Comp 330 - Theory of Computation

Lecture 1 - Fall 2023

Claude Crépeau, Cesare Spinoso-Di Piano

August 31st 2023

McGill University - School of Computer Science

Plan for today

1. Course objective
2. Course outline
3. Maths review

Course objective

What is this course about?

Single sentence summary: To investigate the inherent limits of computation.

Entscheidungsproblem

Is the following mathematical statement S true?

(a) David Hilbert

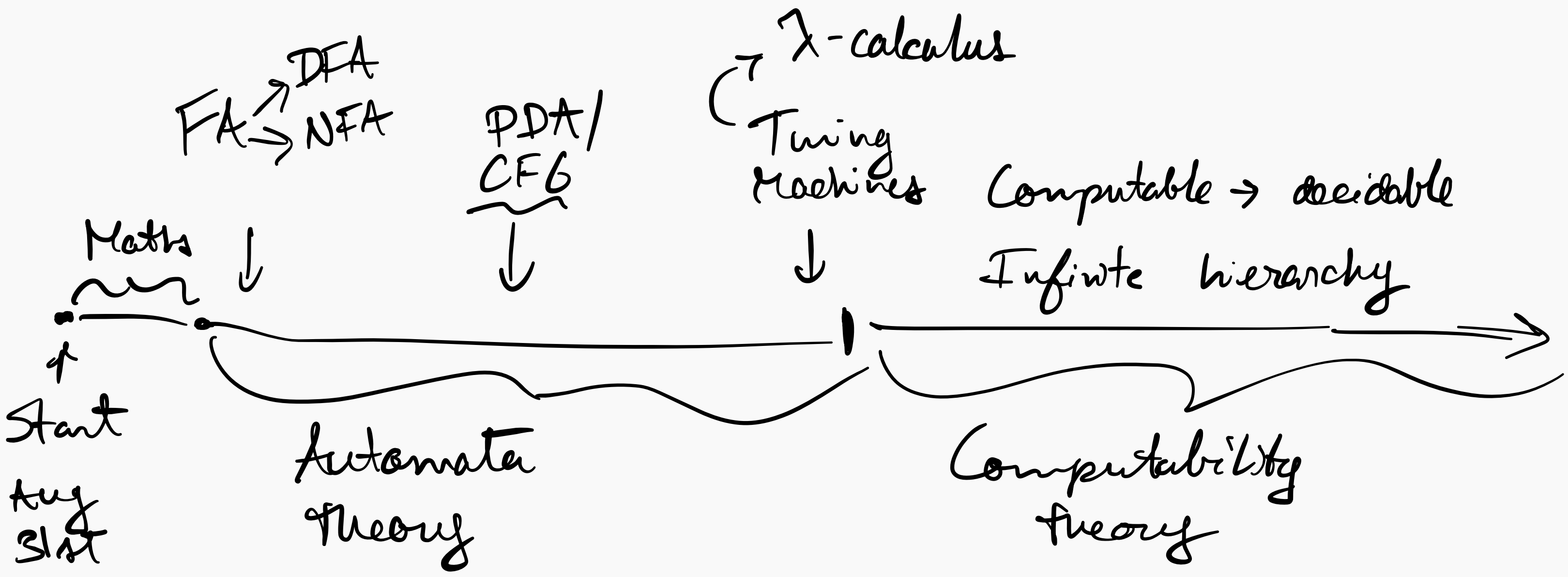
(b) Wilhem Ackermann

Undecidable problems

(c) Alonzo Church

(d) Alan Turing

Course overview



Why is it worth taking?

1. It's useful!
2. It will make you a better computer *scientist*.

Course outline

Lectures

Tuesdays and Thursdays, 8:35 to 9:55, STBIO S1/4

Detailed lecture schedule on myCourses

Lectures are recorded

Mode of delivery: iPad and/or chalkboard

Staff

Pez

↓

Chez

There is/are

A senior instructor: Claude Crépeau

A co-instructor: Cesare Spinoso ~~Bog~~ ~~Sir~~ M~~is~~ter

6 TAs (so far) Chez-array

We will all hold office hours. Instructor office hours already on course outline. TA office hours TBD.

↳ Cesare's:
MC 110 South Wing
Claude's:
MC 110N ~~North Wing~~

Course resources

myCourses: Lecture notes and homework assignments

Crowdmark: Assignment submissions

Ed Discussion: Class discussion/announcements

Course evaluation

6 assignments, 5% each, due at 11:59 PM on Thursdays

1 midterm, 20%, October 13th 2023

↳ 6:05PM

7:25PM

Location TBD

1 final exam, 50%

Advice

Do the assignments **yourselves**!

Discussing difficult problems with friends is encouraged.

Asking ChatGPT to solve the assignment for you is not.

