Intuitionistic provability and uniformly provability in RCA

Makoto Fujiwara

Mathematical Institute, Tohoku University

September 4, 2014

This work is supported by Grant-in-Aid for JSPS Fellows

Contents

1. Introduction.
2. Motivating Results.
3. Investigations.

Constructivity

- The notion of constructivity has been interested in foundation of mathematics.

Constructivity

- The notion of constructivity has been interested in foundation of mathematics.
- The first problem might be how to formulate constructivity in mathematics.

Constructivity

- The notion of constructivity has been interested in foundation of mathematics.
- The first problem might be how to formulate constructivity in mathematics.
- In this talk, we think of constructivity as (Turing) computational algorithm and show some equivalences between **global** and **local** constructive provability with respect to reverse mathematics.

Global Constructivity: Constructive Mathematics

Constructive mathematic was initiated mainly by L.E.J. Brouwer based on his philosophy in the disputation on foundation of mathematics in the early 20th century.

The following is an exposition from

"Douglas Bridges and Erik Palmgren, Constructive Mathematics, The Stanford Encyclopedia of Philosophy (Winter 2013 Edition)".

Constructive mathematics is distinguished from its traditional counterpart, classical mathematics, by the strict interpretation of the phrase "there exists" as "we can construct". In order to work constructively, we need to re-interpret not only the existential quantifier but all the logical connectives and quantifiers as instructions on how to construct a proof of the statement involving these logical expressions.

Intuitionistic Two-sorted Arithmetic

Intuitionistic two-sorted arithmetic EL introduced by A. S. Troelstra in 1970's is served as base theory formalizing constructive mathematics.

Intuitionistic Two-sorted Arithmetic

- As language, EL has two-sorted variables(for numbers and functions), 0, successor S, abstraction operators $\lambda x.$(only for numbers), a recuror R, function constants for all primitive recursive functions and equality $=$ for numbers.
- Terms of EL are defined in the usual manner.
- Axioms and rules of EL include
  - λ-CON: $(\lambda x.t)t' = t[t'/x]$
  - REC: $Rt\varphi 0 = 0$ and $Rt\varphi(St') = \varphi(Rt\varphi t', t')$
  - IND: $A(0) \wedge \forall x\,(A(x) \rightarrow A(Sx)) \rightarrow \forall x A(x)$
  - $\mathrm{QF\text{-}AC}^{0,0}$: $\forall x \exists y A_{qf}(x, y) \rightarrow \exists f \forall x A_{qf}(x, fx)$
- EL does not have the law-of-excluded-middle: $\mathrm{A} \vee \neg \mathrm{A}$.

Intuitionistic Two-sorted Arithmetic

- As language, EL has two-sorted variables(for numbers and functions), 0, successor S, abstraction operators $\lambda x.$(only for numbers), a recuror R, function constants for all primitive recursive functions and equality $=$ for numbers.
- Terms of EL are defined in the usual manner.
- Axioms and rules of EL include
  - λ-CON: $(\lambda x.t)t' = t[t'/x]$
  - REC: $Rt\varphi 0 = 0$ and $Rt\varphi(St') = \varphi(Rt\varphi t', t')$
  - IND: $A(0) \wedge \forall x\,(A(x) \to A(Sx)) \to \forall x A(x)$
  - $\mathrm{QF\text{-}AC}^{0,0}$: $\forall x \exists y A_{qf}(x, y) \to \exists f \forall x A_{qf}(x, fx)$
- EL does not have the law-of-excluded-middle: $\mathrm{A} \vee \neg \mathrm{A}$.

Remark.

$\mathrm{EL} \vdash A \vee B \leftrightarrow \exists k(k = 0 \to A \wedge k \neq 0 \to B)$.

Intuitionistic & Classical Systems

	Intuitionistic	Classical
One-sorted	HA	PA $(= \mathsf{HA} + \mathrm{LEM})$
Two-sorted	EL	
	EL_0	

Intuitionistic & Classical Systems

	Intuitionistic	Classical
One-sorted	HA	PA $(=$ HA $+ \mathrm{LEM})$
Two-sorted	EL	RCA $(=$ EL $+ \mathrm{LEM})$
	EL_0	RCA_0 $(= \mathsf{EL}_0 + \mathrm{LEM})$

- One can identify EL $+ \mathrm{LEM}$ with function-based language as RCA (RCA_0+full induction) with set-based language, since Δ^0_1-CA (by function-based language) is derived from QF-$\mathrm{AC}^{0,0}$ and LEM.
- One can identify EL_0(with QF-IND)+LEM as RCA_0, since Σ^0_1-IND is intuitionistically derived from QF-$\mathrm{AC}^{0,0}$ and QF-IND intuitionistically.

Intuitionistic & Classical Systems

	Intuitionistic	Classical
One-sorted	HA	PA $(= \mathsf{HA} + \mathrm{LEM})$
Two-sorted	EL	RCA $(= \mathsf{EL} + \mathrm{LEM})$
	EL_0	RCA_0 $(= \mathsf{EL}_0 + \mathrm{LEM})$

- One can identify $\mathsf{EL} + \mathrm{LEM}$ with function-based language as RCA (RCA_0+full induction) with set-based language, since Δ^0_1-CA (by function-based language) is derived from QF-$\mathrm{AC}^{0,0}$ and LEM.
- One can identify EL_0(with QF-IND)+LEM as RCA_0, since Σ^0_1-IND is intuitionistically derived from QF-$\mathrm{AC}^{0,0}$ and QF-IND intuitionistically.

