数理解析研究所講究録
第1562巻 2007年 132-142

A generalization of group code

group codeの一般化

静岡理工科大学 情報システム学科 田中源次郎

Tanaka Genjiro

Department of Computer Science, Shizuoka Institute of Science and Technology,
Fukuroi-shi 437-8555 Japan

抄録. group codeの拡張概念について述べる. group codeは群論における基本関係に関する問題とも関連し、自然な形で古くから研究されてきた. コード理論においても、極大なbifix codeの素朴でもっとも簡単な例として研究がなされてきた. ここでは、群の族は完全単純半群の族の部分族であることに注目し, group codeの一般的な構成法を, completely simple semigroup codeと呼べるcodeの族の構成法へと拡張する. その拡張は非常に自然な形のもので無理が無いものである.

1. 基本的諸概念

以下で使用する用語と記号について説明を行う. 説明無く使用される用語については, 例えば, J.Berstel and D.Perrin[1] ,A.H.Clifford and G.B.Preston[2], や G.Lallement[3] を参照されたし.

Aはアルファベット, A^+ はA上の自由半群, A^* はA上の自由単位半群とする. Gは群, HはGの部分群とする. 以上の記号と意味については論文全体を通して固定して用いる. もし$x,y \in G$かつ$xy^{-1} \in H$ならば, $x \equiv y \bmod H$. と書く.

Kを$K \subset H \subset G$なるGの部分群とする. GにおけるHの左剰余類の集合上の右正則表現の核$\cap_{g\in G} g^{-1}Hg$とKとの共通部分を$K(H)$で表す. つまり$K(H) = (\cap_{g\in G} g^{-1}Hg) \cap K$. この部分群はまた次のように書けることは明かであろう.

$$K(H)=\{k \in K \mid Hgk=Hg \quad \forall g \in G\}.$$

Sを半群とし, $S^1=S \cup \{1\}$, $1 \notin S$とする. S^1 中の演算を以下で定める:

(i) 1はS^1の単位元であり,

(ii) すべての$x,y \in S$についてS^1中のxyはS中のそれと等しい.

S^1は1を単位元とするmonoidをなす.

IとJを空でない集合とする. $\Sigma=(\sigma_{ji})$ を群G上の$J \times I$行列とする. 集合$G \times I \times J$に以下の演算を導入する:

$$(g; i, j)(h; k, l)=(g\sigma_{jk}h; i, l).$$

この演算で$G \times I \times J$は半群をなす. この半群は$M(G; I, J; \Sigma)$と書かれ, G上の構造行列Σを持つ$I \times J$ *Rees matrix semigroup* と呼ばれる. 本論分では添字集合IとJは1という記号を共に含んでいるものとする. また, もし$m=Card(I)$と$n=Card(J)$がともに有限の場合は$M(G; I, J; \Sigma)$を$M(G; n, m; \Sigma)$と明示する.

群G上の行列Σのj行とi列をそれぞれ$\sum_j^R$と$\sum_i^C$で表す. KをGの部分群とする. もしすべての

$i \in I$ に対し，$\sigma_{ji}\sigma_{li}^{-1} \in K$ ならば，$\sum_j^R \equiv \sum_l^R \bmod K$ と書く．もしすべての $j \in J$ に対し，$\sigma_{ji}\sigma_{jk}^{-1} \in K$ ならば，$\sum_i^C \equiv \sum_k^C \bmod K$ と書く．

群 G 上の行列 Σ のすべての成分で生成される G の部分群を G_Σ で表す．つまり

$$G_\Sigma = < \sigma_{ji} \mid j \in J, i \in I > .$$

群 G 上の行列 $\Sigma=(\sigma_{ji})$ は以下を満たすとき H-正規化されていると呼ばれる：
(1) Σ は H 上の行列である．
(2) 各 $(i,k) \in I \times I$ に対し，$\sigma_{ti} \equiv \sigma_{tk} \bmod G_\Sigma(H)$ を満たすある $t \in J$ が存在する．
(3) 各 $(j,l) \in J \times J$ に対し，$\sigma_{js} \equiv \sigma_{ls} \bmod G_\Sigma(H)$ を満たすある $s \in I$ が存在する．

$\varphi : A^* \to M(G,I,J,\Sigma)^1$ を準同形写像とする．G の空でない部分集合 S に対し

$$\tilde{S}_{ij}=\{(h;i,j) | h \in S\}, \qquad \tilde{S}=\bigcup_{i\in I, j\in J} \tilde{S}_{ij}, \qquad L_\varphi(S)=\varphi^{-1}(\tilde{S}) \bigcup \{1\}.$$

と定義する．

A^+ から G への写像 $\delta : A^+ \to G$ を，

$$\varphi(w)=(g;i,j) \text{ のとき，} \delta(w)=g,$$

と定義する．このとき $\varphi(u)=(x;i,j)$ かつ $\varphi(v)=(y;k,l)$ ならば，$\delta(uv)=x\sigma_{jk}y=\delta(u)\sigma_{jk}\delta(v)$ となる．

定義 1. A^+ の空でない部分集合 X は，$x_1,...,x_p,y_1,...,y_q \in X, p,q \geq 1$, に対し，

$$x_1 \cdots x_p = y_1 \cdots y_q \text{ ならば } \quad p=q \text{ かつ } x_1=y_1, \cdots, x_p=y_p.$$

なる条件をみたすとき，A 上の *code* と呼ばれる．

A^* の submonoid M は $(M-\{1\})-(M-\{1\})^2$ なる極小生成系を持つ．A^* の submonoid L を生成する code X は L の *base* と呼ばれる．

