Proceedings of the 27th Summer Seminar on Lie Algebras and Related Topics

Held at Hiroshima University,
August 22 – 23, 2011

Hiroshima, Japan

Preface

The 27th Summer Seminar on Lie Algebras and Related Topics was held at Hiroshima University, Kasumi Campus, on August 22 – 23, 2011.

The lectures cover various topics of Lie algebras, algebraic systems and their applications. We would like to thank the lecturers for their interesting talks and the preparation of their papers for this proceedings.

Fujio Kubo

List of talks

Fumiya Suenobu	代数構造の幾何学的様相
Takefumi Shudo	KS_3 の自己同型群
Yoshimi Kashiwagi	Some generalizations of the BCH bound
Yoji Yoshii	極小局所アフィンリー代数について
Manabu Matsuoka	Generalizations of the concept of cyclicity of codes
Naoki Kawamoto	微分方程式による人口変動モデル
Yasuyuki Hirano	Rings over which every free submodule of a free module is a direct summand

代数構造の幾何学的様相

広島大学大学院工学研究科
末信 郁也　　久保 富士男

1　序文

著者らは [1] において，与えられた代数に最も近い結合代数を求める手段を論じ，実数体上の 2 次元結合代数に対しその具体的なアルゴリズムを与えた．本稿では実数体上の 2 次元結合代数の分類に関する論文 [2] を紹介し，著者らの研究結果との関連について調べた．

2　諸定義

基底 $\{e_1, e_2\}$ にもつ実数体 $\mathbb{R}$ 上の 2 次元のベクトル空間を V とする．V 上の積 '$\circ$' をもつ結合代数を A とし，A の構造定数を $(c_{ijk}) \in \mathbb{R}^{n^3}$ とする：

$$e_i \circ e_j = \sum_{k=1}^{2} c_{ijk} e_k.$$

このとき，構造定数 (c_{ijk}) は以下の 16 個の条件式を満たす．

$$\sum_{p=1}^{2} (c_{ijp} c_{pkq} - c_{jkp} c_{ipq}) = 0 \quad (i, j, k, q = 1, 2) \tag{1}$$

(1) を満たす代数多様体を $\mathfrak{C}$ とおく．

V 上対称双線形写像 $\varphi : V \times V \to V$ が任意の $x, y \in V$ に対して

$$\varphi(\varphi(x, x), \varphi(x, y)) - \varphi(x, \varphi(\varphi(x, x), y)) = 0,$$

を満たすとき，(V, φ) をジョルダン代数という．

V 上歪対称双線形写像 $\mu : V \times V \to V$ が任意の $x, y, z \in V$ に対して

$$\mu(\mu(x, y), z) + \mu(\mu(y, z), x) + \mu(\mu(z, x), y) = 0,$$

を満たすとき，(V, μ) をリー代数という．

3　2 次元結合代数のパラメータ表示

代数多様体 $\mathfrak{C}$ はグレブナ基底を用いて，$\mathfrak{C}_1, \ldots, \mathfrak{C}_5$ の 5 つに分割され，パラメータ表示できる．詳細は著者らの論文 [1] を参照されたい．本稿では定理のみを載せる．

定理 3.1 ([1])**.** $\mathfrak{C} \in \mathbb{R}^8$ を式 *(1)* を満たす代数多様体とする．このとき，$\mathfrak{C}$ を次のようにパラメータ表示できる．

$$
\begin{aligned}
\mathfrak{C} &= \mathfrak{C}_1 \cup \mathfrak{C}_2 \cup \mathfrak{C}_3 \cup \mathfrak{C}_4 \cup \mathfrak{C}_5 \\
\mathfrak{C}_1 &= \{(\alpha, 0, \beta, 0, 0, \alpha, 0, \beta) \mid \alpha, \beta \in \mathbb{R}\} \\
\mathfrak{C}_2 &= \{(\alpha, 0, 0, 0, 0, 0, 0, \beta) \mid \alpha, \beta \in \mathbb{R}\} \\
\mathfrak{C}_3 &= \{(\alpha, 0, 0, \alpha, \beta, 0, 0, \beta) \mid \alpha, \beta \in \mathbb{R}\} \\
\mathfrak{C}_4 &= \{(\alpha, \beta, \gamma, 0, \gamma, 0, 0, \gamma) \mid \alpha, \beta, \gamma \in \mathbb{R}\} \\
\mathfrak{C}_5 &= \{(\alpha - p\gamma + p^2\beta, p\alpha, p\beta, \alpha, \\
&\qquad p\beta, \alpha, \beta, \gamma) \mid \alpha, \beta, \gamma, p \in \mathbb{R}\}
\end{aligned}
$$

ここに，$\mathfrak{C}_2 \subseteq \mathfrak{C}_4 \cup \mathfrak{C}_5$ である．

4　2 次元結合代数の分類

Bermúdez 達は 2 次元結合代数を 7 つの非同型な代数に分類した（[2]）．本稿では，その内容を簡単に紹介したい．

命題 4.1. ‘$\circ$’ を V 上の結合積とする．$\varphi(x, y) := (x \circ y + y \circ x)/2$ はジョルダン積となる．$\mu(x, y) := (x \circ y - y \circ x)/2$ はリー積となる．さらに，$x \circ y = \varphi(x, y) + \mu(x, y)$ となる．

補題 4.2 ([2])**.** φ を V 上ジョルダン積とする．φ は以下の非同型なジョルダン積 $\varphi_1, \ldots, \varphi_6$ のいずれかに同型となる．

1. $\varphi_1(e_1, e_1) = e_1, \quad \varphi_1(e_1, e_2) = e_2, \quad \varphi_1(e_2, e_2) = -e_1.$
2. $\varphi_2(e_1, e_1) = e_1, \quad \varphi_2(e_1, e_2) = e_2, \quad \varphi_2(e_2, e_2) = e_1.$
3. $\varphi_3(e_1, e_1) = e_1, \quad \varphi_3(e_1, e_2) = e_2, \quad \varphi_3(e_2, e_2) = 0.$
4. $\varphi_4(e_1, e_1) = 0, \quad \varphi_4(e_1, e_2) = 0, \quad \varphi_4(e_2, e_2) = e_2.$
5. $\varphi_5(e_1, e_1) = e_2, \quad \varphi_5(e_1, e_2) = 0, \quad \varphi_5(e_2, e_2) = 0.$
6. $\varphi_6(e_1, e_1) = e_1, \quad \varphi_6(e_1, e_2) = \dfrac{1}{2}e_2, \quad \varphi_6(e_2, e_2) = 0.$

V 上のリー積を μ とする．μ は，$a, b \in \mathbb{R}$ を用いて以下のように表される:

$$\begin{aligned} &\mu(e_1, e_1) = 0, && \mu(e_1, e_2) = ae_1 + be_2, \\ &\mu(e_2, e_1) = -ae_1 - be_2, && \mu(e_2, e_2) = 0. \end{aligned} \tag{2}$$

命題 4.1 と補題 4.2 より，それぞれの $\varphi_i + \mu$ $(i = 1, \ldots, 6)$ に対して，結合代数の定義式である式 (1) を満たすよう a, b を定めることで $\mathbb{R}$ 上 2 次元結合代数が分類される．

定理 4.3 ([2])**.** *V 上結合代数は以下の構造定数 $\beta_i = (c_{111}, \ldots, c_{222})$ をもつ結合代数のいずれかと同型である:*

$$\begin{aligned} \beta_1 &:= (1,0,0,1,0,1,-1,0) \\ \beta_2 &:= (1,0,0,1,0,1,1,0) \\ \beta_3 &:= (1,0,0,1,0,1,0,0) \\ \beta_4 &:= (0,0,0,0,0,0,0,1) \\ \beta_5 &:= (0,1,0,0,0,0,0,0) \\ \beta_6 &:= (1,0,0,1,0,0,0,0) \\ \beta_7 &:= (1,0,0,0,0,1,0,0) \end{aligned}$$

Proof. μ を式 (2) で表される V 上のリー積とする．補題 4.2 のそれぞれの φ_i に対し，$\varphi_i + \mu$ の構造定数が式 (1) を満たすよう a, b を定める．本稿では，φ_1 の場合のみ計算を行うこととする．$\varphi_1 + \mu$ の構造定数は $(1, 0, a, 1+b, -a, 1-b, -1, 0)$ である．式 (1) の $(i, j, k, q) = (2, 2, 2, 1), (2, 2, 2, 2)$ のそれぞれの場合の式は以下の通りである:

$$\begin{aligned} c_{221}(c_{121} - c_{211}) = 0, \\ c_{221}(c_{122} - c_{212}) = 0. \end{aligned}$$

この 2 式に $\varphi_1 + \mu$ の構造定数を代入すると，$-2a = 0, -2b = 0$ となり，$a = b = 0$ を得る．よって，φ_1 の場合から β_1 が得られる． □

5 代数多様体 $\mathfrak{C}$ と結合代数の軌道

以降の節では，代数 A の構造定数 c_{ijk} を以下の 4×2 の行列で表すものとする：

$$\begin{pmatrix} c_{111} & c_{112} \\ c_{121} & c_{122} \\ c_{211} & c_{212} \\ c_{221} & c_{222} \end{pmatrix}.$$

定理 4.3 の β_i に同型な代数の構造定数 β_i' は，実数体上の 2×2 の正則行列 A を用いて，

$$\beta_i' = (A \otimes A)\beta_i A^{-1},$$

と表される．ここに，$A \otimes A$ は A 同士のクロネッカー積である．例えば，$(A \otimes A)\beta_1 A^{-1}$ は $A = \begin{pmatrix} u & v \\ s & t \end{pmatrix}$ に対し，

$$\begin{aligned} & \frac{1}{ut - vs} \begin{pmatrix} u^2 & uv & uv & v^2 \\ us & ut & vs & vt \\ us & vs & ut & vt \\ s^2 & ts & ts & t^2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} t & -v \\ -s & u \end{pmatrix} \\ = \quad & \frac{1}{ut - vs} \begin{pmatrix} u^2t - v^2t - 2uvs & u^2v + v^3 \\ -vt^2 - vs^2 & v^2t + u^2t \\ -vt^2 - vs^2 & v^2t + u^2t \\ -s^2t - t^3 & -vs^2 + vt^2 + 2ust \end{pmatrix} \end{aligned}$$

となる．各 β_i に対し，

$$\mathcal{O}(\beta_i) := \{(A \otimes A)\beta_i A^{-1} \mid A \in \mathrm{GL}(2, \mathbb{R})\}$$

を β_i の軌道と定義する．

定理 5.1. $i = 1, \ldots 5$ に対し，$\mathfrak{C}_i^* = \mathfrak{C}_i \setminus \{0\}$ とおく．$\beta_1, \ldots, \beta_7$ を定理 *4.3* において与えられた構造定数とし，正則な実行列を $A = \begin{pmatrix} u & v \\ s & t \end{pmatrix}$ とし，さらに $\mathcal{O}(\beta_i)$ を β_i の軌道とする（$i = 1, \ldots, 5$）．このとき，$\mathfrak{C}_i$ はそれぞれの軌道を用いて以下のように表すことができる：

$$\begin{aligned} \mathfrak{C}_1^* &= \mathcal{O}(\beta_7) \\ \mathfrak{C}_2^* &\subseteq \mathcal{O}(\beta_2) \cup \mathcal{O}(\beta_4) \\ \mathfrak{C}_3^* &= \mathcal{O}(\beta_6) \\ \mathfrak{C}_4^* &= \mathcal{O}(\beta_1)_{t=0} \cup \mathcal{O}(\beta_2)_{t=0} \cup \mathcal{O}(\beta_3)_{t=0} \cup \mathcal{O}(\beta_4)_{t=0} \cup \mathcal{O}(\beta_5)_{s=0} \\ \mathfrak{C}_5^* &= \mathcal{O}(\beta_1)_{t\neq 0} \cup \mathcal{O}(\beta_2)_{t\neq 0} \cup \mathcal{O}(\beta_3)_{t\neq 0} \cup \mathcal{O}(\beta_4)_{t\neq 0} \cup \mathcal{O}(\beta_5)_{s\neq 0} \end{aligned}$$

ここに，$\mathcal{O}(\beta_i)_{t=0}, \mathcal{O}(\beta_i)_{s=0}, \mathcal{O}(\beta_i)_{t\neq 0}, \mathcal{O}(\beta_i)_{s\neq 0}$ はそれぞれ A が $t=0, s=0, t\neq 0, s\neq 0$ を満たす $\mathcal{O}(\beta_i)$ の元の集合である．

Proof. 本稿では，$\mathfrak{C}_3^* = \mathcal{O}(\beta_6)$ のみを示すこととする．

$$(A\otimes A)\beta_6 A^{-1} = \begin{pmatrix} u & 0 \\ 0 & u \\ s & 0 \\ 0 & s \end{pmatrix} \in \mathcal{O}(\beta_6)$$

