On harmonic weight enumerators of binary codes

Christine Bachoc

June 30, 2000

Abstract

We define some new polynomials associated to a linear binary code and a harmonic function of degree k. The case $k = 0$ is the usual weight enumerator of the code. When divided by $(xy)^k$, they satisfy a MacWilliams type equality. When applied to certain harmonic functions constructed from Hahn polynomials, they can compute some information on the intersection numbers of the code. As an application, we classify the extremal even formally self-dual codes of length 12.

keywords: codes, harmonic functions, weight enumerator, formally self-dual codes

1 Introduction

In the theory of lattices, some modular forms play a special role, the so-called theta series with spherical coefficients. They are generalizations of the theta series of the lattice which counts the number of vectors of given norm; they are a powerful tool for the study of the spherical codes supported by the vectors of an even unimodular lattice, as shown in [24], and also provide some knowledge on the values of the scalar product of the vectors of the lattice with a given vector of the Euclidean space (i.e. on the so-called Jacobi theta series of the lattice). For example, they have allowed B. Venkov to settle "a priori" the list of the possible root systems of an even unimodular 24-dimensional lattice [7, Chapter 18]. See [1] for a generalization of these methods to non-unimodular lattices.

Inspired by the analogy pointed out in [8], [9] between the theory of combinatorial and euclidean designs and their connection in both cases with harmonic spaces, we define here analogues of these for linear binary codes. More precisely, we associate to a binary code C and a harmonic function f

of degree k in the sense of [8], a polynomial $W_{C,f}(x,y)$, which, when divided by $(xy)^k$, behaves, up to a sign, like the usual weight enumerator $W_C(x,y)$ under the MacWilliams transform. In particular, when C is a doubly even self-dual code, we get a whole set of polynomials which are relative invariants under the usual group $\mathcal{G}_1$ of 2×2-matrices of order 192 generated by $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. In the case of an even formally self-dual code, the group to be considered is the subgroup $\mathcal{G}_2$ generated by $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and the polynomials $(xy)^{-k}(W_{C,f} \pm W_{C^\perp,f})$ are relative invariants for $\mathcal{G}_2$.

In both cases, these results can be used to derive some information on the way a given t-set T meets the codewords. In particular, we give another proof of the fact that the words of fixed weight in an extremal code (resp. and its dual in the case formally self-dual) support "$t\frac{1}{2}$"-designs, as shown in [6], [16].

More generally, we can derive some "invariant linear forms" in the sense of [5] on the so-called intersection numbers:

$$\begin{aligned} n_{w,i}(T) &:= \mathrm{Card}\{u \in C \mid wt(u) = w, |u \cap T| = i\} \\ n^*_{w,i}(T) &:= \mathrm{Card}\{u \in C^\perp \mid wt(u) = w, |u \cap T| = i\} \end{aligned} \qquad (1)$$

not only in the case when $|T| = t$ and one has t-designs, but also for all value of $t = |T|$, through the explicit description of the space of relative invariant polynomials in which $(xy)^{-k}(W_{C,f} \pm W_{C^\perp,f})$ falls. Therefore, we specialize to certain harmonic functions $f = H_{k,T}$ associated to T, which have the property that $H_{k,T}(u)$ only depends on t, $|u|$, and $|u \cap T|$; they are constructed from Hahn polynomials. As an example and application, we derive a classification of the extremal even formally self-dual codes of length 12. This classification has been extended in [11], [12], where intersection numbers play an important role.

Another method is used in [14] to derive analogous results. It involves some other kinds of polynomials, the so-called overlap and covering polynomials, which are closely connected to Ozeki's Jacobi polynomials([18]). The author is grateful to one referee for pointing out this reference.

This paper is organized in the following way: Section 1 contains the needed definitions and properties of harmonic functions and binary linear codes. Section 2 contains the definition of harmonic weight enumerators and the proof of the MacWilliams-type formula (Theorem 2.1). The consequences on the invariance properties of these polynomials in the cases of doubly even self-dual codes and of even formally self-dual codes are stated in Corollaries 2.1 and 2.2. Section 3 gathers the needed results of invariant theory. In Section 4, we reprove Assmus-Mattson theorem and Calderbank-Delsarte strengthening of it for doubly even self-dual codes. Section 5 explains the method based on Hahn polynomials used to compute the intersection numbers, and Section 6 contains the classification of the extremal even formally self-dual codes of length 12 (Theorem 6.1).

We now recall some definitions and properties of discrete harmonic functions, which are developed in [8].

Let $\Omega = \{1, 2, \ldots, n\}$ be a finite set (which will be the set of coordinates of the code C) and let X be the set of its subsets, while, for all $k = 0, 1, \ldots, n$, X_k is the set of its k-subsets. We denote by $\mathbb{R}X$, $\mathbb{R}X_k$ the free real vector spaces spanned by respectively the elements of X, X_k. An element of $\mathbb{R}X_k$ is denoted by

$$f = \sum_{z \in X_k} f(z)z \tag{2}$$

and is identified with the real-valued function on X_k given by $z \to f(z)$. The complementary set of z is denoted by $\overline{z}$.

Such an element $f \in \mathbb{R}X_k$ can be extended to an element $\tilde{f} \in \mathbb{R}X$ by setting, for all $u \in X$,

$$\tilde{f}(u) := \sum_{\substack{z \in X_k \\ z \subset u}} f(z) \tag{3}$$

(In the notations of [8], the restriction of $\tilde{f}$ to $\mathbb{R}X_n$ is defined to be $\psi(f)$.) We may later on denote again $\tilde{f}$ by f. If an element $g \in \mathbb{R}X$ is equal to some $\tilde{f}$, for $f \in \mathbb{R}X_k$, we say that g has *degree k*. The *differentiation* γ is the operator defined by linearity from

$$\gamma(z) := \sum_{y \in X_{k-1}, y \subset z} y \tag{4}$$

for all $z \in X_k$ and for all $k = 0, 1, \ldots n$, and Harm_k is the kernel of γ:

$$\mathrm{Harm}_k := \mathrm{Ker}(\gamma_{|\mathbb{R}X_k}) \tag{5}$$

Concerning codes, we take the following notations: we freely identify words of $\mathbb{F}_2^n$ and subsets of Ω; the weight of an element $u \in \mathbb{F}_2^n$ is also the cardinality of its support and is denoted by $wt(u)$ or $|u|$. We recall some basic notions of coding theory, for which we refer to [17], [22]; we only consider linear codes. The weight enumerator $W_C(x, y)$ of a binary code C is

$$W_C(x,y) := \sum_{u \in C} x^{n-wt(u)} y^{wt(u)} := \sum_{i=0}^{n} A_i x^{n-i} y^i \tag{6}$$

where A_i is the number of codewords of weight i and satisfies the MacWilliams identity:

