LABORATOIRE

INFORMATIQUE, SIGNAUX ET SYSTÈMES
DE SOPHIA ANTIPOLIS
UMR 6070

CUBIC SELF-DUAL BINARY CODES (VERSION 1.3)

A. Bonnecaze, S.T. Dougherty, Patrick Solé

Projet RECIF

Rapport de recherche
I3S/RR–2002-42–FR

Septembre 2002

LABORATOIRE I3S: Les Algorithmes / Euclide B – 2000 route des Lucioles – B.P. 121 –
06903 Sophia-Antipolis Cedex, France – Tél. (33) 492 942 701 – Télécopie : (33) 492 942 898
`http://www.i3s.unice.fr/I3S/FR/`

Self-Dual Binary Codes via the Cubing Construction (Version 1.3)

A. Bonnecaze
INRIA, Action GALAAD,
2004, route des Lucioles - BP 93
06902 Sophia Antipolis Cedex -
France
`Alexis.Bonnecaze@sophia.inria.fr`,
Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510
USA
`doughertys1@uofs.edu`

and
Patrick Solé
CNRS, I3S
ESSI, BP 145
Route des Colles
06 903 Sophia Antipolis
France
`ps@essi.fr`

August 13, 2001

Abstract

We study binary ℓ-quasi cyclic self-dual codes of length 3ℓ as codes of length ℓ over the ring $\mathbf{F}_2 \times \mathbf{F}_4$.

Key Words: Quasi-Cyclic, Self-Dual, Codes over Rings.

1 Introduction

A code is said to be $\ell-$ quasi-cyclic iff it is held invariant by a shift of ℓ coordinate places. It was shown in [7] that all binary ℓ-quasi cyclic codes of length 3ℓ can be obtained by a generalized cubing construction from a binary code and a quaternary code both of length ℓ. From now on we will qualify such codes of **"cubic."**

In this article we view cubic codes as codes of length ℓ over the ring $\mathbf{F}_2 \times \mathbf{F}_4$. We study self-dual codes over that alphabet and introduce the classical tools, Type II codes, shadow codes, and a symmetrized weight enumerator. We give two infinite families of such codes related to Quadratic Residue Codes. As an application we classify all such codes of short length and give examples in higher length.

2 Notation and Definitions

We want to study codes formed by a cubing type construction. Binary codes of length 3ℓ are formed by this construction from a binary code of length ℓ and a quaternary code of length ℓ.

More specifically, if A, B and X are binary vectors of length ℓ then let

$$\begin{aligned} U &= X + A \\ V &= X + B \\ W &= X + A + B \end{aligned}$$

and

$$\Phi(X, A + \omega B) := (U|V|W)$$

defines a Gray map from $\mathbf{F}_2^\ell \times \mathbf{F}_4^\ell \to \mathbf{F}_2^{3\ell}$.

Alternatively we think of this as a vector of length l over $\mathbf{F}_2 \times \mathbf{F}_4$ with the j-th coordinate as $(X_j, A_j + \omega B_j)$.

For a code C over $\mathbf{F}_2 \times \mathbf{F}_4$ we define the symmetric weight enumerator as

$$(1) \qquad swe_C(a,b,c,d) = \sum_{c \in C} w_H(c) = \sum_{c \in C} w_H(u|v|w) = \sum_{c \in C} a^{n_0(c)} b^{n_1(c)} c^{n_2(c)} d^{n_3(c)}$$

where n_i is the number of triples (u_j, v_j, w_j) with Hamming weight $i = 0, 1, 2, 3$ for $0 \leq j \leq \ell$.

It can be shown that the Gray image $\Phi(C_2, C_4)$ where C_2 is a binary code and C_4 is a quaternary code is self-dual (resp. Type II) if and only if C_2 is self-dual (resp. Type II) and C_4 is Hermitian self-dual, see [7]. A self-dual code is said to be Type II if its Gray image is Type II and Type I otherwise.

Note, however, that if C_2 and C_2' are isomorphic binary codes and C_4 and C_4' are isomorphic quaternary codes, this does not necessarily mean that $\Phi(C_2, C_4)$ and $\Phi(C_2', C_4')$ are isomorphic.

For any code the Hamming weight of a vector $wt(v)$ is the number of non-zero coordinates of the code. We define the Hamming weight enumerator by

$$W_C(x,y) = \sum_{c \in C} x^{n-wt(v)} y^{wt(v)}. \tag{2}$$

Often the x is replaced by 1.

