7. Monoid recognition

Defining regular languages via algebra.

Let $M = (M, \cdot, 1)$ be a monoid. A congruence on M is an equivalence relation $\equiv$ on M such that, for any $m, m', x \in M$, if $m \equiv m'$, then $m \cdot x \equiv m' \cdot x$ and $x \cdot m \equiv x \cdot m'$.

Fact. The quotient of M by $\equiv$ gives a monoid $M/_{\equiv} = (M/_{\equiv}, \cdot, 1)$, where, for any $m, n \in M$:

$$[m] \cdot [n] := [m \cdot n] \qquad \text{and} \qquad 1 := [1].$$

Example. Let $A = (Q, \Sigma, \cdot, i, F)$ be a DFA. Define the relation $\equiv_A$ on Σ^* by:

$$\text{for } u, v \in \Sigma^*, \qquad u \equiv_A v \quad \overset{\text{def.}}{\Longleftrightarrow} \quad \text{for all } q \in Q, \quad q \cdot u = q \cdot v.$$

Then $\equiv_A$ is a congruence on Σ^*: it is an equivalence relation (exercise), and, for any $u, u', x \in \Sigma^*$, if $u \equiv_A u'$, then $ux \equiv_A u'x$, because, for all $q \in Q$,
$q \cdot (ux) = (q \cdot u) \cdot x = (q' \cdot u) \cdot x = q \cdot (u'x)$, using the action axioms.

By the isomorphism theorem for monoids, $\Sigma^*/_{\equiv_A} \longrightarrow Q^Q$ is an injective monoid morphism.

$$[u]_A \longmapsto (q \longmapsto q \cdot u).$$

Indeed, $\equiv_A$ is the kernel of $\Sigma^* \xrightarrow{\varphi_\cdot} Q^Q$ obtained by currying $Q \times \Sigma^* \xrightarrow{\cdot} Q$.

Proposition. Let A be a DFA. Then $\mathcal{L}(A) = \varphi_\circ^{-1}(P)$, where $P := \{ f \in Q^Q \mid f(i) \in F \}$.

Proof. For any $w \in \Sigma^*$, $\varphi_\circ(w)(i) = i \cdot w$. Thus, $\varphi_\circ(w) \in P$ if, and only if, $i \cdot w \in F$. $\square$

This suggests a definition of recognition in terms of monoids, instead of DFA's:

Def. Let M be a monoid, and $\varphi : \Sigma^* \longrightarrow M$ a (monoid) morphism.

We say that φ recognizes $L \subseteq \Sigma^*$ if there exists $P \subseteq M$ such that $L = \varphi^{-1}(P)$.

Theorem Let A be a DFA. The morphism $\pi_{\equiv_A}$ recognizes $\mathcal{L}(A)$.

Proof. Note that $\tilde{\varphi}_\circ \circ \pi_{\equiv} = \varphi_\circ$, as in the diagram on the right.

$$\begin{tikzcd} \Sigma^* \arrow[rr, "\varphi_\circ"] \arrow[dr, two heads, "\pi_{\equiv_A}"'] & & Q^Q \\ & \Sigma^*/\equiv_A \arrow[ur, "\tilde{\varphi}_\circ"'] & \end{tikzcd}$$

By the Proposition, $\mathcal{L}(A) = \varphi_\circ^{-1}(P) = \pi_{\equiv_A}^{-1}(\tilde{\varphi}_\circ^{-1}(P))$. $\square$

Corollary Let A be a DFA. For any $w \in \Sigma^*$, if $w \in \mathcal{L}(A)$, then $[w]_{\equiv_A} \subseteq \mathcal{L}(A)$.

Proof. Pick $P \subseteq \Sigma^*/\equiv_A$ such that $\mathcal{L}(A) = \pi_{\equiv_A}^{-1}(P)$. Then $p := \pi_{\equiv_A}(w) \in P$.

