

Goppa 符号と有理点について

(付録論文つき)

京都大学 数理解析研究所

伊 原 康 隆

Yasutaka Ihara

(RIMS, Kyoto Univ.)

V.D. Goppa の発見によって有理点を沢山もつ有限体上の代数曲線が 線型符号の理論に応用されるようになったのは 80年代はじめ ([G]) で; それ以来 有限体上の代数曲線の有理点に関する研究が盛んになり ([S] など), 今日でもかなり活発に研究され進展しつつあります ([GS], [GV], ...). 筆者との関わりは謂わば 昔話——昔の結果が Goppa 等によって使われた —— に属するのですが, その縁もあって今年 (97 年) 7 月 Seattle でのアメリカ数学会 (等) 主催の夏季研究集会 「Finite fields and Applications」 に出席する事になり, そこで最近のいくつかの話題にふれる事が出来ました。(この方面の研究者のかなり多くが出席。) 今日はこれらについてのお話しをしたいと思います。

§1 線型符号

有限体 $\mathbb{F}_q$ をとり,

$$C \subset (\mathbb{F}_q)^n = \{x = (x_1, \dots, x_n) \mid x_i \in \mathbb{F}_q\}$$

を $\mathbb{F}_q$ 上の n 次元横ベクトル空間の一つの線型部分空間とします。 $(\mathbb{F}_q)^n$ の 2 元 $x = (x_i), x' = (x'_i)$ の間の“距離”を

$$d(x, x') = \#\{i \mid x_i \neq x'_i\}$$

と定め,

$$\text{dis}(C) = \min_{\substack{x, x' \in C \\ x \neq x'}} d(x, x') = \min_{\substack{x \in C \\ x \neq 0}} d(x, 0)$$

と置きます。

$\mathbb{F}_q$ の元を“アルファベット”, $(\mathbb{F}_q)^n$ の元を長さ n の単語,

C の元を“許される名前”と考えてみましょう。

そうすると, $\text{dis}(C)$ は “2つの異なる名前は最低何ヶ所で文字が異なるか” を表わす量という事になります。どのように C を選ぶとよいか? C が小さいと “同姓同名” を許さざるを得なくなるし, $\text{dis}(C)$ が小さくても混同しやすい名前があって不都合です。そこで (n に比べて) $\dim(C)$, $\text{dis}(C)$ が 共になるべく大きい C を探したいという事になります。これはそう明らかなような作り方がない (少なくとも知られていない) ので, 応用と直結した面白い研究課題になります。(工学への応用は通信や CD の音の修正などのようです。)

そこで

$$\delta(C) = \frac{\text{dis}(C)}{n}, \quad R(C) = \frac{\dim(C)}{n}$$

(それぞれ, C の相対距離, 情報率とよばれる) と置き, q を固定, n と C を動かして, $(\delta(C), R(C))$ を座標にもつ点を δR 平面上の正方形の上にマークしてゆきます。なるべく“右上”の点がほしいわけです。まず n, C でパラメトライズされる点列 $(\delta(C), R(C))$ の累積点の集合 U_q を研究対象とします。

古典的主結果より (cf. [M])

- 1) ある連続写像 $\alpha_q: [0, 1] \rightarrow [0, 1]$ が存在して,

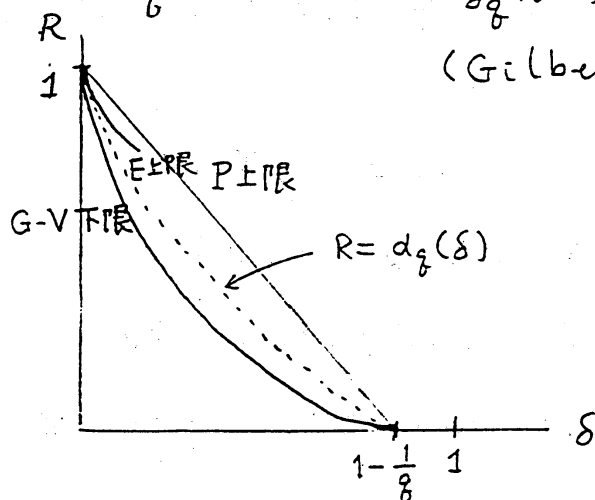
$$U_q = \{(\delta, R) \in [0, 1]^2 \mid 0 \leq R \leq \alpha_q(\delta)\}.$$

