Reverse mathematics and uniformity in proofs without excluded middle

Jeffry L. Hirst
jlh@math.appstate.edu

Carl Mummert
mummertcb@appstate.edu

Appalachian State University

Submitted for publication: 5/3/2006

Abstract

We prove that if a \( \Pi^1_2 \) sentence is provable in a certain theory of higher order arithmetic without the law of the excluded middle then it is uniformly provable in the weak classical theory \( \text{RCA}_0 \). Applying the contrapositive of this result, we give three examples where results of reverse mathematics can be used to show nonexistence of proofs in certain intuitionistic systems.

1 Introduction

We study the proof theory of subsystems of second-order arithmetic. In Section 2, we give the definition of the subsystem of intuitionistic second-order arithmetic known as \( \text{HA}^\# \). This subsystem extends the fragment of constructive analysis captured by \( \text{HA}^\omega + AC \), which is essentially Heyting arithmetic in all finite types with a choice scheme for arbitrary formulas. We prove the following theorem relating provability in \( \text{HA}^\# \) with uniform provability in \( \text{RCA}_0 \). The minimal \( \omega \)-model of \( \text{RCA}_0 \) contains only computable sets, so \( \text{RCA}_0 \) may be viewed as a formalization of computable analysis.

Main Theorem. If \( \text{HA}^\# \) proves a \( \Pi^1_2 \) statement of the form \( \forall A \exists B \Theta(A, B) \), where \( \Theta \) is arithmetical, then the uniformized statement

\[
\forall \langle A_n \mid n \in \mathbb{N} \rangle \exists \langle B_n \mid n \in \mathbb{N} \rangle \forall n \Theta(A_n, B_n)
\]

is provable in \( \text{RCA}_0 \).
The proof uses a variation of the *Dialectica* method of Gödel, which is a well-known tool in proof theory. We have attempted to make Section 2 accessible to a general reader familiar with mathematical logic but possibly not familiar with the *Dialectica* method.

In Section 3, we present several theorems of core mathematics that are provable in $\text{RCA}_0$ but not in $\text{HA}^\#$. A reader who is willing to accept the Main Theorem should be able to skip Section 2 and proceed directly to this section.

We would like to thank Jeremy Avigad for helpful comments on these results. We began this work during a summer school on proof theory taught by Jeremy Avigad and Henry Townser at Notre Dame in 2005. We wish to thank Peter Cholak for his role in organizing the summer school.

## 2 Proof of the main theorem

In this section, we prove Theorem 2.5, our main result linking fragments of constructive and computable analysis. The proof uses Gödel’s *Dialectica* interpretation. We begin by defining the associated axiom systems and then turn to the interpretation itself.

Our definitions make use of the following type notation. The type of a natural number is 0. The type of a functional from objects of type $\rho$ to objects of type $\tau$ is $\rho \rightarrow \tau$. For example, the type of a function from numbers to numbers is $0 \rightarrow 0$. We identify the type $0 \rightarrow 0$ with 1, and in general identify the type $n \rightarrow 0$ with $n + 1$. Consequently, a functional mapping type 1 functions to numbers is assigned the type 2. We will often write superscripts on quantified variables to indicate their type.

The axiom systems we will use are all modifications of $\text{E-PRA}^\omega$. Here we are adopting Kohlenbach’s notation from [3] in which $\text{E-PRA}^\omega$ is the same as the theory $\tilde{\text{T}}$ of Avigad and Feferman [1]. In particular, $\text{E-PRA}^\omega$ consists of $\text{E-PA}^\omega$ (Peano arithmetic in all finite types with the extensionality axioms described below) with induction restricted to quantifier-free formulas and primitive recursion restricted to type 0 functionals with parameters. This theory includes equality as a primitive relation only for type 0 objects (natural numbers). The added extensionality axioms consist of the scheme

$$E: \forall \rho \forall \sigma \forall \eta \forall \tau \forall x \forall y \forall z \rho \rightarrow \sigma \rightarrow \tau \rightarrow (x =_\rho y \rightarrow z(x) =_\tau z(y)),$$

which defines equality for higher types in terms of equality for lower types. $\text{E-PRA}^\omega$ also includes projection and substitution combinators (denoted by $\Pi_{\rho,\tau}$ and $\Sigma_{\delta,\rho,\tau}$ in [3]), which allow terms to be defined using $\lambda$ abstraction.
For example, given \( x \in \mathbb{N} \) and an argument list \( t \), \( \text{E-PRA}^{\omega} \) includes a term for \( \lambda t.x \), the constant function with value \( x \). More details on \( \text{E-PRA}^{\omega} \) may be found in [3].

