Logic

Diana Gründlinger Jamie Hochrainer Christina Kohl

Aart Middeldorp Fabian Mitterwallner Thomas Oberroither

Outline

1. **Summary of Previous Lecture**
2. **Horn Formulas**
3. **Intermezzo**
4. **SAT**
5. **Tseitin's Transformation**
6. **Further Reading**

Definitions

- semantic entailment

$$\varphi_1, \varphi_2, \dots, \varphi_n \vDash \psi$$

  if $\bar{v}(\psi) = \mathsf{T}$ whenever $\bar{v}(\varphi_1) = \bar{v}(\varphi_2) = \cdots = \bar{v}(\varphi_n) = \mathsf{T}$ for every valuation v

- tautology is formula φ such that $\vDash \varphi$
- formula φ is
  - valid if $\bar{v}(\varphi) = \mathsf{T}$ for every valuation v
  - satisfiable if $\bar{v}(\varphi) = \mathsf{T}$ for some valuation v
- formulas φ and ψ are semantically equivalent $(\varphi \equiv \psi)$ if both $\varphi \vDash \psi$ and $\psi \vDash \varphi$

Theorem

formula φ is valid $\iff$ $\neg\varphi$ is unsatisfiable $\iff$ φ is tautology

Definitions

- literal is atom p or negation $\neg p$ of atom
- clause is disjunction $\ell_1 \vee \cdots \vee \ell_n$ of literals
- conjunctive normal form (CNF) is conjunction $C_1 \wedge \cdots \wedge C_n$ of clauses
- literals ℓ_1 and ℓ_2 are complementary if $\ell_1 = \neg\ell_2$ or $\neg\ell_1 = \ell_2$

Theorem

- $\forall$ formula φ $\exists$ CNF ψ such that $\varphi \equiv \psi$
- validity of CNFs is efficiently decidable:

$$\text{CNF } \varphi \text{ is valid} \quad \Longleftrightarrow \quad \text{every clause of } \varphi \text{ contains complementary literals}$$

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, 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

Definitions

- Horn clause is propositional formula

$$P_1 \wedge P_2 \wedge \cdots \wedge P_n \rightarrow Q$$

  with $n \geqslant 1$ and where $P_1, \ldots, P_n, Q$ are atoms, $\bot$ or $\top$
- Horn formula is conjunction of Horn clauses

Backus–Naur Form (H)

$$\begin{aligned} P &::= p \mid \bot \mid \top \\ A &::= P \mid P \wedge A \end{aligned} \qquad \begin{aligned} C &::= A \rightarrow P \\ H &::= C \mid C \wedge H \end{aligned}$$

Theorem

satisfiability of Horn formulas is efficiently decidable

Procedure

① maintain list of atoms, $\bot$, $\top$ occurring in φ

② mark $\top$ if it appears in list

③ **while** Horn clause $P_1 \wedge \cdots \wedge P_n \to Q$ exists in φ such that all $P_1, \dots, P_n$ are marked and Q is unmarked

mark Q

④ **if** $\bot$ is marked **then**

return unsatisfiable

else

return satisfiable

satisfying assignment: $v(P) = \begin{cases} \mathsf{T} & \text{if } P \text{ is marked} \\ \mathsf{F} & \text{if } P \text{ is unmarked} \end{cases}$

Examples

1. Horn formula

$$(p \wedge q \wedge w \rightarrow \bot) \wedge (t \rightarrow \bot) \wedge (r \rightarrow \underset{④}{p}) \wedge (\top \rightarrow \underset{②}{r}) \wedge (\top \rightarrow \underset{③}{q}) \wedge (\top \rightarrow \underset{⑤}{u}) \wedge (u \rightarrow \underset{⑥}{s})$$

list $\quad p \quad q \quad r \quad s \quad t \quad u \quad w \quad \bot \quad \underset{①}{\top}$

satisfiable $\quad v(p) = v(q) = v(r) = v(s) = v(u) = \mathsf{T} \qquad v(t) = v(w) = \mathsf{F}$

2. Horn formula

$$(p \wedge q \wedge w \rightarrow \underset{⑦}{\bot}) \wedge (t \rightarrow \bot) \wedge (r \rightarrow \underset{④}{p}) \wedge (\top \rightarrow \underset{②}{r}) \wedge (\top \rightarrow \underset{③}{q}) \wedge (\top \rightarrow \underset{⑤}{u}) \wedge (u \rightarrow \underset{⑥}{w})$$

list $\quad p \quad q \quad r \quad t \quad u \quad w \quad \bot \quad \underset{①}{\top}$

unsatisfiable

Outline

Particify with session ID **8082 7463**

Question

Consider the formula $\varphi = (p \wedge \neg q \rightarrow \top) \wedge (q \wedge \neg p \rightarrow q)$.