A^* の空でない部分集合 X は，$X \cap XA^+ = \emptyset$ なる条件を満たすとき *prefix code* と呼ばれる．prefix code X はさらに $X \cap A^+X = \emptyset$ なる条件をみたすとき *bifix code* と呼ばれる．code X はそれが他の code に真に含まれることがないならば *maximal code* と呼ばれる．bifix code はそれが他の bifix code に真に含まれることがないならば *maximal bifix code* と呼ばれる．

L を A^* の submonoid とする．任意の $u,v \in A^*$ に対し，

$$u, uv \in L \Longrightarrow v \in L \quad \text{かつ} \quad v, uv \in L \Longrightarrow u \in L$$

なる 2 条件を満たすとき L は *biunitary* であるという．一般に，A^* の submonoid L が biunitary であるための必要十分条件は，L の base X が biprefix code であることである．

monoid M から monoid N への準同形写像 φ は，$\varphi(1_M)=1_N$ を満たすとき *morphism* と呼ばれる，ここで 1_M と 1_N はそれぞれ M と N の単位元である．

定義 2. X を A 上の code とする．もし 群 G のある部分群 H と，$X^*=\varphi^{-1}(H)$ を満たす上への morphism $\varphi : A^* \to G$ が存在するとき，X は *group code* と呼ばれる．

L を A^* の部分集合とする．もし任意の $w \in A^*$ に対し，$L \cap A^*wA^* \neq \emptyset$ が成り立つならば，L は *dense* であるという．dense でない部分集合 L は *thin* であるという．A^* の部分集合 L は，任意の $w \in A^*$ に対し $L \cap wA^* \neq \emptyset$ なる条件を満たすとき *right dense* であるという．同様に，$L \cap A^*w \neq \emptyset$ なる条件をみたすときは *left dense* であるという．

オートマトン $\mathcal{A}$ は以下で定義される 5 項対である；

$$\mathcal{A}=(Q, A, \pi, i, F),$$

ここで，Q は状態の集合，A は入力記号の集合，$i \in Q$ は初期状態，$F \subseteq Q$ は最終状態の集合，$\pi : Q \times A^* \to Q$ は状態遷移関数で次を満たす；

任意の $q \in Q$ と任意の $w, w' \in A^*$ に対し，$\pi(q,1)=q$ かつ，$\pi(\pi(q,w),w')=\pi(q,ww')$.

もし各 $(p,q) \in Q \times Q$ に対し，$\pi(p,w)=q$ となるような $w \in A^*$ が存在するならば，$\mathcal{A}$ は可移オートマトンと呼ばれる．各 $w \in A^*$ に対し Q 上の変換 $\pi_{\mathcal{A}}(w)$ を

$$(q)\pi_{\mathcal{A}}(w)=\pi(q,w), \quad q \in Q,$$

と定める．ただし，変換の積は左から右へと読むものとする．$\pi_{\mathcal{A}} : A^* \to \{\pi_{\mathcal{A}}(w) | w \in A^*\}$ は A^* の Q 上の表現を与える．変換半群 $T(\mathcal{A})=\pi_{\mathcal{A}}(A^*)$ はオートマトン $\mathcal{A}$ の *transition monoid* と呼ばれる．$T(\mathcal{A})$ の部分半群 $\{\pi_{\mathcal{A}}(w) | w \in A^+\}$ を $T(\mathcal{A}^+)$ で表す．

L を A^* の部分集合とする．各 $w \in A^*$ に対し $A^* \times A^*$ の部分集合を次のように定義する；

$$Cont_L(w)=\{(u,v) \mid u,v \in A^*, uwv \in L\}.$$

L の *syntactic congruence* $\equiv_L$ とは次で定義される合同関係である；

$$w \equiv_L w' \iff Cont_L(w)=Cont_L(w').$$

商半群 $A^*/\equiv_L$ は L の *syntactic monoid* と呼ばれる．

2. group code の基本的性質

group code に関する基本的な性質を説明しておく．以下の群についての初等的注意は完全単純半群の部分半群を考える上での注意でもある．

$(G,\cdot)$ を演算 $\cdot$ を持つ群とする．任意に選んだ元 $\alpha \in G$ をひとつ固定する．集合 G に新しい演算 $\circ$ を，$x,y \in G$ のとき，$x \circ y = x \cdot \alpha \cdot y$ と定義したものを $(G,\circ)_\alpha$ とおく．$(G,\circ)_\alpha$ は半群をなす．α^{-1} はその単位元である．各 $x \in G$ は逆元 $\alpha^{-1}x^{-1}\alpha^{-1}$ を持つ．従って $(G,\circ)_\alpha$ は群をなす．この群 $(G,\circ)_\alpha$ は，群 $(G,\cdot)$ 上の 1×1 行列 $\Sigma=(\alpha)$ を構造行列とする Rees matrix semigroup $M(G;1,1;\Sigma)$ に他ならない．$f : x \in G \longrightarrow \alpha^{-1}x$ は $(G,\cdot)$ から $(G,\circ)_\alpha$ への群としての上への同形写像であることは容易に確かめられる．つまり，$(G,\cdot)$ と $(G,\circ)_\alpha$ は群として同形である．群 $(G,\cdot)$ 中の部分群 H は，$(G,\circ)_\alpha$ 中の部分集合とみなしたとき，一般に $(G,\circ)_\alpha$ の部分群になるとは限らない．

