Hokkaido Mathematical Journal Vol. 32 (2003) p. 101–116

Generalized shadows of codes over rings

Steven T. DOUGHERTY*

(Received July 30, 2001; Revised January 30, 2002)

Abstract. We describe different ways of defining shadows for self-dual codes over rings, giving special attention to the rings of order 4. We determine their respective weight enumerators and give the corresponding shadow sum constructions. We also give a connection between the shadow of a code and its construction via the Chinese Remainder Theorem.

Key words: self-dual codes, shadows, codes over rings.

1. Introduction

Self-dual codes over rings have become an important object of study. They are interesting as objects themselves, however they have added importance because of their relationship to real and complex unimodular lattices and their corresponding theta series, which are then used to construct modular forms.

Self-dual codes over $\mathbf{Z}_{2k}$ were introduced in [2] and have been studied extensively elsewhere, see [13]. Self-dual codes over $\mathbf{Z}_4$ have been widely investigated (see [11] and the references given therein). Self-dual code over $\mathbf{F}_2 + u\mathbf{F}_2$ were introduced in [1] and [5]. Three classes namely Type I, Type II and Type IV codes were introduced in [2] and [6].

We shall describe the theory of shadows applied to codes over the rings $\mathbf{Z}_k$ and $\mathbf{F}_2 + u\mathbf{F}_2$. Moreover we shall show how this theory can be applied in different manners.

Shadows for binary codes were introduced in [4]. The definition was generalized for codes over $\mathbf{Z}_4$ in [7], for codes over $\mathbf{Z}_{2k}$ in [2], and for codes over $\mathbf{F}_2 + u\mathbf{F}_2$ in [5]. In [9], a detailed study of these shadows and the corresponding shadows for lattices is given.

There are two primary purposes for shadows:

1) Eliminate a putative code by examining the weight enumerator (Hamming, Symmetric, or Complete) of the shadow by finding a coefficient

---

2000 Mathematics Subject Classification : Primary 94B60; Secondary 11H71.

*Part of the material on codes over rings of order 4 was presented at the Yamagata conference, October, 2000.

in the weight enumerator that is not a non-negative integer.

2) To build larger self-dual codes from existing self-dual codes.

To accomplish 1, it must be possible to find the weight enumerator of the shadow from the weight enumerator of the putative code. To accomplish 2, all that is required is that you know the orthogonality relations and the glue group of the cosets. If you also know the respective weight enumerators then so much the better because then you can determine the weight enumerator of the formed code (parent code). For a complete description of forming new codes from shadows see [10].

1.1. Definitions and Notations

The ring $\mathbf{Z}_k$ is the commutative ring described by $\mathbf{Z}/(k) = \{0, 1, 2, \ldots, k-1\}$ and the ring $\mathbf{F}_2 + u\mathbf{F}_2$ is described by $\mathbf{Z}[i]/(2)$ or $\mathbf{Z}[x]/(2, (x+1)^2)$ and the elements are $\{0, 1, u, 1+u\}$ with $u^2 = 0$. The Euclidean weight of a vector $x = (x_1, x_2, \ldots, x_n)$ in $\mathbf{Z}_k$ is $\sum_{i=1}^{n} \min\{x_i^2, (k-x_i)^2\}$.

Let R be finite commutative ring. A code over R is a subset of R^n and a linear code is a submodule of this space. To the ambient space R^n attach the inner product

$$[v, w] = \sum v_i w_i$$

and define the orthogonal $C^{\perp} = \{v \in R^n \mid [v, w] = 0 \ \forall w \in C\}$. We shall say that a code is self-orthogonal if $C \subseteq C^{\perp}$ and self-dual if $C = C^{\perp}$.

A self-dual code over $\mathbf{Z}_{2k}$ is Type II if all vectors in the code have Euclidean weights which are 0 (mod $4k$) and Type I otherwise. This definition is natural, given the connection to unimodular lattices described below. The same definition is not applied to codes over $\mathbf{Z}_k$ with k odd because the connection to unimodular lattices does not hold.

The explicit connection is the A_{2k} construction of a lattice from a self-dual code over $\mathbf{Z}_{2k}$. Define the reduction modulo $2k$, by $\rho : \mathbf{Z}^n \to \mathbf{Z}_{2k}^n$, by

$$\rho(x_1, \ldots, x_n) = (x_1 \pmod{2k}, \ldots, x_n \pmod{2k}).$$

Given a code C over $\mathbf{Z}_{2k}$ we construct a lattice by

$$\Lambda(C) = \frac{1}{\sqrt{2k}}\{x \in \mathbf{Z}^n \mid \rho(x) \in C\}. \tag{1}$$

In [2], it is proven that if C is a Type I code then $\Lambda(C)$ is a Type I unimodular lattice, and that if C is a Type II code then $\Lambda(C)$ is a Type II unimodular

lattice and that the minimum norm of the lattice is $\min\{2k, \frac{d_E}{2k}\}$, where d_E is the minimum Euclidean weight of the code. Additionally, there is a connection between the shadows, that is, the image of the shadow under Λ is the shadow of the image, see [9] for a complete explanation of the connection between shadow codes and shadow lattices.

