The big five systems of reverse mathematics and their computational interpretation

Gyesik Lee
(Work in progress with Hugo Herbelin and Keiko Nakata)

Hankyong National University

CORCON 2014 Genoa
25 March, 2014

Contents

The “proof-as-program” point of view

Goal: Redefining the “Big Five” as typed programming languages

- Curry [1958]: Hilbert-style propositional logic = simply-typed combinatory logic
- Howard [1969]: Gentzen’s natural deduction = some simply-typed λ-calculus
- Martin-Löf’s type theory with W-type [around 1980]: an intuitionistic logic the strength of Π^1_1-CA_0 which is also a programming language
- Griffin [1990]: Classical logic = control operator (`callcc`/`throw`)
- etc.

Basis of Reverse Mathematics

- Started by Harvey Friedman in the 70's.
- *Determine the logical strength underlying standard mathematical theorems*.

The Big Five Systems

- RCA_0 suffices to prove: Baire category theorem, Intermediate Value Theorem, Soundness of predicate logic, ... (Note: reals are Cauchy sequences, represented as funct. relations)
- 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 colouring's of $[\mathbb{N}]^n$ = ...
- ATR_0 = countable well-orderings are comparable = Perfect Set Theorem = Lusin's separation theorem = ...
- Π^1_1-CA_0 = trees have a largest perfect subtree = Cantor/Bendixson Theorem = Silver's Theorem = ...

The Big Five Systems

- $\text{RCA}_0 = \Sigma^0_1\text{-IND} + \Delta^0_1\text{-CA}$
- $\text{WKL}_0 = \text{RCA}_0$ + Weak König's Lemma
- $\text{ACA}_0 = \text{IND} + \Sigma^0_1\text{-CA}$
- $\text{ATR}_0 = \text{ACA}_0$ + Arithmetic Transfinite Recursion
- $\Pi^1_1\text{-CA}_0 = \text{ACA}_0 + \Pi^1_1\text{-CA}$

Interpolation Scheme

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		$\Psi_0(\Omega_\omega)$
	CZF (Aczel's Constructive Set Theory)		$\Psi_0(\epsilon_{\Omega+1})$ (Bachmann-Howard)
	ATR_0		Γ_0 (Feferman-Schütte)
	ACA_0	Gödel's System T	ϵ_0
	HA^ω (intuit. arithm. in finite types)	Gödel's System T	ϵ_0
	PA	Gödel's System T	ϵ_0
weak	WKL_0	prim. rec. funct.	ω^ω
	RCA_0	prim. rec. funct.	ω^ω
	$I\Sigma_1$	prim. rec. funct.	ω^ω
	PRA (prim. rec. arithmetic)	prim. rec. funct.	ω^ω
	EFA (elementary funct. arithmetic)	prim. rec. funct. up to p^n	ω^3

RCA_0

- RCA_0 is characterised by the axiom of Δ^0_1-comprehension:

$$\Delta^0_1\text{-CA} : \exists X \forall n \, (n \in X \iff A(n))$$

for $A(n) \in \Delta^0_1$ (possibly with parameters)

- The only definable sets are the recursive ones.
- The second-order variant of $\mathsf{I}\Sigma_1$.
- The functions provably total in RCA_0 are the primitive recursive functions.

WKL_0

- WKL_0 extends RCA_0 with Weak König's Lemma:

  (WKL) "Every infinite binary tree has an infinite path."

- WKL is not strong enough to make induction exceed the strength of Σ^0_1-induction.

- Like for RCA_0, the first-order fragment of WKL_0 is $\mathsf{I}\Sigma_1$.

WKL_0 with Separation

- Over RCA_0, WKL is equivalent to separation of non-overlapping Σ^0_1-formulas:

$$\Sigma^0_1\text{-SEP} : \forall n \neg(A_1(n) \wedge A_2(n)) \rightarrow \exists X \forall n \begin{cases} A_1(n) \rightarrow n \in X \\ A_2(n) \rightarrow n \notin X \end{cases}$$

  for any $A_1(n), A_2(n) \in \Sigma^0_1$.

- Σ^0_1-SEP directly implies Δ^0_1-CA

ACA_0

- ACA_0 is characterised by the axiom of Σ^0_1-comprehension:

$$\Sigma^0_1\text{-CA} : \exists X\, \forall n\, (n \in X \iff A(n))$$

for $A(n) \in \Sigma^0_1$ (possibly with parameters)

- Σ^0_1-comprehension is equivalent to

$$\Pi^0_1\text{-CA} : \exists X\, \forall n\, (n \in X \iff A(n))$$

for $A(n) \in \Pi^0_1$ (possibly with parameters)

- Hence, Σ^0_k-CA and Π^0_k-CA are available.

