Finite automata and formal languages (DIT322, TMV028)

Nils Anders Danielsson,
partly based on slides by Ana Bove

2020-01-20–21

Regular expressions

- Used in text editors:

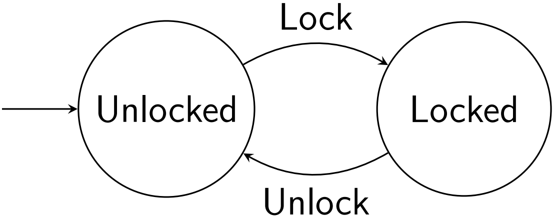
```
M-x replace-regexp RET
  add(\([^,]*\), \([^)]*\)) RET
  \1 + \2 RET
```

- Used to describe the lexical syntax of programming languages.
- Can only describe a limited class of "languages".

Finite automata

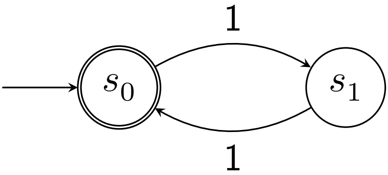
- Used to implement regular expression matching.
- Used to specify or model systems.
  - One kind of finite automaton is used in the specification of TCP.
- Equivalent to regular expressions.

Finite automata



Finite automata

Accepts strings of ones of even length:



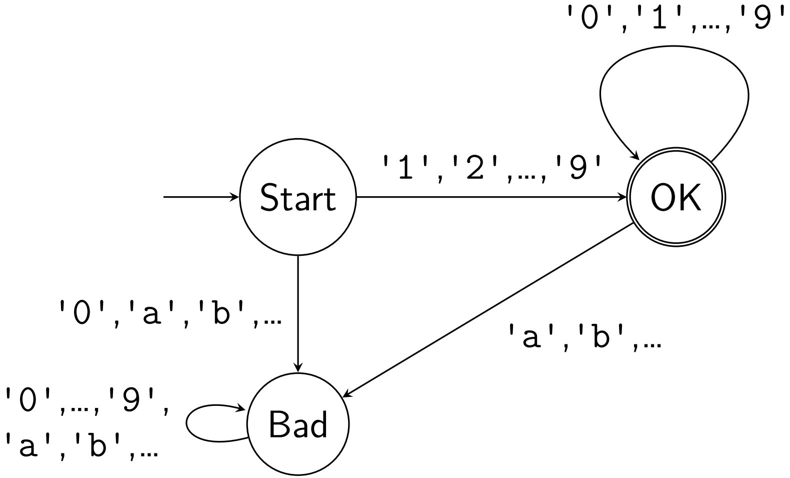
- The states are a kind of memory.
- Finite number of states $\Rightarrow$ finite memory.

Regular expressions

- A regular expression for strings of ones of even length: $(11)^*$.
- A regular expression for some keywords: $while \mid for \mid if \mid else$.
- A regular expression for positive natural number literals (of a certain form): $[1–9][0–9]^*$.

Finite automata

Accepts positive natural number literals:



Conversions

- We will see how to convert regular expressions to and from finite automata.
- In fact, we will discuss several kinds of finite automata, and conversions between the different kinds.

Context-free grammars

- More general than regular expressions.
- Used to describe the syntax of programming languages.
- Used by parser generators. (Often restricted.)

Context-free grammars

$$
\begin{aligned}
\mathit{Expr} &::= \mathit{Number} \\
&\quad\mid\ \mathit{Expr}\ \mathit{Op}\ \mathit{Expr} \\
&\quad\mid\ \texttt{'('}\ \mathit{Expr}\ \texttt{')'} \\
\mathit{Op} &::= \texttt{'+'} \mid \texttt{'-'} \mid \texttt{'*'} \mid \texttt{'/'}
\end{aligned}
$$

Turing machines

- A model of what it means to "compute":
  - Unbounded memory: an infinite tape of cells.
  - A read/write head that can move along the tape.
  - A kind of finite state machine with rules for what the head should do.
- Equivalent to a number of other models of computation.

Proofs

- Used to make it more likely that arguments are correct.
- Used to make arguments more convincing.

Induction

- Regular induction for $\mathbb{N}$.
- Complete (strong, course of values) induction for $\mathbb{N}$.

Inductively defined sets

- An example:
  The natural numbers ($\mathbb{N} = \{ 0, 1, 2, ... \}$).
- Structural induction for
  inductively defined sets.

