TWO-TUPLES WEIGHT ENUMERATORS

Alphonse Baartmans *, Vassil Yorgov †

Abstract

We consider an inner product of a special type in the space of $n-$tuples over a finite field F_q of characteristic p. We prove that there is a very close relationship between the self-dual $q-$ary additive codes under this inner product and the self-dual $p-$ary codes under the usual dot product. We prove the MacWilliams identities for complete weight enumerators of $q-$ary additive codes with respect to the new inner product. We define a two-tuple weight enumerator of a binary self-dual code and prove that it is invariant of a group of order 384. We compute the Molien series of this group and find a good polynomial basis for the ring of its invariants.

1 MacWilliams identities for complete weight enumerators of additive codes

We use the standard notations of coding theory [2].

*Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931.

†Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931. On leave from Department of Mathematics and Computer Science, Shoumen University, Shoumen 9712, Bulgaria.

JCMCC **36** (2001), pp. 207-214

Let F_q be a field of $q = p^m$ elements, p a prime. Any additive subgroup C of F_q^n is called additive code over F_q. If C is an additive code over F_q then C is a linear space over F_p. We call $\dim_{F_p} C$ dimension of the additive code C and refer to C as to an $[n, k]$ additive code over F_q.

Let $Tr : F_q \to F_p$ be the trace function

$$Tr(x) = x + x^p + x^{p^2} + \cdots + x^{p^{m-1}}.$$

We define an inner product in F_q^n by

$$\langle u, v\rangle = \sum_{i=1}^{n} Tr(u_i v_i) = Tr(u.v) \tag{1}$$

where $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n)$. Compare with [4] where additive codes over $GF(4)$ that are self- orthogonal under an Hermitian type inner product are considered. It is clear that if C is an $[n, k]$ additive code over F_q then the dual code under (1) , $C^\perp$, is an $[n, mn - k]$ additive code.

Let $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ be a complex p-th root of unity. For any α in F_q define $\chi(\alpha) = \zeta^{Tr(\alpha)}$. Then χ is a nontrivial additive character of F_q. For given vectors u and v in F_q^n we define $\chi_u(v) = \chi(u.v) = \zeta^{\langle u,v\rangle}$. It follows that χ_u is an additive character of F_q^n. Let K be a commutative ring and $f : F_q^n \to K$ be a map. Define $\hat{f}(u) = \sum_{v\in F_q^n} \chi_u(v) f(v)$.

Lemma 1 *If C is an additive code over F^q then $\sum_{v\in C^\perp} f(v) = \frac{1}{|C|}\sum_{u\in C} \hat{f}(u)$ with respect to the inner product (1).*

Proof. We have $\sum_{u\in C} \hat{f}(C) = \sum_{u\in C}\sum_{v\in F_q^n} \chi_u(v) f(v) = \sum_{v\in F_q^n} f(v) \sum_{u\in C} \chi_u(v) = \sum_{v\in F_q^n} f(v) \sum_{u\in C} \zeta^{\langle u,v\rangle}$. If $v \in C^\perp$ then $\langle u, v\rangle = 0$ and $\sum_{u\in C} \zeta^{\langle u,v\rangle} = |C|$.

Let v not be in $C^\perp$. Hence there exists $u' \in C$ such that $\langle u', v\rangle \neq 0$. Denote $C^{(i)} = \{u \in C : \langle u, v\rangle = i, i = 0, 1, 2, \ldots, p - 1\}$. Hence $C^{(0)}$ is an additive subgroup of C and for $i = 1, 2, \ldots, p-$

1 $C^{(i)}$ is a coset of $C^{(0)}$. Therefore $\sum_{u\in C}\zeta^{\langle u,v\rangle} = |C^{(0)}|(1+\zeta+\zeta^2+\ldots+\zeta^{p-1}) = 0$. Hence $\sum_{u\in C}\hat{f}(u) = |C|\sum_{v\in C^\perp} f(v)$. The lemma is proved.

