Mathematics for Computer Science
6.042J/18.062J

Propositional Algebra

Algebra for Equivalence

Use an algebra of equivalence to prove formulas equivalent.

Proving Equivalence

Have set of equivalence rules that are sound:
if the rules prove that two formulas are $\equiv$, then they really are.

Proving Equivalence

and the rules are complete:
if two formulas are $\equiv$, these rules can prove it.

Strategy: Convert to DNF

Come up with enough equivalence rules to convert any formula to an equivalent canonical DNF.

Strategy: Convert to DNF

Come up with enough equivalence rules to convert any formula to an equivalent canonical DNF. Two formulas are equiv when convert to same canonical DNF.

Algebra for Equivalence

Rules for XOR, IMPLIES

P IMPLIES Q $\equiv$ NOT(P) OR Q

P XOR Q $\equiv$ (NOT(P) AND Q) OR (NOT(Q) AND P)

Just leaves AND, OR, NOT

Algebra for Equivalence

Double Negation

NOT(NOT(P)) $\equiv$ P

Algebra for Equivalence

DeMorgan's law -AND

NOT(P AND Q) ≡

NOT(P) OR NOT(Q)

Algebra for Equivalence

DeMorgan's law -OR

NOT(P OR Q) ≡

NOT(P) AND NOT(Q)

Rewrite left to right until NOT's only on variables

example

converting to a sum of products

move NOTs down to literals

NOT[NOT(P OR Q) OR (R AND Q)]

move NOTs down to literals

NOT[NOT(P OR Q) OR (R AND Q)]

use DeMorgan

move NOTs down to literals

NOT[NOT(P OR Q) OR (R AND Q)]

NOT[NOT(P OR Q)] AND NOT(R AND Q)

move NOTs down to literals

NOT[NOT(P OR Q)] AND NOT(R AND Q)

Double NOT

move NOTs down to literals

NOT[NOT(P OR Q)] AND NOT(R AND Q)

(P OR Q) AND NOT(R AND Q)

move NOTs down to literals

(P OR Q) AND NOT(R AND Q)

use DeMorgan

move NOTs down to literals

(P OR Q) AND NOT(R AND Q)

(P OR Q) AND ($\overline{R}$ OR $\overline{Q}$)

Done move NOTs down to literals

(P OR Q) AND ($\overline{R}$ OR $\overline{Q}$)

Algebra for Equivalence

Distributive Law

$$P \cdot (Q + R) \equiv (P \cdot Q) + (P \cdot R)$$

Algebra for Equivalence

Distributive Law

P AND (Q OR R) $\equiv$

(P AND Q) OR (P AND R)

Rewrite left to right until
" OR of AND's "

Get Sum of Products

(P OR Q) AND ($\overline{R}$ OR $\overline{Q}$)

Distribute (P OR Q)

Get Sum of Products

(P OR Q) AND ($\overline{R}$ OR $\overline{Q}$)

((P OR Q) AND $\overline{R}$) OR
((P OR Q) AND $\overline{Q}$)

Get Sum of Products

((P OR Q) AND $\overline{R}$) OR
((P OR Q) AND $\overline{Q}$)

Get Sum of Products

((P OR Q) AND $\overline{R}$) OR

((P OR Q) AND $\overline{Q}$)

Distribute $\overline{R}$

Get Sum of Products

((P OR Q) AND $\overline{R}$) OR

((P OR Q) AND $\overline{Q}$)

(P AND $\overline{R}$) OR (Q AND $\overline{R}$) OR

((P OR Q) AND $\overline{Q}$)

Get Sum of Products

(P AND $\overline{R}$) OR (Q AND $\overline{R}$) OR

((P OR Q) AND $\overline{Q}$)

Distribute $\overline{Q}$

Get Sum of Products

(P AND $\overline{R}$) OR (Q AND $\overline{R}$) OR

((P OR Q) AND $\overline{Q}$)

(P AND $\overline{R}$) OR (Q AND $\overline{R}$) OR

(P AND $\overline{Q}$) OR (Q AND $\overline{Q}$)

Done: Sum of Products

$(P \text{ AND } \overline{R}) \text{ OR } (Q \text{ AND } \overline{R}) \text{ OR }$
$(P \text{ AND } \overline{Q}) \text{ OR } (Q \text{ AND } \overline{Q})$

Simplification rules

$Q \text{ OR } Q \equiv Q$

$\overline{Q} \text{ OR } Q \equiv \text{True}$

$Q \text{ AND } Q \equiv Q$

$\overline{Q} \text{ AND } Q \equiv \text{False}$

Simplification rules

$Q \text{ OR } T \equiv T$

$Q \text{ AND } T \equiv Q$

$P \text{ OR } F \equiv P$

$P \text{ AND } F \equiv F$

example

$(P \text{ AND } \overline{R}) \text{ OR } (Q \text{ AND } \overline{R}) \text{ OR }$
$(P \text{ AND } \overline{Q}) \text{ OR } (Q \text{ AND } \overline{Q})$

