Coq을 이용한 역수학

이계식

한경대학교

ROSAEC Workshop, 2012년 7월 25 ∼ 28일

내용 소개

프로젝트 소개

- Coq 개발팀장 Hugo Herbelin과 함께 진행
- Coq을 이용한 수리논리 연구 논의
- 역수학(reverse mathematics)에 관심
- POSTECH 박성우 교수, 파리 7대학 Laurent Bienvenue 교수 참여

고전수학과 역수학

고전/일반 수학 (Classical/Ordinary Mathematics)

- 주어진 공리체계 내에서 특정 성질(theorem)의 증명가능성을 연구
- 대수학, 군론, 기하학 등등
- 타입이론, 증명론 등등

일반 수학자들의 연구활동

- 어떤 공리들을 사용하는지 일반적으로 명시하지 않음
- 기본적으로 ZFC 집합론을 가정함

정리증명기(theorem prover)를 이용한 고전수학

- 일부 대학 연구소에서 Coq 등의 proof assistants를 이용하여 고전수학 연구 진행
- Freek Wiedijk: Formalizing 100 Problems (`http://www.cs.ru.nl/~freek/100/`)
- MSR-INRIA joint center (Georges Gonthier: 4색정리 증명)

역수학 (Reverse Mathematics)

- 1970년대 중반 Harvey Friedman이 제창
- ZFC는 너무 강력하여 기초론(foundation) 문제와 관련하여 많은 논쟁이 있음
- 주어진 고전수학의 정리를 증명하기위해 필요충분한 공리들을 찾아낼 필요성 대두
- 공리에서 출발하여 정리를 증명하는 것이 아니라 정리에서 출발하여 공리를 이끌어냄

대표적 다섯 시스템 (The Big Five Systems)

- 상당수의 고전수학 정리가 2계 산술(Second Order Aritmetic)의 부분체계(subsystem)에서 증명가능
- RCA_0, WKL_0, ACA_0, ATR_0, Π^1_1-CA_0가 중요한 역할을 함

- RCA_0: Baire category theorem, Intermediate Value Theorem, Soundness of predicate logic
- WKL_0 = Heine/Borel covering lemma = Gödel's Completeness Theorem = Brouwer's Fixed Point Theorem = Separable Hahn/Banach Theorem = Countable commutative rings have a prime ideal
- ACA_0 = Bolzano/Weierstraß Theorem = Countable commutative rings have a maximal ideal = Ramsey's Theorem for coloring's of $[\mathbb{N}]^n$
- ATR_0 = Countable well-orderings are comparable = Perfect Set Theorem = Lusin's separation theorem
- Π^1_1-CA_0 = Cantor/Bendixson Theorem = Trees have a largest perfect subtree = Silver's Theorem

괴델 계층도

strong	ZF, ZFC, ...	
	Zermelo set theory	System $F_{\omega.2+}$
	HOL (Church's Simple Type Theory)	Girard's System F_ω
medium	Z_2 (full 2nd order arithmetic)	Girard-Reynolds' System F
	Π^1_1-CA_0	
	CZF (Aczel's Constructive Set Theory)	
	ATR_0	
	ACA_0	Gödel's System T
	HA^ω (intuit. arithm. in finite types)	Gödel's System T
	PA	Gödel's System T
weak	WKL_0	prim. rec. funct.
	RCA_0	prim. rec. funct.
	$I\Sigma_1$	prim. rec. funct.
	PRA (prim. rec. arithmetic)	prim. rec. funct.
	EFA (elementary funct. arithmetic)	prim. rec. funct. up to p^n

Coq을 이용한 역수학

1. 대표적 다섯 시스템에 대응하는 타입이론 개발
2. Coq의 서브시스템 개발
3. 구현된 Coq 서브시스템을 이용한 역수학 연구

현재 진행연구

1. 대표적 다섯 시스템에 대응하는 타입이론 개발

대표적 다섯 시스템의 통일된 표현

2계 산술(Second order arithmetic, Z_2)

Z_2의 언어 L_2:

