GEORGIAN MATHEMATICAL JOURNAL: Vol. 5, No. 5, 1998, 469-474

A NOTE ON WEIGHT ENUMERATORS OF LINEAR SELF-DUAL CODES

N. LOMADZE

Abstract. A partial description of (complete) weight enumerators of linear self-dual codes is given.

0. Let $F = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number. If C is a linear code on F of length n, i.e., a linear subspace in F^n, then its (complete) weight enumerator W_C is defined to be

$$\sum_{u \in C} \Big(\prod_{a \in F} x_a^{s_a(u)} \Big).$$

Here x_a, $a \in F$ are indeterminates; $s_a(u)$ denotes the number of entries of u in C equal to a. This is a homogeneous polynomial in p indeterminates of degree n. Define the additive character ψ of F by

$$k \mapsto \Big(e^{\frac{2\pi i}{p}} \Big)^k, \quad k \in F,$$

and let

$$A = \frac{1}{\sqrt{p}} \big(\psi(ij) \big)_{i,j \in F} .$$

Further, for each $a \in F$, let U_a be the diagonal matrix with $\psi(ai^2)$ at the (i,i)th place for each $i \in F$; for each $b \in F^*$, let V_b be the matrix with 1 at the (bi,i)th place for each i and 0 elsewhere. One knows well that weight enumerators of linear self–dual codes are invariant relative to A, U_a, and V_b (see [2]). Therefore, a natural problem is to determine all invariants of these transformations. The problem seems to be difficult. At the moment there are solutions for the case $p = 2$ (Gleason) and $p = 3$ (McEliece) (see [2]).

In [3] we have described the invariant ring of A, which is undoubtely the most interesting transformation. The goal of this short paper is to describe

1991 *Mathematics Subject Classification.* 94B05, 13A50.

Key words and phrases. Linear code, character, group, polynomial, invariant, Gaussian sum.

1072-947X/98/0900-0469$15.00/0

the invariants of A and V_b, $b \in F^*$. It should be pointed out that the exposition is elementary and uses no technique of invariant theory of finite groups.

In what follows $p \neq 2$. Let $R = \mathbb{C}\big[(x_a)_{a\in F}\big]$ be the ring of polynomials with complex coefficients and let G be the group generated by A and V_b, $b \in F^*$.

We remark that the generators of this group satisfy the following relations only:

(1) $b \mapsto V_b$ is a multiplicative homomorphism;
(2) $A^2 = V_{-1}$;
(3) $V_b A = A V_{b^{-1}}$.

1. Choose a generator b of the multiplicative group of F, and denote by V the transformation V_b. Let G_0 be the subgroup in G generated by V. Clearly, G_0 is isomorphic to F^*. It is easy to see that G_0 is a normal subgroup in G of index 2 and $G = G_0 \cup AG_0$.

Let us find the invariants of G_0. Denote by χ that multiplicative character of F which takes b to $e^{\frac{2\pi i}{p-1}}$. For each $k = 0, 1, \ldots, p-2$, put

$$y_k = \sum_{l=0}^{p-2} \chi^k(b^l) x_{b^l}.$$

Clearly, $R = \mathbb{C}[x_0, y_0, y_1, \ldots, y_{p-2}]$.

Lemma 1.1. *One has*
(1) $V(x_0) = x_0$;
(2) $V(y_0) = y_0$;
(3) $V(y_k) = e^{-\frac{2\pi k i}{p-1}} y_k$, $k = 1, \ldots, p-2$.

Proof. (1) and (2) are obvious. To prove (3) take any y_k with $k \neq 0$. We have

$$V(y_k) = \sum_{l=0}^{p-2} \chi^k(b^l) x_{b^{l+1}} = \sum_{l=1}^{p-1} \chi^k(b^{l-1}) x_{b^l} =$$

$$= \chi^{-k}(b) \sum_{l=1}^{p-1} \chi^k(b^l) x_{b^l} = e^{-\frac{2\pi k i}{p-1}} y_k. \qquad \square$$

Denote by I the set of all mappings $i : [1, p-2] \to [0, p-2]$ which satisfy the congruence

$$\sum_{k=1}^{p-2} k i(k) \equiv 0 \mod (p-1).$$

For each $i \in I$, put $\eta_i = y_1^{i(1)} \cdots y_{p-2}^{i(p-2)}$. Let R_0 denote $\mathbb{C}[x_0, y_0, y_1^{p-1}, \ldots, y_{p-2}^{p-1}]$. This is a subring in R.

Lemma 1.2. *The invariant ring of* G_0 *is* $R^{G_0} = \bigoplus_{i\in I} \eta_i R_0$.

