様式 C-19

科学研究費補助金研究成果報告書

平成　21 年　3 月　31 日現在

研究種目：基盤研究（C）
研究期間：2007～2008
課題番号：19540058
研究課題名（和文）　有限体上の組み合わせ論的代数幾何とその応用

研究課題名（英文）　Combinatorial algebraic geometry over a finite field and its application.

研究代表者
本間 正明（HOMMA MASAAKI）
神奈川大学・工学部・教授
研究者番号：80145523

研究成果の概要：この研究は Hermitian 曲線と呼ばれる正標数体上の平面代数曲線を対象として，その幾何的対称性の反映である射影のモノドロミー群という視点からの研究と，応用的側面を持つ符号の研究との２つの部分からなる．前者については，この補助金対象となった研究以前に報告者が得た結果と合わせて，Hermitian 曲線の全ての射影についてモノドロミー群を決定することができた．後者は，この曲線上の「１点符号」と呼ばれている符号の族については，それらの「最小距離」や「一般化された Hamming 重みの最小値」などは詳細に調べられていることに鑑み，その類似を「２点符号」と呼ばれる符号族で行おうという試みの過程であり，GyeongSang National University の Seon Jeong Kim 教授との共同研究である．本補助金研究開始以前にわれわれは「最小距離」は決定済みであったので，次の段階として「第 2 一般化された Hamming 重み」の完全決定に挑みそれを完成した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	**800,000**	**240,000**	**1,040,000**
2008 年度	**900,000**	**270,000**	**1,170,000**
年度			
年度			
年度			
総　計	**1,700,000**	**510,000**	**2,210,000**

研究分野：代数幾何学・組合せ論
科研費の分科・細目：数学・代数学
キーワード：代数幾何，代数曲線，有限体，符号理論

１．研究開始当初の背景

「有限体上の組合せ論的代数幾何」のひとつの源流は Beniamino Segre にあることは論を俟たない．Segre の興味の発端のひとつは Hermitian form と「正標数体の２次拡大という状況」との類似性にあるように思える．それ故，正標数での類似物も「Hermitian」という語を冠して呼ばれ，その曲線の場合が Hermitian 曲線とよばれるものである．これは，アフィン座標を適当にとれば，

$$H: y^q+y = x^{q+1}$$

という形で与えられる．この方程式を 2 次拡大 $\mathbf{F}_{q^2} / \mathbf{F}_q$ という文脈で見ると左辺は y のトレース右辺は x のノルムという形をしている．

それらが等しいすなわち，トレース写像とノルム写像のファイバー積としてこの曲線の $\mathbf{F}_{q2}$ 有理点が与えられている．この構造の美しさが標数 0 では起こりえない興味深い性質をこの Hermitian 曲線にもたらし，その興味深い種々の性質ゆえ，この曲線は正標数体上での幾何的事情を知るための格好の実験場となっている．

したがって，代数曲線符号の理論においても Hermitian 曲線上の符号について詳細に調べることは自然なことであろう．この曲線上の１点符号については，Tiersma (1987)．Stichtenoth (1988) 等の研究を経て，Yang - Kumar により 1992 年にそれらの最小距離が完全に決定された．また，それらの一般化された Hamming 重みの最小値については，90 年代の Munuera (1994)， Munuera – Ramirez (1999) などの論文を経て，最終的には Barbero - Munuera によって，が 2000 年に完全に決定されていた．また，これらの仕事に触発され，われわれ (Homma-Kim) は２点符号の場合の最小距離の決定に取り組み，2005 年から 2006 年にかけて発表した 4 編の論文で解決していた．

一方，射影空間内にある代数曲線の１点を center にする projection のモノドロミー問題（いわゆる，Galois 点の問題）は十余年前に吉原と彼の共同研究者たちによってによって系統的に調べ始められた．彼らは標数 0 の場合について多くの結果を得たが，報告者は正標数体上ではこれらとは異なる現象が生じうる事に興味を持ち，その最初のステップとして Hermitian 曲線の Galois 点を決定していた (2006)．

２．研究の目的

前項で述べた背景の下に，次の２つの目的をたてた．ひとつは，「Hermitian 曲線上の２点符号の一般化された Hamming 重みの最小値を求めること」もうひとつは「Hermitian 曲線 H の Galois 点ではないような，射影平面上の点から projection $H \to \mathbf{P}^1$ を考えるとき，その Galois 閉包 H’ の genus を求めること，および H’/ $\mathbf{P}^1$ の Galois 群を決定すること」である．

３．研究の方法

研究目的の項で述べた第一の目的については GyeongSang National University の Seon Jeong Kim 教授との共同研究，第二の目的については報告者自身による個人研究として行った．前者については，春季と夏季に報告者が Kim 教授を，冬季に Kim 教授が報告者を訪問することにより共同研究を行った．この際，「Hermitian 曲線上の２点符号の場合の最小距離の決定」における共同研究の経験が大きく生かされた．

