数理解析研究所講究録 1361 巻 2004 年 47-50

SOME QUOTIENT CURVES OF FERMAT CURVES ATTAINING SERRE BOUND

お茶の水大・情報 川北 素子 (Motoko Kawakita)
Department of Information Sciences,
Ochanomizu University

1970 年代に Goppa が代数幾何符号を発見して以来, 有限体上において多数の有理点をもつ代数曲線の研究が盛んになった. それが効率よい誤り訂正符号の存在を保証するからである. 本稿では, 特に Serre 上界に達する曲線に関する私の研究成果を紹介する. なお, 曲線は絶対既約かつ非特異な射影曲線とする.

有限体 $\mathbb{F}_q$ 上, 種数 g の曲線 C の有理点数について, Hasse–Weil 上界 $\#C(\mathbb{F}_q) \leq q+1+2g\sqrt{q}$ がある. 1983 年, Serre が [17] で改良し,

$$\#C(\mathbb{F}_q) \leq q+1+g\lfloor 2\sqrt{q}\rfloor$$

($\lfloor\ \rfloor$ はガウス記号) を示した. Serre 上界といい, これに達する曲線の L-多項式は $(1+\lfloor 2\sqrt{q}\rfloor t+qt^2)^g$ である [13]. また Lauter が [14] で, 伊原氏の結果 [6] を一般化し, Serre 上界は $g \leq (q^2-q)/(\lfloor 2\sqrt{q}\rfloor+\lfloor 2\sqrt{q}\rfloor^2-2q)$ のときにしか達しえないことを示した.

Hasse–Weil 上界に達する曲線は最大曲線とよばれ, 多くの性質が知られている. 文献としては [3], [12] などがある. しかし, 最大曲線ではなく, Serre 上界に達する曲線はわずかな例しか知られていないため, ほとんど研究されていない. 私は三浦氏の [16] に掲載された曲線を手がかりに研究を行った.

まず三浦氏が見つけた曲線は同型を除くと 2 本になった. 一つは, $\mathbb{F}_{2^3}$ 上の Klein 曲線 $x^3y+y^3+x=0$ であり, すでに Serre の [18] に紹介されていた. もう一つは, $\mathbb{F}_{2^{11}}$ 上 $y^{23}=x^4(1-x)$ で定義された種数 11 の曲線である. 第 1, 2 節で各々について, 第 3 節で一般化した形の曲線の中をコンピュータ探索して得られた新しい曲線を述べる.

1. KLEIN 曲線

この有名な曲線は古くから研究されており [15], $\mathbb{F}_{2^3}$ 上 Serre 上界に達することがわかってから, 符号理論への応用も試みられた [4], [11]. 曲線

$$y^7=x^4(1-x)$$

と同型であるので, 他の有限体上での有理点数を [8] のアルゴリズムでコンピュータ探索した. 素数 p が以下のとき, $\mathbb{F}_p$ 上 Serre 上界に到達した.

$$1163, 1709, 2311, 3851, 4789, 5783, 5839, 6917, 9437, 13931, \cdots.$$

結果は[1]に含まれてしまったが, 後の研究の指針を与えてくれたので, あえてここに記した.

2. 曲線 $y^{23} = x^4(1-x)$

種数が3より大きく, 最大曲線でないSerre上界に達する曲線はこれしか知られていなかったので, その性質を調べて[9]にまとめた. その一部を紹介する. 以下 $k := \mathbb{F}_{2^{11}}$, M を k 上

$$y^{23} = x^4(1-x)$$

で定義された曲線とする.

命題 1. M の自己同型群は $\mathbb{Z}/23\mathbb{Z}$ と同型あり, 生成元は

$$x \mapsto x,\ y \mapsto \epsilon y$$

で定義される. ただし, ϵ は乗法群 k^* の1の23乗根である.

命題 2. M の k 上の L 多項式は

$$L(M,t) = (1 + 90t + 2048t^2)^{11}$$

である.

命題 3. M のWronskianは

$$\begin{aligned} &y^{17}(x^3+x^2+1)(x^8+x^7+x^6+x^5+x^4+x+1)\\ &(x^{35}+x^{34}+x^{32}+x^{30}+x^{29}+x^{28}+x^{27}+x^{26}\\ &\quad +x^{19}+x^{18}+x^{15}+x^{11}+x^8+x^5+x^4+x^3+1)\\ &(x+1)^3x^{-76}, \end{aligned}$$

である.

命題 4. M は1061個のWeierstrass点をもち, そのgap列は表のようになる.

点	gap列
原点	$\{1,2,3,4,5,6,8,9,12,13,16\}$
無限遠点	$\{1,2,3,4,6,8,9,11,13,16,18\}$
$(1,0)$	$\{1,2,3,4,6,7,8,9,12,13,18\}$
その他	$\{1,2,3,4,5,6,7,8,9,10,12\}$

符号理論への応用については原論文[9]を参照されたい.

なお, この曲線についても, 奇数べき拡大の有限体上でSerre上界に達しないか探索を行ったが, Klein曲線のような結果が得られていない.

