

# Propositional Logic

Matilde Marcolli

Ma6c: Logic, Caltech, Spring 2026

## Semirings $S = (S, \oplus, \odot, 0_{\oplus}, 1_{\odot})$

- set  $S$  with an addition  $\oplus$  and a multiplication  $\odot$
- $(S, \oplus)$  is a commutative monoid: associative, commutative operation with unit  $0_{\oplus}$

$$(x \oplus y) \oplus z = x \oplus (y \oplus z), \quad x \oplus y = y \oplus x, \quad x \oplus 0_{\oplus} = 0_{\oplus} \oplus x = x$$

- note that *addition does not have an inverse* (there is no  $\ominus$ )
- $(S, \odot)$  is a monoid

$$(x \odot y) \odot z = x \odot (y \odot z), \quad x \odot 1_{\odot} = 1_{\odot} \odot x = x$$

- Note: it may or may not be a commutative semiring
- multiplication distributes over addition

$$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$$

$$(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$$

- $0_{\oplus} \odot x = x \odot 0_{\oplus} = 0_{\oplus}$
- semirings are good as **targets of evaluations**
- smallest semiring is **Boolean semiring**  $\mathbb{B}$

## Boolean semiring


- $\mathbb{B}$  Boolean semiring  $\mathbb{B} = (\{0, 1\}, \max, \cdot, 0, 1)$
- addition is  $\oplus = \max$  and usual multiplication  $\odot = \cdot$
- $0 \oplus 0 = 0$ ,  $0 \oplus 1 = 1 \oplus 0 = 1$  and  $1 \oplus 1 = 1$
- $0 \odot 0 = 0 \odot 1 = 1 \odot 0 = 0$  and  $1 \odot 1 = 1$
- think of  $\{0, 1\}$  as truth values False and True
- can interpret semiring operations  $\oplus = \max$  and  $\odot = \cdot$  as

$$\oplus = \max = \vee = \text{OR} \quad \text{and} \quad \odot = \cdot = \wedge = \text{AND}$$

- truth table


INPUT		OUTPUT
A	B	
0	0	0
1	0	0
0	1	0
1	1	1

AND



INPUT		OUTPUT
A	B	
0	0	0
1	0	1
0	1	1
1	1	1

OR



## Propositions

- “statements that are either true or false”  
*what does this mean?*
- specified alphabet  $\mathcal{A}$  and the set  $\mathcal{W}_{\mathcal{A}}^* := \bigcup_n \mathcal{W}_{\mathcal{A},n}$  of strings  $w = a_1 \dots a_n$  in  $a_i \in \mathcal{A}$  of arbitrary length  $n$
- a subset  $\mathcal{S} \subseteq \mathcal{W}_{\mathcal{A}}^*$  with a map  $\tau : \mathcal{S} \rightarrow \mathbb{B}$  that assigns to a string  $w \in \mathcal{S}$  (a statement) its truth value.
- alphabet  $\mathcal{A}$  consists of two subsets: **propositional variables** represented by letters  $x, y, p, q \dots$  and **logical connectives** (with specific symbols) and words formed by combinations of propositional variables and connectives are **propositional formulae**
- propositional variables also called **atomic formulae** or **atomic propositions**

## connectives: examples

<i>connective</i>	<i>symbol</i>
not (negation)	$\neg$
and (conjunction)	$\wedge$
or (disjunction)	$\vee$
implies (implication)	$\Rightarrow$
iff (equivalence)	$\Leftrightarrow$

**Example:** implication ( $\Rightarrow$ ) is a binary connective (two arguments:  $p \Rightarrow q$ ) that is non-symmetric.

- if  $p$  is true then  $p \Rightarrow q$  is true iff  $q$  is true
- if  $p$  is false then  $p \Rightarrow q$  is “vacuously” true

$P$	$Q$	$P \Rightarrow Q$
$T$	$T$	$T$
$T$	$F$	$F$
$F$	$T$	$T$
$F$	$F$	$T$

**Note:** unlike the intuition about “implication”,  $p \Rightarrow q$  is **not** a causal relation between  $p$  and  $q$

**but** it does mean ruling out the possibility that  $q$  is false when  $p$  is true (as the intuition suggests)

- the set  $\mathcal{S}$  consists of particular strings with specified combination rules between atomic propositions  $P_1, P_2 \dots$  and logical connectives  $C_n^m$  and (balanced) bracketing, so that examples like

$$\phi = C_1^3(P_1, C_2^3(P_2, P_3, P_4))$$

are strings in  $\mathcal{S}$  (formulae or propositions)

- connectives  $C_n^m$  are viewed as functions that input (non-necessarily atomic) formulas in  $\mathcal{S}^m$  and output other formulas in  $\mathcal{S}^n$  with  $m$  inputs and  $n$  outputs

## well formed formulae (WFF)

- 1 every propositional variable  $p$  is a WFF
- 2 if  $X$  is a WFF, then  $\neg X$  is also a WFF
- 3 if  $X, Y$  are WFF, then  $(X \vee Y), (X \wedge Y), (X \Rightarrow Y), (X \Leftrightarrow Y)$  are also WFF

so the WFFs form a subset  $\mathcal{S}_{\text{WFF}} \subseteq \mathcal{S}$  involving only the connectives  $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$

**Boolean formula:** a formula  $\phi \in \mathcal{S}$  that only involves the connectives  $\neg, \wedge, \vee$  (NOT, AND, OR)

## support of a WFF

- set of propositional variables occurring in the formula
- example:

$$\text{supp}(\underbrace{((p \wedge q) \Rightarrow (\neg r \vee p))}_A) = \{p, q, r\}$$

- $\text{supp}(p) = \{p\}$
- $\text{supp}(\neg X) = \text{supp}(X)$
- $\text{supp}(A \star B) = \text{supp}(A) \cup \text{supp}(B)$  for  $\star$  one of the binary connectives  $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$

## Boolean valuations

$\nu$  a valuation mapping propositional variables to truth values,  
 $\nu(p) \in \{0, 1\}$ : extended to formulae by

- $\nu(\neg X) = 1 - \nu(X)$
- $\nu(X \wedge Y) = \nu(X)\nu(Y)$
- $\nu(X \vee Y) = 1 - (1 - \nu(X))(1 - \nu(Y))$
- $\nu(X \Rightarrow Y) = \nu(\neg X \vee Y) = 1 - \nu(X)(1 - \nu(Y))$
- $\nu(X \Leftrightarrow Y) = \nu(X)\nu(Y) + (1 - \nu(X))(1 - \nu(Y))$

if  $\text{supp}(X) = \{p_1, \dots, p_n\}$  then  $\nu(X)$  depends only on the  $\nu(q_i)$ :  
another valuation  $\mu$  with  $\mu(q_i) = \nu(q_i)$  would also have  
 $\mu(X) = \nu(X)$

because writing  $X$  as a WFF in the  $p_i$  and the connectives  
 $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$ , replace everywhere  $q_i$  with  $\nu(q_i)$  then evaluate  
(from left to right) at the values  $\nu(q_i)$  (according to truth table)  
each unary/binary Boolean function defined by a connective ( $\neg b$ ,  
 $a \wedge b$ ,  $a \vee b$ ,  $a \Rightarrow b$ ,  $a \Leftrightarrow b$ , with  $a, b \in \mathbb{B}$ ), get value of  $\nu(X) \in \mathbb{B}$

- a valuation  $\nu$  **models** a WFF  $A$  if  $\nu(A) = 1$  (write  $\nu \models A$ )
- $\nu \not\models A$  if  $\nu(A) = 0$

$$\nu \models \neg A \text{ iff } \nu \not\models A$$

$$\nu \models (A \wedge B) \text{ iff } \nu \models A \text{ and } \nu \models B$$

$$\nu \models (A \vee B) \text{ iff } \nu \models A \text{ or } \nu \models B$$

$$\nu \models (A \Rightarrow B) \text{ iff either } \nu \not\models A \text{ or else } \nu \models B$$

$$\nu \models (A \Leftrightarrow B) \text{ iff } (\nu \models A \text{ and } \nu \models B) \text{ or } (\nu \not\models A \text{ and } \nu \not\models B)$$

- $A =$ **tautology**: for every valuation  $\nu$  have  $\nu(A) = 1$
- $A =$ **satisfiable**: for some valuation  $\nu$  have  $\nu(A) = 1$  (has at least one model)
- otherwise **unsatisfiable** or **contradictory**
- $S$  set of WFFs, then  $\nu \models S$  if  $\nu(A) = 1$  for all  $A \in S$
- $S$  has a model if  $\exists \nu$  with  $\nu \models S$  (i.e.  $S$  is satisfiable, or “simultaneously satisfiable”)

## logical implication

- subset  $S \in \mathcal{S}_{WFF}$  and  $X \in \mathcal{S}_{WFF}$
- $S$  logically implies  $X$  (written  $S \models X$ ) if  $\forall \nu$  with  $\nu \models S$  also  $\nu \models X$  (i.e. if  $\nu(Y) = 1$  for all  $Y \in S$  then  $\nu(X) = 1$ )
- for  $S = \emptyset$  the  $\models X = \emptyset \models X$  means  $X$  is a tautology
- **modus ponens**:  $\{A, A \Rightarrow B\} \models B$
- $S \models (A \Rightarrow B)$  iff  $S \cup \{A\} \models B$
- **logical equivalence**:  $X \equiv Y$  iff  $X \models Y$  and  $Y \models X$  (i.e. if  $X \Leftrightarrow Y$  is a tautology)
- it is an equivalence relation on  $\mathcal{S}_{WFF}$
- **cancellation of double negation**:  $X \equiv \neg\neg X$

## De Morgan laws

①  $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$

②  $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$

- verify for  $p, q$  variables

$$\neg(p \wedge q) \equiv (\neg p \vee \neg q) \quad \text{and} \quad \neg(p \vee q) \equiv (\neg p \wedge \neg q)$$

by same table of truth values as functions  $f : \{0, 1\}^2 \rightarrow \{0, 1\}$

- $X \in \mathcal{S}_{WFF}$  with propositional variables  $q_1, \dots, q_n$ , and  $Y_1, \dots, Y_n \in \mathcal{S}_{WFF}$
- if  $X$  is a tautology then so is the formula obtained by replacing each  $q_i$  by  $Y_i$  (because evaluates true for any T/F value of the  $q_i$  so for any truth output of the  $Y_i$ )
- this suggests: equivalence classes of  $\mathcal{S}_{WFF}$  under logical equivalence  $\equiv$  in terms of Boolean functions (truth tables)

## Boolean functions $f : \{0, 1\}^n \rightarrow \{0, 1\}$

- **Example:** the operations  $\oplus = \vee$  and  $\odot = \wedge$  of the Boolean semiring  $\mathbb{B}$  are an example of binary Boolean functions: inputs are pairs  $(x, y) \in \{0, 1\}^2$  and output value by truth table
- **Example:** Boolean functions  $f : \{0, 1\}^2 \rightarrow \{0, 1\}$  there are 16 possible functions

input	$\langle T, T \rangle$	$\langle T, F \rangle$	$\langle F, T \rangle$	$\langle F, F \rangle$
$f_1^2$	T	T	T	T
$f_2^2$	T	T	T	F
$f_3^2$	T	T	F	T
$f_4^2$	T	T	F	F
$f_5^2$	T	F	T	T
$f_6^2$	T	F	T	F
$f_7^2$	T	F	F	T
$f_8^2$	T	F	F	F
$f_9^2$	F	T	T	T
$f_{10}^2$	F	T	T	F
$f_{11}^2$	F	T	F	T
$f_{12}^2$	F	T	F	F
$f_{13}^2$	F	F	T	T
$f_{14}^2$	F	F	T	F
$f_{15}^2$	F	F	F	T
$f_{16}^2$	F	F	F	F

- can reduce Boolean functions to compositions of simple 2-input functions (logic gates)
- **Example:** some of the 2-input functions (logic gates)

2-input logic gates

Input		Output						
A	B	AND	NAND	OR	NOR	XOR	XNOR	IMPLY
0	0	0	1	0	1	0	1	1
0	1	0	1	1	0	1	0	1
1	0	0	1	1	0	1	0	0
1	1	1	0	1	0	0	1	1

**Example:** Boolean function  $\star(A, B, C)$  of arity  $n = 3$

input	$\star$
$\langle \mathbf{T}, \mathbf{T}, \mathbf{T} \rangle$	<b>T</b>
$\langle \mathbf{T}, \mathbf{T}, \mathbf{F} \rangle$	<b>T</b>
$\langle \mathbf{T}, \mathbf{F}, \mathbf{T} \rangle$	<b>F</b>
$\langle \mathbf{T}, \mathbf{F}, \mathbf{F} \rangle$	<b>F</b>
$\langle \mathbf{F}, \mathbf{T}, \mathbf{T} \rangle$	<b>F</b>
$\langle \mathbf{F}, \mathbf{T}, \mathbf{F} \rangle$	<b>T</b>
$\langle \mathbf{F}, \mathbf{F}, \mathbf{T} \rangle$	<b>F</b>
$\langle \mathbf{F}, \mathbf{F}, \mathbf{F} \rangle$	<b>F</b>

can equivalently be written as

$$\star(A, B, C) = (A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C)$$

involving only the connectives  $\neg, \vee, \wedge$

## Boolean functions and Boolean formulae

- Boolean function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  organize as a truth table: input/output

$$(x_1, \dots, x_n) \in \{0, 1\}^n \mapsto f(x_1, \dots, x_n) \in \{0, 1\}$$

- Boolean functions

$$\wedge : \{0, 1\}^2 \rightarrow \{0, 1\}, \quad \vee : \{0, 1\}^2 \rightarrow \{0, 1\}, \quad \neg : \{0, 1\} \rightarrow \{0, 1\}$$

