Discrete Mathematics: Lecture 2

- Last time
  - Chap 1.1: Propositional Logic
  - Chap 1.2: Applications of Propositional Logic
  - Chap 1.3: Propositional Equivalences
- Today
  - Finishing Chap 1.3
  - CNF and DNF
- Next time
  - Chap 1.3: Predicates and Quantifiers
  - Chap 1.4: Nested Quantifiers

Review of last time (1)

- Propositions, atomic propositions, compound propositions
- $p \to q$: it is true if p is false, p and q do not have to be related
- p if q: q is a sufficient condition for p, $q \to p$
- p only if q: q is a necessary condition for p, $p \to q$
- p unless q: p if not q, $\neg q \to p$
- The converse, contrapositive, inverse of $p \to q$
- Translating English into logic: identify atomic propositions and logical connectives

Review of last time (2)

- Satisfiability, validity, logical equivalence
- Commonly used logical equivalences
- Proving logical equivalences
  1. using truth table
  2. using existing logical equivalences

Commonly used logical equivalences

- $p \to q \equiv \neg p \vee q$
- $p \to q \equiv \neg q \to \neg p$
- $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$
- $p \leftrightarrow q \equiv p \wedge q \vee \neg p \wedge \neg q$
- $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Proving logical equivalence: Method 2

A drawback of using truth table: when there are n atoms, there are 2^n rows in the truth table

Use already-known logical equivalences and the following results

- If $A \Leftrightarrow B$ and $B \Leftrightarrow C$, then $A \Leftrightarrow C$
- Replacement theorem: If B is a subformula of A and $B \Leftrightarrow B'$, let A' be the result of replacing B in A by B', then $A \Leftrightarrow A'$

Examples:

- $\neg(p \to q) \Leftrightarrow p \land \neg q$
- $\neg(p \lor (\neg p \land q)) \Leftrightarrow \neg p \land \neg q$
- $p \land q \to p \lor q \Leftrightarrow T$

Propositional satisfiability (命题可满足性)

Are the following formulas satisfiable?

1. $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$
2. $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$
3. $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$

Applications of satisfiability

Sudoku puzzle

Given a partially filled 9×9 grid T, fill T with digits $s.t.$

- each column,
- each row,
- each of the nine 3×3 sub-grids

contains all of the digits from 1 to 9.

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

Modeling the puzzle as a satisfiability problem

$p(i, j, n)$: fill (i, j) with n

- every row contains every number
- every column contains every number
- every 3×3 sub-grid contains every number
- each cell contains at most one number

Solving satisfiability problems

- Using truth table
  1. by hand: ≤ 20 variables, $2^{20} = 1,048,576$
  2. by computer: checking 2^{1000} truth assignments requires $> 10^{12}$ years
- No computer program is known that can determine if an arbitrary formula is satisfiable in a reasonable amount of time
- Many computer programs have been developed for solving satisfiability problems which have practical use

Conjunctive normal from (CNF) and disjunctive normal form (DNF)

- A literal is an atom or its negation, *e.g.*, p, $\neg p$
- A clause is a disjunction of literals, *e.g.*, $p \vee \neg q \vee r$
- A term is a conjunction of literals, *e.g.*, $p \wedge \neg q \wedge \neg r$
- A formula is in CNF if it is a conjunction of clauses, *e.g.*, $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$
- A formula is in DNF if it is a disjunction of terms, *e.g.*, $(p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r)$

Theorem. Every formula is logically equivalent to one in CNF.

Proof method 1: We convert a formula into CNF as follows:

1. Eliminate $\leftrightarrow$ and $\rightarrow$ using $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ and $p \rightarrow q \equiv \neg p \vee q$
2. Push $\neg$ inward using $\neg(p \vee q) \equiv \neg p \wedge \neg q$ and $\neg(p \wedge q) \equiv \neg p \vee \neg q$
3. Distribute $\vee$ over $\wedge$ using $p \vee q \wedge r \equiv (p \vee q) \wedge (p \vee r)$
4. Simplify using $p \vee p \equiv p$, $p \vee \neg p \equiv T$, $p \wedge T \equiv p$

Example: $(p \rightarrow q) \leftrightarrow r$

Theorem. Every formula is logically equivalent to one in CNF.

Proof method 2: Using truth table

1. For a truth assignment τ, we use c_τ to denote the clause c s.t. $c^\tau = 0$, *e.g.*, let $\tau = 001$, then $c_\tau = p \vee q \vee \neg r$
2. c_τ has the property that τ is the unique truth assignment which makes c_τ false
3. For a formula ϕ, let ϕ' be the conjunction of all c^τ s.t. $\phi^\tau = 0$
4. Then $\phi \equiv \phi'$
5. Proof: for any τ', $(\phi')^{\tau'} = 0$ iff there is a τ s.t. $\phi^\tau = 0$ and $c_\tau^{\tau'} = 0$ iff there is a τ s.t. $\phi^\tau = 0$ and $\tau' = \tau$ iff $\phi^{\tau'} = 0$

Example: $(p \to q) \leftrightarrow r$

Theorem. Every formula is logically equivalent to one in DNF.

Proof method 1: We convert a formula into DNF as follows:

1. Eliminate $\leftrightarrow$ and $\rightarrow$ using $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ and $p \rightarrow q \equiv \neg p \vee q$
2. Push $\neg$ inward using $\neg(p \vee q) \equiv \neg p \wedge \neg q$ and $\neg(p \wedge q) \equiv \neg p \vee \neg q$
3. Distribute $\wedge$ over $\vee$ using $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
4. Simplify using $p \wedge p \equiv p$, $p \wedge \neg p \equiv F$, $p \vee F \equiv p$

Example: $(p \rightarrow q) \leftrightarrow r$

Theorem. Every formula is logically equivalent to one in DNF.

Proof method 2: Using truth table

1. For a truth assignment τ, we use t_τ to denote the term t s.t. $t^\tau = 1$, *e.g.*, let $\tau = 001$, then $t_\tau = \neg p \wedge \neg q \wedge r$
2. t_τ has the property that τ is the unique truth assignment which makes t_τ true
3. For a formula ϕ, let ϕ' be the disjunction of all t^τ s.t. $\phi^\tau = 1$
4. Then $\phi \equiv \phi'$
5. Proof: for any τ', $(\phi')^{\tau'} = 1$ iff there is a τ s.t. $\phi^\tau = 1$ and $t_\tau^{\tau'} = 1$ iff there is a τ s.t. $\phi^\tau = 1$ and $\tau' = \tau$ iff $\phi^{\tau'} = 1$

Example: $(p \to q) \leftrightarrow r$