IN3070/4070 – Logic – Autumn 2020

Lecture 1: Introduction

Martin Giese

20th August 2020

Department of
Informatics

University of
Oslo

Today's Plan

- What is Logic?
- Logic in Computer Science
- Three Ingredients
- Applications
- Course Information

Outline

- What is Logic?
- Logic in Computer Science
- Three Ingredients
- Applications
- Course Information

What is Logic?

Wikipedia

Logic (from the Ancient Greek: $\lambda o\gamma\iota\kappa\acute{\eta}$) is the systematic study of the form of valid inference, and the most general laws of truth.

Richard Smullyan

"To make precise the notion of a proof."

Bertrand Russell

"The subject in which nobody knows what one is talking about, nor whether what one is saying is true."

Confusing. . . let's be computer scientists and compute something!

Computation

- What is computation?

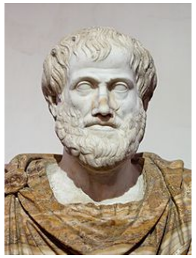
$$\begin{array}{c} A \text{ owns } x\ B\text{s} \\ A \text{ gets another } y\ B\text{s} \\ \hline A \text{ now owns } (x+y)\ B\text{s} \end{array}$$

e.g.

$$\begin{array}{c} \text{Peter owns 1 apple} \\ \text{Peter gets another 4 apples} \\ \hline \text{Peter now owns 5 apples} \end{array}$$

- Computation is algorithmic manipulation of numbers...
- ...where the *meaning* of the numbers is not needed
- Can compute $1 + 4 = 5$ without knowing what is counted
- Abstraction!

Computation with Knowledge



- Can be traced back to Aristotle (384–322 BC)
- Modus Barbara:

$$\begin{array}{c} \text{All } A \text{ are } B \\ \text{All } B \text{ are } C \\ \hline \text{All } A \text{ are } C \end{array}$$

e.g.

$$\begin{array}{c} \text{All Greeks are men} \\ \text{All men are mortal} \\ \hline \text{All Greeks are mortal} \end{array}$$

- Algorithmic manipulation of *knowledge*...
- ...where the *meaning* of the words is not needed!
- Also an abstraction!

Logic as an abstraction

Logic as an abstraction

Logic is the subject that investigates *valid reasoning* while abstracting away from what is being reasoned about.

So Russell was right after all:

- Nobody knows what one is talking about... (A? B? C?)
- ...nor what one is saying is true (what does “Greek” mean?)

And that is great, because it means that:

Computers can do this!

Sure, cool, but why bother?

Outline

- What is Logic?
- Logic in Computer Science
- Three Ingredients
- Applications
- Course Information

Models

- A *model* is a simplified representation of certain aspects of the real world.
    - Also an abstraction
- Made for
    - understanding
    - structuring
    - predicting
    - communicating

- Can be
    - Taxonomies (e.g. species, genus, family, etc. in biology)
    - Domain models, e.g. in UML
    - Numerical Models (Newtonian mechanics, Quantum mechanics)

Models in Computer Science

Models can be

- used to construct (parts of) software
    - Generate classes from UML diagrams
    - Generate code from UML sequence diagrams or state charts
- executed directly (sometimes)
    - Maude programs
    - Prolog programs
    - Models driving simulations
- used to check data
    - Database constraints = information model
    - XSD file = document model

So you also want algorithms to

- Check various properties of models
- Check consistency between models
- Transform models from one language to another
- Check that programs conform to models (verification)
- ...

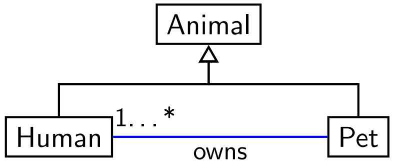
What is a Good Modelling Language

For a model that can be used by a computer...

- there has to be a 'language'
    - language says what is a model and what not
    - programs (and humans...) need to know what to expect
    - often defined by some grammar
    - UML, ER, ORM, OWL, SQL, Java, etc. are all languages
- the meaning of models should be very clear
    - otherwise, different implementations do different things
    - sometimes, 100s of pages of technical text (e.g. JLS)
    - sometimes meaning given by mathematical definitions

Models and Statements

Observation: much of the content of many models can be given as statements:



- Every Human is an Animal.
- Every Pet is an Animal.
- Every Pet is owned by at least one Human.
- Everybody owning a Pet is a Human (?)

