

Logical reasoning and programming

Introduction, propositional logic, and SAT

Karel Chvalovský

CIIRC CTU

What is a formal logic?

It studies inferences. Given a statement φ and a collection of statements Γ , the main problem is whether

φ follows logically from Γ .

The word “formal” here means that only the logical forms of statements matter.

Example

Let statements in Γ describe rules of chess and φ be “Black can always draw.”

Declarative programming

Specify a problem and ask queries.

Syntax and semantics in logic

Syntax

We describe our language and hence we define well-formed statements, called formulae. We want a mechanical calculus that describes how to derive (prove) formulae.

Semantics

We describe the meaning of formulae. The main notions are validity and semantic consequence.

We always want our syntax and semantics to be adequate:

- correctness** only valid formulae are derivable (provable),
- completeness** all valid formulae are derivable (provable).

Fragments from the history of logic

- ▶ Aristotle (384–322 BC) — syllogisms
- ▶ Gottfried Wilhelm Leibniz (1646–1716) — the first attempt to reduce a logical inference to a mechanical process
- ▶ George Boole (1815–1864) — Boolean logic
- ▶ Modern logic was established mainly to deal with issues in the foundations of mathematics in the late 19th century and early 20th century.

Paradoxes

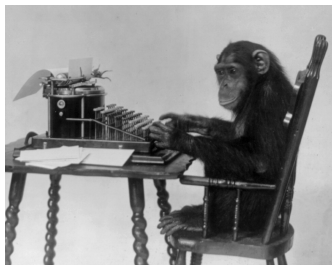
Many paradoxes occurred in set theory, e.g., Russell's paradox. Let $R = \{x : x \notin x\}$, then $R \in R$ iff $R \notin R$. The moral of this is that without solid formal foundations surprising problems can emerge.

Automated theorem proving (ATP)

We have machines so use them to prove things for us. How to do that?

British Museum algorithm

Exhaustively check all possibilities one by one.



If monkeys are placed in front of typewriters and they type in a guaranteed random fashion, they will reproduce all the books of the library of the British Museum, provided they could type long enough.

(Wirth et al. 2009).

We usually have much better options. However, formal methods have their theoretical limits.

Limits of formal methods

Two famous fundamental theoretical problems are:

Incompleteness

Gödel's first incompleteness theorem says that it is impossible to describe basic arithmetic of the natural numbers by a set of axioms that is algorithmically recognizable.

Undecidability

Church and Turing famously proved that there is no decision procedure (algorithm) for validity in first-order logic (FOL). For example the halting problem is expressible in FOL.

It is good to be aware of these results, however, it is also good not to overrate them. We usually face more basic problems.

What are some areas where formal methods occur?

- ▶ mathematics
 - ▶ the Robbins problem
 - ▶ the Boolean Pythagorean triples problem
- ▶ verification
 - ▶ hardware
 - ▶ chip verification at Intel
 - ▶ software
 - ▶ many companies — Amazon, Facebook, Microsoft, . . .
 - ▶ seL4 — verified operating system microkernel
 - ▶ CompCert — verified C compiler
 - ▶ EURO-MILS — verified virtualization platform
 - ▶ CakeML — verified compiler for Standard ML
- ▶ mathematics
 - ▶ the Kepler conjecture

How to select a formal system?

We choose a formal system that is expressive enough to (reasonably) describe the problem and we usually prefer the weakest such system for computational reasons.

Examples of used formal systems include

- ▶ propositional logic — for problems in NP,
- ▶ quantified Boolean formulae (QBF) — for problems in PSPACE,
- ▶ modal (temporal) logics — in verification,
- ▶ satisfiability modulo theories (SMT) — for decidable problems,
- ▶ first-order logic (FOL),
- ▶ higher-order logics (HOL).

Propositional logic

Simple, yet quite powerful, formal system. We have elementary propositions called atomic formulae, or atoms, which can be assigned *truth values*¹, and combine them using Boolean connectives (functions) into more complex propositions.

Example

If I am clever, then I will pass.

- ▶ “I am clever” and “I will pass” are propositions, say p and q , respectively.
- ▶ “if ... then ...” is a connective, called implication and denoted \rightarrow .

Hence the logical form of the sentence in propositional logic is $p \rightarrow q$.