The axiom system \( \text{RCA}_0^{\omega} \) consists of \( \text{E-PRA}^{\omega} \) plus the choice scheme

\[
\text{QF-AC}^{1,0}: \forall x^1 \exists y^0 \Phi(x, y) \rightarrow \exists Y^1 \forall x^1 \Phi(x, Y(x)),
\]

where \( \Phi \) is a quantifier-free formula. We will capitalize on the fact that \( \text{RCA}_0^{\omega} \) is conservative over \( \text{RCA}_0 \), as proved in Proposition 3.1 of [3]. The familiar axiomatization of \( \text{RCA}_0 \) (as in [6]) uses the language \( L_2 \) with a membership relation. An alternative, functional axiomatization known as \( \text{RCA}_2^0 \) uses a language that includes function notation but no membership relation. Each of the theories \( \text{RCA}_0 \) and \( \text{RCA}_2^0 \) is included in a canonical definitional extension of the other theory. In this section, we use the functional variant \( \text{RCA}_2^0 \) for convenience, knowing that our results apply equally to \( \text{RCA}_0 \) via this definitional extension.

The underlying predicate calculus for the preceding systems is that of classical logic, as axiomatized on pages 341–342 of [1]. Omitting the law of the excluded middle yields intuitionistic predicate calculus. Restricting \( \text{E-PRA}^{\omega} \) to intuitionistic predicate calculus yields restricted Heyting arithmetic, the system \( \tilde{\text{HA}}^{\omega} \) of [1]. The system \( \tilde{\text{HA}}^\# \) of [1] consists of \( \tilde{\text{HA}}^{\omega} \) plus the following schemes for all formulas \( \Phi \) and \( \Psi \):

\[
\text{AC}: \forall x \exists y \Phi(x, y) \rightarrow \exists Y \forall x \Phi(x, Y(x)),
\]

\[
\text{IP}': (\forall y \Phi \rightarrow \exists u \forall v \Psi) \rightarrow \exists u (\forall y \Phi \rightarrow \forall v \Psi),
\]

\[
\text{MP}': \neg \forall y \Phi \rightarrow \exists y \neg \Phi .
\]

Thus \( \tilde{\text{HA}}^\# \) is a nonconstructive extension of the fragment of constructive analysis formalized by \( \tilde{\text{HA}}^{\omega} + \text{AC} \). Note that the full theory of second-order arithmetic is obtained if the law of the excluded middle is added to \( \tilde{\text{HA}}^\# \), because the scheme AC for arbitrary \( L_2 \) formulas is classically equivalent to the full comprehension scheme.

Extended discussions of Gödel’s Dialectica interpretation can be found in [1] and [7]. The interpretation assigns to each formula \( \Phi \) a formula \( \Phi^D \) of the form \( \exists x \forall y \Phi_D \), where \( \Phi_D \) is quantifier free and each quantifier may represent a block of quantifiers of the same kind. The blocks of quantifiers in \( \Phi^D \) may include variables of any finite type. We follow [1] in defining the Dialectica interpretation inductively by the following six clauses, in which \( \Phi^D = \exists x \forall y \Phi_D \) and \( \Psi^D = \exists u \forall v \Psi_D \).
(1) If \( \Phi \) is an atomic formula then \( x \) and \( y \) are both empty and \( \Phi^D = \Phi \).

(2) \((\Phi \land \Psi)^D = \exists x \exists y (\Phi_D \land \Psi_D)\).

(3) \((\Phi \lor \Psi)^D = \exists z \exists x \exists y (\Phi_D \land (z = 0 \land \Psi_D) \lor (z = 1 \land \Psi_D))\).

(4) \((\forall z \Phi(z))^D = \exists X \forall z \forall y \Phi_D(X(z), y, z)\).

(5) \((\exists z \Phi(z))^D = \exists z \exists x \forall y \Phi_D(x, y, z)\).

(6) \((\Phi \rightarrow \Psi)^D = \exists U \forall x (\Phi_D(x, Y(x, v)) \rightarrow \Psi_D(U(x), v))\).

The negation \( \neg \Phi \) is treated as an abbreviation of \( \Phi \rightarrow \bot \).

Suppose that \( \Phi \) is arithmetical, and thus contains only type 0 (number) quantifiers. If clauses (4) or (6) are applied in determining \( \Phi^D \), then \( \Phi^D \) may contain quantifiers of higher types. Because \( \Phi \) is arithmetical, these new types will be of the form \( \tau \rightarrow 0 \) for some \( \tau \). Thus the variables denoted by upper-case letters in clauses (4) and (6) represent integer-valued functionals. If \( \Phi \) is not arithmetical then this conclusion may not hold.

Gödel’s theorem on the Dialectica interpretation states that if \( \widetilde{HA}^# \vdash \Phi \) then \( E\text{-PRA}^\omega \vdash \Phi^D \). This is sometimes abbreviated as: \( \widetilde{HA}^# \) is \( D \)-interpreted in \( E\text{-PRA}^\omega \). This result is proved as Theorem 5.1.3 of [1], where \( E\text{-PRA}^\omega \) is denoted \( T \). The following theorem follows immediately, because \( \text{RCA}_0^\omega \) extends \( E\text{-PRA}^\omega \).

