Logic

Diana Gründlinger Aart Middeldorp Fabian Mitterwallner
Alexander Montag Johannes Niederhauser Daniel Rainer

Particify with session ID **0992 9580** for anonymous questions

ars.uibk.ac.at

Outline

Definitions

- sequent

$$\underbrace{\varphi_1, \varphi_2, \dots, \varphi_n}_{\text{premises}} \vdash \underbrace{\psi}_{\text{conclusion}}$$

  with propositional formulas $\varphi_1, \varphi_2, \dots, \varphi_n, \psi$

- sequent $\varphi_1, \varphi_2, \dots, \varphi_n \vdash \psi$ is valid if ψ can be proved from premises $\varphi_1, \varphi_2, \dots, \varphi_n$ using proof rules of natural deduction
- theorem is formula φ such that sequent $\vdash \varphi$ is valid

Theorem

- natural deduction is sound: $\varphi_1, \varphi_2, \dots, \varphi_n \vdash \psi$ is valid $\implies$ $\varphi_1, \varphi_2, \dots, \varphi_n \vDash \psi$
- proof rules MT, $\neg\neg$i, PBC and LEM are derivable from basic proof rules
- proof rules LEM, PBC and $\neg\neg$e are inter-derivable (with respect to other basic proof rules)

Proof Rules of Natural Deduction (1)

	introduction	elimination
$\wedge$	$\dfrac{\varphi \quad \psi}{\varphi \wedge \psi}\ \wedge\mathrm{i}$	$\dfrac{\varphi \wedge \psi}{\varphi}\ \wedge\mathrm{e}_1$ $\quad$ $\dfrac{\varphi \wedge \psi}{\psi}\ \wedge\mathrm{e}_2$
$\vee$	$\dfrac{\varphi}{\varphi \vee \psi}\ \vee\mathrm{i}_1$ $\quad$ $\dfrac{\psi}{\varphi \vee \psi}\ \vee\mathrm{i}_2$	$\dfrac{\varphi \vee \psi \quad \boxed{\begin{array}{c}\varphi \\ \vdots \\ \chi\end{array}} \quad \boxed{\begin{array}{c}\psi \\ \vdots \\ \chi\end{array}}}{\chi}\ \vee\mathrm{e}$
$\rightarrow$	$\dfrac{\boxed{\begin{array}{c}\varphi \\ \vdots \\ \psi\end{array}}}{\varphi \rightarrow \psi}\ \rightarrow\mathrm{i}$	$\dfrac{\varphi \rightarrow \psi \quad \varphi}{\psi}\ \rightarrow\mathrm{e}$

Proof Rules of Natural Deduction ❷

	introduction	elimination
$\bot$		$\dfrac{\bot}{\varphi}\ \bot\mathrm{e}$
$\neg$	$\dfrac{\boxed{\begin{matrix}\varphi\\ \vdots\\ \bot\end{matrix}}}{\neg\varphi}\ \neg\mathrm{i}$	$\dfrac{\varphi \quad \neg\varphi}{\bot}\ \neg\mathrm{e}$
$\top$	$\dfrac{}{\top}\ \top\mathrm{i}$	
$\neg\neg$		$\dfrac{\neg\neg\varphi}{\varphi}\ \neg\neg\mathrm{e}$

derived proof rules

$$\dfrac{\varphi \to \psi \quad \neg\psi}{\neg\varphi}\ \mathrm{MT} \qquad \dfrac{\boxed{\begin{matrix}\neg\varphi\\ \vdots\\ \bot\end{matrix}}}{\varphi}\ \mathrm{PBC} \qquad \dfrac{\varphi}{\neg\neg\varphi}\ \neg\neg\mathrm{i} \qquad \dfrac{}{\varphi \vee \neg\varphi}\ \mathrm{LEM}$$

Example

$((p \to q) \to p) \to p$ is valid:

