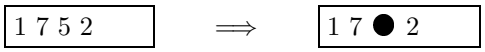
線型符号のゼータ関数 (Iwan Duursma の理論) とその 1 つの拡張

知念 宏司

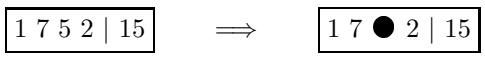
§1 5 分で学ぶ符号理論

本節の内容は昨年のサマースクール報告集にもあるが, 参照できない方もあると思うので再掲させて頂く.

誤り訂正符号 (error correcting code) とは, ディジタル方式で情報を送るとき, できるだけ正確に (電気的なノイズなどの影響を受けても大丈夫なように) 送るための仕組みである. その原理は「虫食い算」を思い出すとよい. いま, カードに数字を書いて誰かに送るとしよう. しかし, 送られる途中で汚れがついて, 1 文字消えてしまうとする.



そこでちょっと余白があるのを利用して, 各数の和 $1+7+5+2=15$ を書き加えておこう:



すると消えてしまった数は $15-(1+7+2)=5$ と復元できる. このように, **余分な情報を少し付け加えておけば, どこかが読めなくなっても復元できる**というのが, 基本的な考え方だ. 実際には, 送りたい情報をベクトル空間 ${\mathbf{F}_2}^k$ の元として表しておき,「余分な情報の付け加え」は, より大きなベクトル空間 ${\mathbf{F}_2}^n$ へ ${\mathbf{F}_2}^k$ を埋め込む, ということで実現される. そこで一般的な線型符号の定義を述べると次のようになる:

定 義 1 q を素数べきとする. ベクトル空間 ${\mathbf{F}_q}^n$ の k 次元部分空間 C $(k \leq n)$ を $\mathbf{F}_q$ 上の $[n,k]$-(線型) 符号 (linear code) という. n, k をそれぞれ C の符号長 (code length), 次元という.

つまり, 埋め込んだあとの像が定義の C である. 実際にどのように誤り訂正が行なわれるかは符号理論の書物に譲ることにして, このあと必要となることをさらに少し準備しよう. C のベクトル c (符号語という) を成分で表したとき, 0 でない成分の個数を c の (Hamming) 重みといい, C の符号語すべて ($\mathbf{0}$ 以外) を考えたときの, 重みの最小値を C の最小距離 (最小重み) という. 最小距離 (d とおく) も明示するときは $[n,k,d]$-符号と書く. d は符号の誤り訂正能力に大きく関わる (大きいほどよい *cf.* [10, p.106], [11, p.99]). 最後に重み多項式を定義する. $c \in C$ の重みを $\mathrm{wt}\,(c)$ で表す. $A_i := \sharp\{c \in C\ ;\ \mathrm{wt}\,(c)=i\}$ とおくとき,

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

を C の**重み多項式** (weight enumerator) と呼ぶ.

例 1 $C=\{00,11\} \subset {\mathbf{F}_2}^2$. このとき $W_C(x,y)=x^2+y^2$. C を 2 つ連ねて $C'=C\oplus C=\{0000,0011,1100,1111\}$ を作ると $W_{C'}(x,y)=x^4+2x^2y^2+y^4=W_C(x,y)^2$. このように, 重み多項式を考えることで, 符号の重みに関するいろいろなことが多項式の計算でわかるというメリットがある.

符号理論全般に関する入門書として [10], [11], [13] (ただしこれはほとんど辞書), [17] など. 保型形式との関連は [9], 代数幾何符号については [19] などがある.

§2 Zeta 関数の定義と性質

符号の zeta 関数は, Duursma [5] で初めて導入された. それは重み多項式から構成される. C を $\mathbf{F}_q$ 上の $[n,k,d]$ 符号, その重み多項式を $W_C(x,y)$ とする. また以下では d も $C^\perp$ (あとで定義) の最小距離も 2 以上とする. C の zeta 関数は次のように定義される:

定 義 2 ([6], p.58) 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.

この定義はやや解りづらいが, 左辺は T の有理式なので, べき級数展開を思い出す. その T^{n-d} の係数に C の重さ多項式が現れるようになる, ということである. また, $P(T)$ の存在と一意性も決して明らかではない (そして原論文の証明は読みづらい) ので, 以下に簡単に証明のアイディアを紹介しよう.