- 2) $\alpha_q(\delta) \leq \max\left\{1 - \frac{q}{q-1}\delta, 0\right\}$ (Plotkin 上限)

- 2)' Elias 上限 (δ の小さいときは $\frac{q}{q-1}\delta$ よりよい) (参考)

- 3) $\alpha_q(\delta) \geq 1 - \delta \log_q(q-1) + \delta \log_q \delta + (1-\delta) \log_q(1-\delta)$

(Gilbert - Varshamov 下限)



[注意 GV]

後の参考の為, G-V 曲線

の勾配 -1 の接線は

$$\delta + R = 1 - \log_q \frac{(2q-1)}{q}$$

で, 接点の δ 座標は $\frac{q-1}{2q-1}$.

Gilbert-Varshamov 下限の上には、 U_q の実 は 約 25 年間
発見されなかった為、GV を 与える 曲線 が α_q の グラフ と
一致する の ではないか との 予想 も あった よう です。しかし
Goppa 符号 によって、有理 真 を 沢山 もつ $\mathbb{F}_q$ 上 の 代数 曲線 の
理論 と 結びつき、昔 の 結果 によって この 記録 は 破 ら れ ま し た。

そこで Goppa 符号 の 説明 に 入 り ま し ょ う。

§2 Goppa 符号

X を $\mathbb{F}_q$ 上 の 滑らか で 完備 絶対 既約 な 代数 曲線 と し、その
種数 を g と し ま す。また X は 相異なる $\mathbb{F}_q$ 有理 点 $P_0, P_1, \dots, P_n$
を 持っ と し ま す。又 m を 自然 数 と し、これらの 資料 によって
定まる Goppa 符号 $C \subset (\mathbb{F}_q)^n$ を、

$$C = \left\{ (f(P_1), \dots, f(P_n)) \mid \begin{array}{l} f \text{ は } X \text{ 上 の 有理 関数 で、} P_0 \text{ で} \\ m \text{ 位 以下 の 極 を も 他 は 正 則} \end{array} \right\}$$

で 定義 し ま す。 $2g-2 < m < n$ と す る と、暗算 により

$$(2-1) \quad \dim(C) = \dim(f \text{ の 空間 の 次元 }) = m - g + 1$$

(m に 関する 右側 の 不等式 から オー の 等式、左側 の から Riemann-Roch に よて オー の
等式 が 出る) また $f \neq 0$ なら $f(P_i) = 0$ と なる i の 個数 は $\leq m$ 。 よって

$$(2-2) \quad \text{dis}(C) \geq n - m.$$

$$\therefore R(C) = \frac{m-g+1}{n}, \quad \delta(C) \geq 1 - \frac{m}{n}.$$

$$\therefore (2-3) \quad \delta(C) + R(C) \geq 1 - \frac{g-1}{n}.$$

よって, n が $g-1$ に比べて大きい程, $(\delta(C), R(C))$ はより右上の方にあることになります. n は $(X$ の $\mathbb{F}_q$ 有理点の個数) $- 1$ にとれますから, $\mathbb{F}_q$ を固定したとき $g-1$ に比べて $\mathbb{F}_q$ 有理点の個数の著しく多い $\mathbb{F}_q$ 上の代数曲線の系列 ($q \rightarrow \infty$) を見つけることが問題となります. 定量的には,

$$(2-4) \quad A(g) = \overline{\lim_{g \rightarrow \infty}} \left(\frac{\mathbb{F}_q \text{ 上の曲線 } X \text{ の有理点の個数}}{X \text{ の種数 } g} \right)$$

とおくとき, Goppa 符号により (m は $2g-2 < m < n$ の範囲ですべての値を用いる), 線分

$$(G_p) \quad \delta + R = 1 - \frac{1}{A(g)}, \quad \frac{1}{A(g)} \leq R \leq 1 - \frac{1}{A(g)}$$

は U_g に属することがすぐわかります. 一方, §1 [注意 GV] より,

$$(2-5) \quad A(g) > \left(\log_g \left(\frac{2g-1}{g} \right) \right)^{-1} \doteq \log_2 g$$

なら 線分 (G_p) の少くも一部が $G-V$ 下限曲線の上にはみ出すことになります. そこで各素数べき g に対して $A(g)$ の値, 又はその下限を求めることが問題になります.

