From syllogism to common sense: a tour through the logical landscape

Propositional logic 2

Mehul Bhatt Oliver Kutz *Thomas Schneider*

1 December 2011

And now ...

Propositional logic ...

- assumes that there are two truth values (bivalence)
- assumes that the truth value of a sentence depends only on the truth value of its parts (extensionality)
- connects atomic propositions using connectives that correspond to Boolean functions
  and, or, not, if-then, iff, nand, nor
- uses a recursive definition to define formulas
- uses the induction principle to prove properties of fma.s
- enjoys the unique formula reconstruction property, which allows to define functions over fma.s recursively

Semantics of Boolean formulas ...

- is given by valuations $w : \text{PV} \to \{0, 1\}$, which can be extended to $w : \mathcal{F} \to \{0, 1\}$
- gives rise to the correspondence formulas $\rightsquigarrow$ Boolean fct.s:
  $\alpha \in \mathcal{F}_n$ represents Boolean function $f \in \mathcal{B}_n$
  if, for all valuations w, it holds that $w\alpha = f(wp_1, \ldots, wp_n)$.

And now ...

What's in this section?

We want to ...

- define when two formulas are logically equivalent
- show that every Boolean function is representable by a formula
- establish the duality principle for two-valued logic

Semantic equivalence

- Formulas α, β are (logically or semantically) equivalent, written $\alpha \equiv \beta$, if for all valuations w: $w\alpha = w\beta$.
- Obviously, $\alpha \equiv \beta$ iff α, β represent the same n-ary function for some $n \geqslant 0$
- Example: $\alpha \equiv \neg\neg\alpha$

$\rightsquigarrow$ At most how many formulas in $\mathcal{F}_n$ can be pairwise inequivalent?

(Note the difference between $\alpha \equiv \beta$ and $\alpha = \beta$.
The latter denotes identity of the strings α, β.)

Prominent examples of equivalences

$$\begin{array}{rclrcll}
\alpha\wedge(\beta\wedge\gamma) & \equiv & \alpha\wedge\beta\wedge\gamma, & \alpha\vee(\beta\vee\gamma) & \equiv & \alpha\vee\beta\vee\gamma & \text{(associativity);}\\
\alpha\wedge\beta & \equiv & \beta\wedge\alpha, & \alpha\vee\beta & \equiv & \beta\vee\alpha & \text{(commutativity);}\\
\alpha\wedge\alpha & \equiv & \alpha, & \alpha\vee\alpha & \equiv & \alpha & \text{(idempotency);}\\
\alpha\wedge(\alpha\vee\beta) & \equiv & \alpha, & \alpha\vee\alpha\wedge\beta & \equiv & \alpha & \text{(absorption);}\\
\alpha\wedge(\beta\vee\gamma) & \equiv & \alpha\wedge\beta\vee\alpha\wedge\gamma, & & & & (\wedge\text{-distributivity});\\
\alpha\vee\beta\wedge\gamma & \equiv & (\alpha\vee\beta)\wedge(\alpha\vee\gamma) & & & & (\vee\text{-distributivity});\\
\neg(\alpha\wedge\beta) & \equiv & \neg\alpha\vee\neg\beta, & \neg(\alpha\vee\beta) & \equiv & \neg\alpha\wedge\neg\beta & \text{(de Morgan rules).}
\end{array}$$

From W. Rautenberg: A Concise Introduction to Mathematical Logic, Springer, 2010.

$$\alpha \wedge \neg\alpha \equiv \bot \qquad \alpha \wedge \top \equiv \alpha$$
$$\alpha \vee \neg\alpha \equiv \top \qquad \alpha \vee \top \equiv \top$$

$$\alpha \to \beta \;\equiv\; \neg\alpha \vee \beta \;\equiv\; \neg(\alpha \wedge \neg\beta)$$
$$\alpha \to \beta \to \gamma \;\equiv\; \alpha \wedge \beta \to \gamma \;\equiv\; \beta \to \alpha \to \gamma$$

(Augustus De Morgan, 1806–1871, British math./logician, Cambridge/London)

A strange natural language example

Consider the two sentences:

1. Students and pensioners pay half price.
2. Students or pensioners pay half price.

They evidently have the same meaning – but why?

