# Aperiodic languages 

Dejan Ničković

Verimag, Grenoble

## Table of Contents

- Introduction
- Aperiodic Sets
- Star-Free Regular Sets
- Schützenberger's theorem
- $\mathrm{SF} \rightarrow \mathrm{AP}$
- Semigroups and Monoids
- Morphisms
- Recognizability
- Transition Monoid
- Syntactic Monoid
- Ideals
- Green Relations
- $\mathrm{AP} \rightarrow \mathrm{SF}$
- Example


## Introduction

- First (and most) significant subclass of regular languages.
- For a language $L \subset A^{*}$, the following conditions are equivalent:
- $L$ is first-order definable (in the signature $<$ )
- L is definable in linear temporal logic (past)
- $L$ is star-free regular
- L is recognized by a counter-free automaton
- Syntactic monoid of $L$ is aperiodic
- Note: Similar results hold for $\omega$-regular star-free languages
- There is an algorithm to decide whether a given recognizable language is star-free


## Aperiodic Sets

- A set $X \subset A^{*}$ is said to be aperiodic if there exists an integer $n>0$ such that for all $u, x, v \in A^{*}$ one has

$$
u x^{n} v \in L \Leftrightarrow u x^{n+1} v \in L
$$

- An automaton is counter-free if there is no word $w$ that permutes a non-trivial subset of $Q$


## Aperiodicity - Intuition



Counter modulo 3


Periodic semigroup generated by $x$ with period $p\left(x^{n}=x^{n+p}\right)$


Counter saturating at 2


Aperiodic semigroup generated by $x$ with index $n\left(x^{n}=x^{n+1}\right)$

## Star-Free Regular Sets

- The set of regular subsets of $A^{*}$ is the smallest set of subsets of $A^{*}$ closed under finite union, concatenation and Kleen star.
- The set of star-free subsets of $A^{*}$ is the smallest set of subsets of $A^{*}$ containing the finite sets and closed under all finite boolean operations and concatenation.
- Extended regular expressions without the Kleene star operator
- Examples:
- $\emptyset$
- $A^{*}=\bar{\emptyset}$
- $(a b)^{*}=\epsilon+\left(a A^{*} \cap A^{*} b\right) \cap \overline{\left(A^{*} a a A^{*} \vee A^{*} b b A^{*}\right)}$
- $(a b \vee b a)^{*}=\overline{\overline{\left(A^{*} a\right)} b(a b)^{*} \overline{\left(a A^{*}\right)}+\overline{\left(A^{*} b\right)}(a b)^{*} a \overline{\left(b A^{*}\right)}}$


## Star-free and Aperiodic Sets

- A rational set $X \subset A^{*}$ is star-free iff it is aperiodic
- Two proofs:
- Schützenberger (based on structure of monoids)
- SF $\rightarrow$ AP : easy
- AP $\rightarrow$ SF : much more difficult
- Use Krohn-Rhodes Decomposition


## Schützenberger's Theorem - SF $\rightarrow$ AP

- Let $i(X)$ be the smallest index that saturates aperiodic set $X \in A^{*}$
- $\quad i(a)=2$ for $a \in A$ (trivial)
- $i(X \cup Y) \leq \min (i(X), i(Y))$ (trivial)
- $i(\bar{X})=i(X)$ (trivial)
- $i(X Y) \leq i(X)+i(Y)$
- Proof
- Let $N=m+n+1$ st $N \geq i(X)+i(Y)$
- Let $u x^{m} r \in X$ and $s x^{n} v \in Y$ such that $x=r s$. Then $u x^{N} v \in X Y$. Either $m \geq i(X)$ or $n \geq i(Y)$. In the first case $u x^{m+1} r \in X$.
- Hence $u x^{m+1} r s x^{n} v=u x^{m+n+2} v=u x^{N+1} v \in X Y$.
- Second case and the other direction of the proof are similar.


