Finite Automata Theory and Formal Languages

TMV027/DIT321– LP4 2017

Lecture 2
Ana Bove

March 21st 2017

Overview of today's lecture:

- Logic;
- Sets;
- Relations;
- Functions.

Propositional Logic

Definition: A *proposition* is an statement which is either *true* (T) or *false* (F).

Example: My name is Ana.

I come from Uruguay.

I have 3 children.

I can speak 4 different languages.

It is not always known what the *truth value* of a proposition is.

Goldbach's conjecture: Every even integer greater than 2 can be expressed as the sum of two primes.

Connective and Truth Tables

We can combine propositions by using *connectives*:

- $\neg$: negation, not
- $\wedge$: conjunction, and
- $\vee$: disjunction, or
- $\Rightarrow$: conditional, if-then, $\rightarrow$
- $\Leftrightarrow$: equivalence, if-and-only-if, $\leftrightarrow$

These are their *truth tables* (observe the conditional...):

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

Conditionals

Example: Is the following statement true?

If I come from Mars then my skin is green.

Recall truth table for conditional:

I come from Mars	my skin is green	I come from Mars $\Rightarrow$ my skin is green
T	T	T
T	F	F
F	T	T
F	F	T

I am NOT from Mars!

So the whole proposition is true!

Combined Propositions

Example: Is the following statement true?

> *Either you study and you will pass the exam, or your won't pass the exam.*

Let us construct the truth table!

Let p be "you study".
Let q be "you will pass the exam".

Then the sentence is expressed by $(p \wedge q) \vee \neg q$.

p	q	$p \wedge q$	$\neg q$	$(p \wedge q) \vee \neg q$
T	T	T	F	T
T	F	F	T	T
F	T	F	F	F
F	F	F	T	T

Tautologies and Logical Equivalence

Definition: A proposition that is always true is called a *tautology*.

Example: The *law of the excluded middle* is a tautology in classical logic

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

Definition: Two propositions are *logically equivalent* ($\equiv$) if they have the same truth table.

Example: $p \Rightarrow q \equiv \neg p \vee q$:

p	q	$p \Rightarrow q$	$\neg p$	$\neg p \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Laws of (Classical) Logic

Equivalence:	$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$	
Implication:	$p \Rightarrow q \equiv \neg p \vee q$	
Double negation:	$\neg\neg p \equiv p$	
Idempotent:	$p \wedge p \equiv p$	$p \vee p \equiv p$
Commutative:	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative:	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	
	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	
Distributive:	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	
	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	
de Morgan:	$\neg(p \wedge q) \equiv \neg p \vee \neg q$	$\neg(p \vee q) \equiv \neg p \wedge \neg q$
Identity:	$p \wedge T \equiv p$	$p \vee F \equiv p$
Annihilation:	$p \wedge F \equiv F$	$p \vee T \equiv T$
Inverse:	$p \wedge \neg p \equiv F$	$p \vee \neg p \equiv T$
Absorption:	$p \wedge (p \vee q) \equiv p$	$p \vee (p \wedge q) \equiv p$

Exercise: Construct the truth tables and check the logical equivalences!

Statements with Variables

By using variables we could talk about any element in a certain domain.

Example: Consider the following property for $x \in \mathbb{N}$ (Natural numbers):

$$x > 4 \Rightarrow x > 2$$

When statements have variables we are actually working on *predicate logic*.

Reasoning in predicate logic is more complicated since variables can range over an infinite set of values.

Predicate Logic

Definition: A *predicate* is a statement with one or more variables.

When we assign values to all variable in a predicate we get a proposition.

Definition: The expressions *for all* ($\forall$) and *exists* ($\exists$) are called *quantifiers*.

Example: Express the following 2 statements in predicate logic:

- For every number x there is a number y such that x is equal to y
  $\forall x.\exists y.x = y$
- There is a number x such that for every number y then x is equal to y
  $\exists x.\forall y.x = y$

Are they the same statement?

More Laws of (Classical) Logic

We have that

$$\neg\forall x.P(x) \equiv \exists x.\neg P(x)$$

and

$$\neg\exists x.P(x) \equiv \forall x.\neg P(x)$$

Sets

Definition: A *set* is a collection of well defined and distinct objects or elements.

A set might be finite or infinite.

Sets can be described/defined in different ways:

Enumeration: mainly finite sets, sometimes with help of ...

