Propositional and Predicate Logic - III

Petr Gregor

KTIML MFF UK

ZS 2014/2015

Horn-SAT

- A *unit clause* is a clause containing a single literal,
- a *Horn clause* is a clause containing at most one positive literal,

$$\neg p_1 \vee \cdots \vee \neg p_n \vee q \quad \sim \quad (p_1 \wedge \cdots \wedge p_n) \rightarrow q$$

- a *Horn formula* is a conjunction of Horn clauses,
- *Horn-SAT* is the problem of satisfiability of a given Horn formula.

Algorithm

(1) *if φ contains a pair of unit clauses l and $\bar{l}$, then it is not satisfiable,*

(2) *if φ contains a unit clause l, then assign 1 to l, remove all clauses containing l, remove $\bar{l}$ from all clauses, and repeat from the start,*

(3) *if φ does not contain a unit clause, then it is satisfied by assigning 0 to all remaining propositional variables.*

Step (2) is called *unit propagation*.

Unit propagation

$$(\neg p \vee q) \wedge (\neg p \vee \neg q \vee r) \wedge (\neg r \vee \neg s) \wedge (\neg t \vee s) \wedge s \qquad v(s) = 1$$
$$(\neg p \vee q) \wedge (\neg p \vee \neg q \vee r) \wedge \neg r \qquad v(\neg r) = 1$$
$$(\neg p \vee q) \wedge (\neg p \vee \neg q) \qquad v(p) = v(q) = v(t) = 0$$

Observation *Let φ^l be the proposition obtained from φ by unit propagation. Then φ^l is satisfiable if and only if φ is satisfiable.*

Corollary *The algorithm is correct (it solves Horn-SAT).*

Proof The correctness in Step (1) is obvious, in Step (2) it follows from the observation, in Step (3) it follows from the *Horn form* since every remaining clause contains at least one negative literal.

Note A direct implementation requires quadratic time, but with an appropriate representation in memory, one can achieve linear time (w.r.t. the length of φ).

Theory

Informally, a theory is a description of "world" to which we restrict ourselves.

- A propositional *theory* over the language $\mathbb{P}$ is any set T of propositions from $\mathrm{VF}_{\mathbb{P}}$. We say that propositions of T are *axioms* of the theory T.
- A *model of theory* T over $\mathbb{P}$ is an assignment $v \in M(\mathbb{P})$ (i.e. a model of the language) in which all axioms of T are true, denoted by $v \models T$.
- A *class of models* of T is $M^{\mathbb{P}}(T) = \{v \in M(\mathbb{P}) \mid v \models \varphi \text{ for every } \varphi \in T\}$.

  For example, for $T = \{p,\ \neg p \vee \neg q,\ q \rightarrow r\}$ over $\mathbb{P} = \{p, q, r\}$ we have

$$M^{\mathbb{P}}(T) = \{(1,0,0), (1,0,1)\}$$

- If a theory is finite, it can be replaced by a *conjunction* of its axioms.
- We write $M(T, \varphi)$ as a shortcut for $M(T \cup \{\varphi\})$.

Semantics with respect to a theory

Semantic notions can be defined with respect to a theory, more precisely, with respect to its models. Let T be a theory over $\mathbb{P}$. A proposition φ over $\mathbb{P}$ is

- *valid in T* (*true in T*) if it is true in every model of T, denoted by $T \models \varphi$, We also say that φ is a (semantic) *consequence* of T.
- *unsatisfiable* (*contradictory*) *in T* (*inconsistent with T*) if it is false in every model of T,
- *independent (or contingency) in T* if it is true in some model of T and false in some other,
- *satisfiable in T* (*consistent with T*) if it is true in some model of T.

Propositions φ and ψ are *equivalent in T* (*T-equivalent*), denoted by $\varphi \sim_T \psi$, if for every model v of T, $v \models \varphi$ if and only if $v \models \psi$.

Note If all axioms of a theory T are valid (tautologies), e.g for $T = \emptyset$, then all notions with respect to T correspond to the same notions in (pure) logic.

Consequence of a theory

The *consequence* of a theory T over $\mathbb{P}$ is the set $\theta^{\mathbb{P}}(T)$ of all propositions that are valid in T, i.e.

$$\theta^{\mathbb{P}}(T) = \{\varphi \in \mathrm{VF}_{\mathbb{P}} \mid T \models \varphi\}.$$

Proposition *For every theories $T \subseteq T'$ and propositions $\varphi, \varphi_1, \ldots, \varphi_n$ over $\mathbb{P}$,*

(1) $T \subseteq \theta^{\mathbb{P}}(T) = \theta^{\mathbb{P}}(\theta^{\mathbb{P}}(T)) \subseteq \theta^{\mathbb{P}}(T')$,

(2) $\varphi \in \theta^{\mathbb{P}}(\{\varphi_1, \ldots, \varphi_n\})$ *if and only if* $\models (\varphi_1 \wedge \ldots \wedge \varphi_n) \rightarrow \varphi$.

