Regular Languages and Finite Automata

Sets

- A *set* is a group of (possibly infinite) objects; its objects are called *elements* or *members*.
- The set without any element is called the *empty* set (written $\emptyset$).
- Let A, B be sets.
  - $A \cup B$ denotes the *union* of A and B.
  - $A \cap B$ denotes the *intersection* of A and B.
  - $\overline{A}$ denotes the *complement* of A (with respect to some *universe* U), i.e., $\overline{A} = \{x : x \in U, x \notin A\}$.A $\subseteq B$ denotes that A is a *subset* of B.

  - $A \subsetneq B$ denotes that A is a *proper subset* of B.
- The *power set* of a set A (written 2^A) is the set consisting of all subsets of A. E.g. $2^{\{0,1\}} = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

Sequences and Tuples

- A *sequence* is a (possibly infinite) list of ordered objects (e.g., 010101). In this course, we only deal with strings of finite length, unless stated otherwise.
- A finite sequence of k elements is also called *k-tuple* (e.g. (a, b, c, d) is a 4-tuple); a 2-tuple is also called a *pair*.
- The *Cartesian product* of sets A and B (written $A \times B$) is defined by

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

  E.g. $\{0, 1\} \times \{a, b\} = \{(0, a), (0, b), (1, a), (1, b)\}$
- We can take Cartesian products of k sets $A_1, A_2, \ldots, A_k$

$$A_1 \times A_2 \times \cdots \times A_k = \{(a_1, a_2, \ldots, a_k) : a_i \in A_i \text{ for every } 1 \leq i \leq k\}.$$

- Define

$$A^k = \overbrace{A \times A \times \cdots \times A}^{k}.$$

Functions and Relations

- A *function* $f : D \rightarrow R$ maps an element in the *domain* D to an element in the *range* R. Write $f(a) = b$ if f maps $a \in D$ to $b \in R$.
- When $f : A_1 \times A_2 \times \cdots \times A_k \rightarrow B$, we say f is a *k-ary function* and k is the *arity* of f ($k = 1$: *unary function*; $k = 2$, *binary function*).
- A *predicate* or *property* is a function whose range is $\{0, 1\}$. E.g. in C language, "$x == y$" is a predicate, which returns 1 if x and y are equal; 0 otherwise.
- A property with domain $\overbrace{A \times A \times \cdots \times A}^{k}$ is a *k-ary relation* on A.
  - When $k = 2$, it is a *binary relation*.
- A binary relation R is an *equivalence relation* if
  - R is *reflexive* (for every x, xRx);
  - R is *symmetric* (for every x and y, xRy implies yRx; and
  - R is *transitive* (for every x, y, and z, xRy and yRz implies xRz.
- R is *antisymmetric* if $\forall$ x and y, xRy and yRx imply $x = y$. (Question: "Antisymmetric" = "not symmetric"?)
- Do you recall what a *partial order* relation is?

More about Sets

A set A is *countably infinite* if there is a bijection $f : \mathbb{N} \to A$.

Theorem 1

Let $\mathbb{B}$ *be* $\{0, 1\}$. *Then* $A = \mathbb{B} \times \mathbb{B} \times \cdots \times \mathbb{B} \times \cdots$ *is uncountable.*

Proof.

$$
\begin{array}{ll}
s_1 & = 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\ldots \\
s_2 & = 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\ldots \\
s_3 & = 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\ldots \\
s_4 & = 1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\ldots \\
s_5 & = 1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,1\ldots \\
s_6 & = 0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\ldots \\
s_7 & = 1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\ldots \\
s_8 & = 0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\ldots \\
s_9 & = 1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\ldots \\
s_{10} & = 1\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\ldots \\
s_{11} & = 1\,1\,0\,1\,0\,1\,0\,0\,1\,0\,0\ldots \\
\vdots & \quad \vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\ddots
\end{array}
$$

$$
s = 1\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\ldots
$$

Induction Proof

- **Induction Principle**:
  $P(0) \wedge (\forall k, P(k) \Rightarrow P(k+1)) \Rightarrow (\forall n \in \mathbb{N}, P(n))$.
  - Why do we call it a "principle"? Why not call it a "Theorem"? (Check out the *axiom of induction* in *Peano Arithmetic*.)
- **Well-founded Relation**:
  A binary R is called *well-founded* on a class X if every **non-empty subset** $S \subseteq X$ has a **minimal element** with respect to R. (E.g., $\mathbb{N}$ is well-founded; $\mathbb{Z}$ is not well-founded.)

Induction Principle $\Leftrightarrow$ $(\mathbb{N}, <)$ is well-founded.

To prove property $P(n)$ holds for all $n \in \mathbb{N}$,

- **(Induction Basis)**: Prove $P(0)$;
- **(Induction Step)**: Prove that if $P(k)$ holds, then $P(k+1)$ also holds.

Strings and Languages

- An *alphabet* is a nonempty finite set. E.g. $\Sigma = \{0, 1\}$.
- Members of an alphabet are called *symbols*. E.g. 0, 1 in Σ.
- A *string* over an alphabet is a finite sequence of symbols from the alphabet. E.g. 000111.
- If w is a string over an alphabet Σ, the *length* of w (written as $|w|$) is the number of symbols in w. E.g. $|000111| = 6$.
- The string of length zero is the *empty string* (written as ϵ).
- Let $x = x_1 x_2 \cdots x_n$ and $y = y_1 y_2 \cdots y_m$ be strings of length n and m respectively. The *concatenation* of x and y (written as $x \cdot y$ or xy) is the string $x_1 x_2 \cdots x_n y_1 y_2 \cdots y_m$ of length $n + m$.
- For any string x, $x^k = \overbrace{xx \cdots x}^{k}$.
- A *language* is a set of strings. E.g. $\{01, 0011, 000111, ...\}$.

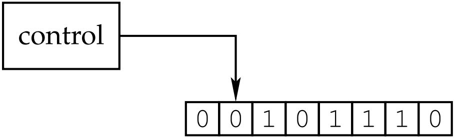
Recall ...

The main goal of Theory of Computation is to learn the **Limitations** and **Capabilities** of computing devices.

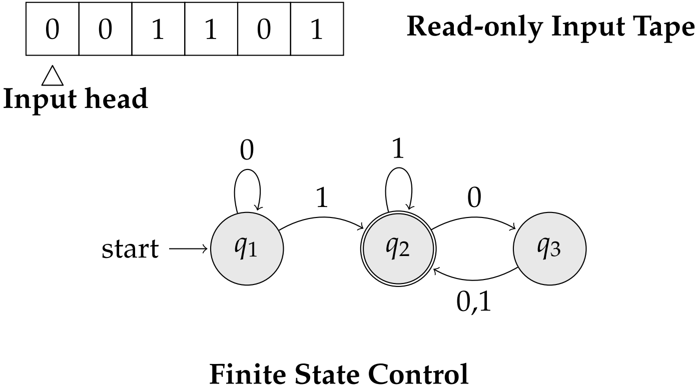
Consider the following sets (languages):

1. $A_1 = \{0, 1, 00, 11, 000, 111, 0000, 1111, ...\}$
2. $A_2 = \{01, 0011, 000111, 0000111, ...\}$
3. $A_3 = \{010, 001100, 000111000, 00001110000, ...\}$
4. $A_4 = \{$0, 1 strings generated by a program P$\}$.

Question: Given a string x (e.g., 00101110), is $x \in A_i$?



Schematic of Finite Automata



- A finite automaton has a finite set of control states.
- A finite automaton reads input symbols from left to right.
- A finite automaton accepts or rejects an input after reading the input.

Finite Automaton M_1

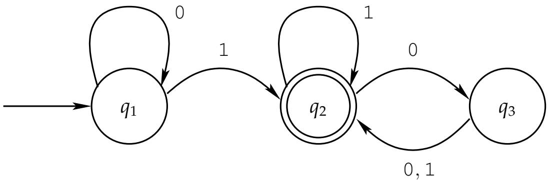
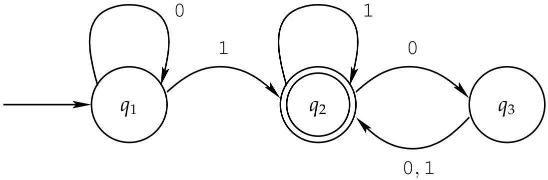


Figure: A Finite Automaton M_1.

The above figure shows the *state diagram* of a finite automaton M_1. M_1 has

- 3 *states*: q_1, q_2, q_3;
- a *start state*: q_1;
- a *accept state*: q_2;
- 6 *transitions*: $q_1 \xrightarrow{0} q_1$, $q_1 \xrightarrow{1} q_2$, $q_2 \xrightarrow{1} q_2$, $q_2 \xrightarrow{0} q_3$, $q_3 \xrightarrow{0} q_2$, and $q_3 \xrightarrow{1} q_2$.

Accepted and Rejected String



- Consider an input string `1100`.
- M_1 processes the string from the start state q_1.
- It takes the transition labeled by the current symbol and moves to the next state.
- At the end of the string, there are two cases:
  - If M_1 is at an accept state, M_1 outputs *accept*;
  - Otherwise, M_1 outputs *reject*.
- Strings accepted by M_1: `1`, `01`, `11`, `1100`, `1101`, ...
- Strings rejected by M_1: `0`, `00`, `10`, `010`, `1010`, ...

Finite Automaton – Formal Definition

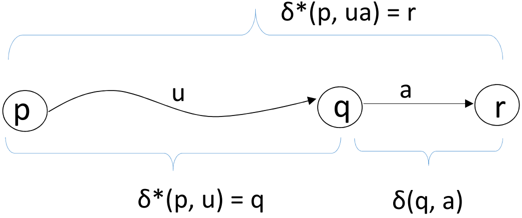
- A *finite automaton* is a 5-tuple $(Q, \Sigma, \delta, q_0, F)$ where
  - Q is a finite set of *states*;
  - Σ is a finite set called *alphabet*;
  - $\delta : Q \times \Sigma \to Q$ is the *transition function*;
  - $q_0 \in Q$ is the *start state*; and
  - $F \subseteq Q$ is the set of *accept states*.
- Accept states are also called *final states*.
- The set of all strings that M accepts is called the *language of machine M* (written $L(M)$).
  - Recall a *language* is a set of strings.
- We also say M *recognizes* (or *accepts*) $L(M)$.

Extended Transition Function

For convenience, we also define the *extended transition function* $\delta^* : Q \times \Sigma^* \to Q$ as follows:

- $\delta^*(p, \epsilon) = p$,
- $\delta^*(p, ua) = \delta(\delta^*(p, u), a)$, where $a \in \Sigma, u \in \Sigma^*$

Intuitively, $\delta^*(p, w)$ is the state reached from state p following the path from p reading w.



M_1 – Formal Definition

- A finite automaton $M_1 = (Q, \Sigma, \delta, q_1, F)$ consists of
  - $Q = \{q_1, q_2, q_3\}$;
  - $\Sigma = \{\texttt{0}, \texttt{1}\}$;
  - $\delta : Q \times \Sigma \to Q$ is

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

  - q_1 is the start state; and
  - $F = \{q_2\}$.
- Moreover, we have

$$L(M_1) = \{w : \; w \text{ contains at least one } \texttt{1} \text{ and an even number of } \texttt{0}\text{'s follow the last } \texttt{1}\}$$

Finite Automaton M_2

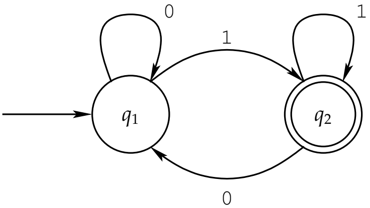


Figure: Finite Automaton M_2

- The above figure shows $M_2 = (\{q_1, q_2\}, \{0, 1\}, \delta, q_1, \{q_2\})$ where δ is

	0	1
q_1	q_1	q_2
q_2	q_1	q_2

- What is $L(M_2)$?
  - $L(M_2) = \{w : w \text{ ends in a } 1\}$.

Finite Automaton M_2

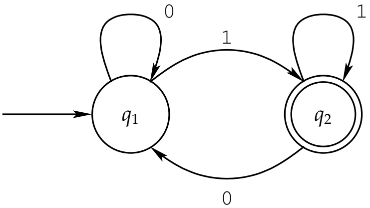


Figure: Finite Automaton M_2

- The above figure shows $M_2 = (\{q_1, q_2\}, \{0, 1\}, \delta, q_1, \{q_2\})$ where δ is

	0	1
q_1	q_1	q_2
q_2	q_1	q_2

- What is $L(M_2)$?
  - $L(M_2) = \{w : w \text{ ends in a } 1\}$.

Finite Automaton M_3

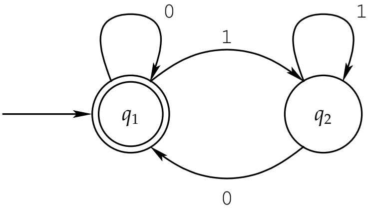


Figure: Finite Automaton M_3

- The above figure shows $M_3 = (\{q_1, q_2\}, \{0, 1\}, \delta, q_1, \{q_1\})$ where δ is

	0	1
q_1	q_1	q_2
q_2	q_1	q_2

- What is $L(M_3)$?
  - $L(M_3) = \{w : w$ is the empty string ϵ or ends in a $0\}$.

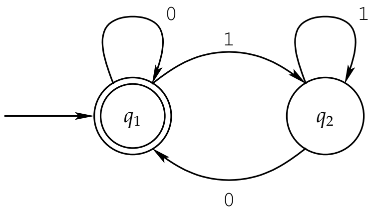


Figure: Finite Automaton M_3

- The above figure shows $M_3 = (\{q_1, q_2\}, \{0, 1\}, \delta, q_1, \{q_1\})$ where δ is

	0	1
q_1	q_1	q_2
q_2	q_1	q_2

- What is $L(M_3)$?
  - $L(M_3) = \{w : w \text{ is the empty string } \epsilon \text{ or ends in a } 0\}$.

Computation – Formal Definition

- Let $M = (Q, \Sigma, \delta, q_0, F)$ be a finite automaton and $w = w_1 w_2 \cdots w_n$ a string where $w_i \in \Sigma$ for every $i = 1, \ldots, n$.
- We say M *accepts* w if there is a sequence of states $r_0, r_1, \ldots, r_n$ such that

$$r_0 \xrightarrow{w_1} r_1 \xrightarrow{w_2} r_2 \cdots r_{n-1} \xrightarrow{w_n} r_n,$$

  - $r_0 = q_0$;
  - $\delta(r_i, w_{i+1}) = r_{i+1}$ for $i = 0, \ldots, n-1$; and
  - $r_n \in F$,
- In the above, $\delta^*(r_0, w_1 \cdots w_n) = \delta(\delta^*(r_0, w_1 \cdots w_{n-1}), w_n) = \delta(r_{n-1}, w_n) = r_n$.
- *M recognizes language A* if $A = \{w : M \text{ accepts } w\}$, or equivalently, $A = \{w : \delta^*(q_0, w) \in F\}$.

Definition 2

A language is called a *regular language* if some finite automaton recognizes it.

Regular Operations

Definition 3

Let A and B be languages. We define the following operations:

- *Union*: $A \cup B = \{x : x \in A \text{ or } x \in B\}$.
- *Concatenation*: $A \cdot B = \{xy : x \in A \text{ and } y \in B\}$.
- *Star*: $A^* = \{x_1 x_2 \cdots x_k : k \geq 0 \text{ and every } x_i \in A\}$.

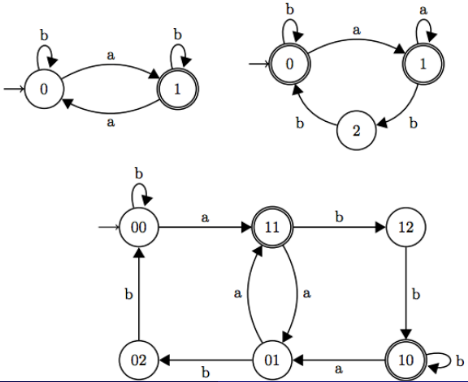
- Note that $\epsilon \in A^*$ for every language A. ($\epsilon \in \emptyset^*$.)
- Another way of defining A^*:
  - $A^0 = \{\epsilon\}$;
  - $A^{k+1} = A \cdot A^k, k \geq 0$.
  - $A^* = \bigcup_{k \geq 0} A^k$
- What is $\emptyset^*$?

