Riemann 予想を満たさない extremal な不変式の構成

近畿大学　理工学部　知念 宏司　(Koji Chinen)
Department of Mathematics, School of Science and Engineering, Kindai University.

概 要

Iwan Duursma は 1999 年に「線型符号の zeta 関数」を導入した. そして「extremal 自己双対符号の重み多項式はすべて Riemann 予想を満たすか ?」という問題を提出, 自身も Type IV extremal 自己双対符号の一部の系列に対してこの問題を肯定的に解決している (2003 年). 符号に直接関連する不変式に対しては現在までに上記問題の反例は見つかっていないと思われる. しかしながら, 符号と関連をもたない不変式にまで考察の対象を広げると, exrtemal と呼ばれるべき性質をもちながら, Riemann 予想を満たさない不変式が具体的に構成できる. これは上記問題への広い意味での反例とも考えられる. 本稿ではこの結果について報告する.

1　導入 — Duursma の理論

素数 p に対して, $q = p^r$ $(r \geq 1)$ とし, C を有限体 $\mathbf{F}_q$ 上の $[n, k, d]$ 符号とする. また C の重み多項式を

$$W_C(x, y) := \sum_{i=0}^{n} A_i x^{n-i} y^i$$

とする. さらに, このあと d および $C^\perp$ の最小距離 $d^\perp$ は $d, d^\perp \geq 2$ を満たすとする. このとき, C の zeta 関数は次のように定義される:

定 義 1.1 C に対して, 次数 $n - d$ 以下のある多項式 $P(T) \in \mathbf{Q}[T]$ がただ 1 つ存在して,

$$\frac{P(T)}{(1-T)(1-qT)}(y(1-T) + xT)^n = \cdots + \frac{W_C(x, y) - x^n}{q-1} T^{n-d} + \cdots$$

が成立する. $P(T)$ を C の **zeta 多項式**, $Z(T) := P(T)/\{(1-T)(1-qT)\}$ を C の **zeta 関数**と呼ぶ.

$P(T)$ の存在と一意性は初等的に証明できる (例えば [2], [4, Appendix A] を参照). 符号 C が自己双対である場合には, $P(T)$ は次の形の関数等式を満たす:

命 題 1.2 $C^\perp = C$ のとき, $g = n/2 - 1 + d$ とすると,

$$P(T) = P\Big(\frac{1}{qT}\Big) q^g T^{2g} \tag{1.1}$$

が成り立つ.

これは代数曲線の zeta 多項式が満たす関数等式と同じ形である．また上の g を, これも代数曲線からの類似で符号 C の種数と呼んでいる．そこで自己双対符号の Riemann 予想を次のように定義する:

定 義 1.3 C を $\mathbf{F}_q$ 上の自己双対符号, その zeta 多項式を $P(T)$ とする．$P(T)$ の任意の根 α に対して,

$$|\alpha| = \frac{1}{\sqrt{q}}$$

が成り立つとき, C は Riemann 予想を満たすという．

自己双対符号の Riemann 予想に関して, Duursma は

問 題 1.4 「Extremal な自己双対重み多項式は Riemann 予想を満たす」は正しいか．

という問題を提起している ([10, Open Problem 4.2])．Extremal な自己双対符号は最小距離が大きく, 誤り訂正能力の高い符号であるから, これはある意味で, 性能のよい符号は Riemann 予想を満たすかどうかを問うているものと考えられ, 応用上も興味深いものである (extremal 自己双対符号の定義についてはあとの定義 3.2, また例えば Pless [17, p.139] を参照)．Duursma 自身は, extremal Type IV 自己双対符号のうち, 符号長が 6 で割り切れる系列に対して, 問題 1.4 を肯定的に解決している ([11])．のちにこれは, 同じく extremal Type IV 自己双対符号で, 符号長が 6 で 割って 4 余る系列に対しても正しいことが示された (奥田 [15])．その他の系列では証明されていないが, 反例 (extremal であって Riemann 予想を満たさない自己双対符号の例) は見つかっていない．