Proof By definition, $T \models \varphi \Leftrightarrow M(T) \subseteq M(\varphi)$ and $M(T') \subseteq M(T) = M(\theta(T))$.

(1) $$\varphi \in T \Rightarrow M(T) \subseteq M(\varphi) \Leftrightarrow T \models \varphi \Leftrightarrow \varphi \in \theta(T) \Leftrightarrow$$
$$M(\theta(T)) \subseteq M(\varphi) \Leftrightarrow \theta(T) \models \varphi \Leftrightarrow \varphi \in \theta(\theta(T)) \Rightarrow$$
$$M(T') \subseteq M(\varphi) \Leftrightarrow T' \models \varphi \Leftrightarrow \varphi \in \theta(T')$$

Part (2) follows similarly from $M(\varphi_1, \ldots, \varphi_n) = M(\varphi_1 \wedge \ldots \wedge \varphi_n)$ and $\models \psi \rightarrow \varphi$ if and only if $M(\psi) \subseteq M(\varphi)$. □

Properties of theories

A propositional theory T over $\mathbb{P}$ is *(semantically)*

- *inconsistent* (*unsatisfiable*) if $T \models \bot$, otherwise is *consistent* (*satisfiable*),
- *complete* if it is consistent, and $T \models \varphi$ or $T \models \neg\varphi$ for every $\varphi \in \mathrm{VF}_{\mathbb{P}}$, i.e. no proposition over $\mathbb{P}$ is independent in T,
- *extension* of a theory T' over $\mathbb{P}'$ if $\mathbb{P}' \subseteq \mathbb{P}$ and $\theta^{\mathbb{P}'}(T') \subseteq \theta^{\mathbb{P}}(T)$; we say that an extension T of a theory T' is *simple* if $\mathbb{P} = \mathbb{P}'$; and *conservative* if $\theta^{\mathbb{P}'}(T') = \theta^{\mathbb{P}}(T) \cap \mathrm{VF}_{\mathbb{P}'}$,
- *equivalent* with a theory T' if T is an extension of T' and vice-versa,

Observation *Let T and T' be theories over $\mathbb{P}$. Then T is (semantically)*

(1) *consistent if and only if it has a model,*

(2) *complete if and only if it has a single model,*

(3) *extension of T' if and only if $M^{\mathbb{P}}(T) \subseteq M^{\mathbb{P}}(T')$,*

(4) *equivalent with T' if and only if $M^{\mathbb{P}}(T) = M^{\mathbb{P}}(T')$.*

Lindenbaum-Tarski algebra

Let T be a consistent theory over $\mathbb{P}$. On the quotient set $\mathrm{VF}_{\mathbb{P}}/\!\sim_T$ we define operations $\neg$, $\wedge$, $\vee$, $\bot$, $\top$ (correctly) by use of representatives, e.g

$$[\varphi]_{\sim_T} \wedge [\psi]_{\sim_T} = [\varphi \wedge \psi]_{\sim_T}$$

Then $AV^{\mathbb{P}}(T) = \langle \mathrm{VF}_{\mathbb{P}}/\!\sim_T, \neg, \wedge, \vee, \bot, \top \rangle$ is *Lindenbaum-Tarski algebra* for T.

Since $\varphi \sim_T \psi \;\Leftrightarrow\; M(T,\varphi) = M(T,\psi)$, it follows that $h([\varphi]_{\sim_T}) = M(T,\varphi)$ is a (well-defined) injective function $h\colon \mathrm{VF}_{\mathbb{P}}/\!\sim_T \to \mathcal{P}(M(T))$ and

$$h(\neg[\varphi]_{\sim_T}) = M(T) \setminus M(T,\varphi)$$
$$h([\varphi]_{\sim_T} \wedge [\psi]_{\sim_T}) = M(T,\varphi) \cap M(T,\psi)$$
$$h([\varphi]_{\sim_T} \vee [\psi]_{\sim_T}) = M(T,\varphi) \cup M(T,\psi)$$
$$h([\bot]_{\sim_T}) = \emptyset, \quad h([\top]_{\sim_T}) = M(T)$$

Moreover, h is *surjective* if $M(T)$ is *finite*.

