数理解析研究所講究録
第1604巻 2008年 120-124

A remark on construction of circular codes

Noboru NAKAHATA (中畑 登)
Tokai University Junior College (東海大学短期大学部)

Yoshiyuki KUNIMOCHI (國持 良行), Genjiro TANAKA (田中 源次郎)
Shizuoka Institute of Science and Technology (静岡理工科大学)

Abstract. In this paper we treat the circular codes. We present a method of constructing circular codes. We first make a "large" very pure monoid by using the homomorphism from a free monoid to a semigroup. Next, by selecting subsets of its base, we can gain various circular codes.

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 を文字 (letter) の集合とする. A の元の有限列 w を A 上の語 (word) と呼び, 語の集合を言語と呼ぶ. A 上の語 w 中の文字の集合を $alph(w)$ で表す. 語の全体からなる集合を A^* で表す. A^* から空語 1 を除いた集合を A^+ で表す. A^* 上に語の並列 (concatenation) で 2 項演算を定義すると,A^* は空語 1 を単位元とする free monoid をなす. A^* の部分半群 M は単位元 1 を持つとき, submonoid と呼ばれる. free monoid の自明でない submonoid M は, 唯一つの極小生成系 $C = (M - \{1\}) - (M - \{1\})^2$ を持つ. この極小生成系を M の基底と呼ぶ. M の基底 C が, すべての $n, m \geq 1$, とすべての $x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m \in C$ に対し

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m \Longrightarrow \ n = m, \ x_i = y_i, 1 \leq i \leq n.$$

を満たすとき, C は code と呼ばれる. このとき M は free submonoid と呼ばれる.
M を free monoid A^* の submonoid とし, C を M の基底とする. もし,

$$CA^+ \cap C = \emptyset$$

が成り立つならば, C は A 上の prefix code と呼ばれる. 右-左双対として $A^+C \cap C = \emptyset$ が成り立つとき C は A 上の suffix code と呼ばれる. C が prefix code かつ suffix code であるとき, C は bifix code であると呼ばれる. 定義により, prefix code C においては, 任意の $w \in C$ の真の左因子は C の元になることはない.

M を A^* の submonoid とする. すべての $u, v \in A^*$ に対し, 誘導式 $[u, uv \in M \Longrightarrow v \in M]$ が成立するとき, M は A^* の right unitary submonoid と呼ばれる. 同様に, すべての $u, v \in A^*$ に対し, 誘導式 $[u, vu \in M \Longrightarrow v \in M]$ が成立するとき, M は A^* の left unitary submonoid と呼ばれる. もし, M が right unitary かつ left unitary ならば, M は biunitary と呼ばれる.

$C \subset A^*$ を code とする.C が prefix code であるための必要十分条件は C^* が right unitary であることである. そして, C が suffix code であるための必要十分条件は C^* が left unitary であることである. ([1,p.46,Prop.2.5]). 従って C が bifix code であるための必要十分条件は C^* が biunitary monoid であることである.

A^* の submonoid M は，以下の条件を満たすとき，*very pure* submonoid と呼ばれる：

$$u, v \in A^*, uv, vu \in M \Rightarrow u, v \in M.$$

very pure submonoid の基底は *circular code* と呼ばれる．

定義 1. $p, q \geq 0$ を整数とする．code C が A^* の語の任意の列 $u_0, u_1, \cdots, u_{p+q}$ について，

$$u_{i-1}u_i \in C^*,\ (1 \leq i \leq p+q) \Longrightarrow u_p \in C^*$$

なる条件を満たすならば，C は (p, q)-limited であると呼ばれる．

C が (p, q)-limited code であるならば，C^* は very pure である ([1], p.329,Proposition 2.1).

J を空でない集合とする．すべての $x, y \in J$ に対し $xy = y$ と定義する．J は右零半群と呼ばれる．同じように，左零半群は $xy = x$ で定義される．左零半群 I と右零半群 J の半群としての直積 $S = I \times J$ は直角帯 (rectangular band, [3,p.51]) と呼ばれる．

命題 1. I を左零半群，J を右零半群とする．$S = I \times J$ を半群としての直積とする．$\varphi : A^* \to S^1$ を morphism とする．T を S の任意の部分半群とすると，$M = \varphi^{-1}(T) \cup \{1\}$ は very pure submonoid である．その基底は (1,1)-limited である．

証明. 明らかに，M は A^* の submonoid である．$u_0, u_1, u_2 \in A^*$ について，$u_0u_1, u_1u_2 \in M$，と仮定する．$\varphi(u_0) = (p, q), \varphi(u_1) = (k, l),\ \varphi(u_2) = (s, t)$ とすると．$\varphi(u_0u_1) = (p, l) \in T,\ \varphi(u_1u_2) = (k, t) \in T$ より $(k, t)(p, l) = (k, l) \in T$. よって $\varphi(u_1) \in T$.　　Q.E.D.