Then we shall use the same notations RCA and RCA_0 respectively for $\mathsf{EL} + \mathrm{LEM}$ and $\mathsf{EL}_0 + \mathrm{LEM}$.

Local Constructivity for Mathematical Statements

Many mathematical statements have Π_2 form:

$$\forall X\,(A(X) \to \exists Y B(X,Y))\,.$$

Intermediate Value Theorem.

For any continuous function $f : [0,1] \to \mathbb{R}$ s.t. $f(0) < 0 < f(1)$, then there exists a point $m \in [0,1]$ s.t. $f(m) = 0$.

Local Constructivity for Mathematical Statements

Many mathematical statements have Π_2 form:

$$\forall X\,(A(X) \to \exists Y B(X, Y))\,.$$

Intermediate Value Theorem.

For any continuous function $f : [0, 1] \to \mathbb{R}$ s.t. $f(0) < 0 < f(1)$, then there exists a point $m \in [0, 1]$ s.t. $f(m) = 0$.

Sequential Version

- Many Π^1_2 statements are provable in RCA (even in RCA_0).

Sequential Version

- Many Π^1_2 statements are provable in RCA (even in RCA_0).
- In some of their proofs, however, the construction of the solution Y from given X is not uniform.

Sequential Version

- Many Π^1_2 statements are provable in RCA (even in RCA_0).
- In some of their proofs, however, the construction of the solution Y from given X is not uniform.
- To reveal the non-uniformity, the following sequential version has been investigated.

$$\forall \langle X_n \rangle_{n\in\mathbb{N}} \left(\forall n A(X_n) \to \exists \langle Y_n \rangle_{n\in\mathbb{N}} \forall n B(X_n, Y_n)\right).$$

Sequential Version

- Many Π^1_2 statements are provable in RCA (even in RCA_0).
- In some of their proofs, however, the construction of the solution Y from given X is not uniform.
- To reveal the non-uniformity, the following sequential version has been investigated.

$$\forall \langle X_n \rangle_{n\in\mathbb{N}} \left(\forall n A(X_n) \to \exists \langle Y_n \rangle_{n\in\mathbb{N}} \forall n B(X_n, Y_n) \right).$$

Examples.

	Pointwise	Sequential
JD (The existence of Jordan decomposition for real square matrices)	RCA	ACA
RT^1 (Infinite pigeonhole principle)	RCA	ACA
IVT (Intermediate value theorem)	RCA	WKL
TET (Tietze extension theorem)	RCA	RCA

Contents

In this 10 years, it had been found that the law-of-excluded-middle(LEM) has an arithmetical hierarchy (over intuitionistic system like EL) as in reverse mathematics.

$$
\begin{tikzcd}
 & \Sigma^0_1\text{-LEM} \arrow[ddl] \arrow[dr] & \\
 & & \Pi^0_1\text{-LEM} \arrow[dd] \\
\mathrm{M}^0 \arrow[ddr] & & \\
 & & \Sigma^0_1\text{-DML} \arrow[dl] \\
 & \Pi^0_1\text{-DML} &
\end{tikzcd}
$$

- $\mathrm{M}^0:\ \neg\neg\exists x A_{qf} \rightarrow \exists x A_{qf}$
- $\Sigma^0_1\text{-LEM}:\ \exists x A_{qf} \vee \neg\exists x A_{qf}$
- $\Sigma^0_1\text{-DML}:\ \neg(\exists x A_{qf} \wedge \exists y B_{qf}) \rightarrow (\neg\exists x A_{qf} \vee \neg\exists y B_{qf})$

In this 10 years, it had been found that the law-of-excluded-middle(LEM) has an arithmetical hierarchy (over intuitionistic system like EL) as in reverse mathematics.

$$
\begin{tikzcd}
 & \Sigma^0_1\text{-LEM} \arrow[dl] \arrow[dr] & \\
\mathrm{M}^0 \arrow[ddr] & & \Pi^0_1\text{-LEM} \arrow[d] \\
 & & \Sigma^0_1\text{-DML} \arrow[dl] \\
 & \Pi^0_1\text{-DML} &
\end{tikzcd}
$$

- M^0 : $\neg\neg\exists x A_{qf} \rightarrow \exists x A_{qf}$
- $\Sigma^0_1\text{-LEM}$: $\exists x A_{qf} \vee \neg\exists x A_{qf}$
- $\Sigma^0_1\text{-DML}$: $\neg(\exists x A_{qf} \wedge \exists y B_{qf}) \rightarrow (\neg\exists x A_{qf} \vee \neg\exists y B_{qf})$

Recently, constructive reverse mathematic, which classify mathematical principles by that hierarchy, has been carried out.

Constructive and Sequential Reverse Mathematics

There are some corresponding results between constructive and sequential reverse mathematics.

Constructive and Sequential Reverse Mathematics

There are some corresponding results between constructive and sequential reverse mathematics.

- $\mathrm{TRIC} : \forall\alpha \in \mathbb{R}\,(\alpha < 0 \lor \alpha = 0 \lor \alpha > 0)$.
- $\mathrm{DIC} : \forall\alpha \in \mathbb{R}\,(\alpha \leq 0 \lor \alpha \geq 0)$.

Fact.

Over EL,

- $\mathrm{TRIC} \leftrightarrow \Sigma^0_1\text{-LEM}$.
- $\mathrm{DIC} \leftrightarrow \Sigma^0_1\text{-DML}$.

Fact.

Over RCA,

- $\mathrm{Seq}(\mathrm{TRIC}) \leftrightarrow \mathrm{ACA}$.
- $\mathrm{Seq}(\mathrm{DIC}) \leftrightarrow \mathrm{WKL}$.

