DIMACS Series in Discrete Mathematics
and Theoretical Computer Science

Harmonic weight enumerators of nonbinary codes and MacWilliams identities

Christine Bachoc

Abstract. We define harmonic weight enumerators asociated to codes defined over a group alphabet F of size q. They generalize the classical Hamming weight enumerator and are associated to the decomposition of the space $L(F^n)$ under the action of the group $S_{q-1}^n \rtimes S_n$. They satisfy a MacWilliams type identity, which leads to relative invariant polynomials in the case of self-dual codes. Applications to the study of additive quaternary codes are developed.

1. Introduction

This paper extends the ideas and results of [**1**] to the case of non-binary linear codes. Let C be a linear code of length n over an alphabet F which is an abelian group of size q. We introduce polynomials which generalize the Hamming weight enumerator of the code, using "harmonic functions", after the work of C. Dunkl on harmonic analysis for the group $S_q^n \rtimes S_n$ and of H. Tarnanen, J. Aaltonen, J.-M. Goethals on the non-binary Johnson scheme (in the setting of association schemes).

We prove a MacWilliams type identity for these polynomials (Theorem 4.1). This identity involves an operator T acting on harmonic functions; in Section 5 we examine the case when T is homothetic. We prove that it corresponds to the binary, ternary and quaternary codes. In Section 6, we study more precisely the ternary and quaternary self-dual codes, because the harmonic weight enumerators are in these cases relative invariant polynomials. In Corollary 6.1, 6.2, we extend results due to P. Delsarte on the existence of generalized designs on the set of codewords of fixed Hamming weight of extremal codes. Section 7 is devoted to the application of this tool to the computation of intersection numbers. It makes use of the zonal functions associated to the subgroup $S_{q-1}^n \rtimes S_n$, which are expressed in terms of Krawtchouk and Hahn polynomials. We work out some examples in the case of even self-dual additive quaternary codes.

1991 *Mathematics Subject Classification.* Primary 94B05; Secondary 05B05, 05E35.

2. Group representation and the non-binary Johnson scheme

In this section we recall some notations and results on the Hamming and Johnson schemes previously settled by C. F. Dunkl ([**6**]) in the language of group representations and by Tarnanen, Aaltonen and Goethals ([**14**]) in terms of association schemes.

Let F be a finite alphabet of size $q \geq 2$. We denote by $F := \{a_0, \dots, a_{q-1}\}$ its elements. The group of permutations on q elements S_q acts on F by $a_i\sigma = a_{\sigma^{-1}(i)}$. We specify a series of subgroups of S_q denoted $\{1\} \subset \cdots \subset S_{q-1} \subset S_q$, where S_{q-i} is the subgroup of S_q fixing $a_0, \dots, a_{i-1}$ and is isomorphic to the group of permutations on $q - i$ elements.

Let $L(F)$ be the space of complex valued functions on F, equiped with the scalar product

$$< f, g >= \frac{1}{q} \sum_{x \in F} f(x)\overline{g(x)}.$$

It is endowed with the left action of S_q given by $(\sigma.f)(x) = f(x\sigma)$. The decomposition into irreducible S_q-modules of $L(F)$ is given by

$$L(F) = \mathbb{C}\mathbf{1} \perp L_1 \tag{1}$$

where $\mathbf{1}$ is the all-one function. We set $z_0 := \mathbf{1}$ and we define by induction an element z_i in L_i, and a subspace L_{i+1} of $L(F)$ such that the decomposition of L_i into S_{q-i}-irreducible modules, equals $\mathbb{C}z_i \perp L_{i+1}$, with trivial action on $\mathbb{C}z_i$. We normalize as in [**6**] the z_i by $(z_i, z_i) = 1/(q-1)$. Note that the z_i are determined from the above properties up to the multiplication by a complex number of module 1. The recursive computation of their values shows that they can be assumed to be real-valued, and hence are uniquely determined up to a sign. In particular, we fix $z_1(a_0) = 1$ and $z_1(a_i) = -1/(q-1)$ for $i \geq 1$. We shall make frequent use of the following properties: for $i \geq 2$, $z_i(a_0) = 0$ and, for $i \geq 1$, $\sum_{j=0}^{q-1} z_i(a_j) = 0$.

The functions z_i are explicitly realized in [**6**] as coordinate functions on F, seen as the regular simplex in $\mathbb{R}^{q-1}$.

Let $X := F^n$. The action of S_n on X given by

$$(x_1, \dots, x_n).\tau = (x_{\tau(1)}, \dots, x_{\tau(n)}),$$

combined with the action of S_q on F gives rise to a transitive action of the group $G := S_q^n \rtimes S_n$ on X. We denote by H the subgroup of G stabilizing $(a_0, \dots, a_0)$. It is isomorphic to $S_{q-1}^n \rtimes S_n$. Again we consider the space $L(X)$ together with the induced action of G (note that it is the representation of G induced by the trivial representation on H), and the hermitian product $< f, g >= \frac{1}{|X|} \sum_{x \in X} f(x)\overline{g(x)}$. Following [**6**], let, for all $u \in \{0, 1, \dots, q-1\}^n$, $z_u \in L(X)$ be defined by

$$z_u(x) := \prod_{i=1}^{n} z_{u_i}(x_i).$$

If $|u|$ denotes the number of non-zero coordinates of u, then we have $< z_u, z_v >= \delta_{u,v}(q-1)^{-|u|}$. From (1), the subspace P_m spanned by $\{z_u \mid |u| = m\}$ is G-invariant and

$$L(X) = \oplus_{m=0}^{n} P_m \tag{2}$$

is the decomposition of $L(X)$ into G-irreducible subspaces.

We shall make use of the description given in [**6**] of the decomposition of each P_m as H-modules. Moreover, the spaces P_m are linked to the Johnson schemes via the following: for $b \in X$, let $|b|$ be the Hamming weight i.e. the number of coordinates of b not equal to a_0, and let $S(b)$ be its support, i.e. the set of coordinates i such that $b_i \neq a_0$. Let

$$U_m := \{b \in X \mid |b| = m\}.$$

Note that the set U_m is one orbit under the action of H. Then, as an H-module, the space $L(U_m)$ is isomorphic to P_m via the map: $\rho : P_m \to L(U_m)$ defined by

$$\rho z_u(b) = \begin{cases} 0 & \text{if } S(b) \neq S(u) \\ z_u(b) & \text{if } S(b) = S(u) \end{cases}.$$

Let, for $0 \leq l \leq m$, $P_{m,l}$ be the subspace of P_m spanned by the z_u such that $u_i = 1$ for exactly $m - l$ coordinates, and let $L(U_m)_l$ be the image of $P_{m,l}$ by ρ. In the special case $q = 2$, of course we only consider the case $l = 0$ and $P_{m,0} = P_m$. From the fact that S_{q-1} acts trivially on z_1, the space $P_{m,l}$ is H-invariant. It is worth noticing that $P_{m,0}$ is the space of functions f such that $f(b)$ only depends on $S(b)$, and hence can be identified with the corresponding space P_m over $\mathbb{F}_2^n$.

If x_i denotes the function defined by $x_i(b) = z_1(b_i)$, the operator

$$d := \sum_{i=1}^{n} \frac{\partial}{\partial x_i}$$

commutes with the action of H and maps $P_{m,l}$ to $P_{m-1,l}$. Its adjoint operator is denoted by d^*. Then, the decomposition of P_m into irreducible H-submodules is given by ([**6**]):

$$P_m = \oplus_{l=0}^{m} \oplus_{k=l}^{\min(m,n+l-m)} P_{m,l,k} \tag{3}$$

where

$$P_{m,l,k} := (d^*)^{m-k}(P_{k,l} \cap \ker d). \tag{4}$$

In the case $q = 2$, there is only the summand $l = 0$.

