Propositional Logic

Syntax (grammar)

We define the language $\mathcal{L}$ of propositional logic inductively, as a subset of all words(*) over the alphabet.

$\{A_i \mid i \in \mathbb{N}\} \cup \{\wedge, \vee, \rightarrow, \leftrightarrow, \mid, \neg\} \cup \{(,)\}$
"truth variables" "connectives" "parentheses"

Empty String is also a word.
given by the inductive structure:

1-ary 1) $\forall i \quad A_i \in \mathcal{L}$ (1-ary) Relation1: $R(B) \Leftrightarrow B$ is a truth variable.

3-ary 2).1) $A, B \in \mathcal{L} \Rightarrow (A \wedge B) \in \mathcal{L}$ Relation: $R(A,B,C) \Leftrightarrow C = (A \wedge B)$
2.2) – " – $\Rightarrow (A \vee B) \in \mathcal{L}$
2.3) – " – $\Rightarrow (A \rightarrow B) \in \mathcal{L}$
2.4) – " – $\Rightarrow (B \rightarrow A) \in \mathcal{L}$?
2.5) – " – $\Rightarrow (A \leftrightarrow B) \in \mathcal{L}$
2.6) $A, B \in \mathcal{L} \Rightarrow (A \mid B) \in \mathcal{L}$
2.7) $A \in \mathcal{L} \Rightarrow \neg A \in \mathcal{L}$

(*) words over an alphabet $\mathcal{A}$ are finite strings of letters of $\mathcal{A}$ (the empty string ε is a word; the empty word)

Definition and induction by an inductive structure.

Have set S; We define subset T by a list of rules r_i $i = 1, \dots, m$
To rule r_i corresponds a relation R_i on S as rule r_i:
$\forall s_1, \dots, s_{n-1}$: $s_1, \dots, s_{n-1} \in T$ and $R_i(s_1, \dots, s_{n-1}, s_n) \Rightarrow s_n \in \mathcal{T}$.

(if R_i is n-ary relation)
[FOR a 1-ary relation R_i the corresp. rule is just:
$\forall s \in \mathcal{L}$ if $R_i(s)$ then $s \in \mathcal{T}$]

$\mathcal{T}$ is defined as the intersection of all subsets of S satisfying the rules $r_1, \dots, r_m$. [Intersection of all subsets of S closed under the relation R_i $i = 1, \dots m$]

Induction using an inductive structure:

If $\mathcal{T}$ is defined inductivly as a subset of S by rules r_i. Then we can prove a statement S about all elements of $\mathcal{T}$ by showing $\forall i$

If S holds for $s_1, \dots, s_{n-1}$ and $R_i(s_1, \dots, s_{n-1}, s_n)$ then S holds for s_n.
(For 1-ary relations R_i this this means we show that S holds for every $s \in \mathcal{L}$ satisfying $R_i(s)$].

For example: to show that some statement holds for every $F \in \mathcal{L}$ (formula of prop. logic), it suffices to show

1) S holds for every A_i (truth var.)

2) if S holds for A, B (words over our alphabet) then S holds for $(A \wedge B)$, for $(A \vee B)$, ... and for $(\neg A)$.

(EX) Show that every $F \in \mathcal{L}$ contains exactly the same number of left parentheses as right parentheses.

(EX) Every proper, non-trivial initial segment of $F \in \mathcal{L}$ contains strictly more "(" then ")".

Def) If w is a word over the alphabet $\mathcal{A}$, $w = a_1 a_2, \dots, a_n$ with $a_i \in \mathcal{A}$ then an initial segment is $a_1, \dots, a_k$, where $0 \leq k \leq n$.
For $k=0$ $a_1, \dots, a_0 = \varepsilon$ is the empty word: the trivial initial segment.

For $0 < k < n$ $a_1, \dots, a_n$ is a proper non-trivial initial segment

For $k = n$ the initial seg. is all of w "not a proper initial seg."