Let $F_q = \{\omega_0, \omega_1, \ldots, \omega_{q-1}\}$. For a vector $u \in F_q^n$ denote $s_i(u)$ the number of coordinates of u equal to ω_i, $i = 0, 1, 2, \ldots, q-1$. The polynomial

$$W_C(z_0, z_1, z_2, \ldots, z_{q-1}) = \sum_{u\in C} z_0^{s_0(u)} z_1^{s_1(u)} \cdots z_{q-1}^{s_{q-1}(u)}$$

in indeterminates $z_0, z_1, \ldots, z_{q-1}$ is called a complete weight enumerator of the additive code C.
From the above lemma we obtain immediately the MacWilliams identities for complete weight enumerators of dual additive codes.

Theorem 1 *Let C be an additive code over F_q. Then with respect to the inner product (1) we have*

$$W_{C^\perp}(z_0, z_1, \ldots, z_{q-1}) = \frac{1}{|C|} W_C\left(\sum_{i=0}^{q-1}\chi(\omega_0\omega_i)z_i, \ldots, \sum_{i=0}^{q-1}\chi(\omega_{q-1}\omega_i)z_i\right).$$

The proof is similar to the proof of the corresponding theorem for linear codes, see [2] page 143.

Example. Let $q = 4$. Hence $p = 2$, $\zeta = -1$, and $\chi(\alpha) = (-1)^{\alpha+\alpha^2}$. Let $F_4 = \{0, \omega, \omega^2, 1\}$ where $\omega + \omega^2 = 1$. Then we have $\chi(0) = \chi(1) = 1$, $\chi(\omega) = \chi(\omega^2) = -1$, and

$$W_{C^\perp}(z_0, z_1, z_2, z_3) =$$

$$\frac{1}{|C|} W_C(z_0+z_1+z_2+z_3, z_0-z_1+z_2-z_3, z_0+z_1-z_2-z_3, z_0-z_1-z_2+z_3).$$

2 Binary images of additive codes

A basis $\gamma_1, \gamma_2, \ldots, \gamma_m$ of F_q, $q = p^m$, is called self-complementary ([2] page 117) if $Tr(\gamma_i\gamma_j) = 0$ for $i \neq j$ and $Tr(\gamma_i\gamma_j) = 1$ for $i = j$.

Example. Let $F_4 = \{0, \omega, \omega^2, 1\}$ where $\omega + \omega^2 = 1$. Then ω, ω^2 is a self-complementary basis of F_4. A self- complementary basis of F_{16} is given in [3]. See also [1].

A p-ary image of a vector $u = (u_1, u_2, \ldots, u_n) \in F_q^n$ with respect to a given basis of F_q over F_p is the mn-tuple obtained by replacinig each u_i by the $m-$tuple of its coordinates. The next lemma is straightforward.

Lemma 2 *The inner product (1) of two vectors over F_q is equal to the usual dot product of their $p-$ary images with respect to a self-complementary basis of F_q.*

The next theorem is an immediate generalization of a result in [3].

Theorem 2 *Let $\gamma_1, \gamma_2, \ldots, \gamma_m$ be a self-complementary basis of F_{p^m}. Any linear code, C, over F_p of length a multiple of m is a $p-$ary image of some additive code, $\hat{C}$, over F_{p^m}. Moreover C is self-orthogonal (self-dual) under the usual dot product if and only if $\hat{C}$ is self-orthogonal (self-dual) under the inner product (1).*

3 Two-tuples weight enumerators of doubly-even self-dual codes

Let $F_4 = \{0, \omega, \omega^2, 1\}$ with $\omega + \omega^2 = 1$. We fix a trace orthogonal basis ω, ω^2 of F_4. With respect to this basis the binary images of $0, \omega, \omega^2$, and 1 are $00, 01, 10$, and 11, respectively. For each vector $u = (u_1, u_2, \ldots, u_n)$ in a binary code C of even block length n denote $\hat{u} = (\alpha_1, \alpha_2, \ldots, \alpha_{n/2})$ where $\alpha_1 = u_1\omega^2 + u_{n/2+1}\omega, \ldots,$ $\alpha_{n/2} = u_{n/2}\omega^2 + u_n\omega$. Then the set $\hat{C} = \{\hat{u} : u \in C\}$ is an additive code over F_4 and C is its binary image.

