

The groups of codes with empty kernel

Meeting in the honor of Toni Machì

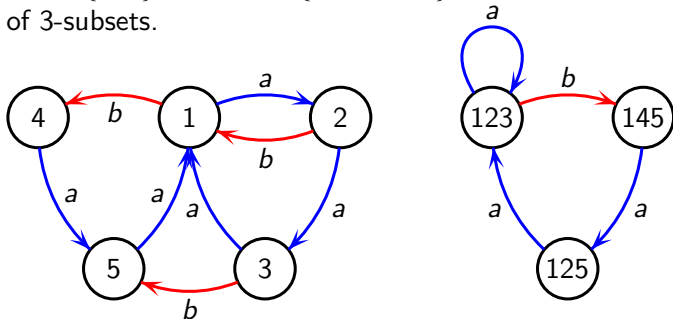
Jean Berstel, Clelia De Felice, Dominique Perrin, Giuseppina
Rindone

10 mars 2011

- 1 Motivating example
- 2 Starting point : Schützenberger's theorem
- 3 Holonomy groups
- 4 Main result
- 5 Examples
- 6 Codes and unambiguous automata
- 7 Sketch of proof
- 8 Abelian groups

Motivating example

An action of $\{a, b\}$ on the set $\{1, 2, 3, 4, 5\}$ and the associated action of 3-subsets.



The words a and baa fix globally the set $\{1, 2, 3\}$. Their action generates the group S_3 (holonomy group).

$$a \rightarrow (123) \quad ba^2 \rightarrow (23)$$

Question : how can one easily predict the groups which will occur ?

Variety of monoids (groups) : family closed by homomorphisms, submonoids (subgroups), direct product.
pseudovariety : finite direct products only.

Theorem

The family of finite monoids containing only groups in a pseudovariety V of groups forms a pseudovariety of monoids.

Examples :

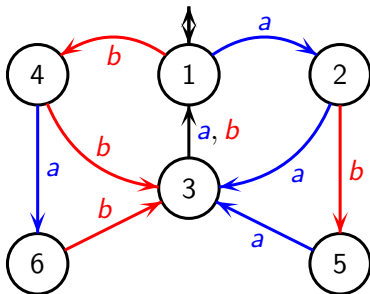
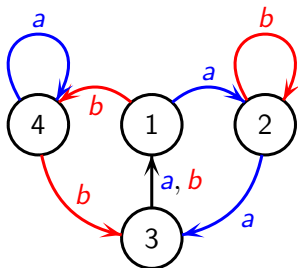
- Trivial groups : aperiodic monoids
- Abelian groups
- ...

The desintegration of groups

Start with the alternating group A_4 generated by $a = (123)$ and $b = (143)$.

Keep only the paths from 1 to 1 which do not have a factor which is also a path from 1 to 1 : finite set of paths.

All holonomy groups are cyclic (ba gives $(16)(23)$).



The starting point

Semaphore code : the set of first words of a left ideal (= first occurrence of a pattern).

Synchronized prefix code X on the alphabet A : there exists a synchronizing word x , i. e. $A^*x \subset X^*$.

Example

$X = a^*b$ is semaphore (first b). It is synchronized : $x = b$ is synchronizing.

$X = (a + ba)^*bb$ is semaphore (first bb). It is synchronized : $x = abb$ is synchronizing.

$X = a^*ba^*b$ is semaphore (the count of b is 2 for the first time). It is not synchronized.

Schützenberger's theorem

Theorem (Schützenberger, 1964)

Any semaphore code is of the form $Y = X^n$ where X is a synchronized semaphore code and $n \geq 1$.

Two proofs :

- Direct combinatorial (very intricate)
- Using the permutation groups and transformation semigroups.

Example

$X = a^*b$ and $Y = a^*ba^*b$ with $n = 2$.

Group of a maximal prefix code X : a transitive permutation group which is trivial iff X is synchronized.

Proposition

The group of a semaphore code is cyclic.

Composition of codes = composition of morphisms :

$$C \xrightarrow{\gamma} Y \subset B^*, \quad B \xrightarrow{\beta} Z \subset A^*$$

gives $C \xrightarrow{\beta\gamma} X$ denoted $X = Y \circ Z$

Example

$$X^n = B^n \circ X$$

$d(X)$ = degree of the permutation group $G(X)$.

Proposition

If $X = Y \circ Z$, then $d(X) = d(Y)d(Z)$.

