CS109B Notes for Lecture 5/17/95

How to Prove Things

1. Truth tables — check it out; it takes $O(2^n)$ time on an expression with n variables, but if n is small this is fine.

   □ Compare with Venn diagrams as a way to prove equivalences of set-expressions.

2. Manipulate equivalences using:

   a) Substitution into a tautology.

   b) Substitution of equals for equals.

   c) Transitive and commutative laws for equivalence.

   □ Compare with "trigonometric identities" from High School.

3. *Deduction*: "proofs" in the sense of High-School geometry, the main topic of this lecture.

Deduction

Proofs constructed as a sequence of logical expressions according to the following rules:

1. Certain expressions $E_1, E_2, \ldots, E_k$, called the *hypotheses* are given.

   □ These are the "givens" in High-School geometry.

2. There is another expression E that is the desired *conclusion.*

3. We write a sequence of *lines of the proof* (logical expressions) $G_1, G_2, \ldots, G_n$ such that

   a) G_n is the desired conclusion E, and

   b) Each G_i is either a hypothesis or follows from some previous lines by a *rule of inference.*

4. The conclusion is $E_1E_2 \cdots E_k \rightarrow E$.

□ Note we do not prove E itself, which may well not be a tautology. We prove that the hypotheses imply E.

Rules of Inference

Any rule may be used, as long as whenever it lets us write line F on the grounds that there are previous lines $F_1, F_2, \ldots, F_m$, then $F_1 F_2 \cdots F_m \rightarrow F$ is a tautology.

We'll use the following rules:

a) Any tautology may be written as a line.

b) *Modus Ponens* (Latin for "logic is the most boring subject I have ever seen"). If E and $E \rightarrow F$ are lines, we may write F as a line.

c) *And-Rule.* If E and F are lines, $E\,\mathtt{AND}\,F$ may be written as a line.

d) *Equivalence Rule.* If E and $E \equiv F$ are lines, F may be written as a line.

Example: Hypotheses: $p \rightarrow q$ and $p \rightarrow r$; conclusion $p \rightarrow qr$.

1)	$p \rightarrow q$	Hypothesis
2)	$(p \rightarrow q) \equiv (\bar{p} + q)$	Law 12.24(a)
3)	$\bar{p} + q$	(d) with (1) and (2)
4)	$p \rightarrow r$	Hypothesis
5)	$(p \rightarrow r) \equiv (\bar{p} + r)$	Law 12.24(a)
6)	$\bar{p} + r$	(d) with (4) and (5)
7)	$(\bar{p} + q)(\bar{p} + r)$	(c) with (3) and (6)
8)	$(\bar{p} + q)(\bar{p} + r) \equiv (\bar{p} + qr)$	Law 12.14
9)	$\bar{p} + qr$	(d) with (7) and (8)
10)	$(\bar{p} + qr) \equiv (p \rightarrow qr)$	Law 12.24(a)
11)	$p \rightarrow qr$	(d) with (9) and (10)

Why Deductive Proofs?

OK, I admit it. This sort of stuff is mind-boggling, and the chances of coming up with the right sequence of steps to yield a proof is slim to none.

- But computers are good at this endless search for the right sequence. Even today, they are of some assistance in proving "theorems" that imply a piece of code or a digital hardware design is correct.

- More importantly, the search doesn't have to be quite as mindless as above.
  - □ "Resolution," the subject of the next lecture, "homes in" on proofs in an uncanny way.
  - □ Yet we should remember that testing tautologies is inherently intractable, and *no method whatsoever* can be less than exponential on "typical" instances.

But Isn't Deduction Trivial Anyway?

Given Hypotheses $E_1, E_2, \ldots, E_k$ and a valid conclusion E such that $E_1 E_2 \cdots E_k \to E$ is a tautology, we can in principle proceed as follows:

1. Write lines $E_1, E_2, \ldots, E_k$.
2. Write $E_1 E_2 \cdots E_k$ as a line, using the and-rule (c).
3. Write as a line the tautology $E_1 E_2 \cdots E_k \to E$.
4. Write line E, using Modus Ponens (b) with (2) and (3).

Why isn't life as simple as this?

- First, the tautology (3) might involve some huge number of variables n and take time $O(2^n)$ to check — we never finish justifying line (3).
- Perhaps more importantly, there are more complex forms of logic than propositional logic, such as predicate logic from Ch. 14.
  - □ These logics do not have a mechanical way, like truth tables, to check all tautologies.

Why Deduction Works

If $E_1, E_2, \ldots, E_k$ are the hypotheses, and $F_1, F_2, \ldots, F_n$ is a proof, we prove by complete induction on i that $E_1E_2\cdots E_k \rightarrow F_i$ is a tautology.

- The hard part is when F_i follows from previous F's by a rule of inference.

Example: If F_i follows from previous lines G and $G \rightarrow F_i$ by Modus Ponens, then we have, by the inductive hypothesis that

1. $E_1E_2\cdots E_k \rightarrow G$ and
2. $E_1E_2\cdots E_k \rightarrow (G \rightarrow F_i)$.

are tautologies. We must show:

3. $E_1E_2\cdots E_k \rightarrow F_i$ is a tautology.

- Suppose not; that is, there is some truth-assignment α that makes (3) false.
  - □ Then α must make $E_1E_2\cdots E_k$ true and F_i false.
- Case 1: α makes G false. Then α makes (1) false, contradicting the inductive hypothesis.
- Case 2: α makes G true. Then since α makes F_i false, it makes $G \rightarrow F_i$ false and thus makes (2) false. Again the inductive hypothesis is contradicted.
- We conclude that no such α exists; i.e., (3) is a tautology.