

전산논리학 소개

박성우
POSTECH 컴퓨터공학과

컴퓨터과학이 여는 세계

철수 지갑의 행방 불명

- 철수는 어제 마트에서 오는 길에 음식점에 들렀다.
- 그런데 지갑을 어디에 두었는지 기억이 안난다.
- 지갑은 어디에 있을까?

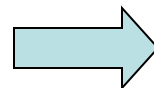
지갑 소재에 대한 추론

- 사실 파악:
 - 만약 마트에 지갑을 놔두고 왔다면,
지갑은 마트에서 찾을 수 있다.
 - 지갑은 마트에서 찾을 수 없었다.
 - 어제 밤 음식점에서 지갑을 열었다.
 - 어제 밤 지갑을 (음식점에서 쓴 뒤) 양복 안주머니에 넣었다.
 - 만약
어제 밤 음식점에서 지갑을 열었고
어제 밤 지갑을 양복 안주머니에 넣었고
어제 밤 이후로 지갑을 쓰지 않았다면,
지갑은 여전히 양복 안주머니에 있다.
 - 어제 밤 이후로 지갑을 쓰지 않았다.
- 결론 도출:
 - 마트에 지갑을 놔두고 오지 않았다.
 - 지갑은 여전히 양복 안주머니에 있다.

산술적으로 추론할 수 있을까?

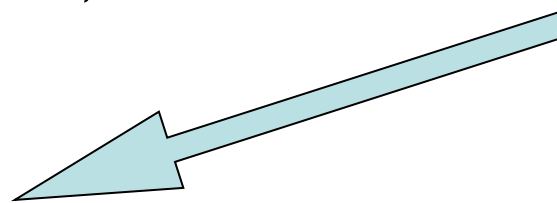
- 문장을 간단하게 표현
 - L = 마트에 지갑을 놔두고 왔다
 - F = 지갑은 마트에서 찾을 수 있었다
 - W = 어제 밤 음식점에서 지갑을 열었다
 - P = 어제 밤 지갑을 (음식점에서 쓴 뒤) 양복 안주머니에 넣었다
 - H = 어제 밤 이후로 지갑을 쓰지 않았다
 - S = 지갑은 여전히 양복 안주머니에 있다

- 사실 파악:
 - If L, then F. - Not F.
 - W and P.
 - If W and P and H, then S.
 - H.



$L(1 - F)$	$=$	0
F	$=$	0
WP	$=$	1
$WPH(1 - S)$	$=$	0
H	$=$	1

- 결론 도출:
 - L = 0, S = 1.



혹은 논리적으로 추론할 수 있을까?

추론규칙

$\frac{A \quad B}{A \wedge B} \wedge I$	$\frac{A \wedge B}{A} \wedge E_L$	$\frac{A \wedge B}{B} \wedge E_R$	$\frac{\overline{A}^x \quad \vdots \quad B}{A \supset B} \supset I^x$	$\frac{A \supset B \quad A}{B} \supset E$
$\frac{A}{A \vee B} \vee I_L$	$\frac{B}{A \vee B} \vee I_R$	$\frac{A \vee B \quad \overline{A}^x \quad \vdots \quad C \quad \overline{B}^y \quad \vdots \quad C}{C} \vee E^{x,y}$		
$\top \quad \perp$	$\frac{\perp}{C} \perp E$	$\frac{\overline{A}^x \quad \vdots \quad \perp}{\neg A} \neg I^x$	$\frac{\neg A \quad \perp}{A} \neg E$	



사실

$L \supset F$
 $\neg F$
 $W \wedge P$
 $(W \wedge P \wedge H) \supset S$
 H



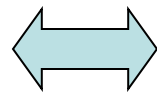
결론

$\boxed{\begin{array}{l} \neg L \\ S \end{array}}$

다음 사실간의 연관성은???