**Theorem 2.1.** If \( \Phi \) is a formula in the language of arithmetic and \( \widetilde{HA}^# \vdash \Phi \), then \( \text{RCA}_0^\omega \vdash \Phi^D \). In proof theoretic terminology, \( \widetilde{HA}^# \) is \( D \)-interpreted in \( \text{RCA}_0^\omega \).

Eventually, we will need to show that if \( \Phi \) is arithmetical, then \( \text{RCA}_0^\omega \) proves \( \Phi^D \rightarrow \Phi \). Both [1] and [7] give proofs of the biconditional \( \Phi^D \leftrightarrow \Phi \), but these proofs necessarily use the choice scheme \( AC \), which is not available in \( \text{RCA}_0^\omega \). However, \( \text{RCA}_0^\omega \) does suffice to prove that if \( \Phi \) is arithmetical then \( \Phi^D \) is equivalent to a canonically determined sentence containing only type 1 and type 0 variables. We denote this sentence by \( \Phi^S \) and call it the \( \Sigma_1^1 \) reduct of the arithmetical formula \( \Phi \). The definition of \( \Phi^S \) parallels the definition of \( \Phi^D \). In particular, \( \Phi^S = \exists x^1 \forall y^0 \Phi_D \), where \( \Phi_D \) is the same quantifier-free formula used in defining \( \Phi^D \). (We are now abusing notation and using \( \exists x^1 \) to denote a block of quantifiers that may include variables of type 1, type 0, or both.) The \( \Sigma_1^1 \) reduct is defined inductively by the following six clauses, in which \( \Phi^S = \exists x^1 \forall y^0 \Phi_D \) and \( \Psi^S = \exists u^1 \forall v^0 \Psi_D \).
(1) If $\Phi$ an atomic formula then $x$ and $y$ are both empty and $\Phi^S = \Phi_D = \Phi$.

(2) $(\Phi \land \Psi)^S = \exists x^1 \exists u^1 \forall y^0 \forall v^0 (\Phi_D \land \Psi_D)$.

(3) $(\Phi \lor \Psi)^S = \exists z^0 \exists x^1 \exists u^0 \forall y^0 ((z = 0 \land \Phi_D) \lor (z = 1 \land \Psi_D))$.

(4) $(\forall z \Phi(z))^S = \exists x^1 \forall z^0 \forall y^0 \Phi_D(x(y, z), y, z)$.

(5) $(\exists z \Phi(z))^S = \exists z^0 \exists x^1 \forall y^0 \Phi_D(x(y), y, z)$.

(6) $(\Phi \rightarrow \Psi)^S = \exists u^1 \exists y^1 \forall x^0 \forall v^0 ((\Phi_D(x, y(x, v)) \rightarrow \Psi_D(u(x, v), v))$.

Naïvely, the *Dialectica* interpretation $\Phi^D$ is a Skolem prenex form of $\Phi$ with functionals replacing some Skolem functions and possible additional constructive information encoded. (The additional constructive information includes the $z$ variable in clause (3).) When $\Phi$ is arithmetical, the functionals of $\Phi^D$ carry no information beyond that of type 1 Skolem functions. Consequently, RCA$_0^\omega$ can prove that $\Phi^D$ is equivalent to the $\Sigma_1^1$ reduct $\Phi^S$, as shown in the following lemma.

**Lemma 2.2.** Suppose $\Phi$ is arithmetical. Then $\text{RCA}_0^\omega \vdash \Phi^D \leftrightarrow \Phi^S$.

**Proof.** The proof proceeds by induction on formula complexity, addressing each clause in the definitions of the *Dialectica* interpretation and the $\Sigma_1^1$ reduct. For atomic formulas, $\Phi^D$ is $\Phi^S$. For the remaining clauses, suppose:

$$
\Phi^D = \exists X \forall Y \Phi_D(X(Y), Y),
$$

$$
\Phi^S = \exists x^1 \forall y^0 \Phi_D(x(y), y),
$$

$$
\Psi^D = \exists U \forall V \Psi_D(U(V), V),
$$

$$
\Psi^S = \exists u^1 \forall v^0 \Psi_D(u(v), v).
$$

Because $\Phi$ and $\Psi$ are arithmetical, the functionals $X$, $Y$, $U$, and $V$ are integer valued. Working in RCA$_0^\omega$, we will assume that $\Phi^D \leftrightarrow \Phi^S$ and $\Psi^D \leftrightarrow \Psi^S$, and prove the equivalence of the formulas defined by the remaining clauses. Equivalence of the *Dialectica* and reduct formulas resulting from clauses (2), (3), or (5) follows from the induction hypothesis and classical predicate calculus. This also holds for clause (4) with one caveat. Our restriction to arithmetical formulas ensures that the new quantified variable $z$ is of type 0, and so $(\forall z^0 \Phi(z))^S$ follows from $\Phi^S$. Clause (6) requires a more extended discussion.