3. 曲線 $y^n = x^4(1-x)$

第1, 2節の曲線の定義方程式をヒントに自然数 n について

$$y^n = x^4(1-x)$$

で定義される曲線を考察した. Faddeev の [2] より, $x = X^n$, $y = X^4Y$ とおくと次数 n の Fermat 曲線 $X^n + Y^n = 1$ からこの曲線への写像ができるので, 商曲線である.

ここで $n = 12$ についてコンピュータ探索をし, 素数 p が

$$15733, 24133, 26029, 27997, 38917, 43789, 51637, 60133,$$
$$72469, 93133, 124717, 142237, 151429, 185869, 196681, \cdots$$

のときに, 曲線が $\mathbb{F}_p$ 上 Serre 上界に達することがわかった. これらを解析して以下の結果を得たが, 詳しくは [10] にまとめた.

定理. p を素数とし, $\mathbb{F}_p$ 上種数 4 の曲線 C が

$$y^{12} = x^4(1-x)$$

で定義されているとする.

曲線 C が Serre 上界に達する必要十分条件は, p が以下を満たすことである.

1. $p \equiv 1 \bmod 12$.
2. $\lfloor 2\sqrt{p} \rfloor \equiv 1 \bmod 3$.
3. $p = \lfloor \sqrt{p} \rfloor^2 + 27r^2$ となる自然数 r が存在する.

定理の証明は, [7] の第8章§3にある Gauss の定理をヒントに, Jacobi 和を使った.

また Hardy–Littlewood が [5] で一般化した次の予想がある.

Buniakowski の予想. a, b, c が整数, a が正, $\gcd(a,b,c) = 1$, $a+b$ と c の少なくとも一方が奇数, $b^2 - 4ac$ が平方でないとすると, $am^2 + bm + c$ の形の素数が無限個ある.

命題 5. Buniakowski の予想が正しいならば, 定理の条件を満たす素数が無限個存在する.

今後 n を大きくした場合についても探索し, 定理を一般化したいと考えている.

謝辞. 本研究を進めるにあたり, 三浦晋示氏より貴重なアドバイスを頂きました. 心よりお礼を申し上げます. また, Jean-Pierre Serre 教授, Arnaldo Garcia 教授, 本間正明教授, 桂利行教授, 關口力教授, 金子晃教授の有益なご助言に深く感謝致します. コンピュータ探索には Kash/Kant を使用しました.

References

[1] R. Auer, J. Top, Some genus 3 curves with many points, Algorithmic number theory (Sydney, July 2002), Lecture Notes in Comput. Sci. **2369**, Springer 2002, 163–171.

[2] D. K. Faddeev, The group of divisor classes on some algebraic curves, Dokl. Akad. Nauk SSSR **136**, 296–298 (Russian); translated as Soviet Math. Dokl. **2**(1961), 67–69.
[3] A. Garcia, H. Stichtenoth, C. P. Xing, On subfields of the Hermitian function field, Compositio Math. **120**(2000), no. 2, 137–170.
[4] J. P. Hansen, Codes on the Klein quartic, ideals, and decoding, IEEE Trans. Inform. Theory **33**(1987), no. 6, 923–925.
[5] G. H. Hardy, J. E. Littlewood, Some problems of 'partitio numerorum'; III: on the expression of a number as a sum of primes, Acta Math. **44**(1923), 1–70.
[6] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28**(1981), no. 3, 721–724.
[7] K. Ireland, M. Rosen, A classical introduction to modern number theory, Second edition, Graduate Texts in Mathematics **84**, Springer-Verlag 1990.
[8] M. Q. Kawakita, Kummer curves and their fibre products with many rational points, Appl. Algebra Engrg. Comm. Comput. **14**(2003), 55–64.
[9] ———, A quotient curve of Fermat curve of degree 23 attaining Serre bound, submitted for publication.
[10] ———, Quotient curve of Fermat curve of degree twelve attaining Serre bound, submitted for publication.
[11] M. S. Kolluru, G. L. Feng, T. R. N. Rao, Construction of improved geometric Goppa codes from Klein curves and Klein-like curves, Appl. Algebra Engrg. Comm. Comput. **10**(2000), no. 6, 433–464.
[12] G. Korchmáros, F. Torres, On the genus of a maximal curve, Math. Ann. **323**(2002), no. 3, 589–608.
[13] G. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, C. R. Acad. Sci. Paris, Sér. I Math. **305**(1987), no. 16, 729–732.
[14] K. Lauter, Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, with an appendix by J.-P. Serre, J. Algebraic Geom. **10**(2001), no. 1, 19–36.
[15] S. Levy (ed.), The eightfold way: the beauty of Klein's quartic curve, Mathematical Sciences Research Institute Publications **35**, Cambridge University Press 1999.
[16] S. Miura, Algebraic geometric codes on certain plane curves (Japanese), IEICE Trans. Fundamentals **J75-A** no. **11** (Nov. 1992), 1735–1745.
[17] J. -P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, C. R. Acad. Sci. Paris Sér. I Math. **296**(1983), no. 9, 397–402. (=Œuvres III, No. 128, 658–663.)
[18] ———, Rational points on curves over finite fields, Note of lectures at Harvard University 1985.

112-8610 東京都文京区大塚 2-1-1 お茶の水女子大学理学部情報科学科金子研究室
E-mail address: kawakita@cc.ocha.ac.jp