Which of the following statements hold for φ ?

A φ is a CNF

B φ is a Horn formula

C $\varphi \equiv p \wedge \neg q$

D φ is satisfiable

E φ is valid

Outline

Satisfiability (SAT)

instance: propositional formula φ

question: is φ satisfiable ?

Theorem

SAT is NP-complete

Links

- SAT competition
- Millennium Problems – P vs NP

SAT Applications

- bounded model checking
- combinatorial design theory
- haplotyping in bioinformatics
- hardware verification
- logic puzzles
- package management in software distributions
- planning and scheduling
- software verification
- sorting networks
- statistical physics
- term rewriting
- $\cdots \quad \cdots \quad \cdots$

Popular SAT Solvers

MiniSat PicoSAT Z3

Example（数独 Sudoku）

	6		1		4		5	
		8	3		5	6		
2								1
8			4		7			6
		6				3		
7			9		1			4
5								2
		7	2		6	9		
	4		5		8		7	

11	12	13	14	15	16	17	18	19
21	22	23	24	25	26	27	28	29
31	32	33	34	35	36	37	38	39
41	42	43	44	45	46	47	48	49
51	52	53	54	55	56	57	58	59
61	62	63	64	65	66	67	68	69
71	72	73	74	75	76	77	78	79
81	82	83	84	85	86	87	88	89
91	92	93	94	95	96	97	98	99

Variables

- propositional atoms x_{ijd} for $i, j, d \in \{1, \dots, 9\}$
- $v(x_{ijd}) = \mathsf{T} \iff$ cell ij contains digit d

11	12	13	14	15	16	17	18	19
21	22	23	24	25	26	27	28	29
31	32	33	34	35	36	37	38	39
41	42	43	44	45	46	47	48	49
51	52	53	54	55	56	57	58	59
61	62	63	64	65	66	67	68	69
71	72	73	74	75	76	77	78	79
81	82	83	84	85	86	87	88	89
91	92	93	94	95	96	97	98	99

Constraints

- every cell contains at least one digit
- every cell contains at most one digit
- in every row / column / 3×3 block every digit appears at most once

Cardinality Constraints

for non-empty set A of propositional atoms:

$$\text{at-least-one}(A) = \bigvee_{x \in A} x \qquad \text{at-most-one}(A) = \bigwedge_{\substack{x,y \in A \\ x \neq y}} (\neg x \vee \neg y)$$

Example

$$\text{at-least-one}(\{p,q,r\}) = p \vee q \vee r$$

$$\text{at-most-one}(\{p,q,r\}) = (\neg p \vee \neg q) \wedge (\neg p \vee \neg r) \wedge (\neg q \vee \neg r)$$

Useful Abbreviations

$$D = \{1,2,3,4,5,6,7,8,9\}$$

$$\mathcal{G} = \{\{1,2,3\},\{4,5,6\},\{7,8,9\}\}$$

$$\mathcal{C} = \{\{x_{ijd} \mid j \in D\} \mid i,\, d \in D\} \cup \{\{x_{ijd} \mid i \in D\} \mid j,\, d \in D\} \cup \{\{x_{ijd} \mid (i,j) \in I \times J\} \mid I, J \in \mathcal{G},\, d \in D\}$$

11	12	13	14	15	16	17	18	19
21	22	23	24	25	26	27	28	29
31	32	33	34	35	36	37	38	39
41	42	43	44	45	46	47	48	49
51	52	53	54	55	56	57	58	59
61	62	63	64	65	66	67	68	69
71	72	73	74	75	76	77	78	79
81	82	83	84	85	86	87	88	89
91	92	93	94	95	96	97	98	99