1	$(p \to q) \to p$	assumption
2	$p \vee \neg p$	LEM
3	p	assumption
4	$\neg p$	assumption
5	p	assumption
6	$\bot$	$\neg$e 5, 4
7	q	$\bot$e 6
8	$p \to q$	$\to$i 5 – 7
9	p	$\to$e 1, 8
10	p	$\vee$e 2, 3 – 3, 4 – 9
11	$((p \to q) \to p) \to p$	$\to$i 1 – 10

Part I: Propositional Logic

algebraic normal forms, binary decision diagrams, conjunctive normal forms, DPLL, Horn formulas, natural deduction, Post's adequacy theorem, resolution, SAT, semantics, sorting networks, soundness and completeness, syntax, Tseitin's transformation

Part II: Predicate Logic

natural deduction, quantifier equivalences, resolution, semantics, Skolemization, syntax, undecidability, unification

Part III: Model Checking

adequacy, branching-time temporal logic, CTL*, fairness, linear-time temporal logic, model checking algorithms, symbolic model checking

Outline

Theorem

natural deduction is complete:

$$\varphi_1, \varphi_2, \dots, \varphi_n \vDash \psi \quad \Longrightarrow \quad \varphi_1, \varphi_2, \dots, \varphi_n \vdash \psi \text{ is valid}$$

all true statements can be proved

Proof structure

① $\varphi_1, \varphi_2, \dots, \varphi_n \vDash \psi$		assumption
② $\vDash \varphi_1 \to (\varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots))$	① $\Longrightarrow$ ②	easy
③ $\vdash \varphi_1 \to (\varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots))$ is valid	② $\Longrightarrow$ ③	difficult
④ $\varphi_1, \varphi_2, \dots, \varphi_n \vdash \psi$ is valid	③ $\Longrightarrow$ ④	easy

Lemma ❶ $\Longrightarrow$ ❷

$$\varphi_1, \varphi_2, \ldots, \varphi_n \vDash \psi \quad \Longrightarrow \quad \vDash \varphi_1 \rightarrow (\varphi_2 \rightarrow (\cdots(\varphi_n \rightarrow \psi)\cdots))$$

Proof

- suppose $\vDash \varphi_1 \rightarrow (\varphi_2 \rightarrow (\cdots(\varphi_n \rightarrow \psi)\cdots))$ does not hold
- $\bar{v}(\varphi_1) = \cdots = \bar{v}(\varphi_n) = \mathsf{T}$ and $\bar{v}(\psi) = \mathsf{F}$ for some valuation v
- $\varphi_1, \varphi_2, \ldots, \varphi_n \vDash \psi$ does not hold

Lemma ❸ $\Longrightarrow$ ❹

$\vdash \varphi_1 \to (\varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots))$ is valid $\Longrightarrow$ $\varphi_1, \varphi_2, \ldots, \varphi_n \vdash \psi$ is valid

Proof

- Π: proof of validity of $\vdash \varphi_1 \to (\varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots))$
- proof of validity of $\varphi_1, \varphi_2, \ldots, \varphi_n \vdash \psi$:

$\varphi_1 \; \varphi_2 \; \cdots \; \varphi_n$	premises
Π	
$\varphi_1 \to (\varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots))$	
$\varphi_2 \to (\cdots(\varphi_n \to \psi)\cdots)$	$\to$e
$\vdots$	$\vdots$
ψ	$\to$e

Lemma

$❷ \Longrightarrow ❸$

$\vDash \varphi \quad \Longrightarrow \quad \vdash \varphi$ is valid

Definition

valuation v, formula φ

$$\langle\varphi\rangle^v = \begin{cases} \varphi & \text{if } \bar{v}(\varphi) = \mathsf{T} \\ \neg\varphi & \text{if } \bar{v}(\varphi) = \mathsf{F} \end{cases}$$

Main Lemma

$p_1, \dots, p_n$ are all atoms in $\varphi \quad \Longrightarrow \quad \langle p_1\rangle^v, \dots, \langle p_n\rangle^v \vdash \langle\varphi\rangle^v$ is valid

every line in truth table corresponds to valid sequent

Main Lemma

$p_1, \ldots, p_n$ are all atoms in $\varphi \implies \langle p_1 \rangle^v, \ldots, \langle p_n \rangle^v \vdash \langle \varphi \rangle^v$ is valid