なお, extremal 自己双対符号で実在するものが有限個しかないことは古くから知られているから (MacWilliams-Sloane [13, Ch. 19, §5], Duursma [11] などを参照), 問題 1.4 は数値計算で片のつく問題と考えられるかも知れないが, 対応する符号が実在するかどうかにかかわらず, 重み多項式は無限系列として構成できるため, これは実在の符号よりも, 重み多項式そのものに関する問題と捉えた方がよいのである．

こうしたことから, 符号の zeta 関数の本質をよりよく理解するために, 必ずしも符号とは関連をもたないが, (自己双対) 符号の重み多項式に近い性質をもつ, より幅広い範囲の不変式を考察の対象に加えるという立場に到達する．そして実際, そのような不変式で, extremal と呼ばれるべき性質をもちながら, Riemann 予想を満たさないものの実例が構成できるのである．これは問題 1.4 の広い意味での反例ともいうべきもので, 符号および不変式の Riemann 予想が妥当な意味をもつ枠組みが何であるか, 再考を迫る事実といえるのではなかろうか．以下の節で, その具体的構成について見ていこう (実在の符号の zeta 関数については [1], [2], [12] にも概説がある)．

2　不変式への拡張とその探索

このあと, $W(x,y)$ は

$$W(x,y) = x^n + A_d x^{n-d} y^d + \cdots \in \mathbf{C}[x,y] \quad (A_d \neq 0) \tag{2.1}$$

の形の n 次斉次多項式で, MacWilliams 変換

$$\sigma_q = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}$$

によって不変 ($W^{\sigma_q}(x,y) = W(x,y)$) であるものとする (以下, σ_q-不変という). ただし, 1 次変換

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

の $f(x,y) \in \mathbf{C}[x,y]$ への作用は $f^\sigma(x,y) = f(ax+by, cx+dy)$ で与えられる. また, 必ずしも符号と関連をもたない不変式を考えるため, σ_q における q の制限は

$$q > 0, \quad q \neq 1 \tag{2.2}$$

程度の緩やかなものとする. さらに, "divisible" という条件を考える: (2.1) において, ある $c \in \mathbf{N}$, $c > 1$ が存在して

$$A_i \neq 0 \Rightarrow c|i$$

が成り立つとき, $W(x,y)$ は "divisible by c" であるという.

なお, $W^{\sigma_q}(x,y) = W(x,y)$ の代わりに $W^{\sigma_q}(x,y) = -W(x,y)$ を満たす多項式 $W(x,y)$ も存在する. この場合, $W(x,y)$ は formal weight enumerator と呼ばれる. この呼び名は Ozeki [16] によって導入された.

例 2.1 (1) $W_8(x,y) = x^8 + 14x^4y^4 + y^8$. これは拡大 Hamming 符号の重み多項式であり, σ_2-不変, かつ divisible by 4 である.

(2) $W_{12}(x,y) = x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12}$. これは $q = 2$ に対する formal weight enumerator で divisible by 4 である. これはまた [16] において, Eisenstein 級数 $E_6(z)$ の構成に用いられた.

実在の divisible な自己双対符号に関しては, 次の定理がある:

定 理 2.2 (Gleason-Pierce) 体 $\mathbf{F}_q$ 上の自己双対符号が divisible by c であるのは

$$(q,c) = (2,2), (2,4), (3,3), (4,2)$$

の場合か, 重み多項式が

$$W_{2,q}(x,y) = x^2 + (q-1)y^2 \tag{2.3}$$

(q は任意) のべきで表される自明な場合のみである.