We define an incidence relation between the elements of X by:

$$x \leq y \text{ if } x_i \neq a_0 \Rightarrow x_i = y_i.$$

An easy computation shows that the operator d induces via the isomorphism ρ an operator again denoted d:

$$\begin{aligned} L(U_m) &\to L(U_{m-1}) \\ x \to (df)(x) &= -\sum_{\substack{y \in U_m \\ x \leq y}} f(y). \end{aligned} \tag{5}$$

We take the following notations:

$$L(U_m)_l := \rho(P_{m,l})$$

and

$$L(U_m)_{(k,l)} := \rho(P_{m,l,k}) = (d^*)^{m-k}(L(U_k)_l \cap \ker d)$$

so that

$$L(U_m) = \bigoplus_{L_m} L(U_m)_{(k,l)} \tag{6}$$

where

$$L_m := \{(k,l) \mid 0 \leq l \leq k \leq \min(m, n+l-m)\}. \tag{7}$$

The general notion of a design in an association scheme has, in the case of the non-binary Johnson scheme, the following combinatorial significance:

PROPOSITION 2.1. *Let $\mathcal{B} \subset U_m$ and let $\beta := \sum_{B\in\mathcal{B}} B \in L(U_m)$ be the characteristic function of $\mathcal{B}$. The following conditions are equivalent:*

1. *For all $T \in U_t$, $\mathrm{card}\{B \in \mathcal{B} \mid T \leq B\}$ only depends on t.*
2. *β is orthogonal to $L(U_m)_{(k,l)}$ for all $(k,l) \in L_m$, $k \leq t$, $(l,k) \neq (0,0)$.*
3. *$\sum_{B\in\mathcal{B}} f(B) = 0$ for all $(k,l) \in L_m$, $k \leq t$, $(l,k) \neq (0,0)$.*

PROOF. This is already proved in [**13**]. Note first that, in the decomposition (6), $L(U_m)_{(0,0)} = \mathbb{C}.\mathbf{1}$ is the one-dimensional subspace spanned by the all-one function on U_m. Let τ be the characteristic function of an element $T \in U_t$. Clearly, from the above interpretation of $d : L(U_m) \to L(U_{m-1})$, the property required in 1) is equivalent to ask that $< \beta, (d^*)^{m-t}\tau >_{L(U_m)}$ only depends on t. But $< (d^*)^{m-t}\tau, \mathbf{1} >_{L(U_m)} = \lambda(t) < \mathbf{1}, \mathbf{1} >_{L(U_m)}$ only depends on t since it counts the number of $x \in U_m$ such that $T \leq x$. From the decomposition (6),

$$\tau = \sum_{\substack{(k,l)\in L_m, k\leq t\\(k,l)\neq(0,0)}} \tau_{k,l} + \lambda(t)\mathbf{1} \tag{8}$$

where $\tau_{k,l} \in L(U_m)_{(k,l)}$. This shows the equivalence of 1) and 2). Point 3) follows from $< \beta, f >_{L(U_m)} = 1/|U_m| \sum_{B\in\mathcal{B}} f(B)$. □

REMARK 2.1. *Note that this is also the notion of "generalized combinatorial design" as introduced by Delsarte in [**5**]. The weaker property that the supports of the blocks hold a t-design in the classical sense is equivalent to the orthogonality of β with the subspaces $L(U_m)_{(k,0)}$ for $k \leq t$ (since, as was already mentionned, $P_{k,0}$ is the space of functions f such that $f(B)$ only depends on $S(B)$).*

3. The alphabet F is a group

In this section we assume that the alphabet F has a structure of an abelian group $(F, +)$, for which $a_0 = 0$. We assume that F is endowed with a non degenerated symmetric bilinear map

$$\begin{aligned} F \times F &\to (\mathbb{C}^*, \times) \\ (x,y) &\to (x,y) \end{aligned} \tag{9}$$

The choice of such a duality is equivalent to a specification of an isomorphism between F and its group of characters, given by $x \to (.,x)$. In particular, we shall make frequent use of the orthogonality relations between the characters of F.

The space $X = F^n$ is endowed with $(x,y) := \prod_{i=1}^n (x_i, y_i)$. If C is a linear code in X, i.e. a subgroup of X, $C^\perp$ denotes its orthogonal code with respect to $(,)$:

$$C^\perp := \{u \in X \mid (u,v) = 1 \ \forall\ v \in C\} \tag{10}$$

We define another operator on $L(U_m)$ which will be of major importance in the generalized MacWilliams formulas:

Definition 3.1. *Let $f \in L(U_m)$. Let Tf be defined, for all $u \in U_m$, by*

$$Tf(u) := \sum_{\substack{b \in U_m \\ S(b)=S(u)}} (u,b) f(b) \tag{11}$$

Note that the operator T depends on the choice of the duality $(,)$. We denote by $\overline{T}$ the operator corresponding to the conjugate duality $\overline{(x,y)}$.

Proposition 3.1. *The following properties hold for the operator T:*

1. *$T\mathbf{1} = (q-1)z_1$, $Tz_1 = -z_1$, and, for $i \geq 2$, Tz_i is a linear combination of $z_2, \ldots, z_{q-1}$.*
2. *If $f = \rho z_u$, $Tf(v) = \prod_{i \in S(u)} Tz_{u_i}(v_i)$.*
3. *The operator T is linear, and maps $L(U_m)_l$ into itself injectively.*
4. *For all $f, g \in L(U_m)$, $< Tf, g > = < f, \overline{T}g >$.*
5. *For all $f \in L(U_m)$, $dTf = -Tdf$ and $d^*Tf = -Td^*f$.*

Proof. We first prove 4.

$$\begin{aligned} < Tf, g > &= \frac{1}{|U_m|} \sum_{u \in U_m} (Tf)(u)\overline{g(u)} \\ &= \frac{1}{|U_m|} \sum_{u \in U_m} (\sum_{\substack{b \in U_m \\ S(b)=S(u)}} (u,b) f(b)) \overline{g(u)} \\ &= \frac{1}{|U_m|} \sum_{b \in U_m} f(b) (\sum_{\substack{u \in U_m \\ S(u)=S(b)}} (u,b)\overline{g(u)}) \\ &= < f, \overline{T}g > . \end{aligned} \tag{12}$$

In order to prove 1., we compute $Tz_1(u)$. From the orthogonality relations, $Tz_1(u) = \sum_{b \neq a_0} (u,b) z_1(b) = -1/(q-1) \sum_{b \neq a_0} (u,b) = -z_1(u)$. The computation of $T\mathbf{1}$ goes the same. The assertion on Tz_i for $i \geq 2$ follows from 4.

Let us prove 2.: we assume $f = \rho z_u$. Let $v \in U_m$ with $S(v) = S(u)$. Then $f(v) = \prod_{i \in S(u)} z_{u_i}(v_i)$ and

$$\begin{aligned}
Tf(v) &= \sum_{\substack{b\in U_m\\ S(b)=S(u)}} (v,b)f(b)\\
&= \sum_{b_i\neq a_0}\prod_{i\in S(u)} (v_i,b_i)z_{u_i}(v_i)\\
&= \prod_{i\in S(u)} \Big(\sum_{\lambda\neq a_0} (v_i,\lambda)z_{u_i}(v_i)\Big)\\
&= \prod_{i\in S(u)} Tz_{u_i}(v_i)
\end{aligned} \tag{13}$$

which proves 2. From 1. and 2., it follows that Tf is a linear combination of some ρz_w, where the number of coordinates of w which are not equal to 0, respectively which are equal to 1, is the same as for u. Hence T maps $L(U_m)_l$ into itself.

Assume $Tf = 0$. Let S be a fixed set of m coordinates. Since for all $u \in U_m$, such that $S(u) = S$, $Tf(u) = 0$, the following system of linear equations holds:

$$\sum_{\substack{b\in U_m\\ S(b)=S(u)}} (u,b)f(b) = 0 \text{ for all } u \in U_m \tag{14}$$

We only have to prove that the matrix of this linear system is invertible. But this matrix is the $(q-1)^m \times (q-1)^m$-symetric matrix $((u,v))_{u,v\in U_m}$; it is a submatrix of the matrix $((u,v))_{u,v\in F^m}$ which is invertible since the characters $(.,v)$ span $L(F^m)$, and hence it has full rank.

We prove the equality $d^*Tf = Td^*f$; a similar proof can be given for d. Let $u \in U_{m+1}$.

$$\begin{aligned}
Td^*f(u) &= \sum_{\substack{c\in U_{m+1}\\ S(c)=S(u)}} (u,c)d^*f(c)\\
&= -\sum_{\substack{c\in U_{m+1}\\ S(c)=S(u)}} (u,c)\sum_{\substack{b\in U_m\\ b\leq c}} f(b)\\
&= -\sum_{\substack{b\in U_m\\ S(b)\subset S(u)}} \Big(\sum_{\substack{c\in U_{m+1}\\ S(c)=S(b)\\ b\leq c}} (u,c)\Big)f(b)
\end{aligned} \tag{15}$$

For a fixed $b \in U_m$ such that $S(b) \subset S(u)$, let i_b be the index in $S(u)$ but not in $S(b)$. Then, $\sum_{\substack{c\in U_{m+1}\\ S(c)=S(b)\\ b\leq c}} (u,c) = (u,b)\sum_{\substack{\lambda\in F\\ \lambda\neq a_0}} (u_{i_b},\lambda) = -(u,b)$, so

$$Td^*f(u) = \sum_{\substack{b\in U_m\\ S(b)\subset S(u)}} (u,b)f(b). \tag{16}$$

But, for a fixed $b \in U_m$ with $S(b) \subset S(u)$, we have $(u,b) = (v,b)$ where v is the only element in F^n such that $v \leq u$ and $S(v) = S(b)$. Hence

$$Td^*f(u) = \sum_{\substack{v\in U_m\\ v\leq u}} \Big(\sum_{\substack{b\in U_m\\ S(b)=S(v)}} (v,b)f(b)\Big) = -d^*Tf(u). \tag{17}$$

□

REMARK 3.1. *The operator T doesn't in general commute with the action of H. We discuss this possibility in section 5.*

In the case of the binary alphabet $F = \mathbb{F}_2$, and more generaly if $l = 0$, meaning that $f(u)$ only depends on $S(u)$, one easily sees that $Tf(u) = (-1)^{|u|}f(u)$.