Proof) that induction on an inductive structure works:

$$\mathcal{S} = \bigcap_{\substack{T \subseteq S \\ T \text{ closed under} \\ R_1, \dots, R_m}} T$$

Consider the set $W \subseteq S$ $W = \{s \in S \mid s \text{ satisfies } S \text{ statements}\}$

Proof by induction shows that W is closed under $R_1, \dots, R_m$ therefore $W \supseteq \mathcal{S}$.

Another way to define language of propositional logic: in postfix notation:

Alphabet $\mathcal{A} = \{ A_i \mid i \in \mathbb{N} \} \cup \{ \wedge, \vee, \rightarrow, \leftrightarrow, 1, \neg \}$

$\mathcal{L}$ defined as subset of $\mathcal{A}^*$ (= words over $\mathcal{A}$) by the rules

1) $\forall i$ $A_i \in \mathcal{L}$
2).1 $A, B \in \mathcal{L}$ $\Rightarrow$ $AB\wedge \in \mathcal{L}$
2.2. $A, B \in \mathcal{L}$ $\Rightarrow$ $AB\vee \in \mathcal{L}$
–II– $\Rightarrow$ $AB\rightarrow \in \mathcal{L}$
etc.
$A \in \mathcal{L}$ $\Rightarrow$ $A\neg \in \mathcal{L}$

The idea is to $(((A_1 \wedge A_2) \vee A_3) \rightarrow A_4)$ corresponds $A_1 A_2 \wedge A_3 \vee A_4 \rightarrow$

Unique readability of an inductive structure:

Remark: if $\mathcal{T} \subseteq \mathcal{S}$ is inductively defined by rules $r_1, \dots, r_n$ then for every $t \in \mathcal{T}$ there exists i, $t_1, \dots, t_{n-1} \in \mathcal{T}$ such that $R_i(t_1, \dots, t_{n-1}, t)$ holds.

$\mathcal{T} \subseteq \mathcal{S}$ inductively defined by rules $r_1, \dots, r_n$: this inductive structure satisfies "unique readability" if and only if for every $t \in \mathcal{T}$ there exists exactly one i and a unique choice of $t_1, \dots, t_{n-1} \in \mathcal{T}$ s.t. $R_i(t_1, \dots, t_{n-1}, t)$ holds (where R_i is n-ary)

Example: language of propositional logic both with parenthes and in postfix, satisfies unique readability.

EX show for language of prop. logic with (,) : unique readability [first show: no proper initial segment of a formula $\in \mathcal{L}$ is itself a formula $\in \mathcal{L}$.]

EX for language of proper. logic in postfix: show unique readability.
[No proper non-trivial final segment of a $w \in \mathcal{L}$ is itself in $\mathcal{L}$; show this by assigning weights to connectives and truth variables, such that sum of weights in $w \in \mathcal{L}$ is zero, say]

Semantics of propositional logic:

An assignment (of truth values to the truth variables) is a function $a: N \to \{0,1\}$ $N \subseteq \{A_i \mid i \in \mathbb{N}\}$

a is a complete assignment, if $a: \{A_i \mid i \in \mathbb{N}\} \to \{0,1\}$

Given complete assignment a, we can extend a to $\bar{a}: \mathcal{L} \to \{0,1\}$ by the following inductive definition:

1) for A_i truth var, a is defined, $\bar{a}(A_i) := a(A_i)$

2.1 if $F = (A \wedge B)$ then $\bar{a}(F) = \phi_\wedge(\bar{a}(A), \bar{a}(B))$ where
$$\phi_\wedge: \{0,1\} \times \{0,1\} \to \{0,1\}$$
$$\phi_\wedge(x,y) = \begin{cases} 1 & \text{if } x=y=1 \\ 0 & \text{else} \end{cases}$$

2.2. if $F = (A \vee B)$ $\bar{a}(F) := \phi_\vee(\bar{a}(A), \bar{a}(B))$ where
$$\phi_\vee: \{0,1\} \times \{0,1\} \to \{0,1\}$$
$$\phi_\vee(x,y) = \begin{cases} 1 & \text{otherwise} \\ 0 & x=y=0 \end{cases}$$
ect.