§3 沢山の有理点をもつ $\mathbb{F}_q$ 上の代数曲線系の研究 (i)

これに係わる筆者自身の昔の結果 (はじめは予想 [I₁]) は、最も手短かに述べれば、次の通りです ([I₂] とその引用文献参).

(※) q が平方数 (素数の偶数乗) のとき, $\mathbb{F}_q$ 上の代数曲線 (すべて滑らかで完備絶対既約なものとする) の可算無限系列 $\{X_i\}_{i \geq 1}$ であって, X_i の種数 g_i は $g_i \geq 2$, $g_i \rightarrow \infty$ を満し, 各 X_i は少なくとも $(\sqrt{q}-1)(g_i-1)$ 個の $\mathbb{F}_q$ -有理点をもつものが存在する。

特に (q が平方数のとき) $A(q) \geq \sqrt{q}-1$

これを $(\log_q (\frac{2q-1}{q}))^{-1}$ と比べると, $q \geq 7^2$ なら確かに $\sqrt{q}-1$ の方が大きくなるので, 部分 [G_p] の一部分が GV 曲線の上にはみ出ることになります。尚 Goppa 自身がすぐ筆者の仕事と結びつけたわけではなく, その前に [TVZ] (上記 (※) の一部) が出てから, (多分 Manin が) 筆者の仕事を思い出してくれたものと思います ([M] 参照)。

さて上記の代数曲線 X_i たちですが, 実際には $\mathbb{F}_q$ 上の志村曲線の良いモデルをとる事によって得られます。これを証明するには, 志村氏による深い理論 (ほとんどすべての p での good reduction と合同関係式) と 森田康夫, 太田雅乙氏による 各 p に因する議論と, それに (次に述べる) 離散群

Γ のゼータ関数 $Z_\Gamma(u)$ の議論が必要ですが, その全体構造を一目で見て X_i は $(\sqrt{p}-1)(q_i-1)$ 個の特殊な有理点をもつ事を納得するには, Γ との関係をみるのが不可欠だと思います. この Γ というのは $\mathrm{PSL}_2(\mathbb{R}) \times \mathrm{PGL}_2(\mathbb{F}_p)$ ($\mathbb{F}_p$ は p 進体, $N(p)^2 = q$) の既約な格子部分群のことで, この Γ に X_i たちの正しいパラメーターなのです. 詳しくは, (この一文に続く "Shimura curves over finite fields and their rational points" (加筆訂正後, 前記の Seattle conference 報告集に提出予定), 又はそこに引用されている各論文を併参照下さい.

§4 沢山の ... (ii).

さて上記 X_i を ($\mathbb{F}_q$ 上の曲線として) 含むことのできる射影空間 $\mathbb{P}^{N_i}$ の次えも ($\mathbb{F}_q$ 有理点の個数を比べれば明らかのように) $N_i \rightarrow \infty$ とならざるを得ないので, X_i たちを具体的に方程式で書き下すことは大変困難 (複雑) に思われます. しかしその関数体なら常に 2 元で生成されるので, 方程式で書けるので, 具体的に書ける可能性もある. 比較的最近 Garcia と Stichtenoth $[GS_1], [GS_2]$ は, §3(*) を満たす X_i の別種の実例を (2通り) その関数体を具体的に与えることにより, 与えました. 少し後に N. Elkies は, $[GS_1]$ で構成された曲線は

Drinfeld modular curve である事を指摘しました。[GS₁]

による X_i の函数体 $K_i = \mathbb{F}_q(X_i)$ の構成は次の通りです。

$$K_1 = \mathbb{F}_q(x_1)$$

$$K_{i+1} = K_i(y_{i+1})$$

$$\left. \begin{aligned} y_{i+1}^{\sqrt{q}} + y_{i+1} &= x_i^{\sqrt{q}+1} \\ x_{i+1} &= x_i^{-1} y_{i+1} \end{aligned} \right\} (i \geq 1).$$