- Abbreviate *student*, *pensioners*, *pay half price* by S, P, H.
- The sentences can be put into propositions as follows.
  1. $\alpha = (S \to H) \wedge (P \to H)$
  2. $\beta = (S \vee P) \to H$
- Now $\alpha \equiv \beta$ (check via truth tables)

Properties of semantic equivalence

- Obviously, $\equiv$ is an equivalence relation:
  - $\alpha \equiv \alpha$ (reflexivity)
  - if $\alpha \equiv \beta$, then $\beta \equiv \alpha$ (symmetry)
  - if $\alpha \equiv \beta$ and $\beta \equiv \gamma$, then $\alpha \equiv \gamma$ (transitivity)
- Also, $\equiv$ is a congruence relation on $\mathcal{F}$:
  If $\alpha \equiv \alpha'$ and $\beta \equiv \beta'$,
  then $\alpha \wedge \beta \equiv \alpha' \wedge \beta'$, $\alpha \vee \beta \equiv \alpha' \vee \beta'$, and $\neg\alpha \equiv \neg\alpha'$
- Consequence: Replacement theorem

Theorem

Let $\alpha \equiv \alpha'$ and φ be formulas,
and let φ' be obtained from φ by replacing one or several occurrences of α with α'.

Then $\varphi \equiv \varphi'$.

(Proof by induction on φ.)

Negation normal form

- Consider the equivalences

$$\begin{aligned} \neg\neg\alpha &\equiv \alpha \\ \neg(\alpha \wedge \beta) &\equiv \neg\alpha \vee \neg\beta \\ \neg(\alpha \vee \beta) &\equiv \neg\alpha \wedge \neg\beta \end{aligned}$$

- Take an arbitrary formula φ,
  systematically apply these equivalences as replacement rules.

$\Rightarrow$ In the resulting formula $\varphi' \equiv \varphi$,
negation only occurs in front of variables.

φ' is in negation normal form (NNF)

Example:

$$\neg(p \wedge q \vee \neg r) \;\equiv\; \neg(p \wedge q) \wedge \neg\neg r \;\equiv\; (\neg p \vee \neg q) \wedge r$$

Conjunctive and disjunctive normal forms

- A literal is an atomic formula or a negation thereof.
- A disjunctive normal form (DNF) is a disjunction
  $\alpha_1 \vee \cdots \vee \alpha_n$, where each α_i is a conjunction of literals.
- A conjunctive normal form (CNF) is a conjunction
  $\alpha_1 \wedge \cdots \wedge \alpha_n$, where each α_i is a disjunction of literals.
- Examples:
  - $(p \wedge \neg q \wedge r) \vee (q \wedge r) \vee (\neg p \wedge r)$ is a DNF.
  - $p \vee q$ is both a DNF and CNF.
  - $p \vee (q \wedge \neg p)$ is neither a DNF nor a CNF.
- Every fma can be transformed into an equivalent DNF (CNF).

Transforming a formula into an equivalent DNF (CNF)

- Idea: for arbitrary n-ary Boolean fct. f in tabular form, compute a DNF α_f (CNF β_f) representing f
- Notation: $p^1 = p$ and $p^0 = \neg p$
- Then:

$$\alpha_f = \bigvee_{f(x_1,\dots,x_n)=1} p_1^{x_1} \wedge \cdots \wedge p_n^{x_n}$$

$$\beta_f = \bigwedge_{f(x_1,\dots,x_n)=0} p_1^{\neg x_1} \vee \cdots \vee p_n^{\neg x_n}$$

- Example: exclusive-or function $+$ has …
  - DNF $(p \wedge \neg q) \vee (\neg q \wedge q)$
  - CNF $(p \vee q) \wedge (\neg p \vee \neg q)$

Consequence

Every $\varphi \in \mathcal{F}$ is equivalent to a DNF and to a CNF.

Functional completeness

- A logical signature S is called functional complete if every Boolean function is represented by some formula in S.
- By construction on previous slide: $\{\neg, \wedge, \vee\}$ is functional complete.
- Can leave out either $\wedge$ or $\vee$ because of the equivalences $p \vee q \equiv \neg(\neg p \wedge \neg q)$ and $p \wedge q \equiv \neg(\neg p \vee \neg q)$

Consequence

Both $\{\neg, \wedge\}$ and $\{\neg, \vee\}$ are functional complete.

Functional completeness

- Another functional complete signature: $\{\rightarrow, 0\}$

  can express $\neg, \wedge$ in $\{\rightarrow, 0\}$:
  $\neg p \equiv p \rightarrow 0, \quad p \wedge q \equiv \neg(p \rightarrow \neg q)$
- Functional complete *singleton* signatures: $\{\uparrow\}$, $\{\downarrow\}$

  (see table on Slide 9 of the previous sets of slides, try yourself)
- A *not* functional complete signature: $\{\rightarrow, \wedge, \vee\}$
  - For every w with $wp = 1$ for all p, and every φ in $\{\rightarrow, \wedge, \vee\}$: $w\varphi = 1$.