$$\phi_\to(x,y) = \begin{cases} 0 & x=1, y=0 \\ 1 & \text{otherwise} \end{cases}$$

$(A \to B) \begin{cases} \text{false} & \text{if } A \text{ true}, B \text{ false} \\ \text{true} & \text{otherwise} \end{cases}$

$$\phi_{\leftrightarrow}(x,y) = \begin{cases} 1 & x=y \\ 0 & \text{otherwise} \end{cases}$$

$$\phi_{\neg}(x,y) = \begin{cases} 1 & x=0 \\ 0 & x=1 \end{cases}$$

$$\phi_{|}(x,y) = \begin{cases} 0 & x=y=1 \\ 1 & \text{otherwise} \end{cases} \quad \text{"NAND"}$$

Sheffer stroke

We have used unique readability.
If a structure satisfies unique readability we can define a function on the set defined $f: \mathfrak{T} \to S$ (S any set) by defining $f(t)$ where $t_1, \dots, t_n \in \mathfrak{T}$ and $R_i(t_1, \dots, t_{n-1}, t)$ (of rule r_i) holds using $f(t_1), \dots f(t_{n-1})$ already assumed known.

IF $F \in \mathcal{L}$ contains no other truth var then $A_1, \dots, A_n$ then $\bar{a}(F)$ depends only on $a(A_1), \dots, a(A_n)$.
A formula F containing no other truth var than $A_1, \dots, A_n$ defines a truth function $\phi_F : \alpha \to \{0,1\}$ where $\alpha = \{a : a$ complete assignment$\}$ by $\phi_F(\ ) = \bar{a}(F)$
similarily for partial assignments $\alpha_n = \{a \mid a: \{A_1, \dots, A_n\} \to \{0,1\}\}$
$\phi_F(\alpha_n) \to \{0,1\}$
$\phi_F(a) = \bar{a}(F)$ if F contains no var. other than $A_1, \dots, A_n$

ϕ_F can be written as a table of values "truth table of F".

A_1	A_2	$(A_1 \to A_2) = F$
0	0	1
0	1	1
1	0	0
1	1	1

Def) formulas $F, G \in \mathcal{L}$ are "logically equivalent" written $F \Leftrightarrow G$ if F and G have the same truth function $\phi_F = \phi_G$, i.e. if $\bar{a}(F) = \bar{a}(G)$ for every (complete) assignment of truth variables.

Example)

$$(A_1 \to A_2) \Leftrightarrow (A_2 \vee (\neg A_1))$$
$$(A_1 \to A_2) \Leftrightarrow ((\neg A_2) \to (\neg A_1))$$
$$A_1 \Leftrightarrow A_1 \vee (A_2 \wedge (\neg A_2))$$
$$A_1 \Leftrightarrow A_1 \wedge (A_1 \vee (\neg A_2))$$

Def) F is a "logical consequence" of G, if and only if for every compl. assignment a with $\bar{a}(G) = 1$, it is true that $\bar{a}(F) = 1$ write $G \Rightarrow F$.

Logic

25.11.10

Instead of Fri Nov 26 10-12
We have class Fri Dec. 10 C208 12-2 pm

---

formulas $F, G \in \mathcal{L}$ are "logically equivalent", written as $F \Leftrightarrow G$
iff $\forall$ complete assignment a $\bar{a}(F) = \bar{a}(G)$.

In other words iff $\phi_F = \phi_G$ (truth function of F, $\phi_F : \{\text{complete ass.}\} \to \{0,1\}$
$\phi_F(a) = \bar{a}(F)$).

Def) $F \in \mathcal{L}$ is a tautology iff ϕ_F is constant 1, i.e. $\forall$ complete assignment $\bar{a}(F) = 1$.

