数理解析研究所講究録 1420 巻 2005 年 106-116

Hermitian曲線の幾何と符号

Geometry of a Hermitian curve and two-point codes on the curve

神奈川大学工学部　本間正明 (Masaaki HOMMA)*
Department of Mathematics, Faculty of engineering, Kanagawa University
homma@kanagawa-u.ac.jp

2002年の夏頃から Seon Jeong Kim 氏 (慶尚国立大, 韓国) と共に Hermitian 曲線上の 2 点符号の最小距離をすべて求めるという作業を始めた. 当初は数ヶ月, 長くても翌夏までにはなんとかなるだろうという見通しで始めたが, 思いのほか最終決着までは時間がかかり一応全てについて証明が確信できるに至ったのは昨年 (2004年) 夏のことである. その間 [3], [4] のような中間報告を書いてきたが, 本稿の一部はそれらと重複する. また, [4] で述べた予想 ([4, 160頁]) は, 完全には正しくなかった (本文, 注意 6.2 参照).

1　状況設定と問題

X を有限体 $\mathbb{F}_{q^2}$ 上定義された Hermitian 曲線

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

とする. 詳しく言えば, (1) を $\mathbb{F}_{q^2}$ 上定義された射影平面内の曲線の非斉次定義方程式と考える. P_∞ をこの定義式による X 上唯一の無限遠点, P_0 を原点 $(0,0)$ とする. また原点以外の $X \setminus \{P_\infty\}$ 上にある $\mathbb{F}_{q^2}$ 有理点 (α, β) は $P_{\alpha,\beta}$ と表し, X の $\mathbb{F}_{q^2}$ 有理点全体は $X(\mathbb{F}_{q^2})$ と表す. 非負整数 m, n について,

$$L(mP_\infty + nP_0) \stackrel{\text{def}}{=} \{f \in \mathbb{F}_{q^2}(X) \setminus \{0\} \mid \operatorname{div} f + mP_\infty + nP_0 \succ 0\} \cup \{0\}$$

を考え, 線形写像

$$\begin{array}{ccc} L(mP_\infty + nP_0) & \to & (\mathbb{F}_{q^2})^{q^3-1} \\ f & \mapsto & (f(P))_{P \in X(\mathbb{F}_{q^2}) \setminus \{P_\infty, P_0\}} \end{array}$$

の像空間として得られる符号ををを $C(m,n)$ で表す. また, その最小距離を $d(C(m,n))$ と書く.

X の曲線としての自己同型はすべて $\mathbb{F}_{q^2}$ 上定義され, したがってその自己同型群は $X(\mathbb{F}_{q^2})$ へ作用する. この作用は2重推移的であるので, X 上の2点符号を考える際に, これら2点 P_∞, P_0 を選ぶことによって特に一般性を失っているわけではない.

以上の状況設定の下で, 符号の最も基本的なパラメータである $\dim C(m,n)$ と $d(C(m,n))$ とを求めることが, われわれの問題である.

さて, 符号の次元と最小距離を問題にする限り, それと同値な符号に取り替えてもそれらの値は変化しない. 関数 y の定める因子は (1) により $(q+1)P_0 - (q+1)P_\infty$ であるので, 同型写像

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

*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.

から定まる線形写像 $C(m,n) \to C(m+q+1, n-q-1)$ は Hamming 距離を保ち，これら 2 つの符号は同値である．したがって，$0 \le n \le q$ の範囲で考えれば十分である．以下では上に述べた状況設定にこの n の範囲も付加する．

なお，Hermitian 曲線上の 1 点符号についての同様な問題については，K. Yang と P. V. Kumar ([9], [10]) によって完全に決着がついている．

2 次元

$\dim C(m,n)$ を求めることは，すでに G. L. Matthews [8] があるので，それに依拠すれば容易である．むしろどのように表現すれば見通しがきくかに腐心する．$\dim C(m-1,n) \le \dim C(m,n)$ であるが，それらの差は 0 または 1 であるので，n $(0 \le n \le q)$ を固定したとき，$\dim C(m-1,n) < \dim C(m,n)$ となる m の表をつくれば，表にあらわれる $m' \le m$ なる m' の数をかぞえることにより $\dim C(m,n)$ を知ることができる．それは 表 1 の通りである．