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y). \tag{7}$$

A code C is said to be *formally self-dual* if $W_C = W_{C^\perp}$. It is *even* if $wt(u) \equiv 0 \mod 2$ for all $u \in C$, and *doubly even* if $wt(u) \equiv 0 \mod 4$ for all $u \in C$. Self-dual codes are even and formally self-dual, while the converse is not true; see [16], [22] for examples. If a formally self-dual code is in addition doubly even, then it is necessarily self-dual. From the facts that the polynomial W_C is invariant under the group $\mathcal{G}_1$ in the self-dual doubly even case (resp. under $\mathcal{G}_2$ in the even formally self-dual case), one deduces the inequalities for the minimal weight $d(C)$ of C: $d(C) \leq 4([n/24] + 1)$ (respectively $d(C) \leq 2([n/8] + 1)$). A code meeting these bounds is said to be extremal; its weight enumerator is then uniquely determined.

2 Harmonic weight enumerators

In this section, we define the harmonic weight enumerators associated to a binary linear code C and prove a MacWilliams type equality.

Definition 2.1 *Let C be a binary code of length n and let $f \in Harm_k$. The harmonic weight enumerator associated to C and f is*

$$W_{C,f}(x,y) := \sum_{u \in C} \tilde{f}(u) x^{n-wt(u)} y^{wt(u)}. \tag{8}$$

Theorem 2.1 *Let $W_{C,f}(x,y)$ be the harmonic weight enumerator associated to the code C and the harmonic function f of degree k. Then*

$$W_{C,f}(x,y) = (xy)^k Z_{C,f}(x,y) \tag{9}$$

where $Z_{C,f}$ is a homogeneous polynomial of degree $n-2k$, and satisfies

$$Z_{C^{\perp},f}(x,y) = (-1)^k \frac{2^{n/2}}{|C|} Z_{C,f}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right). \tag{10}$$

Proof. Like in the classical case of MacWilliams formula for weight enumerators, the proof relies on Poisson summation formula, which we recall here:

Theorem 2.2 (Poisson summation formula) *Let $\phi : \mathbb{F}_2^n \to R$ be a function taking its values into a ring R, and let $\hat{\phi}$ be its Fourier transform, defined by*

$$\hat{\phi}(v) := \sum_{u \in F_2^n} (-1)^{u.v} \phi(u). \tag{11}$$

Then, for all linear code $C \subset \mathbb{F}_2^n$,

$$\sum_{u \in C^{\perp}} \phi(u) = \frac{1}{|C|} \sum_{v \in C} \hat{\phi}(v) \tag{12}$$

We shall apply Poisson formula to each term of $Z_{C,f}$, namely to:

$$\phi(u) := \tilde{f}(u) x^{n-wt(u)-k} y^{wt(u)-k}. \tag{13}$$

Therefore, we compute the Fourier transform of ϕ, first in the case $f = z \in X_k$ (Lemma 2.2), and in the general case but for harmonic functions in Lemma 2.3. In order to prove that the $Z_{C,f}$ are actually polynomials, we start with a technical lemma on harmonic functions.

Lemma 2.1 *Let $f \in Harm_k$ and $v \in \mathbb{F}_2^n$. Let*

$$f^{(i)}(v) := \sum_{\substack{z \in X_k \\ wt(z \cap v) = i}} f(z).$$

Then, for all $0 \leq i \leq k$, $f^{(i)}(v) = (-1)^{k-i}\binom{k}{i}\tilde{f}(v)$.

Proof. For all $0 \le i \le k-1$, $\gamma^{k-i}(f) = 0$, which means (from (4)) that $g_i := \sum_{t \in X_i} (\sum_{\substack{z \in X_k \\ t \subset z}} f(z)) t = 0$. The evaluation at $v \in \mathbb{F}_2^n$ is:

$$g_i(v) = 0 = \sum_{\substack{t \in X_i \\ t \subset v}} (\sum_{\substack{z \in X_k \\ t \subset z}} f(z)) = \sum_{j=i}^{k} \binom{j}{i} f^{(j)}(v)$$

The proof then follows by induction on $k-i$, since clearly $f^{(k)}(v) = \tilde{f}(v)$ and the previous equality implies

$$\begin{aligned} f^{(i)}(v) &= -\sum_{j=i+1}^{k} \binom{j}{i} f^{(j)}(v) = -(\sum_{j=i+1}^{k} (-1)^{k-j} \binom{j}{i} \binom{k}{j}) \tilde{f}(v) \\ &= -\binom{k}{i} (\sum_{j=i+1}^{k} (-1)^{k-j} \binom{k-i}{j-i}) \tilde{f}(v) = (-1)^{k-i} \binom{k}{i} \tilde{f}(v). \end{aligned}$$

$\square$

We can notice now that, for all u such that $wt(u) < k$, from definition (3) of $\tilde{f}$, $\tilde{f}(u) = 0$, and from Lemma 2.1, $\tilde{f}(\overline{u}) = f^{(0)}(u) = 0$; hence $Z_{C,f}(x,y)$ is a polynomial. We now compute the Fourier transform of ϕ (see (13)).

Lemma 2.2 *Let $f = z \in X_k$. Then*

$$\hat{\phi}(v) = x^{-k} (-1)^{wt(v \cap z)} (x+y)^{n-k-wt(v \cap \overline{z})} (x-y)^{wt(v \cap \overline{z})}$$

Proof.

$$\begin{aligned} \hat{\phi}(v) :=& \sum_{u \in \mathbb{F}_2^n} (-1)^{u.v} \phi(u) = \sum_{u \in \mathbb{F}_2^n} (-1)^{u.v} \tilde{f}(u) x^{n-wt(u)-k} y^{wt(u)-k} \\ =& x^{-k} \sum_{\substack{u \in \mathbb{F}_2^n \\ z \subset u}} (-1)^{u.v} x^{n-wt(u)} y^{wt(u)-k}. \end{aligned}$$

We can write $u = z \cup u'$, where u' runs through $\mathbb{F}_2^{n-k}$, with $wt(u) = k + wt(u')$ and $u.v = wt(v \cap z) + u'.(v \cap \overline{z}) \mod 2$; we are then reduced to the usual formula for the Fourier transform of $x^{n-k-wt(v \cap \overline{z})} y^{wt(v \cap \overline{z})}$.

