Evaluation of a Boolean Formula

For $\varphi \in \mathsf{PL}[p_1, \ldots, p_n]$ and $\underline{\mathrm{a}} = (a_1, \ldots, a_n) \in \{0,1\}^n$ we define $\varphi[\underline{\mathrm{a}}] \in \{0,1\}$ as follows.

- $\top[\underline{\mathrm{a}}] = 1$, $\bot[\underline{\mathrm{a}}] = 0$, $p_i[\underline{\mathrm{a}}] = a_i$
- $(\neg\varphi)[\underline{\mathrm{a}}] = \curlywedge(\varphi[\underline{\mathrm{a}}])$
- $(\varphi \wedge \psi)[\underline{\mathrm{a}}] = (\varphi[\underline{\mathrm{a}}]) \mathbb{\wedge} (\psi[\underline{\mathrm{a}}])$,
  $(\varphi \vee \psi)[\underline{\mathrm{a}}] = (\varphi[\underline{\mathrm{a}}]) \mathbb{\vee} (\psi[\underline{\mathrm{a}}])$

The functions $\curlywedge, \mathbb{\wedge}, \mathbb{\vee}$ are given by

x	y	$\curlywedge y$	$x \mathbb{\wedge} y$	$x \mathbb{\vee} y$
0	0	1	0	0
0	1	0	0	1
1	0		0	1
1	1		1	1

Model Relation for Propositional Logic

Writing $\underline{a} \models \varphi$ for $\varphi[\underline{a}] = 1$ we obtain the following.

- $\underline{a} \models \top$ always holds and $\underline{a} \models \bot$ never holds
- $\underline{a} \models \neg\varphi$ holds iff $\underline{a} \models \varphi$ does *not* hold
- $\underline{a} \models \varphi \wedge \psi$ holds if $\underline{a} \models \varphi$ *and* $\underline{a} \models \psi$ both hold.
  $\underline{a} \models \varphi \vee \psi$ holds if $\underline{a} \models \varphi$ holds *or* $\underline{a} \models \psi$ holds.

Expressive Completeness

Theorem. For every $f\colon \{0,1\}^n \to \{0,1\}$ there is some $\varphi \in \mathsf{PL}[p_1, \ldots, p_n]$ such that for all $\underline{\mathrm{a}} \in \{0,1\}^n$ we have $f(\underline{\mathrm{a}}) = \varphi[\underline{\mathrm{a}}]$.

In fact, φ can be chosen to be of the form

$$\bigvee_j \bigwedge_i \xi_{ij} \qquad \text{with } \xi_{ij} \in \{x_i, \neg x_i\}$$

(in "disjunctive normal form")

On Succinctness

Theorem. Let $\varepsilon > 0$. For large n, the fraction of functions

$$\{0,1\}^n \to \{0,1\}$$

that can be represented by formulae of size up to

$$2^{(1-\varepsilon)\cdot n}$$

tends to zero.

In other words, almost all function require exponentially large formulae.

Model Checking in Propositional Logic

Given: Propositional formula $\varphi \in \mathsf{PL}[p_1, \ldots, p_n]$ and $\underline{\mathrm{a}} \in \{0,1\}^n$

Question: $\underline{\mathrm{a}} \models \varphi$?

Solvable in polynomial time (essentially $\mathcal{O}(|\varphi|)$): just compute truth value following the buildup of φ.

Satisfiability in Propositional Logic

Given: Propositional formula $\varphi \in \mathsf{PL}[p_1, \ldots, p_n]$.

Question: Is there some $\underline{\mathrm{a}} \in \{0,1\}^n$ such that $\underline{\mathrm{a}} \models \varphi$?

This problem is NP-complete.

NP

Definition. A problem is said to be in NP iff it can be solved by a non-deterministic Turing machine in polynomial time.

"NP *is verifying proofs*"

Conjecture. P $\neq$ NP.

NP-completeness

Definition. A problem L is NP-complete iff

- it belongs to NP
- for any problem L' in NP there is an easy (say, in polynomial time) function f such that

$$x \in L' \text{ iff } f(x) \in L$$