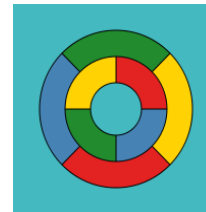
- "논리적으로 말이 되는구나"

비가 오거나 눈이 오면
여행을 취소한다

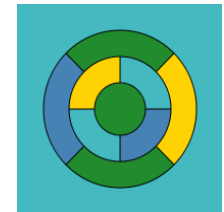


비가오면 여행을 취소하고,
눈이 오면 여행을 취소한다

- 논리학의 응용분야 및 발전



5



4

목차

- 도입 ✓
- 논리학이란?
- 기호논리학
- 전산논리학
- 마침

논리학

- 주어진 문장의 참과 거짓을 판별하는 과정을 다룸
- 특정 논리 체계의 구성
 - 명제
 - 추론 과정에 대한 정의

•명제

- 참과 거짓을 판별할 대상
 - "마트에 지갑을 놔두고 왔다"
 - "지갑은 여전히 양복 안주머니에 있다"
- 논리의 범위를 결정

•추론

- 참과 거짓을 판별하는 과정
 - "마트에 지갑을 놔두고 왔다"는 거짓이다.
 - "지갑은 여전히 양복 안주머니에 있다"는 참이다.
- 논리에서 인정하는 참의 의미를 결정

명제

- 다음 문장은 명제인가?
 - 1과 1의 합은 2이다
 - 1과 1의 합은 0이다
 - 푸른색은 흰색보다 아름답다
- '어떤 문장이 명제이다'의 의미:
 - 문장이 참이라는 증거가 주어졌을 때 증거가 옳바른지 판별할 수 있다

참의 개념

- 모든 논리 체계에 적용되는 절대적인 의미가 아님
- 논리 체계에 따라 달라질 수 있는 상대적인 의미
- 예:
 - 명제 A가 참임을 증명하자
 - 명제 A가 거짓이라고 가정하자
 - ...하면 모순이 나오므로 명제 A는 참이다.
- 예:
 - A = 달나라에는 계수나무가 있다
 - B = 페르마의 마지막 정리는 맞다
 - 'A이면 B이거나 B이면 A이다'는 참이다

참의 상대성

- 정리:
 a^b 이 유리수인 무리수 a 와 b 가 존재한다
- 증명
 - $c = \sqrt{2}^{\sqrt{2}}$ 를 고려하자.
 - 만약 c 가 유리수라면 $a = b = \sqrt{2}$ 로 둔다.
 - 만약 c 가 무리수라면 $a = c$ 와 $b = \sqrt{2}$ 로 둔다.
 - 따라서 조건을 만족하는 무리수는 항상 존재한다.
- 질문:
 - 그러면 a^b 이 유리수인 무리수 a 와 b 는 무엇인가?

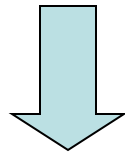
명제를 표현하는 언어

- 명제의 예:
 - 바람이 불고 비가 내린다.
 - 만약 비가 오거나 눈이 오면 여행은 취소된다.
 - 바람이 불지 않는다.
 - 모든 어린이는 예쁘다.
- 논리 접속사
 - ... 그리고 ...
 - ... 또는 ...
 - 만약 ...이면 ...이다
 - ...가 아니다
 - 모든 x 에 대해서 ...이다
 - ...한 어떤 x 가 존재한다
 - 항상 ...이다.
 - 때로는 ...이다.
- 논리 접속사를 이용해서 복잡한 명제를 만들어 냄

추론 방법론

- 예: 가정의 긍정

'만약 A이면 B이다'는 참이다.
A는 참이다.

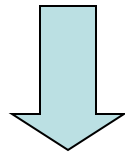


B는 참이다.

추론 방법론

- 예: 삼단논법

'모든 x 는 성질 A 를 만족한다'는 참이다.
' y 는 x 의 일종이다'는 참이다.

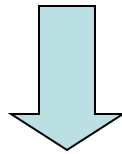


' y 는 성질 A 를 만족한다'는 참이다.

추론 방법론

- 예: 대우

'만약 A이면 B이다'는 참이다.
B는 거짓이다.

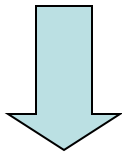


A는 거짓이다.

추론 방법론

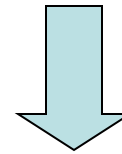
- 예: 자연 추론법

A는 참이다.
B는 참이다.

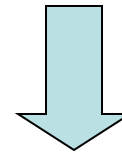


'A 그리고 B'는 참이다.

'A 그리고 B'는 참이다.



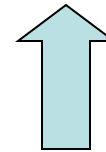
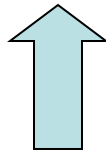
A는 참이다.



B는 참이다.

요약

논리 체계



명제를 표현하는 언어

- 더 이상 쪼갤 수 없는 명제
 - 비가 온다
 - 눈이 내린다
- 논리 접속사
 - ... 그리고 ...
 - ... 또는 ...
 - 만약 ...이면 ...이다

추론 방법론

- 가정의 긍정
- 삼단논법
- 자연 추론법
- ...

