SOME GRADED RINGS COMING FROM CODING THEORY[1]

By Manabu Oura[2]

I will give an elementary example of an infinitely generated graded ring motivated by coding theory.

1. A linear code C of length n means a subspace of $\mathbf{F}_2^n$. C is called self-dual if it coincides with its dual code

$$C^{\perp} = \{x \in C | x \cdot y = \sum_i x_i y_i = 0, \ {}^{\forall} y \in C\}.$$

The number $wt(x)$ of non-zero coordinates of $x \in \mathbf{F}_2^n$ is called the weight of x. We say that C is doubly-even if the weight of x is congruent to 0 (mod 4) for all $x \in C$.

Examples of self-dual doubly-even codes are the $[8,4,4]$ extended Hamming code e_8 and the $[24,12,8]$ extended Golay code g_{24}.

For a linear code C of length n, a homogeneous polynomial W_C of degree[3] n defined by

$$W_C = W_C(x,y) = \sum_{v \in C} x^{n-wt(v)} y^{wt(v)}$$

is called the weight enumerator of C. We can show the identities

$$\begin{aligned} W_{C \oplus D} &= W_C W_D, \\ W_{C^{\perp}}(x,y) &= \frac{1}{|C|} W_C(x+y, x-y), \end{aligned}$$

where $\oplus$ denotes the direct sum of codes and $| * |$ the cardinality of $*$. The second identity is called the MacWilliams identity.

Examples of the weight enumerators are

$$\begin{aligned} W_{e_8} &= x^8 + 14x^4y^4 + y^8, \\ W_{g_{24}} &= x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}. \end{aligned}$$

---

[1]Talk at the conference “Algebraic Geometry, Number Theory, Coding Theory and Cryptography”, Tokyo, January 18, 2003.

[2]This work is supported in part by KAKENHI (No.14740081).

[3]Throughout this note, we assume that each degree of x and y is 1, thus the degree of $x^i y^j$ is $i + j$.

Let $\mathfrak{W}$ be the graded ring generated by the weight enumerators of all self-dual doubly-even codes of any length. We shall quickly describe the structure of $\mathfrak{W}$. Let C be a self-dual doubly-even code. Because of the self-duality, the MacWilliams identity gives the invariance property of the weight enumerators:

$$W_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}) = W_C(x,y).$$

The doubly-evenness, that is, $wt(v) \equiv 0 \pmod 4$ for any $v \in C$, gives the following:

$$W_C(x, iy) = W_C(x,y).$$

From these two identities, we can read off that, for each self-dual doubly-even code C, the weight enumerator W_C is invariant under the action of the group

$$G = \left\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle .$$

Here the action we are assuming is a natural one:

$$\sigma \cdot f(x,y) = f(ax+by, cx+dy)$$

for $f \in \mathbf{C}[x,y]$, $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. We note that G is a finite irreducible unitary reflection group of order 192. If we denote the invariant ring of G by $\mathbf{C}[x,y]^G$, we have

$$\mathbf{C}[W_{e_8},\ W_{g_{24}}] \subset \mathfrak{W} \subset \mathbf{C}[x,y]^G. \tag{1}$$

If we denote by $(\mathbf{C}[x,y]^G)_d$ the homogeneous polynomials of degree d in the invariant ring, then $(\mathbf{C}[x,y]^G)_d$ is a finite dimensional $\mathbf{C}$-vector space and each dimension $\dim(\mathbf{C}[x,y]^G)_d$ can be read off from the formula

$$\begin{aligned}\sum_{d\geq 0} \left(\dim(\mathbf{C}[x,y]^G)_d\right) t^d &= \frac{1}{|G|}\sum_{\sigma\in G} \frac{1}{\det(1-t\sigma)} \\ &= \frac{1}{(1-t^8)(1-t^{24})} \\ &= 1 + t^8 + t^{16} + 2t^{24} + 2t^{32} + 2t^{40} + 3t^{48} + \cdots .\end{aligned}$$

Since the two elements $W_{e_8},\ W_{g_{24}}$ are algebraically independent, we know that the ring $\mathbf{C}[W_{e_8},\ W_{g_{24}}]$ coincides with the invariant ring. Therefore the equality of the three graded rings in (1) holds. This is the structure theorem of $\mathfrak{W}$ (Gleason 1970).

2. We define another homogeneous polynomials coming from codes. Let C be a binary code of length n. For $r = 0, 1$, we define the r-th higher weight enumerator of the code C by

$$\begin{aligned} H_C^{(0)} &= H_C^{(0)}(x, y) = x^n, \\ H_C^{(1)} &= H_C^{(1)}(x, y) = W_C - H_C^{(0)} = W_C - x^n, \end{aligned}$$

where n denotes the length of C. These higher weight enumerators are homogeneous of degree n. We have

$$\begin{aligned} H_{C\oplus D}^{(1)} &= W_{C\oplus D} - x^{n_1+n_2} \\ &= W_C W_D - x^{n_1+n_2} \\ &= (H_C^{(1)} + x^{n_1})(H_D^{(1)} + x^{n_2}) - x^{n_1+n_2}, \end{aligned}$$

where $n_1,\ n_2$ denote the lengths of the codes $C,\ D$, respectively. In particular, for a code C of length n, we have

$$2x^n H_C^{(1)} = H_{C\oplus C}^{(1)} - (H_C^{(1)})^2. \tag{2}$$

For details, we refer to our paper "Higher Weights and Graded Rings for Binary Self-Dual Codes" by S. T. Dougherty, A. Gulliver, M. Oura and its references.