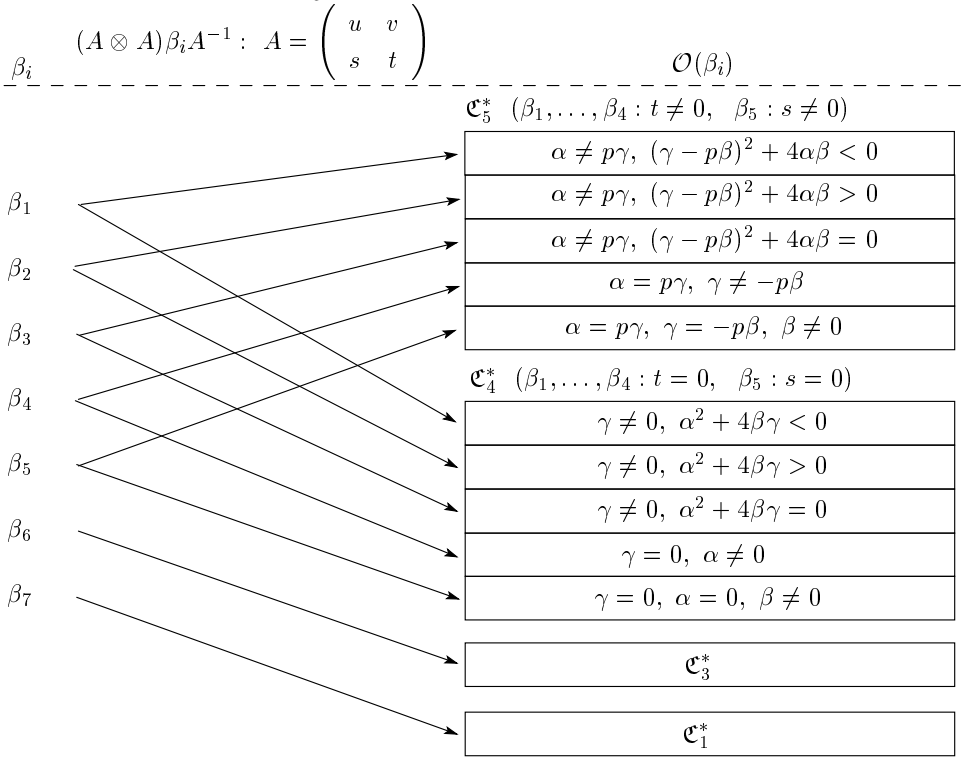
となり，$\mathcal{O}(\beta_6) \subseteq \mathfrak{C}_3$ が成立する．

逆に，

$$(A\otimes A)\beta_i A^{-1} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \\ \beta & 0 \\ 0 & \beta \end{pmatrix}$$

を満たす β_i, A は $\mathfrak{C}_3^*$ の全ての元に対し，β_6 および A の各成分は $u=\alpha, s=\beta, t\neq \dfrac{\beta}{\alpha}v, v\in\mathbb{R}$ と求められる． □

各軌道 $\mathcal{O}(\beta_i)$ が $\mathfrak{C}_1^*, \ldots, \mathfrak{C}_5^*$ のどの部分に移るのかは，以下の図の通りである．



6　結合代数の contraction

定義 6.1. α を V 上結合積とし，$\{f_t\} \subset \mathrm{GL}(2,\mathbb{R})$ をパラメータ t をもつ自己同型の族とする．全ての $x, y \in V$ に対し，極限

$$\alpha_0 := \lim_{t\to 0} f_t^{-1}\left(\alpha(f_t(x), f_t(y))\right)$$

が存在するとき，α_0 を α の **contraction** という．

上記の定義は，基底に対して極限が存在するかどうかを判断すれば十分である．β を V 上結合代数の構造定数とし，2×2 行列 $A(t)$ を以下のように与える：

$$A(t) = \begin{pmatrix} a(t) & b(t) \\ c(t) & d(t) \end{pmatrix}, \quad a(t)d(t) - b(t)c(t) \begin{cases} \neq 0 \ (t \neq 0) \\ = 0 \ (t = 0) \end{cases}.$$

このとき，以下の極限

$$\beta_0 = \lim_{t\to 0} \left(A(t) \otimes A(t)\right) \beta A(t)^{-1}$$

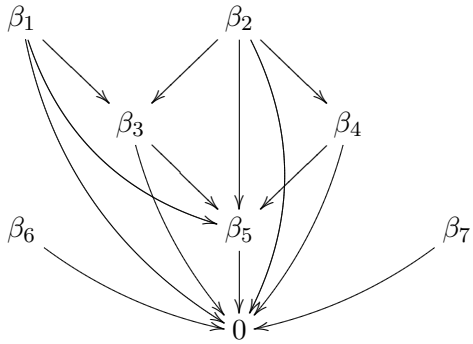
が存在するときに，β_0 は β の contarction であるといえる．

例えば，$A(t) = \begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix}$ とおき，定理 4.3 で定義された β_1 に対して $(A(t)\otimes A(t))\beta_1 A(t)^{-1}$ を計算すると，$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ -t^2 & 0 \end{pmatrix}$ となり，

$$\lim_{t\to 0}(A(t)\otimes A(t))\beta_1 A(t)^{-1} = \beta_3$$

であることが分かる．従って，β_3 は β_1 の contraction である．

$\beta_1, \ldots, \beta_7$ それぞれの contraction をまとめると，以下の図のようになる．ここに，図の矢印がそれぞれの contraction を表している．



前節の図と比較してみると，β_i が β_j $(i \neq j)$ の contraction となっているものは，$\mathcal{O}(\beta_i)$ と $\mathcal{O}(\beta_j)$ が同じ $\mathfrak{C}_p^*$ 上にあり，かつ $\dim \mathcal{O}(\beta_i) < \dim \mathcal{O}(\beta_j)$ を満たしているものであることが分かる．実際，β_3 は β_1 の contraction であるが，確かに $\mathcal{O}(\beta_3)$ と $\mathcal{O}(\beta_1)$ は共に $\mathfrak{C}_4^*$ または $\mathfrak{C}_5^*$ 上にあり，前節の図から $\dim \mathcal{O}(\beta_3) < \dim \mathcal{O}(\beta_1)$ も自明である．唯一この条件に当てはまらないものとして，β_4 が β_1 の contraction となっていないが，これについては以下のように考察できる．β_1, β_4 それぞれの軌道は $\mathfrak{C}_5^*$ 上では $\alpha \neq p\gamma, (\gamma - p\beta)^2 + 4\alpha\beta < 0$ および $\alpha = p\gamma, \gamma \neq -p\beta$ を満たす部分を通っている．β_1 の右側の条件式に $\alpha = p\gamma$ を代入すると $(\gamma - p\beta)^2 + 4p\beta\gamma = (\gamma + p\beta)^2$ となる．従って，$\mathcal{O}(\beta_4)$ の中の点は $\mathcal{O}(\beta_1)$ の条件式 $(\gamma - p\beta)^2 + 4p\beta\gamma < 0$ を満たさない．$\mathfrak{C}_4^*$ の場合も同様であるため，$\mathcal{O}(\beta_4)$ の近傍に $\mathcal{O}(\beta_1)$ は存在しない．

参考文献

[1] F. Kubo, F. Suenobu, “On the associative algebra structures closest to algebra sturctures”, *J. Algebra and its Appl.*, **10**, 365-376(2011).

[2] J. M. A. Bermúdez, J. Fresán, J. S. Hernádez, “On the variety of two dimensional real associative algebras”, *Int. J. Contemp. Math. Science*, **26**, 1293-1305(2007).

KS_3 の自己同型群 II

首 藤　武 史

§0　序

K を代数的閉体とし，p をその標数とする．A が K 上の有限次元多元環であるとき，この自己同型全体のなす群 $\mathrm{Aut}(A)$ が代数群の構造を持つことはよく知られている． $p=0$ の場合にはこのリー環 $\mathrm{L}(\mathrm{Aut}(A))$ は自然に A の導分環 $\mathrm{Der}(A)$ に一致することもよく知られている．しかしながら，$p>0$ の場合には一般にはこのことは成立しないことが簡単な例で示される．これに関して，幾つかの例を計算して次のような予測をしている．

A の根基を保つ導分全体 $\mathrm{der}(A)$ は $\mathrm{Der}(A)$ の部分リー環で，これが $\mathrm{Aut}(A)$ のリー環であろう．

前回の講演では，このことを示す例として，A が 3 次の対称群 S_3 の群環である場合の計算結果を報告した．結果は以下の通りである．

$p\neq 2,3$ のとき，$A\cong K\times K\times \mathrm{M}_2(K)$．これから，$\mathrm{Aut}(A)\cong S_2\times \mathrm{PGL}_2(K)$.

$p=2$ のとき，$A\cong K[x]/(x^2)\times \mathrm{M}_2(K)$．これから，$\mathrm{Aut}(A)\cong K^{\times}\times \mathrm{PGL}_2(K)$.

$p=3$ のとき，$\dim \mathrm{Aut}(A)=4$，$(\mathrm{Aut}(A):\mathrm{Aut}(A)_0)=2$.

いずれの場合にも，$\mathrm{L}(\mathrm{Aut}(A))=\mathrm{der}(A)$ が成立している．

ここで，$p=3$ の場合は，代数群としての次元，連結成分の個数はコンピュータ・ソフトウェアを利用して得た結論である．

今回，$p=3$ の場合に，A の自己準同型全体のなす空間 $\mathrm{End}(A)$ を詳しく調べることにより，上記の結果をコンピュータに依らずに証明できたので，その概略を報告する．

ところで，上記の結果のうち前者 2 つは，K は代数的閉体ではなく任意の体，特に有限体，で成立する．従って，$p=3$ の場合にも，抽象群としてのまとめ方が望ましい．これについて§4 で言及する．

§§ 1, 2 では K は標数 3 の任意の体とし，§ 3 ではさらに代数的閉体とする．代数多様体や代数群の基本的なことは [2] に従う．

§1　KS_3

3 次対称群 S_3 およびこの群環（group algebra）について以下の議論に必要なことをまとめる．

S_3 は位数 6 の群で，2 つの元 e_1，e_2 で生成され，次の基本関係をもつ：

$$e_1^{\,2}=e_0,\quad e_2^{\,2}=e_0,\quad e_2e_1=(e_1e_2)^2 \tag{1.1}$$

ここで，e_0 は S_3 の単位元である．

(1.2) $$e_3=e_1e_2e_1,\quad e_4=e_1e_2,\quad e_5=e_2e_1$$

とおけば,

$$S_3=\{e_0,\ e_1,\ e_2,\ e_3,\ e_4,\ e_5\}$$

で，e_1, e_2, e_3 は位数 2 をもち，e_4, e_5 の位数は 3 である．$A_3=\{e_0,\ e_4,\ e_5\}$ は正規部分群で，3 次の交代群である．

K を標数 3 の任意の体とし，$A=KS_3$ を S_3 の K 上の群環とする．すなわち，A は S_3 の元を基底にもつ K 上の 6 次元ベクトル空間で，S_3 の積を線形に拡大することによって得られる K 上の多元環である．e_0 が単位元である．たびたびこれを 1 で表す.

A は直既約 (すなわち, A は多元環の直積では表されない) である. A の根基（Jacobson radical）R は $\{e_1-e_2, e_1-e_3, e_0-e_4, e_0-e_5\}$ で張られる 4 次元のイデアルで,

$$A/R\cong K\times K.$$

§2 End(A)

A の 1 次変換 σ が，$\sigma(1)=1$ で，A の任意の 2 元 a, b に対して

(2.1) $$\sigma(ab)=\sigma(a)\sigma(b)$$

を満たすとき, A の自己準同型と呼ばれる. これらの全体のなす集合を End(A)で表す. これは 1 次変換の積 (合成) に関して閉じている.

群 S_3 の基本関係 (1.1) より,

(2.2) A の部分集合 $\{e_1, e_2\}$ から，A への写像 f が

$$f(e_1)^2=1,\ f(e_2)^2=1,\ f(e_2)f(e_1)=(f(e_1)f(e_2))^2$$

をみたすとき，f は一意的に A の自己準同型に拡張される．最後の等式は

$$f(e_1)f(e_2)f(e_1)=f(e_2)f(e_1)f(e_2)$$

で置き換えてもよい.

実際，(1.2) より，$f(e_3)=f(e_1)f(e_2)f(e_1)$，$f(e_4)=f(e_1)f(e_2)$，$f(e_5)=f(e_2)f(e_1)$ と定義すればよい.

$A\times A$ の部分集合 B を次のように定義する：

(2.3) $$B=\{(a,b)\in A\times A \mid a^2=1,\ b^2=1,\ aba=bab\}$$

A の自己準同型 f が (2.2) の各式を満たすことは明らかであるから，(2.2) より，

(2.4) 写像 $f\mapsto (f(e_1), f(e_2))$ は $\mathrm{End}(A)$ から B への全単射である．

$\mathrm{Aut}(A)=\mathrm{End}(A)\cap \mathrm{GL}(A)$であるから，

(2.5) (2.4)で，(a, b) に対応する A の自己準同型を σ とするとき，σ が A の自己同型であるための必要純分条件は

$$\{1, a, b, aba, ab, ba\}$$

が 1 次独立であることである．

B を具体的にするために，先ず，A の位数 2 の元を調べる．$a\in A$ が $a^2=1$ であるとする．$a=\sum_{i=0}^{5} x_i e_i$ とおく．S_3 の乗積表により，$x_0, x_1, \dots, x_5$ がみたす関係式を求め整理すると次の結果を得る．

(2.6) $a=\sum_{i=0}^{5} x_i e_i$ のとき，$a^2=1$ となるための必要十分条件は次の (i) または (ii) が成り立つことである：

(i) $x_0=\pm 1,\ x_i=0 \quad (i=1, \dots, 5)$

(ii) $x_0=0,\ x_1+x_2+x_3=\pm 1,\ x_4+x_5=0,\ {x_1}^2+{x_2}^2+{x_3}^2+{x_4}^2=1$

すなわち，

$\{a\in A \mid a^2=1\}$

$=\{\pm e_0\}\cup\{x_1e_2+x_2e_2+x_3e_3+x_4(e_4-e_5) \mid x_1+x_2+x_3=\pm 1,\ {x_1}^2+{x_2}^2+{x_3}^2+{x_4}^2=1\}$

次に，a, b が $a^2=1, b^2=1$ をみたすとき，$(a, b)\in B$ となる条件を求める．先ず次のことは容易に分かる．

(2.7) $a\in A$ とする．

(i) $(\pm e_0, a)\in B \Leftrightarrow a=\pm e_0$ (復号同順)

(ii) $(a, \pm e_0)\in B \Leftrightarrow a=\pm e_0$ (復号同順)

そこで，A の部分集合 D^+ と D^- を次のように定義する：

$$D^+=\{x_1e_1+x_2e_2+x_3e_3+x_4(e_4-e_5) \mid x_1+x_2+x_3=1,\ {x_1}^2+{x_2}^2+{x_3}^2+{x_4}^2=1\}$$

$$D^- = \{x_1e_1 + x_2e_2 + x_3e_3 + x_4(e_4 - e_5) \mid x_1 + x_2 + x_3 = -1,\ x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1\}$$