The complete weight enumerator of a code C over $\mathbf{Z}_k$ is defined by

$$cwe_C(x_0, x_1, \ldots, x_{k-1}) = \sum_{c \in C} x_0^{n_0(c)} x_1^{n_1(c)} \cdots x_{k-1}^{n_{k-1}(c)}, \tag{2}$$

where $n_i(c)$ is the number of coordinates of c that are i, i.e. $n_i(c) = |\{j \mid c_j = i\}|$. The symmetric weight enumerator is defined by

$$swe_C(x_0, x_1, \ldots, x_\ell) = \sum_{c \in C} x_0^{n'_0(c)} x_1^{n'_1(c)} \cdots x_{\ell-1}^{n'_{\ell-1}(c)} x_\ell^{n'_\ell(c)}, \tag{3}$$

where $n'_i(c)$ is the number of coordinates that are $\pm i$ and $\ell = \lceil \frac{k}{2} \rceil$.

The Hamming weight enumerator is given by

$$W_C(x, y) = \sum_{c \in C} x^{n - wt(c)} y^{wt(c)} \tag{4}$$

where $wt(c)$ is the number of non-zero elements of the code.

1.2. Rings of Order 4

We shall examine the weights given in Table 1 for codes over the rings of order 4, namely the Hamming, Euclidean and Lee weights. Specifically, the Hamming weight is the number of non-zero coordinates, the Lee weight is the Hamming weight of its binary image under a gray map, and the Euclidean weight is defined in the natural manner.

Table 1. Weights for $\mathbf{Z}_4$ and $\mathbf{F}_2 + u\mathbf{F}_2$

$\mathbf{Z}_4$	$\mathbf{F}_2 + u\mathbf{F}_2$	Hamming weight	Lee weight	Euclidean weight
0	0	0	0	0
1	1	1	1	1
2	u	1	2	4
3	$1+u$	1	1	1

We say that self-dual codes over $\mathbf{F}_2 + u\mathbf{F}_2$ with the property that all Lee weights are divisible by four are *Type II*. Self-dual codes which are not

Type II are called *Type I*. This is a natural definition given the gray map defined below.

We also consider the following distance preserving gray maps.

ψ	ϕ
$\psi(0) = 00$	$\phi(0) = 00$
$\psi(1) = 01$	$\phi(1) = 01$
$\psi(1+u) = 10$	$\phi(3) = 10$
$\psi(u) = 11$	$\phi(2) = 11$

Note that ψ is $\mathbf{F}_2$-linear and ϕ is not linear.

2. Generalized shadows

Usually, the shadow is defined by taking the subcode C_0 of vectors whose Euclidean weight is 0 (mod $4k$) for a self-dual code over $\mathbf{Z}_{2k}$ and then the shadow $S = C_0^{\perp} - C$. In this section we shall generalize this idea.

In general, all that is required to build a shadow is to find a subcode of index 2. In particular, let C be a self-dual code over R with s a vector not in C, but $s + s \in C$. Define C_0 to be the subcode of C orthogonal to s, i.e.

$$C_0 = \{c \in C \mid [c, s] = 0\}.$$

Let t be a vector such that $\langle C_0, t\rangle = C$, where $\langle C_0, t\rangle$ denotes the space generated by C_0 and t, then $C_1 = C_0 + s$ and $C_3 = C_0 + s + t$.

The shadow is defined by $S = C + s$ or equivalently $S = C_1 \cup C_3$.

We know that $[t, t] = 0$ and so to determine orthogonality relations all that is required is to know $[s, t] = \tau$ and $[s, s] = \sigma$.

More generally, the vector s can be chosen as any vector that is not in C. Then let $\Psi_s : C \to \mathbf{Z}_k$ by $\Psi_s(c) = [s, c]$. Then the kernel of the map is the code C_0 and the image is a subgroup of $\mathbf{Z}_k$, denoted by G. Note that if

Table 2. Orthogonality Relations for Shadows

	C_0	C_1	C_2	C_3
C_0	0	0	0	0
C_1	0	σ	τ	$\alpha + \sigma$
C_2	0	τ	0	τ
C_3	0	$\tau + \sigma$	τ	$\sigma + 2\tau$

$\mathbf{Z}_k$ is a field then there are only two possible choices, i.e. the entire group or the trivial subgroup, however for rings there are many more possibilities for the order. It is easy to see that there exists a vector t such that $\langle C_0, t\rangle = C$ and that $[t, s] \in G$. It is also clear that the index of C_0 in C is the cardinality of the image of the map Ψ_s, specifically, each coset is mapped to an element of this subgroup.

Define the coset $C_{\alpha,\beta}$ of C_0 in $C_0^{\perp}$ by

$$C_{\alpha,\beta} = C_0 + \alpha t + \beta t \tag{5}$$

where $\alpha, \beta \in G$.