## Semigroups and Monoids

- A semigroup is a set equipped with an associative operation. A monoid is a semigroup equipped with an identity
- $(S, ., 1)$
- $a b \in S$ for $a, b \in S$
- $(a b) c=a(b c)$ for all $a, b, c \in S$
- $1 a=a 1=1$ for all $a \in S$
- Example:
- $A^{*}$ is the set of all words over an alphabet $A$ and is called the free monoid with the null word $\epsilon$ and the concatenation of words being the monoid product.
- $(\mathbb{N},+, 0)$
- $(\mathbb{N}, *, 1)$
- Note: We call zero of $S$ an element denoted by 0 such that $0 s=s 0=0$ for all $s \in S$.


## Morphisms

- A morphism between two algebraic structures is a map that preserves the operations and the relations of the structure (applies to semigroups and monoids).
- Given two semigroups $(S,$.$) and (T, *)$, a semigroup morphism $\varphi: S \rightarrow T$ is a map from $S$ into $T$ st for all $x, y \in S, \varphi(x \cdot y)=\varphi(x) * \varphi(y)$ (for monoid morphisms we also need the condition $\left.\varphi\left(1_{S}\right)=1_{T}\right)$.
- $T$ is said to be homomorphic to $S$ and we denote it by $T \leq_{\varphi} S$.
- Two mutually homomorphic semigroups are said to be isomorphic
- We are mainly interested in the homomorphisms from the infinite free monoid $A^{*}$ onto finite monoids.


## Recognizable Languages

- Recognizable languages usually defined in terms of automata
- Let $\mathcal{A}=(Q, A, E, I, F)$ be a finite automaton. The language recognized by $\mathcal{A}$ is the set (denoted by $L^{*}(\mathcal{A})$ ) of the labels of all paths having its origin in $I$ and its and in $F$.
- A language $L$ is recognizabe if there exists a finite automaton $\mathcal{A}$ st $L=L^{*}(\mathcal{A})$
- Recognizible languages coincide with the class of regular languages (Kleene)
- Handling the fine structure of recognizable languages is more appropriate using a more abstract definition, using monoids (or semigroups)
- A monoid morphism $\varphi: A^{*} \rightarrow M$ recognizes a language $L \subset A^{*}$ if $L=\varphi^{-1} \varphi(L)$
- If $u \in L$ and $\varphi(u)=\varphi(v)$ implies $v \in L$
- There is $P \subset M$ such that $L=\varphi^{-1}(P)$


## Transition Monoid

- Equivalence between automata and monoids
- Let $\mathcal{A}=(Q, A, E, I, F)$. To each word $w \in A^{*}$, there corresponds a relation on $Q$, denoted by $\varphi(w)$ and defined by $(p, q) \in \varphi(w)$ if there exists a path from $p$ to $q$ with label $w$.
- Monoid morphism: $\varphi$ : $A^{*} \rightarrow M(\mathcal{A})$
- Monoid morphism from $A^{*}$ into the semigroup of relations on $Q$
- Let $\mathcal{R}_{1}, \mathcal{R}_{2}$ be two relations on $Q$. Then $\mathcal{R}_{1} \mathcal{R}_{2}$ defined by $(p, q) \in \mathcal{R}_{1} \mathcal{R}_{2}$ iff there exists $r \in Q$ st $(p, r) \in \mathcal{R}_{1}$ and $(r, q) \in \mathcal{R}_{2}$.
- $\varphi\left(A^{*}\right)$ is called transition monoid (or transformation monoid) of $\mathcal{A}$ and is denoted by $M(\mathcal{A})$.
- A word $w$ is recognized by $\mathcal{A}$ iff $(p, q) \in \varphi(w)$ for some initial state $p$ and some final state $q$.
- If a finite automaton recognizes a language $L$, then its transition monoid recognizes $L$.