For two codes v, w in $(\mathbf{F}_2 \times \mathbf{F}_4)^\ell$ we define the innerproduct by

$$[v, w] = \sum \psi(v_i, w_i) \tag{3}$$

where

$$\psi(v_i, w_i) = xx' + Tr((a + \omega b)(a' + \overline{\omega} b')) \tag{4}$$

with $v_i = (x, (a + \omega b))$ and with $v_i' = (x', (a' + \omega b'))$ and Tr denotes the trace.

Lemma 2.1 *The inner product given in equation 3 is equivalent to the innerproduct of the Gray image.*

Proof. The binary inner product of the Gray image is:

$$[X_i + A_i, X_i + B_i, X_i + A_i + B_i, X_j' + A_j', X_j' + B_j', X_j' + A_j' + B_j'] = X_i X_j + A_i B_j' + B_i A_i'$$

and the inner product in equation 3

$$\begin{aligned} \psi & \quad (X_i + A_i, X_i + B_i, X_i + A_i + B_i, X_j' + A_j', X_j' + B_j', X_j' + A_j' + B_j') \\ = & \quad X_i X_j' + Tr(A_i A_j' + Tr(A_i A_j' + B_i B_j' + \omega(A_i B_j' + B_i A_i')) \\ = & \quad X_i X_j + A_i B_j' + B_i A_i' \end{aligned}$$

giving the result.

3 First Properties

Proposition 3.1 *Let* $C = \Phi(C_2, C_4)$ *then*

$$W_{C_4}(x,y) = swe_C(x, 0, y, 0) = \frac{1}{|C_2|} swe_C(x, y, y, x) \tag{5}$$

and

$$W_{C_2}(x,y) = swe_C(x, 0, 0, y) = \frac{1}{|C_4|} swe_C(x, y, x, y) \tag{6}$$

Proof. Note that $2w_H(A+wB) = w_H(A) + w_H(B) + w_H(A+B)$. Counting in two ways, we find that $w_H(U+V) + w_H(U+W) + w_H(V+W) = 2n_1 + 2n_2$. Moreover, by definition of U, V and W we have

$$\begin{cases} w_H(A) & = & w_H(U+V) \\ w_H(B) & = & w_H(V+W) \\ w_H(A+B) & = & w_H(U+V) \end{cases}$$

and the evaluation of W_{C_4} follows.
To evaluate W_{C_2} observe that $w_H(U+V+W) = n_1 + n_3$.

Lemma 3.2 *If $C = \Phi(C_2, C_4)$ then $W_C(x,y) = swe_{(C_2,C_4)}(x^3, x^2y, xy^2, y^3)$.*

Theorem 3.3 *If $C = (C_2, C_4)$ with C_2 and C_4 linear then*

$$swe_{C^\perp}(a,b,c,d) = \frac{1}{|C|} T \cdot swe_C(a,b,c,d) \tag{7}$$

where

$$T = \begin{pmatrix} 1 & 3 & 3 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -3 & 3 & -1 \end{pmatrix}$$

Proof. Since the ring $\mathbf{F}_2 \times \mathbf{F}_4$ is quasi Frobenius with admissible character $\phi(z) := (-1)^{[\mathbf{1},\mathbf{z}]}$ there is a linear transformation T satisfying the condition of the theorem. Since the Gray image of a self-dual code is self-dual, the explicit expansion for T follows by Lemma 3.2.

4 Constructions of cubic codes

4.1 Quadratic Residue Codes

Let $QR(p)$ denote the quadratic residue code of length $p+1$.

Theorem 4.1 *If p is a prime $\equiv 23 \pmod{24}$ then $QR(p)$ is a cubic self-dual Type II code of length $p+1$.*

Proof. It is well-known [**?**, Chapter 16, Lemma 14] that $PSL(2,p)$ contains a permutation σ, say, consisting of two disjoint cycles of length $\frac{p+1}{2}$. Let β be σ raised to the power $\frac{p+1}{6}$. We see that β is fixed-point-free of order 3.