Understand the assignment solutions.

Even if you couldn't completely solve the question, understanding what you did wrong will help for the other evaluations.

Come to office hours!

We're here to help :)

Maths review

Discrete math/
structures

Logic

Proof techniques

Set theory

Relations

Supplementary material

Partial orders/

Principle mathematical induction

Maths review

Logic

Definition (Proposition)

A **proposition** is a declarative statement which is either true or false, never/not both.

Example

proposition

Truth value

$p = \text{“}2 + 2 = 4\text{”} \rightarrow T$

prop. variable

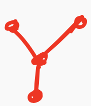
$q = \text{“A tree } T = (V, E) \text{ has exactly one cycle.”} \rightarrow F$

T F

$p \wedge q = F$

$p \vee q = T$

⊛ (This isn't quite a "simple" proposition because "exactly one" requires quantifiers)

q =  has one cycle

Logical connectives

Operators on propositions

Definitions

Given propositions p, q

$\neg p$ is the **negation** of p → Truth value opposite of p

"and" $p \wedge q$ is the **conjunction** of p and q → T when $p = T$ & $q = T$
F otherwise

"or" $p \vee q$ is the **disjunction** of p and q → T when $p = T$ or $q = T$
F otherwise

Example

Using the previous example, what is $p \wedge q, p \vee q$?

Definition (Conditional statement)

p, q propositions. The **conditional statement** $p \to q$ is the proposition "if p, then q". Also called the **implication**.

$p \to q$ T when p is F or when p is T & q is T

Think of the implication as a **contract**.

↳ Valid as long as you don't breach/break it

Example

$\underbrace{\text{If you get 100 on the assignments, midterm and final}}_{p}$, then $\underbrace{\text{you will get an A}}_{q}$.

$\boxed{p \to q}$

Bidirectional implication

Definition (Biconditional statement)

p, q propositions. The **biconditional statement** $p \leftrightarrow q$ is the proposition "p if and only if q". Also called **bidirectional implications**.

truth value $p \Leftrightarrow q$
T when p & q have the same truth value
$p=T, q=T$ or $p=F, q=F$

Example

F T F T

$\left[\underbrace{p \to q}_{\text{Direct implication}} \leftrightarrow \underbrace{\neg q \to \neg p}_{\text{Contrapositive}}\right] \equiv$ T i.e. the implication and its contrapositive are logically equivalent

Predicate logic

Propositions cannot represent statements like "Every even integer is divisble by 2". Requires **predicates** and **quantifiers**.

Definition (Predicate)

Property P than an element x can take on, written $P(x)$. Also called a **propositional function**.

x has property P

Example

True

Let $P(x)$ be "x is greater than 4". Then what is $P(3)$, $P(5)$?

element w/ that property applied

Property

"3 is greater than 4"

False

Quantifiers

In quantification, you specify the range over which $P(x)$ is true.

"for all" Assuming x is in some universe/ domain of discourse

Universal quantifier: $\forall x . P(x)$ $\equiv T$ every x satisfies P(x)

Existential quantifier: $\exists x . P(x)$ $\equiv T$ at least one elt to satisfy P(x)

"there exists"

Example

What is the truth value of each of the following quantified statements?

$\forall x \in \mathbb{R} \ . \ x + 1 > x$ $\equiv T$

$\exists x \in \mathbb{R} \ . \ x^2 = -1$ $\equiv F$

Nested quantifiers

A great source of confusion for students! We will soon see a nested quantified statement that looks like

$$\exists p > 0. \forall w \in L, |w| \geq p. \exists w = xyz. \forall i \geq 0. xy^i z \in L$$

Due to Prakash

n $n+1$ $\mathbb{N}$

Example

Which of the following statements is/are true?

1. $\forall n \in \mathbb{N} \,.\, \exists m \in \mathbb{N} \,.\, n < m$ → You can always find a nat. number greater than n
2. $\exists n \in \mathbb{N} \,.\, \forall m \in \mathbb{N} \,.\, n < m$ → There is a natural number that's strictly less than all nat. numbers

To tackle these statements we will play games! More on this in future lectures. $\mathbb{N} = \{0, 1, 2, 3\}$

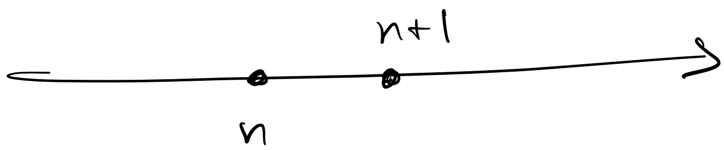
0

$0 < 0$

$\forall n \in \mathbb{N}.\ \exists m \in \mathbb{N}.\ n < m$

↳ "Every nat-number n has a number that's greater than n"

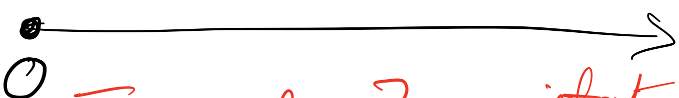
True b/c



$\exists n \in \mathbb{N}.\ \forall m \in \mathbb{N}.\ n < m$

↳ "There is a natural number that's less than every natural number"

This is false



(*) In the lecture I made 2 mistakes

1. I wrote "greater than", this was wrong because the inequality is $n < m$

2. I also said "every other natural number", wrong because the word other implies $n \neq m$ which is not true. Thanks for spotting this!