Examples: • $(A \vee \neg A))$ $A \in \mathcal{L}$
"tertium non datur" (there is no third (possibility))

• $(\neg(A \wedge \neg A))$

• $((A \wedge B) \wedge C) \leftrightarrow (A \wedge (B \wedge C))$

• $(\neg(A \wedge B)) \leftrightarrow (((\neg A) \vee (\neg B)))$ „De Morgan"

Informally, we don't write all parentheses: conventions

- $\neg A \wedge B$ means $((\neg A) \wedge B)$
- $\neg A \vee B$ —"— $((\neg A) \vee B)$
- $A \wedge B \rightarrow C \vee D$ means $((A \wedge B) \rightarrow (C \vee D))$

Connectives listed from strongest (highest priority) to weakest:
$\neg$ stronger than $\wedge, \vee$
$\wedge, \vee$ stronger than $\rightarrow, \leftrightarrow$.

EX: for any formulas $F, G \in \mathcal{L}$
$F \Leftrightarrow G$ iff $(F \leftrightarrow G)$ is a tautology.

statement in meta-Language

formula in formal language

EX: for formulas $F, G \in \mathcal{L}$
$F \Rightarrow G$ (G is a logical consequence of F) iff
$(F \rightarrow G)$ is a tautology.

Normal forms of formulas (up to logical equivalence)

Example:

A	B	$A \to B$
0	0	1
0	1	1
1	0	0
1	1	1

equivalent formula in disjunction 2-form
$((\neg A) \wedge (\neg B)) \vee ((\neg A) \wedge B) \vee (A \wedge B)$

Convention: $F_1 \vee F_2 \vee F_3 \vee \dots \vee F_n$ means $((((F_1 \vee F_2) \vee F_3) \vee F_4) \vee \dots \vee F_n)$
similar for $\wedge$:

— " — (equivalent formula to $A \to B$ in conjunctive 2-form)

idea: $(A \to B) \iff \neg(A \wedge \neg B)$
$\neg(A \wedge \neg B) \iff (\neg A \vee B)$
$(\neg A \vee B)$ is formula in conj. 2-form.

actually instead of A, B we should have written A_1, A_2.

Formal Def. of disjunctive / conjunctive normal forms:
An expression $(B_1 \vee B_2 \vee \dots \vee B_n)$, where each B_i is either A_i or $(\neg A_i)$ is called n-clause.

A formula in **conjunctive n-form** is a conjunction of clauses:

$(B_1^{(1)} \vee B_2^{(1)} \vee \dots \vee B_n^{(1)}) \wedge (B_1^{(2)} \vee B_2^{(2)} \vee \dots \vee B_n^{(2)}) \wedge \dots \wedge (B_1^{(k)} \vee B_2^{(k)} \vee \dots B_n^{(k)})$

where each $B_i^{(m)}$ is either A_i or $(\neg A_i)$ and the clauses are ordered lexicographically (clauses with $B_1 = A_1$ before these with $\neg A_i$).
and $k \geq 1$.

A dual n-clause is a formula $(B_1 \wedge B_2 \wedge \dots \wedge B_n)$ each B_i either A_i or $\neg A_i$ disjunctive n-form: disjunction of $k \geq 1$ dual n-clauses.

$(B_1^{(1)} \wedge B_2^{(1)} \wedge \dots \wedge B_n^{(1)}) \vee \dots \vee (B_1^{(k)} \wedge B_2^{(k)} \wedge \dots \wedge B_n^{(k)})$

A formula in conjunctive normal form is an expression

$(B_{1_1}^{(1)} \vee B_{1_2}^{(1)} \vee \dots \vee B_{1_{n_1}}^{(1)}) \wedge \dots \wedge (B_{j_1}^{(k)} \vee B_{j_2}^{(k)} \vee \dots \vee B_{j_{n_k}}^{(k)})$ where each $B_i^{(j)}$ is either A_m or $\neg A_m$ for some $m \in \mathbb{N}$.
" conjunction of disjunction of literals "
Literal: either A_m or $\neg A_m$

Disjunctive normal form (like conj., with $\wedge, \vee$ interchanged)
a disjunction of conjunctions of literals

(EX) every $F \in \mathcal{L}$ is logically equivalent to a (non-unique) formula in conj. normal form and a (non-unique) formula in disj. normal form.

