有限体上の函数体の塔の漸近的 zeta 函数：その一

長谷川　武博*

概　要

この Note では，有限体上の函数体の塔の漸近的 zeta 函数 (おもちゃ) を定義し，そこにいままでに証明されてきた函数体の塔の結果を当て嵌め，この漸近的 zeta 函数が **数学的に興味深い対象** であることを説く．

1. 函数体

この §1 と次の §2 は，§3 で函数体の塔の漸近的 zeta 函数を，§4 で代数幾何符号を楽しむための枕である．この Note を通して q を素数の冪とし，K を有限体 $\mathbb{F}_q$ とする：$K = \mathbb{F}_q$．その他は H. Stichtenoth の textbook [S]，または A. Garcia と Stichtenoth の論文 [GS1, GS2] に従う．

体 F が K 上の 1 変数 **代数函数体** であるとは，F が K の拡大体かつ K 上超越的なある元 $x \in F$ があって，拡大 $F/K(x)$ が有限次代数的かつ K が F で代数的に閉じているときをいう[1]：$K = \{z \in F \mid z \text{ は } K \text{ 上代数的}\}$．この Note では代数函数体を F/K とかいて，単に **函数体** とよぶ．

1992 年に Garcia [G] は，次の函数体 H を構成した．

例 1.1.　q を素数の冪とし，r を正の奇数とする．このとき，

$$H = \mathbb{F}_{q^{2r}}(x, y)$$

は，次数 1 の有理点の個数が $N(H/\mathbb{F}_{q^{2r}}) = q^{2r+1} + 1$ かつ種数は $g(H) = q^r(q-1)/2$ なる $\mathbb{F}_{q^{2r}}$ 上の函数体である[2]．また $r = 1$ のとき，H を **Hermite 函数体** という[3]．

注意.　もし $r \geq 3$ なら，射影代数曲線

*Present Address: Department of Mathematics, School of Education, Waseda University, Tokyo 169-8050, Japan, E-mail: thasegawa@aoni.waseda.jp

1) 任意の代数函数体 F は，ある有理函数体 $K(x)$ の単純代数拡大体である．すなわち，F はある既約多項式 $\varphi \in K(x)[T]$ の根 y を $K(x)$ に添加した体 $K(x, y)$ である．

2) この場合の既約多項式は $\varphi = T^{q^r+1} - x^q - x \in \mathbb{F}_{q^{2r}}(x)[T]$ である．

3) これは，次数 1 の有理点をたくさんもつので，良い代数幾何符号 (幾何学的 Goppa 符号ともいう) を作ることができる ([KKO], [HKK]).

$$Y^{q^r+1} = X^q Z^{q^r-q+1} + XZ^{q^r}$$

は無限遠点 Q を特異点にもつ．$r = 1$ のときは非特異である．

n を正整数とし，$B_n(F/K)$ を函数体 F/K の次数 n の有理点全体の集合とする．ただし $B_1(F/K)$ は単に $N(F/K)$ とかく．F の種数を $g(F)$ とかく．次数 1 の有理点の個数については，Hasse-Weil (-Serre) 限界

$$|N(F/K) - q - 1| \leq 2g\sqrt{q} \qquad (\text{resp. } \leq g[2\sqrt{q}])$$

が知られている．ここで $[r]$ は Gauss 記号とする．もし $N(F/K) = q + 1 + 2g\sqrt{q}$ なら，F/K を **最大 (maximal) 函数体** という．例 1.1 の函数体 $H/\mathbb{F}_{q^{2r}}$ は最大である．なぜなら，

$$N(H/\mathbb{F}_{q^{2r}}) = q^{2r+1} + 1 = q^{2r} + 1 + q^r(q-1)\cdot q^r = q^{2r} + 1 + 2g(H)q^r$$

となる．他にも，Suzuki 函数体や Ree 函数体も最大である[4]．最大函数体の有理点の個数については，次の命題がある：

命題 1.2 ([H1])． l を素数とし，$F/\mathbb{F}_{q^2}$ を種数 g の最大函数体とする．このとき，次数 l の有理点の個数は，

$$B_l(F/\mathbb{F}_{q^2}) = \frac{q(q^{l-1} + (-1)^l)(q^l + (-1)^{l-1}q + (-1)^{l-1}2g)}{l}$$