$\eta : A^* \to (G,\cdot)$ を上への morphism とする．$(G,\cdot)$ から $(G,\circ)_\alpha$ への群としての同形写像 $f : x \in G \longrightarrow \alpha^{-1}x$ と η の合成写像を ψ とする；

$$\psi : A^* \xrightarrow{\eta} (G,\cdot) \xrightarrow{f} (G,\circ)_\alpha.$$

$(G,\cdot)$ の部分群 H に対し $\alpha^{-1}H$ は $(G,\circ)_\alpha$ の部分群である．従って $L'=\psi^{-1}(\alpha^{-1}H)$ は A^* の biunitary submonoid であり，その基底は group code である．$L=\eta^{-1}(H)$ とおく．$\psi(w)=\alpha^{-1}(\eta(w))$ であることより $L=L'$ が示される．group code についての基本的事実をまとめておく：
群 G の上への morphism $\varphi:A^*\to G$, $\varphi(1)=1_G$, と部分群 H について，
$L_H=\varphi^{-1}(H)$ の syntactic monoid $A/\equiv_{L_H}$ の性質．
(1) $A/\equiv_{L_H}$ は商群 $G/(\cap_{g\in G}g^{-1}Hg)$ と同型．
(2) L_H の基底は極大な code である．
(3) 上への morphism $\eta:A^*\to G^1$, G^1 は G の 1 添加，を $\varphi(1)=1$, $\eta|_A=\varphi|_A$ で定義する．

$$L_\eta(H)=\eta^{-1}(H)\cup\{1\}$$

と置くと，$A/\equiv_{L_H}\cong A/\equiv_{L_\eta(H)}$ (群として同型)．
(4) $L_\eta(H)-\{1\}=L_H-\{1\}$ であるから，$L_\eta(H)$ と L_H の基底は一致する．
注意．従って，group code は群を用いなくとも得ることが出来る．
注意．group code は次の例が示すように，上の注意のような形で (上のような φ,η で) のみ得られるわけではない．例えば，
$A=\{a,b\}$, $G=<x,y\,|\,x^3=y^2=(xy)^2=1>$, $H=<y>$,

$$\Sigma=\begin{pmatrix} y & y \\ y & y \end{pmatrix}.\qquad \varphi(a)=(x:1,1),\ \varphi(b)=(x^2:2,2)$$

により，$M(G;I,J;\Sigma)$ と上への morphism $\varphi:A^*\to M(G;I,J;\Sigma)^1$ を定義すると，$L_\varphi(H)$ の基底は $C=ab^*a+ba^*b$ であり，かつ $A^*/\equiv_{L_\varphi(H)}$ は G と同型である．
注意．上述の，φ は $\varphi|_{A^+}=\eta|_{A^+}$ と定義することにより，定義が確定した．逆の操作は可能ではない．つまり，はじめに上への morphism $\varphi:A^*\to G^1$ が与えられているとき，φ を用いて，$w\in A^+$ に対し $\eta(w)=\varphi(w)$ かつ $\eta(1)=1_G$ で $\eta:A^*\to G$ を定義することは，次の例が示すように，一般に可能ではない．
$A=\{a,b\}$. $G=<x\,|\,x^2=1_G>$ (位数 2 の巡回群)，$H=\{1_G\}$ (自明な部分群) とする．$\varphi:A^*\to G^1$ を，$\varphi(1)=1,\varphi(a)=1,\varphi(b)=x$ で定義する．φ に対し，$\eta(1)=1_G,\eta(b)=x$ ではあるが，$\eta(a)=1\notin G$ となり，η は A^* から G への写像ではない．

3. group code の一般化

group code は A^* から群 G の上への morphism と群 G の部分群 H を決めることによって構成される．群の族は完全単純半群の部分族と見なせる．従って以下の 2 条件を満たすような定義を導入したい；

(1) 自由半群 A^* から完全単純半群 R の上への準同形と，群 G の部分群 H を用いて直接記述出来る R の部分半群を用いて code を構成する．

(2) その構成法は group code の構成法の自然な拡張になっていて，得られる code X 達は group code の以下の基本的性質を満たす．

(2-i) X は maximal biprefix code である．

(2-ii) X^* は dense である．

(2-iii) X^* を受理するオートマトン $\mathcal{A}$ の変換半群 $T(\mathcal{A}^+)$ は完全単純半群である．

上記の (1),(2) を満たすような，group code の新たな拡張概念を定義導入のためには，はじめに G の部分群 H を無条件に選択するのではなく，構造行列 Σ についての条件を先行させなければならない．つまり，構造行列 Σ にかかわる部分群を考える方が自然な定義と見なせるであろう (田中 [9])．結論を言えば，行列 Σ の全成分を用いて生成される部分群を K とすると，$G \supset H \supset K$ であるような部分群 H についての $\tilde{H}$ は $M(G;I,J;\Sigma)$ の部分半群をなす．このような部分群を考察の中心に置くことによって group code の自然な拡張概念の定義導入が可能となる．

命題 1. $\varphi : A^* \to M(G;I,J;\Sigma)^1$ を上への morphism とすると，集合 $L_\varphi(H)$ は right dense かつ left dense である．

一般に，$\varphi : A^* \to M(G;I,J;\Sigma)^1$ を上への morphism とすると，
(1) $L_\varphi(H)$ は A^* の submonoid である
ための必要かつ十分な条件は
(2) Σ は H 上の行列である．ことである．
という事実はすぐに証明できる．しかしながら以下の議論において，上への morphism を厳密に区別しておく必要が起る．