また後者については，本学の研修施設を利用して「ガロ点ワワークショップ」を開催し関連研究者と意見を交換したことは研究の進展におおいに資した．

４．研究成果

(1) *Hermitian 曲線上の２点符号の一般化された Hamming 重みの最小値*

有限体 $\mathbf{F}$ 上の符号 $C \subset \mathbf{F}^n$ を固定する．C の{0}ではない部分空間 V について，その重み w(V) を

$$\#\{\, i \mid {}^{\exists}x=(x_1,\cdots,x_n) \in V \ \text{s.t.}\ x_i \neq 0 \,\}$$

によって定め，C の第 i Hamming 重みを

$$\mathrm{Min}\{\, w(V) \mid V \text{ は } C \text{ の } i \text{ 次元部分空間} \}$$

で定める．第 1 Hamming 重みは C の最小距離に他ならない．

一般に有限体 $\mathbf{F}$ 上定義された代数曲線 X を考える．X の $\mathbf{F}$ 上定義された因子 G と X の $\mathbf{F}$ 有理点の集合で G と共通部分を持たない集合$\{P_\lambda\}$ (これを因子とみて $D=\sum P_\lambda$ と書く) とを固定し，高々G に極を持つ $\mathbf{F}$ 上定義された関数全体のなす $\mathbf{F}$ ベクトル空間 L(G) と書く．

$$L(G) \ni f \mapsto (\ \ldots, f(P_\lambda), \ldots) \in \mathbf{F}^N$$

(ただし，N = #(D) である.) によって得られる $\mathbf{F}^n$ の部分空間(= 符号)を C(D,G) と書きこれを代数曲線符号とよぶ．X の $\mathbf{F}$ 有理点全体の集合を $X(\mathbf{F})$ で表す．$G = m_1Q_1+\ldots+m_rQ_r$ $(Q_1,\ldots,Q_r \in X(\mathbf{F}))$，D を $X(\mathbf{F})\setminus\{Q_1,\ldots,Q_r\}$ を並べた因子として作った C(D,G) を r 点符号と呼ぶ．Hermitian 曲線 $H : y^q+y = x^{q+1}$ の場合には，$\mathbf{F}=\mathbf{F}_{q2}$ とする．このとき，$H(\mathbf{F})$ は q^3+1 個の点からなる．われわれの考察する対象は $Q_1, Q_2 \in H(\mathbf{F})$，$D = H(\mathbf{F}) \setminus \{Q_1,Q_2\}$ として，$C(D, mQ_1+nQ_2)$ である．ところで H の自己同型はすべて $\mathbf{F}$ 上定義され，従って $H(\mathbf{F})$ に作用するが，この作用は 2 重推移的であるので，Q_1, Q_2 として，このアフィン座標で原点 $P_0=(0,0)$ と(この曲線上では唯一の)無限遠点 P_∞ としてよい．$C(D, mP_\infty+nP_0)$ を簡単に C(m,n) と表す．H 上で因子 $(q+1)P_0$ は $(q+1)P_\infty$ と線形同値であるので，$0 \le n \le q$ と仮定してよい．また，n を固定して m を動かすと $\ldots \subseteq C(m-1, n) \subseteq C(m,n) \subseteq \ldots$ という上昇列を得る．したがって，$\dim C(m,n) > \dim C(m-1, n)$ となるような，(m,n) について考えれば良い．このような枠組みで C(m,n) の第 2 Hamming 重みを完全に決定し記述した．

この記述の詳細には，さらに多くの準備を要し余りにも専門的であり，またすでに入手しやすい著名なジャーナルに発表済みであることを考慮し，ここでは，それは省略し，この結果を得るための道具立ておよび今後の展望等を記すことにとどめる．

この第 2 Hamming 重みを決定するためのア

イデアは極めて単純である．代数曲線符号の最小距離，それは一般化された Hamming 重みの立場からすれば，第 1 Hamming 重みに他ならないが，その考察には関数の振る舞いを調べることが重要であった．このような見方をすれば，第 2 Hamming 重みを調べることはある種の 1 次元線形系を調べることに対応するはずである．幸いにも，われわれは，これについての知識が豊富であったので Coppens による 90 年代の平面代数曲線上の 1 次元線形系の理論が適用できる事を見てとることができた．また，この仕事以前に C(m,n)の最小距離の決定を行った経験が，かなり役立った．すなわち，この以前の仕事の中でわれわれは Hermitian 曲線の幾何に習熟しており，例えば，2 次曲線と Hermitian 曲線がどのような関わり方をするかについて詳細に調べてあった．また，これは以下に述べる (2) の成果へも良い影響を与えたように思う．さらに，Munuera 等の「Hermitian 曲線上の 1 点符号についての一般化された Hamming 重みの最小値の最終決定」に至るまでの一連の論文にも大きなヒントを得た．