4. A MacWilliams type identity

Let C be a linear code in F^n and let $C^\perp$ be its orthogonal code as defined in previous section. We are going to define harmonic weight enumerators associated to C and to prove a MacWilliams type identity for them.

Let $f \in L(U_k)_l \cap \ker d$. We set, for all $x \in X = F^n$,

$$D^*f(x) := \sum_{\substack{u\in U_k\\ u\leq x}} f(u) \tag{18}$$

Note that, if $|x| \geq k$, $D^*f(x) = (-1)^{|x|-k}\frac{(d^*)^{|x|-k}}{(|x|-k)!}f(x)$. If $|x| < k$, $D^*f(x) = 0$.

DEFINITION 4.1. *Let $f \in L(U_k)_l \cap \ker d$. The harmonic weight enumerator associated to C and f is*

$$Z_{C,f}(X,Y) := \sum_{u\in C} D^*f(u)X^{n-|u|-k+l}Y^{|u|-k}$$

REMARK 4.1. *Note that it is not clear yet that $Z_{C,f}$ is a polynomial. It will derive from Proposition 4.1. In the binary case, $l = 0$ is the only possibility, and $Z_{C,f}$ coincides with the notion introduced in* [**1**]. *The slightly more general case $l = 0$ over $\mathbb{F}_q$ is actually treated in* [**12**].

The following proposition is the key property needed to prove that $Z_{C,f}$ is a polynomial satisfying a MacWilliams type transformation formula. Its proof is postponed to Subsection 4.1.

PROPOSITION 4.1. *Let $f \in L(U_k)_l \cap \ker d$ and let $u \in X = F^n$.*
For all $i = 0, \ldots, k$,

$$\sum_{\substack{b\in U_k\\ |S(b)\cap S(u)|=k-i}} (u,b)f(b) = (q-1)^i\binom{k-l}{i}D^*Tf(u) \tag{19}$$

The main property of the $Z_{C,f}$ is the following:

THEOREM 4.1. *Let $f \in L(U_k)_l \cap \ker d$ and let C be a linear subcode of F^n. Let $C^\perp$ be its orthogonal code. Then, $Z_{C,f}(X,Y)$ is a homogeneous polynomial of degree $n-2k+l$, and*

$$Z_{C^\perp,f}(X,Y) = \frac{1}{|C|}q^{k-l}Z_{C,Tf}(X+(q-1)Y, X-Y) \tag{20}$$

4.1. Proof of Proposition 4.1. We proceed by induction on i. The case $i=0$ is the identity

$$\sum_{\substack{b\in U_k\\ S(b)\subset S(u)}} (u,b)f(b) = D^*Tf(u)$$

which derives from (16) and (17) by iteration of d^*. Let us now assume the identity for all $j\leq i-1$. From the fact that $f\in\ker d$ and from $Tdf=-dTf$, we know that $Tf\in\ker d$. Let $y\in U_{k-i}$. We have

$$\sum_{\substack{t\in U_k\\ y\leq t}} Tf(t)=0 \tag{21}$$

which means

$$\sum_{\substack{t\in U_k\\ y\leq t}}\sum_{\substack{b\in U_k\\ S(b)=S(t)}} (t,b)f(b)=0 \tag{22}$$

We sum up these equations over the set of $y\leq u$, with $y\in U_{k-i}$. Hence all the $b\in U_k$ such that $|S(b)\cap S(u)|\geq k-i$ will contribute in the sum. We rearrange the sum over j such that $|S(b)\cap S(u)|=k-j$. We set

$$S(u,j) := \{b\in U_k \mid |S(b)\cap S(u)| = k-j\} \tag{23}$$

and obtain:

$$\sum_{j=0}^{i}\sum_{b\in S(u,j)} A_b f(b)=0 \tag{24}$$

where

$$A_b := \sum_{\substack{y\in U_{k-i}\\ y\leq u\\ S(y)\subset S(u)\cap S(b)}}\ \sum_{\substack{t\in U_k\\ S(t)=S(b)\\ y\leq t}} (b,t). \tag{25}$$

If we denote by $b_{S(y)}$ the element of F^n which is equal to b over $S(y)$ and to a_0 outside, we have

$$\begin{aligned}\sum_{\substack{t\in U_k\\ S(t)=S(b)\\ y\leq t}} (b,t) =&(b_{S(y)},u)\sum_{t_s\neq a_0}\prod_{s\in S(b)\setminus S(y)}(b_s,t_s)\\ =&(b_{S(y)},u)\prod_{s\in S(b)\setminus S(y)}\Big(\sum_{\lambda\neq a_o}(b_s,\lambda)\Big)\\ =&(b_{S(y)},u)(-1)^i\end{aligned} \tag{26}$$

and we are left with, if $S_{k-i}:=S(y)$ runs over subsets of size $k-i$,

$$A_b = (-1)^i \sum_{S_{k-i} \subset S(b) \cap S(u)} (b_{S_{k-i}}, u). \tag{27}$$

LEMMA 4.1. *If $f \in L(U_k)_l$, for all $u \in F^n$,*

$$\sum_{b \in S(u,j)} A_b f(b) = (-1)^j \binom{k-l-j}{i-j} (q-1)^{i-j} \sum_{b \in S(u,j)} (b,u) f(b) \tag{28}$$

PROOF. The equality (28) is linear in f, so it is enough to verify it for $f = \rho z_v$. The fact that $f \in L(U_k)_l$ means that the number of non zero coordinates of v is k and that the number of coordinates of v equal to 1 is $k-l$. Let $S := S(v)$; from the definition of ρz_v, the only b having a non zero contribution in the left or right handsides are the ones with $S(b) = S$. Hence, if $|S(u) \cap S| \neq k-j$, both sides are equal to 0, so we assume that $|S(u) \cap S| = k-j$. Then, if L denotes the left handside of (28), and from the expression (27) for A_b,

$$\begin{aligned} L &= (-1)^i \sum_{\substack{b \in U_k \\ S(b)=S}} \sum_{S_{k-i} \subset S \cap S(u)} \prod_{s \in S_{k-i}} (b_s, u_s) \prod_{s \in S} z_{v_s}(b_s) \\ &= (-1)^i \sum_{S_{k-i} \subset S \cap S(u)} \sum_{\substack{b \in U_k \\ S(b)=S}} \prod_{s \in S_{k-i}} (b_s, u_s) z_{v_s}(b_s) \prod_{s \in S \setminus S_{k-i}} z_{v_s}(b_s) \\ &= (-1)^i \sum_{S_{k-i} \subset S \cap S(u)} \prod_{s \in S_{k-i}} \Big(\sum_{\lambda \neq a_0} (\lambda, u_s) z_{v_s}(\lambda) \Big) \prod_{s \in S \setminus S_{k-i}} \Big(\sum_{\lambda \neq a_0} z_{v_s}(\lambda) \Big). \end{aligned} \tag{29}$$

But $\sum_{\lambda \neq a_0} z_{v_s}(\lambda) = -z_{v_s}(a_0)$ since $s \in S$, and $z_{v_s}(a_0) = 1$ or 0, respectively if $v_s = 1$ or $v_s \geq 2$. Hence the only subsets S_{k-i} having a non zero contribution are the ones for which $S \setminus S_{k-i} \subset \{s \mid v_s = 1\}$. Such subsets exist only if $v_s = 1$ outside of $S(u)$, and if $l \leq k-i$ (since S_{k-i} must cover the coordinates s of v with $v_s \neq 1$). Moreover, in that case, since $v_s = 1$ outside of S_{k-i}, since $Tz_1 = -z_1$ and $z_1(\lambda) = -1/(q-1)$ if $\lambda \neq a_0$,

$$\prod_{s \in S_{k-i}} \Big(\sum_{\lambda \neq a_0} (\lambda, u_s) z_{v_s}(\lambda) \Big) = \prod_{s \in S_{k-i}} T z_{v_s}(u_s) = (q-1)^{i-j} \prod_{s \in S \cap S(u)} T z_{v_s}(u_s).$$