$L_\varphi(H)$ が submonoid であると仮定する．ある $a \in A$ について $\varphi(a)=1$ となっている場合を考える．X を $L_\varphi(H)$ の極小生成系とし，$w \in X$ を X 中の長さが最小な語とする．$\varphi(a^n) \notin \tilde{H}$ であるから，任意の $n \geq 1$ について $a^n \notin X^*$．$\varphi(a^n w)=\varphi(w) \in \tilde{H}$ より，すべての $n \geq 1$ に対し $a^n w \in X^*$．もし $a^n w \in X^+ - X$ ならば，$a^n w = a^n uv$ を満たすような，$u \in A^+$ と $v \in X$ が存在する．これは w の長さの最小性に反する．従って $a^n w \in X$．同様に $wa^n \in X$ であることが示される．従って $wa^n w$ は X 中で異なるふたつの分解を持つ．よって，X は code ではない．本論文の主目的は，上への morphism $\varphi : A^* \to M(G;I,J;\Sigma)^1$ と，その極小生成系 X が code であるような $L_\varphi(H)$ の syntactic monoids との関係を考察することである．従ってその極小生成系 X が code でないようなものは取扱わない．よって，議論の煩雑化を避けるためには「上への morphism $\varphi : A^* \to M(G;I,J;\Sigma)^1$」という用語は，「すべての $a \in A$ に対し $\varphi(a) \neq 1$ であるような上への morphism φ」を扱うべきである．

命題 2. $\varphi : A^* \to M(G;I,J;\Sigma)^1$ を上への morphism とする．もし Σ が H 上の行列ならば，$L_\varphi(H)$ は A^* の biunitary submonoid である．

従って，Σ が H 上の行列ならば，$L_\varphi(H)$ の基底 X は biprefix code である．さらに X が code として極大であることも示せる．

Σ を H 上の行列，$\varphi : A^* \to M(G;I,J;\Sigma)^1$ を上への morphism とする．$L_\varphi(H)$ の基底 X について，X^* は dense であり，X は maximal biprefix code である．X^* を受理するオートマトン $\mathcal{A}$ の $T(\mathcal{A}^+)$ は完全単純半群である．そして，2節で述べたように，group code は $\varphi : A^* \to M(G;1,1;\Sigma)^1$, $\Sigma = (1_G)$ を用いて得ることが出来る．従って，上への morphism φ を用い code を構成する方法は group code の構成法の一般化になっている．

例 (tanaka[10]). $A=\{a,b\}$, $G=<x,y \mid x^3=y^2=(xy)^2=1>$, そして

$$\Sigma_1=\begin{pmatrix} 1 & 1 \\ 1 & x \end{pmatrix}, \quad \Sigma_2=\begin{pmatrix} 1 & 1 \\ 1 & y \end{pmatrix}, \quad \Sigma_3=\begin{pmatrix} 1 & 1 \\ y & 1 \end{pmatrix}.$$

とする．

(1) Σ_1 は $H=<x>$ の行列である．上への morphism $\varphi : A^* \to M(G;2,2;\Sigma_1)^1$ を $\varphi(a)=(y;1,1)$, $\varphi(b)=(x;2,2)$. で定義すると，$L_\varphi(H)$ の基底は maximal biprefix code$X=b+ab^*a$ である．上への morphism $\theta : A^* \to G$ を $\theta(a)=y$ かつ $\theta(b)=x$ で定義すると，$\theta^{-1}(H)$ の基底は X と一致する．よって X は group code である．

(2) Σ_2 は $H=<y>$ 上の行列である．上への morphism $\varphi : A^* \to M(G;2,2;\Sigma_2)^1$ を $\varphi(a)=(x;1,1)$ かつ $\varphi(b)=(xy;2,2)$ で定義すると．$L_\varphi(H)$ の基底は有限な maximal biprefix code

$$X=\{a^3, a^2b, aba^2, abab, ab^2, ba, b^2a^2, b^2ab, b^3\}$$

である．

(3) Σ_3 は $H=<y>$ 上の行列である．上への morphism $\varphi : A^* \to M(G;2,2;\Sigma_3)^1$ を $\varphi(a)=(x;1,1)$, $\varphi(b)=(y;2,2)$ で定義する．すると $L_\varphi(H)$ の基底は次の無限な maximal biprefix code

$$X=b+a^2(b^2(b^2)^*a)^*a+ab(b^2+ab^2)^*a^2+(a^2b+ab^2+abab)(b^2+bab)^*a.$$

命題 3. $\varphi : A^* \to M(G;I,J;\Sigma)^1$, $\Sigma=(\sigma_{ji})$, を上への morphism，そして $\Sigma'=(\rho_j\sigma_{ji}\tau_i)$, $\rho_j, \tau_i \in G$, $j \in J, i \in I$, とする．$\varphi' : A^* \to M(G;I,J;\Sigma')^1$ を

$$a \in A, \varphi(a)=(g;i,j) \text{ ならば } \varphi'(a)=(\tau_i^{-1}g\rho_j^{-1};i,j), \quad \text{そして，} \varphi'(1)=1$$

と定義すると以下が成立つ；
(1) φ' は上への morphism である．
(2) もし Σ が H 上の行列で，すべての $j \in J, i \in I$ に対し $\rho_j, \tau_i \in H$ ならば，$L_{\varphi'}(H)=L_\varphi(H)$.

