

Hermitian 曲線上の 2 点符号 (予報)

Two-point codes on a Hermitian curve (announcement)

神奈川大学工学部 本間正明 (Masaaki HOMMA)*

Department of Mathematics, Faculty of engineering, Kanagawa University

homma@cc.kanagawa-u.ac.jp

小論は Seon Jeong Kim (Gyeongsang National University) と著者による「Hermitian 曲線上の 2 点符号の最小距離」についての共同研究で得られた結果の予報であり、詳細はいくつかの論文に分けて発表する予定である。

1 Goppa 符号

有限体 \mathbb{F} 上定義された代数曲線 X の上で、 \mathbb{F} 有理因子 F と、 F の support に含まれない相異なる \mathbb{F} 有理点 P_1, \dots, P_n を考える. 便宜上 $D = P_1 + \dots + P_n$ と因子の記号を用いる. $\mathbb{F}(X)$ を X の \mathbb{F} 上の代数関数体, $L(F) = \{f \in \mathbb{F}(X) \mid \text{div } f + F \text{ が非負因子}\} \cup \{0\}$ として、線形写像

$$L(F) \ni f \mapsto (f(P_1), \dots, f(P_n)) \in \mathbb{F}^n.$$

の像を $C_L(D, F)$ であらわす. これが Goppa 符号の L 構成法である. ついでであるから、ここで Ω 構成法についても定義を述べておく. $\Omega_{\mathbb{F}(X)/\mathbb{F}}$ を $\mathbb{F}(X)$ の \mathbb{F} 上の微分加群とし、 $\Omega(F - D) = \{\omega \in \Omega_{\mathbb{F}(X)/\mathbb{F}} \mid \text{div } \omega - (F - D) \text{ が非負因子}\} \cup \{0\}$ とする. このとき、

$$\Omega(F - D) \ni \omega \mapsto (\text{res}_{P_1}(\omega), \dots, \text{res}_{P_n}(\omega)) \in \mathbb{F}^n.$$

の像を $C_\Omega(D, F)$ であらわし、この構成法を Ω 構成法とよぶ. ただし、 $\text{res}_{P_i}(\omega)$ は微分 ω の P_i における留数である.

通常は F を正因子にとることが多く、われわれも以下ではそのように仮定しよう.

周知の通り、 $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}^n$ について、

$$d(\mathbf{x}, \mathbf{y}) \stackrel{\text{def}}{=} \#\{i \mid x_i \neq y_i\}$$

によって、 \mathbb{F}^n に距離 (Hamming 距離) が定義される.

*この研究は日本学術振興会科学研究費補助金 (基盤 C) (15500017) の援助を受けた.

線形符号 $C \subset \mathbb{F}^n$ について、その2つの異なる元間の距離の最小値 $d(C)$ は C の最小距離とよばれ、その次元 $k(C) \stackrel{\text{def}}{=} \dim_{\mathbb{F}} C$ と共に考えている符号の基本的量である。 $\mathbf{x} \in \mathbb{F}^n$ に対して、その重み $w(\mathbf{x})$ を $w(\mathbf{x}) \stackrel{\text{def}}{=} d(\mathbf{x}, 0)$ によって定めれば、 C は線形空間であるから $d(C)$ は最小重み $\min\{w(\mathbf{x}) \mid \mathbf{x} \in C \setminus \{0\}\}$ に等しい。

$f \in L(F)$ について、 $\#\{P_i \mid 1 \leq i \leq n, f(P_i) = 0\}$ は当然 f の極因子の次数を超える事はないから、

$$w((f(P_1), \dots, f(P_n))) \geq n - \deg F \quad (1)$$

となる。小論では $n - \deg F$ を (負かもしれないが) $C_L(D, F)$ の設計距離とよぶことにする。 $n > \deg F$ のとき、 $d(C_L(D, F))$ が設計距離に一致することを示すには、丁度 F を極に持つ関数で D にだけ零点を持ち、それらが1位の零であるようなものを構成すればよい。