Proof (cont'd on subsequent slides)

induction on structure of φ

Example

formula $\varphi = \neg p \vee q$

valuation	p	q	sequent
v_1	T	T	$p, q \vdash \neg p \vee q$
v_2	T	F	$p, \neg q \vdash \neg(\neg p \vee q)$
v_3	F	T	$\neg p, q \vdash \neg p \vee q$
v_4	F	F	$\neg p, \neg q \vdash \neg p \vee q$

Base Cases

$\varphi = p$

- $v(p) = \mathsf{T}$: $\langle p \rangle^v = \langle \varphi \rangle^v = p$ $p \vdash p$ is valid
- $v(p) = \mathsf{F}$: $\langle p \rangle^v = \langle \varphi \rangle^v = \neg p$ $\neg p \vdash \neg p$ is valid

$\varphi = \top$ $\vdash \top$ is valid

$\varphi = \bot$ $\vdash \neg\bot$ is valid

Induction Step (4 cases)

case 1: $\varphi = \neg\psi$

induction hypothesis: $\langle p_1 \rangle^v, \ldots, \langle p_n \rangle^v \vdash \langle \psi \rangle^v$ is valid — Π

- $\bar{v}(\varphi) = \mathsf{T}$: $\langle \varphi \rangle^v = \varphi = \neg\psi = \langle \psi \rangle^v$
- $\bar{v}(\varphi) = \mathsf{F}$: $\langle \varphi \rangle^v = \neg\varphi = \neg\neg\psi$ and $\langle \psi \rangle^v = \psi$

  extend Π with $\neg\neg$i to get proof of $\langle p_1 \rangle^v, \ldots, \langle p_n \rangle^v \vdash \langle \varphi \rangle^v$

Induction Step (4 cases)

case 2: $\varphi = \psi_1 \wedge \psi_2$

- $q_1, \dots, q_l$: all atoms in ψ_1 $r_1, \dots, r_k$: all atoms in ψ_2
- induction hypothesis: $\langle q_1 \rangle^v, \dots, \langle q_l \rangle^v \vdash \langle \psi_1 \rangle^v$ and $\langle r_1 \rangle^v, \dots, \langle r_k \rangle^v \vdash \langle \psi_2 \rangle^v$ are valid
- $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \psi_1 \rangle^v$ and $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \psi_2 \rangle^v$ are valid
- $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \psi_1 \rangle^v \wedge \langle \psi_2 \rangle^v$ is valid (using $\wedge$i) — Π
- to prove: $\langle \psi_1 \rangle^v \wedge \langle \psi_2 \rangle^v \vdash \langle \varphi \rangle^v$ is valid — Π'

$\bar{v}(\psi_1)$	$\bar{v}(\psi_2)$	$\langle \psi_1 \rangle^v \wedge \langle \psi_2 \rangle^v$	$\langle \varphi \rangle^v$
T	T	$\psi_1 \wedge \psi_2$	$\psi_1 \wedge \psi_2$
T	F	$\psi_1 \wedge \neg\psi_2$	$\neg(\psi_1 \wedge \psi_2)$
F	T	$\neg\psi_1 \wedge \psi_2$	$\neg(\psi_1 \wedge \psi_2)$
F	F	$\neg\psi_1 \wedge \neg\psi_2$	$\neg(\psi_1 \wedge \psi_2)$

- combining Π and Π' yields validity of $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \varphi \rangle^v$

Induction Step (4 cases)

case 3: $\varphi = \psi_1 \vee \psi_2$

- $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \psi_1 \rangle^v$ and $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \psi_2 \rangle^v$ are valid
- $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \psi_1 \rangle^v \wedge \langle \psi_2 \rangle^v$ is valid (using $\wedge$i) — Π
- to prove: $\langle \psi_1 \rangle^v \wedge \langle \psi_2 \rangle^v \vdash \langle \varphi \rangle^v$ is valid — Π'

