Séminaire Dubreil.
Algèbre et théorie
des nombres

Dominique Perrin

Codes bipréfixes et groupes de permutations

Séminaire Dubreil. Algèbre et théorie des nombres, tome 28, n° 1 (1974-1975), exp. n° 13, p. 1-6

<http://www.numdam.org/item?id=SD_1974-1975__28_1_A8_0>

Séminaire P. DUBREIL
(Algèbre)
28e année, 1974/75, n° 13, 6 p.

10 mars 1975

CODES BIPRÉFIXES ET GROUPES DE PERMUTATIONS

par Dominique PERRIN

Les codes bipréfixes sont des ensembles de mots possédant de remarquables propriétés combinatoires. Ils ont été introduits par M. P. SCHÜTZENBERGER dans le cadre plus général de la théorie des codes, qui sont un objet fondamental de l'étude combinatoire du monoïde libre.

A tout code bipréfixe fini est associé un groupe de permutations, et le but de cet exposé est de montrer qu'on obtient ainsi une présentation non classique de groupes fortement transitifs. Nous ne donnons pas ici les preuves des résultats ; elles figurent dans notre thèse de Doctorat, en cours d'achèvement.

I. Codes bipréfixes

1. Notations.

Etant donné un ensemble fini X, on note X^* le monoïde libre sur l'ensemble X ; et pour un mot f de X^*, on note $\tilde{f}$ l'image-miroir de f : si $f=x_1 x_2 \dots x_n$, avec $x_i \in X$, alors $\tilde{f} = x_n x_{n-1} \dots x_1$.

On dira qu'une partie L de X^* est rationnelle s'il existe un homomorphisme φ de X^* sur un monoïde fini M qui sature L, i. e. $\varphi^{-1}\varphi L = L$.

Pour toute partie L de X^*, on notera $\tilde{L}$ l'ensemble des images-miroir des mots de L : $\tilde{L} = \{\tilde{f} \ ; \ f \in L\}$.

On notera $\underset{\sim}{L}$ la série caractéristique d'une partie L de X^* ; c'est un élément de l'algèbre large $\mathbb{Z}\langle\langle X\rangle\rangle$: $\underset{\sim}{L} = \sum_{\ell \in L} \ell$.

2. Codes bipréfixes.

Définition. - Un code bipréfixe est une partie A de X^* vérifiant les deux conditions suivantes :

1° A ne contient aucun des facteurs gauches ou droits d'un de ses éléments.

2° A est maximal pour cette propriété.

Remarquons que si A est un code bipréfixe, il en est de même de $\tilde{A}$.

Le sous-monoïde engendré par un code bipréfixe A est évidemment isomorphe au monoïde libre sur l'ensemble A. De plus, ces sous-monoïdes sont caractérisés ainsi, dans le cas où ils sont rationnels (et donc en particulier dans le cas où ils sont finiment engendrés) :

PROPOSITION [3]. - Un sous-monoïde rationnel P de X^* est engendré par un code bipréfixe si, et seulement si,

1° $\forall\, u, v \in X^*$, $(u, uv \in P) \Longrightarrow (v \in P)$ et $(v, uv \in P) \Longrightarrow (u \in P)$,

2° tout mot de X^* a une puissance dans P.

Ce résultat nous permet de donner des exemples de codes bipréfixes.

Exemple 1. - Pour tout entier $n \in \underset{\sim}{N}$, l'ensemble de tous les mots de longueur n est un code bipréfixe nommé code homogène de longueur n.

Exemple 2. - Soient G un groupe fini, H un sous-groupe de G, et φ un homomorphisme de X^* sur G ; l'image réciproque $p = \varphi^{-1}(H)$ de H est engendré par un code bipréfixe.

L'exemple 1 correspond au cas $G = \underset{\sim}{Z}/n$ et $H = \{1\}$; on démontre [3] que c'est le seul cas où le code bipréfixe obtenu est fini.

3. La construction des codes bipréfixes finis.

Soit A un code bipréfixe sur X ; on dira qu'un mot $f \in X^*$ est bon pour A si l'ensemble des mots de A dont il est facteur gauche, et celui des mots de A dont il est facteur droit, sont deux ensembles non vides et disjoints.

Soit alors f un bon mot pour A, et soient G, D les ensembles :

$$G = \{g \in X^* \ ; \ gf \in A\} \ ; \quad D = \{d \in X^* \ ; \ fd \in A\} .$$

L'ensemble B défini par l'égalité : $\underset{\sim}{B} = \underset{\sim}{A} + (1 - \underset{\sim}{G})f(1 - \underset{\sim}{D})$ est un code bipréfixe ; on dit que B dérive de A relativement au bon mot f.

THÉORÈME [1]. - Tout code bipréfixe fini peut être obtenu par dérivations successives à partir d'un code homogène.

