GEORGIAN MATHEMATICAL JOURNAL: Vol. 4, No. 5, 1997, 451-460

ON McELIECE'S THEOREM

N. LOMADZE

ABSTRACT. A new simple proof of the well-known theorem of McEliece about the complete weight enumerators of ternary self-dual codes is given.

0. Introduction. Let C be a ternary linear code of length n. The complete weight enumerator of C is the homogeneous polynomial

$$W_C(x_0, x_1, x_2) = \sum_{i+j+k=n} A_{ijk} x_0^i x_1^j x_2^k,$$

where A_{ijk} stands for the number of codewords that consist of i zeros, j ones, and k twos. One knows well that the function $W_C(x_0, x_1, x_2)$ satisfies the MacWilliams identity

$$W_C(x_0, x_1, x_2) =$$
$$= W_C\Big(\frac{1}{\sqrt{3}}(x_0 + x_1 + x_2), \frac{1}{\sqrt{3}}(x_0 + \omega x_1 + \omega^2 x_2), \frac{1}{\sqrt{3}}(x_0 + \omega^2 x_1 + \omega x_2)\Big)$$

(here and below $\omega = e^{2\pi i/3}$); in other words, the polynomial W_C is invariant under the linear transformation

$$\alpha = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}.$$

Further, since the weight of any codeword of C is divisible by 3, one has

$$W_C(x_0, x_1, x_2) = W_C(x_0, \omega x_1, \omega x_2);$$

Key words and phrases. Linear code, group, invariant, reflection, character, homogeneous polynomial.

1072-947X/97/0900-0451$12.50/0

this is equivalent to saying that the polynomial W_C is invariant under the linear transformation

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

Thus the complete weight enumerator of the ternary self-dual code C is invariant relative to the group generated by the matrices α and β. Let $\overline{G}$ denote this group. This is a group of cardinality 96. (See [1].)

The question of describing all invariants of this group arises naturally. This was done by McEliece using the method of invariant theory for finite groups. (See [1,2].) In this way McEliece obtained

Theorem. *Let $x = x_0$, $y = x_1 + x_2$ and $z = x_1 - x_2$. Then*

$$W_C(x_0, x_1, x_2) \in \bigoplus_{k=0}^{5} h_k z^{2k} \mathbb{C}[f, \psi^3, z^{12}],$$

where

$$f = x^4 + xy^3, \quad \psi = y(8x^3 - y^3), \quad \varphi = 8x^6 - 20x^3y^3 - y^6,$$
$$h_0 = 1, \quad h_1 = \varphi\psi, \quad h_2 = \psi^2, \quad h_3 = \varphi, \quad h_4 = \psi, \quad h_5 = \varphi\psi^2.$$

The goal of this paper is to carry out a proof of this important theorem which, we believe, is much simpler and clearer than that given by McEliece [1].

Our approach is based on the following observation. The whole space on which $\overline{G}$ acts splits up into a direct sum of two invariant irreducible subspaces, two-dimensional and one-dimensional ones. The "restriction" of $\overline{G}$ on the two-dimensional subspace is therefore a two-dimensional group generated by reflections. Finding invariants of such a group (both absolute and relative) is very easy. Knowledge of all such invariants leads immediately to McEliece's result.

It should be pointed out that the idea to apply invariant theory of finite groups to coding theory goes back to Gleason. Gleason himself described complete weight enumerators of binary codes. McEliece's theorem is one of the most interesting generalizations of Gleason's theorem.

Concluding the introduction, we would like to thank the anonymous referee for useful suggestions.

1. Preliminaries. We recall here the definitions and facts concerning invariant theory which are needed. For details we refer to [3–6]. We restrict ourselves to the two-dimensional case.

Let V be a two-dimensional complex vector space, and let $R = \mathbb{C}[x, y]$ be the ring of polynomials in the variables x and y with complex coefficients.

Fix a basis (e_1, e_2) in V and identify via it transformations of V with nonsingular complex 2×2 matrices, and polynomials in R with complex valued functions on V.

The group $GL_2(\mathbb{C})$ of all nonsingular 2×2 matrices acts on R in the following way. If

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C}) \text{ and } f = f(x, y) \in R,$$

then

$$Mf = f(ax + by, cx + dy).$$

Let Γ be a finite subgroup in $GL_2(\mathbb{C})$. A polynomial $f \in R$ is said to be an invariant of Γ if

$$Mf = f \quad \text{for all} \quad M \in \Gamma.$$

Clearly, the invariants of Γ form a subring in R, denoted by R^Γ.