まず,

$$f(T):=\frac{(y(1-T)+xT)^n}{(1-T)(1-qT)}$$

という関数を考える. つまり, 定義 2 で $P(T)=1$ とした場合である. これのべき級数展開を

$$\Big\{\sum_{j=0}^{n}\binom{n}{j}(x-y)^jy^{n-j}T^j\Big\}(1+c_1T+c_2T^2+\cdots)$$

とおく. つまり $\{\quad\}$ の中は $(y(1-T)+xT)^n=((x-y)T+y)^n$ の (T の多項式としての) 2 項展開, $(1+c_1T+c_2T^2+\cdots)$ は $1/\{(1-T)(1-qT)\}$ のべき級数展開を整理したものである. これをさらに展開して $1, T, T^2, \cdots, T^{n-d}$ の係数を調べる. すると, 適当な整数 b_{ij} が存在して,

$$\begin{array}{ll}
1\text{ の係数 (定数項)} & y^n\\
T\text{ の係数} & nxy^{n-1}+(c_1-n)y^n\\
\cdots\cdots & \cdots\cdots\cdots\\
T^i\text{ の係数} & b_{i0}x^iy^{n-i}+b_{i1}x^{i-1}y^{n-i+1}+\cdots+b_{ii}y^n\\
\cdots\cdots & \cdots\cdots\cdots\\
T^{n-d}\text{ の係数} & b_{n-d,0}x^{n-d}y^d+b_{n-d,1}x^{n-d-1}y^{d+1}+\cdots+b_{n-d,n-d}y^n
\end{array}\qquad(1)$$

となることが簡単な計算からわかる. そこで今度は, 有理数 $a_0, a_1, \cdots, a_{n-d}$ が与えられているとして, $(a_0+a_1T+\cdots+a_{n-d}T^{n-d})f(T)$ の T^{n-d} の係数を見てみよう. それは

$$\begin{array}{r}
a_{n-d}y^n\\
+a_{n-d-1}\{xy^{n-1}+(c_1-n)y^n\}\\
\cdots\cdots\cdots\\
+a_0\{b_{n-d}x^{n-d}y^d+\cdots+b_1xy^{n-1}+b_0y^n\}
\end{array}$$

であることがわかる. 一方, $(W_C(x,y)-x^n)/(q-1)=(A_dx^{n-d}y^d+\cdots+A_ny^n)/(q-1)$ であるから, これらが一致するように, 上の $a_0, a_1, \cdots, a_{n-d}$ を順次決めていくことができる (しかも可能性は 1 通り). 正確に言えば, (1) において $b_{00}=1$ (定数項 y^n の係数 1 をこうおく), $b_{10}=n$, $b_{11}=c_1-n$

とすると, 上の $a_0, \cdots, a_{n-d}$ は連立 1 次方程式

$$\begin{bmatrix} b_{n-d,0} & 0 & \cdots & \cdots & 0 \\ b_{n-d,1} & b_{n-d-1,0} & 0 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ & & & \ddots & 0 \\ b_{n-d,n-d} & b_{n-d-1,n-d-1} & \cdots & & b_{00} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ \vdots \\ a_{n-d} \end{bmatrix} = \frac{1}{q-1} \begin{bmatrix} A_d \\ A_{d+1} \\ \vdots \\ \vdots \\ A_n \end{bmatrix}$$

の解となるが, 各対角成分 b_{i0} は実は 2 項係数 $\binom{n}{i}$ に等しいことがわかり, したがって解はつねに一意的に存在するのである. そこで $a_0 + a_1 T + \cdots + a_{n-d} T^{n-d} = P(T)$ とすればよいことがわかる.

次に, C の**双対符号** (dual code) $C^\perp$ を

$$C^\perp := \{u \in {\mathbf{F}_q}^n \ ; \ u \cdot v = 0, \forall v \in C\}$$

で定義する. ただし, $u = (u_1, u_2, \cdots, u_n), v = (v_1, v_2, \cdots, v_n) \in {\mathbf{F}_q}^n$ に対して,

$$u \cdot v = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n.$$

また, $C^\perp = C$ のとき C を**自己双対** (self-dual) であるという.

まず C, $C^\perp$ の zeta 多項式 $P(T)$, $P^\perp(T)$ の間には

$$P^\perp(T) = P\Big(\frac{1}{qT}\Big) q^g T^{g+g^\perp}$$

という関係がある ([6, p.59]). ただし, $g := n + 1 - k - d$, $g^\perp$ は $C^\perp$ の対応する量. 証明には MacWilliams の恒等式

$$W_{C^\perp}(x, y) = \frac{1}{\sharp C} W_C(x + (q-1)y, x - y)$$

([13, p.146, Th. 13]) が用いられる. よって特に, C が自己双対なら, $P(T) = P^\perp(T)$ により, **関数等式**

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

が成り立つ. このように**代数曲線の合同 zeta の場合と全く同じ形**になるところが極めて興味深い.