Constructive and Sequential Reverse Mathematics

There are some corresponding results between constructive and sequential reverse mathematics.

- $\mathrm{TRIC} : \forall \alpha \in \mathbb{R}\, (\alpha < 0 \vee \alpha = 0 \vee \alpha > 0)$.
- $\mathrm{DIC} : \forall \alpha \in \mathbb{R}\, (\alpha \leq 0 \vee \alpha \geq 0)$.

Fact.

Over EL,

- $\mathrm{TRIC} \leftrightarrow \Sigma^0_1\text{-LEM}$.
- $\mathrm{DIC} \leftrightarrow \Sigma^0_1\text{-DML}$.

Fact.

Over RCA,

- $\mathrm{Seq}(\mathrm{TRIC}) \leftrightarrow \mathrm{ACA}$.
- $\mathrm{Seq}(\mathrm{DIC}) \leftrightarrow \mathrm{WKL}$.

Proposition. (Ishihara 2005)

- $\mathrm{EL} \vdash \mathrm{ACA} \leftrightarrow \Sigma^0_1\text{-LEM} + \Pi^0_1\text{-AC}^{0,0}$.
- $\mathrm{EL} \vdash \mathrm{WKL} \leftrightarrow \Sigma^0_1\text{-DML} + \Pi^0_1\text{-AC}^{\vee}$.

Contents

Let us consider a Π^1_2 statement

$$\forall X^1 \left(A(X) \to \exists Y^1 B(X, Y)\right).$$

- Its provability in RCA corresponds to Y is Muchnik reducible to X, i.e. for all X satisfying $A(X)$, there is a program Φ of Turing machine with oracle s.t. Φ^X compute Y satisfying $B(X, Y)$

Let us consider a Π^1_2 statement

$$\forall X^1 \left(A(X) \to \exists Y^1 B(X, Y) \right).$$

- Its provability in RCA corresponds to Y is Muchnik reducible to X, i.e. for all X satisfying $A(X)$, there is a program Φ of Turing machine with oracle s.t. Φ^X compute Y satisfying $B(X, Y)$
- On the other hand, what one intend to represent by its sequential provability in RCA is that Y is Medvedev reducible to X, i.e. there is a uniform program Φ of Turing machine with oracle s.t. for all X satisfying $A(X)$, Φ^X compute Y satisfying $B(X, Y)$

Let us consider a Π^1_2 statement

$$\forall X^1\left(A(X) \to \exists Y^1 B(X,Y)\right).$$

- Its provability in RCA corresponds to Y is Muchnik reducible to X, i.e. for all X satisfying $A(X)$, there is a program Φ of Turing machine with oracle s.t. Φ^X compute Y satisfying $B(X,Y)$
- On the other hand, what one intend to represent by its sequential provability in RCA is that Y is Medvedev reducible to X, i.e. there is a uniform program Φ of Turing machine with oracle s.t. for all X satisfying $A(X)$, Φ^X compute Y satisfying $B(X,Y)$

Thus, if its sequential version derives WKL or ACA, then there is no uniform program Φ of Turing machine with oracle s.t. for all X satisfying $A(X)$, Φ^X compute Y satisfying $B(X,Y)$

By the way, what is the formal representation to capture precisely the uniform provability in RCA?

Two candidates;

By the way, what is the formal representation to capture precisely the uniform provability in RCA?

Two candidates;

1. There exists a (primitive recursive) term t^1 of RCA s.t.

$$\mathsf{RCA} \vdash \forall X\,(A(X) \to t|X\downarrow \wedge B(X, t|X))\,,$$

where $|$ is the partial continuous operation from $\mathbb{N}^{\mathbb{N}}$ to $\mathbb{N}^{\mathbb{N}}$.

By the way, what is the formal representation to capture precisely the uniform provability in RCA?

Two candidates;

1. There exists a (primitive recursive) term t^1 of RCA s.t.

$$\mathsf{RCA} \vdash \forall X\,(A(X) \to t|X\downarrow \wedge B(X, t|X)),$$

   where $|$ is the partial continuous operation from $\mathbb{N}^{\mathbb{N}}$ to $\mathbb{N}^{\mathbb{N}}$.

2. There exists a (Gödel primitive recursive) term $t^{1\to 1}$ of RCA^{ω} s.t.

$$\mathsf{RCA}^{\omega} \vdash \forall X\,(A(X) \to B(X, tX)),$$

   where $\mathsf{RCA}^{\omega} (:= \mathsf{E\text{-}HA}^{\omega} + \mathrm{QF\text{-}AC}^{1,0} + \mathrm{LEM})$ is a conservative extension of RCA in all finite types.

By the way, what is the formal representation to capture precisely the uniform provability in RCA?

Two candidates;

1. There exists a (primitive recursive) term t^1 of RCA s.t.

$$\mathrm{RCA} \vdash \forall X\,(A(X) \to t|X\downarrow \wedge B(X, t|X)),$$

   where $|$ is the partial continuous operation from $\mathbb{N}^{\mathbb{N}}$ to $\mathbb{N}^{\mathbb{N}}$.
2. There exists a (Gödel primitive recursive) term $t^{1\to 1}$ of RCA^ω s.t.

$$\mathrm{RCA}^\omega \vdash \forall X\,(A(X) \to B(X, tX)),$$

   where $\mathrm{RCA}^\omega (:= \text{E-HA}^\omega + \mathrm{QF\text{-}AC}^{1,0} + \mathrm{LEM})$ is a conservative extension of RCA in all finite types.

