符号の重み多項式にまつわる歴史[1]

大浦 学[2]
札幌医科大学医学部数学教室

知られている結果を組み合わせることにより, 符号の重み多項式を古典的不変式論の立場から眺めたいと思います.

符号と重み多項式

まず, 符号とそこから得られる多項式 (重み多項式) について述べます. $\mathbf{F}_2 = \{0, 1\}$ は二元体を表すものとします. $\mathbf{F}_2^n$ の部分空間 C を長さ n の線型符号と言います. "線型" を省略することもあり, この講演でもそうします. $\mathbf{F}_2^n$ には標準的な内積 $(x, y) = \sum_i x_i y_i$ をいれ, これにより C の双対符号 $C^\perp := \{x \in \mathbf{F}_2^n | (x, y) = 0, \ ^\forall y \in C\}$ を考えることができます. 符号がその双対符号と一致する ($C = C^\perp$) とき, C は自己双対符号であると言われます. $\mathbf{F}_2^n$ の元 v の重さとは non-zero coordinate の数をいい, $wt(v)$ で表します. C の全ての元の重さが 4 の倍数であるとき, C は重偶符号であると言われます. 以下では自己双対重偶符号を主に考えていくことになります.

例をあげます. 最初に考える自己双対重偶符号は 4 つのベクトル

$$(11110000), \ (00111100), \ (00001111), \ (10101010)$$

で生成される $\mathbf{F}_2^8$ の 4 次元部分空間 e_8 でここでは単にハミング符号と呼ぶことにします (詳しくは $[8, 4, 4]$ 拡張ハミング符号). もう一つ, $\mathbf{F}_2^{24}$ 内の 12 次元部分空間であるゴーレイ符号 g_{24} を取り扱いますが, 定義は省略します.

次に符号の重み多項式を定義します. C を長さ n の符号とするとき, C の重み多項式 $W_C(x, y)$ は次で定義されます:

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

定義からわかるようにこの多項式は次数 n の斉次多項式です. 簡単な例で計算してみると, たとえば $C = \{(00), (11)\}$ に対して

$$\begin{aligned} W_C(x, y) &= x^{2 - wt((00))} y^{wt((00))} + x^{2 - wt((11))} y^{wt((11))} \\ &= x^2 + y^2 \end{aligned}$$

となります. 先にあげた自己双対重偶符号 e_8, g_{24} については

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

です. 自己双対重偶符号の重み多項式に関して言うと, "ある意味" $W_{e_8}(x, y)$ と $W_{g_{24}}(x, y)$ で十分なことが分かります. つまり, 任意の自己双対重偶符号の重み多項式は $W_{e_8}(x, y)$ と $W_{g_{24}}(x, y)$ の多項式として表すことができます. このとき, 係数には有理数があらわれますが, 分母には $2, 3, 7$ しかあらわれません. ここでは次のような解釈をしておきます: $\mathfrak{W}$ を全ての自己双対重偶符号の重み多項式達から生成される $\mathbf{C}$ 上の次数付き環とするとき, $\mathfrak{W}$ は代数的独立な二つの元 $W_{e_8}(x, y)$ と $W_{g_{24}}(x, y)$ で生成される (Gleason, 1970).

---

[1] "数学史シンポジウム" (世話人 杉浦光夫, 笠原乾吉, 長岡一昭), 津田塾大学, 2003 年 10 月 25 日

[2] 科研費 (No.14740081) の援助を受けています.

符号を利用したモジュラ形式の構成

次に符号理論を応用してモジュラ形式を構成します. 間を取り持つのはテータ函数です. テータ函数を

$$\theta_{ab}(\tau,z)=\sum_{n\in\mathbf{Z}}\exp 2\pi\sqrt{-1}\left\{\frac{1}{2}\tau\left(n+\frac{a}{2}\right)^2+\left(n+\frac{a}{2}\right)\left(z+\frac{b}{2}\right)\right\}$$

とおきます. ここで, $\tau\in\mathfrak{H}$(= 上半空間), $z\in\mathbf{C}$, $a,b\in\{0,1\}$ です. 今, C を長さ n の自己双対重偶符号とします. ここで述べたかったモジュラ形式の構成というのは

$$W_C(\theta_{00}(2\tau,0),\theta_{10}(2\tau,0))\text{ は }SL(2,\mathbf{Z})\text{ に関する重さ }\frac{n}{2}\text{ のモジュラ形式である}$$

という事実です. $x\mapsto\theta_{00}(2\tau,0)$, $y\mapsto\theta_{10}(2\tau,0)$ を Broué-Enguehard map と呼ぶことにします.