Goppa 符号の具体例を構成し、これら基本量を求める、あるいは評価しようとするとき、多くの場合 F として、 X のある点 Q の何倍か、すなわち $F = mQ$ の形が好んで用いられる。この場合、Weierstrass 点の理論がしばしば有効に働く。このような符号 $C_L(D, mQ)$, $C_{\Omega}(D, mQ)$ は、安易な命名ではあるが、「1点符号 (one-point code)」とよばれる。また $D = \sum_{P \in X(\mathbb{F}) \setminus \{Q\}} P$ とすることが多い。ここで、 $X(\mathbb{F})$ は X の \mathbb{F} 有理点全体を意味する。

「1点符号」の一般化として、 $F = m_1Q_1 + \dots + m_rQ_r$, $D = \sum_{P \in X(\mathbb{F}) \setminus \{Q_1, \dots, Q_r\}} P$ とし、考えた符号 $C_L(D, F)$, $C_{\Omega}(D, F)$ を「 r 点符号」とよぶことにする。

2 Hermitian 曲線

素数 p とその冪 $q = p^e$ を固定する。アフィン方程式

$$y^q + y = x^{q+1} \quad (2)$$

で定義された平面射影曲線を \mathbb{F}_{q^2} 上で考えたものを Hermitian 曲線とよぶ。以後、この曲線を (\mathbb{F}_p の代数閉包で考えたものを) X であらわす。 X は無限遠直線上にはただ1点を持ち、これは \mathbb{F}_{q^2} 有理点である。この点を P_{∞} であらわす。 \mathbb{F}_{q^2} 有理点全体 $X(\mathbb{F}_{q^2})$ は $q^3 + 1$ 個の点からなる。 P_{∞} 以外の X 上の点は、そのアフィン座標を用いて $P_{\alpha, \beta}$ のように書く。記号の簡易化の為、 $P_0 := P_{0,0}$ と表す。

この曲線の自己同型は全て \mathbb{F}_{q^2} 上定義され、 $X(\mathbb{F}_{q^2})$ に2重推移的に働く。従って、この曲線上の1点符号を考えるときは、 $Q = P_{\infty}$ 、2点符号を考えるときは、 $Q_1 = P_{\infty}$, $Q_2 = P_0$ として一般性を失わない。以下、 P_{∞} , P_0 以外の \mathbb{F}_{q^2} 有理点全てを並べてできる因子を D , $\bar{D} = D + P_0$ と表し、

$$C_m = C_L(\bar{D}, mP_{\infty}),$$

$$C(m, n) = C_L(D, mP_\infty + nP_0)$$

と書く. $\deg \bar{D} = q^3$, $\deg D = q^3 - 1$ であるから, C_m の符号長は q^3 , $C(m, n)$ の符号長は $q^3 - 1$ である.

Hermitian 曲線上の 1 点符号 C_m は, Goppa 符号の初期の段階から, 多くの著者によって恰好な例として取り上げられていたが, 組織的に全ての m について考察したのは, Tiersma [7] をもって嚆矢とする. 実際, 彼はこの論文で

C_m の双対符号が $C_{q^3+q^2-q-2-m}$ となる¹

ことを確立し, $q = 2$ の場合に限ってではあるが, C_m について重み分布まで含めて記述している². その直後, Stichtenoth [5] は任意の q について, 全ての C_m について次元 $k(C_m)$ を求め, さらに, $d(C_m)$ が設計距離となるような m を殆ど見出した. 全ての m について, $d(C_m)$ の正確な値を求める事は, Yang と Kumar [8] [9] によってなされた. Stichtenoth, Yang と Kumar の結果は次のような表にまとめると見やすい.