Remark: Both of them imply sequential provability in RCA.

Kleene's Partial Continuous Operation

We use a partial operation $(\cdot)(\cdot) : \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}} \to \mathbb{N}$ to define $| : \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}} \to \mathbb{N}^{\mathbb{N}}$.

For $\alpha, \beta : \mathbb{N} \to \mathbb{N}$,

$$\alpha(\beta) := \begin{cases} \alpha(\bar{\beta} n) - 1 \text{ where n is the least } n' \text{ s.t. } \alpha(\bar{\beta} n') \neq 0. \\ \uparrow \text{ if there is no such } n'. \end{cases}$$

Then

$$\alpha | \beta := \lambda n.\ \alpha(\langle n \rangle ^\frown \beta).$$

Proposition. (Dorais 2014, via Realizability interpretation)

If $\mathsf{EL} + \mathrm{M}^0 \vdash \forall X^1 \, (A(X) \to \exists Y^1 B(X, Y))$, then there exists a term t^1 s.t.

$$\mathsf{EL} \text{ (hence } \mathsf{RCA}) \vdash \forall X \, (A(X) \to t|X \downarrow \wedge B(X, t|X)) \, ,$$

provided that $A(X) \in \mathrm{N_K}$ and $B(X, Y) \in \mathrm{L_K}$.

Proposition. (Dorais 2014, via Realizability interpretation)

If $\mathrm{EL} + \mathrm{M}^0 \vdash \forall X^1 (A(X) \to \exists Y^1 B(X, Y))$, then there exists a term t^1 s.t.

$$\mathrm{EL}\ (\text{hence RCA}) \vdash \forall X \left(A(X) \to t|X\downarrow \wedge B(X, t|X)\right),$$

provided that $A(X) \in \mathrm{N_K}$ and $B(X, Y) \in \mathrm{L_K}$.

- $\mathrm{N_K}$ is the class of formulas defined inductively as;
  - $\mathrm{A_{qf}}$, $\exists x^\rho \mathrm{A_{qf}}$ are in $\mathrm{N_K}$.
  - If $\mathrm{A_1}, \mathrm{A_2}$ are in $\mathrm{N_K}$, then $\mathrm{A_1} \wedge \mathrm{A_2}$, $\mathrm{A_1} \to \mathrm{A_2}$, $\forall \mathrm{x}^\rho \mathrm{A_1}$ are in $\mathrm{N_K}$.
- $\mathrm{L_K}$ is the class of formulas defined inductively as;
  - $\mathrm{A_{qf}}$ is in $\mathrm{L_K}$.
  - If $\mathrm{A_1}, \mathrm{A_2}$ are in $\mathrm{L_K}$, then $\mathrm{A_1} \wedge \mathrm{A_2}$, $\forall \mathrm{x}^\rho \mathrm{A_1}$ and $\exists \mathrm{x}^\rho \mathrm{A_1}$ are in $\mathrm{L_K}$.
  - If $\mathrm{A_1}$ is in $\mathrm{N_K}$ and $\mathrm{A_2}$ is in $\mathrm{L_K}$, then $\mathrm{A_1} \to \mathrm{A_2}$ is in $\mathrm{L_K}$.

Corollary.

If EL $+ \mathrm{M}^0 \vdash \forall X^1 (A(X) \to \exists Y^1 B(X, Y))$, then

$$\mathsf{RCA} \vdash \forall \langle X_n \rangle_{n \in \mathbb{N}} (\forall n A(X_n) \to \exists \langle Y_n \rangle_{n \in \mathbb{N}} \forall n B(X_n, Y_n))\,.$$

provided that $A(X) \in \mathrm{N_K}$ and $B(X, Y) \in \mathrm{L_K}$.

Corollary.

If $\mathsf{EL} + \mathrm{M}^0 \vdash \forall X^1 (A(X) \to \exists Y^1 B(X, Y))$, then

$$\mathsf{RCA} \vdash \forall \langle X_n \rangle_{n\in\mathbb{N}} (\forall n A(X_n) \to \exists \langle Y_n \rangle_{n\in\mathbb{N}} \forall n B(X_n, Y_n)) .$$

provided that $A(X) \in \mathrm{N_K}$ and $B(X, Y) \in \mathrm{L_K}$.

Remark. (Yokoyama-F. 2013)

The class $\mathrm{N_K}$ for A cannot be extended to involve $\exists u^0 \forall v^0 A_{qf}$ in the previous proposition.

Theorem.

If there exists a term t^1 s.t.

$$\mathsf{RCA} \vdash \forall X^1 \left(A(X) \to t|X \downarrow \wedge B(X, t|X) \right),$$

then

$$\mathsf{EL} + \mathrm{M}^0 \vdash \forall X \left(A(X) \to \exists Y B(X, Y) \right),$$

provided that $A(X) \in \mathrm{N_M}$ and $B(X, Y)$ is equivalent to some formula $\forall w^\rho \exists s^0 B_{qf}(X, Y, w, s)$ over $\mathsf{EL} + \mathrm{M}^0$.

- $\mathrm{N_M}$ is the class of formulas defined inductively as;
  - $\mathrm{A_{qf}}$ is in $\mathrm{N_M}$.
  - If $\mathrm{A_1}, \mathrm{A_2}$ are in $\mathrm{N_M}$, then $\mathrm{A_1} \wedge \mathrm{A_2}$, $\mathrm{A_1} \vee \mathrm{A_2}$, $\forall \mathrm{x}^\rho \mathrm{A_1}$, $\exists \mathrm{x}^\rho \mathrm{A_1}$ are in $\mathrm{N_M}$.
  - If A is in $\mathrm{N_M}$, then $\forall u^\rho \exists v^0 \mathrm{A_{qf}} \to \mathrm{A}$ is in $\mathrm{N_M}$.

