Contents

1 Lecture 1 *<2017-09-05 Tue>*

Logic & Computability Prof. Dirk Schlimm

- Find out what Schlimm means for the next lecture
- Great for people in computer science, but everyone else too

  - Essential material that everyone should know
  - Stable material, as the material is old
  - Very abstract and technical material, even if it does not require a solid mathematical background
  - Hard course
    * Important to give feedback to the professor

This course complements the textbook, Godel, Escher Bach.

1.1 Homework

is not graded, just checked if done.

- Why?
  - To motivate us to do homework exercises
  - Practice is important, the course is hard
  - TAs don't need to correct them, so they can hold more office hours

Discussion board on MyCourses. Do not email the professor, ask questions on discussion board so everyone can see the answer (incase they have the same question).

Some times there will be intentional mistakes on the board.

- To make it easier to ask questions
- To motivate us to pay attention

There are no stupid questions, even if you ask the same question as the person before you. Perhaps the professor's answer was unclear. The most stupid question is the one not being asked.

1.2 Quizzes

- 3 quizzes throughout this course
- Dates will be on the schedule on professor's website
- In class, 15-20 minutes long
- Each one is graded and worth 10%
- Fairly straightforward, some are even definitions

- To make sure you've done your work

Midterm is 25%, Final is 40%

1.3 Proofs

We will see lots of proofs, different kinds of proofs.

- Direct: Go from assumption towards the theorem
- Indirect: Negation of claim $\rightarrow$ contradiction $\rightarrow$ claim
  - Sometimes called proof by contradiction
- Biconditional: 2 claims, p, q
  - Start with p and prove q but also start with q and prove p
- By cases: Split claim into several cases
  - case 1, case 2, case 3
  - Each one proves the same conclusion
  - If the cases were exhaustive, then you have proved the claim
- Induction (to be taught next lecture)

So you can split a proof into subproofs of these kinds.

1.3.1 Example Proofs

1. Thm $\sqrt{2}$ is nor rational.
   - Rational: Fractions: $\frac{x}{y}$

   If you have a square with sides of length 1, the length of the diagonal is $\sqrt{2}$ Pythagoras proved this.

   (a) Def 1 A natural number a is even if and only if (iff) $\exists$ a natural number b, such that $a = 2b$.

   (b) Lemma 1 For any number a, a^2 is even iff a is even.
   - Biconditional, since iff

i. Proof: $\leftarrow$ Assume: $\underline{a \text{ is even}}$. So there is: $a = 2b$ (by def. 1) $a^2 = (2b)^{=}4b^2 = 2(\underbrace{2b^2}_{c})$ (square) So, $\underline{a^2 \text{ is even}}$, since it is 2 times c, a natural number.
$\rightarrow$ (DIY) Assume: $\underline{a^2 \text{ is even}}$. So there is: $a^2 = 2b$ (by def. 1)

(c) Lemma 2 For any rational number x, there are natural numbers a and b, $\underline{\text{not both even}}$, s.t. $x = \frac{a}{b}$

- If they were both even, you could simplify the fraction by dividing by 2.

Proof omitted for this lemma.

(d) Proof of Thm: Indirect proof. (Contradiction) Assume (for reductio/contradiction): $\sqrt{2}$ is rational. By Lemma 2, $\exists$ natural numbers $\underline{a \text{ and } b \text{ not both even}}$ s.t. $\sqrt{2} = \frac{a}{b}$
Square: $2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$ $a^2 = 2b^2$
So a^2 is even (by def. 1) $\underline{a \text{ is even}}$ by (lemma 1) If a is even, we can write: $a = 2c$ (by def 1) Square: $a^2 = (2c)^2 = 4c^2 = a^2$
$4c^2 = 2b^2$
Divide by 2: $2c^2 = b^2$ So b^2 is even (def. 1) $\underline{b \text{ is even}}$ (by lemma 1)
Contradiction! Assumption is false, therefore $\sqrt{2}$ is $\underline{\text{not}}$ rational. $\square$

2. **TODO** Download Handout and read it

2 Lecture 2 *<2017-09-07 Thu>*

Last class we talked about proofs & types of proofs. Next week we'll be talking about sets and countability and comparing them all. Will talk about density of rationals and irrationals, to say which is bigger.

2.1 Things that are infinite

- Natural numbers
- Rational numbers
- Infinite lists

1. How do you prove things about infinitely large things?

- Counter example
  - All swans are white
    - Show one that isn't white
- Pick an arbitrary example and show that it works for that
  - Use particular properties about an arbitrary object to show that something works for all of them

2.2 Mathematical induction

- Inference (step):
  - Certain number of assumptions/premises $A_n \dots A_n$
  - Conclusion

2.2.1 Deduction:

- It is impossible for the premises of an inference step to be true and the conclusion false.
- The conclusion follows necessarily from the premises. (reformulation of above)

1. e.g. $\frac{\text{if } A \text{ then } B \quad A}{B}$
   - MODUS PONENS (type of deductive inference)

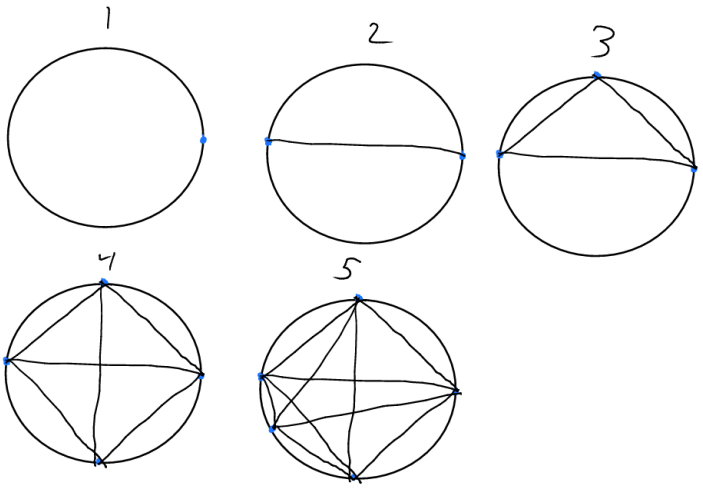
2.2.2 Induction:

- The premises make the conclusion more likely
- My cat is smart, my friend's cat is smart, my parent's cat is smart, so all cats are smart
  - Inductive argument, makes it more likely, but doesn't see them all

2.2.3 Inductive or Deductive?

1. Claim Let n be the number of points on a circle. Then the number of regions obtained by pairwise connecting each point is $R = 2^{n-1}$
   (a) Argument

n	R
1	$1 = 2^0$
2	$2 = 2^1$
3	$4 = 2^2$
4	$8 = 2^3$
5	$16 = 2^4$
6	31



- Inductive argument
- What was wrong with the argument?
  - We saw a pattern, but...
    - There's no reason for the jump from each n to have something in common
    - If they had something in common, then it would continue holding for the next one
  - Therefore induction makes the premise more likely
    - But does not establish it deductively
  - So in order to rigorously prove something inductively, we need mathematical induction

