Des. Codes Cryptogr. (2012) 63:105–112
DOI 10.1007/s10623-011-9538-5

A note on cyclic codes over GR(p^2, m) of length p^k

Han Mao Kiah · Ka Hin Leung · San Ling

Received: 3 October 2009 / Revised: 30 January 2011 / Accepted: 17 June 2011 /
Published online: 9 July 2011
© Springer Science+Business Media, LLC 2011

Abstract The number of self-dual cyclic codes of length p^k over GR(p^2, m) is determined by the nullity of a certain matrix $M(p^k, i_1)$. With the aid of Genocchi numbers, we determine the nullity of $M(p^k, i_1)$ and hence determine completely the number of such codes.

Keywords Self-dual · Cyclic codes · Galois rings · Genocchi numbers

Mathematics Subject Classification (2000) Primary: 94B15T · Secondary: 11T71

1 Introduction

The study of cyclic codes over finite rings started in the 1990s. It was motivated by the discovery 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 $\mathbb{Z}_4$ [5]. Note that cyclic codes of length N over the ring R are described by the ideals of the ring $R[X]/\langle X^N - 1\rangle$. Furthermore, Blackford [2], Dougherty and Park [4] showed that for a prime p, the ring $\mathbb{Z}_{p^e}[X]/\langle X^N - 1\rangle$ is isomorphic to the direct sum of rings of the form GR(p^e, m)$[u]/\langle u^{p^k} - 1\rangle$, where GR($p^e$, m) denotes the Galois ring

Communicated by G. McGuire.

H. M. Kiah (✉) · S. Ling
Division of Mathematical Sciences, School of Physical and Mathematical Sciences,
Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Republic of Singapore
e-mail: kiah0001@ntu.edu.sg

S. Ling
e-mail: lingsan@ntu.edu.sg

K. H. Leung
Department of Mathematics, National University of Singapore, Block S17,
10 Lower Kent Ridge Road, Singapore 119076, Republic of Singapore
e-mail: matlkh@nus.edu.sg

of characteristic p^e with $(p^e)^m$ elements, and k is the largest integer such that p^k divides N. Hence, to study cyclic codes over $\mathbb{Z}_{p^e}$, it suffices to study ideals in $\mathrm{GR}(p^e, m)[u]/\langle u^{p^k} - 1\rangle$.

Abualrub, Oehmke [1], Dougherty and Ling [3] then proceeded to account for all the ideals in the ring $\mathrm{GR}(4, m)[u]/\langle u^{2^k} - 1\rangle$. Modifying their approach, the present authors found a new way in [6] to represent those ideals in $\mathrm{GR}(p^2, m)[u]/\langle u^{p^k} - 1\rangle$ and therefore accounted for all of them. It was shown that the number of ideals corresponding to self-dual codes of length p^k over $\mathrm{GR}(p^2, m)$ is actually the number of solutions of certain matrix equations. Unfortunately, there was an error in [6] as observed by Sobhani and Esmaeili [7]. Using a similar approach, they corrected this error and provided the correct matrix equations. However, they did not provide the number of solutions for these matrix equations in general. In this note, we find this number and hence determine the number of self-dual ideals of length p^k over $\mathrm{GR}(p^2, m)$.

2 The matrix $M(p^k, i_1)$ and the existence of self-dual ideals

We follow the notations used in [6] and [7].

It has been shown in [6] that any self-dual ideal in $\mathrm{GR}(p^2, m)/\langle u^{p^k} - 1\rangle$ can be written as $\langle (u-1)^{i_0} + p\sum_{j=0}^{i_1-1} x_j (u-1)^j,\ p(u-1)^{i_1}\rangle$, where $x_0, x_1, \ldots, x_{i_1-1} \in \mathcal{T}_m$, the set of Teichmüller representatives in $\mathrm{GR}(p^2, m)$, and $i_0 + i_1 = p^k$. The number i_1 is called the first torsional degree. If $i_1 = 0$, it is trivial to note that there is only one self-dual ideal and it is the ideal generated by p.