Thus, $[w]_{\equiv_A} = \pi_{\equiv_A}^{-1}(\{p\}) \subseteq \pi_{\equiv_A}^{-1}(P) = \mathcal{L}(A)$. $\square$

Let A be a DFA. We call the image of the morphism $\varphi_\circ : \Sigma^* \longrightarrow Q^Q$ the transition monoid of A, and denote it by $T(A)$.

Concretely, $T(A)$ is the set of functions $Q \xrightarrow{f} Q$ which "act like a word", i.e., for which there exists $w \in \Sigma^*$ such that $f(q) = q \cdot w$ for all $q \in Q$.

Since $\varphi_\circ : \Sigma^* \longrightarrow T(A)$ is a surjective morphism and $\equiv_A$ is its kernel, we have

$$T(A) \cong \Sigma^* / {\equiv_A},$$

by the isomorphism theorem for monoids.

In particular, $T(A)$ also recognizes $\mathcal{L}(A)$.

We can think of $T(A)$ as analogous to the automaton $\mathrm{Reach}(A)$: for any $q \in Q$, q is reachable if, and only if, there exists $f \in T(A)$ such that $f(i) = q$

We have seen that any DFA gives rise to a finite monoid recognizing the same language. Conversely, let $M = (M, \cdot_M, 1_M)$ be a finite monoid, $\varphi : \Sigma^* \to M$ a morphism, and $P \subseteq M$.

We define the DFA $A_{\varphi,P} := (M, \Sigma, \bullet, 1_M, P)$, where, for $q \in M$ and $a \in \Sigma$:

$$q \bullet a := q \cdot_M \varphi(a).$$

Lemma. For any $w \in \Sigma^*$, $q \in M$, $q \bullet w = q \cdot_M \varphi(w)$. (Proof: next slide.)

Theorem. $\mathcal{L}(A_{\varphi,P}) = \varphi^{-1}(P)$

Proof. Let $w \in \Sigma^*$. Then

$$\begin{aligned} w \in \mathcal{L}(A_{\varphi,P}) &\iff 1_M \bullet w \in P && \text{(def. of acceptance)} \\ &\iff 1_M \cdot_M \varphi(w) \in P && \text{(Lemma)} \\ &\iff w \in \varphi^{-1}(P). && \text{(definition \& unit law in } M) \ \square \end{aligned}$$

Conclusion. A language $L \subseteq \Sigma^*$ is regular if, and only if, L can be recognized by a finite monoid.

Lemma. For any $w \in \Sigma^*$, $q \in M$, $q \cdot w = q \cdot_M \varphi(w)$.

Proof. Induction on w. $w = \varepsilon$:

$$
\begin{aligned}
q \cdot_M \varphi(\varepsilon) &= q \cdot_M 1_M && (\varphi \text{ morphism}) \\
&= q && (\text{unit law in } M) \\
&= q \cdot \varepsilon . && (\text{def. of } \cdot)
\end{aligned}
$$

$w = ua$, where $u \in \Sigma^*$, $a \in \Sigma$:

$$
\begin{aligned}
q \cdot_M \varphi(ua) &= q \cdot_M \varphi(u) \cdot_M \varphi(a) && (\varphi \text{ morphism}) \\
&= (q \cdot u) \cdot_M \varphi(a) && (\text{IH}) \\
&= (q \cdot u) \cdot a && (\text{def. of } \cdot) \\
&= q \cdot (ua) . && (\text{def. of } \cdot)
\end{aligned}
$$

$\square$

Proposition. Let $f : \Sigma^* \longrightarrow \Delta^*$ be a morphism. If $L \in \mathrm{Rec}(\Delta^*)$, then $f^{-1}(L) \in \mathrm{Rec}(\Sigma^*)$

Proof. Pick a finite monoid M, a morphism $\varphi : \Delta^* \longrightarrow M$ and $P \subseteq M$ such that $L = \varphi^{-1}(P)$. We define $\psi := \varphi \circ f$, which is also a monoid morphism.