(truth tables of connectives  $\wedge, \vee, \neg$ )

- **algorithm** for writing  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  as a composition of the  $\wedge, \vee, \neg$  Boolean functions:

①  $\mathcal{I}_T = f^{-1}(1) \subset \{0, 1\}^n$

② for each  $a \in \mathcal{I}_T$  take the function  $f_a : \{0, 1\}^n \rightarrow \{0, 1\}$

$$f_a(x_1, \dots, x_n) = \bigwedge_{j \in J_{T,a}} x_j \wedge \bigwedge_{i \in J_{F,a}} \neg x_i$$




$$J_{T,a} = \{j \in \{1, \dots, n\} \mid a_j = 1\} \quad J_{F,a} = \{j \in \{1, \dots, n\} \mid a_j = 0\}$$

- ③ then have the Boolean function





$$\bigvee_{a \in \mathcal{I}_T} f_a(x_1, \dots, x_n) = f(x_1, \dots, x_n)$$

## Boolean Functions and Circuits

- by previous argument can write Boolean functions  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  as compositions of the unary and binary Boolean functions  $\neg, \wedge, \vee$
- realize each Boolean function as a **circuit**: a directed graph with vertices decorated by operations with inputs incoming edges and output single outgoing edge (single valued functions)
- all vertices have either one or two inputs and are decorated by an operation that is either  $\neg$  or  $\wedge$  or  $\vee$
- each such operation represented by a **logical gate**

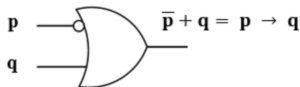
Logic Gate	Symbol	OCR Notation
AND		$A \wedge B$
OR		$A \vee B$
NOT		$\neg A$

other logic gates (obtainable from  $\neg, \wedge, \vee$  but with own notation)

NAND		$\neg(A \wedge B)$
NOR		$\neg(A \vee B)$
XOR		$A \underline{\vee} B$
XNOR		$\neg(A \underline{\vee} B)$

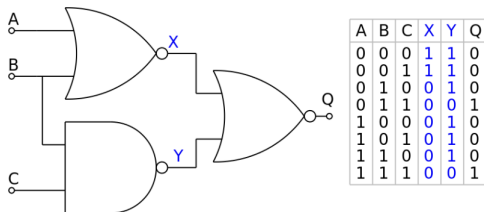
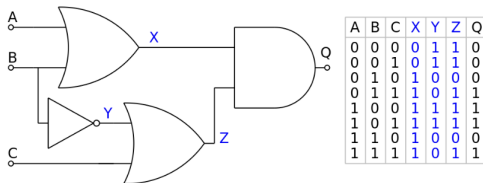
- XOR (exclusive OR):  $A \text{ XOR } B = (A \vee B) \wedge \neg(A \wedge B)$
- XNOR = NOT XOR
- implication  $A \Rightarrow B$  gate

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

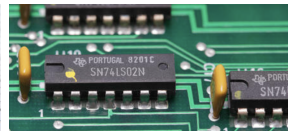
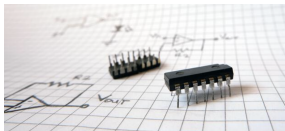


$$(A \Rightarrow B) \equiv (B \vee \neg A)$$

## circuits: examples



fundamental building blocks of digital electronics



## Other complete sets of gates

- $\{\neg, \wedge\}$  and  $\{\neg, \vee\}$  are complete sets
- to see can reduce from  $\{\neg, \wedge, \vee\}$  to just  $\{\neg, \wedge\}$  use De Morgan's law

$$X \vee Y \equiv \neg(\neg X \wedge \neg Y)$$

similar for reducing to  $\{\neg, \vee\}$

- or can use  $\{\neg, \Rightarrow\}$ , also complete because

$$X \vee Y \equiv \neg X \Rightarrow Y$$

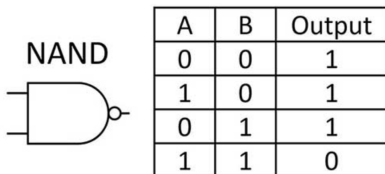
- example **not** complete:  $\{\neg, \Leftrightarrow\}$  because there binary  $f : \{0, 1\}^2 \rightarrow \{0, 1\}$  truth table of  $X(p, q)$  with only  $\neg, \Leftrightarrow$  gates has values satisfying

$$X(1, 1) + X(0, 0) + X(1, 0) + X(0, 1) = 0 \in \mathbb{Z}/2\mathbb{Z}$$

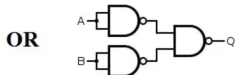
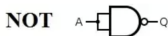
- true for  $X = p$  or  $X = q$ ; true for  $X \equiv \neg Y$  if true for  $Y$ , true for  $X \equiv (A \Leftrightarrow B)$  if true for  $A$  and  $B$  (check by truth table), so inductively true
- so cannot get  $X = p \wedge q$  because sum is 1

## NAND gate

in fact can generate Boolean functions as circuits with a single gate NAND



$$\neg X = X \text{ NAND } X \quad X \vee Y = (X \text{ NAND } X) \text{ NAND } (Y \text{ NAND } Y)$$



## truth-function analysis of propositional logic

- $\mathbb{B}\mathcal{F}$  = set of Boolean functions,  $\tau : \mathcal{S} \rightarrow \mathbb{B}\mathcal{F}$
- $\tau$  assigns  $n$ -ary truth functions  $f_X : \{0, 1\}^n \rightarrow \{0, 1\}$  to  $n$ -ary propositional connectives  $C^n = C_1^n$  (truth table)
- given a formula  $X \in \mathcal{S}$  that has  $n$  inputs (formula variables)  $p_i$  and  $\tau(X) = f_X : \{0, 1\}^n \rightarrow \{0, 1\}$  the associated truth value function
  - 1  $X$  is a **classical propositional validity** if it evaluates to 1 (T true) for **every** possible assignment of Boolean values to the atomic propositional variables (tautology)
  - 2  $X$  is **classically satisfiable** if it evaluates to 1 (T true) for **some** assignment (satisfiable)
  - 3  $X$  is **classically unsatisfiable** otherwise (it evaluates 0(F) on all assignments, contradictory)
  - 4  $X$  is a **classical propositional consequence** of  $Y$  if on every assignment of Boolean values to the variables of  $X$  and  $Y$  where  $Y$  evaluates as 1(T)  $X$  cannot evaluate as 0(F) ( $\models$ )
  - 5  $X$  is a **classical propositional equivalent** of  $Y$  if  $X$  and  $Y$  evaluate 1(T) on the same assignments of values to the atoms ( $\equiv$ )

## Connectives and Boolean formulae

- **connective**  $C_n$  with  $n$  inputs, specified via its **truth table**

$$(p_1, \dots, p_n) \in \{T, F\}^n \mapsto C_n(p_1, \dots, p_n) \in \{T, F\}$$

- **algorithm** for realizing  $C_n$  as a Boolean formula: apply algorithm that associates to the truth table seen as a Boolean function  $f_{C_n} : \{T, F\}^n \rightarrow \{T, F\}$  an expression that uses only compositions of Boolean functions  $\neg, \wedge, \vee$
- seen as truth table of a Boolean formula
- then realization of Boolean functions via a complete set of gates becomes logical equivalence of formulae  $X \in \mathcal{S}$  to formulae in  $\mathcal{S}_{WFF}$  or to Boolean formulae or to those generated by a chosen complete set of connectives
- for example: realizing as Boolean formula (reformulation of algorithm described for Boolean functions in terms of logical connectives)

## Connectives as Boolean formulae

**algorithm** for realizing  $C_n$  as a Boolean formula

- 1 to each row  $k \in \mathcal{I}_T \subset \{1, \dots, 2^n\}$  of the truth table of  $C_n$  for which the output is  $T = \text{true}$ , assign a Boolean formula of the form

$$\mathcal{B}_k = \bigwedge_{j \in J_{T,k}} p_j \wedge \bigwedge_{i \in J_{F,k}} \neg p_i$$

with  $J_{T,k} \subset \{1, \dots, n\}$  the set of  $p_j$  that are valued  $T$  in the  $k$ -th row of the truth table and  $J_{F,k} = \{1, \dots, n\} \setminus J_{T,k}$  the set of those that are valued  $F$

- 2 then combine the Boolean formula  $\mathcal{B}_k$  associated to the rows of the truth table into a single formula

$$\mathcal{B} = \bigvee_{k \in \mathcal{I}_T} \mathcal{B}_k$$

## Boolean algebras $(\mathcal{B}, \leq, \wedge, \vee, \neg)$ or $(\mathcal{B}, \wedge, \vee, \neg, 0, 1)$

(complemented distributive lattice)

- partially ordered set  $(\mathcal{B}, \leq)$ :
  - reflexivity  $a \leq a$ ; anti-symmetry: if  $a \leq b$  and  $b \leq a$  then  $a = b$ ;
  - transitivity: if  $a \leq b$  and  $b \leq c$  then  $a \leq c$
- two associative and commutative operations,  $\wedge$  and  $\vee$
- if  $a_1 \leq a_2$  and  $b_1 \leq b_2$  then  $a_1 \vee b_1 \leq a_2 \vee b_2$  and  $a_1 \wedge b_1 \leq a_2 \wedge b_2$
- idempotent:  $a \wedge a = a$  and  $a \vee a = a$
- absorption law:  $a \vee (a \wedge b) = a$  and  $a \wedge (a \vee b) = a$
- distributivity:  $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$  and  $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
- least element 0 and greatest element 1 with  $a \vee 0 = a$  and  $a \vee 1 = 1$ , and  $a \wedge 0 = 0$  and  $a \wedge 1 = a$
- complement:  $\neg a$  with  $a \vee \neg a = 1$  and  $a \wedge \neg a = 0$
- also satisfy **De Morgan law**

$$\neg a \wedge \neg b = \neg(a \vee b) \quad \neg a \vee \neg b = \neg(a \wedge b)$$

## Boolean algebra structure

$$a \vee (b \vee c) = (a \vee b) \vee c$$

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

associativity

$$a \vee b = b \vee a$$

$$a \wedge b = b \wedge a$$

commutativity

$$a \vee (a \wedge b) = a$$

$$a \wedge (a \vee b) = a$$

absorption

$$a \vee 0 = a$$

$$a \wedge 1 = a$$

identity

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

distributivity

$$a \vee \neg a = 1$$

$$a \wedge \neg a = 0$$

complements















**Concrete Boolean algebras:** set theoretic operations

- a given set  $\mathcal{X}$  and a subset  $\mathcal{B} \subset 2^{\mathcal{X}}$  (where  $2^{\mathcal{X}}$  power set, set of all subsets of  $\mathcal{X}$ ) such that  $\mathcal{B}$  is closed under union, intersection, complement, containing  $\mathcal{X}$  and  $\emptyset$
- for instance  $\mathcal{B} = 2^{\mathcal{X}}$
- then taking, for  $A, B \in \mathcal{B}$

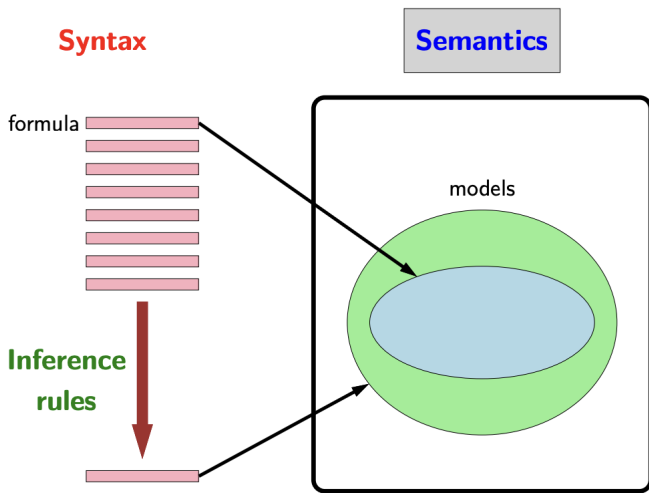
$$A \wedge B := A \cap B \quad A \vee B := A \cup B \quad \neg A = A^c = \mathcal{X} \setminus A$$

- and partial order on  $\mathcal{B}$  by inclusion  $A \leq B := A \subseteq B$
- $0 = \emptyset$  and  $1 = \mathcal{X}$
- satisfies all properties of Boolean algebra

**semantics:** all logical gates and circuits acquire set-theoretic interpretation

Expression	Symbol	Venn diagram	Boolean algebra	Values		
				A	B	Output
AND			$A \cdot B$	0	0	0
				0	1	0
				1	0	0
				1	1	1
				1	1	1
OR			$A + B$	A	B	Output
				0	0	0
				0	1	1
				1	0	1
				1	1	1
XOR			$A \oplus B$	A	B	Output
				0	0	0
				0	1	1
				1	0	1
				1	1	0
NOT			$\bar{A}$	A		Output
				0	1	
				1	0	
NAND			$\overline{A \cdot B}$	A	B	Output
				0	0	1
				0	1	1
				1	0	1
				1	1	0
NOR			$\overline{A + B}$	A	B	Output
				0	0	1
				0	1	0
				1	0	0
				1	1	0
XNOR			$\overline{A \oplus B}$	A	B	Output
				0	0	1
				0	1	0
				1	0	0
				1	1	1