	6		1		4		5	
		8	3		5	6		
2								1
8			4		7			6
		6				3		
7			9		1			4
5								2
		7	2		6	9		
	4		5		8		7	

SAT Encoding

$$\begin{aligned}\varphi\colon\quad & \bigwedge\{\text{at-least-one}(\{x_{ijd} \mid d \in D\}) \mid i,j \in D\} \wedge \bigwedge\{\text{at-most-one}(A) \mid A \in \mathcal{C}\} \wedge \\ & \bigwedge\{\text{at-most-one}(\{x_{ijd} \mid d \in D\}) \mid i,j \in D\} \wedge x_{126} \wedge x_{141} \wedge x_{164} \wedge \cdots \wedge x_{987}\end{aligned}$$

- φ is satisfiable $\iff$ Sudoku puzzle has solution
- satisfying assignment gives rise to Sudoku solution

$$\mathcal{D} = \{1,2,3,4\}$$
$$\mathcal{G} = \{\{1,2\},\{3,4\}\}$$
$$\mathcal{C} = \{\{x_{ijd} \mid j \in D\} \mid i, d \in D\} \cup \{\{x_{ijd} \mid i \in D\} \mid j, d \in D\} \cup \{\{x_{ijd} \mid (i,j) \in I \times J\} \mid I, J \in \mathcal{G}, d \in D\}$$

Example (2 × 2 数独 Sudoku)

		1	
3			
	4		

11	12	13	14
21	22	23	24
31	32	33	34
41	42	43	44

$$\begin{aligned}\mathcal{C} = {} & \{\{x_{111},x_{121},x_{131},x_{141}\},\{x_{112},x_{122},x_{132},x_{142}\},\dots,\{x_{414},x_{424},x_{434},x_{444}\}\} \\ & \cup \{\{x_{111},x_{211},x_{311},x_{411}\},\{x_{121},x_{221},x_{321},x_{421}\},\dots,\{x_{144},x_{244},x_{344},x_{444}\}\} \\ & \cup \{\{x_{111},x_{121},x_{211},x_{221}\},\{x_{112},x_{122},x_{212},x_{222}\},\dots,\{x_{334},x_{344},x_{434},x_{444}\}\}\end{aligned}$$

Pythagorean Triples Problem

can one color all natural numbers with two colors such that whenever $x^2 + y^2 = z^2$ not all of x, y, z have same color ?

Example

$$3^2 + 4^2 = 5^2 \qquad 5^2 + 12^2 = 13^2 \qquad \dots$$

1 2 3 4 5 6 7 8 9 10 11 12 13 ... ☹

SAT Encoding

- propositional atoms x_i for $1 \leqslant i \leqslant n$
- $v(x_i) = \mathsf{T} \quad \iff \quad$ number i is colored red
- encoding contains clauses $(x_a \vee x_b \vee x_c)$ and $(\neg x_a \vee \neg x_b \vee \neg x_c)$ for all $a^2 + b^2 = c^2$

Solution

- NO if (and only if) $n \geqslant 7825$
- 2 days (in May 2016) on University of Texas' Stampede supercomputer with 800 processors
- 200 terabyte proof of unsatisfiability
- extensive media coverage (Nature, der Spiegel)

Example (Sports League Scheduling)

- round robin tournament scheduling for n teams and p periods consisting of $n-1$ rounds, satisfying several other constraints like venue restrictions
- Austrian Football Bundesliga

  12 teams play 2 periods (of 11 rounds), periods 1 and 2 are mirrored

- SAT encoding
  - variables x_{ijpr} with $v(x_{ijpr}) = \mathsf{T}$ if team i plays team j at home in round r of period p
  - constraints (fragment):

$$\bigwedge_{i,p,r} \bigvee_{j \neq i} (x_{ijpr} \vee x_{jipr}) \qquad \bigwedge_{i,p,r} \bigwedge_{j \neq i} \bigwedge_{k \neq i} (x_{ijpr} \to \neg(x_{ikpr} \vee x_{kipr})) \qquad \bigwedge_{i,j,r} (x_{ij1r} \to x_{ji2r})$$