	0	•	...	•	•
	q	$q+1$...	•	•
	•	•	•	•	•
	•	•	•	•	•
$[q^3 - m]$	$(q-2)q$	$(q-2)q+1$...	$(q-2)q+(q-2)$	$(q-1)q+(q-1)$
	$(q-1)q$	$(q-1)q+1$...	•	•
	•	•	•	•	•
	$(q^2 - q - 1)q$	$(q^2 - q - 1)q + 1$...	•	$(q^2 - q - 1)q + (q - 1)$
$[q^2] \Rightarrow$	$(q^2 - q)q$	$(q^2 - q)q + 1$...	•	$(q^2 - q)q + (q - 1)$
$[(q-1)q] \Rightarrow$	$(q^2 - q + 1)q$	$(q^2 - q + 1)q + 1$...	•	$(q^2 - q + 1)q + (q - 1)$
	•	•	•	•	•
	•	•	•	•	•
$[3q] \Rightarrow$	$(q^2 - 3)q$	$(q^2 - 3)q + 1$...	$(q^2 - 3)q + (q - 2)$	$(q^2 - 3)q + (q - 1)$
$[2q] \Rightarrow$	$(q^2 - 2)q$	$(q^2 - 2)q + 1$...	$(q^2 - 2)q + (q - 2)$	$(q^2 - 2)q + (q - 1)$
$[q] \Rightarrow$	$(q^2 - 1)q$	$(q^2 - 1)q + 1$...	•	$(q^2 - 1)q + (q - 1)$
	•	$q^3 + 1$	•	•	$q^3 + (q - 1)$ $\Leftarrow [q-1]$
	•	•	•	•	•
	•	•	•	•	•
	•	•	•	$(q^2 + q - 3)q + (q - 2)$	$(q^2 + q - 3)q + (q - 1)$ $\Leftarrow [2]$
	•	•	•	$(q^2 + q - 2)q + (q - 1)$	$(q^2 + q - 2)q + (q - 1)$ $\Leftarrow [1]$

表 1: C_m の次元と最小距離

この表の見方について説明しよう. $m = aq + b$ ($0 \leq b < q$) と書くとき, $\dim C_m > \dim C_{m-1}$ となる m はこの表に現れた数字, すなわち, $b \leq a \leq b + (q^2 - 1)$ を満たす m だけである. このとき, $\dim C_m = \dim C_{m-1} + 1$ であるので, $\dim C_m$ は m 以下の整数でこの表にあらわれるものの個数と一致する. 例えば $m = q + 1$ とすれば, $q + 1$ 以下の整数でこの表にあらわれるものは, $1, q, q + 1$ であるから $\dim C_{q+1} = 3$ と

¹この事実により, 1 点符号については Ω 構成法による符号を考えることは C_m を考えることと同じ事となる.

²実際には $m \leq 4$ に限って記述しているが, 上記 1 により, MacWilliams の恒等式 [3, Ch. 5, Thm 13] を用いれば原理的には全ての C_m について重み分布が算出可能であり, 煩雑ではあるが(手でも)実行可能である.

なる. また square brackets $[\]$ 内の数字が対応する C_m の最小距離をあらわす. すなわち, $b \leq a \leq b + (q^2 - q - 1)$ なる m についてはちょうど設計距離 $d(C_m) = q^3 - m$ である³. また \Rightarrow はその行にある m で | 線より左にあるものについては $d(C_m)$ がちょうど $[\]$ 内の値, 例えば $d(C_{(q^2-3)q}) = d(C_{(q^2-3)q+1}) = \cdots = d(C_{(q^2-3)q+(q-3)}) = 3q$ である. \Leftarrow はその行にある m で | 線より右にあるものについては $d(C_m)$ がちょうど $[\]$ 内の値となる事を意味する.

以上と同じような問題意識で $C(m, n)$ を調べようというのが, われわれの方向である.

3 問題の簡易化と次元

Hermitian 曲線 X の定義式 (2) によって, $y \in \mathbb{F}_{q^2}(X)$ とみると,

$$\operatorname{div} y = (q+1)P_0 - (q+1)P_\infty$$

であるから, \mathbb{F}_{q^2} -同型

$$\begin{array}{ccc} L(mP_\infty + nP_0) & \longrightarrow & L((m+q+1)P_\infty + (n-q-1)P_0) \\ f & \longmapsto & fy \end{array}$$

を得る. すべての $P_{\alpha,\beta} \in \operatorname{supp} D$ について $y(P_{\alpha,\beta}) \neq 0$ であるから, この同型は Hamming 距離を保存する同型

$$C(m, n) \rightarrow C(m+q+1, n-q-1)$$

を引き起こす. したがって, $\dim C(m, n)$ や $d(C(m, n))$ を問題にする限り, $0 \leq n \leq q$ と仮定して良い.