# Propositional logic



## Semantics of Propositional Logic

- already seen that **valuations**  $\nu : \{p_1, p_2, \dots\} \rightarrow \{0, 1\}$  assigning truth values to propositional variables give an assignment of truth values to propositions  $X \in \mathcal{S}$

$$\nu : \mathcal{S} \rightarrow \mathbb{B}$$

- with  $\nu^{-1}(1) = \{X \in \mathcal{S} \mid \nu \models X\}$  and  $\nu(X) = \nu(Y)$  for  $X \equiv Y$
- the Boolean semiring  $\mathbb{B}$  is an example of a Boolean algebra
- a valuation  $\nu : \mathcal{S} \rightarrow \mathbb{B}$  “interprets” propositions in  $\mathbb{B}$  (as true or false)
- more generally **Boolean algebras** provide **semantics** for propositional logic: **key idea**:
  - 1 equivalence classes of propositions  $\mathcal{S}/\equiv$  under the logical equivalence relation (different syntax same semantics) form a Boolean algebra
  - 2 Boolean homomorphisms  $\mathcal{S}/\equiv \rightarrow \mathcal{B}$  to a Boolean algebra are a choice of semantics
  - 3 in particular truth values by  $\nu : \mathcal{S}/\equiv \rightarrow \mathbb{B}$

## Propositional Logics

- **syntax** of propositional logic: symbols (variables and connectives) and rules for well formed expressions
- **semantics**: assignment of “meaning” to propositions (including logical implications)
- **deduction function**: mapping  $X \in \mathcal{S}$  to “set of consequences” of  $X$  (varying possible deduction functions)
- **a propositional logic**:  $\text{Prop}(\Pi, \Theta)$  with  $\Pi$  in syntax and  $\Theta$  in semantics
- $\Pi = \{p_1, p_2, \dots\}$  (propositional variables, atoms of syntax)
- connectives: assume  $\neg, \wedge, \vee$  (but can use other complete set)
- $\Theta \subset \mathcal{S}$  a set of formulae: a **theory**

- **Example:** with  $\Pi = \{p_1, p_2, \dots\}$  one can take

$$\Theta = \{\neg p_j \vee \neg p_k \mid j \neq k\}$$

so this expresses a rule that at most one of the propositional variables (atoms) can be assigned value “true”

- the formulae in  $\Theta$  are **equations** constraining valuations  $\nu$
- $\nu : \mathcal{S} \rightarrow \mathbb{B}$  from valuation is a  **$\Theta$ -truth function** if:
  - $\nu \models \Theta$ : for any  $X \in \Theta$  have  $\nu(X) = 1$  (solve the equations)
  - $\nu(\neg X) = \neg \nu(X)$  (where  $\neg 0 = 1$  and  $\neg 1 = 0$  in  $\mathbb{B}$ )
  - $\nu(\bigvee_{a \in \mathcal{I}} X_a) = 1$  if  $\exists a \in \mathcal{I}$  with  $\nu(X_a) = 1$  and  $\nu(\bigvee_{a \in \mathcal{I}} X_a) = 0$  otherwise
  - $\nu(\bigwedge_{a \in \mathcal{I}} X_a) = 1$  if  $\nu(X_a) = 1, \forall a \in \mathcal{I}$ , and  $\nu(\bigwedge_{a \in \mathcal{I}} X_a) = 0$  otherwise
  - these three properties:  $\nu$  compatible with truth table of  $\neg, \wedge, \vee$  (ok if build  $\nu$  from valuation on atoms via these truth tables)
- when  $\Theta = \emptyset$  just arbitrary truth functions  $\nu : \mathcal{S} \rightarrow \mathbb{B}$  (arbitrary valuations) with no constraints

- a set  $S \subset \mathcal{S}$  is  **$\Theta$ -satisfiable** iff  $S \cup \Theta$  is satisfiable  
( $\exists \nu \models S \cup \Theta$ )
- $S \models_{\Theta} X$ : a set  $S \subset \mathcal{S}$   **$\Theta$ -logically-implies**  $X \in \mathcal{S}$  iff  
 $S \cup \Theta \models X$
- **$\Theta$ -logical-equivalence**:  $X \equiv_{\Theta} Y$  if  $X \models_{\Theta} Y$  and  $Y \models_{\Theta} X$
- $\Theta$ -logical-equivalence compatible with connectives: if  $X \equiv_{\Theta} Y$   
and  $A \equiv_{\Theta} B$  then  $\neg X \equiv \neg Y$  and  $X \vee A \equiv_{\Theta} Y \vee B$  and  
 $X \wedge A \equiv_{\Theta} Y \wedge B$  (valuations  $\nu$ 's are)
- so connectives pass to the quotient by the equivalence relation  
 $\mathcal{S}/\equiv_{\Theta}$
- $\Theta$ -truth functions also pass to quotient  $\nu : \mathcal{S}/\equiv_{\Theta} \rightarrow \mathbb{B}$
- set of equivalence classes

$$\mathcal{L}_{\Theta} = \mathcal{S}/\equiv_{\Theta} \quad \mathcal{L} = \mathcal{S}/\equiv$$

depend on set  $\Pi$  of atoms  $\mathcal{L}_{\Theta}(\Pi)$

## clauses (some terminology)

- **literal** = a propositional variable (atom)  $p$  or its negation  $\neg p$
- notation: write  $l$  for literal and  $\bar{l} := \neg l$
- **clause** = a formula  $l_1 \vee \dots \vee l_n$
- **positive clause**  $p_1 \vee \dots \vee p_n$  (no  $\neg p$  involved)
- **empty clause**: symbol  $\square$  (and symbol  $\top = \neg \square$ )
- complete set of connectives  $\{\neg, \vee\}$ : every  $X \in \mathcal{P}$  is  $X \equiv_{\Theta} Y$  for some  $Y = \alpha_1 \vee \dots \vee \alpha_r$  with  $\alpha_i$  clauses (conjunction of clauses)
- $X \subseteq Y$ : clause  $X$  **subsumes** clause  $Y$  if  $\exists l_i$  literals,

$$Y = X \vee l_1 \vee \dots \vee l_n$$

## deduction function

- power set  $\mathcal{P}(S) = 2^S$  (set of all subsets)
- $\mathcal{Cl}$  set of clauses
- **deduction function**:  $\mathcal{D} : \mathcal{P}(\mathcal{Cl}) \rightarrow \mathcal{P}(\mathcal{Cl})$
- notation:  $S \subset \mathcal{Cl}$  set of clauses, then for  $X \in \mathcal{D}(S)$  write  $S \vdash_{\mathcal{D}} X$ ,  $X$   $\mathcal{D}$ -deduced from  $S$

## resolvent

- $p \in \Pi$  atom

$$\mathcal{R}_p : \mathcal{Cl} \times \mathcal{Cl} \rightarrow \mathcal{Cl}$$

$$\mathcal{R}_p(X \vee p, Y \vee \neg p) = X \vee Y$$

with  $\mathcal{R}_p(p, Y \vee \neg p) = Y$  and  $\mathcal{R}_p(X \vee p, \neg p) = X$  and  $\mathcal{R}_p(p, \neg p) = \square$

## $\Theta$ -resolution deduction function

$$\mathcal{R}_\Theta : \mathcal{P}(\mathcal{Cl}) \rightarrow \mathcal{P}(\mathcal{Cl})$$

for  $S \subseteq \mathcal{Cl}$  the image  $\mathcal{R}_\Theta(S)$  is constructed inductively by

- 1  $S \cup \Theta \subseteq \mathcal{R}_\Theta(S)$
- 2 if  $A, B \in \mathcal{R}_\Theta(S)$  and  $X = \mathcal{R}_p(A, B)$  for some  $p \in \Pi$  then  $X \in \mathcal{R}_\Theta(S)$

$$\mathcal{R} = \mathcal{R}_{\Theta=\emptyset}$$

always have  $\Theta \subseteq \mathcal{R}_\Theta(S)$

Equivalent description of  $\mathcal{R}_\Theta(S)$

- $X \in \mathcal{R}_\Theta(S)$  iff  $\exists$  sequence  $X_1, \dots, X_m = X$  such that each  $X_i$  is either in  $S \cup \Theta$  or  $\exists j, k < i$  such that  $X_i = \mathcal{R}_p(X_j, X_k)$
- such a sequence  $X_1, \dots, X_m = X$  is a  $\mathcal{R}_\Theta$ -deduction of  $X$  from  $S$  (or a  $\mathcal{R}_\Theta$ -derivation of  $X$  from  $S$ )

## Deduction vs Logical Implication

- both describe a “something follows from something” relation, but depend on different data
- deduction function is a “syntactic approach” while logical implication is a “semantic approach”
- deduction function  $\mathcal{D}$  is **strongly  $\Theta$ -sound** if for all  $S \subset \mathcal{Cl}$  and any  $X \in \mathcal{Cl}$

$$\text{if } S \vdash_{\mathcal{D}} X \text{ then } S \models_{\Theta} X$$

- a weaker notion of soundness:  $\mathcal{D}$  is **refutation  $\Theta$ -sound** if for all  $S \subset \mathcal{Cl}$

$$\text{if } S \vdash_{\mathcal{D}} \square \text{ then } S \models_{\Theta} \square$$

- **example**  $\mathcal{D}_p(S) = S \cup \{p\}$  is refutation sound not strongly sound: if  $S \vdash_{\mathcal{D}_p} \square$  then  $\square \in S$  so  $S \models \square$ , but if  $S = \{q\}$  with  $q \neq p$  then  $S \vdash_{\mathcal{D}_p} p$  but  $S \not\models p$

- deduction function  $\mathcal{D}$  is **strongly  $\Theta$ -complete** if for all  $S \subset \mathcal{Cl}$  and any  $X \in \mathcal{Cl}$

$$\text{if } S \models_{\Theta} X \text{ then } S \vdash_{\mathcal{D}} X$$

- deduction function  $\mathcal{D}$  is **refutation  $\Theta$ -complete** if for all  $S \subset \mathcal{Cl}$

$$\text{if } S \models_{\Theta} \square \text{ then } S \vdash_{\mathcal{D}} X$$

- Main interesting case:** the  $\Theta$ -resolution deduction function  $\mathcal{R}_{\Theta}$  is both strongly  $\Theta$ -sound and refutation  $\Theta$ -complete

- case of  $\Theta = \emptyset$  is a result of Robinson (1955) and also follows from a result of Quine (1955)
- other  $\Theta$  reducible to  $\Theta = \emptyset$ : for soundness  $S \vdash_{\mathcal{R}_{\Theta}} X$  is  $S \cup \Theta \vdash_{\mathcal{R}} X$  and  $\mathcal{R}$  is sound so  $S \cup \Theta \models X$ ; for refutation completeness if  $S \cup \Theta \models \square$  then  $S \cup \Theta \vdash_{\mathcal{R}} \square$  which is  $S \vdash_{\mathcal{R}_{\Theta}} X$

## Lindenbaum algebra of a theory $\Theta$    Boolean algebra

$$\mathfrak{L}_\Theta = (\mathcal{L}_\Theta = \mathcal{S}/\equiv_\Theta, \vee, \wedge, \neg, \square, \top)$$

- **Boolean homomorphism**

$$f : (\mathcal{B}, \vee, \wedge, \neg, 0, 1) \rightarrow (\mathcal{B}', \vee', \wedge', \neg', 0', 1')$$

- map of sets  $f : \mathcal{B} \rightarrow \mathcal{B}'$  with

- $f(a \wedge b) = f(a) \wedge' f(b)$ ;  $f(a \vee b) = f(a) \vee' f(b)$ ;

$$f(\neg a) = \neg' f(a); f(0) = 0'; f(1) = 1'$$

- Boolean isomorphism if  $f : \mathcal{B} \rightarrow \mathcal{B}'$  is bijection

- $\mathcal{B}$  and  $\mathcal{B}'$  Boolean algebras:  $\text{BoolHom}(\mathcal{B}, \mathcal{B}')$  set of all Boolean homomorphisms  $f : \mathcal{B} \rightarrow \mathcal{B}'$

## $\Theta$ -truth functions and Boolean homomorphisms

- $\Theta\mathcal{F}$  = set of  $\Theta$ -truth functions
- map  $BH : \Theta\mathcal{F} \rightarrow \text{BoolHom}(\mathcal{L}_\Theta, \mathbb{B})$

$$BH(\nu)([X]_\Theta) := \nu(X)$$

for  $[X]_\Theta \in \mathcal{L}_\Theta = \mathcal{S}/\equiv_\Theta$

- **Claim:** the map  $BH$  is a bijection
  - $BH$  well defined: if  $X \equiv_\Theta Y$  then for  $\nu \in \Theta\mathcal{F}$  have  $\nu(X) = \nu(Y)$
  - $BH(\nu)$  is Boolean homomorphism because seen that  $\nu : \mathcal{S} \rightarrow \mathbb{B}$  exchanges  $\wedge, \vee, \neg$  on  $\mathcal{S}$  with  $\wedge, \vee, \neg$  on  $\mathbb{B}$
  - bijection:  $BH$  has an inverse obtained by assigning to Boolean homomorphism  $g : \mathcal{L}_\Theta \rightarrow \mathbb{B}$  the function  $\nu_g(X) := g([X]_\Theta)$