2.3 Handout

2.3.1 Recursive (inductive) definition:

1. Base clause(s) defines basic elements.

2. Inductive clause(s): How to build up complex elements from parts
3. Final clause: Nothing else is an element (bookkeeping)

1. E.g.
   (a) $\mathbb{N}$
      - Base clause 0 is in $\mathbb{N}$
      - Inductive clause: if $x \in \mathbb{N}$ then $s(x)$ (successor of x) then $s(x)$ is in $\mathbb{N}$
      - Final clause: Nothing else is in $\mathbb{N}$
      - So natural numbers are:
        - $0, s(0), s(s(0)), \ldots$
   (b) Even numbers or odd numbers
      - Take successor of successor, take 0 as base clause for even, 1 for odd
   (c) Lists
      - Empty list is a list
      - What you get from adding to a list is also a list
   (d) Dominoes
      - When you have a domino, you can place one 2 cm behind it
      - Push first one, they all fall
        - To prove they all fall, have to show they all have a certain amount of space between them
          * Relates to proof by mathematical induction

2. Proof by mathematical induction
   (a) Base case: Show that the property holds of the basic elements.
   (b) Inductive step:
      i. Assume that the property holds for some element n (Inductive Hypothesis)
      ii. Show: holds for elements generated from n by inductive clauses.
   (c) Conclusion: Property holds for all elements.

   This is **deductive inference**! What are the premises?

   - For natural numbers:

$$\frac{\overbrace{P(0)}^{\text{Base case}} \quad \overbrace{P(n)}^{\text{IH}} \overbrace{\rightarrow}^{\text{Ind. step}} P(s(n))}{\forall x P(x)}$$

3. Variant (strong/complete induction):
   - Ind. Step.
     (a) Assume that P holds for all elements less than n
     (b) Show: P holds of n
   - No base case
   - See example 5.5!

2.3.2 Theorem

For any nat. number $n \geq 1$, the sum $\underbrace{1 + 2 + \ldots + n}_{\sum_{i=1}^{n} i} = \frac{n(n+1)}{2}$ (If you do a proof for your homework or on an exam, always include many details. You can even use a template to structure your proofs the same way, useful for steps for induction.)

1. Proof (by math. ind)
   (a) Base case: Show claim holds for $n = 1 = \frac{1(1+1)}{2}$
   (b) Ind. step.
      i. I.H. The claim holds for m: $\sum_{i=1}^{m} i = \frac{m(m+1)}{2}$
      ii. Show: The claim holds for $m + 1$

   2 strategies, either $\frac{n(n+1)}{2} \rightarrow 1 + 2 + \ldots + n$ or $1 + 2 + \ldots + n \rightarrow \frac{n(n+1)}{2}$. Will be doing 2nd. $1 + 2 + \ldots + (m + 1) = \sum_{i=1}^{m+1} i = \sum_{i=1}^{m} i + (m + 1)$
   $= \frac{m(m+1)}{2} + (m + 1)$ (by I.H.)
   $= \frac{m(m+1)+2m+2}{2} = \frac{(m+1)(m+2)}{2}$

   (a) Conclusion: The claim holds for all $n \geq 1$ $\square$

3 Lecture 3 *<2017-09-12 Tue>*

3.1 Set theory

All that is being said here is taken from the reading mathematical introduction to logic chapter zero.

A set is a thing with elements. We can present sets in two ways:

- Extensional:
  - Presentation
  - $\{1, 2, 3\}$
- Intensional:
  - Given a set A, and a property P: $\{x \in A | P(x)\}$

3.1.1 Ex

$\mathbb{N}$: the set of natural numbers.
$D = \{x \in \mathbb{N} | x \text{ is prime}\} = \{2, 3, 5, 7, 11, \ldots\}$

3.1.2 Definitions

- $A \subseteq B \iff \forall x, x \in A \implies x \in B$
- $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$
- $A \underbrace{\subset}_{\text{Proper subset}} B \iff (A \subseteq B) \wedge (A \neq B)$
- Empty set: $\emptyset, \{\}$
  - When is $x \in \emptyset$? Never.
  - $\emptyset \subseteq X$? Always.
    - Since all elements of the empty set are in X.
  - $\emptyset \in X$?. If X contains $\emptyset$.
    - E.g. $X = \{\{\}, 4\}$

$A = \{2, 4, 8\}, B = \{a, 4, z\}$

- $\underbrace{A \cap B}_{\text{intersection}} : \forall x, (x \in A) \wedge (x \in B)$
  - $A \cap B = \{4\}$
- $\underbrace{A \cup B}_{\text{union}} : \forall x, (x \in A) \vee (x \in B)$
  - $A \cup B = \{2, 4, 8, a, z\}$

- complement: $\bar{A}$: all elements that are not in A (from the universe of discourse, the universe we're talking about)
- Power set $\mathfrak{P}(A)$: the set of all subsets of A
  - E.g. $\mathfrak{P}(B) = \{\emptyset, \{a\}, \{4\}, \{z\}, \{a, 4\}, \{a, z\}, \{4, z\}, \{a, 4, z\}\}$
  - If A has n elements, $\mathfrak{P}(A)$ has 2^n elements.
- Is $\{\emptyset, a\} \subseteq \{a, 4, z\}$? No.

3.2 Tuples:

Like sets, but order matters.

- Ordered pair: $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$
- $\langle a, 4, z\rangle \neq \langle 4, a, z\rangle$

3.2.1 Cross-product

$A \times B \iff \{\langle x, y\rangle | x \in A \wedge y \in B\}$

- If A has n elements, B has m elements
- then $A \times B$ has $n \cdot m$ elements
- and there are $2^{n \cdot m}$ relations between A and B
  - Since this is essential just the cardinality of the power set of the cross product
  - E.g. $n = 5, m = 5$. 2 pairs of 5 friends. How many relations are possible? $2^{25} = 33,554,432$

3.2.2 Relations

- $A = \{\text{John, Paul, George}\}$
- $B = \{\text{guitar, bass}\}$
- $\{\langle\text{John, guitar}\rangle, \langle\text{Paul, bass}\rangle, \langle\text{George, guitar}\rangle\} = R_1$
- $R_2 = \{\langle\text{John, bass}\rangle\}$

A relation R on A and B is a subset of $A \times B$.