Negative Translation

To show this theorem, we use the following negative translation.

Definition. (Kuroda 1951)

A^N is defined as $A^N :\equiv \neg\neg A^*$, where A^* is defined by induction on the logical structure of A:

- $A^* :\equiv A$, if A is a prime formula,
- $(A \Box B)^* :\equiv (A^* \Box B^*)$, where $\Box \in \{\wedge, \vee, \rightarrow\}$,
- $(\exists x^\rho A)^* :\equiv \exists x^\rho A^*$,
- $(\forall x^\rho A)^* :\equiv \forall x^\rho \neg\neg A^*$.

Example.

- $\mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)$:
  $(\forall u^0 A_{qf} \to \exists x^0 B_{qf}) \to \exists x^0 \, (\forall u^0 A_{qf} \to B_{qf})$
  where A_{qf} does not contain x free.

Example.

- $\mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)$:
  $(\forall u^0 A_{qf} \to \exists x^0 B_{qf}) \to \exists x^0 \, (\forall u^0 A_{qf} \to B_{qf})$
  where A_{qf} does not contain x free.

$$\mathrm{IP}(\Pi^0_1, \Sigma^0_0)^N \equiv \neg\neg \left(\begin{array}{l} (\forall u \neg\neg A_{qf} \to \exists x B_{qf}) \\ \to \exists x \, (\forall u \neg\neg A_{qf} \to B_{qf}) \end{array} \right),$$

Example.

- $\mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)$:
  $(\forall u^0 A_{qf} \to \exists x^0 B_{qf}) \to \exists x^0 \, (\forall u^0 A_{qf} \to B_{qf})$
  where A_{qf} does not contain x free.

$$\mathrm{IP}(\Pi^0_1, \Sigma^0_0)^N \equiv \neg\neg \left(\begin{array}{l} (\forall u \neg\neg A_{qf} \to \exists x B_{qf}) \\ \to \exists x \, (\forall u \neg\neg A_{qf} \to B_{qf}) \end{array} \right),$$

which is intuitionistically equivalent to

$$(\forall u A_{qf} \to \exists x B_{qf}) \to \neg\neg\exists x \, (\forall u A_{qf} \to B_{qf}) \, .$$

Lemma.

If RCA $\vdash A$, then EL $+ \mathrm{M}^0 \vdash A^N$.

Idea of Proof.
Induction on the length of the derivation. It is enough to check all the axioms and rules of RCA. Actually M^0 is used only to derive $(\mathrm{QF\text{-}AC}^{0,0})^N$ intuitionistically from $\mathrm{QF\text{-}AC}^{0,0}$. □

Lemma.

If RCA $\vdash A$, then EL $+ \mathrm{M}^0 \vdash A^N$.

Idea of Proof.
Induction on the length of the derivation. It is enough to check all the axioms and rules of RCA. Actually M^0 is used only to derive $(\mathrm{QF\text{-}AC}^{0,0})^N$ intuitionistically from $\mathrm{QF\text{-}AC}^{0,0}$. $\square$

Fact.

EL $+ \mathrm{M}^0 \vdash \mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)$.

Lemma.

If RCA $\vdash A$, then EL $+ \mathrm{M}^0 \vdash A^N$.

Idea of Proof.
Induction on the length of the derivation. It is enough to check all the axioms and rules of RCA. Actually M^0 is used only to derive $(\mathrm{QF\text{-}AC}^{0,0})^N$ intuitionistically from $\mathrm{QF\text{-}AC}^{0,0}$. □

Fact.

EL $+ \mathrm{M}^0 \vdash \mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)$.

Proof.

$$\begin{array}{ll} & \mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)^N \\ \to_i & (\forall u A_{qf} \to \exists x B_{qf}) \to \neg\neg\exists x\, (\forall u A_{qf} \to B_{qf}) \end{array}$$

Lemma.

If RCA $\vdash A$, then EL $+ \mathrm{M}^0 \vdash A^N$.

Idea of Proof.
Induction on the length of the derivation. It is enough to check all the axioms and rules of RCA. Actually M^0 is used only to derive $(\mathrm{QF\text{-}AC}^{0,0})^N$ intuitionistically from $\mathrm{QF\text{-}AC}^{0,0}$. □

Fact.

EL $+ \mathrm{M}^0 \vdash \mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)$.

Proof.

$$
\begin{array}{ll}
 & \mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)^N \\
\to_i & (\forall u A_{qf} \to \exists x B_{qf}) \to \neg\neg\exists x\, (\forall u A_{qf} \to B_{qf}) \\
\to_{\text{using } \mathrm{M}^0} & (\forall u A_{qf} \to \exists x B_{qf}) \to \neg\neg\exists x, u\, (A_{qf} \to B_{qf})
\end{array}
$$

Lemma.

If RCA $\vdash A$, then EL $+ \mathrm{M}^0 \vdash A^N$.

Idea of Proof.
Induction on the length of the derivation. It is enough to check all the axioms and rules of RCA. Actually M^0 is used only to derive $(\mathrm{QF\text{-}AC}^{0,0})^N$ intuitionistically from $\mathrm{QF\text{-}AC}^{0,0}$. □

Fact.

EL $+ \mathrm{M}^0 \vdash \mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)$.