$C(m, n)$ の次元については, Matthews [4] の「Hermitian 曲線上の点の対 (P_∞, P_0) における Weierstrass gap set」の記述を参照すれば, $0 \leq n \leq q$ なる各 n について表 1 と同様な意味の表現を得る. すなわち \mathbb{F}_{q^2} 部分空間の列

$$(0) \subseteq \cdots \subseteq C(-1, n) \subseteq C(0, n) \subseteq C(1, n) \subseteq \cdots \subseteq C(m, n) \subseteq \cdots \subseteq \mathbb{F}_{q^2}^{q^3-1},$$

において, 各段階で $\dim C(m, n) = \dim C(m-1, n)$ または $\dim C(m, n) = \dim C(m-1, n) + 1$ であるので, $\dim C(m, n) > \dim C(m-1, n)$ なる m を明示すれば $C(m, n)$ の次元については理解できたことになる.

注意 $0 \leq n < q$ の場合は $C(-1, n) = (0)$, $\dim C(0, n) = 1$ であるが, $n = q$ の場合は $x/y \in L(-P_\infty + qP_0)$ であるので, $\dim C(-1, q) = 1$, $\dim C(0, q) = 2$ である.

³設計距離に一致するのは, この範囲と $\{m = aq|q^2 - q \leq a \leq q^2 - 1\}$ を合わせた部分である.

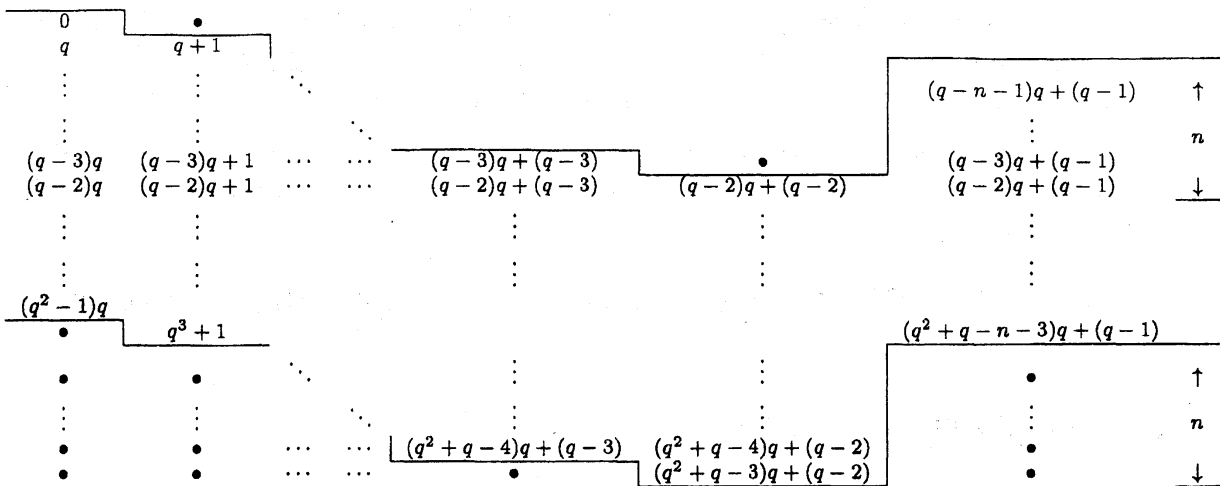


表 2: $\dim C(m, n) > \dim C(m - 1, n)$ となる m (n は固定)