Modeling with Logic

- Logical languages are made for expressing statements
  - They are more general than most other modeling languages
- Logical languages have a precise (mathematical) meaning
  - Implementation-independent by design
- Many things we do with models can be understood in terms of logical consequence

E.g.

- $\forall x.Human(x) \rightarrow Animal(x)$
- $\forall x.Pet(x) \rightarrow Animal(x)$
- $\forall x.Pet(x) \rightarrow \exists y.(Human(y) \land owns(y,x))$
- $\forall x,y.((Pet(x) \land owns(y,x)) \rightarrow Human(y))$

Logics are a very expressive and precise
family of modelling languages

Outline

- What is Logic?
- Logic in Computer Science
- Three Ingredients
- Applications
- Course Information

Three Central Ingredients

- Syntax (i.e. the language)
- Semantics (i.e. the meaning)
- Calculus (i.e. method, algorithm, usually rules)

Syntax

Most logics have some kind of *formulas*.
The syntax says which strings of characters are formulas.

Syntax of Propositional Formulae

Propositional formulas are defined inductively as follows

- Every lower case letter (p, q, r,...) is a formula
- If A and B are formulae, then $\neg A$, $(A \land B)$, $(A \lor B)$ and $(A \rightarrow B)$ are formulae.

Inductively defined (remember IN1150): only what can be constructed using these rules is a formula.

$$p, \quad (p \land \neg p), \quad (p \rightarrow q) \lor (q \rightarrow p), \ldots$$

But not: $((p, \quad \neg \rightarrow q, \ldots$

Model Semantics

We usually define some kind of *interpretation* or *model* or *structure*… Always the same idea:

- We don't know what we talk about (p, q, r, x, y, z)
- We don't know what is true (p or $\neg q$?)
- So we use a mathematical object that tells us what they mean and what is true or not

Interpretation

An interpretation is a function $\mathcal{I} : \mathit{Letters} \to \{T, F\}$ that assigns one of the truth values T or F to every lower case letter

---

Model Semantics (cont.)

Truth Value

The truth value of formulas $v_{\mathcal{I}}(A)$ is defined inductively by

- $v_{\mathcal{I}}(A) = \mathcal{I}(A)$ for letters A
- $v_{\mathcal{I}}(\neg A) = T$ if $v_{\mathcal{I}}(A) = F$ and
  $v_{\mathcal{I}}(\neg A) = F$ if $v_{\mathcal{I}}(A) = T$
- $v_{\mathcal{I}}(A \land B) = T$ if $v_{\mathcal{I}}(A) = T$ and $v_{\mathcal{I}}(B) = T$
  $v_{\mathcal{I}}(A \land B) = F$ otherwise
- …

Entailment

Formula A *entails* formula B ($A \models B$) if for every $\mathcal{I}$ with $v_{\mathcal{I}}(A) = T$ it also holds that $v_{\mathcal{I}}(B) = T$.

Model Semantics: Take Aways

Model Semantics defines the meaning of logical formulas…

- i.e. truth/falsity in some interpretation/model/…
- relations between formulas like entailment, equivalence…

…by *mathematical definitions*.

- We assume that maths, set theory, etc. "work"
- We assume that people can read formulas, understand words like "and" or "not" or "otherwise," look up truth values in tables, etc.
- The definitions can often not be implemented directly
  - E.g. loop over infinitely many interpretations in 1st order logic

---

Calculi

- A calculus works on formulas, i.e. *syntax*
- Usually by *inference rules* saying how to *derive* new formulas

$$\frac{A \to B \qquad A}{B}$$

- Always with some machinery that says how to use the rules
- Can be used to check entailment etc. between formulas
- Can be implemented on a computer

Natural Deduction for Propositional Logic

- rules for $\wedge$ (conjunction)

$$\frac{A \qquad B}{A \wedge B}\wedge\text{-I} \qquad\qquad \frac{A \wedge B}{A}\wedge\text{-E} \qquad\qquad \frac{A \wedge B}{B}\wedge\text{-E}$$