A character of the group Γ is a homomorphism of Γ into the multiplicative group of complex numbers. If χ is a character of Γ, then a polynomial $f \in \Gamma$ is called a χ-invariant of Γ if

$$Mf = \chi(M)f \quad \text{for all} \quad M \in \Gamma.$$

It is clear that the χ-invariants of Γ form a R^Γ-submodule in R which is denoted by R^Γ_χ.

A reflection of V is a transformation one of whose eigenvalues is equal to 1 and the other is distinct from 1. If P is a reflection, then the eigenvectors corresponding to 1 form a one-dimensional subspace in V, i.e., a line. This is called the reflecting line of P.

From now on we assume that Γ is generated by reflections. Let χ be a character of Γ and H be a line. Denote by $\Gamma(H)$ the subgroup in Γ consisting of those transformations which are identical on H. The determinant induces an injective homomorphism of $\Gamma(H)$ into the group $\mathbb{C}^*$ and hence $\Gamma(H)$ is cyclic. Let $s(\chi, H)$ denote the least nonnegative integer s such that

$$\chi(P) = (\det P)^s, \tag{1.1}$$

where P is any generator of $\Gamma(H)$. This is well defined. Let L_H be any linear form which determines the line H. This is determined uniquely up to a constant factor. For any character χ of Γ, set

$$h_\chi = \prod_H L_H^{s(\chi, H)}, \tag{1.2}$$

where H runs over different reflecting lines of reflections in Γ.

We shall need the following two lemmas.

Lemma 1.1. *Suppose that the Molien series of* Γ *is*

$$\Phi(\lambda) = \frac{1}{(1-\lambda^{d_1})\cdot(1-\lambda^{d_2})},$$

where d_1 *and* d_2 *are nonnegative integers. If* Θ_1 *and* Θ_2 *are algebraically independent homogeneous invariants of* Γ *having degrees* d_1 *and* d_2*, respectively, then*

$$R^\Gamma = \mathbb{C}[\Theta_1, \Theta_2].$$

Lemma 1.2. *Let* χ *be a character of* Γ*. Then* R^Γ_χ *is a free* R^Γ*-module of rank* 1 *and*

$$R^\Gamma_\chi = h_\chi R^\Gamma.$$

2. Group G**.** Let G denote the group generated by the matrices

$$A = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}.$$

Notice that $A^2 = E$ and $B^3 = E$. For any integers k and l, set

$$A(k,l) = B^k A B^l = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & \omega^l \\ 2\omega^k & -\omega^{k+l} \end{pmatrix}.$$

One can easily check that

$$A(k,l)\cdot A(m,n) = \begin{cases} B^{k+n} & \text{if } \ l+m \equiv 0 \ (\mathrm{mod}\ 3), \\ iA(k+2, n+2) & \text{if } \ l+m \equiv 1 \ (\mathrm{mod}\ 3), \\ -iA(k+1, n+1) & \text{if } \ l+m \equiv 2 \ (\mathrm{mod}\ 3). \end{cases}$$

This computation leads to

Lemma 2.1. G *is a disjoint union*

$$G = \{i^\alpha A(k,l)\} \cup \{i^\beta B^m\},$$

where $0 \le \alpha, \beta \le 3$, $0 \le k, l, m \le 2$.

This lemma implies in particular that G consists of 48 elements.

It is clear that among the transformations $i^\beta B^m$ only B and B^2 are reflections. A transformation $i^\alpha A(k,l)$ is not identical and therefore is a reflection if and only if 1 is a root of its characteristic polynomial, i.e., when

$$1 + \frac{i^\alpha}{\sqrt{3}}(\omega^{k+l} - 1) - (-1)^\alpha \omega^{k+l} = 0.$$

Considering separately the cases $\alpha = 0, 1, 2, 3$ we find that $i^\alpha A(k,l)$ is a reflection if and only if (α, k, l) is one of the following:

$$\begin{aligned} &(000),\ (021),\ (012),\ (200),\ (221),\ (212), \\ &(110),\ (101),\ (122),\ (320),\ (311),\ (302). \end{aligned} \tag{2.1}$$