Corollary If T is a consistent theory over a finite $\mathbb{P}$, then $AV^{\mathbb{P}}(T)$ is a Boolean algebra *isomorphic* via h to the (finite) algebra of sets $\underline{\mathcal{P}}(M(T))$.

Analysis of theories over finite languages

Let T be a consistent theory over $\mathbb{P}$ where $|\mathbb{P}| = n \in \mathbb{N}^+$ and $m = |M^{\mathbb{P}}(T)|$.
Then the number of (mutually) nonequivalent

- propositions (or theories) over $\mathbb{P}$ is 2^{2^n},
- propositions over $\mathbb{P}$ that are valid (contradictory) in T is $2^{2^n - m}$,
- propositions over $\mathbb{P}$ that are independent in T is $2^{2^n} - 2.2^{2^n - m}$,
- simple extensions of T is 2^m, out of which 1 is inconsistent,
- complete simple extensions of T is m.

And the number of (mutually) T-nonequivalent

- propositions over $\mathbb{P}$ is 2^m,
- propositions over $\mathbb{P}$ that are valid (contradictory) (in T) is 1,
- propositions over $\mathbb{P}$ that are independent (in T) is $2^m - 2$.

Proof By the bijection of $\mathrm{VF}_{\mathbb{P}}/\sim$ resp. $\mathrm{VF}_{\mathbb{P}}/\sim_T$ with $\mathcal{P}(M(\mathbb{P}))$ resp. $\mathcal{P}(M^{\mathbb{P}}(T))$ it suffices to determine the number of appropriate subsets of models. □

Formal proof systems

We formalize precisely the notion of proof as a syntactical procedure.

In *(standard)* formal proof systems,

- a proof is a finite object, it can be built from axioms of a given theory,
- $T \vdash \varphi$ denotes that φ is *provable* from a theory T,
- if a formula has a proof, it can be found *"algorithmically"*,
  (If T is *"given algorithmically"*.)

We usually require that a formal proof system is

- *sound*, i.e. every formula provable from a theory T is also valid in T,
- *complete*, i.e. every formula valid in T is also provable from T.

Examples of formal proof systems (calculi): tableaux methods, *Hilbert systems, Gentzen systems, natural deduction systems*.

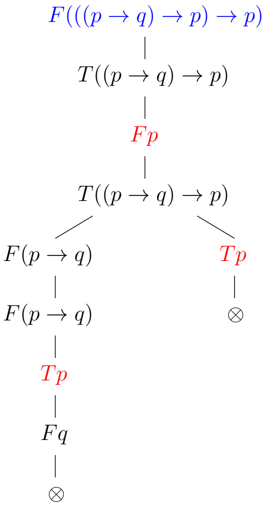
Tableau method - introduction

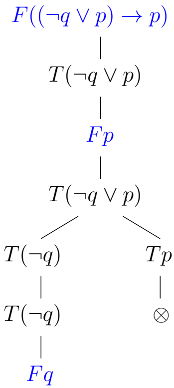
We assume that the language is fixed and at most countable, i.e. the set of propositional letters $\mathbb{P}$ is at most countable. Then every theory over $\mathbb{P}$ is at most countable.

Main features of the tableau method *(informally)*

- a tableau for a formula φ is a binary labeled tree representing systematic search for *counterexample* to φ, i.e. a model of theory is which φ is false,
- a formula is proved if every branch in tableau 'fails', i.e counterexample was not found. In this case the (systematic) tableau will be finite,
- if a counterexample exists, there will be a branch in a (finished) tableau that provides us with this counterexample, but this branch can be infinite.

Introductory examples





Explanation to examples

Nodes in tableaux are labeled by *entries*. An entry is a formula with a *sign* T / F representing an assumption that the formula is true / false in some model. If this assumption is correct, then it is correct also for all the entries in some branch below that came from this entry.

In both examples we have finished (systematic) tableaux from no axioms.

- On the left, there is a *tableau proof* for $((p \to q) \to p) \to p$. All branches *"failed"*, denoted by $\otimes$, as each contains a pair $T\varphi$, $F\varphi$ for some φ *(counterexample was not found)*. Thus the formula is provable, written by

$$\vdash ((p \to q) \to p) \to p$$

- On the right, there is a (finished) tableau for $(\neg q \vee p) \to p$. The left branch did not *"fail"* and is finished (all its entries were considered) *(it provides us with a counterexample $v(p) = v(q) = 0$)*.