## Syntactic Monoid

- Let $L \subset A^{*}$. The syntactic congruence $\sim_{L}$ is defined over $A^{*}$ by $u \sim_{L} v$ iff for all $x, t \in A^{*}, x u y \in L \Leftrightarrow x v y \in L$
- Syntactic monoid of $L$ is the quotient monoid $M=A^{*} / \sim_{L}$.
- Each word in $A^{*}$ is mapped to the congruence class modulo $L$ of which that word is a member (many-to-one mapping).
- It is the smallest monoid recognizing $L$.
- Syntactic monoid recognizing $L$ is the transition monoid of the minimal deterministic automaton recognizing $L$.


## Syntactic Monoid - Example


$A=\{a, b\}$

| $L_{1}=(a b)^{*}, M_{1}=\varphi\left(L_{1}\right)$ |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | 1 | $\alpha$ | $\beta$ | 0 | $\alpha \beta$ | $\beta \alpha$ |
| 1 | 1 | 2 | 1 | / | 1 | / |
| 2 | 2 | / | 1 | 1 | / | 2 |

$L_{2}=(a a)^{*}, M_{2}=\varphi\left(L_{2}\right)$

|  | 1 | $\alpha$ | 0 |
| :--- | :--- | :--- | :--- |
| 1 | 1 | 2 | 1 |
| 2 | 2 | 1 | 1 |

$$
\begin{gathered}
M_{1}=\{1, \alpha, \beta, 0, \alpha \beta, \beta \alpha\} \\
\alpha \beta \alpha=\alpha, \beta \alpha \beta=\beta, \alpha^{2}=\beta^{2}=0 \\
\forall x, x^{2}=x^{3} \\
L_{1} \text { aperiodic }
\end{gathered}
$$

$$
M_{2}=\{1, \alpha, \beta\}
$$

$$
\alpha^{2}=1, \alpha^{3}=\alpha, \beta=0
$$

$$
\forall n, \alpha^{n} \neq \alpha^{n+1}
$$

$L_{2}$ not aperiodic

## Syntactic Monoid - Monoid Graph

| $\varphi\left((a b)^{*}\right)$ |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | 1 | $\alpha$ | $\beta$ | 0 | $\alpha \beta$ | $\beta \alpha$ |
| 1 | 1 | $\alpha$ | $\beta$ | 0 | $\alpha \beta$ | $\beta \alpha$ |
| $\alpha$ | $\alpha$ | 0 | $\alpha \beta$ | 0 | 0 | $\alpha$ |
| $\beta$ | $\beta$ | $\beta \alpha$ | 0 | 0 | $\beta$ | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $\alpha \beta$ | $\alpha \beta$ | $\alpha$ | 0 | 0 | $\alpha \beta$ | 0 |
| $\beta \alpha$ | $\beta \alpha$ | 0 | $\beta$ | 0 | 0 | $\beta \alpha$ |



Example: $\varphi(a)=\varphi(a b a)=\varphi(a b a b a)=\alpha$
$\alpha$ is the class of words which need abin order to be accepted.

## Sketch of Proof AP $\rightarrow$ SF

- Show that each subset of an aperiodic monoid can be rewritten as a bollean compination of left, right and full ideals that it generates.
- Write the inverse morphism of the aperiodic monoid as a boolean combination of sets of prefix and suffix patterns of the words that are part of the language recognized by that monoid, as well as of the patterns not allowed in the middle of the accepted words.
- Prove by induction on the cardinality of the $\mathcal{J}$-classes of the aperiodic monoid that the sets generated by the inverse morphism are star-free.


## Ideals

- Let $S$ be a semigroup and $M=S \cup\{1\}$ a monoid.
- Right ideal of $S$ is $R \subset S$ such that $R M=R$
- Left ideal of $S$ is $L \subset S$ such that $M L=L$
- Ideal of $S$ is $I \subset S$ such that $M I M=I$
- Example: Let $P$ be the set of pair positive integers. $P$ is an ideal of $\mathbb{Z}$.
- A principal ideal $I$ in a monoid $M$ if it is generated by a single element $m \in M$.
- Example: Let $P=2 \mathbb{Z} . P$ is a principal ideal of $\mathbb{Z}$.