However, when i_1 is positive, the situation is more complicated. First, we recall that $M(p^k, i_1)$ is the $i_1 \times i_1$ matrix over $\mathbb{F}_{p^m}$ defined in [7],

$$M(p^k, i_1) := \begin{pmatrix} (-1)^{i_0}+1 & 0 & 0 & \cdots & 0 \\ (-1)^{i_0}\binom{i_0}{1} & (-1)^{i_0+1}+1 & 0 & \cdots & 0 \\ (-1)^{i_0}\binom{i_0}{2} & (-1)^{i_0+1}\binom{i_0-1}{1} & (-1)^{i_0+2}+1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (-1)^{i_0}\binom{i_0}{i_1-1} & (-1)^{i_0+1}\binom{i_0-1}{i_1-2} & (-1)^{i_0+2}\binom{i_0-2}{i_1-3} & \cdots & (-1)^{i_0+i_1-1}+1 \end{pmatrix}.$$

It is also known that the ideal $\langle (u-1)^{i_0} + p\sum_{j=0}^{i_1-1} x_j (u-1)^j,\ p(u-1)^{i_1}\rangle$ is self-dual if and only if $x_0, x_1, \ldots, x_{i_1-1}$ satisfy the following matrix equations:

i. when $i_1 < \frac{p^{k-1}+1}{2}$,

$$M(p^k, i_1)\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{i_1-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}; \tag{1}$$

ii. when $i_1 \geq \frac{p^{k-1}+1}{2}$,

$$M(p^k, i_1) \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{p^{k-1}-i_1} \\ \vdots \\ x_{i_1-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow (p^{k-1} - i_1 + 1)\text{-th coordinate.} \tag{2}$$

First, we shall demonstrate when these equations admit solutions. For (1), it is clear $x_0 = x_1 = \cdots = x_{i_1-1} = 0$ is a solution and the ideal given by $\langle (u-1)^{p^k - i_1}, p(u-1)^{i_1} \rangle$ is indeed self-dual in $\mathrm{GR}(p^2, m)/\langle u^{p^k} - 1 \rangle$.

For (2), we observe that, when p is odd, the $(p^{k-1} - i_1 + 1)$-th column of $M(p^k, i_1)$ is

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ (-1)^{i_0+p^{k-1}-i_1} + 1 \\ (-1)^{i_0+p^{k-1}-i_1} \binom{i_0 - (p^{k-1} - i_1)}{1} \\ \vdots \\ (-1)^{i_0+p^{k-1}-i_1} \binom{i_0 - (p^{k-1} - i_1)}{i_1 - (p^{k-1} - i_1) - 1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 2 \\ \binom{p^k - p^{k-1}}{1} \\ \vdots \\ \binom{p^k - p^{k-1}}{2i_1 - p^{k-1} - 1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 2 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

When $p = 2$ and $2^{k-2} + 1 \leq i_1 < 2^{k-1}$, we observe that the $(2^{k-1} - i_1)$-th column of $M(2^k, i_1)$ is

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ \binom{i_0 - (2^{k-1} - i_1 - 1)}{1} \\ \vdots \\ \binom{i_0 - (2^{k-1} - i_1 - 1)}{i_1 - (2^{k-1} - i_1 - 1) - 1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \binom{2^{k-1} + 1}{1} \\ \vdots \\ \binom{2^{k-1} + 1}{2i_1 - 2^{k-1}} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}.$$

Thus, we conclude that, in the above cases, the matrix equation admits a solution. Finally, if $p = 2$ and $i_1 = 2^{k-1}$, then the first row of $M(2^k, 2^{k-1})$ is all-zero, while the first coordinate on the right hand side of (2) is 1. Therefore, (2) has no solution in this case.

Since the number of solutions to the matrix equations is equal to the number of self-dual ideals, we have the following proposition.

Proposition 2.1 *Let $i_1 > 0$, let κ be the nullity of $M(p^k, i_1)$ over $\mathbb{F}_{p^m}$ and let N be the number of self-dual ideals with first torsional degree i_1 in $\mathrm{GR}(p^2, m)[u]/\langle u^{p^k} - 1 \rangle$. Then*

$$N = \begin{cases} 0, & \text{if } p = 2 \text{ and } i_1 = 2^{k-1}, \\ (p^m)^\kappa, & \text{otherwise.} \end{cases}$$