となる．もし最大函数体 $F/\mathbb{F}_{q^2}$ が次数 2 の有理点をもたないなら，これは *Hermite* 函数体に $\mathbb{F}_{q^2}$ 上同型である．この逆も成り立つ[5]．

函数体 F/K と K の代数拡大体 $\mathbb{F}_{q^n}$ との合成体 $F\mathbb{F}_{q^n}$ は $\mathbb{F}_{q^n}$ 上の函数体になる．ここで $l = 2$ の証明の概略を，函数体 $F/\mathbb{F}_{q^2}$ の **合同 zeta 函数**

$$Z_F(t) = \exp\left(\sum_{n=1}^{\infty} \frac{N(F\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^{2n}})}{n} \cdot t^n\right)$$

を使って，おさらいする：$F/\mathbb{F}_{q^2}$ の合同 zeta 函数 $Z_F(t)$ を

$$Z_F(t) = \prod_{i=1}^{g}(1 - (\overbrace{\alpha_i + \alpha_{g+i}}^{\text{実数}})t + q^2t^2) \Big/ (1-t)(1-q^2t), \quad g = g(F)$$

とかけば，次数 2 の有理点の個数は

$$2\cdot B_2(F/\mathbb{F}_{q^2}) = \overbrace{q^4 - q^2 + 2gq^2}^{\text{正の整数}} + \sum_{i=1}^{g}(\alpha_i + \alpha_{g+i}) - \sum_{i=1}^{g}(\alpha_i + \alpha_{g+i})^2$$

である．もし F が最大なら，すべての $1 \leq i \leq g$ に対して $\alpha_i + \alpha_{g+i}$ は最小値 $-2q$ をとるので，各 i において $(\alpha_i + \alpha_{g+i})^2$ は最大値 $4q^2$ をとる．

4) Ree 函数体については J. P. Pedersen の論文 [P] をみろ．

5) $l = 2$ のとき $B_2(F/\mathbb{F}_{q^2}) = q(q+1)(q^2 - q - 2g)$ である．Hermite 函数体の種数は $g = q(q-1)/2$ なので $B_2(H/\mathbb{F}_{q^2}) = 0$ を得る．

注意. ここから，函数体 $F/\mathbb{F}_{q^2}$ を **どんどん** 最大函数体に近づけると，次数 2 の有理点の個数 $B_2(F/\mathbb{F}_{q^2})$ は **だんだん** 小さくなる，ことがわかる．

2. 函数体の塔

1996 年に Garcia と Stichtenoth [GS2] は，漸近的に良い代数幾何符号の列を構成する為に，函数体の塔を紹介した．函数体 F_i/K の列

$$\mathcal{F} = (F_0, F_1, F_2, \ldots)$$

が **K-函数体の塔** (または単に K-塔) であるとは，$F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots$ かつ各拡大 F_{i+1}/F_i は分離的かつある s に対して $g(F_s) > 1$ であるときをいう．K-塔 $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ と K の代数拡大体 $\mathbb{F}_{q^n}$ との合成列

$$\mathcal{F}\mathbb{F}_{q^n} := (F_0\mathbb{F}_{q^n}, F_1\mathbb{F}_{q^n}, F_2\mathbb{F}_{q^n}, \ldots)$$

は $\mathbb{F}_{q^n}$-函数体の塔になる．n を正整数とし，

$$\Delta_n(\mathcal{F}/K) = \lim_{i\to\infty} \frac{B_n(F_i/K)}{g(F_i)}$$

を $\mathcal{F}$ の **一般化 Garcia-Stichtenoth 不変量** とよぶ[6]．これは非負整数である．$\Delta_1(\mathcal{F}/K)$ を $\lambda(\mathcal{F}/K)$ とかいて，Garcia-Stichtenoth 不変量とよぶこともある．もし $\lambda(\mathcal{F}/K) > 0$ (resp. $\lambda(\mathcal{F}/K) = 0$) なら $\mathcal{F}/K$ を **漸近的に良い** (resp. **漸近的に悪い**) という[7]．

$$A(q) = \limsup_{g\to\infty} \frac{\max\{N(F/K) \mid F/K \text{ は種数 } g \text{ の函数体 }\}}{g}$$

とおけば，これは $\lambda(\mathcal{F}/K)$ の上限を与える．すなわち $\lambda(\mathcal{F}/K) \le A(q)$ を得る．もし $\lambda(\mathcal{F}/K) = A(q)$ なら $\mathcal{F}/K$ を **漸近的に最良** という[8]．