The inner-product of any vector in $C_{\alpha,\beta}$ with a vector in $C_{\alpha',\beta'}$ will be denoted by $[C_{\alpha,\beta}, C_{\alpha',\beta'}]$. This can be computed by taking an arbitrary vector from both, $c_0 + \alpha t + \beta s \in C_{\alpha,\beta}$ and $c_0' + \alpha' t + \beta' s \in C_{\alpha',\beta'}$, with c_0 and c_0' elements of C_0. Then

$$\begin{aligned}&[c_0 + \alpha t + \beta s \in C_{\alpha,\beta}, c_0' + \alpha' t + \beta' s \in C_{\alpha,\beta}]\\ &\quad = (\alpha\beta' + \beta\alpha')[t, s] + \beta\beta'[s, s].\end{aligned}$$

Note that the subgroup G consists of all the elements that are possible values for the above computations.

In this more general setting there are $|G| - 1$ shadows, specifically, each $C + \beta s$, $(\beta \neq 0)$ is a shadow of the code.

A similar construction can be made for lattices constructed from self-dual codes. Specifically, let C_0 be the subcode orthogonal to the vector s, then the following diagram commutes.

$$\begin{array}{ccc} C_0^{\perp} & \xrightarrow[A_{2k}]{} & \Lambda_0^* \\ \uparrow & & \uparrow \\ C & \xrightarrow[A_{2k}]{} & \Lambda \\ \uparrow & & \uparrow \\ C_0 & \xrightarrow[A_{2k}]{} & \Lambda_0 \end{array}$$

Specifically, Λ_0 are those vectors w such that $w \cdot A_{2k}(v) \in \mathbf{Z}$.

2.1. Shadow sums

The above technique is useful when using shadows to build larger self-dual codes. That is, one specifies a vector s and then one can determine the vector t. Then the following technique applies, which generalizes the

techniques given in [10] and the references therein.

Let C and D be self-dual codes of length n and n' respectively. Let C_0 and D_0 be subcodes of C and D both of index r and subgroup G.

Let s and t be vectors such that $C = \langle C_0, t\rangle$ and $C_0^{\perp} = \langle C, s\rangle$. Let s' and t' be vectors such that $D = \langle D_0, t'\rangle$ and $D_0^{\perp} = \langle D, s'\rangle$. The vectors t' and s' can be chosen so that

$$[s, s] = -[s', s'] \tag{6}$$

and

$$[s, t] = -[s', t'] \tag{7}$$

We can make $[s, s] = -[s', s']$ by noting that the map $F : (C_0^{\perp} - C) \to G$ given by $F(X) = [x, x]$ is injective. Moreover Ψ_r is also injective so t' can be chosen likewise.

Define the shadow sum of C and D by

$$C \bigoplus_S D = \bigcup_{\alpha,\beta} (C_{\alpha,\beta}, D_{\alpha,\beta}) \tag{8}$$

where $(C_{\alpha,\beta}, D_{\alpha,\beta}) = \{(v|v')\}$ with $v \in (C_{\alpha,\beta}$ and $v' \in D_{\alpha,\beta})$.

Theorem 2.1 *Let C and D be self-dual codes over $\mathbf{Z}_k$ of length n and n' with C_0 and D_0 of index r with group G, then the shadow sum $C \bigoplus_S D$ is a self-dual code of length $n + n'$. If $W(X)$ is any weight enumerator then*

$$W_{C \bigoplus_S D}(X) = \sum_{\alpha,\beta} W_{C_{\alpha,\beta}}(X) \times W_{D_{\alpha,\beta}}(X) \tag{9}$$

Proof. We have that $|C_0| = \frac{|C|}{r} = \frac{1}{r} k^{\frac{n}{2}}$ and $|D_0| = \frac{|D|}{r} = \frac{1}{r} k^{\frac{n'}{2}}$. Then $|C \bigoplus_S D| = r^2 |C_0||D_0| = k^{\frac{n+n'}{2}}$. The code is linear by construction.

To show the new code is self-orthogonal we consider the inner-product of two arbitrary vectors. Consider $(v|v') \in (C_{\alpha,\beta}, D_{\alpha,\beta})$ and $(w, w') \in (C_{\alpha',\beta'}, D_{\alpha',\beta'})$, then

$$\begin{aligned}
&[(v|v'), (w|w')] \\
&= [(v_0 + \alpha t + \beta s \mid v_0' + \alpha t' + \beta s'), (w_0 + \alpha' t + \beta' s \mid w_0' + \alpha' t' + \beta' s')] \\
&= (\alpha\beta' + \beta\alpha')[s, t] + \beta\beta'[s, s] + (\alpha\beta' + \beta\alpha')[s', t'] + \beta\beta'[s', s'] \\
&= 0.
\end{aligned}$$