Proof.

$$
\begin{array}{ll}
 & \mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)^N \\
\to_i & (\forall u A_{qf} \to \exists x B_{qf}) \to \neg\neg\exists x\,(\forall u A_{qf} \to B_{qf}) \\
\to_{\text{using } \mathrm{M}^0} & (\forall u A_{qf} \to \exists x B_{qf}) \to \neg\neg\exists x, u\,(A_{qf} \to B_{qf}) \\
\to_{\text{using } \mathrm{M}^0} & (\forall u A_{qf} \to \exists x B_{qf}) \to \exists x, u\,(A_{qf} \to B_{qf})
\end{array}
$$

Lemma.

If RCA $\vdash A$, then EL $+ \mathrm{M}^0 \vdash A^N$.

Idea of Proof.
Induction on the length of the derivation. It is enough to check all the axioms and rules of RCA. Actually M^0 is used only to derive $(\mathrm{QF\text{-}AC}^{0,0})^N$ intuitionistically from $\mathrm{QF\text{-}AC}^{0,0}$. □

Fact.

EL $+ \mathrm{M}^0 \vdash \mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)$.

Proof.

$$
\begin{array}{ll}
 & \mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)^N \\
\to_i & (\forall u A_{qf} \to \exists x B_{qf}) \to \neg\neg\exists x\, (\forall u A_{qf} \to B_{qf}) \\
\to_{\text{using } \mathrm{M}^0} & (\forall u A_{qf} \to \exists x B_{qf}) \to \neg\neg\exists x, u\, (A_{qf} \to B_{qf}) \\
\to_{\text{using } \mathrm{M}^0} & (\forall u A_{qf} \to \exists x B_{qf}) \to \exists x, u\, (A_{qf} \to B_{qf}) \\
\to_i & (\forall u A_{qf} \to \exists x B_{qf}) \to \exists x\, (\forall u A_{qf} \to B_{qf}).
\end{array}
$$

□

Lemma.

For any formula $A \in \mathrm{N_M}$, $\mathsf{EL} + \mathrm{M_0} \vdash A \to A^*$.

Proof is by induction on the structure of $\mathrm{N_M}$.

- $\mathrm{N_M}$ is the class of formulas defined inductively as;
  - $\mathrm{A_{qf}}$ is in $\mathrm{N_M}$.
  - If $\mathrm{A_1}, \mathrm{A_2}$ are in $\mathrm{N_M}$, then $\mathrm{A_1} \wedge \mathrm{A_2}$, $\mathrm{A_1} \vee \mathrm{A_2}$, $\forall \mathrm{x}^\rho \mathrm{A_1}$, $\exists \mathrm{x}^\rho \mathrm{A_1}$ are in $\mathrm{N_M}$.
  - If A is in $\mathrm{N_M}$, then $\forall u^\rho \exists v^0 \mathrm{A_{qf}} \to \mathrm{A}$ is in $\mathrm{N_M}$.

Theorem.

If there exists a term t^1 s.t.

$$\mathsf{RCA} \vdash \forall X^1 \left(A(X) \to t|X \downarrow \wedge B(X, t|X) \right),$$

then

$$\mathsf{EL} + \mathrm{M}^0 \vdash \forall X \left(A(X) \to \exists Y B(X, Y) \right),$$

provided that $A(X) \in \mathrm{N}_{\mathrm{M}}$ and $B(X, Y)$ is equivalent to some formula $\forall w^\rho \exists s^0 B_{qf}(X, Y, w, s)$ over $\mathsf{EL} + \mathrm{M}^0$.

Proof Sketch.

Theorem.

If there exists a term t^1 s.t.

$$\mathsf{RCA} \vdash \forall X^1 \left(A(X) \to t|X \downarrow \wedge B(X, t|X)\right),$$

then

$$\mathsf{EL} + \mathrm{M}^0 \vdash \forall X \left(A(X) \to \exists Y B(X, Y)\right),$$

provided that $A(X) \in \mathrm{N_M}$ and $B(X, Y)$ is equivalent to some formula $\forall w^\rho \exists s^0 B_{qf}(X, Y, w, s)$ over $\mathsf{EL} + \mathrm{M}^0$.

Proof Sketch.

By negative translation, we have that $\mathsf{EL} + \mathrm{M}^0$ derives

$$\forall X^1 \left(A^*(X) \to \neg\neg \left(t|X \downarrow\right)^* \wedge \neg\neg\left(\forall w \exists s B_{qf}(X, t|X, w, s)\right)^*\right).$$

By the previous lemma and multiple use of M^0, one obtain that

$$\mathsf{EL} + \mathrm{M}^0 \vdash \forall X^1 \left(A(X) \to t|X \downarrow \wedge B(X, t|X)\right).$$

Therefore $\mathsf{EL} + \mathrm{M}^0 \vdash \forall X \left(A(X) \to \exists Y B(X, Y)\right)$. $\square$

Combining the theorem with Dorais's result, we have the following.

Combining the theorem with Dorais's result, we have the following.

Proposition.

There exists a term t^1 s.t.

$$\mathsf{RCA} \vdash \forall X^1 \left(A(X) \to t|X\downarrow \wedge B(X, t|X)\right)$$

if and only if

$$\mathsf{EL} + \mathrm{M}^0 \vdash \forall X \left(A(X) \to \exists Y B(X, Y)\right),$$

provided that $A(X) \in \mathrm{N}_{\mathrm{KM}}$ and $B(X, Y)$ is equivalent to some formula $\forall w^\rho \exists s^0 B_{qf}(X, Y, w, s)$ over $\mathsf{EL} + \mathrm{M}^0$.