  $\Rightarrow$ Never $\neg p \equiv \varphi$ for any such formula φ

  $\Rightarrow$ $\neg$ cannot be expressed in $\{\rightarrow, \wedge, \vee\}$

Duality for formulas

- Given a formula φ, we obtain its dual formula φ^δ by interchanging $\wedge$ and $\vee$:

$$p^\delta = p \qquad (\alpha \wedge \beta)^\delta = \alpha^\delta \vee \beta^\delta$$
$$(\neg\alpha)^\delta = \neg\alpha \qquad (\alpha \vee \beta)^\delta = \alpha^\delta \wedge \beta^\delta$$

- Obviously:

  α is a DNF $\Rightarrow$ α^δ is a CNF

  α is a CNF $\Rightarrow$ α^δ is a DNF

Duality for Boolean functions

- Given a Boolean fct. $f \in \mathcal{B}_n$, we obtain its dual function f^δ by negating arguments and function value: (cf. de Morgan)

$$f^\delta(x_1, \dots, x_n) = \neg f(\neg x_1, \dots, \neg x_n)$$

- Obviously, $(f^\delta)^\delta = f$.
- Observation:

$$\begin{array}{llll} \wedge^\delta = \vee & \leftrightarrow^\delta = + & \downarrow^\delta = \uparrow & \neg^\delta = \neg \\ \vee^\delta = \wedge & +^\delta = \leftrightarrow & \uparrow^\delta = \downarrow & \end{array}$$

  That is, $\neg$ is self-dual.
- As an aside:
  - There are no *essentially* binary self-dual Boolean functions.
  - Dedekind discovered the following ternary self-dual function.

$$d_3 : (x, y, z) \;\mapsto\; x \wedge y \;\vee\; x \wedge z \;\vee\; y \wedge z$$

(Richard Dedekind, 1831–1916, German mathematician, BS, GÖ, B, Zürich)

The duality principle for two-valued logic

Theorem

If α represents the function f,
then α^δ represents the dual function f^δ.

(Proof by induction on α.)

Consequences:

- We know that $\leftrightarrow$ is represented by $p \wedge q \;\vee\; \neg p \wedge \neg q$.
  Hence $+$ is represented by $(p \vee q) \wedge (\neg p \vee \neg q)$.
- If a canonical DNF α represents $f \in \mathcal{B}_n$,
  then the canonical CNF α^δ represents f^δ.
- Since Dedekind's d_3 is self-dual, it holds that:

$$p \wedge q \;\vee\; p \wedge r \;\vee\; q \wedge r \;\equiv\; (p \vee q) \wedge (p \vee r) \wedge (q \vee r)$$

And now ...

What's in this section?

We want to ...

- define when a formula is "always true" (a tautology) or "can be true" (is satisfiable)
- look at the decision problem for tautologies/satisfiablity
- define when a set of fmas is a logical consequence of another
- examine properties of logical consequence

Satisfiability and models

- instead of $w\alpha = 1$, write $w \models \alpha$, read w satisfies α
- for a set X of fmas, write $w \models X$ for "$w \models \alpha$ for *all* $\alpha \in X$"
  read w is a (propositional) model for X
- α is satisfiable if $(w \models \alpha)$ for *some* w (analogously for X)
- satisfaction relation $\models$ evidently has the following properties:

$$\begin{array}{lcl} w \models p & \Leftrightarrow & wp = 1 \quad (p \in \mathrm{PV}) \\ w \models \neg\alpha & \Leftrightarrow & w \not\models \alpha \\ w \models \alpha \wedge \beta & \Leftrightarrow & w \models \alpha \text{ and } w \models \beta \\ w \models \alpha \vee \beta & \Leftrightarrow & w \models \alpha \text{ or } w \models \beta \end{array}$$

(and can again be extended to other connectives, e.g., $\rightarrow$)

Tautologies

- α is logically valid or a tautology, written $\models \alpha$,
  if $w \models \alpha$ for all valuations w
- α is a contradiction if α is not satisfiable, i.e.,
  if $w \not\models \alpha$ for all valuations w
- Examples for tautologies
  - $p \vee \neg p$
  - even $\alpha \vee \neg\alpha$ for any formula α
    law of excluded middle *(tertium non datur)*
- Examples for contradictions
  - $\alpha \wedge \neg\alpha$
  - $\alpha \leftrightarrow \neg\alpha$