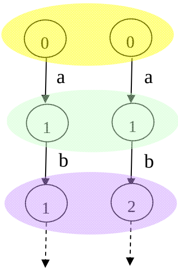
Product Construction

Given two automata $A_1 = (Q_1, \Sigma, \delta_1, q_1, F_1)$ and $A_2 = (Q_2, \Sigma, \delta_2, q_2, F_2)$, the product A of A_1 and A_2 (written as $A_1 \times A_2$), is $(Q, \Sigma, \delta, q, F)$, where

- $Q = Q_1 \times Q_2; \quad q = (q_1, q_2)$,
- $\delta((p_1, p_2), a) = (p'_1, p'_2)$ if $\delta_1(p_1, a) = p'_1$ and $\delta_2(p_2, a) = p'_2$
- F is defined depending on the goal of the construction.

Intuitively, A can be thought of as running A_1 and A_2 in parallel.





Running the two FAs in parallel

Closure Property – Union

Theorem 4

The class of regular languages is closed under the union operation. That is, $A_1 \cup A_2$ is regular if A_1 and A_2 are.

Proof.

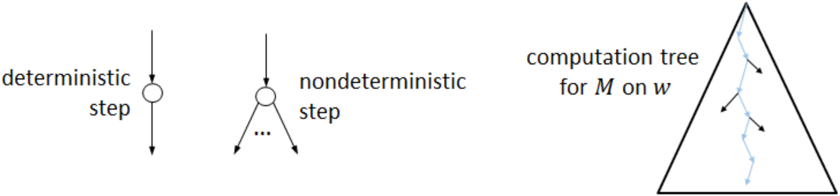
Let $M_i = (Q_i, \Sigma, \delta_i, q_i, F_i)$ recognize A_i for $i = 1, 2$. Construct $M = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = Q_1 \times Q_2 = \{(r_1, r_2) : r_1 \in Q_1, r_2 \in Q_2\}$;
- $\delta((r_1, r_2), a) = (\delta_1(r_1, a), \delta_2(r_2, a))$;
- $q_0 = (q_1, q_2)$;
- $F = (F_1 \times Q_2) \cup (Q_1 \times F_2) = \{(r_1, r_2) : r_1 \in F_1 \text{ or } r_2 \in F_2\}$. □

- Why is $L(M) = A_1 \cup A_2$?
- Can you use product construction to show that regular languages are closed under intersection?

Nondeterminism

- When a machine is at a given state and reads an input symbol, there is precisely one choice of its next state.
- This is call *deterministic* computation.
- In *nondeterministic* machines, multiple choices may exist for the next state.
- A deterministic finite automaton is abbreviated as *DFA*; a nondeterministic finite automaton is abbreviated as *NFA*.
- A DFA is also an NFA.
- Since NFA allow more general computation, they can be much smaller than DFA.



NFA N_4

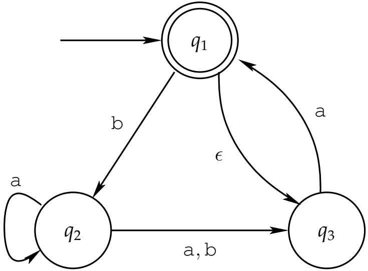


Figure: NFA N_4

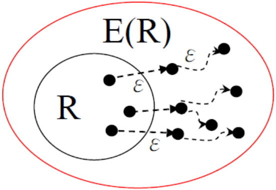
- On input string baa, N_4 has several possible computations:
  - $q_1 \xrightarrow{\texttt{b}} q_2 \xrightarrow{\texttt{a}} q_2 \xrightarrow{\texttt{a}} q_2$;
  - $q_1 \xrightarrow{\texttt{b}} q_2 \xrightarrow{\texttt{a}} q_2 \xrightarrow{\texttt{a}} q_3$; or
  - $q_1 \xrightarrow{\texttt{b}} q_2 \xrightarrow{\texttt{a}} q_3 \xrightarrow{\texttt{a}} q_1$.

Nondeterministic Finite Automaton – Formal Definition

- $\mathcal{P}(Q)$ (also written as 2^Q) $= \{R : R \subseteq Q\}$ denotes the *power set* of Q.
- For any alphabet Σ, define Σ_ϵ to be $\Sigma \cup \{\epsilon\}$.
- A *nondeterministic finite automaton* is a 5-tuple $(Q, \Sigma, \delta, q_0, F)$ where
  - Q is a finite set of states;
  - Σ is a finite alphabet;
  - $\delta : Q \times \Sigma_\epsilon \to \mathcal{P}(Q)$ is the transition function;
  - $q_0 \in Q$ is the start state; and
  - $F \subseteq Q$ is the accept states.
- In some textbooks, δ is defined as a relation $\delta \subseteq Q \times \Sigma \times Q$. E.g., $\delta(q, a) = \{q_1, q_2\}$ can the thought of as $(q, a, q_1), (q, a, q_2) \in \delta$.

ϵ-closure of NFA

Given a set R, we define the ϵ-*closure*(R) ($E(R)$) as follows:

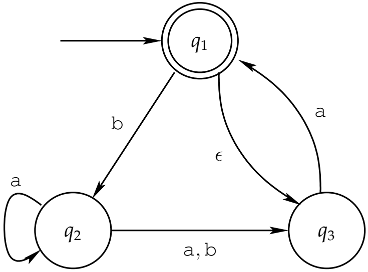


- Intuitively, ϵ-closure(p) is the set of states reachable from p by an ϵ-path.
- How to compute ϵ-closure(p)?

The *extended transition function* $\delta^* : Q \times \Sigma^* \to 2^Q$ is as follows:

- $\delta^*(p, \epsilon) = \epsilon$-closure$(\{p\})$
- $\delta^*(p, ua) = \epsilon$-closure$(\bigcup_{s \in \delta^*(p,u)} \delta(s, a))$

NFA N_4 – Formal Definition



- $N_4 = (Q, \Sigma, \delta, q_1, \{q_1\})$ is a nondeterministic finite automaton where
  - $Q = \{q_1, q_2, q_3\}$;
  - Its transition function δ is

	ϵ	a	b
q_1	$\{q_3\}$	$\emptyset$	$\{q_2\}$
q_2	$\emptyset$	$\{q_2, q_3\}$	$\{q_3\}$
q_3	$\emptyset$	$\{q_1\}$	$\emptyset$

Nondeterministic Computation – Formal Definition

- Let $N = (Q, \Sigma, \delta, q_0, F)$ be an NFA and w a string over Σ. We say N *accepts* w if w can be rewritten as $w = y_1 y_2 \cdots y_m$ with $y_i \in \Sigma_\epsilon$ and there is a sequence of states $r_0, r_1, \ldots, r_m$ such that

$$r_0 \xrightarrow{y_1} r_1 \xrightarrow{y_2} r_2 \cdots r_{m-1} \xrightarrow{y_m} r_m,$$

  - $r_0 = q_0$;
  - $r_{i+1} \in \delta(r_i, y_{i+1})$ for $i = 0, \ldots, m-1$; and
  - $r_m \in F$.
- Note that finitely many empty strings can be inserted in w.
- Also note that *one sequence* satisfying the conditions suffices to show the acceptance of an input string.
- *M recognizes language A* if $A = \{w : M \text{ accepts } w\}$, or equivalently, $A = \{w : \delta^*(q_0, w) \cap F \neq \emptyset\}$.

Equivalence of NFA's and DFA's via Subset Construction

Theorem 5

Every nondeterministic finite automaton has an equivalent deterministic finite automaton. That is, for every NFA N, there is a DFA M such that $L(M) = L(N)$.

Proof.

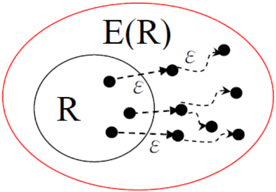
Let $N = (Q, \Sigma, \delta, q_0, F)$ be an NFA. For $R \subseteq Q$, define $E(R) = \{q : q$ can be reached from R along 0 or more ϵ transitions $\}$. Construct a DFA $M = (Q', \Sigma, \delta', q'_0, F')$ where

- $Q' = \mathcal{P}(Q)$;
- $\delta'(R, a) = \{q \in Q : q \in E(\delta(r, a))$ for some $r \in R\}$;
- $q'_0 = E(\{q_0\})$; $F' = \{R \in Q' : R \cap F \neq \emptyset\}$. □

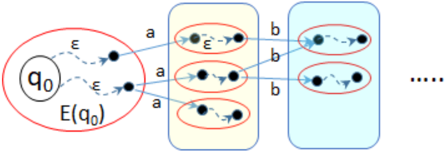
- Why is $L(M) = L(N)$?

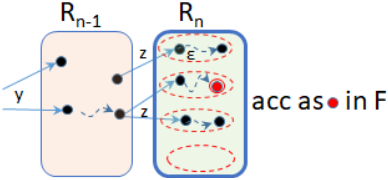
Equivalence of NFA's and DFA's

- ϵ-closure $E(R)$:



- Transition $\delta'(R, a) = \{q \mid q \in E(\delta(r, a)),\ \text{for some } r \in R\}$





Correctness Proof of Subset Construction

In NFA N, we write $r_0 \overset{w}{\Longrightarrow} r_m$ if $r_0 \overset{y_1}{\rightarrow} r_1 \overset{y_2}{\rightarrow} r_2 \cdots r_{m-1} \overset{y_m}{\rightarrow} r_m$, and $y_1 y_2 \cdots y_m = w$, where $y_i \in \Sigma_\epsilon$. I.e., there is a path from r_0 to r_m reading w. In what follows, we prove the following lemma by induction on the length of w that

Lemma 6

$$\overbrace{(\delta')^*(E(\{q_0\}), w)}^{DFA\ M} = \overbrace{\{r \in Q \mid q_0 \overset{w}{\Longrightarrow} r\}}^{NFA\ N}.$$

- **Induction Basis**: Consider the case $|w| = 0$, i.e., $w = \epsilon$. Clearly,

  $(\delta')^*(E(\{q_0\}), \epsilon) = R \quad \Leftrightarrow \quad R = E(\{q_0\}) = \{r \in Q \mid q_0 \overset{\epsilon}{\Longrightarrow} r\}$
  [Def. of $\Longrightarrow$ and $E(\{q_0\})$]

- **Induction Hypothesis**: Assume that the assertion holds for $0 \leq |w| \leq k$.

Correctness Proof of Subset Construction (Cont'd)

- **Induction Step**: Consider the case when $|w| = k + 1$, i.e., $w = xa$, where $x \in \Sigma^*$, $|x| = k$, and $a \in \Sigma$. Recall
  $\delta'(R, a) = \{q \in Q : q \in E(\delta(r, a)) \text{ for some } r \in R\} = \bigcup_{r \in R} E(\delta(r, a))$
  $\delta^*(p, ua) = \delta(\delta^*(p, u), a)$, if deterministic

  $$
  \begin{aligned}
  & q_0 \overset{xa}{\Longrightarrow} r \\
  \Leftrightarrow \quad & (\exists s, t \in Q) q_0 \overset{x}{\Longrightarrow} s \ \wedge \ s \overset{a}{\to} t \ \wedge \ t \overset{\epsilon}{\Longrightarrow} r && [\text{Def. of } \Longrightarrow] \\
  \Leftrightarrow \quad & (\exists s, t \in Q) q_0 \overset{x}{\Longrightarrow} s \ \wedge \ s \overset{a}{\to} t \ \wedge \ r \in E(\{t\}) && [\text{Def. of } E] \\
  \Leftrightarrow \quad & (\exists s, t \in Q) s \in (\delta')^*(E(\{q_0\}), x) \ \wedge \ t \in \delta(s, a) \ \wedge \ r \in E(\{t\}) \\
  & \qquad [\text{Ind. Hyp.; Defs. of } \delta \text{ and } \Longrightarrow] \\
  \Leftrightarrow \quad & (\exists s \in Q) s \in (\delta')^*(E(\{q_0\}), x) \ \wedge \ r \in E(\delta(s, a)) && [\text{Def. of } E] \\
  \Leftrightarrow \quad & r \in \bigcup_{s \in S} E(\delta(s, a)) \text{ for } S = (\delta')^*(E(\{q_0\}), x) && [\text{Def. of } \textstyle\bigcup] \\
  \Leftrightarrow \quad & r \in \delta'(S, a) \text{ for } S = (\delta')^*(E(\{q_0\}), x) && [\text{Def. of } \delta'] \\
  \Leftrightarrow \quad & r \in \delta'((\delta')^*(E(\{q_0\}), x), a)) \\
  \Leftrightarrow \quad & r \in (\delta')^*(E(\{q_0\}), xa) && [\text{Def. of } (\delta')^*]
  \end{aligned}
  $$

Hence, $(\delta')^*(E(q_0), w) \ = \ \{r \in Q \mid q_0 \overset{w}{\Longrightarrow} r\}$.

Correctness Proof of Subset Construction (Cont'd)

- **Induction Step**: Consider the case when $|w| = k+1$, i.e., $w = xa$, where $x \in \Sigma^*$, $|x| = k$, and $a \in \Sigma$. Recall
  $\delta'(R,a) = \{q \in Q : q \in E(\delta(r,a)) \text{ for some } r \in R\} = \bigcup_{r \in R} E(\delta(r,a))$
  $\delta^*(p,ua) = \delta(\delta^*(p,u),a)$, if deterministic

$$
\begin{array}{lll}
q_0 \stackrel{xa}{\Longrightarrow} r & & \\
\Leftrightarrow & (\exists s,t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \wedge s \stackrel{a}{\rightarrow} t \wedge t \stackrel{\epsilon}{\Longrightarrow} r & [\text{Def. of } \Longrightarrow] \\
\Leftrightarrow & (\exists s,t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \wedge s \stackrel{a}{\rightarrow} t \wedge r \in E(\{t\}) & [\text{Def. of } E] \\
\Leftrightarrow & (\exists s,t \in Q) s \in (\delta')^*(E(\{q_0\}),x) \wedge t \in \delta(s,a) \wedge r \in E(\{t\}) & \\
& \quad [\text{Ind. Hyp.; Defs. of } \delta \text{ and } \Longrightarrow] & \\
\Leftrightarrow & (\exists s \in Q) s \in (\delta')^*(E(\{q_0\}),x) \wedge r \in E(\delta(s,a)) & [\text{Def. of } E] \\
\Leftrightarrow & r \in \bigcup_{s \in S} E(\delta(s,a)) \text{ for } S = (\delta')^*(E(\{q_0\}),x) & [\text{Def. of } \bigcup] \\
\Leftrightarrow & r \in \delta'(S,a) \text{ for } S = (\delta')^*(E(\{q_0\}),x) & [\text{Def. of } \delta'] \\
\Leftrightarrow & r \in \delta'((\delta')^*(E(\{q_0\}),x),a)) & \\
\Leftrightarrow & r \in (\delta')^*(E(\{q_0\}),xa) & [\text{Def. of } (\delta')^*]
\end{array}
$$

Hence, $(\delta')^*(E(q_0),w) = \{r \in Q \mid q_0 \stackrel{w}{\Longrightarrow} r\}$.

Correctness Proof of Subset Construction (Cont'd)

- **Induction Step**: Consider the case when $|w| = k + 1$, i.e., $w = xa$, where $x \in \Sigma^*$, $|x| = k$, and $a \in \Sigma$. Recall
  $\delta'(R, a) = \{q \in Q : q \in E(\delta(r, a))$ for some $r \in R\} = \bigcup_{r \in R} E(\delta(r, a))$
  $\delta^*(p, ua) = \delta(\delta^*(p, u), a)$, if deterministic

  $q_0 \stackrel{xa}{\Longrightarrow} r$

  $\Leftrightarrow \quad (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \wedge s \stackrel{a}{\rightarrow} t \wedge t \stackrel{\epsilon}{\Longrightarrow} r$ [Def. of $\Longrightarrow$]

  $\Leftrightarrow \quad (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \wedge s \stackrel{a}{\rightarrow} t \wedge r \in E(\{t\})$ [Def. of E]

  $\Leftrightarrow \quad (\exists s, t \in Q) s \in (\delta')^*(E(\{q_0\}), x) \wedge t \in \delta(s, a) \wedge r \in E(\{t\})$
  [Ind. Hyp.; Defs. of δ and $\Longrightarrow$]

  $\Leftrightarrow \quad (\exists s \in Q) s \in (\delta')^*(E(\{q_0\}), x) \wedge r \in E(\delta(s, a))$ [Def. of E]

  $\Leftrightarrow \quad r \in \bigcup_{s \in S} E(\delta(s, a))$ for $S = (\delta')^*(E(\{q_0\}), x)$ [Def. of $\bigcup$]

  $\Leftrightarrow \quad r \in \delta'(S, a)$ for $S = (\delta')^*(E(\{q_0\}), x)$ [Def. of δ']

  $\Leftrightarrow \quad r \in \delta'((\delta')^*(E(\{q_0\}), x), a))$

  $\Leftrightarrow \quad r \in (\delta')^*(E(\{q_0\}), xa)$ [Def. of $(\delta')^*$]

  Hence, $(\delta')^*(E(q_0), w) = \{r \in Q \mid q_0 \stackrel{w}{\Longrightarrow} r\}$.