$$
\begin{aligned}
\hat{\phi}(v) =& x^{-k}(-1)^{wt(v\cap z)} \sum_{u' \in \mathbb{F}_2^{n-k}} (-1)^{u'.(v\cap\overline{z})} x^{n-k-wt(u')} y^{wt(u')} \\
=& x^{-k}(-1)^{wt(v\cap z)}(x+y)^{n-k-wt(v\cap\overline{z})}(x-y)^{wt(v\cap\overline{z})}.
\end{aligned}
$$

□

We now consider the case of a harmonic function of degree k and prove

Lemma 2.3 *Let $f \in Harm_k$. Then*

$$
\hat{\phi}(v) = (-1)^k 2^k \tilde{f}(v)(x+y)^{n-wt(v)-k}(x-y)^{wt(v)-k}
$$

Proof. Since $f = \sum_{z\in X_k} f(z)z$, and from Lemma 2.2,

$$
\begin{aligned}
\hat{\phi}(v) =& x^{-k} \sum_{z\in X_k} f(z)(-1)^{wt(v\cap z)}(x+y)^{n-k-wt(v\cap\overline{z})}(x-y)^{wt(v\cap\overline{z})} \\
=& x^{-k}(x+y)^{n-wt(v)-k}(x-y)^{wt(v)-k} \\
& \cdot \sum_{z\in X_k} f(z)(-1)^{wt(v\cap z)}(x+y)^{wt(v\cap z)}(x-y)^{k-wt(v\cap z)}.
\end{aligned}
$$

To conclude for Lemma 2.3, we need another last lemma:

Lemma 2.4 *Let $f \in Harm_k$. Then, for all $v \in \mathbb{F}_2^n$,*

$$
\sum_{z\in X_k} f(z)(-1)^{wt(v\cap z)}(x+y)^{wt(v\cap z)}(x-y)^{k-wt(v\cap z)} = (-1)^k 2^k \tilde{f}(v) x^k
$$

Proof. Let B_s be the coefficient of $x^{k-s}y^s$ in this polynomial. We must show that $B_0 = (-1)^k 2^k \tilde{f}(v)$ and $B_s = 0$ for all $s \geq 1$.

We sum over $i = wt(v \cap z)$; with the notations of Lemma 2.1, it is equal to $\sum_{i=0}^{k} f^{(i)}(v)(-1)^i(x+y)^i(x-y)^{k-i}$, and, by Lemma 2.1,

$$
\begin{aligned}
B_s =& \sum_{i=0}^{k} f^{(i)}(v)(-1)^i \sum_{\substack{j,l,j\leq i,l\leq k-i\\ j+l=s}} \binom{i}{j}\binom{k-i}{l}(-1)^l \\
=& \tilde{f}(v)\sum_{i=0}^{k}\binom{k}{i}(-1)^k \sum_{\substack{j,l,j\leq i,l\leq k-i\\ j+l=s}} \binom{i}{j}\binom{k-i}{l}(-1)^l \\
=& (-1)^k \tilde{f}(v) \sum_{\substack{i,j,l\\ 0\leq j\leq i\leq k\\ 0\leq l\leq k-i\\ j+l=s}} (-1)^l \frac{k!}{j!l!(i-j)!(k-i-l)!} \\
=& (-1)^k \tilde{f}(v) \sum_{\substack{j,l,t,r\\ 0\leq j,l,t,r\leq k\\ j+l=s\\ j+l+t+r=k}} (-1)^l \frac{k!}{j!l!t!r!} \\
=& (-1)^k \tilde{f}(v) 2^k \delta_{s,0}
\end{aligned}
$$

where the last equality is the computation of the coefficient of x^s in the specialization of $(x-y+z+w)^k$ at $x=y$, $z=w=1$.

□

□

Theorem 2.1 now follows from Lemma 2.3 and the Poisson summation formula (12).

□

In the special case of doubly even self-dual codes, an immediate consequence of Theorem 2.1 is that the polynomials $Z_{C,f}$ are relative invariants for the group $\mathcal{G}_2$. This result is stated in Corollary 2.1, and an analogous result for even formally self-dual codes is stated in Corollary 2.2.

We take the following notations:

$$
T_1 := \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right), T_2 := \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right), T_3 := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right). \tag{14}
$$

We consider the group $\mathcal{G}_1 =< T_1, T_2 >$ together with the characters χ_k defined by:

$$
\chi_k(T_1) = (-1)^k, \quad \chi_k(T_2) = i^{-k} \tag{15}
$$

and the group $\mathcal{G}_2 =< T_1, T_3 >$ together with the characters χ_k^+, χ_k^- defined by

$$\chi_k^+(T_1) = \chi_k^+(T_3) = (-1)^k \tag{16}$$
$$\chi_k^-(T_1) = (-1)^k, \quad \chi_k^-(T_3) = (-1)^{k+1} \tag{17}$$

Corollary 2.1 *If C is a self-dual, doubly even code of length n, for all $f \in Harm_k$, the polynomial $Z_{C,f}(x,y)$ satisfies*

$$Z_{C,f}(A(x,y)) = \chi_k(A) Z_{C,f}(x,y)$$

for all matrix $A \in \mathcal{G}_1$.

Corollary 2.2 *If C is an even formally self-dual code of length n, for all $f \in Harm_k$, the polynomials $Z_{C,f} \pm Z_{C^\perp,f}$ satisfy*

$$(Z_{C,f} + Z_{C^\perp,f})(A(x,y)) = \chi_k^+(A)(Z_{C,f} + Z_{C^\perp,f})(x,y)$$
$$(Z_{C,f} - Z_{C^\perp,f})(A(x,y)) = \chi_k^-(A)(Z_{C,f} - Z_{C^\perp,f})(x,y)$$

for all matrix $A \in \mathcal{G}_2$.

3 Some invariant theory

We gather here some well-known results of invariant theory that will be of further use. We denote by $\mathbb{C}[x_1,\dots,x_n]$ the polynomial algebra in n variables, together with the left action of the algebra $M_n(\mathbb{C})$ of $n\times n$ complex matrices given by $(M.P)(x) = P(Mx^t)$ (where $x = (x_1,\dots,x_n)$ and x^t is the transposition).