On nommera degré d'un code bipréfixe la longueur du code homogène dont il dérive. On voit aisément que le degré d'un code bipréfixe A est l'entier n tel que $x^n \in A$, pour tout $x \in X$.

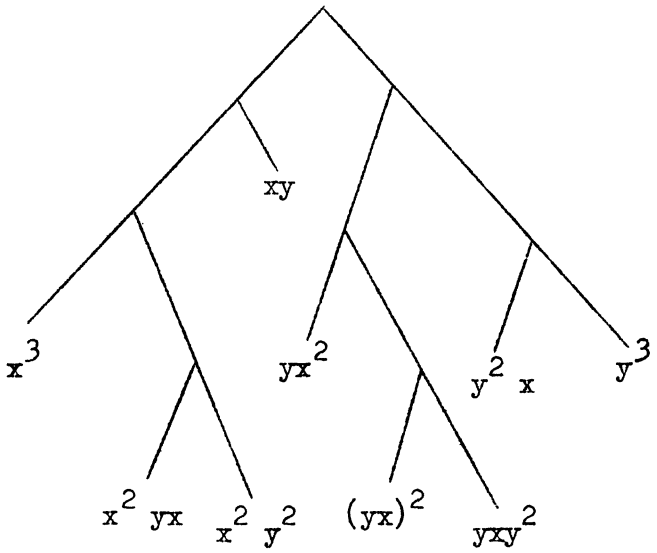
On sait (cf. [3]) que le nombre de codes bipréfixes finis de degré donné n est fini ; notons B(n) ce nombre, et examinons à titre d'exemple les cas $n = 2,3,4$ sur un alphabet $X = \{x, y\}$ à deux éléments.

(a) $B(2) = 1$: le seul code bipréfixe fini de degré 2 est X^2.

(b) $B(3) = 3$: le code homogène de longueur 3 admet deux bons mots : xy et yx. Les deux dérivés de X^3 relativement à ces mots sont image-miroir l'un de l'autre puisque $\widetilde{xy} = yx$ (ils sont aussi échangés par l'automorphisme de X^* qui échange x et y).

Le dérivé de X^3 relativement à xy, par exemple, peut être représenté graphi-

quement ainsi :



Ce code n'admet aucun bon mot, et il n'y a donc que trois codes bipréfixes finis de degré 3 sur un alphabet à deux lettres.

(c) $B(4) = 73$.

II. Groupe d'un code bipréfixe fini

1. Le groupe $G(A)$.

Soit A un code bipréfixe sur X ; soit S l'ensemble des facteurs gauches propres des éléments de A .

Tout mot $f \in A^*$ définit une application $f\varphi$ de S dans lui-même de la manière suivante $\forall\, s \in S$, $sf\varphi = t$ si $sf \in A^* t$.

L'application $f \longmapsto f\varphi$ est un homomorphisme de X^* dans le monoïde des applications de S dans lui-même.

Si le code A est fini, le monoïde $X^*\varphi$ est fini. Son idéal minimal est une union de groupes de permutations équivalents ; on désigne par $G(A)$, nommé groupe de A , cette classe d'équivalence ([1]). On voit facilement que l'on obtient la proposition suivante.

PROPOSITION. - Le groupe d'un code bipréfixe fini de degré n est un groupe transitif de degré n contenant un cycle de longueur n .

Exemple 1. - Le groupe du code homogène de longueur n est $\mathbb{Z}/n$. Réciproquement, on montre qu'un code bipréfixe fini dont le groupe est $\mathbb{Z}/n$ est homogène [2].

([1]) Le groupe $G(A)$ est aussi isomorphe au groupe de structure de l'idéal minimal du monoïde syntaxique de A^* ; on peut ainsi définir $G(A)$ pour tout code bipréfixe rationnel.

Exemple 2. - Les deux codes bipréfixes finis non homogènes de degré 3 ont un groupe équivalent au groupe symétrique S_3 .

2. Groupes imprimitifs.

Posons une définition : étant donnés deux codes bipréfixes A et B , si A est inclus dans le sous-monoïde B^* engendré par B , son image dans le monoïde libre sur l'ensemble B est encore un code bipréfixe qu'on notera C . On dit dans ce cas que A se décompose sur B , et on note $A = C \otimes B$.

Le degré de A est alors le produit des degrés de C et B . On dit qu'un code A est indécomposable s'il ne se décompose que sur lui-même et sur X .

THÉORÈME [2]. - Un code bipréfixe fini est décomposable si, et seulement si, le groupe G(A) est imprimitif.

Il y a en fait, plus précisément, bijection entre les systèmes d'imprimitivité de G(A) et les codes B tels que A se décompose sur B .