証 明. Sloane [19]. ▮

この定理によれば, 実在の符号に関連する σ_q-不変な多項式で, なおかつ divisible であるものが存在する q は非常に少ないことがわかる. しかし, 符号から離れた場合はどうであろうか ? そこでこのあと, divisible by 2 で, σ_q-不変な (2.1) の形の多項式 $W(x,y)$ を探索する (divisible by 2 である formal weight enumerator についても, 最後に少し述べる). 探索の道具は次の binomial moment 公式である:

補 題 2.3 (2.1) の形の多項式 $W(x,y)$ が $W^{\sigma_q}(x,y) = \pm W(x,y)$ を満たすとき, $\nu = 0,1,\cdots,n$ に対して

$$\sum_{i=0}^{n-\nu} \binom{n-i}{\nu} A_i = \pm q^{\frac{n}{2}-\nu} \sum_{i=0}^{\nu} \binom{n-i}{n-\nu} A_i \tag{2.4}$$

が成り立つ.

証 明. 関係式 $W^{\sigma_q}(x,y) = \pm W(x,y)$ において $y=1$ として x について ν 回微分し, 次いで $x=1$ とすればよい ([13, p.131, Problem (6)] も参照). ∎

補題 2.3 の複号のうち, マイナスは formal weight enumerator の場合で, プラスが σ_q-不変の場合である. また, (2.4) 式は, $W(x,y)$ の係数 A_i たちが満たす斉次連立 1 次方程式と見ることができる.

さて, 補題 2.3 はいくつかの場合に適用できるが, いま $W(x,y)$ が σ_q-不変で $n = \deg W(x,y) = 2k+1$ の場合を考える. すると, ν を 0 から $2k+1$ まで動かして得られる $2k+2$ 個の式のうち, 後半の $k+1$ 個は前半 $k+1$ 個と本質的に同じであることが, 少しの計算でわかる. さらに $W(x,y)$ が divisible by 2 であることから, 係数 $A_0, A_1, \cdots, A_{2k+1}$ のうち, 添字が奇数の $k+1$ 個は 0 である. したがって本質的な未知数の個数は $k+1$ 個となる. つまり, 連立 1 次方程式系としては, 未知数の個数と方程式の個数が一致する場合であり, 係数行列が正方行列となる場合である. しかも $A_0 = 1$ であるから, この連立 1 次方程式系は非自明な解をもつ. したがって, 係数行列を $C(n,q)$ ($n = \deg W(x,y)$) とおくとき, その行列式について $|C(n,q)| = 0$ でなければならない. この式は q を含むので, これを解くことで σ_q-不変式が存在する q の候補が得られる. こうして σ_q-不変式探索の 1 つのアルゴリズムが得られる.

注 意. 実在の自己双対符号 C で divisible by 2 である重み多項式 $W_C(x,y)$ に上記を適用すると, まず $n = \deg W_C(x,y)$ は偶数である. このときも (2.4) 式における本質的未知数はやはり $n/2$ 個であるが, $\nu = n/2$ の場合に (2.4) 式は自明な式となり, 本質的な方程式の個数 ($n/2 - 1$ 個) は未知数の個数より少なくなる. したがってこの場合, 上記の方法で q の候補を決めることはできない.

例 2.4 $n=5$ ($k=2$) として 5 次の不変式が存在する q の候補を求めてみる.

$$C(5,q) = \begin{pmatrix} 1-q^2\sqrt{q} & 1 & 1 \\ 5(1-q\sqrt{q}) & 3 & 1 \\ 10(1-\sqrt{q}) & 3-\sqrt{q} & 0 \end{pmatrix}$$

となり, $|C(5,q)| = -(t-1)^3(t+2)(t^2-2t-4)$ ($\sqrt{q} = t$) がわかる. よって $|C(2,q)| = 0$ から $t = 1+\sqrt{5}$ が出て, $q = (1+\sqrt{5})^2 = 6+2\sqrt{5}$ が得られる.

実際に $q = 6+2\sqrt{5}$ のときに 5 次の σ_q-不変式が存在するかどうかは, 目標の式を $W(x,y) = x^5 + A_2x^3y^2 + A_4xy^4$ とおいて, これが $\sigma_{6+2\sqrt{5}}$ で不変となる条件から A_2, A_4 を決めてやればよい. やってみると,

$$\psi_5(x,y) = x^5 - (50+20\sqrt{5})x^3y^2 + (225+100\sqrt{5})xy^4 \tag{2.5}$$

が条件を満たすことがわかり, 5 次の不変式が見つかった.