この命題より，Σ が H 上の行列で $\varphi : A^* \to M(G;I,J;\Sigma)^1$ が上への morphism ならば，$L_\psi(H)=L_\varphi(H)$ を満たすような H-normalized 行列 Σ' と上への morphism $\psi : A^* \to M(G;I,J;\Sigma')^1$ が存在することが分かる．

命題 4. Σ を H 上の行列，$\varphi : A^* \to M(G;I,J;\Sigma)^1$ を上への morphism，さらに $L_\varphi(H)$ の base を X とする．X が A 上で分解不可能であるための必要かつ十分な条件は，H が G の極大部分群であることである．

4. syntactic monoid

$L_\varphi(H)$ に関する合同関係 $\equiv_{L_\varphi(H)}$ について次が成り立つ．

命題 5. Σ を H-正規化された $J \times I$ 行列とする．$\varphi : A^* \to M(G;I,J;\Sigma)^1$ を上への morphism, $w, w' \in A^+$ を $\varphi(w)=(\delta(w);i,j)$ そして $\varphi(w')=(\delta(w');k,l)$ であるような語とする．$w \equiv_{L_\varphi(H)} w'$ であるための必要十分条件は次の 3 条件が成り立つことである；
(1) $\delta(w) \equiv \delta(w') \bmod H(H)$,
(2) $\sum_i^C \equiv \sum_k^C \bmod G_\Sigma(H)$,
(3) $\sum_j^R \equiv \sum_l^R \bmod G_\Sigma(H)$.

monoid M 上の 3 つの同値関係 $\mathcal{R}, \mathcal{L}, \mathcal{H}$ (Green's relations) を以下のように定義する；

$$m\mathcal{R}m' \text{ iff } mM=m'M, \quad m\mathcal{L}m' \text{ iff } Mm=Mm' , \quad \mathcal{H}=\mathcal{R}\cap\mathcal{L}.$$

系 6. 命題 4.1 で用いた記号と仮定のもとで次が成立する.

(1) $[w]\mathcal{R}[w'] \Longleftrightarrow \sum_i^C \equiv \sum_k^C \bmod G_\Sigma(H)$,

(2) $[w]\mathcal{L}[w'] \Longleftrightarrow \sum_j^R \equiv \sum_l^R \bmod G_\Sigma(H)$,

(3) $[w]\mathcal{H}[w'] \Longleftrightarrow \sum_i^C \equiv \sum_k^C \bmod G_\Sigma(H)$ かつ
$\sum_j^R \equiv \sum_l^R \bmod G_\Sigma(H)$.

次の命題は $A^*/\equiv_{L_\varphi(H)}$ は, group code でなければ, 完全単純半群の 1 添加になっていることを示す. G が有限群無限群であることを問わず, また添え字集合 I や J が有限無限を問わず命題は成立することに注意すべきである. なぜならば, G.Lallement and C. Reis[6] により, G,I,J の全てが有限の場合の全ての"elementary codes"の構成法が与えられている. しかし, 例えば G が無限群の場合はいかようにして"elementary codes"を構成するかはこれまでほとんど知られていなかった. 僅かに中畑 [7] の構成例があるくらいである.

命題 7. Σ は H-正規化された行列で, $\varphi : A^* \to M(G;I,J;\Sigma)^1$ は上への morphism とする. このとき $A^*/\equiv_{L_\varphi(H)}$ は群であるか, または完全単純半群に 1 添加したものである.

集合 I 上の同値関係 $\approx_C$ を $i,k \in I$ に対し

$$i \approx_C k \Longleftrightarrow \sum_i^C \equiv \sum_k^C \bmod G_\Sigma(H)$$

で定義する. I' を I 上の同値関係 $\approx_C$ の代表系とする. $[i]_C$ で $i \in I'$ の $\approx_C$-類を表す. 同様に, J 上の同値関係 $\approx_C$ を $j,l \in J$ に対し

$$j \approx_R l \Longleftrightarrow \sum_j^R \equiv \sum_l^R \bmod G_\Sigma(H)$$

で定義する. J' を J 上の同値関係 $\approx_R$ の代表系とする. $[j]_R$ で $j \in J'$ の $\approx_R$-類を表す.

もし $[u],[v] \in A^*/\equiv_{L_\varphi(H)}$, $u,v \in A^+$, でかつ
$\varphi(u)=(x;i,j), \varphi(u)=(y;k,l)$
ならば, 命題 5 により,

$$[u]=[v] \Longleftrightarrow xy^{-1} \in H(H), i \approx_C k, j \approx_R l.$$

命題 8. Σ は H-正規化された行列で, $\varphi : A^* \to M(G;I,J;\Sigma)^1$ は上への morphism とする. もし $A^*/\equiv_{L_\varphi(H)}$ が群でないならば, $A^*/\equiv_{L_\varphi(H)}$ は $M(G/H(H);I',J';\Sigma')^1$ に同形である.

$M(G/H(H);I',J';\Sigma')$ は $M(G;I,J;\Sigma)$ と H で決定される. つまり, $M(G/H(H);I',J';\Sigma')^1$ の構成は φ によらない. 従って, 命題 8 により, もし φ と ψ が A^* から $M(G;I,J;\Sigma)^1$ の上への morphism ならば, $A^*/\equiv_{L_\varphi(H)}$ と $A^*/\equiv_{L_\psi(H)}$ は同形である.

命題 9. Σ を群 G の部分群 H 上の行列とする. $\varphi : A^* \to M(G;I,J;\Sigma)^1$ が上への morphism ならば, $L_\varphi(H)$ の syntactic monoid の自明でない $\mathcal{H}$-class は剰余群 $G/H(H)$ と同形である.

命題 10. H を群 G の部分群, Σ を H-正規化された行列とする. $\varphi : A^* \to M(G;I,J;\Sigma)^1$ を上への morphism とする. 次の 3 条件は同値である.