Suppose that $\Upsilon$ is $\Phi \rightarrow \Psi$, where $\Phi$ and $\Psi$ are as above. Then we have:

$$
\Upsilon^D = \exists U \exists Y \forall X \forall V (\Phi_D(X(Y(X, V)), Y(X, V)) \rightarrow \Psi_D(U(X, V), V)),
$$

$$
\Upsilon^S = \exists u^1 \exists y^1 \forall x^0 \forall v^0 ((\Phi_D(x, y(x, v)) \rightarrow \Psi_D(u(x, v), v)).
Our goal is to prove $\Upsilon^S \leftrightarrow \Upsilon^D$, working in $\mathsf{RCA}_0^\omega$.

To prove that $\Upsilon^D \rightarrow \Upsilon^S$, assume $\Upsilon^D$. Then we can find functionals $U_0$ and $Y_0$ such that

$$\forall X \forall V (\Phi_D(X(Y_0(X,V)), Y_0(X,V)) \rightarrow \Psi_D(U_0(X,V), V)).$$

Here $X$ and $V$ are integer valued functionals. Let $t$ denote the argument list of $X$ and $s$ the argument list of $V$. Then for any $x, v \in \mathbb{N}$, we may substitute $\lambda t.x$ for $X$ and $\lambda s.v$ for $V$, yielding

$$\Phi_D(\lambda t.x, Y_0(\lambda t.x, \lambda s.v)) \rightarrow \Psi_D(U_0(\lambda t.x, \lambda s.v), \lambda s.v)).$$

Defining $y(x, v) = Y_0(\lambda t.x, \lambda s.v)$ and $u(x, v) = U_0(\lambda t.x, \lambda s.v)$, substitution yields $\Phi_D(x, y(x, v)) \rightarrow \Psi_D(u(x, v), v)$. Note that $y$ and $u$ are functions from $\mathbb{N}$ to $\mathbb{N}$ and so are type 1. Restoring the quantifiers, we have shown that $\exists y \exists u \forall x \forall v (\Phi_D(x, y(x, v)) \rightarrow \Psi_D(u(x, v), v))$, so $\Upsilon^S$ follows from $\Upsilon^D$.

We will prove that $\Upsilon^S \rightarrow \Upsilon^D$ by assuming $\Upsilon^S$ and considering two cases. For the first case, suppose $\Phi^D$, that is, $\exists X \forall Y \Phi_D(X(Y), Y)$. Instantiating $X$ as $X_0$ in $\Phi^D$ yields $\forall Y \Phi_D(X_0(Y), Y)$. Since $Y$ is an integer valued functional, for each integer $y$ we have $\Phi_D(X_0(\lambda t.y), \lambda t.y)$. Defining the type 1 function $\tilde{X}(y) = X_0(\lambda t.y)$ and generalizing yields $\forall y \Phi_D(\tilde{X}(y), y)$. Turning to $\Upsilon^S$, instantiating $u$ and $y$ as $u_0$ and $y_0$ and letting $x$ be free yields

$$\forall u \forall y (\Phi_D(x, y_0(x, v)) \rightarrow \Psi_D(u_0(x, v), v)). \tag{1}$$

Treating $x$ as a parameter, $y_0$ and $u_0$ depend only on $v$, so we may write $\forall u \forall y (\Phi_D(x, y_0(v)) \rightarrow \Psi_D(u_0(v), v))$. Since $u_0$ and $y_0$ are type 1 functions, the composition $\tilde{X}(y_0(v))$ is integer valued. Substituting it for $x$ in equation (1) yields

$$\forall u \forall y (\Phi_D(\tilde{X}(y_0(v)), y_0(v)) \rightarrow \Psi_D(u_0(v), v)). \tag{2}$$

As noted above, we have $\forall y \Phi_D(\tilde{X}(y), y)$, so $\Phi_D(\tilde{X}(y_0(v)), y_0(v))$ holds for every $v$. From equation (2) we may deduce $\forall u \forall y \Phi_D(\tilde{X}(y_0(v)), y_0(v))$. For each integer valued functional $V$, define $U(X, V) = u_0(V)$. Then for all $X$ and $V$, $\Psi_D(U(X, V), V)$ holds and $\Upsilon^D$ follows, regardless of the choice of the functional $Y$. In summary, $\Upsilon^S$ implies $\Upsilon^D$ when $\Phi^D$ holds.