¹1 is true and 0 is false.

Formulae

Placeholders for atomic formulae (propositions) are called propositional variables *Var*, say p, q, r, \dots . We also have a unary connective negation (\neg) and binary connectives conjunction (\wedge), disjunction (\vee), and implication (\rightarrow).²

Definition

The set of (propositional) formulae *Fml* is the smallest set satisfying:

- ▶ every propositional variable is a formula,
- ▶ if φ is a formula, then $(\neg\varphi)$ is a formula,
- ▶ if φ and ψ are formulae, then $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, and $(\varphi \rightarrow \psi)$ are formulae.

We usually write only parentheses that are necessary for unambiguous reading.

A formula ψ is a *subformula* of φ if ψ is a substring of φ .

²We also use $\varphi \leftrightarrow \psi$ as a shortcut for $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.

Semantics

Formally describes the meaning of formulae.

A valuation v is an assignment of truth values to propositional variables, that is a function $v: Var \rightarrow \{0, 1\}$. It can be uniquely extended to all formulae, because connectives are functions of truth values, and we freely use valuations this way.

Hence $v(\neg\varphi) = 1 - v(\varphi)$ and $v(\varphi \circ \psi) = v(\varphi) \bullet v(\psi)$, for $\circ \in \{\wedge, \vee, \rightarrow\}$, where \bullet is the Boolean function defining \circ .

If $v(\varphi) = 1$, then we also write $v \models \varphi$ and say “formula φ is satisfied by valuation v ” or “valuation v satisfies formula φ ”.

Truth tables

Example

$v(p)$	$v(q)$	$v(p \rightarrow q)$
0	0	1
0	1	1
1	0	0
1	1	1

Let φ be a formula and v, v' be two valuations such that they are equal on all propositional variables occurring in φ , then clearly $v(\varphi) = v'(\varphi)$. Hence only the valuation of variables occurring in a formula matters.

Semantic consequence I.

A formula φ follows from (or is a consequence of) a formula ψ , we write $\psi \models \varphi$, if φ is satisfied by every valuation v that satisfies ψ .

Relation \models is clearly reflexive and transitive, but not symmetric.

Two formulae φ and ψ are equivalent, we write $\varphi \equiv \psi$ or $\varphi \models \psi$, if $\varphi \models \psi$ and $\psi \models \varphi$.

A very important property of propositional logic is that we can freely replace a subformula by an equivalent formula. Formally, let ψ be a subformula of φ and $\psi \equiv \chi$. If we replace ψ in φ by χ , then the resulting formula is equivalent to φ .

Some useful properties of $\{\neg, \wedge, \vee\}$

The following equivalences hold

- ▶ $\varphi \equiv \neg\neg\varphi$, (double negation)
- ▶ $\varphi \equiv \varphi \circ \varphi$, for $\circ \in \{\wedge, \vee\}$, (idempotency)
- ▶ $\varphi \circ \psi \equiv \psi \circ \varphi$, for $\circ \in \{\wedge, \vee\}$, (commutativity)
- ▶ $\varphi \circ (\psi \circ \chi) \equiv (\varphi \circ \psi) \circ \chi$ for $\circ \in \{\wedge, \vee\}$, (associativity)
- ▶ $\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$, (DeMorgan's law)
- ▶ $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$, (DeMorgan's law)
- ▶ $\varphi \wedge (\psi \vee \chi) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \chi)$, (distributivity)
- ▶ $\varphi \vee (\psi \wedge \chi) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \chi)$ (distributivity)

for all formulae φ , ψ , and χ .

Thanks to associativity we can write $\varphi_1 \circ \dots \circ \varphi_n$ without parentheses, for $\circ \in \{\wedge, \vee\}$.

Some useful properties of \rightarrow

The following equivalences hold

- ▶ $\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi,$
- ▶ $\varphi \rightarrow \psi \equiv \neg(\varphi \wedge \neg\psi),$
- ▶ $\varphi \rightarrow \psi \equiv \neg\psi \rightarrow \neg\varphi,$
- ▶ $\varphi \rightarrow (\psi \rightarrow \chi) \equiv \psi \rightarrow (\varphi \rightarrow \chi),$
- ▶ $\varphi \rightarrow (\psi \rightarrow \chi) \equiv (\varphi \wedge \psi) \rightarrow \chi,$
- ▶ $(\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow (\psi_1 \vee \dots \vee \psi_m) \equiv \neg\varphi_1 \vee \dots \vee \neg\varphi_n \vee \psi_1 \vee \dots \vee \psi_m$

for all formulae φ , ψ , χ , φ_i , and ψ_i .