(1) $L_\varphi(H)$ の基底は group code である.
(2) $1 \in A^*$ の $\equiv_{L_\varphi(H)}$-class $[1]$ は一元集合ではない.
(3) 任意の $i, k \in I$ に対し, $\sum_i^C \equiv \sum_k^C \bmod G_\Sigma(H)$ が成立し, 任意の $j, l \in J$ に対し, $\sum_j^R \equiv \sum_l^R \bmod G_\Sigma(H)$ が成立する.

命題 11. C を thin maximal biprefix code , $\mathcal{A}$ を C^* を認識する可移オートマトンとする. もし transition semigroup $T(\mathcal{A}^+)$ が完全単純半群ならば, $X^*=L_\varphi(H)$ を満たすような, ある完全単純半群 $M(G; I, J; \Sigma)$, と群 G のある部分群 H とある上への morphism $\varphi : A^* \to M(G; I, J; \Sigma)^1$ が存在する.

5. $L_\varphi(H)$ を受理するオートマトンと有限な elementary code

C^* の syntactic monoid が完全単純半群の 1 添加になるような有限 bifix code C は (有限な) elementary code と呼ばれる. 有限な elementary code は適当な有向グラフ (チームトーナメント) から得られる (G.Lallement and C. Reis,[6]). このチームトーナメントの拡張版としての有向グラフによる構成法もある (G.Lallement and D.Perrin,[5]). 一方上記命題のオートマトンは, $\varphi : A^* \to M(G; I, J; \Sigma)^1$, $\Sigma=(\sigma_{ji})$ は H 上の行列, なる上への morphism に対し, G の H についての剰余類の集合と A の組を考え, 行列 Σ を介してオートマトンを作っていく. syntactic monoid が完全単純半群の 1 添加になるような全ての thin bifix code C は無限の場合も直接構成出来る. このとき, その syntactic monoid を知るために, オートマトンの transition monoid を直接計算する必要はない. φ と H と Σ の形から transition monoid の構造は決定されるからである (Tanaka [10]).

$\Sigma = (\sigma_{ji})$ を H 上の行列, $\varphi : A^* \to M(G; I, J; \Sigma)^1$ を上への morphism とする. $a, b \in A$, $\varphi(a) = (\delta(a); i, j)$, $\varphi(b)=(\delta(b); k, l)$ のとき $\sigma(a, b)=\sigma_{jk}$ とおく. $Q=\{H\} \cup \{(Hg, a) | g \in G-H,\ a \in A\}$. とおく. オートマトン $\mathcal{A}_\varphi=(Q, A, \pi, H, \{H\})$ を以下のように定義する;
$a, b \in A$ and $H, (Hg, a) \in Q$ に対し π は以下で定義する,
$\pi(H, b)=H$ if $H\delta(b)=H$, $\pi(H, b)=(H\delta(b), b)$ if $H\delta(b) \neq H$ そして,

$$\pi((Hg, a), b)=\begin{cases} H & \text{if } Hg\sigma(a, b)\delta(b)=H, \\ (Hg\sigma(a, b)\delta(b), b) & \text{otherwise.} \end{cases}$$

$\mathcal{A}_\varphi$ によって認識される言語を $L(\mathcal{A}_\varphi)$ で表す.

命題 12. $L(\mathcal{A}_\varphi)=L_\varphi(H)$.

注意: 一般に $\mathcal{A}_\varphi$ は $L_\varphi(H)$ を受理する極小オートマトンとは限らない.
チームトーナメント *team tournament* $\mathcal{T}$ とは以下のような有向グラフである; $\mathcal{T}$ は互いに素な p 個の集合 $\mathcal{T}_1, \mathcal{T}_2, \ldots, \mathcal{T}_n$ からなる. 各 $\mathcal{T}_i$ は $m-1$ 個の点を含む. そして, 一本の鎖をなしている. 各 $\mathcal{T}_i$ と $\mathcal{T}_i$ 中の点達は以下のような規則で辺が引かれる. $\mathcal{T}_i$ は以下のような鎖である.
$\mathcal{T}_i=\{c_1^i \to c_2^i \to \cdots \to c_{m-1}^i\}$.
$\mathcal{T}_i$ と $\mathcal{T}_j$ 間の辺 (矢) は次のような規則で与える.
(1) $c_l^i \to c_p^i$ ならば $p \neq 1$.
(2) 各 i, j, p, $i \neq j$, $p \neq 1$ に対し, $c_l^i \to c_p^j$ であるような, 唯一つの $l \leq p$ が存在する.

(3) 各 i,j,k,l,p について，もし $c_l^i \to c_p^j$ かつ $c_l^i \to c_k^j$ ならば k=p.
(4) グラフはいかなるループも含まない.
チームトーナメントより，以下のようにしてオートマトンを構成出来る:
(5) $\mathcal{T}_i$ の点に到達する辺にはすべて a_i でラベル付けする.
(6) 0 で表される特別な状態を加える. (1)-(5) において a_i でラベル付けされない辺があれば， a_i でラベル付けされた 0 への辺を引く.

$\mathcal{T}_i$ から $\mathcal{T}_j$ への辺は次のような $\{0,1,\dots m-1\}$ 上の置換 f_{ij} を定義する;
(0)f_{ij}=1, もし $c_l^i \to c_p^j$, ならば (l)f_{ij}=p. もし $p, c_l^i \to c_p^j$ が $\mathcal{T}$ 中に存在しなければ (l)f_{ij}=0.