General information

See the course web pages.

Repetition (?) of some classical logic

Propositions

- A proposition is, roughly speaking, some statement that is true or false.
  - $2 = 3$.
  - The program `while true do {x := 4}` terminates.
  - $P = NP$.
  - If $P = NP$, then $2 = 3$.
- It may not always be known what the truth value ($\top$ or $\bot$) of a proposition is.

Some logical connectives

- And: $\wedge$.
- Or: $\vee$.
- Not: $\neg$.
- Implies: $\Rightarrow$.
- If and only if (iff): $\Leftrightarrow$.

Some logical connectives

Truth tables for these connectives:

p	q	$p \wedge q$	$p \vee q$	$\neg p$	$p \Rightarrow q$	$p \Leftrightarrow q$
$\top$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\top$

Note that $p \Rightarrow q$ is true if p is false.

Which of the following truth tables are correct for the proposition $(p \vee q) \Rightarrow p$?

A:

p	q	$(p \vee q) \Rightarrow p$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

B:

p	q	$(p \vee q) \Rightarrow p$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

C:

p	q	$(p \vee q) \Rightarrow p$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\top$

D:

p	q	$(p \vee q) \Rightarrow p$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

Respond at `https://pingo.coactum.de/536622`.

Validity

- A proposition is *valid*, or a *tautology*, if it is satisfied for all assignments of truth values to its variables.
- Examples:
  - $p \Rightarrow p$.
  - $p \vee \neg p$.

Logical equivalence

- Two propositions p and q are *logically equivalent* if they have the same truth tables, i.e. if $p \Leftrightarrow q$ is valid.
- Examples:
  - $\neg \neg p \quad \Leftrightarrow \quad p$.
  - $(p \Leftrightarrow q) \quad \Leftrightarrow \quad (p \Rightarrow q) \wedge (q \Rightarrow p)$.
  - $p \wedge q \quad \Leftrightarrow \quad q \wedge p$.
  - $p \wedge (q \vee r) \quad \Leftrightarrow \quad (p \wedge q) \vee (p \wedge r)$.
  - $p \wedge (p \vee q) \quad \Leftrightarrow \quad p$.

Which of the following propositions are valid?

1. $(p \Rightarrow q) \Leftrightarrow \neg p \vee q$.
2. $(p \Rightarrow q) \Leftrightarrow p \vee \neg q$.
3. $\neg(p \wedge q) \Leftrightarrow \neg p \wedge \neg q$.
4. $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$.
5. $((p \Rightarrow p) \Rightarrow q) \Rightarrow p$.
6. $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$.

Predicates

A predicate is, roughly speaking, a function to propositions.

- $P(n) =$ "n is a prime number".
- $Q(a, b) =$ "$(a + b)^2 = a^2 + 2ab + b^2$".

Quantifiers

Quantifiers:

- For all: $\forall$.
  - $\forall x.\ x = x$.
  - $\forall a, b \in \mathbb{R}.\ (a + b)^2 = a^2 + 2ab + b^2$.
- There exists: $\exists$.
  - $\exists n \in \mathbb{N}.\ n = 2n$.

Which of the following propositions, involving predicate variables, are valid?

1. $(\neg\forall n \in \mathbb{N}.\ P(n)) \Leftrightarrow (\forall n \in \mathbb{N}.\ \neg P(n))$.
2. $(\neg\forall n \in \mathbb{N}.\ P(n)) \Leftrightarrow (\exists n \in \mathbb{N}.\ \neg P(n))$.
3. $(\forall m \in \mathbb{N}.\ \exists n \in \mathbb{N}.\ P(m,n)) \Leftrightarrow$
   $(\exists n \in \mathbb{N}.\ \forall m \in \mathbb{N}.\ P(m,n))$.

Repetition (?) of some set theory

Sets

- A *set* is, roughly speaking, a collection of elements.
- Some notation for defining sets:
  - $\{ 0, 1, 2, 4, 8 \}$.
  - $\{ n \in \mathbb{N} \mid n > 2 \}$.
  - $\{ 2^n \mid n \in \mathbb{N} \}$.