We call the complete weight enumerator, $W_{\hat{C}}(z_0, z_1, z_2, z_3)$, of $\hat{C}$ a two-tuples weight enumerator of C. From theorem 1 and theorem 2 we know that if C is self-dual then

$$W_{\hat{C}}(z_0, z_1, z_2, z_3) =$$

$$2^{-n/2} W_{\hat{C}}(z_0+z_1+z_2+z_3, z_0-z_1+z_2-z_3, z_0+z_1-z_2-z_3, z_0-z_1-z_2+z_3).$$

As $W_{\hat{C}}(z_0, z_1, z_2, z_3)$ is a homogeneous polynomial of degree $n/2$ the above equality shows that the two-tuples weight enumerator of C is invariant under the linear transform defined by the matrix

$$A = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

In the following we will assume that C is a doubly-even self-dual code containing the vector $1^{n/2}0^{n/2}$. The code C is invariant under addition by this vector. Hence $\hat{C}$ is invariant under the transformation $0 \to \omega^2, \omega \to 1, \omega^2 \to 0, 1 \to \omega$. Thus $W_{\hat{C}}(z_0, z_1, z_2, z_3)$ is invariant under the linear transform $z_0 \to z_2$, $z_1 \to z_3$, $z_2 \to z_0$, $z_3 \to z_1$ which has as its matrix

$$B_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

It is clear that $1^n \in C$. Therefore $0^{n/2}1^{n/2}$ is in C. We obtain as above that $W_{\hat{C}}(z_0, z_1, z_2, z_3)$ is invariant under the linear transform defined by the matrix

$$B_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Obviously $W_{\hat{C}}(x^2, xy, xy, y^2) = W_C(x, y)$ (the usual weight enumerator of C). If $z_0^{i_0} z_1^{i_1} z_2^{i_2} z_3^{i_3}$ is a monomial of $W_{\hat{C}}(z_0, z_1, z_2, z_3)$

then $x^{2i_0}(xy)^{i_1}(xy)^{i_2}y^{2i_3} = x^{2i_0+i_1+i_2}y^{i_1+i_2+2i_3}$ must be a monomial in $W_C(x,y)$. Since C is doubly-even we obtain $i_1+i_2+2i_3 \equiv 0(mod 4)$. Therefore $W_{\hat{C}}(z_0,z_1,z_2,z_3)$ is invariant under a linear transform with a matrix

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

where $i^2 = -1$. Thus we have obtained the following lemma.

Lemma 3 *Let C be a double-even self-dual code containing the vector $1^{n/2}0^{n/2}$ and $\hat{C}$ be the corresponding additive code over F_4. Then $W_{\hat{C}}(z_0,z_1,z_2,z_3)$ is invariant of a group G generated by the matrices A, B_1, B_2, and D*

Using GAP and Mathematica we determined that the order of G is 384 and its Molien series ([2], p.600) is

$$\Phi_G(\lambda) = \frac{1}{|G|}\sum_{M\in G}\frac{1}{det(I-\lambda M)} = \frac{1+\lambda^8+\lambda^{16}+\lambda^{24}}{(1-\lambda^4)^2(1-\lambda^8)(1-\lambda^{12})}.$$

We write $\Phi_G(\lambda)$ in the form

$$\Phi_G(\lambda) = \frac{1+\lambda^8}{(1-\lambda^4)^2(1-\lambda^8)(1-\lambda^{12})}+\lambda^{16}\frac{1+\lambda^8}{(1-\lambda^4)^2(1-\lambda^8)(1-\lambda^{12})}$$

and use it to find a good polynomial basis of the ring of invariants of G.

Let $a = z_0 + z_3$, $b = z_0 - z_3$, $c = z_1 + z_2$, and $d = z_1 - z_2$. The transformations defined by the matrices A, B_1, B_2, and D act on a, b, c, and d, as follows:

A	$a \to a$	$b \to c$	$c \to b$	$d \to -d$;
B_1	$a \to a$	$b \to -b$	$c \to c$	$d \to -d$;
B_2	$a \to c$	$b \to d$	$c \to a$	$d \to b$;
D	$a \to b$	$b \to a$	$c \to ic$	$d \to id$.