- first order quantification over natural numbers $(n, m, ...)$:
  - 자연수, 정수, 유리수, 리스트, 유한수열, 유한나무 등등을 대상
- second order quantification over sets of natural numbers $(X, Y, ...)$ 와 $n \in X$:
  - countable sequences, 실수, 그룹, fields, 벡터공간, 함수 등등을 대상

2계 산술 공리

(i) basic axioms:

$$
\begin{aligned}
&n + 1 \neq 0 \\
&m + 1 = n + 1 \to m = n \\
&m + 0 = m \\
&m + (n + 1) = (m + n) + 1 \\
&m \cdot 0 = 0 \\
&m \cdot (n + 1) = (m \cdot n) + m \\
&\neg m < 0 \\
&m < n + 1 \leftrightarrow (m < n \vee m = n)
\end{aligned}
$$

(ii) inducion axiom:

$$(\mathsf{IND}) \quad 0 \in X \to \forall n(n \in X \to n+1 \in X) \to \forall n(n \in X)$$

(iii) comprehension scheme:

$$(\mathsf{CA}) \quad \exists X \, \forall n(n \in X \leftrightarrow A(n))$$

where $A(n)$ is any L_2 formula in which X does not occur freely.

Z_2의 표현력(expressiveness)

- 정수($\mathbb{Z}$): 자연수들의 쌍으로 표현
- 유리수($\mathbb{Q}$): 정수와 양의 정수($\mathbb{Z}^+$)의 쌍으로 표현
- 실수($\mathbb{R}$): 유리수를 이용한 코시 수열(Cauchy sequences)
  $x = \langle q_n : n \in \mathbb{N} \rangle$, $q_n \in \mathbb{Q}$ 이용:

$$\forall \epsilon \in \mathbb{Q} \left[\epsilon > 0 \rightarrow \exists m \forall n \left(m < n \ \rightarrow \mid q_m - q_n \mid < \epsilon \right) \right]$$

The Arithmetical Hierarchy

- $A \in \Sigma_0^0$ iff $A \leftrightarrow B(n, m, Y)$ with B primivie recursive
- $A \in \Pi_0^0$ iff $A \leftrightarrow B(n, m, Y)$ with B primivie recursive
- $A \in \Sigma_{k+1}^0$ iff $A \leftrightarrow \exists n\, B(n, m, Y)$ with $B \in \Pi_k^0$
- $A \in \Pi_{k+1}^0$ iff $A \leftrightarrow \forall n\, B(n, m, Y)$ with $B \in \Sigma_k^0$

The Analytical Hierarchy

- $A \in \Sigma_0^1$ iff $A \leftrightarrow B(m, Y) \in \Sigma_n^0$ for some k
- $A \in \Pi_0^1$ iff $A \leftrightarrow B(m, Y) \in \Sigma_n^0$ for some k
- $A \in \Sigma_{k+1}^1$ iff $A \leftrightarrow \exists X\, B(X, m, Y)$ with $B \in \Pi_k^1$
- $A \in \Pi_{k+1}^1$ iff $A \leftrightarrow \forall X\, B(X, m, Y)$ with $B \in \Sigma_k^1$

The big five

- $\mathrm{RCA}_0 =$ Recursive Comprehension Axiom (CA on Δ^0_1 formulae)
- $\mathrm{WKL}_0 = \mathrm{RCA}_0 +$ Weak König's Lemma (WKL)
- $\mathrm{ACA}_0 = \mathrm{RCA}_0 +$ Arithmetic Comprehension Axiom (CA on Σ^0_1 formulae)
- $\mathrm{ATR}_0 = \mathrm{ACA}_0 +$ Arithmetic Transfinite Recursion (ATR on arithmetic formulae)
- Π^1_1-$\mathrm{CA}_0 = \mathrm{ACA}_0 +$ CA on Π^1_1 formulae

Comprehension vs. Separation

(S-CA):

$$\exists X \forall n (n \in X \leftrightarrow A(n))$$

for any $A \in S$

(S-SEP)

$$\forall n \neg (A_1(n) \wedge A_2(n)) \rightarrow \exists X \forall n ((A_1(n) \rightarrow n \in X) \wedge (A_2(n) \rightarrow n \notin X))$$

for any $A_1(n), A_2(n) \in S$.

