数理解析研究所講究録
第1769巻 2011年 7-12

Conformal code について

On conformal codes

田中 源次郎 (Genjiro Tanaka)

静岡理工科大学総合情報学部コンピュータシステム学科

Dept. of Computer Science, Shizuoka Institute of Science and Technology,

Fukuroi-shi, 437-8555 Japan.

0. 序

Extractable code と conformal code の関係について述べる．語の集合 C が code をなすとき，正整数 n に対し $C^{(n)} = \{w^n \mid w \in C\}$ は再び code をなす．しかしながら，$C^{(n)}$ が extractable になるような code C の性質はほとんど分かっていない．文献 [7] で，C が uniform code あるいは reflective code であれば $C^{(n)}$ が extractable であることを報告した ([7],Prop.9 及び Prop.16)．この結果は別々に証明を与えている．この二つの結果を同時に証明することが本論文の目的である．そのために，conformal code なる概念を定義導入する．

1. 記号と基本的諸概念

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] や G.Lallement[3] を参照されたし．

A は字母系 (アルファベット)，A^+ は A 上の free semigroup(自由半群)，A^* は，空語 1 を単位元とする，A 上の free monoid(自由単位半群) とする: $A^* = A^+ \cup \{1\}$. free monoid A^* の元 $w \in A^*$ は語ろ呼ばれる．語 $w(\in A^*)$ 中の A の元の個数を $|w|$ で表し語 w の長さと呼ぶ．

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

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

なる条件をみたすとき，A 上の *code* と呼ばれる．

A^* の submonoid M は $(M - \{1\}) - (M - \{1\})^2$ なる唯 1 つの極小生成系を持つ（一般に極小生成系は基底 (*base*) と呼ばれる）．
A^* の部分半群 M は A^* の単位元 1 を含むとき *submonoid* と呼ばれる．M を A^* の submonoid とする．ある字母系 B 上の free monoid B^* から M の上への isomorphism $f : B^* \to M$ が存在するとき M は A^* の free submonoid と呼ばれる．free submonoid の極小生成系は code であり，逆に任意の code X が生成する submonoid X^* は free である ([1],p.43])．

This is an extended abstract and the paper will appear elsewhere.

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．X は $X \cap A^+X = \emptyset$ なる条件をみたすとき *suffix code* と呼ばれる．code X は，prefix でありかつ suffix であるときは *bifix* code と呼ばれる．

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

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

なる２条件を満たすとき M は *biunitary* であるという．一般に，A^* の submonoid M が biunitary であるための必要十分条件は，M の極小生成系 X が bifix code であることである ([1],Prop.2.5).

code C が，任意の $x, y \in A^*$ と任意の $z \in C$ に対し，$[xzy \in C \implies x = y = 1]$ なる条件を満たすとき，C は *infix code* と呼ばれる．infix code が bifix code であることは定義より明らかである．A 上の長さ $m \geq 1$ の語の全体 A^m の空でない任意の部分集合は code C をなす．これらの code C は uniform code と呼ばれる．uniform code が bifix code であることは明らかであろう．

A^* の submonoid M は次の条件を満たすとき *extractable*(可抽) であると呼ばれる．

$$\text{任意の } x, y \in A^*,\ z \in M \text{に対し，}\ \ xzy \in M \text{ ならば } xy \in M.$$

定義. C を A 上の code とする．C^* が A^* の extractable submonoid ならば，C は extractable と呼ばれる．

「可抽な部分半群 (extractable subsemiguroup)」や「可挿な部分半群 (insertable subsemigroup)」の概念は Tamura[4,p.191] に見い出せる．可抽な code の例は，文献 [6] に見い出せる．つまり，ペトリネット PN に付随する D-type のペトリネット code $D(PN)$ ([5],Def.2.6) は可抽であるという性質を持っている ([6],Prop.2.3).
一般に，extractable code の部分集合は extractable とは限らない．例えば，$A = \{a, b\}$ 上の code A^2 は extractable code である．しかし，その部分集合 $C = \{a^2, ab, ba\}$ は extractable ではない．