Members, subsets

- Membership: $\in$.
  - $4 \in \{ 2^n \mid n \in \mathbb{N} \}$.
  - $2 \notin \{ n \in \mathbb{N} \mid n > 2 \}$.
- Two sets are equal if they have the same elements: $(A = B) \Leftrightarrow (\forall x.\ x \in A \Leftrightarrow x \in B)$.
- Subset relation:
  $(A \subseteq B) \Leftrightarrow (\forall x.\ x \in A \Rightarrow x \in B)$.
  - $\{ 2^n \mid n \in \mathbb{N} \} \subseteq \mathbb{N}$.
  - $\{ 0, 1, 2, 4, 8 \} \not\subseteq \{ n \in \mathbb{N} \mid n > 2 \}$.

An aside

- Unrestricted naive set theory can be inconsistent.
- Russell's paradox:
  - Define $S = \{ X \mid X \notin X \}$, where X ranges over all sets.
  - We have $S \in S \Leftrightarrow S \notin S$!?
  - One can fix this problem by imposing rules that ensure that S is not a set.

Set operations

- The empty set: $\emptyset$.
- Union: $A \cup B = \{ x \mid x \in A \vee x \in B \}$.
- Intersection: $A \cap B = \{ x \mid x \in A \wedge x \in B \}$.
- Cartesian product:
  $A \times B = \{ (x, y) \mid x \in A \wedge y \in B \}$.
- Set difference:
  $A \setminus B = A - B = \{ x \in A \mid x \notin B \}$.
- Complement: $\overline{A} = U \setminus A$
  (if U is fixed in advance and $A \subseteq U$).
- Power set: $\wp(S) = 2^S = \{ A \mid A \subseteq S \}$.

Which of the following propositions are valid? Variables range over sets. U is non-empty.

1. $\overline{A \cap B} = \overline{A} \cap \overline{B}$.
2. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
3. $\emptyset = \{ \emptyset \}$.
4. $A \in \wp(A)$.
5. $A \cup (B \cap C) = (A \cup B) \cap C$.
6. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Relations

- A binary relation R on A is a subset of $A^2 = A \times A$: $R \subseteq A^2$.
- Notation: xRy means the same as $(x, y) \in R$.
- Can be generalised from $A \times A$ to $A \times B \times C \times \cdots$.

Properties of binary relations

- Reflexive: $\forall x \in A.\ xRx$.
- Symmetric: $\forall x, y \in A.\ xRy \Rightarrow yRx$.
- Transitive: $\forall x, y, z \in A.\ xRy \wedge yRz \Rightarrow xRz$.
- Antisymmetric:
  $\forall x, y \in A.\ xRy \wedge yRx \Rightarrow x = y$.

Partial orders

A *partial order* is reflexive, antisymmetric and transitive.

- $\leq$ for $\mathbb{N}$.
- Not $<$.

Which of the following sets are partial orders on $\{ 0, 1 \}$?

1. $\{ (0,0) \}$.
2. $\{ (0,0), (1,1) \}$.
3. $\{ (0,0), (0,1), (1,1) \}$.
4. $\{ (0,0), (0,1), (1,0) \}$.

Equivalence relations

An *equivalence relation* is reflexive, symmetric and transitive.

- $\{ (n,n) \mid n \in \mathbb{N} \} \subseteq \mathbb{N}^2$.
- Not $\{ (n,n) \mid n \in \mathbb{N} \} \subseteq \mathbb{R}^2$.

Which of the following sets are equivalence relations on $\{ 0, 1 \}$?

1. $\{ (0, 0) \}$.
2. $\{ (0, 0), (1, 1) \}$.
3. $\{ (0, 0), (0, 1), (1, 0) \}$.
4. $\{ (0, 0), (0, 1), (1, 0), (1, 1) \}$.

Partitions

A partition of the set A is a set $P \subseteq \wp(A)$ satisfying the following properties:

- Every element is non-empty: $\forall B \in P.\ B \neq \emptyset$.
- The elements cover A: $\bigcup_{B \in P} B = A$.
- The elements are mutually disjoint: $\forall B, C \in P.\ B \neq C \;\Rightarrow\; B \cap C = \emptyset$.

Equivalence classes

- The equivalence classes of an equivalence relation R on A: $[x]_R = \{ y \in A \mid xRy \}$.
- Note that $\forall x, y \in A.\ [x]_R = [y]_R \Leftrightarrow xRy$.
- The equivalence classes $\{ [x]_R \mid x \in A \}$ partition A.
- The quotient set $A/R = \{ [x]_R \mid x \in A \}$.