- rules for $\rightarrow$ (implication)

$$\frac{\begin{array}{c}[A]^n \\ \vdots \\ B\end{array}}{A \rightarrow B}\rightarrow\text{-I}^n \qquad\qquad \frac{A \rightarrow B \qquad A}{B}\rightarrow\text{-E}$$

Calculi: Take Aways

Calculi allow to determine

- *semantic properties* like equivalence, satisfiability etc.
- by *syntactic means*

. . . i.e. in ways that can be implemented

Semantics vs. Calculus

- Entailment ($A \models B$): semantic notion
- Derivability ($A \vdash B$): syntactic notion

Soundness

What can be derived is entailed

$$A \vdash B \implies A \models B$$

Completeness

What is entailed can be derived

$$A \models B \implies A \vdash B$$

Two central properties; we will study how to prove them

- for different logics
- for different calculi

Learn techniques to handle languages and their semantics

Logic without Semantics?

- Much of mathematical logic stems from attempts at a formal foundation of mathematics itself
- End of 19th, beginning og 20th century
- Try to use logic to build mathematics from the bottom up
- But without mathematics. . .
- . . . how do we define model semantics!?

Foundational mathematics considers logics without (model) semantics

- More focus on manipulating proofs
- Known as the ‘proof theoretic approach’
- We concentrate on ‘model theoretic approach’
- As computer scientists, we take maths for granted.
- Foundations are not (usually) our problem :-)

Outline

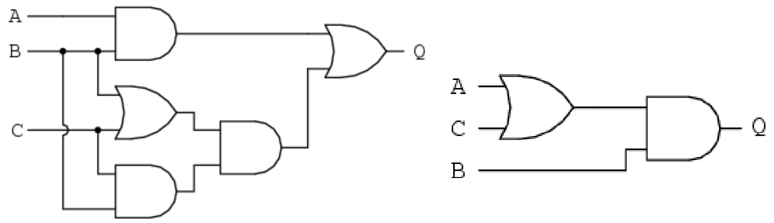
- What is Logic?
- Logic in Computer Science
- Three Ingredients
- Applications
- Course Information

SAT

- SAT-solving: given a propositional formula A, is there an interpretation $\mathcal{I}$ such that $v_{\mathcal{I}}(A) = T$?
- `https://en.wikipedia.org/wiki/Boolean_satisfiability_problem`
- NP-hard, i.e. takes time exponential in size of A
- Can often be done for very large problems, over 1M variables
- Will learn more about how in a later lecture
- See here for a talk about applications `http://www.carstensinz.de/talks/RISC-2005.pdf`

SAT applications: circuit verification

Are these two circuits the same?



$(A \land B) \lor ((B \lor C) \land (B \land C))$ vs. $(A \lor C) \land B$

Logically equivalent?

Today, theorem provers are routinely used to check Boolean circuits

---

SAT applications: program verification

- A 32 bit int can be encoded as 32 boolean variables
- If SAT can handle 1M boolean variables, it can handle thousands of 32 bit words.
- Properties of programs (without loops) can be handled by SAT solvers
- Experimental, but works in many cases

SAT applications: puzzle solving

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

- Use 4 bits to encode the number in each of the 81 squares ($\leq$ 324 bits)
- Add axioms that ensure each number 1–9 occurs in each square, each row, each column
- A satisfying interpretation is a solution of the puzzle

SAT: problems that require finding one of a large, fixed number of combinations, but checking is easy

---

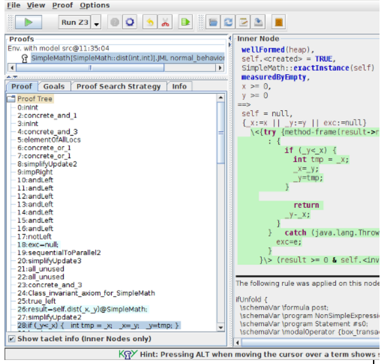
First-order logic

- $\forall x \forall y \exists z (p(x, y) \to p(x, z) \wedge p(z, y))$
- Undecidable in general
- More 'brittle' than SAT: small changes in formulation can make a big difference for a prover
- Therefore fewer 'industrial' applications
- Can be used to formalise parts of mathematics (algebra)
- Add induction to reason about numbers and datatypes
- First-order theorem provers have been used to prove difficult open problems in (unintuitive parts of) mathematics
- In combination with other techniques, first-order logic can used to reason about programs