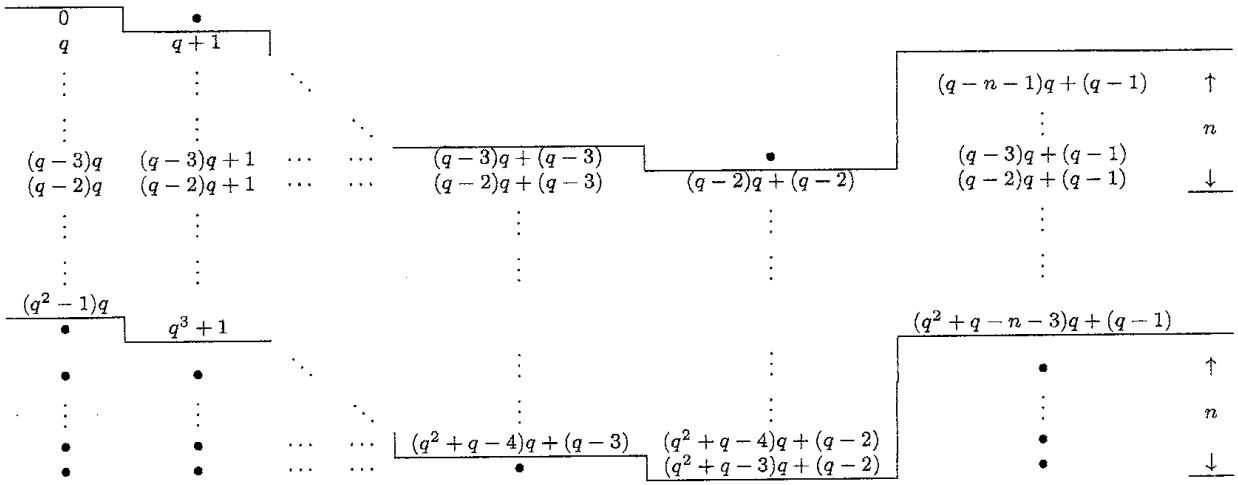

表 1: m with $\dim C(m,n) = \dim C(m-1,n) + 1$

3 $L(mP_\infty + nP_0)$ の基底

われわれの目的には必要ではないが，これらの 2 点符号の復号を考えるためには $L(mP_\infty + nP_0)$ の基底が具体的に書き下されている必要がある[1]．しかし，[5] では次元を求める際 [8] を用いたので基底を書き下すことはしなかった．それを補充するためここで一組の基底を与える．

定義 3.1 $0 \le n \le q$ について，

$$\tilde{I}_n = \{aq+b \mid \min\{a, q-1\} \ge b \text{ または } q-n-1 \le a < b = q-1\}$$

とする．

$\tilde{I}_n$ は整数全体を表 1 のように，mod q で配列したとき，表 1 の $0, q+1, \ldots, (q-2)q+(q-2)$, $(q-n-1)q+(q-1)$ を結ぶ境界線より下にある整数全体である[2]．

[1] 坂田省二郎先生の示唆による．

[2] 下の領域の • に対応する整数も含む．

定義 3.2 $aq+b \in \tilde{I}_n$ に対応して，X 上の有理関数 e_{aq+b} を

$$e_{aq+b} = \begin{cases} x^{a-b}y^b & (a \geq b) \\ x^{a+2}/y & (q-n-1 \leq a < b = q-1) \end{cases}$$

と定める．

命題 3.3 n $(0 \leq n \leq q)$ を固定したとき，$\dim L(mP_\infty+nP_0) = \dim L((m-1)P_\infty+nP_0)+1$ となる必要十分条件は $m \in \tilde{I}_n$ となること．さらに，このとき，$\{e_{aq+b} \mid aq+b \leq m\}$ は $L(mP_\infty+nP_0)$ の基底をなす．

証明．有理関数 x, y について

$$\operatorname{div} x = P_0 + \sum_{\substack{\beta \neq 0 \\ \mathrm{Tr}\,\beta = 0}} P_{0,\beta} - qP_\infty, \quad \operatorname{div} y = (q+1)P_0 - (q+1)P_\infty$$

であるから，$m = aq+b \in \tilde{I}_n$ について，$e_{aq+b} \in L(mP_\infty+nP_0) \setminus L((m-1)P_\infty+nP_0)$ である．したがって，この固定した n $(0 \leq n \leq q)$ について，

$$\{m \in \mathbb{N}_0 \mid \dim L(mP_\infty+nP_0) = \dim L((m-1)P_\infty+nP_0)\} \subseteq \mathbb{N}_0 \setminus \tilde{I}_n \tag{2}$$

である．一方 m が十分大きいとき，Riemann-Roch により $\dim L(mP_\infty+nP_0) = m+n+1-q(q-1)/2$ であり，また $\dim L(nP_0) = \begin{cases} 1 & (n<q) \\ 2 & (n=q) \end{cases}$ であるから，(2) の左辺の位数は $\begin{cases} q(q-1)/2-n & (n<q) \\ q(q-1)/2-(q-1) & (n=q) \end{cases}$ となり，これは，(2) の右辺の位数であるから，(2) の両辺は一致する．ただし，$n=q$ のとき，右辺の元の個数を数える際に $-1 \in \tilde{I}_q$ であることに注意されたい． □