チームトーナメント $\mathcal{T}$ のオートマトンにおいて、0 から 0 への極小な道 (simple path) で表される語の全体 X は有限で極大な bifix code である. 上記の $\{0,1,\dots m-1\}$ 上の置換 f_{ij} 達を用いて n^2 個の以下のような置換が作れる.

$$\sigma_{ij}=f_{1i}f_{ij}f_{1j}^{-1},\ 1 \le i,j \le n.$$

すると， bifix code X の Suschkewitsch group(定義は [4.p217]) は置換 σ_{ij}, $1 \le i,j \le n$ で生成される. ([6]).

補題 13 A=$\{a_1,a_2\dots a_n\}$ とする. かつ Σ=(σ_{ji}) は有限群 G 上の $n \times n$ 行列で次の (1) と (2) を満たすとする.
(1) σ_{11}=σ_{12}=$\dots$=σ_{1n}
(2) G は Σ の成分で生成される. つまり, G=G_Σ.
すると, $\varphi(a_i)$=$(1;i,i)$, $1 \le i \le n$, で定義される morphism $\varphi : A^* \to M(G;n,n;\Sigma)^1$ は全射である.

α=$(0,1,2,\dots,m-1)$ を m-cycle とする. G 上の $n \times n$ 行列を Σ_0=(σ_{ji}), $\sigma_{ji} = f_{1j}f_{ji}f_{1i}^{-1}$, $1 \le i,j \le n$, によって定義する. すべての $1 \le i \le n$ について σ_{1i}=f_{11}=α であることに注意する. $\varphi_0 : A^* \to M(G;n,n;\Sigma_0)^1$ を $\varphi_0(a_j)$=$(1;j,j)$, $a_j \in A$, $1 \le j \le n$ によって定義する. 補題により φ_0 は上への morphism である.

$$\Sigma=(\sigma_{j1}^{-1}\sigma_{ji}) \text{ and } \varphi(a_j)=(\sigma_{j1};j,j),\ 1 \le i,j \le n.$$

とおくと,φ も上への morphism である.

全ての $1 \le i \le n$ について $\sigma_{11}^{-1}\sigma_{1i}$=1 であるから, Σ の第 1 行と第 1 列は G の単位元である (つまり Σ は正規化されている).

$$0 \xrightarrow{f_{11}} 1 \xrightarrow{f_{j1}^{-1}} 0 \xrightarrow{f_{ji}} 1 \xrightarrow{f_{1i}^{-1}} 0,$$

であるから $\sigma_{j1}^{-1}\sigma_{ji}$=$f_{11}f_{j1}^{-1}f_{ji}f_{1i}^{-1}$ は 0 の固定部分群 H に含まれる. 従って Σ は H-正規化された行列である.

$$G=H\alpha^0+H\alpha^1+\cdots+H\alpha^{m-1},\quad H\alpha^s=\{g \in G \mid (0)g=s\},$$

であり，且つ

$$\begin{aligned}\sigma_{i1}^{-1}\sigma_{ii}\delta(a_i)&=\sigma_{i1}^{-1}\sigma_{ii}\sigma_{i1}=\alpha f_{i1}^{-1}\alpha f_{i1}\alpha^{-1}=(f_{i1}\alpha^{-1})^{-1}\alpha f_{i1}\alpha^{-1}\\ &=(0,(1)f_{i1}\alpha^{-1},(2)f_{i1}\alpha^{-1},\dots,(m-1)f_{i1}\alpha^{-1}),\qquad (m\text{-cycle}).\end{aligned}$$

であることに注意する. $(s)f_{i1}\alpha^{-1}=\lfloor s\rfloor$, とおくと, $\sigma_{i1}^{-1}\sigma_{ii}\delta(a_i)=(0,\lfloor 1\rfloor,\lfloor 2\rfloor,\cdots,\lfloor m-1\rfloor)$ であり, 且つ

$$H\alpha^{\lfloor k\rfloor}\sigma_{i1}^{-1}\sigma_{ii}\delta(a_i)=\{g\in G\mid (0)g=\lfloor k+1\rfloor\}=H\alpha^{\lfloor k+1\rfloor}.$$

$\sigma_{i1}^{-1}\sigma_{ii}\in H$ であるから, $H\delta(a_i)=H\sigma_{i1}^{-1}\sigma_{ii}\delta(a_i)$. 従ってオートマトン A_φ の状態図において,

$$H\xrightarrow{a_i}(H\alpha^{\lfloor 1\rfloor},a_i)\xrightarrow{a_i}(H\alpha^{\lfloor 2\rfloor},a_i)\xrightarrow{a_i}\cdots\xrightarrow{a_i}(H\alpha^{\lfloor m-1\rfloor},a_i)\xrightarrow{a_i}H.$$

$j\neq i$ and $(s)f_{ij}=t$ とする. $(s)f_{j1}\alpha^{-1}=\lceil s\rceil, 0\leq s\leq m-1$, と置くと,

$$\begin{aligned}&(\lfloor s\rfloor)\sigma_{i1}^{-1}\sigma_{ij}\delta(a_j)\\ &= (s)f_{ij}f_{j1}\alpha^{-1}=(s)f_{j1}\alpha^{-1}\cdot\alpha f_{j1}^{-1}f_{ij}f_{j1}\alpha^{-1}\\ &= (\lceil s\rceil)(f_{j1}\alpha^{-1})^{-1}\cdot f_{ij}\cdot f_{j1}\alpha^{-1}=(\lceil s\rceil)(\cdots,(s)f_{j1}\alpha^{-1},(t)f_{j1}\alpha^{-1},\cdots)\cdots=\lceil t\rceil.\end{aligned}$$

従って, $c_s^i\xrightarrow{a_j}c_t^j$ より $(H\alpha^{\lfloor s\rfloor},a_i)\xrightarrow{a_j}(H\alpha^{\lceil t\rceil},a_j)$ が結論出来る. これは, チームトーナメントのオートマトンは, オートマトンとして, A_φ と同型であることを意味する. 命題 12 により $X^*=L_\varphi(H)$. よって φ は $X^*=L_\varphi(H)$ を満たす morphism である.