(EX) Every formula F that contains no other truth var. than $A_1, \dots, A_n$ that is not a tautology is equivalent to a unique formula in conj. n-form.

(EX) Every formula $F \in \mathcal{L}$ that is not a contradiction and contains no truth var. other than $A_1, \dots, A_n$ is equivalent to a unique formula in conj. n-form.

Def) $F \in \mathcal{L}$ is a contradiction iff ϕ_F is constant 0
($\forall a$ | complete assignment $\bar{a}(F)=0$)

$F \in \mathcal{L}$ is satisfiable if it is not a contradiction.
(there exists an assignment a with $\bar{a}(F)=1$).

(EX) Show how to list all (up to logical equivalence) consequences for a given formula, using disj. n-form or conj. n-forms.
Similarly; how to list (up to logical equiv.) all formulas of which the given formula is a consequence (for given F, all G with $G \Rightarrow F$).

Boolean Algebras

(Can be defined as a special kind of ring or a special kind of lattice).

Boolean algebras as rings:

Def) A ring $(R, +, \cdot)$ is called Boolean Algebra iff every element is idempotent, i.e. $\forall r \in R \quad r \cdot r = r$

EX $R = \prod_{s \in S} \mathbb{F}_2$ (product of copies indexed by a set S of finite field with 2 elements

$\mathbb{F}_2 \ (\{0,1\}, +, \cdot)$

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

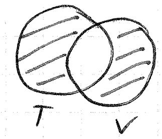
addition, multiplication coordinate-wise

$(x_s)_{s \in S} \cdot (y_s)_{s \in S} = (x_s \cdot y_s)_{s \in S}$
$(x_s)_{s \in S} + (y_s)_{s \in S} = (x_s + y_s)_{s \in S}$

Can identify elements of $\prod_{s \in S} \{0,1\}$ with subsets of S, each subset corresponds to its characteristic function

$T \subseteq S$ corresp. to $\chi_T : S \to \{0,1\}$

$$\chi_T(s) = \begin{cases} 1 & s \in T \\ 0 & s \notin T \end{cases}$$



then $\chi_{T \cap V} = \chi_T \cdot \chi_V$

$\chi_{T \Delta V} = \chi_T + \chi_V$ — $T \Delta V$ symmetric difference of T, V: $x \in T \Delta V$ iff $(x \in T \wedge x \notin V) \vee (x \notin T \wedge x \in V)$

__Lemma:__ R Boolean algebra, then R is commutative ($r \cdot s = s \cdot r$ for all $r, s \in R$) and R is of characteristic 2, i.e. $\forall r \in R$ $r + r = 0$ (i.e. $r = -r$).

__Proof:__ we show for all $r, s \in R$ $r \cdot s = -s \cdot r$

$r + s = (r+s)^2 = r^2 + rs + sr + s^2 = r + s + rs + sr$

$0 = rs + sr$, $rs = -sr$

Set $s = 1$: $r = -r$

using that $s = -s$, we get $rs = -sr = sr$ commutativity ✓

Lattices

(Two unrelated (not very much related) math. objects called lattice: this one is "Verband", there is a kind of Lattice in number theory, called "Gitter" in German).

A Lattice can be defined as a partially ordered set or as a set with two binary operations: $\wedge, \vee$ satisfying certain axioms).

Def) A (partially) ordered set $(S, \leq)$ is called lattice, if for any two elements $s, t \in S$ there exists $\sup(s,t)$ and $\inf(s,t)$ in S.