4 $C(m, n)$ の最小距離

ここでは、結果を $n = 0, n = q, 0 < n < q$ の三つの場合に分けて記述する。

4.1 $n = 0$ の場合

この場合は C_m についての結果から容易に導ける。

補題 1 $d(C_m) \geq 2$ なる m について、 $d(C(m, 0)) = d(C_m) - 1$ である。

証明. $d(C(m, 0)) \geq d(C_m) - 1$ は明らか. $f \in L(mP_\infty)$ を C_m の最小重みを到達する符号語に対応する関数とする $d(C_m) \geq 2$ だから、少なくとも 2 点 $P, Q \in X(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ が存在して $f(P) \neq 0, f(Q) \neq 0$. X の \mathbb{F}_{q^2} 上の自己同型群は $X(\mathbb{F}_{q^2})$ に 2 重推移的に働くから、ある自己同型 σ が存在して、 $\sigma(P_\infty) = P_\infty, \sigma(P_0) = P$. このとき、 $f \circ \sigma$ は零でない $C(m, 0)$ の符号語に対応し、重みは $d(C_m) - 1$. \square

よって、この場合は表 1 を見比べて次の表をえる。(表の見方は、表 1 に準ずる.)

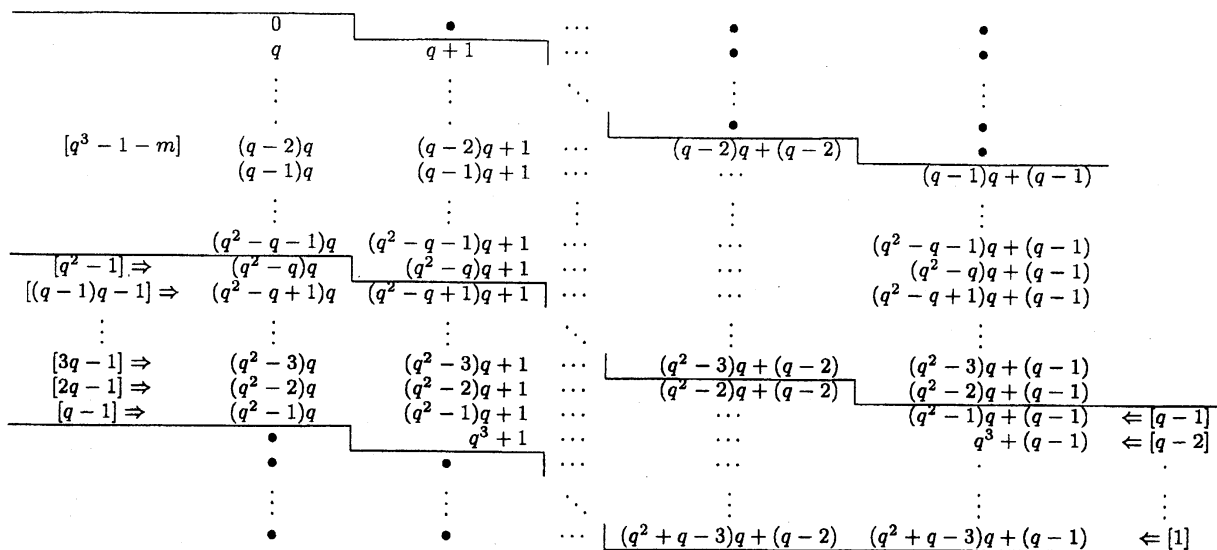


表 3: $C(m, 0)$ の最小距離

4.2 $n = q$ の場合

この場合、 $d(C(m, q))$ が、ちょうど設計距離となるような m は次の定理により決定できる。

定理 2 $0 < m + n < q^3 - 1$ を満たす整数 m, n について、 $d(C(m, n))$ が設計距離に一致することと $d(C(q^3 - q - 1 - m, q - n))$ が設計距離に一致することは同値である。

証明. X 上の関数

$$w = \left(\prod_{\alpha \in \mathbb{F}_{q^2}} (x - \alpha) \right) / y$$

を考えると、

$$\text{div} w = \sum_{P \in X(\mathbb{F}_{q^2}) \setminus \{P_\infty, P_0\}} P - (q^3 - q - 1)P_\infty - qP_0$$