- **Induction Step**: Consider the case when $|w| = k+1$, i.e., $w = xa$, where $x \in \Sigma^*$, $|x| = k$, and $a \in \Sigma$. Recall
  $\delta'(R, a) = \{q \in Q : q \in E(\delta(r, a))$ for some $r \in R\} = \bigcup_{r \in R} E(\delta(r, a))$
  $\delta^*(p, ua) = \delta(\delta^*(p, u), a)$, if deterministic

  $q_0 \stackrel{xa}{\Longrightarrow} r$

  $\Leftrightarrow \quad (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \ \wedge \ s \stackrel{a}{\rightarrow} t \ \wedge \ t \stackrel{\epsilon}{\Longrightarrow} r$ [Def. of $\Longrightarrow$]

  $\Leftrightarrow \quad (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \ \wedge \ s \stackrel{a}{\rightarrow} t \ \wedge \ r \in E(\{t\})$ [Def. of E]

  $\Leftrightarrow \quad (\exists s, t \in Q) s \in (\delta')^*(E(\{q_0\}), x) \ \wedge \ t \in \delta(s, a) \ \wedge \ r \in E(\{t\})$
  [Ind. Hyp.; Defs. of δ and $\Longrightarrow$]

  $\Leftrightarrow \quad (\exists s \in Q) s \in (\delta')^*(E(\{q_0\}), x) \ \wedge \ r \in E(\delta(s, a))$ [Def. of E]

  $\Leftrightarrow \quad r \in \bigcup_{s \in S} E(\delta(s, a))$ for $S = (\delta')^*(E(\{q_0\}), x)$ [Def. of $\bigcup$]

  $\Leftrightarrow \quad r \in \delta'(S, a)$ for $S = (\delta')^*(E(\{q_0\}), x)$ [Def. of δ']

  $\Leftrightarrow \quad r \in \delta'((\delta')^*(E(\{q_0\}), x), a))$

  $\Leftrightarrow \quad r \in (\delta')^*(E(\{q_0\}), xa)$ [Def. of $(\delta')^*$]

Hence, $(\delta')^*(E(q_0), w) = \{r \in Q \mid q_0 \stackrel{w}{\Longrightarrow} r\}$.

Correctness Proof of Subset Construction (Cont'd)

- **Induction Step**: Consider the case when $|w| = k+1$, i.e., $w = xa$, where $x \in \Sigma^*$, $|x| = k$, and $a \in \Sigma$. Recall
  $\delta'(R,a) = \{q \in Q : q \in E(\delta(r,a))$ for some $r \in R\} = \bigcup_{r \in R} E(\delta(r,a))$
  $\delta^*(p, ua) = \delta(\delta^*(p,u), a)$, if deterministic

$$q_0 \stackrel{xa}{\Longrightarrow} r$$

$$\Leftrightarrow \quad (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \wedge s \stackrel{a}{\to} t \wedge t \stackrel{\epsilon}{\Longrightarrow} r \qquad [\text{Def. of } \Longrightarrow]$$

$$\Leftrightarrow \quad (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \wedge s \stackrel{a}{\to} t \wedge r \in E(\{t\}) \qquad [\text{Def. of } E]$$

$$\Leftrightarrow \quad (\exists s, t \in Q) s \in (\delta')^*(E(\{q_0\}), x) \wedge t \in \delta(s,a) \wedge r \in E(\{t\})$$
$$[\text{Ind. Hyp.; Defs. of } \delta \text{ and } \Longrightarrow]$$

$$\Leftrightarrow \quad (\exists s \in Q) s \in (\delta')^*(E(\{q_0\}), x) \wedge r \in E(\delta(s,a)) \qquad [\text{Def. of } E]$$

$$\Leftrightarrow \quad r \in \bigcup_{s \in S} E(\delta(s,a)) \text{ for } S = (\delta')^*(E(\{q_0\}), x) \qquad [\text{Def. of } \bigcup]$$

$$\Leftrightarrow \quad r \in \delta'(S,a) \text{ for } S = (\delta')^*(E(\{q_0\}), x) \qquad [\text{Def. of } \delta']$$

$$\Leftrightarrow \quad r \in \delta'((\delta')^*(E(\{q_0\}), x), a))$$

$$\Leftrightarrow \quad r \in (\delta')^*(E(\{q_0\}), xa) \qquad [\text{Def. of } (\delta')^*]$$

Hence, $(\delta')^*(E(q_0), w) = \{r \in Q \mid q_0 \stackrel{w}{\Longrightarrow} r\}$.

- **Induction Step**: Consider the case when $|w| = k + 1$, i.e., $w = xa$, where $x \in \Sigma^*$, $|x| = k$, and $a \in \Sigma$. Recall
  $\delta'(R, a) = \{q \in Q : q \in E(\delta(r, a))$ for some $r \in R\} = \bigcup_{r \in R} E(\delta(r, a))$
  $\delta^*(p, ua) = \delta(\delta^*(p, u), a)$, if deterministic

$$
\begin{array}{lll}
q_0 \stackrel{xa}{\Longrightarrow} r & & \\
\Leftrightarrow & (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \ \wedge \ s \stackrel{a}{\rightarrow} t \ \wedge \ t \stackrel{\epsilon}{\Longrightarrow} r & [\text{Def. of} \Longrightarrow] \\
\Leftrightarrow & (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \ \wedge \ s \stackrel{a}{\rightarrow} t \ \wedge \ r \in E(\{t\}) & [\text{Def. of } E] \\
\Leftrightarrow & (\exists s, t \in Q) s \in (\delta')^*(E(\{q_0\}), x) \ \wedge \ t \in \delta(s, a) \ \wedge \ r \in E(\{t\}) & \\
 & \quad [\text{Ind. Hyp.; Defs. of } \delta \text{ and} \Longrightarrow] & \\
\Leftrightarrow & (\exists s \in Q) s \in (\delta')^*(E(\{q_0\}), x) \ \wedge \ r \in E(\delta(s, a)) & [\text{Def. of } E] \\
\Leftrightarrow & r \in \bigcup_{s \in S} E(\delta(s, a)) \text{ for } S = (\delta')^*(E(\{q_0\}), x) & [\text{Def. of} \bigcup] \\
\Leftrightarrow & r \in \delta'(S, a) \text{ for } S = (\delta')^*(E(\{q_0\}), x) & [\text{Def. of } \delta'] \\
\Leftrightarrow & r \in \delta'((\delta')^*(E(\{q_0\}), x), a)) & \\
\Leftrightarrow & r \in (\delta')^*(E(\{q_0\}), xa) & [\text{Def. of } (\delta')^*]
\end{array}
$$

Hence, $(\delta')^*(E(q_0), w) \ = \ \{r \in Q \mid q_0 \stackrel{w}{\Longrightarrow} r\}$.

Correctness Proof of Subset Construction (Cont'd)

- **Induction Step**: Consider the case when $|w| = k+1$, i.e., $w = xa$, where $x \in \Sigma^*$, $|x| = k$, and $a \in \Sigma$. Recall
  $\delta'(R,a) = \{q \in Q : q \in E(\delta(r,a))$ for some $r \in R\} = \bigcup_{r \in R} E(\delta(r,a))$
  $\delta^*(p, ua) = \delta(\delta^*(p,u), a)$, if deterministic

$$
\begin{array}{ll}
q_0 \stackrel{xa}{\Longrightarrow} r & \\
\Leftrightarrow \quad (\exists s,t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \ \wedge \ s \stackrel{a}{\rightarrow} t \ \wedge \ t \stackrel{\epsilon}{\Longrightarrow} r & [\text{Def. of } \Longrightarrow] \\
\Leftrightarrow \quad (\exists s,t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \ \wedge \ s \stackrel{a}{\rightarrow} t \ \wedge \ r \in E(\{t\}) & [\text{Def. of } E] \\
\Leftrightarrow \quad (\exists s,t \in Q) s \in (\delta')^*(E(\{q_0\}), x) \ \wedge \ t \in \delta(s,a) \ \wedge \ r \in E(\{t\}) & \\
\qquad \qquad [\text{Ind. Hyp.; Defs. of } \delta \text{ and } \Longrightarrow] & \\
\Leftrightarrow \quad (\exists s \in Q) s \in (\delta')^*(E(\{q_0\}), x) \ \wedge \ r \in E(\delta(s,a)) & [\text{Def. of } E] \\
\Leftrightarrow \quad r \in \bigcup_{s \in S} E(\delta(s,a)) \text{ for } S = (\delta')^*(E(\{q_0\}), x) & [\text{Def. of } \bigcup] \\
\Leftrightarrow \quad r \in \delta'(S,a) \text{ for } S = (\delta')^*(E(\{q_0\}), x) & [\text{Def. of } \delta'] \\
\Leftrightarrow \quad r \in \delta'((\delta')^*(E(\{q_0\}), x), a)) & \\
\Leftrightarrow \quad r \in (\delta')^*(E(\{q_0\}), xa) & [\text{Def. of } (\delta')^*]
\end{array}
$$

Hence, $(\delta')^*(E(q_0), w) \ = \ \{r \in Q \mid q_0 \stackrel{w}{\Longrightarrow} r\}$.

Correctness Proof of Subset Construction (Cont'd)

- **Induction Step**: Consider the case when $|w| = k+1$, i.e., $w = xa$, where $x \in \Sigma^*$, $|x| = k$, and $a \in \Sigma$. Recall
  $\delta'(R, a) = \{q \in Q : q \in E(\delta(r, a)) \text{ for some } r \in R\} = \bigcup_{r \in R} E(\delta(r, a))$
  $\delta^*(p, ua) = \delta(\delta^*(p, u), a)$, if deterministic

  $q_0 \stackrel{xa}{\Longrightarrow} r$

  $$\Leftrightarrow \quad (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \wedge s \stackrel{a}{\to} t \wedge t \stackrel{\epsilon}{\Longrightarrow} r \qquad \text{[Def. of } \Longrightarrow]$$
  $$\Leftrightarrow \quad (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \wedge s \stackrel{a}{\to} t \wedge r \in E(\{t\}) \qquad \text{[Def. of } E]$$
  $$\Leftrightarrow \quad (\exists s, t \in Q) s \in (\delta')^*(E(\{q_0\}), x) \wedge t \in \delta(s, a) \wedge r \in E(\{t\})$$
  [Ind. Hyp.; Defs. of δ and $\Longrightarrow$]
  $$\Leftrightarrow \quad (\exists s \in Q) s \in (\delta')^*(E(\{q_0\}), x) \wedge r \in E(\delta(s, a)) \qquad \text{[Def. of } E]$$
  $$\Leftrightarrow \quad r \in \bigcup_{s \in S} E(\delta(s, a)) \text{ for } S = (\delta')^*(E(\{q_0\}), x) \qquad \text{[Def. of } \bigcup]$$
  $$\Leftrightarrow \quad r \in \delta'(S, a) \text{ for } S = (\delta')^*(E(\{q_0\}), x) \qquad \text{[Def. of } \delta']$$
  $$\Leftrightarrow \quad r \in \delta'((\delta')^*(E(\{q_0\}), x), a))$$
  $$\Leftrightarrow \quad r \in (\delta')^*(E(\{q_0\}), xa) \qquad \text{[Def. of } (\delta')^*]$$

Hence, $(\delta')^*(E(q_0), w) = \{r \in Q \mid q_0 \stackrel{w}{\Longrightarrow} r\}$.

- **Induction Step**: Consider the case when $|w| = k+1$, i.e., $w = xa$, where $x \in \Sigma^*$, $|x| = k$, and $a \in \Sigma$. Recall
  $\delta'(R, a) = \{q \in Q : q \in E(\delta(r, a))$ for some $r \in R\} = \bigcup_{r \in R} E(\delta(r, a))$
  $\delta^*(p, ua) = \delta(\delta^*(p, u), a)$, if deterministic

$$
\begin{array}{lll}
q_0 \stackrel{xa}{\Longrightarrow} r & & \\
\Leftrightarrow & (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \wedge s \stackrel{a}{\rightarrow} t \wedge t \stackrel{\epsilon}{\Longrightarrow} r & [\text{Def. of } \Longrightarrow] \\
\Leftrightarrow & (\exists s, t \in Q) q_0 \stackrel{x}{\Longrightarrow} s \wedge s \stackrel{a}{\rightarrow} t \wedge r \in E(\{t\}) & [\text{Def. of } E] \\
\Leftrightarrow & (\exists s, t \in Q) s \in (\delta')^*(E(\{q_0\}), x) \wedge t \in \delta(s, a) \wedge r \in E(\{t\}) & \\
& \quad [\text{Ind. Hyp.; Defs. of } \delta \text{ and } \Longrightarrow] & \\
\Leftrightarrow & (\exists s \in Q) s \in (\delta')^*(E(\{q_0\}), x) \wedge r \in E(\delta(s, a)) & [\text{Def. of } E] \\
\Leftrightarrow & r \in \bigcup_{s \in S} E(\delta(s, a)) \text{ for } S = (\delta')^*(E(\{q_0\}), x) & [\text{Def. of } \bigcup] \\
\Leftrightarrow & r \in \delta'(S, a) \text{ for } S = (\delta')^*(E(\{q_0\}), x) & [\text{Def. of } \delta'] \\
\Leftrightarrow & r \in \delta'((\delta')^*(E(\{q_0\}), x), a)) & \\
\Leftrightarrow & r \in (\delta')^*(E(\{q_0\}), xa) & [\text{Def. of } (\delta')^*]
\end{array}
$$

Hence, $(\delta')^*(E(q_0), w) = \{r \in Q \mid q_0 \stackrel{w}{\Longrightarrow} r\}$.

- **Induction Step**: Consider the case when $|w| = k+1$, i.e., $w = xa$, where $x \in \Sigma^*$, $|x| = k$, and $a \in \Sigma$. Recall
  $\delta'(R,a) = \{q \in Q : q \in E(\delta(r,a))$ for some $r \in R\} = \bigcup_{r \in R} E(\delta(r,a))$
  $\delta^*(p, ua) = \delta(\delta^*(p,u), a)$, if deterministic

$$
\begin{array}{lll}
q_0 \overset{xa}{\Longrightarrow} r & & \\
\Leftrightarrow & (\exists s,t \in Q) q_0 \overset{x}{\Longrightarrow} s \ \wedge\ s \overset{a}{\to} t \ \wedge\ t \overset{\epsilon}{\Longrightarrow} r & [\text{Def. of } \Longrightarrow] \\
\Leftrightarrow & (\exists s,t \in Q) q_0 \overset{x}{\Longrightarrow} s \ \wedge\ s \overset{a}{\to} t \ \wedge\ r \in E(\{t\}) & [\text{Def. of } E] \\
\Leftrightarrow & (\exists s,t \in Q) s \in (\delta')^*(E(\{q_0\}), x) \ \wedge\ t \in \delta(s,a) \ \wedge\ r \in E(\{t\}) & \\
 & \quad [\text{Ind. Hyp.; Defs. of } \delta \text{ and } \Longrightarrow] & \\
\Leftrightarrow & (\exists s \in Q) s \in (\delta')^*(E(\{q_0\}), x) \ \wedge\ r \in E(\delta(s,a)) & [\text{Def. of } E] \\
\Leftrightarrow & r \in \bigcup_{s \in S} E(\delta(s,a)) \text{ for } S = (\delta')^*(E(\{q_0\}), x) & [\text{Def. of } \bigcup] \\
\Leftrightarrow & r \in \delta'(S,a) \text{ for } S = (\delta')^*(E(\{q_0\}), x) & [\text{Def. of } \delta'] \\
\Leftrightarrow & r \in \delta'((\delta')^*(E(\{q_0\}), x), a)) & \\
\Leftrightarrow & r \in (\delta')^*(E(\{q_0\}), xa) & [\text{Def. of } (\delta')^*]
\end{array}
$$

Hence, $(\delta')^*(E(q_0), w) \ = \ \{r \in Q \mid q_0 \overset{w}{\Longrightarrow} r\}$.

Correctness Proof of Subset Construction (Cont'd)

Now we are ready to show $L(M) = L(N)$.