3 Nullity of the matrix $M(p^k, i_1)$

In [6], the nullity of the matrix $M(p^k, i_1)$ over $\mathbb{F}_{p^m}$, when $p = 2$ and $k \in \{1, 2, 3, 4\}$, was determined. In [7], Sobhani and Esmaeili have listed all the self-dual ideals when $p = 3$ and $k \in \{1, 2, 3\}$, and for all values of p when $k = 1$. However, the general case remains open. Our strategy here is to consider $M(p^k, i_1)$ first as a matrix over $\mathbb{Q}$, and then deduce its rank as a matrix over $\mathbb{F}_{p^m}$. For convenience, we define the following matrix $T(a + b, b)$ for any positive integers a, b with $a \geq b$:

$$T(a+b,b) := \begin{pmatrix} (-1)^a+1 & 0 & 0 & \cdots & 0 \\ (-1)^a\binom{a}{1} & (-1)^{a+1}+1 & 0 & \cdots & 0 \\ (-1)^a\binom{a}{2} & (-1)^{a+1}\binom{a-1}{1} & (-1)^{a+2}+1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (-1)^a\binom{a}{b-1} & (-1)^{a+1}\binom{a-1}{b-2} & (-1)^{a+2}\binom{a-2}{b-3} & \cdots & (-1)^{a+b-1}+1 \end{pmatrix}.$$

Note that $M(p^k, i_1) = T(i_0 + i_1, i_1) \mod p$ and also, $T(a+b, b)$ is a $b \times b$ matrix over $\mathbb{Z}$. We first consider the case where a is odd. We also fix the following notation. We denote the first row of $T(a + b, b)$ as r_0, the second row as r_1, and so on. We call a row r_j *odd* if j is odd, and *even* if j is even. For each row r_j, we denote its first entry as $r_j^{(0)}$, its second entry as $r_j^{(1)}$, and so on.

With these notations, we have

$$T(a+b,b) := \begin{pmatrix} r_0^{(0)} & r_0^{(1)} & \cdots & r_0^{(b-1)} \\ r_1^{(0)} & r_1^{(1)} & \cdots & r_1^{(b-1)} \\ \vdots & \vdots & \ddots & \vdots \\ r_{b-1}^{(0)} & r_{b-1}^{(1)} & \cdots & r_{b-1}^{(b-1)} \end{pmatrix}, \text{ where } r_j^{(l)} = \begin{cases} (-1)^{a+l}\binom{a-l}{j-l}, & \text{when } j > l, \\ (-1)^{a+l}+1, & \text{when } j = l, \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 3.1 *For all* $1 \leq j \leq \lfloor \frac{b-1}{2} \rfloor$, *we have*

$$r_{2j} = \alpha_1 r_1 + \alpha_3 r_3 + \cdots + \alpha_{2j-1} r_{2j-1},$$

for some $\alpha_i \in \mathbb{Z}$.

Before we prove the above lemma, we first define a sequence of numbers, called the *Genocchi numbers* and denoted by G_n. These numbers are defined by the generating function

$$\frac{2t}{1+e^t} = \sum_{n=0}^{\infty} \frac{G_n}{n!} t^n. \tag{3}$$

It is well known that $G_0 = G_3 = G_5 = \cdots = 0$, $G_1 = 1$ and $G_2 = -1$ [8]. Rearranging (3), we have

$$2t = \left(\sum_{n=0}^{\infty} \frac{G_n}{n!} t^n\right)(1+e^t) = \left(\sum_{n=0}^{\infty} \frac{G_n}{n!} t^n\right)\left(2 + \sum_{n=1}^{\infty} \frac{1}{n!} t^n\right).$$

Comparing the coefficients of t^n where $n \geq 3$, we have the following:

$$\frac{1}{(n-1)!} = -\sum_{i=1}^{\frac{n-1}{2}} \frac{G_{2i}}{(2i)!(n-2i)!}, \text{ when } n \text{ is odd,} \tag{4}$$

and

$$\frac{1}{(n-1)!} = -\left(\sum_{i=1}^{\frac{n}{2}-1} \frac{G_{2i}}{(2i)!(n-2i)!}\right) - \frac{2G_n}{n!}, \text{ when } n \text{ is even.} \tag{5}$$

With these identities, we proceed to prove Lemma 3.1.