$\bar{v}(\psi_1)$	$\bar{v}(\psi_2)$	$\langle \psi_1 \rangle^v \wedge \langle \psi_2 \rangle^v$	$\langle \varphi \rangle^v$
T	T	$\psi_1 \wedge \psi_2$	$\psi_1 \vee \psi_2$
T	F	$\psi_1 \wedge \neg\psi_2$	$\psi_1 \vee \psi_2$
F	T	$\neg\psi_1 \wedge \psi_2$	$\psi_1 \vee \psi_2$
F	F	$\neg\psi_1 \wedge \neg\psi_2$	$\neg(\psi_1 \vee \psi_2)$

- combining Π and Π' yields validity of $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \varphi \rangle^v$

Induction Step (4 cases)

case 4: $\varphi = \psi_1 \to \psi_2$

- $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \psi_1 \rangle^v$ and $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \psi_2 \rangle^v$ are valid
- $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \psi_1 \rangle^v \wedge \langle \psi_2 \rangle^v$ is valid (using $\wedge$i) — Π
- to prove: $\langle \psi_1 \rangle^v \wedge \langle \psi_2 \rangle^v \vdash \langle \varphi \rangle^v$ is valid — Π'

$\bar{v}(\psi_1)$	$\bar{v}(\psi_2)$	$\langle \psi_1 \rangle^v \wedge \langle \psi_2 \rangle^v$	$\langle \varphi \rangle^v$
T	T	$\psi_1 \wedge \psi_2$	$\psi_1 \to \psi_2$
T	F	$\psi_1 \wedge \neg\psi_2$	$\neg(\psi_1 \to \psi_2)$
F	T	$\neg\psi_1 \wedge \psi_2$	$\psi_1 \to \psi_2$
F	F	$\neg\psi_1 \wedge \neg\psi_2$	$\psi_1 \to \psi_2$

- combining Π and Π' yields validity of $\langle p_1 \rangle^v, \dots, \langle p_n \rangle^v \vdash \langle \varphi \rangle^v$

Theorem

$\models \varphi \implies \vdash \varphi$ is valid

Proof

suppose $\models \varphi$

- for every valuation v $\langle\varphi\rangle^v = \varphi$
- for every valuation v $\langle p_1\rangle^v, \ldots, \langle p_n\rangle^v \vdash \varphi$ is valid sequent
- combine all proofs of these sequents into proof of validity of

$$\vdash \varphi$$

by $2^n - 1$ applications of LEM and $\vee$e

Example

$\vdash p \land q \to q$ is valid

valuation	p	q	sequent	proof
v_1	T	T	$p, q \vdash p \land q \to q$	Π_1
v_2	T	F	$p, \neg q \vdash p \land q \to q$	Π_2
v_3	F	T	$\neg p, q \vdash p \land q \to q$	Π_3
v_4	F	F	$\neg p, \neg q \vdash p \land q \to q$	Π_4

$p \lor \neg p$ LEM

- Box 1:
  - p assumption
  - $q \lor \neg q$ LEM
  - Box 1a:
    - q ass
    - $\cdots \Pi_1 \cdots$
    - $p \land q \to q$
  - Box 1b:
    - $\neg q$ ass
    - $\cdots \Pi_2 \cdots$
    - $p \land q \to q$
  - $p \land q \to q$ $\lor$e
- Box 2:
  - $\neg p$ assumption
  - $q \lor \neg q$ LEM
  - Box 2a:
    - q ass
    - $\cdots \Pi_3 \cdots$
    - $p \land q \to q$
  - Box 2b:
    - $\neg q$ ass
    - $\cdots \Pi_4 \cdots$
    - $p \land q \to q$
  - $p \land q \to q$ $\lor$e

$p \land q \to q$ $\lor$e

Demo

Natural Deduction Tool

by Andreas Schnabl (2005)

Outline

Definitions

- clause is set of literals $\{\ell_1, \dots, \ell_n\}$ representing formula

$$\begin{cases} (\ell_1 \vee \cdots \vee \ell_n) & \text{if } n \geqslant 1 \\ \bot & \text{if } n = 0 \end{cases}$$