If G is a subgroup of $M_n(\mathbb{C})$, we denote by $\mathcal{I}_G$ the algebra of invariants of G, namely

$$\mathcal{I}_G = \{P(x_1,\dots x_n) \in \mathbb{C}[x_1,\dots x_n] \mid g.P = P \quad \forall g \in G\}.$$

If χ is a character of G, the space of relative invariants with respect to χ is

$$\mathcal{I}_{G,\chi} = \{P(x_1,\dots x_n) \in \mathbb{C}[x_1,\dots x_n] \mid g.P = \chi(g)P \quad \forall g \in G\}.$$

It is clearly a module over $\mathcal{I}_G$. In view of our situation, we need to compute $\mathcal{I}_{\mathcal{G}_1,\chi_k}$, for the characters χ_k defined in (15). It is well-known to be, in the case $k \equiv 0 \mod 4$, the polynomial algebra $\mathbb{C}[P_8, P_{24}]$, where $P_8 = x^8 + 14x^4y^4 + y^8$ and $P_{24} = x^4y^4(x^4 - y^4)^4$. The other cases are probably also very classical, but we recall the result:

Lemma 3.1

$$\mathcal{I}_{\mathcal{G}_1,\chi_k} = \begin{cases} P_{12}\mathcal{I}_{\mathcal{G}_1} \text{ if } k \equiv 2 \mod 4, \text{ where } P_{12} = x^2y^2(x^4 - y^4)^2 \\ P_{18}\mathcal{I}_{\mathcal{G}_1} \text{ if } k \equiv 3 \mod 4, \text{ where } P_{18} = xy(x^8 - y^8)(x^8 - 34x^4y^4 + y^8) \\ P_{30}\mathcal{I}_{\mathcal{G}_1} \text{ if } k \equiv 1 \mod 4, \text{ where } P_{30} = P_{12}P_{18} \end{cases}$$

Proof. The dimension $a_{\chi,d}$ of $(\mathcal{I}_{G,\chi})_d$, the homogeneous component of degree d of $(\mathcal{I}_{G,\chi})$ is computed by Molien's series:

$$\sum_{d\leq 0} a_{\chi,d}X^d = \frac{1}{|G|}\sum_{g\in G}\frac{\overline{\chi(g)}}{\mathrm{Det}(I - Xg)}.$$

In the case of the group $\mathcal{G}_1$, and for the characters χ_k given by (15), we find respectively $1/((1-X^8)(1-X^{24}))$, $X^{30}/((1-X^8)(1-X^{24}))$, $X^{12}/((1-X^8)(1-X^{24}))$, $X^{18}/((1-X^8)(1-X^{24}))$. It is easy to verify that the polynomials announced in the lemma do belong to the spaces $\mathcal{I}_{\mathcal{G}_1,\chi_k}$; the result then follows from the equality of the dimensions.

□

The case of the group $\mathcal{G}_2$ goes the same; we have $\mathcal{I}_{\mathcal{G}_2} = \mathbb{C}[P_2, P_8']$, where $P_2 = x^2+y^2$, $P_8' = P_8 - P_2^4 = x^2y^2(x^2-y^2)^2$, and the $\mathcal{I}_{\mathcal{G}_2,\chi_k^{\pm}}$ for the characters (16), (17), are principal ideals. Clearly these characters only depend on k mod 2.

Lemma 3.2

$$\mathcal{I}_{\mathcal{G}_2,\chi} = \begin{cases} Q_4\mathcal{I}_{\mathcal{G}_2} \text{ if } \chi = \chi_0^-, \text{ where } Q_4 = xy(x^2 - y^2) \\ Q_8\mathcal{I}_{\mathcal{G}_2} \text{ if } \chi = \chi_1^+, \text{ where } Q_8 = xy(x^6 - 7x^4y^2 + 7x^2y^4 - y^6) \\ R_4\mathcal{I}_{\mathcal{G}_2} \text{ if } \chi = \chi_1^-, \text{ where } R_4 = x^4 + y^4 - 6x^2y^2 \end{cases}$$

4 New proofs of some classical results

In this section, we recover the classical results on t-designs supported by words of binary linear codes, using the harmonic weight enumerators previously defined, and the characterization of designs in terms of the harmonic spaces given in [8]: a set $\mathcal{B}$ of blocks is a t-design if and only if $\sum_{b\in\mathcal{B}}\tilde{f}(b) = 0$

for all $f \in \mathrm{Harm}_k$, $1 \le k \le t$. Hence, the set of words of fixed weight in a code C form a t-design if and only if $W_{C,f}(x,y) = 0$ for all $f \in \mathrm{Harm}_k$, $1 \le k \le t$.

We start with Assmus-Mattson theorem:

Theorem 4.1 (Assmus-Mattson) *Let C be a binary code of length n and distance d, and let $C^\perp$ be its dual, of distance e. If $t \le d$ is such that the number of non zero weights of $C^\perp$ which are lower or equal to $n-t$, is at most $d-t$, then the set of codewords of C (respectively $C^\perp$) of fixed weight w form a t-design, for $d \le w \le n$ (respectively $e \le w \le n-t$).*

Proof. Let $f \in \mathrm{Harm}_k$, $1 \le k \le t$. Write $A_{i,f} := \sum_{u \in C, wt(u)=i} \tilde{f}(u)$ and $B_{i,f} := \sum_{u \in C^\perp, wt(u)=i} \tilde{f}(u)$. We want to prove that, for all i (rep. $i \le n-t$), $A_{i,f} = 0$ (rep. $B_{i,f} = 0$). Theorem 2.1 translates, in terms of these, into:

$$\frac{(-1)^k 2^k}{|C^\perp|} \sum_{k \le i \le n-k} P_j^{(n-2k)}(i-k) B_{i,f} = A_{j,f} \tag{18}$$

for all j, $k \le j \le n-k$, where the $P_j^{(n-2k)}$ are the Krawtchouck polynomials ([17, Chap 5]). Since C has distance d, we have $A_{k,f} = \cdots = A_{d-1,f} = 0$, which leads to $d-k$ independent equations in the $B_{i,f}$, $k \le i \le n-k$. By hypothesis, there are at most $d-k$ unknowns and hence the only solution is trivial . Hence $B_{i,f} = 0$ for all $i \le n-t$ and $k \le t$.

Now the $n-2k+1$ equations $B_{i,f} = 0$, $k \le i \le n-k$, translate into equations in the $A_{i,f}$, $d \le i \le n-d$, using equations (18) applied to $C^\perp$; since $k \le d$ and the equations are independent, the only solution is trivial.