The Golay code is the case $p = 23$ of the preceding Theorem. This is equivalent to Turyn's construction. The case $p = 47$ is described in [6]. By subtracted quadratic residue code (denoted here by $SQR(p)$) we shall mean the self-dual code obtained by subtraction at the places 0 and ∞. More formally,

$$SQR(p) := \{s \in \mathbf{F}_2^{p-1} \,|(0,s,0) \in QR(p) \ \vee (1,s,1) \in QR(p)\}.$$

Theorem 4.2 *If p is a prime $\equiv 7 \pmod{24}$ then $SQR(p)$ is a cubic self-dual Type I code of length $p-1$.*

Proof. It is a well-known property of subtraction that $SQR(p)$ is self-dual. Since $p-1$ is not a multiple of 8 we see that $SQR(p)$ is a Type I code. We proceed to show that it is left wholly invariant by a fixed-point-free permutation of order 3. Since 3 divides $p-1$ we know that $GF(p)^\times$ contains a cubic root α, say, of unity. Now the matrix $A := (\alpha, \ \alpha^{-1})$ belongs to $SL(2,p)$, and satisfies $A^3 = I$. Because A is diagonal, its image in $PSL(2,p)$ fixes 0 and ∞.

It can be shown [8] that the automorphism group of $SQR(p)$ is the dihedral group D_{p-1}. By Dirichlet Theorem on primes in arithmetic progression there are infinitely many primes satisfying the hypothesis of the preceding theorem. The first few relevant values of p are $p = 31,\ 79,\ 103, \ldots$ For $p = 31$ the Type I code $SQR(31)$ is extremal of parameters $[30,15,6]$.

4.2 Reed-Muller Codes

Let $RM(r,m)$ denote the Reed-Muller code of order r and length 2^m. As is well-known it is self-dual for m odd and $r = \frac{m-1}{2}$. Let $SRM(m)$ denote the self-dual code obtained by subtraction at $x = \mathbf{0}$ and $x = \mathbf{1}$ (the all-one vector) from the preceding code.

Theorem 4.3 *If $m \geq 3$ is odd then $SQR(m)$ is a cubic self-dual Type I code of length $2^m - 2$.*

Proof. First, we determine the automorphism group of $SRM(m)$. Recall that the automorphism group of $RM(r,m)$ is $GL(m,2)$ acting on $\mathbf{F}_2^n$. Every $A \in GL(m,2)$ has fixed point $x = \mathbf{0}$. If, furthermore, $\mathbf{1}$ is a fixed point of A, that means, in terms of linear algebra, that it is an eigenvector of A for the eigenvalue 1. Let V denote an orthogonal complement of the line spanned by $\mathbf{1}$ in $\mathbf{F}_2^n$. Then V is stable by action of A, and any A satisfying $A\mathbf{1} = \mathbf{1}$ is uniquely determined by its restriction to A. We thus see that the stabilizer of $\{\mathbf{0}, \mathbf{1}\}$ is isomorphic to $GL(m-1,2)$.

Next, we show that $Aut(SRM(m)$ contains a fixed point free element of order 3. In other words we need an element of $GL(m-1,2)$ which does not fix any point of V but $\mathbf{0}$. For odd m, it is readily checked that $2^m - 1$ is a multiple of 3. Therefore $GF(2^{m-1})^\times$ contains an element α of order 3. Identifying $\mathbf{F}_2^{m-1}$ and $GF(2^{m-1})$, we see that the matrix of $x \mapsto \alpha x$ satisfies our requirements.

For $m = 5$ the Type I code $SRM(5)$ is extremal of parameters $[30, 15, 6]$.

5 Shadows

For a binary code C the shadow is well defined (see [4]). We extend this definition to codes over $\mathbf{F}_2 \times \mathbf{F}_4$. Let C be a Type I code over $\mathbf{F}_2 \times \mathbf{F}_4$. Let D_0 be the subcode consisting of those vectors whose under Φ has weight congruent to $0 \pmod 4$. This subcode is of index 2 in C. Let $D_2 = C - D_0$ and $D_0^\perp = C \cup S$, with the shadow $S = D_1 \cup D_3$. The glue group for $D_0^\perp / D_0$ is the Klein-4 group for all ℓ.

Theorem 5.1 *If C is a self-dual code over $\mathbf{F}_2 \times \mathbf{F}_4$ then*

$$swe_{D_0}(a,b,c,d) = \frac{1}{2}(swe_C(a,b,c,d) + swe_C(a,ib,-c,-id)) \tag{8}$$

and

$$swe_S(a,b,c,d) = M \cdot swe_C(a,ib,-c,-id). \tag{9}$$

Proof. The weight enumerator $swe_C(a,ib,-c,-id)$ negates only those vectors whose Gray image has singly even weight. The standard computation gives the rest.