Proof. Let i run over all the mappings of $[1, p-2]$ into $[0, p-2]$. Then, every element in R can be written uniquely as a sum

$$\sum_i \Big(\prod_{k=1}^{p-2} y_k^{i(k)}\Big) f_i,$$

where $f_i \in R_0$. Notice that $Vf = f$ for each $f \in R_0$. So letting c_i denote $\Big(e^{-\frac{2\pi i}{p-1}}\Big)^{\sum_{k=1}^{p-2} ki(k)}$, we have

$$V\bigg(\sum_i \Big(\prod_{k=1}^{p-2} y_k^{i(k)}\Big) f_i\bigg) = \sum_i \Big(\prod_{k=1}^{p-2} y_k^{i(k)}\Big) c_i f_i.$$

One can therefore see that

$$V\bigg(\sum_i \Big(\prod_{k=1}^{p-2} y_k^{i(k)}\Big) f_i\bigg) = \sum_i \Big(\prod_{k=1}^{p-2} y_k^{i(k)}\Big) f_i$$

if and only if, for each i, either $c_i = 1$ or $f_i = 0$. Certainly, $c_i = 1 \Longleftrightarrow i \in I$. $\square$

2. For each $k = 1, \ldots, p-2$ put

$$\tau(k) = \frac{1}{\sqrt{p}} \sum_{l=0}^{p-2} \chi^k(b^l)\psi(b^l).$$

These are the so-called Gaussian sums. They satisfy the relations

$$\tau(k)\tau(p-1-k) = \chi^k(-1), \quad k = 1, \ldots, r-1.$$

Here and below $r = \frac{p-1}{2}$. These relations are immediate consequences of Theorem 4 in [1, Ch. I, §2] and the fact that $\overline{\tau}(k) = \chi^k(-1)\tau(p-1-k)$. One has also

$$\tau(r) = \begin{cases} 1 & \text{if} \quad p \equiv 1 \bmod 4, \\ i & \text{if} \quad p \equiv 3 \bmod 4 \end{cases}$$

(see Theorem 7 in [1, Ch. V, §4]).

Lemma 2.1. *One has*

$$\begin{aligned} Ax_0 &= \frac{1}{\sqrt{p}}(x_0 + y_0), \\ Ay_0 &= \frac{1}{\sqrt{p}}((p-1)x_0 - y_0), \\ Ay_k &= \tau(k) y_{p-1-k}, \quad k = 1, \ldots, p-2. \end{aligned}$$

Proof. This can easily be checked. See also [1, Ch. V, §4, Exercise 17].

From the above lemma follows in particular that

$$AR_0 \subseteq R_0.$$

We want now to find the absolute and relative invariants of A belonging to R_0, in other words, those polynomials f, $g \in R_0$ which satisfy the conditions

$$Af = f, \quad Ag = -g.$$

Put

$$\begin{aligned} z_{01} &= (1+\sqrt{p})x_0 + y_0; \\ z_{02} &= (1-\sqrt{p})x_0 + y_0; \\ z_{k1} &= y_k^{p-1} + \tau(k)^{p-1} y_{p-1-k}^{p-1}, \quad k = 1, \ldots, r-1; \\ z_{k2} &= y_k^{p-1} - \tau(k)^{p-1} y_{p-1-k}^{p-1}, \quad k = 1, \ldots, r-1; \\ z_r &= y_r^{p-1}. \end{aligned}$$

Certainly, $R_0 = \mathbb{C}[z_{01}, z_{02}, z_{11}, z_{12}, \ldots, z_{r-1,1}, z_{r-1,2}, z_r]$. □

Lemma 2.2. *One has*

$$\begin{aligned} Az_{01} &= z_{01}, \quad Az_{02} = -z_{02}, \\ Az_{k1} &= z_{k1}, \quad Az_{k2} = -z_{k2}, \quad k = 1, \ldots, r-1; \\ Az_r &= (-1)^r z_r. \end{aligned}$$

Proof. Follows easily from the preceding lemma. One should have in mind the relations $\tau(k)^{p-1}\tau(p-1-k)^{p-1} = 1$ $(k = 1, \ldots, r-1)$ and $\tau(r)^{p-1} = (-1)^r$.

Consider two cases.

(1) $p \equiv 1(\bmod 4)$. Let α, β run over all the mappings $[0, r-1] \to \{0, 1\}$ satisfying the conditions

$$\sum_{k=0}^{r-1} \alpha(k) \equiv 0 \bmod 2, \quad \sum_{k=0}^{r-1} \beta(k) \equiv 1 \bmod 2$$

respectively. Put

$$f_\alpha = z_{02}^{\alpha(0)} \cdots z_{r-1,2}^{\alpha(r-1)}, \quad g_\beta = z_{02}^{\beta(0)} \cdots z_{r-1,2}^{\beta(r-1)}.$$

Set

$$\begin{aligned} S_1 &= \bigoplus_\alpha f_\alpha \mathbb{C}[z_{01}, \ldots, z_{r-1,1}, z_{02}^2, \ldots, z_{r-1,2}^2, z_r], \\ S_2 &= \bigoplus_\beta g_\beta \mathbb{C}[z_{01}, \ldots, z_{r-1,1}, z_{02}^2, \ldots, z_{r-1,2}^2, z_r]. \end{aligned}$$