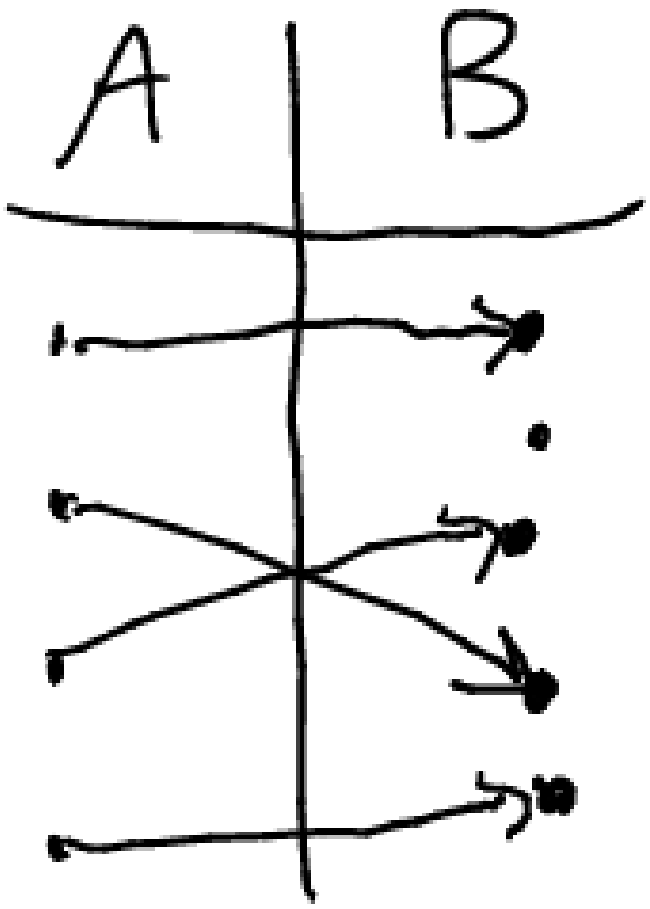
- Elements of relations are tuples.

Domain of a relation $R : \{a|\text{there is a b, s.t. } \langle a, b\rangle \in R\}$

- domain of $R_1 : \{\text{John, Paul, George}\}$
- domain of $R_2 : \{\text{John}\}$

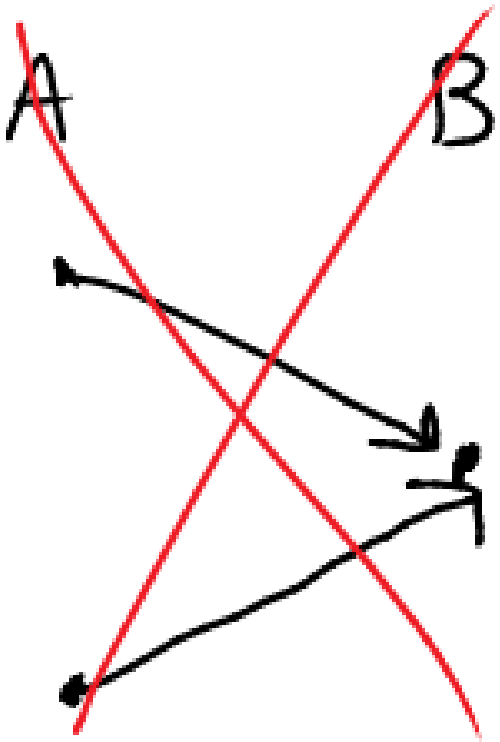
Range of a relation R: $\{b|\text{there is an a, s.t. } \langle a, b\rangle \in R\}$

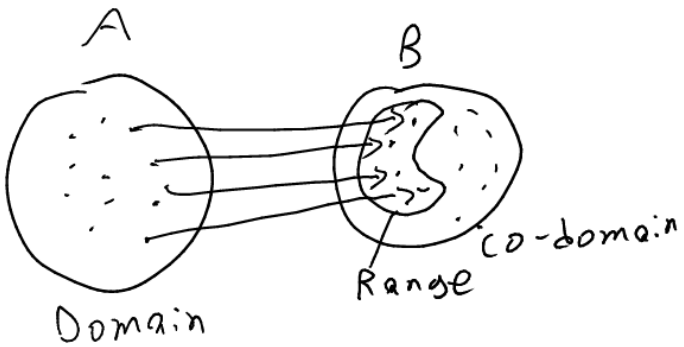
1. Functions A total function $f : A \to B$ is a binary relation R, on A and B such that.
   - It is single-valued
     - Every element in A is mapped to exactly one element in B
   - The domain of R is A



(a) Definitions

- A function is injective (one-to-one), if each element in the range is mapped to by exactly one element.
  - To show this: Assume $f(x) = f(y)$
    - Show $x = y$
  - So you don't have the situation that:





- A function is surjective if the *range* = *codomain*.
- A function that is both injective and surjective is bijective.

4 Lecture 4 *<2017-09-14 Thu>*

4.1 Recap

We talked about sets last class, such as:

- $\{1, 4, z\}$
- $|\{1, 4, z\}| = 3$ (Cardinality)

Are there more students or chairs in this class?

- There are more chairs.
- Matched students with chairs and to see what is left
- f(students) $\rightarrow$ chairs
  - Injective function (can't have 2 students on one chair)
  - Every element of the range must be mapped to something
  - No element in the range can map to two elements
- $\implies |S| \leq |C| \iff$ there is an injective function from S to C.

Cantor: $|A| = |B| \iff |A| \leq |B|$ and $|B| \leq |A| \iff$ there is a bijection between A and B.

4.2 More on sets

4.2.1 Cardinalities

A set D is finite if its cardinality is a natural number.

- $D \leftrightarrow \{1, \ldots, n\}$ (bijective function with natural numbers exists)

A set is countably infinite (denumerable), if it is equinumerous to $\mathbb{N}$ (bijection from this set to all the natural numbers).

- $E = \{2, 4, 6, 8, \ldots\}$
  - $|E| = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}|$

$\mathbb{N}$	1	2	3	4	$\ldots$	n
E	2	4	6	8	$\ldots$	$2n$

$f(x) = 2x, \mathbb{N} \to E$

$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- Is this bigger than the cardinality of the natural numbers?
  - No, it's the same size, bijection. Even to positive, odds to negative.

-3	-2	-1	0	1	2	3
5	3	1	0	2	4	6

$\mathbb{Q}^+ = \{\frac{x}{y} | x, y \in \mathbb{N}\}$

- Are there more?

	1	2	3	4	5	6	$\ldots$
1	$1/1$	$1/2$	$1/3$	$1/4$	$1/5$	$1/6$	$\ldots$
2	$2/1$	$2/2$	$2/3$	$2/4$	$2/5$	$2/6$	$\ldots$
3	$3/1$	$3/2$	$3/3$	$3/4$	$3/5$		
4	$4/1$	$4/2$	$4/3$	$4/4$			
5	$5/1$	$5/2$	$5/3$				
6							

There are duplicates here though. So, instead of counting left to right, count diagonally.

- i.e. 1:1/1, 2:1/2, 3:2/1, 4:3/1, 5:2/2, 6:1/3, ...

$\mathbb{R} = \mathbb{Q} \cup \{\text{irrationals}\}$

- What are real numbers? All numbers that can be expressed via decimal expansion.
- $x.xxxxx\ldots$
- Is this countably infinite? No.

4.2.2 Proof (by contradiction):

Assume $|\mathbb{N}| = |\mathbb{R}^{0.1}|$. ($\mathbb{R}^{0.1} = \{x \in \mathbb{R} | 0 < x < 1\}$.)