Now $f^{-1}(L) = f^{-1}(\varphi^{-1}(P)) = \psi^{-1}(P)$, so $\psi : \Sigma^* \to M$ recognizes $f^{-1}(L)$. $\square$

Proposition ("stability") Let M be a monoid. If N is a quotient or a submonoid of M, and N recognizes a language L, then M also recognizes L.

Recall:
$$\begin{tikzcd} \Sigma^* \arrow[r, dashed, "\overline{\varphi'}"] & M \\ \Sigma \arrow[u, phantom, "\cup"] \arrow[ur, "\varphi'"'] & \end{tikzcd}$$

Proof. Suppose N is a quotient of M, say by $\psi : M \twoheadrightarrow N$.

Let $\varphi : \Sigma^* \longrightarrow N$ and $P \subseteq N$ be such that $L = \varphi^{-1}(P)$. For each $a \in \Sigma$, pick $\varphi'(a) \in M$ such that $\psi(\varphi'(a)) = \varphi(a)$. By induction/free property, $\psi \circ \overline{\varphi'} = \varphi$.

Therefore, $L = \varphi^{-1}(P) = \overline{\varphi'}^{-1}(\psi^{-1}(P))$, so $\overline{\varphi'} : \Sigma^* \longrightarrow M$ recognizes L.

Exercise: the case where N is a submonoid. $\square$

8. The syntactic monoid

An algebraic analogue of the minimal automaton.

Let $L \subseteq \Sigma^*$. The syntactic congruence of L is the relation $\sim_L$ on Σ^* defined by:

for $u, v \in \Sigma^*$, $\quad u \sim_L v \quad \overset{\text{def.}}{\iff}$ for all $x, y \in \Sigma^*$, $xuy \in L$ if, and only if, $xvy \in L$.

Theorem The syntactic congruence $\sim_L$ coincides with $\equiv_{A_L}$, where A_L is the Nerode automaton of L.

Proof. For any $u, v \in \Sigma^*$, we have

$$
\begin{aligned}
u \equiv_{A_L} v &\iff \text{for all } K \in Q_L, \quad K \cdot u = K \cdot v && (\text{def. of } \equiv_{A_L}) \\
&\iff \text{for all } x \in \Sigma^*, \quad (x^{-1}L) \cdot u = (x^{-1}L) \cdot v && (\text{def. of } Q_L) \\
&\iff \text{for all } x, y \in \Sigma^*, \quad y \in (xu)^{-1}L \text{ iff } y \in (xv)^{-1}L && (\text{def. of } \cdot \text{ and } =) \\
&\iff u \sim_L v. && (\text{def. of } \sim_L). \quad \square
\end{aligned}
$$

In particular, $\sim_L$ is a congruence, and we can define a monoid $M_L := \Sigma^*/\sim_L$, which we call the syntactic monoid of the language L.

Theorem. The syntactic monoid M_L is isomorphic to the transition monoid of the Nerode automaton of L.

Proof. $\varphi_0 : \Sigma^* \twoheadrightarrow T(A_L)$ is surjective, so $\Sigma^*/_{\ker \varphi_0} \cong T(A_L)$, and $\ker \varphi_0 = \equiv_{A_L} = \sim_L$. $\square$

Example Let $L = (ab)^*$. We compute the syntactic monoid $M_L = \Sigma^*/\sim_L$.

We start with $[\varepsilon]$ and $[a]$, which are distinct because $\varepsilon b \notin L$ but $ab \in L$.

Similarly, we have $[b]$, distinct from $[\varepsilon]$ and $[a]$. (Why?)

Now $[ab] \neq [\varepsilon]$ because $a \cdot (ab) \cdot b \notin L$ but $a \cdot \varepsilon \cdot b \in L$.

Also, $[ab] \neq [a]$ and $[ab] \neq [b]$.

Similarly, $[ba] \notin \{[\varepsilon], [a], [b]\}$. Also, $[ba] \neq [ab]$, since $ba \cdot ab \notin L$ but $abab \in L$.