For example, if X is synchronized, $G(X^n)$ is cyclic of order n .

Proposition

The group of a maximal prefix code is regular if and only if $X = Y \circ Z \circ T$ where Y, T are synchronized and Z is a regular group code.

Group code : $Z^* = \alpha^{-1}(H)$ for $\alpha : A^* \rightarrow G$ morphism on a group G and H subgroup of G .

Example

Let $X = a^*ba^*b$. Then $X = a^*(Z \setminus a)$ with $Z = a \cup ba^*b$.
Fortunately, one has also $X = Z \circ T$ with $Z = B^2$ and $T = a^*b$.

Let M be a monoid of transformations on a set Q . For $P \subset Q$, let

$$\text{Stab}(P) = \{m \in M \mid Pm = P\}$$

The restriction of $\text{Stab}(P)$ to P is a permutation group called the **holonomy group** of M relative to P (Eilenberg).

The holonomy groups of an automaton \mathcal{A} are those of its monoid of transitions $M(\mathcal{A})$.

The group $G(X)$ of a maximal prefix code X is the holonomy group of its minimal automaton \mathcal{A} relative to a image of minimal cardinality of an element of $M(\mathcal{A})$.

$G(X)$ is trivial if and only if X is synchronized.

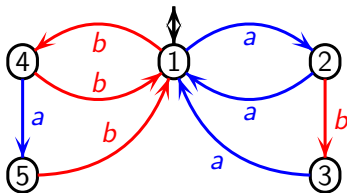
A word s is an **internal** factor of w if $w = rst$ with r, s nonempty.
Kernel of $X = X \cap$ internal factors of X

Theorem

Let $X \subset A^+$ be a finite prefix code with empty kernel. Let $\mathcal{A} = (Q, 1, 1)$ be an automaton recognizing X^ . Then any holonomy group of \mathcal{A} is cyclic and regular.*

Example 1

Let $X = \{aa, aba, bab, bb\}$. The set X is an infix code. The minimal automaton \mathcal{A} of X^* is



The transition monoid M of \mathcal{A} contains groups which are cyclic of order 1, 2 or 3. For example, ab contains the cycle (134) while a contains the cycle (12) .

Let us note an interesting feature of this example. Any word w in $(a \cup babb^*aba)^*$ fixes globally the set $\{1, 2\}$ and defines a cyclic group of order 2. But the set of these words is a submonoid which is not cyclic and not even finitely generated.

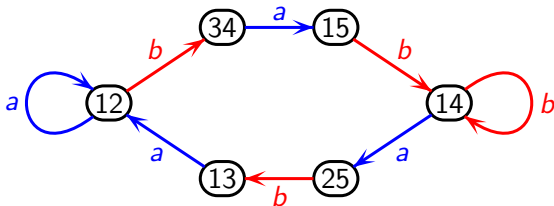


FIG.: The action of A^* on the 2-element subsets reachable from $\{1, 2\}$

Example 2

Let $X = \{aaa, aab, abaa, abab, baba, babb, bba, bbb\}$. The set X is an infix code. The minimal automaton of X^* is

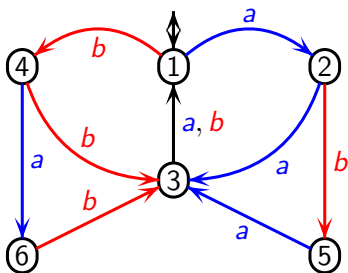


FIG.: An infix code with a group of degree 4 and order 2.

The transition monoid $M = \varphi(A^*)$ of \mathcal{A} contains cyclic groups of degree 1, 2, 3 and 4. For example the word a contains the cycle (123) . In turn, ba contains the permutation $(16)(23)$.

This example shows another interesting feature. Consider the group G containing $\varphi(ba)$. The neutral element of G is $e = \varphi(baba)$ and its set of fixpoints is $\{1, 2, 3, 6\}$. The group G is of degree 4. It is composed of the permutation $(16)(23)$ and the identity. It is thus of order 2. Actually, M does not contain any cyclic group of order 4.

From groups to monoids

Let G be a transitive permutation group on $R = \{1, 2, \dots, n\}$ and let $\varphi : A^* \rightarrow G$ be a surjective morphism. Let H be the subgroup of G which fixes 1. Let Z be the bifix code generating the submonoid $\varphi^{-1}(H)$. Let X be the set of elements of Z which have no proper factor in Z .

