Chapter 3

Proving methods

Discrete Structures for Computing

Huynh Tuong Nguyen, Tran Tuan Anh, Nguyen Ngoc Le
Faculty of Computer Science and Engineering
University of Technology - VNUHCM
{htnguyen;trtanh}@hcmut.edu.vn

Contents

Course outcomes

	Course learning outcomes
L.O.1	Understanding of logic and discrete structures
	L.O.1.1 – Describe definition of propositional and predicate logic L.O.1.2 – Define basic discrete structures: set, mapping, graphs
L.O.2	Represent and model practical problems with discrete structures
	L.O.2.1 – Logically describe some problems arising in Computing L.O.2.2 – Use proving methods: direct, contrapositive, induction L.O.2.3 – Explain problem modeling using discrete structures
L.O.3	Understanding of basic probability and random variables
	L.O.3.1 – Define basic probability theory L.O.3.2 – Explain discrete random variables
L.O.4	Compute quantities of discrete structures and probabilities
	L.O.4.1 – Operate (compute/ optimize) on discrete structures L.O.4.2 – Compute probabilities of various events, conditional ones, Bayes theorem

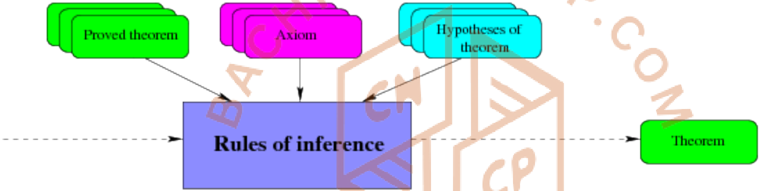
Introduction

Definition

A proof is a sequence of logical deductions from
- axioms, and
- previously proved theorems

that concludes with a new theorem.

Terminology



- **Theorem** (*định lý*) = a statement that can be shown to be true
- **Axiom** (*tiên đề*) = a statement we assume to be true
- **Hypothesis** (*giả thiết*) = the premises of the theorem

- **Lemma** (*bổ đề*) = less important theorem that is helpful in the proofs of other results
- **Corollary** (*hệ quả*) = a theorem that can be established directly from a proved theorem
- **Conjecture** (*phỏng đoán*) = statement being proposed to be true, when it is proved, it becomes theorem

Proving a Theorem

Many theorem has the form $\forall x P(x) \to Q(x)$

Goal:

- Show that $P(c) \to Q(c)$ is true with arbitrary c of the domain
- Apply universal generalization

$\Rightarrow$ How to show that conditional statement $p \to q$ is true.

Methods of Proof

- Direct proofs (*chứng minh trực tiếp*)
- Proof by contraposition (*chứng minh phản đảo*)
- Proof by contradiction (*chứng minh phản chứng*)
- Mathematical induction (*quy nạp toán học*)

Direct Proofs

Definition

A direct proof shows that $p \to q$ is true by showing that if p is true, then q must also be true.

Example

Ex.: If n is an odd integer, then n^2 is odd.

Pr.: Assume that n is odd. By the definition, $n = 2k + 1$, $k \in \mathbb{Z}$. $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is an odd number.

Proof by Contraposition

Definition

$p \to q$ can be proved by showing (directly) that its contrapositive, $\neg q \to \neg p$, is true.

Example

Ex.: Given an integer n, show that if $3n + 2$ is odd, then n is odd.

Pr.: Assume that "n is even", so $n = 2k$, $k \in \mathbb{Z}$. Substituting $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$ is even. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, *Q.E.D.*

Proofs by Contradiction

Definition

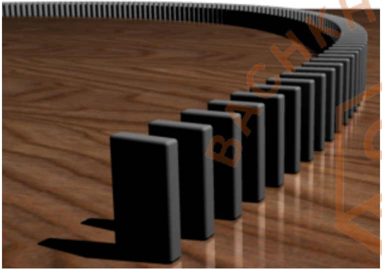
p is true if if can show that $\neg p \to (r \wedge \neg r)$ is true for some proposition r.

Example

Ex.: Prove that $\sqrt{2}$ is irrational.

Pr.: Let p is the proposition "$\sqrt{2}$ is irrational". Suppose $\neg p$ is true, which means $\sqrt{2}$ is rational. If so, $\exists a, b \in \mathbb{Z}, \sqrt{2} = a/b$, a, b have no common factors. Squared, $2 = a^2/b^2$, $2b^2 = a^2$, so a^2 is even, and a is even, too. Because of that $a = 2c, c \in \mathbb{Z}$. Thus, $2b^2 = 4c^2$, or $b^2 = 2c^2$, which means b^2 is even and so is b. That means 2 divides both a and b, contradict with the assumption.

Problem



Assume that we have an infinite domino string, we want to know whether every dominoes will fall, if we only know two things:

1. We can push the first domino to fall
2. If a domino falls, the next one will be fall

We can! Mathematical induction.