Therefore, there is a bijection $f : \mathbb{N} \to \mathbb{R}^{0.1}$

Then, we can build the following table:

$\mathbb{N}$	
0	$f(0) = 0.12345\ldots$
1	$f(1) = 0.33333\ldots$
2	$f(2) = 0.5000\ldots$
3	$f(3) = 0.011101\ldots$
4	$\ldots$
$\ldots$	$\ldots$
n	$f(n) = 0.112\ldots = z$

Can you explain this table? Not really. Why?

- Construct new number z:
  - $z = 0.z_1z_2z_3z_4\ldots$
  - Rule for constructing z:

$$z_i = \begin{cases} 1 & \text{if } f(i)_j \neq 1 \text{ where } f(i)_j \text{ is the ith digit in the decimal expansion of f(i)} \\ 2 & \text{otherwise} \end{cases}$$

- $f(1)_1 = 3$
- $f(2)_2 = 0$
- $f(3)_3 = 1$
- $\implies z = 0.112\ldots$
- By construction, z is a real number between 0 and 1.
- So it must be in the table, say in line n.

What is z_n?

- Two cases:
  - $z_n = 2 = f(n)_n$ if $f(n)_n = 1$`
  - $z_n = 1 = f(n)_n$ of $f(n)_n \neq 1$`
  - $\implies$ contradiction!
    - The assumption is false.

5 Lecture 5 *<2017-09-19 Tue>*

- Quiz in one week
- 20 minutes, in class
- 8-10 questions, very simple
  - Everything that was said in class
  - Everything done in the homework
  - Readings

5.1 Recap

Last class, we proved: (Size of Natural numbers) $\aleph_0 < |\mathbb{R}| \implies$ Diagonalization

- We had a table and changed every element on the diagonal in order to get a new element
- We will see many more proofs by diagonalization
- Homework question: $|\mathfrak{P}(\mathbb{N})| > |\mathbb{N}|$
  - In general though, $|\mathfrak{P}(x)| > |x|$ (Cantor's theorem)
    - What does this imply? There are infinite amount of infinite cardinalities (power set is bigger, power set of the power set is even bigger, ...)
    - $|\mathbb{N}| < |\mathfrak{P}(\mathbb{N})| = |\mathbb{R}| = 2^{\aleph_0} < |\mathfrak{P}(\mathfrak{P}(\mathbb{N}))|$

5.2 Cardinality

Things that have the same cardinality:

5.2.1 Countable:

$|\mathbb{N}|$:

- E
- $\mathbb{Z}$
- $\mathbb{Q}$

- English words
- Sentences
  - Finite objects that you can list
  - Why doesn't diagonalization work on sentences?
- Programs
- MIU strings
- MIU theorems
- If you can list them, they're countable

5.2.2 Uncountable

$|\mathfrak{P}(\mathbb{N})|$

- $\mathbb{C}$
- $\mathbb{R}$
- Functions from $\mathbb{N} \to \mathbb{N}$
  - From $\mathbb{N} \to \{0, 1\}$

5.3 Formal Systems (GEB CH. 1)

5.3.1 Examples

- Programming languages
- Logic
- Computation: TM
- Formal arithmetic

---

2 things in formal systems:

- The distinction between the two is very important

- Important concepts in this course:
  - Induction
  - Diagonalization
  - Distinction between these 2 things

Syntax	Semantics
- Grammar	- Meaning
- Formal Structure	- Context

13 -> What is this?

- 13 is a numeral
  - The meaning of this numeral is the number 13 (abstraction)
- Why this example? We looked at the syntax of 13 but we said it was the number 13 (the meaning)
  - During everyday life we don't often make the distinction
- dog
  - Syntactically, has 3 letters
  - Semantically, has fur

5.3.2 MIU-System:

Alphabet: MIU

Strings (sequences of elements from the alphabet).

Rec. def:

- Base clause: $\emptyset$ is a MIU-string
- Inductive clause:
  1. If x is a MIU-String, then xM is a MIU string
     - Is x an MIU-String? No, that's it's meaning, not it's syntax. It's a letter (also a meta-variablee)
  2. xI
  3. xU
- Final clause: Nothing else.

1. MIU-Theorems

   (a) Axiom: MI.

   (b) Inference rules:
   I. xI $\rightarrow$ xIU
   II. Mx $\rightarrow$ Mxx
   III. xIIIy $\rightarrow$ xUy
   IV. xUUy $\rightarrow$ xy
   (for x,y MIU strings, possibly empty)

   (a) Def. Derivation A derivation is a sequence of strings such that each element is either an axiom or obtained by applying an inference rule to an element earlier in the sequence
   The last element in a derivation is a theorem.

   - This is a recursive definition.
     - Includes base clause
     - Inductive clause
     - Recursive clause

   (b) Ex.

   i. MI is a derivation
   ii. MIU by I on line 1.
   iii. MII by II on line 1.
   iv. MIUIU II on line 2.

   These are all theorems since they're the last element of a derivation.

   (c) Random theorems

   - MIIII
   - MIIIIU
   - MIUU
   - MIUUIUU
   - MIIUU
   - They all have something in common, all start with M

2. Reasoning Reason inside (M-mode)

   - Generate theorems "within" the formal system

- Can be done by a machine
- Object language

Outside a system (I-mode)

- Show properties of the system, reason about it
- Meta-language
  - All theorems start with M
  - Looking on the outside
  - When do we use other languages to describe another language
  - Using English to talk about programming
  - Using English to talk about Mandarin
  - If you speak English, then you're reasoning inside

3. Bijection with Natural Numbers MIU strings are countably infinite. You can construct a bijection like:

   (a) M
   (b) I
   (c) U
   (d) MM
   (e) MI
   (f) MU
   (g) II
   (h) IM
   (i) IU
   (j) UU
   (k) ...

MIU theorems are also countably infinite? Why?

- Subset of MIU strings
- Why not finite? Inference II, can keep expanding

4. Theorem All MIU-theorems begin with M.

   - This is a proof about the MIU-system, not within

(a) Proof By induction (strong induction) on the length of derivations: (number of steps to derive)

- Base case: Derivation of length 1: MI (good)
- Induction step:
  - IH: The claim holds for all derivations of length $< n$
  - Show: The claim holds for a derivation of length n
  - Line n is either an axiom or derived by rule I, II, III or IV.
- Case 1: Line n is an axiom: MI (you can write an axiom at any step, reverting back to MI)
- Case 2: Line n is derived from an earlier line (say $m < n$) by Rule I. By IH, the theorem in line m begins with M. Rule I doesn't change the first letter, so it is also an M.
- Case 3:
- Case 4:
- Case 5:
- (DIY)

6 Lecture 6 *<2017-09-21 Thu>*

6.1 Quiz prep

- What is derivation?
- What is a theorem?
- How many infinite cardinalities are there?
- Can a set have the same cardinality as its power set?
- Is the empty set a subset of every set?
- How do you prove something is inductive?