Proposition

The set X is a finite infix code. The groups in the syntactic monoid M of X^ , not reduced to the neutral element of M , are cyclic and regular of degree at most n .*

Example 1 again

Let G be the symmetric group on the set $R = \{1, 2, 3\}$ and let $A = \{a, b\}$. Let $\varphi : A^* \rightarrow G$ be the morphism defined by $\varphi(a) = (12)$, $\varphi(b) = (13)$. The bifix code Z is the infinite set represented on the left and the code X on the right. It is the code of Example 1.

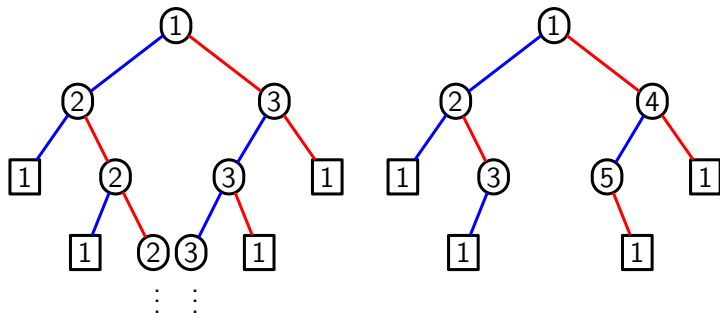


FIG.: The infinite group code Z and the finite code X

Example 2 again

The code X of Example 2 corresponds to the above construction with G being the alternating group on the set $\{1, 2, 3, 4\}$ and $\varphi(a) = (123)$, $\varphi(b) = (143)$.

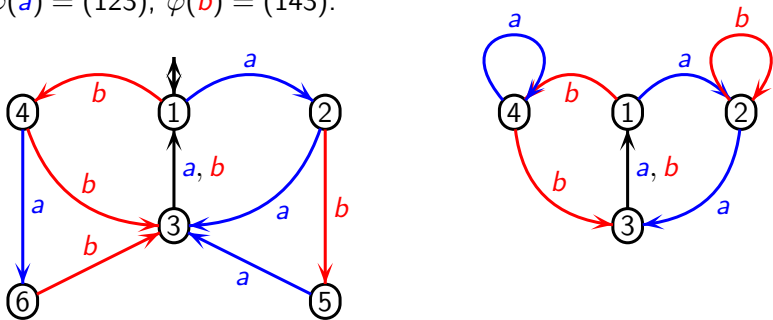


FIG.: An infix code with a group of degree 4 and order 2.

Note that a^2ba^2 is an element of rank 2 which contains the transposition (13) which does not belong to A_4 .

Example 3

Let φ be the morphism onto the alternating group A_5 defined by $\varphi(a) = (123)$, $\varphi(b) = (145)$. We obtain $X = \{aaa, aaba, aabba, abaa, ababa, abbaa, baabb, babab, babb, bbaab, bbab, bbb\}$. The transitions of the minimal automaton \mathcal{A} of X^* are .

	1	2	3	4	5	6	7	8	9	10	11	12	13
a	2	3	1	8	9	7	1	13	10	—	1	11	—
b	4	6	7	5	1	12	11	9	1	1	—	—	10

The monoid $M(\mathcal{A})$ has 14351 elements (software Semigroupes).

- ab contains the cycle (1 6 11 4 9).
- $a^2ba^2b^2$ contains the permutation (1 12)(5 11) of degree 4 but there is no cyclic group of order 4 in M .
- a and b contains cycles of degree 3.
- a^4ba^5 contains the identity on $\{1, 2\}$ and $a^2bab^2a^2ba^4$ contains the transposition (1 2).

Codes and unambiguous automata

Code : basis of a free submonoid of A^* .

Unambiguous automaton : at most one path with given origin, label and end.

Unambiguous monoid of relations M on a set Q : for $p, q \in Q$ and $m, n \in M$, there is at most one $r \in Q$ such that $(p, r) \in m$ and $(r, q) \in n$.

Holonomy groups : the same (in a monoid of unambiguous relations, the invertible relations are permutations).

Example

Let $X = \{aa, bb, baa, bba\}$. The set X is a code with empty kernel.
An unambiguous automaton recognizing X^* :

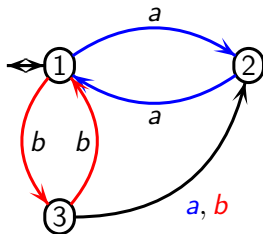


FIG.: A code with empty kernel defining cyclic groups of order 2.