- The first-order part of ACA_0 is Peano Arithmetic.

ATR_0

- ATR_0 extends further arithmetical comprehension (i.e. Σ^0_k-CA) using arithmetical transfinite recursion:

$$\mathsf{ATR} : \forall <_J \ (\mathrm{WO}(<_J) \to \exists Y\,((n,j) \in Y \iff j \in J \wedge A(n, Y^j)))$$

  where:
  - $A(n, X)$ is a Σ^0_1-formula (or any arbitrary arithmetical formula)
  - Y^j is the unique set defined by $(n, i) \in Y^j \iff i <_J j \wedge (n, i) \in Y$
  - $\mathrm{WO}(<_\mathrm{J})$ means that $<_J$ is a set of pairs defining a well-ordered subset of $\mathbb{N}$

- It is said to be that it has the same ordinal strength as that of Martin-Löf's type theory with countably many universes but no W-type.

ATR_0 with Separation

- ATR is indeed equivalent to separation of non-overlapping Σ^1_1-formulas:

$$\Sigma^1_1 - \text{SEP} : \forall n \neg (A_1(n) \wedge A_2(n)) \to \exists X \forall n \begin{cases} A_1(n) \to n \in X \\ A_2(n) \to n \notin X \end{cases}$$

for any $A_1(n), A_2(n) \in \Sigma^1_1$

Π^1_1-CA$_0$

- Π^1_1-CA$_0$ is characterised by the axiom of Σ^1_1-comprehension:

$$\Sigma^1_1\text{-CA} : \exists X \, \forall n \, (n \in X \iff A(n))$$

for $A(n) \in \Sigma^1_1$ (possibly with parameters)

- We also have

$$\Pi^1_1\text{-CA} : \exists X \, \forall n \, (n \in X \iff A(n))$$

for $A(n) \in \Pi^1_1$ (possibly with parameters)

How to make the big 5 look uniform?

RCA_0	Δ^0_1-CA
WKL_0	Weak König's Lemma
ACA_0	Σ^0_1-CA
ATR_0	Arithmetic Transfinite Recursion
Π^1_1-CA_0	Π^1_1-CA

Summary (Simpson '99)

RCA_0	Δ^0_1-CA
WKL_0	Σ^0_1-SEP (or WKL)
ACA_0	Σ^0_1-CA (or Π^0_1-CA)
ATR_0	Σ^1_1-SEP (or ATR)
Π^1_1-CA_0	Σ^1_1-CA (or Π^1_1-CA)

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

S_1-S_2-Interpolation

$$S_1\text{-}S_2\text{-INTERPOL}: \forall n\,(A_1(n) \to A_2(n)) \to \exists X\,\forall n \begin{cases} A_1(n) \to n \in X \\ n \in X \to A_2(n) \end{cases}$$

for $A_i(n) \in S_i$ (possibly with parameters).

- S-CA iff S-S-INTERPOL.
- S-SEP iff S-$\neg S$-INTERPOL where $\neg S := \{\neg A \mid A \in S\}$.

Summary again

System	*Characterization*
RCA_0	Δ^0_1-Δ^0_1-INTERPOL (i.e. Δ^0_1-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)

Summary again

System	*Characterization*
RCA_0	Π^0_1-Σ^0_1-INTERPOL (i.e. Π^0_1-SEP)
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)

Hierarchy of Interpolation: first-order (Simpson)

- Π^0_1-Σ^0_1-INTERPOL $\prec$ Σ^0_1-Π^0_1-INTERPOL $\prec$ Σ^0_1-Σ^0_1-INTERPOL.
- Σ^0_1-Σ^0_1-INTERPOL $=$ Σ^0_k-Σ^0_k-INTERPOL $=$ Π^0_k-Π^0_k-INTERPOL for all $k \geq 1$.
- Π^0_k-Σ^0_k-INTERPOL $=$ Σ^0_k-Π^0_k-INTERPOL $=$ Σ^0_k-Σ^0_k-INTERPOL for all $k > 1$.
- For $k > 0$, Π^0_k-Σ^0_k-INTERPOL, Σ^0_k-Π^0_k-INTERPOL, and Σ^0_k-Σ^0_k-INTERPOL is equivalent to one of RCA$_0$, WKL$_0$, or ACA$_0$.