□

As an example, let C be the self-dual code of length 3 over $\mathbf{Z}_4$ generated by $\{(200), (020), (002)\}$ and let D be the self-dual code of length 2 over $\mathbf{Z}_4$ generated by $\{(20), (02)\}$. Let $s = (123)$ and $s' = (13)$, then $[s, s] = -[s', s']$. Both C_0 and D_0 are of index 2. We have

$$\begin{aligned} swe_{C_{0,0}} &= x_0^3 + x_0^2 x_2 + x_0 x_2^2 + x_2^3 \\ swe_{C_{0,1}} &= 2x_{\pm 1}^2 x_2 + 2x_0 x_{\pm 1}^2 = swe_{C_{1,1}} \\ swe_{C_{1,0}} &= 2x_0^2 x_2 + 2x_0 x_2^2 \end{aligned}$$

and

$$swe_{D_{0,0}} = x_0^2 + x_2^2, \quad swe_{D_{0,1}} = 2x_{\pm 1}^2 = swe_{D_{1,1}}, \quad swe_{D_{1,0}} = 2x_0 x_2.$$

The shadow sum $C \bigoplus_S D$ is a self-dual code of length 5 and has the following symmetric weight enumerator:

$$\begin{aligned} &swe_{C_{0,0}} swe_{D_{0,0}} + swe_{C_{1,0}} swe_{D_{1,0}} + swe_{C_{0,1}} swe_{D_{0,1}} + swe_{C_{1,1}} swe_{D_{1,1}} \\ &= x_0{}^5 + 6x_0{}^3 x_2{}^2 + x_0{}^4 x_2 + 6x_0{}^2 x_2{}^3 + x_0 x_2{}^4 + x_2{}^5 + 8x_{\pm 1}{}^4 x_2 + 8x_{\pm 1}{}^4 x_0 \end{aligned}$$

3. Shadows from constant vectors

As an example of a useful construction technique and of a subcode whose weight enumerator is determinable, we shall examine shadows formed from constant weight vectors.

Let C be a self-dual code over $\mathbf{Z}_k$ of length n with $s = (\gamma, \gamma, \ldots, \gamma)$ not in C. Very often, such a vector can be found, for example the all one vector of length n is only self-orthogonal if k divides n.

We note that for codes over $\mathbf{Z}_{2k}$ the constant vector $(k, k, \ldots, k)$ is always in a self-dual code, see [3]. However, there are self-dual codes over $\mathbf{Z}_k$ with k odd that contain no constant vectors, for example, $\langle (1, 2) \rangle$ over $\mathbf{Z}_5$ or $\langle (1, 8) \rangle$ over $\mathbf{Z}_{65}$. The fact that $(k, k, \ldots, k) \in C$ for self-dual code over $\mathbf{Z}_{2k}$ limits the size of the index of C_0 in C, since at best it can be k and not $2k$.

Let $C_0 = \{v \mid v \in V,\ [v, s] = 0\}$ with C_0 of index r in C. We note that

$$[v, s] = 0 \iff \sum_{i=1}^{n} \gamma v_i = \gamma \sum_{i=1}^{n} v_i = 0. \tag{10}$$

The values $[s, v]$ takes on for $v \in C$ are the elements of the subgroup G of $\mathbf{Z}_k$ with $|G| = r$.

Let $cwe_C(x_0, x_1, \ldots, x_{k-1}) = \sum A_{a_0,a_1,\ldots,a_{k-1}} x_0^{a_0} x_1^{a_1} \cdots x_{k-1}^{a_{k-1}}$ be the complete weight enumerator for the code C, where $A_{a_0,a_1,\ldots,a_{k-1}}$ denotes the number of vectors in C with a_i coordinates that are an i, for $i = 0, \ldots, k-1$. Note that if a vector v is represented by the monomial $x_0^{a_0} x_1^{a_1} \cdots x_{k-1}^{a_{k-1}}$ then $\sum v_i = \sum a_i i$ and $[v, s] = \sum_{i=1}^{n} \gamma a_i i$. Let ξ_r be a complex r-th root of unity. We are now in a position to determine the weight enumerator of the subcode C_0.

Lemma 3.1 *Let C be a self-dual code of length n over $\mathbf{Z}_k$ with $s = (\gamma, \gamma, \ldots, \gamma)$ with C_0 the subcode of C orthogonal to s then*

$$cwe_{C_0}(x_0, x_1, \ldots, x_{k-1}) = \frac{1}{r} \sum_{j=0}^{r-1} cwe_C((\xi_r^j)^0 x_0, (\xi_r^j)^1 x_1, \ldots, (\xi_r^j)^{k-1} x_{k-1}) \tag{11}$$

Proof. A monomial representing a vector v which is orthogonal to s will have a coefficient of r in the summation, and a vector which is not orthogonal will have $1 + \xi_r + \xi_r^2 + \cdots + \xi_r^{r-1} = 0$ for a coefficient. □

If $P(x_0, x_1, \ldots, x_{k-1})$ is a polynomial, then let $T \cdot P(x)$ be the action of the MacWilliams transform on the polynomial (without the constant).