One sees easily that the number of S_{k-i} with such a contribution is equal to $\binom{k-l-j}{i-j}$. Finally, L equals 0 if $v_s \neq 1$ on $S \setminus S(u)$ and equals $\binom{k-l-j}{i}(q-1)^{i-j} \prod_{s \in S \cap S(u)} T z_{v_s}(u_s)$ otherwise. Since $Tz_1(a_0) = -z_1(a_0) = -1$ while, for $s \geq 2$, $Tz_s(a_0) = 0$, in any case,

$$L = (-1)^j \binom{k-l-j}{i-j} (q-1)^{i-j} \prod_{s \in S} T z_{v_s}(u_s).$$

The right handside of (28) is easily computed:

$$\begin{aligned}\sum_{b\in S(u,j)}(b,u)f(b) &= \sum_{\substack{b\in U_k\\ S(b)=S}}\prod_{s\in S}(b_s,u_s)z_{v_s}(b_s)\\ &= \prod_{s\in S}\Big(\sum_{\lambda\neq a_0}(\lambda,u_s)z_{v_s}(\lambda)\Big)\\ &= \prod_{s\in S}Tz_{v_s}(u_s).\end{aligned}\tag{30}$$

□

We return to the proof of Proposition 4.1. Equation (24) becomes, applying Lemma 4.1,

$$\sum_{j=0}^{i}(-1)^j\binom{k-l-j}{i-j}(q-1)^{i-j}\sum_{b\in S(u,j)}(b,u)f(b)=0\tag{31}$$

and, applying the induction hypothesis to $j\leq i-1$,

$$(-1)^i\sum_{b\in S(u,i)}(b,u)f(b)=-(q-1)^i\sum_{j=0}^{i-1}(-1)^j\binom{k-l-j}{i-j}\binom{k-l}{j}D^*Tf(u).\tag{32}$$

From $\binom{k-l-j}{i-j}\binom{k-l}{j}=\binom{k-l}{i}\binom{i}{j}$, we get

$$\begin{aligned}(-1)^i\sum_{b\in S(u,i)}(b,u)f(b) &= -(q-1)^i\binom{k-l}{i}D^*Tf(u)\sum_{j=0}^{i-1}(-1)^j\binom{i}{j}\\ &= (q-1)^i\binom{k-l}{i}D^*Tf(u)(-1)^i\end{aligned}\tag{33}$$

which is the expression of Proposition 4.1.

4.2. Proof of Theorem 4.1. We first prove that $Z_{C,f}(X,Y)$ is a polynomial. If $u\in C$ satisfies $n-|u|-k+l<0$, let i be an integer with $n-|u|<i\leq k-l$. Equation (19) of Proposition 4.1 proves that $D^*Tf(u)=0$, since no $b\in U_k$ with $|S(b)\cap S(u)|=k-i$ can exist. We conclude from the property $D^*Tf=-TD^*f$ and from the injectivity of T (see Proposition 3.1).

Now we prove the transformation formula (20). Therefore, as in [**1**], we compute the Fourier transform (over F^n) of

$$\Phi(u):=D^*f(u)X^{n-|u|-k+l}Y^{|u|-k}\tag{34}$$

which is

$$\hat{\Phi}(u):=\sum_{v\in F^n}(u,v)\Phi(v).\tag{35}$$

The formula will then derive directly from the Poisson summation formula:

$$\sum_{u\in C^{\perp}} \Phi(u) = \frac{1}{|C|}\sum_{v\in C} \hat{\Phi}(v). \tag{36}$$

Just like in the binary case [**1**], we first consider the case $f=\delta_b$ where δ_b is defined by $\delta_b(u)=1$ if $u=b$ and 0 if $u\neq b$. We denote by $u_{\overline{S(b)}}$ the element of F^n which is equal to u on the complementary set of $S(b)$ and to a_0 elsewhere.

Lemma 4.2. *Let $f=\delta_b\in L(U_k)$. Then*

$$\hat{\Phi}(u) = (u,b)X^{-k+l}(X+(q-1)Y)^{n-k-|u_{\overline{S(b)}}|}(X-Y)^{|u_{\overline{S(b)}}|} \tag{37}$$

Proof. Since $D^*\delta_b(u)=1$ if $b\leq u$ and 0 otherwise,

$$\hat{\Phi}(u) = \sum_{\substack{v\in F^n\\ b\leq v}} (u,v)X^{n-|v|-k+l}Y^{|v|-k}. \tag{38}$$

We can write $v=b+v'$, where $S(v')$ is the complementary set of $S(b)$. Hence $(u,v)=(u,b)(u,v')$ and v' can be considered to run over F^{n-k}.

$$\begin{aligned}\hat{\Phi}(u) &= (u,b)\sum_{v'\in F^{n-k}} (u,v')X^{n-2k+l-|v'|}Y^{|v'|}\\ &= (u,b)X^{-k+l}(X+(q-1)Y)^{n-k-|u_{\overline{S(b)}}|}(X-Y)^{|u_{\overline{S(b)}}|}\end{aligned} \tag{39}$$

where the last equality is the usual computation of the Fourier transform of the function $x\to X^{n-k-|x|}Y^{|x|}$ over F^{n-k}.

□

Lemma 4.3. *Let $f\in L(U_k)_l\cap \ker d$.*

$$\hat{\Phi}(u) = q^{k-l}D^*Tf(u)(X+(q-1)Y)^{n-|u|-k+l}(X-Y)^{|u|-k} \tag{40}$$

Proof. Since $f=\sum_{b\in U_k} f(b)\delta_b$ and from (37),

$$\hat{\Phi}(u) = X^{-k+l}\sum_{b\in U_k}(u,b)f(b)(X+(q-1)Y)^{n-k-|u_{\overline{S(b)}}|}(X-Y)^{|u_{\overline{S(b)}}|}. \tag{41}$$

Then $|u_{\overline{S(b)}}| = |u|-|S(u)\cap S(b)|$; we set $|S(u)\cap S(b)|=k-i$ and sum over $i\in\{0\dots k\}$. We get

$$\hat{\Phi}(u) = X^{-k+l}(X+(q-1)Y)^{n-k+l-|u|}(X-Y)^{|u|-k}\Psi(u) \tag{42}$$

where

$$\Psi(u) := \sum_{i=0}^{k}\Big(\sum_{\substack{b\in U_k\\ |S(b)\cap S(u)|=k-i}} (u,b)f(b)\Big)(X+(q-1)Y)^{k-l-i}(X-Y)^{i} \tag{43}$$

which becomes, by Proposition 4.1,

$$
\begin{aligned}
\Psi(u) &= \sum_{i=0}^{k} (q-1)^i \binom{k-l}{i} D^*Tf(u)(X+(q-1)Y)^{k-l-i}(X-Y)^i \\
&= D^*Tf(u) \sum_{i=0}^{k-l} \binom{k-l}{i} (X+(q-1)Y)^{k-l-i}((q-1)(X-Y))^i \qquad (44)\\
&= D^*Tf(u)(X+(q-1)Y+(q-1)(X-Y))^{k-l} \\
&= D^*Tf(u)(qX)^{k-l}.
\end{aligned}
$$

Replacing (44) in (42), we obtain (40).

□

5. The operator T

We study in this section the possibility for the operator T to be homothetic on the spaces $L(U_k)_l \cap \ker d$. This case is especially interesting because Theorem 4.1 can in that case be read as a linear invariance property for a certain polynomial (see next section).

PROPOSITION 5.1. *The following statements are equivalent:*

- *For all k, l, there exists $\lambda_{k,l} \in \mathbb{C}$ such that, for all $f \in L(U_k)_l \cap \ker d$, $Tf = \lambda_{k,l} f$.*
- *$F = \mathbb{F}_2, \mathbb{F}_3$ and $(x,y) = \chi(xy)$, where χ is a non-trivial character of F, or $F = \mathbb{F}_4$ and $(x,y) = \chi(trace(xy^2))$ and χ is the non-trivial character of $\mathbb{F}_2$.*

If $F = \mathbb{F}_2, \mathbb{F}_4$, $\lambda_{k,l} = (-1)^{k-l}2^l$, and, if $F = \mathbb{F}_3$, $\lambda_{k,l} = (-1)^{k-l}(\sqrt{-3})^l$.

REMARK 5.1. *In terms of coding theory, the cases of the proposition are the binary, ternary, and quaternary additive codes, with the terminology of* [**11**]. *We have kept the usual notation for F, although the field structure has no importance here. In particular, the quaternary additive codes are the same as the Kleinian codes studied in* [**9**].