Some further useful properties

The following relations hold

- ▶ $\varphi \models \varphi \vee \psi$,
- ▶ $\varphi \wedge \psi \models \varphi$,
- ▶ $\varphi \models \psi \rightarrow \varphi$,
- ▶ $\neg\varphi \models \varphi \rightarrow \psi$

for all formulae φ , ψ , and χ .

Semantic consequence II.

A formula φ follows from a set of formulae Γ , we write $\Gamma \models \varphi$, if φ is satisfied by every valuation v that satisfies all formulae in Γ .

$$\Gamma \models \varphi \text{ iff } \forall v(\text{if } v \models \Gamma \text{ then } v \models \varphi),$$

where $v \models \Gamma$ means that $v \models \psi$ for all $\psi \in \Gamma$. We also say that φ is a consequence of Γ .

The relation is clearly monotone, if $\Gamma \models \varphi$, then $\Gamma \cup \Delta \models \varphi$.

We have $\Gamma \cup \varphi \models \psi$ iff $\Gamma \models \varphi \rightarrow \psi$. Hence $\varphi \models \psi$ iff $\models \varphi \rightarrow \psi$.
Hence $\varphi \equiv \psi$ iff $\models \varphi \leftrightarrow \psi$.

Example

$$p, p \rightarrow q, q \rightarrow r \models r$$

$$p \rightarrow q, q \rightarrow r \models p \rightarrow r$$

$$p \rightarrow q \models (q \rightarrow r) \rightarrow (p \rightarrow r)$$

$$\models (p \rightarrow q) \rightarrow ((q \rightarrow r) \rightarrow (p \rightarrow r))$$

Satisfiable formulae and tautologies

We say that a formula φ is

- ▶ *satisfiable* if there is a valuation v s.t. $v(\varphi) = 1$, that is $v \models \varphi$,
- ▶ *tautology* if for every valuation v holds $v(\varphi) = 1$, that is $\models \varphi$,
- ▶ *contradiction* if for every valuation v holds $v(\varphi) = 0$, we also call it *unsatisfiable*.

Two formulae φ and ψ are *equisatisfiable* if either both formulae are satisfiable, or both are unsatisfiable.

We call the set of all satisfiable and tautological formulae SAT and TAUT, respectively.

For any formula φ we have

$$\varphi \in \text{TAUT} \quad \text{iff} \quad \neg\varphi \text{ is a contradiction} \quad \text{iff} \quad \neg\varphi \notin \text{SAT}$$

and hence

$$\neg\varphi \notin \text{TAUT} \quad \text{iff} \quad \varphi \text{ is not a contradiction} \quad \text{iff} \quad \varphi \in \text{SAT}.$$

Special formulae \top and \perp

We either define special formulae \top and \perp directly as propositional constants (nullary connectives), $v(\top) = 1$ and $v(\perp) = 0$ for every valuation v , or equivalently we can define them as shortcuts

$\top = p \vee \neg p$ and $\perp = p \wedge \neg p$.

The following relations hold

- ▶ $\models \top$,
- ▶ $\perp \models \varphi$,
- ▶ if $\varphi \in \text{TAUT}$, then $\varphi \equiv \top$,
- ▶ if $\varphi \notin \text{SAT}$, then $\varphi \equiv \perp$

for every formula φ .

Some further useful properties

It is possible to have both $\varphi \in \text{SAT}$ and $\neg\varphi \in \text{SAT}$.

If $\varphi \in \text{TAUT}$, then $\varphi \in \text{SAT}$. Hence $\text{TAUT} \subset \text{SAT}$.

A set of formulae Γ is satisfiable, we write $\Gamma \in \text{SAT}$, if there is a valuation v such that $v \models \varphi$ for every formula $\varphi \in \Gamma$.

If $\Gamma \cup \Delta \in \text{SAT}$, then $\Gamma \in \text{SAT}$ and $\Delta \in \text{SAT}$.