注 意. (1) $n = 3$ の場合は

$$C(3, q) = \begin{pmatrix} 1 - q\sqrt{q} & 1 \\ 3(1 - \sqrt{q}) & 1 \end{pmatrix}$$

となって $|C(3, q)| = -(\sqrt{q} + 2)(\sqrt{q} - 1)^2$, したがって $q > 0$ の範囲では $q = 1$ しかなく, 非自明な不変式は存在しない.

(2) Formal weight enumerator の場合, divisible by 2 で偶数次のものが, 同様のアルゴリズムで求まる. それによると, $q = 2$ (4 次), $q = 4/3$ (6 次), $q = 4 \pm 2\sqrt{2}$ (8 次) などで formal weight enumerator が見つかる (最後の節で少し詳しく述べるが, 詳しくは [6] を参照). またこの場合の q の値は, 第 1 種 Chebyshev 多項式の根を用いて記述できるのではないかという指摘が, 山岸正和氏 (名古屋工大) によってなされている ([6]).

このあと, (2.5) をもとにして, 新しい不変式環を構成し, Riemann 予想を調べていく.

3 不変式環の構成と Mallows-Sloane bound の類似

まず実在の自己双対符号の場合の Mallows-Sloane bound と extremal 自己双対符号について整理しよう. Gleason-Pierce の定理 (定理 2.2) によって, 非自明な divisible 自己双対符号が存在するのは $(q, c) = (2, 2), (2, 4), (3, 3), (4, 2)$ の場合であることがわかるが, これらは順にそれぞれ Type I, II, III, IV と呼ばれる. そして各 Type に対し, 最小距離 d を 符号長 n で評価する限界式がある. それが Mallows-Sloane bound である:

定 理 3.1 各 Type の $[n, n/2, d]$ 自己双対符号について, 次が成り立つ:

$$\begin{array}{llll} \text{(Type I)} & d \leq 2\left[\dfrac{n}{8}\right] + 2, & \text{(Type II)} & d \leq 4\left[\dfrac{n}{24}\right] + 4, \\ \text{(Type III)} & d \leq 3\left[\dfrac{n}{12}\right] + 3, & \text{(Type IV)} & d \leq 2\left[\dfrac{n}{6}\right] + 2. \end{array}$$

ここで, $[x]$ は x を越えない最大の整数を表す.

証 明. [14], [13, Ch. 19, §5].

これにより, extremal 自己双対符号の概念が導入できる:

定 義 3.2 定理 3.1 において等号が成立する自己双対符号を extremal 自己双対符号という.

注 意. 実在する Type I 自己双対符号に対しては, より鋭い評価が Rains [18] によって得られているが, われわれは実在の符号よりも重み多項式に興味があるため, 古典的な上記の定義を採用する.

さて, 前節で構成した不変式 (2.5) および (2.3) を用いて不変式環を構成しよう. ここで (2.3) は, 条件 (2.2) のもとでも (q が素数べきでなくても) σ_q-不変となることに注意しよう. このあと $q=6+2\sqrt{5}$ とし,

$$\sigma=\sigma_q=\frac{1}{\sqrt{q}}\begin{pmatrix}1 & q-1\\ 1 & -1\end{pmatrix}=\frac{1}{1+\sqrt{5}}\begin{pmatrix}1 & 5+2\sqrt{5}\\ 1 & -1\end{pmatrix}$$

とする. また

$$\tau=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

とおく. そして群 $G_{6+2\sqrt{5}}=\langle\sigma,\tau\rangle$ を考える. このとき, 次が成り立つ:

命 題 3.3 (i) $|G_{6+2\sqrt{5}}|=10$.
(ii) 群 $G_{6+2\sqrt{5}}$ の Molien 級数は

$$\Phi(\lambda)=\frac{1}{(1-\lambda^2)(1-\lambda^5)}.$$

証 明. (i) σ, τ とも位数は 2 で, $\tau\sigma$ の位数は 5 であることが確かめられる. このことから

$$G_{6+2\sqrt{5}}=\{(\tau\sigma)^i\tau^j\ ;\ 0\le i\le 4, j=0,1\}=\langle\tau\sigma\rangle\rtimes\langle\tau\rangle.$$

がわかり, この分解から結論が得られる.