2. Conformal Code

conformal code は以下のように定義される．

定義. C を A 上の code とする．任意の $d, c \in C$ と任意の $\alpha, \beta \in A^*$ に対し，

$$d^2 = \alpha c \beta \implies d = \alpha\beta,\ c = \beta\alpha,$$

が成立するとき，C は *conformal* code（共形的コード）と呼ばれる．

注意. 一般に conformal code C において $d, c \in C$, $d^2 = \alpha c\beta = \alpha' c\beta'$ から $\alpha = \alpha'$, $\beta = \beta'$ が結論出来るとは限らない．

例1. (1) $C = \{ab^2, (ab)^2\}$ は conformal code である.
(2) $C = \{a^2b^3, aba\}$ は conformal code である.

次の性質は定義から直接得られる自明な事実であるが有用である.

性質 1. conformal code の空でない任意の部分集合は conformal code である.

例 2. uniform code A^n, $n \geq 1$, は conformal code である. 従って, A^n の任意の空でない部分集合は conformal である.

証明. C を uniform code とする. $d, c \in C$, $\alpha, \beta \in A^*$ について $d^2 = \alpha c \beta$ とする (下図).

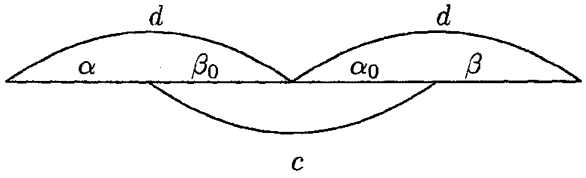

Fig. 1.

C は uniform なので, $|d| = |c|$ である. 従って,

$$|\alpha| + |\beta_0| = |\beta_0| + |\alpha_0| = |\alpha_0| + |\beta|.$$

従って, $|\alpha| = |\alpha_0|$, $|\beta_0| = |\beta|$. つまり $\alpha = \alpha_0$, $\beta = \beta_0$. 従って $d = \alpha\beta$, $c = \beta\alpha$.

命題 1. conformal code は infix code である.

証明. Z を A 上の conformal code とする. $d = xcy$, $c, d \in Z$, $x, y \in A^*$ とする. $d^2 = x \cdot c \cdot yxcy$ より $d = x \cdot yxcy$ かつ $c = yxcy \cdot x$. 従って $|c| = |yxcyx|$. 従って $yx = 1$, つまり $x = y = 1$.

A 上の code Z は任意の $u, v \in A^*$ に対し $[uv \in Z \implies vu \in Z]$ を満たすとき *reflective code* と呼ばれる. 定義より, reflective code は共役類 (conjugacy class) の和集合である. reflective code は infix code である ([7],Prop.7). 従って, reflective code は bifix code である. 以下の例 4 に示すように共役類の和集合は reflective code を成すとは限らない.

例 3. C=$Cl(a^2b) + Cl(ab^3) = \{a^2b, aba, ba^2, ab^3, bab^2, b^2ab, b^3a\}$ は reflective code である. 実際, C が code を成すことは, C が prefix code であることにより確かめられる.

例 4. 注意. $L = Cl(ab) + Cl(ab^2) = \{ab, ba, ab^2, bab, b^2a\}$ は共役類の和であるから, $[uv \in L,\ u, v \in A^* \implies vu \in L]$ なる条件を満たす. しかし $(ab) \cdot (bab) = (abb) \cdot (ab) \in L^*$ であるから L は code ではない. つまり共役類の和が常に reflective code になるとは限らない.

例 5. 注意. C が reflective code であっても, C^* について条件 $[uv \in C^* \implies vu \in C^*]$ が成立するとは限らない.

命題 2. reflective code は conformal である.