Theorem 3.2 *Let C be a self-dual code as described in Lemma* 3.1. *Then*

$$cwe_S = \frac{1}{k^{\frac{n}{2}}} \sum_{j=1}^{r-1} T \cdot cwe_C((\xi_r^j)^0 x_0, (\xi_r^j)^1 x_1, \ldots, (\xi_r^j)^{k-1} x_{k-1}) \tag{12}$$

Proof. We compute

$$cwe_{C_0^\perp}(x_0, x_1, \ldots, x_{k-1}) = \frac{1}{|C_0|} T \cdot \frac{1}{r} \sum_{j=0}^{r-1} cwe_C((\xi_r^j)^0 x_0, (\xi_r^j)^1 x_1, \ldots, (\xi_r^j)^{k-1} x_{k-1}) \tag{13}$$

Then the first summand becomes

$$\frac{1}{|C|} T \cdot cwe_C(x_0, x_1, \ldots, x_{k-1}) = cwe_C(x_0, x_1, \ldots, x_{k-1}),$$

and

$$cwe_S(x_0, x_1, \ldots, x_{k-1}) = cwe_{C_0^\perp}(x_0, x_1, \ldots, x_{k-1}) - cwe_C(x_0, x_1, \ldots, x_{k-1}).$$

□

It is clear that the symmetric weight enumerator can be computed similarly, as follows.

Corollary 3.3 *Let C be a self-dual code as described in Lemma* 11. *Then*

$$swe_{C_0}(x_0, x_1, \ldots, x_\ell) = \frac{1}{r}\sum_{j=0}^{r-1} cwe_C((\xi_r^j)^0 x_0, (\xi_r^j)^1 x_1, \ldots, (\xi_r^j)^{k-1} x_\ell) \tag{14}$$

and

$$swe_S = \frac{1}{k^{\frac{n}{2}}}\sum_{j=1}^{r-1} T' \cdot swe_C((\xi_r^j)^0 x_0, (\xi_r^j)^1 x_1, \ldots, (\xi_r^j)^\ell x_\ell) \tag{15}$$

where T' is the action of the MacWilliams relation for the symmetric weight enumerator.

4. Shadows for $\mathbf{F_2} + u\mathbf{F_2}$

In [5], a shadow is defined for codes over $\mathbf{F}_2 + u\mathbf{F}_2$ using the Lee weight. This is a natural definition since the shadow defined in this manner corresponds via the gray map to the standard shadow of the formed binary self-dual code. Specifically from [5], we have that if C is Type I then $\phi(C_j) = \phi(C)_j$ for $j = 0, 1, 2, 3$, that is,

$$\begin{array}{ccc} C & \xrightarrow[\phi]{} & \phi(C) \\ \text{coset}\downarrow & & \downarrow\text{coset} \\ C_j & \xrightarrow[\phi]{} & \phi(C_j) = \phi(C)_j \end{array}$$

If C is a Type I code of length n then $\phi(S)$ is the shadow of $\phi(C)$.

Moreover, it is an interesting weight with respect to the formed Complex lattice. That is with every code C over $\mathbf{F}_2 + u\mathbf{F}_2$ the lattice

$$A(C) = L(C)/\sqrt{2}$$

with

$$L(C) = \{x \in \mathbf{Z}[i]^n \mid x \pmod 2 \in C\}$$

is formed. Moreover, if C is a Type II code over $\mathbf{F}_2 + u\mathbf{F}_2$ then $A(C)$ is even unimodular, and unimodular if C is Type I.

It is natural to ask whether a shadow can be formed based on Lee weight for self-dual codes over $\mathbf{Z}_4$. Consider the following two vectors $v = (221111)$ and $w = (313100)$. The vector v has Lee weight $8 \equiv 0 \pmod 4$ and the vector w has Lee weight $4 \equiv 0 \pmod 4$. Moreover $[v, v] = [w, w] = [v, w] = 0$. Now $v + w = (130211)$ has Lee weight $6 \not\equiv 0 \pmod 4$. Hence the sum of two vectors with Lee weight $0 \pmod 4$ does not necessarily have Lee weight congruent to $0 \pmod 4$, so no such shadow is possible, given the usual construction. This is not surprising because the corresponding gray map is not linear.

Unlike the case for $\mathbf{Z}_4$, we can define an additional shadow for codes over $\mathbf{F}_2+u\mathbf{F}_2$, namely the Euclidean shadow. The Euclidean weight of every codeword in a self-dual code is even. We define an **E4 code** C as a self-dual code C with the property that the Euclidean weight of every codeword in C is divisible by four. For example, the code $\{(0), (u)\}$ is the smallest E4 code. Notice that $\{(0), (u)\}$ is not a Type II code in the usual sense. This implies that there is an E4 code for any length. Moreover we define an **E8 code** C as a self-dual code C with the property that the Euclidean weight of every codeword in C is divisible by eight. For example, K_{8m} is a E8 code, where K_{8m} is the $\mathbf{F}_2 + u\mathbf{F}_2$ analog of the Klemm code of length $8m$ defined in [12]. A self-dual code with the property that the Euclidean weight is not divisible by 4 is called **E2**.