である。したがって、 $d(C(m, n))$ が設計距離に一致するとき、その値を重みに持つ $L(mP_\infty + P_0)$ の関数を f とすれば、 $w/f \in L((q^3 - q - 1 - m)P_\infty + (q - n)P_0)$ であり、対応する $C(q^3 - q - 1 - m, q - n)$ の符号語の重みはこの設計距離の値に一致する。□

$n = q$ の場合の最小距離を表にまとめると次のとおりである。最小距離が設計距離を真に上回る場合の考察はここでは省略する。(詳細は [2] を参照。)

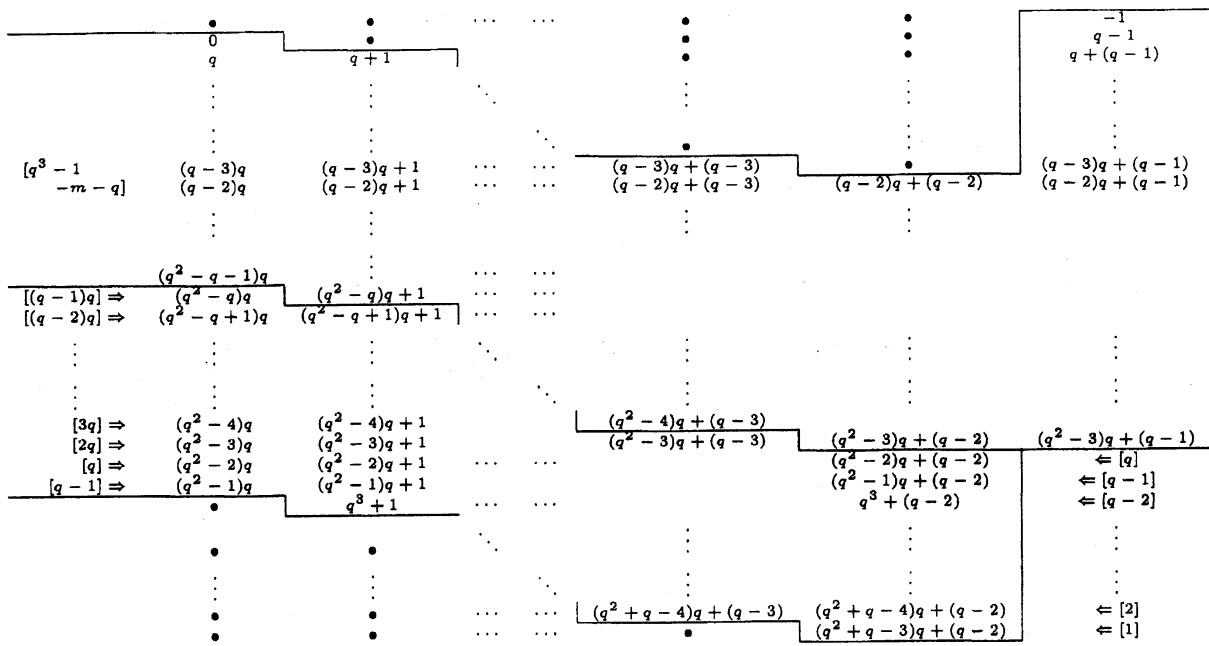


表 4: $\dim C(m, q)$ の最小距離

4.3 $0 < n < q$ の場合

表 2 で示した $\{m \mid \dim C(m, n) > \dim C(m-1, n)\}$ の領域を 6 つの部分に分けて記述する (表 5).

表 5 中の a_1, \dots, a_9 は以下のとおり: $a_1 = q - n - 1$, $a_2 = q - 2$, $a_3 = q^2 - q$, $a_4 = q^2 - (n + 2)$, $a_5 = a_4 + 1 = q^2 - (n + 1)$, $a_6 = q^2 - 2$, $a_7 = a_6 + 1 = q^2 - 1$, $a_8 = q^2 + q - n - 3$, $a_9 = q^2 + q - 3$.