목차

- 도입
- 논리학이란? ✓
- 기호논리학
 - 진리표
 - 자연추론법
- 전산논리학
- 마침

자연 언어를 이용한 논리학

- 명제 해석의 모호함
 - '만약 A이면 B이다'는 정확하게 무슨 뜻인가?
 - A가 거짓이면 어떻게 되는가?
- 추론의 현실적 한계

'만약 마트에 지갑을 놔두고 왔다면 지갑은 마트에서 찾을 수 있을 것이고 지갑은 마트에서 찾을 수 없었다고 하고 어제 밤 음식점에서 지갑을 열었고 그 뒤 양복 안주머니에 넣었고 어제 밤 음식점에서 지갑을 열었고 지갑을 양복 안주머니에 넣었고 어제 밤 이후로 지갑을 쓰지 않았다면 지갑은 여전히 양복 안주머니에 있을 것이고 어제 밤 이후로 지갑을 쓰지 않았다면 지갑은 여전히 양복 안주머니에 있다'는 참인가?

기호논리학

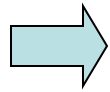
- 기호를 이용하여
 - 복잡한 명제를 간단하게 표현
 - 추론 과정을 이해하기 쉽게 설명
- 자연 언어의 모호함을 해결
- 자연 언어를 이용한 추론의 현실적 한계 극복

기호를 이용한 명제의 표현

- P, Q, R, \dots = 더 이상 쪼갤 수 없는 명제
 - $A \supset B$ = 만약 A이면 B이다
 - $A \wedge B$ = A 그리고 B
 - $A \vee B$ = A 또는 B
 - $\neg A$ = A가 아니다
 - $\forall x.A$ = 모든 x 에 대해서 A이다
 - $\exists x.A$ = A를 만족하는 x 가 존재한다
- 명제논리

술어논리

만약 마트에 지갑을 놔두고 왔다면 지갑은 마트에서 찾을 수 있을 것이고 지갑은 마트에서 찾을 수 없었다고 하고 어제 밤 음식점에서 지갑을 열었고 그 뒤 양복 안주머니에 넣었고 어제 밤 음식점에서 지갑을 열었고 지갑을 양복 안주머니에 넣었고 어제 밤 이후로 지갑을 쓰지 않았다면 지갑은 여전히 양복 안주머니에 있을 것이고 어제 밤 이후로 지갑을 쓰지 않았다.



$L \supset F$
 $\neg L$
 $W \wedge P$
 $(W \wedge P \wedge H) \supset S$
 H

Everyone loves a lover $\Leftrightarrow \forall x.\exists y.[(\exists z.L(y, z)) \supset L(x, y)]$
 where $L(x, y)$ for x loves y

기호논리학의 추론 과정 - 진리표

- 모든 명제에 진리값 참(T) 또는 거짓(F)을 부여
- ‘그리고’ \wedge 의미

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

기호논리학의 추론 과정 - 진리표

- '또는' \vee 의 의미
- '만약 ...이면 ...이다' \supset 의 의미

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

A	B	$A \supset B$
T	T	T
T	F	F
F	T	T
F	F	T

진리표를 이용한 기계적 추론

- A의 진리값은 B의 진리값에 영향받지 않는다

A	B	$B \supset A$	$A \supset (B \supset A)$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	T	T

진리표를 이용한 기계적 추론

- Peirce 법칙 (무슨 의미일까?)

A	B	$A \supset B$	$(A \supset B) \supset A$	$((A \supset B) \supset A) \supset A$
T	T	T	T	T
T	F	F	T	T
F	T	T	F	T
F	F	T	F	T

기호논리학의 추론 과정 - 자연 추론법

- 추론 규칙의 형식

$$\frac{A_1 \quad A_2 \quad \cdots \quad A_n}{C} R$$

- A_i = 가정 ($1 \leq i \leq n$)
- C = 결론
- R = 추론 규칙의 이름

$$\frac{I \text{ have an umbrella}}{My \text{ coat is wet}} \text{Weird}$$

$$\frac{My \text{ coat is wet}}{It \text{ is raining}} \text{Rain}$$

자연 추론법에서 '그리고' \wedge

- '그리고' \wedge 의미를 설명하는 추론 규칙
 - 어떻게 '그리고' \wedge 를 도입(Introduce)할 수 있는가?