§3 Riemann 予想

代数曲線 ($\mathbf{F}_q$ 上) の合同 zeta 関数の場合「Riemann 予想」 (Weil によって証明された) とは

$$\text{zeta 多項式の任意の根 } \alpha \text{ に対して, } |\alpha| = \frac{1}{\sqrt{q}}$$

というものである. 前節で見た通り, 自己双対符号の zeta 関数 $P(T)$ も同じ関数等式を満たすことから, 自己双対符号に対する Riemann 予想は, 代数曲線と同様次のように定式化するのが適当であろう:

定 義 3 ([7], p.119) C を自己双対符号, 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.

これは単なる形式的類似のようにも思えるが, 概してよい符号は **Riemann 予想を満たす**という数値的観察もあったようだ. 実は, 符号の zeta 関数についての最も大きな未解決問題は,

問 題 1 Riemann 予想を満たす自己双対符号とはどのようなものか定式化せよ.

というものである. これに関して Duursma は 1 つの十分条件を予想している:

問 題 2 ([7], p.119) 「Extremal な自己双対符号は Riemann 予想を満たす」は正しいか.

ここで, 符号長 n の自己双対符号の中で, 最小距離が最も大きいものを extremal code という. 最小距離は符号の誤り訂正能力を決定づける量 (大きいほど能力が高い) だから, これは確かによい性質と言える.

例 2 $[8,4,4]$ 拡大 Hamming 符号 C_8 ([11, p.112], [17, p.35] 等). これは $\mathbf{F}_2$ 上の extremal な自己双対符号. 重み多項式は $W_{C_8}(x,y) = x^8 + 14x^4y^4 + y^8$ で ([17, p.135]),

$$P(T) = \frac{1}{5}(1 + 2T + 2T^2).$$

$P(T)$ の根は $\alpha = (-1 \pm i)/2$ なので, $|\alpha| = 1/\sqrt{2} = 1/\sqrt{q}$, Riemann 予想を満たす.

自己双対符号には代表的な系列が 4 つある (I 型 $\sim$ IV 型, *cf.* [4]) が, そのうちの実在する extremal code すべてに対して Riemann 予想が成り立つことは数値的に確かめられている. また Duursma は IV 型自己双対符号の系列に対して「extremal ならば Riemann 予想成立」を示している ([8]).

§4 拡 張

本節では筆者の [3] の内容を紹介する. 符号の zeta 関数は,「符号 C に」というより「符号の重み多項式に」対して定義されている. そして本質は, 符号の重み多項式が x, y の斉次多項式であるという事実だ. ということは, 実在の符号の重み多項式でない斉次多項式にも同様に zeta 多項式 $P(T)$ が定義できる, ということである. 例えば

$$W_{12}(x,y) = x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12}.$$

係数に負の数が現れるため, これは実在する符号の重み多項式ではない. しかし, これを仮想的な $[12,6,4]$ 符号の重み多項式と見るのである. 符号長 $n = 12$, 最小距離 $d = 4$ とみなすことに異論はないだろう. 次元を 6 と見るのは, 自己双対性を意識してのことである. また, $\mathbf{F}_2$ 上の自己双対符号に関連があるので $q = 2$ とする ([2, §5], [14, pp.104-105]). この zeta 多項式を求めると

$$P(T) = \frac{1}{15}(2T^2 - 1)(2T^2 + 1)(2T^2 + 2T + 1)$$

となり, これは Riemann 予想 (すべての根 α が $|\alpha| = 1/\sqrt{2}$) を満たす!

上の $W_{12}(x,y)$ は, 実は不変式環 $\mathbf{C}[x,y]^{G_8}$ の元である. ここで, G_8 は Shephard-Todd による複素鏡映群の分類 ([18]) において No.8 と名づけられている群である ([14] も参照):

$$G_8 := \left\langle \frac{1-i}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

$\mathbf{C}[x,y]^{G_8}$ は, この群 G_8 の作用 (多項式の変数に 1 次変換として作用) で不変に保たれる多項式のなす環で, 生成元は前述の $W_{12}(x,y)$ と拡大 Hamming 符号の重み多項式 $W_8(x,y) = x^8 + 14x^4y^4 + y^8$ であることが知られている (符号に関連する不変式環については [13, Ch.19] が詳しい).