表の各領域を正確に記述すれば, $m = aq + b$ ($0 \leq b \leq q - 1$) と表すとき,

- (I) $b \leq a \leq a_1$
- (II) $\cdot b = 0$ のとき, $a_1 + 1 \leq a \leq a_5$
 $\cdot 0 < b < q - 1$ のとき, $\max\{b, a_1 + 1\} \leq a \leq \min\{b + a_3 - 1, a_4\}$
 $\cdot b = q - 1$ のとき, $a_1 \leq a \leq a_4$
- (III) $0 < b$ かつ $b + a_3 \leq a \leq a_5$
- (IV) $a_5 \leq a \leq b + a_3 - 1$
- (V) $\max\{b + a_3, a_5 + 1\} \leq a \leq a_6$
- (VI) $\cdot b < q - 1$ のとき, $a_7 \leq a \leq b + a_7$
 $\cdot b = q - 1$ のとき, $a_7 \leq a \leq a_8$

である.

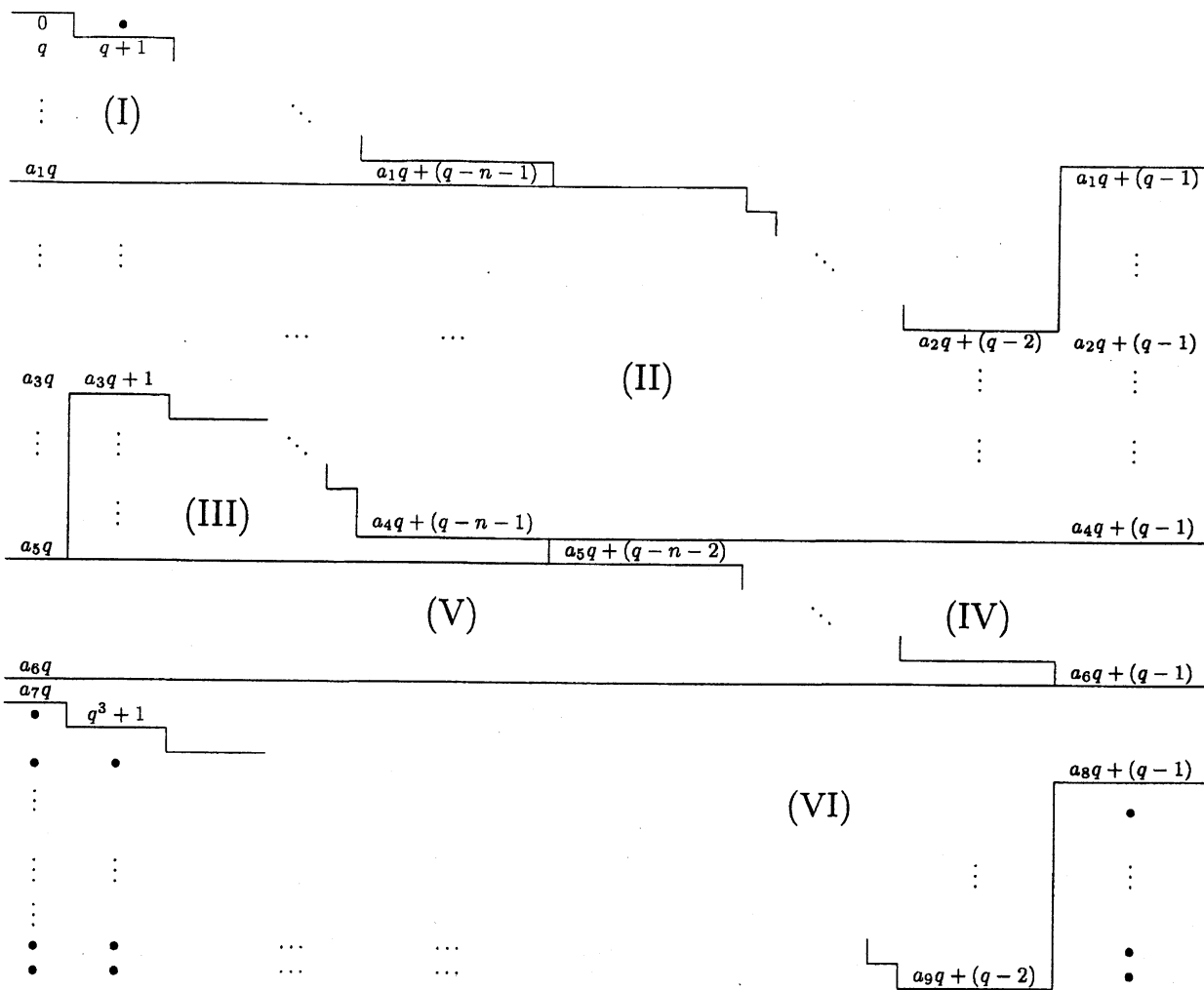


表 5: $d(C(m, n))$ を記述するための領域区分 (n は固定)

各領域について最小距離は以下のように記述できる.

(I) $d(C(m, n))$ は $d(C(m, 0))$ に等しい. すなわち,

$$d(C(m, n)) = q^3 - 1 - m$$

である.

(II) この場合は設計距離となる. すなわち,

$$d(C(m, n)) = q^3 - 1 - (m + n)$$

である.

(III), (IV), (V) について述べる前に (VI) を片付ける.

(VI) $a = q^2 - 2 + \mu$ とかくと, μ の値のとりうる範囲は $1 \leq \mu \leq q - 1$ であるが,

$$d(C(q^2 - 2 + \mu)q + b, n) = q - \mu$$

である.

(III), (IV), (V) の場合は, $a = q^2 - \rho$ と表しておくのが便利である. ρ の値のとりうる範囲は $1 < \rho < q$ である.

(III) $d(C((q^2 - \rho)q + b, n))$ は $d(C((q^2 - \rho)q, n))$ に等しく, これは (II) よりわかるので,

$$d(C((q^2 - \rho)q + b, n)) = \rho q - (n + 1)$$

となる.

(IV) この場合は

$$d(C((q^2 - \rho)q + b, n)) = (\rho - 1)q - (b + \rho - q - 1)$$

となる.

(V) この部分だけが未決定部分として残されており

$$\rho q - (n + 1) \leq d(C((q^2 - \rho)q + b, n)) \leq \rho q - \rho$$

である.