- $\square$ denotes empty clause $\varnothing$
- clausal form is set of clauses $\{C_1, \dots, C_m\}$ representing formula

$$\begin{cases} C_1 \wedge \cdots \wedge C_m & \text{if } m \geqslant 1 \\ \top & \text{if } m = 0 \end{cases}$$

Remark

every CNF can be written in clausal form

Example

CNF	clausal form
$(\neg p) \wedge (\neg q \vee \neg p) \wedge (\neg p \vee \neg r)$	$\{\{\neg p\}, \{\neg q, \neg p\}, \{\neg p, \neg r\}\}$
$(\neg p \vee q) \wedge (q \vee \neg r) \wedge (p \vee q \vee \neg r)$	$\{\{\neg p, q\}, \{q, \neg r\}, \{p, q, \neg r\}\}$
$(\neg p \vee \neg p) \wedge (q \vee r) \wedge (r \vee q)$	$\{\{\neg p\}, \{q, r\}\}$

Definition

literals ℓ_1 and ℓ_2 are **complementary** if $\underbrace{\ell_1 = \neg \ell_2 \text{ or } \neg \ell_1 = \ell_2}_{\ell_1 = \ell_2^c}$

Notation

if ℓ is literal then $\ell^c = \begin{cases} \neg p & \text{if } \ell = p \\ p & \text{if } \ell = \neg p \end{cases}$

Definition

- clauses C_1 and C_2 clash on literal ℓ if $\ell \in C_1$ and $\ell^c \in C_2$
- resolvent of clauses C_1 and C_2 clashing on literal ℓ is clause

$$(C_1 \setminus \{\ell\}) \cup (C_2 \setminus \{\ell^c\})$$

- C_1 and C_2 are parent clauses of resolvent

Examples

- clauses $\{\neg p, \neg q, r\}$ and $\{p, r\}$ clash with resolvent $\{\neg q, r\}$
- clauses $\{p, \neg p, q\}$ and $\{q, r\}$ do not clash
- clauses $\{\neg p, \neg q\}$ and $\{p, q\}$ clash with resolvents $\{\neg q, q\}$ and $\{\neg p, p\}$
- clauses $\{p, \neg p, q\}$ and $\{p, \neg p, q\}$ clash with resolvent $\{p, \neg p, q\}$

Resolution

input: clausal form S

output: yes if S is satisfiable

no if S is unsatisfiable

① repeatedly add (new) resolvents of clashing clauses in S

② return no as soon as empty clause is derived

③ return yes if all clashing clauses have been resolved

Theorem

resolution is terminating

Definition

refutation of S is resolution derivation of $\square$ from S

Theorem

resolution is sound and complete:

$$S \text{ admits refutation} \iff \text{clausal form } S \text{ is unsatisfiable}$$

Definition

- resolvent of clauses C_1 and C_2 clashing on literal ℓ is clause $(C_1 \setminus \{\ell\}) \cup (C_2 \setminus \{\ell^c\})$
- special case (unit resolution): $C_1 = \{\ell\}$ with resolvent $C_2 \setminus \{\ell^c\}$

Example ❶

$$(\neg p \vee \neg q \vee r) \wedge (p \vee r) \wedge (q \vee r) \wedge \neg r$$

1 $\{\neg p, \neg q, r\}$

2 $\{p, r\}$

3 $\{q, r\}$

4 $\{\neg r\}$

5 $\{\neg q, r\}$ resolve 1, 2, p

6 $\{r\}$ resolve 3, 5, q

7 $\square$ resolve 4, 6, r

unsatisfiable

Example ❷

$$p \wedge (p \to ((q \vee r) \wedge \neg(q \wedge r))) \wedge (p \to ((s \vee t) \wedge \neg(s \wedge t))) \wedge (s \to q) \wedge (\neg r \to t) \wedge (t \to s)$$