PROOF. From [**6**], we know that $L(U_k)_l \cap \ker d$ is a H-irreducible module. Hence, T is homothetic over $L(U_k)_l \cap \ker d$ if and only if T commutes with the action of H, i.e. if and only if $T(h.f) = h.T(f)$ for all $h \in H$, $f \in L(U_k)_l \cap \ker d$. If this is true for all k, l, since we have already seen that $Td^* = -d^*T$, and from the decomposition (6), it must be true for all $f \in L(U_k)$. The space $L(U_k)$ is generated by $\{\delta_b, b \in U_k\}$. We have $h.\delta_b = \delta_{bh^{-1}}$, and $T\delta_b(u) = (b,u)$ if $S(u) = S(b)$, and 0 otherwise. Hence it turns out that T commutes with H over $L(U_k)$ if and only if $(u,v) = (uh, vh)$ for all $h \in H$ and $u, v \in U_k$ with $S(u) = S(v)$. Since the permutation on the coordinates of the elements of F^n has no incidence on the duality (because we assume $(u,v) = \prod_i (u_i, v_i)$), we are left with the condition that $(,)$ must be constant on the orbits of $F \times F$ under the action of S_{q-1}, which means that $\alpha := (x,x)$ is independant of the choice of $x \neq 0$ in F, and $\beta := (x,y)$ is independant of the choice of $x \neq y \neq 0$ in F. Hence, $(,)$ takes at most three values: $\{1, \alpha, \beta\}$. Since they form a subgroup of $\mathbb{C}^*$ of order $d = 2, 3$, since $dF = 0$ and since, for each $x \neq 0$, the kernel of $(.,x)$ has order q/d, one easily sees that the only possibilities left are the ones listed in the proposition.

We now compute $\lambda_{k,l}$. We have already seen that $Tz_1 = -z_1$. If $i \geq 2$, $Tz_i(x) = \sum_{y \neq a_0} (x,y) z_i(y) = \alpha z_i(x) + \beta \sum_{y \neq a_0, x} z_i(y)$. But $\sum_{y \neq a_0} z_i(y) = 0$, so

$Tz_i(x) = (\alpha-\beta)z_i(x)$. Hence, if $f = \rho z_u \in L(U_k)_l$, from property 2. of Proposition 3.1, $Tf = (-1)^{k-l}(\alpha-\beta)^l f$. In the cases $F = \mathbb{F}_2, \mathbb{F}_4$, $\alpha - \beta = 1-(-1) = 2$, and in the case $F = \mathbb{F}_3$, $\alpha - \beta = \pm(j - j^2) = \pm i\sqrt{3}$ where j is a cubique root of 1.

□

REMARK 5.2. *In the ternary case, there are two conjugate choices for the duality* $(,)$. *Since* $Tf(-u) = \overline{T}f(u)$, *we have* $Z_{C,Tf} = Z_{C,(Tf+\overline{T}f)/2}$. *The eigenvalue of* $\overline{T}$ *over* $L(U_k)_l$ *is the conjugate of the one associated to* T*; but, we have seen that* $\lambda_{k,l}$ *has a trivial real part in the case* $l \equiv 1 \mod 2$. *Hence, in this case,* $Z_{C,Tf} = 0$, *and so* $Z_{C,f} = 0$. *Note that it fits with the fact that the set* $C^\perp$ *only depends on the choice of the duality up to conjugation.*

6. Applications to self-dual codes

In this section, we consider the case of self-dual ternary and additive quaternary codes. The binary case was previously studied in [**1**]. In these cases, Theorem 4.1 shows that the polynomials $Z_{C,f}$ are relative invariants for the group of transformation acting on the Hamming weight enumerator.

6.1. Ternary self-dual codes. Let $M = \frac{1}{\sqrt{3}}\left(\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right)$ and $D = \left(\begin{smallmatrix} 1 & 0 \\ 0 & j \end{smallmatrix}\right)$ where $j = e^{2i\pi/3}$. Let G_3 be the group generated by M and D. It is well-known that, if C is a self-dual ternary code, then its weight enumerator W_C is invariant under G_3, and hence belongs to its algebra of invariants $\mathcal{I}_{G_3}$, which is the polynomial ring in the polynomials $g_4 := x^4 + 8xy^3$, $g_{12} := y^3(x^3 - y^3)^3$ (see [**11**]).

We define the following characters $\psi_{u,v}$ of the group G_3:

$$\psi_{u,v}(M) = (-1)^u \quad \psi_{u,v}(D) = j^v \tag{45}$$

and we denote by $\mathcal{I}_{G_3,\psi_{u,v}}$ the space of relative invariants:

$$\mathcal{I}_{G_3,\psi_{u,v}} := \{P(x,y) \in \mathbb{C}[x,y] \mid P.M = \psi_{u,v}(M)P \text{ for all } M \in G_3\}. \tag{46}$$

The following polynomials are relative invariants, as one can check easily:

$$\begin{aligned} p_4 &= y(x^3 - y^3) \in \mathcal{I}_{G_3,\psi_{0,1}} \\ p_6 &= x^6 - 20x^3y^3 - 8y^6 \in \mathcal{I}_{G_3,\psi_{1,0}} \end{aligned} \tag{47}$$

LEMMA 6.1. *The spaces of relative invariants* $\mathcal{I}_{G_3,\psi_{u,v}}$ *are free modules over* $\mathcal{I}_{G_3}$. *More precisely:*

- $\mathcal{I}_{G_3,\psi_{0,1}} = p_4\mathbb{C}[g_4, g_{12}]$
- $\mathcal{I}_{G_3,\psi_{0,2}} = p_4^2\mathbb{C}[g_4, g_{12}]$
- $\mathcal{I}_{G_3,\psi_{1,0}} = p_6\mathbb{C}[g_4, g_{12}]$
- $\mathcal{I}_{G_3,\psi_{1,1}} = p_4p_6\mathbb{C}[g_4, g_{12}]$
- $\mathcal{I}_{G_3,\psi_{1,2}} = p_4^2p_6\mathbb{C}[g_4, g_{12}]$

PROOF. It follows easily from the computation of the Molien series of the corresponding spaces (see [**11**] and [**1**] for examples of such computations). □

PROPOSITION 6.1. *Let* C *be a self-dual ternary code of length* n. *Let* f *belong to* $L(U_k)_l \cap \ker d$. *If* $l \equiv 1 \mod 2$, $Z_{C,f} = 0$. *If* $l \equiv 0 \mod 2$, *let* $u \in \{0,1\}$ *be equal to* $k + l/2$ *modulo* 2, *and let* $v \in \{0,1,2\}$ *be equal to* $-k$ *modulo* 3. *Then*

$$Z_{C,f} \in \mathcal{I}_{G_3,\psi_{u,v}}.$$

PROOF. Straightforward from Theorem 4.1, Remark 5.2 and Proposition 5.1. □

In the special case of extremal codes, we can derive from previous proposition that $Z_{C,f} = 0$ for certain values of (k, l). We briefly recall what an extremal code is (see [**11**]): if C is a self-dual ternary code of length n, then n is a multiple of 4. Write $n = 12q + 4r$ with $r = 0, 1, 2$. Then the fact that W_C belongs to $\mathcal{I}_{G_3}$ shows that the minimum weight $w(C)$ of C satisfies

$$w(C) \leq 3q + 3. \tag{48}$$

A code meeting this bound is called extremal. Its weight enumerator is then uniquely determined.

COROLLARY 6.1. *Let C be an extremal self-dual ternary code of length $n = 12q + 4r$. Let $f \in L(U_k)_l \cap \ker d$. Then $Z_{C,f} = 0$ when $l \equiv 1 \mod 2$ from Remark 5.2, but also in the following cases:*

- *If $r = 0$: for $k = 1, 2, 3$ and all $l \leq k$, and for $(k, l) = (4, 0), (4, 2), (5, 0), (5, 4), (6, 2), (7, 0)$.*
- *If $r = 1$: for $k = 1, 2$ and all $l \leq k$, and for $(k, l) = (3, 0), (4, 2), (5, 0)$.*
- *If $r = 2$: for $(k, l) = (1, 0), (2, 2), (3, 0)$.*

REMARK 6.1. *In view of Proposition 2.1, the property $Z_{C,f} = 0$ is related to the fact that the set of codewords of fixed Hamming weight form a design. We recover here results already known from* [**5**] *and* [**3**]*, namely that extremal ternary self-dual codes hold generalized 3-designs and classical $\{1, 2, 3, 4, 5, 7\}$-designs when $r = 0$ (respectively for the corresponding weaker results when $r = 1, 2$), which were derived from generalized Assmus-Mattson theorems. We obtain here some additional properties; in particular it is worth noticing that, for instance in the case $r = 0$, the generalized 3-designs are actually nearly 4-designs since the only property missing is orthogonality with $L(U_4)_4 \cap \ker d$.*

6.2. Even quaternary additive self-dual codes. Here we follow the same line as for ternary codes, so we omit the proofs and some comments since they are completely similar. Let $M = \frac{1}{2}\begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix}$ and $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Let G_4 be the group generated by M and D. If C is a self-dual even quaternary additive code, then its weight enumerator W_C is invariant under G_4, and hence belongs to its algebra of invariants $\mathcal{I}_{G_4}$, which is the polynomial ring in the polynomials $h_2 := x^2 + 3y^2$, $h_6 := y^2(x^2 - y^2)^2$ (see [**11**]).

