An example of an infinitely generated graded ring motivated by coding theory

By Manabu Oura

Division of Mathematics, School of Medicine, Sapporo Medical University
Minami-1 Nishi-17, Chuo-ku, Sapporo, Hokkaido 060-8556

(Communicated by Heisuke Hironaka, M. J. A., Oct. 14, 2003)

Abstract: Let $\widetilde{\mathfrak{H}}^{(g)}$ be the graded ring generated by the r-th higher weight enumerators of all codes of any length, $1 \le r \le g$. In this note we will prove that $\widetilde{\mathfrak{H}}^{(g)}$ is not finitely generated.

Key words: Code; weight enumerator; higher weight enumerator; graded ring.

1. Preliminaries. Let q be a power of an arbitrary prime number and $\mathbf{F}_q$ the field of q elements. A code C of length n means a subspace of $\mathbf{F}_q^n$. For the details of coding theory and the weight enumerators we shall next define, we refer to [4] and its references.

Let C be a code of length n. For a positive integer g we define the g-th complete weight enumerator $W_C^{(g)}(x_a : a \in \mathbf{F}_q^g)$ of the code C by

$$W_C^{(g)}(x_a : a \in \mathbf{F}_q^g) = \sum_{v_1,\dots,v_g \in C} \prod_{a \in \mathbf{F}_q^g} x_a^{n_a(v_1,\dots,v_g)},$$

where $n_a(v_1,\dots,v_g)$ denotes the number of i such that $a = (v_{1i},\dots,v_{gi})$. This is a homogeneous polynomial of degree*) n. Direct computation shows

$$(1) \qquad W_{C_1 \oplus C_2}^{(g)}(x_a : a \in \mathbf{F}_q^g) = W_{C_1}^{(g)}(x_a : a \in \mathbf{F}_q^g) \cdot W_{C_2}^{(g)}(x_a : a \in \mathbf{F}_q^g)$$

for codes C_1 and C_2, where $\oplus$ denotes the direct sum of codes.

Let C be a code of length n. We write $W_C^{(g)}(x,y)$ after transforming the variables of $W_C^{(g)}(x_a : a \in \mathbf{F}_q^g)$ as

$$x_a \rightsquigarrow \begin{cases} x & \text{if } a = 0 \in \mathbf{F}_q^g, \\ y & \text{otherwise.} \end{cases}$$

We define the 0-th higher weight enumerator by $H_C^{(0)}(x,y) = x^n$ and for a positive integer g we inductively define the g-th higher weight enumerator $H_C^{(g)}(x,y)$ by the formula

$$(2) \qquad W_C^{(g)}(x,y) = \sum_{0 \le r \le g} [g]_r H_C^{(r)}(x,y),$$

where $[g]_0 = 1$ and $[g]_r = (q^g - q^{r-1})(q^g - q^{r-2}) \cdots (q^g - q)(q^g - 1)$ for $1 \le r \le g$. Compare with [1, 2].

2. Result. Let $\widetilde{\mathfrak{H}}^{(g)}$ be the ring generated by the $H_C^{(r)}(x,y)$'s, $1 \le r \le g$, of all codes of any length over the complex number field $\mathbf{C}$. Our result in this note is

Theorem. *The ring $\widetilde{\mathfrak{H}}^{(g)}$ is not finitely generated.*

In order to prove Theorem we need the following

Lemma. *Let C be a code of length n. Then $x^n H_C^{(r)}(x,y)$ is contained in $\widetilde{\mathfrak{H}}^{(g)}$ for any r, $1 \le r \le g$.*

Proof of Lemma. We prove this by induction on r. Recall that C is a code of length n.

If $r = 1$, we have

$$W_{C \oplus C}^{(1)}(x,y) = x^{2n} + H_{C \oplus C}^{(1)}(x,y).$$

Using the identity (1), we have

$$2x^n H_C^{(1)}(x,y) = H_{C \oplus C}^{(1)}(x,y) - \left(H_C^{(1)}(x,y)\right)^2.$$

The right hand side of this formula, thus $x^n H_C^{(1)}(x,y)$, lies in $\widetilde{\mathfrak{H}}^{(g)}$.