1983 年に V. G. Drinfeld と S. G. Vlăduţ は，任意の q に対して，いわゆる Drinfeld-Vlăduţ 限界 $A(q) \le \sqrt{q} - 1$ を示した．また 1968 年頃，伊原康隆氏は有限体上の Shimura 曲線の理論を使って，任意の q^2 に対して $A(q^2) = q - 1$ を示した[9]．

Garcia と Stichtenoth [GS1, GS2] は次の函数体の塔を紹介した．

例 2.1. (i) 整数 $e > 1$ と素数 p に対して，

$$\varphi(x, y) = y^m + (x+1)^m - 1, \quad m = \frac{p^e - 1}{p - 1}$$

6) この極限は実際に存在する [H4].
7) この奇妙な呼び名は符号理論からきている.
8) 1997 年ごろ，N. Elkies [E] は次のことを予想した：$\mathbb{F}_{q^2}$-函数体の塔 $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ は modular である．すなわち，$\mathcal{F}$ における各 F_i は楕円 modular 曲線，Shimura modular 曲線，または Drinfeld modular 曲線のいずれかの還元の函数体である.
9) 1982 年に M. A. Tsfasman と S. G. Vlăduţ と T. Zink は楕円 modular 曲線の理論を使って，伊原氏とは独立に任意の素数の冪 p^2 に対して $A(p^2) = p - 1$ を示した.

とおく．F_0 を有理函数体 $\mathbb{F}_{p^e}(x_0)$ とする：$F_0 = \mathbb{F}_{p^e}(x_0)$．さらに，各 $i > 0$ について F_i を $\varphi(x_{i-1}, T)$ の根 x_i を F_{i-1} に添加した体 $F_{i-1}(x_i)$ とする：$F_i = F_{i-1}(x_i)$．このとき，$\mathcal{F} = (F_0, F_1, F_2, \ldots)$ は

$$\lambda(\mathcal{F}/\mathbb{F}_{p^e}) \geq \frac{2}{p^e - 2}$$

なる $\mathbb{F}_{p^e}$-函数体の塔である．もし $e = p = 2$ なら漸近的に最良となる[10]．なぜならば $\lambda(\mathcal{F}/\mathbb{F}_4) = A(4) = 2$ である．また，各 n について，合成塔 $\mathcal{F}\mathbb{F}_{p^{ne}}$ の Garcia-Stichtenoth 不変量は

$$\lambda(\mathcal{F}\mathbb{F}_{p^{ne}}/\mathbb{F}_{p^{ne}}) \geq \frac{2}{p^e - 2} \tag{1}$$

となる．

(ii) $r > 2$ を素数の冪とし，n を正の整数とする．このとき，

$$\varphi(x, y) = y^{r-1} + (x+1)^{r-1} - 1$$

は $\mathbb{F}_{r^{2n}}$-函数体の塔 $\mathcal{F}\mathbb{F}_{r^{2n}}$ を構成し，$\lambda(\mathcal{F}\mathbb{F}_{r^{2n}}/\mathbb{F}_{r^{2n}}) \geq 2/(r-2)$ となる．もし $r = 3$ かつ $n = 1$ なら，この塔は漸近的に最良である[11]．

(iii) q を素数の冪とする．このとき，

$$\varphi(x, y) = (x^{q-1} + 1)(y^q + 1) - x^q$$

は $\lambda(\mathcal{F}/\mathbb{F}_q) = q - 1$, $\Delta_n(\mathcal{F}/\mathbb{F}_q) = 0$, $n \geq 2$ なる最良塔を作る[12]．

注意． 不等式 (1) は **おそらく** 等号である．実際，もし $n = 1$ なら，この予想は正しい [H5]．任意の n で成り立ちそうな **感触** はある．

最近，近藤庄一氏らは，次の函数体の塔から漸近的に良い 1 点代数幾何符号の列を構成した．これについては §4 で詳しく採り上げる．

例 2.2 ([HKK], cf. 例 1.1). r を正の奇数とする．このとき，$\varphi(x, y) = y^{q^r+1} - x^q - x$ は $\mathbb{F}_{q^{2r}}$-函数体の塔 $\mathcal{F}$ を構成する．ところが，この塔は漸近的に悪い[13]．さらに，任意の $n \geq 1$ について $\Delta_n(\mathcal{F}/\mathbb{F}_{q^{2r}}) = 0$ である．

一般化 Garcia-Stichtenoth 不変量の上限と下限について，次のような定理がある：

---

10) これは楕円 modular 曲線 $\{X_0(3^i)\}$ の modulo 2 還元である [E].
11) こっちは $\{X_0(2^i)\}$ の modulo 3 還元 [E].
12) これは Drinfeld modular 曲線の還元 [E].
13) $\deg_x \varphi \neq \deg_y \varphi$ なる $\varphi = 0$ から作った塔は漸近的に悪い [GS3].