For the second case, suppose $\neg \Phi^D$. By the induction hypothesis we have $\Phi^D \rightarrow \Phi^S$, so $\neg \Phi^S$ holds also. Thus we have $\forall x \exists y \neg \Phi_D(x(y), y)$. Recall that $\neg \Phi^D$ is $\forall X \exists Y \neg \Phi_D(X(Y), Y)$, and choose an arbitrary functional $X$ of the type in $\Phi^D$. Since $Y$ is integer valued, we can define a type 1 functional $x$ such that $x(y) = X(\lambda t.y)$ for every $y \in \mathbb{N}$. By $\neg \Phi^S$, $\exists y \neg \Phi_D(x(y), y)$, so $\exists y \neg \Phi_D(X(\lambda t.y), y)$. For any choice of $X$ and $V$, define $Y(X,V)$ by
$Y(X, V) = \mu m(\neg \Phi_D(X(\lambda t.m), m))$. Informally, $Y(X, V)$ is computable, so $\text{RCA}_0^\omega$ proves its existence. More formally, one proves that $Y(X, V)$ exists by applying $\text{QF-AC}^{1,0}$ to the formula $\forall x^1 \exists y^0 (\neg \Phi(x(y), y) \land \forall z < y \Phi(x(z), z))$. Given the function $Y(X, V)$, we may verify that for all $X$ and $V$ the formula $\neg \Phi_D(X(Y(X, V)), Y(X, V))$ holds, and that $\Upsilon^D$ follows, regardless of the choice of the functional $U$. In summary, $\Upsilon^S$ implies $\Upsilon^D$ when $\neg \Phi^D$ holds.

We have shown that if $\Phi^D$ holds or $\neg \Phi^D$ holds then $\Upsilon^S \rightarrow \Upsilon^D$ follows. By the law of the excluded middle (which is included in $\text{RCA}_0$), we can conclude that $\Upsilon^S \rightarrow \Upsilon^D$. Combining this with the previously proven converse, we see that $\Upsilon^S \Leftrightarrow \Upsilon^D$ whenever $\Upsilon$ is the result of an application of clause (6). This completes our induction on formula complexity and the proof. 

Lemma 2.3. Suppose $\Theta$ is arithmetical. Then $\text{RCA}_0^\omega \vdash \Theta^D \rightarrow \Theta$.

Proof. In light of Lemma 2.2, it suffices to show that if $\Theta$ is arithmetical then $\Theta^S \rightarrow \Theta$. This is provable in classical predicate calculus. First note that if $\Phi^S = \exists x^1 \forall y^0 \Phi_D$ and $\Psi^S = \exists u^1 \forall v^0 \Psi_D$ then

$$(\Phi \lor \Psi)^S = \exists z^0 \exists x^1 \exists u^1 \forall v^0 \forall v^0 ((z = 0 \land \Phi_D) \lor (z = 1 \land \Psi_D)).$$

Classical predicate calculus proves that $(\Phi \lor \Psi)^S$ implies $\exists x^1 \exists u^1 \forall v^0 \forall v^0 (\Phi_D \lor \Psi_D)$. Thus, given any formula $\Theta^S$, we can derive the variant $\Theta'$ that results from replacing the disjuncts in $\Theta^S$ with this weaker form. The variant $\Theta'$ is a Skolem prenex form of $\Theta$ that can be shown to imply $\Theta$ by means of predicate calculus alone. 

If $\Phi$ is of the form $\forall x^1 \exists y^1 \Theta(x, y)$ where $\Theta$ is arithmetical (so $\Phi$ is $\Pi_1^1$ in the terminology of [6]), then the uniformization of $\Phi$ is denoted by $\Phi^U$ and defined by

$$\Phi^U = \forall(X_n | n \in \mathbb{N}) \exists(Y_n | n \in \mathbb{N}) \forall n \Theta(X_n, Y_n).$$

Since we may view sequences of sets as objects of type $0 \rightarrow 1$, we could also write the uniformization as $\forall x^0 \exists y^0 \forall n^0 \Theta(x(n), y(n))$. The next lemma relates the Dialectica interpretation of a formula to its uniformization.

Lemma 2.4. If the formula $\Phi$ is $\forall x^1 \exists y^1 \Theta$ where $\Theta$ is arithmetical then $\text{RCA}_0^\omega \vdash \Phi^D \rightarrow \Phi^U$.