1	$\{p\}$	
2	$\{\neg p, q, r\}$	
3	$\{\neg p, \neg q, \neg r\}$	
4	$\{\neg p, s, t\}$	
5	$\{\neg p, \neg s, \neg t\}$	
6	$\{\neg s, q\}$	
7	$\{r, t\}$	
8	$\{\neg t, s\}$	
9	$\{\neg q, \neg r\}$	resolve 1, 3, p
10	$\{s, t\}$	resolve 1, 4, p
11	$\{\neg s, \neg t\}$	resolve 1, 5, p
12	$\{\neg s, \neg r\}$	resolve 6, 9, q
13	$\{s\}$	resolve 8, 10, t
14	$\{\neg t\}$	resolve 11, 13, s
15	$\{r\}$	resolve 7, 14, t
16	$\{\neg r\}$	resolve 12, 13, s
17	$\square$	resolve 15, 16, r

unsatisfiable

Example ③

$$(p \vee q) \wedge (\neg p \vee \neg r) \wedge (\neg q \vee s) \wedge (p \vee \neg r) \wedge (r \vee \neg s)$$

1	$\{p, q\}$		12	$\{\neg p, \neg q\}$	resolve 3, 9, s	23	$\{q, \neg q\}$	resolve 6, 11, r
2	$\{\neg p, \neg r\}$		13	$\{p, \neg s\}$	resolve 4, 5, r	24	$\{p, \neg p\}$	resolve 7, 9, s
3	$\{\neg q, s\}$		14	$\{\neg r, \neg s\}$	resolve 4, 9, p	25	$\{p\}$	resolve 7, 19, s
4	$\{p, \neg r\}$		15	$\{p, \neg q\}$	resolve 4, 11, r	26	$\{\neg q\}$	resolve 8, 11, r
5	$\{r, \neg s\}$		16	$\{\neg q, \neg r\}$	resolve 4, 12, p			
6	$\{q, \neg r\}$	resolve 1, 2, p	17	$\{q, \neg s\}$	resolve 5, 6, r			
7	$\{p, s\}$	resolve 1, 3, q	18	$\{p, r\}$	resolve 5, 7, s			
8	$\{\neg r\}$	resolve 2, 4, p	19	$\{\neg s\}$	resolve 5, 8, r			
9	$\{\neg p, \neg s\}$	resolve 2, 5, r	20	$\{s, \neg s\}$	resolve 5, 10, r			
10	$\{\neg r, s\}$	resolve 2, 7, p	21	$\{r, \neg r\}$	resolve 5, 10, s			
11	$\{\neg q, r\}$	resolve 3, 5, s	22	$\{\neg q, \neg s\}$	resolve 5, 16, r			

no further resolvents

$\Longrightarrow$

satisfiable

Example ❹

$$\neg\big((p \vee q) \wedge (\neg s \vee \neg u) \wedge (\neg r \vee \neg w) \wedge (t \vee u) \wedge (\neg p \vee \neg r) \wedge (\neg q \vee \neg s) \wedge (\neg p \vee \neg t) \wedge (\neg q \vee \neg u) \wedge (r \vee s) \wedge (\neg t \vee \neg v) \wedge (v \vee w) \big)$$

1	$\{p, q\}$	
2	$\{\neg s, \neg u\}$	
3	$\{\neg r, \neg w\}$	
4	$\{t, u\}$	
5	$\{\neg p, \neg r\}$	
6	$\{\neg q, \neg s\}$	
7	$\{\neg p, \neg t\}$	
8	$\{\neg q, \neg u\}$	
9	$\{r, s\}$	
10	$\{\neg t, \neg v\}$	
11	$\{v, w\}$	
12	$\{\neg s, t\}$	resolve 2, 4, u
13	$\{\neg p, s\}$	resolve 5, 9, r
14	$\{\neg p, \neg s\}$	resolve 7, 12, t
15	$\{\neg p\}$	resolve 13, 14, s
16	$\{q\}$	resolve 1, 15, p
17	$\{\neg s\}$	resolve 6, 16, q
18	$\{r\}$	resolve 9, 17, s
19	$\{\neg w\}$	resolve 3, 18, r
20	$\{v\}$	resolve 11, 19, w
21	$\{\neg t\}$	resolve 10, 20, v
22	$\{u\}$	resolve 4, 21, t
23	$\{\neg q\}$	resolve 8, 22, u
24	$\Box$	resolve 16, 23, q
	valid	