Classical tautologies in $\rightarrow$

$$\begin{array}{ll} p \rightarrow p & \text{(self-implication)}, \\ (p \rightarrow q) \rightarrow (q \rightarrow r) \rightarrow (p \rightarrow r) & \text{(chain rule)}, \\ (p \rightarrow q \rightarrow r) \rightarrow (q \rightarrow p \rightarrow r) & \text{(exchange of premises)}, \\ p \rightarrow q \rightarrow p & \text{(premise charge)}, \\ (p \rightarrow q \rightarrow r) \rightarrow (p \rightarrow q) \rightarrow (p \rightarrow r) & \text{(Frege's formula)}, \\ ((p \rightarrow q) \rightarrow p) \rightarrow p & \text{(Peirce's formula)}. \end{array}$$

From W. Rautenberg: A Concise Introduction to Mathematical Logic, Springer, 2010.

Later: all tautologies in $\rightarrow$ derivable from the last 3 fma.s

Decidability of the tautology and satisfiability problems

Decidable problems:

- Given α, is α a tautology?
- Given α, is α satisfiable?

Decision procedure for satisfiability

input α
for every valuation w of the variables of α {
  if $(w \models \alpha)$ /* polynomial-time subroutine */
    then return "satisfiable"
}
return "unsatisfiable"

- Deterministic, exponential-time procedure
- Analogous procedure for tautology problem

Complexity of tautology and satisfiability problems

Nondeterministic decision procedure for satisfiability

input α
guess valuation w of the variables of α
if ($w \models \alpha$)
  then return 1
  else return 0

- Nondeterministic, polynomial-time procedure
- Analogous procedure for tautology problem

$\Rightarrow$ SAT $\in$ NP, TAUT $\in$ coNP

- SAT (TAUT) is NP-hard (coNP-hard) [Cook, Levin 1971–3]

Reduction to the tautology problem

Various questions such as checking the equivalence of formulas can be reduced to deciding tautologies:

e.g., $\alpha \equiv \beta$ iff $\models \alpha \leftrightarrow \beta$

Decision procedure for equivalence using tautology test

input α, β
if $\alpha \leftrightarrow \beta$ is a tautology
  then return "equivalent"
  else return "not equivalent"

Logical consequence

Let α be a formula and X a set of formulas.

- α is a logical consequence of X, written $X \models \alpha$, if every model of X satisfies α, i.e., $w \models X$ implies $w \models \alpha$ for all valuations w
- Overload the symbol $\models$: meaning "consequence" or "satisfies" or "tautology" (particular meaning is always clear from context)
- Clear: α is a tautology iff $\emptyset \models \alpha$
  $\rightsquigarrow$ "$\models \alpha$" can be seen as abbreviation of "$\emptyset \models \alpha$"

Some convenience notation

- $X \models \alpha, \beta$ means "$X \models \alpha$ and $X \models \beta$"
- $X \models Y$ means "$X \models \alpha$ for all $\alpha \in Y$"
- $\alpha_1, \ldots, \alpha_n \models \beta$ means "$\{\alpha_1, \ldots, \alpha_n\} \models \beta$"
- $X, \alpha \models \beta$ means "$X \cup \{\alpha\} \models \beta$"

Examples of logical consequence

- $\alpha, \beta \models \alpha \wedge \beta$ (consult truth table of $\wedge$)
- $\alpha \wedge \beta \models \alpha, \beta$ (ditto)
- $\alpha,\ \alpha \to \beta \models \beta$ (truth table: if $1 \to x = 1$, then $x = 1$)
  modus ponens
- $X \models \bot$, then $X \models \alpha$ for each α
  (because $X \models \bot$ means that X has *no* model)
- If $X, \alpha \models \beta$ and $X, \neg\alpha \models \beta$, then $X \models \beta$
  (Take $w \models X$. If $w \models \alpha$, conclude $w \models \beta$ from first assumption.
  If $w \not\models \alpha$, i.e., $w \models \neg\alpha$, conclude $w \models \beta$ from second assumption.)
  "proof by case distinction"

General properties of logical consequence

Reflexivity
If $\alpha \in X$, then $X \models \alpha$.

Monotonicity
If $X \models \alpha$ and $X \subseteq X'$, then $X' \models \alpha$.

Transitivity
If $X \models Y$ and $Y \models \alpha$, then $X \models \alpha$.