It is known that deciding $\varphi \in \text{SAT}$ is an NP-complete problem and hence $\varphi \in \text{TAUT}$ is a coNP-complete problem. Therefore any problem in NP can be formulated as a satisfiability question, without greatly (see polynomial reductions) increasing the problem size.

Normal forms

A *literal* is a propositional variable p or a negation of propositional variable $\neg p$. In this context we write \bar{p} instead of $\neg p$. A *clause* is any disjunction of finitely many literals. An important special case is the empty clause, we write \square .

A formula φ is in conjunctive normal form (CNF) if φ is a conjunction of clauses.

Remark

Analogously disjunctive normal form (DNF) is defined as a disjunction of conjunctions of literals.

Theorem

For every formula φ exist formulae φ' in CNF and φ'' in DNF such that φ , φ' , and φ'' are all equivalent.

Example

Formula $(p \rightarrow q) \wedge (q \rightarrow p)$ is equivalent to $(\bar{p} \vee q) \wedge (\bar{q} \vee p)$ and $(\bar{p} \wedge \bar{q}) \vee (p \wedge q)$.

DNF

Easy to obtain using truth tables:

p	q	$(p \rightarrow q) \wedge (q \rightarrow p)$	
0	0	1	$\neg p \wedge \neg q$
0	1	0	
1	0	0	
1	1	1	$p \wedge q$

A formula in DNF obtained this way is in so called full disjunctive normal form. It is a unique representation up to ordering.

It is easy to test whether a formula in DNF is satisfiable, but transforming a formula into DNF can lead to an exponential increase in the size of formula, see later. Hence we, perhaps surprisingly, prefer CNF for testing satisfiability. The reasons will be clear later on.

CNF

We obtain a CNF from a formula using following steps:

1. First, use the following rewriting rules as long as possible:

$$\begin{aligned}\varphi \rightarrow \psi &\rightsquigarrow \neg\varphi \vee \psi \\ \neg\neg\varphi &\rightsquigarrow \varphi \\ \neg(\varphi \vee \psi) &\rightsquigarrow \neg\varphi \wedge \neg\psi && \text{DeMorgan's law} \\ \neg(\varphi \wedge \psi) &\rightsquigarrow \neg\varphi \vee \neg\psi && \text{DeMorgan's law}\end{aligned}$$

2. Second, distribute disjunctions until a CNF is obtained:

$$\begin{aligned}\varphi \vee (\psi \wedge \chi) &\rightsquigarrow (\varphi \vee \psi) \wedge (\varphi \vee \chi) \\ (\psi \wedge \chi) \vee \varphi &\rightsquigarrow (\psi \vee \varphi) \wedge (\chi \vee \varphi)\end{aligned}$$

Some properties of normal forms

Formulae can be transformed to normal forms in many ways and this can significantly influence their size and also the behavior of algorithms used for testing satisfiability.

Remark

Normal forms are not unique, e.g., $(p \rightarrow q) \wedge (q \rightarrow r) \wedge (r \rightarrow p)$ is equivalent to both $(\bar{p} \vee q) \wedge (\bar{q} \vee r) \wedge (\bar{r} \vee p)$ and $(\bar{p} \vee r) \wedge (\bar{q} \vee p) \wedge (\bar{r} \vee q)$.

Example

Transforming

$$\varphi = (p_1 \wedge q_1) \vee \cdots \vee (p_n \wedge q_n)$$

into a CNF leads to

$$\varphi' = \bigwedge_{\Delta} \bigvee \Delta, \text{ where } \Delta = \{ r_i : \text{either } r_i = p_i, \text{ or } r_i = q_i, \text{ for } 1 \leq i \leq n \}.$$

Hence the length of φ' is $\mathcal{O}(2^n)$, but the length of φ is $\mathcal{O}(n)$.

Tseytin transformation

We can avoid this possible exponential blowup³ by introducing new variables that encode values of all subformulae in the original formula. The obtained formula is not equivalent (it has new variables) to the original one, but they are equisatisfiable.