5.1 Shadow Sum

Let C be a self-dual code of length ℓ over $\mathbf{F}_2 \times \mathbf{F}_4$ and let D_i be defined as above. Note that $\Phi(D_i) = \Phi(C)_i$ for $i = 0, 2$ and up to labeling for $i = 1, 3$. We note that the Gray image of the shadow is the shadow of the Gray image. Then since the inner product defined on the ambient space is equivalent to the inner product defined by the Gray images by Lemma 2.1 we obtain the orthogonality relations given in Table 1 and Table 2.

Table 1: Orthogonality Relations for $\ell \equiv 2 \pmod 4$

	C_0	C_1	C_2	C_3
C_0	$\perp$	$\perp$	$\perp$	$\perp$
C_1	$\perp$	$\not\perp$	$\not\perp$	$\perp$
C_2	$\perp$	$\not\perp$	$\perp$	$\not\perp$
C_3	$\perp$	$\perp$	$\not\perp$	$\not\perp$

Table 2: Orthogonality Relations for $\ell \equiv 0 \pmod 4$

	C_0	C_1	C_2	C_3
C_0	$\perp$	$\perp$	$\perp$	$\perp$
C_1	$\perp$	$\perp$	$\not\perp$	$\not\perp$
C_2	$\perp$	$\not\perp$	$\perp$	$\not\perp$
C_3	$\perp$	$\not\perp$	$\not\perp$	$\perp$

We shall now describe the shadow sum construction for codes over $\mathbf{F}_2 \times \mathbf{F}_4$ using the notation in [5].

Let C and C' be self-dual codes of length ℓ and ℓ' respectively. Define D_i and D'_i as above.

Let

$$E = (D_0, D'_0) \cup (D_1, D'_1) \cup (D_2, D'_2) \cup (D_3, D'_3) \tag{10}$$

and

$$F = (D_0, D'_0) \cup (D_1, D'_3) \cup (D_2, D'_2) \cup (D_3, D'_1) \tag{11}$$

where $(D_i, D'_j) = \{(v, w) \mid v \in D_i, w \in D'_j\}$. The codes E and F are called the shadow sum of C and C' depending on which case produces a self-dual code and is denoted by $C \oplus_s C'$.

Theorem 5.2 *Let C and C' be self-dual codes over $\mathbf{F}_2 \times \mathbf{F}_4$ of length ℓ and ℓ' respectively. If $\ell \equiv \ell' \equiv 0 \pmod 4$ then E is a self-dual code of length $\ell + \ell'$. If $\ell \equiv \ell' \equiv 2 \pmod 4$ then F is a self-dual code of length $\ell + \ell'$. Moreover E and F are Type II codes if and only if $\ell + \ell' \equiv 0 \pmod 8$.*

Proof. Linearity follows from the fact that the glue group is the Klein Group for both codes C and C'. The fact that they are self-orthogonal follows from Table 1 and Table 2. Self-duality follows by considering their cardinality, i.e.

$$|E| = |F| = 4|D_i||D'_j| = 4\frac{|C|}{2}\frac{|C'|}{2} = |C||C'| = 8^{\frac{\ell+\ell'}{2}}$$

as desired.

For Type II the weights in the shadow are $\frac{\ell}{2} \pmod 4$ and $\frac{\ell'}{2} \pmod 4$ respectively. So in (D_i, D'_j), $i = 1, 3$ the weights are $\frac{\ell+\ell'}{2} \pmod 4$. The weights in (D_0, D'_0) and (D_2, D'_2) are always $0 \pmod 4$.

Corollary 5.3 *If E and F are the shadow sum of C and C' as defined above then*

$$swe_E(a, b, c, d) = \sum_{i=0}^{3} swe_{D_i}(a, b, c, d) \cdot swe_{D'_i}(a, b, c, d) \tag{12}$$

$$\begin{aligned} swe_F(a,b,c,d) &= \sum_{i\in\{0,2\}} swe_{D_i}(a,b,c,d)\cdot swe_{D'_i}(a,b,c,d) \\ &+ \sum_{i\in\{1,3\}} swe_{D_i}(a,b,c,d)\cdot swe_{D_{-i'} \pmod 4}(a,b,c,d) \end{aligned}$$

Lemma 5.4 *If* $A, B \in \mathbf{F}_2^n$ *then* $2wt(A+\omega B) = wt(A)+wt(B)+wt(A+B)$. *In particular* $d(C_4) \geq \frac{d(C)}{2}$.