- further details

Outline

Remark

most SAT solvers require CNF as input

Theorem

deciding satisfiability of CNF formulas is NP-complete

DIMACS Input Format

`c`	
`c comments`	
`c`	
`p cnf 4 3`	4 atoms and 3 clauses
`1 -2 4 0`	$x_1 \vee \neg x_2 \vee x_4$
`-1 2 -3 -4 0`	$\neg x_1 \vee x_2 \vee \neg x_3 \vee \neg x_4$
`3 -2 0`	$x_3 \vee \neg x_2$

Remarks

- translation from arbitrary formula to equivalent CNF is expensive
- translation to equisatisfiable CNF is possible in linear time

Definition

formulas φ and ψ are equisatisfiable $(\varphi \approx \psi)$ if

$$\varphi \text{ is satisfiable} \quad \Longleftrightarrow \quad \psi \text{ is satisfiable}$$

Examples

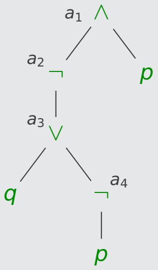
$$(p \vee q) \wedge \neg p \;\approx\; \top \qquad\qquad (p \vee q) \wedge \neg p \;\not\approx\; q \wedge \neg q$$

Example (Tseitin's Transformation)

- $\varphi = \neg(q \vee \neg p) \wedge p$
- introduce new variable for each propositional connective:

a_1	$\neg(q \vee \neg p) \wedge p$	a_3	$q \vee \neg p$
a_2	$\neg(q \vee \neg p)$	a_4	$\neg p$

- $\varphi \approx a_1 \wedge (a_1 \leftrightarrow a_2 \wedge p) \wedge (a_2 \leftrightarrow \neg a_3) \wedge (a_3 \leftrightarrow q \vee a_4) \wedge (a_4 \leftrightarrow \neg p)$



Definition

new propositional connective

- equivalence $\leftrightarrow$ $\qquad p \leftrightarrow q$ $\qquad$ "p is equivalent to q"
- $$\bar{v}(\varphi \leftrightarrow \psi) = \begin{cases} \mathrm{T} & \text{if } \bar{v}(\varphi) = \bar{v}(\psi) \\ \mathrm{F} & \text{otherwise} \end{cases}$$

Notational Convention

binding precedence $\neg \quad > \quad \wedge, \vee \quad > \quad \rightarrow, \leftrightarrow$

Lemma

$$\varphi \leftrightarrow \psi \;\equiv\; (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$$

Proof

φ	ψ	$\varphi \leftrightarrow \psi$	$(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	T	T

Lemma

1. $(\varphi \leftrightarrow \neg\psi) \equiv (\varphi \vee \psi) \wedge (\neg\varphi \vee \neg\psi)$
2. $(\varphi \leftrightarrow \psi \wedge \chi) \equiv (\neg\varphi \vee \psi) \wedge (\neg\varphi \vee \chi) \wedge (\varphi \vee \neg\psi \vee \neg\chi)$
3. $(\varphi \leftrightarrow \psi \vee \chi) \equiv (\varphi \vee \neg\psi) \wedge (\varphi \vee \neg\chi) \wedge (\neg\varphi \vee \psi \vee \chi)$

Example (cont'd)

$$
\begin{aligned}
\varphi &\approx a_1 \wedge (a_1 \leftrightarrow a_2 \wedge p) \wedge (a_2 \leftrightarrow \neg a_3) \wedge (a_3 \leftrightarrow q \vee a_4) \wedge (a_4 \leftrightarrow \neg p) \\
&\equiv a_1 \wedge (\neg a_1 \vee a_2) \wedge (\neg a_1 \vee p) \wedge (a_1 \vee \neg a_2 \vee \neg p) \wedge (a_2 \vee a_3) \wedge (\neg a_2 \vee \neg a_3) \\
&\qquad \wedge (a_3 \vee \neg q) \wedge (a_3 \vee \neg a_4) \wedge (\neg a_3 \vee q \vee a_4) \wedge (a_4 \vee p) \wedge (\neg a_4 \vee \neg p)
\end{aligned}
$$