予想 $2 \leq \rho \leq \min\{n, q - b\}$ のとき, $d(C((q^2 - \rho)q + b, n)) = \rho q - \rho$

この予想は部分的に正しいことは確認済みである. [1, 4.2] で構成した例, それは Ω -構成法で得られているのであるが, を L -構成法に翻訳したものは ((V) の領域にある $C(m, n)$ に対応し) その最小距離が予想の等式を満たす.

参考文献

- [1] M. Homma and S. J. Kim, *Goppa codes with Weierstrass pairs*, J. Pure Appl. Algebra, **162** (2001), 273–290
- [2] M. Homma and S. J. Kim, *Determination of the minimum distance of two-point codes on a Hermitian curve: a first step*, preprint 2003
- [3] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*, North-Holland, Amsterdam 1977
- [4] G. L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Designs, Codes and Cryptography, Vol. 22 (2001) pp. 107–121.
- [5] H. Stichtenoth, *A note on Hermitian codes*, IEEE Trans. Inform. Theory **34** (1988), 1345–1348.

- [6] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer - Verlag, Berlin - Heidelberg 1992.
- [7] H. J. Tiersma, *Remarks on codes from Hermitian curves*, IEEE Trans. Inform. Theory **33** (1987), 605-609.
- [8] K. Yang, *On the weight hierarchy of Hermitian and other geometric Goppa codes*, Ph. D. Thesis, University of Southern California, 1992.
- [9] K. Yang, P. V. Kumar, *On the true minimum distance of Hermitian codes*, in: H. Stichtenoth, M. A. Tsfasman (eds.), *Coding Theory and Algebraic Geometry (Luminy, 1991)*, Lecture Note in Mathematics 1518, Springer - Verlag, Berlin - Heidelberg, 1992, 99-107.