## Ideals - Example



## Green Relations

- Let $M$ be a monoid. We define 4 equivalence relations over $M(\mathcal{L}, \mathcal{R}, \mathcal{J}$ and $\mathcal{H})$, called Green relations:
- $a \mathcal{R} b \Leftrightarrow a M=b M$
- $a \mathcal{L} b \Leftrightarrow M a=M b$
- $a \mathcal{J} b \Leftrightarrow M a M=M b M$
- $a \mathcal{H} b \Leftrightarrow a \mathcal{R} b \cap a \mathcal{L} b$
- $a \mathcal{D} b$ iff $\exists c \in M$ st $a \mathcal{L} c$ and $c \mathcal{R} b$
- So $a \mathcal{R} b$, if there exist $c, d \in M$ such that $a c=b$ and $b d=a$.
- $\quad a$ and $b$ are $\mathcal{R}$-related if they generate the same right (principal) ideal.


Given that $M$ is a finite monoid and $m, n \in M, m \mathcal{D} n$ iff $m \mathcal{J} n$.

## Green Relations - Example

|  | 1 | $\alpha$ | $\beta$ | 0 | $\alpha \beta$ | $\beta \alpha$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 1 | $\alpha$ | $\beta$ | 0 | $\alpha \beta$ | $\beta \alpha$ |
| $\alpha$ | $\alpha$ | 0 | $\alpha \beta$ | 0 | 0 | $\alpha$ |
| $\beta$ | $\beta$ | $\beta \alpha$ | 0 | 0 | $\beta$ | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $\alpha \beta$ | $\alpha \beta$ | $\alpha$ | 0 | 0 | $\alpha \beta$ | 0 |
| $\beta \alpha$ | $\beta \alpha$ | 0 | $\beta$ | 0 | 0 | $\beta \alpha$ |

$$
\begin{array}{ll}
1 M=M & M 1=M \\
0 M=0 & M 0=0 \\
\alpha M=\{\alpha, \alpha \beta, 0\} & M \alpha=\{\alpha, \beta \alpha, 0\} \\
\beta M=\{\beta, \beta \alpha, 0\} & M \beta=\{\beta, \alpha \beta, 0\} \\
\alpha \beta M=\alpha M(\alpha \beta \mathcal{R} \alpha) & M \alpha \beta=M \beta(\alpha \beta \mathcal{L} \beta) \\
\beta \alpha M=\beta M(\beta \alpha \mathcal{R} \beta) & M \beta \alpha=M \alpha(\beta \alpha \mathcal{L} \alpha)
\end{array}
$$

## Green Relations - Example

$\mathcal{L}$-classes


## Schützenberger's Theorem - Lemma 1

- Lemma 1 Let $M$ be an aperiodic monoid and let $p, q, r \in M$. If $p q r=q$, then $p q=q=q r$.
- Simplification rule (SR)
- Proof

○ Let $p q r=q$. Then $p^{n} q r^{n}=q$ (let $n$ be the index of $M$ )

- $p^{n+1} q r^{n}=p^{n} q r^{n}=q$ ( $M$ aperiodic)
- $q=p\left(p^{n} q r^{n}\right)=p q$
- Similar for $q=q r$
- Example:
- $\alpha \beta \alpha \beta \alpha=\alpha$
- $\alpha \beta \alpha=\alpha \beta \alpha=\alpha$


## Schützenberger's Theorem - Lemma 2

- Lemma 2 Let $M$ be an aperiodic monoid and let $p, q, r \in M$. Then $\{q\}=(q M \cap M q) \backslash J_{q}$, with $J_{q}=\{s \in M \mid q \notin M s M\}$.
- Intuition: decompose each subset of M into a boolean combination of right ideals, left ideals and ideals.
- Proof

1. $q \in(q M \cap M q) \backslash J_{q}$ (trivial)
2. Let $s \in(q M \cap M q) \backslash J_{q}$
3. $\exists p, r$ st $s=p q=q r($ by (2))
4. $s \notin J_{q}$. Hence $q \in M s M$ (by definition of $J_{q}$ )
5. $\exists u, v$ st $q=u s v$ (by (4))
6. Replace $s$ by $p q$ (by (3)). Hence $q=u p q r=(u p) q(r)$.
7. $q=(u p) q$ (SR). Replace $p q$ by $s . q=u s$.
8. Replace $s$ by $q r$. Then $q=u q r$. Using SR $q=q r$.
9. Since $s=q r$, we can conclude that $q=s$.