例 1. $A = \{a, b\}$, S=$\{1, 2\} \times \{1, 2\}$ とする．$\varphi(a) = (1, 1), \varphi(b) = (2, 2)$ とする．$S_{11} = \{(1, 1)\}$ について，$M_{11} = \varphi^{-1}(S_{11}) \cup \{1\} = \{1, a\} \cup aA^*a$ は明らか．M_{11} の基底 C_0 は，命題 1 により，(1,1)-limited code である．しかしながら C_0 は (1,0)-limited でも (0,1)-lmited でもない．なぜなら，$ab \cdot a = a \cdot ba \in C_0^*$ であるが，$ab,\ ba \notin C_0^*$ であるからである．また，語の列 $ab,\ a,\ aba,\ ba \in A^*$ について，$aba,\ aaba,\ ababa \in C_0^*$ であるから (3,0)-limited でも (0,3)-limited でもない．

$$C = \{a\} \cup \{ab^{m_1}ab^{m_2} \cdots ab^{m_r}a \mid r \geq 1,\ m_i \geq 1, 1 \leq i \leq r\}.$$

とおく．C が $\{1,\ a\} \cup aA^*a$ を生成するのは明らかである．
$U_1 = C^{-1}C - \{1\} = \{b^{m_1}ab^{m_2} \cdots ab^{m_r}a \mid r \geq 1,\ m_i \geq 1, 1 \leq i \leq r\}$.
つまり，U_1 は b で始まる語のみからなる．よって，$U_2 = C^{-1}U_1 \cup U_1^{-1}C = \emptyset$. よって，$U_i \cap C = \emptyset, i = 1, 2$. よって C は code であり，$C = C_0$ である．つまり，C は M_{11} の基底である．よって，命題により C は (1,1)-limited である．また，$M_{12} = \varphi^{-1}(1, 2) \cup \{1\} = \{1\} \cup aA^*b$ でその基底は

$$a^+b^+ = \{a^mb^n \mid m,\ n \geq 1\}.$$

である．

このような無限 limited code を作れば，それは無限 circular code である．従って，その任意の空でない部分集合 D も circular code である．従って，適当な部分集合 D をとることにより再び D が limited code になる可能性もある．実際，C の空でない任意の部分集合は limited code である．C は (1,1)-limited であるから，C は (2,1)-,(1,2)-limited であることに注意する．

C の任意の空でない部分集合もまた (2,1)-,(1,2)-limited であることをより一般的な形で証明しておく.

命題 2. $u, v \in A^+$ を $alph(u) \cap alph(v) = \emptyset$ であるような元とする. もし $u(A^*)^{-1} \cap (A^*)^{-1}u = \{1, u\}$ ならば

$$C = u + (uv^+)^+u = \{u\} \cup \{uv^{m_1}uv^{m_2} \cdots uv^{m_r}u \mid r \geq 1,\ m_i \geq 1, 1 \leq i \leq r\}.$$

の空でない任意の部分集合は (1,2)-, (2,1)-limited code である.

証明. C は code である. 初めに次のことに注意する. D を C の部分集合とする. $x \in A^*$ を $D(A^*)^{-1} \cap (A^*)^{-1}D$ の元とすると $u(A^*)^{-1} \cap (A^*)^{-1}u = \{1, u\}$ であるから, $x = 1$, $x = u$ または, ある $p_1, p_2, \cdots p_s \in N$, $s \geq 1$, について $x = uv^{p_1}uv^{p_2} \cdots uv^{p_s}u$ である. つまり $D(A^*)^{-1} \cap (A^*)^{-1}D = \{1\} \cup D \cup \{u\}$.
D が (1,2)-,(2,1)-limited であることを示す. $u_0, u_1, u_2, u_3 \in A^*$ について, $u_iu_{i+1} \in D^*$, $i = 0, 1, 2$, が成立しているとすると,

$$u_0 = w_0x_1,\ u_1 = y_1w_1',\ x_1y_1 \in D,\ w_0, w_1' \in D^*,$$

$$u_1 = w_1x_2,\ u_2 = y_2w_2',\ x_2y_2 \in D,\ w_1, w_2' \in D^*,$$

$$u_2 = w_2x_3,\ u_3 = y_3w_3',\ x_3y_3 \in D,\ w_2, w_3' \in D^*,$$

と書ける. x_2 は D の元の左因子である. そしてまた x_2 は $u_0u_1 \in D^*$ の右因子である. よって次の二つの場合を考える.
Case (a). x_2 が D のある元の右因子である.
この場合, x_2 は D の元の右因子であり, かつ D のある元の左因子である. つまり $x_2 \in D(A^*)^{-1} \cap (A^*)^{-1}D = \{1\} \cup D \cup \{u\}$. したがって, $u_1, u_2 \in D^*$.
Csae (b). x_2 が D の元を右因子として含む.
この場合ある $d \in D$, $x' \in A^*$ について $x_2 = x'd$ である. 従って x_2 は u で終わる. つまりある $z \in A^*$ について $x_2 = zu$. 一方 y_2 は $u_2u_3 \in D^*$ の左因子であるから, $y_2 = 1$ または y_2 は u のある左因子 $u' \neq 1$ について, $y_2 = u'v$, $v \in A^*$ である. 後者の場合は $x_2y_2 = zuu'v \in D$ である. これは矛盾. 従って, $y_2 = 1$. よって, $x_2 \in D$. よって $u_1, u_2 \in D^*$. Q.E.D.