Def) $(S, \leq)$ partially ordered set $x, y, i, s \in S$. i is called $\inf(x,y)$ iff
1) $i \leq x$ and $i \leq y$
2) $\forall z \in S$ if $(z \leq x \wedge z \leq y)$ then $z \leq i$

s is called $\sup(x,y)$ if
1) $x \leq s$ and $y \leq s$ and
2) $\forall z \in S$ if $(x \leq z \wedge y \leq z)$ then $s \leq z$

In an ordered set $(S, =)$ $\sup(x,y)$, $\inf(x,y)$ do not always exist, but if $\inf(x,y)$ ~~and $\sup(x,y)$~~ exists, it is unique. similary for sup.

Def) A lattice $(S, \leq)$ is called a complete lattice, if for every subset $T \subseteq S$ $\inf T$, $\sup T$ exist in S.
i is $\inf T$ if
1) $\forall t \in T \quad i \leq t$
2) $\forall z \in S$, if $\forall t \in T \quad z \leq t$ then $z \leq i$

s is $\sup T$ if
1) $\forall t \in T \quad t \leq s$
2) $\forall z \in S$ if $\forall t \in T \quad t \leq z$ then $s \leq z$

Examples of complete lattices (all ordered by $\subseteq$ set-th. inclusion)
- sub-groups of a group
- normal sub-groups of a group
- ideals of a ring
- sub-spaces of a vector-space

In general, sub structures of an algebraic structure, provided that the intersection of an arbitrary collection of substructures is again a substructure

Then $\inf \mathcal{T} = \bigcap_{T \in \mathcal{T}} T$, $\sup \mathcal{T} = \bigcap_{\substack{W \text{ sub str. of } S \\ \forall T \in \mathcal{T} \; T \subseteq W}} W$

Part 2   25.11.10

Lattice defined as set with binary operations $\wedge$, ~~$\vee$~~ "meet" and $\vee$ "join": A set $(L, \wedge, \vee)$ with binary operations $\wedge, \vee$ is a lattice if the 4 lattice axioms hold:

L1: associativity of $\wedge, \vee$ $\quad \forall a, b, c \in L \quad ((a \wedge b) \wedge c) = (a \wedge (b \wedge c))$
similar for $\vee$.

L2: commutativity of $\wedge, \vee$ $\quad \forall a, b \quad (a \wedge b) = (b \wedge a)$
similar for $\vee$.

L3: idempotence of $\wedge, \vee$ $\quad \forall a \in L \quad a \wedge a = a, \quad a \vee a = a$

L4: $\forall a, b \in L \quad ((a \wedge b) \vee b) = b$ and $((a \vee b) \wedge b) = b$

Lattice as ordered set with sup, inf and lattice as $(L, \wedge, \vee)$ satisfying L1-L4 are equivalent concepts in the following sense:

Given $(L, \leq)$ such that $\forall x, y \in L$ $\sup(x,y)$, $\inf(x,y)$ exist in L, define $x \wedge y := \inf(x,y)$ $\quad x \vee y := \sup(x,y)$.
Then axioms L1-L4 are satisfied.

Ad L1: show that both $((x \wedge y) \wedge z)$ and $(x \wedge (y \wedge z))$ satisfy ~~the~~ conditions for $\inf(x,y,z)$. Therefore equal.
Similarly $(x \vee y \vee z)$ and $(x \vee (y \vee z))$ both satisfy conditions for $\sup(x,y,z)$. Therefore they are equal.

Remark: in a lattice, sup and inf of any finite set of elements $x_1, \dots, x_n$ exist, namely $x_1 \wedge x_2 \wedge \dots \wedge x_n = \inf(x_1, \dots, x_n)$
$x_1 \vee x_2 \vee \dots \vee x_n = \sup(x_1, \dots, x_n)$

Ad L2: $\sup(x,y) = \sup(y,x)$
$\inf(x,y) = \inf(y,x)$

Ad L3: $\sup(x,x) = x$ $\quad \inf(x,x) = x$

Ad L4: EX

Conversely, given a lattice $(L, \wedge, \vee)$ define $\leq$ on L by
$x \leq y \iff x \wedge y = x$

[EX: for x, y in a lattice $x \wedge y = x$ if and only if $x \vee y = y$]
by commutativity equiv: $y \vee x = y$

(We could also define $x \leq y \iff x \vee y = y$)

Then for all $x, y \in L$ $\quad \sup(x,y) = x \vee y$ and $\inf(x,y) = x \wedge y$.