(2.8) $(a, b) \neq (\pm e_0, \pm e_0)$ とする．このとき，

$$(a, b) \in B \Leftrightarrow a, b \in D^+ \text{または} a, b \in D^-.$$

証明の概略．必要性．$\pi : A \to A/R$ を標準写像とする．§1 の議論より，

$$\pi(x_1e_1 + x_2e_2 + x_3e_3 + x_4(e_4 - e_5)) = (x_1 + x_2 + x_3)\pi(e_1),\ \pi(e_1) \neq 0$$

仮定より $a, b \in D^+ \cup D^-$ で，$\pi(a) = \pi(b)$．これから $a, b \in D^+$ または $a, b \in D^-$ が分かる．
十分性．$a = x_1e_1 + x_2e_2 + x_3e_3 + x_4(e_4 - e_5)$，$b = y_1e_1 + y_2e_2 + y_3e_3 + y_4(e_4 - e_5)$ が条件をみたすとする．このとき，aba を計算すると，文字 x, y について対称であることが分かる．このことは $aba = bab$ を意味する．

(2.7) および (2.8) より，

(2.9) $$B = \{(e_0, e_0)\} \cup \{(-e_0, -e_0)\} \cup (D^+ \times D^+) \cup (D^- \times D^-).$$

§3 Aut(A)

この節では K は代数的閉体であるとする．A を底 $\{e_0, \ldots, e_5\}$ により 6 次元アファイン空間 K^6 と同一視する．A の 1 次変換全体の空間を $\mathrm{E}(A)$ で表す．これは，K 上の 6 次正方行列の全体であるから，36 次元アファイン空間とみなされる．A, $A \times A$ および，$\mathrm{E}(A)$ は Zariski 位相により位相空間である．A の正則な 1 次変換全体のなす群 $\mathrm{GL}(A)$ は $\mathrm{E}(A)$ の開集合である．(2.1) は座標の間の多項式関係を意味するから，$\mathrm{End}(A)$ は $\mathrm{E}(A)$ の閉集合，$\mathrm{Aut}(A) = \mathrm{GL}(A) \cap \mathrm{End}(A)$ は $\mathrm{End}(A)$ の開集合である．

(3.1) B は $A \times A$ の閉集合で，写像 (2.4) は $\mathrm{End}(A)$ から B への代数多様体の同型でもある．

実際，$f(e_1), f(e_2)$ はそれぞれ f の表現行列の第 1 列，第 2 列である (列は第 0 列から数える) からこれは多項式写像であり，(1.2) より逆写像も多項式写像である．

(3.2) D^+，D^- はともに $A\,(= K^6)$ の閉部分集合で，既約な 2 次元代数多様体である．

証明の概略．これらは明らかに K^4 の代数多様体に同型である．さらに，アファイン座標変換を利用して K^3 に埋め込むことができる．この像は，1 つの既約多項式で定義され，従って，K^3 の既約な超局面に同型である．これから，2 次元の既約代数多様体であることが分かる．

(3.3) (1) $\sigma\in\mathrm{Aut}(A)$ に対して，A の 1 次変換 σ' を次のように決める：

$$\sigma'(e_i)=-\sigma(e_i)\quad(i=1,2,3),\quad \sigma'(e_i)=\sigma(e_i)\quad(i=0,4,5)$$

このとき，σ' は A の自己同型である，すなわち，$\sigma'\in\mathrm{Aut}(A)$.

(2) $\varepsilon=(id_A)'$ とおく．これは A の自己同型である：$\varepsilon\in\mathrm{Aut}(A)$.

証明．(1) σ は A の自己同型だから，容易に $\sigma'\in\mathrm{Aut}(A)$ も分かる．

(2) $id_A\in\mathrm{Aut}(A)$ であるから $\varepsilon=(id_A)'\in\mathrm{Aut}(A)$.

(2.4) および (3.1) によって，$\mathrm{End}(A)$ と B を同一視する．このとき，

$$\mathrm{Aut}(A)\cap(D^+\times D^+)\neq\phi,\quad \mathrm{Aut}(A)\cap(D^-\times D^-)\neq\phi \tag{3.4}$$

実際，$id_A\in\mathrm{Aut}(A)\cap(D^+\times D^+)$，$\varepsilon\in\mathrm{Aut}(A)\cap(D^-\times D^-)$.

(e_0, e_0)，$(-e_0, -e_0)\notin\mathrm{Aut}(A)$ であるから，(2.8) より，

$$\mathrm{Aut}(A)=(\mathrm{Aut}(A)\cap(D^+\times D^+))\cup(\mathrm{Aut}(A)\cap(D^-\times D^-)) \tag{3.5}$$

右辺は $\mathrm{Aut}(A)$ の既約成分への分解である．従って，

(i) $\dim\mathrm{Aut}(A)=4$,

(ii) $\mathrm{Aut}(A)_0=\mathrm{Aut}(A)\cap(D^+\times D^+)$,

(iii) $(\mathrm{Aut}(A):\mathrm{Aut}(A)_0)=2$.

実際，(3.2) より $D^+\times D^+$，$D^-\times D^-$ は 4 次元の既約な代数多様体で，$\mathrm{Aut}(A)$ との共通部分は稠密であるから，それぞれ既約である．$\dim D^{\pm}=2$ より，(i) が成り立つ．(3.4) の議論より，$\mathrm{Aut}(A)\cap(D^+\times D^+)$ は単位元を含む $\mathrm{Aut}(A)$ の既約成分である．すなわち，(ii)．さらにこれから (iii) が従う．

§4 有限体の場合

A の内部自己同型群を $\mathrm{Int}(A)$ で表す．これは $\mathrm{Aut}(A)$ の閉正規部分群で連結である．従って，$\mathrm{Int}(A)\subset\mathrm{Aut}(A)_0$ が成り立ち，前回の講演で次の代数群の完全系列があることを報告した [3, Remark]:

$$\{1\}\to\mathrm{Int}(A)\to\mathrm{Aut}(A)_0\to K^\times\to\{1\} \tag{4.1}$$

これらの群はいずれも素体上で定義されているので，k が K の部分体であるとき，k 有理点の系列

(4.2) $\{1\} \to \mathrm{Int}(A)(k) \to \mathrm{Aut}(A)_0(k) \to k^\times \to \{1\}$

も完全ではないかと思われる．これが 0 系列であることは明らかである．問題は $\mathrm{Aut}(A)_0(k) \to k^\times$ が全射であることである．k が有限体の場合，[1] (16.5) よりこの写像は全射であることが分かる．従って (4.2) は完全系列である．

k を有限体とし，元の個数が $|k|=3^m$ とする．S_3 の k 係数の群環を改めて A とおく．このとき，(4.2) は次の系列を意味する：

(4.3) $\{1\} \to \mathrm{Int}(A) \to \mathrm{Aut}(A)_0 \to k^\times \to \{1\}$

ここで，D^+ を (2.7) の直後に定義した A の部分集合として，

(4.4) $\mathrm{Aut}(A)_0 = \mathrm{Aut}(A) \cap (D^+ \times D^+) = \mathrm{GL}(A) \cap (D^+ \times D^+)$

とおく．これは $\mathrm{Aut}(A)$ の指数 2 の正規部分群である．

$\mathrm{Int}(A) \cong A^\times/\mathrm{Z}(A)^\times$ であるから，この右辺の群の位数を計算すると，

(4.5) $|\mathrm{Int}(A)| = (3^m-1)\cdot 3^{2m}$

が分かる．$|k^\times| = 3^m-1$ であり，(4.3) が完全系列であることから $\mathrm{Aut}(A)_0$ の位数は $(3^m-1)^2\cdot 3^{2m}$ であることが分かる．これから従って，

(4.6) $|\mathrm{Aut}(A)| = 2\cdot(3^m-1)^2\cdot 3^{2m}$

が分かる．

k の標数が 3 以外の場合には，序文に述べた結果から計算出来る．すべてをまとめると次のようになる．

(4.7) k を位数 p^m をもつ有限体とし，A を k 係数の S_3 の群環とする．A の自己同型群 $\mathrm{Aut}(A)$の位数は

(i) $p \neq 2, 3$ の場合，$|\mathrm{Aut}(A)| = 2\cdot p^m\cdot(p^{2m}-1)$

(ii) $p=2$ の場合，$|\mathrm{Aut}(A)| = (2^m-1)\cdot 2^m\cdot(2^{2m}-1)$

(iii) $p=3$ の場合，$|\mathrm{Aut}(A)| = 2\cdot(3^m-1)^2\cdot 3^{2m}$

参考文献

[1] A. Borel, Linear Algebraic Groups Second Enlarged Edition, G.T.M. **126**, Springer-Verlag, 1991.

[2] J. E. Humphreys, Linear algebraic groups, G. T. M. **21**, Springer-Verlag, 1975.

[3] 太田友明・首藤武史，KS3 の自己同型群，Proceedings of Summer Seminar on Lie Algebras and Related Topics, **26**，26－29 (2010).

Some Generalizations of the BCH Bound

山口大学経済学部

柏木　芳美

1 はじめに

巡回符号という実用上重要な符号がある．その最小重さは BCH bound と呼ばれるもので評価される．それを改良した HT bound, Roos bound，Roos bound の変形を紹介する．

2 諸定義

- q を素数巾，$F = \mathrm{GF}(q)$ を位数 q の有限体，n を自然数とする．F^n の部分空間を長さ n の符号(code) という．基底が固定されていることに注意すること．

- C を次元が k で長さが n の符号とする．C の基底を行とする (k, n) 行列を C の生成行列という．

- $\mathbf{x} = (x_1, \cdots, x_n)$，$\mathbf{y} = (y_1, \cdots, y_n) \in F^n$ $(x_i,\ y_i \in F)$ に対して内積を

$$(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} x_i y_i$$

により定める．

C を符号としたとき，

$$C^{\perp} = \{\mathbf{x} \in F^n \mid (\mathbf{x}, \mathbf{u}) = 0 \text{ for } \mathbf{u} \in C\}$$

により C の双対符号 (dual code) を定める．$C^{\perp}$ の生成行列を C のパリティ検査行列(parity check matrix) という．

- $\mathbf{u} = (u_1, u_2, \cdots, u_n) \in F^n$ としたとき，

$$w(\mathbf{u}) = |\{i \in \{1, \cdots, n\} : u_i \neq 0\}|$$

を元 $\mathbf{u}$ の weight(重さ) という.

C を $\{\mathbf{0}\}$ とは異なる符号とする.

$$\min\{w(\mathbf{u}) \,|\, \mathbf{u} \in C \setminus \{\mathbf{0}\}\}$$

を C の最小重さといい,

$$d(C)$$

と書くことにする.

$\dim C$ は送信できる情報量を表し，大きければ大きいほどよい. $d(C)$ は訂正できる誤りの量を表し，これも大きければ大きいほどよい．一方，これらには，Singleton bound

$$d(C) \leqq n - \dim C + 1$$

というトレイドオフの関係がある.

- C を長さ n の符号とする．$(u_1, u_2, \cdots, u_n)$ が C の元ならその巡回シフト $(u_n, u_1, \cdots, u_{n-1})$ も C の元であるとき，C は巡回符号(cyclic code) と呼ばれる.

  巡回符号は剰余環 $F[x]/(x^n - 1)$ のイデアルと同じものである.

- 以下，$(n, q) = 1$ とする．このとき，$x^n - 1$ は重根を持たない. モニックな F 係数の多項式 $g(x)$ が $x^n - 1$ を割るとする．剰余環 $F[x]/(x^n - 1)$ において $g(x)$ の生成するイデアルは巡回符号になり，任意の巡回符号はこの形で得られる．この巡回符号は

  $$< g(x) >$$

と書かれ，$g(x)$ はこの巡回符号の生成多項式といわれる．

$$\dim <g(x)>= n - \deg g(x)$$

となる．尚，巡回符号の元は，$n-1$ 次以下の多項式として扱うこともあるし，1，x，x^2，$\cdots$，x^{n-1} $(\bmod (x^n-1))$ を基底とする行ベクトルとして扱うこともある．

- 巡回符号はその生成多項式を定めれば定まる．ところで生成多項式は x^n-1 を割るので，その根は1の n 乗根である．

  C を巡回符号とし，N を1の n 乗根からなる集合とする．C の元を多項式と見る．$u(x) \in C$ であるための必要十分条件がすべての N の元 α に対して $u(\alpha)=0$ であるとき，N は C を定めるあるいは C は N で定まるということにする．

- $g(x) \in F[x]$ を既約な多項式とする．α を1の原始 n 乗根の1つとする．α^l $(0 \leqq l \leqq n-1)$ が $g(x)$ の根ならば，$(\alpha^l)^q = \alpha^{lq}$ も $g(x)$ の根である．従って，$g(x)$ の根全体は

  $$\{\alpha^l, \alpha^{lq}, \alpha^{lq^2}, \alpha^{lq^3}, \cdots\}$$

  の形をしている．肩の

  $$\{l, lq, lq^2, lq^3, \cdots\}$$

  を cyclotomic coset という．ただし，modulo n で考えている．

  生成多項式を既約因子に分解する．各既約因子は適当な cyclotomic coset の集合に対応している．このように，cyclotomic coset の集合を指定すれば巡回符号は定まる．

例 1. この例 ([7, Roos, Example 1, 1983]) はこれ以降でも再三使う．$n = 21$，$q = 2$ とする．α を 1 の原始 21 乗根の 1 つとする．1，3，7，9 を含む cyclotomic cosets は

$$\{1, 2, 4, 8, 16, 11\}, \qquad \{3, 6, 12\}, \qquad \{7, 14\}, \qquad \{9, 15, 18\}$$