4 最小距離 $(n=0)$

以下最小距離について考えるが，$n=0$ の場合は 1 点符号の結果を用いることにより容易にわかり，それは表 2 としてまとめられる．

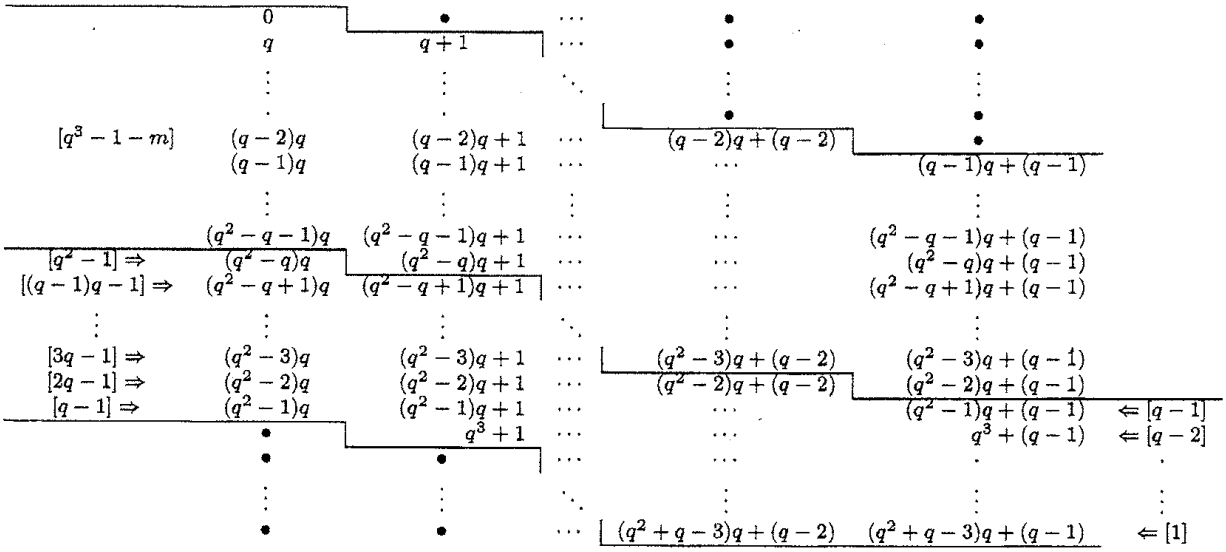

表 2: The minimum distance of $C(m,0)$

表 2 の見方について説明する．$m = aq+b$ $(0 \leq b < q)$ と書くとき，$\dim C(m,0) > \dim C(m-1,0)$ となる m はこの表に現れた数字だけであることは 2 節で述べた．このとき，square brackets

[ ] 内の数字が対応する $C(m,0)$ の最小距離をあらわす．すなわち，$b \le a \le b+(q^2-q-1)$ なる m についてはちょうど設計距離[3]$d(C(m,0)) = q^3-1-m$ である．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 $d(C(m,0))$ がちょうど [ ] 内の値，例えば $d(C((q^2-2)q,0)) = d(C(q^2-2)q+1,0)) = \cdots = d(C((q^2-2)q+(q-2)) = 2q-1$ 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 $d(C(m,0))$ がちょうど [ ] 内の値となる事を意味する．