Check condition for $\inf(x,y)$.
to show 1) $x \wedge y \leq x \quad x \wedge y \leq y$
$x \wedge (x \wedge y) \overset{L1}{=} (x \wedge x) \wedge y \overset{L3}{=} x \wedge y$

therefore $x \wedge y \leq x$ $\quad$ similar: $x \wedge y \leq y$

2) suppose $z \leq x$, $z \leq y$ to show $z \leq x \wedge y$ we have
$z \wedge x = z$, $z \wedge y = z$

$z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$

therefore $z \leq x \wedge y$. $\quad$ similarly $x \vee y$ satisfies conditions for $\sup(x,y)$.

<u>It remains to check:</u>
If we start with $(L, \leq)$ with sup, inf and we define $x \wedge y := \inf(x,y)$, $x \vee y = \sup(x,y)$ and then consider $\trianglelefteq$ defined as $x \trianglelefteq y :\iff x \wedge y = x$ then the order relation $\trianglelefteq$ is the same as $\leq$ the original order relation. on L.

This amounts showing $x \leq y$ iff $\inf(x,y) = x$ OK ✓

<u>Conversly we have to check:</u>
if we start with $(L, \wedge, \vee)$ satisfying L1 - L4 and we define $x \leq y :\iff x \wedge y = x$ and then we define $x \vartriangle y := \inf(x,y)$ and $x \veebar y := \sup(x,y)$ then $\vartriangle$ is the same as $\wedge$; $\veebar$ is the same as $\vee$.
Exercise

We forgot to check the axioms for <u>order relation</u> after defining $x \leq y \Leftrightarrow x \wedge y = x$ (given $(L, \wedge, \vee)$ satisfying L1 - L4.

<u>$\leq$ reflexive:</u> $x \leq x$ is $x \wedge x = x$ L3 ✓

<u>$\leq$ transitive:</u> $x \leq y$ and $y \leq z$, i.e. $x \wedge y = x$
$y \wedge z = y$
to show $x \leq z$; to show $x \wedge z = x$
$x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$ ✓

<u>$\leq$ antisymmetric:</u> if $x \leq y$ and $y \leq x$ show $x = y$;
if $x \wedge y = x$ and $y \wedge x = y$
then $x = y$. By L2 $x \wedge y = y \wedge x$ ✓

Def) A lattice is called complementary if
1) $\min L$, $\max L$
(written as 0 and 1)
$\exists\, 0 \in L: \forall x \in L \quad 0 \leq x$
$\exists\, 1 \in L: \forall x \in L \quad x \leq 1$ and

2) $\forall x \in L: \exists\, x^c$ (or $\bar{x}$, x' sometimes also written) such that $x \wedge x^c = 0$ and $x \vee x^c = 1$.
x^c is called the complement of x.

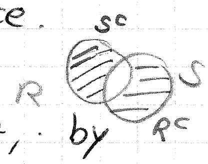
Def) A lattice $(L, \wedge, \vee)$ is distributive iff
$\forall\, a, b, c \in L \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Remark: a lattice is distributive iff $\forall a, b, c \in L \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

(EX) Show equivalence of the two distributive laws (show one implication, using ~~any~~ only the lattice axioms. Since lattice axioms are symmetric in $\wedge, \vee$ the argument works with ~~$\vee \wedge$~~ $\vee, \wedge$ interchanged - other direction)

The concepts of Boolean algebra and complementary distributive lattice are equivalent in the following sense:

I) Given Boolean algebra $(R, +, \cdot)$, define $\leq$ on R by $r \leq s \Leftrightarrow r \cdot s = r$ then $(R, \leq)$ is distr. compl. lattice.