Exemple 1. - Tout code bipréfixe fini de degré 4 , non homogène, a un groupe isomorphe au groupe symétrique S_4 . En effet, les seuls groupes de degré 4 contenant un 4-cycle sont $\mathbb{Z}/4$, S_4 et le groupe diétral D_4 . Mais ce dernier est imprimitif, et un code dont le groupe serait équivalent à D_4 serait décomposable ; cela est impossible puisqu'il n'existe qu'un code bipréfixe fini de degré 2 , qui est homogène.

Exemple 2. - Soit n un entier impair, et soit A un code dérivé du code homogène X^n relativement à un bon mot de longueur impaire. Tous les mots de A sont alors de longueur impaire. Ainsi A^2 se décompose à la fois sur A et sur X^2 . Son groupe $G(A^2)$ est isomorphe au produit direct $\mathbb{Z}/2 \times G(A)$.

3. Le degré minimal de G(A) .

Rappelons que le degré minimal d'un groupe de permutations G de degré n est l'entier $n - k$, où k est le nombre maximum de points que fixe un élément de G (qui n'est pas l'élément neutre).

Le résultat suivant montre que, pour un code bipréfixe fini de degré n dont le groupe a un degré minimal d , la différence $n - d$ tend vers l'infini avec n .

THÉORÈME. - Soit A un code bipréfixe fini de degré n , non homogène ; le degré minimal d du groupe G(A) vérifie l'inégalité $d \leqslant n - (\sqrt{n}/2) + 1$.

Et dès que n est au moins égal à 4 , on a $d \leqslant n - 2$.

Ainsi, en particulier, dès que n est différent de 3 , le groupe G(A) ne peut être un groupe de Frobénius (pour $n = 3$, ce cas peut évidemment se produire puisque le groupe symétrique est de degré minimal 2) ; de même, le groupe G(A) ne

peut pas non plus être un groupe de Zassenhaus ($d = n - 2$) dès que $n \geq 37$ (on peut montrer qu'il suffit en fait que $n \geq 15$).

4. Groupes primitifs.

D'après ce que nous avons vu, le groupe $G(A)$ est primitif si, et seulement si, le code est indécomposable. Une conséquence du résultat précédent est le théorème suivant.

THÉORÈME. - Soit A un code bipréfixe fini qui n'est pas homogène. Alors si A est indécomposable, $G(A)$ est deux fois transitif.

Nous verrons plus bas qu'il existe des codes bipréfixes dont le groupe est deux fois transitif, mais pas trois fois.

5. Groupes de petit degré.

Nous présentons maintenant une classification des codes de petit degré ($n \leq 9$) d'après leur groupe.

Nous donnons pour chaque entier n la liste des groupes réalisables de degré n (i. e. qui sont les groupes de codes bipréfixes finis), les autres ne l'étant pas en vertu des résultats précédents.

Nous avons déjà examiné les cas des degrés 2 , 3 ou 4 .

En degré 5 , il existe, en dehors du code homogène, deux classes de codes bipréfixes, suivant que leur groupe est le groupe symétrique S_5 ou le groupe alterné A_5 .

En degré 6 , il existe deux classes de codes bipréfixes indécomposables selon que $G(A) \simeq S_6$ ou $G(A) \simeq PGL(2 , 5)$, le groupe projectif linéaire, en dimension 2 sur le corps $\mathbb{F}_5$ (qui est isomorphe à S_5).

En degré 7 , hormis les codes dont le groupe est $\mathbb{Z}/7$, A_7 ou S_7 , il existe une classe de codes bipréfixes dont le groupe est équivalent à $GL(3 , 2)$, le groupe linéaire en dimension 3 sur $\mathbb{F}_2$; on remarque que ce groupe est 2-transitif mais pas 3-transitif.

Les codes indécomposables de degré 8 ont un groupe équivalent au groupe symétrique S_8 ou au groupe $PGL(2 , 7)$.

En degré 9 , hormis les groupes alternés et symétriques, il existe deux groupes primitifs réalisables : le groupe $PGL(2 , 8)$ et son produit semi-direct par son groupe d'automorphismes extérieur, noté $P\Gamma L(2 , 8)$.

Signalons enfin que le groupe de Mathieu de degré 11 , M_{11} , est réalisable.

BIBLIOGRAPHIE

[1] CESARI (Y.). - Sur un algorithme donnant les codes bipréfixes finis, Math. Syst. Theory, t. 6, 1972, p. 221-225.

[2] PERROT (J.-F.). Contribution à l'étude des monoïdes syntaxiques et de certains groupes associés aux automates finis, Thèse Sc. math., Paris 1972.

[3] SCHÜTZENBERGER (M. P.). - On a special class of recurrent events, Annals of math. Stat., t. 32, 1961, p. 1201-1213.

(Texte reçu le 7 mai 1975)

Dominique PERRIN
Département de Mathématiques
Université de Paris-7, Tour 55
2 place Jussieu
75221 PARIS CEDEX 05