universität innsbruck

26S lecture 6

Logic

Luca Campa Philipp Dablander Aaron Groß Aart Middeldorp

Alexander Montag Johannes Niederhauser Vera Schmitt

articify with session ID **6893 6178** for anonymous questions

ars.uibk.ac.at

Outline

BDD Algorithms

- **reduce** input: • OBDD
  output: • equivalent reduced OBDD with compatible variable ordering
- **restrict** input: • OBDD B_f, variable x, $i \in \{0,1\}$
  output: • reduced OBDD of $f[i/x]$ with compatible variable ordering
- **apply** input: • binary operation $\star$ on boolean functions
  • OBDDs B_f and B_g with compatible variable orderings
  output: • reduced OBDD of $f \star g$ with compatible variable ordering

Theorem (Shannon expansion)

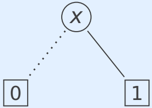
$f = \overline{x} \cdot f[0/x] + x \cdot f[1/x] = \overline{x} \cdot f[0/x] \oplus x \cdot f[1/x]$ for every boolean function f and variable x

Definition

quantification of boolean function f over variable x:

$$\exists x.f = f[0/x] + f[1/x] \qquad \forall x.f = f[0/x] \cdot f[1/x]$$

BDD operations

function f	OBDD B_f	function f	OBDD B_f	function f	OBDD B_f
0	0	$g + h$	$\mathrm{apply}(+, B_g, B_h)$	$g[0/x]$	$\mathrm{restrict}(0, x, B_g)$
1	1	$g \oplus h$	$\mathrm{apply}(\oplus, B_g, B_h)$	$g[1/x]$	$\mathrm{restrict}(1, x, B_g)$
x		$g \cdot h$	$\mathrm{apply}(\cdot, B_g, B_h)$	$\exists x.g$	$\mathrm{apply}(+, B_{g[0/x]}, B_{g[1/x]})$
		$\overline{g}$	$\mathrm{apply}(\oplus, B_g, B_1)$	$\forall x.g$	$\mathrm{apply}(\cdot, B_{g[0/x]}, B_{g[1/x]})$

Remark

(reduced ordered) BDDs are not always efficient representation

hidden weighted bit function multiplication

Definitions

- **terms** in predicate logic are built from function symbols and variables according to BNF grammar $t ::= x \mid c \mid f(t, \dots, t)$
- **formulas** in predicate logic are built according to BNF grammar

$$\varphi ::= P \mid P(t, \dots, t) \mid t = t \mid \bot \mid \top \mid (\neg\varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \to \varphi) \mid (\forall x\, \varphi) \mid (\exists x\, \varphi)$$

- occurrence of variable x in formula φ is **free in φ** if it is leaf node in parse tree of φ such that there is no node $\forall x$ or $\exists x$ on path to root node; all other occurrences of x are bound
- $\varphi[t/x]$ is result of replacing all **free** occurrences of x in φ by t
- t is **free for** x in φ if variables in t do not become bound in $\varphi[t/x]$
- **sentence** is formula without free variables

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

Definition

model $\mathcal{M}$ for pair $(\mathcal{F}, \mathcal{P})$

- $\mathcal{F}$ set of function symbols
- $\mathcal{P}$ set of predicate symbols

consists of

① non–empty set A (universe of concrete values)

② function $f^{\mathcal{M}} \colon A^n \to A$ for every n–ary function symbol $f \in \mathcal{F}$

③ subset $P^{\mathcal{M}} \subseteq A^n$ for every n–ary predicate symbol $P \in \mathcal{P}$

"P holds for all tuples $(a_1, \dots, a_n)$ in $P^{\mathcal{M}}$"

④ $=^{\mathcal{M}}$ is identity relation on A

Remark

if P is constant then $P^{\mathcal{M}} \subseteq A^0 = \{()\}$: $P^{\mathcal{M}} = \varnothing$ or $P^{\mathcal{M}} = \{()\}$