Comprehension vs. Separation

(S-CA):

$$\exists X \, \forall n (n \in X \leftrightarrow A(n))$$

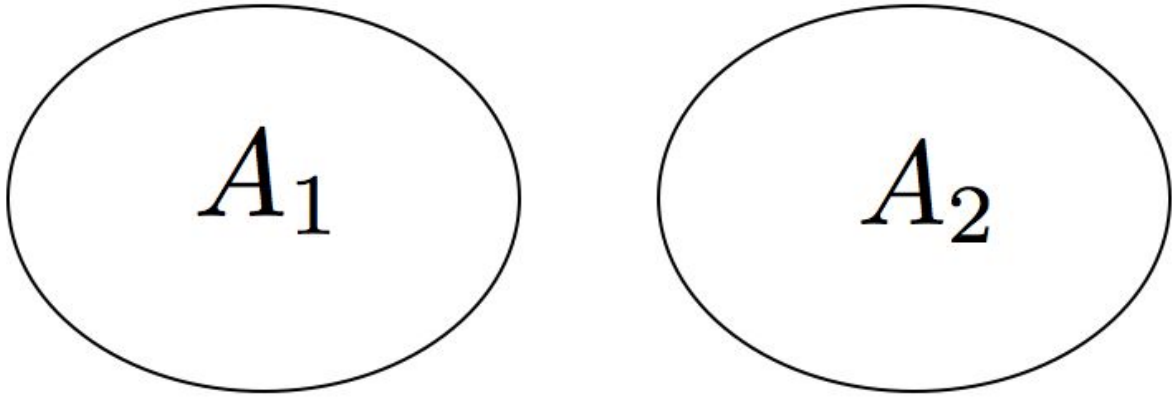
for any $A \in S$

(S-SEP)

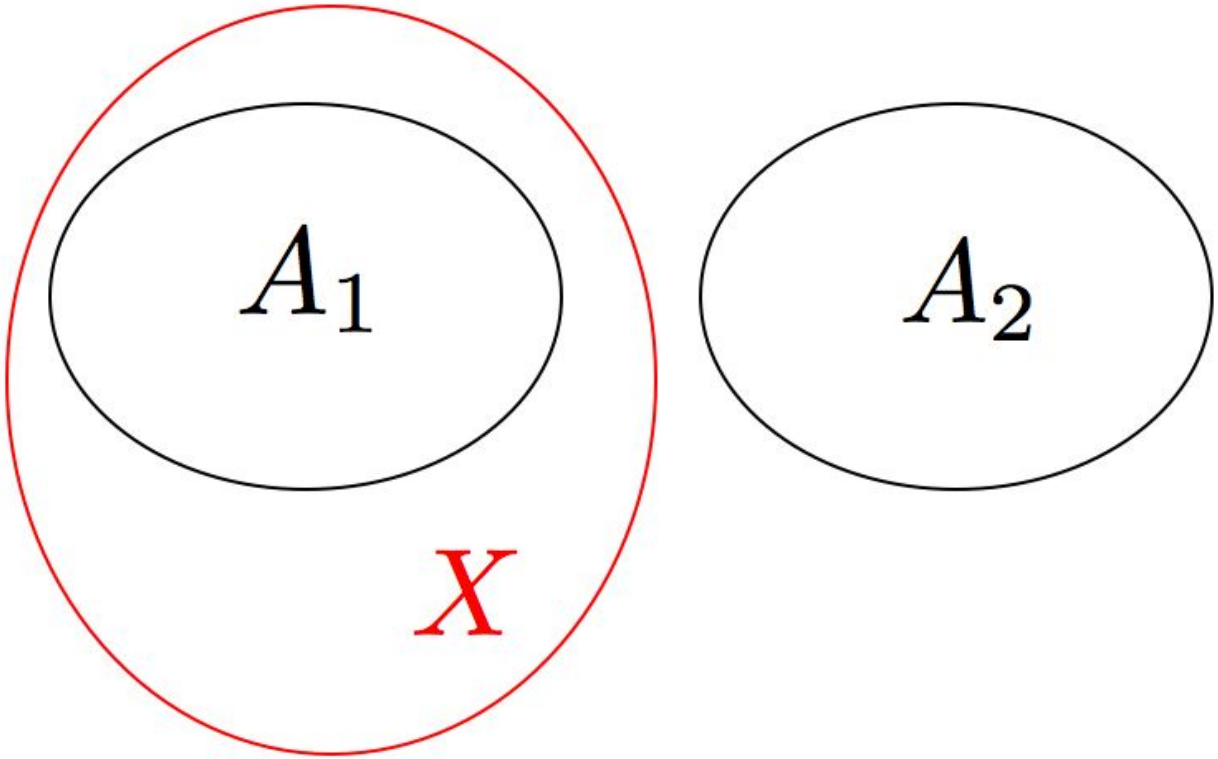
$$\forall n \, \neg (A_1(n) \wedge A_2(n)) \rightarrow \exists X \, \forall n ((A_1(n) \rightarrow n \in X) \wedge (A_2(n) \rightarrow n \notin X))$$