となる．i を $n - 1 = 20$ 以下の奇数かまたは 0 とする．α^i を根に持つ monic な既約多項式を $m_i(x)$ と書くことにする．上の cyclotomic cosets に対応する既約多項式は $m_1(x)$，$m_3(x)$，$m_7(x)$，$m_9(x)$ となる．

$$g(x) = m_1(x)m_3(x)m_7(x)m_9(x)$$

とおくと，$g(x)$ の根は

$$\{\alpha^i \mid i = 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 14, 15, 16, 18\} \tag{1}$$

となる．

$$C = < g(x) >$$

が今後具体例として扱う符号である． □

3 BCH bound

Bose と Ray-Chaudhuri([1, 1960]) および Hocquenghem([3, 1959]) は，巡回符号の最小重さに関する次の評価式を与えた．これは，最も基本的なものである．

命題 1 (BCH bound)**.** C を長さ n の巡回符号，$g(x)$ を C の生成多項式，α を 1 の原始 n 乗根の 1 つとする．b を自然数，δ を 2 以

上の自然数として，連続した $\delta-1$ 個の

$$\alpha^{b+i} \quad (0 \leqq i \leqq \delta-2)$$

が $g(x)$ の根ならば，C の最小重さは δ 以上である．この δ を C の designed distance と呼ぶことがある．

言葉 M を1の n 乗根からなる集合とし，b，l を自然数とする．

$$M=\{\alpha^{b+i}\,|\,0 \leqq i \leqq l\}$$

となる1の原始 n 乗根 α が存在するとき，M を(1の n 乗根の) consecutive set という．また，巡回符号 C の生成多項式 $g(x)$ の根全体の集合が M を含むとき，C は M を consecutive set に持つという． □

例 2. 例1の巡回符号 $C=<g(x)>$ を考える．式(1)より，$g(x)$ はある1の原始 n 乗根 α を用いて

$$\{\alpha^i\,|\,i=1,2,3,4,6,7,8,9,11,12,14,15,16,18\}$$

をすべての根とした．C は例えば

$$\{\alpha^i\,|\,i=1,2,3,4\}$$

を consecutive set に持つ($\delta=5$)．よって BCH bound より，$d(C) \geqq 5$ となる．

尚，

$$\{\alpha^i\,|\,i=6,7,8,9\}$$

も consecutive set であることを注意しておく． □

1 の原始 n 乗根の取り方を変えると，consecutive set は次のような形になる．

α，β を 1 の原始 n 乗根とする．$\alpha = \beta^{c_1}$ となる自然数 c_1 が存在するが，α が原始 n 乗根なので $(n, c_1) = 1$ となる．b，l を自然数とし $f = bc_1$ とおくと，α に関する consecutive set

$$\alpha^b, \qquad \alpha^{b+1}, \qquad \alpha^{b+2}, \qquad \cdots, \qquad \alpha^{b+l}$$

は β を用いて

$$\beta^{c_1 b} = \beta^f, \qquad \beta^{f+c_1}, \qquad \beta^{f+2c_1}, \qquad \ldots, \qquad \beta^{f+lc_1}$$

と書ける．また逆に，下の形の集合は，上の形の α に関する consecutive set になる．

原始 n 乗根の取り方を考慮して BCH bound を書き直すと次のようになる．

命題 2. C を長さ n の巡回符号，$g(x)$ を C の生成多項式，α を 1 の原始 n 乗根の 1 つとする．b を自然数，δ を 2 以上の自然数，c_1 を $(n, c_1) = 1$ となる自然数とする．

$$\alpha^{b+i_1 c_1} \quad (0 \leqq i_1 \leqq \delta - 2)$$

が $g(x)$ の根ならば，C の最小重さは δ 以上である．

4 HT bound

Hartmann と Tzeng は，命題 2 の形の BCH bound を次のように一般化した ([2, 1972]).

命題 3 (HT bound)**.** C を長さ n の巡回符号，$g(x)$ を C の生成多項式，α を1の原始 n 乗根の1つとする．b，s を自然数，δ を2以上の自然数とする．c_1 を $(n, c_1) = 1$ となる自然数とし，c_2 を $(n, c_2) < \delta$ となる自然数とする．このとき，

$$\alpha^{b+i_1c_1+i_2c_2} \quad (0 \leqq i_1 \leqq \delta - 2, \quad 0 \leqq i_2 \leqq s)$$

が $g(x)$ の根ならば，C の最小重さは $\delta + s$ 以上である．

例 3. 例2の巡回符号 C を考える．

$$\{\alpha^i \mid i = 1, 2, 3, 4\}, \qquad \{\alpha^i \mid i = 6, 7, 8, 9\}$$

は C の consecutive sets であった．命題3で

$$b = 1, \qquad c_1 = 1, \qquad c_2 = 5, \qquad \delta = 5, \qquad s = 1$$

として

$$b + i_1c_1 + i_2c_2 = 1 + i_1 + 5i_2 \qquad (0 \leqq i_1 \leqq 3, \quad 0 \leqq i_2 \leqq 1)$$

を考える．$i_2 = 0$ なら $1 + i_1$ は，1，2，3，4 になる．$i_2 = 1$ なら $6 + i_1$ は，6，7，8，9 になる．従って HT bound (命題 3) より，$d(C) \geqq \delta + s = 6$ となる．

BCH bound は5だったので改良されている． □

5 Roos bound

Roos は HT bound をさらに一般化した ([6, 1982]).

命題 4 (Roos bound)**.** C を長さ n の巡回符号，$g(x)$ を C の生成多項式，α を 1 の原始 n 乗根の 1 つとする．b，s_i を自然数 $(1 \leqq i \leqq k)$，δ を 2 以上の自然数とする．c_i $(1 \leqq i \leqq k)$ を $(n, c_1) = 1$，$(n, c_j) < 2 + s_1 + s_2 + \cdots + s_{j-1}$ $(2 \leqq j \leqq k)$ となる自然数とする．このとき，

$$\alpha^{b+i_1c_1+i_2c_2+\cdots+i_kc_k} \quad (0 \leqq i_t \leqq s_t\,(1 \leqq t \leqq k))$$

が $g(x)$ の根ならば，C の最小重さは

$$2 + s_1 + s_2 + \cdots + s_k$$

以上である．

注意. $\delta - 2 = s_1$ とすると $\delta = 2 + s_1$ である．

6 Roos bound の変形

Roos bound は，命題 4 の形では使いにくい面がある．Roos は [7, 1983] で少し形を変えた．次の記号を導入する．

m を multiplicative order of q modulo n とする ($q^m \equiv 1 \mod n$ となる最小の自然数)．$K = \mathrm{GF}(q^m)(\supset F = \mathrm{GF}(q))$ とおく．

$N = \{\alpha_1, \alpha_2, \cdots, \alpha_t\}$ を 1 の n 乗根からなる集合とする $(N \subset K)$．N に対し，

$$H_N = \begin{pmatrix} \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} & \alpha_1^n(=1) \\ \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} & \alpha_2^n(=1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_t & \alpha_t^2 & \cdots & \alpha_t^{n-1} & \alpha_t^n(=1) \end{pmatrix}$$

とおく．巡回符号 C が N で定められると，H_N は C のパリティ検査行列になる．

K 上の長さ n の符号 C_N を

$$C_N = \{\mathbf{u} \in K^n \,|\, H_N \mathbf{u}^t = \mathbf{0}\}$$

により定める．$\mathbf{u} = (u_1, u_2, \cdots, u_n) \in K^n$ $(u_k \in K)$ としたとき，

$$\sum_{k=1}^{n} \alpha_i^k u_k = 0 \iff \sum_{k=1}^{n} \alpha_i^{k+1} u_k = 0 \qquad (i = 1, 2, \cdots, t)$$

なので，C_N は巡回符号になる．

$d_N = d(C_N)$ とおく．巡回符号 C が N で定められているとすると，集合として $C \subset C_N$ なので，

$$d(C) \geqq d_N$$

に注意しておく．

以上の記号の下で Roos は次を示した ([7])．尚，M，N が 1 の n 乗根からなる集合ならば $MN = \{\alpha\beta \,|\, \alpha \in M, \beta \in N\}$ も 1 の n 乗根からなる集合である．

命題 5. M，N を 1 の n 乗根からなる空でない集合とする．このとき，$M \subset \bar{M}$ かつ $|\bar{M}| \leqq |M| + d_N - 2$ を満たす consecutive set $\bar{M}$ が存在すれば，$d_{MN} \geqq |M| + d_N - 1$ となる．

M が必ずしも consecutive でないことがポイントである．

N が consecutive ならば $d_N = |N| + 1$ であることが示される．従って，次が得られる．

系 6. N，M，$\bar{M}$ を命題 5 と同じとする．もし N が consecutive で $|\bar{M}| \leqq |M| + |N| - 1$ ならば $d_{MN} \geqq |M| + |N|$ となる．更に C が MN で定まる巡回符号ならば $d(C) \geqq |M| + |N|$ となる．

例 4. 今までの巡回符号 C を考える．

$$N = \{\alpha^i \,|\, i = 2, 3, 4\} = \{\alpha^2, \alpha^3, \alpha^4\},$$
$$M = \{\beta^j \,|\, j = 0, 1, 3, 5\} = \{1, \beta, \beta^3, \beta^5\} = \{1, \alpha^4, \alpha^{12}, \alpha^{20}\}$$

とする．ただし，$\beta = \alpha^4$ も 1 の原始 21 乗根である ($(21, 4) = 1$ より)．

$$\begin{aligned} MN &= N \cup \alpha^4 N \cup \alpha^{12} N \cup \alpha^{20} N \\ &= \{\alpha^2, \alpha^3, \alpha^4\} \cup \{\alpha^6, \alpha^7, \alpha^8\} \cup \{\alpha^{14}, \alpha^{15}, \alpha^{16}\} \cup \{\alpha, \alpha^2, \alpha^3\} \\ &= \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^7, \alpha^8, \alpha^{14}, \alpha^{15}, \alpha^{16}\} \end{aligned}$$

となる．

ここで，生成多項式 $g(x) = m_1(x)m_3(x)m_7(x)m_9(x)$ の根を考える．MN の元は $g(x)$ の根となっている．また，$\alpha = \alpha^1$，α^3，$\alpha^7 \in MN$ で，

$$9 \times 2^2 = 36 \equiv 15 \pmod{21}$$

より，$\alpha^{15} \in MN$ となっている．従って，MN で定まる巡回符号は $C = <g(x)>$ である．

次に系 6 を適用する．まず，$N = \{\alpha^i \,|\, i = 2, 3, 4\}$ は consecutive である．

$$\bar{M} = \{\beta^0, \beta^1, \beta^2, \beta^3, \beta^4, \beta^5\} (\supset M)$$

とすると $\bar{M}$ は consecutive である．また，

$$|\bar{M}| = 6 \leqq 4 + 3 - 1 = |M| + |N| - 1$$

となっている．従って，系 6 より

$$d(C) \geqq |M| + |N| = 7$$

となる． □

7 まとめ

巡回符号の最小重さを評価する BCH bound，HT bound，Roos bound および Roos bound を少し変形したものを簡単に紹介した．具体例の巡回符号 C の最小重さの評価は

$$\text{BCH bound} : d(C) \geqq 5,$$
$$\text{HT bound} : d(C) \geqq 6,$$
$$\text{Roos bound の変形} : d(C) \geqq 7$$

と，段々と良い評価が得られている．尚，この例の実際の最小重さは

$$d(C) = 8$$

となることが知られている ([4, Peterson and Weldon, 1972]).

また，$x^n - 1$ を $x^n - a$ $(a \in F \setminus \{0\})$ に変えた符号は constacyclic code と呼ばれるが，今まで述べてきたこととほぼ同様のことが成り立つことが知られている ([5, Radkova and Van Zanten, 2009]).

参考文献

[1] R. C. Bose and D. K. Ray-Chaudhuri, On a class of error-correcting binary group codes, Inform. Contr. 3, pp.68–79, 1960.

[2] C. R. P. Hartmann and K. K. Tzeng, Generalizations of the BCH-bound, Inform. Contr. 20, pp.489–498, 1972.

[3] A. Hocquenghem, Codes correcteurs d'erreurs, Chiffres (Paris) 2, pp.147–156, 1959.

[4] W. W. Peterson and E. J. Weldon, JR., Error-Correcting Codes, 2nd ed., MIT Press, Cambridge, Mass., 1972.

[5] D. Radkova and A. J. Van Zanten, Constacyclic codes as invariant subspaces, Linear Alg. and Its Applic. 430, pp.855–864, 2009.

[6] C. Roos, A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound, J. Comb. Theory Ser. A 33, pp.229–232, 1982.

[7] C. Roos, A new lower bound for the minimum distance of a cyclic code, IEEE Trans. Inform. Theory 29, pp.330–332, 1983.