Finally, $[aa] = [bb]$ since for all $x, y \in \Sigma^*$, $xaay \notin L$, and $xbby \notin L$.

We thus obtain 6 classes: $[\varepsilon], [a], [b], [ab], [ba], [aa]$. The union is Σ^* (check!)

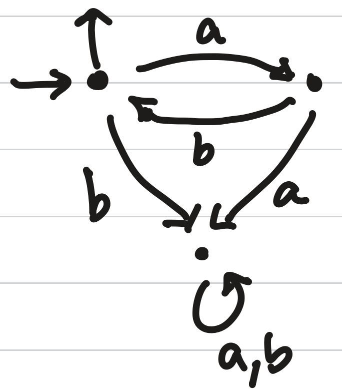
Multiplication table:

(we write $0 := [aa]$, $1 := [\varepsilon]$, and omit all $[\;]$.)

	1	a	b	ab	ba	0
1	1	a	b	ab	ba	0
a	a	0	ab	0	a	0
b	b	ba	0	b	0	0
ab	ab	a	0	ab	0	0
ba	ba	0	b	0	ba	0
0	0	0	0	0	0	0

This is also $T(A_L)$, where

A_L:



The syntactic monoid is also minimal, in a precise algebraic sense.

Let M, N be monoids. We say M **divides** N if there exist a (non-strict) submonoid N' of N and a surjective morphism $N' \twoheadrightarrow M$.

Notation: $M \prec N$

(Unproved)
Remark. $\prec$ is the smallest transitive relation on monoids that contains "submonoid" and "quotient".

Theorem. Let $L \in \mathrm{Rec}(\Sigma^*)$. A finite monoid N recognizes L if, and only if, M_L divides N.

Proof. "$\Leftarrow$" If M_L divides N, then, since M_L recognizes L, so does N by **stability**.

"$\Rightarrow$" Suppose $\varphi : \Sigma^* \to N$ and $P \subseteq N$ are such that $L = \varphi^{-1}(P)$. We claim: $\ker \varphi \subseteq \sim_L$.

To see this, let $u, v \in \Sigma^*$ with $\varphi(u) = \varphi(v)$. Let $x, y \in \Sigma^*$. Then $\varphi(xuy) = \varphi(x)\varphi(u)\varphi(y)$
$= \varphi(x)\varphi(v)\varphi(y) = \varphi(xvy)$,
so in particular, $\varphi(xuy) \in P$ iff $\varphi(xvy) \in P$. Thus, $u \sim_L v$. $\square$

By the claim, there is a morphism $\Sigma^*/\ker\varphi \overset{f}{\twoheadrightarrow} \Sigma^*/\sim_L$, sending $[u]_{\ker\varphi}$ to $[u]_{\sim_L}$.

The image of $\tilde{\varphi} : \Sigma^*/\ker\varphi \to N$ is a submonoid N' of N isomorphic to $\Sigma^*/\ker\varphi$, say $\psi : N' \xrightarrow{\cong} \Sigma^*/\ker\varphi$.

Now $f \circ \psi : N' \twoheadrightarrow M_L$ is the required morphism. $\square$

Conclusion. M_L is a powerful invariant for a regular language L.

We will see that properties of finite monoids can often be shown to correspond precisely to properties of regular languages.

9. Star-free languages

What can we do without Kleene star?

A star-free expression over alphabet Σ is an expression e built from the syntax:

$$e ::= a \mid e+e \mid e \cdot e \mid e^c \mid \varepsilon \mid \emptyset \quad \text{where } a \in \Sigma.$$

The language defined by a star-free expression e is $\mathcal{L}(e)$, defined inductively as:

- $\mathcal{L}(a) := \{a\}$
- $\mathcal{L}(\varepsilon) := \{\varepsilon\}$
- $\mathcal{L}(e^c) := \Sigma^* \setminus \mathcal{L}(e)$.
- $\mathcal{L}(e_1 + e_2) := \mathcal{L}(e_1) \cup \mathcal{L}(e_2)$
- $\mathcal{L}(e_1 \cdot e_2) := \mathcal{L}(e_1) \cdot \mathcal{L}(e_2)$
- $\mathcal{L}(\emptyset) := \emptyset$

A language L is starfree if $L = \mathcal{L}(e)$ for some starfree expression e.

