Mathematics for Computer Science
6.042J/18.062J

The Logic of Propositions

Proving Validity

Instead of truth tables, can try to prove valid formulas symbolically using axioms and deduction rules

Proving Validity

The text describes a bunch of algebraic rules to prove that propositional formulas are equivalent

Algebra for Equivalence

for example,
the distributive law

P AND (Q OR R) $\equiv$
(P AND Q) OR (P AND R)

Algebra for Equivalence

for example,
DeMorgan's law

NOT(P AND Q) $\equiv$

NOT(P) OR NOT(Q)

Algebra for Equivalence

The set of rules for $\equiv$ in the text are complete: if two formulas are $\equiv$, these rules can prove it.

A Proof System

Another approach is to start with some valid formulas (axioms) and deduce more valid formulas using proof rules

A Proof System

Lukasiewicz' proof system is a particularly elegant example of this idea.

A Proof System

Lukasiewicz' proof system is a particularly elegant example of this idea. It covers formulas whose only logical operators are IMPLIES ($\rightarrow$) and NOT.

Lukasiewicz' Proof System

Axioms:

1) $(\neg P \rightarrow P) \rightarrow P$
2) $P \rightarrow (\neg P \rightarrow Q)$
3) $(P \rightarrow Q) \rightarrow ((Q \rightarrow R) \rightarrow (P \rightarrow R))$

The only rule: modus ponens

Lukasiewicz' Proof System

Prove formulas by starting with axioms and repeatedly applying the inference rule.

To illustrate the proof system we'll do an example, which you may safely skip.

Lukasiewicz' Proof System

Prove formulas by starting with axioms and repeatedly applying the inference rule.

For example, to prove:

$$P \rightarrow P$$

A Lukasiewicz' Proof

3rd axiom:

$$(P \rightarrow \quad Q \quad) \rightarrow$$
$$((\quad Q \quad \rightarrow R) \rightarrow (P \rightarrow R))$$

replace R by P

A Lukasiewicz' Proof

3rd axiom:

$$(P \rightarrow \quad Q \quad) \rightarrow$$
$$((\quad Q \quad \rightarrow P) \rightarrow (P \rightarrow P))$$

replace Q by $(\overline{P} \rightarrow P)$

A Lukasiewicz' Proof

3rd axiom:

$$\overbrace{(P \rightarrow (\overline{P} \rightarrow P)\,)}^{\text{Axiom 2)}} \rightarrow$$
$$(((\overline{P} \rightarrow P) \rightarrow P) \rightarrow (P \rightarrow P))$$

A Lukasiewicz' Proof

so apply modus ponens:

$$\overbrace{(P \rightarrow (\overline{P} \rightarrow P)\,)}^{\text{Axiom 2)}} \rightarrow$$
$$(((\overline{P} \rightarrow P) \rightarrow P) \rightarrow (P \rightarrow P))$$

A Lukasiewicz' Proof

so apply modus ponens:

Axiom 1)

$$(((\overline{P} \rightarrow P) \rightarrow P) \rightarrow (P \rightarrow P))$$

A Lukasiewicz' Proof

so apply modus ponens:

$$(P \rightarrow P)$$

QED

The 3 Axioms are all valid (verify by truth table). We know modus ponens is sound. So every provable formula is also valid.

Lukasiewicz is Complete

Conversely, every valid (NOT,$\rightarrow$)-formula is provable:

system is "complete"

Not hard to verify but would take a full lecture; we omit it.

validity checking still inefficient

Algebraic & deduction proofs in general are no better than truth tables.

No efficient method for verifying validity is known.