極小局所アフィンリー代数について

秋田工業高等専門学校

吉 井　洋 二

（筑波大学 森田純 教授との共同研究）

F を標数 0 の体とする。また、$\otimes$ はすべて F 上のテンソル積とする。

F 上のリー代数 $\mathcal{L}$ とその部分代数 $\mathcal{H}$ に関して、

$$\mathcal{L} = \bigoplus_{\xi \in \mathcal{H}^*} \mathcal{L}_\xi$$

なる分解をもつとき、$\mathcal{L}$ は $\mathcal{H}$ に関して**ルート空間分解**（root space decomposition）をもつという。但し、$\mathcal{H}^*$ は $\mathcal{H}$ の双対空間を表し、$\mathcal{L}_\xi$ は、

$$\mathcal{L}_\xi = \{x \in \mathcal{L} \mid [h, x] = \xi(h)x \text{ for all } h \in \mathcal{H}\}$$

とする。このとき $\mathcal{H}$ は**可換になる**。また、集合

$$R = \{\xi \in \mathcal{H}^* \mid \mathcal{L}_\xi \neq 0\}$$

の要素を**ルート**（root）と呼ぶ。

$\mathcal{B}$ を $\mathcal{L}$ 上の対称不変双一次形式（symmetric invariant bilinear form）とするとき、次の 4 つの公理を満たすリー代数を**局所拡大アフィンリー代数**（locally extended affine Lie algebra）という。以下、略して **LEALA** と呼ぶ。

(1) $\mathcal{H}$ は自己中心的（self-centralizing）、即ち $\mathcal{L}_0 = \mathcal{H}$

(2) $\mathcal{B}$ は非退化（nondegenerate）

(3) 任意の要素 $\xi \in R^\times$ と $x \in \mathcal{L}_\xi$ に対して $\mathrm{ad}x \in \mathrm{End}_F\mathcal{L}$ は局所巾零（locally nilpotent）

(4) $R^\times$ は既約（irreducible）、即ち、

$$R^\times = R_1 \cup R_2 \text{ and } (R_1, R_2) = 0 \implies R_1 = \emptyset \text{ or } R_2 = \emptyset.$$

但し、$R^\times$ と (R_1, R_2) の括弧の意味は以下の通りである。まず公理 (1) と (2) から任意の $\xi \in R$ に対して $\mathcal{B}|_{\mathcal{L}_\xi \times \mathcal{L}_{-\xi}}$ が非退化になる。特に $\mathcal{B}|_{\mathcal{H}\times\mathcal{H}}$ も非退化になるので、

$$\mathcal{B}(h, t_\xi) = \xi(h) \quad \text{for all } h \in \mathcal{H}$$

となる $t_\xi \in \mathcal{H}$ が一意的に定まる。この t_ξ を通して、R で張られる F 上のベクトル空間に対称双一次形式 $(\ ,\ )$ を次のように定義することができる：

$$(\xi, \eta) := \mathcal{B}(t_\xi, t_\eta) \quad \text{for } \xi, \eta \in R$$

そこで $R^\times$ を

$$R^\times := \{\xi \in R \mid (\xi, \xi) \neq 0\}$$

と定義する。

２つの LEALA $(\mathcal{L}, \mathcal{H}, \mathcal{B})$ と $(\mathcal{L}', \mathcal{H}', \mathcal{B}')$ が**同型**であるとは、リー代数としての同型写像 $\varphi : \mathcal{L} \to \mathcal{L}'$ が存在して $\varphi(\mathcal{H}) = \mathcal{H}'$ と $\mathcal{B}'\big(\varphi(x), \varphi(y)\big) = \mathcal{B}(x, y)$ （for all $x, y \in \mathcal{L}$）が成り立つことである。

局所拡大アフィンリー代数の特別なクラスとして、$\mathcal{H}$ が有限次元の場合を**拡大アフィンリー代数**（extended affine Lie algebra）という。以下、略して **EALA** と呼ぶ（[Ne] 参照)。

また、$R^\times = \emptyset$ の場合もあるわけだが、この場合、公理 (3) と (4) の主張は空となる。$R^\times \neq \emptyset$ を公理に入れた方が便利な場合も多いが、我々は、$R^\times = \emptyset$ の場合を **isotropic LEALA** と名付けている。もちろん $\mathcal{H}$ が有限次元ならば **isotropic EALA** と呼べばよい。Heisengerg リー代数にその微分作用素を付け加えてできる oscillator 代数などは isotropic EALA の例となる。筆者が知る限り、まだ誰も isotropic EALA の分類を始めていない。

本ノートでは $R^\times \neq \emptyset$ を仮定する。このとき、$R^\times$ の性質を使って、

$$(\xi, \eta) \in \mathbb{Q} \quad \text{for all } \xi, \eta \in R$$

となるように $(\ ,\ )$ をスカラー倍調整することができる。このとき、$\mathcal{L}$ が EALA ならば、$(\ ,\ )$ は R で張られる $\mathbb{Q}$ 上のベクトル空間 V で**半正定値**（positive semidefinite）になると Kac が予想し、[AABGP] で肯定的に証明された。この定理の拡張として、$\mathcal{L}$ が LEALA でも $(\ ,\ )$ が半正定値になることが、[MY1] において証明された。さらに、$R^\times$ で張られる $\mathbb{Q}$ 上のベクトル空間において、$R^\times$ は**局所拡大アフィンルート系**（locally extended affine root system）になることがわかった。このルート系は、通常の**有限既約ルート系**（finite irreducible root system)、**局所有限既約ルート系**（locally finite irreducible root system）[LN]、Macdonald の**アフィンルート系**（affine root system）[M]（または [A] 参照)、そして斎藤恭司先生の**拡大アフィンルート系**（extended affine root system）[S] を自然に拡張した概念である（[Y] 参照)。

ここで LEALA $\mathcal{L}$ に対して、nullity、core そして tame という概念を定義する。まず、

$$R^0 := \{\xi \in R \mid (\xi, \xi) = 0\}$$

で生成される V の加法的部分群が自由（free）のとき、そのランクを **nullity** と呼ぶ。従って例えば nullity 1 と言えば、その加法群は $\mathbb{Z}$ に同型ということである。次に、

$$\mathcal{L}_\xi \quad \text{for all } \xi \in R^\times$$

で生成される $\mathcal{L}$ の部分代数を $\mathcal{L}$ の **core** と呼び、$\mathcal{L}_c$ で表す。このとき、$\mathcal{L}_c$ は $\mathcal{L}$ のイデアルになることがわかる。さらに、$\mathcal{L}_c$ の $\mathcal{L}$ での centralizer が $\mathcal{L}_c$ に含まれるとき、$\mathcal{L}$ は **tame** であるという。

tame EALA の分類はほぼ完成したといってよいが（[Ne] 参照）、LEALA についてはまだ始まったばかりである。最も簡単な場合、即ち、$R^0 = \{0\}$ の場合、別の言葉でいえば nullity 0 の場合であるが、これは [MY1] において分類された。

大雑把にいうと、tame LEALA of nullity 0 は、**有限次元スプリット単純リー代数**（finite-dimensional split simple Lie algebra）を包含するクラス、**局所有限スプリット単純リー代数**（locally finite split simple Lie algebra）[NS]（または [St] 参照）、さらにこれに無限対角行列を付け加えてできる新しいタイプのリー環に分類できる。tame でないものは、これらにさらに split center を付け加えただけとなることも証明された。

かくして次のターゲットは nullity 1 となる。そこで nullity 1 の tame LEALA を**局所アフィンリー代数**（locally affine Lie algebra）ということにする。以下、略して **LALA** と呼ぶ。LALA のルート系は**局所アフィンルート系**（locally affine root system）と呼ばれ、[Y] で分類された。LALA は**アフィンリー代数**（affine Lie algebra）、別名、**ユークリッド代数**（euclidean Lie algebra）[Mo] を含むクラスである。また、LALA の特別なクラスである tame EALA of nullity 1 はアフィンリー代数に他ならないことが [ABGP] で証明されている。

ここでは、アフィンリー代数ではない、最も簡単といえる LALA を紹介する。まず、$\mathrm{gl}_{\mathbb{N}}(F)$ を、サイズが $\mathbb{N}$ で、有限個以外の成分がすべて 0 の無限次正方行列全体が作るリー代数とし、その部分代数

$$\mathrm{sl}_{\mathbb{N}}(F) = \{x \in \mathrm{gl}_{\mathbb{N}}(F) \mid \mathrm{tr}(x) = 0\}$$

を考える。これは局所有限スプリット単純リー代数の最も簡単な例といってよい。ここで、$\mathfrak{h}$ を対角行列全体からなる $\mathrm{sl}_{\mathbb{N}}(F)$ の可換部分代数とし、T を（$\mathfrak{h}$ を含む）サイズ $\mathbb{N}$ の対角行列全体からなる可換リー代数とする。また、$\iota \in T$ を対角成分がすべて 1 の対角行列とする。特に $\iota \notin \mathrm{gl}_{\mathbb{N}}(F)$ に注意せよ。このとき、

$$p \notin \mathfrak{h} \oplus F\iota$$

を満たす対角行列 $p \in T$ を考える。たとえば

$$p = \begin{pmatrix} 1 & 0 & 0 & \\ 0 & 2 & 0 & \\ 0 & 0 & 3 & \\ \vdots & & & \ddots \end{pmatrix}$$

なる無限対角行列のこともあるし、$p \in \mathrm{gl}_{\mathbb{N}}(F) \setminus \mathrm{sl}_{\mathbb{N}}(F)$ のこともある。たとえば、(i,i) 成分だけが 1 で他成分がすべて 0 の (i,i)-行列単位（matrix unit）e_{ii} を p としてもよい。

さて、どんな対角行列も $\mathrm{gl}_{\mathbb{N}}(F)$ に微分作用素として働く（ブラケットが定義できる）ので

$$A := \mathrm{sl}_{\mathbb{N}}(F) \oplus Fp$$

は自然にリー代数となる。双一次形式 $\mathcal{B}$ を

$$\mathcal{B}(x,y) := \mathrm{tr}(xy) \quad \text{for } x \in \mathrm{sl}_{\mathbb{N}}(F) \text{ and } y \in A$$

のように定義すれば、$\mathcal{B}(p,p)$ をどのように定めても $\mathcal{B}$ は A 上非退化になる。

ここで

$$H := \mathfrak{h} \oplus Fp$$

とすると $(A, H, \mathcal{B})$ は tame LEALA of nullity 0 の例となる。この三つ組みを拡張して LALA を構成する。まず、L を A のループ代数（loop algebra）

$$L := A \otimes F[t^{\pm 1}]$$

とし、$x \otimes t^m \in \mathrm{sl}_{\mathbb{N}}(F) \otimes F[t^{\pm 1}]$ と $y \otimes t^n \in L$ に対して、$\mathcal{B}$ を

$$\mathcal{B}(x \otimes t^m, y \otimes t^n) := \mathrm{tr}(xy)\delta_{m+n,0} \quad \text{and} \quad \mathcal{B}(p \otimes t^m, p \otimes t^n) := 0 \tag{1}$$

のように拡張する。次に L の 1 次元中心拡大 $L \oplus Fc$ を、$\mathcal{B}$ を使って次のブラケットで定義する：

$$[x \otimes t^m, y \otimes t^n] := [x,y] \otimes t^{m+n} + \mathcal{B}(d_0(x \otimes t^m), y \otimes t^n)c \tag{2}$$

但し、

$$d_0 = 1 \otimes t\frac{d}{dt}$$

であり、これは次数を掛ける作用といってよい。従って、

$$\mathcal{B}(d_0(x \otimes t^m), y \otimes t^n) = m\mathcal{B}(x \otimes t^m, y \otimes t^n) = m\mathrm{tr}(xy)\delta_{m+n,0}$$

に他ならないが、$\mathcal{B}(d_0(\quad), \quad)$ という形は、これが 2-cocyle になるという一般論が使えるので、(2) がリー代数の中心拡大であることがすぐにわかるという利点をもつ。

最後に、d_0 の自然な作用を L とのブラケット、即ち

$$[d_0, x\otimes t^m] = mx\otimes t^m = \quad [x\otimes t^m, d_0]$$

とし、

$$[c, d_0] = [d_0, c] = 0$$

とすることで、

$$\mathcal{L}(p) := L \oplus Fc \oplus Fd_0$$

はリー代数となる。さらに、$\mathcal{B}$ を

$$\mathcal{B}(c,c) = \mathcal{B}(d_0,d_0) = \mathcal{B}(c,L) = \mathcal{B}(d_0,L) = 0 \quad \text{and} \quad \mathcal{B}(c,d_0) = 1 \tag{3}$$

のように拡張すれば、$\mathcal{B}$ は非退化対称不変双一次形式となる。そこで

$$\mathcal{H} := H \oplus Fc \oplus Fd_0$$

とすれば $\mathcal{L}(p) = \big(\mathcal{L}(p), \mathcal{H}, \mathcal{B}\big)$ は LALA となる。

$\mathcal{L}(p)$ の部分代数の中で、

$$\mathcal{L}^{ms} := \big(\mathrm{sl}_{\mathbb{N}}(F)\otimes F[t^{\pm1}]\big) \oplus Fc \oplus Fd_0 \quad \text{and} \quad \mathcal{H}^{ms} := \mathfrak{h} \oplus Fc \oplus Fd_0$$

$$\mathcal{L}_1(p) := \big(\mathrm{sl}_{\mathbb{N}}(F)\otimes F[t^{\pm1}]\big) \oplus Fc \oplus F(p+d_0) \quad \text{and} \quad \mathcal{H}_1 := \mathfrak{h} \oplus Fc \oplus F(p+d_0)$$

$$\mathcal{L}_2(p) := \big(\mathrm{sl}_{\mathbb{N}}(F)\otimes F[t^{\pm1}]\big) \oplus Fc \oplus Fp \oplus Fd_0 \quad \text{and} \quad \mathcal{H}_2 := \mathfrak{h} \oplus Fc \oplus Fp \oplus Fd_0$$

なども LALA であることが証明できる。またこれら $\mathcal{L}(p)$, $\mathcal{L}^{ms}$, $\mathcal{L}_1(p)$, $\mathcal{L}_2(p)$ すべての core は一致して

$$\mathcal{L}_c := \big(\mathrm{sl}_{\mathbb{N}}(F)\otimes F[t^{\pm1}]\big) \oplus Fc$$

になることも証明できる。

アフィンリー代数同様、この core $\mathcal{L}_c$ は $\mathrm{sl}_{\mathbb{N}}(F)\otimes F[t^{\pm1}]$ の**普遍中心拡大**（universal central covering）になっていることを注意しておく（[MY2] 参照）。

一般に、LALA $\mathcal{L}$ の core $\mathcal{L}_c$ が $\mathcal{L}$ で超平面（hyperplane of codimension 1）のとき、$\mathcal{L}$ を**極小**という。上の例では、$\mathcal{L}^{ms}$ も $\mathcal{L}_1(p)$ も**極小** LALA である。また、LALA $\mathcal{L}$ が d_0 を含むとき**標準**という。上の例では、$\mathcal{L}(p)$, $\mathcal{L}^{ms}$, $\mathcal{L}_2(p)$ は標準であるが、$\mathcal{L}_1(p)$ は標準ではない。