Outline

Question

Which clauses can be obtained by resolving two clauses from the following clausal form ?

$$\{\{p, q, \neg q\}, \{r, \neg q\}, \{p, \neg r\}, \{q, \neg s\}, \{\neg r, s\}\}$$

A $\{p, s\}$

B $\{p, \neg q\}$

C $\{\neg r, q, \neg q\}$

D $\{r, \neg r\}$

E $\{p, q, \neg s\}$

F $\{p\}$

Outline

Definitions

- boolean function f of n arguments is mapping from $\{0,1\}^n$ to $\{0,1\}$
- four basic functions

complement	$\overline{}$
product	$\cdot$
sum	$+$
exclusive or	$\oplus$

(xy denotes $x \cdot y$)

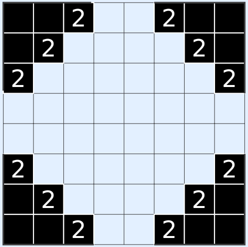
x	$\overline{x}$
0	1
1	0

x	y	xy	$x+y$	$x \oplus y$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

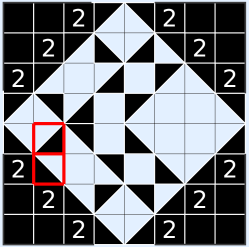
Remarks

- every boolean function can be expressed in terms of basic functions
- propositional formulas and truth tables are different representations of boolean functions

Exclusive Or or Or



Shakashaka




```
(assert (=> (= x0y3 SW) (and
    (= x0y4 NW)
    (xor (= x1y2 SW) (= x1y3 SE))
    (or (= x1y4 W) (= x1y4 NE))
)))
```

Representations of Boolean Functions

		test for		boolean operation		
representation	compact ?	satisfiability	validity	product	sum	complement
propositional formulas	often	hard	hard	easy	easy	easy
truth tables	never	hard	hard	hard	hard	hard
CNFs	sometimes	hard	easy	easy	hard	hard
DNFs	sometimes	easy	hard	hard	easy	hard
?	often	easy	easy	medium	medium	easy

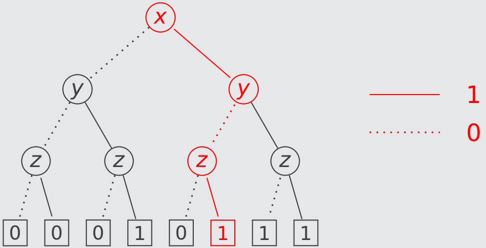
? = reduced ordered binary decision diagrams

Example

- majority function

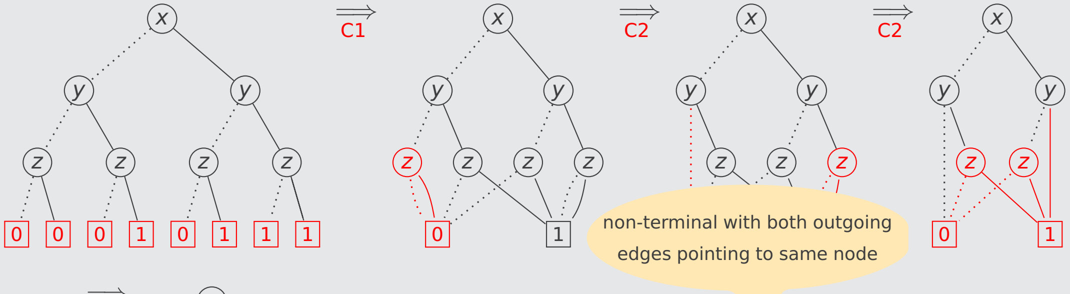
$$f(x, y, z) = \begin{cases} 1 & \text{if } x + y + z > 1 \\ 0 & \text{otherwise} \end{cases}$$