Proof of Lemma 3.1 We fix j and claim that

$$r_{2j} = -\sum_{i=1}^{j} \frac{G_{2i}}{a-2(j-i)} \binom{a-2(j-i)}{a-2j} r_{2(j-i)+1}. \tag{6}$$

To prove the two vectors on both sides to be equal, we consider the k-th coordinates of the two vectors. The k-th coordinates of both vectors are 0 if $k > 2j$. For the $2j$-th coordinates, since a is odd, the right hand side of (6) is

$$-\frac{G_2}{a-2j+2} \binom{a-2j+2}{a-2j} \cdot 2 = a-2j+1 = r_{2j}^{(2j-1)}.$$

Next, the $(2j-1)$-th coordinate of the right hand side of (6) is

$$-\frac{G_2}{a-2j+2} \binom{a-2j+2}{a-2j} \cdot (-1)^{a+2j-2} \binom{a-2j+2}{1} = (-1)^{a+2j-2} \binom{a-2j+2}{2} = r_{2j}^{(2j-2)}.$$

Next, we consider the $(2l+1)$-th coordinates on both sides of the equation (6) for $0 \leq l \leq j-2$. Note that $r_{2l-1}^{(2l)} = r_{2l-3}^{(2l)} = \cdots = r_1^{(2l)} = 0$ and $r_{2l+1}^{(2l)} = -\binom{a-2l}{1}$. Thus the $(2l+1)$-th coordinate of the vector on the right is:

$$\begin{aligned}
&-\sum_{i=1}^{j} \frac{G_{2i}}{a-2(j-i)} \binom{a-2(j-i)}{a-2j} r_{2(j-i)+1}^{(2l)} \\
&= \sum_{i=1}^{j-l} \frac{G_{2i}}{a-2(j-i)} \binom{a-2(j-i)}{a-2j} \binom{a-2l}{2(j-i-l)+1} \\
&= \sum_{i=1}^{j-l} \frac{G_{2i}}{a-2(j-i)} \frac{(a-2(j-i))!}{(a-2j)!(2i)!} \frac{(a-2l)!}{(2(j-l-i)+1)!(a-2(j-i))!} \\
&= \frac{(a-2l)!}{(a-2j)!} \left(\sum_{i=1}^{j-l} \frac{G_{2i}}{(2i)!(2(j-l)-2i)!}\right) \\
&= -\frac{(a-2l)!}{(a-2j)!(2j-2l)!} \text{ (this follows from (4))} \\
&= -\binom{a-2l}{2j-2l} = r_{2j}^{(2l)}.
\end{aligned}$$

Similarly, we consider the $(2l+2)$-th coordinates for $0 \le l \le j-2$. Again, observe that $r_{2l-1}^{(2l+1)} = r_{2l-3}^{(2l+1)} = \cdots = r_1^{(2l+1)} = 0$ and $r_{2l+1}^{(2l+1)} = 2$. So, the $(2l+2)$-th coordinate is:

$$\begin{aligned}
&-\sum_{i=1}^{j} \frac{G_{2i}}{a-2(j-i)} \binom{a-2(j-i)}{a-2j} r_{2(j-i)+1}^{(2l+1)} \\
&= \left(\sum_{i=1}^{j-l-1} \frac{G_{2i}}{a-2(j-i)} \binom{a-2(j-i)}{a-2j} \binom{a-2l-1}{2(j-i-l)} \right) - \left(\frac{G_{2(j-l)}}{a-2l} \binom{a-2l}{a-2j} \cdot 2 \right) \\
&= \cdots \\
&= \frac{(a-2l-1)!}{(a-2j)!} \left(- \left(\sum_{i=1}^{j-l-1} \frac{G_{2i}}{(2i)!(2(j-l)-2i)!} \right) - 2\frac{G_{2(j-l)}}{(2j-2l)!} \right) \\
&= \frac{(a-2l-1)!}{(a-2j)!(2j-2l-1)!} \text{ (this follows from (5))} \\
&= \binom{a-2l-1}{2j-2l-1} = r_{2j}^{(2l+1)}.
\end{aligned}$$

For simplicity, we define $\alpha_i = -\frac{G_{2j-i+1}}{a-i+1} \binom{a-i+1}{a-2j}$ for odd $1 \le i \le 2j-1$. It remains to prove that $\alpha_i \in \mathbb{Z}$ for all odd $1 \le i \le 2j-1$. We proceed by induction. Clearly, $\alpha_{2j-1} = -\frac{G_2}{a-2j+2} \binom{a-2j+2}{a-2j} = -\frac{G_2(a-2j+1)}{2}$ is an integer as $G_2 = -1$ and $a-2j+1$ is even.