We define the following characters $\psi_{u,v}$ of the group G_4:

$$\psi_{u,v}(M) = (-1)^u \quad \psi_{u,v}(D) = (-1)^v \tag{49}$$

and we denote by $\mathcal{I}_{G_4,\psi_{u,v}}$ the space of relative invariants. The following polynomials are relative invariants, as one can check easily:

$$\begin{aligned} q_3 &= y(x^2 - y^2) \in \mathcal{I}_{G_4,\psi_{0,1}} \\ r_3 &= x^3 - 9xy^2 \in \mathcal{I}_{G_4,\psi_{1,0}} \end{aligned} \tag{50}$$

LEMMA 6.2. *The spaces of relative invariants $\mathcal{I}_{G_4,\psi_{u,v}}$ are free modules over $\mathcal{I}_{G_4}$. More precisely:*

- $\mathcal{I}_{G_4,\psi_{0,1}} = q_3\mathbb{C}[h_2, h_6]$
- $\mathcal{I}_{G_4,\psi_{1,0}} = r_3\mathbb{C}[h_2, h_6]$
- $\mathcal{I}_{G_4,\psi_{1,1}} = q_3 r_3\mathbb{C}[h_2, h_6]$

PROPOSITION 6.2. *Let C be a self-dual even quaternary additive code of length n. Let $f \in L(U_k)_l \cap \ker d$. Let $u \in \{0,1\}$ be equal to $k-l$ modulo 2, and let $v \in \{0,1\}$ be equal to k modulo 2. Then*

$$Z_{C,f} \in \mathcal{I}_{G_4,\psi_{u,v}}.$$

Here the extremal codes have weight $w(C) = 2q+2$, where $n = 6q+2r$.

COROLLARY 6.2. *Let C be an extremal self-dual even quaternary additive code of length $n = 6q+2r$. Let $f \in L(U_k)_l \cap \ker d$. Then $Z_{C,f} = 0$ in the following cases:*

- *If $r = 0$: for $k = 1,2$ and all $l \leq k$, and for $(k,l) = (3,0),(3,1),(3,2),(4,0),(4,1),(4,3),(5,0),(5,2),(6,1),(7,0)$.*
- *If $r = 1$: for $(k,l) = (1,0),(1,1),(2,0),(2,1),(3,0),(3,2),(4,1),(5,0)$.*
- *If $r = 2$: for $(k,l) = (1,0),(2,1),(3,0)$.*

7. Intersection numbers

Just like in the binary case [**1**], the polynomials $Z_{C,f}$ and their invariance properties can be used to compute certain invariants associated to a fixed element $v \in F^n$ and to a code C. We fix $v \in U_t$.

DEFINITION 7.1. *Let $v \in U_t$ and $u \in U_w$. We define*

$$n(u,v) := \operatorname{card}(S(u) \cap S(v))$$

$$e(u,v) := \operatorname{card}\{s \in [1..n] \mid u_s = v_s \neq 0\}$$

and

Let $i = i(u,v) := t - e(u,v)$ and $j := j(u,v) = t - n(u,v)$. The group H acts on $U_t \times U_w$ and one can see easily that the orbits of this action are given by the values of (i,j). Equivalently, in the case $t = w$, (i,j) gives the relations of the non-binary Johnson scheme [**14**]. Clearly, the values of $(i(u,v), j(u,v))$ belong to the set

$$K_{t,w} := \{(i,j) \mid 0 \leq j \leq i \leq t,\ t-w \leq j \leq n-w\}. \tag{51}$$

Let

$$K_t := K_{t,t} := \{(i,j) \mid 0 \leq j \leq i \leq t,\ j \leq n-t\} \tag{52}$$

and

$$L_t := \{(k,l) \mid 0 \leq l \leq k \leq \min(t, n+l-t)\}. \tag{53}$$

The decomposition of the space $L(U_t)$ into irreducible H-subspaces given by $L(U_t) = \oplus_{(k,l)\in L_t} L(U_t)_{(k,l)}$ (see (6)) allows us to consider the zonal elements associated to this decomposition. These are functions $g_{k,l}$ having the characteristic property that $g_{k,l}(u)$ only depends on $i(u,v)$, $j(u,v)$. In our situation they are uniquely determined up to a scalar multiple because the subspaces $L(U_t)_{(k,l)}$ are pairwise non isomorphic. We recall that they can be constructed the following way: take any orthonormal basis (f_i) of $L(U_t)_{(k,l)}$, and set $E_{(k,l)}(u,v) := \sum_i f_i(u)\overline{f_i(v)}$. This definition is independant of the choice of the basis, and hence is invariant under the action of H on $(u,v) \in U_t^2$. Hence $E_{(k,l)}(u,v)$ is a function of $(i(u,v), j(u,v))$. In the setting of association schemes, the $E_{(k,l)}$ are the idempotents of the non-binary Johnson scheme and its expression in terms of $(i(u,v), j(u,v))$ is given by the second eigenvalues, which are computed in [**14**]. We recall in next proposition their expression in terms of Hahn and Krawtchouk polynomials.

Proposition 7.1. [**14**]

$$E_{(k,l)}(u,v) = h_{(k,l),t}(i(u,v), j(u,v)), \tag{54}$$

where, for all $(k,l) \in L_t$ and $(i,j) \in K_t$,

$$h_{(k,l),t}(i,j) = \frac{\binom{n}{l}}{\binom{t}{l}} K_l(t-j, q-1, i-j) Q_{k-l}(n-l, t-l, j) \tag{55}$$

where K_k, Q_k are respectively Krawtchouk and Hahn polynomials, given by the following formulas:

$$\begin{aligned} K_k(n,q,x) &:= \sum_{i=0}^{k} (-1)^i (q-1)^{k-i} \binom{n-x}{k-i}\binom{x}{i} \\ E_k(n,t,x) &:= \sum_{r=0}^{k} (-1)^r \binom{x}{r}\binom{t-x}{k-r}\binom{n-t-x}{k-r} \\ Q_k(n,t,i) &= \frac{\binom{n}{k} - \binom{n}{k-1}}{\binom{t}{i}\binom{n-t}{i}} E_i(n,t,k) \end{aligned} \tag{56}$$

In view of applications to codes, we shall make use of the polynomials $Z_{C,f}$ for $f \in L(U_k)_l \cap \ker d$ such that $D^* f(u) = E_{(k,l)}(u,v)$ for $u \in U_t$. We denote by $H_{(k,l),v}$ such a function f. Therefore we need to compute $D^* f(u)$ for $u \in U_w$ for any $w \geq k$ (and not only for $w = t$). From last proposition, $D^* H_{(k,l),v}(u) = h_{(k,l),t}(i,j)$ for $u \in U_t$ and $i = i(u,v)$, $j = j(u,v)$. For the general case $u \in U_w$, we have a more complicated and rather ugly formula:

Proposition 7.2. *For all $w \geq k$ and all $u \in U_w$, the value of $D^* H_{(k,l),v}(u)$ only depends on $(i(u,v), j(u,v))$. We set again*

$$D^* H_{(k,l),v}(u) = h^w_{(k,l),t}(i(u,v), j(u,v)), \tag{57}$$

where

$$\begin{aligned} &h^w_{(k,l),t}(i,j) = c \sum_I (q-2)^{i_2+j_2+l_2}(q-3)^{k_3}(q-1)^{t-s}. \\ &\binom{w+j-t}{i_1, i_2}\binom{t-i}{j_1, j_2}\binom{i-j}{k_1,k_2,k_3}\binom{j}{l_1,l_2}\binom{n-w-j}{t-s}\binom{i_1+j_1+k_1}{k}. \\ &h_{(k,l),t}(t-j_1-k_2-l_1, t-j_1-j_2-k_1-k_2-k_3-l_1-l_2) \end{aligned} \tag{58}$$

where

$$c=\frac{1}{(q-1)^{t-k}\binom{n+l-2k}{t-k}} \tag{59}$$

and

$$\begin{aligned}I =\{&(i_1,i_2,j_1,j_2,k_1,k_2,k_3,l_1,l_2) \mid \\ &i_1\in[0..w+j-t], i_2\in[0..w+j-t-i_1],\\ &j_1\in[0..t-i], j_2\in[0..t-i-j_1],\\ &k_1\in[0..i-j], k_2\in[0..i-j-k_1], k_3\in[0..i-j-k_1-k_2],\\ &l_1\in[0..j], l_2\in[0..j-l_1],\\ &i_1+j_1+k_1\geq k, t-(j_1+j_2+k_1+k_2+k_3+l_1+l_2)\leq n-t,\\ &s:=i_1+i_2+j_1+j_2+k_1+k_2+k_3+l_1+l_2\leq t\}.\end{aligned} \tag{60}$$

PROOF. We use the formula $(dd^*-d^*d)_{|L(U_k)_l}=(q-1)(n+l-2k)\mathrm{Id}$ ([**6**, Proposition 2.6]). Taking account of the fact that $H_{(k,l),v}\in\ker d$, and iterating it, we get