$w \in L(M)$	$\Leftrightarrow$	$(\delta')^*(E(\{q_0\}), w) \in F'$	
	$\Leftrightarrow$	$(\exists r \in F)\ r \in (\delta')^*(E(\{q_0\}), w)$	[Def. of F']
	$\Leftrightarrow$	$(\exists r \in F)\ q_0 \stackrel{w}{\Longrightarrow} r$	[Lemma 6]
	$\Leftrightarrow$	$w \in L(N)$	[Def. of $L(N)$]

Correctness Proof of Subset Construction (Cont'd)

Now we are ready to show $L(M) = L(N)$.

$$
\begin{array}{rcll}
w \in L(M) & \Leftrightarrow & (\delta')^*(E(\{q_0\}), w) \in F' & \\
& \Leftrightarrow & (\exists r \in F)\ r \in (\delta')^*(E(\{q_0\}), w) & [\text{Def. of } F'] \\
& \Leftrightarrow & (\exists r \in F)\ q_0 \stackrel{w}{\Longrightarrow} r & [\text{Lemma 6}] \\
& \Leftrightarrow & w \in L(N) & [\text{Def. of } L(N)]
\end{array}
$$

Correctness Proof of Subset Construction (Cont'd)

Now we are ready to show $L(M) = L(N)$.

$$
\begin{array}{llll}
w \in L(M) & \Leftrightarrow & (\delta')^*(E(\{q_0\}), w) \in F' & \\
 & \Leftrightarrow & (\exists r \in F)\ \ r \in (\delta')^*(E(\{q_0\}), w) & \text{[Def. of } F'\text{]} \\
 & \Leftrightarrow & (\exists r \in F)\ \ q_0 \stackrel{w}{\Longrightarrow} r & \text{[Lemma 6]} \\
 & \Leftrightarrow & w \in L(N) & \text{[Def. of } L(N)\text{]}
\end{array}
$$

Correctness Proof of Subset Construction (Cont'd)

Now we are ready to show $L(M) = L(N)$.

$w \in L(M)$	$\Leftrightarrow$	$(\delta')^*(E(\{q_0\}), w) \in F'$	
	$\Leftrightarrow$	$(\exists r \in F)\ \ r \in (\delta')^*(E(\{q_0\}), w)$	[Def. of F']
	$\Leftrightarrow$	$(\exists r \in F)\ \ q_0 \overset{w}{\Longrightarrow} r$	[Lemma 6]
	$\Leftrightarrow$	$w \in L(N)$	[Def. of $L(N)$]

Correctness Proof of Subset Construction (Cont'd)

Now we are ready to show $L(M) = L(N)$.

$$
\begin{array}{llll}
w \in L(M) & \Leftrightarrow & (\delta')^*(E(\{q_0\}), w) \in F' & \\
 & \Leftrightarrow & (\exists r \in F)\ \ r \in (\delta')^*(E(\{q_0\}), w) & \text{[Def. of } F'\text{]} \\
 & \Leftrightarrow & (\exists r \in F)\ \ q_0 \stackrel{w}{\Longrightarrow} r & \text{[Lemma 6]} \\
 & \Leftrightarrow & w \in L(N) & \text{[Def. of } L(N)\text{]}
\end{array}
$$

A DFA Equivalent to N_4

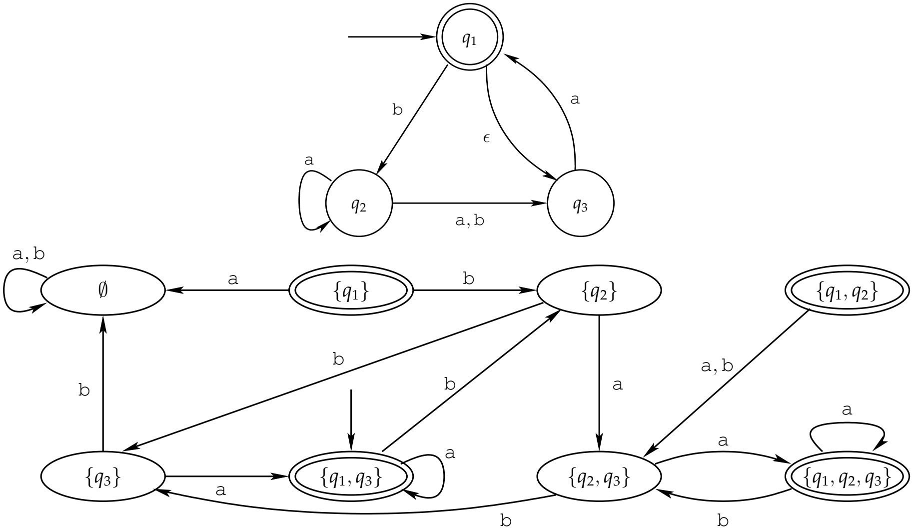
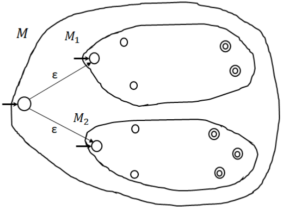


Figure: A DFA Equivalent to N_4

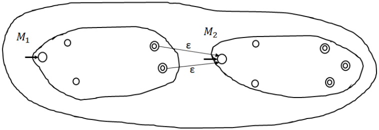
Closure Properties – Revisited

Closed under *Union*, *Concatenation* and *Star*. (Proof Idea):

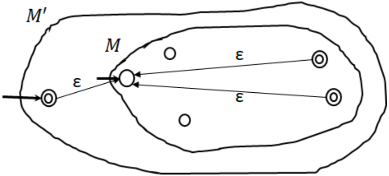
Union



Concatenation



Star



(Figures from M. Sipser's lecture notes)

Closure Properties – Revisited

Theorem 7

The class of regular languages is closed under the union operation.

Proof.

Let $N_i = (Q_i, \Sigma, \delta_i, q_i, F_i)$ recognize A_i for $i = 1, 2$. Construct $N = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{q_0\} \cup Q_1 \cup Q_2$;
- $F = F_1 \cup F_2$; and
- $\delta(q, a) = \begin{cases} \delta_1(q, a) & q \in Q_1 \\ \delta_2(q, a) & q \in Q_2 \\ \{q_1, q_2\} & q = q_0 \text{ and } a = \epsilon \\ \emptyset & q = q_0 \text{ and } a \neq \epsilon \end{cases}$

□

- Why is $L(N) = L(N_1) \cup L(N_2)$?

Closure Properties – Revisited

Theorem 8

The class of regular languages is closed under the concatenation operation.

Proof.

Let $N_i = (Q_i, \Sigma, \delta_i, q_i, F_i)$ recognize A_i for $i = 1, 2$. Construct $N = (Q, \Sigma, \delta, q_1, F_2)$ where

- $Q = Q_1 \cup Q_2$; and
- $$\delta(q, a) = \begin{cases} \delta_1(q, a) & q \in Q_1 \text{ and } q \notin F_1 \\ \delta_1(q, a) & q \in F_1 \text{ and } a \neq \epsilon \\ \delta_1(q, a) \cup \{q_2\} & q \in F_1 \text{ and } a = \epsilon \\ \delta_2(q, a) & q \in Q_2 \end{cases}$$

□

- Why is $L(N) = L(N_1) \cdot L(N_2)$?

Closure Properties – Revisited

Theorem 9

The class of regular languages is closed under the star operation.

Proof.

Let $N_1 = (Q_1, \Sigma, \delta_1, q_1, F_1)$ recognize A_1. Construct $N = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{q_0\} \cup Q_1$;
- $F = \{q_0\} \cup F_1$; and
- $\delta(q, a) = \begin{cases} \delta_1(q, a) & q \in Q_1 \text{ and } q \notin F_1 \\ \delta_1(q, a) & q \in F_1 \text{ and } a \neq \epsilon \\ \delta_1(q, a) \cup \{q_1\} & q \in F_1 \text{ and } a = \epsilon \\ \{q_1\} & q = q_0 \text{ and } a = \epsilon \\ \emptyset & q = q_0 \text{ and } a \neq \epsilon \end{cases}$

□

- Why is $L(N) = [L(N_1)]^*$?

Closure Properties – Revisited

Theorem 10

The class of regular languages is closed under complementation.

Proof.

Let $M = (Q, \Sigma, \delta, q_0, F)$ be a DFA recognizing A. Consider $\overline{M} = (Q, \Sigma, \delta, q_0, Q \setminus F)$. We have $w \in L(M)$ if and only if $w \notin L(\overline{M})$. That is, $L(\overline{M}) = \overline{A}$ as required. □

Theorem 11

The class of regular languages is closed under intersection.

Proof.

Recall that $R \cap S = \overline{\overline{R} \cup \overline{S}}$. □

Other Variants of Finite Automata

- 2-Way Finite Automata: In each transition, the input head can move either left ($\leftarrow$) or right ($\rightarrow$).
  - 2DFA: $\delta : Q \times \Sigma \rightarrow Q \times \{\leftarrow, \rightarrow\}$
  - 2NFA: $\delta : Q \times \Sigma \rightarrow 2^{Q \times \{\leftarrow, \rightarrow\}}$
- Co-deterministic FA: If $p \xrightarrow{a} r, q \xrightarrow{a} r$, then $p = q$.

  Recall that for DFA, if $p \xrightarrow{a} q, p \xrightarrow{a} r$, then $q = r$.
- Reversible FA: FA that are both deterministic and co-deterministic.

FACTS:

- DFA $\equiv$ co-det FA $\equiv$ NFA $\equiv$ 2DFA $\equiv$ 2NFA.
- 1-way reversible FA are weaker than DFA. (Note: $(aa)^* \cup \{a\}$ cannot be accepted by a Reversible FA.
- 2-way reversible FA accept exactly regular languages.
- Converting a 2DFA to a DFA incurs an exponential blowup in the number of states.

Regular Expressions (Syntax)

Definition 12

R is a *regular expression* if R is

- a for some $a \in \Sigma$;
- ϵ;
- $\emptyset$;
- $(R_1 + R_2)$ where R_1 and R_2 are regular expressions;
- $(R_1 \cdot R_2)$ where R_1 and R_2 are regular expressions; or
- (R_1^*) where R_1 is a regular expression.

- We write R^+ for $R \cdot R^*$. Hence $R^* = R^+ + \epsilon$.
- Moreover, write R^k for $\overbrace{R \cdot R \cdot \cdots \cdot R}^{k}$.
  - Define $R^0 = \epsilon$. We have $R^* = R^0 + R^1 + \cdots + R^n + \cdots$.
- $L(R)$ denotes the language described by the regular expression R.
- Note that $\emptyset \neq \{\epsilon\}$. $+$ is also written as "$\cup$" is many textbooks

Regular Expressions (Semantics)

Definition 13

The language associated with a regular expression R, written as $L(R)$, is defined recursively as

- $L(a) = \{a\}, a \in \Sigma$;
- $L(\epsilon) = \{\epsilon\}$;
- $L(\emptyset) = \emptyset$;
- $L(R_1 + R_2) = L(R_1) \cup L(R_2)$
- $L(R_1 \cdot R_2) = L(R_1) \cdot L(R_2)$
- $L(R_1^*) = (L(R_1))^*$

Examples of Regular Expressions

- For convenience, we write RS for $R \cdot S$.
- We may also write the regular expression R to denote its language $L(R)$.
- $L(\mathtt{0}^*\mathtt{1}\mathtt{0}^*) = \{w : w \text{ contains a single } \mathtt{1}\}$.
- $L(\Sigma^*\mathtt{1}\Sigma^*) = \{w : w \text{ has at least one } \mathtt{1}\}$.
- $L((\Sigma\Sigma)^*) = \{w : w \text{ is a string of even length }\}$.
- $(\mathtt{0} + \epsilon)(1 + \epsilon) = \{\epsilon, \mathtt{0}, \mathtt{1}, \mathtt{01}\}$.
- $\mathtt{1}^*\emptyset = \emptyset$.
- $\emptyset^* = \{\epsilon\}$.
- For any regular expression R, we have $R + \emptyset = R$ and $R \cdot \epsilon = R$.

Regular Expressions and Finite Automata

Lemma 14

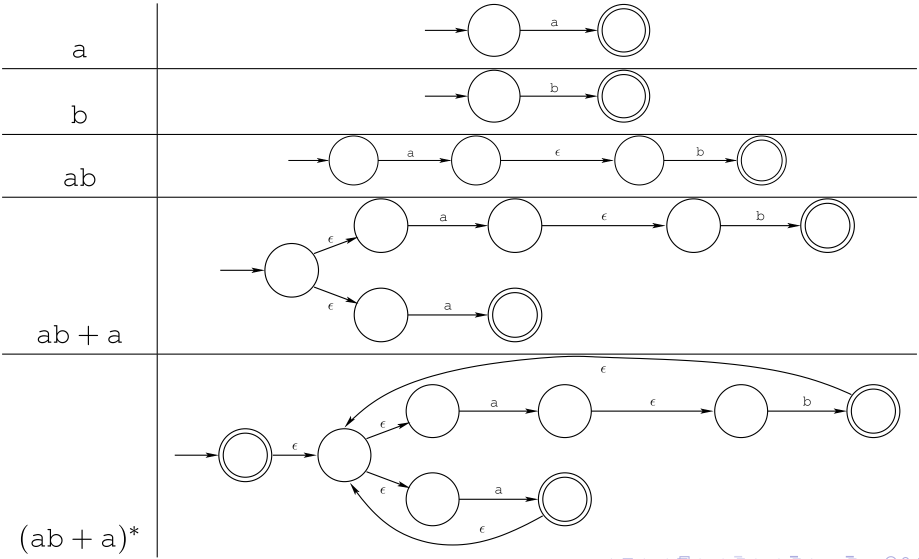
If a language is described by a regular expression, it is regular.

Proof.

We prove by induction on the regular expression R.

- $R = a$ for some $a \in \Sigma$. Consider the NFA $N_a = (\{q_1, q_2\}, \Sigma, \delta, q_1, \{q_2\})$ where
$$\delta(r, y) = \begin{cases} \{q_2\} & r = q_1 \text{ and } y = a \\ \emptyset & \text{otherwise} \end{cases}$$
- $R = \epsilon$. Consider the NFA $N_\epsilon = (\{q_1\}, \Sigma, \delta, q_1, \{q_1\})$ where $\delta(r, y) = \emptyset$ for any r and y.
- $R = \emptyset$. Consider the NFA $N_\emptyset = (\{q_1\}, \Sigma, \delta, q_1, \emptyset)$ where $\delta(r, y) = \emptyset$ for any r and y.
- $R = R_1 + R_2$, $R = R_1 \cdot R_2$, or $R = R_1^*$. By inductive hypothesis and the closure properties of finite automata. □

Regular Expressions and Finite Automata



Lemma 15

If a language is regular, it is described by a regular expression.

For the proof, we introduce a generalization of finite automata.

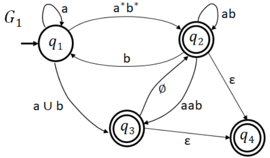
Generalized Nondeterministic Finite Automata

Definition 16

A *generalized nondeterministic finite automaton* is a 5-tuple $(Q, \Sigma, q_{\text{start}}, q_{\text{accept}})$ where

- Q is the finite set of states; Σ is the input alphabet;
- $\delta : (Q - \{q_{\text{accept}}\}) \times (Q - \{q_{\text{start}}\}) \to \mathcal{R}$ is the transition function, where $\mathcal{R}$ denotes the set of regular expressions;
- q_{start} is the start state; and q_{accept} is the accept state.

A GNFA *accepts* a string $w \in \Sigma^*$ if $w = w_1 w_2 \cdots w_k$ where $w_i \in \Sigma^*$ and there is a sequence of states $r_0, r_1, \ldots, r_k$ such that $r_0 = q_{\text{start}}$; $r_k = q_{\text{accept}}$; and for every i, $w_i \in L(R_i)$ where $R_i = \delta(q_{i-1}, q_i)$.



(Fig. from M. Sipser)

Finite Automata to Regular Expressions - State Elimination

Proof of Lemma.

Let M be the DFA for the regular language. Construct an equivalent GNFA G by adding $q_{\text{start}}, q_{\text{accept}}$ and necessary ϵ-transitions.
CONVERT (G):

1. Let k be the number of states of G.
2. If $k = 2$, then return the regular expression R labeling the transition from q_{start} to q_{accept}.
3. If $k > 2$, select $q_{\text{rip}} \in Q \setminus \{q_{\text{start}}, q_{\text{accept}}\}$. Construct $G' = (Q', \Sigma, \delta', q_{\text{start}}, q_{\text{accept}})$ where
   - $Q' = Q \setminus \{q_{\text{rip}}\}$;
   - for any $q_i \in Q' \setminus \{q_{\text{accept}}\}$ and $q_j \in Q' \setminus \{q_{\text{start}}\}$, define $\delta'(q_i, q_j) = (R_1)(R_2)^*(R_3) \cup R_4$ where $R_1 = \delta(q_i, q_{\text{rip}})$, $R_2 = \delta(q_{\text{rip}}, q_{\text{rip}})$, $R_3 = \delta(q_{\text{rip}}, q_j)$, and $R_4 = \delta(q_i, q_j)$.
4. return CONVERT (G').