Mathematical Induction

Huynh Tuong Nguyen, Tran Tuan Anh, Nguyen Ngoc Le

Definition (Induction)

To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

- **Basis Step**: Verify that $P(1)$ is true.
- **Inductive Step**: Show that the conditional statement $P(k) \to P(k+1)$ is true for all positive integers k

Logic form:

$[P(1) \land \forall k P(k) \to P(k+1))] \to \forall n P(n)$

What is $P(n)$ in domino string case?

Example on Induction

Huynh Tuong Nguyen, Tran Tuan Anh, Nguyen Ngoc Le

Example

Show that if n is a positive integer, then

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Solution

Let $P(n)$ be the proposition that sum of first n is $n(n+1)/2$

- Basis Step: $P(1)$ is true, because $1 = \frac{1(1+1)}{2}$
- Inductive Step:
  Assume that $1 + 2 + \ldots + k = \frac{k(k+1)}{2}$.
  Then:

$$\begin{aligned} 1 + 2 + \ldots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

shows that $P(k+1)$ is true under the assumption that $P(k)$ is true.

Example on Induction

Huynh Tuong Nguyen, Tran Tuan Anh, Nguyen Ngoc Le

Example

Prove that $n < 2^n$ for all positive integers n.

Solution

Let $P(n)$ be the proposition that $n < 2^n$.

- Basis Step: $P(1)$ is true, because $1 < 2^1 = 2$
- Inductive Step:
  Assume that $P(k)$ is true for the positive k, that is, $k < 2^k$.
  Add 1 to both side of $k < 2^k$, note that $1 \leq 2^k$.

$$k + 1 < 2^k + 1 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}.$$

  shows that $P(k+1)$ is true, namely, that $k + 1 < 2^{k+1}$, based on the assumption that $P(k)$ is true.

Exercise

Huynh Tuong Nguyen, Tran Tuan Anh, Nguyen Ngoc Le

Hãy chứng minh rằng nếu n là số nguyên dương và $7n + 9$ là số chẵn thì n là số lẻ bằng cách:

1. Chứng minh trực tiếp.
2. Chứng minh gián tiếp (phản đảo).
3. Chứng minh phản chứng.

Exercise

Chứng minh trực tiếp

Giả sử: $7n + 9$ là số chẵn. Do đó, $7n + 9 = 2k, (k \in \mathbb{Z})$
Ta suy ra: $n = 2k - 6n - 9 = 2k - 6n - 10 + 1 = 2(k - 3n - 5) + 1$
Nghĩa là n là số lẻ. Vậy suy ra đpcm.

Chứng minh gián tiếp (phản đảo)

Để chứng minh phát biểu trên là đúng. Ta viết phát biểu này dưới dạng phép kéo theo $p \to q$ với $p = 7n + 9$ là số chẵn và $q = n$ là số lẻ.
Đảo đề của nó là "Nếu n không là số lẻ thì $7n + 9$ không là số chẵn". Và ta có thể chứng minh phát biểu này đúng như sau:
Nếu n không là số lẽ, nghĩa là n chia hết cho 2. Do đó, $n = 2k, (k \in \mathbb{Z})$
Ta suy ra: $7n + 9 = 7(2k) + 9 = 14k + 9 = 2(7k + 4) + 1$
Nghĩa là: $7n + 9$ không là số chẵn. Vì mệnh đề phản đảo là đúng nên do chứng minh đảo đề, ta suy ra $p \to q$ cũng đúng.

Chứng minh phản chứng

Giả sử $7n + 9$ là số chẵn và n không là số lẻ tức là n là số chẵn.
Bởi vì n là số chẵn. Do đó, $n = 2k, (k \in \mathbb{Z})$
Ta suy ra: $7n + 9 = 7(2k) + 9 = 14k + 9 = 2(7k + 4) + 1$
Nghĩa là: $7n + 9$ là số lẻ. Ta có thể chỉ ra rằng nếu n là số chẵn thì $7n + 9$ là số lẻ. Điều này mâu thuẫn với giả thuyết $7n + 9$ là số chẵn. Vậy suy ra đpcm.

Exercise

Huynh Tuong Nguyen, Tran Tuan Anh, Nguyen Ngoc Le

Kiểu chứng minh nào đã được sử dụng trong chứng minh bên dưới đây

Để chứng minh *"Nếu m và n là những số nguyên và mn là chẵn, thì hoặc là m chẵn, hoặc là n chẵn"*, người ta suy diễn như sau: Giả sử m và n là số lẻ. Khi đó có thể biểu diễn $m = 2k + 1$ và $n = 2l + 1$. Như vậy tích $mn = (2k + 1)(2l + 1) = 2(2kl + k + l) + 1$ là số lẻ. Sai giả thiết. Kết luận, hoặc là m chẵn, hoặc là n chẵn.