WeekDays = {Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday}

OddNat $= \{1, 3, 5, 7, \dots\}$

Characteristic Property: OddNat $= \{x \in \mathbb{N} \mid x \text{ is odd}\}$.

Operations on Other Sets: $A \cup B$, $A \cap B$, ... (see slide 12)

Inductive Definitions: More on this next lecture ...

⋮

Membership on Sets

Definition: We denote that x is an *element* of set A by $x \in A$.

It is important to determine whether $x \in A$ or $x \notin A$.
However this is not always possible.

Example: Let P be the set of programs that always terminate.

Can we always be sure if a certain program $pgr \in P$?

Russell's paradox: Let $R = \{x \mid x \notin x\}$.

Then $R \in R \Leftrightarrow R \notin R$!

Some Operations and Properties on Sets

Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

Cartesian Product: $A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$.
Observe this is a collection of ordered pairs! $(x, y) \neq (y, x)$.

Difference: $S - A = \{x \mid x \in S \text{ and } x \notin A\}$.

Complement: When the set S is known, $S - A$ is written $\overline{A}$.
$S - A$ is sometimes denoted $S \backslash A$ and $\overline{A}$ is sometimes denoted A'.

Subset: $A \subseteq B$ if for all $x \in A$ then $x \in B$.

Equality: $A = B$ if $A \subseteq B$ and $B \subseteq A$.

Proper Subset: $A \subset B$ if $A \subseteq B$ and $A \neq B$.

Some Particular Sets

Empty set: $\emptyset$ is the set with no elements.
We have $\emptyset \subseteq S$ for any set S.

Singleton sets: Sets with only one element: $\{p_0\}$, $\{p_1\}$.

Finite sets: Set with a finite number n of elements:
$\{p_1, \ldots, p_n\} = \{p_1\} \cup \ldots \cup \{p_n\}$.

Power sets: $\mathcal{P}ow(S)$ the set of all subsets of the set S.
$\mathcal{P}ow(S) = \{A \mid A \subseteq S\}$.

Observe that $\emptyset \in \mathcal{P}ow(S)$ and $S \in \mathcal{P}ow(S)$.
Also, if $|S| = n$ then $|\mathcal{P}ow(S)| = 2^n$.

Note: $\emptyset \neq \{\emptyset\}$!!

Algebraic Laws for Sets

Idempotent:	$A \cup A = A$		$A \cap A = A$
Commutative:	$A \cup B = B \cup A$		$A \cap B = B \cap A$
Associative:	$(A \cup B) \cup C = A \cup (B \cup C)$		
	$(A \cap B) \cap C = A \cap (B \cap C)$		
Distributive:	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$		
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$		
de Morgan:	$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$		$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$
Laws for $\emptyset$:	$A \cup \emptyset = A$		$A \cap \emptyset = \emptyset$
Laws for Universe:	$A \cup U = U$		$A \cap U = A$
Complements:	$\overline{\overline{A}} = A$	$A \cup \overline{A} = U$	$A \cap \overline{A} = \emptyset$
	$\overline{U} = \emptyset$	$\overline{\emptyset} = U$	
Absorption:	$A \cup (A \cap B) = A$		$A \cap (A \cup B) = A$

Exercise: Prove the equality of the sets by showing the double inclusion!

Relations

Definition: A (binary) *relation* R between two sets A and B is a subset of $A \times B$, that is, $R \subseteq A \times B$.

Notation: $(a, b) \in R$, $a\, R\, b$, $R(a, b)$, (a, b) satisfies R.

Definition: A relation R over a set S, that is $R \subseteq S \times S$, is

- Reflexive if $\forall a \in S.\ a\, R\, a$;
- Symmetric if $\forall a, b \in S.\ a\, R\, b \Rightarrow b\, R\, a$;
- Transitive if $\forall a, b, c \in S.\ a\, R\, b \wedge b\, R\, c \Rightarrow a\, R\, c$.

Definition: If S has an equality relation $= \subseteq S \times S$ and $R \subseteq S \times S$ then R is antisymmetric if $\forall a, b \in S.\ a\, R\, b \wedge b\, R\, a \Rightarrow a = b$.

Example of Relations

Let $S = \{1, 2, 3\}$ and let $= \subseteq S \times S$ be as expected.
Which of these relations are reflexive, symmetric, antisymmetric, and/or transitive?