□

FA to RE - State Elimination

Lemma 17

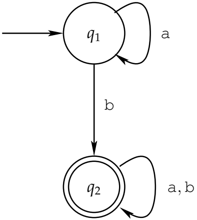
For any GNFA G, CONVERT (G) is equivalent to G.

Proof.

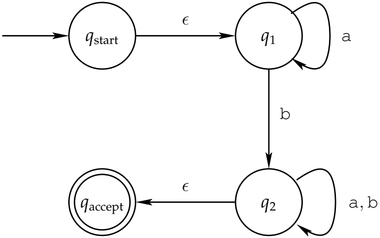
We prove by induction on the number k of states of G.

- $k = 2$. Trivial.
- Assume the lemma holds for $k - 1$ states. We first show G' is equivalent to G. Suppose G accepts an input w. Let $q_{\text{start}}, q_1, q_2, \ldots, q_{\text{accept}}$ be an accepting computation of G. We have $q_{\text{start}} \xrightarrow{w_1} q_1 \cdots q_{i-1} \xrightarrow{w_i} q_i \xrightarrow{w_{i+1}} q_{\text{rip}} \cdots q_{\text{rip}} \xrightarrow{w_{j-1}} q_{\text{rip}} \xrightarrow{w_j} q_j \cdots q_{\text{accept}}$. Hence $q_{\text{start}} \xrightarrow{w_1} q_1 \cdots q_{i-1} \xrightarrow{w_i} q_i \xrightarrow{w_{i+1} \cdots w_j} q_j \cdots q_{\text{accept}}$ is a computation of G'. Conversely, any string accepted by G' is also accepted by G since the transition between q_i and q_j in G' describes the strings taking q_i to q_j in G. Hence G' is equivalent to G. By inductive hypothesis, CONVERT (G') is equivalent to G'. □

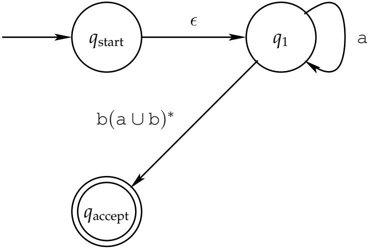
Finite Automata to Regular Expressions - State Elimination

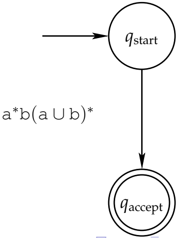


(a) DFA M

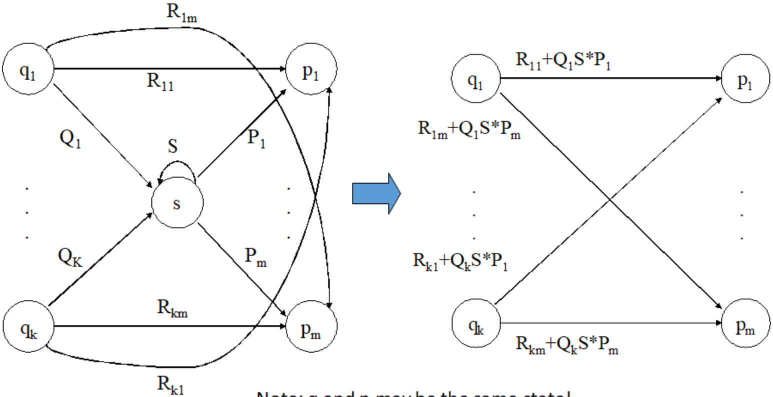


(b) GNFA G





In general ...



Note: q and p may be the same state!

Theorem 18

A language is regular if and only if some regular expression describes it.

Pumping Lemma

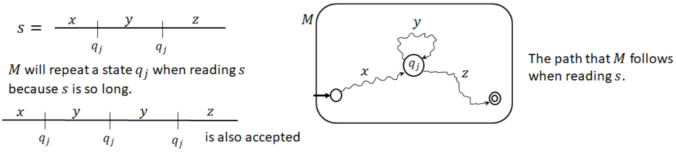
A tool for proving non-regularity.

Lemma 19

If A is a regular language, then there is a number p such that for any $s \in A$ of length at least p, there is a partition $s = xyz$ with

1. *for each $i \geq 0$, $xy^iz \in A$;*
2. $|y| > 0$; *and*
3. $|xy| \leq p$.

Proof Idea:



(Fig. from M. Sipser)

Pumping Lemma (Proof)

Proof.

Let $M = (Q, \Sigma, \delta, q_1, F)$ be a DFA recognizing A and $p = |Q|$. Consider any string $s = \sigma_1\sigma_2 \cdots \sigma_{m-1}$ of length $m - 1 \geq p$. Let $q_1, \ldots, q_m$ be the sequence of states such that $q_{i+1} = \delta(q_i, \sigma_i)$ for $1 \leq i \leq m - 1$. Since $m \geq p + 1 = |Q| + 1$, there are $1 \leq s < t \leq p + 1$ such that $q_s = q_t$ (why?). Let $x = \sigma_1 \cdots \sigma_{s-1}$, $y = \sigma_s \cdots \sigma_{t-1}$, and $z = \sigma_t \cdots \sigma_{m-1}$. Note that $q_1 \xrightarrow{x} q_s$, $q_s \xrightarrow{y} q_t$, and $q_t \xrightarrow{z} q_m \in F$. Thus M accepts xy^iz for $i \geq 0$. Since $t \neq s$, $|y| > 0$. Finally, $|xy| \leq p$ for $t \leq p + 1$. □

How to Use Pumping Lemma?

Recall that Pumping Lemma can be expressed as the following logical formula:

$$A \text{ is regular } \Rightarrow \exists p \in \mathbb{N}, \forall_{s,(s\in A)\wedge(|s|\geq p)} \exists_{x,y,z,\ s=xyz}((1) \wedge (2) \wedge (3))$$

which is equivalent to

$$\neg(\exists p \in \mathbb{N}, \forall_{s,(s\in L)\wedge(|s|\geq p)} \exists_{x,y,z,\ s=xyz}((1) \wedge (2) \wedge (3))) \Rightarrow A \text{ is NOT regular}$$

Note that the left-hand side is

$$\forall p \in \mathbb{N}, \exists_{s,(s\in A)\wedge(|s|\geq p)}, \forall_{x,y,z,\ s=xyz}(\neg(1) \vee \neg(2) \vee \neg(3))$$

How to Use Pumping Lemma?

In view of "

$\forall p \in \mathbb{N}, \exists_{s,(s \in A) \wedge (|s| \geq p)}, \forall_{x,y,z,\ s=xyz} (\neg(1) \vee \neg(2) \vee \neg(3))$, " $\Rightarrow$ NOT regular

proving A is not regular resembles a *two-player game* between **YOU** and your **adversary** (ADV), such that your goal is to prove non-regularity, while ADV wants to spoil it.

1. ADV picks an arbitrary $p \in \mathbb{N}$
2. YOU pick an s, $s \in A, |s| \geq p$
3. ADV picks *arbitrary* x, y, z with $s = xyz$
4. YOU show $\neg(1) \vee \neg(2) \vee \neg(3)$
   - $\neg(2)$ and $\neg(3)$ are trivial to check
   - YOU establish $(2) \wedge (3) \Rightarrow \neg(1)$, i.e., $(|y| > 0) \wedge (|xy| \leq p) \ \Rightarrow \ \exists i \geq 0, xy^iz \notin A$.

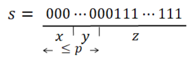
Applications of Pumping Lemma

Example 20

$B = \{0^n 1^n : n \geq 0\}$ is not a regular language.

Proof.

Choose $s = 0^p 1^p$. Then $s \in B$ and $|s| \geq p$, there is a partition $s = xyz$



such that $xy^i z \in B$ for $i \geq 0$.

- $y \in 0^+$ or $y \in 1^+$. $xz \notin B$. A contradiction.
- $y \in 0^+1^+$. $xyyz \notin B$. A contradiction. □

Corollary 21

$C = \{w : w$ has an equal number of 0's and 1's$\}$ is not a regular language.

Proof.

Suppose C is regular. Then $B = C \cap 0^*1^*$ is regular. □

Applications of Pumping Lemma

Example 22

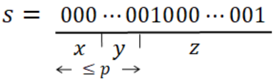
Is $B' = \{\texttt{0}^n\texttt{1}^n : 0 \leq n \leq 10^{100}\}$ regular?
(What if ADV picks $p = 2 \times 10^{101}$?)

Example 23

$F = \{ww : w \in \{\texttt{0}, \texttt{1}\}^*\}$ is not a regular language.

Proof.

Suppose F is a regular language and p the pumping length. Choose $s = \texttt{0}^p\texttt{1}\texttt{0}^p\texttt{1}$. By the pumping lemma, there is a partition $s = xyz$ such that $|xy| \leq p$ and $xy^iz \in F$ for $i \geq 0$. Since $|xy| \leq p$, $y \in \texttt{0}^+$. But then $xz \notin F$. A contradiction. □



Applications of Pumping Lemma

Example 24

$D = \{1^{n^2} : n \geq 0\}$ is not a regular language.

Proof.

Suppose D is a regular language and p the pumping length. Choose $s = 1^{p^2}$. By the pumping lemma, there is a partition $s = xyz$ such that $|y| > 0$, $|xy| \leq p$, and $xy^iz \in D$ for $i \geq 0$.
Consider the strings xyz and xy^2z. We have $|xyz| = p^2$ and $|xy^2z| = p^2 + |y| \leq p^2 + p < p^2 + 2p + 1 = (p+1)^2$. Since $|y| > 0$, we have $p^2 = |xyz| < |xy^2z| < (p+1)^2$. Thus $xy^2z \notin D$. A contradiction. □

Theorem 25

For $\{1^{f(n)} : n \geq 0\}$ to be regular, $f(n)$ must be a linear function of the form $f(n) = an + b$.

Applications of Pumping Lemma

Example 26

$E = \{0^i 1^j : i > j\}$ is not a regular language.

Proof.

Suppose E is a regular language and p the pumping length. Choose $s = 0^{p+1}1^p$. By the pumping lemma, there is a partition $s = xyz$ such that $|y| > 0$, $|xy| \leq p$, and $xy^iz \in E$ for $i \geq 0$. Since $|xy| \leq p$, $y \in 0^+$. But then $xz \notin E$ for $|y| > 0$. A contradiction. □

Example 27

$F = \{a^p : p \text{ is prime}\}$ is not a regular language.

Proof.

(Sketch) Suppose $a^p = a^x a^y a^z$, i.e., $p = x + y + z$. Consider $q = x + z$. Then $a^x (a^y)^q a^z = a^{x+y(x+z)+z} = a^{(x+z)(y+1)}$. □

Pumping Lemma is not a Sufficient Condition

Example 28

We know $L = \{b^m c^m | m > 0\}$ is not regular. Let us consider $L' = a^+ L \cup (b + c)^*$. L' is not regular. If L' would be regular, then we can prove that L is regular (using the closure properties we will see next). However, the Pumping lemma does apply for L' with $n = 1$.

Consider string $ab^n c^n$ and partition $\overbrace{\epsilon}^{u}\overbrace{a}^{v}\overbrace{b^n c^n}^{w}$. Then $uv^i w, \forall i \geq 0$ remains in L'.

This shows the Pumping lemma is not a sufficient condition for a language to be regular. That is, satisfying PL does not always yield a regular language.

Be cautious that you CANNOT use partition $\overbrace{a}^{u}\overbrace{b}^{v}\overbrace{b^{n-1} c^n}^{w}$ to establish a contradiction, because it is the role of ADV (not YOU) to pick a partition.

Use of closure properties to show non-regularity

- We can easily prove $L_1 = \{0^n 1^n | n > 0\}$ is not a regular language.
- L_2 = the set of strings with an equal number of 0's and 1's isn't either, but that fact is trickier to prove.
- Regular languages are closed under $\cap$.
- If L_2 were regular, then $L_2 \cap L(0^* 1^*) = L_1$ would be, but it isn't.

Closure properties

Let L and M be regular. Then $L = L(R) = L(D)$ and $M = L(S) = L(F)$ for regular expressions R and S, and DFA D and F.
We have seen that RL are closed under the following operations:

- Union : $L \cup M = L(R + S)$
- Complement : $\bar{L} = L(\bar{D})$
- Intersection : $L \cap M = \overline{\bar{L} \cup \bar{M}}$
- Difference : $L - M = L \cap \bar{M}$
- Concatenation : $LM = L(RS)$
- Closure : $L^* = L(R^*)$
- Prefix : $Prefix(L) = \{x \mid \exists y \in \Sigma^*, xy \in L\}$ (Hint: in D, make final all states in a path from the start state to final state)
- quotient, morphism, inverse morphism, substitution, ...

Quotient

Definition 29

$L_1, L_2 \subseteq \Sigma^*, L_1/L_2 = \{x \in \Sigma^* \mid \exists y \in L_2, xy \in L_1\}$.

$\overbrace{q_0 \xrightarrow{x} q}^{x \in L_1/L_2} \overbrace{\xrightarrow{y} \circledcirc}^{y \in L_2}$, where $xy \in L_1$. E.g. $\{00, 111\}/\{\epsilon, 1\} = \{00, 111, 11\}$

Note: $\mathit{Pref}(L) = L/\Sigma^*$.

Theorem 30

$L, R \subseteq \Sigma^*$. *If R is regular, then R/L is also regular.*

Proof Idea: Given an FA, change F to $F' = \{q \in Q \mid \exists y \in L, \delta^*(q, y) \in F\}$,

i.e., mark q as "Accept" if $\overbrace{q_0 \xrightarrow{x} q}^{x \in R/L} \overbrace{\xrightarrow{y} \circledcirc}^{y \in L}$. Note that L can be an arbitrary language.

Example 31

$L = \{a^{n^2} \mid n \geq 0\}$. $L/L = \{a^{n^2 - m^2} \mid m, n \geq 0\} = a(aa)^* + (a^4)^*$. Notice that L is not regular, but L/L is regular.

Morphisms (also called Homomorphisms)

- A morphism h is a mapping: $h : \Sigma \rightarrow \Delta^*$
- h can be extended to $h : \Sigma^* \rightarrow \Delta^*$ with $h(xy) = h(x)h(y), h(\epsilon) = \epsilon$
- Given a language $L \subseteq \Sigma^*$, $h(L) = \bigcup_{x \in L} \{h(x)\} \subseteq \Delta^*$

Example 32

$h(0) = ab, h(1) = ba, h(2) = \epsilon$.
$h(00212) = ababba$; $h(0022212222) = ababba$; (h is many-to-one)
$h(\{0^n21^n | n \geq 0\}) = \{(ab)^n(ba)^n | n \geq 0\}$

Theorem 33

Regular Languages are closed under morphism.

Note that $h(K \cup L) = h(K) \cup (L)$; $h(K \cdot L) = h(K) \cdot h(L)$; $h(K^*) = h(K)^*$.

Inverse Morphisms

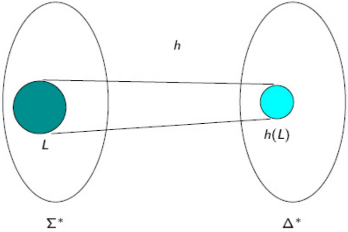
Given $h : \Sigma^* \to \Delta^*$, and $K \subseteq \Delta^*$, the inverse morphism $h^{-1}(K) = \{x \in \Sigma^* \mid h(x) \in K\}$.

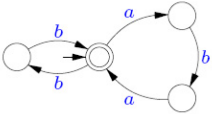
- It is easy to see $L \subseteq h^{-1}(h(L))$. How about R vs. $h(h^{-1}(R))$?
- Note that in Example 32, $\{0^n 2 1^n | n \geq 0\} \subsetneq h^{-1}(\{(ab)^n (ba)^n | n \geq 0\})$

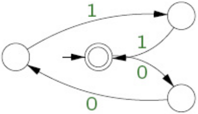
Theorem 34

Regular languages are closed under inverse morphism.

- Consider $h(0) = ab; h(1) = ba$, and FA M accepting $R \subseteq \{a, b\}^*$. Find FA M' accepting $h^{-1}(R) \subseteq \{0, 1\}^*$.
- M and M' have identical states
- $p \xrightarrow{ab} q$ in M iff $p \xrightarrow{0} q$ in M'; $\quad p \xrightarrow{ba} q$ in M iff $p \xrightarrow{1} q$ in M'







Shuffle

Definition 35

$x \| \epsilon = \epsilon \| x = \{x\}$
$ax \| by = a(x \| by) \cup b(ax \| y)$
$K \| L = \bigcup_{x \in K, y \in L} x \| y$

$abb \| aca = \{a\underline{a}bb\underline{ca}, \underline{aa}b\underline{c}b\underline{a}, aabcab, aacabb, aacbab,$
$aacbba, abbaca, ababca, abacba, abacab, acabba, acabab, acaabb\}.$

Theorem 36

If K, L are regular, so is $K \| L$.