今後考察すべき問題として，当然「第 2 Hamming 重み」のみならず，すべての「一般化された Hamming 重み」の最小値の決定がある．しかし，われわれが「第 2 Hamming 重み」でとった方針を維持するとすれば，平面代数曲線上の n 次元線形系について深く考察する必要がありそうで，これは必ずしも容易なこととは思えない．むしろ「1 点符号」の場合に Munuera 等が一連の仕事の途中で方針転換したように order bound 的アプローチが有効かもしれない．

(2) *射影平面内にある Hermitian 曲線の射影平面上の点から projection のモノドロミー群*

代数閉体 k 上の平面代数曲線 $X \subset \mathbf{P}^2$ と点 $P \in \mathbf{P}^2$ について P からの projection $\pi_P: X \to \mathbf{P}^1$ を考える．このとき，π_P から得られる体の拡大 $k(X)/k(\mathbf{P}^1)$ の Galois closure に対応する X の被覆となる曲線を Y とするとき，$k(Y)/k(\mathbf{P}^1)$ の Galois 群の構造を決定すること，および Y の種数を求めるという問題がある．この一般的な問題に対して X が Hermitian 曲線 H の場合に完全な解答を与えた．

X が非特異でその次数が 4 以上のとき，標数が 0 ならば，ガロワ点，すなわち，projection π_P がガロワ被覆となるような点の個数は X の中では 4 以下，外では 3 以下であることが知られていた(吉原 2001)．しかし，定義方程式から容易にわかるように，Hermitian 曲線の場合はこのアフィン座標での原点は明らかにガロワ点であり，また H の自己同型群は H の $\mathbf{F}_{q^2}$ 有理点全体 $H(\mathbf{F}_{q^2})$ へ推移的に作用することにより，H の中に少なくとも $H(\mathbf{F}_{q^2})$ の個数 q^3+1 のガロワ点があることがわかる．これは上の問題が正標数では，標数 0 の場合とはかなり異なった様相を示すことを示唆しており，「正標数体上での幾何的事情を知るための格好の実験場」としての Hermitian 曲線の真価を発揮させるべく，この曲線について「projection π_P のモノドロミー問題」の全面的な解決を目指した．ガロワ点については，2006 年に，この方程式を考えた座標系では H のガロワ点全体はその射影平面の $\mathbf{F}_{q^2}$ 有理点全体と一致するという結果を得た．(ガロワ点という概念は考えている曲線の定義体には依存しないので，このような，やや回りくどい表現となる．)

以下，ガロワ点ではない $P \in \mathbf{P}^2 \setminus \mathbf{P}^2(\mathbf{F}_{q^2})$ を考え，P からの projection $\pi_P: H \to \mathbf{P}^1$ に対応する $\mathbf{P}^1$ のガロワ被覆を H'_P で表し，G_P で $k(H'_P)/k(\mathbf{P}^1)$ のガロワ群を表す．このとき，次の事実が証明できた．

① $P \in H$ のとき，$G_P = AGL(1, \mathbf{F}_q)$ であり，H'_P の genus は $q(q-1)^2/2$ である．

② $P \notin H$ のとき，$G_P = PGL(2, \mathbf{F}_q)$ であり，H'_P の genus は $q(q^3 - q - 2)/2$ である．

この証明には，Abhyankar の “method of throwing away roots” と呼ばれている手法を用いる．π_P から得られる拡大 $k(H)/k(\mathbf{P}^1)$ は比較的単純な方程式で記述されるので，Abhyankar の方法が計算可能なレベルで適用できる．また H'_P の genus を求める原理は次のようなものである．Abhyankar の方法により方程式の根を分離する各ステップで対応する曲線の被覆の分岐を丁寧に調べることにより，やや繁雑な計算ではあるが H'_P の genus を求めることができる．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　　2 件）

① M. Homma, The Galois group of a projection of a Hermitian curve, Int. J. Algebra 1 (2007)563-585.
http://www.m-hikari.com/ija/ija-password-2007/ija-password9-12-2007/hommaIJA9-12-2007.pdf

② M. Homma and S. J. Kim, The second generalized Hamming weight for two-point codes on a Hermitian curve, Designs, Codes and Cryptography 50 (2009) 1-40.
http://www.springerlink.com/content/l8175uw825081t7w/

〔学会発表〕（計　1 件）
① 本間正明, 有限体上の射影平面を覆う非特異代数曲線, 日本数学会代数分科会　2007 年 9 月 22 日　東北大学

６．研究組織
(1)研究代表者
本間 正明　(HOMMA MASAAKI)
神奈川大学・工学部・教授
研究者番号：80145523

(2)研究分担者
なし

(3)連携研究者
なし

(4) 海外共同研究者
KIM SEONJEONG
GyeongSang National University/Faculty of Natural Science/Professor