- A) Chứng minh trực tiếp (*direct proof*)
- B) Chứng minh phản chứng (*contradiction proof*) hoặc phản đảo (*contra-positive proof*)
- C) Chứng minh quy nạp (*inductive proof*)
- D) Các chọn lựa khác đều sai

Huynh Tuong Nguyen, Tran Tuan Anh, Nguyen Ngoc Le

Điều gì sai trong chuỗi lý luận dưới đây rằng tất cả các bông hoa đều có cùng một màu?

1. Đặt $P(n)$ là một mệnh đề rằng tất cả các bông hoa trong một tập n bông đều có cùng màu.
2. Ta thấy rõ ràng, $P(1)$ luôn đúng.
3. Nếu giả sử $P(n)$ đúng. Nghĩa là, giả sử rằng tất cả các bông hoa trong một tập n bông hoa bất kỳ đều có cùng màu sắc.
4. Xét một tập bất kỳ $n+1$ bông; được đánh số lần lượt là $1, 2, 3, \ldots, n, (n+1)$.
5. Dựa theo giả định trên, chuỗi n bông hoa đầu tiên của những bông hoa này có cùng màu, và chuỗi n bông hoa sau cũng sẽ có cùng một màu.
6. Do hai tập hợp bông hoa này có sự giao thoa $n-1$ bông, nên tất cả $n+1$ bông hoa này phải cùng một màu.
7. Điều này chứng minh rằng $P(n+1)$ là đúng và được chứng minh bằng phương pháp qui nạp.

Xét một tập con D ($\mathcal{N} \times N$) được định nghĩa đệ quy như sau:

- i) $(n, 0) \in D$.
- ii) nếu $(n, m) \in D$, thì $(n, n + m) \in D$.

Hãy

1) xác định vài phần tử của D.
2) chứng minh bằng phép quy nạp trên k rằng 'nếu $m = k.n$ thì '$(n, m) \in D$'.
3) chứng minh rằng nếu $(n, m) \in D$, thì chúng ta sẽ có $m = kn$ với $k \in \mathcal{N}$.

a) Chứng minh rằng $\forall n \in \mathcal{N}^+$
$(n+1)^2 - (n+2)^2 - (n+3)^2 + (n+4)^2 = 4.$

b) Từ đó suy ra rằng với mọi số tự nhiên m, tồn tại n nguyên dương để có thể viết m dưới dạng tổng bình phương của 1^2, 2^2, ..., n^2, nghĩa là: $\forall m \in \mathcal{N}^+$, $\exists n \in \mathcal{N}^+$, $\exists \varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$, $m = \varepsilon_1 1^2 + \varepsilon_2 2^2 + \ldots + \varepsilon_n n^2$.
(**Gợi ý**: thử biểu diễn các giá trị $m \in \{1, 2, 3, 4, 5, 6\}$)

Huynh Tuong Nguyen, Tran Tuan Anh, Nguyen Ngoc Le

Hãy chứng minh các đẳng thức sau bằng cách sử dụng phương pháp chứng minh quy nạp:

1. $1.2 + 2.5 + 3.8 + \ldots + n.(3n-1) = n^2(n+1), n \geq 1$
2. $1 + \frac{1}{1+2} + \frac{1}{1+2+3} + \ldots + \frac{1}{1+2+3+\ldots+n} = \frac{2n}{n+1}, n \geq 1$
3. $\sum_{i=1}^{n} 2^{i-1} = 2^n - 1$
4. Chứng minh $\log_5(2)$ là số vô tỷ.

Exercise

Hãy sử dụng phương pháp chứng minh quy nạp để chứng minh:

1. Chứng minh rằng với mọi số nguyên $n \geq 1$, $3^{2n-1} + 1$ chia hết cho 4.
2. Chứng minh rằng với mọi số nguyên $n \geq 1$, $6^n - 1$ đều chia hết cho 5.
3. Chứng minh rằng với mọi số nguyên $n \geq 1$, $5^{2n-1} + 1$ đều chia hết cho 6.
4. Chứng minh rằng với mọi số nguyên $n \geq 1$, $8^n - 1$ đều chia hết cho 7.
5. Chứng minh rằng với mọi số nguyên $n \geq 1$, $4^n + 15n - 1$ đều chia hết cho 9.

Hãy chứng minh các bất đẳng thức sau bằng cách sử dụng phương pháp chứng minh quy nạp:

1. Chứng minh rằng với mọi số nguyên $n \geq 1$, $3^n > n^2$.
2. Chứng minh rằng với mọi số nguyên $n \geq 4$, $n! > 2^n$.

Chứng minh rằng số lượng đường chéo trong một đa giác lồi với n đỉnh là $\frac{1}{2}n(n-3)$, với $n \geq 4$