Play at `kahoot.it`!

- $R_1 = \emptyset$ — *Symmetric, Antisymmetric, Transitive*
- $R_2 = \{(1, 2)\}$ — *Antisymmetric, Transitive*
- $R_3 = \{(1, 2), (2, 3)\}$ — *Antisymmetric*
- $R_4 = \{(1, 2), (2, 3), (1, 3)\}$ — *Antisymmetric, Transitive*
- $R_5 = \{(1, 2), (2, 1)\}$ — *Symmetric*
- $R_6 = \{(1, 2), (2, 1), (1, 1)\}$ — *Symmetric*
- $R_7 = \{(1, 2), (2, 1), (1, 1), (2, 2)\}$ — *Symmetric, Transitive*
- $R_8 = \{(1, 2), (2, 1), (1, 1), (2, 2), (3, 3)\}$ — *Reflexive, Symm, Trans*

Equivalent Relations and Orders

Definition: A relation R over a set S that is *reflexive, symmetric* and *transitive* is called an *equivalence relation* over S.

Example: $=$ is an equivalence over $\mathbb{N}$.

Definition: A relation R over a set S that is reflexive, antisymmetric and transitive is called a *partial order* over S.

Example: $\leqslant$ is a partial order over $\mathbb{N}$ but and $<$ not!

Definition: A relation R over a set S is called a *total order* over S if:

- R is a partial order;
- $\forall a, b \in S.\ a\,R\,b \vee b\,R\,a$.

Example: $\leqslant$ is a total order over $\mathbb{N}$.

Partitions

Definition: A set P is a *partition* over the set S if:

- Every element of P is a non-empty subset of S

$$\forall C \in P.\ C \neq \emptyset \wedge C \subseteq S;$$

- Elements of P are pairwise disjoint

$$\forall C_1, C_2 \in P.\ C_1 \neq C_2 \Rightarrow C_1 \cap C_2 = \emptyset;$$

- The union of the elements of P is equal to S

$$\bigcup_{C \in P} C = S.$$

Equivalent Classes

Let R be an equivalent relation over S.

Definition: If $a \in S$, then the *equivalent class* of a in S is the set defined as $[a] = \{b \in S \mid a\,R\,b\}$.

Lemma: $\forall a, b \in S,\ [a] = [b]$ *iff* $a\,R\,b$.

Theorem: *The set of all equivalence classes in S w.r.t. R form the quotient partition over S.*

Notation: This partition is denoted as S/R.

Example: The rational numbers $\mathbb{Q}$ can be formally defined as the equivalence classes of the quotient set $\mathbb{Z} \times \mathbb{Z}^+/\sim$, where $\sim$ is the equivalence relation defined by $(m_1, n_1) \sim (m_2, n_2)$ iff $m_1 n_2 =_{\mathbb{Z}} m_2 n_1$.

Functions

Definition: A *function* f from A to B is a relation $f \subseteq A \times B$ such that, given $x \in A$ and $y, z \in B$, if $x\,f\,y$ and $x\,f\,z$ then $y = z$.

Notation: If f is a function from A to B we write $f : A \to B$.

Notation: That $x\,f\,y$ is usually written as $f(x) = y$.

Example: $\mathrm{sq} : \mathbb{Z} \to \mathbb{N}$ such that $\mathrm{sq}(n) = n^2$.

Observe that $\mathrm{sq}(2) = 4$ and $\mathrm{sq}(-2) = 4$.

Domain, Codomain, Range and Image

Let $f : A \to B$.

Definition: The sets A and B are called the *domain* and the *codomain* of the function, respectively.

Definition: The set $\mathrm{Dom}(f)$ or Dom_f for which the *function is defined* is given by $\{x \in A \mid \exists y \in B . f(x) = y\} \subseteq A$.

We will also refer to $\mathrm{Dom}(f)$ as the domain of f.

Definition: The set $\{y \in B \mid \exists x \in A . f(x) = y\} \subseteq B$ is called the *range* or *image* of f and denoted $\mathrm{Im}(f)$ or Im_f.

Example: The image of sq is NOT all $\mathbb{N}$ but $\{0, 1, 4, 9, 16, 25, 36, \ldots\}$.

Total and Partial Functions

Let $f : A \to B$.

Definition: If $\text{Dom}(f) = A$ then f is called a *total* function.