Proof. Suppose $\Phi$ is as in the hypothesis of the lemma. We will work in $\text{RCA}_0^\omega$. Write the Dialectica interpretation of $\Theta$ as $\Theta^D = \exists u \forall v \Theta_D(u, v, x, y)$, where $\Theta_D$ is quantifier free, $x$ and $y$ are type 1, and $u$ and $v$ are integer valued.
functionals or integers. Then from the definition of the Dialectica interpretation, \( \Phi^D \) is \( \exists y^{1-1} \exists u x^1 \forall v \Theta_D(u(x), v, x, y(x)) \). (Note that y is not type 1, which is to be expected because \( \Phi \) is not arithmetical.) By instantiating the existential quantifiers, we obtain \( \forall x^1 \forall v \Theta_D(u_0(x), v, x, y_0(x)) \). If we view a sequence of sets \( \langle X_n \mid n \in \mathbb{N} \rangle \) as a functional of type \( 0 \to 1 \) then by composition the sequence (functional) \( \langle y_0(X_n) \mid n \in \mathbb{N} \rangle \) exists. Consequently, we have

\[
\forall n \forall v \Theta_D(u_0(X_n), v, X_n, y_0(X_n)). \tag{3}
\]

Now \( (\forall n \Theta(X_n, y_0(X_n)))^D \) is \( \exists \hat{u} \forall n \forall v \Theta_D(\hat{u}(n), v, X_n, y_0(X_n)) \), which may be derived from equation (3) by defining \( \hat{u} \) by \( \hat{u}(n) = u_0(X_n) \). Since we have proved \( (\forall n \Theta(X_n, y_0(X_n)))^D \), by an application of Lemma 2.3 the non-Dialectica form \( \forall n \Theta(X_n, y_0(X_n)) \) follows. Summarizing, we have shown that for any sequence \( \langle X_n \mid n \in \mathbb{N} \rangle \) there is a sequence \( \langle Y_n \mid n \in \mathbb{N} \rangle = \langle y_0(X_n) \mid n \in \mathbb{N} \rangle \) such that \( \forall n \Theta(X_n, Y_n) \). Restoring quantifiers yields

\[
\forall \langle X_n \mid n \in \mathbb{N} \rangle \exists \langle Y_n \mid n \in \mathbb{N} \rangle \forall n \Theta(X_n, Y_n),
\]

which is the uniformization \( \Phi^U \).

We now prove the main theorem from the introduction. Informally, it says that if we can prove a \( \Pi^1_1 \) statement without using the law of the excluded middle then we can prove it uniformly in a fragment of computable analysis.

**Theorem 2.5.** Suppose \( \Theta \) is arithmetical and \( \Phi \) is \( \forall x^1 \exists y^1 \Theta \). If \( \text{HA}^\# \vdash \Phi \) then \( \text{RCA}_0 \vdash \Phi^U \).

**Proof.** Suppose \( \Phi \) is as described and that \( \text{HA}^\# \vdash \Phi \). By Theorem 2.1, \( \text{RCA}_0^\# \vdash \Phi^D \). By Lemma 2.4, \( \text{RCA}_0^\# \vdash \Phi^U \). By Proposition 3.1 of [3], \( \text{RCA}_0^\# \vdash \Phi^U \). Since \( \text{RCA}_0^\# \) is a definitional extension of \( \text{RCA}_0 \), \( \text{RCA}_0 \vdash \Phi^U \). In this last translation from \( \text{RCA}_0 \) to \( \text{RCA}_0^\# \), we are suppressing the translation from a purely functional axiomatization to the axiomatization in terms of sets traditionally used in reverse mathematics. \( \square \)

Theorem 2.5 is in some sense analogous to the well-known characterization of the provably total functions of the first-order theory \( \Sigma^0_1\text{-IND} \), which consists of first-order arithmetic with only \( \Sigma^0_1 \) induction. It is known that if a sentence of the form \( \forall n \exists m \theta(n, m) \) is provable in \( \Sigma^0_1\text{-IND} \), where \( \theta \) is \( \Sigma^0_1 \), then there is a primitive recursive function term \( t \) such that \( \forall n \theta(n, t(n)) \) is provable in primitive recursive arithmetic. It follows from the proof of Theorem 2.5 that if \( \text{HA}^\# \) proves a sentence of the form \( \forall A \exists B \Theta(A, B) \),
where Θ is arithmetical, then RCA₀^2 proves there is a functional T such that ∀A Θ(A, T(B)). This functional need not be primitive recursive.

It appears that Theorem 2.5 can be proved for extensions of our axiom systems, provided that the Dialectica interpretation of each axiom of the extension of HA^# can be proved in the extension of RCA₀^ω. Rather than address extensions in this paper, we will turn to applications of Theorem 2.5 and its contrapositive.

3 Applications of the main theorem

In this section, we consider several theorems of core mathematics that are provable in RCA₀ but have uniformized versions that are not provable in RCA₀. In light of the Main Theorem, such results are not provable in HA^#.

Recall that RCA₀ is the subsystem of classical second-order arithmetic containing the Δ₁⁰ comprehension scheme and the Σ₀¹ induction scheme, and is typically used as a weak base system in the program of reverse mathematics. Simpson [6] gives a complete account of the parts of classical mathematics that can be developed in RCA₀.