Suppose that $r \ge 2$. Considering $C \oplus C$ instead of C in the identity (2), we have

$$\left(\sum_{i=0}^{r} [r]_i H_C^{(i)}(x,y)\right)^2 = \sum_{i=0}^{(r)} [r]_i H_{C \oplus C}^{(i)}(x,y),$$

or,

$$2x^n H_C^{(r)}(x,y) = \sum_{i=1}^{r} [r]_i H_{C \oplus C}^{(i)}(x,y)$$

2000 Mathematics Subject Classification. 11T71, 94B05.

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

$$
-\left\{\left(\sum_{i=1}^{r-1}[r]_i H_C^{(i)}(x,y)\right)^2 + \left([r]_r H_C^{(r)}(x,y)\right)^2 + 2x^n\left(\sum_{i=1}^{r-1}[r]_i H_C^{(i)}(x,y)\right) + 2\left(\sum_{i=1}^{r-1}[r]_i H_C^{(i)}(x,y)\right)[r]_r H_C^{(r)}(x,y)\right\}.
$$

Applying the induction hypothesis to the right hand side of this identity, we conclude that $x^n H_C^{(r)}(x,y)$ lies in $\widetilde{\mathfrak{H}}^{(g)}$. This completes the proof of Lemma. □

Proof of Theorem. If

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

then we write $w(f) = -\ell$. We put $w(0) = \infty$. For any code C of length n and any positive integer r, we have $w(H_C^{(r)}(x,y)) > -n$. This fact will be used below.

Preparing this, we shall show that $\widetilde{\mathfrak{H}}^{(g)}$ is not finitely generated. Assume that $\widetilde{\mathfrak{H}}^{(g)}$ is finitely generated: $\widetilde{\mathfrak{H}}^{(g)} = \mathbf{C}[H_{C_1}^{(i_1)}(x,y), \ldots, H_{C_k}^{(i_k)}(x,y)]$. For a positive integer d, we shall denote by $\widetilde{\mathfrak{H}}^{(g)}(d)$ the subring of $\widetilde{\mathfrak{H}}^{(g)}$ generated by all elements of $\widetilde{\mathfrak{H}}^{(g)}$ whose degrees are multiples of d. The degrees of the generators of $\widetilde{\mathfrak{H}}^{(g)}$ may be different, however, a certain subring of $\widetilde{\mathfrak{H}}^{(g)}$ is able to be generated by the elements whose degrees are the same. More precisely there exists a positive integer r such that $\widetilde{\mathfrak{H}}^{(g)}(r)$ can be generated by the $F_1, \ldots, F_m$ whose degrees (as homogeneous polynomials in $\mathbf{C}[x,y]$) are r (*cf.* [3], p. 89 Lemma 3). Here we may take each F_i as a monomial of $H_{C_1}^{(i_1)}(x,y), \ldots, H_{C_k}^{(i_k)}(x,y)$. Moreover we assume $w(F_1) \geq w(F_2) \geq \cdots \geq w(F_m)$. We remark that $w(F_m) > -r$ because of the fact stated after the definition of $w(*)$. By Lemma, $x^r F_m$ belongs to $\widetilde{\mathfrak{H}}^{(g)}(r)$ and must be written in the form

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

But this is not the case because of the fact $w(x^r F_m) = -r + w(F_m) < w(F_i F_j)$ for every i, j. Hence $\widetilde{\mathfrak{H}}^{(g)}$ is not finitely generated. □

Acknowledgement. This work is supported in part by KAKENHI (No. 14740081).

References

[1] Dougherty, S. T., Gulliver, T. A., and Oura, M.: Higher weights and binary self-dual codes. Discrete Appl. Math. **128**, 121–143 (2003).

[2] Dougherty, S. T., Gulliver, T. A., and Oura, M.: Higher weights for ternary and quaternary self-dual codes. (Preprint).

[3] Igusa, J.: Theta Functions. Grundlehren der Math. Wiss. vol. 194, Springer, Berlin-Heidelberg-New York (1972).

[4] Nebe, G., Rains, E. M., and Sloane, N. J. A.: The invariants of the Clifford groups. Designs, Des. Codes Cryptogr., **24**, 99–121 (2001).