As before C_0 is the subcode of vectors whose Euclidean weight is $0 \pmod 4$. The code C_0 is of index 2 in C. Let the symmetric weight enumerator be defined by $swe_C(a, b, c) = \sum_{c \in C} a^{n_c(0)} a^{n_c(1,1+u)} a^{n_c(u)}$, where $a^{n_c(i)}$ is the number of coordinates in c that are i.

Theorem 4.1 *If C is an* E2 *code, then the swe of C_0 is*

$$swe_{C_0}(a, b, c) = \frac{1}{2}(swe_C(a, b, c) + swe_C(a, ib, c)).$$

The swe of S is related to the swe of C by the relation

$$swe_S(a, b, c) = swe_C(b + (a + c)/2, (a - c)i/2, (a + c)/2 - b)$$

If the swe of an E2 *code* C *can be expressed as*

$$\sum_{j,k} \alpha_{jk}(a+c)^{n-2j-4k}(ac-b^2)^j(b^2(a-c)^2)^k, \tag{16}$$

then the swe of its shadow is

$$\sum_{j,k} \alpha_{jk}(-1)^k 2^{-j}(a+c)^{n-2j-4k}(a^2+c^2-2b^2)^j((a-c)^2b^2)^k. \tag{17}$$

Note that this shadow can be used to eliminate a putative code over $\mathbf{F}_2+u\mathbf{F}_2$. More to the point given a putative weight enumerator for a code over $\mathbf{F}_2+\mathbf{F}_2$ both the Euclidean and Lee shadows should be investigated to determine if there is a possible inconsistency.

We see from Equation 17 that any vector in the shadow is self-orthogonal since it has $n_{1,1+u} \equiv 0 \pmod 2$. Hence $\sigma = [s,s] = 0$. Also we have $[s,ut] = u[s,t] = 0$ since ut has only u for non-zero coordinates and is therefore in C_0. Moreover, $[s,t] \neq 0$ by construction, so $\tau = [s,t] = u$.

Thus we have the following orthogonality relations given in Table 3.

Table 3. Orthogonality Relations for the Euclidean Shadow for $\mathbf{F}_2+u\mathbf{F}_2$

	C_0	C_1	C_2	C_3
C_0	0	0	0	0
C_1	0	0	u	u
C_2	0	u	0	u
C_3	0	u	u	0

In contrast the Lee weight shadow is computed (see [5]) by the following. If C is a Type I code, then the *swe* of C_0 is

$$swe_{C_0}(a,b,c) = \frac{1}{2}(swe_C(a,b,c) + swe_C(a,ib,-c)).$$

The *swe* of S is related to the *swe* of C by the relation

$$swe_S(a,b,c) = swe_C(b+(a+c)/2, i(a-c)/2, b-(a+c)/2)$$

5. Rings of order 4

We shall give a concrete example of constant vector shadows over rings of order 4. Let $\mathbf{j}$ denote the all one vector.

Case 1: $R = \mathbf{Z}_4$

We note that $[v, v] = 0$ implies that $[v, 2\mathbf{j}] = 0$, so $2\mathbf{j} \in C$. (This is Proposition 4.1 in [7], i.e. all self-dual codes over $\mathbf{Z}_4$ contain $2\mathbf{j}$). Hence $\mathbf{j} + \mathbf{j} \in C$ and thus C is index 2 in $C_0^{\perp}$ giving us the desired situation.

The weight enumerator of C_0 is easily computed, i.e.

$$cwe_{C_0}(x_0, x_1, x_2, x_3) = \frac{1}{2}(cwe_C(x_0, ix_1, -x_2, -ix_3) + cwe_C(x_0, x_1, x_2, x_3)) \tag{18}$$

Hence we can compute the weight enumerator of the shadow simply by noting that $S = C + \mathbf{j}$, i.e.

$$cwe_S(x_0, x_1, x_2, x_3) = cwe_C(x_1, x_2, x_3, x_0) \tag{19}$$

Notice also that 11111113 has Euclidean weight 8 but is not perpendicular to $\mathbf{j}$ so it is not the same subcode as those vectors that have Euclidean weight congruent to 0 (mod 8).

We have that $2t \in C_0$ and $[t, \mathbf{j}] \neq 0$ so $2[t, \mathbf{j}] = 0$ and then $[t, \mathbf{j}] = 2$. Also we have that $[\mathbf{j}, \mathbf{j}] = n \pmod 4$ which gives the orthogonality relations for this case.

Now $C_1 + C_1 = (C_0 + \mathbf{j}) + (C_0 + \mathbf{j}) = (C_0 + 2\mathbf{j})$. If $n \equiv 1 \pmod 2$ then $2n \equiv 2 \pmod 4$ then $C_1 + C_1 = C_2$ and we have that the glue group, $C_0^{\perp}/C_0$, is isomorphic to the cyclic group of order 4. If $n \equiv 2 \pmod 2$ then $2n \equiv 0 \pmod 4$ and $C_1 + C_1 = C_0$ and the glue group is the Klein-4 group.