The terminology in the following theorem is well known; we give formal definitions as needed later in the section.

**Theorem 3.1.** Each of the following statements is provable in RCA₀ but not provable in HA^#.

1. Every 2 × 2 matrix has a Jordan decomposition.

2. Every quickly converging Cauchy sequence of rational numbers can be converted to a Dedekind cut representing the same real number.

3. Every enumerated filter on a countable poset can be extended to an unbounded enumerated filter.

We show that each statement (3.1.1)–(3.1.3) is provable in RCA₀ but not HA^# by showing that the uniformization of each statement implies a stronger subsystem over RCA₀. The Main Theorem shows that this is sufficient. The stronger subsystems include WKL₀ and ACA₀. The theory WKL₀ appends a weak form of König’s lemma to the axioms of RCA₀, while ACA₀ appends comprehension for sets defined by arithmetical formulas. We remark that there are many other statements that are provable in RCA₀ but not HA^#; we have chosen these three to illustrate the what we believe to be the ubiquity of this phenomenon in various branches of core mathematics.
We begin with statement (3.1.1). We consider only finite square matrices whose entries are complex numbers represented by quickly converging Cauchy sequences. In $\text{RCA}_0$, we say that a matrix $M$ has a Jordan decomposition if there are matrices $(U, J)$ such that $M = UJU^{-1}$ and $J$ is a matrix consisting of Jordan blocks. We call $J$ the Jordan canonical form of $M$.

**Lemma 3.2.** $\text{RCA}_0$ proves that every $2 \times 2$ matrix has a Jordan decomposition.

**Proof.** Let $M$ be a $2 \times 2$ matrix. $\text{RCA}_0$ proves that the eigenvalues of $M$ exist and that for each eigenvalue there is an eigenvector. (Compare Exercise II.4.11 of [6], in which Simpson notes that the basics of linear algebra, including fundamental properties of Gaussian elimination, are provable in $\text{RCA}_0$.) If the eigenvalues of $M$ are distinct then the Jordan decomposition is trivial to compute from the eigenvalues and eigenvectors. If there is a unique eigenvalue and there are two linearly independent eigenvectors then the Jordan decomposition is similarly trivial to compute.

Suppose that $M$ has a unique eigenvalue $\lambda$ but not two linearly independent eigenvectors. Let $u$ be any eigenvector and let $\{u, v\}$ be a basis. It follows that $(M - \lambda I)v = au + bv$ is nonzero. Now $(M - \lambda I)(au + bv) = b(M - \lambda I)v$ since $u$ is an eigenvector of $M$ with eigenvalue $\lambda$. This shows $(M - \lambda I)$ has eigenvalue $b$, which can only happen if $b = 0$, that is, if $(M - \lambda I)v$ is a scalar multiple of $u$. Thus $\{u, v\}$ is a chain of generalized eigenvectors of $M$; the Jordan decomposition can be computed directly from this chain. \qed

It is not difficult to see that the previous proof makes use of the law of the excluded middle.

**Remark 3.3.** Proofs similar to that of Lemma 3.2 can be used to show that for each standard natural number $n$ the principle that every $n \times n$ matrix has a Jordan decomposition is provable in $\text{RCA}_0$. We do not know whether the principle that every finite matrix has a Jordan decomposition is provable in $\text{RCA}_0$.

The next lemma is foreshadowed by previous research. It is well known that the function that sends a matrix to its Jordan decomposition is discontinuous. Kohlenbach [3] has shown that, in the extension $\text{RCA}_0^\omega$ of $\text{RCA}_0$ to all finite types, the existence of a higher-type object encoding a non-sequentially-continuous real-valued function is equivalent to the corresponding type extension of $\text{ACA}_0$. 

10
Lemma 3.4. The following principle implies ACA₀ over RCA₀: For every sequence \(\langle M_i \mid i \in \mathbb{N} \rangle\) of \(2 \times 2\) real matrices, such that each matrix \(M_i\) has only real eigenvalues, there are sequences \(\langle U_i \mid i \in \mathbb{N} \rangle\) and \(\langle J_i \mid i \in \mathbb{N} \rangle\) such that \(\langle U_i, J_i \rangle\) is a Jordan decomposition of \(M_i\) for all \(i \in \mathbb{N}\).

Proof. We first demonstrate a concrete example of the discontinuity of the Jordan form. For any real \(z\), let \(M(z)\) denote the matrix

\[
M(z) = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}.
\]

The matrix \(M(0)\) is the identity matrix, and so is its Jordan canonical form. If \(z \neq 0\) then \(M(z)\) has the following Jordan decomposition:

\[
M(z) = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ z & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ z & 0 \end{pmatrix}^{-1}.
\]

The crucial fact is that the entry in the upper-right-hand corner of the Jordan canonical form of \(M(z)\) is 0 if \(z = 0\) and 1 if \(z \neq 0\).