Examples

function and predicate symbols

- $\mathcal{P}$ A, B: arity 2 P, S, L: arity 1 $\mathcal{F}$ m: arity 0

1. model $\mathcal{M}_1$ is well–defined only if Aki Suzuki $\in A_1$ ("natural" model)
   - universe A_1: set of computer science students and professors of University of Innsbruck together with all lectures offered in 26S in bachelor program computer science
   - $A^{\mathcal{M}_1} = \{(x, y) \mid x \text{ admires } y\}$ $P^{\mathcal{M}_1} = \{x \mid x \text{ is professor}\}$ $L^{\mathcal{M}_1} = \{x \mid x \text{ is lecture}\}$
     $B^{\mathcal{M}_1} = \{(x, y) \mid x \text{ attended } y\}$ $S^{\mathcal{M}_1} = \{x \mid x \text{ is student}\}$ $m^{\mathcal{M}_1} = \text{Aki Suzuki}$
2. model $\mathcal{M}_2$
   - universe A_2: set of natural numbers
   - $A^{\mathcal{M}_2} = \{(x, y) \mid x > y\}$ $P^{\mathcal{M}_2} = \{x \mid x \text{ is prime number}\}$ $L^{\mathcal{M}_2} = \{2, 7, 111\}$
     $B^{\mathcal{M}_2} = \{(x, y) \mid x + y = 5\}$ $S^{\mathcal{M}_2} = \{x^2 \mid x > 1\}$ $m^{\mathcal{M}_2} = 13$

Definitions

- environment (look–up table) for model $\mathcal{M} = (A, \{f^{\mathcal{M}}\}_{f \in \mathcal{F}}, \{P^{\mathcal{M}}\}_{P \in \mathcal{P}})$ is mapping I from variables to elements of A
- value $t^{\mathcal{M},I}$ of term t in model $\mathcal{M}$ relative to environment I is defined inductively:

$$t^{\mathcal{M},I} = \begin{cases} I(t) & \text{if } t \text{ is variable} \\ f^{\mathcal{M}}(t_1^{\mathcal{M},I}, \dots, t_n^{\mathcal{M},I}) & \text{if } t = f(t_1, \dots, t_n) \end{cases}$$

- given environment I, variable x, and element $a \in A$, environment $I[x \mapsto a]$ is defined as

$$I[x \mapsto a](y) = \begin{cases} a & \text{if } y = x \\ I(y) & \text{if } y \neq x \end{cases}$$

Example

function symbols $\mathcal{F}$

- f: arity 2 $\quad g, h$: arity 1 $\quad a$: arity 0

model $\mathcal{M}$

- universe A: set of natural numbers
- $f^{\mathcal{M}}(x,y) = x \times y \qquad g^{\mathcal{M}}(x) = x + 1 \qquad h^{\mathcal{M}}(x) = x^2 \qquad a^{\mathcal{M}} = 2$

environment I

- $I(x) = 3 \qquad I(y) = 5 \qquad \dots$

$$f(x, g(y))^{\mathcal{M},I} = 18 \qquad f(x, g(f(x, h(x))))^{\mathcal{M},I} = 84 \qquad f(h(a), g(f(a, h(h(a)))))^{\mathcal{M},I} = 132$$

Definition

satisfaction relation $\mathcal{M} \vDash_I \varphi$ (model $\mathcal{M}$, enviroment I, formula φ) is defined inductively:

$$\mathcal{M} \vDash_I \top$$

$$\mathcal{M} \nvDash_I \bot$$

$$\mathcal{M} \vDash_I \varphi \iff \begin{cases} (t_1^{\mathcal{M},I}, \dots, t_n^{\mathcal{M},I}) \in P^{\mathcal{M}} & \text{if } \varphi = P(t_1, \dots, t_n) \\ t_1^{\mathcal{M},I} = t_2^{\mathcal{M},I} & \text{if } \varphi = (t_1 = t_2) \\ \mathcal{M} \nvDash_I \psi & \text{if } \varphi = \neg\psi \\ \mathcal{M} \vDash_I \psi_1 \text{ and } \mathcal{M} \vDash_I \psi_2 & \text{if } \varphi = \psi_1 \wedge \psi_2 \\ \mathcal{M} \vDash_I \psi_1 \text{ or } \mathcal{M} \vDash_I \psi_2 & \text{if } \varphi = \psi_1 \vee \psi_2 \\ \mathcal{M} \nvDash_I \psi_1 \text{ or } \mathcal{M} \vDash_I \psi_2 & \text{if } \varphi = \psi_1 \rightarrow \psi_2 \\ \mathcal{M} \vDash_{I[x \mapsto a]} \psi \text{ for all } a \in A & \text{if } \varphi = \forall x\, \psi \\ \mathcal{M} \vDash_{I[x \mapsto a]} \psi \text{ for some } a \in A & \text{if } \varphi = \exists x\, \psi \end{cases}$$

Notation

$\mathcal{M} \nvDash_I \psi$ denotes "not $\mathcal{M} \vDash_I \psi$"