定理 2.3 ([H4]). $\mathcal{F}$ を K-函数体の塔とする．

(i) すべての $n \geq 2$ に対して

$$\Delta_n(\mathcal{F}/K) \leq \frac{\sqrt{q^n}-1}{n}\left(1-\frac{\lambda(\mathcal{F}/K)}{\sqrt{q}-1}\right)$$

が成り立つ[14]．

(ii) $q = \square$ とする．もし $\mathcal{F}$ が漸近的に最良な塔なら，各 $n \geq 2$ に対し

$$\Delta_n(\mathcal{F}/K) = 0, \qquad \lambda(\mathcal{F}\mathbb{F}_{q^n}/\mathbb{F}_{q^n}) = \sqrt{q}-1$$

を得る．よって，合成塔 $\mathcal{F}\mathbb{F}_{q^n}$ *(*$n \geq 2$*)* は漸近的に最良でない．

定理 2.4 ([H4]). n を正整数とし，もし K-塔 $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ が

(a) 各 *step* F_{i+1}/F_i は順 *(tame)* 拡大；

(b) $V = \{P \ : \ P$ はある拡大 F_s/F_0 で分岐する有理点 $\}$ は有限集合；

(c) 集合

$$Spl_n = \{P \ : \ P \text{ はすべての拡大 } F_i/F_0 \text{ において}$$
$$\text{完全分解する次数 } n \text{ の有理点}\}$$

は空でない；

を充たすなら，

$$\Delta_n(\mathcal{F}/K) \geq \frac{2 \cdot \#Spl_n}{2g(F_0)-2+\sum_{P\in V}\deg P} > 0$$

が成り立つ．

定理 2.3 と定理 2.4 を併せると，次の系を得る：

系 2.5. $q = \square$ とする．もし K-函数体の塔 $\mathcal{F}$ が，ある $n \geq 2$ に対して，定理 *2.4* のすべての条件を充たすなら，$\mathcal{F}$ は漸近的に最良でない．

注意. 定理 2.3 (i) の上限よりも，もっと具体的な計算に適した上限もある [H2]．有限体上の函数体の類体塔を使うと，定理 2.4 の下限よりも，もっとよい下限を得ることができるが，まだ具体例がみつかっていない [H3].

予想. 定理 2.3 (ii) とは違って，ある $n \geq 2$ で

$$0 < \lambda(\mathcal{F}/K) < \lambda(\mathcal{F}\mathbb{F}_{q^n}/\mathbb{F}_{q^n})$$

なる漸近的に良い K-函数体の塔 $\mathcal{F}$ は，まだ構成されていない[15]．

14) この主張は M. A. Tsfasman [T] によっても示された．証明はまったく異なる．
15) 2つ以上の方程式から作られる漸近的に良い函数体の塔を構成してみてはどうか．

3. 函数体の塔の zeta 函数

§1 では，合同 zeta 函数という scope を使って，最大函数体 $F/\mathbb{F}_{q^2}$ と次数 2 の有理点の個数 $B_2(F/\mathbb{F}_{q^2})$ が不仲なことをみた．ここでは，合同 zeta 函数の類似物なる函数体の塔の漸近的 zeta 函数を定義して，漸近的に最良な $\mathbb{F}_{q^2}$-函数体の塔の漸近的 zeta 函数の様子をみる．

K-函数体の塔 $\mathcal{F}$ の **漸近的 zeta 函数**[16] は，函数体の合同 zeta 函数と同様に，形式的冪級数

$$\mathcal{Z}_{\mathcal{F}}(t) = \exp\left(\sum_{n=1}^{\infty} \frac{\lambda(\mathcal{F}\mathbb{F}_{q^n}/\mathbb{F}_{q^n})}{n} \cdot t^n\right) \in \mathbb{C}[[t]]$$

