CS109A Notes for Lecture 1/12/96

The Essence of Proof

Mathematical proof is essentially persuasive prose.

- Like an essay, it is effective if it convinces the listener.
- Also like an essay, we can learn certain rhetorical tricks, e.g. "proof by induction" or "use of the contrapositive."

Two Parts of a Proof

Some parts of a proof involve logical manipulation, regardless of what our statements mean.

Example: *Modus Ponens* is the rule that says "if you know p and you know $p \rightarrow q$, then you may conclude q.

- This rule does not depend on what p and q "mean."

Other parts of a proof depend on the meaning of propositional variables or predicates.

Example:

$$(\forall X)\big(greenElephant(X) \rightarrow wearsBoxers(X)\big)$$

is true (vacuously!) because we can argue that there are no green elephants.

- The general statement $(\forall X)\big(p(X) \rightarrow q(X)\big)$ is not a theorem.

Succinct Notation

- `AND` replaced by concatenation (no operator, like multiplication).
- `OR` replaced by $+$.
- `NOT` replaced by $\neg$.
- `TRUE` and `FALSE` replaced by 0 and 1.

Truth Tables

The *truth table* for an expression has one row for each combination of truth-values for its variables, i.e., 2^n rows if there are n variables.

- Assignment of `TRUE` or `FALSE` to each variable of the expression is a *truth assignment*.

The value in each row is the value of the expression for that truth assignment.

- Often, we evaluate an expression "bottom-up," with a column for each subexpression.
  - □ Apply an operator to two columns by applying the operator row-wise.

Example: $(p \rightarrow q) \equiv (\neg q \rightarrow \neg p)$.

- The *contrapositive law*.

p	q	$p \rightarrow q$	$\neg p$	$\neg q$	$\neg\, q \rightarrow \neg\, p$	whole
0	0	1	1	1	1	1
0	1	1	1	0	1	1
1	0	0	0	1	0	1
1	1	1	0	0	1	1

Algebraic Laws (Tautologies)

1. *Commutative laws*: $(p + q) \equiv (q + p)$ and $pq \equiv qp$.

2. *Associative laws*: $(p+q)+r \equiv p+(q+r)$ and $(pq)r \equiv p(qr)$.

3. *Distributive laws*: $p(q + r) \equiv pq + pr$ and $p + qr \equiv (p + q)(p + r)$.
   - □ That last one is a surprise; the other laws so far make `AND` and `OR` look just like times and plus.

4. *Idempotence laws*: $pp \equiv p$ and $p + p \equiv p$.

5. *DeMorgan's laws*: $\neg(pq) \equiv \neg p + \neg q$ and $\neg(p + q) \equiv (\neg p)(\neg q)$.

- □ Generalizes to any number of variables: the negation of any product is the sum of the negations, and the negation of any sum is the product of the negations.

- □ Also generalizes to the "infinite case" involving quantifiers: $\neg\big((\forall X)e(X)\big) \equiv (\exists X)\big(\neg e(X)\big)$ and $\neg\big((\exists X)e(X)\big) \equiv (\forall X)\big(\neg e(X)\big)$.

Example: $\neg(pq + r) \equiv \big(\neg(pq)\big)(\neg r) \equiv (\neg p + \neg q)(\neg r)$.

6. *Double negation*: $\neg(\neg p) \equiv p$.

Laws Useful in Designing Proofs

7. *Contrapositive law*: $(p \to q) \equiv (\neg q \to \neg p)$.

   - □ To prove an implication, prove the reverse implication of the negations.

Example: Consider "if X is not divisible by 4, then either X is odd or $X = 2Y$ and Y is odd."

- Use propositions:
  - □ p: "X is divisible by 4."
  - □ q: "X is odd."
  - □ r: "X is twice an odd number."
- Statement is: $\neg p \to q + r$.
- Contrapositive: $(\neg q)(\neg r) \to p$.
- Argument:
  - □ $\neg q$ says "X is even," i.e., $X = 2A$ for some A.
  - □ $\neg r$ says X is not twice any odd number. Since X is twice A, A is not odd. Thus, $A = 2B$ for some B.
  - □ Thus, $X = 4B$, which is statement p: "X is divisible by 4."

8. *Proof by contradiction*: $p \equiv (\neg p) \to 0$.

- □ Prove a statement by showing that its negation implies **`FALSE`**, i.e., a contradiction such as $q(\neg q)$.

9. *Modus ponens*: $\big(p(p \to q)\big) \to q$.
   - □ One way to prove a statement q is to prove some statement p and also show that p implies q.

10. *Transitivity of implication*: $\big((p \to q)(q \to r)\big) \to (p \to r)$.
    - □ To prove p implies r, find some intermediate q; show $p \to q$ and $q \to r$.
    - □ Likewise $\equiv$: $\big((p \equiv q)(q \equiv r)\big) \to (p \equiv r)$

11. *Replacing implications*: $(p \to q) \equiv (\neg p + q)$.
    - □ Because we can often manipulate **`AND`** and **`OR`** by the familiar rules for times and plus, it is often easier to replace implications this way.
    - □ Similarly, $(p \equiv q) \equiv \big(pq + (\neg p)(\neg q)\big)$.

12. *Case analysis*: $\big((p \to q)(\neg p \to q)\big) \to q$.
    - □ If q follows from both p and $\neg p$, then q must be true.
    - □ More generally, if q follows from each of $p_1, p_2, \ldots, p_n$, and at least one of the p_i's must be true, then we may conclude q.

Example: Consider

- p: "X is divisible by 4."
- q: "X is odd."
- r: "X is twice an odd number."

We want to prove $\neg p \to q + r$, or equivalently using (11): $p + q + r$.

- Consider 4 cases, depending on whether the remainder of $X/4$ is 0, 1, 2, or 3.
  - □ Surely at least one (in fact, exactly one) of these cases is true for any integer X.

0: Then p is true. Since $p \rightarrow p + q + r$ is a tautology, we may use modus ponens to conclude from that and p that $p + q + r$.

1: Then q is true. Since $q \rightarrow p + q + r$ is also a tautology, we can conclude $p+q+r$ by modus ponens.

2: Then $X/2$ is odd, so r is true. $r \rightarrow p + q + r$ is a tautology, so we conclude $p + q + r$ by modus ponens.

3: Like case 1.

Substitution Principle

You may substitute for any or all propositional variables in a tautology.

- □ Even expressions involving predicate logic may be substituted.

Example: $p + \neg p$ is a tautology. Substitute $s(X, Y) + s(Y, X)$ for p. It follows that

$$s(X, Y) + s(Y, X) + \Big(\neg\big(s(X, Y) + s(Y, X)\big)\Big)$$

is a tautology.

Substitution of Equals for Equals

Take any expression E, find some subexpression F, substitute for F an equivalent expression, and the resulting expression will be equivalent to E.

Example: A substituted instance of DeMorgan's law says $\neg\big(s(X, Y) + s(Y, X)\big) \equiv \Big(\big(\neg s(X, Y)\big)\big(\neg s(Y, X)\big)\Big)$. Substitute the right side for the left in previous example to conclude $s(X, Y)+s(Y, X)+\big(\neg s(X, Y)\big)\big(\neg s(Y, X)\big)$ is a tautology.