Let \(h\) be an arbitrary function from \(\mathbb{N}\) to \(\mathbb{N}\). We will assume the principle of the theorem and show that the range of \(h\) exists. It is well known that RCA₀ can construct a function \(n \mapsto z_n\) that assigns each \(n\) a quickly converging Cauchy sequence \(z_n\) such that, for all \(n\), \(z_n = 0\) if and only if \(n\) is not in the range of \(h\). Form a sequence of matrices \(\langle M(z_n) \mid n \in \mathbb{N} \rangle\); according to the principle, there is an associated sequence of Jordan canonical forms. The upper-right-hand entry of each of these canonical forms is either 0 or 1, and it is possible to effectively decide between these two cases. Thus, in RCA₀, we may form the range of \(h\) using the sequence of Jordan canonical forms as a parameter.

We now turn to statement (3.1.2). Recall that the standard formalization of the real numbers in RCA₀, as described by Simpson [6], makes use of quickly converging Cauchy sequences of rationals. Alternative formalizations of the real numbers may be considered, however. We define a Dedekind cut to be a subset \(Y\) of the rational numbers such that not every rational number is in \(Y\) and if \(p \in Y\) and \(q < p\) then \(q \in Y\). We say that a Dedekind cut \(Y\) is equivalent to a quickly converging Cauchy sequence \(\langle a_i \mid i \in \mathbb{N} \rangle\) if any only if the equivalence

\[
q \in Y \iff q \leq \lim_{i \to \infty} a_i
\]

holds for every rational number \(q\).
Hirst [2] has proved the following results relating Cauchy sequences with Dedekind cuts. Together with the Main Theorem, these results show that statement (3.1.2) is provable in RCA₀ but not \( \mathcal{HA}^# \).

**Lemma 3.5** (Corollary 4 in [2]). The following is provable in RCA₀. For any quickly converging Cauchy sequence \( x \) there is an equivalent Dedekind cut.

**Lemma 3.6** (Corollary 9 in [2]). The following principle is equivalent to WKL₀ over RCA₀: For each sequence \( \langle X_i \mid i \in \mathbb{N} \rangle \) of quickly converging Cauchy sequences there is a sequence \( \langle Y_i \mid i \in \mathbb{N} \rangle \) of Dedekind cuts such that \( X_i \) is equivalent to \( Y_i \) for each \( i \in \mathbb{N} \).

Statement (3.1.3), which is our final application of the Main Theorem, is related to countable posets. In RCA₀, we define a **countable poset** to be a set \( P \subseteq \mathbb{N} \) with a coded binary relation \( \preceq \) that is reflexive, antisymmetric, and transitive. A function \( f: \mathbb{N} \to P \) is called an **enumerated filter** if for every \( i, j \in \mathbb{N} \) there is a \( k \in \mathbb{N} \) such that \( f(k) \preceq f(i) \) and \( f(k) \preceq f(j) \), and for every \( q \in P \) if there is an \( i \in \mathbb{N} \) such that \( f(i) \preceq q \) then there is a \( k \in \mathbb{N} \) such that \( f(k) = q \). An enumerated filter is called **unbounded** if there is no \( q \in P \) such that \( q \prec f(i) \) for all \( i \in \mathbb{N} \). An enumerated filter \( f \) **extends** a filter \( g \) if the range of \( g \) (viewed as a function) is a subset of the range of \( f \).

Mummert has proved the following two lemmas about extending filters to unbounded filters (see Mummert and Lempp [4] and the remarks after Lemma 4.1.1 of [5]). These lemmas show that (3.1.3) is provable in RCA₀ but not \( \mathcal{HA}^# \).

**Lemma 3.7** (Theorem 3.5 in [4]). RCA₀ proves that any enumerated filter on a countable poset can be extended to an unbounded enumerated filter.

**Lemma 3.8** (Theorem 3.6 in [4]). The following statement implies ACA₀ over RCA₀: Given a sequence \( \langle P_i \mid i \in \mathbb{N} \rangle \) of countable posets and a sequence \( \langle f_i \mid i \in \mathbb{N} \rangle \) such that \( f_i \) is an enumerated filter on \( P_i \) for each \( i \in \mathbb{N} \), there is a sequence \( \langle g_i \mid i \in \mathbb{N} \rangle \) such that, for each \( i \in \mathbb{N} \), \( g_i \) is an unbounded enumerated filter on \( P_i \) extending \( f_i \).

We close by noting that the proof-theoretic results of Section 2 are proved by finitistic methods. Consequently, intuitionists might accept arguments like those of Section 3 as viable formal alternatives to the construction of weak counterexamples.
References


Appalachian State University
Department of Mathematical Sciences
Walker Hall
Boone, NC 28608