$\square$

In the case of extremal doubly even self-dual codes, we can prove the result directly from the description of the relative invariants of the group $\mathcal{G}_1$, avoiding the use of Krawtchouck polynomials; moreover, the extra property that the t-designs are "$t\frac{1}{2}$"-designs (which was shown first by B. Venkov by means of spherical theta series, then in [6] in a combinatorial setting) follows easily, and is very similar to the initial proof of B.Venkov [24] concerning the spherical designs in extremal even unimodular lattices. We recall the slightly more general definition of the notion of a T-design, for a subset T of $\{1, 2, \ldots, n\}$: a set $\mathcal{B}$ of blocks is called a T-design if and only if $\sum_{b \in \mathcal{B}} \tilde{f}(b) = 0$ for all $f \in \mathrm{Harm}_k$ and for all $k \in T$. Hence a t-design is a $T = \{1, \ldots, t\}$-design.

Theorem 4.2 ([5]) *Let C be an extremal self-dual doubly even code of length n.*

- *If $n \equiv 0 \mod 24$, the codewords of fixed weight in C form a $\{1,2,3,4,5,7\}$ – design.*
- *If $n \equiv 8 \mod 24$, the codewords of fixed weight in C form a $\{1,2,3,5\}$ – design.*
- *If $n \equiv 16 \mod 24$, the codewords of fixed weight in C form a $\{1,3\}$ – design.*

Proof. Let $n = 24m+r$; the extremality of C means that $d(C) = 4(m+1)$. We prove that $W_{C,f}(x,y) = 0$ for all $f \in \mathrm{Harm}_k$, $k = 1,5$, and $r = 0,8$, the other cases being similar. From Theorem 2.1 and Lemma 3.1, for all $f \in \mathrm{Harm}_k$, $W_{C,f}(x,y) = (xy)^k Z_{C,f}(x,y) = (xy)^k P_{30} Q$, where $Q \in \mathbb{C}[P_8, P_{24}]$. Since the valuation at y of Q, (i.e. the least power of y in Q) is $4(m+1)-k-3$, $Q = P_{24}^{m+1-\frac{k+3}{4}}.Q'$, with $Q' \in \mathbb{C}[P_8, P_{24}]$. We compute the degree of Q': if this polynomial is non zero, it has degree $n - 2k - 30 - 24(m+1-\frac{k+3}{4}) = r + 4k - 36$. Hence $Q' = 0$ and $W_{C,f}(x,y) = 0$ for $r = 0,8$ and $k = 1,5$. Notice that, if $k = 9$, the polynomial Q' is determined up to a scalar: it is proportional to 1 if $r = 0$, respectively to P_8 if $r = 8$.

□

Remark 4.1 *With the same method, we can recover the results of [16] on the designs supported by codewords of fixed weight in $C \cup C^{\perp}$, when C is an extremal even formally self-dual code. We omit the proof.*

5 Harmonic weight enumerators and the computation of Jacobi polynomials

In this section, we show how harmonic weight enumerators can be used to compute Jacobi polynomials. We first recall the definition of these: Let C be a binary code of length n and $T \subset \{1, \ldots, n\}$.

$$J_{C,T}(v,z,x,y) := \sum_{u \in C} v^{m_0(u)} z^{m_1(u)} x^{n_0(u)} y^{n_1(u)} \tag{19}$$

where, for $i = 0,1$, $m_i(u)$ (respectively $n_i(u)$) is the number of coordinates of $u \cap T$ (respectively of $u \cap \overline{T}$) equal to i. They have been introduced by Ozeki

[18] in analogy with Jacobi forms of lattices, and studied by A. Bonnecaze, P. Solé *et al.* [2], [3], [4] in the case of type II binary and Z_4-codes. In particular they point out the following characterization of codes supporting designs: the set of codewords of a code C form a t-design for every fixed weight, if and only if the Jacobi polynomial $J_{C,T}$ for a t-set T is independent of T.

Since we can also characterize this property of a code C by the set of conditions:

$$W_{C,f}(x,y) = 0 \quad \forall f \in \mathrm{Harm}_k, 1 \leq k \leq t \tag{20}$$

a natural question is: how can one compute $J_{C,T}$ for a t-set T given in (19) from the set of conditions (20)? The answer lies in the fact that one can attach to every t-set T some harmonic functions $H_{k,T}$ of degree k, $1 \leq k \leq t$; the values $H_{k,T}(u)$ are expressed in terms of Hahn polynomials, and only depend on $|u|$ and $|u \cap T|$. They are described in [8] as the orthogonal projection of $T \in \mathbb{R}X_t$ over Harm_k. In view of our applications, we need to generalize [8, Theorem 5] to the case of subsets of non equal cardinality. For the definition and properties of Hahn polynomials, we refer to [15].

Proposition 5.1 *[8, Theorem 5] Let T be a t-subset of $\{1, \ldots, n\}$. For all k, $1 \leq k \leq t \leq n/2$, let $H_{k,T} \in \mathbb{R}X_t$ be given by:*

$$H_{k,T}(u) = Q_k^t(t - |u \cap T|)$$

for all t-set u, where ([15]) $Q_k^t(x) = Q_k(x; t-n-1, -t-1, t+1)$ are orthogonal Hahn polynomials. Then $H_{k,T} \in \mathrm{Harm}_k$.

Proof. In the notations of [8], $H_{k,T}(u) = E_k(T,u)$ and $Q_{k,T} = Q_k$. □

Proposition 5.2 *With the same hypothesis, as an element of $\mathbb{R}X$, the $H_{k,T}(u)$ for all subsets u of $\{1, \ldots, n\}$ only depend on $w = |u|$ and $|u \cap T|$. We set $H_{k,T}(u) = h_{k,t}(|u|, |u \cap T|)$. Then:*

$$h_{k,t}(w,i) = \frac{1}{\lambda_{k,t}} \sum_I \nu_{k,t}(w,i) Q_k^t(t - i_1 - i_2) \tag{21}$$

where

$$I = \{i_1, i_2, i_3 \mid 0 \le i_1 \le i,\; 0 \le i_2 \le t-i,\; 0 \le i_3 \le w-i,\; i_1+i_2+i_3 \le t,\; i_1+i_3 \ge k\} \tag{22}$$

$$\lambda_{k,t} = \binom{n-2k}{t-k} \tag{23}$$

$$\nu_{k,t}(w,i) = \binom{i}{i_1}\binom{t-i}{i_2}\binom{w-i}{i_3}\binom{n-w-t+i}{t-i_1-i_2-i_3}\binom{i_1+i_3}{k}. \tag{24}$$