(ii) Molien 級数の定義 ([13, p.600]) を用いて直接計算できる. ∎

この命題から, 群 $G_{6+2\sqrt{5}}$ の不変式環 $R_{6+2\sqrt{5}}:=\mathbf{C}[x,y]^{G_{6+2\sqrt{5}}}$ は, 次数 2, および次数 5 の生成元をもつことがわかる ([13, p.601] と同様の議論による). そして (2.3), (2.5) がともに σ_q-不変であることから, 次の定理が得られる:

定 理 3.4

$$R_{6+2\sqrt{5}}=\mathbf{C}[W_{2,6+2\sqrt{5}}(x,y),\psi_5(x,y)],$$

ただし

$$\begin{aligned}W_{2,6+2\sqrt{5}}(x,y) &= x^2+(5+2\sqrt{5})y^2, \\ \psi_5(x,y) &= x^5-(50+20\sqrt{5})x^3y^2+(225+100\sqrt{5})xy^4.\end{aligned}\tag{3.1}$$

環 $R_{6+2\sqrt{5}}$ に含まれる (2.1) の形の多項式はすべて σ_q-不変, かつ divisible by 2 である. そのような不変式で偶数次数であるものに対して, 次が成り立つ. これは $R_{6+2\sqrt{5}}$ における Mallows-Sloane bound の類似である:

定 理 3.5 多項式 $W(x,y)\in R_{6+2\sqrt{5}}$ は (2.1) の形であるとし, $\deg W(x,y)$ は偶数とする. このとき, 次の不等式が成り立つ:

$$d\le 2\left[\frac{n}{10}\right]+2. \tag{3.2}$$

証 明. [13, p.624-628] と同様である (詳しくは [5, Theorem 2.4] を参照). ∎

これにより, $R_{6+2\sqrt{5}}$ の (2.1) の形である $W(x,y)$ で, 次数が偶数のものに対しては extremal の概念が次のように定義できることとなる:

定 義 3.6 多項式 $W(x,y) \in R_{6+2\sqrt{5}}$ が (2.1) の形で次数が偶数であるとする. これが

$$d = 2\left[\frac{n}{10}\right] + 2 \tag{3.3}$$

を満たすとき, $W(x,y)$ は extremal であるという.

注 意. 奇数次の元に対しては, 定理 3.5 のかわりに

$$d \leq 2\left[\frac{n-5}{10}\right] + 2 \tag{3.4}$$

が成り立つと予想されるが, 技術的困難のため, 現在のところ証明できていない.

4 Riemann 予想を満たさない extremal な不変式の構成

環 $R_{6+2\sqrt{5}}$ における extremal な元を具体的に構成し, その Riemann 予想を調べよう. 式 (2.1) の形で次数が偶数の $W(x,y) \in R_{6+2\sqrt{5}}$ は,

$$W_{2,6+2\sqrt{5}}(x,y)^l \psi_5(x,y)^{2m} \qquad (l, m \geq 0, \quad (l,m) \neq (0,0)) \tag{4.1}$$

の形, あるいは, 同じ次数のものが複数あれば (つまり, (l,m) は異なるが $2l+10m$ の値が同じである (l,m) の組が複数あれば), それらの適当な 1 次結合である. 例えば次数が 10 のものは次のように構成できる:

例 4.1 次数が 10 の場合, 上記 l,m の可能な組み合わせは $(l,m) = (5,0), (0,1)$ である. そこで

$$\begin{aligned} W_{10}^{\mathrm{E}}(x,y) &:= \frac{4}{5}W_{2,6+2\sqrt{5}}(x,y)^5 + \frac{1}{5}\psi_5(x,y)^2 \\ &= x^{10} + (1350+600\sqrt{5})x^6y^4 - (5100+2280\sqrt{5})x^4y^6 \\ &\quad +(36225+16200\sqrt{5})x^2y^8 + (30500+13640\sqrt{5})y^{10} \end{aligned} \tag{4.2}$$