によって定義する．これは半径 $\sqrt{q}^{-1}$ の開円板上の解析函数である．なぜなら，Drinfeld-Vlăduţ 限界によって $\lambda(\mathcal{F}\mathbb{F}_{q^n}/\mathbb{F}_{q^n}) \leq \sqrt{q^n} - 1$ を得る．他方，

$$\lim_{n\to\infty} \frac{\sqrt{q^{n+1}} - 1}{\sqrt{q^n} - 1} = \sqrt{q}$$

から，$\lim_{n\to\infty} \sqrt[n]{\sqrt{q^n} - 1} = \sqrt{q}$ となる．よって，$\lim_{n\to\infty} \sqrt[n]{n} = 1$ なので

$$\lim_{n\to\infty} \sqrt[n]{\frac{\sqrt{q^n} - 1}{n}} = \sqrt{q}$$

を得る．したがって，形式的冪級数

$$\sum_{n=1}^{\infty} \frac{\lambda(\mathcal{F}\mathbb{F}_{q^n}/\mathbb{F}_{q^n})}{n} \cdot t^n$$

は，とにかく収束半径 $\sqrt{q}^{-1}$ をもつので，$\mathcal{Z}_{\mathcal{F}}(t)$ は，この半径の開円板上解析的である．これで証明が終わる．

そこで，漸近的 zeta 函数は次の性質をもつ：

命題 3.1. (i) もし $\mathbb{F}_{q^2}$-函数体の塔 $\mathcal{F}$ が漸近的に最良なら

$$\mathcal{Z}_{\mathcal{F}}(t) = \left(\frac{1}{1-t}\right)^{q-1} \quad \left(= \left(\frac{1}{1-t}\right)^{\lambda(\mathcal{F}/\mathbb{F}_{q^2})}\right)$$

となる．また，これは函数等式

$$\mathcal{Z}_{\mathcal{F}}\left(\frac{1}{t}\right) \cdot \mathcal{Z}_{\mathcal{F}}\left(\frac{1}{1-t}\right) = 1$$

をもつ[17]．

(ii) すべての拡大 F_i/F_0 が *abel* な K-塔 $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ に対し

$$\mathcal{Z}_{\mathcal{F}}(t) = 1$$

である．

16) 最近になって，漸近的 zeta 函数は M. A. Tsfasman-S. G. Vlăduţ [TV] でも定義されてることがわかった．
17) 定数 1 ってのは気になるが，対応 $t \leftrightarrow 1-t$ は **いかにも** 函数等式らしい？

Proof. (i) いま $\mathcal{F}$ は漸近的に最良なので，任意の $n \geq 1$ について $\lambda(\mathcal{F}\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^{2n}}) = q-1$ となる．したがって，$|t| < 1$ に対して

$$\frac{d}{dt}\log \mathcal{Z}_{\mathcal{F}}(t) = (q-1)\cdot\sum_{n=1}^{\infty} t^{n-1} = \frac{q-1}{1-t}, \quad \mathcal{Z}_{\mathcal{F}}(0) = 1$$

なので，$\mathcal{Z}_{\mathcal{F}}(t) = (1-t)^{1-q}$ を得る．函数等式は明らか．

(ii) このような塔は漸近的に悪い[18] ので明らか． □

注意. (ii) の漸近的 zeta 函数を

$$\mathcal{Z}_{\mathcal{F}}(t) = \left(\frac{1}{1-t}\right)^{0} \quad \left(= \left(\frac{1}{1-t}\right)^{\lambda(\mathcal{F}/K)}\right)$$

とみれば，これは (i) と同じ形になる．

予想. (い) 例 2.1 (i) の函数体の塔について，漸近的 zeta 函数は

$$\mathcal{Z}_{\mathcal{F}}(t) = \left(\frac{1}{1-t}\right)^{2/(p^e-2)}$$

となるか？ では，例 2.1 (ii) についてはどうか？

(ろ) 次数の関係が

$$\max\{\deg f_1, \deg f_2\} = \max\{\deg g_1, \deg g_2\}$$

なる４つの多項式 $f_1, f_2, g_1, g_2 \in K[T]$ に対して，

$$\frac{f_1(y)}{f_2(y)} = \frac{g_1(x)}{g_2(x)}$$

から作られた K-函数体の塔 $\mathcal{F}$ の zeta $\mathcal{Z}_{\mathcal{F}}(t)$ はどのような形か？ 例えば，$f_2 = 1$ かつ $0 < \deg g_2 < \deg g_1$ のときは，**ほとんど** が

$$\mathcal{Z}_{\mathcal{F}}(t) = \left(\frac{1}{1-t}\right)^{\lambda(\mathcal{F}/K)}$$

となる[19].