5 最小距離 $(n=q)$

$n=q$ の場合は表 3 の如くまとめられる．表の見方は先に述べた「表 2 の見方」に準ずる．

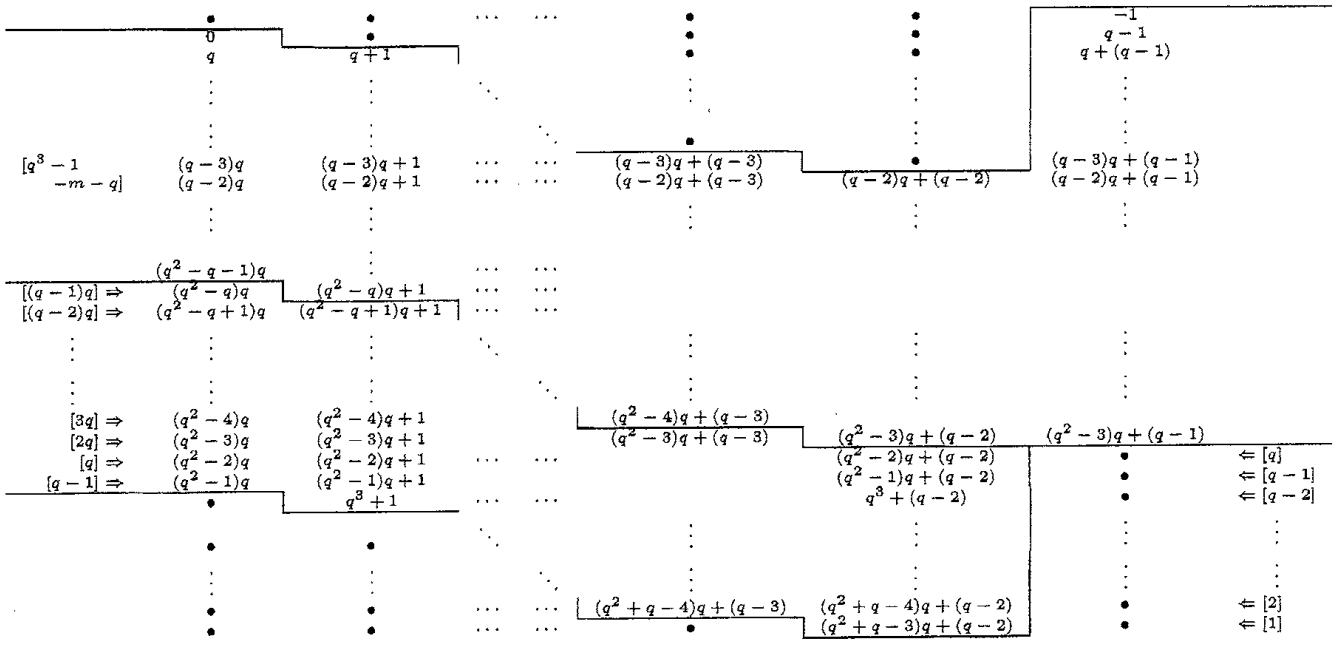

表 3: The minimum distance of $\dim C(m,q)$

$d(C(m,q))$ が設計距離となるのがいつ起きるかは次の定理により，$d(C(m,0))$ についての結果から容易に分かる．

定理 5.1 $0 < m+n < q^3-1$ 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，

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

[3]全射 $L(mP_\infty + nP_0) \to C(m,n)$ により，$C(m,n)$ の code word に対し，$L(mP_\infty+nP_0)$ の関数が対応するが，その関数は恒等的に 0 でない限りその零点の個数は高々 $m+n$ であるから，不等式 $d(C(m,n)) \ge q^3-1-(m+n)$ が成り立つ．この右辺の値を $C(m,n)$ の設計距離という．

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．□

6 $0<n<q$ についての最小距離

以下 $0<n<q$ の場合を考える．最小距離を記述するため，表 1 の領域を次ページ以下に示すように I から VI の 6 つの領域に区分する．その表示のため次の記法を用いる．

$$\begin{aligned}
a_1 &= a_1(n) = q-(n+1)\\
a_2 &= a_2(n) = q-n\\
a_3 &= q-2\\
a_4 &= q^2-q\\
a_5 &= q^2-(q-1)\\
a_6 &= a_6(n) = q^2-(n+2)\\
a_7 &= a_7(n) = q^2-(n+1)\\
a_8 &= a_8(n) = q^2-n\\
a_9 &= q^2-2\\
a_{10} &= q^2-1\\
a_{11} &= a_{11}(n) = q^2+q-(n+3)\\
a_{12} &= q^2+q-3.
\end{aligned}$$

定理 6.1 n $(0<n<q)$ を固定する．m が表 4, 5, 6 の領域 I ~ VI のうち，どの領域に属するかに従って，$d(C(m,n))$ は次のように記述される．

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

II $m=aq+b$ $(0\le b<q)$ と表すとき，$d(C(m,n)) = q^2+q-a-2.$

III $d(C(m,n)) = q^3-1-(m+n)$ (設計距離に一致).

IV ~ VI については，$m=(q^2-\rho)q+b$ $(0\le b<q)$ と表す．

IV $d(C(m,n)) = \rho q-(n+1).$

V $d(C(m,n)) = (\rho-1)q-(b+\rho-q-1)$

VI "$n<q-1$" または "$n=q-1$, $\rho+b<q$" のとき，$d(C(m,n)) = \rho q-\rho$

"$n=q-1$, $\rho+b=q$" のとき，$d(C(m,n)) = (\rho-1)q$

注意 6.2 VI の例外「"$n=q-1$, $\rho+b=q$" のとき」は表 6 にだけ現れる．これが最後まで梃摺った場合で，この場合に限り，[4] での予想が正しくなかった．

I, II の場合は $n=0$ と $n=q$ の場合を見比べることによって得られる [5].