(61)
$$(q-1)^{t-k}\binom{n+l-2k}{t-k}H_{(k,l),v}=((-1)^{t-k}\frac{d^{t-k}}{(t-k)!})((-1)^{t-k}\frac{{d^*}^{t-k}}{(t-k)!})H_{(k,l),v}.$$

Let $K:=(-1)^{t-k}\frac{{d^*}^{t-k}}{(t-k)!}H_{(k,l),v}\in L(U_t)$. For all $u\in U_t$, $K(u)=D^*H_{(k,l),v}(u)=h_{(k,l),t}(i(u,v),j(u,v))$. We get, for all $u\in U_w$,

$$\begin{aligned}D^*H_{(k,l),v}(u)&=\frac{1}{(q-1)^{t-k}\binom{n+l-2k}{t-k}}\sum_{\substack{u_k\in U_k\\ u_k\leq u}}\sum_{\substack{z\in U_t\\ u_k\leq z}}K(z)\\ &=\frac{1}{(q-1)^{t-k}\binom{n+l-2k}{t-k}}\sum_{\substack{z\in U_t\\ e(z,u)\geq k}}\binom{e(z,u)}{k}K(z).\end{aligned} \tag{62}$$

The parameters $e(z,u)$, $i(z,v)$, $j(z,v)$ express easily in terms of:
$i_1:=\mathrm{card}\{i\mid z_i=u_i\neq 0, v_i=0\}$, $i_2:=\mathrm{card}\{i\mid z_i\neq u_i\neq 0, v_i=0\}$,
$j_1:=\mathrm{card}\{i\mid z_i=u_i=v_i\neq 0\}$, $j_2:=\mathrm{card}\{i\mid z_i\neq u_i\neq 0, v_i=u_i\}$,
$k_1:=\mathrm{card}\{i\mid z_i=u_i\neq 0, v_i\neq u_i\neq 0\}$, $k_2:=\mathrm{card}\{i\mid z_i\neq u_i\neq v_i\neq 0\}$,
$k_3:=\mathrm{card}\{i\mid z_i\neq u_i\neq 0, z_i=v_i\}$, $l_1:=\mathrm{card}\{i\mid z_i=v_i\neq 0, u_i=0\}$,
$l_2:=\mathrm{card}\{i\mid z_i\neq v_i\neq 0, u_i=0\}$.

The formula then follows from the enumeration of all possibilities. □

REMARK 7.1. *In the case when $t\leq w$, there is a more simple formula for $D^*H_{(k,l),v}(u)$ coming from: ${d^*}^{w-k}H_{(k,l),v}={d^*}^{w-t}{d^*}^{t-k}H_{(k,l),v}$.*

Let C_w denote the set of words in C of Hamming weight w, i.e. $C_w=C\cap U_w$. Let $v\in U_t$. We set, for $(i,j)\in K_{t,w}$,

$$n_{w,(i,j)}(v):=\mathrm{card}\{u\in C_w\mid (i(u,v),j(u,v))=(i,j)\}. \tag{63}$$

TABLE 1. The $n_{w,(i,j)}(v)$ for $|v|=1$

(i,j)	$(0,0)$	$(1,0)$	$(1,1)$
$w=6$	66	132	198
$w=8$	330	660	495
$w=10$	550	1100	330
$w=12$	78	156	0

TABLE 2. The $n_{w,(i,j)}(v)$ for $|v|=2$

(i,j)	$(0,0)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$	$(2,2)$
$w=6$	10	40	72	40	144	90
$w=8$	70	280	240	280	480	135
$w=10$	150	600	200	600	400	30
$w=12$	26	104	0	104	0	0

From Proposition 7.2, for each $(k,l)\in L_t$, the coefficient of $x^{n-w-k+l}y^{w-k}$ in $Z_{C,H_{(k,l),v}}$ is:

$$\sum_{(i,j)\in K_{t,w}} h^*_{(k,l),t}(i,j)n_{w,(i,j)}(v). \tag{64}$$

The claims in Propositions 6.1, 6.2, and the descriptions of the spaces of relative invariants involved, can then be turned out into linear relations between the unknowns $n_{w,(i,j)}(v)$. See [**1**] for examples in the binary case. We work out examples in the case of even quaternary additive self-dual codes.

7.1. The dodecacode. Let $n=12$. It is known ([**11**]) that there is up to equivalence only one $[12,6,6]$ even self-dual quaternary additive code, the so-called dodecacode. We show what can be said *a priori* on the intersection numbers $n_{w,(i,j)}(v)$ defined in (63) of such a code C by use of the method described in section 7. We fix an element $v\in U_t$.

From Corollary 6.2, all the linear forms in (64) are equal to zero for $t\le 2$ and $(k,l)\in L_t$. Moreover, the knowledge of the weight enumerator of such a code C

$$W_C(x,y)=x^{12}+396x^6y^6+1485x^4y^8+1980x^2y^{10}+234y^{12} \tag{65}$$

leads to more equations:

$$\sum_{(i,j)\in K_{t,w}} n_{w,(i,j)}(v)=\mathrm{card}(C_w). \tag{66}$$

We find for $t=1,2$ uniquely determined intersection numbers (see Table 1 and 2), in accordance with the fact that, for all w, C_w holds 2-generalized designs (see Corollary 6.2).

If $t=3$, the intersection numbers are not uniquely determined (Table 3). They depend on one parameter $x(v)=x$ which is the number of weight 3 words in the

TABLE 3. The $n_{w,(i,j)}(v)$ for $|v| = 3$

(i,j)	$(0,0)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$	$(2,2)$
$w=6$	$x-1$	$-3x+15$	18	$3x+9$	72	54
$w=8$	$-3x+21$	$9x+63$	84	$-9x+189$	336	108
$w=10$	$3x+133$	$-9x+261$	90	$9x+459$	360	30
$w=12$	$-x+11$	$3x+45$	0	$-3x+111$	0	0

(i,j)	$(3,0)$	$(3,1)$	$(3,2)$	$(3,3)$
$w=6$	$-x+13$	72	108	36
$w=8$	$3x+105$	336	216	27
$w=10$	$-3x+327$	360	60	0
$w=12$	$x+67$	0	0	0

coset $v+C$ (because clearly this number equals $1+n_{6,(0,0)}(v)$). Clearly, x can take the values $1,2,3,4$.

If $t=4$, we moreover assume that v is a minimum weight word in its coset $v+C$. Again, the intersection numbers are computed from one of them. We don't give the full details of their expression but notice that the number of weight 6 codewords, the support of which contain the support of v, is a constant (because the supports hold classical 5-design from Assmus-Mattson theorem) and that this number equals $n_{6,(2,0)}+n_{6,(3,0)}+n_{6,(4,0)}$. The computation shows that the intersection numbers can all be expressed affinely in $x := n_{6,(4,0)}$ like $n_{6,(2,0)} = x+4$ and $n_{6,(3,0)} = -2x+8$. The weight distribution of $v+C$ itself doesn't depend on x (see Table 4). Note that, in general, the weight distribution of $v+C$ derives from the intersection numbers because $|u+v| = |u| + i(u,v) + j(u,v) - t$.

We display in Table 4 the coset distribution of such a code. The weight of the cosets is at most 4. This can be proved directly by elementary counting arguments, or derives from [**5**]. Note that the coset distribution could also be computed using Delsarte method explained in [**5**]. If the coset has weight 3, it may contain $1,2,3$ or 4 coset leaders. For the dodecacode, one finds respectively 792, 1314, 756, 63 cosets of weight 3 with respectively 1, 2, 3, 4 leaders. Hence the dodecacode has got 540 cosets of weight 4.

7.2. Length 14. The extremal even self-dual codes of length 14 have weight 6 and weight enumerator

$$W_C(x,y) = x^{14} + 273x^8y^6 + 2457x^6y^8 + 7098x^4y^{10} + 6006x^2y^{12} + 549y^{14}. \tag{67}$$

It is known that there is a unique one which is $\mathbb{F}_4$-linear hermitian ([**11**]). The whole number of extremal additive codes seems huge, since we have found 490 such codes with the additional condition that at least two codewords of weight 6 have the same support ([**2**]). Information on the coset distribution of such codes could be computed in the same way as for $n=12$. Here, we take v to be a codeword of weight 6. Because v is in the code C, additional constraints hold for $n_{w,(i,j)}(v)$: since $(u,v) = i(u,v) - j(u,v) \mod 2$, we have $n_{w,(i,j)}(v) = 0$ if $i+j \equiv 1 \mod 2$; also, since $|u+v| = |u| + i + j - t$, we have $n_{w,(i,j)}(v) = 0$ if $0 < w+i+j-t < 6$.