特に $\mathcal{L}^{ms}$ は**極小標準 LALA**（minimal standard LALA）といえる。また、$\mathcal{L}^{ms}$ における $\mathbb{N}$ を $n+1$ に変えれば、いわゆる $\mathrm{A}_n^{(1)}$ 型アフィンリー代数のことである。

実はこのあと、$\mathcal{L}^{ms}$ と $\mathcal{L}_1(e_{ii})$ などは LALA として同型になることを示すが、たとえば、p を

$$\begin{pmatrix} 1 & 0 & 0 & \\ 0 & \frac{1}{2} & 0 & \\ 0 & 0 & \frac{1}{3} & \\ \vdots & & & \ddots \end{pmatrix}$$

のように、対角成分が $\frac{1}{n}$ であるような行列にすると、極小標準 LALA に同型でないことが証明できる。

さて、以下が極小 LALA が極小標準 LALA に同型となる 1 つの十分条件である。

補題 1　上記 $LALA$ $\mathcal{L}(p)$ において、対角行列 p の成分がすべて整数ならば、$\mathcal{L}(p)$ の部分リー代数

$$\mathcal{L}_1(p) = \big(\mathrm{sl}_{\mathbb{N}}(F) \otimes F[t^{\pm 1}]\big) \oplus Fc \oplus F(d_0 + p)$$

は極小標準 $LALA$ $\mathcal{L}^{ms}$ に $LALA$ として同型である。

証明）　まず

$$p = \begin{pmatrix} m_1 & 0 & 0 & \\ 0 & m_2 & 0 & \\ 0 & 0 & m_3 & \\ \vdots & & & \ddots \end{pmatrix} \quad \text{for } m_1, m_2, m_3, \ldots \in \mathbb{Z}$$

とし、

$$g := \sum_{i \in \mathbb{N}} e_{ii} \otimes t^{m_i} \quad \text{and} \quad g^{-1} = \sum_{i \in \mathbb{N}} e_{ii} \otimes t^{-m_i}$$

を考える。また、

$$\mathcal{M} := \big(\mathrm{gl}_{\mathbb{N}}(F) + T\big) \otimes F[t^{\pm 1}]$$

は通常の行列の積で $\iota \otimes 1$ を単位元とする結合代数となる。特に $\mathcal{M}$ は $F[t^{\pm 1}]$ 成分の対角行列か、対角でなければ有限個の成分以外すべて 0 の行列全体と考えてよい。たとえば

$$g = \begin{pmatrix} t^{m_1} & 0 & 0 & \\ 0 & t^{m_2} & 0 & \\ 0 & 0 & t^{m_3} & \\ \vdots & & & \ddots \end{pmatrix} \quad \text{and} \quad g^{-1} = \begin{pmatrix} t^{-m_1} & 0 & 0 & \\ 0 & t^{-m_2} & 0 & \\ 0 & 0 & t^{-m_3} & \\ \vdots & & & \ddots \end{pmatrix}$$

のように行列と考えて計算した方が分かり易い。さらに trace も定義できて、例えば任意の行列 $X \in \mathrm{gl}_{\mathbb{N}}(F[t^{\pm 1}]) = \mathrm{gl}_{\mathbb{N}}(F) \otimes F[t^{\pm 1}]$ に対して $\mathrm{tr}(g^{-1}Xg) = \mathrm{tr}(X)$ などは成立する。ここで $\mathrm{tr}(X) \in F[t^{\pm 1}]$ だが、

$$\mathrm{tr}_0(X) := \begin{cases} \mathrm{tr}(x) & \text{if } X = x \otimes 1 \\ 0 & \text{if } X = x \otimes t^m \text{ for } m \neq 0 \end{cases}$$

とおけば、任意の $X \in L = A \otimes F[t^{\pm 1}]$ と $Y \in \mathrm{sl}_{\mathbb{N}}(F) \otimes F[t^{\pm 1}]$ に対して、

$$\mathcal{B}(X, Y) = \mathrm{tr}_0(XY)$$

となる。さて、$X \in L$ に対して、

$$\theta_g(X) := g^{-1}Xg$$

と定義する。このとき、$Y \in \mathrm{sl}_{\mathbb{N}}(F) \otimes F[t^{\pm 1}]$ に対して、

$$\mathcal{B}\big(\theta_g(X), \theta_g(Y)\big) = \mathcal{B}\big(g^{-1}Xgg^{-1}Yg\big) = \mathrm{tr}_0(g^{-1}XYg) = \mathrm{tr}_0(XY) = \mathcal{B}(X,Y)$$

が成り立つから、θ_g が対角行列を固定することを考慮すれば、任意の $X, Y \in L$ に対して

$$\mathcal{B}\big(\theta_g(X), \theta_g(Y)\big) = \mathcal{B}(X,Y) \tag{4}$$

が成り立つ。

ここで、$X, Y \in \mathrm{sl}_{\mathbb{N}}(F) \otimes F[t^{\pm 1}]$ に対して、$\mathcal{L}_c = \mathrm{sl}_{\mathbb{N}}(F) \otimes F[t^{\pm 1}] \oplus Fc$ でのブラケットを $[\,,\,]^{\sim}$ と書くことにする。まず、θ_g が $\mathcal{L}_c$ まで拡張できたとする。詳しく述べると、

$$\tilde{\theta}_g(X) = \theta_g(X) + a_X c \qquad (a_X \in F)$$

を満たす自己同型写像 $\tilde{\theta}_g : \mathcal{L}_c \ \to \mathcal{L}_c$ と線形形式

$$a : \mathrm{sl}_{\mathbb{N}}(F) \otimes F[t^{\pm 1}] \ \to F$$

が存在したとする。このとき、

$$\tilde{\theta}_g([X,Y]^{\sim}) = \tilde{\theta}_g\big([X,Y] + \mathcal{B}\big(d_0(X), Y\big)c\big) = \theta_g\big([X,Y]\big) + a_{[X,Y]}c + \mathcal{B}\big(d_0(X), Y\big)\tilde{\theta}_g(c)$$

となる。一方、

$$[\tilde{\theta}_g(X), \tilde{\theta}_g(Y)]^{\sim} = [\theta_g(X), \theta_g(Y)]^{\sim} = [\theta_g(X), \theta_g(Y)] + \mathcal{B}\big(d_0(\theta_g(X)), \theta_g(Y)\big)c$$

となる。ここで、$\theta_g\big([X,Y]\big) = [\theta_g(X), \theta_g(Y)]$ は成り立つので、

$$a_{[X,Y]}c + \mathcal{B}\big(d_0(X), Y\big)\tilde{\theta}_g(c) = \mathcal{B}\big(d_0(\theta_g(X)), \theta_g(Y)\big)c$$

となる線形形式 a を見つけたい。簡単な行列計算を行うと、

$$\mathcal{B}\big((d_0 + \mathrm{ad}\, p)(\theta_g(X)), \theta_g(Y)\big) = \mathcal{B}\big(d_0(X), Y\big)$$

なる等式に気づくので

$$a_X := \quad \mathcal{B}\big(p, \theta_g(X)\big) \tag{5}$$

と置いてみると、

$$a_{[X,Y]} = \quad \mathcal{B}\big(p, \theta_g([X,Y])\big)\big) = \quad \mathcal{B}\big([p, \theta_g(X)], \theta_g(Y)\big) = \quad \mathcal{B}\big(\,\mathrm{ad}\, p(\theta_g(X)), \theta_g(Y)\big)$$

となる。従って、

$$\tilde{\theta}_g(c) = c$$

と決めることで

$$\tilde{\theta}_g([X,Y]^\sim) = [\tilde{\theta}_g(X), \tilde{\theta}_g(Y)]^\sim$$

を得る。よって a を (5) によって定義すれば、θ_g は $\mathcal{L}_c$ まで拡張できたことになる。

さらに、$\mathcal{L}$ への拡張をまた $\tilde{\theta}_g$ と書くことにする。$\tilde{\theta}_g$ が同型写像になるように d_0 の行き先を決めたいわけだが、

$$\tilde{\theta}_g(d_0) := d_0 + p$$

と定めればよいことがわかる。実際、e_{ij} を (i,j)-行列単位とすれば、

$$\tilde{\theta}_g([d_0, e_{ij} \otimes t^k]) = k\theta_g(e_{ij} \otimes t^k) = ke_{ij} \otimes t^{k-m_i+m_j}$$

であり、

$$\begin{aligned}
[\tilde{\theta}_g(d_0), \tilde{\theta}_g(e_{ij} \otimes t^k)] &= [d_0 + p, e_{ij} \otimes t^{k-m_i+m_j}] \\
&= (k \quad m_i + m_j + m_i \quad m_j)e_{ij} \otimes t^{k-m_i+m_j} \\
&= ke_{ij} \otimes t^{k-m_i+m_j}
\end{aligned}$$

となるから

$$\tilde{\theta}_g([d_0, e_{ij} \otimes t^k]) = [\tilde{\theta}_g(d_0), \tilde{\theta}_g(e_{ij} \otimes t^k)]$$

が成り立つ。従って $\tilde{\theta}_g$ は同型となり、$\tilde{\theta}_g$ の定義から $\tilde{\theta}_g(\mathcal{H}^{ms}) = \mathcal{H}_1$ もよい。また、$\mathcal{B}$ について、(1) そして (4)、さらに (3) を思い出せば、任意の $X, Y \in \mathcal{L}^{ms}$ に対して $\mathcal{B}\big(\tilde{\theta}_g(X), \tilde{\theta}_g(Y)\big) = \mathcal{B}(X,Y)$ となる。故に $\mathcal{L}_1(p)$ は極小標準 LALA に LALA として同型となる。□

注意 1　実は $\mathcal{L}_c$ は普遍中心拡大なので、θ_g を $\mathcal{L}_c$ まで拡大できることは保証されている（たとえば [MP] 参照)。従って、$\tilde{\theta}_g(d_0)$ をうまく定義できるかどうかが本質的問題となる。

例えば、$p = e_{ii}$ は補題 1 の条件を満たしているが、今のところ、$\mathcal{L}_1\big(\frac{1}{2}e_{ii}\big)$ などが極小標準 LALA に同型かどうか判っていない。

最近の Neeb の論文 [N] において、LALA の core は分類され、$\mathbb{C}$ 上の極小標準 LALA のユニタリー表現が研究されている。一般の LALA の分類については、[MY2] で詳しく論じられる。

参考文献

[A] S. Azam, *Extended affine root systems*, J. Lie Theory, no. 2, **12** (2002), 515–527.

[AABGP] B. Allison, S. Azam, S. Berman, Y. Gao and A. Pianzola, *Extended affine Lie algebras and their root systems*, Mem. Amer. Math. Soc. 126 (1997), no. 603.

[ABGP] B. Allison, S. Berman, Y. Gao, A. Pianzola *A characterization of affine Kac-Moody Lie algebras*, Commun. Math. Phys., **185** (1997) 671–688.

[LN] O. Loos, E. Neher, *Locally finite root systems*, Memoirs Amer. Math. Soc., **811** vol.171 (2004).

[M] M. Macdonald, *Affine root systems and Dedekind's η-functions*, J. Invent. Math., **15** (1972), 91–143.

[Mo] R. Moody, *Euclidean Lie algebras*, Can. J. Math., **21** (1969), 1432-1454.

[MP] R. Moody, A. Pianzola, *Lie algebras with triangular decompositions*, Can. Math. Soc. Series of Monographs and Advanced Texts, John Wiley (1995).

[MY1] J. Morita and Y. Yoshii, *Locally extended affine Lie algebras*, J. Algebra 301 (2006), 59–81.

[MY2] J. Morita and Y. Yoshii, *Locally loop algebras and locally affine Lie algebras*, under preparation.

[N] K.-H. Neeb, *Unitary highest weight modules of locally affine Lie algebras*, Quantum affine algebras, extended affine Lie algebras, and their applications,. Contemp. Math., 506, Amer. Math. Soc., Providence, RI (2010), 227–262.

[Ne] E. Neher, *Extended affine Lie algebras*, C. R. Math. Acad. Sci. Soc. R. Can. **26** (2004), no. 3, 90–96.

[NS] K.-H. Neeb, N. Stumme, *The classification of locally finite split simple Lie algebras*, J. reine angew. Math., **533** (2001), 25–53.

[S] K. Saito, *Extended affine root systems 1 (Coxeter transformations)*, RIMS., Kyoto Uviv. **21** (1985), 75–179.

[St] N. Stumme, *The structure of locally finite split Lie algebras*, J. Algebra **220** (1999), 664–693.

[Y] Y. Yoshii, *Locally extended affine root systems*, Proc. on Quantum Affine Algebras, Extended Affine Lie Algebras and Applications, Contemp. Math., **508** (2010), 285–302.

GENERALIZATIONS OF THE CONCEPT OF CYCLICITY OF CODES

MANABU MATSUOKA

Abstract. In this paper we generalize the notion of cyclicity of codes, that is, polycyclic codes and sequential codes. We study the relation between polycyclic codes and sequential codes over finite commutative QF rings. Furthermore, we characterized the family of some constacyclic codes.

1. Introduction

In [6], S. R. López-Permouth, B. R. Parra-Avila and S. Szabo studied the duality between polycyclic codes and sequential codes. By the way, J. A. Wood establish the extension theorem and MacWilliams identities over finite frobenius rings in [9]. M. Greferath and M. E. O'Sullivan study bounds for block codes on finite frobenius rings in [2]. In this paper, we generalize the result of [6] to codes with finite commutative QF rings.

In section 2 we define polycyclic codes over finite commutative rings. And we study the properties of polycyclic codes. In section 3 we define sequential codes and consider the properties of sequential codes. In section 4 we study the relation between polycyclic codes and sequential codes over finite commutative QF rings. And we characterized the family of some constacyclic codes.

Throughout this paper, R denotes a finite commutative ring with $1 \neq 0$, n denotes a natural number with $n \geq 2$, unless otherwise stated.