Hierarchy of Interpolation: second-order (Simpson)

- Π^1_0-Σ^1_0-INTERPOL $=$ Σ^1_0-Π^1_0-INTERPOL $=$ Σ^1_0-Σ^1_0-INTERPOL $=$ Π^1_0-Π^1_0-INTERPOL $\prec$ Π^1_1-Σ^1_1-INTERPOL.
- Π^1_1-Σ^1_1-INTERPOL $\prec$ Σ^1_1-Π^1_1-INTERPOL $\prec$ Σ^1_1-Σ^1_1-INTERPOL $=$ Π^1_1-Π^1_1-INTERPOL $\prec$ Π^1_2-Σ^1_2-INTERPOL.
- Π^1_2-Σ^1_2-INTERPOL $\prec$ Σ^1_2-Π^1_2-INTERPOL $=$ Σ^1_2-Σ^1_2-INTERPOL $=$ Π^1_2-Π^1_2-INTERPOL.
- Σ^1_k-Σ^1_k-INTERPOL $=$ Π^1_k-Π^1_k-INTERPOL $\prec$ Π^1_{k+1}-Σ^1_{k+1}-INTERPOL $\preceq$ Σ^1_{k+1}-Σ^1_{k+1}-INTERPOL $=$ Π^1_{k+1}-Π^1_{k+1}-INTERPOL.
- Σ^1_k-Σ^1_k-INTERPOL $=$ Π^1_k-Π^1_k-INTERPOL $\prec$ Σ^1_{k+1}-Π^1_{k+1}-INTERPOL $\preceq$ Σ^1_{k+1}-Σ^1_{k+1}-INTERPOL $=$ Π^1_{k+1}-Π^1_{k+1}-INTERPOL.

Hierarchy of Interpolation: second-order (Simpson)

- $$\begin{aligned} \Delta^1_0\text{-CA} = \Sigma^1_0\text{-}\Sigma^1_0\text{-INTERPOL} &= \Pi^1_0\text{-}\Pi^1_0\text{-INTERPOL} \\ &\prec \Delta^1_{k+1}\text{-CA} \\ &\prec \Sigma^1_{k+1}\text{-}\Sigma^1_{k+1}\text{-INTERPOL} = \Pi^1_{k+1}\text{-}\Pi^1_{k+1}\text{-INTERPOL} \\ &\prec \Delta^1_{k+2}\text{-CA} \end{aligned}$$

- $$\begin{aligned} \Delta^1_2\text{-CA}_0 &= \Pi^1_2\text{-}\Sigma^1_2\text{-INTERPOL} \\ &\prec \Sigma^1_2\text{-}\Pi^1_2\text{-INTERPOL} \\ &= \Pi^1_2\text{-CA} = \Sigma^1_2\text{-}\Sigma^1_2\text{-INTERPOL} = \Pi^1_2\text{-}\Pi^1_2\text{-INTERPOL} \end{aligned}$$

Questions

- Δ^1_1-CA$_0$ $=$ Π^1_1-Σ^1_1-INTERPOL?
- Δ^1_{k+3}-CA$_0$ $=$ Π^1_{k+3}-Σ^1_{k+3}-INTERPOL?
- Π^1_{k+3}-Σ^1_{k+3}-INTERPOL $\preceq$ Σ^1_{k+3}-Π^1_{k+3}-INTERPOL, or even
- Π^1_{k+3}-Σ^1_{k+3}-INTERPOL $\prec$ Σ^1_{k+3}-Π^1_{k+3}-INTERPOL?

Questions

- Δ^1_1-CA$_0$ $=$ Π^1_1-Σ^1_1-INTERPOL? (No! by A. Montalbán, 2008)
- Δ^1_{k+3}-CA$_0$ $=$ Π^1_{k+3}-Σ^1_{k+3}-INTERPOL?
- Π^1_{k+3}-Σ^1_{k+3}-INTERPOL $\preceq$ Σ^1_{k+3}-Π^1_{k+3}-INTERPOL, or even
- Π^1_{k+3}-Σ^1_{k+3}-INTERPOL $\prec$ Σ^1_{k+3}-Π^1_{k+3}-INTERPOL?