## Schützenberger's Theorem - Lemma 2

- Example:
- $\alpha M=\{\alpha, \alpha \beta, 0\}, M \alpha=\{\alpha, \beta \alpha, 0\}$
- $J_{\alpha}=\{s \in M \mid \alpha \notin M s M\}$
- $\alpha M \cap M \alpha=\{\alpha, 0\}$
- $M \alpha M=\{\alpha, \beta, \alpha \beta, \beta \alpha, 0\}$
- $M 0 M=\{0\}$
- $J_{\alpha}=\{0\}$
- $(\alpha M \cap M \alpha) \backslash J_{\alpha}=\alpha$


## Schützenberger's Theorem - Proof objective

- We want to prove that if $\varphi: A^{*} \rightarrow M$ is a morphism from $A^{*}$ into an aperiodic monoid $M$, the set $\varphi^{-1}(P)$ is star-free for every subset $P$ of $M$

$$
\varphi^{-1}(P)=\bigcup_{m \in P} \varphi^{-1}(m)
$$

- Example: Let $L_{1}=(a b)^{*}$ and $M_{1}=\varphi\left(L_{1}\right)=\{1, \alpha, \beta, 0, \alpha \beta, \beta \alpha\} . P=\{1, \alpha \beta\}$ (elements that lead from initial to final state). Then $L_{1}=\varphi^{-1}(1)+\varphi^{-1}(\alpha \beta)$. We need to show that $\varphi^{-1}(1)$ and $\varphi^{-1}(\alpha \beta)$ are star-free sets.
- We should show that $\varphi^{-1}(m)$ is star-free by induction on the integer $r(m)=\operatorname{Card}(M \backslash M m M)$.


## Schützenberger's Theorem - Inverse morphism

- Let

$$
L=\left(U A^{*} \cap A^{*} V\right) \backslash\left(A^{*} C A^{*} \cup A^{*} W A^{*}\right)
$$

- We need to show the correctness of the formula $\varphi^{-1}(m)=L$ where

$$
\begin{aligned}
U & =\bigcup_{(n, a) \in E} \varphi^{-1}(n) a \\
C & =\{a \in A \mid m \notin M \varphi(a) M\} \quad W=\bigcup_{(a, n) \in F} a \varphi^{-1}(n) \\
E & =\{(n, a) \in M \times A \mid n \varphi(a) \mathcal{R} m \text { but } n \notin m M\} \\
F & =\{(a, n) \in A \times M \mid \varphi(a) n \mathcal{L} m \text { but } n \notin M m\} \\
G & =\{(a, n, b) \in A \times M \times A \mid m \in(M \varphi(a) n M \cap M n \varphi(b) M) \backslash M \varphi(a) n \varphi(b) M\}
\end{aligned}
$$

- We need to show that the sets $U, V, C$ and $W$ are star-free


## Schützenberger's Theorem - $\varphi^{-1}(m) \subset L$

- $U=\bigcup_{(n, a) \in E} \varphi^{-1}(n) a$
- $E=\{(n, a) \in M \times A \mid n \varphi(a) \mathcal{R} m$ but $n \notin m M\}$
- Let $u \in \varphi^{-1}(m)$ and $p$ the shortest prefix of $u$ st $\varphi(p) \mathcal{R} m$. $p$ cannot be empty, otherwise $1 \mathcal{R} m$, and in that case $m=1$ (by SR).
- Let $p=r a$ with $r \in A^{*}$ and $a \in A$. Let $n=\varphi(r)$.
- $n \notin m M$ and $n \varphi(a) \mathcal{R} m$, hence $(n, a) \in E$.
- By construction $u \in \varphi^{-1}(n) a A^{*}$. Therefore, $u \in U A^{*}$.
- Symmetric argument in order to show that $u \in A^{*} V$.