Example: sq is a total function.

Definition: If $\text{Dom}(f) \subset A$ then f is called a *partial* function.

Example: $\text{sqr} : \mathbb{N} \to \mathbb{N}$ such that $\text{sqr}(n) = \sqrt{n}$ is a partial function.

Note: In some cases it is not known if a function is partial or total.

Example: It is not known if $\text{collatz} : \mathbb{N} \to \mathbb{N}$ is total or not.

$$\text{collatz}(0) = 1 \qquad \text{collatz}(1) = 1 \qquad \text{collatz}(n) = \begin{cases} \text{collatz}(n/2) & \text{if } n \text{ even} \\ \text{collatz}(3n+1) & \text{if } n \text{ odd} \end{cases}$$

Injective or One-to-one Functions

Let $f : A \to B$.

Definition: f is called an *injective* or *one-to-one* function if $\forall x, y \in A. f(x) = f(y) \Rightarrow x = y$.

Alternatively:

Definition: f is called an *injective* or *one-to-one* function if $\forall x, y \in A. x \neq y \Rightarrow f(x) \neq f(y)$.

Exercise: Prove that $\text{double} : \mathbb{N} \to \mathbb{N}$ such that $\text{double}(n) = 2n$ is injective.

The Pigeonhole Principle

"If you have more pigeons than pigeonholes and each pigeon flies into some pigeonhole, then there must be at least one hole with more than one pigeon."

More formally: if $f : A \to B$ and $|\text{Dom}_f(A)| > |B|$ then f cannot be *injective*.
That is, there must exist $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

This principle is often used to show the existence of an object without building this object explicitly.

Example: In a room with at least 13 people, at least 2 of them are born the same month.

Surjective or Onto Functions

Let $f : A \to B$.

Definition: f is called an *surjective* or *onto* function if $\forall y \in B. \exists x \in A. f(x) = y$.

Note: If f is surjective then $\text{Im}(f) = B$.

Exercise: Prove that $\text{f} : \mathbb{R} \to \mathbb{R}$ such that $\text{f}(n) = 2n + 1$ is surjective.

Bijective and Inverse Functions

Definition: A function that is both injective and surjective is called a *bijective* function.

Definition: If $f : A \to B$ is a bijective function, then there exists an *inverse* function $f^{-1} : B \to A$ such that $\forall x \in A.f^{-1}(f(x)) = x$ and $\forall y \in B.f(f^{-1}(y)) = y$.

Exercise: Is $\mathrm{g} : \mathbb{Z} \to \mathbb{Z}$ such that $\mathrm{g}(n) = 2n + 1$ bijective?

Exercise: Which is the inverse of $\mathrm{f} : \mathbb{R} \to \mathbb{R}$ such that $\mathrm{f}(n) = 2n + 1$?

Lemma: *If $f : A \to B$ is a bijective function, then $f^{-1} : B \to \mathrm{Dom}_f(A)$ is also bijective.*

Composition and Restriction

Definition: Let $f : A \to B$ and $g : B \to C$. The *composition* $g \circ f : A \to C$ is defined as $g \circ f(x) = g(f(x))$.

Note: We need that $\mathrm{Im}(f) \subseteq \mathrm{Dom}(g)$ for the composition to be defined.

Example: If $\mathrm{f} : \mathbb{Z} \to \mathbb{Z}$ is such that $\mathrm{f}(n) = 3n - 2$ and $\mathrm{g} : \mathbb{R} \to \mathbb{R}$ is such that $\mathrm{g}(m) = m/2$, then $\mathrm{g} \circ \mathrm{f} : \mathbb{Z} \to \mathbb{R}$ is $\mathrm{g} \circ \mathrm{f}(x) = (3x - 2)/2$.

Definition: Let $f : A \to B$ and $S \subset A$. The *restriction* of f to S is the function $f_{|S} : S \to B$ such that $f_{|S}(x) = f(x), \forall x \in S$.

Overview of Next Lecture

Sections 1.2–1.4 in the main book and chapters 1 and 5 in the *Mathematics for Computer Science* book:

- Formal Proofs;
- Simple/Strong Induction;
- Mutual induction;
- Inductively defined sets;
- Recursively defined functions.

See even Koen Claessen's notes on proof methods (see course web page on Literature).

DO NOT MISS THIS LECTURE!!!