設計距離となる場合 III はそれを到達する関数を構成する必要がある．そのためにわれわれは Hermitian 曲線と 2 次曲線の族 $\{y=\varphi x^2 | \varphi\in\mathbb{F}_{q^2}^\times\}$ および直線の 2 つの族 $\{x=\alpha \mid \alpha\in\mathbb{F}_{q^2}^\times\}$,

$\{y = \kappa x \mid \kappa \in \mathbb{F}_{q^2}^{\times}\}$ との関係を観察することによって構成した．その一端は [3] に解説した．詳細は [6] を参照．ただし，q が小さい場合と 2 冪の場合には別途扱わなければならない．残りの部分 IV ～ VI については [7] に譲る．

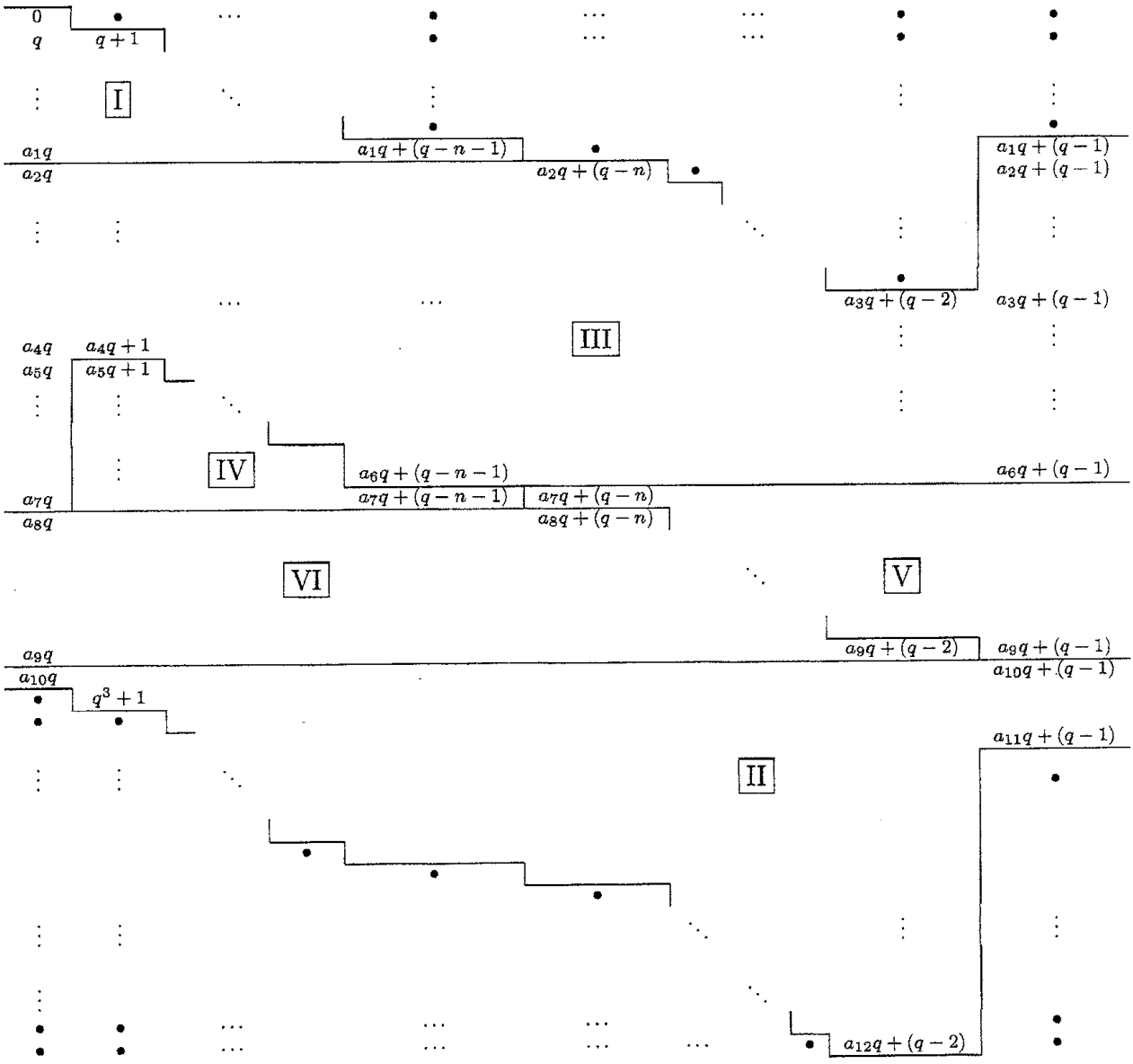

表 4: $2 \leq n \leq q-2$

$n=1$ と $n=q-1$ の場合は表 4 は以下の表 5 ($n=1$), および表 6 ($n=q-1$) のように退化する.