$$\frac{A \quad B}{A \wedge B} \wedge I$$

- 어떻게 '그리고' \wedge 를 이용(Eliminate)할 수 있는가?

$$\frac{A \wedge B}{A} \wedge E_L \quad \frac{A \wedge B}{B} \wedge E_R$$

자연 추론법에서 '만약 ...이면 ...이다' \supset

- '만약 ...이면 ...이다' \supset 를 설명하는 추론 규칙
 - 어떻게 '만약 ...이면 ...이다' \supset 를 도입할 수 있는가?

$$\frac{\begin{array}{c} \overline{A}^x \\ \vdots \\ B \end{array}}{A \supset B} \supset I^x$$

- 어떻게 '만약 ...이면 ...이다' \supset 를 이용할 수 있는가?

$$\frac{A \supset B \quad A}{B} \supset E$$

자연 추론법에서 '또는' \vee

- '또는' \vee 의미를 설명하는 추론 규칙
 - 어떻게 '또는' \vee 을 도입할 수 있는가?

$$\frac{A}{A \vee B} \vee I_L \qquad \frac{B}{A \vee B} \vee I_R$$

- 어떻게 '또는' \vee 을 이용할 수 있는가?

$$\frac{A \vee B \quad \begin{array}{c} \overline{A}^x \\ \vdots \\ C \end{array} \quad \begin{array}{c} \overline{B}^y \\ \vdots \\ C \end{array}}{C} \vee E^{x,y}$$

자연 추론법에서 명제논리의 추론 규칙

$$\frac{A \quad B}{A \wedge B} \wedge I \quad \frac{A \wedge B}{A} \wedge E_L \quad \frac{A \wedge B}{B} \wedge E_R$$

$$\frac{\begin{array}{c} \overline{A}^x \\ \vdots \\ B \end{array}}{A \supset B} \supset I^x \quad \frac{A \supset B \quad A}{B} \supset E$$

$$\frac{A}{A \vee B} \vee I_L \quad \frac{B}{A \vee B} \vee I_R \quad \frac{A \vee B \quad \begin{array}{c} \overline{A}^x \\ \vdots \\ C \end{array} \quad \begin{array}{c} \overline{B}^y \\ \vdots \\ C \end{array}}{C} \vee E^{x,y}$$

자연 추론법을 이용한 기계적 추론

$$\begin{array}{c}
 \frac{\frac{\frac{A \supset (B \supset C)^x}{B \supset C}}{C} \supset E \quad \frac{\frac{\frac{\overline{A \wedge B}^y}{A} \wedge E_L}{\overline{A \wedge B}^y} \supset E}{B \supset C} \wedge E_R}{(A \wedge B) \supset C} \supset I^y}{(A \supset (B \supset C)) \supset ((A \wedge B) \supset C)} \supset I^x
 \end{array}$$

$$\begin{array}{c}
 \frac{\frac{\frac{(A \wedge B) \supset C^x}{C} \supset E \quad \frac{\frac{\overline{A}^y \quad \overline{B}^z}{A \wedge B} \wedge I}{(A \wedge B) \supset C} \supset E}{B \supset C} \supset I^z}{A \supset (B \supset C)} \supset I^y}{((A \wedge B) \supset C) \supset (A \supset (B \supset C))} \supset I^x
 \end{array}$$

- $(A \wedge B) \supset C$ 와 $A \supset (B \supset C)$ 는 논리적으로 동등
- 위 명제의 의미는 무엇일까?

자연 추론법을 이용한 기계적 추론

$$\frac{\frac{\frac{\overline{(A \vee B) \supset C}^x}{}{} \quad \frac{\overline{A}^y}{A \vee B} \vee I_L}{\frac{C}{A \supset C} \supset I^y} \supset E \quad \frac{\frac{\overline{(A \vee B) \supset C}^x}{}{} \quad \frac{\overline{B}^y}{A \vee B} \vee I_R}{\frac{C}{B \supset C} \supset I^y} \supset E}{\frac{(A \supset C) \wedge (B \supset C)}{\overline{((A \vee B) \supset C) \supset ((A \supset C) \wedge (B \supset C))} \supset I^x} \wedge I} \supset I^x$$