## Schützenberger's Theorem - $\varphi^{-1}(m) \subset L$

- $C=\{a \in A \mid m \notin M \varphi(a) M\}$
- Suppose that $u \in A^{*} C A^{*}$. Then, $\exists a$ st $m=\varphi(u) \in M \varphi(a) M$ which is a contradiction with the definition of $C$
- $W=\bigcup_{(a, n, b) \in G} a \varphi^{-1}(n) b$
- $G=\{(a, n, b) \in A \times M \times A \mid m \in(M \varphi(a) n M \cap M n \varphi(b) M) \backslash M \varphi(a) n \varphi(b) M\}$
- Suppose that $u \in A^{*} W A^{*}$. Then exists $(a, n, b) \in G$ st $m \in M \varphi(a) n \varphi(b) M$ which is a contradiction with the definition of $G$
- This concludes our proof that $\varphi^{-1}(m) \subset L$


## Schützenberger's Theorem - $L \subset \varphi^{-1}(m)$

- Let $u \in L$ and $s=\varphi(u)$.
- $\{m\}=(m M \cap M m) \backslash J_{m}$, with $J_{m}=\{s \in M \mid m \notin M s M\}$
- Since $u \in U A^{*} \cap A^{*} V$ (by def of $L$ ), we have $s \in m M \cap M m$.
- To prove that $s=m$ and hence $u \in \varphi^{-1}(m)$, it is enough to prove that $s \notin J_{m}$, ie. $m \in M s M$ (by Lemma 2)
- Suppose $m \notin M s M$. Let the word $f$ be the minimal factor of $u$ st $m \notin M \varphi(f) M$
- $f$ non-empty
- Case 1: $f$ is a letter. Then this letter is in $C$ and $u \in A^{*} C A^{*}$. Impossible.
- Case 2: Let $f=a g b$ with $a, b \in A$. Let $n=\varphi(g)$.
- $f$ is of minimal legth, hence $m \in M \varphi(a) n M$ and $m \in M n \varphi(b) M$. In that case we have $n \in G$ and $f \in W$. Impossible.
- We can conclude that $s=m$.
- This concludes our proof that $L \subset \varphi^{-1}(m)$.
- $\varphi^{-1}(m)=L$


## Schützenberger's Theorem - Inductive Base

- Let $B=\{a \in A \mid \varphi(a)=1\}$
- $B$ is the set of letters which are self-loops on all the states in the automaton
- Base: $r(m)=0$
- Then $m=1$, and we can show that $\varphi^{-1}(1)=B^{*}$ and $B^{*}$ is a star-free set.
- $r(m)=0$ then $M=M m M$. Hence, there exists $u, v \in M$ st $u m v=(u m) 1(v)=(u) 1(m v)=1$. Apply simplification rule:

$$
(u) 1=1,1(v)=1, \text { hence } u=v=1 \text { and consequently } m=1
$$

$\circ B^{*}=A^{*} \backslash \bigcup_{a \in A \backslash B} A^{*} a A^{*}$

## Schützenberger's Theorem - Inductive Step

1. Let $r(m)>0$
2. Assume that we have established that $\varphi^{-1}(s)$ is star-free for each element $s$ with $r(s)<r(m)$
3. We need to show that $U A^{*}, A^{*} V, A^{*} C A^{*}$ and $A^{*} W A^{*}$ are star-free.
4. $U=\bigcup_{(n, a) \in E} \varphi^{-1}(n) a A^{*}$
5. $E=\{(n, a) \in M \times A \mid n \varphi(a) \mathcal{R} m$ but $n \notin m M\}$
6. Let $(n, a) \in E$. Given that $n \varphi(a) \mathcal{R} m$ we have $M m M \subset M n M$ and hence $r(n) \leq r(m)$
7. Suppose $r(n)=r(m)$. Then $n \in M m M$
8. $\exists u, v \in M$ st $n=u m v(b y$ (7))
9. Since, $m \in n \varphi(a) M$ (by (6)), $\exists p \in M$ st $m=n p$
10. $n=u n p v$ ((8) and substitution by (9))
11. $n=n p v=m v$ (by SL and substitution by (9))
12. $n=m v$ is a contradiciton with $n \notin m M$
13. Hence, $r(n)<r(m)$
14. Symmetric argument to prove that $A^{*} V$ is star-free.