## $\Theta$ -truth functions and Boolean atoms

- Boolean algebra  $(\mathcal{B}, \vee, \wedge, \neg, 0, 1)$  (or equivalently  $(\mathcal{B}, \leq, \vee, \wedge, \neg)$ )
- **Boolean atom**  $a \in \mathcal{B}$ ,  $a \neq 0$ :  
if  $x \leq a$  then either  $x = a$  or  $x = 0$
- **set of Boolean atoms**:  $\text{BAtm}(\mathcal{B})$
- **examples** in  $\mathcal{B} = 2^{\mathcal{X}} = \mathcal{P}(\mathcal{X})$  power set,  
 $\text{BAtm}(\mathcal{P}(\mathcal{X})) = \{S = \{x\} \mid x \in \mathcal{X}\}$  (singleton sets are atoms); in Boolean semiring  $\mathbb{B} = \{0, 1\}$  set  $\text{BAtm}(\mathbb{B}) = \{1\}$
- $\text{BAtm}(\mathcal{L}_\Theta)$  Boolean atoms of the Lindenbaum algebra
- Note: these Boolean atoms *not* same as propositional atoms
- **Stone representation** (finite case):  $\mathcal{B}$  finite Boolean algebra and Boolean algebra  $\mathcal{P}(\text{BAtm}(\mathcal{B}))$

$$h_{\mathcal{B}} : \mathcal{B} \rightarrow \mathcal{P}(\text{BAtm}(\mathcal{B}))$$

$$h_{\mathcal{B}}(x) = \{a \in \text{BAtm}(\mathcal{B}) \mid a \leq_{\mathcal{B}} x\}$$

this map is a Boolean isomorphism

## Characteristic function $\mathcal{B}$ finite Boolean algebra

$$\chi : \text{BAtm}(\mathcal{B}) \rightarrow \text{BoolHom}(\mathcal{B}, \mathbb{B})$$

$$\chi(a)(x) = \begin{cases} 1 & a \leq_{\mathcal{B}} x \\ 0 & \text{otherwise} \end{cases}$$

- $\chi(a)$  is indeed a Boolean homomorphism: enough to show  $\neg$  and  $\vee$  preserved (complete set):
  - $\chi(a)(x \vee y) = 1$  iff  $a \leq x \vee y$  iff  $a \leq x$  or  $a \leq y$  (for atom iff  $\chi(a)(x) = 1$  or  $\chi(a)(y) = 1$ ) iff  $\chi(a)(x) \vee \chi(a)(y) = 1$
  - $\chi(a)(\neg x) = 1$  iff  $a \leq \neg x$  iff  $a \not\leq x$  (for an atom  $a$ , for any  $x$  either  $a \leq x$  or  $a \leq \neg x$  but not both) iff  $\neg(\chi(a)(x)) = 1$

## characteristic function $\chi$ is a bijection

- **injectivity**

- if  $\chi(a)(x) = \chi(b)(x)$  for all  $x \in \mathcal{B}$  then  $a \leq x$  iff  $b \leq x$
- in particular for  $x = b$  get  $b \leq b$  (reflexivity of  $\leq$ ) and  $a \leq b$
- for  $x = a$  also get  $b \leq a$ : anti-symmetry of  $\leq$  gives  $a = b$

- **surjectivity**

- $f \in \text{BoolHom}(\mathcal{B}, \mathbb{B})$  take  $f^{-1}(1)$  and (assuming  $\mathcal{B}$  is finite)

$$a = \bigwedge_{x \in f^{-1}(1)} x$$

- also  $a = \bigvee_{b \in h_{\mathcal{B}}(a)} b$  and  $f(a) = \bigvee_{b \in h_{\mathcal{B}}(a)} f(b) = 1$
- so there is at least one  $b' \in h_{\mathcal{B}}(a)$  with  $f(b') = 1$ , so  $b' \in f^{-1}(1)$  and  $a \leq b'$
- also  $b' \leq \bigvee_{b \in h_{\mathcal{B}}(a)} b = a$  so  $b' \leq a$ : anti-symmetry  $a = b'$
- so  $a$  Boolean atom
- also  $f(x) = 1$  iff  $x \in f^{-1}(1)$  iff  $a \leq x$  iff  $\chi(a)(x) = 1$  so  $\chi(a) = f$

- **consequence:** if  $f \in \text{BoolHom}(\mathcal{B}, \mathbb{B})$  has  $f(a) = 1$  for  $a \in \text{BAtm}(\mathcal{B})$  then  $f = \chi(a)$
- i.e. for any  $f \in \text{BoolHom}(\mathcal{B}, \mathbb{B})$  there is a unique atom  $a \in f^{-1}(1)$  (and  $f = \chi(a)$ )

### $\Theta$ -truth functions and atoms of the Lindenbaum Boolean algebra

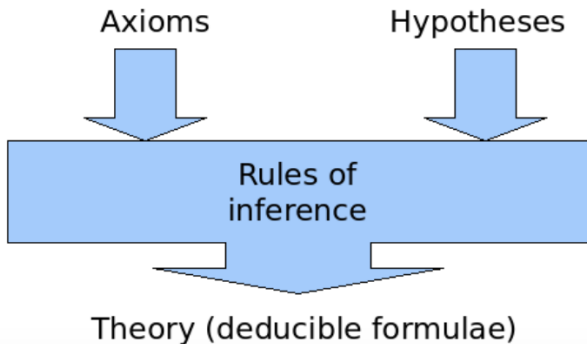
- assume  $\Pi$  finite set so get finite Boolean algebra  $\mathcal{L}_\Theta(\Pi)$
- $\Theta$ -truth functions, already know  $\Theta\mathcal{F} \cong \text{BoolHom}(\mathcal{L}_\Theta, \mathbb{B})$  so can also identify with  $\text{BAtm}(\mathcal{L}_\Theta)$  via isomorphism

$$\chi : \text{BAtm}(\mathcal{L}_\Theta) \rightarrow \Theta\mathcal{F}$$

$$\chi([X]_\Theta)(Y) = 1 \quad \text{iff} \quad X \models_\Theta Y$$

and  $\chi([X]_\Theta)(Y) = 0$  otherwise

## Proof systems for Propositional Logic



## Hilbert Proof System

- another formulation of deduction (instead of deduction functions on clauses  $\mathcal{D} : \mathcal{P}(\mathcal{Cl}) \rightarrow \mathcal{P}(\mathcal{Cl})$ )
- **formal language in alphabet:**  
 $\mathcal{A} = \{\neg, \Rightarrow, \wedge, \vee, (, p_1, p_2, \dots, p_n, \dots\}$
- using  $\{\neg, \Rightarrow\}$  complete set, so that

$$A \wedge B = \neg(A \Rightarrow \neg B), \quad A \vee B = (\neg A \Rightarrow B)$$

$$A \Leftrightarrow B = \neg((A \Rightarrow B) \Rightarrow \neg(B \Rightarrow A))$$

- a set of three **logical axioms** (tautologies) Mendelson's version
  - 1  $A \Rightarrow (B \Rightarrow A)$
  - 2  $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
  - 3  $((\neg B \Rightarrow \neg A) \Rightarrow ((\neg B \Rightarrow A) \Rightarrow B))$
- **inference rule:**  $\{A, A \Rightarrow B\} \models B$  **modus ponens**

$$\frac{A, A \Rightarrow B}{B}$$

## formal proof from $S$ $S \vdash A$

- set of formulae  $S$  (set of strings in the formal language)
- formal proof from  $S$  in the Hilbert Proof System is
  - a string  $A_i$  of formulae  $A_1, A_2, \dots, A_n = A$
  - each  $A_i$  is either a logical axiom, or an element of  $S$ , or the result of applying modus ponens (for some  $j, k < i$ )

$$\frac{A_j, A_k}{A_i}$$

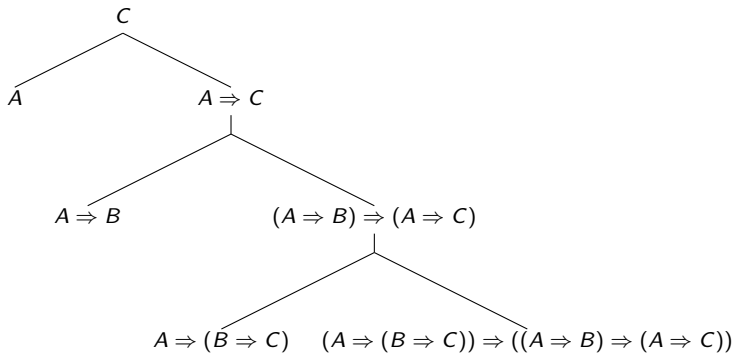
- equivalently if  $\exists j, k < i$  with  $A_k = (A_j \Rightarrow A_i)$

**Example**  $S = \{(A \Rightarrow B), A \Rightarrow (B \Rightarrow C), A\}$

1.  $A \Rightarrow (B \Rightarrow C)$  (in  $S$ )
2.  $((A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)))$  (axiom (ii))
3.  $(A \Rightarrow B) \Rightarrow (A \Rightarrow C)$  (MP from 1, 2)
4.  $A \Rightarrow B$  (in  $S$ )
5.  $A \Rightarrow C$  (MP from 3, 4)
6.  $A$  (in  $S$ )
7.  $C$  (MP from 5, 6)

## production rules and deduction tree

- view a formal proof from  $S$  as a generative system that uses modus ponens as “production rule”
- deduction can then be written as a tree



## Soundness of the Hilbert Proof System

if  $S \vdash A$  then  $S \models A$

- $S \models A$  holds if  $A \in S$  or if  $A$  is a logical axiom (since tautology)
- if  $S \models A$  and  $S \models (A \Rightarrow B)$  then  $S \models B$
- so if  $S \vdash A$  at each step of the chain  $A_1, \dots, A_n = A$  get  $S \models A_i$ ; so  $S \models A$

## Completeness of the Hilbert Proof System (hard part)

if  $S \models A$  then  $S \vdash A$

### Steps

- 1 **Deduction theorem**: if  $S \cup \{A\} \vdash B$  then  $S \vdash (A \Rightarrow B)$
- 2 **Formal consistency**: if  $S$  formally consistent then  $S$  satisfiable
- 3 **Extend formally consistent to complete** sets of formulae

## Deduction Theorem induction on proofs of $B$ from $S \cup \{A\}$

if  $S \cup \{A\} \vdash B$  then  $S \vdash (A \Rightarrow B)$

*Basis.*

- (i)  $B$  is a logical axiom. Then clearly  $S \vdash B$ . But  $B \Rightarrow (A \Rightarrow B)$  is a logical axiom, thus  $S \vdash B \Rightarrow (A \Rightarrow B)$ , so, by modus ponens,  $S \vdash A \Rightarrow B$ .
- (ii)  $B$  is in  $S \cup \{A\}$ . There are two subcases:
  - (a)  $B$  is in  $S$ . Then again  $S \vdash B$  and the proof is completed as in (i).
  - (b)  $B = A$ . Then  $\vdash A \Rightarrow A$  by example 1.11.4, so  $S \vdash A \Rightarrow A$ , which is the same as  $S \vdash A \Rightarrow B$

*Induction step.* We assume that we have shown that  $S \vdash A \Rightarrow (B \Rightarrow C)$  and  $S \vdash A \Rightarrow B$ , and want to show that  $S \vdash A \Rightarrow C$ . Now  $((A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)))$  is a logical axiom, so

$$S \vdash ((A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))),$$

and then, by MP applied twice, we have

$$S \vdash A \Rightarrow C.$$

## Formal Consistency

- $S$  is **formally inconsistent** if  $S \vdash A$  and  $S \vdash \neg A$  for some formula  $A$
- formally consistent otherwise
- if  $S \cup \{A\}$  formally inconsistent then  $S \vdash \neg A$  (**proof by contradiction**)
- if  $S \cup \{A\} \vdash \neg B$  then  $S \cup \{B\} \vdash \neg A$  (**proof by contraposition**)
- if  $S$  formally consistent then  $S$  satisfiable

## Complete set $\bar{S}$ of formulae

- $\bar{S}$  complete if for any formula  $A$  either  $A \in \bar{S}$  or  $\neg A \in \bar{S}$

**Extend formally consistent to complete:** set of formulae  $S$  that is formally consistent, find  $\bar{S}$  complete with  $S \subset \bar{S}$

- enumerate all WFF:  $A_1, A_2, A_3, \dots, A_n, \dots$
- $S_0 = S$ , and recursively

$$S_{n+1} = \begin{cases} S_n \cup \{A_{n+1}\} & \text{if } S_n \cup \{A_{n+1}\} \text{ is formally consistent} \\ S_n \cup \{\neg A_{n+1}\} & \text{otherwise} \end{cases}$$

- note that if  $S$  formally consistent, for any formula  $A$  at least one of  $S \cup \{A\}$  and  $S \cup \{\neg A\}$  is also formally consistent: if both inconsistent then (proof by contradiction)  $S \vdash A$  and (since  $S \vdash B$  for  $B \in S$ ) then  $S \vdash B$  for all  $B \in S \cup \{A\}$ , but  $S \cup \{A\}$  also inconsistent so  $S$  inconsistent
- $\bar{S} = \cup_n S_n$  is complete and still formally consistent

- for  $\bar{S}$  formally consistent and complete define a valuation  $\bar{v}$  with  $\bar{v}(p_i) = 1$  if  $p_i \in \bar{S}$  and  $\bar{v}(p_i) = 0$  if  $\neg p_i \in \bar{S}$
- this implies  $\bar{v}(A) = 1$  iff the formula  $A \in \bar{S}$
- in particular  $\bar{v}(A) = 1$  for any formula  $A \in S$  so  $S$  is satisfiable
- so formal consistency implies satisfiability