TABLE 4. Coset distribution of a $[12,6,6]$ even self-dual code

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1				66	132	528	660
	1		10	40	182	424	760
		x	$15-3x$	48	$8x+148$	$432-6x$	$810-6x$
			15	48	148	432	810

9	**10**	**11**	**12**
1045	1100	408	156
1080	961	504	134
$1040+8x$	948	$528-3x$	$127+x$
1040	948	528	127

Altogether, the intersection numbers for $v \in C_6$ depend on three positive and integral parameters x, y, z. One of them is $2x := n_{6,(6,0)}(v)$ and counts the number of codewords with the same support as v. Clearly this number is either 0 or 2 (they come by pairs $(u, u+v)$ and they are minimal). The general expression shows that, if $x = 1$, i.e. if the support of v is also the support of some other word in C, then y and z are uniquely determined. Note that, if C is $\mathbb{F}_4$-linear, then it is the case for all $v \in C$ since wv and w^2v would provide codewords with the same support as v. If $x = 0$, then the fact that the intersection numbers are natural numbers show that $y \in [0..3]$ and $z \in [0..4]$. Among the 490 non equivalent codes found, all these possiblities for (y,z) occur. Table 5 gives the expression of the $n_{w,(i,j)}$ for the weights $w = 6, 8$. Note that the $n_{w,(i,j)}(v)$ for $j = 6$ give the weight distribution of the subcode

$$C_v := \{u \in C \mid S(u) \cap S(v) = \varnothing\}. \tag{68}$$

7.3. Length 18. The weight of the extremal codes of length 18 is 8. There is a unique $\mathbb{F}_4$-linear hermitian code of weight 8, named S_{18} ([**11**]). It is not known whether other additive self-dual codes meet this bound. We compute the coset distribution with the help of the intersection numbers. Table 6 gathers the results up to weight 9.

PROPOSITION 7.3. *Let C be an even self-dual additive quaternary code of weight 8. Then the covering radius R of C satisfies* $5 \le R \le 6$.

PROOF. For all i, we denote c_i a coset of C of weight i and by n_i the number of cosets of weight i. Let X_i denote the set of weight i words in F^{18}. Of course, $\operatorname{card}(X_i) = \binom{18}{i} 3^i$. Note that, for $i = 1, 2, 3$, $n_i = \operatorname{card}(X_i)$. We start with the weight enumerators of the cosets of C of weight up to 6, computed with the help of the intersection numbers. With the notations of Table 6, we count the words of weight 4, 5, 6. We have:

TABLE 5. Computation of $n_{w,(i,j)}(v)$ for $v \in C_6$ and $w = 6, 8$

	w = 6	
(i,j)	$x=1$	$x=0$
$(0,0)$	1	1
$(3,3)$	0	$-4z+16$
$(4,2)$	24	$-4y+2z+24$
$(4,4)$	42	$2z+18$
$(5,1)$	0	$2y$
$(5,3)$	96	$8y+4z+72$
$(5,5)$	0	$-2y+24$
$(6,0)$	2	0
$(6,2)$	12	$-3y-2z+24$
$(6,4)$	84	$-2y-2z+90$
$(6,6)$	12	$y+4$

	w = 8	
(i,j)	$x=1$	$x=0$
$(2,2)$	42	$2z+18$
$(3,1)$	96	$8y+4z+72$
$(3,3)$	0	$4y+8z+48$
$(4,0)$	12	$-3y-2z+24$
$(4,2)$	528	$-16y-10z+564$
$(4,4)$	156	$-y-4z+84$
$(5,1)$	192	$2y-4z+192$
$(5,3)$	768	$-8z+816$
$(5,5)$	0	$2y+24$
$(6,0)$	0	$2z$
$(6,2)$	348	$5y+8z+312$
$(6,4)$	312	$4z+300$
$(6,6)$	3	$-y+3$

TABLE 6. Coset distribution for a $[18, 9, 8]$ even self-dual code

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1						408	816	4930
	1				56	224	1304	3360
		1		x	$63-3x$	$303-2x$	$978+14x$	$3730-5x$
			y	z	$84-7y-3z$	$288-8y-2z$	$936+45y+14z$	$3680+8y-5z$
				t	$84-3t$	$288-2t$	$936+14t$	$3680-5t$
					84	288	936	3680

$$\begin{aligned} &\operatorname{card}(X_4) = \sum_{c_4} y \\ (69)\quad &\operatorname{card}(X_5) = \sum_{c_3} x + \sum_{c_4} z + \sum_{c_5} t \\ &\operatorname{card}(X_6) = 56n_2 + \sum_{c_3}(63-3x) + \sum_{c_4}(84-7y-3z) + \sum_{c_5}(84-3z) + 84n_6 \end{aligned}$$

From these equations, we get

$$n_4 + n_5 + n_6 = 238680. \tag{70}$$

But we can check that $1 + n_1 + n_2 + n_3 + n_4 + n_5 + n_6 = 2^{18}$, so we have proved that $R \leq 6$ (it derives also from [**5**] since 6 is the number of different weights of $C^{\perp} = C$). Now we assume that $R \leq 4$, so that $n_5 = n_6 = 0$. For $y \in [1..4]$, we denote n_4^y the number of cosets of weight 4 containing exactly y coset leaders. Clearly, two coset leaders in a coset of weight 4 have disjoint supports because the code has minimal weight 8, so their number is upper bounded by 4. And the sum of two such words is a codeword of weight 8, so, if v is a coset leader of a fixed coset of weight 4,

$$y = 1 + \mathrm{card}\{u, u \in C_8 \mid v \leq u\} = n_{8,(0,0)}(v). \tag{71}$$

If C_8 was a 4-design, the cardinality of $\{u, u \in C_8 \mid v \leq u\}$ would be a constant. However, we can compute its average value

$$\mu := \frac{1}{\mathrm{card}(X_4)} \sum_{v \in X_4} \mathrm{card}\{u, u \in C_8 \mid v \leq u\} \tag{72}$$

by the usual formula:

$$\mu = \frac{\binom{6}{2}\lambda_2}{\binom{16}{2}3^2} \tag{73}$$

where, for $v \in U_2$, $\lambda_2 = \mathrm{card}\{u, u \in C_8 \mid v \leq u\} = 55$. This last value can be read in Table 6. Now, we have

$$\sum_{v \in X_4} y = \sum_{c_4} y^2 = \mathrm{card}(X_4)(1 + \mu). \tag{74}$$

Finally, we obtain the following system of equations:

$$\begin{aligned} n_4^1 + n_4^2 + n_4^3 + n_4^4 &= 238680 \\ n_4^1 + 2n_4^2 + 3n_4^3 + 4n_4^4 &= \mathrm{card}(X_4) \\ n_4^1 + 4n_4^2 + 9n_4^3 + 16n_4^4 &= \mathrm{card}(X_4)(1 + \mu) \end{aligned} \tag{75}$$

One can parametrize the solutions by n_4^1 and see that it doesn't admit any positive integral solutions.

Remark 7.2. *In the case of the code S_{18}, one can compute all these parameters. One finds: $(n_4^1, n_4^2, n_4^3, n_4^4) = (122400, 36720, 12240, 3865)$, and, with obvious notations, $(n_5^{10}, n_5^{12}, n_5^{16}) = (24480, 38250, 765)$. Hence the covering radius of S_{18} is equal to 5. It would be interesting to know if a non $\mathbb{F}_4$-linear code with covering radius 6 exists.*

□

References

[1] C. Bachoc, *On harmonic weight enumerators of binary codes*, to appear in Designs, Codes and Cryptography.

[2] C. Bachoc, P. Gaborit, *Extremal self-dual even quaternary additive codes*

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

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

[5] P. Delsarte, *Four fondamental parameters of a code and its combinatorial significance* Information and Control **23** (1973), 407-438

[6] C. F. Dunkl, *A Krawtchouk polynomial addition theorem and wreath products of symmetric groups* Ind. Univ. Math. Journal **25** 4 (1976), 335-358

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

[8] 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
[9] G. Höhn, *Self-dual codes over the Kleinian four-group*, preprint (1996)
[10] S. Karlin, J. McGregor, *The Hahn polynomials, formulas and an application* Scripta Math. **26** (1961), 33-46
[11] E. Rains, N.J.A. Sloane, *Self-dual codes*, Handbook of Coding Theory, V. Pless and W. C. Huffman editors, North Holland, Amsterdam, 1998
[12] K. Tanabe, *A new proof of Assmus-Mattson theorem for non-binary codes*, Codes, Designs and Cryptography, to appear.
[13] H. Tarnanen, *An approach to constant weight and Lee codes by using the methods of association schemes*, PHD thesis, Turku University 1982
[14] H. Tarnanen, M. J. Aaltonen, J.-M. Goethals, *On the nonbinary Johnson scheme*, Europ. J. Comb. **6** (1985), 279-285

Laboratoire A2X, Université de Bordeaux, 351, cours de la libération, 33405 Talence

E-mail address: bachoc@math.u-bordeaux.fr