Definition

sentence is formula without free variables

Lemma

if φ is sentence then

$$\mathcal{M} \vDash_{I} \varphi \iff \mathcal{M} \vDash_{I'} \varphi$$

for all environments I and I'

truth value of sentence does not depend on environment

Notation

$\mathcal{M} \vDash \varphi$ instead of $\mathcal{M} \vDash_{I} \varphi$ for sentences φ

Example

- function and predicate symbols $\mathcal{P}$ R: arity 2 $\mathcal{F}$ f: arity 1 a: arity 0
- model $\mathcal{M}_1$: universe $A_1 = \mathbb{N}$ $R^{\mathcal{M}_1} = \{(x,y) \mid x < y\}$ $f^{\mathcal{M}_1}(x) = 2x$ $a^{\mathcal{M}_1} = 0$
- model $\mathcal{M}_2$: universe $A_2 = \mathbb{R}$ $R^{\mathcal{M}_2} = \{(x,y) \mid x < y\}$ $f^{\mathcal{M}_2}(x) = 2x$ $a^{\mathcal{M}_2} = 0$
- model $\mathcal{M}_3$: universe $A_3 = \{0,1\}$ $R^{\mathcal{M}_3} = \{(x,y) \mid x < y\}$ $f^{\mathcal{M}_3}(x) = \overline{x}$ $a^{\mathcal{M}_3} = 0$
- formulas

$\varphi_1 = \exists\, x\, R(a,x)$ $\mathcal{M}_1 \vDash \varphi_1$ $\mathcal{M}_2 \vDash \varphi_1$ $\mathcal{M}_3 \vDash \varphi_1$

$\varphi_2 = \forall\, x\, (R(x,f(x)) \vee x = a)$ $\mathcal{M}_1 \vDash \varphi_2$ $\mathcal{M}_2 \nvDash \varphi_2$ $\mathcal{M}_3 \nvDash \varphi_2$

$\varphi_3 = \forall\, x\, \forall\, y\, (R(x,y) \rightarrow \exists\, z\, (R(x,z) \wedge R(z,y)))$ $\mathcal{M}_1 \nvDash \varphi_3$ $\mathcal{M}_2 \vDash \varphi_3$ $\mathcal{M}_3 \nvDash \varphi_3$

Example

some professor admires Mary

$$\varphi = \exists x\,(P(x) \wedge A(x,m)) \qquad\qquad \psi = \exists x\,(P(x) \rightarrow A(x,m))$$

- model $\mathcal{M}$: universe is set of persons living in Innsbruck

  $P^{\mathcal{M}} = \varnothing$ $\quad A^{\mathcal{M}} = \varnothing$ $\quad m^{\mathcal{M}} =$ Diana
- $\mathcal{M} \nvDash \varphi$
- $\mathcal{M} \vDash \psi$

Definitions

formula ψ, (possibly infinite) set of formulas Γ

- ψ is satisfiable if $\mathcal{M} \vDash_I \psi$ for some model $\mathcal{M}$ and environment I
- Γ is satisfiable (consistent) if $\mathcal{M} \vDash_I \varphi$ for all $\varphi \in \Gamma$, for some model $\mathcal{M}$ and environment I

Example

$\Gamma = \{\varphi_1, \varphi_2, \varphi_3\}$ with

$$\begin{aligned} \varphi_1 &= \exists\, x\, R(a, x) \\ \varphi_2 &= \forall\, x\, (R(x, f(x)) \vee x = a) \\ \varphi_3 &= \forall\, x\, \forall\, y\, (R(x, y) \rightarrow \exists\, z\, (R(x, z) \wedge R(z, y))) \end{aligned}$$

is satisfiable in model $\mathcal{M}$:

- universe A: set of natural numbers
- $R^{\mathcal{M}} = \{(x, y) \mid x \leqslant y\}$ $\quad f^{\mathcal{M}}(x) = x$ $\quad a^{\mathcal{M}} = 0$

Definitions

formula ψ, (possibly infinite) set of formulas Γ

- $\Gamma \vDash \psi$ (semantic entailment) if $\mathcal{M} \vDash_l \psi$ whenever $\mathcal{M} \vDash_l \varphi$ for all $\varphi \in \Gamma$, for all (appropriate) models $\mathcal{M}$ and environments l
- ψ is valid if $\mathcal{M} \vDash_l \psi$ for all (appropriate) models $\mathcal{M}$ and environments l

Example

- $\Gamma \vDash \neg R(a,a) \to \exists x \, \neg(x = a)$ for $\Gamma = \{\varphi_1, \varphi_2, \varphi_3\}$ with

$$\begin{aligned} \varphi_1 &= \exists x \, R(a,x) \\ \varphi_2 &= \forall x \, (R(x,f(x)) \vee x = a) \\ \varphi_3 &= \forall x \, \forall y \, (R(x,y) \to \exists z \, (R(x,z) \wedge R(z,y))) \end{aligned}$$

- $\forall x \, \forall y \, (x = y \to f(x) = f(y))$ is valid

Outline

Question

Which of the following statements are true ?