Quotients

Some examples:

- $\mathbb{Z} = \mathbb{N}^2 / \sim_{\mathbb{Z}}$,
  where
  $(m_1, n_1) \sim_{\mathbb{Z}} (m_2, n_2) \Leftrightarrow m_1 + n_2 = m_2 + n_1$.
- $\mathbb{Q} = \{ (m, n) \mid m \in \mathbb{Z}, n \in \mathbb{N} \setminus \{ 0 \} \} / \sim_{\mathbb{Q}}$,
  where
  $(m_1, n_1) \sim_{\mathbb{Q}} (m_2, n_2) \Leftrightarrow m_1 n_2 = m_2 n_1$.

Which of the following propositions are true?

1. $[(2,5)]_{\sim_{\mathbb{Z}}} = [(0,3)]_{\sim_{\mathbb{Z}}}$.
2. $[(2,5)]_{\sim_{\mathbb{Z}}} = [(3,0)]_{\sim_{\mathbb{Z}}}$.
3. $[(2,5)]_{\sim_{\mathbb{Q}}} = [(4,10)]_{\sim_{\mathbb{Q}}}$.
4. $[(2,5)]_{\sim_{\mathbb{Q}}} = [(10,4)]_{\sim_{\mathbb{Q}}}$.

More properties of relations

For $R \subseteq A \times B$:

- Total (left-total): $\forall x \in A.\ \exists y \in B.\ xRy$.
- Functional/deterministic:
  $\forall x \in A.\ \forall y, z \in B.\ xRy \wedge xRz \Rightarrow y = z$.

Functions

- The set of *functions* from the set A to the set B is denoted by $A \to B$.
- It is sometimes defined as the set of total and functional relations $f \subseteq A \times B$.
- Notation: $f(x) = y$ means $(x, y) \in f$.
- If the requirement of totality is dropped, then we get the set of *partial* functions, $A \rightharpoonup B$.
- The *domain* is A, and the *codomain* B.
- The *image* is $\{\, y \in B \mid x \in A, f(x) = y \,\}$.

Which of the following relations on $\{ a, b \}$ are functions?

1. $\{ \}$.
2. $\{ (a, a) \}$.
3. $\{ (a, a), (a, b) \}$.
4. $\{ (a, a), (b, a) \}$.
5. $\{ (a, a), (b, a), (b, b) \}$.

Identity, composition

- The *identity function* id on a set A is defined by $id(x) = x$.
- For functions $f \in B \rightarrow C$ and $g \in A \rightarrow B$ the *composition* $f \circ g \in A \rightarrow C$ is defined by $(f \circ g)(x) = f(g(x))$.

Injections

The function $f \in A \to B$ is *injective* if $\forall x, y \in A.\ f(x) = f(y) \Rightarrow x = y$.

- Every input is mapped to a unique output.
- Means that A is "no larger than" B.
- Holds if f has a left inverse $g \in B \to A$: $g \circ f = id$.

Surjections

The function $f \in A \to B$ is *surjective* if $\forall y \in B.\ \exists x \in A.\ f(x) = y$.

- The function "targets" every element in the codomain.
- Means that A is "no smaller than" B.
- Holds if f has a right inverse $g \in B \to A$: $f \circ g = id$.

Bijections

The function $f \in A \to B$ is *bijective* if it is both injective and surjective.

- Means that A and B have the same “size”.
- Holds if and only if f has a left and right inverse $g \in B \to A$.

Which of the following functions are injective? Surjective?

- $f \in \mathbb{N} \rightarrow \mathbb{N}$, $f(n) = n + 1$.
- $g \in \mathbb{Z} \rightarrow \mathbb{Z}$, $g(i) = i + 1$.
- $h \in \mathbb{N} \rightarrow Bool$, $h(n) = \begin{cases} true, & \text{if } n \text{ is even,} \\ false, & \text{otherwise.} \end{cases}$

The pigeonhole principle

- If there are n pigeonholes, and $m > n$ pigeons in these pigeonholes, then at least one pigeonhole must contain more than one pigeon.
- If $f \in \{ k \in \mathbb{N} \mid k < m \} \to \{ k \in \mathbb{N} \mid k < n \}$ for $m, n \in \mathbb{N}$, and $m > n$, then f is not injective.

Next lecture

- Proofs.
- Induction for the natural numbers.
- Inductively defined sets.
- Recursive functions.

Deadline for the first quiz: 2020-01-23, 10:00.