(は) いままでは，１つの方程式 $\varphi(x,y) = 0$ のみで作った函数体の塔の zeta をみてきたが，２つ以上の方程式から構成される函数体の塔の zeta はどのような形か？ **おそらく** この形でない zeta を含む．

(に) $\mathcal{F}$ を K-函数体の塔とする．このとき，**解析的なもの** $\mathcal{Z}_{\mathcal{F}}(t)$ の性質を使って，**代数的なもの** $\mathcal{F}$，または (もし $\mathcal{F}$ が $\varphi = 0$ によって作られているなら) **幾何的なもの** $\varphi(x,y) = 0$ についてなにが云えるか．

18) この事実は G. Frey-M. Perret-H. Stichtenoth の論文 [FPS] をみてほしい．
19) 詳細は P. Beelen の論文 [B] の §4 と §5 をみてほしい．

4. 塔から代数幾何符号の列の構成 (付録)

ここでは，§2 の例 2.2 でみた漸近的に悪い塔から漸近的に良い 1 点代数幾何符号の列を構成する．

$n > 0$ を整数とする．$\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in K^n$ に対して，$d(\mathbf{a}, \mathbf{b}) = \#\{i \mid a_i \neq b_i\}$ を K^n 上の Hamming 距離という．K^n の部分空間 C $(\neq \{0\})$ を，長さ n かつ次元 $k = \dim C$ の **線型符号** とよぶ．

$$d(C) = \min\{d(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in C, \mathbf{a} \neq \mathbf{b}\}$$

を C の最小距離という．このような線型符号 C を $[n, k, d]_q$-符号とよぶ．

$[n, k, d]_q$-符号 C に対して

$$\delta = d/n, \qquad R = k/n$$

を，それぞれ **相対最小距離** と **伝送率** という．この 2 つの値がともに小さくないとき，C を **良い符号** とよぶ．Singleton 限界

$$\delta + R \leq 1 + 1/n$$

から，δ と R を同時に大きくすることはできない．

符号理論の進む道は，いつも良い符号を具体的に作ることにある．しかし，勝手な符号の相対最小距離や伝送率の計算はとても難しい．よって，その符号が良い符号かどうかをみることができない．V. D. Goppa は，符号に代数的な構造を入れることで，この問題を **ほぼ** 解決した：

F/K を，次数 1 の有理点 $P_1, \ldots, P_n, Q$ をもった種数 g の函数体とする．$m > 0$ を整数とし，K 上の有限次元の線型空間

$$L(mQ) = \{f \in F \mid \mathrm{div}(f) + mQ \geq 0\} \cup \{0\}, \quad \ell(mQ) = \dim L(mQ)$$

を定義する．そこで，$D = P_1 + \cdots + P_n$ と mQ を付随させた

$$C(D, mQ) = C(F, D, mQ) = \{(f(P_1), \ldots, f(P_n)) \in K^n \mid f \in L(mQ)\}$$

を 1 **点代数幾何符号** とよぶ[20]．もし $m < n$ なら，符号 $C(D, mQ)$ に対し

$$\delta + R \geq 1 + 1/n - g/n$$

が成り立つ．よって，もし n/g が大きいなら，良い符号を得る．

近藤庄一氏らは，次の定理を示した．

定理 4.1 ([HKK]). r を正の奇数とし，$\mathcal{F} = (F_0, F_1, F_2, \cdots)$ を例 *2.2* の $\mathbb{F}_{q^{2r}}$-函数体の塔とする．このとき，各 F_i について

20) いま P_i の離散賦値環を $\mathcal{O}_i$ とかく．任意の $f \in L(mQ)$ に対して $f \in \mathcal{O}_i$ である．したがって，P_i は次数 1 なので $f(P_i) := f + P_i \in \mathcal{O}_i/P_i \simeq K$ を得る．