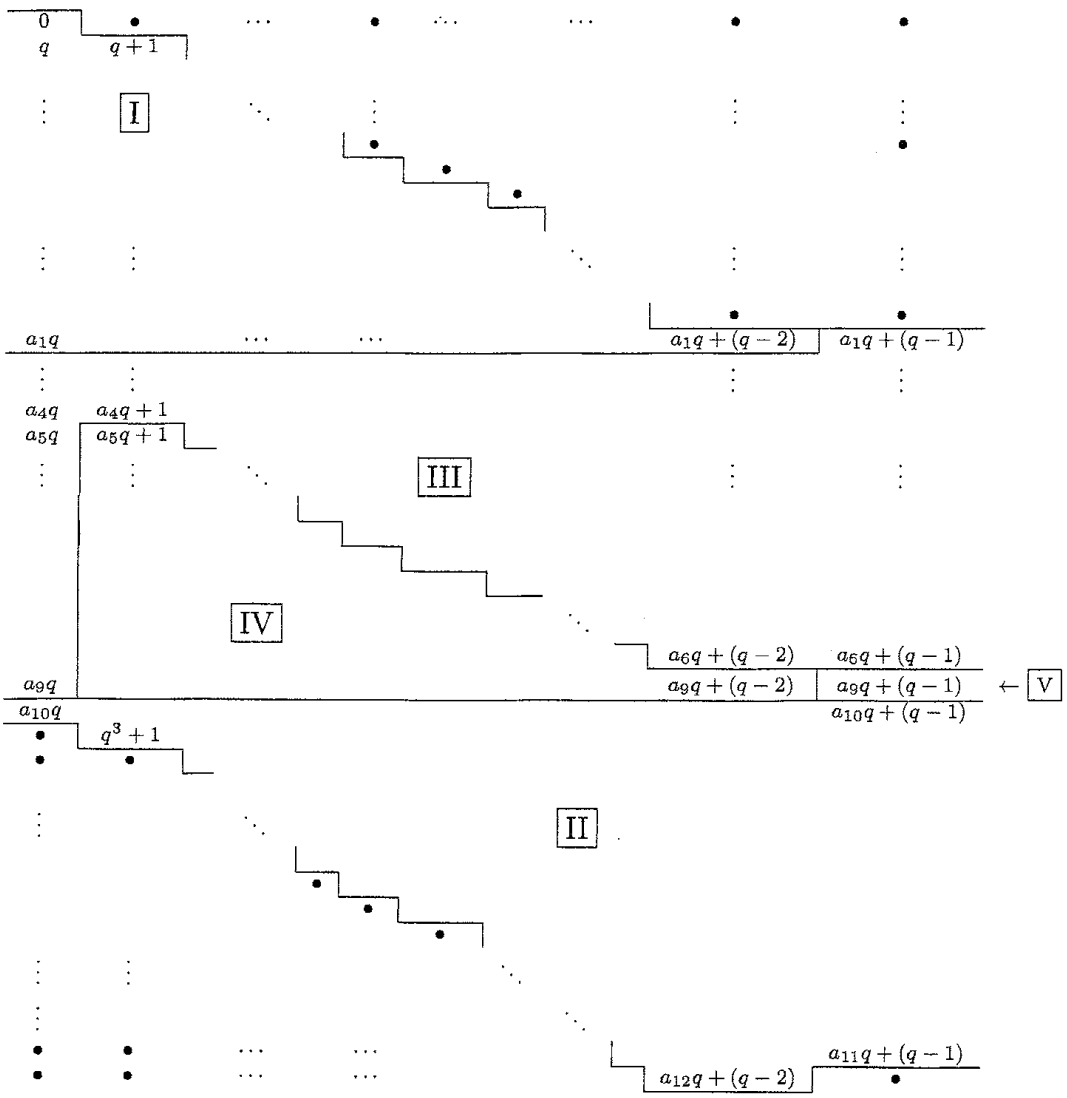

表 5: $n=1$

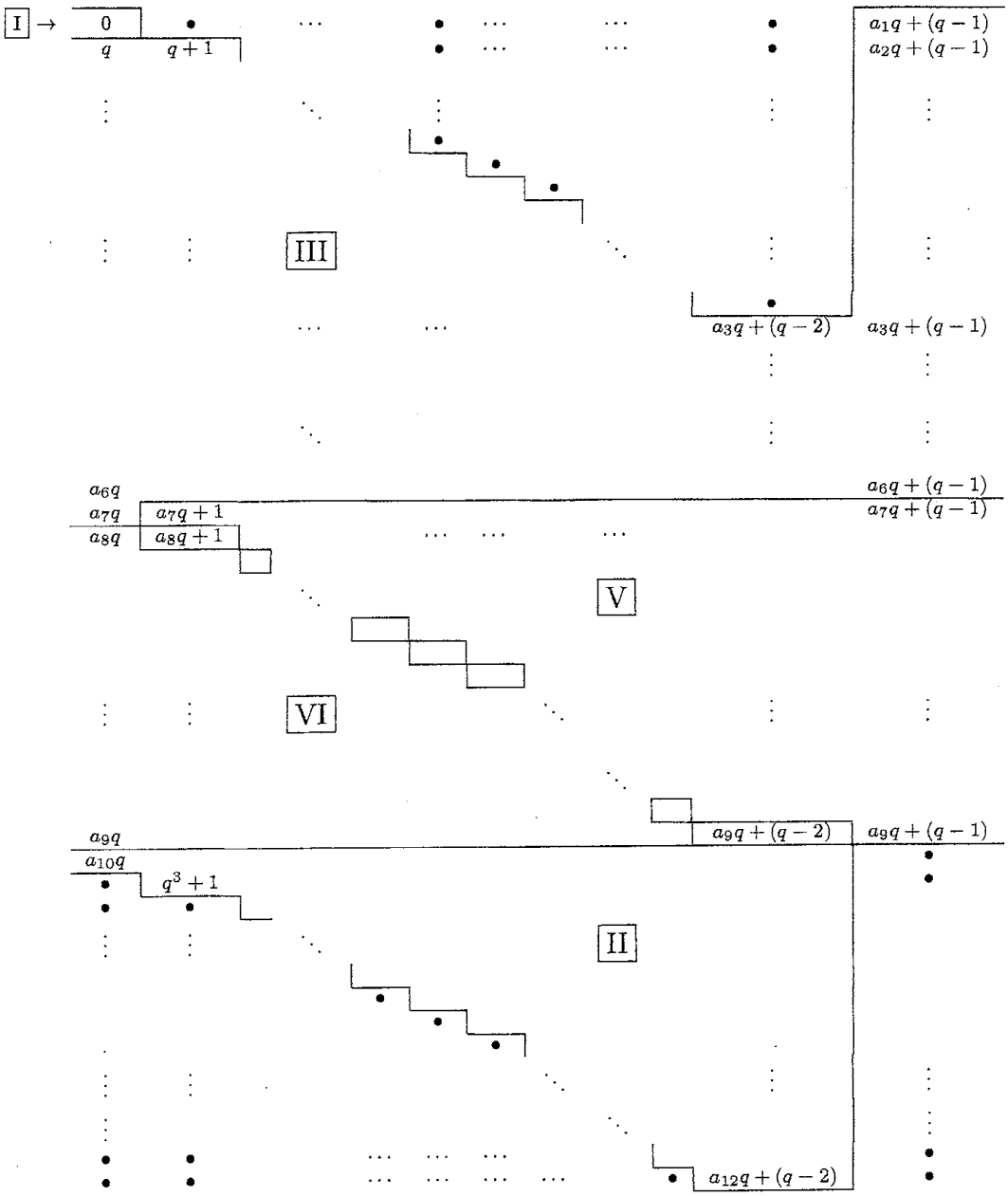

表 6: $n = q - 1$

7 Ω構成法との関係

かつて，われわれは [1] の中で Weierstrass pair の理論を用いて最小距離の比較的大きいΩ構成法による符号を生成する方法を提案し，Hermitian 曲線の上で実際に適用できることを見た．しかし Hermitian 曲線上で構成した符号の最小距離は下からの評価式を与えたのみで，その値が実際にその符号の最小距離を与えているか否かは不明であった．今回得られれた結果を用いるとその疑問に肯定的に答えることができる．ここでそれを説明したい．

注意 7.1 (構成法) $q \geq 4$ とする．Hermitian 曲線 X の P_∞, P_0 以外の $\mathbb{F}_{q^2}$ 有理点を並べた因子

$\sum_{P\in X(\mathbb{F}_{q^2})\setminus\{P_\infty,P_0\}} P$ を D と記す．i, j を自然数で $(q+1)/2 < i+j \leq q-1$ を満たすものとし，非負整数 u_1, u_2, v_1, v_2 を

$$\begin{aligned}(u_1, u_2) &= (iq-(q-i), jq-(q-j))\\ (v_1, v_2) &= (iq-j, jq-i-1)\end{aligned}$$

で定める．Hermitian 曲線上の因子

$$F = (u_1+v_1-1)P_\infty + (u_2+v_2-1)P_0$$

を選ぶと

$$\dim C_\Omega(D,F) = q^3+q^2/2-(2(i+j)-3/2)\,q+1$$

であり [1, Lemma 4.3],

$$d(C_\Omega(D,F)) \geq (2(i+j)-q)(q-1) \tag{3}$$

となる [1, Theorem 3.3 と page 283 の説明].