6.2 Review

- Is U a MIU-theorem?
  - No, it doesn't start with M
- Is MU a MIU-theorem?

6.3 Decision Procedure

Guarantees a yes or a no answer in a finite amount of time

- A set/question that has a decision procedure is decidable
- If given 2 functions with inputs and outputs, can we tell if they're identical? Is it decidable?
  - No, infinite amount of inputs
- Decision procedure for getting someone's cellphone number?
  - Try all combinations until the phone rings, if no ring, no number
  - Not feasible, but we care what you can do in principal, as long as its finite
- Given a computer program
  - Can we decide if it terminates in 10 minutes?
    - Yes, just wait
  - Can we decide if it terminates in finite time?
    - No, if it doesn't stop, you'll never know

6.4 pq-system

- Alphabet: p, q, -
- Axiom(s): xp-qx-
  - What is x here? An arbitrary number of hyphens, meta-variable (used to describe system, not part of the system)
  - How many axioms? $\aleph_0$, x can be uncountably many
    - The written axiom is more like an axiom "template"
  - Is there a **decision procedure** to check if something is an axiom?
    - Yes, just count number of hyphens.
  - Axioms in a formal system **have to be decidable**
- IR: If xpyqz is a thm, then xpy-qz- is a thm
  - E.g. *--p--q-----*

6.4.1 Interpretation:

pq-system: p (plus) q (equals) - (1) -- (2) ---(3)

plus	equals	1	2	3	(Semantics)	Math structure $\langle \mathbb{N}, +, = \rangle$
p	q	--	--	---	(syntax)	Typographical structure $\langle \{\text{-}, \text{--}, \text{---}\}, p, q \rangle$

- GEB: Calls this an Isomorphism
  - Misleading, because in mathematics, it's a structure preserving bijection
  - $\langle \mathbb{N}, + \rangle$ is isom $\langle Even, + \rangle$ by $f(x) = 2x$
  - $a + b = c \iff f(a) + f(b) = f(c)$

Are $\langle \mathbb{N}, + \rangle$ and $\langle \mathbb{N}, x \rangle$ isom?

- $a + b = c \iff f(a) \times f(b) = f(c)$
- $f(x) = 2^x$
  - $3 + 5 = 8 \to 2^3 \times 2^5 = 2^8$
  - Does this work? No. Not surjective.
  - Is there a bijection?

If an interpretation makes all axioms and thm true, it is called a model.

- Is our interpretation a model?
- Yes, argue by saying it makes axioms true and IR keeps it true.
  - E.g. *--p--q-----*
  - $2 + 3 = 5$

6.4.2 More Interpretations

Change p to times. It's still an interpretation, but not a model. It's false, as all axioms and theorems must be true.

- Keep p to plus, but change all dashes to negative integers. Is it also a model?
  - Yes. We can still have multiple models for

pq-system: p (equals) q (taken from) - (2) -- (4) ---(6)

- E.g. --*p*--*q*-----
- 6 = 4 taken from 10
- Still a model!
- Formal system can have many models, just depends on interpretation

6.5 geq-system:

- Thms:
  - - geq -
  - -- geq -
  - --- geq ---
- Model: geq -> ≥
  - - 1
  - -- 2
  - ...
- Soundness: Every **thm** in a formal system is **true** under an interpretation
- Completeness: Every **truth** in an interpretation is a **theorem**
- Soundness and completeness relate semantic and syntactic notions with each other
- Our interpretation is sound and complete
- Different interpretation, if we make geq -> =
  - Is it sound? No. Some theorems are true, but some, like -- geq - are not true
  - Is it complete? Yes. Every equality that can be expressed via this interpretation is a theorem.
  - Soundness and completeness are independent, so it was possible for us to get completeness and not soundness, but it's also possible to get the opposite (think of an example)

- model $\iff$ sound
- Syntax and semantics can be switched, which we'll see later
  - We'll be looking at formal systems of numbers/arithmetic that mean different things

6.6 Infinite Prime Numbers

Theorem: There are infinitely many prime numbers.

6.6.1 Proof (by contradiction):

Assumption: There are finitely many prime numbers:

- $\{p_1, p_2, \ldots, p_n\}$
- So there is a greatest prime number, say p_n
- Define: $g = (p_1 \times p_2 \times \ldots \times p_n) + 1$
  - Is g a prime number?
    - Case 1: Yes. Then $g > p_n$ ↯
    - Case 2: g is not prime.
      - But then it must be divisible by some prime number.
      - But, it cannot be divisible by $p_1, p_2, \ldots, p_n$, as there will be a remainder of 1 ↯
- So, assumption is false.

7 Lecture 7 *<2017-09-26 Tue>*

7.1 Quiz review

- Try to use diagonalization on rational numbers?
  - Produced number may not be rational.
- Show 2 sets have the same cardinality
  - Prove there's a bijection
- Show a set has less than or the same amount of cardinality

  - Injection

- Adding something to a set of size $\aleph_0$
  - Size is still $\aleph_0$
- What is a derivation?
  - Sequence of formulas such that each element is an axiom or obtained from an axiom
- Theorem?
  - Last element in a derivation
- When is a formal system complete?
  - Every truth in the interpretation is a theorem
- When is a formal system sound?
  - Every theorem is a truth in the interpretation

7.2 Decision procedure

- What does it mean for a set to be decidable?
  - If it has a decision procedure.
    - Algorithm that gives a yes or no answer in a finite amount of time.
- A set is X decidable if there is a decision procedure for it.
  - Characteristic function:
    -

$$C_x(n) = \begin{cases} 1 & \text{if } n \in X \\ 0 & \text{if } n \notin X \end{cases}$$

Later we will see that decidable set $\iff$ characteristic function computable.

7.3 FS for addition

Write down properties of addition to try and come up with a formal system to fit that interpretation.

Recursive definition of addition:

- $x + 1 = (x + 1)$
- $x + (n + 1) = (x + n) + 1$
  - This allows you to compute any addition
  - $x + 4 = (x + 3) + 1 = (x + 2) + 1 + 1 = (x + 1) + 1 + 1 + 1$

Now translating it to the pq system:

Axiom	xp-qx-	x+1=(x+1)
IR	If xpyqz is a theorem then xpy-qz-	x+(n+1)= (x+n)+1

7.4 FS for multiplication

Want FS for multiplication (tq system) x t y q z

- $x \times 1 = x$
- $x \times (n + 1) = (x \times n) + x$

Translating:

- Axiom: $xt\text{-}qx$ ($\aleph_0$ axioms)
- Inference Rule: If $xtyqz$ is a thm, then $xt\overbrace{y\text{-}}^{n+1}qzx$

Modification of tq system above.