Proof. From [8, Theorem 3] applied to $f = H_{k,T}$ and $g = \tilde{z}$, $z \in X_k$, we have $H_{k,T}(z) = \binom{n-2k}{t-k}^{-1} \sum_{x\in X_t, z\subset x} H_{k,T}(x)$. Then, for all $u \in X$,

$$\begin{aligned} H_{k,T}(u) &= \sum_{z\in X_k, z\subset u} H_{k,T}(z) \\ &= \binom{n-2k}{t-k}^{-1} \sum_{\substack{z\in X_k\\ z\subset u}} \sum_{\substack{x\in X_t\\ z\subset x}} H_{k,T}(x) \qquad (25)\\ &= \binom{n-2k}{t-k}^{-1} \sum_{x\in X_t} \binom{|x\cap u|}{k} Q_k^t(t-|x\cap T|) \qquad (26) \end{aligned}$$

which leads to the announced formula by setting $i_1 := |x \cap (u \cap T)|$, $i_2 := |x \cap (\overline{u} \cap T)|$, $i_3 := |x \cap (u \cap \overline{T})|$. □

Remark: The same argumentation as in [8] applied to $H_{k,T}(u) = E_k(T,u)$ for $|u| > t$ show that they are also linked to Hahn polynomials but for the parameters (with the notations of [15]): $Q_k(x; |u|-n-1, -|u|-1, t+1)$.

From (1) and (19), the numbers $n_{w,i}(T)$ are the coefficients of $J_{C,T}$:

$$J_{C,T}(v,z,x,y) = \sum_{i=0}^{t} n_{w,i}(T) v^{t-i} z^i x^{n-t-w+i} y^{w-i}. \tag{27}$$

On the other hand, the harmonic weight enumerators $W_{C,H_{k,T}}$ have the following expression:

$$
\begin{aligned}
W_{C,H_{k,T}}(x,y) &= \sum_{u\in C} H_{k,T}(u) x^{n-wt(u)} y^{wt(u)} \\
&= \sum_{w=0}^{n} \{ \sum_{i=0}^{t} h_{k,t}(w,i) n_{w,i}(T) \} x^{n-w} y^{w}
\end{aligned}
\tag{28}
$$

Hence the set of equations (20) for $f = H_{k,T}$, $k \leq t$ leads for every w to the following t linear equations in the $t+1$ unknowns $n_{w,i}(T)$, $0 \leq i \leq t$:

$$
\forall\ 0 \leq k \leq t,\ \sum_{i=0}^{t} h_{k,t}(w,i) n_{w,i}(T) \tag{29}
$$

We denote by C_w the set of codewords of weight w. Its cardinality is is equal to the coefficient A_w of the weight enumerator of the code C, defined by (6). Then, another equation, corresponding to the degree 0 case, is:

$$
\sum_{i=0}^{t} n_{w,i}(T) = A_w \tag{30}
$$

For all w, the $n_{w,i}(T)$ are the solutions of the system of equations (29), (30).

Remark: In the cases when the polynomials $Z_{C,H_{k,T}}$ are invariant polynomials, i.e. in the cases of doubly even self-dual codes or of even formally self-dual codes, we can more generally get some information on the $n_{w,i}(T)$, not only when the codewords support t-designs, in the following way: a condition of the type $Z_{C,f} \in \mathcal{I}_{\mathcal{G},\chi}$, joined with the knowledge of $d(C)$, says that $Z_{C,f}$ sits in a finite-dimensional vector space, which is explicitly described. Hence this information can be turned into linear equations in the $n_{w,i}(T)$. Of course, the smaller this dimension is, the more equations we get, and the case when the codewords support designs is the 0-dimensional case. The higher $d(C)$ is, the smaller are these dimensions, the most interesting cases being the extremal codes. An example of this method is treated in next section.

6 A classification result

In this section, we classify, with the help of harmonic weight enumerators, the extremal even formally self-dual codes of length 12. These codes have weight 4 and their weight enumerator is

$$W_C(x,y) = W_{C^\perp}(x,y) = x^{12} + 15x^8y^4 + 32x^6y^6 + 15x^4y^8 + y^{12}. \qquad (31)$$

There is a unique code which is self-dual; it is the code B_{12} with component d_{12} of [19], [20]; we find two other codes which are isodual, one of them is described in [22, Chap.3]. They both appear in [13] as double circulant codes.

First step in this classification result is the computation of the $\{n_{w,i}(T), n^*_{w,i}(T)\}_{0\le i\le t}$ (see (1)). We first show that, if T is a word of C of weight 4 or 6, there are only two solutions for $\{n_{w,i}(T), n^*_{w,i}(T)\}_{0\le i\le t}$; therefore, we use the results of the previous section to derive some equations satisfied by these numbers.

Lemma 6.1 *Let C be an extremal even formally self-dual code of length 12 and let $T \in C$, of weight 4 or 6. There are only two possibilities for $\{n_{w,i}(T), n^*_{w,i}(T)\}_{0\le i\le t}$, which are given in the following tables:*

- *If $wt(T) = 4$*

	$T \in C \cap C^\perp$					$T \in C, T \notin C^\perp$				
i	0	1	2	3	4	0	1	2	3	4
$n_{4,i}(T)$	6	0	8	0	1	2	8	4	0	1
$n_{6,i}(T)$	0	0	32	0	0	0	8	16	8	0
$n^*_{4,i}(T)$	6	0	8	0	1	5	0	10	0	0
$n^*_{6,i}(T)$	0	0	32	0	0	2	0	28	0	2

- *If $wt(T) = 6$*

	$T \in C \cap C^\perp$							$T \in C, T \notin C^\perp$						
i	0	1	2	3	4	5	6	0	1	2	3	4	5	6
$n_{4,i}(T)$	0	0	15	0	0			0	4	7	4	0		
$n_{6,i}(T)$	1	0	15	0	15	0	1	1	0	7	16	7	0	1
$n^*_{4,i}(T)$	0	0	15	0	0			1	0	13	0	1		
$n^*_{6,i}(T)$	1	0	15	0	15	0	1	0	0	16	0	16	0	0

Proof. We first make some easy remarks: since $T \in C$, $n^*_{w,i}(T) = 0$ if i is odd. Moreover, since the all-one word **1** belongs to $C \cap C^\perp$, $n_{12-w,t-i}(T) = n_{w,i}(T)$ and $n^*_{12-w,t-i}(T) = n^*_{w,i}(T)$.