Substitution invariance
If $X \models \alpha$, then $X^\sigma \models \alpha^\sigma$, where

- σ is a substitution, i.e., a mapping $\sigma : \mathrm{PV} \to \mathcal{F}$
- σ is extended to formulas naturally:
  α^σ = result of replacing all variables p in α with $\sigma(p)$
- X^σ is "X with σ applied to all fmas in X"
- Example: from $p \vee \neg p$ being a tautology,
  we can infer that $\alpha \vee \neg\alpha$ is a taut., for every α

More properties of logical consequence

$\models$ shares the previous 4 properties with almost all classical and non-classical (many-valued) propositional consequence relations.

Special properties of $\models$:

Finitarity
If $X \models \alpha$, then $X_0 \models \alpha$ for some finite subset $X_0 \subseteq X$.

Deduction theorem
If $X, \alpha \models \beta$, then $X \models \alpha \to \beta$

makes it easy to prove tautologies:
$\models p \to q \to p$ because $p \models q \to p$ because $p, q \models p$ (refl.)

And now ...

What's in this section?

We want to ...

- find a means to "compute" $\models$ *syntactically*:
- define a derivability relation $\vdash$ by means of a calculus that operates solely on the structure of formulas
- prove that $\vdash$ and $\models$ are identical

The $\vdash$ calculus is of the Gentzen type

(Gerhard Gentzen, 1909–1945, German mathematician/logician, GÖ, Prague)

Basic notation

- Again, use α for formulas and X for sets thereof
- Write $X \vdash \alpha$ to denote: "α is derivable (provable) from X"
- Gentzen called the pairs (X, α) in the $\vdash$-relation sequents
- sequent calculus consists of 6 basic rules (for $\{\wedge, \neg\}$) of the form

$$\frac{\text{premise}}{\text{conclusion}}$$

The basic rules

$$(\mathrm{IS}) \ \frac{}{\alpha \vdash \alpha} \ (\text{initial sequent}) \qquad (\mathrm{MR}) \ \frac{X \vdash \alpha}{X' \vdash \alpha} \ (X' \supseteq X),$$

$$(\wedge 1) \ \frac{X \vdash \alpha, \beta}{X \vdash \alpha \wedge \beta} \qquad (\wedge 2) \ \frac{X \vdash \alpha \wedge \beta}{X \vdash \alpha, \beta}$$

$$(\neg 1) \ \frac{X \vdash \alpha, \neg\alpha}{X \vdash \beta} \qquad (\neg 2) \ \frac{X, \alpha \vdash \beta \ \big| \ X, \neg\alpha \vdash \beta}{X \vdash \beta}$$

From W. Rautenberg: A Concise Introduction to Mathematical Logic, Springer, 2010.

- use convenience notation as for $\models$, see Slide 48
- (IS) has no premises; initial sequences start derivations
- (MR): monotonicity rule
- $(\wedge 1)$, $(\neg 1)$, $(\neg 2)$ have two premises; $(\wedge 2)$ has two conclusions $\rightsquigarrow$ is actually 2 rules

Using the calculus

- derivation = finite sequence $S_0, \ldots, S_n$ of sequents where every S_i is either
  - an initial sequent or
  - is obtained by applying some basic rule to elements from $S_0, \ldots, S_{i-1}$
- α is derivable (or provable) from X, written $X \vdash \alpha$, if there is a derivation with $S_n = X \vdash \alpha$.

Examples

1	$\alpha \vdash \alpha$	(IS)
2	$\alpha, \beta \vdash \alpha$	(MR) 1
3	$\beta \vdash \beta$	(IS)
4	$\alpha, \beta \vdash \beta$	(MR) 3
5	$\alpha, \beta \vdash \alpha \wedge \beta$	$(\wedge 1)$ 2, 4 $\Rightarrow$ $\underline{\underline{\{\alpha, \beta\} \vdash \alpha \wedge \beta}}$

1	$p \wedge \neg p \vdash p \wedge \neg p$	(IS)
2	$p \wedge \neg p \vdash p$	$(\wedge 2)$ 1
3	$p \wedge \neg p \vdash \neg p$	$(\wedge 2)$ 1
4	$p \wedge \neg p \vdash \neg(p \wedge \neg p)$	$(\neg 1)$ 2, 3
5	$\neg(p \wedge \neg p) \vdash \neg(p \wedge \neg p)$	(IS)
6	$\emptyset \vdash \neg(p \wedge \neg p)$	$(\neg 2)$ 4, 5 $\Rightarrow$ $\underline{\underline{\vdash \top}}$

. . .

. . .

And now . . .

. . .

. . .