- Alphabet: t q - C
- Second Inference Rule: If $x\text{-}ty\text{-}qz$ is a theorem then Cz is a theorem. (x,y,z non-empty strings of -)
- Example theorems:
  - -t-q-
  - --t--q----

- C----
- ---t--q------
- C------

Cx is true if x is a composite number (not a prime)

- If Cx is not a Cqt theorem, then Px (prime)
  - Can we add this as another inference rule? No. Not saying how to get primes, just what isn't a prime. It's not an inference rule, you have to be able to apply an inference rule mechanically (has to be decidable)

7.5 Recursively enumerable set (r.e.)

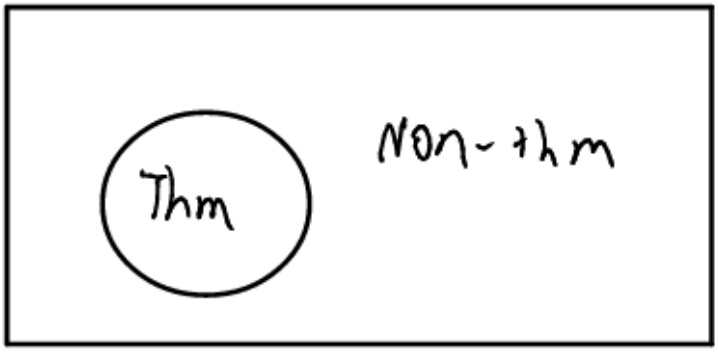
A recursively enumerable set can be generated as theorems of a formal system.

- Ex. Natural numbers

7.6 Recursive set

A set is recursive if it is r.e. and its complement is also r.e. Only want to talk about the complement in a clearly defined realm (universe).

- Well-formed expressions:



- In GEB, he calls the circle the figure and the ground the non-thms that are the non-thms of the circle but they are theorems themselves.

- Recursive sets are decidable. Why?
- Can a set be recursively enumerable but not recursive.

8 Lecture 8 *<2017-09-28 Thu>*

8.1 Theorems

P is equivalent to Q relative to $A_1 \dots A_n$:

- $A_1 \dots A_n, P$ prove Q
- $A_1 \dots A_n, Q$ prove P

8.1.1 E.g.

Relative to Euclid's axioms:
Proclus' axiom

- If a line intersects 2 parallels it must intersect the other

Playfail's axiom

- If a line is parallel to a point, then there exists one parallel containing that point

Parallel postulate
Are equivalent.

- If you cannot prove P from $A_1 \dots A_n$ then P is <u>independent</u> of $A_1 \dots A_n$

Parallel postulate is independent from the axioms of Euclid.

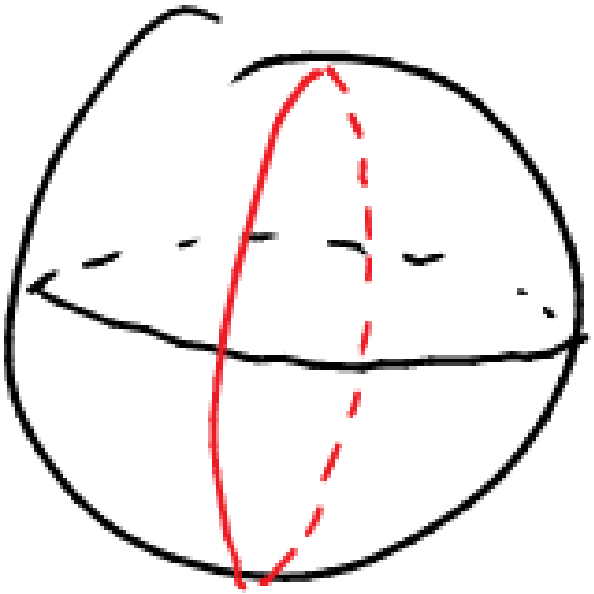
- One way to show:
  - Give a model for $A_1 \dots A_n$ in which P is false. (If a model makes P false, then P cannot be a theorem.)
- How to show that there are certain models for Euclid's axioms where the parallel postulate is false? Well, we have to come up with a model.

1. Playfail's axiom There exists exactly one parallel to a given line through a given point.
   - What would it mean for this to be false?

- Playfair's axiom can be false in 2 ways:
  a) More than one parallel exists
  b) No parallel exists

b)

- Line -> great circle on a sphere



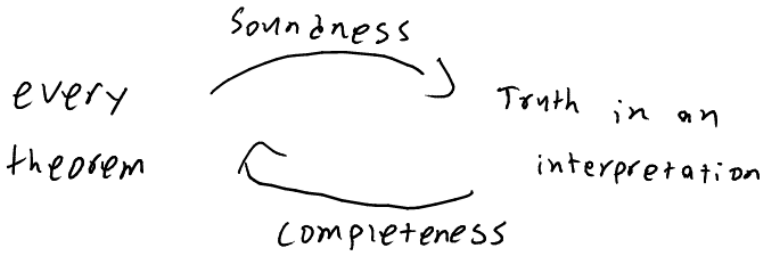
All great circles intersect, no parallels (Elliptic geometry)

- Point -> Point and it's antipode

a)

- Line -> line inside disc
- Point -> point inside the disk

Infinitely many parallel lines (Hyperbolic geom.)



8.2 PQ*-system

- Ax. schema 1: xp-qx-
- IR: xpyqz → xpy-qz-
- Ax. schema 2: xp - qz
- Interpretation:
  - p -> plus
  - q -> equals
  - - -> unit
- -p-q--
- Now, --p-q-- is a thm
- Meaning: 2+1 = 2 false.
- Complete but not sound with respect to interpretation 1 (p -> plus)
  - Different interpretation (2):
    - p -> plus
    - q -> greater or equal
    - - -> unit
    - Sound but not complete with respect to interpretation 2.
      - Ex. ---p--q- is not a theorem, but $3 + 1 \geq 1$ is a truth
      - Axiom schema 2 only gives you things greater by 1
  - Different interpreation (3):

* p -> plus
* q -> greater by 1 or equal
* - -> unit
* Sound and complete with respect to interpretation 3

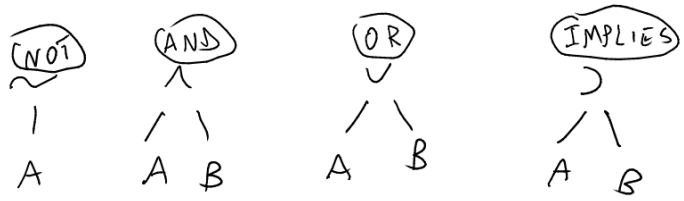
8.3 Propositional Logic

- Today's presentation is harder for those who already know propositional logic, next week will be the standard presentation.