Proof. Observe that $wt(A+B) = wt(A \vee B)$. By inspection of the Karnaugh table for $A_i, B_i, A_i \vee B_i$, and $A_i + B_i$ for each coordinate i the result follows.

Lemma 5.5 *If* $x \in C_2$ *a Type II binary code and* $a+\omega b \in C_4$ *a quaternary self-dual code then* $wt(\Phi(x, a+\omega b)) \equiv wt(x) \pmod 4$.

Proof. Since $\Phi(C_2, C_4)$ is Type II we see that $wt(\Phi(X, A+\omega B)) \equiv wt(\Phi(X,0)) + wt(\Phi(0, A+\omega B)) \pmod 4$. Now $wt(\Phi(0, A+\omega B)) = 2wt(A+\omega B)$ by Lemma 5.4. Since C_4 is Type IV we see that $wt(A+\omega B)$ is even. Since $wt(\Phi(X,0)) = 3wt(X) \equiv wt(X) \pmod 4$ the result follows.

Theorem 5.6 *If* $C_2 \times C_4)$ *is a code* C *over* $\mathbf{F}_2 \times \mathbf{F}_4$ *then* $D_i = (C_2)_i \times C_4$ *where* $(C_2)_0$ *is the subcode of doubly-even vectors of the binary code* C_2 *and then* $(C_2)_i$ *are defined as usual.*

Proof. The fact that $D_0 = (C_2)_\times C_4$ follows from the previous Lemma and the rest from a straightforward calculation.

Theorem 5.7 *If* $C_2 \times C_4$ *is a code over* $\mathbf{F}_2 \times \mathbf{F}_4$ *and* $C'_2 \times C'_4$ *is a code over* $\mathbf{F}_2 \times \mathbf{F}_4$ *then*

$$C \oplus_s C' = (C_2 \oplus C'_2) \times (C_4 \oplus C'_4) \tag{13}$$

and

$$\Phi(C_2, C_4) \oplus_s \Phi(C'_2, C'_4) = \Phi(C_2 \oplus_s C'_2, C_4 \oplus C'_4). \tag{14}$$

Proof. Follows from Lemma 5.5. The following corollary will be used in constructing examples.

Corollary 5.8 *If* C *and* C' *are cubic binary codes so is* $C \oplus C'$.

6 Invariants

The *swe* of a Type II code is held invariant by the matrix

$$\Omega_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}$$

since the weights in the Gray image are congruent to $0 \pmod 4$, by

$$\Omega_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$$

since C_2 is Type II binary (see Proposition 3.1), and by

$$\Omega_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

since C_4 is a Type IV quaternary code (see Proposition 3.1), and by $M = \frac{1}{\sqrt{8}}T$ since it is self-dual.

Let $G_{II} = \langle \Omega_1, \Omega_2, \Omega_3, M \rangle$. A Magma computation gives that $|G_{II}| = 1152$ and the Molien Series is: $1 + 3\,t^8 + 9\,t^{16} + 26\,t^{24} + 52\,t^{32} + 91\,t^{40} + 155\,t^{48} + 237\,t^{56} + 341\,t^{64} + 484\,t^{72} + 654\,t^{80} + 855\,t^{88} + 1109\,t^{96} + \cdots$

The *swe* of a Type I code is held invariant by Ω_1^2 since the weights in the Gray image are congruent to $0 \pmod 2$, and by Ω_3 and M. Let $G_I = \langle \Omega_1^2, \Omega_3, M \rangle$. By a Magma computation we have that $|G_I| = 96$ and the Molien Series is: $1 + t^2 + 2\,t^4 + 3\,t^6 + 6\,t^8 + 8\,t^{10} + 13\,t^{12} + 16\,t^{14} + 24\,t^{16} + 32\,t^{18} + 42\,t^{20} + 50\,t^{22} + 68\,t^{24} + 82\,t^{26} + 100\,t^{28} + 118\,t^{30} + 145\,t^{32} + 168\,t^{34} + 200\,t^{36} + 227\,t^{38} + 266\,t^{40} + 305\,t^{42} + 349\,t^{44} + 388\,t^{46} + 447\,t^{48} + 499\,t^{50} + 558\,t^{52} + 617\,t^{54} + 692\,t^{56} + 760\,t^{58} + 843\,t^{60} + 918\,t^{62} + 1012\,t^{64} + 1106\,t^{66} + 1208\,t^{68} + 1302\,t^{70} + 1426\,t^{72} + 1540\,t^{74} + 1664\,t^{76} + 1788\,t^{78} + 1935\,t^{80} + 2072\,t^{82} + 2230\,t^{84} + 2377\,t^{86} + 2550\,t^{88} + 2723\,t^{90} + 2907\,t^{92} + 3080\,t^{94} + 3293\,t^{96} + 3493\,t^{98} + \cdots$