Since $[\mathbf{j}, \mathbf{j}] = n \pmod 4$ we have that $\sigma = n \pmod 4$. Notice that $2t \in C_0$, hence $[2t, \mathbf{j}] = 2[t, \mathbf{j}] = 0$ and $[t, \mathbf{j}] \neq 0$ so $\tau = [t, \mathbf{j}] = 2$, giving the orthogonality relations.

Theorem 5.1 *Let C be a self-dual code over $\mathbf{Z}_4$ and let s be the all one vector with $C_0 = \{c \in C \mid [c, s] = 0\}$ then the glue group $C_0^{\perp}/C_0$ is isomorphic to the cyclic group of order 4 if $n \equiv 1 \pmod 2$ and isomorphic to the Klein-4 group if $n \equiv 0 \pmod 2$ and the orthogonality relations are given by Table 4. The shadow $S = C_1 \cup C_3$ has weight enumerator $cwe_S(x_0, x_1, x_2, x_3) = cwe_C(x_1, x_2, x_3, x_0)$.*

Table 4. Orthogonality Relations for the all one shadow for $\mathbf{Z}_4$ Codes (read (mod 4))

	C_0	C_1	C_2	C_3
C_0	0	0	0	0
C_1	0	n	2	$n+2$
C_2	0	2	0	2
C_3	0	$n+2$	2	n

Case 2: $R = \mathbf{F}_2 + u\mathbf{F}_2$

Let

$$cwe_C(x_0, x_1, x_u, x_{1+u}) = \sum A_{(a,b,c,d)} x_0^{n_0(c)} x_1^{n_1(c)} x_u^{n_u(c)} x_{1+u}^{n_{1+u}(c)}. \tag{20}$$

The vector v with $wt(v) = x_0^{n_0(c)} x_1^{n_1(c)} x_u^{n_u(c)} x_{1+u}^{n_{1+u}(c)}$ is in C_0 if and only if $n_1(c) \equiv n_u(c) \equiv n_{1+u}(c)$. Hence C_0 can be computed. As in the previous case it is easy to compute the weight enumerator of the shadow, i.e. $cwe_S(x_0, x_1, x_u, x_{1+u}) = cwe_C(x_1, x_0, x_{1+u}, x_u)$.

Since $[\mathbf{j}, \mathbf{j}] = n \pmod 2$ we have that $\beta = n \pmod 2$. Notice that $[t, t] = 0$ implies that $n_1(t) + n_{1+u}(t) \equiv 0 \pmod 2$. This implies ut has $n_u(ut) \equiv 0 \pmod 2$ and $n_1(ut) = n_{1+u}(ut) = 0$. Then we have that $ut \in C_0$. Since $ut \in C_0$, we have $[ut, \mathbf{j}] = u[t, \mathbf{j}] = 0$ and $[t, \mathbf{j}] \neq 0$ so $\alpha = [t, \mathbf{j}] = u$, giving the orthogonality relations.

The glue group is always the Klein 4 group since the sum a vector with itself is always the 0 vector.

Theorem 5.2 *Let C be a self-dual code over $\mathbf{F}_2 + u\mathbf{F}_2$ and let s be the all one vector with $C_0 = \{c \in C \mid [c, s] = 0\}$ then the glue group $C_0^{\perp}/C_0$ is isomorphic to the Klein-4 group and the orthogonality relations are given by Table 5. The shadow $S = C_1 \cup C_3$ has weight enumerator $cwe_S(x_0, x_1, x_u, x_{1+u}) = cwe_C(x_1, x_0, x_{1+u}, x_u)$.*

Example 1 Let C be the following self-dual code:

$$C = \{(0,0,0), (0,1,1), (0,u,u), (0,1+u,1+u), (u,0,0), (u,1,1), (u,u,u), (u,1+u,1+u)\}$$

Table 5. Orthogonality Relations for the all one shadow for $\mathbf{F}_2 + u\mathbf{F}_2$ Codes (read (mod 2))

	C_0	C_1	C_2	C_3
C_0	0	0	0	0
C_1	0	n	u	$n+u$
C_2	0	u	0	u
C_3	0	$n+u$	u	n

If C_0 is the subcode formed by those vectors with Lee weight congruent to 0 (mod 4) then

$$C_0 = \{(0,0,0),(0,u,u),(u,1,1),(u,1+u,1+u)\} \tag{21}$$

If C_0 is the subcode formed by those vectors with Euclidean weight congruent to 0 (mod 4) then

$$C_0 = \{(0,0,0),(0,u,u),(u,0,0),(u,u,u)\} \tag{22}$$

If C_0 consists of those vectors orthogonal to $\mathbf{j}$ then

$$C_0 = \{(0,0,0),(0,1,1),(0,u,u),(0,1+u,1+u)\} \tag{23}$$

Hence C_0 and the shadows are distinct for this code. Note that each of these subcodes is mapped linearly to a subcode of the formed binary self-dual code. Each can be used to form a shadow in the manner given above for that binary code. Moreover, the formed binary shadows are the images of the shadows over $\mathbf{F}_2 + u\mathbf{F}_2$.

