Discrete Mathematics

Lecture 4. 증명법

- Lecturer: Suhyung Park, PhD

- Office: 공과대학 7호관 431호
- Contact: 062-530-1797
- E-mail: suhyung@jnu.ac.kr

* 본 강의 자료는 생능출판사와 한빛아카데미 "PPT 강의자료"를 기반으로 제작되었습니다.

강의 내용

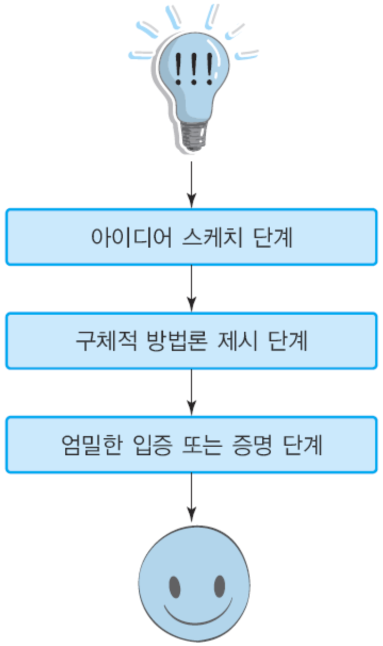
1) 증명의 방법론
2) 여러가지 증명 방법
3) 프로그램의 입증

증명의 방법론

- 공학이나 컴퓨터 관련 학문에 있어서 주어진 문제를 해결하기 위해서는 증명의 단계적 접근 방식이 효과적임

> **정의 4-1** 증명(proof)이란 논리적 법칙을 이용하여 주어진 가정으로부터 결론을 유도해내는 추론의 한 방법으로서, 어떠한 명제나 논증이 적절하고 타당한지를 입증하는 작업이다.

- **증명의 단계적 접근 방법**
  - **1. 아이디어 스케치 단계**
    - 문제 해결의 핵심적인 실마리를 찾아내어 기술함
    - 문제를 해결할 수 있는 방법론을 구상하게 되며 개략적인 아이디어를 스케치함
  - **2. 구체적인 방법론 제시 단계**
    - 아이디어를 묶어서 구체적인 블록 다이어그램(block diagram) 등으로 표현함
    - 프로그래밍의 경우 유사 코드(pseudo code) 단계까지 구체화하는 단계
  - **3. 엄밀한 입증이나 증명의 단계**
    - 자기가 내린 결론을 객관적인 증명 방법을 통해 누구나 공감할 수 있게 증명함



〈그림 4.1〉 증명의 단계적 접근 방법

여러가지 증명 방법

수학이나 공학에서의 증명 문제는 p → q와 같은 논리 함축을 증명함

논리 함축 p → q가 참이 되기 위해서는 p, q가 모두 참이거나 q에 관계없이 p가 거짓임을 보이면 됨

✓ 증명 방법은 직접 증명법과 간접 증명법 그리고 기타 증명법으로 구분함

- 직접 증명법은 p → q를 직접 증명하는 것임
- 간접 증명법은 논리적 동치를 이용하거나 다른 특수한 방법으로 증명함

✓ 주어진 문제 유형에 따라 다양한 방법으로 접근하는 것이 효율적임

수학이나 공학에서 새로운 결과를 얻는 2가지 중요한 방법론

- **연역법(deduction)**

  주어진 사실(facts)들과 공리(axioms)들에 입각하여 추론(inference)을 통하여 새로운 사실을 도출하는 것임

- **귀납법(induction)**

  관찰과 실험에 기반한 가설을 귀납 추론을 통하여 일반적인 규칙을 입증하는 것임

여러가지 증명 방법: 수학적 귀납법

수학적 귀납법(Mathematical Induction)

- 명제 p_1, p_2, p_3, ⋯, p_n이 사실이라고 할 때, p_{n+1}의 경우에도 성립함을 보이면 됨
- 먼저 n이 1인 경우에 성립하는 것을 보이고, 모든 양의 정수 n에 대해 성립한다고 가정하면 n + 1의 경우에도 성립함을 보여주면 됨

  - 기초 단계(basic)

    출발점이 되는 n의 값
  - 귀납 가정(inductive assumption)

    p_1, p_2, p_3, ⋯, p_n이 성립한다고 가정하면
  - 귀납 단계(inductive step)