Towards a computational meaning to the big five

- Comprehension S-CA has a standard computational interpretation resulting from skolemisation

$$\begin{array}{llll} \textit{formulas} & A & ::= & ... \\ \textit{sets} & P & ::= & X \mid \{n|A\} \end{array}$$

Comprehension rules

$$\frac{\Gamma \vdash A[t/n] \qquad A \in S}{\Gamma \vdash t \in \{n|A\}}\,\mathsf{Compr}_I \qquad \frac{\Gamma \vdash t \in \{n|A\} \qquad A \in S}{\Gamma \vdash A[t/n]}\,\mathsf{Compr}_E$$

Towards a computational meaning to the big five

- A similar approach can be taken for S_1-S_2-interpolation:

$$\begin{array}{llll} \textit{formulas} & A & ::= & \ldots \\ \textit{sets} & P & ::= & X \mid \{n|A \triangleright A\} \end{array}$$

Interpolation rules

$$\frac{\Gamma \vdash A_1[t/n] \qquad A_1 \in S_1}{\Gamma \vdash t \in \{n|A_1 \triangleright A_2\}}\ \text{Interpol}_I$$

$$\frac{\Gamma \vdash t \in \{n|A_1 \triangleright A_2\} \qquad A_2 \in S_2 \qquad \Gamma, A_1 \vdash A_2}{\Gamma \vdash A_2[t/n]}\ \text{Interpol}_E$$

The Resulting System (Syntax)

formulae	A, B, C	$::=$	$t \in P \mid t = t \mid \top \mid \bot \mid A \Rightarrow A \mid A \wedge A \mid A \vee A$
		$\mid$	$\forall n\, A \mid \exists n\, A \mid \forall X A \mid \exists X\, A$
sets	P	$::=$	$X \mid \{n \mid A \triangleright A\}$
terms	t, u	$::=$	$n \mid 0 \mid t + 1 \mid \texttt{rec}\ t\ \texttt{of}\ [t \mid (x, y).t]$
proofs	p, q	$::=$	$a \mid \iota_i(p) \mid (p_1, p_2) \mid (t, p) \mid (P, p) \mid \lambda a.p \mid \lambda x.p \mid \lambda X.p \mid ()$
		$\mid$	$p\, q \mid p\, t \mid p\, P \mid \texttt{absurd}\ p$
		$\mid$	$\texttt{case}\ p\ \texttt{of}\ [a_1.p_1 \mid a_2.p_2] \mid \pi_i\, p$
		$\mid$	$\texttt{dest}\ p\ \texttt{as}\ (x, a)\ \texttt{in}\ q \mid \texttt{dest}\ p\ \texttt{as}\ (X, a)\ \texttt{in}\ q$
		$\mid$	$\texttt{refl} \mid \texttt{subst}\, p\, q \mid \texttt{ind}\ t\ \texttt{of}\ [p \mid (x, a).q]$
		$\mid$	$\texttt{catch}_\alpha p \mid \texttt{throw}_\alpha p$
		$\mid$	$\texttt{interpol}\ p \mid \texttt{compose}\ p\ \texttt{as}\ a\ \texttt{in}\ q$

The Resulting System (Congruence)

- The congruence rules express Peano's axioms, generalising the axioms for $+$ and $\times$ into defining rules for a primitive recursion operator.

$$
\begin{array}{lcl}
\mathtt{rec}\ 0\ \mathtt{of}\ [t_0 \,|\, (x,y).t_S] & \to & t_0 \\
\mathtt{rec}\ t+1\ \mathtt{of}\ [t_0 \,|\, (x,y).t_S] & \to & t_S[t/x][\mathtt{rec}\ t\ \mathtt{of}\ [t_0 \,|\, (x,y).t_S]/y]
\end{array}
$$

$$
\begin{array}{lclcl}
0 & = & t+1 & \to & \bot \\
t+1 & = & 0 & \to & \bot \\
0 & = & 0 & \to & \top \\
t+1 & = & u+1 & \to & t = u
\end{array}
$$

The Resulting System (Inference rules, part 1)

$$\frac{(a : A) \in \Gamma}{\Gamma \vdash a : A}\text{AXIOM} \qquad \frac{\Gamma \vdash p : A \qquad A \equiv B}{\Gamma \vdash p : B}\text{CONV}$$

$$\frac{\Gamma \vdash p_1 : A_1 \qquad \Gamma \vdash p_2 : A_2}{\Gamma \vdash (p_1, p_2) : A_1 \wedge A_2}\wedge_I \qquad \frac{\Gamma \vdash p : A_1 \wedge A_2}{\Gamma \vdash \pi_i\, p : A_i}\wedge_E^o$$

$$\frac{\Gamma \vdash p : A_i}{\Gamma \vdash \iota_i(p) : A_1 \vee A_2}\vee_I^i \qquad \frac{\Gamma \vdash p : A_1 \vee A_2 \qquad \Gamma, a_1 : A_1 \vdash p_1 : B \qquad \Gamma, a_2 : A_2 \vdash p_2 : B}{\Gamma \vdash \texttt{case}\ p\ \texttt{of}\ [a_1.p_1 \mid a_2.p_2] : B}\vee_E$$

$$\frac{\Gamma, a : A \vdash p : B}{\Gamma \vdash \lambda a.p : A \Rightarrow B}\Rightarrow_I \qquad \frac{\Gamma \vdash p : A \Rightarrow B \qquad \Gamma \vdash q : A}{\Gamma \vdash p\, q : B}\Rightarrow_E$$

$$\frac{}{\Gamma \vdash () : \top}\top_I \qquad \frac{\Gamma \vdash p : \bot}{\Gamma \vdash \text{absurd}\ p : C}\bot_E$$