**Completeness follows** from formal consistency implying satisfiability

- start with  $S \models A$ : this implies that  $S \cup \{\neg A\}$  is not satisfiable
- then by “formal consistency implies satisfiability”  $S \cup \{\neg A\}$  is inconsistent
- proof by contradiction:  $S \vdash \neg\neg A$  hence  $S \vdash A$
- so get completeness: if  $S \models A$  then  $S \vdash A$

## Quick Digression: Propositional Logic and Human Language

- the formulation of propositional logic influenced the modeling of human languages
- syntax of human language is based on phrases and sentences that can be seen as “similar” to the well formed formulae of propositional logic
- the theory of *formal languages* describes rules for *generating* “well formed formulae” in language
- connectives in propositional logic and their composition show that there is more structure than just strings of symbols, a hierarchical structure (rooted trees with  $(n + 1)$ -ary nodes that are  $C_n$  connectives with  $n$  inputs and one output)
- similarly in syntax of human language there are hierarchical structures formed by trees (production rules in the formal languages approach to syntax)

- analogy between language and propositional logic also suggests a modeling of the different roles of syntax and semantics and an “interface” between them
- there is an algebraic structure of syntax (formal languages in this earlier formulation) and some algebraic structure (e.g. semirings) on the semantics side and a mapping from syntax to semantics
- this viewpoint naturally presents a “syntax-first” model of languages, based on the autonomy of syntax from semantics
- these are some of the key modeling assumptions of modern linguistics
  
- Noam Chomsky, *The Logical Structure of Linguistic Theory*, 1955 (published Plenum, 1975): first extensive modeling of syntax of human languages as a mathematical/computational structure

## Gödel Compactness of Propositional Logic

- **motivation for the notion of compactness:** consider for example set  $S \subset \mathcal{S}_{WFF}$

$$S = \{p_1, p_2, p_3, \neg(p_1 \wedge p_2 \wedge p_3)\}$$

every proper subset of  $S$  is **simultaneously satisfiable** (there is an assignment  $\nu$  of  $\{0, 1\}$  values to the  $p_1, p_2, p_2$  variables that makes all formulae  $X$  in the subset evaluate to  $\nu(X) = 1$ , **but**  $S$  itself is **not** simultaneously satisfiable since if  $\nu(p_1) = \nu(p_2) = \nu(p_3) = 1$  then  $\nu(\neg(p_1 \wedge p_2 \wedge p_3)) = 0$

- what happens with an **infinite** set  $S \subset \mathcal{S}_{WFF}$  ?
- how does simultaneous satisfiability of  $S$  relate to simultaneous satisfiability of its finite subsets?

## Gödel compactness theorem

if each finite subset of  $S$  is simultaneously satisfiable then  $S$  is simultaneously satisfiable

(note if  $S$  finite then all finite subsets includes  $S$  so statement becomes tautological)

logical implication is finitely determined (equivalent form of compactness)



- suppose  $S \models X$  with  $S \subset \mathcal{S}_{WFF}$  an infinite set
- if every  $F \cup \{\neg X\}$  with  $F \subset S$  finite is simultaneously satisfiable, by compactness also  $S \cup \{\neg X\}$  is simultaneously satisfiable: this contradicts  $S \models X$
- so  $\exists F \subset S$  finite with  $F \cup \{\neg X\}$  not simultaneously satisfiable: no assignment  $\nu$  of truth values to variables that evaluates all formulae in  $F$  to 1 and  $X$  to 0
- so  $F \models X$  so compactness implies finitely determined



- if  $S$  not satisfiable  $S \models \square$  and by finite determination  $\exists F \subset S$  finite with  $F \models \square$  so  $F$  is not satisfiable
- $S$  non-satisfiable implies some finite subset of  $S$  is non-satisfiable equivalent to all finite subsets satisfiable implies  $S$  satisfiable, so compactness

## argument for compactness:

- assuming all finite subsets are satisfiable so each finite  $F \subset S$  has a choice  $\nu_F$  of values of the variable with  $\nu_F(X) = 1$  for all  $X \in F$ : want to construct from these  $\nu_F$  a  $\nu$  that makes all of  $S$  simultaneously satisfiable
- choose an enumeration of the set  $\mathcal{S}_{WFF}$  of well formed formulae so any  $S \subset \mathcal{S}_{WFF}$  has an induced enumeration, so have  $S = \{X_1, X_2, X_3, \dots, X_n, \dots\}$
- also choose an enumeration of  $\Pi = \{p_1, p_2, \dots\}$  so that there is a sequence  $k_1 < k_2 < k_3 < \dots < k_n < \dots$  so that the variables that  $X_n$  depends on are contained in the set  $\{p_1, \dots, p_{k_n}\}$
- use a result on trees (König lemma) and branching to assemble the  $\nu_n = \nu_{\{X_1, \dots, X_n\}}$  into a single  $\nu \models S$

## König lemma:

every infinite rooted tree  $T$  ( $\#V(T) = \infty$ ) with finite valencies ( $\deg(v) < \infty, \forall v \in V(T)$ ) has an infinite path (also called an “infinite branch” of  $T$ ): sequence  $v_0, v_1, \dots, v_n \dots$  of vertices  $v_0$  root,  $d(v_0, v_{n+1}) = d(v_0, v_n) + 1$ , and  $\{v_{n+1}, v_n\} = \partial(e)$  edge  $e \in E(T)$  (i.e.  $v_{n+1}$  child of  $v_n$ )

- $T_v \subset T$ : induced subtree containing  $v$  and all descendants
- “pigeon hole principle”: if  $S$  infinite set and  $S = S_1 \cup \dots \cup S_k$  then at least one  $S_i$  is infinite
- $\{v_{0,1}, \dots, v_{0,k}\}$  children of root vertex  $v_0$

$$V(T) = \{v_0\} \cup V(T_{v_{0,1}}) \cup \dots \cup V(T_{v_{0,k}})$$

- $\exists k_i$  with  $\#V(T_{v_{0,k_i}}) = \infty$ : take  $v_1 = v_{0,k_i}$
- continue same way with children of  $v_1$  etc
- get sequence as above where at each  $n$  one has  $\#V(T_{v_n}) = \infty$

## build a tree for compactness

- choose a root vertex  $\nu_0$
- consider all the assignments  $\nu_1 = (a_1, \dots, a_{k_1}) \in \mathbb{F}_2^{k_1}$  of truth values to the  $p_1, \dots, p_{k_1}$  variables that satisfies  $X_1$
- take the set of these  $\nu_1$  as the children vertices of  $\nu_0$
- below each such  $\nu_1$  there are all the assignments

$$\nu_2 = (a_1, \dots, a_{k_1}, a_{k_1+1}, \dots, a_{k_2}) \in \mathbb{F}_2^{k_2}$$

that satisfy  $X_2$  and that agree with  $\nu_1$  in the first  $k_1$  coordinates

- proceed in this way: get an infinite tree
- by König lemma: there is an infinite branching  
 $\nu_1, \nu_2, \nu_3, \dots, \nu_n \dots$
- these have  $\nu_{n+1} = (\nu_n, a_{k_n+1}, \dots, a_{k_{n+1}}) \in \mathbb{F}_2^{k_{n+1}}$
- so taking  $\nu = (a_1, a_2, a_3, \dots, a_n, \dots)$  gives a valuation  $\nu(p_k) = a_k$  that satisfies all the  $X_k$
- so  $S$  is satisfiable

## Infinite branching from Gödel Compactness

- $T$  an infinite rooted tree, root  $v_0$ , finite valences of vertices (finite branching), assign to each vertex  $v$  a variable  $p_v$
- consider the set  $S \subset \mathcal{S}_{WFF}$  that has as elements the formulae
  - 1  $p_{v_0}$
  - 2  $p_v \Rightarrow \neg p_u$  for  $v \neq u$  at same level, or with  $v$  level  $n$  (path of length  $n$  from  $v_0$  to  $v$ ) and  $u$  level  $n+1$  not a child of  $v$  (immediately below  $v$ )
  - 3  $p_{v_1} \vee \dots \vee p_{v_{k_n}}$  for  $\{v_1, \dots, v_{k_n}\}$  the set of vertices at level  $n$
- **First:** any finite subset  $F$  of  $S$  is satisfiable
  - since  $F$  finite there is some large  $N$  s.t. all variables involved in formulae in  $F$  are in levels  $n \leq N$
  - choose one vertex  $v_N$  at level  $N$ : this determines a path from the root  $v_0$  to  $v_N$
  - take valuation  $\nu_N(p_v) = 1$  iff  $v$  is on the path  $v_0, \dots, v_N$
  - this valuation  $\nu_N$  satisfies all the formulae of the three forms above that are in  $F$  so  $\nu_N \models F$

- **Second:** using compactness,  $S$  is simultaneously satisfiable
- so there is a valuation  $\nu$  for which  $\nu \models S$
- take set of vertices  $V_\nu = \{v \in V(T) \mid \nu(p_v) = 1\}$
- **Claim:**  $V_\nu$  forms a path from  $v_0$  with a single vertex  $v_n$  at each level  $n$  and  $v_{n+1}$  child of  $v_n$
- since  $\nu \models S$  we have:
  - $v_0 \in S$  so  $\nu(p_{v_0}) = 1$  hence  $v_0 \in V_\nu$
  - also  $\nu(p_{v_1} \vee \dots \vee p_{v_{k_n}}) = 1$  so at least one vertex  $v$  at level  $n$  has  $\nu(p_v) = 1$
  - but also  $\nu(p_v \Rightarrow \neg p_j) = 1$  for all the other  $p_j$  at level  $n$  so all those have  $\nu(p_j) = 0$ : only one vertex at level  $n$  in  $V_\nu$
  - suppose vertex  $v_{n+1}$  in  $V_\nu$  is not a child of vertex  $v_n$ , then  $p_{v_n} \Rightarrow \neg p_{v_{n+1}} \in S$  so we have  $\nu(p_{v_n}) = 1$ ,  $\nu(p_{v_{n+1}}) = 1$  and also  $\nu(p_{v_n} \Rightarrow \neg p_{v_{n+1}}) = 1$  which is not possible
- **Note** that compactness also follows from completeness of the Hilbert Proof System because  $S \vdash A$  implies (by form of derivations) that there is some finite  $F \subset S$  with  $F \vdash A$  and also by completeness  $S \models A$  gives  $S \vdash A$  and by soundness  $F \vdash A$  gives  $F \models A$  (finitely determined)

## Other forms of Propositional Logic

- intuitionistic logic (also known as Brouwer logic or constructive logic)
- intermediate logics (between intuitionistic and classical logic)
- Modal logics

## Intuitionistic Propositional Logic

- also known as **constructive logic** or **Brouwer's logic**
- differs from classical propositional logic in two main properties
  - 1 **cancellation of double negation**

$$\neg\neg A = A$$

- 2 **law of the excluded middle**

$$\neg A \wedge A = 1$$

- both are satisfied in classical propositional logic but **not** in intuitionistic logic

## Some facts about Intuitionistic versus Classical Propositional Logic

- Intuitionistic propositional logic **does not have a finite truth-table interpretation**
- there are **infinitely many** distinct axiomatic systems between intuitionistic and classical logic (intermediate logics)
- Intuitionistic propositional logic is effectively decidable: finite **constructive process** producing proof of a formula or disproving by deducing a contradiction from it
- each **proof** of a propositional formula is considered a valid “propositional value”
- Heyting’s “propositions-as-sets” idea: propositional formulae are (possibly infinite) **sets of their proofs**

## Heyting Algebras (also known as Brouwer lattices)

- Boolean algebras provide semantics for classical propositional logic
- Heyting Algebras provide semantics for intuitionistic propositional logic
- Heyting Algebras structure:
  - $(\mathcal{H}, \leq, \wedge, \vee, 0, 1)$  same properties
  - instead of  $A \rightarrow B = \neg A \vee B$  of classical logic have relative pseudo-complement

$$C = \psi(A, B) \text{ greatest element satisfying } A \wedge C \leq B$$

then define

$$A \xrightarrow{\mathcal{I}} B := \psi(A, B)$$

- instead of complement  $\neg$  as in Boolean have pseudocomplement

$$\neg_{\mathcal{I}} A := \psi^c(A) = A \xrightarrow{\mathcal{I}} 0 = \psi(A, 0)$$

- binary operation  $A \xrightarrow{I} B$  characterized by property that

$$(A \wedge C) \leq B \quad \text{equivalent to} \quad C \leq (A \xrightarrow{I} B)$$

- so  $A \leq B$  equivalent to  $1 \leq (A \xrightarrow{I} B)$
- meaning that  $A \xrightarrow{I} B$  is the weakest proposition for which modus ponens inference rule is sound
- also gives  $1 \leq (0 \xrightarrow{I} A)$  (any proposition  $A$  is implied by a contradiction  $0$ )
- negation  $\neg_I A = A \xrightarrow{I} 0$  meaning that  $\neg_I A$  is the proposition that “assuming  $A$  would lead to a contradiction”

- definition of  $\neg_{\mathcal{I}} A$  implies **no contradiction principle**

$$A \wedge \neg_{\mathcal{I}} A = 0$$

- but unlike Boolean case where this is equivalent (by complement) to excluded middle  $A \vee \neg A = 1$  in Heytling algebras this is **not true**
- it also follows from definition of  $\neg_{\mathcal{I}} A$  that

$$A \leq \neg_{\mathcal{I}} \neg_{\mathcal{I}} A$$

- but  $\neg_{\mathcal{I}} \neg_{\mathcal{I}} A \leq A$  **does not work**
- so do not have cancellation of double negation
- no proofs by contradiction** “*reductio ad absurdum*”: in classical logic  $(\neg A \rightarrow 0) \rightarrow A$ , but in intuitionistic logic since don't have  $\neg_{\mathcal{I}} \neg_{\mathcal{I}} A \leq A$  also **don't have**  $\neg_{\mathcal{I}} \neg_{\mathcal{I}} A \xrightarrow{\mathcal{I}} A$  which means don't have  $(\neg_{\mathcal{I}} A \xrightarrow{\mathcal{I}} 0) \xrightarrow{\mathcal{I}} A$  (only constructive proofs, constructive mathematics)