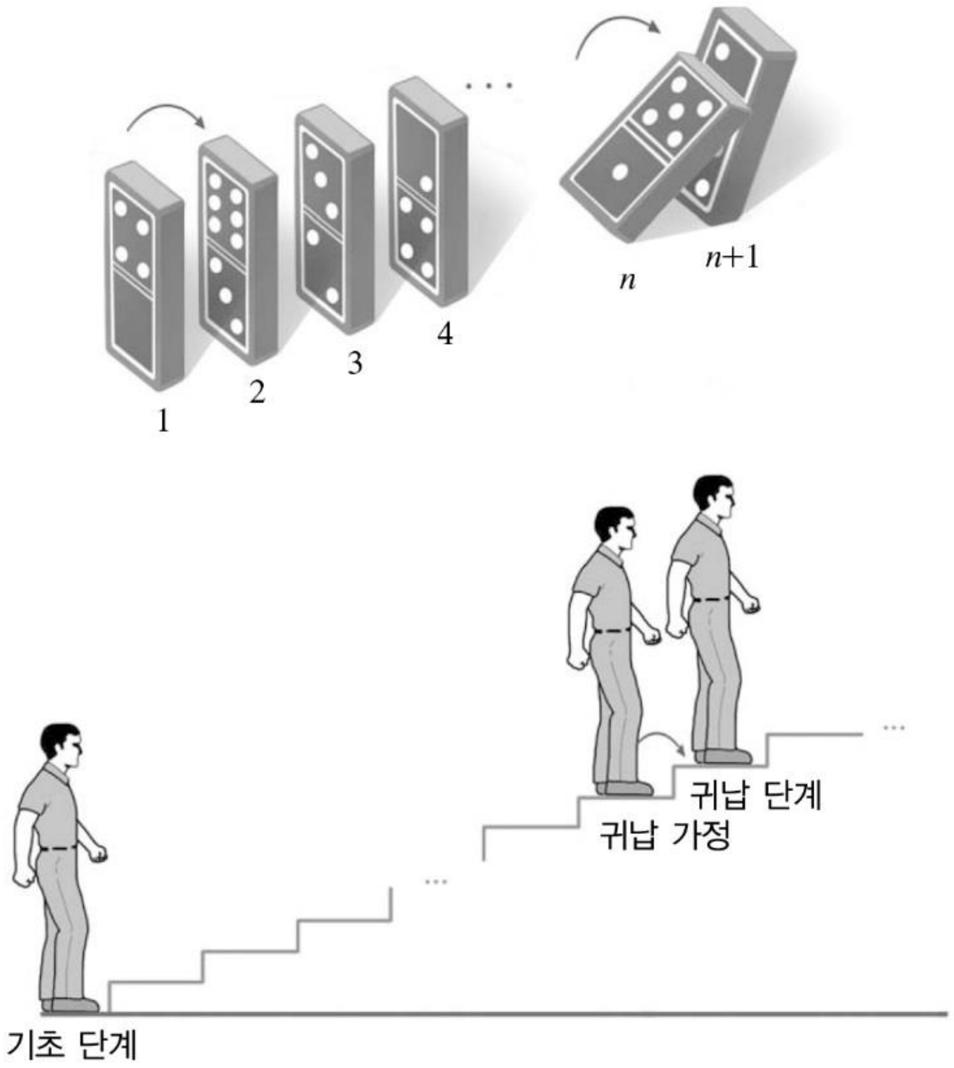
    p_{n+1}의 경우에도 성립함

여러가지 증명 방법: 수학적 귀납법

수학적 귀납법을 보다 직관적이면서도 쉽게 이해하기 위해 도미노와 계단이 인용됨

- 예1) 첫 번째 도미노를 건드리면 두 번째 도미노가 넘어지고, 그 뒤에 있던 도미노 들이 연속해서 계속 넘어지면, n번째 도미노가 넘어지면 n + 1번째 도미노도 연속해서 넘어지는 현상 으로 비유됨

- 예2) 계단을 오를 경우, 첫 번째 계단을 오르고 그 후 n번째 계단을 지나 n+1번째 계단을 같은 방법으로 오르는 것에 비유됨



〈그림 4.2〉 도미노와 계단 오르기

여러가지 증명 방법: 수학적 귀납법

수학적 귀납법은 논리식을 증명하는 데에도 이용

예) ‘ 모든 양의 정수 x에 대해 $p(x)$가 만족된다’ 는 명제를 증명하자

증명: $p(x)$에 모든 양의 정수 x를 대입한 경우, 즉 $p(1)$, $p(2)$, ⋯, $p(n)$, $p(n+1)$이 모두 참(true)이 됨을 보임으로써 주어진 논리식을 증명함

정리 4-1
수학적 귀납법의 원리

모든 정수 n에 대해 어떤 명제 $p(n)$이 주어졌을 경우 $p(n)$이 $n \geq 1$인 모든 정수에 대해 참이라는 것을 증명하기 위한 방법은 다음과 같다.