Simplify

example

(P AND $\overline{R}$) OR (Q AND $\overline{R}$) OR

(P AND $\overline{Q}$) OR (Q AND $\overline{Q}$)

Simplify

example

(P AND $\overline{R}$) OR (Q AND $\overline{R}$) OR

(P AND $\overline{Q}$) OR (False)

Simplify

example

(P AND $\overline{R}$) OR (Q AND $\overline{R}$) OR

(P AND $\overline{Q}$)

Simplify

we have DNF!

(P AND $\overline{R}$) OR (Q AND $\overline{R}$) OR (P AND $\overline{Q}$)

now to get Full DNF:

Full DNF for an AND-term

(P AND $\bar{R}$) unsimplify

(P AND $\bar{R}$) AND (Q OR $\bar{Q}$)

Full DNF for an AND-term

(P AND $\bar{R}$)

(P AND $\bar{R}$) AND (Q OR $\bar{Q}$) distribute

(P AND $\bar{R}$ AND Q) OR

(P AND $\bar{R}$ AND $\bar{Q}$)

Full DNF for an AND-term

(P AND $\bar{R}$)

(P AND $\bar{R}$ AND Q) OR

(P AND $\bar{R}$ AND $\bar{Q}$)

Full!

Rearrangement rules

P AND Q $\equiv$ Q AND P

(P AND Q) AND R $\equiv$

(P AND Q AND R)

...likewise for OR

example

(P AND $\overline{R}$ AND Q) OR
(P AND $\overline{R}$ AND $\overline{Q}$)

example

(P AND $\overline{R}$ AND Q) OR
(P AND $\overline{R}$ AND $\overline{Q}$)

sort

example

(P AND Q AND $\overline{R}$) OR
(P AND $\overline{Q}$ AND $\overline{R}$)

Sorted Full DNF for (P AND $\overline{R}$)

(P AND Q AND $\overline{R}$) OR
(P AND $\overline{Q}$ AND $\overline{R}$)

example

same for each AND-term, and OR them together:

(P AND Q AND $\overline{R}$) OR
(P AND $\overline{Q}$ AND $\overline{R}$)

OR (P AND Q AND $\overline{R}$) OR
($\overline{P}$ AND Q AND $\overline{R}$) OR

(P AND $\overline{Q}$ AND R) OR
(P AND $\overline{Q}$ AND $\overline{R}$)

example

simplify (duplicates)

(P AND Q AND $\overline{R}$) OR
(P AND $\overline{Q}$ AND $\overline{R}$)

OR (P AND Q AND $\overline{R}$) OR
($\overline{P}$ AND Q AND $\overline{R}$) OR

(P AND $\overline{Q}$ AND R) OR
(P AND $\overline{Q}$ AND $\overline{R}$)

example

simplify (duplicates)

(P AND Q AND $\overline{R}$) OR
(P AND $\overline{Q}$ AND $\overline{R}$)

OR ~~(P AND Q AND $\overline{R}$) OR~~
($\overline{P}$ AND Q AND $\overline{R}$) OR

(P AND $\overline{Q}$ AND R) ~~OR~~
~~(P AND $\overline{Q}$ AND $\overline{R}$)~~

example

also sort the clauses

(P AND Q AND $\overline{R}$) OR
(P AND $\overline{Q}$ AND $\overline{R}$) OR
($\overline{P}$ AND Q AND $\overline{R}$) OR
(P AND $\overline{Q}$ AND R)

Canonical DNF

(P AND Q AND $\overline{R}$) OR (P AND $\overline{Q}$ AND R) OR
(P AND $\overline{Q}$ AND $\overline{R}$) OR ($\overline{P}$ AND Q AND $\overline{R}$)

Done Sorted Full DNF

unique for each formula

Algebra for Equivalence

Thm. These rules are complete: if two formulas are $\equiv$, these rules can prove it.

Algebra for Equivalence

Because two formulas are equivalent

Algebra for Equivalence

Because two formulas are equivalent iff have same truth table

Algebra for Equivalence

Because two formulas are equivalent iff have same truth table iff have same canonical DNF.

Validity Checking still hard

Algebraic proofs in general don't beat truth tables.

Validity Checking still hard

Algebraic proofs in general don't beat truth tables. The canonical DNF is just a copy of the truth table as an algebraic formula.

Validity Checking still hard

Algebraic proofs in general don't beat truth tables. No efficient method known for equivalence or validity.