(2) $p \equiv 3(\mathrm{mod}\ 4)$. Let α, β run over all the mappings $[0,r] \to \{0,1\}$ satisfying the conditions

$$\sum_{k=0}^{r} \alpha(k) \equiv 0 \bmod 2, \quad \sum_{k=0}^{r} \beta(k) \equiv 1 \bmod 2,$$

respectively. Put

$$f_\alpha = z_{02}^{\alpha(0)} \cdots z_{r-1,2}^{\alpha(r-1)} z_r^{\alpha(r)}, \quad g_\beta = z_{02}^{\beta(0)} \cdots z_{r-1,2}^{\beta(r-1)} z_r^{\beta(r)}.$$

Set

$$S_1 = \bigoplus_\alpha f_\alpha \mathbb{C}[z_{01}, \ldots, z_{r-1,1}, z_{02}^2, \ldots, z_{r-1,2}^2, z_r^2],$$
$$S_2 = \bigoplus_\beta g_\beta \mathbb{C}[z_{01}, \ldots, z_{r-1,1}, z_{02}^2, \ldots, z_{r-1,2}^2, z_r^2].$$

In both cases there holds the following

Lemma 2.3.
(a) $S_1 = \{f \in R_0 | Af = f\}$ *and* $S_2 = \{g \in R_0 | Ag = -g\}$;
(b) $R_0 = S_1 \oplus S_2$.

Proof. Left to the reader. □

3. We are now ready to describe the invariants of G.

For each $i \in I$, put

$$a_i = \prod_{k=1}^{p-2} \tau(k)^{i(k)}.$$

For each $i \in I$, let $\bar{i}$ be the function defined by the formula

$$\bar{i}(k) = i(p-1-k) \quad k = 1, \ldots, p-2.$$

It is clear that $\bar{i} \in I$ and $\bar{\bar{i}} = i$. Let $I_0 = \{i \in I | \bar{i} = i\}$. The complement to I_0 in I breaks into two parts I_1 and I_2 so that $i \in I_1 \Rightarrow \bar{i} \in I_2$ and $i \in I_2 \Rightarrow \bar{i} \in I_1$.

Lemma 3.1. *For each* $i \in I$ $a_i a_{\bar{i}} = 1$.

Proof. We have

$$a_i a_{\bar{i}} = \prod_{k=1}^{p-2} \tau(k)^{i(k)} \prod_{k=1}^{p-2} \tau(p-1-k)^{i(k)} =$$
$$= \prod_{k=1}^{p-2} (\chi^k(-1))^{i(k)} = \chi(-1)^{\sum_{k=1}^{p-2} k i(k)} = 1. \quad \square$$

Lemma 3.2. *For each* $i \in I$ $A\eta_i = a_i \eta_{\bar{i}}$.

Proof. It is obvious. □

Lemma 3.3. *Suppose we are given a polynomial*

$$\sum_{i\in I} \eta_i h_i \in R^{G_0}$$

with $h_i \in R_0$. *It is invariant under* A *if and only if, for each* i, $Ah_i = a_{\bar{i}} h_{\bar{i}}$.

Proof. We have

$$A\Big(\sum_{i\in I} \eta_i h_i\Big) = \sum_{i\in I} \eta_{\bar{i}} (a_i A h_i).$$

From this and from the fact that $AR_0 \subseteq R_0$ follows the assertion.

By Lemma 3.1, if $i \in I_0$, then $a_i = \pm 1$. Put

$$I_{01} = \big\{i \in I_0 | a_i = 1\big\} \quad \text{and} \quad I_{02} = \big\{i \in I_0 | a_i = -1\big\}. \qquad \square$$

Theorem. *Every polynomial which is invariant relative to the action of* G *can be written uniquely as*

$$\sum_{i\in I_{01}} f_i + \sum_{i\in I_{02}} g_i + \sum_{i\in I_1} (\eta_i h_i + a_i \eta_{\bar{i}} A h_i),$$

where $f_i \in S_1$, $g_i \in S_2$, $h_i \in R_0$.

Proof. Follows from Lemmas 2.3 and 3.2. □

References

1. Z. Borevich and I. Shafarevich, Number theory, 3rd ed. (Russian) *Nauka, Moscow,* 1985.

2. F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane, Generalizations of Gleason's theorem on weight enumerators of self–dual codes. *IEEE Trans. Inform. Theory* **18**(1972), 794–805.

3. N. G. Lomadze, Formally self-dual polynomials. *Problemy Peredachi Informatsii* **24**(1988), 22–30.

(Received 27.06.1996)

Author's address:
Department of Applied Mathematics
Georgian Technical University
77, Kostava St., Tbilisi 380075
Georgia