for any $A_1(n), A_2(n) \in S$.

Separation 공리



Separation 공리



요약 (Simpson '99)

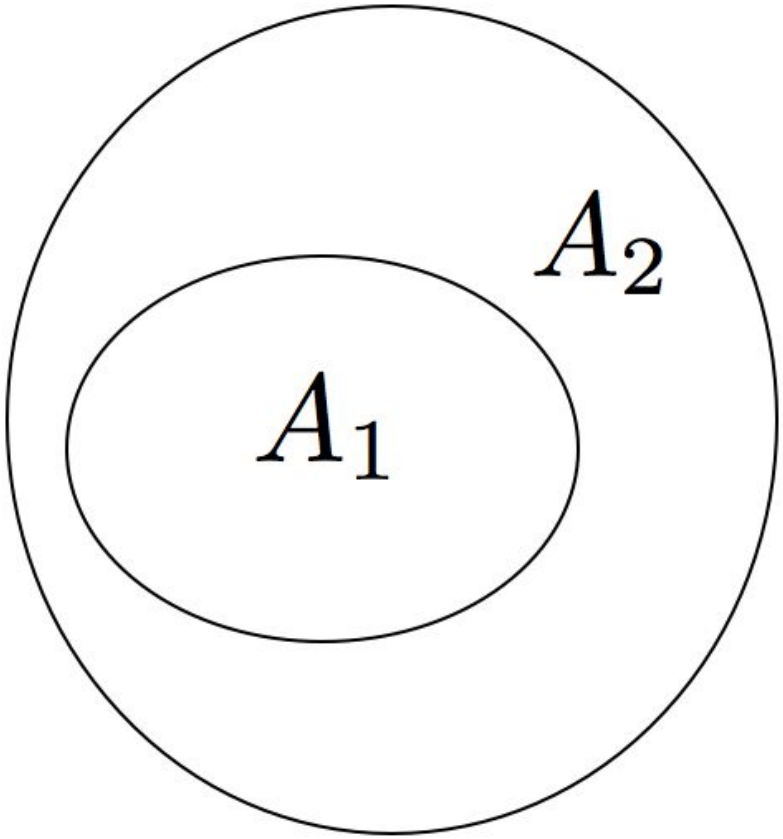
system	characterization	f.o. fragment	functions
RCA_0	Δ^0_1-CA	$I\Sigma_1$	prim. rec
WKL_0	Σ^0_1-SEP	$I\Sigma_1$	prim. rec.
ACA_0	Σ^0_1-CA	PA	System T
ATR_0	Σ^1_1-SEP		
Π^1_1-CA_0	Σ^1_1-CA		