---

The KeY tool

- `https://www.key-project.org/`
- Verify behaviour of Java programs
- Based on 1st-order logic
- Extended with program operators
  - $\langle Prog \rangle\, p$
    Prog terminates and p holds afterwards
- Based on a Sequent Calclus



Env. with model src@11:35:04
SimpleMath[SimpleMath::dist(int,int)].JML normal_behavior

```
0:inInt
2:concrete_and_1
3:inInt
4:concrete_and_3
5:elementOfAllLocs
6:concrete_or_1
7:concrete_or_1
8:simplifyUpdate2
9:impRight
10:andLeft
11:andLeft
12:andLeft
13:andLeft
14:andLeft
15:andLeft
16:andLeft
17:notLeft
18:exc=null;
19:sequentialToParallel2
20:simplifyUpdate3
21:all_unused
22:all_unused
23:concrete_and_3
24:Class_invariant_axiom_for_SimpleMath
25:true_left
26:result=self.dist(_x,_y)@SimpleMath;
27:simplifyUpdate2
28:if (_y<_x) {   int tmp = _x;   _x=_y;   _y=tmp; }
```

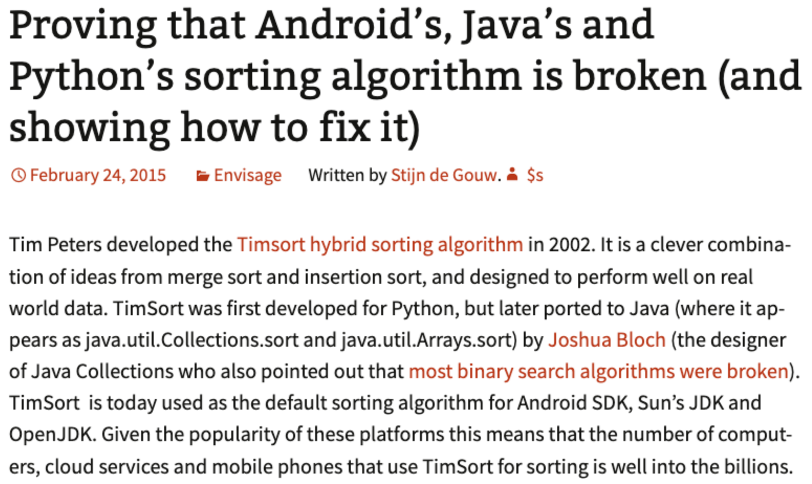
```
wellFormed(heap),
self.<created> = TRUE,
SimpleMath::exactInstance(self)
measuredByEmpty,
x >= 0,
y >= 0
==>
self = null,
{_x:=x || _y:=y || exc:=null}
  \<{try {method-frame(result->r
      : {
          if (_y<_x) {
            int tmp = _x;
            _x=_y;
            _y=tmp;
          }

            return
          _y-_x;
        }
      }   catch (java.lang.Throw
        exc=e;
      }
    }\> (result >= 0 & self.<inv
```

The following rule was applied on this node

```
ifUnfold {
  \schemaVar \formula post;
  \schemaVar \program NonSimpleExpressi
  \schemaVar \program Statement #s0;
  \schemaVar \modalOperator {box_transa
```

Hint: Pressing ALT when moving the cursor over a term shows

The TimSort bug



Proving that Android's, Java's and Python's sorting algorithm is broken (and showing how to fix it)

February 24, 2015 Envisage Written by Stijn de Gouw. $s

Tim Peters developed the Timsort hybrid sorting algorithm in 2002. It is a clever combination of ideas from merge sort and insertion sort, and designed to perform well on real world data. TimSort was first developed for Python, but later ported to Java (where it appears as java.util.Collections.sort and java.util.Arrays.sort) by Joshua Bloch (the designer of Java Collections who also pointed out that most binary search algorithms were broken). TimSort is today used as the default sorting algorithm for Android SDK, Sun's JDK and OpenJDK. Given the popularity of these platforms this means that the number of computers, cloud services and mobile phones that use TimSort for sorting is well into the billions.