Definition (Tseitin's Transformation)

for propositional formula φ

- atom a_φ is defined as $a_\varphi = \begin{cases} \varphi & \text{if } \varphi \text{ is atom} \\ \text{fresh atom} & \text{otherwise} \end{cases}$
- formula $\mathsf{TT}(\varphi)$ is defined as

$$\mathsf{TT}(\varphi) = \begin{cases} a_\varphi & \text{if } \varphi \text{ is atom} \\ a_\varphi \wedge \mathsf{TT}'(a_\varphi, \varphi) & \text{otherwise} \end{cases}$$

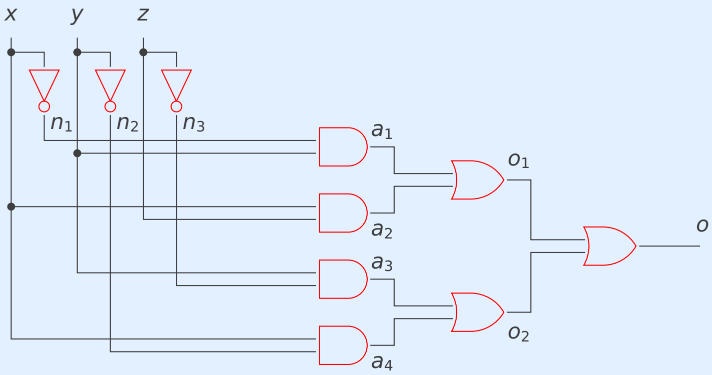
with

$$\mathsf{TT}'(a, \varphi) = \begin{cases} (a \leftrightarrow \neg a_\psi) \wedge \mathsf{TT}'(a_\psi, \psi) & \text{if } \varphi = \neg\psi \\ (a \leftrightarrow (a_{\psi_1} \wedge a_{\psi_2})) \wedge \mathsf{TT}'(a_{\psi_1}, \psi_1) \wedge \mathsf{TT}'(a_{\psi_2}, \psi_2) & \text{if } \varphi = \psi_1 \wedge \psi_2 \\ (a \leftrightarrow (a_{\psi_1} \vee a_{\psi_2})) \wedge \mathsf{TT}'(a_{\psi_1}, \psi_1) \wedge \mathsf{TT}'(a_{\psi_2}, \psi_2) & \text{if } \varphi = \psi_1 \vee \psi_2 \\ (a \leftrightarrow (a_{\psi_1} \rightarrow a_{\psi_2})) \wedge \mathsf{TT}'(a_{\psi_1}, \psi_1) \wedge \mathsf{TT}'(a_{\psi_2}, \psi_2) & \text{if } \varphi = \psi_1 \rightarrow \psi_2 \\ \top & \text{if } \varphi \text{ is atom} \end{cases}$$

Lemma

1. any satisfying valuation for φ can be (uniquely) extended to satisfying valuation for $\mathsf{TT}(\varphi)$
2. restriction of any satisfying valuation for $\mathsf{TT}(\varphi)$ to atoms in φ is satisfying valuation for φ

Logic Circuit



Equisatisfiable CNF

$$o \wedge (o \leftrightarrow o_1 \vee o_2) \wedge (o_1 \leftrightarrow a_1 \vee a_2) \wedge (o_2 \leftrightarrow a_3 \vee a_4) \wedge (a_1 \leftrightarrow n_1 \wedge y) \wedge (a_2 \leftrightarrow x \wedge z)$$
$$\wedge (a_3 \leftrightarrow y \wedge n_3) \wedge (a_4 \leftrightarrow x \wedge n_2) \wedge (n_1 \leftrightarrow \neg x) \wedge (n_2 \leftrightarrow \neg y) \wedge (n_3 \leftrightarrow \neg z)$$

Outline

Huth and Ryan

- Section 1.5

SAT

- SAT live! [accessed December 3, 2022]
- The Science of Brute Force

  Marijn J. H. Heule and Oliver Kullmann

  Communications of the ACM 60(8), pp. 70–97, 2017

  doi: 10.1145/3107239

P – NP

- Fifty Years of P vs. NP and the Possibility of the Impossible

  Lance Fortnow

  Communications of the ACM 65(1), pp. 76–85, 2022

  doi: 10.1145/3460351

Important Concepts

- DIMACS format
- equisatisfiability
- equivalence
- Horn clause
- Horn formula
- SAT
- Tseitin's transformation

homework for March 16