命題 3. $u, v \in A^+$ を $alph(u) \cap alph(v) = \emptyset$ とする.

$$C = (uv^+)^+ = \{uv^{m_1}uv^{m_2} \cdots uv^{m_r}u \mid r \geq 1,\ m_i \geq 1, 1 \leq i \leq r\}.$$

の空でない任意の部分集合は (1,2)-, (2,1)-limited code である.

命題 2 と同様な証明による. よって証明を略す.

以上により, 例 1 における code C の空でない任意の部分集合は (2,1)-,(1,2)-limited である. C 中の部分集合についての主なもののカタログは以下である;

(1) $D=(abb^*)(abb^*)^*a$ の空でない任意の部分集合 D_0 は，$p+q=2$ であるような任意の $p,\ q\geq 0$ に対し，(p,q)-limited ではない．

(2) $X\subset A^*$ を code とする．X が，$p+q=3$ であるような任意の $p,q\geq 3$ に対し $(p,\ q)$-limited であり，かつ $A^+XA^+\cap X=\emptyset$ であるとき，X は comma-free と呼ばれる．

正整数 n を固定する．$D=(abb^*)^na$ の空でない任意の部分集合 D_0 は comma-free である．

(3) $n\geq 3$ とする．$C^{(n)}=A^n\cap C$ の任意の部分集合 D_0 は comma-free である．

(4) D_0 を $D=(ab)^*a$ の任意の部分集合とする．

(i) $Card(D_0)=1$, $D_0=\{w\}$, $w\neq a$, ならば，D_0 は (3,0)-,(0,3)-limited である．

(ii) $Card(D_0)\geq 2$ ならば，D_0 は任意の整数 $k\geq 1$ に対し $(k,0)$-,$(0,k)$-limited ではない．

(iii) 次の条件 (*) を満たす $n\geq 0$, $m\geq 2$, が存在したら，D_0 は $(1,1)$-, $(0,k)$-, $(k,0)$-limited ではない，ただし $k\geq 2$.

(*) $(ab)^na,\ (ab)^{n+m}a\in D_0$ かつ ある $n\leq l\leq n+m$, であるような l に対し $(ab)^la\notin D_0$.

(iv) $Card(D_0)\geq 2$, $a\in D_0$ であり，かつ次の条件 (**) を満たすとき D_0 は (1,1)-limitted である．

(**) $(ab)^na,\ (ab)^{n+m}a\in D_0,\ m>0,\ n\geq 0\Longrightarrow (ab)^la\in D_0,\forall l,\ n\leq l\leq n+m.$

例えば，$D_0=\{a,\ aba,\ ababa\}$ は (1,1)-limited code である．

$M_{12}=L_\varphi((1,2))=aA^*b$ でその基底は

$$C=\{a^mb^n\mid m,\ n\geq 1\}.$$

この C についての空でない部分集合 D は code である．以下 D について基本的なものを見出す．

命題 4. $u,v\in A^+$, $alph(u)\cap alph(v)=\emptyset$ とする．u^+v^+ の任意の空でない部分集合は (1,2)-,(2,1)-limited である．

証明略．

(5) T を自然数全体の集合 N, $0\notin N$, の任意の空でない部分集合とする．$\alpha:S\longrightarrow N$ を任意の単射とする．$D=\{a^nb^{\alpha(n)}\mid n\in S\}$ とおく．

(i) もし任意の $m,n\in S$ に対し，条件 $[m<n\Longrightarrow\alpha(m)<\alpha(n)]$ を満たすならば，D は $p+q=2$ であるような任意の $p,q\geq 0$ に対し $(p,q)-$limited である．また $Card(D)\geq 2$ ならば，D は comma-free ではない．

(ii) もし任意の $m,n\in S$ に対し，条件 $[m>n\Longrightarrow\alpha(m)<\alpha(n)]$ を満たすならば，D は comma-free である．また $Card(D)\geq 2$ ならば，任意の $p,q\geq 0$, $p+q=2$, に対し $(p,q)-$limited でない．特に $D=\{a^kb^{n-k}\mid k=1,2,\cdots,n-1\}$, $n\geq 2$, とおくと D は comma-free である．

(6) $n\geq 1$, $a^nb^+=\{a^nb^k\mid k\geq 1\}$ の空でない任意の部分集合 D_0 は，

(i) (0,2)-,(1,1)-limited である．

(ii) もし $Card(D_0)=1$ ならば，D_0 は $(2,0)$-limited である．もし $Card(D_0)\geq 2$ ならば，$p\geq 2$ に対し $(p,0)$-limited ではない．

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

[4] H.J.Shyr, *Free Monoid and Languages*, Hon Min Book Co, Taichung, Taiwan,1991.

[5] Shyr-shen Yu, *Languages and Codes*. Tsang Hai Book Publishing Co, Taiwan, 2005.