Examples of the $H_C^{(1)}$'s are

$$\begin{aligned} H_{e_8}^{(1)} &= 14x^4y^4 + y^8, \\ H_{g_{24}}^{(1)} &= 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}. \end{aligned}$$

As in the case of the weight enumerators, we consider the graded rings of the higher weight enumerators. We recall that a self-dual doubly-even code of length n exists if and only if $n \equiv 0 \pmod 8$. Using this fact, the graded ring generated by $H_C^{(0)}$ of all self-dual doubly-even codes C is just $\mathbf{C}[x^8]$. Let $\mathfrak{H}$ (resp. $\widetilde{\mathfrak{H}}$) be the graded ring generated by the $H_C^{(0)}$'s and the $H_C^{(1)}$'s (resp. the $H_C^{(1)}$'s) of all self-dual doubly-even codes C of any length.

3. The graded ring $\mathfrak{H}$ is a free $\mathbf{C}[x^8, H_{e_8}^{(1)}]$-module with the basis $1,\ H_{g_{24}}^{(1)}$, which is stated in our paper cited above. We shall sketch a proof of this fact. Let C be any self-dual doubly-even code of length n. The weight enumerator W_C can be written in the form $P(W_{e_8}, W_{g_{24}})$ for some polynomial $P(X, Y)$. This is a consequence of the structure theorem of $\mathfrak{W}$. Therefore we have

$$\begin{aligned} H_C^{(1)} &= W_C - x^n \\ &= P(W_{e_8}, W_{g_{24}}) - x^n \\ &= P(H_{e_8}^{(1)} + x^8, H_{g_{24}}^{(1)} + x^{24}) - x^n \end{aligned}$$

and this gives $\mathfrak{H} \subset \mathbf{C}[x^8, H_{e_8}^{(1)}, H_{g_{24}}^{(1)}]$, thus $\mathfrak{H} = \mathbf{C}[x^8, H_{e_8}^{(1)}, H_{g_{24}}^{(1)}]$. The computations show that we have

$$\mathfrak{H} = \mathbf{C}[x^8, H_{e_8}^{(1)}] \oplus \mathbf{C}[x^8, H_{e_8}^{(1)}] H_{g_{24}}^{(1)},$$

where $\oplus$ denotes the direct sum as modules.

4. The graded rings considered so far in this note are finitely generated. In this section, we will show that $\widetilde{\mathfrak{H}}$ is infinitely generated.

If

$$\begin{gathered} f = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_0 y^n, \\ a_n = \cdots = a_{\ell-1} = 0,\ a_\ell \neq 0, \end{gathered}$$

then we write $w(f) = \ell$. We put $w(0) = \infty$. For any code C, we have $w(H_C^{(1)}) < n$, where n denotes the length of C. This fact will be used below.

Preparing this, we shall show that $\widetilde{\mathfrak{H}}$ is infinitely generated. Assume that $\widetilde{\mathfrak{H}}$ is finitely generated: $\widetilde{\mathfrak{H}} = \mathbf{C}[H_{C_1}^{(1)}, \ldots, H_{C_k}^{(1)}]$. For any positive integer d, we denote by $\widetilde{\mathfrak{H}}^{(d)}$ the subring of $\widetilde{\mathfrak{H}}$ generated by all elements of $\widetilde{\mathfrak{H}}$ whose degrees are multiples of d. The degrees of the generators of $\widetilde{\mathfrak{H}}$ may be different, however, some subring of $\widetilde{\mathfrak{H}}$ is able to be generated by the elements whose degrees are the same. More precisely there exists a positive integer r such that $\widetilde{\mathfrak{H}}^{(r)}$ can be generated by the $F_1, \ldots, F_m$

whose degrees (as homogeneous polynomials in $\mathbf{C}[x,y]$) are r (*cf.* J. Igusa, "Theta Functions", Springer-Verlag, p.89 Lemma 3). Here we may take each F_i as a monomial of $H^{(1)}_{C_1}, \ldots, H^{(1)}_{C_k}$. Moreover we assume $w(F_1) \leq w(F_2) \leq \cdots \leq w(F_m)$. We remark that $w(F_m) < r$ because of the fact stated after the definition of $w(*)$. By the formula (2), $x^r F_m$ belongs to $\widetilde{\mathfrak{H}}^{(r)}$ and can be written in the form

$$x^r F_m = \sum (\text{const.}) F_i F_j.$$

But this is impossible because of $w(x^r F_m) = r + w(F_m) > w(F_i F_j)$ for any $i,\ j$. Hence $\widetilde{\mathfrak{H}}$ is infinitely generated.

Division of Mathematics
School of Medicine
Sapporo Medical University