例. チームトーナメントのオートマトンを次の表で与える.

	0	c_1^1	c_2^1	c_3^1	c_4^1	c_5^1	c_1^2	c_2^2	c_3^2	c_4^2	c_5^2
a	c_1^1	c_2^1	c_3^1	c_4^1	c_5^1	0	c_3^1	c_2^1	c_5^1	c_4^1	0
b	c_1^2	c_2^2	c_3^2	c_4^2	c_5^2	0	c_2^2	c_3^2	c_4^2	c_5^2	0

すると

$f_{11}=f_{12}=f_{22}=\alpha=(0\,1\,2\,3\,4\,5)$, $f_{21}=(0\,1\,3\,5)(2)(4)$,

$\sigma_{11}=f_{11}f_{11}f_{11}^{-1}=\alpha$, $\sigma_{12}=f_{11}f_{12}f_{12}^{-1}=\alpha$, $\sigma_{21}=f_{12}f_{21}f_{11}^{-1}=(0\,2\,4\,5)(1)(3)$,

$\sigma_{22}=f_{12}f_{22}f_{12}^{-1}=\alpha$.

$G=<\sigma_{11},\sigma_{21}>$ とすると, G は置換群として $PGL(2,5)$([8]) と同値である. H を 0 の固定部分群とする.

$$\varphi(a)=(\alpha;1,1),\ \varphi(b)=((0\,2\,4\,5);2,2),\ \Sigma=\begin{pmatrix}1 & 1\\ 1 & (1\,2)(3\,4)\end{pmatrix}.$$

G は可移群であり H が 0 の固定部分群であることから, $H(H)=G_\Sigma(H)=\{1\}$. よって, 命題 により syntactic monoid は $M(G;2,2;\Sigma)^1$ と同型である.

置換 F_{ij} を次で定義する. $F_{ij}=\sigma_{i1}^{-1}\sigma_{ij}\delta(a_j)$, i.e., $F_{ij}:(s)f_{i1}\alpha^{-1}\to(s)f_{ij}f_{j1}\alpha^{-1}$. すると

$F_{11}=\alpha$, $F_{22}=\sigma_{21}^{-1}\sigma_{22}\sigma_{21}=(0\,\lfloor 1\rfloor\,\lfloor 2\rfloor\,\lfloor 3\rfloor\,\lfloor 4\rfloor\,\lfloor 5\rfloor)=(0\,2\,1\,4\,3\,5)$,

$F_{12}=(0\,2\,4\,5)$, $F_{21}=\alpha$.

従って, オートマトン $\mathcal{A}_\varphi$ は次の表で与えられる:

	H	$(H\alpha^1,a)$	$(H\alpha^2,a)$	$(H\alpha^3,a)$	$(H\alpha^4,a)$	$(H\alpha^5,a)$	$(H\alpha^1,b)$
a	$(H\alpha^1,a)$	$(H\alpha^2,a)$	$(H\alpha^3,a)$	$(H\alpha^4,a)$	$(H\alpha^5,a)$	H	$(H\alpha^2,a)$
b	$(H\alpha^2,b)$	$(H\alpha^1,b)$	$(H\alpha^4,b)$	$(H\alpha^3,b)$	$(H\alpha^5,b)$	H	$(H\alpha^4,b)$

	$(H\alpha^2, b)$	$(H\alpha^3, b)$	$(H\alpha^4, b)$	$(H\alpha^5, b)$
a	$(H\alpha^3, a)$	$(H\alpha^4, a)$	$(H\alpha^5, a)$	H
b	$(H\alpha^1, b)$	$(H\alpha^5, b)$	$(H\alpha^3, b)$	H

References

[1] J.Berstel and D.Perrin, *Theory of Codes*, Academic Press, New York, 1985.

[2] A.H.Clifford and G.B.Preston, *The Algebraic Theory of Semigroups*, Vol.1, American Mathematical Society, Mathematical Surveys 7, 1961.

[3] M.Katsura and G.Tanaka, Groups of finite elementary codes, Theoretical Computer Science 108 (1993), pp.119-149.

[4] G.Lallement, *Semigroup and Combinatorial Applications*. Wiley, New York, 1979.

[5] G.Lallement and D.Perrin, A graph covering construction of all the finite complete biprefix codes, *Discrete Math.*36 (1981) 261-271.

[6] G.Lallement and C. Reis, Team tournaments and finite elementary codes, *Inform. and Control* 48 (1981) 11-29.

[7] 中畑登, biprefix code の 1 つの族について, 京都大学数理解析研究所講究録 697,1989, pp.70-89.

[8] D.Perrin, Codes Bipréfixes et groupes de permutations, Thèse Doctorat d'État, Université de Paris VII, 1975.

[9] 田中源次郎, 自由単位半群の biunitary submonoid の syntactic monoid について I, 静岡理工科大学紀要 2004, pp.151-164.

[10] G.Tanaka, On syntactic monoids of biunitary submonoids determined by homomorphisms from free semigroups onto completely simple semigroups, Theoretical Computer Science 352 (2006), pp.57-70.