Next, we assume that $\alpha_{i+2}, \alpha_{i+4}, \ldots \alpha_{2j-1} \in \mathbb{Z}$. Our aim is to show that $\alpha_i \in \mathbb{Z}$.

By considering the $(i+1)$-th and i-th coordinates of the vector r_{2j}, we obtain

$$2\alpha_i = r_{2j}^{(i)} - \alpha_{i+2} r_{i+2}^{(i)} - \alpha_{i+4} r_{i+4}^{(i)} - \cdots - \alpha_{2j-1} r_{2j-1}^{(i)}$$

and

$$(a-i+1)\alpha_i = r_{2j}^{(i-1)} - \alpha_{i+2} r_{i+2}^{(i-1)} - \alpha_{i+4} r_{i+4}^{(i-1)} - \cdots - \alpha_{2j-1} r_{2j-1}^{(i-1)}.$$

By the inductive hypothesis, $2\alpha_i$ and $(a-i+1)\alpha_i$ are integers. As i is odd, $a-i$ is even. Therefore, $\alpha_i = (a-i+1)\alpha_i - \frac{a-i}{2} \cdot 2\alpha_i$ is also an integer. □

We now consider the case when a is even. Note that the matrix $T(a+b, b)$ can be regarded as a submatrix of $T((a+1)+(b+1), (b+1))$ as follows:

$$T((a+1)+(b+1), (b+1)) = \left(\begin{array}{c|ccc} * & 0 & \cdots & 0 \\ \hline * & & & \\ \vdots & & T(a+b, b) & \\ * & & & \end{array} \right).$$

By Lemma 3.1, we conclude that each even row r_{2j} of $T((a+1)+(b+1), b+1)$ is an integral linear combination of the odd rows $r_1, r_3, \ldots, r_{2j-1}$ in $T((a+1)+(b+1), b+1)$. This implies that each odd row r_{2j-1} of $T(a+b, b)$ is an integral linear combination of the even rows $r_0, r_2, \ldots, r_{2j-2}$ of $T(a+b, b)$.

We now summarize these results as follows:

Lemma 3.2 *Consider the matrix $T(a+b, b)$. When a is odd, each even row r_{2j} is an integral linear combination of the odd rows $r_1, \ldots, r_{2j-1}$. When a is even, each odd row r_{2j+1} is an integral linear combination of the even rows $r_0, \ldots, r_{2j}$.*

Finally, we consider the matrix $M(p^k, i_1)$. Since the matrix $M(p^k, i_1)$ is $T(i_0 + i_1, i_1)$ mod p, we can apply Lemma 3.2. There are two cases.

(I) p is odd.
In this case, $M(p^k, i_1)$ is of the form:

$$\begin{matrix}\star\\ \circ\\ \star\\ \circ\\ \vdots\\ \star\end{matrix}\begin{pmatrix} 2\,0\,0\,0\cdots 0\\ *\,0\,0\,0\cdots 0\\ *\,*\,2\,0\cdots 0\\ *\,*\,*\,0\cdots 0\\ \vdots\;\vdots\;\vdots\;\vdots\;\ddots\;\vdots\\ *\,*\,*\,*\cdots 2\end{pmatrix} \quad \text{and} \quad \begin{matrix}\circ\\ \star\\ \circ\\ \star\\ \vdots\\ \star\end{matrix}\begin{pmatrix} 0\,0\,0\,0\cdots 0\\ *\,2\,0\,0\cdots 0\\ *\,*\,0\,0\cdots 0\\ *\,*\,*\,2\cdots 0\\ \vdots\;\vdots\;\vdots\;\vdots\;\ddots\;\vdots\\ *\,*\,*\,*\cdots 2\end{pmatrix}$$

when i_1 is odd, when i_1 is even.

By Lemma 3.2, each of the rows labeled $\circ$ is an integral linear combination of the rows labeled $\star$. Moreover, when p is odd, 2 is a unit in $\mathbb{F}_{p^m}$. Therefore, the nullity of $M(p^k, i_1)$ is $\lfloor \frac{i_1}{2} \rfloor$.