The Resulting System (Inference rules, part 2)

$$\frac{\Gamma \vdash p : A(x) \qquad x \text{ fresh}}{\Gamma \vdash \lambda x.p : \forall x\, A(x)}\forall_I \qquad \frac{\Gamma \vdash p : \forall x\, A(x)}{\Gamma \vdash p\, t : A(t)}\forall_E$$

$$\frac{\Gamma \vdash p : A(X) \qquad X \text{ fresh}}{\Gamma \vdash \lambda X.p : \forall X\, A(X)}\forall^2_I \qquad \frac{\Gamma \vdash P : \forall X\, A(X)}{\Gamma \vdash p\, P : A(P)}\forall^2_E$$

$$\frac{\Gamma \vdash p : A(t)}{\Gamma \vdash (t, p) : \exists x\, A(x)}\exists_I \qquad \frac{\Gamma \vdash p : \exists x\, A(x) \qquad \Gamma, a : A(x) \vdash q : B \qquad x \text{ fresh}}{\Gamma \vdash \mathtt{dest}\ p\ \mathtt{as}\ (x, a)\ \mathtt{in}\ q : B}\exists_E$$

$$\frac{\Gamma \vdash p : A(P)}{\Gamma \vdash (P, p) : \exists X\, A(X)}\exists^2_I \qquad \frac{\Gamma \vdash p : \exists X\, A(X) \qquad \Gamma, a : A(X) \vdash q : C \qquad X \text{ fresh}}{\Gamma \vdash \mathtt{dest}\ p\ \mathtt{as}\ (X, a)\ \mathtt{in}\ q : C}\exists^2_E$$

$$\frac{\Gamma, \alpha : T^{\perp\!\!\!\perp} \vdash p : T}{\Gamma \vdash \mathtt{catch}_\alpha\, p : T}\text{CATCH} \qquad \frac{\Gamma \vdash p : T \qquad (\alpha : T^{\perp\!\!\!\perp}) \in \Gamma}{\Gamma \vdash \mathtt{throw}_\alpha\, p : C}\text{THROW}$$

The Resulting System (Inference rules, part 3)

$$\frac{}{\Gamma \vdash \texttt{refl} : (t = t)}\text{REFL} \qquad \frac{\Gamma \vdash p : (t = u) \qquad \Gamma \vdash q : A[t/x]}{\Gamma \vdash \texttt{subst}\ p\ \texttt{in}\ q : A[u/x]}\text{SUBST}$$

$$\frac{\Gamma \vdash p : A(0) \qquad \Gamma, a : A(n) \vdash q : A(n+1) \qquad n \text{ fresh} \qquad A \in \Sigma^0_1}{\Gamma \vdash \texttt{ind}\ t\ \texttt{of}\ [p \mid (n, a).q] : A(t)}\text{IND}$$

$$\frac{\Gamma \vdash p : A_1[t/n] \qquad A_1 \in S_1}{\Gamma \vdash \texttt{interpol}\ p : (t \in \{n | A_1 \triangleright A_2\})}\text{INTERPOL}_I$$

$$\frac{\Gamma \vdash p : (t \in \{n | A_1 \triangleright A_2\}) \qquad A_2 \in S_2 \qquad \Gamma, a : A_1 \vdash q : A_2 \qquad n \text{ fresh}}{\Gamma \vdash \texttt{compose}\ p\ \texttt{as}\ a\ \texttt{in}\ q : A_2[t/n]}\text{INTERPOL}_E$$

The Resulting System

- The system is fully constructive.
- It is equipped with a normalisation procedure that we believe to be terminating (by adaptation of the normalisation of System F with interpolation replacing comprehension).
- We immediately obtain intuitionistic restrictions by dropping the rule for classical reasoning.
- We expect also that the intuitionistic restrictions prove similar Σ^0_1-formulas. (work in progress)

Contributions

- Cross-fertilization of computer science and reverse mathematics
  - What is the computational contents of the Big Five?
  - What results become different if intuitionistic logic or type theory is adopted instead?
  - What computability can say about reverse mathematics?