証明. C を A 上の reflective code とする. $d^2 = \alpha c \beta$, $d, c \in C$, $\alpha, \beta \in A^*$, とする. C は code であるから $\alpha = \beta = 1$ ではない.
Case 1. $\alpha = 1$, $\beta \neq 1$ の場合. この場合 $d^2 = c\beta$. C は prefix code であるから $d = c$, $d = \beta$. 従って, $d = 1 \cdot \beta = \alpha\beta$, $c = d = \beta \cdot 1 = \beta\alpha$.
$\beta = 1$, $\alpha \neq 1$ の場合. C は suffix code であるから, $d = \alpha\beta$, $c = \beta\alpha$ が成立する.
Case 2. $\alpha \neq 1$ かつ $\beta \neq 1$ のとき. この場合 $d = \alpha\beta_0 = \alpha_0\beta$, $c = \beta_0\alpha_0$ であるような $\alpha_0, \beta_0 \in A^*$ が存在する (Fig. 2).

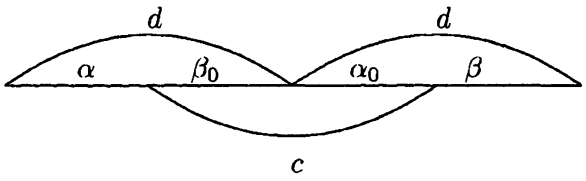

Fig. 2.

もし $|\alpha_0| = |\alpha|$ ならば, $d = \alpha\beta_0 = \alpha_0\beta$ より $\beta_0 = \beta$ である. そして, $d = \alpha\beta$, $c = \beta\alpha$ を得る. つまり, C は conformal である.
Case 2-1. $|\alpha| > |\alpha_0|$ のとき. この場合, $\alpha = \alpha_0 u$ となる $u \in A^*$ が存在する. C は reflective であり, かつ $d = \alpha_0 u \beta_0 \in C$ であるから, $\beta_0\alpha_0 u, \beta_0\alpha_0 \in C$ である. これは C が prefix code であることに矛盾する. 従って, Case 2-1 は起こらない.
Case 2-2. $|\alpha| < |\alpha_0|$ のとき. この場合, $\alpha_0 = \alpha u$ となる $u \in A^*$ が存在し, $c = \beta_0\alpha u$, $d = \alpha\beta_0 \in C$. C が reflective であることより $\beta_0\alpha \in C$. C は prefix だからこれは起こり得ない.
以上で reflective code は conformal であるいことが示せた.

注意. 性質 1 と命題 2 より, reflective code の任意の空でない部分集合は conformal code である.

C を A 上の code とし, n を正整数とする. 集合 $C^{(n)}$ を次で定義する.

$$C^{(n)} = \{c^n \mid c \in C\}.$$

一般に, C が code であれば, $C^{(n)}$ は code である ([3,Prop.10.2, Cor.10.3]). この事実は code の合成 (composition) という概念 ([1,p.71]) を使えばより明確に説明できる.
$Z \subset A^*$ と $Y \subset B^*$ を code とする. ただし, Y 中の語に出現する文字の集合は B に一致するものとする (B の真部分集合ではないとする). もし, B から Z への全単射 β が存在するならば, Y と Z は β を通して合成可能であるという. 集合

$$X = \beta(Y) \subset Z^* \subset A^*$$

は Y と Z の合成 (composition) と呼ばれる. X を $X = Y \circ_\beta Z$ と表記する. 一般に次の命題が成り立つ

命題 3([1],Prop.6.1). Y と Z が β を通して合成可能な code であれば，$X = Y \circ_\beta Z$ も code である．

C を A 上の code とする．code C を添字集合とする新しいアルファベット B を作る．

$$B = \{b_x \mid x \in C\}.$$

N を正整数の集合とする．$\varphi : C \to N$ を C から N への任意の写像とする．相異なる文字の冪からなる集合 $Y = \{b_x^{\varphi(x)} \mid a_x \in B\}$ は明らかに B 上の (bifix) code である．$\pi : B \to C$, $\pi(b_x) = x$, は B から C への全単射である．従って，Y と C は合成可能である．従って，上記の命題により，$X = Y \circ_\pi C$ は code である．つまり $X = \{x^{\varphi(x)} \mid x \in C\}$ は code である．特に $\varphi(C) = \{n\}$ つまり，$\varphi(C)$ が一元集合の場合が $X = C^{(n)}$ である．