The word a contains the cycle (12) and the word b the cycle (13) .

Sketch of proof

- Interpretations
- Cyclic set of interpretations
- Two lemmas
- Conclusion

Interpretations

Let $X \subset A^+$ be a code. Let P be the set of proper prefixes of the words of X and let S be the set of proper suffixes of the words of X . An **interpretation** of a word $w \in A^*$ with respect to X is a factorization $\alpha = (s, x_1, x_2, \dots, x_n, p)$ of w such that $s \in S$, $n \geq 0$, $x_i \in X$ and $p \in P$.

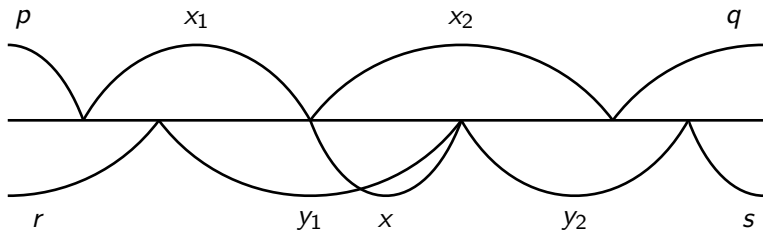
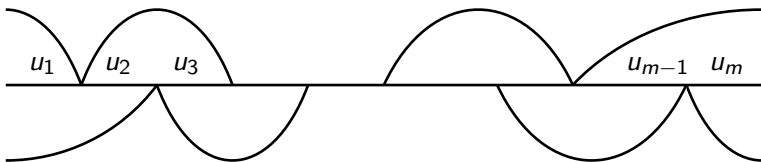


FIG.: Two connected interpretations

Cyclic set of interpretations

A factorization (u_1, u_2, \dots, u_m) of a word w is said to be **n -periodic** with respect to a code X if for any r, ℓ with $1 \leq \ell \leq r \leq m-1$, one has $u_{\ell+1} \cdots u_r \in X$ if and only if $r - \ell = n$. Thus, in other terms, the factorization is n -periodic if and only if the number of consecutive nonempty factors u_i with $2 \leq i \leq m-1$ whose product is in X is constant and equal to n . A set I of n interpretations of a word w with respect to a code X is said to be **cyclic** if the supremum (u_1, u_2, \dots, u_m) of the n interpretations is n -periodic with respect to X .



Lemma

Let $X \subset A^+$ be a code with empty kernel. Any set of independent interpretations of a word with respect to X is cyclic.

Lemma

Let $X \subset A^+$ be a finite prefix code. Let \mathcal{A} be the minimal automaton of X^* . Let G be a holonomy group of \mathcal{A} with respect to $R \subset Q$. For any any word $w \in \varphi_{\mathcal{A}}^{-1}(G)$ which is not an internal factor of X and each $r \in R$, there is a unique interpretation α_r of w such that there are paths $r \xrightarrow{s_{\alpha_r}} 1$ and $1 \xrightarrow{p_{\alpha_r}} rg$ which are simple or null. Moreover, the set $I = \{\alpha_r \mid r \in R\}$ is formed of independent interpretations.

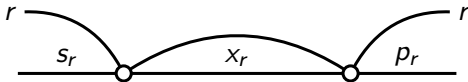


FIG.: The interpretation α_r .

Conclusion

Set $R = \{1, 2, \dots, n\}$.

We may suppose that s_i is a proper prefix of s_{i+1} for $1 \leq i < n$.

All elements of G are powers of the permutation $\alpha = (1\ 2 \cdots n)$.

This implies the conclusion since a subgroup of a cyclic and regular group is also cyclic and regular.

Observe that α is not necessarily in the group.

For a variety \mathbf{V} of monoids, the **associated** variety of sets is the set of $S \subset A^*$ such that the syntactic monoid of S is in \mathbf{V}

Let \mathbf{V} be the variety of finite monoids containing only Abelian groups. Let \mathcal{V} be the associated variety of sets. This variety has been studied by Schützenberger, who has described the variety \mathcal{V} using another closure property.

Theorem

For any code X with empty kernel which belongs to \mathcal{V} , the set X^ is in \mathcal{V} .*