AN EXAMPLE OF AN INFINITELY GENERATED GRADED RING MOTIVATED BY CODING THEORY

By Manabu OURA[1]

Abstract

Let $\widetilde{\mathfrak{H}}^{(g)}$ be the graded ring generated by the r-th higher weight enumerators of all codes of any length, $1 \leq r \leq g$. In this note we will prove that $\widetilde{\mathfrak{H}}^{(g)}$ is infinitely generated.

1. *Preliminaries.* Let $\mathbf{F}_q$ be 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 and $W_C^{(g)}(x_a : a \in \mathbf{F}_q^g)$ the g-th complete weight enumerator of the code C, that is,

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

where $n_a(v_1,\ldots,v_g)$ denotes the number of i such that $a = (v_{1i},\ldots,v_{gi})$. This is a homogeneous[2] polynomial of degree n. Direct computation shows

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

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

We write $W_C^{(g)}(x,y)$ after transforming the variables of $W_C^{(g)}(x_a : a \in \mathbf{F}_2^g)$ as

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

We inductively define the r-th weight enumerator by the identity

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

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

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

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. Our result in this note is

Theorem. The ring $\widetilde{\mathfrak{H}}^{(g)}$ is infinitely 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. We prove this by induction on r. Let C be 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,

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

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

Proof of Theorem. If

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

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 infinitely 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, 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 $w(F_1) \leq w(F_2) \leq \cdots \leq w(F_m)$. We remark that $w(F_m) < r$ because of the fact stated after the definition of $w(*)$. By Lemma, $x^r F_m$ belongs to $\widetilde{\mathfrak{H}}^{(g)}(r)$ 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 $\widetilde{\mathfrak{H}}^{(g)}$ is infinitely generated.

Division of Mathematics
School of Medicine
Sapporo Medical University

References

[1] Dougherty, S. T., Gulliver, T. A., Oura, M., Higher weights and binary self-dual codes, to appear in Discrete Applied Math.

[2] Dougherty, S. T., Gulliver, T. A., Oura, M., Higher Weights for Ternary and Quaternary Self-Dual Codes, preprint.

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

[4] Nebe, G., Rains, E. M., Sloane, N. J. A., The invariants of the Clifford groups, Designs, Codes and Cryptography, **24** (2001), 99–122.