`http://www.envisage-project.eu/proving-android-java-and-python-sorting-algorithm-is-broken-and-how-to-fix-it/`

The World In Between

- Many logics are stronger than propositional logic, but still decidable.
- Often efficiently in practice
- E.g. Description Logics
  - “A ProudMother is a Person who is Female and has at least one child who is a Professor”
  - $\mathsf{ProudMother} \equiv \mathsf{Person} \sqcap \mathsf{Female} \sqcap \exists\, \mathsf{hasChild.Professor}$
  - Can define and reason about terminologies of up to 100.000s of concepts
  - Applications in semantic web, data integration,. . .
- E.g. Temporal Logic
  - “Every request is eventually followed by an acknowledgement”
  - $\Box(Req \to \Diamond Ack)$
  - Can check properties of systems with hundreds of variables
  - Applications in dynamic circuit verification etc.
- Knowledge logics, probabilistic logics, alternating logics, belief logics, . . .

Outline

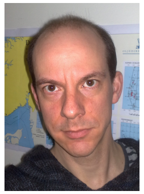
- What is Logic?
- Logic in Computer Science
- Three Ingredients
- Applications
- Course Information

When, Where, and Who

When and Where

- Lectures
  - Tuesdays 10:15–12:00 in OJD 2458, Postscript and/or
  - **Thursdays 10:15–12:00 in KN Store Aud**
  - **When fewer students, move to OJD 3438, Caml**
- Homepage: `https://www.uio.no/studier/emner/matnat/ifi/IN3070/index-eng.html`

Lecturer



Martin Giese (`martingi@ifi.uio.no`)

Exercises

Exercises

- Practical exercises every week,
- Thursdays 12:15–14:00 in OJD 3468 Fortress, from **27 August** and
- **Tuesdays 10:15–12:00 in OJD 2458, Postscript, from 1 Sept.**
- Exercises available on website well in advance. Come prepared!
- In general: part repetition of lectures, part exercises

Teacher

Ida Sandberg Motzfeldt
(`idasmot@ifi.uio.no`)

Mandatory Assignments

Assignments

- Two mandatory assignments (obliger)
- Will be in October/November
- Corrected by teacher.
- Pass/Fail
- Must have passed all assignments in order to attend exam
- For IN4070 (MSc version): one extra question in each oblig

Prover Hacking – Competition?

- One of your assignments will be to program a simple prover.
- Doesn't need to be very powerful to get 'pass.'
- But hacking is fun, right?
- May organise a little prover competition at the end of the semester.
- Strictly for fun, no influence on grade.

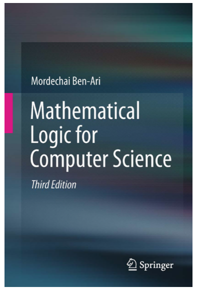
Padlet

`https://uio.padlet.org/martingi/8swc2uezt4sy2nsk`

Exam

- Four hours written home exam
  - In case of few students, might be oral exam instead
- Same exam for IN3070 and IN4070
- Grades A–F
- Probably 4 December – Check semester page!
- Unsure, due to Corona

Textbook



Mordechai Ben-Ari

Mathematical Logic for Computer Science

Third Edition

Springer

- Mordechai Ben-Ari
  Mathematical Logic for Computer Science
  3rd edition, Springer, 2012.
- only chapters 1–4 and 6–12;
  not part of the curriculum:
  chapter 5 (binary decision diagrams) and
  chapters 13–16 (temporal logic, verification of programs)
- download for free (within the UiO network) from Springer's website at `http://www.springer.com/gp/book/9781447141280`

Next weeks. . .

- Propositional Logic
- Tableaux/Sequent calculi for propositional Logic
- Soundness and Completeness
- Resolution calculus for propositional Logic
- Soundness and Completeness
- First-order logic
- Tableaux/Sequent calculi and resolution for 1st order logic
- Soundness and Completeness for those calculi