この環には

$$W^{\perp}(x,y) := W\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) = -W(x,y)$$

という変換式を満たすものがあり, それは Ozeki [15] により "formal weight enumerator" と名づけられた ($W_{12}(x,y)$ もその 1 つ). $\mathbf{F}_2$ 上の実在する自己双対符号の重み多項式ならマイナスのない $W^{\perp}(x,y) = W(x,y)$ が成り立つので, 違いはこのマイナスの有無である.

このことを反映し, formal weight enumerator の関数等式は

$$P(T) = -P\Big(\frac{1}{2T}\Big)2^g T^{2g}$$

という形をとる. そして, 代数曲線や実在の符号の場合と同様に $P(T)$ の根の分布を調べてみると, Riemann 予想も同様に定義できることがわかる (任意の根 α が $|\alpha| = \frac{1}{\sqrt{2}}$ を満たすこと, と定める). さらに, extremal という概念も定義でき, Riemann 予想に関して, 実在の符号の世界と同じようなこと (extremal なら Riemann 予想成立 ?) が起きていると見られるのである (詳しくは [2], [3] を参照).

他にも, $\mathbf{F}_3$ 上の自己双対符号に関連した formal weight enumerator もある. それは, 群

$$G := \left\langle \sigma_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/3} \end{pmatrix} \right\rangle.$$

で不変な多項式のなす環 $\mathbf{C}[x,y]^G$ において $w((x+2y)/\sqrt{3}, (x-y)/\sqrt{3}) = -w(x,y)$ をみたすもので,

$$w_6(x,y) = x^6 - 20x^3y^3 - 8y^6$$

などの例がある (Ozeki [16]). この場合の zeta 多項式は関数等式 $P(T) = -P\Big(\frac{1}{3T}\Big)3^g T^{2g}$ ($g = \frac{n}{2} + 1 - d$) を満たし, Riemann 予想は「$P(T)$ のすべての根が半径 $1/\sqrt{3}$ の円周上にある」となる. 上の例 $w_6(x,y)$ の zeta 多項式は $P_6(T) = \frac{1}{2}(3T^2 - 1)$ で, これは Riemann 予想を満たしている. この環の formal weight enumerator についてもやはり「 extremal なら Riemann 予想成立 ?」を窺わせる数値実験結果が得られている ([3, §4]).

これらの観察から,「符号の zeta 関数」の性質解明には, 実在の符号の重み多項式にこだわらず, より広い範囲の不変多項式を考察の対象にした方がよいのではないかと思われるのである.

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, または http://www.math.is.tohoku.ac.jp/~taya/sendaiNC/2004/program.html.

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

[4] Conway, J, H. and Sloane, N. J. A. : Sphere Packings, Lattices and Groups, 3rd Ed., Springer Verlag, 1999.

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

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

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

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

[9] Ebeling, W. : Lattices and Codes, 2nd Ed., Vieweg, 2002.

[10] 藤原 良, 神保 雅一 : 符号と暗号の数理, 共立出版, 1993.

[11] 平松 豊一 : 応用代数学, 裳華房, 1997.

[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] 小関 道夫 : 符号理論と unitary reflection groups の不変式環との関連について, 第 12 回代数的組合わせ論シンポジウム報告集 (1996), 96-116.

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

[16] _____ : Invariant rings associated with ternary self-dual codes and their connections with Jacobi forms, in Proceedings of the Third Spring Conference "Modular Forms and Related Topics" at Hotel Curreac, Hamamatsu, Japan (ed. T. Ibukiyama et al.), Ryushi-do, 2004.

[17] Pless, V. : Introduction to the Theory of Error-Correcting Codes, 3rd Ed., John Wiley & Sons, 1998.

[18] Shephard, G. C. and Todd, J. A. : Finite unitary reflection groups, Canad. J. Math. **6** (1954), 274-304.

[19] Stichtenoth, H. : Algebraic Function Fields and Codes, Springer Verlag, 1993.

知念 宏司
大阪工業大学工学部
〒 535-8585 大阪市旭区大宮 5-16-1
email: YHK03302@nifty.ne.jp

Koji Chinen
Osaka Institute of Technology
Faculty of Engineering
Asahi-ku, Osaka, 535-8585 JAPAN