CE 474 - LOGIC OF COMPUTER SCIENCE

Lecture Note 5

1. Why Proof Techniques Matter

In programming, systems design, and AI, proofs guarantee correctness. For example:

- Ensuring a sorting algorithm truly sorts.
- Verifying an authentication protocol is secure.
- Proving a compiler transformation preserves semantics.

Proofs are your guarantee of trust in systems.

2. Learning Objectives

By the end of this lecture, you should be able to:

- Distinguish and apply direct proof, proof by contrapositive, and proof by contradiction.
- Plan proofs effectively by breaking complex statements into sub-goals.
- Identify which proof technique is most suitable for a given theorem.

3. Direct Proof vs. Contrapositive

Direct Proof

Goal: Prove an implication $P \to Q$.
Method:

1. Assume P is true.
2. Use definitions, algebra, and earlier results to derive Q.

Example: Prove: If n is even, then $n + 1$ is odd.
Assume n is even: $n = 2k$ for some integer k. Then $n + 1 = 2k + 1$, which is odd.

Proof by Contrapositive

Key: $P \to Q$ is logically equivalent to $\neg Q \to \neg P$.
When to use: If assuming $\neg Q$ simplifies the argument.
Method:

1. Assume $\neg Q$.
2. Show $\neg P$ follows.

Example: Prove: If n^2 is even, then n is even.
Contrapositive: If n is odd, then n^2 is odd.
Assume n is odd: $n = 2k + 1$. Then

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

which is odd.

4. Proof by Contradiction

Goal: Prove P is true by showing $\neg P$ leads to a contradiction.
Method:

1. Assume $\neg P$.
2. Derive a contradiction.
3. Conclude $\neg P$ is false, so P is true.

Classic Example: $\sqrt{2}$ is irrational.
Assume $\sqrt{2} = a/b$ in lowest terms. Then $2 = a^2/b^2 \Rightarrow a^2 = 2b^2$, so a is even. Let $a = 2k$. Then $b^2 = 2k^2$, so b is even. Both a and b even contradicts "lowest terms."

5. Proof Planning Strategy

1. **Understand the Statement:** Identify the goal and givens.
2. **Choose a Technique:**
   - Direct if forward implication is straightforward.
   - Contrapositive if assuming $\neg Q$ simplifies proof.
   - Contradiction for existential/negative statements or blocked direct paths.
3. **Break into Sub-goals:** For compound statements (e.g., $P \wedge Q$), prove each part.
4. **Work Backwards:** Ask "what would I need to prove Q?"
5. **Outline First:** Draft key steps before writing formally.

6. Example Theorem

Theorem: If n^2 is even, then n is even.
Proof (Contrapositive).

1. Prove equivalent: If n is odd, then n^2 is odd.
2. Assume $n = 2k + 1$.
3. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd.
4. Therefore, if n^2 is even, n is even.

7. In-Class Strategy Workshop

Activity: Work in groups on one statement:

1. The sum of two odd integers is even.
2. Every factor of a prime number is either 1 or the prime itself.
3. If $a|bc$ and $gcd(a, b) = 1$, then $a|c$.

Tasks:

1. Decide which proof technique fits best.
2. Outline proof in 5–7 bullet steps.
3. Present strategy to class.

8. Summary Key Takeaways

- Different techniques suit different statements.
- Direct proofs follow forward logic.
- Contrapositive flips direction for easier assumptions.
- Contradiction assumes negation to reach inconsistency.
- Effective proofs begin with planning and outlining.

References

- Rosen, K. H. (2011). Discrete Mathematics and Its Applications.
- Huth, M. Ryan, M. (2004). Logic in Computer Science: Modelling and Reasoning about Systems.
- Halmos, P. R. (1960). Naive Set Theory.