

# 컴퓨터를 이용한 역수학 (Reverse Mathematics)

이계식

한경대학교

ROSAEC Workshop, 2013년 1월 30 ~ 2월 2일

## 타입이론에 기초한 (역)수학 정형화

질문 하나 드리겠습니다.

- 수학을 Coq과 같은 증명보조기로 정형화(formalization)해야 하나요?
- 왜 해야한다고 생각하나요?

- 수학 기초론에 대한 연구와 더불어 1970년 전후로 수학적 증명을 검증하는 다섯 개의 시스템이 개발됨
  - ▶ Automath: De Bruijn
  - ▶ Nqthm: Boyer Moore (Austin, Texas)
  - ▶ LCF: Milner (Stanford; Edinburgh)
  - ▶ Mizar: Trybulec (Bialystok, Poland)
  - ▶ Evidence Algorithm: Glushkov (Kiev, Ukrain)

- 신뢰성을 높이니까.
- PL 분야에서는 Coq을 이용한 증명이 대세가 되어버렸음.

- 하지만 수학 분야에서는 상황이 좀 다름.
  - ▶ 신뢰성에 대한 인식이 다름.
  - ▶ 자부심이 보다 강함
  - ▶ 소위 마인드가 다름: 수학자 마인드는 프로그래밍을 근본적으로 싫어한다. (왜?)
  - ▶ 하지만 정말로 이게 전부인가?
  - ▶ 정형화 수준(?)이 다름: Latex vs. Coq?

- 수학을 정형화하는 게 L<sup>A</sup>T<sub>E</sub>X을 사용하는 것 만큼 쉬운 일인가?
- 수학자와 엔지니어들이 Computer Algebra 시스템을 사용하는 반면에 증명보조기는 사용하지 않는 이유는 무엇인가?



1918년 7월 9일 ~ 2012년 2월 17일

*As a kind of dream I played (in 1968) with the idea of a future where every mathematician would have a machine on his desk, all for himself, on which he would write mathematics and which would verify his work. But, by lack of experience in such matters, I expected that such machines would be available within 5 years from then. But now, 23 years later, we are not that far yet.*

44년이 지난 현재의 상황은 좀 더 나아졌나?

*Anyway I expected in 1968 that the memory capacity of main frame computers would grow rapidly in the next few years, but that was a deception too. Implementing Automath on the quite advanced computers available to us in the years 1970-1975 was to a large extent to struggle for living with the limitations of fast accessible memory.*

- 하드웨어 측면에서는 훨씬 상황이 좋아졌다.  
(황의 법칙?)
- 소프트웨어 측면에서는?

# 다시 개인적인 견해

- de Bruijn이 1968년에 기대한 바가 이루어지기 위해서는 20년 정도 더 기다려야 하지 않을까 함.
- 이유
  - ▶ 증명보조기가 아직도 수학자들이 사용하기에는 쉽지 않다.
  - ▶ 전산학자에게조차도 dependent types과 관련된 프로그래밍은 꽤 어려움.
  - ▶ Georges Gonthier 같은 전문가도 Coq을 사용할 때의 기술적 어려움을 언급하곤 함.
  - ▶ 보다 근본적인 문제가 있어 보임.

# 근본적인 문제

- 수학자들의 마인드는 왜 프로그래밍을 싫어하는가?
- 19세기 후반부터 이루어진 현대 수학의 역사와 관련 있어 보임.
- 고전주의 대 직관주의의 경쟁에서 고전주의의 거의 일방적인 승리

배중율을 왜 안써?

그러면 더 적은 정리를 증명할 수 밖에 없잖은가!?

난 보다 많은 정리를 증명하고 싶다!

# 수학적 마인드의 한계

- 수학자들이 사용하는 논리적 기초론에 근본적인 질문을 던질 수밖에 없다.
- 예를 들어, 선택공리를 무슨 근거로 인정할 수 있는가?
- 실제로 수학기초론에 대한 논쟁은 여전히 진행중이다!
- (개인 견해) 20세기 초반의 Hilbert와 Brouwer의 논쟁 이후 2차 논쟁이 본격적으로 진행되고 있어 보임.

# 수학의 또다른 한계

- Shinichi Mochizuki라는 일본 교토대학교 수학자가 2012년 8월에 소위 ABC Conjecture라고 알려진 문제를 풀었다며 500쪽짜리 논문을 공개함.
- 잘 알려지지 않는 문제지만 영향력은 매우 큼. (많은 유명한 Diophantine 문제들, Fermat 정리 등등이 단숨에 풀릴 수 있음.)
- 하지만 하지도 제시된 증명이 옳은지 여부를 판단 못함.

- 수학적 증명의 신뢰성이 보다 절실했다.
- 단순한 수학적 기초론의 문제가 아닌 현실적인 문제로도 대두됨.

# 수학자들의 변화



- Vladimir Voevodsky (프린스턴 고등과학원 교수, 1966년생)
- 2002년 Homotopy theory 관련 업적으로 필드상 수여
- 현재 Homotopy type theory에 기반한 증명보조기 개발 연구 진행

# 정형화 관련 근본적인 질문

수학자들이 하는 것을 정형화할 것인가?  
아니면 수학자들이 하는 것을 바꿀 것인가?

# 고전수학 정형화의 문제점

- 정형화와 관련해서 Martin-Löf의 type theory가 수학기초론의 대세로 논리학자들 사이에서 인정됨.
- 고전수학 자체가 증명보조기를 이용한 증명에는 너무 어렵다.
- 기초론적 질문이 다시 대두되는 이유
- Homotopy type theory가 엄청난 관심을 끌고 있음.

# 역수학 (Reverse Mathematics) 소개

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

- Coq을 이용한 수리논리 연구 논의
- 역수학(reverse mathematics)에 관심
- 역수학에서 가장 중요시 여겨지는 다섯 개의 고전논리 시스템을 inductive definitions에 기초한 type theory로 구현하는 것이 주목표임.

# 타입이론에 바탕을 둔 역수학

- 대표적 다섯 시스템에 대응하는 타입이론 개발
- Coq의 서브시스템 개발
- 구현된 Coq 서브시스템을 이용한 역수학 연구

# 타입이론에 바탕을 둔 역수학

- 고전수학 대신에 타입이론을 사용할 경우 어떤 차이점이 존재하는가?
- 역수학 증명들 속에 내재되어 있는 프로그램 성질 연구.  
(Program-as-proof 관계 연구)

감사합니다!