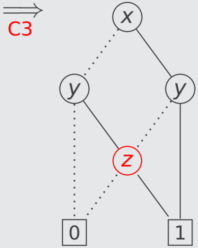
- binary decision tree for f



- $f(1, 0, 1) = 1$

Example (Binary Decision Diagram)





Optimisation Rules

C1 remove duplicate terminals

C2 remove redundant tests

C3 remove duplicate non-terminals

Remark

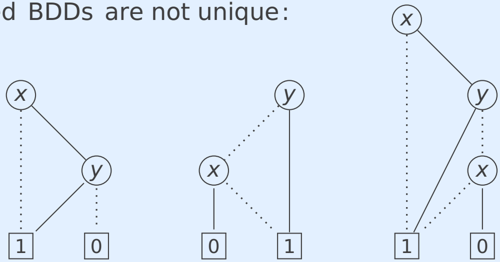
binary decision diagram (BDD) is directed acyclic graph (dag)

Definition

BDD is reduced if C1, C2, C3 are not applicable

Remark

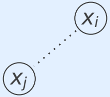
reduced BDDs are not unique:

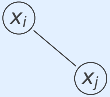


represent boolean function $\overline{x} + y$

Definition

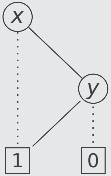
BDD B is ordered if there exists order $[x_1, \ldots, x_n]$ of variables in B such that

$i < j$ for all edges 

and 

in B

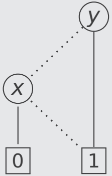
Examples



OBDD

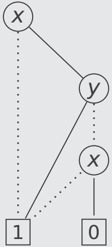
$[x, y]$

$[z, x, y]$ $[x, z, y]$ $[x, y, z]$



OBDD

$[y, x]$



not ordered

Definition

orders o_1 and o_2 are compatible if o_1 and o_2 are subsequences of some order o

Example

four variable orders

$$o_1 = [x, y, z] \qquad o_2 = [x, v] \qquad o_3 = [z, x] \qquad o_4 = [v, z, w]$$

- o_1 and o_2 are compatible (e.g. $o = [x, y, v, z]$)
- o_1 and o_3 are not compatible
- o_2 and o_4 are compatible

Lemma

reductions C1, C2, C3 preserve order

Theorem

reduced OBDD representation of boolean function for given order is unique

Corollary

checking

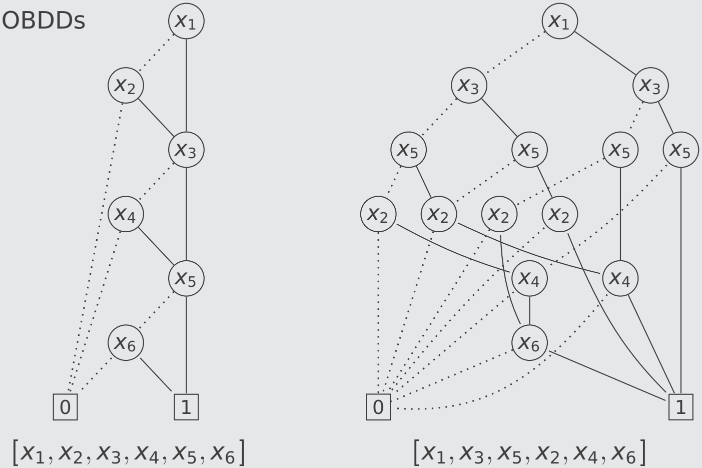
- satisfiability
- validity
- equivalence

is trivial for reduced OBDDs (with compatible variable orders)

Example

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1 + x_2) \cdot (x_3 + x_4) \cdot (x_5 + x_6)$$

different reduced OBDDs



Outline

Huth and Ryan

- Section 1.4.4
- Section 6.1

Resolution

- Wikipedia [accessed December 7, 2022]

Important Concepts

- binary decision diagram
- binary decision tree
- boolean function
- complementary literals
- completeness
- clashing
- clausal form
- clause
- compatible variable order
- empty clause
- exclusive or
- ordered BDD
- parent clauses
- reduced BDD
- refutation
- resolution
- resolvent
- variable order

homework for April 11