とすることにより, y^2 の項を消去して $d=4$ の式 $W_{10}^{\mathrm{E}}(x,y)$ が得られ, これが 10 次の extremal な不変式である (定義 3.6 において $n=10$, $d=4$). 実際, $d \geq 4$ を満たす不変式が他に存在しないことは容易にわかる (他の次数の場合も extremal な元はこうして構成できる).

次数が奇数の場合も, (3.4) はまだ証明できていないが, 一旦次数を具体的に指定すれば, その次数において (4.1) の形で表せる不変式がいくつあるかはわかるから, y 低次の項がいくつ消せるかもわかり, extremal な元を構成することは可能である. 例えば, $\psi_5(x,y)$ 自身は 5 次の extremal な不変式である (5 次では他に不変式が存在しないため).

環 $R_{6+2\sqrt{5}}$ の (2.1) の形の多項式 $W(x,y)$ に対しても, 定義 1.1 と同様に, その zeta 多項式 $P(T)$ を構成できる. そしてその Riemann 予想は次のようになる:

定 義 4.2 多項式 $P(T)$ の任意の根 α に対して,

$$|\alpha| = \frac{1}{\sqrt{q}} = \frac{1}{1+\sqrt{5}}$$

が成り立つとき, $W(x,y) \in R_{6+2\sqrt{5}}$ は Riemann 予想を満たすという.

まず例 4.1 の $W_{10}^{\mathrm{E}}(x,y)$ を調べよう:

定 理 4.3 多項式 $W_{10}^{\mathrm{E}}(x,y)$ は Riemann 予想を満たさない.

証 明. 多項式 $W_{10}^{\mathrm{E}}(x,y)$ の zeta 多項式 $P_{10}^{\mathrm{E}}(T)$ は

$$\begin{aligned} P_{10}^{\mathrm{E}}(T) &= \frac{1}{7}\Big\{(520+232\sqrt{5})T^4 - (320+144\sqrt{5})T^3 \\ &\quad -(168+76\sqrt{5})T^2 - (30+14\sqrt{5})T + 5 + 2\sqrt{5}\Big\} \end{aligned} \tag{4.3}$$

と計算される. これから $P_{10}^{\mathrm{E}}(99/100) = -122341/2500000 - (40154771/87500000)\sqrt{5} < 0$ がわかる. 一方 $P_{10}^{\mathrm{E}}(1) = 1 > 0$ である (これは zeta 多項式一般に対して成立する. 例えば [9, p.59, (7) 式] を参照). よって中間値の定理により, $P_{10}^{\mathrm{E}}(T)$ は実軸上の区間 $(99/100, 1)$ に少なくとも 1 つの根をもつが, $1/(1+\sqrt{5}) \approx 0.3090$ だから, $W_{10}^{\mathrm{E}}(x,y)$ は定義 4.2 の条件を満たさない. ∎

これで, 環 $R_{6+2\sqrt{5}}$ において, extremal であるが Riemann 予想を満たさない不変式の実例が構成できた.

他に, 5 次の extremal 不変式 $\psi_5(x,y)$ の zeta 多項式は

$$P_5(T) = -\frac{2+\sqrt{5}}{4}(4T-1+\sqrt{5})(8T^2-4\sqrt{5}T+3-\sqrt{5})$$

である. これは根が具体的に求まり, やはり Riemann 予想を満たさないことが確認できる (後ろの 2 次式の根が円 $|T| = 1/\sqrt{q}$ から外れる).