- N_{KM} is the class of formulas defined inductively as;
  - A_{qf} and $\exists \mathrm{x}^\rho \mathrm{A}_{\mathrm{qf}}$ are in N_{KM}.
  - If $\mathrm{A}_1, \mathrm{A}_2$ are in N_{KM}, then $\mathrm{A}_1 \wedge \mathrm{A}_2$, $\forall \mathrm{x}^\rho \mathrm{A}_1$ are in N_{KM}.
  - If A is in N_{KM}, then $\forall u^\rho \exists v^0 \mathrm{A}_{\mathrm{qf}} \to \mathrm{A}$ is in N_{KM}.

On the Syntactical Restriction

- Annoying feature of Intuitonistic systems is lack of the following properties.
  - $(A \rightarrow \exists x B) \rightarrow \exists x\,(A \rightarrow B)$.
  - $(\forall x A \rightarrow B) \rightarrow \exists x\,(A \rightarrow B)$.

On the Syntactical Restriction

- Annoying feature of Intuitonistic systems is lack of the following properties.
  - $(A \to \exists x B) \to \exists x\,(A \to B)$.
  - $(\forall x A \to B) \to \exists x\,(A \to B)$.
- However, under the M^0, one can intuitionistically show the followings.
  - $\mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)$:
    $\left(\forall u^0 A_{qf} \to \exists x^0 B_{qf}\right) \to \exists x^0 \left(\forall u^0 A_{qf} \to B_{qf}\right)$.
  - $\left(\exists x^0 A_{qf} \to B_{qf}\right) \to \exists x^0 \left(A_{qf} \to B_{qf}\right)$.

On the Syntactical Restriction

- Annoying feature of Intuitonistic systems is lack of the following properties.
  - $(A \to \exists x B) \to \exists x\,(A \to B)$.
  - $(\forall x A \to B) \to \exists x\,(A \to B)$.
- However, under the M^0, one can intuitionistically show the followings.
  - $\mathrm{IP}^0(\Pi^0_1, \Sigma^0_0)$:
    $\left(\forall u^0 A_{qf} \to \exists x^0 B_{qf}\right) \to \exists x^0 \left(\forall u^0 A_{qf} \to B_{qf}\right)$.
  - $\left(\exists x^0 A_{qf} \to B_{qf}\right) \to \exists x^0 \left(A_{qf} \to B_{qf}\right)$.

$\Rightarrow$ Our proposition seems to be applicable to a lot of mathematical statements.

Proposition (Hirst-Mummert 2011, via Modified Realizability Interpretation)

If $\mathsf{E\text{-}HA}^\omega + \mathrm{AC} \vdash \forall X^1 \left(A(X) \to \exists Y^1 B(X, Y)\right)$,
then there exists a term $t^{1\to1}$ s.t.

$$\mathsf{E\text{-}HA}^\omega \vdash \forall X \left(A(X) \to B(X, tX)\right),$$

provided that $A(X)$ is existential-free and $B(X, Y) \in \Gamma_1$ where Γ_1 is the class of formulas defined inductively as;

- $\mathrm{A_{qf}}$ is in Γ_1.
- If $\mathrm{A_1}, \mathrm{A_2}$ are in $\mathrm{L_K}$, then $\mathrm{A_1} \wedge \mathrm{A_2}$, $\forall \mathrm{x} \mathrm{A_1}$ and $\exists \mathrm{x} \mathrm{A_1}$ are in Γ_1.
- If $\mathrm{A_1}$ is existential-free and $\mathrm{A_2}$ is in Γ_1, then $\mathrm{A_1} \to \mathrm{A_2}$ is in Γ_1.

Corollary.

If $\mathsf{EL} \vdash \forall X\,(A(X) \to \exists Y B(X,Y))$,
then there exists a term $t^{1\to 1}$ of RCA^{ω} s.t.

$$\mathsf{RCA}^{\omega} \vdash \forall X\,(A(X) \to B(X, tX))\,,$$

provided that $A(X)$ is existential-free and $B(X,Y) \in \Gamma_1$.

Theorem.

If there exists a term $t^{1\to 1}$ of RCA^ω s.t.

$$\mathrm{RCA}^\omega \vdash \forall X\,(A(X) \to B(X, tX))\,,$$

then

$$\mathrm{EL} \vdash \forall X\,(A(X) \to \exists Y B(X, Y))\,,$$

provided that $A(X)$ is purely universal and $B(X, Y)$ is equivalent to some formula $\forall w^\rho \exists s^0 B_{qf}(X, Y, w, s)$ over EL.

Theorem.

If there exists a term $t^{1\to 1}$ of RCA^ω s.t.

$$\mathsf{RCA}^\omega \vdash \forall X\,(A(X) \to B(X, tX))\,,$$

then

$$\mathsf{EL} \vdash \forall X\,(A(X) \to \exists Y B(X, Y))\,,$$

provided that $A(X)$ is purely universal and $B(X, Y)$ is equivalent to some formula $\forall w^\rho \exists s^0 B_{qf}(X, Y, w, s)$ over EL.

Proof Sketch.

As in the previous theorem, by negative translation, we have

$$\mathsf{E\text{-}HA}^\omega + \mathrm{QF\text{-}AC}^{1,0} + \mathrm{M}^0 \vdash \forall X\,(A(X) \to \exists Y B(X, Y))\,.$$

By using elimination of extensionality and Dialectica interpretation, we obtain

$$\mathsf{WE\text{-}HA}^\omega \vdash \forall X\,(A(X) \to \exists Y B(X, Y))\,.$$

The conclusion follows from the conservatively of $\mathsf{WE\text{-}HA}^\omega$. $\square$

Combining the theorem with Hirst-Mummert's result, we have the following.