Maths review

Proof techniques

A one slide review

We will prove many statements in this class using the following proof techniques:

W.T.S. $\Rightarrow$ want to show

- Direct proof

  $P \to Q$, Assume P is true, show Q is true

- Proof by contraposition

  $P \to Q \Leftrightarrow \neg Q \to \neg P$

  Assume $\neg Q$, show $\neg P$

- Proof by contradiction

  $\neg P$, Assume P, derive a contradiction

- Proof of equivalence (i.e. $\iff$ -proofs)

  $P \Leftrightarrow Q$

  1. $P \Rightarrow Q$ 2. $Q \Rightarrow P$

- Set equality proof

  $A = B$, $A \subseteq B$, $B \subseteq A$

  $\forall x \in U.\ x \in A \Leftrightarrow x \in B$

- Proof by induction

  $P(n)$: 1. BC $P(n_0)$ 2. Assume $P(n)$ show $P(n+1)$

  $\mapsto$ Supplement. material

- Proof of uniqueness

  W.T.S. Unique element x that satisfies property P

If you need a refresher, some of these are covered here.

Maths review

Set theory

What is a set?

Definition (Set)

A **set** is an unordered collection of distinct objects.

We use the definition of sets from "naive set theory". This is sufficient for the purposes of this course.

Example

$$S_1 = \{1, 2, 3, \ldots, 49\}\ 4$$

for some $k \in \mathbb{Z}$

$$S_2 = \{n \in \mathbb{Z} : n \geq 0 \ \& \ n = 2k\} = \{\text{non-neg even integers}\}$$

S_2 uses **set builder notation**, notice its implicit universal quantifier.

↳ Properties

$\forall x \in U .\ x \in S_2 \iff x$ satisfies

Set membership and containement

Set membership. If an element x belongs to a set A, write $x \in A$. Otherwise, $x \notin A$.

Example

$A_1 = \{1, 2, 3, ..., 75\}$ Does $2 \in A_1$? Does $-45 \in A_1$?

Set containement. A set A is a *subset* of B if every element in A is also in B. We write $A \subseteq B$. If additionally $A \neq B$ then A is a *proper subset* of B written $A \subset B$.

$A \subseteq A$

Example

Let $A = \{1, 3, 5\}$, $B = \{1, 3, 4, 5\}$. Which of the following is correct?

$A \subseteq B$, $A \subset B$

An important set to remember

Definition (Empty set) NOT NOTHING

The **empty set** denoted as $\varnothing, \emptyset, \{\}$ is the set that does not contain any elements. That is

$$[\forall x \in U \;.\; x \notin \emptyset] \equiv T$$

Always keep the empty set in mind when answering True/False questions :)

Set operations

Definitions

Let A, B be sets

- $A \cup B = \{x : x \in A \vee x \in B\}$
- $A \cap B = \{x : x \in A \wedge x \in B\}$
- $A - B = A \setminus B = \{x : x \in A \wedge x \notin B\}$
- $\overline{A} = A^c = \{x \in U : x \notin A\}$
- $A \times B = \{(a, b) : a \in A \wedge b \in B\}$