5 Formal weight enumerator の場合

多項式 $W(x,y)$ が $W^{\sigma_q}(x,y) = -W(x,y)$ を満たすとき, これを formal weight enumerator と呼ぶことはすでに述べた. この場合の最近の結果を簡単に報告する (本節の結果は Chinen [6] による). 第 2 節の探索法は, divisible by 2 の formal weight enumerator (以下 FWE と略す) にも適用でき, 次数 4 で $q=2$ に対する FWE である

$$\varphi_4(x,y) = x^4 - 6x^2y^2 + y^4 \tag{5.1}$$

が見つかる. これは $W_{2,2}(x,y) = x^2 + y^2$ と組にすると Type I および Type II 自己双対符号の重み多項式をすべて生成する. また次数 6 で $q = 4/3$ に対する FWE である

$$\varphi_6(x,y) = x^6 - 5x^4y^2 + \frac{5}{3}x^2y^4 - \frac{1}{27}y^6 \tag{5.2}$$

が見つかる. 他にも $q=4\pm 2\sqrt{2}$ に対して

$$\begin{aligned}\varphi_8^{\pm}(x,y) &= x^8-(84\pm 56\sqrt{2})x^6y^2+(1190\pm 840\sqrt{2})x^4y^4\\ &\quad -(2772\pm 1960\sqrt{2})x^2y^6+(577\pm 408\sqrt{2})y^8, \end{aligned}\tag{5.3}$$

$q=2\pm 2\sqrt{5}/5$ に対して

$$\begin{aligned}\varphi_{10}^{\pm}(x,y) &= x^{10}-(45\pm 18\sqrt{5})x^8y^2+(378\pm 168\sqrt{5})x^6y^4-\left(714\pm\frac{1596}{5}\sqrt{5}\right)x^4y^6\\ &\quad +\left(\frac{1449}{5}\pm\frac{648}{5}\sqrt{5}\right)x^2y^8-\left(\frac{61}{5}\pm\frac{682}{125}\sqrt{5}\right)y^{10}, \end{aligned}\tag{5.4}$$

さらには $q=8\pm 4\sqrt{3}$ に対して

$$\begin{aligned}\varphi_{12}^{\pm}(x,y) &= x^{12}-(462\pm 264\sqrt{3})x^{10}y^2+(48015\pm 27720\sqrt{3})x^8y^4\\ &\quad -(1248324\pm 720720\sqrt{3})x^6y^6+(9314415\pm 5377680\sqrt{3})x^4y^8\\ &\quad -(17297742\pm 9986856\sqrt{3})x^2y^{10}+(3650401\pm 2107560\sqrt{3})y^{12} \end{aligned}\tag{5.5}$$

といった奇妙な FWE が存在する. また奇数次では $q=4$ に対する $\varphi_3(x,y)=x^3-9xy^2$ (これは Type IV 自己双対符号の重み多項式にも関連), $q=6-2\sqrt{5}$ に対する

$$\varphi_5(x,y)=x^5+(-50+20\sqrt{5})x^3y^2+(225-100\sqrt{5})xy^4 \tag{5.6}$$

なども探索できる (これは (2.5) の $\psi_5(x,y)$ と対をなすように見える).

おもしろいのは, これらの中で $q=2,4$ という, 実在の符号にも関連する場合とともに, q が比較的小さい $q=4/3, 4-2\sqrt{2}, 2-2\sqrt{5}/5, 8-4\sqrt{3}, 6-2\sqrt{5}$ では「extremal ならば Riemann 予想成立」という現象が観察できる (証明はできない) のに対し, q が大きい $q=4+2\sqrt{2}, 2+2\sqrt{5}/5, 8+4\sqrt{3}$ ではそれが不成立ではないかと想像される結果が得られることである. 理由はわからないが, q が大きいと不変式の Riemann 予想は成り立ちにくい傾向にあるように思われる. この観察は別の角度からの考察でも支持される (Chinen-Imamura [7]).