A There exists a model $\mathcal{M}$ such that $\mathcal{M} \vDash \exists\, x\, P(x) \to \forall\, x\, P(x)$ holds.

B The semantic entailment $f(x) = f(y) \vDash x = y$ holds.

C The set $\{\forall\, x\, (P(x) \to \bot), \exists\, y\, (Q(y) \to P(y))\}$ is consistent.

D The semantic entailment $\neg\forall\, x\, \neg\varphi \vDash \neg\exists\, x\, \neg\varphi$ is valid for all formulas φ.

Outline

Proof Rules of Natural Deduction ❶

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

Proof Rules of Natural Deduction ❷

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

derived proof rules

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

Outline

Definitions

- equality introduction

$$\frac{}{t = t}\ {=}\mathrm{i}$$

- equality elimination "replace equals by equals"

$$\frac{t_1 = t_2 \qquad \varphi[t_1/x]}{\varphi[t_2/x]}\ {=}\mathrm{e}$$

provided t_1 and t_2 are free for x in φ

Examples

1. $s = t \vdash t = s$ is valid:

1	$s = t$	premise	
2	$s = s$	$=$i	
3	$t = s$	$=$e $1, 2$	with $\varphi = (x = s)$, $t_1 = s$, $t_2 = t$

2. $s = t, t = u \vdash s = u$ is valid:

1	$s = t$	premise	
2	$t = u$	premise	
3	$s = u$	$=$e $2, 1$	with $\varphi = (s = x)$, $t_1 = t$, $t_2 = u$

Outline

Definitions

- $\forall$ elimination

$$\frac{\forall x\, \varphi}{\varphi[t/x]}\ \forall e$$

provided t is free for x in φ

- $\forall$ introduction

$$\frac{\boxed{\begin{array}{l} x_0 \\ \quad\vdots \\ \quad\varphi[x_0/x] \end{array}}}{\forall x\, \varphi}\ \forall i$$

where x_0 is fresh variable that is used only inside box

Example

$\forall x\,(P(x) \to Q(x)),\ \forall x\,P(x) \vdash \forall x\,Q(x)$ is valid:

1		$\forall x\,(P(x) \to Q(x))$	premise
2		$\forall x\,P(x)$	premise
3	x_0	$P(x_0) \to Q(x_0)$	$\forall$e 1
4		$P(x_0)$	$\forall$e 2
5		$Q(x_0)$	$\to$e 3, 4
6		$\forall x\,Q(x)$	$\forall$i 3–5

Example

$P \to \forall x\, Q(x) \vdash \forall x\, (P \to Q(x))$ is valid:

1	$P \to \forall x\, Q(x)$	premise
2	x_0	
3	P	assumption
4	$\forall x\, Q(x)$	$\to$e 1, 3
5	$Q(x_0)$	$\forall$e 4
6	$P \to Q(x_0)$	$\to$i 3–5
7	$\forall x\, (P \to Q(x))$	$\forall$i 2–6

Outline

Definitions

- ∃ introduction

$$\frac{\varphi[t/x]}{\exists x\, \varphi}\ \exists i$$

provided t is free for x in φ

- ∃ elimination

$$\frac{\exists x\, \varphi \qquad \boxed{\begin{array}{cc} x_0 & \varphi[x_0/x] \\ & \vdots \\ & \chi \end{array}}}{\chi}\ \exists e$$

where x_0 is fresh variable that is used only inside box

Example

$\forall x\,(P(x) \to Q(x)),\ \exists x\,P(x) \vdash \exists x\,Q(x)$ is valid:

1		$\forall x\,(P(x) \to Q(x))$	premise
2		$\exists x\,P(x)$	premise
3	x_0	$P(x_0)$	assumption
4		$P(x_0) \to Q(x_0)$	$\forall$e 1
5		$Q(x_0)$	$\to$e 4, 3
6		$\exists x\,Q(x)$	$\exists$i 5
7		$\exists x\,Q(x)$	$\exists$e 2, 3–6