- Given $L(M_1) = K, L(M_2) = L$, can you construct an FA M s.t. $L(M) = K \| L$?
- The next page contains an alternative proof using closure properties of regular languages.

Proof.

copies of alphabet

$$\Sigma,\ \Sigma_1 = \{\, a_1 \mid a \in \Sigma \,\},\ \Sigma_2 = \{\, a_2 \mid a \in \Sigma \,\}$$

$$h_1 : \Sigma_1 \cup \Sigma_2 \to \Sigma^* \qquad a_1 \mapsto a \qquad a_2 \mapsto \epsilon$$

$$h_2 : \Sigma_1 \cup \Sigma_2 \to \Sigma^* \qquad a_1 \mapsto \epsilon \qquad a_2 \mapsto a$$

$$g : \Sigma_1 \cup \Sigma_2 \to \Sigma^* \qquad a_1 \mapsto a \qquad a_2 \mapsto a$$

$$\begin{array}{ccccc} abbba & \stackrel{h_1}{\leftarrow} & a_1 b_1 a_2 c_2 b_1 a_2 c_2 b_1 a_1 & \stackrel{h_2}{\to} & acac \\ \in K & & \downarrow g & & \in L \\ & & abacbacba & & \end{array}$$

$$K \parallel L = g(\, h_1^{-1}(K) \cap h_2^{-1}(L) \,)$$

$\frac{1}{2}L$

Definition 37

$\frac{1}{2}L = \{x \in \Sigma^* | \exists y \in \Sigma^*, xy \in L; \;\; |y| = |x|\}.$

Theorem 38

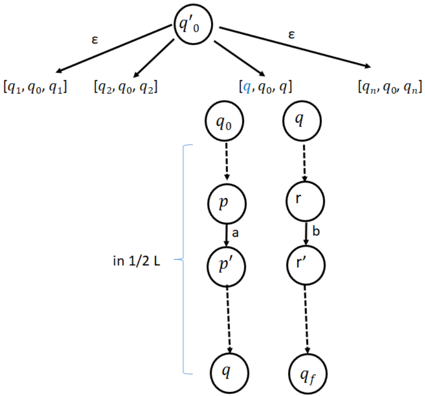
If L is regular, so is $\frac{1}{2}L$.

Proof.

guess middle state, simulate halves in parallel
$Q' = \{q'_0\} \cup Q \times Q \times Q$ (Note: middle, 1st, 2nd)
$\delta'(q'_0, \epsilon) = \{[q, q_0, q] | q \in Q\}$ – ϵ-move
$\delta'([q, p, r], a) = \{[q, \delta(p, a), \delta(r, b)]|$ some $b \in \Sigma\}$
$F' = \{[q, q, p] | q \in Q, p \in F\}$ □

Note: $x \in \frac{1}{2}L$ if $\exists q \in Q, v \in \Sigma^*, q_0 \overbrace{\to \ldots \to}^{x} q; q \overbrace{\to \ldots \to}^{v} p; |x| = |v|$ and $p \in F$.

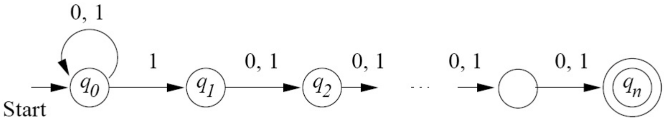
$\frac{1}{2}L$



- Can you show $\frac{1}{3}L = \{x \in \Sigma^* | \exists yz \in \Sigma^*, xyz \in L; \ |x| = |y| = |z|\}$ to be regular as well?
- How about $\frac{2}{3}L_{*-*} = \{xz | \exists x, y, z \in \Sigma^*, xyz \in L; |x| = |y| = |z|\}$?
(Not regular; Consider $L = a^*bc^*$. $\frac{2}{3}L_{*-*} \cap a^*c^* = ?$)

Exponential Blow-Up in Subset Construction

There is an NFA N with $n+1$ states that has no equivalent DFA with fewer than 2^n states.



$$L(N) = \{x\overbrace{1c_2c_3\cdots c_n}^{\text{length } n} : x \in \{0,1\}^*, c_i \in \{0,1\}\}.$$

- Suppose an equivalent DFA $D = (Q_D, \Sigma, \delta_D, q_0', F_D)$ with <u>fewer than</u> 2^n states exists. read.
- There are 2^n bit sequences $a_1a_2\cdots a_n \in \{0,1\}^n$.
- $\exists q \in Q_D,\ a_1a_2\cdots a_n,\ b_1b_2\cdots b_n \in \{0,1\}^n,\ a_1a_2\cdots a_n \neq b_1b_2\cdots b_n$ $\delta_D^*(q_0', a_1a_2\cdots a_n) = q = \delta_D^*(q_0', b_1b_2\cdots b_n)$

Exponential Blow-Up (Cont'd)

Let i be the first position from the right such that $a_i \neq b_i$. I.e.,
$a_1 \cdots a_{i-1} 1 a_{i+1} \cdots a_n$
$b_1 \cdots b_{i-1} 0 b_{i+1} \cdots b_n$
and $a_{i+1} \ldots a_n = b_{i+1} \ldots b_n$

Now

$$\delta_D^*(q_0', a_1 \cdots a_{i-1} 1 a_{i+1} \cdots a_n 0^{i-1}) = \delta_D^*(q_0', b_1 \cdots b_{i-1} 0 b_{i+1} \cdots b_n 0^{i-1})$$

as for some $r \in Q_D$

$$q_0' \overset{a_1 \cdots a_{i-1} 1 a_{i+1} \cdots a_n}{\rightarrow} q \overset{0^{i-1}}{\rightarrow} r$$

and

$$q_0' \overset{b_1 \cdots b_{i-1} 0 b_{i+1} \cdots b_n}{\rightarrow} q \overset{0^{i-1}}{\rightarrow} r.$$

Furthermore

$$\delta_D^*(q_0', a_1 \cdots a_{i-1} 1 a_{i+1} \cdots a_n 0^{i-1}) \in F_D$$
$$\delta_D^*(q_0', b_1 \cdots b_{i-1} 0 b_{i+1} \cdots b_n 0^{i-1}) \notin F_D$$

– A contradiction!

Decision Properties

- A decision property for a class of languages is an algorithm that takes a formal description of a language (e.g., a DFA) and tells whether or not some property holds.
- Example: Is language L empty?
  - Suppose the representation is a DFA (or a RE that you will convert to a DFA).
  - Can you tell if $L(A) = \emptyset$ for DFA A?
- The complexity depends on how languages are represented. E.g., DFA vs. NFA vs. RE for regular languages.

Why Decision Properties

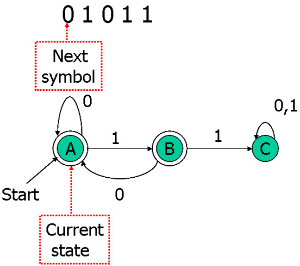
- When we talked about protocols represented as DFAs, we noted that important properties of a good protocol were related to the language of the DFA.
- Example: Does the protocol terminate? = Is the language finite?
- Example: Can the protocol fail? = Is the language nonempty?

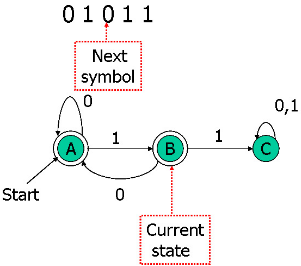
The Membership Question

Definition 39

Is string w in regular language L?

- Assume L is represented by a DFA A.
- Simulate the action of A on the sequence of input symbols forming w. (Question: What is the running time?)





The Emptiness Problem

Definition 40

Given a regular language, does the language contain any string at all.

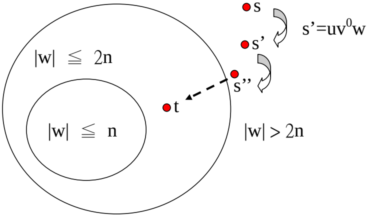
- Assume representation is DFA.
- Construct the transition graph.
- Compute the set of states reachable from the start state.
- If any final state is reachable, then yes, else no.
- Question: What is the running time?

The Infiniteness Problem

Definition 41

Is a given regular language infinite?

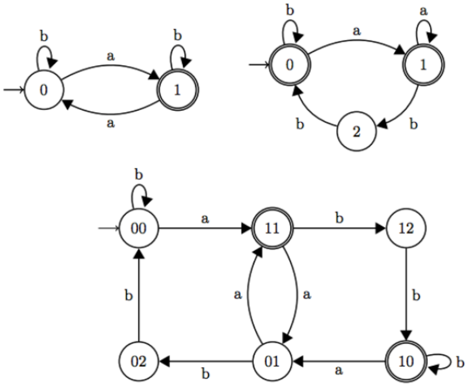
- Start with a DFA for the language.
- **Key idea**: if the DFA has n states, and the language contains any string of length n or more, then the language is infinite.
- **Second key idea**: if there is a string of length $> n$ (= number of states) in L, then there is a string of length between n and $2n - 1$.

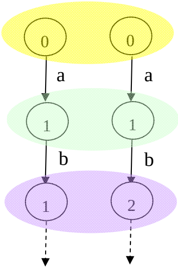


- Test for membership all strings of length between n and $2n - 1$. If any are accepted, then infinite, else finite.

The Product Automaton $M \times N$

Idea: Running two automata M and N in parallel.





Running the two FAs in parallel

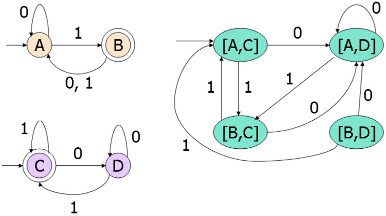
The Equivalence Problem

Definition 42

Given regular languages L and M, is $L = M$?

- Algorithm involves constructing the product DFA from DFA's for L and M.
- Let these DFA's have sets of states Q and R, respectively.
- Product DFA has set of states $Q \times R$. I.e., pairs $[q, r]$ with q in Q, r in R.

- Make the final states of the product DFA be those states $[q, r]$ such that exactly one of q and r is a final state of its own DFA. Thus, the product accepts w iff w is in exactly one of L and M.
- The product DFA's language is empty iff L = M.

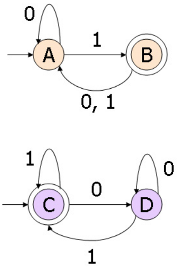


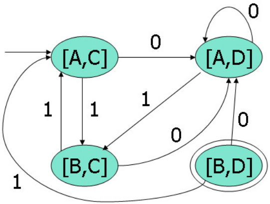
The Containment Problem

Definition 43

Given regular languages L and M, is $L \subseteq M$?

- Algorithm also uses the product automaton.
- How do you define the final states $[q, r]$ of the product so its language is empty iff $L \subseteq M$?
  - Answer: q is final; r is not.





Note: the only final state is unreachable, so containment holds.

The Minimum-State DFA for a Regular Language

- In principle, since we can test for equivalence of DFA's we can, given a DFA A find the DFA with the fewest states accepting $L(A)$.
- Test all smaller DFA's for equivalence with A.
- But that's a terrible algorithm.

– **Efficient State Minimization**

- Construct a table with all pairs of states.
- If you find a string that *distinguishes* two states (takes exactly one to an accepting state), mark that pair.
- Algorithm is a recursion on the length of the shortest distinguishing string.

Equivalence Relation

Definition 44

A binary relation R on a set S is a subset of $S \times S$. An *equivalence relation* on a set satisfies

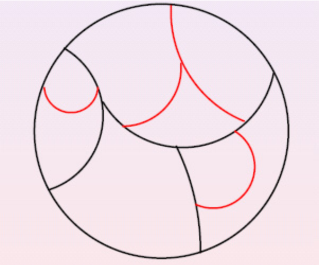
1. Reflexivity: For all x in S, xRx
2. Symmetry: For $x, y \in S$ $xRy \Leftrightarrow yRx$
3. Transitivity: For $x, y, z \in S$ $\ xRy \wedge yRz \Rightarrow xRz$

- Every equivalence relation on S partitions S into *equivalence classes*.
- The number of equivalence classes is called the *index* of the relation.
- An equivalence class containing x is written as $[x]$.
- E.g., *Mod* 3 is an equivalence relation which partitions $\mathbb{N}$ into equivalence classes $\{0, 3, 6, \ldots\}$, $\{1, 4, 7, \ldots\}$, and $\{2, 5, 8, \ldots\}$. The index is 3.

Refinement

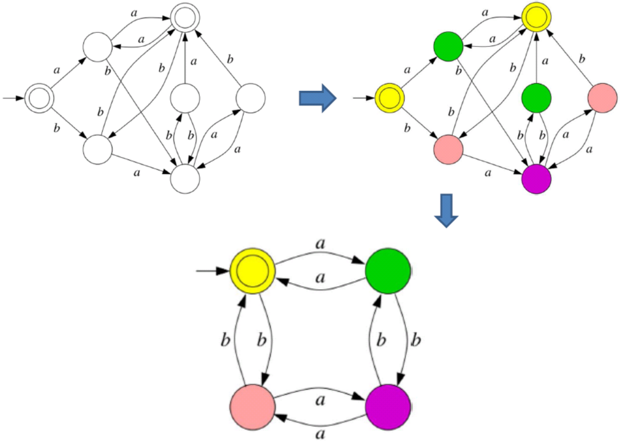
Definition 45

An equivalence relation R_1 is a refinement of R_2 if $R_1 \subseteq R_2$, i.e.
$(x, y) \in R_1 \Rightarrow (x, y) \in R_2$



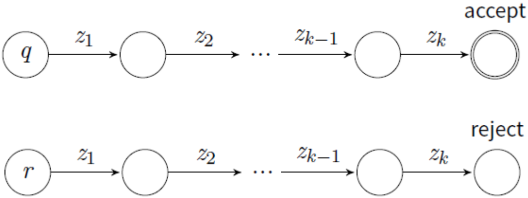
Minimizing DFAs

The Idea: Identify "indistinguishable states"; Merge those states.



Distinguishable States

Two states q and r are *distinguishable* if $\exists z_1, \ldots, z_k$

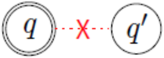


$$\text{I.e., } L_M(q) \neq L_M(r).$$

Indistinguishability (over Q) is also an equivalence relation, which partitions the set of states into equivalence classes.

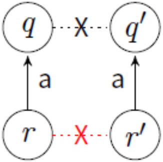
Finding (In)distinguishable States

Phase 1:



If q is accepting and q' is rejecting
Mark (q, q') as distinguishable (X)

Phase 2:

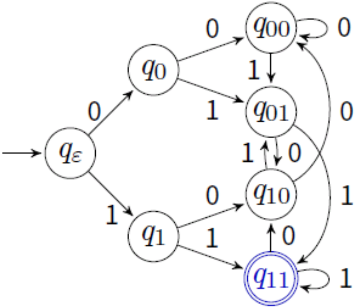


If (q, q') are marked
Mark (r, r') as distinguishable (X)

Phase 3:

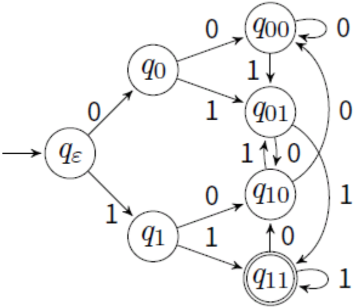
Unmarked pairs are indistinguishable
Merge them into groups

(Phase 1) q_{11} is distinguishable from all other states



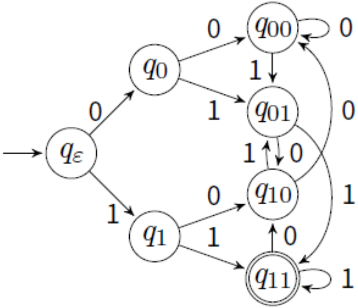
	q_ε	q_0	q_1	q_{00}	q_{01}	q_{10}
q_0						
q_1						
q_{00}						
q_{01}						
q_{10}						
q_{11}	X	X	X	X	X	X

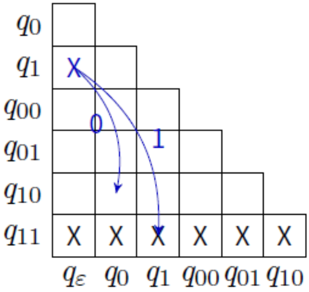
(Phase 2) Looking at $(r, r') = (q_\epsilon, q_0)$, Neither $(q_0, q_{00})_{input\ 0}$ nor $(q_1, q_{01})_{input\ 1}$ are distinguishable



	q_ε	q_0	q_1	q_{00}	q_{01}	q_{10}
q_0						
q_1						
q_{00}						
q_{01}						
q_{10}						
q_{11}	X	X	X	X	X	X

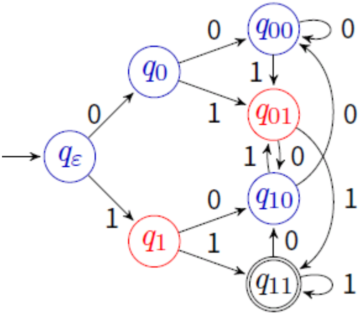
(Phase 2) Looking at $(r, r') = (q_\epsilon, q_1)$, $(q_1, q_{11})_{input\ 1}$ is distinguishable





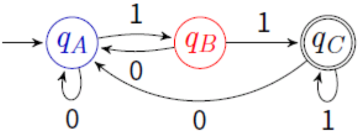
Example

(Phase 3) Merge states into groups (also called *equivalence classes*)



	q_ε	q_0	q_1	q_{00}	q_{01}	q_{10}
q_0	A					
q_1	X	X				
q_{00}	A	A	X			
q_{01}	X	X	B	X		
q_{10}	A	A	X	A	X	
q_{11}	X	X	X	X	X	X

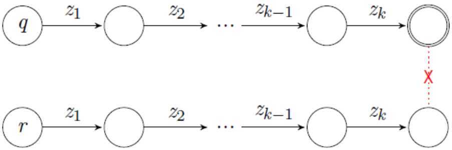
Minimized DFA:

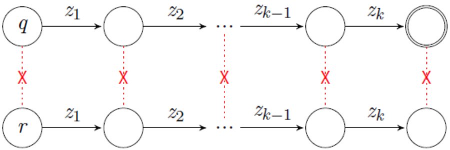


Why It Works?