Combining the theorem with Hirst-Mummert's result, we have the following.

Proposition.

There exists a term $t^{1\to 1}$ of RCA^ω s.t.

$$\mathrm{RCA}^\omega \vdash \forall X\,(A(X) \to B(X, tX))$$

if and only if

$$\mathrm{EL} \vdash \forall X\,(A(X) \to \exists Y B(X, Y)),$$

provided that $A(X)$ is purely universal and $B(X, Y)$ is equivalent to some formula $\forall w^\rho \exists s^0 B_{qf}(X, Y, w, s)$ over EL.

Remarks

1. Our two propositions express that in ω structures, for practical Π_2 statements, intuitionistic (or constructive recursive) provability is identical with the existence of a uniform algorithm obtaining the witness from the problem and its verification is done in computable mathematics with classical logic.

Remarks

1. Our two propositions express that in ω structures, for practical Π_2 statements, intuitionistic (or constructive recursive) provability is identical with the existence of a uniform algorithm obtaining the witness from the problem and its verification is done in computable mathematics with classical logic.
2. One can show the versants of our two propositions where RCA^ω and EL are replaced by RCA_0^ω and EL_0 respectvely in the same manner. (Note that term $t^{1\to 1}$ of RCA_0^ω is a primitive recursive functional in the sense of Kleene.)

Remarks

1. Our two propositions express that in ω structures, for practical Π_2 statements, intuitionistic (or constructive recursive) provability is identical with the existence of a uniform algorithm obtaining the witness from the problem and its verification is done in computable mathematics with classical logic.
2. One can show the versants of our two propositions where RCA^ω and EL are replaced by RCA_0^ω and EL_0 respectvely in the same manner. (Note that term $t^{1\to1}$ of RCA_0^ω is a primitive recursive functional in the sense of Kleene.)
3. All proofs of our propositions are syntactic (just translating formal proofs inductively).

Remarks

1. Our two propositions express that in ω structures, for practical Π_2 statements, intuitionistic (or constructive recursive) provability is identical with the existence of a uniform algorithm obtaining the witness from the problem and its verification is done in computable mathematics with classical logic.
2. One can show the versants of our two propositions where RCA^ω and EL are replaced by RCA_0^ω and EL_0 respectvely in the same manner. (Note that term $t^{1\to 1}$ of RCA_0^ω is a primitive recursive functional in the sense of Kleene.)
3. All proofs of our propositions are syntactic (just translating formal proofs inductively).
4. One might obtain this kind of results also for $\mathsf{RCA} + \mathrm{WKL}$.

References

- F. G. Dorais, Classical consequences of continuous choice principles from intuitionistic analysis, Notre Dame Journal of Formal Logic, 55 (2014), pp. 25-39.
- J. L. Hirst and C. Mummert, Reverse mathematics and uniformity in proofs without excluded middle, Notre Dame J. Form. Log. 52 (2011), no. 2, 149-162.

All of the proof theoretic techniques used for our results are developed in the following books.

- A. S. Troelstra, Metamathematical Investigation of Intuitionistic Arithmetic and Analysis, 1973.
- U. Kohlenbach, Applied Proof Theory: Proof Interpretations and their Use in Mathematics, 2008.

Remark. (Yokoyama-F. 2013)

The class $\mathrm{N_K}$ for A cannot be extended to involve $\exists u^0 \forall v^0 A_{qf}$ in the previous proposition.

Proof.

There is a simple counterexample B:
$\forall X\,(X$ is finite $\to \exists Y$ s.t. its upper bound is in $Y)$.

B is a statement of form $\forall X\,(\exists u \forall v A_{qf}(X) \to \exists Y B(X, Y))$ s.t.

- it is provable in EL.
- its strong sequential version:
  $\forall \langle X_n \rangle_{n\in\mathbb{N}}\,(\forall n \exists u \forall v A_{qf}(X_n, u, v) \to \exists \langle Y_n \rangle_{n\in\mathbb{N}} \forall n B(X_n, Y_n))$
  implies ACA over RCA.

$\square$

Remark. (Yokoyama-F. 2013)

The class $\mathrm{N_K}$ for A cannot be extended to involve $\exists u^0 \forall v^0 A_{qf}$ in the previous proposition.

Proof.

There is a simple counterexample B:
$\forall X\,(X$ is finite $\rightarrow \exists Y$ s.t. its upper bound is in Y).

B is a statement of form $\forall X\,(\exists u \forall v A_{qf}(X) \rightarrow \exists Y B(X,Y))$ s.t.

- it is provable in EL.
- its strong sequential version:
  $\forall \langle X_n \rangle_{n\in\mathbb{N}}\,(\forall n \exists u \forall v A_{qf}(X_n, u, v) \rightarrow \exists \langle Y_n \rangle_{n\in\mathbb{N}} \forall n B(X_n, Y_n))$
  implies ACA over RCA.

□

Remark: Its weak sequential version:
$\forall \langle X_n \rangle_{n\in\mathbb{N}} \forall \langle u_n \rangle_{n\in\mathbb{N}}\,(\forall n \forall v A_{qf}(X_n, u_n, v) \rightarrow \exists \langle Y_n \rangle_{n\in\mathbb{N}} \forall n B(X_n, Y_n))$
is trivially provable in RCA.