## Boolean and Heyting algebras

- element  $A \in \mathcal{H}$  Heyting algebra is **regular** if  $A = \bigwedge_I \bigwedge_I A$  (not always true but for some elements it is)
- elements  $A, B \in \mathcal{H}$  are **complements** of each other if

$$A \wedge B = 0 \quad \text{and} \quad A \vee B = 1$$

- $A \in \mathcal{H}$  is **complemented** if it has a complement  $B$ : then this is unique and must be  $B = \bigwedge_I A$
- if  $A$  is complemented then so is  $\bigwedge_I A$  and they are complements
- **but**  $A$  may be not-complemented and  $\bigwedge_I A$  may be complemented (with complement  $\bigwedge_I \bigwedge_I A$  different from  $A$ )
- Boolean algebra is a Heyting algebra where every  $A$  is regular
- equivalently Boolean algebra is a Heyting algebra where every  $A$  is complemented
- Boolean algebra is a Heyting algebra with excluded middle

## What happens to De Morgan laws in Intuitionistic Logic?

- usual De Morgan laws in **classical logic**:

①  $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$  or equivalently tautologies

$$\neg(A \vee B) \rightarrow (\neg A \wedge \neg B) \quad \text{and} \quad (\neg A \wedge \neg B) \rightarrow \neg(A \vee B)$$

②  $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$  or equivalently tautologies

$$\neg(A \wedge B) \rightarrow (\neg A \vee \neg B) \quad \text{and} \quad (\neg A \vee \neg B) \rightarrow \neg(A \wedge B)$$

- instead of this completely symmetric form of De Morgan laws in **intuitionistic logic** only have

- ① still have the same: tautologies

$$\neg_I(A \vee B) \xrightarrow{I} (\neg_I A \wedge \neg_I B) \quad \text{and} \quad (\neg_I A \wedge \neg_I B) \xrightarrow{I} \neg_I(A \vee B)$$

- ② but only have one of the other pair

$$(\neg_I A \vee \neg_I B) \xrightarrow{I} \neg_I(A \wedge B)$$

## Topological spaces

A **topological space** is a pair  $(X, \tau)$ , where  $X$  is a set and  $\tau \subseteq \mathcal{P}(X)$  such that

- $X, \emptyset \in \tau$ ,
- $\tau$  is closed under finite intersections,
- $\tau$  is closed under arbitrary unions.

Elements of  $\tau$  are called **open sets**.

Complements of open sets are called **closed sets**.

An open set containing  $x \in X$  is called an **open neighbourhood** of  $x$ .

## Topological spaces: Interior and Closure

The **interior** of a set  $A \subseteq X$  is the largest open set contained in  $A$  and is denoted by  $\text{Int}(A)$ .

That is,  $\text{Int}(A) = \bigcup \{U \in \tau : U \subseteq A\}$

The **closure** of  $A$  is the least closed set containing  $A$  and is denoted by  $\text{Cl}(A)$ .

That is,  $\text{Cl}(A) = \bigcap \{F : X \setminus F \in \tau, A \subseteq F\}$ .

It is easy to check that  $\text{Cl}(A) = X \setminus \text{Int}(X \setminus A)$ .

# Topological semantics of intuitionistic logic

Let  $(X, \tau)$  be a topological space.

An **intuitionistic valuation** is a map  $V : \text{Prop} \rightarrow \tau$ .

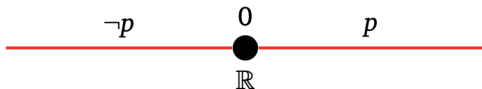
We extend it to all formulas by the following inductive definition:

$$\begin{array}{ll} \llbracket \perp \rrbracket = \emptyset, & \llbracket p \rrbracket = V(p) \\ \llbracket \varphi \wedge \psi \rrbracket = \llbracket \varphi \rrbracket \cap \llbracket \psi \rrbracket & \llbracket \varphi \vee \psi \rrbracket = \llbracket \varphi \rrbracket \cup \llbracket \psi \rrbracket \\ \llbracket \varphi \rightarrow \psi \rrbracket = \text{Int}((X \setminus \llbracket \varphi \rrbracket) \cup \llbracket \psi \rrbracket) & \llbracket \neg \varphi \rrbracket = \text{Int}(X \setminus \llbracket \varphi \rrbracket) \end{array}$$

Intuitionistic Propositional Logic is sound and complete with respect to topological semantics

## lack of excluded middle: topological example

Let  $V(p) = (0, \infty)$ .



$$\llbracket p \vee \neg p \rrbracket \neq \mathbb{R}$$

This is a topological refutation of the law of excluded middle.

## weaker De Morgan law: topological example

- same example with  $\mathbb{R}$ : take  $A = (0, \infty)$  and  $B = (-\infty, 0)$
- have

$$\int (A \cap B) = \text{Int}(\emptyset^c) = \text{Int}(\mathbb{R}) = \mathbb{R}$$

- but have

$$\int \neg A \cup \int \neg B = \text{Int}[0, \infty) \cup \text{Int}(-\infty, 0] = (0, \infty) \cup (-\infty, 0) = \mathbb{R} \setminus \{0\}$$

- so  $(\int \neg A \cup \int \neg B) \xrightarrow{\int} \int (A \cap B)$  gives  $\text{Int}(\{0\} \cup \mathbb{R}) = \mathbb{R}$  OK if tautology
- but  $\int (A \cap B) \xrightarrow{\int} (\int \neg A \cup \int \neg B) = \mathbb{R} \setminus \{0\}$  not OK
- while both

$$\int (A \cup B) \xrightarrow{\int} (\int \neg A \cap \int \neg B) = \mathbb{R} \quad \text{and} \quad (\int \neg A \cap \int \neg B) \xrightarrow{\int} \int (A \cup B) = \mathbb{R}$$

## Hilbert-type proof system for Intuitionistic Propositional Logic

- again **only inference rule is modus ponens**
- **cannot use**  $\{\neg, \rightarrow\}_{\mathcal{I}}$  as not complete set, also cannot reduce  $\wedge, \vee$  (because no elimination of double negation)
- **can use**  $\{\rightarrow, \wedge, \vee, 0\}_{\mathcal{I}}$  or  $\{\rightarrow, \wedge, \vee, \neg\}_{\mathcal{I}}$
- for formulae written with  $\{\rightarrow, \wedge, \vee, 0\}_{\mathcal{I}}$  **axioms**

$$A \rightarrow (B \rightarrow A)$$

$$(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$(A \wedge B) \rightarrow A$$

$$(A \wedge B) \rightarrow B$$

$$A \rightarrow (B \rightarrow (A \wedge B))$$

$$A \rightarrow (A \vee B)$$

$$B \rightarrow (A \vee B)$$

$$(A \rightarrow C) \rightarrow ((B \rightarrow C) \rightarrow ((A \vee B) \rightarrow C))$$

$$\perp \rightarrow A$$

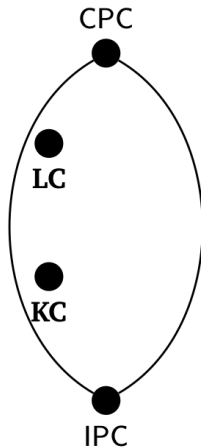
- for formulae written with  $\{\rightarrow, \wedge, \vee, \neg\}_{\mathcal{I}}$  replace last axiom with

$$(A \rightarrow \neg A) \rightarrow \neg A \quad \text{and} \quad \neg A \rightarrow (A \rightarrow B)$$

## intermediate logics

**LC** = IPC +  $(p \rightarrow q) \vee (q \rightarrow p)$   
Gödel-Dummett calculus

**KC** = IPC +  $(\neg p \vee \neg\neg p)$   
weak law of excluded middle



## Propositional Modal Logic

- *logic of necessity and possibility*
- two additional unary connectives:  $\diamond$  = **possible** and  $\square$  = **necessary**
- usual assumptions about these operators (tautologies)

$$\begin{aligned}\square(A \rightarrow B) &\rightarrow (\square A \rightarrow \square B) && \textit{The K axiom} \\ \square(A \wedge B) &\leftrightarrow (\square A \wedge \square B)\end{aligned}$$

$$(\square A \rightarrow A) \quad \textit{The T axiom}$$

$$(A \rightarrow \diamond A)$$

$$(\square A \rightarrow \diamond A)$$

$$(A \rightarrow \square \diamond A) \quad \textit{The B axiom}$$

$$(\square A \rightarrow \square \square A) \quad \textit{The S4 axiom}$$

$$(\diamond \diamond A \rightarrow \diamond A)$$

$$(\diamond A \rightarrow \square \diamond A) \quad \textit{The S5 axiom}$$

$$(\diamond \square A \rightarrow \square A)$$

- well formed formulae (WFF):
  - 1 propositional variables  $p$
  - 2 if  $X$  is WFF then  $\neg X$ ,  $\diamond X$  and  $\square X$  are WFF
  - 3 if  $\alpha, \beta$  WFF then  $\alpha \wedge \beta$ ,  $\alpha \vee \beta$ ,  $\alpha \Rightarrow \beta$  (also written  $\alpha \rightarrow \beta$ ) are WFF

## interpretation of modality: Kripke's many worlds semantics

- tempting to think of  $\diamond$  and  $\square$  as some way of incorporating quantifiers (possible as  $\exists$ , necessary as  $\forall$ ), but it's not quite that interpretation: for example what about  $\diamond\diamond$  "it is possible that it is possible"? weaker than "it is possible"?
- $\square P$  as " $P$  true in all worlds" and  $\diamond P$  as " $P$  true in some world" but difficult to assess relation between  $\diamond\diamond P$  and  $\diamond P$
- introduce a notion of **accessibility relation**:  $\diamond P$  as " $P$  true in some world accessible from this one"
- $\square P$  true in this world iff  $\forall$  worlds accessible from this  $P$  true in that world
- $\diamond P$  true in this world if  $\exists$  world accessible from this where  $P$  true
- *transitivity* of accessibility relation gives  $\diamond\diamond P \Leftrightarrow \diamond P$  tautology
- what other properties of accessibility? symmetric? reflexive? (different logical systems, each with its tautologies/theorems)

## Setting for Kripke's many worlds semantics

- $\mathcal{S}_{WFF}^{\text{mod}}$  set of modal well formed formulae
- Set  $W$  (**possible worlds**)
- binary relation  $R \subset W \times W$  (**accessibility**)
- the pair  $\langle W, R \rangle$  is called a **frame**
- binary relation  $\Vdash \subset W \times \mathcal{S}_{WFF}^{\text{mod}}$  called **forcing**
- for  $\Gamma \in W$  the forcing  $\Vdash$  satisfies rules
  - For all propositional variables  $P$ , either  $\Gamma \Vdash P$  or  $\Gamma \Vdash \neg P$ .
  - If  $\alpha$  is a wff, then  $\Gamma \Vdash \neg\alpha$  if and only if  $\Gamma \not\Vdash \alpha$ .
  - If  $\alpha$  and  $\beta$  are wffs, then  $\Gamma \Vdash (\alpha \vee \beta)$  if and only if  $\Gamma \Vdash \alpha$  or  $\Gamma \Vdash \beta$ .
  - If  $\alpha$  and  $\beta$  are wffs, then  $\Gamma \Vdash (\alpha \wedge \beta)$  if and only if  $\Gamma \Vdash \alpha$  and  $\Gamma \Vdash \beta$ .
  - If  $\alpha$  and  $\beta$  are wffs, then  $\Gamma \Vdash (\alpha \implies \beta)$  if and only if  $\Gamma \not\Vdash \alpha$  or  $\Gamma \Vdash \beta$ .
  - $\Gamma \Vdash \Box\alpha$  only if for every  $\Delta \in W$ ,  $\Gamma R\Delta$  implies that  $\Delta \Vdash \alpha$ .
  - $\Gamma \Vdash \Diamond\alpha$  only if there exists a  $\Delta \in W$  such that  $\Gamma R\Delta$  and  $\Delta \Vdash P$ .
- **model**: data  $\langle W, R, \Vdash \rangle$  **propositional modal model**
- Note: except last two same as classical logic (and only involve *one world*), only last two involve many worlds and accessibility

## complete set of connectives (gates)

- complete set for classical logic (like  $\{\neq, \wedge\}$  or NAND gate)
- together with  $\Box$
- the other modal connective  $\Diamond$  is obtained as  $\neg\Box\neg$
- because  $\Diamond P$  is false in a world means false in every accessible world so  $\neg P$  would be true in every accessible world so  $\Box\neg P$  true, so  $\neg\Diamond P \equiv \Box\neg P$  so  $\Diamond P \equiv \neg\Box\neg P$
- no standard “gate symbol” for  $\Box$
- let's just invent one...