Why have we found all distinguishable pairs?

- Because we work backwards!





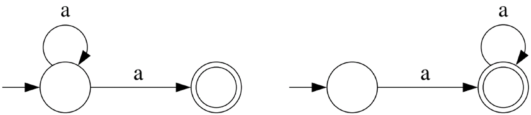
- It suffices to iterate Phase 2 at most $|Q|^2$ times. Why? What is the shortest string that distinguishes two states?

Unique Minimum DFA

Theorem 46

Every regular language has a single minimal automaton (up to isomorphism).

However, minimal NFAs are not unique as the following examples show.



Theorem 47

Given an NFA M and a number k, deciding if there is another NFA M' equivalent to M with at most k states is PSPACE-complete (polynomial-space complete).

Another way of Characterizing Regular Languages – Residuals of Languages

- The residual of a language $L \subseteq \Sigma^*$ with respect to a word w is the language
$$L^w = \{u \in \Sigma^* \mid wu \in L\}$$
- A language $L' \subseteq \Sigma^*$ is a residual of L if $L' = L^w$ for some $w \in \Sigma^*$.
- We define "indistinguishability" over strings
$$x \equiv_L y \Leftrightarrow (\forall z \in \Sigma^*, xz \in L \Leftrightarrow yz \in L).$$
$\equiv_L$ is an equivalence relation. Note that $x \equiv_L y \Leftrightarrow L^x = L^y$.
- Note that $\forall a \in \Sigma, (L^x = L^y) \Rightarrow (L^{xa} = L^{ya})$
  - The implication is that if we treat each residual L^w of L as a "state" and define $\delta(L^w, a) = L^{wa}$, δ is "consistent" in that $L^x = L^y$ (same state) implies $\delta(L^x, a) = L^{xa} = L^{ya} = \delta(L^y, a)$ (also same state).

Myhill-Nerode Theorem

Theorem 48 (Myhill-Nerode Theorem)

A language is regular iff it has finitely many residuals.

Proof.

($\Rightarrow$) Let $A = (Q, \Sigma, \delta, q_0, F)$ be a DFA. The language recognized by A with q the initial state, denoted by $L_A(q)$, is a residual of $L(A)$. Moreover, if $\delta(q_0, x) = \delta(q_0, y) = q$, for some q, then $L^x = L^y$.

($\Leftarrow$) Let $L \subseteq \Sigma^*$ be a regular language, the canonical DFA of L $M_L = (Q_L, \Sigma, \delta_L, q_{0L}, F_L)$ is

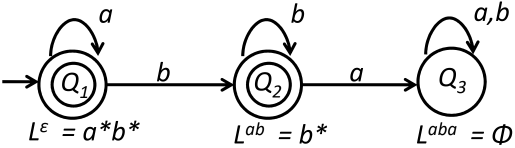
- Q_L is the set of residuals of L, i.e., $Q_L = \{L^w \mid w \in \Sigma^*\}$
- $\delta_L(R, a) = L^{wa}$, where $R = L^w$, for some w, where $R \in Q_L$ and $a \in \Sigma$
- $q_{0L} = L^\epsilon = L$
- $F_L = \{R \in Q_L \mid \epsilon \in R\}$

It is easy to show that $L(M_L) = L$. □

An Example of M_L

$L = a^*b^* \subseteq \{a, b\}^*$

- $Q_L = \{Q_1, Q_2, Q_3\}$, where
  $Q_1 = a^*b^*(= L^\epsilon), Q_2 = b^*(= L^{ab}), Q_3 = \emptyset(= L^{aba})$
  (How about L^{aaa}, L^{aabbb}?)
- $q_{0L} = Q_1$
- $F_L = \{Q_1, Q_2\}$
- $\delta_L(Q_1, a) = Q_1$, $\delta_L(Q_1, b) = Q_2$, $\delta_L(Q_2, a) = Q_3$, $\delta_L(Q_2, b) = Q_2$, $\delta_L(Q_3, a \mid b) = Q_3$.
  - E.g., $\delta_L(Q_2, a) = \delta_L(L^{ab}, a) = L^{aba} = \emptyset = Q_3$



Uniqueness of the Canonical DFA

Theorem 49

If L is regular, then M_L is the unique minimal DFA up to isomorphism recognizing L.

- Let $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ be a DFA accepting L. Define a relation $R_{\mathcal{A}}$ as follows:
  - For $x, y \in \Sigma^*, xR_{\mathcal{A}}y \Leftrightarrow \delta(q_0, x) = \delta(q_0, y)$.

FACT: $R_{\mathcal{A}}$ refines $\equiv_L$.

- Can you show $xR_{\mathcal{A}}y \implies x \equiv_L y$?
- If so, $|Q| \geq$ the index of L under $\equiv_L$. Hence, M_L is a minimal DFA.

In Summary

Let $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ be a DFA. Consider two computations

$$q_0 \xrightarrow{x} p \xrightarrow{z} r_1 \qquad q_0 \xrightarrow{y} q \xrightarrow{z} r_2$$

- The min. proc. is to identify all *indistinguishable* pairs (p, q) such that $L_{\mathcal{A}}(p) = L_{\mathcal{A}}(q)$. That is, $\forall z$, either $r_1, r_2 \in F$ or $r_1, r_2 \notin F$.
  - Define $R_{\mathcal{A}}$ over Σ^* as $xR_{\mathcal{A}}y$ iff $\delta^*(q_0, x) = \delta^*(q_0, y)$, i.e., $p = q$ in Fig.
- Another viewpoint is to identify x, y with identical residual, i.e., $L^x = L^y$. In this case, x and y are *indistinguishable* strings.
  - The notion of residuals induces an equivalence relation $\equiv_L$ over Σ^* s.t. $x \equiv_L y$ iff $L^x = L^y$
  - **Myhill-Nerode Thm**: $\equiv_L$ is of finite index iff L is regular.
- $R_{\mathcal{A}}$ refines $\equiv_L \quad \Rightarrow \quad \equiv_L$ induces a minimal equivalent DFA.

Applications of the Myhill-Nerode Theorem

The MN theorem can be used to show that a particular language is regular without actually constructing the automaton or to show conclusively that a language is not regular.
Example. Is the following language regular

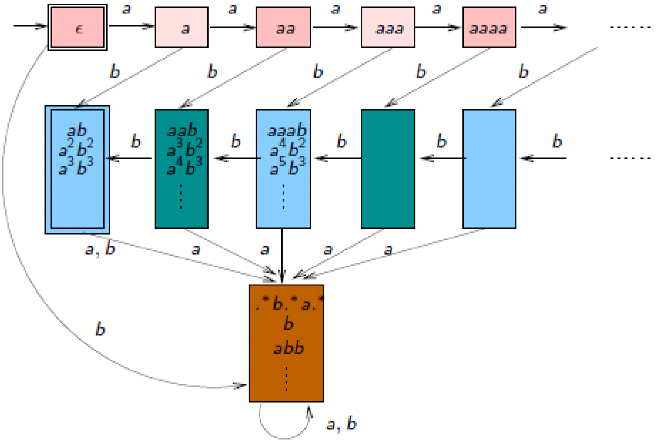
1. $L_1 = \{xy : |x| = |y|, x, y \in \Sigma^*\}$?
2. Example. What about the language
   $L_2 = \{xy : |x| = |y|, x, y \in \Sigma^* \text{ and } y \text{ ends with a } 1\}$?
3. Example. What about the language
   $L_3 = \{xy : |x| = |y|, x, y \in \Sigma^* \text{ and } y \text{ contains a } 1\}$?

Applications of the Myhill-Nerode Theorem (cont'd)

1. For the language L_1 there are two equivalence classes of $\equiv_{L_1}$. The first C_1 contains all strings of *even* length and the second C_2 all strings of *odd* length.
2. For L_2 we have the additional constraint that y ends with a 1. Class C_2 remains the same as that for L_1. Class C_1 is refined into classes C_1' which contains all strings of even length that end in a 1 and C_1'' which contains all strings of even length which end in a 0. Thus L_1 and L_2 are both regular.
3. For L_3 we have to distinguish for example, between the even length strings in the sequence 01, 0001, 000001,..., as 00 distinguishes the first string from all the others after it in the sequence (0100 $\notin L_3$, but 000100, 00000100... $\in L_3$), 0000 distinguishes the second from all the others ...

The $\equiv_L$ for $L = \{a^n b^n \; n \geq 0\}$

Describe the equivalence classes of $\equiv_L$ for $L = \{a^n b^n \; n \geq 0\}$



The automaton is NOT of finite state.

Supplementary Materials

Other Variants of Finite Automata

1. Weighted Finite Automata
2. Finite Transducer
3. Probabilistic Finite Automata
4. Tree Automata
5. Quantum Finite Automata

Finite Automata

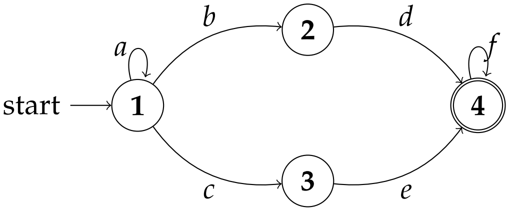


Figure: A Finite Automaton accepting string *abdf*.

Finite Transducers

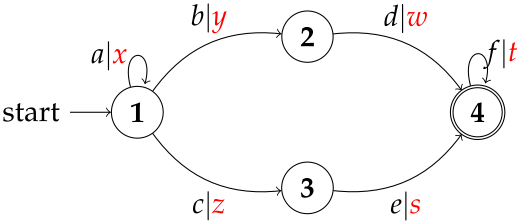


Figure: A Finite Transducer generating string *xywt* on input *abdf*.

Weighted Finite Automata

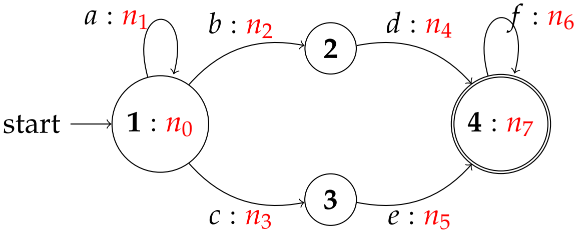


Figure: A Weighted Finite Automaton with weight $n_0 \otimes n_1 \otimes n_2 \otimes n_4 \otimes n_6 \otimes n_7$ on input *abdf*.

Weighted Finite Transducer

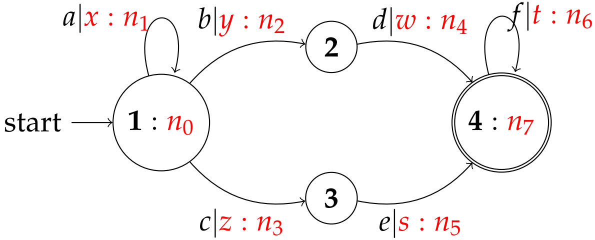
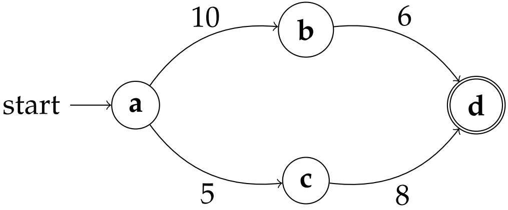


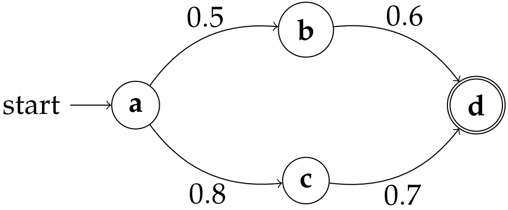
Figure: A Weighted Finite Transducer with output *xywt* and weight $n_0 \otimes n_1 \otimes n_2 \otimes n_4 \otimes n_6 \otimes n_7$ on input *abdf*.

Shortest Path



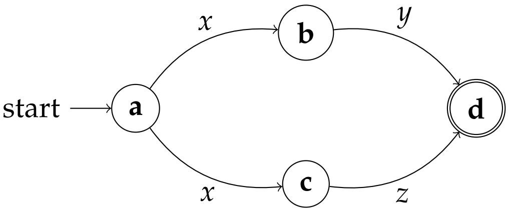
- Compute $10 + 6 = 16$ and $5 + 8 = 13$
- Output $min\{16, 13\}$.

Maximum Reliability



- Compute $0.5 \times 0.6 = 0.3$ and $0.8 \times 0.7 = 0.56$
- Output $max\{0.3, 0.56\}$.

Language Acceptor



- Compute $\{x\} \cdot \{y\}$ and $\{x\} \cdot \{z\} = xz$
- Output $\bigcup\{xy, xz\}$.

Generic Problem Solving

The above three problems were different on the surface, but at the core, they are actually very much the same problem. Consider:

- $min\{(10+6),(5+8)\}$
- $max\{(0.5 \times 0.6),(0.8 \times 0.7)\}$
- $\bigcup\{\{x\}\cdot\{y\},\{x\}\cdot\{z\}\}$

Hence, it is interesting to see how to unify the above in a single framework – Semiring.

The above three are semirings with operators $(min,+)$, $(max,\times)$ and $(\bigcup,\cdot)$.