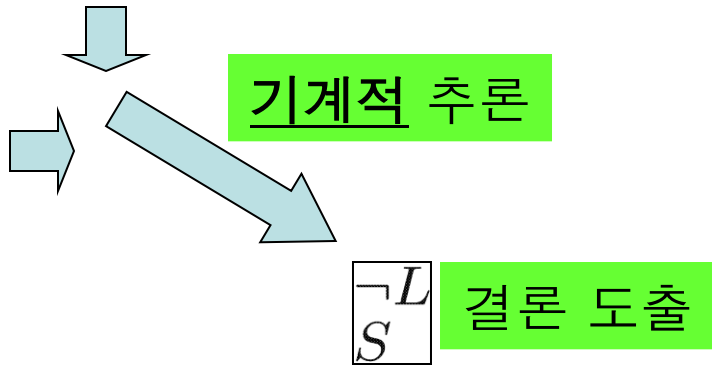
$$\frac{\frac{\frac{\overline{(A \supset C) \wedge (B \supset C)}^x}{A \supset C} \wedge E_L \quad \frac{\overline{A}^z}{A \supset C} \supset E}{\frac{C}{A \vee B} \supset I^y} \supset E \quad \frac{\frac{\overline{(A \supset C) \wedge (B \supset C)}^x}{B \supset C} \wedge E_R \quad \frac{\overline{B}^w}{B \supset C} \supset E}{C} \vee E^{z,w}}{\frac{C}{(A \vee B) \supset C} \supset I^y} \supset E}{\overline{((A \supset C) \wedge (B \supset C)) \supset ((A \vee B) \supset C)} \supset I^x} \supset I^x$$

- $(A \vee B) \supset C$ 와 $(A \supset C) \wedge (B \supset C)$ 는 논리적으로 동등
 - "비가 오거나 눈이 오면 여행을 취소한다"
 - "비가오면 여행을 취소하고, 눈이 오면 여행을 취소한다"

요약: 기호논리학에서 추론

추론규칙으로
논리체계 완성

$$\begin{array}{c}
 \frac{A \quad B}{A \wedge B} \wedge I \quad \frac{A \wedge B}{A} \wedge E_L \quad \frac{A \wedge B}{B} \wedge E_R \quad \frac{\overline{A}^x}{B} \supset I^x \quad \frac{A \supset B \quad A}{B} \supset E \\
 \\
 \frac{A}{A \vee B} \vee I_L \quad \frac{B}{A \vee B} \vee I_R \quad \frac{A \vee B \quad \overline{A}^x \quad \overline{B}^y}{C} \vee E^{x,y} \\
 \\
 \top \top I \quad \frac{\perp}{C} \perp E \quad \frac{\perp}{\neg A} \neg I^x \quad \frac{\neg A \quad A}{\perp} \neg E
 \end{array}$$



논리식으로
사실 표현

$$\begin{array}{l}
 L \supset F \\
 \neg L \\
 W \wedge P \\
 (W \wedge P \wedge H) \supset S \\
 H
 \end{array}$$

목차

- 도입
- 논리학이란?
- 기호논리학 ✓
- 전산논리학
- 마침

전산논리학

- 기호논리학 + 컴퓨터를 이용한 계산
 - 명제를 컴퓨터 언어로 표현
 - 추론 과정을 컴퓨터 언어로 설명
- 복잡한 추론의 자동화 가능
- 모든 산업 분야에서 이용됨



- 수학의 세번째 혁명을 유발

500 BC 그리스 과학계

- 질문: 우주는 무엇으로 이루어져 있는가?
- 논의:
 - A - 물은 생명에게 필요하니 우주의 일부이다*
 - B - 나도 그렇게 생각한다*
 - C - 불은 물과 다른 성질을 가진 것으로 우주의 일부이다*
 - A, B - 우리도 동의한다*
 - ...*
- 결론: 우주는 공기, 불, 물, 땅으로 이루어져 있다
- 과학 = 사회적 토론