Fact. Any starfree language is regular. **Proof** Closure properties of $Rec(\Sigma^*)$. $\square$

Examples.

- Any finite language is starfree.
- Any cofinite language is starfree.
- The intersection of two starfree languages is starfree, and Σ^* is starfree.

  $((e_1)^c + (e_2)^c)^c$ $\qquad$ $\emptyset^c$
- The language $(ab)^*$ is ... starfree! $(ab)^* = \{\varepsilon\} \cup (a\Sigma^* \cap \Sigma^* b \cap \Sigma^* \setminus (\Sigma^* aa \Sigma^* \cup \Sigma^* bb \Sigma^*))$
- How about the language $(aa)^*$?

Let M be a monoid. A subset G of M is a group contained in M if:

- G is closed under multiplication: for all $m_1, m_2 \in G$, $m_1 \cdot m_2 \in G$
- G has a unit 1_G: for all $m \in G$, $1_G \cdot m = m = m \cdot 1_G$
- for every $x \in G$, there exists $y \in G$ such that $xy = 1_G = yx$.

groups contained in M
$\not\subseteq \longleftarrow \supseteq$
subgroups of M

NB: We do not require that $1_G = 1_M$, and it is not the case in general.

Example The transition monoid of A has three elements: 1, a, and a^2. The subset $\{a, a^2\}$

$\cdot$	1	a	a^2
1	1	a	a^2
a	a	a^2	a
a^2	a^2	a	a^2

is a group contained in $T(A)$, with unit element $a^2 \neq 1$.

Example If M is a monoid and $e \in M$ is idempotent, i.e., $e^2 = e$, then $\{e\}$ is a group contained in M.

We call this a trivial group contained in M.

Equivalently, G contained in M is trivial iff $\#G = 1$.

A monoid M is aperiodic if every group contained in M is trivial.

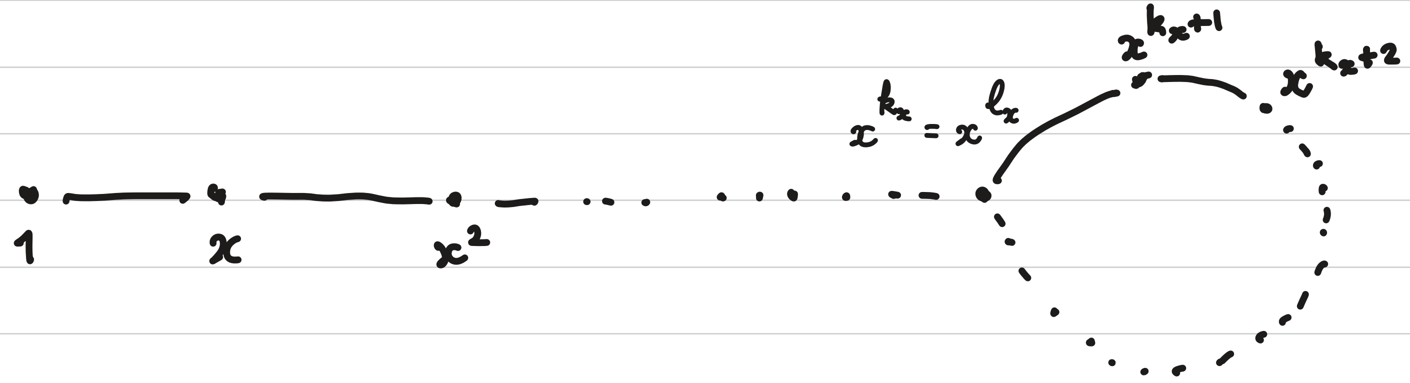
Theorem. A language L is starfree if, and only if, M_L is finite and aperiodic.