結び. 実在の自己双対符号の重み多項式がなす環, 特に divisible という条件を伴う Type I から IV までの環においては, 確かに Riemann 予想を満たす不変式は extremal なところに集中しており, extremal という条件が重要な役割を果たしているように見える. しかし今回構成した環 $R_{6+2\sqrt{5}}$ においては, 上の 2 つの例をはじめとして, extremal でも Riemann 予想を満たさない不変式が存在する. というより, Riemann 予想を満たす不変式が, そもそもまだ見つからない. 不変式環の構造としては似通っているにもかかわらず, Riemann 予想をめぐる状況は相当に異なっているようである. この理由が何であるのか, まだわからない. ところで, divisible という条件を課さない状況で考えると (そこでは Mallows-Sloane 型の限界式が存在しない), 可能なほぼすべての (n,d) の組に対して Riemann 予想を満たす不変式が存在する ([4]). 不変式の Riemann 予想がどのような意味をもつのか, そしてその必要十分条件は何か, あらためて考える必要がありそうだ.

参考文献

[1] 知念 宏司, 平松 豊一：線形符号のゼータ関数とリーマン予想の類似 (Iwan Duursma の仕事の紹介), 符号と暗号の代数的数理, 京都大学数理解析研究所講究録 1361 (2004), 91-101.

[2] 知念 宏司：線型符号のゼータ関数とそのリーマン予想 (Iwan Duursma の仕事の紹介, 及び 1 つの拡張), 仙台数論及び組合せ論小研究集会 2004 報告集 (2005), 31-44.

[3] Chinen, K : Zeta functions for formal weight enumerators and the extremal property, Proc. Japan Acad. **81** Ser. A. (2005), 168-173.

[4] ________ : An abundance of invariant polynomials satisfying the Riemann hypothesis, Discrete Math. **308**, 6426-6440 (2008).

[5] ________ : Extremal invariant polynomials not satisfying the Riemann hypothesis, to appear in Appl. Algebra Engrg. Comm. Comput.

[6] ________ : Construction of divisible formal weight enumerators and extremal polynomials not satisfying the Riemann hypothesis, arXiv:1709.03380.

[7] Chinen, K and Y. Imamura : On the Riemann hypothesis for self-dual weight enumerators of genus three, arXiv:1811.08246.

[8] Duursma, I. : Weight distribution of geometric Goppa codes, Trans. Amer. Math. Soc. **351**, No.9 (1999), 3609-3639.

[9] ________ : From weight enumerators to zeta functions, Discrete Appl. Math. **111** (2001), 55-73.

[10] ________ : A Riemann hypothesis analogue for self-dual codes, DIMACS series in Discrete Math. and Theoretical Computer Science **56** (2001), 115-124.

[11] ________ : Extremal weight enumerators and ultraspherical polynomials, Discrete Math. **268**, No.1-3 (2003), 103-127.

[12] 平松 豊一, 知念 宏司：線形符号のゼータ関数とそのリーマン予想, 特集「符号化理論の新時代」, 数理科学 **497** (2004), 42 - 47.

[13] MacWilliams, F. J. and Sloane, N. J. A. : The Theory of Error-Correcting Codes, North-Holland, 1977.

[14] Mallows, C. L. and Sloane, N. J. A. : An upper bound for self-dual codes, Infor. and Control **22** (1973), 188-200.

[15] 奥田 隆幸：不変式環上のリーマン仮説類似について, 有限群論と代数的組合せ論, 京都大学数理解析研究所講究録 **1593** (2008), 145-153.

[16] Ozeki, M. : On the notion of Jacobi polynomials for codes, Math. Proc. Camb. Phil. Soc. **121** (1997), 15-30.

[17] Pless, V. : Introduction to the Theory of Error-Correcting Codes, John Wiley & Sons, 1998 (Third Edition).

[18] Rains, E. M. : Shadow bounds for self-dual codes, IEEE Trans. Inform. Theory **44**(1) (1998), 134-139.

[19] Sloane, N. J. A. : Self-dual codes and lattices, in: Relations Between Combinatorics and Other Parts of Mathematics, Proceedings of Symposium on Pure Mathematics 34, Ohio State University, Columbus, OH, 1978, Amer. Math. Soc., Providence, RI, 273-208 (1979).