① (기초 단계) $p(1)$이 참임을 보인다.

② (귀납 가정) $p(n)$이 참이라고 가정한다.

③ (귀납 단계) 귀납 가정에 입각하여 $p(n+1)$이 참임을 보인다.

추론: $(P(1) \wedge \forall k(P(k) \rightarrow P(k+1))) \rightarrow \forall n P(n)$

여러가지 증명 방법: 수학적 귀납법

수학적 귀납법의 장단점

장점: 한 명제에 추측을 하고 그 추측이 사실이라면 증명에 사용 가능

단점: 새로운 정리를 발견하는 데는 사용될 수 없음

여러가지 증명 방법: 수학적 귀납법

예제 4-1 $S_n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$임을 증명해보자.

증명 (n에 대한 수학적 귀납법을 이용)

(기초 단계) $n=1$인 경우 왼쪽 $= S_1 = 1 = \frac{1 \cdot 2}{2} =$ 오른쪽

(귀납 가정) 만약 $S_n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ 이라고 가정하면

(귀납 단계) 왼쪽 $= S_{n+1} = S_n + (n+1)$

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

$$= \frac{n^2 + n + 2n + 2}{2}$$

$$= \frac{n^2 + 3n + 2}{2}$$

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

= 오른쪽 [n 대신 $n+1$을 각각 대입한 값]

여러가지 증명 방법: 수학적 귀납법

예제 ④-2 $1^2+2^2+\cdots+n^2=\dfrac{n(n+1)(2n+1)}{6}$임을 증명해보자.

증명 (n에 대한 수학적 귀납법을 이용)

(기초 단계) $n=1$인 경우 왼쪽 $=1^2=\dfrac{1\cdot2\cdot3}{6}=$ 오른쪽

(귀납 가정) 만약 $1^2+2^2+\cdots+n^2=\dfrac{n(n+1)(2n+1)}{6}$이라고 가정하면

(귀납 단계) 왼쪽 $=1^2+2^2+\cdots+n^2+(n+1)^2$

$$=\frac{n(n+1)(2n+1)}{6}+(n+1)^2$$

$$=\frac{n(n+1)(2n+1)+6(n+1)^2}{6}$$

$$=\frac{(n+1)\{n(2n+1)+6(n+1)\}}{6}$$

$$=\frac{(n+1)(2n^2+7n+6)}{6}$$

$$=\frac{(n+1)(n+2)(2n+3)}{6}$$

$$=\frac{(n+1)(n+2)\{2(n+1)+1\}}{6}$$

$=$ 오른쪽 [n 대신 $n+1$을 각각 대입한 값]

여러가지 증명 방법: 수학적 귀납법

예제 4-4 $n \geq 4$인 모든 정수에 대하여 $2^n \geq n^2$임을 증명해보자.

증명 (n에 대한 수학적 귀납법을 이용)

(기초 단계) $n \geq 4$이므로 n이 성립하는 가장 작은 수는 $n=4$이다.

좌변 $= 2^n = 2^4 = 16 = 4^2 = 16 =$ 우변

그러므로 좌변 $\geq$ 우변이다. 즉, $n=4$일 때 성립한다.

(귀납 가정) $n \geq 4$인 모든 정수에 대하여 $2^n \geq n^2$이 성립한다고 가정하자.

(귀납 단계) 여기서는 $2^{n+1} \geq (n+1)^2$일 경우에도 성립함을 보인다.

$2^{n+1} = 2 \times 2^n \geq 2 \times n^2 = n^2 + n^2$

그런데 $n \geq 4$에 대해서는 항상 $n^2 \geq 2n+1$인 성질을 이용하면

$(n-1)^2 \geq 0$

$2^{n+1} \geq n^2 + n^2 \geq n^2 + 2n + 1 = (n+1)^2$이다.

그러므로 $2^{n+1} \geq (n+1)^2$ [n 대신 $n+1$을 대입한 값]

∴ 위의 식이 성립한다. ■

여러가지 증명 방법: 수학적 귀납법

예제 4-32

$n \geq 3$인 자연수에 대해 $n^2 > 2n+1$이 성립함을 수학적 귀납법으로 증명하라.