(Schützenberger, 1965)

Let M be a finite monoid. For every $x \in M$, there exist $k > l \geq 0$ such that $x^k = x^l$.
(by the Pigeon-hole principle)

Define $k_x :=$ the smallest k such that there exists $0 \leq l < k$ with $x^k = x^l$, and
$l_x :=$ the smallest $l \geq 0$ such that $x^l = x^{k_x}$, and $p_x := k_x - l_x$.

Since $x^0, x^1, \ldots, x^{k_x - 1}$ are all distinct, we can visualize this as:



"the frying pan"

Exercise. $\{x^i \mid l_x \leq i < k_x\}$ is a group contained in M, isomorphic to $\mathbb{Z}/p_x\mathbb{Z}$.

This lets us characterize aperiodic finite monoids in a concrete way, and shows how they are "opposite" to finite groups:

Proposition Let M be a finite monoid. The following are equivalent:

(1) M is aperiodic ; (2) for all $x \in M$, $p_x = 1$; (3) there exists $\ell \in \mathbb{N}$ such that $x^\ell = x^{\ell+1}$ for all $x \in M$.

Proof (1) $\Rightarrow$ (2) By the Exercise, $G_x := \{ x^{\ell_x}, \dots, x^{k_x - 1} \}$ is a group contained in M.

If M is aperiodic, then this group must be trivial. Thus, $p_x = \# G_x = 1$.

(2) $\Rightarrow$ (3) Note that $x^{\ell_x} = x^{\ell_x + p_x} = x^{\ell_x + 1}$. Define $\ell := \max \{ \ell_x : x \in M \}$.

Then, for any $x \in M$, $x^{\ell+1} = x^{\ell_x + 1} \underbrace{x^{\ell - \ell_x}} = x^{\ell_x} \underbrace{x^{\ell - \ell_x}} = x^\ell$.

this notation is legal since $\ell \geq \ell_x$!
it is NOT allowed to have negative exponents.

(3) $\Rightarrow$ (1) Let G be a group contained in M. Let $g \in G$ be arbitrary. By (3), $g^\ell = g^{\ell+1}$.

Pick $h \in G$ such that $gh = 1_G$. Then $1_G = g^\ell h^\ell = g^{\ell+1} h^\ell = g$.

We conclude that $G = \{1_G\}$, so G is trivial. $\square$

Exercise. Let M be a finite monoid. The following are equivalent:

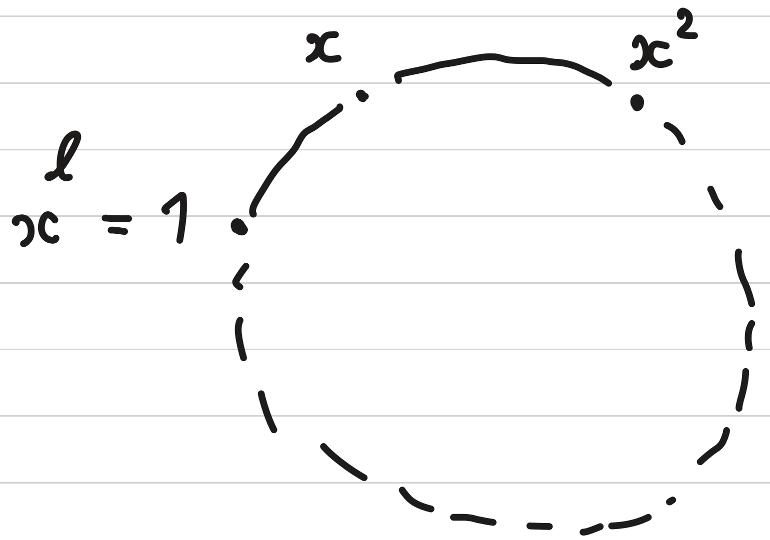
(1) M is a group ; (2) for all $x \in M$, $\ell_x = 0$; (3) there exists $\ell \in \mathbb{N}$ such that $x^\ell = 1_M$ for all $m \in M$.