Thus we have

Lemma 2.2. *The group G possesses 14 reflections. These are*

$$A_0 = B, \quad A_1 = A, \quad A_2 = B^2AB, \quad A_3 = BAB^2,$$
$$A_4 = -A, \quad A_5 = -B^2AB, \quad A_6 = -BAB^2, \quad A_7 = iBA,$$
$$A_8 = iAB, \quad A_9 = iB^2AB^2, \quad A_{10} = -iB^2A, \quad A_{11} = -iBAB,$$
$$A_{12} = -iAB^2, \quad A_{13} = B^2.$$

The vector $ae_1 + be_2 \in V$ is invariant under the reflection $i^\alpha A(k,l)$ if and only if

$$(i^\alpha - \sqrt{3})a + (i^\alpha \omega^l)b = 0.$$

Hence the reflecting line of $i^\alpha A(k,l)$ is given by the linear form

$$L = (i^\alpha - \sqrt{3})x + (i^\alpha \omega^l)y. \tag{2.2}$$

It is obvious that the reflecting line of both B and B^2 is given by the linear form $L = y$.

Denote by H_i the reflecting line of A_i and by L_i the corresponding linear form. Here $i = 0, ..., 13$. Substituting the triples (α, k, l) from table (2.1) into (2.2) we get the linear forms L_i $(i = 1, ..., 12)$. It is easy to see that

$$H_0 = H_{13}, \quad H_7 = H_{12}, \quad H_8 = H_{10}, \quad H_9 = H_{11}.$$

Thus we have

Lemma 2.3. *The reflections of G have 10 different reflecting lines determined by the following linear forms:*

$$\begin{array}{ll} L_0 = y, & L_1 = (1-\sqrt{3})x + y, \\ L_2 = (1-\sqrt{3})x + \omega y, & L_3 = (1-\sqrt{3})x + \omega^2 y, \\ L_4 = (1+\sqrt{3})x + y, & L_5 = (1+\sqrt{3})x + \omega y, \\ L_6 = (1+\sqrt{3})x + \omega^2 y, & L_7 = (i-\sqrt{3})x + iy, \\ L_8 = (i-\sqrt{3})x + i\omega y, & L_9 = (i-\sqrt{3})x + i\omega^2 y. \end{array}$$

3. Absolute Invariants of G. To begin with we remark that the group G^{tr} obtained from the group G by transposing its matrices was considered by Gleason when he studied the Hamming weight enumerator of a self-dual linear code over $GF(3)$. (See [1,3].) In particular, he computed the Molien series of this group. Since the transposition does not change the characteristic polynomial of a matrix, we can use his result. Letting Φ denote the Molien series of G we have

$$\Phi(\lambda) = \frac{1}{(1-\lambda^4)(1-\lambda^{12})}.$$

The series tells us that there are two algebraically independent invariants of degrees 4 and 12.

Lemma 3.1.

(a) *The polynomial* $f = x^4 + xy^3$ *is a unique* (*up to a nonzero constant multiple*) *homogeneous invariant of degree* 4.

(b) *The polynomial* $g = y^3(8x^3 - y^3)^3$ *is a unique* (*up to a nonzero constant multiple*) *homogeneous invariant of degree* 12 *which does not contain the term* x^{12}.

Proof. We remark that a polynomial which is invariant with respect to B must be a linear combination of monomials of the form

$$x^i y^{3j}.$$

(a) A homogeneous invariant of degree 4 has the form $ax^4 + bxy^3$ where a and b are the complex numbers and at least one of them is not zero. Since this polynomial is invariant with respect to A, we have

$$f = x(ax^3 + by^3) = \frac{1}{\sqrt{3}}(x + y)h(x, y), \tag{3.1}$$

where $h(x, y) = A(ax^3 + by^3)$. Putting $y = 1$ in (3.1) we get $x(ax^3 + b) = \frac{1}{\sqrt{3}}(x + 1)h(x, 1)$. It follows that the number -1 is a root of the binomial $ax^3 + b$, and so $a = b$. Taking $a = b = 1$ we get the polynomial f. Indeed, f is an invariant of A and B. This can be easily checked.