## Schützenberger's theorem - Inductive Step

1. $W=\bigcup_{(a, n, b) \in G} A^{*} a \varphi^{-1}(n) b A^{*}$
2. $G=\{(a, n, b) \in A \times M \times A \mid m \in(M \varphi(a) n M \cap M n \varphi(b) M) \backslash M \varphi(a) n \varphi(b) M\}$
3. Let $(a, n, b) \in G$. Since $m \in M n M, r(n) \leq r(m)$.
4. Assume $r(n)=r(m)$. Then $M m M=M n M$
5. $n \in M m M$ (by (4))
6. Since $m \in M \varphi(a) n M$ and $m \in M n \varphi(b) M$ (by (3)), then also $n \in M \varphi(a) n M$ and $n \in M n \varphi(b) M$
7. $\exists u, v \in M$ st $n=u n \varphi(b) v$ (by (6))
8. $n=n \varphi(b) v$ (by SR and (7))
9. $\exists x, y \in M$ st $m=x \varphi(a) n y$ (by (6))
10. $m=x \varphi(a) n \varphi(b) v y$ (replace $n$ in (9) using (8))
11. $m \in M \varphi(a) n \varphi(b) M$ Contradiction with definition of $G$
12. We can conclude that $r(n)<r(m)$

## Schützenberger's theorem - Example

- Let us calculate $\varphi^{-1}(\alpha \beta)$
- UA*: Find $n \varphi(a) \mathcal{R} \alpha \beta$ such that $n \notin \alpha \beta M . \alpha \mathcal{R} \alpha \beta . \alpha=1 \alpha=1 \varphi(a)$. $1 \notin \alpha \beta M$. Hence $U A^{*}=a A^{*}$.
- $A^{*} V$ : Find $\varphi(a) n \mathcal{L} \alpha \beta$ such that $n \notin M \alpha \beta . \beta \mathcal{L} \alpha \beta . \beta=\beta 1=\varphi(b) 1$. $1 \notin M \alpha \beta$. Hence $A^{*} V=A^{*} b$.
- $A^{*} W A^{*}$ : Let us first find $k$ such that $k \notin M \alpha \beta M . k=\alpha^{0}=\alpha 1 \alpha=\varphi(a) 1 \varphi(a)$. Remember that also $\alpha^{2}=\beta^{2}=\beta 1 \beta=\varphi(b) 1 \varphi(b)$. We verify that $\alpha \beta \in M \alpha M$ and $\alpha \beta \in M \beta M$. Hence $A^{*} W A^{*}=A^{*} a a A^{*} \cup A^{*} b b A^{*}$.
- $\varphi^{-1}(\alpha \beta)=\left(a A^{*} \cap A^{*} b\right) \backslash\left(A^{*} a a A^{*} \cup A^{*} b b A^{*}\right)$


## References

- G. Lallement, "Semigroups and Combinatorial Applications"
- O. Maler and A. Pnueli, "On the Cascaded Decomposition of Automata, its Complexity and its Application to Logic"
- R. McNaughton and S. Papert, "Counter-Free Automata"
- D. Perrin and J. E. Pin, "Infinite Words"
- D. Perrin, "Finite Automata", in Handbook of Theoretical Computer Science, Volume B
- J. E. Pin, "Finite Semigroups and Recognizable Languages: an Introduction"
- J. E. Pin, "Logic, Semigroups and Automata on Words"
- J. E. Pin, "Syntactic Semigroups"
- J. E. Pin, "Variétés de Languages Formels"