K_i の完備滑らかなモデル X_i について,

$$\begin{aligned} X_i \text{ の } \mathbb{F}_q \text{ 有理点の個数} &\geq (q-1)q^{\frac{i-1}{2}} + 2q^{\frac{i}{2}} \\ &\geq (\sqrt{q}-1)(q_i-1) \end{aligned}$$

となります。例えば $i=2$ のとき, X_2 は

$$y^{\sqrt{q}} + y = x^{\sqrt{q}+1}$$

の 1 点コンパクト化ですが, この各辺は $\mathbb{F}_q/\mathbb{F}_{\sqrt{q}}$ での y (ないし x) のトレース (ないし ノルム) を表わしており, トレース が全射であることから, X_2 の有理点の個数 $= q\sqrt{q} + 1$, 一方 $g_2 = \frac{1}{2}(q - \sqrt{q})$ で, X_2 は g_2 を種数とする $\mathbb{F}_q$ 上の曲線の持ち得る最大の $\mathbb{F}_q$ 有理点を有している (Weil の Riemann 予想から出る評価: $\#(X(\mathbb{F}_q)) \leq q+1+2q\sqrt{q}$ の等式で成立つ).

以上は $q = p^{2f}$ 型のときの話ですが, $q = p^{2f-1}$ 型についての話に入る前に, $A(g)$ のとり得る値の範囲について復習します。

§5 $A(g)$ について

まず $\mathbb{F}_q$ 上の種数 g の代数曲線 X の $\mathbb{F}_q$ 有理点の個数 $\#(X(\mathbb{F}_q))$ の, q と g を固定して X を動かしたときの最大値を $N_g(q)$ と置いて, こんについて考えると,

$$(5-1) \quad \#(X(\mathbb{F}_q)) = q + 1 - \sum_{j=1}^g (\pi_j + \bar{\pi}_j), \quad \pi_j \bar{\pi}_j = q$$

と表わせるので (A. Weil),

$$(5-2) \quad \#(X(\mathbb{F}_q)) \leq q + 1 + 2g\sqrt{q},$$

$$(5-3) \quad N_g(q) \leq q + 1 + 2g\sqrt{q} \quad (\text{Weil 上界}).$$

$$(5-4) \quad A(g) = \lim_{q \rightarrow \infty} \frac{N_g(q)}{q} \leq 2\sqrt{g}.$$

次に $([I_3])$, (H_1) は $X \otimes \mathbb{F}_{q^2}$ でも考え比較することより

$$(5-5) \quad N_g(q) \leq q + 1 + \frac{1}{2} (\sqrt{(8g+1)q^2 + 4(g^2-g)q} - q)$$

により

$$(5-6) \quad A(g) \leq \sqrt{2g}.$$

q が g に比べて大きいと, Weil 上界は最良ではないのです.

具体的には,

$$(5-7) \quad q > \frac{g - \sqrt{g}}{2} \quad \text{ならば} \quad (5-5) \text{ の方が } (5-3) \text{ より強い.}$$

$N_g(q)$ 自身を正確に求める研究も Van der Geer 等により盛んになされていますが, こんについては §7 で触れることにして, $A(g)$ 自身に戻ると, §§3, 4 で述べたように, $g = p^{2f}$ なら

$A(q) \geq \sqrt{q} - 1$. これらを見て Drinfeld-Vladut は, $-A$ の q についても

$$(5-8) \quad A(q) \leq \sqrt{q} - 1$$

である事を証明しました. 一方, $q = p^{2f-1}$ 型については, Serre が

$$(5-9) \quad A(q) > c \log q \quad (\exists c > 0)$$

を証明しました. 簡約すると,

$$\begin{cases} q = p^{2f} \text{ なら} & A(q) = \sqrt{q} - 1 & ([I_3], [DV]) \\ q = p^{2f-1} \text{ なら} & c \log q < A(q) \leq \sqrt{q} - 1 & ([S], [DV]) \end{cases}$$

という事になります. Serre の定数 c は かなり小さく, $\log_2 e$ には達しないので, $q = p^{2f-1}$ 型のとき §2 の部分 (G_p) は $G-V$ 曲線の上に出るかどうかが判明していませんでした.

最近 $q = p^{2f-1}$ のときも有理点の比較的多い曲線族が構成され, それによって, この場合にも (G_p) が $G-V$ を突破するような q がいろいろある事がわかってきました. 以下これについて一筋を報告したいと思います.