(II) $p = 2$.
In this case, $M(2^k, i_1)$ is of the form:

$$\begin{matrix}\circ\\ \star\\ \circ\\ \star\\ \vdots\\ \circ\end{matrix}\begin{pmatrix} 0\,0\,0\,0\cdots 0\\ 1\,0\,0\,0\cdots 0\\ *\,*\,0\,0\cdots 0\\ *\,*\,1\,0\cdots 0\\ \vdots\;\vdots\;\vdots\;\vdots\;\ddots\;\vdots\\ *\,*\,*\,*\cdots 0\end{pmatrix} \quad \text{and} \quad \begin{matrix}\circ\\ \circ\\ \star\\ \circ\\ \vdots\\ \circ\end{matrix}\begin{pmatrix} 0\,0\,0\,0\cdots 0\\ 0\,0\,0\,0\cdots 0\\ *\,1\,0\,0\cdots 0\\ *\,*\,*\,0\cdots 0\\ \vdots\;\vdots\;\vdots\;\vdots\;\ddots\;\vdots\\ *\,*\,*\,*\cdots 0\end{pmatrix}$$

when i_1 is odd, when i_1 is even.

Again, by Lemma 3.2, each of the rows labeled $\circ$ is an integral linear combination of the rows labeled $\star$. Therefore, the nullity of $M(2^k, i_1)$ is $\lceil \frac{i_1+1}{2} \rceil$. We summarize the results in the following proposition.

Proposition 3.3 *Let κ be the nullity of $M(p^k, i_1)$. Then $\kappa = \lfloor \frac{i_1}{2} \rfloor$ when p is odd, and $\kappa = \lceil \frac{i_1+1}{2} \rceil$ when $p = 2$.*

Finally, we restate Proposition 2.1 as follows:

Proposition 3.4 *Let $i_1 > 0$ and let N be the number of self-dual ideals with first torsional degree i_1 in $\mathrm{GR}(p^2, m)[u]/\langle u^{p^k} - 1\rangle$. Then*

$$N = \begin{cases} 0, & \text{if } p = 2 \text{ and } i_1 = 2^{k-1}, \\ (p^m)^{\lceil \frac{i_1+1}{2} \rceil}, & \text{if } p = 2 \text{ and } i_1 < 2^{k-1}, \\ (p^m)^{\lfloor \frac{i_1}{2} \rfloor}, & \text{otherwise.} \end{cases}$$

The number of self-dual codes of length p^k over $\mathrm{GR}(p^2, m)$ is then given by the following corollary.

Corollary 3.5 *Let $S = \mathrm{GR}(p^2, m)/\langle u^{p^k} - 1\rangle$. When p is odd, the number of self-dual ideals in S is*

$$2 + 2(p^m) + \cdots + 2(p^m)^{\frac{p^{k-1}-1}{2}} = 2\left(\frac{(p^m)^{\frac{p^{k-1}+1}{2}} - 1}{p^m - 1}\right).$$

When $p = 2$, the number of self-dual ideals in S is

$$\begin{cases} 1, & \text{when } k = 1, \\ 1 + 2^m, & \text{when } k = 2, \\ 1 + 2^m + 2(2^m)^2 + 2(2^m)^3 + \cdots + 2(2^m)^{2^{k-2}} & \\ = 1 + 2^m + 2(2^m)^2\left(\frac{(2^m)^{(2^{k-2}-1)}-1}{2^m-1}\right), & \text{when } k \geq 3. \end{cases}$$

Acknowledgments We are grateful to the anonymous referees for their valuable comments. The research of Han Mao Kiah and San Ling is partially supported by Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

References

1. Abualrub T., Oehmke R.: On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e. IEEE. Trans. Inform. Theory. **49**(9), 2126–2133 (2003).
2. Blackford T.: Cyclic codes over $\mathbb{Z}_4$ of oddly even length. Discret. Appl. Math. **128**, 27–46 (2003).
3. Dougherty S.T., Ling S.: Cyclic codes over $\mathbb{Z}_4$ of even length. Des. Code. Cryptogr. **39**(2), 127–153 (2006).
4. Dougherty S.T., Park Y.H.: On modular cyclic codes. Finite Fields Appl. **13**, 31–57 (2007).
5. Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.: The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals, and related codes. IEEE. Trans. Inform. Theory. **40**, 301–319 (1994).
6. Kiah H.M., Leung K.H., Ling S.: Cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k. Finite Fields Appl. **14**, 834–846 (2008).
7. Sobhani R., Esmaeili M.: A note on cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k. Finite Fields Appl. **15**, 387–391 (2009).
8. Weisstein E.W.: Genocchi number. From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/GenocchiNumber.html. Accessed 15 Jul 2009.