Lemma

$\forall x\, \varphi \vdash \exists x\, \varphi$ is valid

Proof

1	$\forall x\, \varphi$	premise
2	$\varphi[x/x]$	$\forall$e 1
3	$\exists x\, \varphi$	$\exists$i 2

Example

$\exists x\, P(x),\ \forall x\, \forall y\, (P(x) \rightarrow Q(y)) \vdash \forall y\, Q(y)$ is valid:

1		$\exists x\, P(x)$	premise
2		$\forall x\, \forall y\, (P(x) \rightarrow Q(y))$	premise
3	z		
4	y_0	$P(y_0)$	assumption
5		$\forall y\, (P(y_0) \rightarrow Q(y))$	$\forall$e 2
6		$P(y_0) \rightarrow Q(z)$	$\forall$e 5
7		$Q(z)$	$\rightarrow$e 6, 4
8		$Q(z)$	$\exists$e 1, 4–7
9		$\forall y\, Q(y)$	$\forall$i 3–8

Lemma

$\neg \forall x\, \varphi \vdash \exists x\, \neg \varphi$ is valid

Proof

1	$\neg \forall x\, \varphi$	premise
2	$\neg \exists x\, \neg \varphi$	assumption
3	x_0	
4	$\neg \varphi[x_0/x]$	assumption
5	$\exists x\, \neg \varphi$	$\exists$i 4
6	$\bot$	$\neg$e 5, 2
7	$\varphi[x_0/x]$	PBC 4 – 6
8	$\forall x\, \varphi$	$\forall$i 3 – 7
9	$\bot$	$\neg$e 8, 1
10	$\exists x\, \neg \varphi$	PBC 2 – 9

Example

$\forall x\, \exists y\, P(x,y),\ \forall x\, \forall y\, (P(x,y) \rightarrow Q(x,y)) \vdash \exists y\, \forall x\, Q(x,y)$ is not valid:

1		$\forall x\, \exists y\, P(x,y)$	premise
2		$\forall x\, \forall y\, (P(x,y) \rightarrow Q(x,y))$	premise
3	x_0	$\exists y\, P(x_0,y)$	$\forall$e 1
4		$\forall y\, (P(x_0,y) \rightarrow Q(x_0,y))$	$\forall$e 2
5	y_0	$P(x_0,y_0)$	assumption
6		$P(x_0,y_0) \rightarrow Q(x_0,y_0)$	$\forall$e 4
7		$Q(x_0,y_0)$	$\rightarrow$e 6, 5
8		$Q(x_0,y_0)$	$\exists$e 3, 5–7
9		$\forall x\, Q(x,y_0)$	$\forall$i 3–8
10		$\exists y\, \forall x\, Q(x,y)$	$\exists$i 9

Example

$\forall x \, \exists y \, P(x,y), \; \forall x \, \forall y \, (P(x,y) \to Q(x,y)) \not\models \exists y \, \forall x \, Q(x,y)$

model $\mathcal{M}$

- universe A: set of natural numbers
- $P^{\mathcal{M}} = Q^{\mathcal{M}} = \{(x,y) \mid x < y\}$

$\mathcal{M} \models \forall x \, \exists y \, P(x,y)$

$\mathcal{M} \models \forall x \, \forall y \, (P(x,y) \to Q(x,y))$

$\mathcal{M} \not\models \exists y \, \forall x \, Q(x,y)$

Outline

Definition

(possibly infinite) set of formulas Γ, formula ψ

- sequent $\Gamma \vdash \psi$ is valid if there exists (finite) natural deduction proof of ψ in which all premises are from Γ

Theorem (Gödel's Completeness Theorem)

natural deduction for predicate logic is sound and complete:

$$\Gamma \vDash \psi \quad \Longleftrightarrow \quad \Gamma \vdash \psi \text{ is valid}$$

Decision Problem (Church's Theorem)

instance: set of formulas Γ, first–order formula φ

question: $\Gamma \vDash \varphi$?

is undecidable even when $\Gamma = \varnothing$ (lecture 8)

Outline

Huth and Ryan

- Section 2.3
- Section 2.4

Gödel's Completeness Theorem

- Wikipedia [accessed December 27, 2024]

Important Concepts

- ∀ elimination
- ∀ introduction
- ∃ elimination
- ∃ introduction
- consistency
- environment
- equality
- equality elimination
- equality introduction
- Gödel’s completeness theorem
- look–up table
- model
- satisfaction relation
- satisfiability
- semantic entailment
- universe
- validity of formulas
- validity of sequents

homework for April 30