Set difference

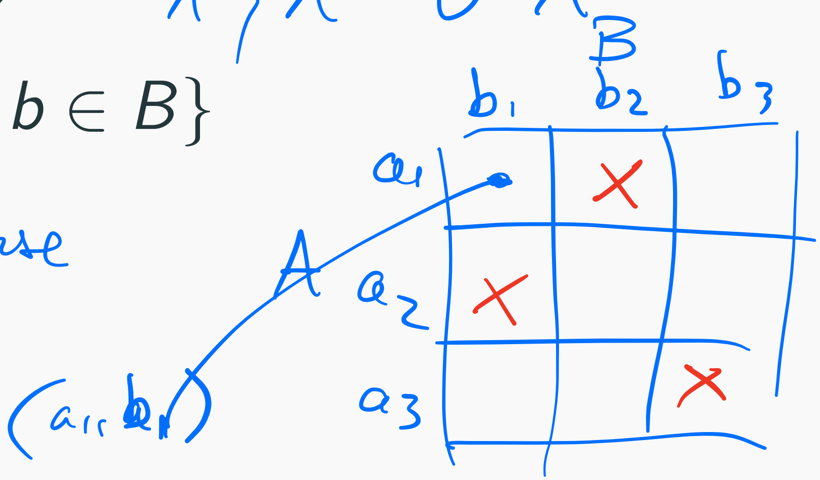
Universe

tuples

Cartesian product

A' ; $\overline{A} = U - A$

$\mathbb{R}$



Extra set theory facts

Other things that you should know about

Cardinality

Power sets $A \to 2^A$, $\mathcal{P}(A)$

Set identities e.g., $\underbrace{A \cap \emptyset}_{=\emptyset}$, $\underbrace{U \cup B}_{=U}$

Proving that two sets are equal

Double inclusion

Review exercises

Let $U = \{1, 2, 4, 7, 8, 9, 10, 11\}, A = \{7, 8, 9\}, B = \{4, 9, 10\}$.
What is the result of the following set operations?[1]

a. $A \cup B$

b. $A \cap B$

c. $A - B$

d. $\overline{A} \cap B$

e. $A \times \{1, 2\}$

f. $U \times \emptyset$

g. $(\overline{A} \cup \overline{\emptyset}) \cap U$

---

[1] These are exercises I used from my days as a TA at Concordia.

Maths review

Relations

What are relations?

Definition (Relation)

A **binary relation** R from set A to set B is a subset of $A \times B$ i.e. $R \subseteq A \times B$. If $x \in A, y \in B$ are related by R we often write xRy. $(x, y) \in R$ is less commonly used.

Intuitively, relations specify the *relationship* between elements of (the same or different) sets.

Example

Let S be the set of students and C be the set of courses (at McGill). The enrollment of students to courses can be seen as a relation R^{enroll} where for $s \in S, c \in C$

$$sR^{\text{enroll}}c \text{ if and only if } s \text{ is enrolled in } c$$

More on relations

$R \subseteq A \times A$

Remark

A relation *on a set* A is a relation from A to A.

Example $f(x) = x^2$ $f: \mathbb{R} \to \mathbb{R}$

A *function* $f : X \to X$ on X is a relation on X with what kind of restriction?

injective, bijective, surjective

Properties of relations

Definitions

Let X be a set and let R be a relation on X. Then R is

- **Reflexive** if $\forall a \in X . aRa$ $\quad [a] = \{a$
- **Symmetric** if $\forall a, b \in X . aRb \to bRa$
- **Transitive** if $\forall a, b, c \in X . [aRb \land bRc] \to aRc$

Example

Is the relation is-related-to symmetric? What about the relation is-a-parent-of?

Equivalence relation

Definition (Equivalence relation)

A relation R on a set X is an **equivalence relation** if it is reflexive, symmetric and transitive.

R S T

$1 = 1$, $\mathbb{N}$ R

An equivalence relation abstracts the notion of equality of numbers to elements of arbitrary sets.

Example

Let E be the set of all strings made up of English letters. Define R as $x, y \in E, xRy \leftrightarrow |x| = |y|$. Is R an equivalence relation?

Exercise: Prove that R is an eq. relation

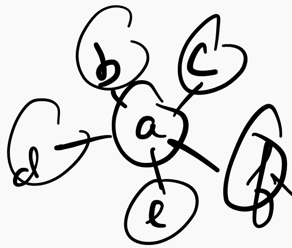
1. R
2. S
3. T

A1Q2

Equivalence class

Definition (Equivalence class)

Let R be an equivalence relation on a set X. Then the **equivalence class** of $a \in X$ is the set of all elements in X which are related to a. This is denoted as



$a \in X$

$$[a]_R = \{b \in X : aRb\}$$

We say that a is the **representative** of the equivalence class $[a]_R$.

Example

If R is an equivalence relation on X and $X \neq \emptyset$, can R have an empty equivalence class? → No! B/c R is reflexive

What happens when X is ϕ?

Equivalence classes partition X

eq R

Partition on X

$A_1, A_2, A_3, \dots$ $A_i \cap A_j = \emptyset$ if $i \neq j$

$A_1 \cup A_2 \cup A_3 \cup \dots = X$

Proposition

Let R be an equivalence relation on a set X. For every $a, b \in X$, **either** $[a] = [b]$ **or** $[a] \cap [b] = \emptyset$ **but not both**.

Exercise: A1Q1

Proposition

Let R be an equivalence relation on a set X. The collection of equivalence classes of R on X, denoted X/R, **partitions** the set X.

This final fact will be important as we study automata theory!

- Next class is September 5th and will (most likely) be completely hand-written.
- Assignment 1 will be released September 5th and will be due September 21st.
- Have a nice long weekend!