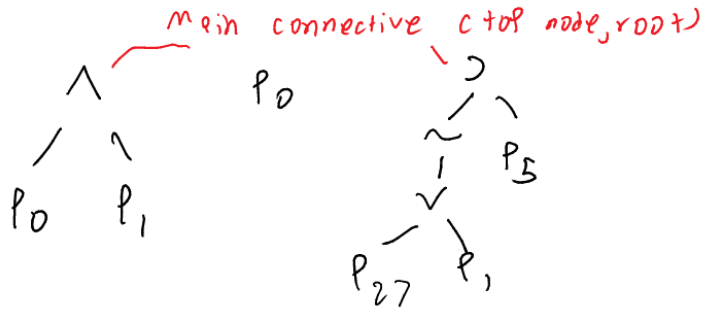
8.3.1 Formula trees:

- Language: Propositional variables: $P_0, P_1, P_2, \ldots$
  - Unary connective: $\sim$ (negation)
  - Binary connectives: $\wedge$ (conjunction)
    * $\vee$ (disjunction)
    * $\supset$ (implication)

1. Inductive Definition
   (a) Base clause: A prop. variable is a formula tree
   (b) Inductive clauses: If A, B are formula trees then



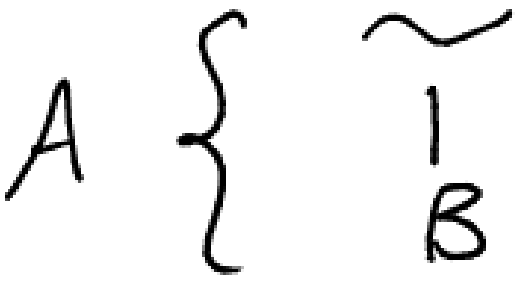
   are also formula trees (with A, B as subtrees)
   (c) Nothing else is a formula tree
2. E.g.



The tree to the right has 5 subtrees (main connective is not a subtree of itself)

3. Truth value assignment A truth value assignment is a function from propositional variables to $\{T, F\}$ (True, False). The truth value of a formula tree A under the truth value assignment f is:

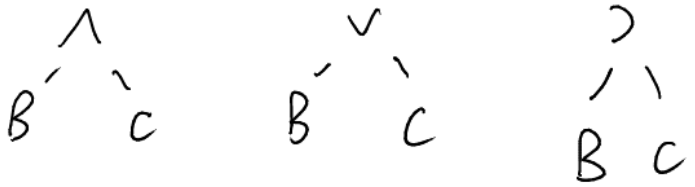
   - Case 1: A is a propositional variable: f(A)
     - E.g. $f(P_0) = T$, $f(P_1) = F$, $f(P_{27}) = T$, $f(P_5) = F$
   - Case 2: A is of the form:



     - Truth values:

B	A
T	F
F	T

   - Case 3: A is of the form



B	C	A_1	A_2	A_3
T	T	T	T	T
T	F	F	T	F
F	T	F	F	T
F	F	F	F	T

9 Lecture 9 *<2017-10-03 Tue>*

9.1 Propositional Logic

Most of this is on handout 2b.

Let's define logic as a formal system.

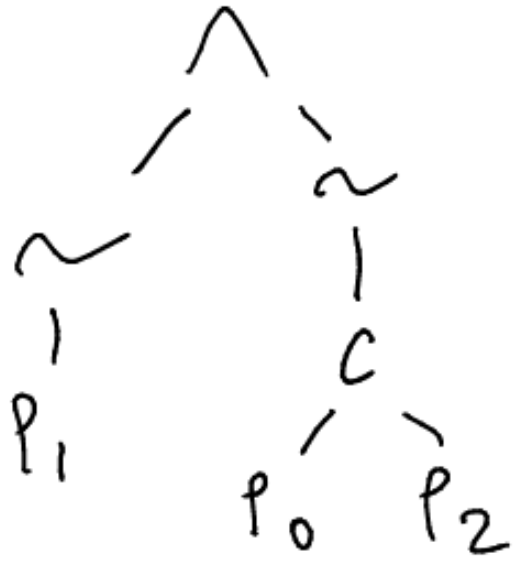
- Alphabet: $P_0, P_1, P_2, \ldots$ ($\aleph_0$ propositional variables)
- Connectives: $\wedge$ (conjunction), $\vee$ (disjunction), $\supset$ (implication), $\sim$ (negation)
- Parentheses

9.1.1 Well-formed formulas (wff)

1. Base clause: P_i is a wff ($i \in \mathbb{N}$) (called atomic)
2. Inductive clause: If A and B are wffs, then so are:
   - $\sim A$ "not"
   - $(A \wedge B)$ "and"
   - $(A \vee B)$ "or"
   - $(A \supset B)$ "implies"
3. Nothing else is.

E.g.

- $P_0 \supset P_1$ is **not well formed**, lack of parentheses.
- $(P_0 \supset P_1)$
- (P_{27}) is **not well formed**, shouldn't have parentheses in atomic form.
- $(\sim P_1 \wedge \sim (P_0 \supset P_2))$
- Can be shown as:



Convention: outer parens are omitted (except if asked for a well formed expression explicitly, as parentheses are required to comply with rules that give us the nice structure)

1. Interpretation Propositional variables $\rightarrow$ truth values:

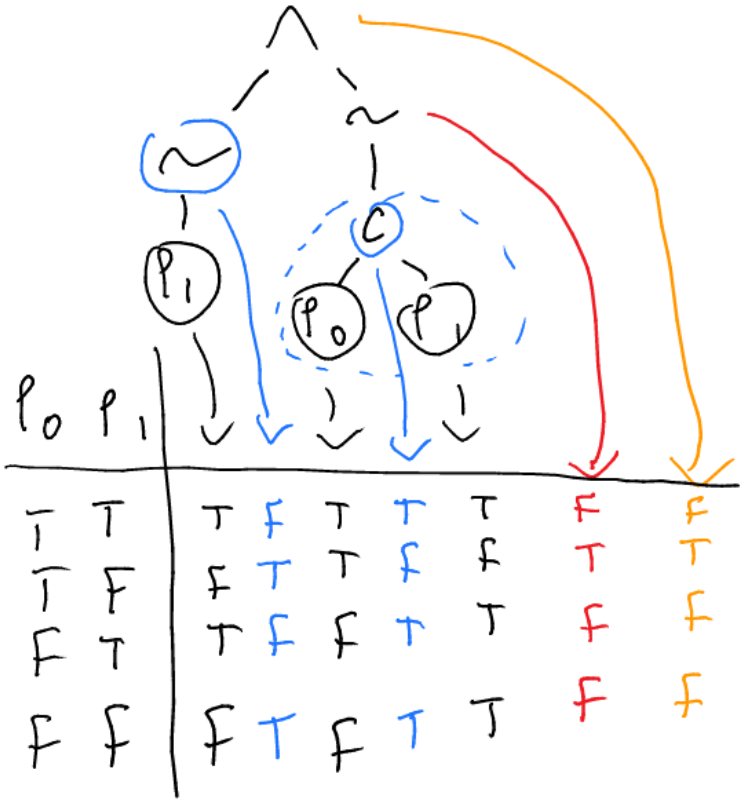
True	False
T	F
1	0
T	$\perp$

(Bivalence)

2. Truth tables A,B (metavariables that stand for wff):

A	B	A ∧ B	A ∨ B	∼ A	A ⊃ B
T	T	T	T	F	T
T	F	F	T	F	F
F	T	F	T	T	T
F	F	F	F	T	T

- $A \supset B$ -> if . . . then . . .
  - A is the antecedent
  - B is the consequent
  - This is material implication, not causal implication
  - The light (B) can be on even if I didn't flip the switch (A)
- Ex.