S_1-S_2-Interpolation

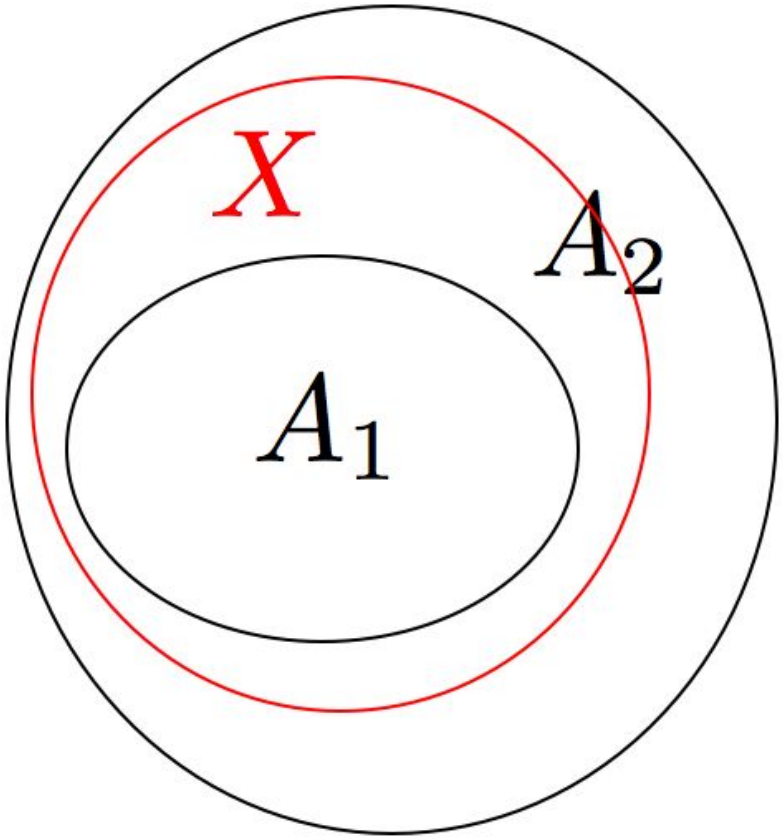
$$\forall n\,[\,A_1(n) \to A_2(n)\,] \to \exists X\,\forall n\,[\,(A_1(n) \to n \in X) \wedge (n \in X \to A_2(n))\,]$$

for $A_i(n) \in S_i$.

Interpolation 공리



Interpolation 공리



S_1-S_2-Interpolation

- S-CA iff S-S-INTERPOL.
- S-SEP iff S-$\neg S$-INTERPOL.

where $\neg S := \{\neg A \mid A \in S\}$.

요약 2

system	new characterization	old characterization
RCA_0	Π^0_1-Σ^0_1-INTERPOL	(i.e. Δ^0_0-CA)
WKL_0	Σ^0_1-Π^0_1-INTERPOL	(i.e. Σ^0_1-SEP)
ACA_0	Σ^0_1-Σ^0_1-INTERPOL	(i.e.,Σ^0_1-CA)
ATR_0	Σ^1_1-Π^1_1-INTERPOL	(i.e., Σ^1_1-SEP)
Π^1_1-CA_0	Σ^1_1-Σ^1_1-INTERPOL	(i.e.,Σ^1_1-CA)

추론규칙

$$\frac{\Gamma \vdash (0 \in P) \quad \Gamma, n \in P \vdash n+1 \in P \quad n \text{ fresh}}{\Gamma \vdash t \in P} \text{ (IND)}$$

$$\frac{\Gamma \vdash A_1[t/n] \quad A_1 \in S_1}{\Gamma \vdash t \in \{n \mid A_1 \lhd A_2\}} \text{ (INTERPOL}_I\text{)}$$

$$\frac{\Gamma \vdash t \in \{n \mid A_1 \rhd A_2\} \quad A_2 \in S_2 \quad \Gamma, A_1 \vdash A_2}{\Gamma \vdash A_2[t/n]} \text{ (INTERPOL}_E\text{)}$$

감사합니다.