It can be checked easily that the polynomials

$$\sigma_1^2 = (a^2 - b^2 - c^2 + d^2)^2,$$

$$\sigma_2 = -a^2b^2 - a^2c^2 + a^2d^2 + b^2c^2 - b^2d^2 - c^2d^2,$$

$$\sigma_3^2 = (a^2b^2c^2 - a^2b^2d^2 - a^2c^2d^2 + b^2c^2d^2)^2,$$

$$\sigma_4 = a^2b^2c^2d^2$$

are invariants of G. As σ_1, σ_2, σ_3, and σ_4 are algebraically independent, σ_1^2, σ_2, σ_3^2, and σ_4 are also algebraically independent with degrees 4, 4, 12, and 8, respectively.

The polynomial $q_8 = \sigma_1\sigma_3 = (a^2 - b^2 - c^2 + d^2)(a^2b^2c^2 - a^2b^2d^2 - a^2c^2d^2 + b^2c^2d^2)$ is an invariant of degree 8 which is not in the polynomial ring $\mathbf{C}(\sigma_1^2, \sigma_2, \sigma_3^2, \sigma_4)$ but $(\sigma_1\sigma_3)^2 = (\sigma_1)^2(\sigma_3)^2 \in \mathbf{C}(\sigma_1^2, \sigma_2, \sigma_3^2, \sigma_4)$ where $\mathbf{C}$ is the complex number field.

The polynomial $q_{16} = (a^2+b^2)(a^2+c^2)(b^2-c^2)(a^2-d^2)(b^2+d^2)(c^2+d^2)abcd$ is an invariant of G of degree 16. Each monomial of q_{16} contains odd powers of a, b, c, and d while each monomial of any polynomial in σ_1^2, σ_2, σ_3^2, σ_4, and q_8 contains even powers of a, b, c, and d. Hence q_{16} is not in $\mathbf{C}(\sigma_1^2, \sigma_2, \sigma_3^2, \sigma_4) \oplus q_8\mathbf{C}(\sigma_1^2, \sigma_2, \sigma_3^2, \sigma_4)$. But $q_{16}^2 \in \mathbf{C}(\sigma_1^2, \sigma_2, \sigma_3^2, \sigma_4) \oplus q_8\mathbf{C}(\sigma_1^2, \sigma_2, \sigma_3^2, \sigma_4)$ since $q_{16}^2 = [-4\sigma_1^2\sigma_2^3\sigma_4 + 16\sigma_2^4\sigma_4 + \sigma_1^2\sigma_2^2\sigma_3^2 - 4\sigma_2^3\sigma_3^2 - 6\sigma_1^2\sigma_3^2\sigma_4 + 144\sigma_2\sigma_3^2\sigma_4 - 27\sigma_1^4\sigma_4^2 + 144\sigma_1^2\sigma_2\sigma_4^2 - 128\sigma_2^2\sigma_4^2 + 256\sigma_4^3 - 27\sigma_3^4 + q_8(18\sigma_1^2\sigma_2\sigma_4 - 80\sigma_1^4\sigma_4 - 4\sigma_1^2\sigma_3^2 + 18\sigma_2\sigma_3^2 - 192\sigma_4^2)]\sigma_4$. Thus we have obtained the following theorem.

Theorem 3 *Any self-dual doubly-even code of length n which contains a vector of weight $n/2$ has a two-tuples weight enumerator from* $\mathbf{C}(\sigma_1^2, \sigma_2, \sigma_3^2, \sigma_4) \oplus q_8\mathbf{C}(\sigma_1^2, \sigma_2, \sigma_3^2, \sigma_4) \oplus q_{16}(\mathbf{C}(\sigma_1^2, \sigma_2, \sigma_3^2, \sigma_4) \oplus q_8\mathbf{C}(\sigma_1^2, \sigma_2, \sigma_3^2, \sigma_4))$.

Acknowledgements: The second author is grateful to Michigan Technological University for the excellent working conditions provided.

References

[1] A. Lempel, Matrix factorization over $GF(2)$ and trace orthogonal basis of $GF(2^n)$, *SIAM J. Comput.* 4 1975.

[2] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1992.

[3] G. Pasqueir, A binary extremal doubly even self-dual code (64,32,12) obtained from an extended Reed-Solomon code over F_{16}, *IEEE Trans. Info. Theory* **IT-27** (1981), 807–808.

[4] E.M. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Info. Theory* **IT-44** (1998), 134–139.