補題 4. C を A 上の code とする．C が infix ならば $C^{(n)}$ は infix である．

証明. $C = \{w_i \mid i \in I\}$ とする．ここで，I は添字集合である．ある $w_i^n, w_j^n \in C^{(n)}$ とある $x, y \in A^*$ について $w_j^n = x w_i^n y$ と仮定する．
初めに，$x \neq 1$ かつ $y \neq 1$ が起こらない事を示す．

$x \neq 1$ かつ $y \neq 1$ と仮定する．$n = 1$ ならば，$w_j = x w_i y$．これは C が infix であることに反する．従って $n \geq 2$ である．$|x| + n|w_i| + |y| = n|w_j|$ より $|w_j| > |w_i|$．x は w_j^n の左因子だから，$x = w_j^p \alpha$ となる，$p \geq 0$ と w_j の左因子 α が存在する．もし $\alpha = 1$ または $\alpha = w_j$ ならば，w_i は w_j の左因子となり，これは C が infix code であることに反する．従って α は w_j の 1 と異なる左因子である．$|\alpha w_i| \leq |w_j|$ ならば，w_i は w_j の内部因子となる．これは C が infix code であることに反する．従って $|\alpha w_i| > |w_j|$ である．よって，$\alpha\beta_1 = w_j$ となる w_i の左因子 $\beta_1 (\neq 1, w_i)$ が存在する．このとき $w_j^{p+1} = x\beta_1$ である．もし，$|\beta_1 w_j| \leq |w_i|$ ならば，w_j は w_i の内部因子となり C が infix code であることに反する．よって $|\beta_1 w_j| > |w_i|$．従って，$\beta_1 w_j = w_i \beta_2$ となる w_i の左因子が存在する．このとき $w_j^{p+2} = x w_i \beta_2$ である．この議論をくりかえすと，w_i の左因子 $\beta_1, \beta_2, \cdots, \beta_k, \cdots$, で $w_j^{p+k} = x w_i^{k-1} \beta_k$, $k = 1, 2, \cdots k, \cdots$, となるものが存在する．しかしながら，$k = n - p$ に対して，$w_j^n = x w_j^{n-p-1}$ であるが，これは $x w_i^n y$ の真の左因子であるから矛盾である．従って，$x \neq 1$ かつ $y \neq 1$ は起こりえない．
もし，$x = 1$ かつ $y \neq 1$ ならば，w_i は w_j の真の左因子である．これは矛盾．同様に $x \neq 1$ かつ $y = 1$ も起こりえない．従って、$C^{(n)}$ は infix code である．

上記の補題は直感的に明らかであろうが次の命題 5 の証明に必要不可欠であるので証明を書いた．C が conformal code ならば，命題 1 により，C は infix code である．従って補題 4 により，$C^{(n)}$ は infix code である．この事実を用いることにより次の命題を得る:

命題 5. C が conformal code の空でない部分集合ならば，$C^{(n)}$, $n \geq 2$, は extractable である．

証明略.

References

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

[2] Lallement, G. *Semigroup and Combinatorial Applications.* Wiley. 1979.

[3] Shyr, H.J., *Free Monoids and Languages.* 2nd edition. Hon Min Book Company, Taichung, Taiwan. 1991

[4] Tamura, T. Theory of Semigroups, Kyoritu-Shuppan, Tokyo,1972. (In Japanese)

[5] Tanaka, G. Prefix codes determined by Petri nets, Algebra Colloquium 5:3, pp.255-264 (1988)

[6] Tanaka, G. Limited codes associated with Petri nets, *Acta Cybernetica*, 19 (2009), pp.217-230.

[7] Tanaka, G., Kunimochi, Y., and Katsura, M. Remarks on extractable codes, In Kometa. J.(ed.) *Proc. Symposium on Algebras, Languages, Computations and their Applications, RIMS Kokyuroku*, No.1655, pp.106-110, (2009).

[8] Tanaka, G. On constructions of extractable codes, In Tsuji. K.(ed.) *Proc. Symposium on Algebras, Languages, Algorithms in Algebraic Systems and Computations, RIMS Kokyuroku*, No.1712, pp.27-38, (2010).