(b) A homogeneous invariant of degree 12 which does not contain x^{12} has the form

$$g = y^3(ax^9 + bx^6y^3 + cx^3y^6 + dy^9), \tag{3.2}$$

where $a,\ b,\ c,\ d$ are the complex numbers and at least one of them is not zero. The condition that this is invariant with respect to A implies that

$$y^3(ax^9 + bx^6y^3 + cx^3y^6 + dy^9) = \frac{1}{3\sqrt{3}}(2x - y)^3h(x, y), \tag{3.3}$$

where $h(x, y) = A(ax^9 + bx^6y^3 + cx^3y^6 + dy^9)$. Putting $y = 1$ in (3.3) we get

$$ax^9 + bx^6 + cx^3 + d = \frac{1}{3\sqrt{3}}(2x - 1)^3h(x, 1).$$

We see that the number $1/2$ is a root of the polynomial $ax^9 + bx^6 + cx^3 + d$ of multiplicity 3. Hence $1/2$ is a root of this polynomial and of its first and second derivatives as well.

We therefore have

$$\begin{cases} a(1/2)^9 + \quad b(1/2)^6 + \quad c(1/2)^3 + d & = 0, \\ 9a(1/2)^8 + \quad 6b(1/2)^5 + 3c(1/2)^2 & = 0, \\ 72a(1/2)^7 + 30b(1/2)^4 + 6c(1/2) & = 0. \end{cases} \tag{3.4}$$

Solving this system of linear equations we find that

$$a = -8^3 d, \quad b = 3 \cdot 8^2 d, \quad c = -3 \cdot 8 d.$$

System (3.4) has only one solution (up to a constant factor)

$$a = 8^3, \quad b = -3 \cdot 8^2, \quad c = 3 \cdot 8, \quad d = -1.$$

Substituting these values into (3.2) we get the polynomial g. It is easily checked that g is an invariant. □

Lemma 3.2. *The polynomials f and g are algebraically independent.*

Proof. We recall that the main term of a polynomial is defined to be the first term in its standard representation (see [3], for example.) Let $\sum_{i,j} c_{ij} f^i g^j = 0$, where $c_{ij} \in \mathbb{C}$. The main term of f is x^4, and the main term of g is $8^3 x^9 y^3$. Hence the main term of $f^i g^j$ is $8^{3j} x^{4i+9j} y^{3j}$. It is clear that different summands in the $\sum_{i,j} c_{ij} f^i g^j$ have different main terms. From this it follows that all c_{ij} are equal to 0. □

Applying now Lemma 1.1 we get

Proposition 3.1.

$$R^G = \mathbb{C}[f, g].$$

4. Relative Invariants of G. The determinant clearly induces a character of G. Let χ denote this character. Since $\det A = -1$ and $\det B = \omega$, the image of χ is the group $\mu_6 = \{\pm 1, \pm\omega, \pm\omega^2\}$. This is a cyclic group. Let G_1 be the kernel of χ. Clearly, G/G_1 is a maximal abelian quotient group of G, and since it is cyclic, we have

Lemma 4.1. *The characters of G are χ^k $(k = 0, \ldots, 5)$.*

Let us describe all R^G-modules

$$R_k^G = R_{\chi^k}^G = \left\{ f \in R | Mf = \chi^k(M) f, \forall M \in G \right\} \quad (k = 0, \ldots, 5).$$

We have

$$G(H_0) = \{B, B^2, E\}, \quad G(H_i) = \{A_i, E\} \quad (i = 1, \ldots, 6),$$
$$G(H_7) = \{A_7, A_{12}, E\}, \quad G(H_8) = \{A_8, A_{10}, E\}, \quad G(H_9) = \{A_9, A_{11}, E\}.$$

For any integer k and any positive integer m denote by $k \pmod m$ the least nonnegative residue of k modulo m. Applying (1.1) and Lemma 4.1, it is easy to see that

$$\begin{aligned} &s(\chi^k, H_i) = k \pmod 2 \quad (i = 1, \dots, 6;\ k = 0, \dots, 5), \\ &s(\chi^k, H_i) = k \pmod 3 \quad (i = 0, 7, 8, 9;\ k = 0, \dots, 5). \end{aligned} \tag{4.1}$$

By (1.2) we have

$$h_k = h_{\chi^k} = \prod_{i=0}^{9} L_i^{s(\chi^k, H_i)} \quad (k = 0, \dots, 5).$$

Applying Lemma 2.3 and (4.1) we find that

$$h_k = \varphi^{k \pmod 2} \psi^{k \pmod 3} \quad (k = 0, \dots, 5),$$

where

$$\varphi = -\prod_{j=0}^{2} \big((1-\sqrt{3})x + \omega^j y\big)\big((1+\sqrt{3})x + \omega^j y\big) = 8x^6 - 20x^3y^3 - y^6,$$

$$\psi = \frac{y}{i} \prod_{j=0}^{2} \big((1-\sqrt{3})x + i\omega^j y\big) = y(8x^3 - y^3).$$