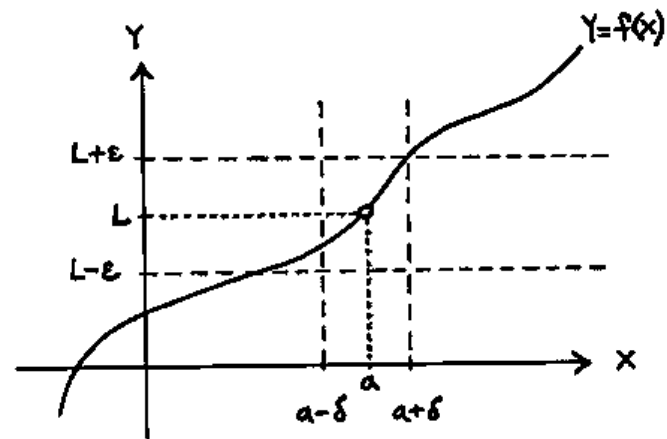
수학의 첫번째 혁명, 400 BC 그리스

- 증명 개념의 도입
 - 의견의 교환으로 결론에 도달하는 과정 탈피
 - 논리적 추론을 거쳐 결론에 도달
- 유클리드(Euclid) 기하학 (Elements) (300 BC)
 - 정의
 - 공리
 - 명제
 - 수학적 증명



수학의 두번째 혁명, 19세기 유럽

- 수학적 '엄밀함'의 도입
 - 코쉬(Cauchy) (1789-1857)
 - 뉴턴(Newton)과 라이프니치(Leibniz)의 미적분법을 극한의 정의를 도입해서 설명
 - epsilon/delta 정의



현대 수학은 엄밀한 증명을 다루는가?


엄밀한: 수학의 두번째 혁명

증명: 수학의 첫번째 혁명

Almgren Regularity 정리

- 고차원 공간에서 비누 거품은 뾰족하지 않다.
- 증명 초안 1728 페이지
- 한 줄을 이해하기 쉽지 않음
- 작성에만 10년 넘게 걸림
- 증명이 맞을 거라고 대부분의 수학자는 동의

케플러(Kepler) 정리

- 구를 이렇게  쌓으면 공간을 제일 적게 쓴다
- Hales의 증명
 - 300쪽의 증명 + 4만 라인의 컴퓨터 프로그램
- 모든 수학자가 동의하는가?
 - 여러 수학자가 몇 달 동안 세미나를 해 가면서 검증 시도
 - "They have not been able to certify the correctness of the proof, and will not be able to certify it in the future, because they have run out of energy to devote to the problem."
- 99% 증명이 맞을 거라고 대부분의 수학자는 동의

