論文の内容の要旨

論文題目： Curves with Many Rational Points
和　　訳： 多数の有理点を持つ曲線

氏　　名： 川北　素子

1977年にGoppaにより代数幾何符号が発見されて以来, 有限体上において多数の有理点を持つ代数曲線の研究が盛んに行われるようになった. このような代数曲線が効率的な符号の存在を保証するからである. ここではそれを良い曲線と呼ぶ.

本論文は良い曲線の構築と探索を目的とする. 前半では二次形式とファイバー積を利用して最大曲線を構築し, さらに符号理論への応用を考慮して平面曲線としての定義方程式を与えた. 後半ではクンマー曲線とそのファイバー積に注目し, この種の代数曲線を探索する方法を提案した. 限定した範囲で計算機探索を実行した結果, 存在の知られていない代数曲線を見付ける事が出来た.

初めに q を素数のべきとし, 有限体 $\mathbb{F}_{q^m}$ 上で考える. まず $\mathbb{F}_{q^m}$ 上のある種の二次形式の有理点数を決定し, それに関連したアルティン-シュウライア曲線の種数と有理点数を定式化した.

定理. 自然数 h と $R(X) \in R_h$ が存在して

$$Q(X) \equiv \mathrm{Tr}(XR(X)) \mod (X^{q^m} - X)$$

である. この $R(X)$ を用いて曲線 C_R を

$$Y^q - Y = XR(X)$$

で定義すると以下が成り立つ.

(i) $a_1, a_2, \cdots, a_M, b_1, b_2, \cdots, b_M$ が $\mathbb{F}_q$ 上線形独立ならば C_R の有限体 $\mathbb{F}_{q^m}$ 上の有理点数は $\#C_R(\mathbb{F}_{q^m}) = q^m + 1 + (q-1)\sqrt{q^m \cdot q^w}$ で与えられる.

(ii) 次のいずれかが成り立つとする.

1. q が偶数であり, $\deg R(X) \geq 2$ である.
2. q が奇数であり, $\deg R(X) \geq 1$ である.

この時 C_R の種数は

$$g(C_R) = \frac{(q-1) \cdot \deg R(X)}{2}$$

で与えられる.

さらにこの種のアルティン-シュウライア曲線の種数が下がる条件を与えた. 具体的に計算した結果, 以下のようなアルティン-シュウライア曲線のファイバー積で得られる最大曲線を見付ける事が出来た. このような最大曲線の存在は知られていたものの定義方程式は与えられていなかった.

命題. m を偶数とする. 次のいずれかが成り立つと仮定する.

1. q が偶数であり, $m \geq 4, l \leq \frac{m}{2} - 1$ である.
2. q が奇数であり, $l \leq \frac{m}{2}$ である.

有限体 $\mathbb{F}_{q^m}$ 上種数

$$g = \frac{(q^l - 1) \cdot q^{\frac{m-2}{2}}}{2}$$

の最大曲線が存在し, 以下の曲線のファイバー積で定義される.

$$Y_i^q - Y_i = X \cdot r_i(X).$$

ここで $i = 1, \cdots, l$ について

$$r_i(X) := b_i X + \sum_{j=1}^{\frac{m-2}{2}} (b_i + b_i^{q^j}) X^{q^j},$$

${b_i}^{q^{\frac{m}{2}}} + b_i = 0$, ${b_i}^q - b_i \neq 0$ である. さらに $b_1, b_2, \cdots, b_l$ は $\mathbb{F}_q$ 上線形独立である.

そして上の最大曲線を含む一群のアルティン-シュウライア曲線のファイバー積で作られる代数曲線に平面曲線としての定義方程式を与えた. これにより符号理論へ応用し易くなる.

次に有限体 $\mathbb{F}_q$ を固定し, n を $q-1$ の約数とする. 以下 $Y^n - f(X) \in \mathbb{F}_q(X)[Y]$ で定義される代数曲線をクンマー曲線と呼び, その性質を考える.

まずある条件の下で

$$Y^a f(Y)(Y-1)^b - X^n \in \mathbb{F}_q[X,Y]$$

で定義されるクンマー曲線が原点, $(0,1)$ 及び無限遠点以外では非特異な時の種数が

$$g = \frac{1}{2}(\deg f(Y)+1)(n-1) - \Delta$$

である事を見出した. ここで Δ が比較的小さい負でない整数なので, $f(Y)$ と n を固定させ, a と b を走らせる事により有理点を多数持つ代数曲線を探索出来る. 種数の計算はプリュカの公式を使った.

そして $f(X) \in \mathbb{F}_q[X]$, $q-1$ の約数 n_1 と n_2 に対し,

$$Y_1^{n_1} = X(X-1),$$
$$Y_2^{n_2} = X^a(X-1)^b f(X),$$

で定義された二つのクンマー曲線のファイバー積がある条件の下で種数が

$$g = \frac{1}{2}(u+1)n_1 n_2 + 1 - \Delta$$

である事を見出した. ここで u は $f(X)$ に依存する負でない整数であり, Δ は比較的小さい負でない整数である. 従って $f(X)$ と n_1, n_2 を固定させ, a と b を走らせる事により有理点を多数持つ代数曲線を探索出来る. 種数の計算にはフルビッツの公式を使った.

提案方式で具体的に探索を行った結果, 新しい曲線を得た. 表 1 のように G. van der Geer らがまとめた評価を更新することが出来た.

表 1: $N_q(g)$ の評価

q	g	new entry	old entry
16	16	[95-118]	[93-118]
64	16	[267-318]	
64	34	[447-582]	
27	37	[236-326]	
27	49	[316-409]	[314-409]
81	7	[180-208]	[172-208]
81	13	[256-314]	[243-314]
81	34	[494-692]	
81	37	[568-743]	