| | |
|---|---|
| **CS280, Spring 2001** | **Handout 12** |
| **February 16, 2001** | |

1. Reading: K. Rosen *Discrete Mathematics and Its Applications*, 3.1
2. The main message of this lecture:

**Finding a proof is a kind of art which can be taught but cannot be completely automated. On the other hand, proof checking is an efficient algorithmic procedure.**

Proof is a systematic method of deriving new facts from given assumptions called **axioms**. There are usually two different sorts of axioms:

**logical axioms** that hold in each proof systems independently of its specifics,

**proper axioms** reflecting specifics of the underlying mathematical structure.

Examples. Logical axioms: $\neg\neg A \rightarrow A$, $\neg\forall x A(x) \rightarrow \exists x \neg A(x)$, etc. Proper axioms for integers): $x + y = y + x$, $x(y + z) = x \cdot y + x \cdot z$, etc. Those axioms are true, but not universally true, since not every operation is commutative, not every two operations are distributive, etc.

**Hypotheses:** assumptions made for a particular theorem (e.g. "Let $p, q$ be relatively prime integers ...). **Theorems, Lemmas, Corollaries:** conclusions made as the result of a proof. **Rules of Inference:** correct methods of reasoning. We suggest the notation: $H_1, H_2, \ldots, H_n \vdash T$ for the rule that allows us to conclude $T$ given hypotheses $H_1, H_2, \ldots, H_n$.

In a propositional logic (when no quantifiers are involved) there is test on what method of reasoning is correct: for every correct rule of inference there is a corresponding tautology.

**Theorem 12.1.** (Deduction Theorem) *In a propositional logic a sentence $T$ is provable from hypotheses $H_1, H_2, \ldots, H_n$ if and only if $H_1 \wedge H_2 \wedge \ldots \wedge H_n) \rightarrow T$ is a tautology.*

The proof of this theorem can be found in any logic textbook. Here is a table of some common rules of inference and the corresponding tautologies. For some of them we give two essentially equivalent formulations: one in the form $(X \wedge Y) \rightarrow Z$ and the other in the form $X \rightarrow (Y \rightarrow Z)$.

| **Rule of inference** | **Tautology** | **Name** |
|---|---|---|
| $p \vdash p \vee q$ | $p \rightarrow (p \vee q)$ | Addition |
| $p \wedge q \vdash p$ | $(p \wedge q) \rightarrow p$ | Simplification |
| $p, q \vdash p \wedge q$ | $p \rightarrow (q \rightarrow (p \wedge q))$ | Conjunction |
| $p, p \rightarrow q \vdash q$ | $p \rightarrow ((p \rightarrow q) \rightarrow q)$ | Modus ponens |
| | $(p \wedge (p \rightarrow q)) \rightarrow q$ | |
| $\neg q, p \rightarrow q \vdash \neg p$ | $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ | Modus tollens |
| $p \rightarrow q \vdash \neg q \rightarrow \neg p$ | $(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$ | Contraposition |
| $p \rightarrow q, q \rightarrow r \vdash p \rightarrow r$ | $(p \rightarrow q) \rightarrow ((q \rightarrow r) \rightarrow (p \rightarrow r))$ | Hypothetical syllogism |
| | $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ | |
| $p \vee q, \neg p \vdash q$ | $(p \vee q) \rightarrow (\neg p \rightarrow q)$ | Disjunctive syllogism |
| | $((p \vee q) \wedge \neg p) \rightarrow q)$ | |

**Definition 12.2.** **A proof** is a finite sequence of sentences each of which is either a logical axiom (tautology) or a hypothesis or follows from the previous ones in this sequence by a correct inference rule.

**Example 12.3.** A proof from hypotheses. Let $p$:= *You send me email message*, $q$:= *I will finish writing a program*, $r$:=*I will go to sleep early*, $s$:=*I will wake up feeling refreshed*. Hypotheses: $p \to q$, $\neg p \to r$, $r \to s$, $\neg s$. The goal: $q$. The argument (which is not unique, of course):

| | |
|---|---|
| 1. $p \to q$ | Hypothesis |
| 2. $\neg q \to \neg p$ | Contrapositive of 1 |
| 3. $\neg p \to r$ | Hypothesis |
| 4. $\neg q \to r$ | Hypothetical syllogism, from 2,3 |
| 5. $\neg r \to s$ | Hypothesis |
| 6. $\neg q \to s$ | Hypothetical syllogism, from 4,5 |
| 7. $\neg s$ | Hypothesis |
| 8. $\neg\neg q$ | Modus tollens, from 6,7 |
| 9. $\neg\neg q \to q$ | Logical axiom |
| 10. $q$ | Modus ponens, from 8,9. |

**Fallacy** is an incorrect rule of inference. Example: $p \to q, q \vdash p$ (fallacy of affirming the conclusion). This "rule" is represented by a proposition $((p \to q) \wedge q) \to p$ (or, equivalently, $(p \to q) \to (q \to p)$), which is NOT a tautology: make $p$ true, $q$ false and use the truth tables.

Another common fallacy is a **circular reasoning** (or **begging the question**), when a statement is proved using itself. It is clear that such a "reasoning" does not satisfy the definition of a proof 12.2, since the first occurrence of that statement in a proof sequence is not justified.

Some inference rules involving quantifiers.

| **Rule of inference** | **Name** |
|---|---|
| $\forall x P(x) \vdash P(c)$ | Universal instantiation |
| $P(a)$ *for arbitrary* $a \vdash \forall x P(x)$ | Universal generalization |
| $P(c) \vdash \exists x P(x)$ | Existential generalization |

A comment concerning the rule of universal generalization. The words "for arbitrary $a$" mean that we cannot conclude "For all integers $n$ the property $A(n)$ holds" from, say $A(3)$, or even from $A(0), A(1), \dots, A(100)$. What is needed is a general argument saying "Let $n$ be an arbitrary integer. Then ..., and thus $A(n)$." In other words, if we derived $A(n)$ *without making any specific assumptions concerning* $n$, then we are entitled to conclude $\forall n A(n)$.

Example on universal instantiation: *Twiggy*. Here is a correct reasoning: birds can fly, Twiggy is a bird, then Twiggy can fly. To formalize this reasoning assume $B(x) \sim$ *x is a bird*, $F(x) \sim$ *x can fly*, $t$ is Twiggy. Then

| | |
|---|---|
| 1. $\forall x(B(x) \to F(x))$ | Hypothesis |
| 2. $B(t) \to F(t)$ | by universal instantiation from 1 |
| 3. $B(t)$ | Hypothesis |
| 4. $F(t)$ | By modus ponens from 2,3 |

Example on universal generalization: *For all integers* $n$ $6|(n^3 - n)$. Proof: let $n$ be an arbitrary integer. Then $n^3 - n = n(n^2 - 1) = (n-1)n(n+1)$, i.e. $n^3 - n$ is a product of three consecutive integers one of which then is a multiple of 3 and at least one is a multiple of 2. Therefore $3|(n^3 - n)$ and $2|(n^3 - n)$, hence $6|(n^3 - n)$.

Example on existential generalization: *There exists an odd integer which is not a prime.* Proof. Take $c = 9$ which is clearly odd, and not prime. Therefore, there exists an integer which is both odd and not prime.

**Homework assignments.** (due Friday 02/23).

12A:Rosen3.1-2ade; 12B:Rosen3.1-10acd; 12C:Rosen3.1-12; 12D:Rosen3.1-26