So we have

$$h_0 = 1,\ \ h_1 = \varphi\psi,\ \ h_2 = \psi^2,\ \ h_3 = \varphi,\ \ h_4 = \psi,\ \ h_5 = \varphi\psi^2.$$

Applying now Lemma 1.2 we get

Proposition 4.1. *For $k = 0, \dots, 5$,*

$$R_k^G = h_k \mathbb{C}[f, \psi^3].$$

5. Proof of McEliece's Theorem. Let us introduce new variables

$$x = x_0, \quad y = x_1 + x_2, \quad z = x_1 - x_2.$$

The matrix α becomes then

$$\frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 0 \\ 2 & -1 & 0 \\ 0 & 0 & \sqrt{3}i \end{pmatrix}.$$

The matrix β does not change. Take any polynomial $P \in \mathbb{C}[x, y, z]$ and write it as

$$P = \sum_{k=0}^{\infty} p_k z^k$$

with $p_k \in \mathbb{C}[x, y]$. Certainly, for all but finitely many k, $p_k = 0$.

We have

$$\alpha P = \sum_{k=0}^{\infty} \alpha p_k \cdot \alpha z^k = \sum_{k=0}^{\infty} i^k (A p_k) z^k,$$
$$\beta P = \sum_{k=0}^{\infty} \beta p_k \cdot \beta z^k = \sum_{k=0}^{\infty} \omega^k (B p_k) z^k.$$

We see that P is invariant with respect to the transformations α and β if and only if, for all $k = 0, 1, 2, \ldots$

$$\begin{cases} p_k = i^k A p_k, \\ p_k = \omega^k B p_k. \end{cases} \tag{5.1}$$

Notice that if p is a nonzero polynomial in $\mathbb{C}[x, y]$ such that $p = i^k A p$ for some k, then k must be even. This is because $A^2 = E$. Thus system (5.1) takes the form

$$\begin{cases} p_k = i^{2k} A p_k, \\ p_k = \omega^{2k} B p_k. \end{cases}$$

This is equivalent to

$$\begin{cases} A p_k = (-1)^k p_k = \chi^{k \pmod 6}(A) p_k, \\ B p_k = \omega^k p_k = \chi^{k \pmod 6}(B) p_k. \end{cases} \tag{5.2}$$

System (5.2) is equivalent to the condition

$$p_k \in R^G_{k \pmod 6}.$$

Hence P is an invariant of $\overline{G}$ if and only if

$$P = \sum_{k=0}^{\infty} p_k z^{2k},$$

where $p_k \in \mathbb{C}[x, y]$. By Proposition 4.1,

$$p_k = h_{k \pmod 6} r_k, \quad r_k \in \mathbb{C}[f, \psi^3].$$

Therefore

$$P = \sum_{k=0}^{\infty} h_{k \pmod 6} r_k z^{2k} =$$
$$= \sum_{k=0}^{5} h_k z^{2k} \Big(\sum_{i=0}^{\infty} r_{k+6i} z^{12i} \Big) \in \bigoplus_{k=0}^{5} h_k z^{2k} \mathbb{C}[f, \psi^3, z^{12}].$$

It follows that the ring of invariants of the group $\overline{G}$ is

$$R^{\overline{G}} = \bigoplus_{k=0}^{5} h_k z^{2k} \mathbb{C}[f, \psi^3, z^{12}]. \qquad \square$$

References

1. 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.

2. C. L. Mallows, V. Pless, and N. J. A. Sloane, Self-dual codes over GF(3). *SIAM J. Appl. Math.* **31**(1976), 649–666.

3. F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes. *North-Holland, Amsterdam*, 1977.

4. N. J. A. Sloane, Error-correcting codes and invariant theory: new applications of a nineteenth-century technique, *Amer. Math. Monthly* **84**(1977), 82–107.

5. T. A. Springer, Invariant theory. *Lecture Notes in Math.* 585, *Springer-Verlag, Berlin*, 1977.

6. R. P. Stanley, Invariants of finite groups and their applications to combinatorics. *Bull. Amer. Math. Soc.* (*N.S.*) **1**(1979), 475–511.

(Received 12.09.95)

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