From (31), we have:

$$\sum_i n_{4,i}(T) = \sum_i n^*_{4,i}(T) = 15 \tag{32}$$

and

$$\sum_i n_{6,i}(T) = \sum_i n^*_{6,i}(T) = 32. \tag{33}$$

• $wt(T) = 4$. Some of the entries are easily computed from the hypothesis on the code C: $n_{4,3}(T) = 0$ and $n_{6,4}(T) = 0$ otherwise the sum with T would be a weight 2 word in C, and clearly $n_{4,4}(T) = 1$. Taking into account the equations (32) and (33), we are reduced to the set of six unknowns: $S := \{n_{4,0}(T), n_{4,1}(T), n_{6,1}(T), n^*_{4,0}(T), n^*_{4,2}(T), n^*_{6,0}(T)\}$. We now consider the harmonic weight enumerators $W_{C,H_{k,T}}$ defined in the previous section. From Corollary 2.2 and Lemma 3.2, $Z_{C,H_{1,T}} + Z_{C^\perp,H_{1,T}} \in Q_8\mathbb{C}[P_2, P'_8]$; but, since C and $C^\perp$ have weight 4, $Z_{C,H_{1,T}} + Z_{C^\perp,H_{1,T}}$ must be a multiple of $(xy)^3$, and hence of $Q_8P'_8$. This last polynomial is of degree 16 while $Z_{C,H_{1,T}} + Z_{C^\perp,H_{1,T}}$ is of degree 10; hence it is zero. A similar discussion shows that $Z_{C,H_{1,T}} - Z_{C^\perp,H_{1,T}} = 0$, $Z_{C,H_{2,T}} + Z_{C^\perp,H_{2,T}} \in \mathbb{C}P'_8 = \mathbb{C}(x^6y^2 - 2x^4y^4 + x^2y^6)$ and that $Z_{C,H_{2,T}} - Z_{C^\perp,H_{2,T}} = 0$. We derive the following equations:

$$\begin{aligned}
&\sum_{i=0}^{4} h_{1,4}(4,i)n_{4,i}(T) = 0 \\
&\sum_{i=0}^{4} h_{1,4}(4,i)n^*_{4,i}(T) = 0 \\
&2(\sum_{i=0}^{4} h_{2,4}(4,i)n_{4,i}(T) + \sum_{i=0}^{4} h_{2,4}(4,i)n^*_{4,i}(T)) \\
&\qquad + (\sum_{i=0}^{6} h_{2,4}(6,i)n_{6,i}(T) + \sum_{i=0}^{6} h_{2,4}(6,i)n^*_{6,i}(T)) = 0 \\
&\sum_{i=0}^{4} h_{2,4}(4,i)n_{4,i}(T) - \sum_{i=0}^{4} h_{2,4}(4,i)n^*_{4,i}(T) = 0 \\
&\sum_{i=0}^{6} h_{2,4}(6,i)n_{6,i}(T) - \sum_{i=0}^{6} h_{2,4}(6,i)n^*_{6,i}(T) = 0
\end{aligned} \tag{34}$$

which, in terms of our six unknowns, the coefficients $h_{k,4}(w,i)$ being computed from equation (), lead to:

$$\begin{aligned}
n_{4,0}(T) &= -18 + 4n^*_{4,0}(T) \\
n_{4,1}(T) &= 48 - 8n^*_{4,0}(T) \\
n^*_{4,2}(T) &= 20 - 2n^*_{4,0}(T) \\
n^*_{6,0}(T) &= 12 - 2n^*_{4,0}(T) \\
n_{6,1}(T) &= 48 - 8n^*_{4,0}(T)
\end{aligned} \tag{35}$$

Since we look for positive integral solutions, we see from the first two equations of (35) that the only possibilities are $n^*_{4,0}(T) = 5, 6$ which give the two announced solutions. Clearly, $n^*_{4,4}(T) = 1, 0$, depending whether T belongs to $C^\perp$ or not.

- $w(T) = 6$. Similar arguments lead to the result. □

Theorem 6.1 *There are exactly three extremal formally self-dual codes with even weights of length 12; one is the unique self-dual code B_{12} and the two others are given by the following generator matrices:*

$$C_{12}^{(1)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$C_{12}^{(1)} \cap (C_{12}^{(1)})^{\perp} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Permutation group of order 384

$$C_{12}^{(2)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$C_{12}^{(2)} \cap (C_{12}^{(2)})^{\perp} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Permutation group of order 120

Proof. Let C be such a code. Let $T_6 \in C$ be a word of weight 6, not belonging to $C^{\perp}$. From Lemma 6.1 we know that $n^*_{4,4}(T_6) = 1$, i.e. there is a unique word u_4 of weight 4 in $C^{\perp}$ whose support is contained in T_6. Clearly u_4 doesn't belong to C because $u_4 + T_6$ has weight 2. On the other hand, since $n^*_{6,4}(u_4) = 2$, we see that each such u_4 is associated to exactly two weight 6 words of C (we have reversed the roles of C and $C^{\perp}$ in Lemma 6.1). Hence the number of weight 6 words in C but not in $C^{\perp}$ is at most $2.15 = 30$. Since $\mid C_6 \mid = 32$, there is at least one pair $(T, \mathbf{1} + T)$ of words of weight 6 belonging to $C \cap C^{\perp}$.

Each of the words of weight 4 in C intersects T in two positions, which are never the same, otherwise the sum of two such words with $\mathbf{1}+T$ would be a weight 2 word in C. Hence there is a one-to-one correspondence between the 15 elements in C_4 and the $\binom{6}{2} = 15$ 2-subsets of T (respectively of $\mathbf{1}+T$). We denote them by $u \to t(u)$, $u \to \overline{t}(u)$.