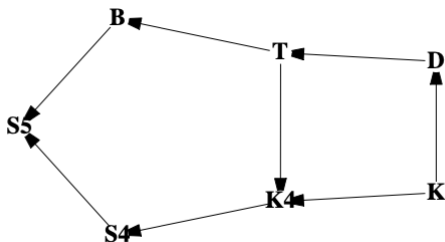


together with NAND

but this gate has to look into all the accessible worlds to act  
unlike Boolean gates

## Modal systems

- fix a given model  $\langle W, R, \Vdash \rangle$
- a WFF  $\alpha \in \mathcal{S}_{WFF}^{\text{mod}}$  is **valid** in  $\langle W, R, \Vdash \rangle$  if  $\Gamma \Vdash \alpha$  for all  $\Gamma \in W$
- $\alpha \in \mathcal{S}_{WFF}^{\text{mod}}$  is valid in the frame  $\langle W, R \rangle$  if valid in every model  $\langle W, R, \Vdash \rangle$  based on the frame  $\langle W, R \rangle$
- $\mathbb{L}$  a collection of frames  $\langle W, R \rangle$
- $\alpha \in \mathcal{S}_{WFF}^{\text{mod}}$  is  **$\mathbb{L}$ -valid** if valid in all frames  $\langle W, R \rangle$  in  $\mathbb{L}$
- collections  $\mathbb{L}$  of frames are usually chosen on the basis of fixing some properties of the accessibility relation  $R$
- simplest class is “no restriction on the relation  $R$ ”: this is called **system  $K$**
- another class is “ $R$  is **serial**” (called **system  $D$** ): for every world  $\Gamma \in W$  there is at least one  $\Delta \in W$  that is accessible from  $\Gamma$  (written  $\Gamma R \Delta$ )



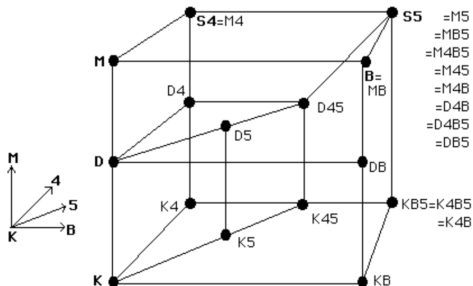
Logic	Frame Conditions
<b>K</b>	no conditions
<b>D</b>	serial <sup>4</sup>
<b>T</b>	reflexive
<b>B</b>	reflexive, symmetric
<b>K4</b>	transitive
<b>S4</b>	reflexive, transitive
<b>S5</b>	reflexive, symmetric, transitive

## Proof Systems

- **logical axioms** (tautologies) basic axioms for the  $K$  system
  - 1 3 logical axioms of the classical case
  - 2  $\Box(A \Rightarrow B) \Rightarrow (\Box A \Rightarrow \Box B)$  (called “schema  $K$ ”)
- **inference rules**: pairs  $(S, \alpha)$  with  $S \subset \mathcal{S}_{WFF}^{\text{mod}}$  and  $\alpha \in \mathcal{S}_{WFF}^{\text{mod}}$ 
  - 1 **modus ponens** (as for classical case): pairs  $(\{\alpha, \alpha \Rightarrow \beta\}, \beta)$
  - 2 **necessitation**: pairs  $(\{\alpha\}, \Box\alpha)$
- when considering another Modal System (adding conditions on the accessibility relation  $R$ ) also adding axioms

Name	Scheme
$D$	$\Box P \Rightarrow \Diamond P$
$T$	$\Box P \Rightarrow P$
$4$	$\Box P \Rightarrow \Box \Box P$
$B$	$P \Rightarrow \Box \Diamond P$

the  $T$  system is also called  $M$  sometimes (reflexivity of  $R$ )



Axiom Name	Axiom	Condition on Frames	R is...
(D)	$\Box A \rightarrow \Diamond A$	$\exists u wRu$	Serial
(M)	$\Box A \rightarrow A$	$wRw$	Reflexive
(4)	$\Box A \rightarrow \Box \Box A$	$(wRv \& vRu) \Rightarrow wRu$	Transitive
(B)	$A \rightarrow \Box \Diamond A$	$wRv \Rightarrow vRw$	Symmetric
(5)	$\Diamond A \rightarrow \Box \Diamond A$	$(wRv \& wRu) \Rightarrow vRu$	Euclidean
(CD)	$\Diamond A \rightarrow \Box A$	$(wRv \& wRu) \Rightarrow v=u$	Unique
( $\Box$ M)	$\Box(\Box A \rightarrow A)$	$wRv \Rightarrow vRv$	Shift Reflexive
(C4)	$\Box \Box A \rightarrow \Box A$	$wRv \Rightarrow \exists u(wRu \& uRv)$	Dense
(C)	$\Diamond \Box A \rightarrow \Box \Diamond A$	$wRv \& wRx \Rightarrow \exists u(vRu \& xRu)$	Convergent

**Derived rules:** rules of inference that are deduced from the axioms and the basic rules of inference

### Example

- **Derived rule of regularity:**  $(\{X \Rightarrow Y\}, \Box X \Rightarrow \Box Y)$

$X \Rightarrow Y$	Occurs somewhere in the proof Necessitation on the previous Axiom <b>K</b> Modus Ponens on the previous two lines
$\Box(X \Rightarrow Y)$	
$\Box(X \Rightarrow Y) \Rightarrow (\Box X \Rightarrow \Box Y)$	
$\Box X \Rightarrow \Box Y$	

**formal proofs** (theorems) in the proof system

- a proof is a finite sequence  $A_1, \dots, A_N$  of formulae, each either an axiom or obtained from earlier terms of the sequence by applying the rules of inference
- the final element  $A_N$  of such a sequence is a theorem in the proof system

- Example:  $\Box(A \wedge Y) \Rightarrow (\Box X \wedge \Box Y)$  is a theorem with proof

1	$(X \wedge Y) \Rightarrow X$	Tautology
2	$\Box(X \wedge Y) \Rightarrow \Box X$	Regularity on 1
3	$(X \wedge Y) \Rightarrow Y$	Tautology
4	$\Box(X \wedge Y) \Rightarrow \Box Y$	Regularity on 3
5	$[\Box(X \wedge Y) \Rightarrow \Box X] \Rightarrow$ $\{[\Box(X \wedge Y) \Rightarrow \Box Y] \Rightarrow$ $[\Box(X \wedge Y) \Rightarrow (\Box X \wedge \Box Y)]\}$	Tautology
6	$[\Box(X \wedge Y) \Rightarrow \Box Y] \Rightarrow$ $[\Box(X \wedge Y) \Rightarrow (\Box X \wedge \Box Y)]$	Modus Ponens, 2, 5
7	$\Box(X \wedge Y) \Rightarrow (\Box X \wedge \Box Y)$	Modus Ponens, 4, 6

**Soundness and Completeness:** we can ask for Modal Proof Systems the same questions about soundness and completeness that we discussed for the Hilbert Proof System of classical logic

**$K$ -system is sound:** if  $X$  has a proof from  $K$ -axioms then  $X$  is  $K$ -valid

- **rules of inference** are valid
  - 1 **modus ponens:** assume  $X$  and  $X \Rightarrow Y$  are  $K$ -valid (for any given model based on an unrestricted frame  $\langle W, R \rangle$  and for all  $\Gamma \in W$ , have  $\Gamma \Vdash X$  and  $\Gamma \Vdash (X \Rightarrow Y)$ ), then since  $\Gamma \Vdash (X \Rightarrow Y)$  have either  $\Gamma \not\Vdash X$  or  $\Gamma \Vdash Y$ , and also know  $\Gamma \Vdash X$  so also  $\Gamma \Vdash Y$ , this for arbitrary world, model, frame so  $Y$  is  $K$ -valid
  - 2 **necessitation:** assume  $X$  is  $K$ -valid (for any model, frame, world  $\Gamma \Vdash X$ ) if there is  $\Delta \in W$  with  $\Gamma R \Delta$  then also  $\Delta \Vdash X$  since for every world, so  $X$  true in every accessible world hence  $\Box X$  is  $K$ -valid

- **axioms** are valid
  - 1 for the 3 classical tautologies follows as in soundness of Hilbert Proof System
  - 2 **schema K**: showing  $\Box(A \Rightarrow B) \Rightarrow (\Box A \Rightarrow \Box B)$  true in all worlds for all frames. If  $\Box(A \Rightarrow B)$  true in  $\Gamma$  world then for  $\Gamma R \Delta$  have  $\Delta \Vdash (A \Rightarrow B)$  and want to show  $(\Box A \Rightarrow \Box B)$  true in  $\Gamma$  namely either  $\Box A$  not true in  $\Gamma$  or  $\Box B$  true in  $\Gamma$ . If  $\Box A$  true in  $\Gamma$  then for  $\Gamma R \Delta$  have  $\Delta \Vdash A$ , but know  $\Delta \Vdash (A \Rightarrow B)$  so  $B$  true in  $\Delta$  so  $\Box B$  true in  $\Gamma$ , so getting that in any  $\Gamma$  either  $\Box(A \Rightarrow B)$  is false or  $\Box A \Rightarrow \Box B$  true.

How about soundness for other Modal Proof Systems? (more axioms to check soundness of)

typical systems usually considered for modal logic:

Logic	Added Axioms
<b>D</b>	$D$
<b>T</b>	$T$
<b>K4</b>	$4$
<b>B</b>	$T, B$
<b>S4</b>	$T, 4$
<b>S5</b>	$T, 4, B$

- all these Modal Proof Systems are **sound** (for each of them use soundness of  $K$ -system and check that each additional axiom is valid)

as in classical more difficult part to prove is completeness

**$K$ -system is complete:** if  $X$  is  $K$ -valid then there is a proof of  $X$  in the  $K$ -system

- same idea as for Hilbert Proof System: make completeness follow from **consistency** (need to prove consistency)
- set  $S = \{X_1, \dots, X_n\} \subset \mathcal{S}_{WFF}^{mod}$  is  **$\mathbb{L}$ -consistent** for a Modal Proof System  $\mathbb{L}$  if

$$X_1 \wedge \dots \wedge X_n \Rightarrow \perp$$

is **not** provable in  $\mathbb{L}$ , where  $\perp$  stands for any  $P \wedge \neg P$  statement

- if  $S$  infinite:  $\mathbb{L}$ -consistent if all finite subsets  $\mathbb{L}$ -consistent
- $S$  is **maximally  $\mathbb{L}$ -consistent** if  $\mathbb{L}$ -consistent and if  $S' \supseteq S$  is  $\mathbb{L}$ -consistent then  $S' = S$
- **canonical model** for  $\mathbb{L}$ :  $\langle W, R, \Vdash \rangle$  with
  - 1  $W$  = set of all maximally  $\mathbb{L}$ -consistent subsets of  $\mathcal{S}_{WFF}^{mod}$
  - 2  $\Gamma R \Delta$  iff for every  $\Box X$  in  $\Gamma$  have  $X$  true in  $\Delta$
  - 3 for  $P$  propositional variable  $\Gamma \Vdash P$  iff  $P \in \Gamma$

## Steps of proof

- 1 every  $\mathbb{L}$ -consistent set  $S$  can be extended to a maximally  $\mathbb{L}$ -consistent  $S^* \supseteq S$
- 2 if a set  $\{\neg\Box B, \Box A_1, \dots, \Box A_N, \dots\}$  is  $\mathbb{L}$ -consistent then  $\{\neg B, A_1, \dots, A_N, \dots\}$  also is
- 3 in canonical model  $\langle W, R, \Vdash \rangle$  for  $\mathbb{L}$  world  $\Gamma \in W$  and  $\alpha \in \mathcal{S}_{WFF}^{\text{mod}}$  have

$$\Gamma \Vdash \alpha \quad \text{iff} \quad \alpha \in \Gamma$$

- then prove completeness by showing that if  $X$  has no proof in the  $K$ -system the set  $\{\neg X\}$  is consistent (cannot derive  $X$  so also cannot derive  $X \wedge \neg X$ ), then extend this set to a *maximally consistent* set  $X^*$  (for which must have  $X \notin X^*$ ), so  $X$  not true in  $X^*$  so not  $K$ -valid

**Step N.1:** every  $\mathbb{L}$ -consistent set  $S$  can be extended to a maximally  $\mathbb{L}$ -consistent  $S^* \supseteq S$

- enumerate all WFF:  $X_0, X_1, \dots, X_n, \dots$  and construct sequence of sets

$$S_0 = S, \quad S_{n+1} = \begin{cases} S_n \cup \{X_{n+1}\} & \text{if } S_n \cup \{X_{n+1}\} \text{ consistent} \\ S_n & \text{otherwise} \end{cases}$$

- each  $S_n$  consistent and  $S_n \subseteq S_{n+1}$
- take  $S^* = S_0 \cup S_1 \cup \dots \cup S_n \dots$  show maximally consistent ( $\mathbb{L}$ -consistent and any  $S' \supseteq S^*$   $\mathbb{L}$ -consistent is  $S' = S^*$ )
- $S^*$  is  $\mathbb{L}$ -consistent: assume not, so there is some  $(A_1 \wedge \dots \wedge A_m) \Rightarrow \perp$
- can't have all these  $A_i$  in same  $S_n$  as each  $S_n$  consistent, but finitely many so in some suff large  $S_n$  (contradiction)
- $S^*$  maximal: suppose not, so there is some consistent extension of  $S^*$  so some formula  $X_i$  with  $S^* \cup \{X_i\} \supsetneq S^*$  and  $\mathbb{L}$ -consistent, but so  $X_i \notin S_i$  so  $S_{i-1} \cup \{X_i\}$  not consistent (contradiction)

**Step N.2:** if  $\Gamma = \{\neg\Box B, \Box A_1, \dots, \Box A_N, \dots\}$  is  $\mathbb{L}$ -consistent then  $\{\neg B, A_1, \dots, A_N, \dots\}$  also