4색 문제

- 모든 지도는 4색으로 칠할 수 있다

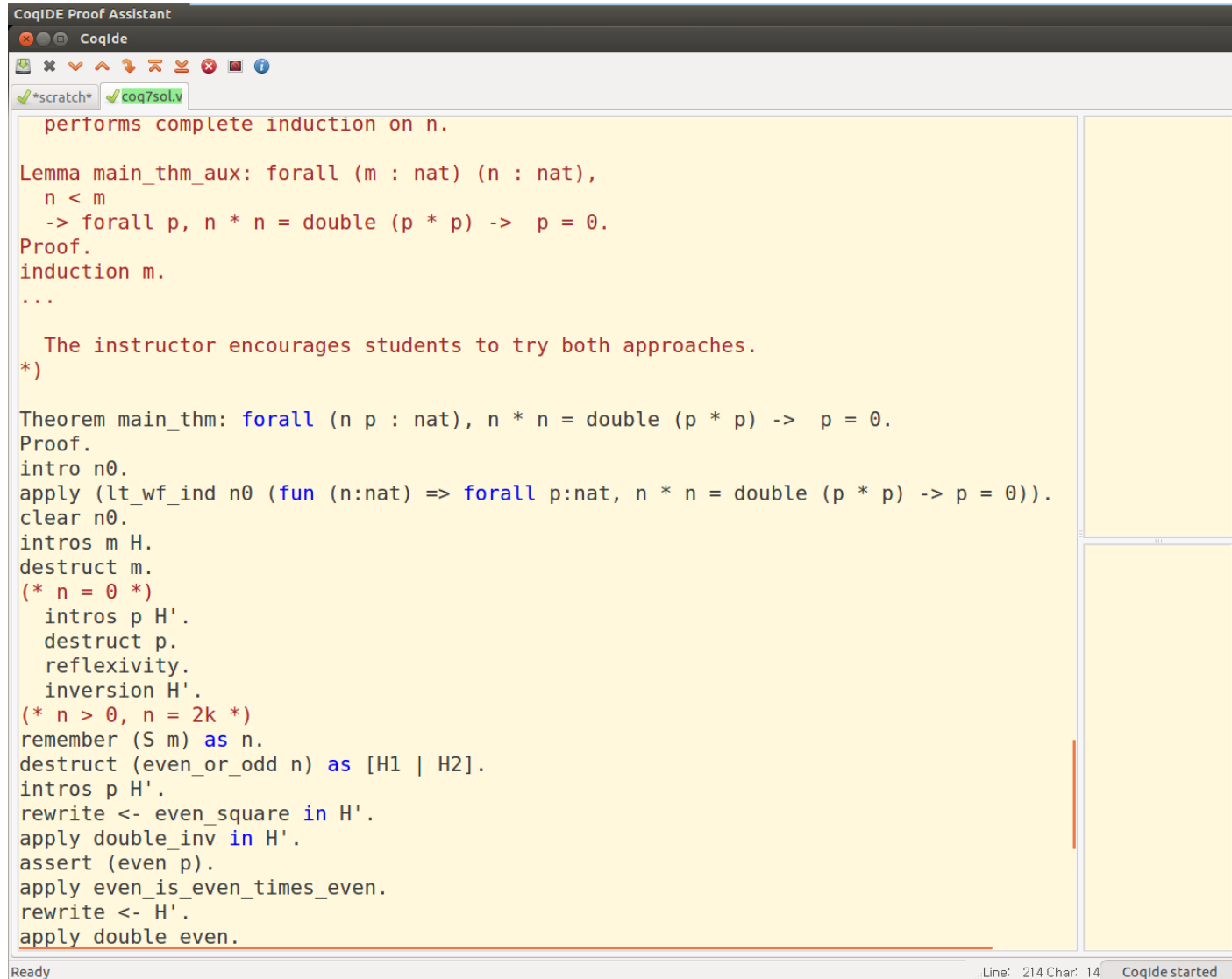


- 1852년 처음 제안
- Kempe의 1879년 증명은 10년 뒤 오류 발견
- 1970년대 컴퓨터를 이용한 검증 시도

컴퓨터를 이용한 증명보조기의 등장

- 전산논리학의 결집체
- 증명의 기계적 검증
 - 증명이 올바른지 검증
 - 검증이 완료되면 증명에는 오류가 없음
- 증명의 자동화 가능
 - 단순한 증명은 자동으로 완성
 - 계속 발전 중
- 수학자가 찾아내지 못한 증명을 찾아내기도 함
 - Robbins Conjecture

증명보조기로 피타고라스 정리 증명



```
CoqIDE Proof Assistant
CoqIde
*scratch* coq7sol.v
performs complete induction on n.

Lemma main_thm_aux: forall (m : nat) (n : nat),
  n < m
  -> forall p, n * n = double (p * p) -> p = 0.
Proof.
induction m.
...

The instructor encourages students to try both approaches.
*)

Theorem main_thm: forall (n p : nat), n * n = double (p * p) -> p = 0.
Proof.
intro n0.
apply (lt_wf_ind n0 (fun (n:nat) => forall p:nat, n * n = double (p * p) -> p = 0)).
clear n0.
intros m H.
destruct m.
(* n = 0 *)
  intros p H'.
  destruct p.
  reflexivity.
  inversion H'.
(* n > 0, n = 2k *)
remember (S m) as n.
destruct (even_or_odd n) as [H1 | H2].
intros p H'.
rewrite <- even_square in H'.
apply double_inv in H'.
assert (even p).
apply even_is_even_times_even.
rewrite <- H'.
apply double even.
```

Ready .Line: 214 Char: 14 CoqIde started

수학의 세번째 혁명, 1990년대 ~ 현재

- 형식 수학 (formal mathematics)
 - 증명보조기를 이용하여 수학 증명을 작성
- 형식 수학의 성공 예
 - 4색 문제 증명, 2002년, Coq
 - Feit-Thompson 정리 (Odd Order 정리), 2012년, Coq
- 현 상황
 - 대부분의 수학자는 세번째 혁명을 인지 못함
 - 현실적 제약: 증명을 형식화하는 시간이 오래 걸림
 - 학부 교과서 1 페이지를 형식화 = 1주일
- 100년 후
 - 증명을 형식화하는 것이 관행이 될 것임

목차

- 도입
- 논리학이란?
- 기호논리학
- 전산논리학 V
- 마침

전산논리학을 공부하면...

- 논리학으로부터
⇒ 참의 의미를 배운다!
- 기호논리학으로부터
⇒ 아름다움의 의미를 배운다!
- 전산논리학으로부터
⇒ 재미의 의미를 배운다!
- ... 참으로 아름다운 재미를 발견하게 된다!

감사합니다

gla@postech.ac.kr