以下，**(3) で等号が成り立つ**ことを示す．

正整数 l について，differential

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

を考える．このとき，

$$\begin{aligned}&\operatorname{div} y^l = l(q+1)P_0 - l(q+1)P_\infty\\ &\operatorname{div} \textstyle\prod_{\alpha\in\mathbb{F}_{q^2}}(x-\alpha) = P_0 + D - q^3P_\infty\\ &\operatorname{div} dx = (q^2-q-2)P_\infty\end{aligned}$$

であるから，

$$\operatorname{div}\omega_l = (q^3+q^2-(l+1)q-(l+2))P_\infty + (lq+l-1)P_0 - D$$

となる．したがって，次の補題を得る．

補題 7.2 m, n, m', n は非負整数で

$$\begin{aligned}m+m' &= q^3+q^2-(l+1)q-(l+2)\\ n+n' &= lq+l-1\end{aligned}$$

を満たす．このとき，

$$\begin{array}{ccc} L(mP_\infty+nP_0) & \to & \Omega(m'P_\infty+n'P_0-D)\\ f & \mapsto & f\omega_l\end{array}$$

は同型写像である．ただし，$\Omega(m'P_\infty+n'P_0-D)$ は X 上の differential でその因子が $m'P_\infty+n'P_0-D$ より小さくないものおよび 0 のなすベクトル空間である．

この補題で見た同型写像はHamming距離を保つ同型

$$C(m,n) \tilde{\to} C_\Omega(D, m'P_\infty + n'P_0) \tag{4}$$

を引き起こす．実際，D にあらわれる点 $P_{\alpha,\beta}$ について，$t = x - \alpha$ とおくと t は $P_{\alpha,\beta}$ での local parameter であり，$P_{\alpha,\beta} \neq P_0$ より $y(P_{\alpha,\beta}) = \beta \neq 0$ である．よって，ω_l をこの点で t によって展開すれば，

$$\omega_l = \left(\frac{\beta^l}{\prod_{\alpha' \in \mathbb{F}_{q^2} \setminus \{\alpha\}} (\alpha - \alpha')} t^{-1} + \cdots \right) dt.$$

となり，$\mathrm{res}_{P_{\alpha,\beta}} \omega_l \neq 0$ である．

さて，(4) において，

$$\begin{aligned} m' &= u_1 + v_1 - 1 = (2i-1)q + i - j - 1 \\ n' &= u_2 + v_2 - 1 = (2j-1)q + j - i - 2 \end{aligned}$$

として，$l = 2j - 1$ とすると，

$$\begin{aligned} m &= (q^2 - (2(i+j) - q))q + q - (i+j) \\ n &= i + j \end{aligned}$$

すなわち，

$$d(C_\Omega(D,F)) = d(C((q^2 - (2(i+j) - q))q + q - (i+j), i+j))$$

である．仮定より $0 < q - (i+j) < q$ であり，$0 < i + j < q$ であるから，右辺の表示は $n = i + j$, $a = q^2 - (2(i+j) - q), b = q - (i+j)$ として，定理 6.1 に適合する．さらに $1 < 2(i+j) - q = n - b \leq n$ であるから，$\rho = 2(i+j) - q$ とおいて VI の場合であり，$\rho + b = i + j \leq q - 1$ であるから，この中の例外の場合ではない．

したがって，期待通り

$$\begin{aligned} d(C((q^2 - (2(i+j) - q))q + q - (i+j), i+j)) &= d(C((q^2 - \rho)q + b, n)) \\ &= \rho(q-1) = (2(i+j) - q)(q-1) \end{aligned}$$

となる．

参考文献

[1] M. Homma and S. J. Kim, *Goppa codes with Weierstrass pairs*, J. Pure Appl. Algebra **162** (2001) pp. 273–290.

[2] M. Homma, *Various aspects of codes on a Hermitian curve*, 第5回代数幾何・数論および符号・暗号研究集会 (2003年1月東大) 報告集, (2003) pp. 48–54.

[3] 本間正明, *Conics with a Hermitian curve*, 2004 代数幾何学シンポジュウム (2004年2月ウエルシティ新潟) 報告集, (2004) pp. 67–75.

[4] 本間正明, *Hermitian* 曲線上の2点符号 (予報), 数理研講究録 **1361** (2004), 152–161.

[5] M. Homma and S. J. Kim, *Toward the determination of the minimum distance of two-point codes on a Hermitian curve*, Designs, Codes and Cryptography, to appear.

[6] M. Homma and S. J. Kim, *The two-point codes on a Hermitian curve with the designed minimum distance*, Designs, Codes and Cryptography, to appear.

[7] M. Homma and S. J. Kim, *The complete determination of the minimum distance of two-point codes on a Hermitian curve*, in preparation.

[8] G. L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Designs, Codes and Cryptography **22** (2001), 107–121.

[9] K. Yang, *On the weight hierarchy of Hermitian and other geometric Goppa codes*, Ph. D. Thesis, University of Southern California, (1992).

[10] 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.