II) Given a complementary distr. lattice $(L, \wedge, \vee)$, define $+$, $\cdot$ by
$r \cdot s := r \wedge s$
$r + s := (r \wedge s^c) \vee (r^c \wedge s)$

Remark: in any compl. distr. lattice $(r \wedge s^c) \vee (r^c \wedge s) = (r \vee s) \wedge (r^c \vee s^c)$
(EX)

(We could define $r+s = (r \vee s) \wedge (r^c \vee s^c)$)
Then $(L, +, \cdot)$ is Boolean algebra.

Ad I) first show order relation.
show sup, inf exist.

$\leq$ refl: $r \leq r$ means $r \cdot r = r$ Boolean alg. axiom ✓
$\leq$ trans: $\underset{r \leq s}{r \cdot s = r}$ $\underset{s \leq t}{s \cdot t = s}$ to show $\underset{r \leq t}{r \cdot t = r}$
$r \cdot t = r \cdot s \cdot t = r \cdot s = r$
$\leq$ antisymm: $r \leq s$ and $s \leq r$ to show $r = s$.
if $r \cdot s = r$ and $s \cdot r = s$ then $r = s$
by commutativity of $\cdot$ of a Boolean algebra ✓

show $\inf(r,s) = r \cdot s$
$\sup(r,s) = r + s + r \cdot s$

check: $r \cdot s \leq r$, $r \cdot s \leq s$

$r(r \cdot s) = r^2 s = rs \quad \Rightarrow \quad (r \cdot s \leq r)$
$(r \cdot s) \cdot s = r s^2 = rs \quad \Rightarrow \quad (r \cdot s \leq s)$

- commutativity in Boolean alg.

supp.: $z \leq r$, $z \leq s$ to show $z \leq r \cdot s$
$z \cdot r = z$, $z \cdot s = z$ to show $z \cdot r \cdot s = z$
$z \cdot r \cdot s = z \cdot s = z$ ✓

check sup:
to show $s \leq r+s+rs$, $r \leq r+s+rs$
$(r+s+rs)s = rs + s^2 + rs^2 = rs + s + rs = s$ ✓
$r(r+s+rs) = r^2 + rs + r^2 s = r + rs + rs = r$ ✓

Suppose $r \leq z$, $s \leq z$ to show $r+s+rs \leq z$
$r \cdot z = r$ $s \cdot z = s$

$(r+s+rs)z = rz + sz + rsz = r + s + rs$ ✓

show complementary lattice 0 and 1 (elements of ring $(R, +, \cdot)$)
are min and max:
$\forall x \in R \quad x \cdot 0 = 0$ means $\forall x \in R \quad 0 \leq x$
$\forall x \in R \quad x \cdot 1 = x$ means $\forall x \in R \quad x \leq 1$

Complement of x is $x+1$
check: $(x+1) \wedge x = 0$ and $(x+1) \vee x = 1$

$\cancel{(x+1) \cdot x = x^2 + x = x + x = 0}$ ✓
We get $\wedge, \vee$ from $(R, \leq)$ by $x \wedge y := \inf(x,y)$.
So $x \wedge y = x \cdot y$
and by $x \vee y = \sup(x,y) = x + y + xy$

$(x+1)\cdot x = x^2 + x = x + x = 0$ ✓
$(x+1) + x + (x+1)x = x + 1 + x + x^2 + x = 1$ ✓

distributivity
show : $x \wedge (y \vee z) = (x \overset{xy}{\wedge} y) \vee (x \overset{xz}{\wedge} z)$

to show: $x \cdot (y + z + y \cdot z) = xy + xz + \cancel{xy + x}\ xyz =$
$= x(y + z + yz) = xy + xz + xyz$

$xyz = x^2yz = xyxz$ ✓

From Boolean Algebra $(R, +, \cdot)$ we have constructed distr. comple. lattice by defining $r \le s \iff r \cdot s = r$.