(i) x_i の極 Q_i は唯１つ；

(ii) 次数 1 の有理点 $P_1, \ldots, P_{q^{2r+i}}, Q_i$ は $q^{2r+i}+1$ 個；

が成り立つ．また，２つの因子 $D_i = P_1 + \cdots + P_{q^{2r+i}}$ と m_iQ_i を付随させた符号 $C(F_i, D_i, m_iQ_i)$ は，適当な $m_i = \alpha q^i + \beta q^{i-1}(q^r+1) < q^{2r+i}$ に対し

$$\delta_i + R_i \geq 1 - \frac{1}{q^{2r}}\alpha - \frac{q^r+1}{q^{2r+1}}\beta$$

を充たして，$i \to \infty$ のとき，

$$\delta_\infty + R_\infty = 1 - \frac{1}{q^{2r}}\alpha - \frac{q^r+1}{q^{2r+1}}\beta$$

を得る．

注意． H. Chen [C1, C2] は，例 2.1 (iii) の漸近的に最良な塔から，漸近的に良い代数幾何符号の列を得た．

予想． 例 2.1 の最良塔から漸近的に良い代数幾何符号の列が作れるか？

参考文献

［B］ P. Beelen, Graphs and recursively defined towers of function fields, *J. Number Theory* **108** (2004), 217–240.

［C1］ H. Chen, Codes on Garcia-Stichtenoth curves with true distance greater than Feng-Rao distance, *IEEE Trans. Inform. Theory* **45** (1999), 706–709.

［C2］ —, On the number of correctable errors of the Feng-Rao decoding algorithm for AG codes, *IEEE Trans. Inform. Theory* **45** (1999), 1709–1712.

［E］ N. Elkies, Explicit modular towers, Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing, Urbana, IL, 1997.

［FPS］ G. Frey, M. Perret, and H. Stichtenoth, On the different of abelian extensions of global fields, in: *Coding theory and algebraic geometry*, Proceedings, Luminy 1991, H. Stichtenoth and M. A. Tsfasman, Eds., Springer Lect. Notes Math. 1518 (1992), 26–32.

［G］ A. Garcia, On Goppa codes and Artin-Schreier extensions, *Comm. Algebra* **20** (1992), 3683–3689.

［GS1］ A. Garcia, and H. Stichtenoth, Asymptotically good towers of function fields over finite fields, *C. R. Acad. Sci. Paris Sér. I Math.* **322** (1996), 1067–1070.

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

［GS3］ —, Skew pyramids of function fields are asymptotically bad, in: *Coding Theory, Cryptography and Related Areas*, Proceedings of a Conference in Guanajuato 1998, J. Buchmann et al., Eds., Springer-Verlag, Berlin (2000), 111–113.

［H1］ T. Hasegawa, On the number of places of function fields and congruence zeta functions, *Nihonkai Math. J.* **16** (2005), 77–84.

［H2］ —, An upper bound for the Garcia-Stichtenoth numbers of towers, *Tokyo J. Math.* **28** (2005), 471–481.

［H3］ —, The generalized Garcia-Stichtenoth numbers and classfield towers, *Gakujutsu Kenkyu, School of Education, Waseda University* **54** (2006), 19–22.

［H4］ —, A note on optimal towers over finite fields, to appear in *Tokyo J. Math.*.

［H5］ —, A exact limit of towers of function fields not attaining the Drinfeld-Vlăduţ bound, (2006), preprint.

［HKK］ T. Hasegawa, S. Kondo, and H. Kurusu, A sequence of one-point codes from a tower of function fields, to appear in *Des. Codes Cryptogr.*.

［KKO］ S. Kondo, T. Katagiri, and T. Ogihara, Automorphism groups of one-point codes from the curves $y^q + y = x^{q^r+1}$, *IEEE Trans. Inform. Theory* **47** (2001), 2573–2579.

［P］ J. P. Pedersen, A function field related to the Ree group, in: *Coding theory and algebraic geometry*, Proceedings, Luminy 1991, H. Stichtenoth and M. A. Tsfasman, Eds., Springer Lect. Notes Math. 1518 (1992), 122–131.

［S］ H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, Berlin-Heidelberg-New York 1993.

［T］ M. A. Tsfasman, Some remarks on the asymptotic number of points, in: *Coding theory and algebraic geometry*, Proceedings, Luminy 1991, H. Stichtenoth and M. A. Tsfasman, Eds., Springer Lect. Notes Math. 1518 (1992), 178–192.

［TV］ M. A. Tsfasman, and S. G. Vlăduţ, Asymptotic properties of zeta-functions, *J. Math. Sci.* (New York) **84** (1997), 1445–1467.