A finite monoid is aperiodic iff all of its frying pans are only handles:

for all x:

A finite monoid is a group iff all of its frying pans have no handles:

for all x:



(The technical term for "frying pan" is cyclic submonoid or single-generated submonoid)

An additional perspective on starfree languages, via **first-order logic**:

Let φ be a sentence in the (relational) signature

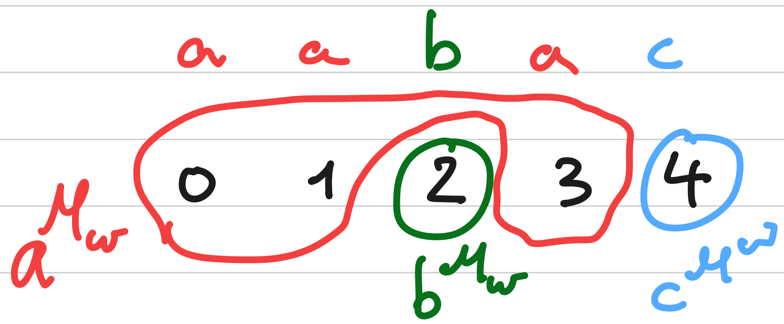
$$L = (\phi, \{\leq\} \cup \Sigma, ar), \text{ with } ar(a) := 1 \text{ for all } a \in \Sigma,$$
$$\text{and } ar(\leq) := 2.$$

R. Bob-Waksberg et al., "BoJack Horseman" (2014-2020)

A finite word $w \in \Sigma^*$ gives an L-structure $\mathcal{M}_w := (M_w, \leq^{\mathcal{M}_w}, (a^{\mathcal{M}_w})_{a \in \Sigma})$, where:

$M_w := \{0, \dots, |w|-1\}$, $\leq^{\mathcal{M}_w} := \leq$, for each $a \in \Sigma$, $a^{\mathcal{M}_w} := \{0 \leq i < |w| : w \text{ has letter } a \text{ at position } i\}$.

Example. Let $\Sigma = \{a,b,c,d\}$, $w := aabac$. Then $\mathcal{M}_w = (\{0,1,2,3,4\}, \leq, (\overset{a}{\{0,1,3\}}, \overset{b}{\{2\}}, \overset{c}{\{4\}}, \overset{d}{\phi}))$



$$\mathcal{M}_w \models \exists x (a(x) \wedge \exists y (x \leq y \wedge b(y)))$$
$$\mathcal{M}_w \not\models \exists x (\forall y (x \leq y \rightarrow a(y)))$$

We define $\mathcal{L}(\varphi) := \{w \in \Sigma^* \mid \mathcal{M}_w \models \varphi\}$ and call this the **language defined by** φ.

A language $L \subseteq \Sigma^*$ is **first-order definable** if $L = \mathcal{L}(\varphi)$ for some first-order formula φ.

Exercise. Give first-order definitions of the languages $\Sigma^* aa \Sigma^*$, $a\Sigma^*$, and $(ab)^*$.

Theorem (Schützenberger; McNaughton & Papert) A language $L \subseteq \Sigma^*$ is starfree if, and only if, L is first-order definable.

We thus have three equivalent conditions on a language $L \subseteq \Sigma^*$:

1) L is starfree
2) L is first-order definable
3) M_L is finite and aperiodic.

We will only prove $(1) \Leftrightarrow (3)$ and $(1) \Rightarrow (2)$ here. (We may do $(2) \Rightarrow (3)$ in the Logic course.)

The proof will take us on a little tour of typical techniques in the theory of monoids, automata, and logic, of which we will only see the tip of the iceberg here.