2. Polycyclic codes

A linear $[n, k]$-code over a finite commutative ring R is a submodule $C \subseteq R^n$ of rank k. We define polycyclic codes over a finite commutative ring.

Definition 1. *Let C be a linear code of length n over R. C is a polycyclic code induced by c if there exists a vector $c = (c_0, c_1, \cdots, c_{n-1}) \in$*

2010 Mathematics Subject Classification: Primary 94B60; Secondary 94B15.
Key words and phrases: finite rings, (θ, δ)-codes, skew polynomial rings.
The detailed version of this paper will be submitted for publication elsewhere.

R^n such that for every $(a_0, a_1, \cdots, a_{n-1}) \in C$, $(0, a_0, a_1, \cdots, a_{n-2}) + a_{n-1}(c_0, c_1, \cdots, c_{n-1}) \in C$. In this case we call c an associated vector of C.

As cyclic codes, polycyclic codes may be understood in terms of ideals in quotient rings of polynomial rings. Given $c = (c_0, c_1, \cdots, c_{n-1}) \in R^n$, if we let $f(X) = X^n - c(X)$, where $c(X) = c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ then the R-module homomorphism $\rho : R^n \to R[X]/(f(X))$ sending the vector $a = (a_0, a_1, \cdots, a_{n-1})$ to the equivalence class of polynomial $\overline{a_{n-1}X^{n-1} + \cdots + a_1X + a_0}$, allows us to identify the polycyclic codes induced by c with the ideal of $R[X]/(f(X))$.

Definition 2. *Let C be a polycyclic code in $R[X]/(f(X))$. If there exist monic polynomials g and h such that $\rho(C) = (g)/(f)$ and $f = hg$, then C is called a principal polycyclic code.*

Proposition 1. *A code $C \subseteq R^n$ is a principal polycyclic code induced by some $c \in C$ if and only if C is a free R-module and has a $k \times n$ generator matrix of the form*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}$$

with an invertible g_{n-k}. In this case

$$\rho(C) = \left(\overline{g_{n-k}X^{n-k} + \cdots + g_1X + g_0}\right)$$

is the ideal of $R[X]/(f(X))$.

Definition 3. *Let $C = (g)/(f) \subseteq R[X]/(f(X))$ be a principal polycyclic code. If the constant term of g is invertible, then C is called a principal polycyclic code with an invertible constant term.*

For a $c = (c_0, c_1, \cdots, c_{n-1}) \in R^n$, let D_c be the following square matrix;

$$D_c = \begin{pmatrix} 0 & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \\ c_0 & c_1 & \cdots & c_{n-1} \end{pmatrix}.$$

It follows that a code $C \subseteq R^n$ is polycyclic with an associated vector $c \in R^n$ if and only if it is invariant under right multiplication by D_c.

3. Sequential codes

Definition 4. *Let C be a linear code of length n over R. C is a sequential code induced by c if there exists a vector $c = (c_0, c_1, \cdots, c_{n-1}) \in R^n$ such that for every $(a_0, a_1, \cdots, a_{n-1}) \in C$, $(a_1, a_2, \cdots, a_{n-1}, a_0c_0 + a_1c_1 + \cdots + a_{n-1}c_{n-1}) \in C$. In this case we call c an associated vector of C.*

Let C be a sequential code with an associated vector $c = (c_0, c_1, \cdots, c_{n-1})$. Then C is invariant under right multiplication by the matrix

$$ {}^tD_c = \begin{pmatrix} 0 & & 0 & c_0 \\ 1 & & & c_1 \\ & \ddots & & \vdots \\ 0 & & 1 & c_{n-1} \end{pmatrix} $$

On R^n define the standard inner product by

$$< x, y >= \sum_{i=0}^{n-1} x_i y_i$$

for $x = (x_0, x_1, \cdots, x_{n-1})$, $y = (y_0, y_1, \cdots, y_{n-1}) \in R^n$.

The dual code $C^\perp$ of a linear code C is defined by

$$C^\perp = \{a \in R^n | < c, a >= 0 \text{ for any } c \in C\}.$$

Clearly, $C^\perp$ is a linear code over R.

Theorem 1. *For a code $C \subseteq R^n$, we have the following assertions:*
(1) *If C is polycyclic, then $C^\perp$ is sequential.*
(2) *If C is sequential, then $C^\perp$ is polycyclic.*

4. Codes over finite commutative QF rings

Let R be a (not necessarily commutative) ring. A left R-module P is projective if for every R-epimorphism $g : M \to N$ and every R-homomorphism $f : P \to N$, there exists a R-homomorphism $h : P \to M$ with $f = g \circ h$.

A left R-module Q is injective if for every R-monomorphism $g : N \to M$ and every R-homomorphism $f : N \to Q$, there exists a R-homomorphism $h : M \to Q$ with $f = h \circ g$.

The ring R is said to be left (resp. right) self-injective if R itself is injective as left (resp. right) R-module. If both conditions hold, R is said to be a self-injective ring.

A left R-module M is Artinian if M is satisfies the descending chain condition on submodules. A ring R is left (resp. right) Artinian if R itself is Artinian as left (resp. right) R-module. If both conditions hold, R is said to be an Artinian ring.

It is clear that a finite ring is an Artinian ring.

Definition 5. *For a (not necessarily commutative) ring R, R is called a QF (quasi-Frobenius) ring if R is left Artinian and left self-injective.*

It is well-known that the definition of a QF ring is left-right symmetric.

For any R-submodule $C \subseteq R^n$, C° is defined by

$$C^\circ = \{\lambda \in Hom_R(R^n, R) | \lambda(C) = 0\}.$$

Theorem 2. *For a (not necessarily commutative) ring R, the following conditions are equivalent:*
(1) *R is a QF ring.*
(2) *For submodules $M \subseteq R^n$, $M^{\circ\circ} = M$.*

Theorem 3. *For a (not necessarily commutative) ring R, the following are equivalent:*
(1) *R is a QF ring.*
(2) *A left module is projective if and only if it is injective.*

We define an R-module homomorphism $\delta_x : R^n \to R$ as $\delta_x(y) =< y, x >$ for any $x \in R^n$.

Proposition 2. *The homomorphism $\delta : C^\perp \to C^\circ$ sending x to δ_x is an isomorphism of R-modules.*

Theorem 4. *Let R be a finite commutative QF ring. For a submodule $C \subseteq R^n$, $(C^\perp)^\perp = C$.*

By Theorem 1 and Theorem 4, we can get the following corollary.

Corollary 1. *Let R be a finite commutative QF ring. Then C is a polycyclic code if and only if $C^\perp$ is a sequential code.*

Theorem 5. *Let R be a finite commutative QF ring. If $C \subseteq R^n$ is a free R-module of finite rank, then $C^\perp$ is a free R-module of* $\mathrm{rank}C^\perp = n - \mathrm{rank}C$.

Definition 6. *Let R be a finite commutative QF ring. For a sequential code $C \subseteq R^n$, C is called a principal sequential code if $C^\perp$ is a principal polycyclic code. And C is called a principal sequential code with an invertible constant term if $C^\perp$ is a principal polycyclic code with an invertible constant term.*

Now we can get the main theorem.

Theorem 6. *Let R be a finite commutative QF ring. Suppose C is a free codes of R^n. Then the following conditions are equivalent:*
(1) *Both C and $C^\perp$ are principal polycyclic codes with invertible constant terms.*

(2) *Both C and $C^{\perp}$ are principal sequential codes with invertible constant terms.*
(3) *C is a principal polycyclic and sequential code with an invertible constant term.*
(4) *$C^{\perp}$ is a principal polycyclic and sequential code with an invertible constant term.*
(5) *$C = (g)/(X^n - \alpha)$ is a constacyclic code with an invertible α.*
(6) *$C^{\perp} = (q)/(X^n - \beta)$ is a constacyclic code with an invertible β.*

Acknowledgement. The author wishes to thank Prof. Y. Hirano, Naruto University of Education, for his helpful suggestions and valuable comments.

References

[1] D. Boucher and P. Solé, Skew constacyclic codes over Galois rings, Advances in Mathematics of Communications, Volume 2, No.3 (2008), 273-292.
[2] M. Greferath, M. E. O'Sullivan, On bounds for codes over Frobenius rings under homogeneous weights, Discrete Math, 289 (2004), 11-24.
[3] Y. Hirano, On admissible rings, Indag. Math. 8 (1997), 55-59.
[4] S. Ikehata, On separable polynomials and Frobenius polynomials in skew polynomial rings, Math. J. Okayama. Univ. 22 (1980), 115-129.
[5] T. Y. Lam, Lectures on Modules and Rings (Graduate Texts in Mathematics, Vol.189), Springer-Verlag, New York, 1999.
[6] S. R. López-Permouth, B. R. Parra-Avila and S. Szabo, Dual generalizations of the concept of cyclicity of codes, Advances in Mathematics of Communications, Volume 3, No.3 (2009), 227-234.
[7] M. Matsuoka, θ-polycyclic codes and θ-sequential codes over finite fields, International Journal of Algebra, Vol. 5 (2011), no. 2, 65-70.
[8] B. R. McDonald, Finite Rings With Identity (Pure and Applied Mathematics, Vol. 28), Marcel Dekker, Inc., New York, 1974.
[9] J. A. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math, 121 (1999), 555-575.

Yokkaichi-Highscool
4-1-43 Tomida Yokkaichi Mie 510-8510 Japan
E-mail address: e-white@hotmail.co.jp

微分方程式による人口変動モデル

河本直紀

１．はじめに

人口の変動を法則として表現したものとしてはマルサスによるモデルがよく知られている[1, 2]．このモデルは，人口の変化率はそのときの人口に比例すると表現される．数式で表わせば，時刻 t における人口を $p = p(t)$ とすると

$$\frac{dp}{dt} = c\,p \quad (1)$$

となる．ただし，c は定数である．１年間の人口の増減数はそのときの総人口に比例すると考えるのは自然であり，微分方程式にすれば(1)のような式となる．明治以降の日本の人口に当てはめてみても 1970 年頃までの人口増加については良い近似を与えていることが分かる．しかしながら $c>1$ の場合には(1)の解は $t \to \infty$ のときに $p \to \infty$ となり現実的ではない．ここでは(1)における定数 c を t の関数 $q = q(t)$ で置き換えることにより，現在の人口減少まで近似できて，近い将来の予測も可能になることを示したい．ただし，関数 $q(t)$としては区分的に線形な関数を採ることにする．

２．日本の人口

日本では大正９年（1920 年）から昭和２０年を除き５年ごとに国勢調査が行われ人口の変動が調べられている．総務省統計局[3]によるとこれらを基にした明治以降の日本の人口変動の様子は図１のようになっている．この変動は時系列と見ることもできるが，その場合には因果関係が表面から隠れてしまう．人口の変動は出生数と死亡数という二つの変数で決まるのでこれらを考慮に入れておくことが望ましいと思われる．さらに詳しくは，同じ時期に生まれた人の集団が時間を追ってどのように減少してゆくかを，それぞれの階層ごとに調べれば（コホート法），そこから全体の変

化も自然に得られるが，ここでは出生数と死亡数のデータを挙げておく．

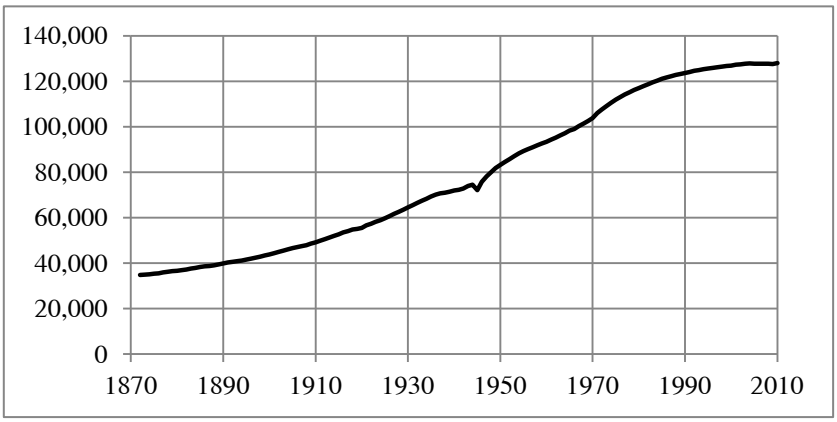


図 1　総人口（単位 1,000 人）

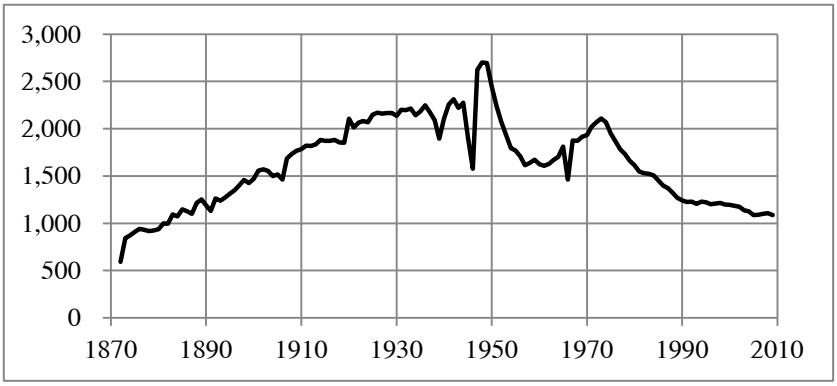


図 2　出生数（単位 1,000 人）

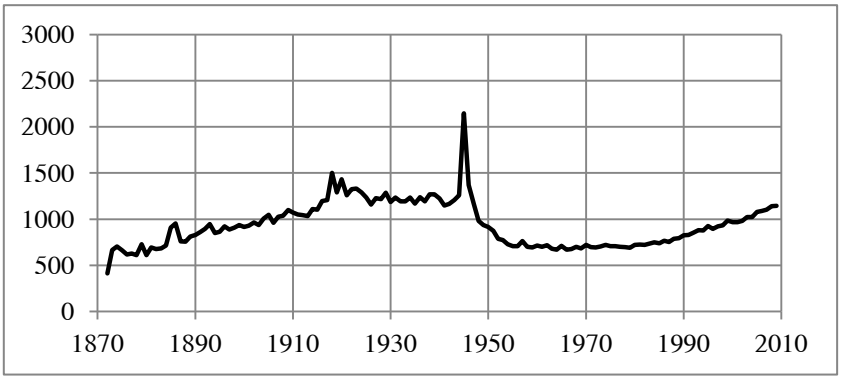


図 3　死亡数（単位 1,000 人）

３．モデル化

人口変動の基本的な変数としては上で述べたように年間の出生数と死亡数があるが，ここでは簡単のためにその差を取ることにより一変数にする．いわゆる自然増減である．人口変動は移住等のいわゆる社会増減によっても引き起こされるが，統計局のデータによれば第二次大戦の時期を除けばそれほど大きな値にはなっていない．これによりここでは自然増減のみとしてモデル化する．自然増減の値は図 2 の値から図 3 の値を引けば得られるが，さらに総人口に対する比を取っておく．すると次のようなグラフが得られる．