- assume  $\Gamma$  inconsistent with  $\mathbb{L}$ : there is some finite  $\Delta \subset \Gamma$  with  $\bigwedge_{X \in \Delta} X \Rightarrow \perp$
- any extension of inconsistent set is inconsistent, so can assume  $\Delta$  contains  $\neg B$  and write (up to relabeling others) as  $\Delta = \{\neg B, A_1, \dots, A_n\}$

- then proceed as

$$\begin{aligned}
 & (\neg B \wedge A_1 \wedge A_2 \dots \wedge A_n) \Rightarrow \perp \\
 & (A_1 \wedge A_2 \wedge \dots \wedge A_n) \Rightarrow (\neg B \Rightarrow \perp) \\
 & (A_1 \wedge A_2 \wedge \dots \wedge A_n) \Rightarrow B \\
 & \Box((A_1 \wedge A_2 \wedge \dots \wedge A_n) \Rightarrow B) \\
 & \Box(A_1 \wedge A_2 \wedge \dots \wedge A_n) \Rightarrow \Box B \\
 & (\Box A_1 \wedge \Box A_2 \wedge \dots \wedge \Box A_n) \Rightarrow \Box B \\
 & (\Box A_1 \wedge \Box A_2 \wedge \dots \wedge \Box A_n) \Rightarrow (\neg\Box B \Rightarrow \perp) \\
 & (\neg\Box B \wedge \Box A_1 \wedge \Box A_2 \wedge \dots \wedge \Box A_n) \Rightarrow \perp
 \end{aligned}$$

Assumed  
 $((X \wedge Y) \Rightarrow Z)$  is the same  
as  $X \Rightarrow (Y \Rightarrow Z)$   
 $(\neg X \Rightarrow \perp)$  is equivalent to  $X$   
Necessitation  
**Schema K**  
**Theorem 2.9**  
 $\neg X \Rightarrow \perp$  is equivalent to  $X$   
 $((X \wedge Y) \Rightarrow Z)$  is the same  
as  $X \Rightarrow (Y \Rightarrow Z)$

- so  $\{\neg B, A_1, \dots, A_N, \dots\}$  has an inconsistent finite subset so inconsistent

**Step N.3:** from  $\Gamma \Vdash P$  iff  $P \in \Gamma$  for propositional variables to  $\Gamma \Vdash \alpha$  iff  $\alpha \in \Gamma$  for WFF

- OK for atoms: inductively on connectives
- **negation:**  $\alpha = \neg\gamma$  and assuming  $\Gamma \Vdash \gamma$  iff  $\gamma \in \Gamma$ .
  - If  $\Gamma \Vdash \neg\gamma$  then  $\gamma \notin \Gamma$ , but  $\Gamma$  max consistent so  $\neg\gamma \in \Gamma$ .
  - if  $\neg\gamma \in \Gamma$ , with  $\Gamma$  consistent then  $\gamma \notin \Gamma$  but then  $\Gamma \Vdash \neg\gamma$  by ind hypothesis
- **modalities:**  $\alpha = \Box\gamma$ ,
  - assuming  $\Box\gamma \in \Gamma$  and  $\Delta$  accessible from  $\Gamma$ , then  $\Delta \Vdash \gamma$  (but  $\Delta$  arbitrary with  $\Gamma R \Delta$ ) so  $\Box\gamma$  true in  $\Gamma$
  - assume  $\Box\gamma \notin \Gamma$  (max consistent so  $\neg\Box\gamma \in \Gamma$ ); take set of all WFF  $\Box X_0, \Box X_1, \dots$ , know that if  $\{\neg\Box\gamma, \Box X_0, \Box X_1, \dots\}$  consistent then also  $\{\neg\gamma, X_0, X_1, \dots\}$ , extend to max consistent  $\Delta$  so that for  $\Box P \in \Gamma$  have  $P \in \Delta$ : inductively  $\Delta \Vdash P$ , and  $\Gamma R \Delta$  so if  $\neg\gamma$  true in  $\Delta$  have  $\Box\gamma$  not true in  $\Gamma$
- **AND:**  $\alpha = \gamma \wedge \delta$  with  $\gamma, \delta$  true iff in  $\Gamma$ 
  - assume  $\Gamma \Vdash \gamma \wedge \delta$  then both  $\gamma, \delta$  must be true so  $\gamma, \delta \in \Gamma$
  - assume  $\gamma, \delta \in \Gamma$  then  $\Gamma \Vdash \gamma$  and  $\Gamma \Vdash \delta$ , so also have  $\Gamma \Vdash \gamma \wedge \delta$

## Completeness of other Modal Proof Systems

- all  $D, T, K4, B, S4, S5$  are complete
- to show completeness of system  $\mathbb{L}$ , use proof of completeness of  $K$ -system and in addition just need to prove that the frame  $\langle W, R \rangle$  of the canonical model for  $\mathbb{L}$  is in the class  $\mathbb{L}$  (then same proof adapts)
- axioms for these  $\mathbb{L}$  are based on properties of  $R$  (seriality, reflexivity, transitivity, symmetry, etc) so need to show  $R$  of the canonical model of  $\mathbb{L}$  has these properties
- Example:  $D$  (seriality) for every  $\Gamma \in W$  there is some  $\Delta \in W$  with  $\Gamma R \Delta$ ; axiom  $\Box P \Rightarrow \Diamond P = \neg \Box \neg P$ 
  - for  $\Gamma \in W$  have  $(\Box P \Rightarrow \neg \Box \neg P) \in \Gamma$ . If no  $\Delta \in W$  with  $\Gamma R \Delta$  for  $Q$  prop variable  $\Box Q$  vacuously true (no accessible worlds in which to check) but then  $\neg \Box \neg Q$  is true in  $\Gamma$  by axiom  $D$ ;  $\Gamma$  is max consistent so  $\Box \neg Q$  false in  $\Gamma$  (there must be accessible  $\Delta$  where  $\Delta \not\models \neg Q$ ), contradiction
- Other cases with other axioms are similar

## Topological Semantics of S4 Modal Logic

- S4 Modal Logic ( $T$  and 4 axioms: reflexive and transitive accessibility relation  $R$ )

$$T \quad \Box P \implies P$$

$$4 \quad \Box P \implies \Box \Box P$$

- $\langle W, R, \Vdash \rangle$  a Kripke model, where  $R$  is reflexive and transitive
- for  $\alpha \in \mathcal{S}_{WFF}^{\text{mod}}$  set

$$[[\alpha]] := \{\Gamma \in W : \Gamma \Vdash \alpha\}$$

$$R(\Gamma) := \{\Delta \in W : \Gamma R \Delta\}$$

so that

$$[[\Box \alpha]] = \{\Gamma \in W : R(\Gamma) \subset [[\alpha]]\}$$

$$[[\Diamond \alpha]] = \{\Gamma \in W : R(\Gamma) \cap [[\alpha]] \neq \emptyset\}$$

## Topological model

- $(X, \tau)$  topological space,  $\nu : \mathcal{S}_{WFF}^{\text{mod}} \rightarrow \mathcal{P}(X)$
- topological semantics of modal formulas:

$$\begin{array}{ll} \llbracket \perp \rrbracket = \emptyset, & \llbracket p \rrbracket = \nu(p) \\ \llbracket \varphi \wedge \psi \rrbracket = \llbracket \varphi \rrbracket \cap \llbracket \psi \rrbracket & \llbracket \varphi \vee \psi \rrbracket = \llbracket \varphi \rrbracket \cup \llbracket \psi \rrbracket \\ \llbracket \neg \varphi \rrbracket = X \setminus \llbracket \varphi \rrbracket & \llbracket \Box \varphi \rrbracket = \text{Int}[\llbracket \varphi \rrbracket] \end{array}$$

Since  $\Diamond \varphi = \neg \Box \neg \varphi$ , we have  $\llbracket \Diamond \varphi \rrbracket = \text{Cl}[\llbracket \varphi \rrbracket]$ .

- topological properties of Interior and Closure correspond to properties of modalities with  $S4$  axioms

$Cl(\emptyset) = \emptyset$	$\Diamond \perp \leftrightarrow \perp$
$Cl(A \cup B) = Cl(A) \cup Cl(B)$	$\Diamond(p \vee q) \leftrightarrow \Diamond p \vee \Diamond q$
$A \subseteq Cl(A)$	$p \rightarrow \Diamond p$
$Cl(Cl(A)) \subseteq Cl(A)$	$\Diamond \Diamond p \rightarrow \Diamond p$

$Int(X) = X$	$\Box \top \leftrightarrow \top$
$Int(A \cap B) = Int(A) \cap Int(B)$	$\Box(p \wedge q) \leftrightarrow \Box p \wedge \Box q$
$Int(A) \subseteq A$	$\Box p \rightarrow p$
$Int(A) \subseteq Int(Int(A))$	$\Box p \rightarrow \Box \Box p$

# Relation between topological semantics of Intuitionistic logic and of Modal S4 logic

## Gödel translation

There is a celebrated Gödel translation from IPC to S4 defined as follows:

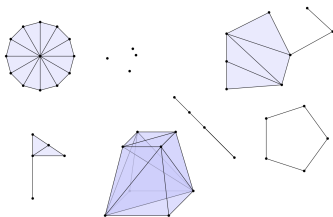
- $Tr(p) = \Box p$ ,
- $Tr(\varphi \wedge \psi) = Tr(\varphi) \wedge Tr(\psi)$ ,
- $Tr(\varphi \vee \psi) = Tr(\varphi) \vee Tr(\psi)$ ,
- $Tr(\varphi \rightarrow \psi) = \Box(Tr(\varphi) \rightarrow Tr(\psi))$ .

This translation is full and faithful, i.e.

$$IPC \vdash \varphi \text{ iff } S4 \vdash Tr(\varphi)$$

**Polyhedral Semantics:** another **modal companion** of Intuitionistic Propositional Logic (from Nick Bezhanishvili)

- **Polyhedra:** Boolean combinations (unions, intersections) of convex hulls of finite sets of points in a Euclidean space
- need not be themselves convex or connected
- can be arbitrary dimension (no fixed ambient space)



- set  $\text{Sub}(P)$  of *subpolyhedra* of a fixed polyhedron  $P$  forms a Boolean algebra
- set  $\text{Op}(P)$  of *open subpolyhedra* of a fixed polyhedron  $P$  forms a Heyting algebra
- what about Modal?

## Polyhedral valuation

- fix a polyhedron  $P$
- **valuation**  $V : \text{Prop} \rightarrow \text{Sub}(P)$  for classical well formed formulae
- extends to modal formulae by

$$V(\Box\phi) = \text{Int}(V(\phi)) \quad \text{and} \quad V(\Diamond\phi) = \text{Cl}(V(\phi))$$

- $P \models \phi$  ( $P$  validates/models  $\phi$ ) if  $V(\phi) = P$  under any valuation:  $\phi$  is valid in  $\text{Sub}(P)$
- **lower dimensional boundary strata in polyhedra:**  
 $A, B \in \text{Sub}(P)$ , if  $A \cap B = \emptyset$  and  $A \subseteq \text{Cl}(B)$  then  $\dim(A) < \dim(B)$
- can define **boundary** as  $\partial A = \text{Cl}(A) \cap \text{Cl}(A^c)$
- so get that **Grzegorzcyk axiom** (Grz)

$$\Box(\Box(A \rightarrow \Box A) \rightarrow A) \rightarrow A$$

holds in polyhedral semantics

- Modal system with axioms S4 plus Grz

## Gödel embedding

- Intuitionistic Propositional Logic embeds faithfully in Modal S4 plus Grz with same Gödel embedding
  - $Tr(p) = \Box p$ ,
  - $Tr(\varphi \wedge \psi) = Tr(\varphi) \wedge Tr(\psi)$ ,
  - $Tr(\varphi \vee \psi) = Tr(\varphi) \vee Tr(\psi)$ ,
  - $Tr(\varphi \rightarrow \psi) = \Box(Tr(\varphi) \rightarrow Tr(\psi))$ .

Then

$$\mathbf{IPC} \vdash \varphi \text{ iff } \mathbf{S4} \vdash Tr(\varphi)$$

$$\mathbf{IPC} \vdash \varphi \text{ iff } \mathbf{S4.Grz} \vdash Tr(\varphi)$$

# Applications of Intuitionistic and Modal Logic

## Intuitionistic Logic

- **functional programming**: formulae (propositions) correspond to data types, proofs of formulae correspond to programs of that type
- functional languages (Haskell, Coq, Agda)
- Lean is also based on intuitionistic logic

## Modal Logic

- **program verification**: reasoning about correctness of computer programs and verification of discrete-state systems
- $\Box A$  meaning  $A$  holds after all possible executions
- linear-time temporal logic (LTL): modal  $\Box, \Diamond$  as “always” or “eventually”
- propositional dynamic logic (PDL): programs composed from ‘atomic’ building blocks
- $\phi \rightarrow \Box\psi$  as input/output behavior of a program: if  $\phi$  holds before the execution of the program then  $\psi$  holds afterwards

## Credits

Slides incorporate material taken from:

- Alexander S. Kechris, Michael A. Shulman, Andrés E. Caicedo, *Math/CS 6c Notes*, 2020
- Stuart A. Kurtz, *A Brief Introduction to the Intuitionistic Propositional Calculus*, 2003
- Joel McCance, *A brief introduction to Modal Logic*
- P. Parrilo and S. Lall, *Positivstellensatz*, 2003
- Nick Bezhanishvili, *Topological semantics of modal logic*, 2021
- Nick Bezhanishvili, *Polyhedral modal logic*, 2021

in addition to material drawn from suggested references posted on the Ma6c course webpage