$\mathfrak{M}$ を $SL(2,\mathbf{Z})$ に関するモジュラ形式のなす ($\mathbf{C}$ 上の) 次数付き環としますと, この環は代数的に独立な二つの Eisenstein series $E_4(\tau)$, $E_6(\tau)$ で生成されます. ここで Eisenstein series は正規化されているとします: $E_k(\tau)=1+\cdots$, $k=4,6$. さらに重さ 12 の尖点形式 $\Delta(\tau)=q+\cdots$, $q=\exp 2\pi\sqrt{-1}\tau$, も準備しておきます. これらの間には関係式

$$2^6 3^3\Delta(\tau)=E_4(\tau)^3-E_6(\tau)^2$$

が成り立ちます. 一般に次数付き環 $A=A_0\oplus A_1\oplus A_2\oplus\cdots$ に対して $A^{(d)}=A_0\oplus A_d\oplus A_{2d}\oplus\cdots$ と書くことにすると, $\mathfrak{M}$ には重さが奇数の元がないので $\mathfrak{M}=\mathfrak{M}^{(2)}$ です. さらに, $\mathfrak{M}^{(4)}=\mathbf{C}[E_4(\tau),\Delta(\tau)]$ です. 自己双対重偶符号は長さ n が 8 の倍数のときに存在し, またそのときのみ存在することを考えると, 符号理論とは $\mathfrak{M}$ よりも $\mathfrak{M}^{(4)}$ の方が話しが合いそうです. 実は先の Broué-Enguehard map は degree-preserving な同型

$$\begin{array}{rcl}\mathfrak{W} & \xrightarrow{\sim} & \mathfrak{M}^{(4)}\\ W_{e_8}(x,y) & \longmapsto & W_{e_8}(\theta_{00}(2\tau,0),\theta_{10}(2\tau,0))=E_4(\tau)\\ W_{g_{24}}(x,y) & \longmapsto & W_{g_{24}}(\theta_{00}(2\tau,0),\theta_{10}(2\tau,0))=E_4(\tau)^3-2^5 3\cdot 7\Delta(\tau)\end{array}$$

を与えます.

不変式環の関係

上で述べてきたことは様々な方向に拡張されています. Rains, E. M., Sloane, N. J. A., Self-dual codes, in Handbook of coding theory, Vol. I, II, 177–294, North-Holland, Amsterdam, 1998, 及び, そこに挙げてある参考文献を参照してください. さて, 今までにでてきた言葉を使って最初に述べたことを言い換えると, $\mathfrak{W}$ を古典的な不変式論から眺める, ということになります. そこで次に (ここで意味する) 古典的不変式論について Schur の講義録をもとに解説します. $SL(2,\mathbf{C})$ を

$$f=\sum_{i=0}^{4}\binom{4}{i}u_i x^{4-i}y^i$$

に自然に作用させます. これを

$$f'=\sum_{i=0}^{4}\binom{4}{i}u'_i x^{4-i}y^i$$

と等しいとおくことにより, $SL(2,\mathbf{C})$ の $\mathbf{C}[u_0,u_1,u_2,u_3,u_4]$ への作用が定まります. その不変式環を $S(2,4)$ と表すことにします. 2 は f の変数 (ここでは x,y のこと) の数, 4 は斉次多項式 f の

次数を表しています. この環 $S(2,4)$ は二つの代数的独立な元

$$P = u_0u_4 - 4u_1u_3 + 3u_2^2,$$
$$Q = \det \begin{pmatrix} u_0 & u_1 & u_2 \\ u_1 & u_2 & u_3 \\ u_2 & u_3 & u_4 \end{pmatrix}$$

で生成されます. 以上で言葉は揃いました. この講演で述べたかったことは重み多項式環 $\mathfrak{W}$ と $SL(2,\mathbf{C})$ に関する不変式環 $S(2,4)$ の関係です. 井草準一は論文 "Modular forms and projective invariants", Amer.J.Math., 89(1967), 817–855, のなかで, ある条件のもとで $\Gamma_g = Sp(g,\mathbf{Z})$ に関するジーゲルモジュラ形式のなす環から $S(2,2g+2)$ への写像 ρ を与えています. この ρ は一般に上への同型を与えませんが, 我々の場合 ($g=1$), $\rho : \mathfrak{M} \xrightarrow{\sim} S(2,4)$ となります. ここで $\rho(E_4(\tau)) = 2^2 3P$, $\rho(E_6(\tau)) = 2^3 3Q$ です (記号の取り方が井草の論文とは異なっています). 先の Broué-Enguehard map と ρ との合成を考えますと, degree-preserving な同型

$$\begin{aligned} \mathfrak{W} &\xrightarrow{\sim} S(2,4)^{(2)} \\ W_{e_8}(x,y) &\longmapsto 2^2 3P \\ W_{g_{24}}(x,y) &\longmapsto 2^5 3(11P^3 + 3^3 7Q^2) \end{aligned}$$

が得られます. これがこの講演で述べたかったことです. $\mathfrak{W}$ は位数 192 の群

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

の不変式環と一致することが知られており, 上の同型は有限群 G の不変式環から $SL(2,\mathbf{C})$ の不変式環の部分環への同型写像と見ることができます. この辺りの話しは Oura, M., "Observation on the weight enumerators from classical invariant theory", preprint, に書きました.