풀이

$P(n): n^2 > 2n+1$일 때, 이 명제의 논의영역은 $n \geq 3$인 자연수이다.

기본가정) 이 논의영역의 첫 번째 값은 3이고 $P(3): 3^2 = 9 > 2 \cdot 3 + 1 = 7$이다.

$\therefore$ $P(3)$은 참(T)이다.

귀납가정) $P(k): k^2 > 2k+1$이 참(T)이라고 가정한다.

귀납증명) 위의 두 가정을 이용해 $P(k+1): (k+1)^2 > 2(k+1)+1$이 성립하는지 증명한다.

$$(k+1)^2 > 2(k+1)+1 = 2k+3 \quad \cdots\cdots ①$$

귀납가정에서 $k^2 > 2k+1$이라고 했으므로 귀납가정의 양변에 $2k+1$을 더하면

$$k^2 + 2k + 1 = (k+1)^2 > 2k+1+2k+1 = 4k+2 \quad \cdots\cdots ②$$

②의 $4k+2$가 ①의 $2k+3$보다 크다면 $(k+1)^2$도 $2k+3$보다 논의영역 내에서 항상 크다고 할 수 있으므로 $4k+2 > 2k+3$이 성립하는지 확인한다.

여러가지 증명 방법: 수학적 귀납법

예제 4-33

$n \geq 1$인 자연수일 때, $n! \geq 2^{n-1}$이 성립함을 수학적 귀납법으로 증명하라.

풀이

$P(n)$: $n! \geq 2^{n-1}$일 때, 이 명제의 논의영역은 $n \geq 1$인 자연수이다.

기본가정) 이 논의영역의 첫 번째 값은 1이고, $P(1)$: $1! = 1 \geq 2^{1-1} = 2^0 = 1$이다.

$\therefore$ $P(1)$은 참(T)이다.

귀납가정) $P(k)$: $k! \geq 2^{k-1}$이 참(T)이라고 가정한다.

귀납증명) $P(k+1)$: $(k+1)! \geq 2^{(k+1)-1}$이 성립하는지 증명한다. ································ ①

$(k+1)! = k!(k+1)$로 귀납가정의 좌변에 $k+1$을 곱한 것과 같은 형식이다. 귀납가정의 양변에 $k+1$을 곱하면,

$$k!(k+1) \geq 2^{k-1}(k+1)$$

②의 $2^{k-1}(k+1)$이 ①의 $2^{(k+1)-1}$보다 크다면, $(k+1)!$도 $2^{(k+1)-1}$보다 논의영역 내에서 항상 크다고 할 수 있으므로 $2^{k-1}(k+1) \geq 2^{(k+1)-1}$이 성립하는지 확인한다.

$$2^{k-1}(k+1) \geq 2^{(k+1)-1} = 2^k = 2^{(k-1)} \times 2$$

$k+1 \geq 2$ $\because$ 양변을 항상 0보다 큰 $2^{k-1}(k \geq 1)$로 나누므로 부등호 변화가 없다.

$\therefore$ $k \geq 1$

여러가지 증명 방법: 수학적 귀납법

예제 4-34

$n>0$ 인 짝수일 때, n^2+n이 2로 나누어떨어짐을 증명하라.

풀이

$P(n)$: $2\mid(n^2+n)$일 때, 이 명제의 논의영역은 $n>0$인 짝수이다.

기본가정) 이 논의영역의 첫 번째 값은 2이다. $2^2+2=6$이므로 $P(2)$: $2\mid 6$은 참(T)이다.

귀납가정) $P(k)$: $2\mid(k^2+k)$가 참(T)이라고 가정한다.

귀납증명) $P(k+1)$: $2\mid[(k+1)^2+(k+1)]$이 성립하는지 증명한다.

$$(k+1)^2+(k+1)=k^2+2k+1+k+1=k^2+k+2(k+1) \quad \cdots\cdots ①$$

귀납가정에서 $2\mid(k^2+k)$가 성립한다고 했으므로 $k^2+k=2q(q\in N)$로 정의할 수 있다. ①에서 $k^2+k+2(k+1)=2q+2(k+1)=2(q+k+1)$로 $2\mid[(k+1)^2+(k+1)]$이다.

∴ 기본가정과 귀납가정에 의해 $P(k+1)$: $2\mid[(k+1)^2+(k+1)]$은 참(T)이다.

∴ $n>0$인 짝수일 때, n^2+n이 2로 나누어떨어진다.