§6 沢山の... (iii) $q = p^{2f-1}$ (p : 素数) の場合の $A(q)$

のよい下界についてですが、現在知られている主なことをまとめると、

$$f \geq 2, p > 2 \text{ なら}$$

$$(6-1) \quad A(q) > \sqrt{p/2}$$

が成立つ (主に Niederreiter-Xing)

というものです ($f=2$ のときは Zink が Shimura surface を使って示した)。又 $f \geq 2$ - 般は、Niederreiter-Xing の結果として Xing によって Seattle で報告された。Seattle 集会の報告集 (Contemp. Math?) に論文が出ることを期待している)

p が f に比べて十分大きければ

$$\sqrt{p/2} > (\log_q \left(\frac{2q-1}{q} \right))^{-1} (\doteq \log_2 q)$$

となるので、(6-1) によって (2-5) が満たされ、従ってこの場合も線分 (G_p) の一部が $G-V$ 下界を上まわることになります。

尚 Zink や Niederreiter-Xing の結果をもとの精密な形で述べると、

$$A(p^3) \geq \frac{2(p^2-1)}{p+2} \quad (\text{Zink}),$$

$q = q_1^m$ (q_1 : 素数べき), $m > 1$ (整数) と分解するとき

$$A(q) \geq \frac{2q_1}{[\sqrt{2(2q_1+1)}]+1} \geq \sqrt{\frac{q_1}{2}} - \frac{1}{2} \quad (\text{Niederreiter-Xing}).$$

$g = p$ のとき, このような結果は, まだ知られていないようです. 個別の小さい p については,

$$\frac{81}{317} \leq A(2) \leq \sqrt{2}-1, \quad \frac{62}{163} \leq A(3) \leq \sqrt{3}-1,$$

等が知られています ([GV] 参照).

§7. その他の観測

今まで触れませんでした, [GV] に於て, Vander Geer と M. van der Vlugt は, Goppa 符号とは異なる方法で有限体上の代数曲線の有理点と符号を結びつけて大変興味深い研究を進めています. どちらかというところ上で見てきた場合 (g : 小, g : 大) とは逆の場合が ここでは興味を中心になるようです. $N_g(g)$ に関する研究や表 (Wirfz の表の改善など) も出ています. 大変わかりやすく書かれています.

その他, Perret, Lauter, Schoof, Thomas, 等の研究や少し以前の 伊吹山, Fried 等の研究もそれぞれ興味深い結果や方法を与えています.

[文献表]

(基本的文献)

- [G] V. D. Goppa : Codes on algebraic curves,
Sov. Math. Dokl 24 (1981), 170-172
- [M] Y. I. Manin : What is the maximum number of points on a
curve over $\mathbb{F}_2$? J. Fac. Sci. U. Tokyo 28 (1981), 715-720
- [I₁] Y. Ihara : The congruence monodromy problems, J. Math. Soc.
Japan 20 (1968), 107-121
- [I₂] — : Some remarks on the number of rational
points of algebraic curves over finite fields,
J. Fac. Sci. U. Tokyo 28 (1981), 721-724
- [TVZ] M. A. Tsfasman, S. G. Vladut, T. Zink : Modular curves,
Shimura curves and Goppa codes, better than the
Varshamov-Gilbert bound,
Math. Nachr 109 (1982), 21-28
- [DV] V. G. Drinfeld, S. G. Vladut : The number of points on an
algebraic curve, Funct Anal and Appl 17 (1983), 53-54
- [S] J.-P. Serre : Sur le nombre des points rationnels d'une
courbes algébrique sur un corp fini,
CR Acad. Sci Paris 296 (1983), 397-402
- [GV] Van der Geer and M. van der Vlugt : How to construct
curves over finite fields with many points,
"Algebraic Geometry" (Cambridge Univ. Press)
p 169-189 Istituto Nazionale di Alta Mat 1997.

(その他)

[GS₁] A. Garcia, H. Stichtenoth: A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound; *Invent. math.* 121 (1995), 211-222

[GS₂] — : On the asymptotic behavior of some towers of function fields over finite fields,
J. Number Theory 61 (1996), 248-273.