Example

For $\varphi = (p_1 \wedge q_1) \vee \cdots \vee (p_n \wedge q_n)$ we set

$$r_i \leftrightarrow (p_i \wedge q_i),$$

for $1 \leq i \leq n$, that is equivalent to

$$(\bar{p}_i \vee \bar{q}_i \vee r_i) \wedge (p_i \vee \bar{r}_i) \wedge (q_i \vee \bar{r}_i).$$

Taking a conjunction of all these formulae and $r_1 \vee \cdots \vee r_n$ gives us a formula φ' in a CNF such that φ and φ' are equisatisfiable. Moreover, $|\varphi'| = \mathcal{O}(|\varphi|)$.

³If connectives occurring in the formula have linear clausal encoding.

Tseytin transformation — algorithm

Let φ be a non-atomic formula and ψ_1, \dots, ψ_m be all unique non-atomic subformulae of φ such that no ψ_i is a subformula of ψ_j if $1 \leq j < i \leq m$. Hence $\psi_m = \varphi$. Let $\{r_1, \dots, r_m\}$ be fresh variables not occurring in φ .

Start with $\Delta = \emptyset$. Iteratively process ψ_i , for $1 \leq i \leq m$, as follows

- if $\psi_i = \bar{p}$ add $(\bar{p} \vee \bar{r}_i) \wedge (p \vee r_i)$ to Δ ,
- if $\psi_i = p \wedge q$ add $(\bar{p} \vee \bar{q} \vee r_i) \wedge (p \vee \bar{r}_i) \wedge (q \vee \bar{r}_i)$ to Δ ,
- if $\psi_i = p \vee q$ add $(p \vee q \vee \bar{r}_i) \wedge (\bar{p} \vee r_i) \wedge (\bar{q} \vee r_i)$ to Δ ,
- if $\psi_i = p \rightarrow q$ add $(\bar{p} \vee q \vee \bar{r}_i) \wedge (p \vee r_i) \wedge (\bar{q} \vee r_i)$ to Δ

and replace all occurrences of ψ_i in $\psi_{i+1}, \dots, \psi_m$ by r_i .

The formulae $r_m \wedge \bigwedge \Delta$ and φ are equisatisfiable.

SAT problem

Given a formula φ in CNF decide whether $\varphi \in \text{SAT}$.

We can use truth tables, but that is in many cases too complicated. It means to test all possible valuations and for example $p \wedge \bar{p} \wedge (q_1 \vee \dots \vee q_n)$ is clearly unsatisfiable regardless of values of q_1, \dots, q_n .

In the next lecture we will present better ways how to test satisfiability. We can think about transformations of formulae that preserve satisfiability. A trivial example is to handle clauses as sets of literals and formulae in CNF as sets of clauses.

The Boolean Pythagorean triples problem

It was a long-standing open problem in Ramsey theory that was solved using a SAT solver in 2016. The proof requires 200TB (compressed 68GB) and was computed on a cluster with 800 cores in 2 days.

Positive integers a, b, c form a Pythagorean triple if $a^2 + b^2 = c^2$. We know, e.g., $3^2 + 4^2 = 5^2$.

Can the set $\{1, 2, 3, \dots\}$ of the positive integers be divided into two parts in such a way that no part contains a Pythagorean triple?

The set $\{1, \dots, 7824\}$ can be divided into two such parts, but that is not possible for $\{1, \dots, 7825\}$.

Note that there are 2^{7825} possible divisions in the later case and all these divisions must be ruled out. Hence some “clever” reasoning had to be used. For details see (Heule, Kullmann, and Marek 2016).

Bibliography I



Heule, Marijn J. H., Oliver Kullmann, and Victor W. Marek (2016). “Solving and Verifying the Boolean Pythagorean Triples Problem via Cube-and-Conquer”. In: *Theory and Applications of Satisfiability Testing – SAT 2016: 19th International Conference, Bordeaux, France, July 5-8, 2016, Proceedings*. Ed. by Nadia Creignou and Daniel Le Berre. Cham: Springer International Publishing, pp. 228–245. ISBN: 978-3-319-40970-2. DOI: [10.1007/978-3-319-40970-2_15](https://doi.org/10.1007/978-3-319-40970-2_15).



Wirth, Claus-Peter et al. (2009). “Jacques Herbrand: Life, Logic, and Automated Deduction”. In: *Handbook of the History of Logic*. Elsevier, pp. 195–254. DOI: [10.1016/s1874-5857\(09\)70009-3](https://doi.org/10.1016/s1874-5857(09)70009-3).