Let u be a fixed weight 4 word in C. Up to permutation, we can assume that T, u are in the following position:

$$\begin{array}{cccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0
\end{array}$$

We assume first that $u \in C \cap C^{\perp}$. From Lemma 6.1, there are 8 words u' in C_4 meeting u in two positions; since $t(u') \neq t(u)$, $\bar{t}(u') \neq \bar{t}(u)$, there are four possibilities for $u \cap u'$: 0110, 1001, 1010, 0101. Assume one of them appears at least three times, say the first one and for u_2, u_3, u_4. Again because t and $\bar{t}$ are bijections, there is up to permutation only one possibility:

$$\begin{array}{c|cccccccccccc}
u & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
u_2 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
u_3 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
u_4 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0
\end{array}$$

Then $\{\mathbf{1}, T, u, u_2, u_3, u_4\}$ generates the self-dual code B_{12} ([19],[20]). We can next assume that the eight u' reach exactly twice the four possibilities for $u \cap u'$. Again for the same argument, there is up to permutation only one possibility:

$$\begin{array}{c|cccccccccccc}
u & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
u_2 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
u_3 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
u_4' & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{array}$$

and now $\{\mathbf{1}, T, u, u_2, u_3, u_4'\}$ generates the code $C_{12}^{(1)}$.

The last case to consider is the case when no weight 4 word in C belongs to $C^{\perp}$. Hence $C \cap C^{\perp}$ is the 2-dimensional code generated by T and $\mathbf{1}$. From Lemma 6.1, we know that eight words of weight 4 in C meet u in one position. Then, at least one position is reached at least twice, say by u_2, u_3. Since $u + u_2 + u_3$ cannot have weight 10, u_2 and u_3 must share another position outside u. Up to permutation, they are in the following positions:

$$\begin{array}{c|cccccccccccc}
u & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
u_2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
u_3 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0
\end{array}$$

If a third word u_4 meets u again in the same position as u_2 and u_3, this is also true for the other pairs (u_2, u_4) and (u_3, u_4); but then either $u_2 + u_3 + u_4 + T$ or $u_2 + u_3 + u_4 + T + \mathbf{1}$ has weight 2, which is not possible.

Hence each position in u corresponds to a pair of weight 4 words in C intersecting at that position. From the previous discussion, the sum is a weight 4 word which is disjoint from u; there are exactly two such words since $n_{4,0}(u) = 2$ and they are necessarily disjoint (if w is one of them, the other is $w' = \mathbf{1} + w + u$). Then (u_2, u_3) corresponds to $w = 001100001010$ and let (u_4, u_5) be such that $u_4 + u_5 = w'$. We have two choices up to permutation for the common position of u, u_4, u_5; it can be (on u) either 1000 or 0010. But it is easy to see that the first one is not possible under the condition that t, $\bar{t}$ are bijective and that the second one leads to only one possibility:

$$\begin{array}{cccccccccccccc}
u & & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
u_2 & & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
u_3 & & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
u_4 & & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
u_5 & & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{array}$$

In that case, $\{\mathbf{1}, T, u, u_2, u_3, u_4, u_5\}$ generate the code $C_{12}^{(2)}$.

Since we find up to permutation two codes, which are distinguished by the dimension of $C \cap C^{\perp}$, and since the dual of an extremal even formally self-dual code is again an extremal formally self-dual code with even weights, these codes are necessarily equivalent to their duals. The automorphism groups have been computed with Magma. □

Remark 6.1 *By "construction A", these codes construct non-isometric lattices which are* 4*-modular and extremal in the sense of H.-G. Quebbemann [21].*

References

[1] C. Bachoc, B. Venkov, *Modular forms, lattices and spherical designs* preprint

[2] A. Bonnecaze, B. Mourrain, P. Solé, *Jacobi polynomials, type II codes, and designs*, to appear in Designs, Codes and Cryptography

[3] A. Bonnecaze, E. Rains, P. Solé, *3-colored 5-designs and $\mathbb{Z}_4$-codes*, to appear in J. Stat. Inf. and Planning

[4] A. Bonnecaze, P. Udaya, P. Solé, *Strong 4-colored 5-designs*, preprint

[5] A.R. Calderbank, P. Delsarte, *On error-correcting codes and invariant linear forms* SIAM J. Disc. Math. **6.1** (1993), 1-23

[6] A.R. Calderbank, P. Delsarte, N.J.A. Sloane, *A strengthening of the Assmus-Mattson theorem* IEEE Trans. Inf. Th. **37** (1991), 1261-1268

[7] J. Conway, N.J.A. Sloane, "Sphere packings, Lattices and Groups", Springer-Verlag, 1988

[8] P. Delsarte, *Hahn polynomials, discrete harmonics and t-designs* SIAM J. Appl. Math. **34.1** (1978), 157-166

[9] Ph. Delsarte, J.M. Goethals, J.J. Seidel, *Spherical codes and designs* Geom. Dedicata **6** (1977), 363-388

[10] W. Ebeling, "Lattices and Codes" Vieweg Editor, 1994

[11] J. E. Fields, P. Gaborit, W. C. Huffman, V. Pless, *On the classification of extremal even formally self-dual codes*, preprint

[12] J. E. Fields, P. Gaborit, W. C. Huffman, V. Pless, *On the classification of extremal even formally self-dual codes of length* 20 *and* 22, to appear

[13] T.A. Gulliver, M. Harada, *Classification of extremal double circulant formally self-dual even codes* Designs, Codes and Cryptography **11** (1997), 25-35

[14] G. J. Janusz, *Overlap and covering polynomials with applications to designs and self-dual codes*, preprint

[15] S. Karlin, J. McGregor, *The Hahn polynomials, formulas and an application* Scripta Math. **26** (1961), 33-46

[16] G.T. Kennedy, V. Pless, *On designs and formally self-dual codes* Designs, Codes and Cryptography **4** (1994), 43-55

[17] F.J. MacWilliams, N.J.A. Sloane, "The theory of error-correcting codes", North-Holland Editor, 1977

[18] M. Ozeki, *On the notion of Jacobi polynomial for codes* Math. Proc. Camb. Phil. Soc. **121** (1997), 15-30

[19] V. Pless, *A classification of self-orthogonal codes over GF(2)*, Discrete Math. **3** (1972), 209-246

[20] V. Pless, N.J.A. Sloane, *On the classification and enumeration of self-dual codes*, J. Comb. Th. A **18** (1975), 313-335

[21] H.-G. Quebbemann, *A shadow identity and an application to isoduality* Abh. Math. Sem. Univ. Hamburg **68** (1998), 339-345

[22] E. Rains, N.J.A. Sloane, *Self-dual codes*, Handbook of Coding Theory, V. Pless and W. C. Huffman editors, North Holland, Amsterdam, 1998

[23] B. Venkov, *Réseaux et designs sphériques*, Notes de cours, rédigées par J. Martinet, to appear

[24] B. Venkov, *Even unimodular extremal lattices* Proc. Stecklov Inst. Math. **165** (1984), 47-52