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*

2005.8.22 第 13 回整数論サマースクール 宵の時間

§1 5 分で学ぶ符号理論

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.

$$\boxed{1\ 7\ 5\ 2} \quad \Longrightarrow \quad \boxed{1\ 7\ \bullet\ 2}$$

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:

$$\boxed{1\ 7\ 5\ 2 \mid 15} \quad \Longrightarrow \quad \boxed{1\ 7\ \bullet\ 2 \mid 15}$$

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), [15] など. 保型形式との関連は [9], 代数幾何符号については [16] などがある.

*大阪工業大学ほか, 非常勤

§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が, これについては [1], [2], [12] などを参照.

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,

$$u \cdot v = u_1v_1 + u_2v_2 + \cdots + u_nv_n.$$

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

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

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

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

が成り立つ (代数曲線の合同 zeta と全く同じ形 !).

§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 (これは確かによい性質だ).

例 2 $[8, 4, 4]$ 拡大 Hamming 符号 C_8 ([11, p.112], [15, 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 ([15, 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

最近筆者は, 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 $P(T)$ が定義できることに気づいた. 例えば

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

これはある不変式環の元で, $\mathbf{F}_2$ 上の自己双対符号に関連がある ([2, §5], [14, pp.104-105]). そこで $q = 2$ として 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！実は関数等式は

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

という, 少し違った形をとる. 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. 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).

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.

(2005 年 11 月 28 日提出)

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, submitted.

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

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