7 Examples

1. n=2

   Let i_2 denote the binary repetition code of length 2. The unique binary self-dual code of length 6 is obtained by $i_6 = \Phi(i_2, i_2 \otimes \mathbf{F}_4)$.

2. n=4

   The shadow sum of i_6 with itself yields a cubic code of length 12 with weight enumerator:
   $$1 + 15y^4 + 32y^6 + 15y^8 + y^{12}.$$

3. n=6

   The minimum Lee distance of a self-dual code of length 6 over $\mathbf{F}_2 \times \mathbf{F}_4$ is 4. It is a simple calculation to see from the invariants of degree 6 for G_I that its Gray image must be
   $$1 + 9y^4 + 75y^6 + 171y^8 + 171y^{10} + 75y^{12} + 9y^{14} + y^{18}$$

   It is shown in [4] that there are two possible weight enumerators for Type I codes over length 18 with minimum distance 4. The code $(d_{10}e_7f_1)^+$ has weight enumerator $1 + 17y^4 + \dots$ and hence cannot be 6-quasi cyclic. The code d_6^{3+} is $\Phi(C_2, C_4)$ where C_4 is the Hexacode with weight enumerator $1 + 45y^4 + 18y^6$ and $C_2 = I_2^3$ with weight enumerator $1 + 3y^2 + 3y^4 + y^6$. Notice that no information about the automorphism group of $(d_{10}e_7f_1)^+$ is needed to show that it cannot be 6-quasi cyclic.

4. n=8

   The highest minimum Lee distance of a self-dual code of length 8 over $\mathbf{F}_2 \times \mathbf{F}_4$ is 8. Hence its Gray image must be the Golay code with weight enumerator
   $$1 + 759\,y^8 + 2576\,y^{12} + 759\,y^{16} + y^{24}.$$

   Moreover, the binary code must have weight enumerator: $1 + 14\,y^4 + y^8$, that is it is the $[8, 4, 4]$ Hamming code.

5. n=10

   Using invariant theory, we can see that the minimum Lee distance of a self-dual code of length 10 over $\mathbf{F}_2 \times \mathbf{F}_4$ is at most 8. But since the highest minimal distance of a $[10, 5]$ binary self-dual code is 2 (see [4]), the best minimal distance we can reach is 6. It is attained for the inverse Gray image of $SQR(31)$.

6. n=12

   The minimum Lee distance of a self-dual code of length 12 over $\mathbf{F}_2 \times \mathbf{F}_4$ is at most 10. It is a simple calculation to see that its Gray image must be
   $$1 + 3366\,y^{10} + 6630\,y^{12} + 30600\,y^{14} + 58905\,y^{16} + 63140\,y^{18} +$$
   $$58905\,y^{20} + 30600\,y^{22} + 6630\,y^{24} + 3366\,y^{26} + y^{36}$$

References

[1] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, *IEEE Trans. Inform. Theory* **45** (1999), 1194–1205.

[2] R.A. Brualdi and V. Pless, Weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* **37** (1991), 1222–1225.

[3] J.H. Conway and N.J.A. Sloane, On the enumeration of lattices of determinant one, *J. Number Theory* **15** (1982), 83–94.

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

[5] S.T. Dougherty and P. Solé, Shadows of Codes and Lattices, submitted.

[6] W. Cary Huffman, Automorphisms of codes with applications to extremal doubly even codes of length 48, *IEEE Trans. Inform. Theory* **28** (1982), 511–521.

[7] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes I: Finite Fields, *IEEE Trans. Inform. Theory* **47** (2001), in press.

[8] L.R. Nochefranca, personal communication.