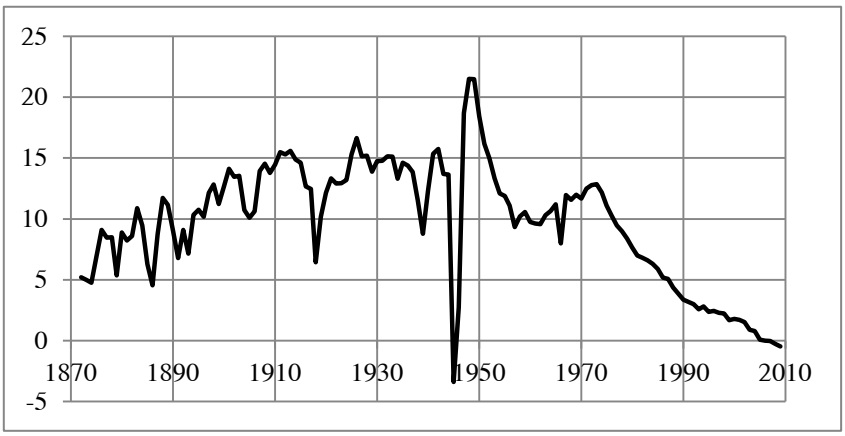


図 4　増加率（1,000 人あたり）

このグラフによれば戦後の第一次ベビーブームの時期を除くと増加率のピークは意外なことに昭和元年（1926 年）にある．このことは通常あまり言及されることは無いが, いわゆる少子化傾向は長期的には昭和の初めから始まっていたということになる. 明治期のデータについては信頼性に疑問があるともいわれるが, 別の見方をすれば日本社会の近代化が全体的には大正末に成し遂げられたということではなかろうか. なお, グラフの落ち込みは戦争, 疫病（スペイン風邪，コレラ）等によるものである．

図 5 の変化を年 t の関数として $q(t)$ と表現できれば人口変動の微分方程式は

$$\frac{dp}{dt} = q(t)p \quad (2)$$

となり，これを解けば総人口 $p = p(t)$ の変化が分かる．解は形式的には

$$p = c\exp(\int q(t)dt)$$

と表わされる．ただし c は定数である．

４．区分的線形近似

図 3 の変化を表わす関数 $q(t)$をここでは次のように定める．上で述べたように極大値の一つは昭和元年（1926 年）にあるが，もう一つの極大値が昭和 48 年（1973 年）のいわゆる第二次ベビーブームのときにある．図 1 によればこの前後で総人口の曲線が下に凸から上に凸になって，変曲点となっている．また図 4 によればこれ以降曲線はほぼ単調減少である．これによって昭和 48 年（1973 年）を境としてその前後をそれぞれ線形近似することとする．

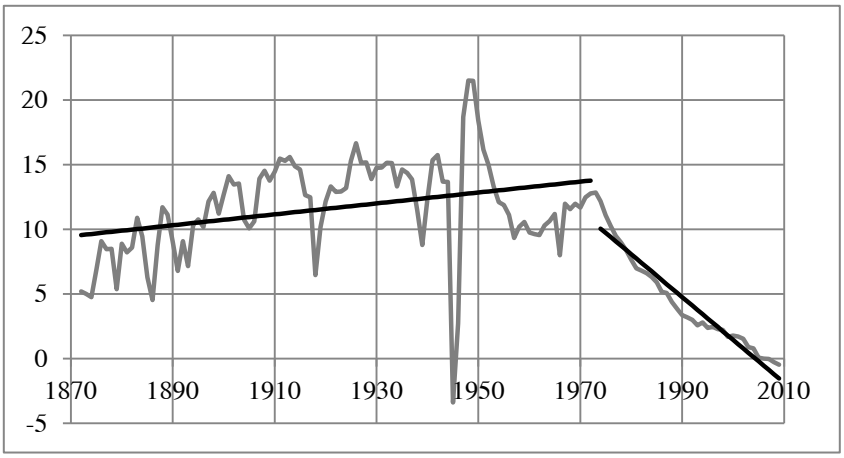


図 5　増加率の直線による近似

具体的には

$$q(t) = a \cdot t + b$$

とする．ただし，t は西暦の年数，a, b は最小二乗法により次のように定める．

1872 年～1973 年	a = 0.0421807	b = -69.4094
1973 年～2009 年	a = -0.331195	b = 663.839

初期値としては昭和 48 年（1973 年）の人口 1 億 910.4 万人を採り，これを基準としてそれ以前，および以後に延長する．結果は次のようになる．

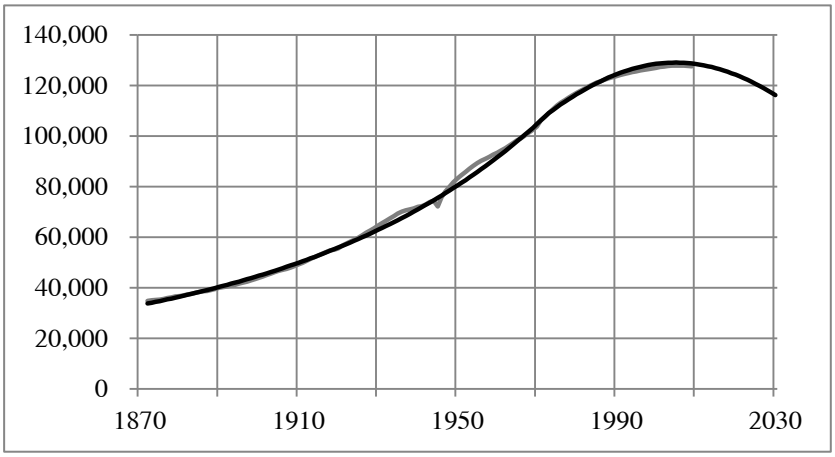


図 6　モデル化した人口変動

ここでの近似はかなり粗い方式ではあるが，結果は長期的な変動をかなり良く捉えていると思われる．また 2030 年までの人口の予測もしているが，この計算によれば 2030 年の人口は 1 億 1618 万人となっている．国立社会保障・人口問題研究所の出生中位（死亡中位）の将来推計[4]では 2030 年に 1 億 1522 万人となっていて，差は 1%以下である．

５．課題

増加率のグラフ（図 4）のモデル化でどのようなモデルが最適であるかの問題がある．ここではなるべく簡単でかつある程度良い近似を与えるということで，区分的線形近似を行ったが他にも様々な定式化が可能であろう．また，出生数と死亡数を別々に近似することも可能であるが，精度がどの程度改善されるかという点が問題となる．

参考文献

[1] 岡崎陽一，人口統計学（増補改訂版），古今書院，東京，1999
[2] 稲葉　寿，数理人口学，東京大学出版会，東京，2002

[3] 総務省統計局，日本の長期統計系列，第２章人口・世帯２－１男女別人口・人口増減及び人口密度（明治５年～平成２１年）
http://www.stat.go.jp/data/chouki/zuhyou/02-01.xls
[4] 国立社会保障・人口問題研究所，日本の将来推計人口（平成１８年１２月推計）将来推計人口 2006～2055 年，表１出生中位（死亡中位）推計
http://www.ipss.go.jp/tohkei/suikei07/houkoku/kekka-1/1-1.xls

〒737-8512
呉市若葉町 5-1
海上保安大学校
基礎教育講座
E-mail: kawamoto@jcga.ac.jp

RINGS OVER WHICH EVERY FREE SUBMODULE OF A FREE MODULE IS A DIRECT SUMMAND

YASUYUKI HIRANO

Department of Mathematics,
Naruto university of Education,
Takashima, Naruto, 772-8502, Japan,
E-mail: *yahirano@naruto-u.ac.jp*

Abstract. In this note, we prove that if R is a commutative artinian ring then every finitely generated free R-submodule N of a finitely generated free R-module M is a direct summand of M.

Lemma 1. *Let R be a commutative artinian local ring with Jacobson radical J. Let N be a free submodule of rank n of a free module M. Then the submodule $\bar{N} = (N + JM)/JM$ of M/JM is a R/J-free module of rank n.*

Proof. We may assume that $J \neq 0$. Then there is a positive integer k such that $J^k \neq 0$ and $J^{k+1} = 0$. Let $N = Rx_1 \quad \cdots \quad Rx_n$ be a free module of rank n with free basis $\{x_1, \cdots, x_n\}$ and let $\bar{x}_i = x_i + JM \in M/JM$ for each $i = 1, \cdots, n$. Suppose $\bar{a}_1\bar{x}_1 + \cdots + \bar{a}_n\bar{x}_n = 0$ for some $\bar{a}_i = a_i + J \in R/J$. Then $a_1x_1 + \cdots + a_nx_n \in JM$. Since $J^k \neq 0$, we can take $b_1, \cdots, b_k \in J$ such that $b_1 \cdots b_k \neq 0$. Since $J^{k+1} = 0$, $b_1 \cdots b_k a_1 x_1 + \cdots + b_1 \cdots b_k a_n x_n = 0$. However $x_1, \cdots, x_n$ are linearly independent over R, we obtain $b_1 \cdots b_k a_1 = \cdots = b_1 \cdots b_k a_n = 0$. Since R is a local ring, these mean $a_1, \cdots, a_n \in J$, that is $\bar{a_i} = a_i + J = 0$ for all $i \in \{1, \cdots, n\}$. □

Theorem 1. *Let R be a commutative artinian ring. Then every nitely generated free R-submodule N of a nitely generated free R-module M is a direct summand of M.*

Proof. First consider the case when R is a local ring. Let $N = Rx_1 \quad \cdots \quad Rx_m$ and $M = Ry_1 \quad \cdots \quad Ry_n$ $(m < n)$ with free bases $\{x_1, \cdots, x_m\}$ and $\{y_1, \cdots, y_n\}$. By Lemma 1, $\bar{N} = \bar{R}\bar{x}_1 \quad \cdots \quad \bar{R}\bar{x}_m$ is a subspace of $\bar{R}\bar{y}_1 \quad \cdots \quad \bar{R}\bar{y}_n = M/JM$ and of dimension m. Then we can select $y_{i_1}, \cdots, y_{i_{n-m}}$ from $\{y_1, \cdots, y_n\}$ such that $\{x_1, \cdots, x_m, y_{i_1}, \cdots, y_{i_{n-m}}\}$ is a basis of $\bar{M} = M/JM$. Then $M = (Rx_1 + \cdots + Rx_n) + (Ry_{i_1} + \cdots + Ry_{i_{n-m}}) + JM = M$. Since JM is small in M, we obtain $M = (Rx_1 + \cdots + Rx_n) + (Ry_{i_1} + \cdots + Ry_{i_{n-m}}) = M$. This means that M is a homomorphic image of $(Rx_1 \quad \cdots \quad Rx_n) \quad (Ry_{i_1} \quad \cdots \quad Ry_{i_{n-m}})$. Since M is a free module of rank n over a commutative artinian local ring R, by Theorem of Jordan-Hölder ([1, Theorerm 2.5.2]), the composition length of M is equal to

Key words and phrases: rings, free module, direct summand.

that of $(Rx_1 \quad \cdots \quad Rx_n) \quad (Ry_{i_1} \quad \cdots \quad Ry_{i_{n-m}})$. Therefore we conclude that $M = (Rx_1 \quad \cdots \quad Rx_n) \quad (Ry_{i_1} \quad \cdots \quad Ry_{i_{n-m}}) = N \quad (Ry_{i_1} \quad \cdots \quad Ry_{i_{n-m}})$.

Next consider the case when R is a commutative artinian ring. We can easily see that R is a direct sum of local artinian rings. So let $R = Re_1 \quad \cdots \quad Re_k$, where each Re_i is a local artinian ring. Now let N be a nitely generated free R-submodule of a nitely generated free R-module M. Then, for each i, e_iN be a free Re_i-submodule of rank m of a nitely generated free Re_i-module e_iM. Then $e_iM = e_iN \quad N_i'$ for some Re_i-submodule N_i' of e_iM. Then $M = (e_1N \quad \cdots \quad e_kN) \quad (N_1' \quad \cdots \quad N_k') = N \quad (N_1' \quad \cdots \quad N_k')$. □

The following example shows that a commutative noetherian ring need not have the property that every nitely generated free submodule N of a nitely generated free module M is a direct summand of M.

Example 1. *Let* $\mathbf{Z}$ *denote the ring of integers. It is easy to see that* $\mathbf{Z}$ *is a commutative noetherian ring. Consider the* $\mathbf{Z}$*-module* $\mathbf{Z}$ *and its submoduole* $2\mathbf{Z}$*. Clearly* $\mathbf{Z}$ *and* $2\mathbf{Z}$ *are nitely generated free* $\mathbf{Z}$*-module. However* $2\mathbf{Z}$ *is not a direct summand of* $\mathbf{Z}$*.*

References

[1] J. Beachy: Introductory Lectures on Rings and Modules, London Mathematical Society Student Texts, 47, Cambridge University Press, Cambridge, 1999.