Types of "Extended" Finite Automata

Type	Input	Output	Weight	Mapping
Finite Automata (FA)	✓			$\Sigma^* \to \{accept, reject\}$
Finite Transducer (FT)	✓	✓		$\Sigma^* \to 2^{\Gamma^*}$
Weighted FA (WFA)	✓		✓	$\Sigma^* \to S$
Weighted FT (WFT)	✓	✓	✓	$\Sigma^* \to 2^{\Gamma^*} \times S$

Abstract Algebra – Field

A Field is a 5-tuple $(S, \oplus, \otimes, \overline{0}, \overline{1})$, where S is a set and $\oplus$ and $\otimes$ are two operators, such that

Addition $\oplus$

- Associativity: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
- Commutativity: $a \oplus b = b \oplus a$
- Identity $\overline{0}$: $\overline{0} \oplus a = a \oplus \overline{0} = a$
- Inverse $-a$: $-a \oplus a = a \oplus -a = \overline{0}$

Multiplication $\otimes$

- Associativity: $(a \otimes b) \otimes c = a \otimes (b \otimes c)$
- Commutativity: $a \otimes b = b \otimes a$
- Identity $\overline{1}$: $\overline{1} \otimes a = a \otimes \overline{1} = a$
- Inverse a^{-1}: $a^{-1} \otimes a = a \otimes a^{-1} = \overline{1}$

Distributivity of Multiplication over Addition

- $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
- $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$

Abstract Algebra – Ring

A Ring is a 5-tuple $(S, \oplus, \otimes, \overline{0}, \overline{1})$, where S is a set and $\oplus$ and $\otimes$ are two operators, such that

Addition $\oplus$

- Associativity: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
- Commutativity: $a \oplus b = b \oplus a$
- Identity $\overline{0}$: $\overline{0} \oplus a = a \oplus \overline{0} = a$
- Inverse $-a$: $-a \oplus a = a \oplus -a = \overline{0}$

Multiplication $\otimes$

- Associativity: $(a \otimes b) \otimes c = a \otimes (b \otimes c)$
- Identity $\overline{1}$: $\overline{1} \otimes a = a \otimes \overline{1} = a$

Distributivity of Multiplication over Addition

- $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
- $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$

Example: Square Matrices

Abstract Algebra – Semiring

A Semiring is a 5-tuple $(S, \oplus, \otimes, \overline{0}, \overline{1})$, where S is a set and $\oplus$ and $\otimes$ are two operators, such that

Addition $\oplus$

- Associativity: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
- Commutativity: $a \oplus b = b \oplus a$
- Identity $\overline{0}$: $\overline{0} \oplus a = a \oplus \overline{0} = a$

Multiplication $\otimes$

- Associativity: $(a \otimes b) \otimes c = a \otimes (b \otimes c)$
- Identity $\overline{1}$: $\overline{1} \otimes a = a \otimes \overline{1} = a$

Distributivity of Multiplication over Addition

- $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
- $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$

Example: Probability

Examples of Semirings

- Probability: $([0,1], +, \times, 0, 1)$
- Boolean: $(\{0,1\}, \vee, \wedge, 0, 1)$
- Tropical: $(R, min, +, \infty, 0)$
- Log : $(R, \oplus_{LOG}, +, \infty, 0)$, where
  $x \oplus_{LOG} y = -\log(e^{-x} + e^{-y})$

An Algebraic View of DFA

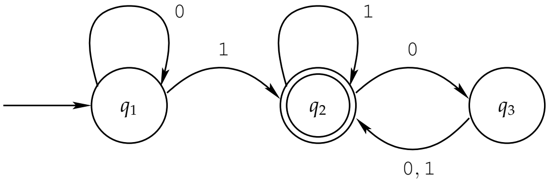


Figure: A Finite Automaton M_1

Consider the following matrix representation:

- Initial state $I = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$; final state $F = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$;

  $M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$; $M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

Algebraic View of DFA

The computation $q_1 \xrightarrow{1} q_2 \xrightarrow{0} q_3 \xrightarrow{1} q_2$ is represented by

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}^T \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} =$$

$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}^T \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} =$$

$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}^T \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}^T$$

As $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}^T \cdot F = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}^T \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 1$, the input "101" is accepted.

Algebraic View of NFA

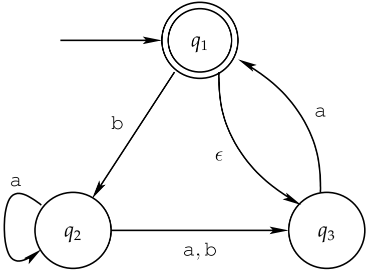


Figure: NFA N_4

$$M_a = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} ; M_b = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} ; M_\epsilon = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

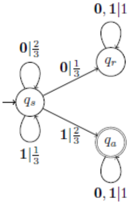
Matrix Multiplication

Question:
How to define matrix multiplication

$$\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \cdot \begin{pmatrix} b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,1} & b_{3,2} & b_{3,3} \end{pmatrix}$$ for the above examples"

- In $(a_{1,1} \cdot b_{1,1} + a_{1,2} \cdot b_{2,1} + a_{1,3} \cdot b_{3,1})$, for instance, the operations "." and "+" stand for integer multiplication and addition, resp.
- Suppose "1" and "0" stand for Boolean "True" and "False", resp., the operations "." and "+" stand for Boolean operations $\wedge$ and $\vee$, resp.
- Hence, conventional FA are with respect to $(\vee, \wedge)$-Semiring.

Probabilistic FA: $(+, \times)$-Semiring



PFA A_0: $q_s = q_1, q_r = q_2, q_a = q_3$

$$M_0 = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; M_1 = \begin{pmatrix} \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On input 011, we calculate

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}^T \cdot \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} \frac{2}{9} \\ \frac{1}{3} \\ \frac{4}{9} \end{pmatrix}^T \cdot \begin{pmatrix} \frac{1}{3} & 0 & \frac{2}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{2}{27} \\ \frac{1}{3} \\ \frac{16}{27} \end{pmatrix}^T$$

, where $\frac{16}{27}$ corresponds to

- $q_s \xrightarrow{0|\frac{2}{3}} a_s \xrightarrow{1|\frac{1}{3}} q_s \xrightarrow{1|\frac{2}{3}} q_a \Rightarrow$ prob. $= \frac{4}{27}$
- $q_s \xrightarrow{0|\frac{2}{3}} a_s \xrightarrow{1|\frac{2}{3}} q_a \xrightarrow{1|1} q_a \Rightarrow$ prob. $= \frac{4}{9}$

Probabilistic Finite Automaton – Formal Definition

A *probabilistic finite automaton* (PFA) A is a 5-tuple $(Q, \Sigma, \delta, q_0, F)$ where

- Q is a finite set of states;
- Σ is a finite alphabet;
- $\delta : Q \times \Sigma \times Q \to [0, 1]$ is the transition function, such that $\forall q, \in Q, \forall a \in \Sigma, \sum_{q' \in Q} \delta(q, a, q') = 1$, where $\delta(q, a, q')$ is a rational number;
- $q_0 \in Q$ is the start state; and
- $F \subseteq Q$ is the accept states.

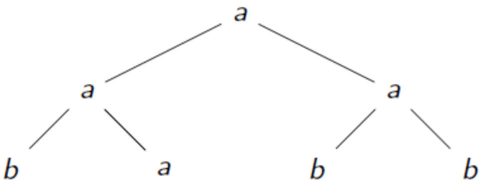
The language $L_{\Diamond x}(A) = \{u \in \Sigma^* \mid P_A(u) \Diamond x\}$, where $P_A(u)$ is the probability of acceptance on u, $x \in [0, 1]$, and $\Diamond \in \{<, \leq, =, \geq, >\}$.

- In general, $L_{\Diamond x}(A)$ may not be regular. For instance, $L_{>\frac{1}{2}}(A_0)$ and $L_{\geq\frac{1}{2}}(A_0)$ are not regular.
- $L_{\Diamond x}(A)$ is regular, if $x \in \{0, 1\}$.

Why Tree Automata?

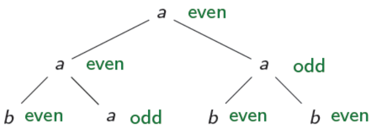
- Foundations of XML type languages (DTD, XML Schema, Relax NG...)
- Provide a general framework for XML type languages
- A tool to define regular tree languages with an operational semantics
- Provide algorithms for efficient validation
- Basic tool for static analysis (proofs, decision procedures in logic)
- ...

E.g. Binary trees with an even number of a's

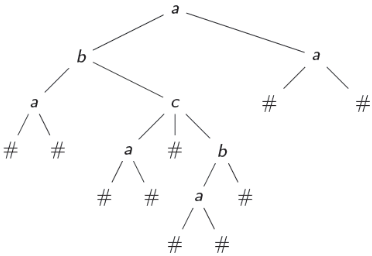


Binary Trees & Ranked Trees

- Binary trees with an even number of a's
- How to write transitions?
  - $(\text{even}, \text{odd}) \xrightarrow{a} \text{even}$
  - $(\text{even}, \text{even}) \xrightarrow{a} \text{odd}$
  - ...



- Ranked Tree:
  - Alphabet: $\{a^{(2)}, b^{(2)}, c^{(3)}, \#^{(0)}\}$
  - $a^{(k)}$: symbol a with arity$(a) = k$



Bottom-up (Ranked) Tree Automata

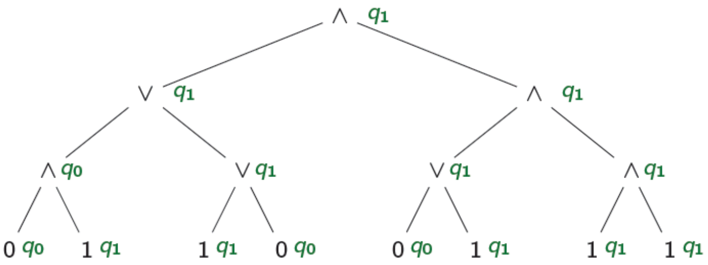
A **ranked bottom-up tree automaton** A consists of:

- $Alphabet(A)$: finite alphabet of symbols
- $States(A)$: finite set of states
- $Rules(A)$: finite set of transition rules
- $Final(A)$: finite set of final states ($\subseteq States(A)$)

where $Rules(A)$ are of the form $(q_1, ..., q_k) \stackrel{a^{(k)}}{\rightarrow} q$;

if $k = 0$, we write $\epsilon \stackrel{a^{(0)}}{\rightarrow} q$

Bottom-up Tree Automata: An Example



Principle

- $\mathsf{Alphabet}(A) = \{\wedge, \vee, 0, 1\}$
- $\mathsf{States}(A) = \{q_0, q_1\}$
- 1 accepting state at the root: $\mathsf{Final}(A) = \{q_1\}$

Rules(A)

$\epsilon \xrightarrow{0} q_0$	$\epsilon \xrightarrow{1} q_1$
$(q_1, q_1) \xrightarrow{\wedge} q_1$	$(q_0, q_1) \xrightarrow{\vee} q_1$
$(q_0, q_1) \xrightarrow{\wedge} q_0$	$(q_1, q_0) \xrightarrow{\vee} q_1$
$(q_1, q_0) \xrightarrow{\wedge} q_0$	$(q_1, q_1) \xrightarrow{\vee} q_1$
$(q_0, q_0) \xrightarrow{\wedge} q_0$	$(q_0, q_0) \xrightarrow{\vee} q_0$

Top-down (Ranked) Tree Automata

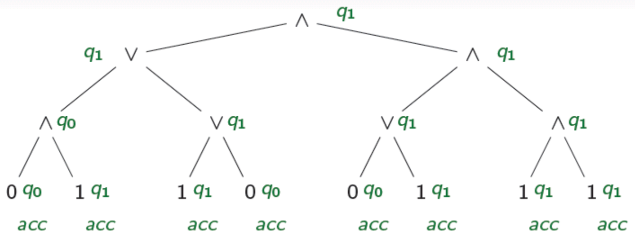
A **ranked top-down tree automaton** A consists of:

- $Alphabet(A)$: finite alphabet of symbols
- $States(A)$: finite set of states
- $Rules(A)$: finite set of transition rules
- $Final(A)$: finite set of final states ($\subseteq States(A)$)

where $Rules(A)$ are of the form $q \stackrel{a^{(k)}}{\rightarrow} (q_1, ..., q_k)$;
if $k = 0$, we write $\epsilon \stackrel{a^{(0)}}{\rightarrow} q$

Top-down tree automata also recognize all regular tree languages

Top-down Tree Automata: An Example



Principle

- starting from the root, guess correct values
- check at leaves
- 3 states: q_0, q_1, acc
- initial state at the root: q_1
- accepting if all leaves labeled acc

Transitions

$q_1 \xrightarrow{\wedge} (q_1, q_1)$ $\quad$ $q_1 \xrightarrow{\vee} (q_0, q_1)$

$q_0 \xrightarrow{\wedge} (q_0, q_1)$ $\quad$ $q_1 \xrightarrow{\vee} (q_1, q_0)$

$q_0 \xrightarrow{\wedge} (q_1, q_0)$ $\quad$ $q_1 \xrightarrow{\vee} (q_1, q_1)$

$q_0 \xrightarrow{\wedge} (q_0, q_0)$ $\quad$ $q_0 \xrightarrow{\vee} (q_0, q_0)$

$q_1 \xrightarrow{1} acc$ $\quad$ $q_0 \xrightarrow{0} acc$

Expressive Power of Tree Automata

Theorem 50

The following properties are equivalent for a tree language L:

(a) *L is recognized by a* **bottom-up non-deterministic** *tree automaton*

(b) *L is recognized by a* **bottom-up deterministic tree** *automaton*

(c) *L is recognized by a* **top-down non-deterministic** *tree automaton*

(d) *L is generated by a* **regular** *tree grammar*

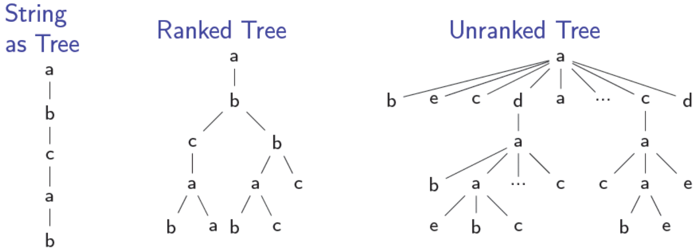
Deterministic Top-down Tree Automata

Deterministic top-down tree automata do not recognize all regular tree languages

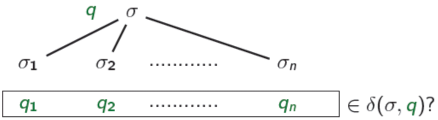
- Example:

$\text{Initial}(A) = q_0$
$q_0 \xrightarrow{a} (q, q)$
$q \xrightarrow{b} \epsilon$
$q \xrightarrow{c} \epsilon$
also accepts...

Unranked Trees



$\delta(\sigma, q)$: specified by a regular expression (i.e., regular language).



Quantum Entanglement

- An n-qubit system can exist in any superposition of the 2^n basis states.

$$\alpha_0|000...000\rangle + \alpha_1|000...001\rangle + \cdots + \alpha_{2^n-1}|111...111\rangle$$

- Sometimes such a state can be decomposed into the states of individual bits

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}((|0\rangle + |1\rangle))$$

- But,

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

is not decomposible, which is called an *entangled state*.

Unitary Evolution

- A quantum system that is not measured (i.e. does not interact with its environment) evolves in a unitary fashion.
- That is, it's evolution in a time step is given by a *unitary linear operation*.
- Such an operator is described by a matrix U such that

$$UU^* = I$$

where U^* is the *conjugate transpose* of U.

$$\begin{pmatrix} 3 & 3+i \\ 2-i & 2 \end{pmatrix}^* = \begin{pmatrix} 3 & 2+i \\ 3-i & 2 \end{pmatrix}$$

Quantum Automata

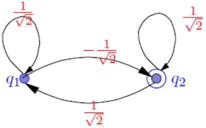
- Quantum finite automata are obtained by letting the matrices M_σ have complex entries. We also require each of the matrices to be unitary. E.g.

$$M_\sigma = \begin{pmatrix} -1 & 0 \\ 0 & i \end{pmatrix}$$

- If all matrices only have 0 or 1 entries and the matrices are unitary, then the automaton is deterministic and reversible.

Quantum Automata

Consider the automaton in a one letter alphabet as:



$$M_a = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

- The initial state $|\psi_0\rangle = 1 \cdot |0\rangle + 0 \cdot |1\rangle = (1,0)^T$
- $M_{aa} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Hence, upon reading *aa*, *M*'s state is

  $|\psi\rangle = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = 0 \cdot |0\rangle + -1 \cdot |1\rangle$
- There are two distinct paths labelled *aa* from q_1 back to itself, and each has non-zero probability, the net probability of ending up in q_1 is 0.
- The automaton accepts a string of odd length with probability 0.5 and a string of even length with probability 1 if its length is not a multiple of 4 and probability 0 otherwise.

Measure-once Quantum Automata

- The accept state of the automaton is given by an $N \times N$ projection matrix P, so that, given a N-dimensional quantum state $|\psi\rangle$, the probability of $|\psi\rangle$ being in the accept state is $\langle\psi|P|\psi\rangle = \|P|\psi\rangle\|^2$. In the previous example, $P = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$
- The probability of the state machine accepting a given finite input string $\sigma = (\sigma_0, \sigma_1, \cdots, \sigma_k)$ is given by $Pr(\sigma) = \|PU_{\sigma_k} \cdots U_{\sigma_1} U_{\sigma_0} |\psi\rangle\|^2$. In the previous example, Pr(aa)= $\begin{pmatrix} 0 \\ -1 \end{pmatrix}^T \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ -1 \end{pmatrix} = 1$
- A regular language is accepted with probability p by a quantum finite automaton, if, for all sentences σ in the language, (and a given, fixed initial state $|\psi\rangle$), one has $p < Pr(\sigma)$.

Language Accepted

- Measure Many 1-way QFA: Measurement is performed after each input symbol is read.
- Measure-many model is more powerful than the measure-once model, where the power of a model refers to the acceptance capability of the corresponding automata.
- MM-1QFA can accept more languages than MO- 1QFA.
- Both of them accept proper subsets of regular languages.