6. Chinese Remainder Theorem

Let C be a self-dual code over $\mathbf{Z}_k$ where $k = \prod_{i=1}^{r} p_i^{q_i}$ where $\gcd(p_i, p_j) = 1$ if $i \neq j$. If C is read mod $p_i^{q_i}$ then C is a self-dual code over $\mathbf{Z}_{p_i^{q_i}}$. Moreover, if E_i is a self-dual code over $\mathbf{Z}_{p_i^{q_i}}$ for $i = 1, \ldots, r$ then $CRT(E_1, E_2, \ldots, E_r)$ is the unique self-dual code such that the image of C (mod $p_i^{q_i}$) $= E_i$, see [8] for a complete description.

Let $C = CRT(E_1, E_2, \ldots, E_r)$ and let D_i be a subcode of E_i of index g. Then $C_0 = CRT(E_1, E_2, \ldots, D_i, \ldots, E_r)$ is a subcode of C of index g and $C_0^{\perp} = CRT(E_1, E_2, \ldots, D_i^{\perp}, \ldots, E_r)$. Then the shadow is defined by $C_0^{\perp} - C$.

Proposition 6.1 *Let $C = CRT(E_1, E_2, \ldots, E_r)$ be a self-dual code over $\mathbf{Z}_{2k}$, with $p_1 = 2$ and let D_1 be the subcode of whose Euclidean weights are* 0 (mod $2(2^{q_1})$) *then C_0 is the subcode of vectors whose Euclidean weight are* 0 (mod $4k$) *and the shadow is the usual shadow.*

Proof. In the proof of Theorem 2.3 in [8] it is shown that a vector over $\mathbf{Z}_{2^{q_1}r}$ where r is odd is doubly-even if and only if its image (mod 2^{q_1}) is doubly even. The result follows. □

Proposition 6.2 *Let $C = CRT(E_1, E_2, \ldots, E_r)$ be a self-dual code over $\mathbf{Z}_k$ and let D_i be the subcode orthogonal to the constant vector v, then C_0 is the subcode orthogonal to a constant vector.*

Proof. If v is a constant vector, then $C_0^{\perp} = \langle C, s \rangle$ where s (mod $p_i^{q^i}$) $= v$. We can take $s = CRT(\mathbf{0}, \mathbf{0}, \ldots, v, \ldots, \mathbf{0})$ and then C_0 is described by Lemma 3.1 and Theorem 3.2. □

Acknowledgment The author is grateful to Masaaki Harada for helpful discussions.

References

[1] Bachoc C., *Application of coding theory to the construction of modular lattices*. J. Combin. Theory Ser. A **78** (1997), 92–119.

[2] Bannai E., Dougherty S.T., Harada M. and Oura M., *Type II codes, even unimodular lattices and invariant rings*. IEEE-IT **45**, No.4 (1999), 1194–1205.

[3] Bonnecaze A., Choie Y., Dougherty S.T. and Solé P., *Splitting the shadow*. Submitted.

[4] Conway J.H. and Sloane N.J.A., *A new upper bound on the minimum distance of self-dual codes*. IEEE Trans. Inform. Theory **36** (1990), 1319–1333.

[5] Dougherty S.T., Gaborit P., Harada M. and Solé P., *Type II codes over $F_2 + uF_2$*. IEEE-IT **45**, No.1 (1999), 32–45.

[6] Dougherty S.T., Gaborit P., Harada M., Munemasa A. and Solé P., *Type IV self-dual codes over rings*. IEEE-IT, **45**, No.7 (1999), 2345–2360.

[7] Dougherty S.T., Harada M. and Solé P., *Shadow codes for $\mathbf{Z}_4$*. To appear in Finite Fields and their Applications.

[8] Dougherty S.T., Harada M. and Solé P., *Self-dual codes over rings and the Chinese remainder theorem*. Hokkaido Math. J. **28** (1999), 253–283.

[9] Dougherty S.T., Harada M. and Solé P., *Shadow lattices and shadow codes*. Discrete Math. **219** (2000), 49–64.

[10] Dougherty S.T. and Solé P., *Shadows of codes and lattices*. Submitted to the Third Asian Mathematical Conference (AMC 2000).

[11] Gaborit P., Harada M. and Solé P., *Self-dual codes over* $\mathbf{Z}_4$ *and unimodular lattices, a survey*. The Proceedings of ICAC- 1997, Hong Kong, Springer Verlag (1999), 255–275.

[12] Klemm M., *Selbstduale Codes über dem ring der ganzen Zahlen modulo* 4. Arch. Math. **53** (1989), 201–207.

[13] Rains E. and Sloane N.J.A., *Self-dual codes, in the Handbook of Coding Theory*. V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 1998, 177–294.

Department of Mathematics
University of Scranton
Scranton, PA 18510
U. S. A.
E-mail: doughertys1@uofs.edu