langle\langle (u-1)^{14}+2(h_1(u-1)+h_0), 2(u-1)^2\rangle\rangle$, $\langle\langle (u-1)^{13}+2(h_2(u-1)^2+h_1(u-1)), 2(u-1)^3\rangle\rangle$, $\langle\langle (u-1)^{12}+2(h_3(u-1)^3+h_2(u-1)^2+h_0), 2(u-1)^4\rangle\rangle$, $\langle\langle (u-1)^{11}+2(h_4(u-1)^4+h_3(u-1)^3+(1-h_1)(u-1)^2+h_1(u-1)), 2(u-1)^5\rangle\rangle$, $\langle\langle (u-1)^{10}+2(h_5(u-1)^5+h_4(u-1)^4+h_2(u-1)^2+(1-h_0)(u-1)+h_0), 2(u-1)^6\rangle\rangle$, *or*, $\langle\langle (u-1)^9+2(h_6(u-1)^6+h_5(u-1)^5+h_3(u-1)^4+h_3(u-1)^3+h_1(u-1)+1), 2(u-1)^7\rangle\rangle$,

where $h_j \in \mathcal{T}_m$.

Moreover, the number of self-dual ideals in S is

(i) $(k=1)$ 1;
(ii) $(k=2)$ $1+2^m$;
(iii) $(k=3)$ $1+2^m+2(2^m)^2$;
(iv) $(k=4)$ $1+2^m+2(2^m)^2+2(2^m)^3+2(2^m)^4$.

Remark 4.6. We note that: the results of Corollary 4.5(i), (ii) and (iii) agree with Corollaries 5.6 and 5.7 in [3]. However, in (iv), we note that authors in [3] has left out the case where $i_1 = 7$.

5. Conclusion

We have introduced a method of representing the ideals in $\mathrm{GR}(p^e,m)[u]/\langle u^{p^k}-1\rangle$. The method enabled us to classify all ideals in the ring $\mathrm{GR}(p^2,m)/\langle u^{p^k}-1\rangle$. We also analysed the duals, and identified all the self-dual ideals when p is odd. When $p=2$, we analysed for the case where k is small. An open problem is to derive a closed formula for the number of self-dual ideals for all k when $p=2$.

Another problem is to classify all ideals in $\mathrm{GR}(p^e,m)[u]/\langle u^{p^k}-1\rangle$ for $e \geqslant 3$ and for any prime p. Here, one could follow an approach similar to that in Theorem 3.7. To verify if $\langle\langle f_0(u), f_1(u), \ldots, f_{e-1}(u)\rangle\rangle$ is the representation of an ideal in $\mathrm{GR}(p^e,m)[u]/\langle u^{p^k}-1\rangle$, one could construct polynomials $g_0(u), g_1(u), \ldots, g_{e-1}(u)$ such that $f_i(u)g_j(u)=0$ for all $i,j=0,1,\ldots,e-1$ and $\sum_{i=0}^{e-1}\deg f_i(u)+\deg g_i(u) = e\cdot p^k$. However, such a constructive approach gets unwieldy with large e.

Acknowledgments

We would like to thank the referees for their invaluable comments.

References

[1] T. Abualrub, R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e, IEEE Trans. Inform. Theory 49 (9) (2003) 2126–2133.

[2] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, Discrete Appl. Math. 128 (2003) 27–46.

[3] S.T. Dougherty, S. Ling, Cyclic codes over $\mathbb{Z}_4$ of even length, Des. Codes Cryptogr. 39 (2) (2006) 127–153.

[4] S.T. Dougherty, Y.H. Park, On modular cyclic codes, Finite Fields Appl. 13 (1) (2007) 31–57.

[5] S. Ling, C. Xing, Coding Theory: A First Course, Cambridge Univ. Press, 2004.