P_1	$\wedge$	$\sim$	P_1
T	F	F	T
F	F	T	F

P_1	$\vee$	$\sim$	P_1
T	T	F	T
F	T	T	F

Something that is always true is a **tautology**.

- Two wff are logically equivalent if their TV agrees on all possible TV-assignments:

A	B	A $\supset$ B	$\sim$ A $\vee$ B
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Do we read $\sim A \vee B$ as $(\sim A) \vee B$ or $\sim (A \vee B)$?

- $(\sim A) \vee B$ due to the way we defined wff

Minimal sets of connectives:

- $\{\sim, \vee\}$
- $\{\sim, \wedge\}$
- $\{\sim, \supset\}$
- $\Longrightarrow$ Sheffer-Stroke

For a wff with n prop. vars, the truth table has 2^n lines.

Is finding out if a proposition is a tautology decidable or not? Yes, just write out the truth table.

3. Inferences An inference is **valid** if it is impossible for all the premises to be true and the conclusion false at the same time.

	Premises		Conclusion
A	B	A A $\supset$ B	B
T	T	T T	T
T	F	T F	F
F	T	F T	T
F	F	F T	F

This is a valid inference, when both premises are true, the conclusion is also true. Thus:

- A, A $\supset$ B $\models$ B
  - Where $\models$ is the (semantic) consequence
  - Can check if something is semantically implied by checking the truth table and when all premises are true.

Generalizing: $A_1, \ldots A_n \models B$

- $\models$ B (tautology)

4. Natural Deduction (Syntax) Introduced by Gentzen, 1934.
   $\frac{\text{Premises}}{\text{Conclusion}}$
   - $\frac{A \ A \supset B}{B}$ $\supset$ Elimination (Implication Elimination) or MODUS PONENS
   - $\frac{A \ B}{A \wedge B} \wedge$ Introduction (since it introduces conjunction)
   - $\frac{A \wedge B}{A} \wedge$ Elim
   - $\frac{A \wedge B}{B} \wedge$ Elim
     - Not the same as the rule above! You cannot get to B from the first one, you must use this one.
     - Also, $A \wedge B$ and $B \wedge A$ are not the same! They might have the same meaning, but they are different as strings, syntactically
   - $\frac{A}{A \vee B} \vee$ Intro
   - $\frac{A}{B \vee A} \vee$ Intro

   Missing:

   - $\vee$ Elim
   - $\supset$ Intro
   - $\sim$ Intro
   - $\sim$ Elim

10 Lecture 10 *<2017-10-05 Thu>*

10.1 Natural Deduction

- Proof system for propositional logic

- In the land of syntax when we do this
  - Remember that if something looks different, it is different
  - $A \wedge B$ is not the same as $B \wedge A$!

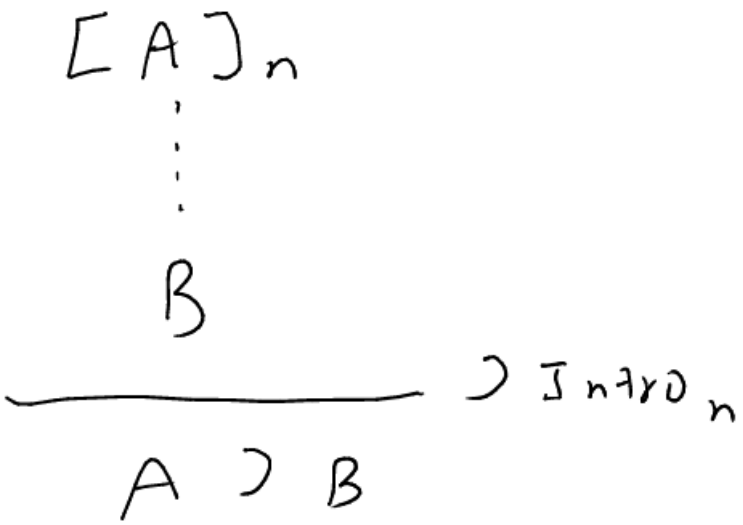
Some rules:

- $\frac{A \ A \supset B}{B} \supset Elim$
- $\frac{A \ B}{A \vee B} \vee Intro$
- $\frac{A \wedge B}{A} \wedge ElimR$
- $\frac{A \wedge B}{B} \wedge ElimL$
- $\frac{A}{A \vee B} \vee Intro$
- $\frac{A}{B \vee A} \vee Intro$

Note that $A, A \supset B \models B$ consists of semantics, not **syntax**. The above rules mentioned are rules to infer other things syntactically.

$\frac{\frac{A \wedge B}{B} \wedge ElimL \ \frac{A \wedge B}{A} \wedge ElimR}{B \wedge A} \wedge Intro$ can be abbreviated as: $A \wedge B \vdash_{ND} B \wedge A$ (ND stands for natural deduction, don't confuse this symbol with the semantic one)

- If you can get from A to B, then you can box A (canceling this assumption A) with a subscript of the amount of steps.

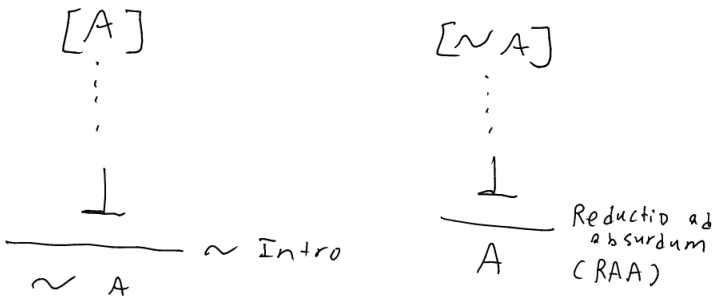


- $\underbrace{\dfrac{\dfrac{[A]_2\ [B]_1}{\frac{B \supset A}{A \supset (B \supset A)}\ \supset Intro_2}}{\vdash_{ND} A \supset (B \supset A)}\ \supset Intro_1}$
  - A and B don't prefix $\vdash$ since they were eliminated (boxed)
  - You can get final result from no assumptions
- $\underbrace{\dfrac{A\ [B]_1}{B \supset A}\ \supset Intro_1}_{A \vdash_{ND} B \supset A}$ `./Images/i16`
- A and B both have subscript 1 because they're eliminated at the same time
- This is like a formal definition for a proof by cases

10.2 Exercise

Prove: $A \vee C, A \supset B, C \supset D \vdash_{ND} B \vee D$ `./Images/i17`

- New symbol: $\perp$ false/falsum
- Generated by:
  - $\frac{A \ \sim A}{\perp} \sim Elim$
- Can use to:
  - $\frac{\perp}{A} Exfalsum$ (can introduce anything)



- RAA is a proof by contradiction.

Prove: $\vdash_{ND} \sim A \supset (A \supset B)$