Reverse Mathematics of Divisibility in Integral Domains

Valentin Bura

joint work with Noam Greenberg

Overview

1. The framework of Reverse Mathematics
2. A Reverse Algebra Problem

Background

Second Order Arithmetic

The language $\mathcal{L}_2$ is a two sorted language, which has two types of variables: number variables, which are denoted by lower-case letters, and set variables, which are denoted by upper-case letters. $\mathcal{L}_2$ also has two types of quantifiers, $\exists x$, $\forall x$ and $\exists X$, $\forall X$.

Axioms

The axioms for $\mathcal{Z}_2$ come in three categories: axioms specifying the properties of $+, \cdot, 0, 1, <, \in$, to which we add an induction axiom:

$$((0 \in X \wedge \forall n(n \in X \rightarrow n+1 \in X)) \rightarrow \forall n(n \in X))$$

and a version of the comprehension scheme for forming sets:

$$\exists X \forall n(n \in X \leftrightarrow \phi(n)).$$

Background

Arithmetical Hierarchy

- A formula ψ of Second Order Arithmetic is Σ_0^0 and Π_0^0 if it is logically equivalent to a first order formula with only bounded quantifiers.
- A formula is classified as Σ_{n+1}^0 (or Σ_{n+1}) if it is logically equivalent to a formula of the form:

  $$\exists n_1 \exists n_2 \cdots \exists n_k \psi,$$

  where ψ is a Π_n^0 formula.
- A formula is classified as Π_{n+1}^0 (or Π_{n+1}) if it is logically equivalent to a formula of the form:

  $$\forall n_1 \forall n_2 \cdots \forall n_k \psi,$$

  where ψ is a Σ_n^0 formula.

Background

Computability Theory

Functions computed by Turing Machines are called *partially computable*.
We can effectively enumerate the partially computable functions:
$\varphi_0, \varphi_1, \varphi_2 \cdots$
For a set A (oracle), we can compute the list of oracle machines:
$\Phi_1^A, \Phi_2^A, \cdots$
A set is computably enumerable (c.e.) it can be listed effectively. If a set is c.e. and co-c.e. then we call it computable.
The canonical (non-computable) c.e. set is $\emptyset' = \{e \mid \varphi_e(e)\downarrow\}$.
There is an entire hierarchy of such sets, for instance: $\emptyset'' = \{e \mid \Phi_e^{\emptyset'}(e)\downarrow\}$.

Note that $\emptyset'$ is Σ_1 while $\emptyset''$ is Σ_2.
In general, the nth Turing Jump $\emptyset^{(n)}$ is Σ_n.

Background

Turing reducible

We say A is Turing below B, written $A \leq_T B$, if $\chi_A = \phi^B$ for some oracle machine ϕ.
If $A \leq_T B$ and $B \leq_T A$, then $A \equiv_T B$.

Turing degrees

A Turing Degree is an $\equiv_T$-equivalence class.

The join of two sets A and B is defined as
$A \oplus B = \{2a \mid a \in A\} \cup \{2b + 1 \mid b \in B\}$.
The join is the least upper bound of the Turing Degrees of A and B.
Hence, the Turing Degrees form a join-semi lattice.

Overview

Reverse Mathematics was introduced by Harvey Friedman in the seventies.

The Main Question

Which set-existence axioms are sufficient to prove Theorems of ordinary, non-set-theoretic Mathematics?

The Systems

Most Theorems of ordinary Mathematics are equivalent to one of five Subsystems of Second Order Arithmetic:
RCA_0, WKL_0, ACA_0, ATR_0 and $\Pi^1_1 - CA_0$.

We start with a direct proof from a system to the theorem, to which we append a "reversal step", in which we show that some axiom follows (over base system RCA_0) if we assume the Theorem.

RCA_0

Proofs in RCA_0

A result is provable in RCA_0 if it uses only:

- basic arithmetic facts,
- comprehension restricted to computable properties: $\exists S \forall x(\phi(x) \Leftrightarrow x \in S)$,
- induction restricted to Σ_1 sets: $((0 \in X \wedge \forall n(n \in X \rightarrow n+1 \in X)) \rightarrow \forall n(n \in X))$.

Theorem

If H is a normal subgroup of a group G, then G/H is a group.

Effective version:
If H is a *computable* normal subgroup of a *computable* group G, then G/H is a *computable* group.

WKL_0

Weak König's Lemma

Theorem

Any binary branching infinite tree has an infinite path.

Notice that the effective version of this theorem fails. Hence, this statement is not provable in RCA_0.

The system WKL_0 comprises of RCA_0 and the above theorem.
Results equivalent to WKL_0 over RCA_0 fail to hold effectively.

ACA_0

ACA_0

ACA_0 comprises of:

- RCA_0
- The comprehension scheme $\exists X \forall n (n \in X \leftrightarrow \phi(n))$ applied to arithmetical formulas ϕ.

- ACA_0 can define the Turing Jump of any set S: $S' = \{e \mid \Phi_e^S(e)\downarrow\}$.
- Any finite iteration of the Jump operator can be defined.
- KL: any finitely branching infinite tree has an infinite path.
- In particular, if we want to prove in the "reversal step" that a Theorem implies ACA_0, it is sufficient to show that a model of Theorem + RCA_0 is closed under the Turing Jump.

ATR_0 and $\Pi^1_1 - CA_0$

ATR_0

The third subsystem is ATR_0, which stands for Arithmetic Transfinite Recursion.

- Allows the iteration of the Turing Jump operator along any countable well-ordering,
- Any two well-orderings are comparable.

$\Pi^1_1 - CA_0$

Formally defined as ACA_0 plus the comprehension scheme for Π^1_1 sets (defined by a formula of the type $\forall X \varphi(X, a)$).

- For any sequence of trees $\langle T_k \mid k \in \omega \rangle$, there exists a set X such that $k \in X$ if and only if T_k has an infinite path.

Definitions

We look at computable commutative rings with unity $\mathbf{R} = (R, +, \cdot, 1, 0)$.
unit: $a \in R$ s.t. $\exists b$ such that $a \cdot b = 1$.
associates: $a, b \in R$ s.t. $\exists c$ a unit with $a \cdot c = b$.
division: $a \mid b$ if $\exists c$ s.t. $a \cdot c = b$.
integral domain: a ring with no zero divisors.
proper division: a properly divides b if $a \mid b$ and they are not associates.
irreducible: a non-unit element for which the only divisors are units or associates.
irreducible factorization of a: a multiset $B = [p \mid p \text{ is irreducible}]$ such that $a = u \prod_{p \in B} p$ for a unit u.
ACCP: the ring contains no infinite chain $(r_i)_{i \in \omega}$ s.t. r_{i+1} properly divides r_i.
Atomic: an integral domain in which every element has an irreducible factorization.

The Theorem

Theorem (ACA_0)

If an integral domain satisfies the ACCP, then it is Atomic.

first proof.

Let R be a non-atomic integral domain. There is a non-unit a of R that does not have an irreducible factorization.
Build a $\emptyset'$ computable infinite binary branching tree T recursively.
Let a be a leaf of T. For each leaf b of T, search using $\emptyset'$ for pairs c, d such that $cd = b$.When found, test using $\emptyset'$ whether either of c, d is a unit.If positive, loop to the next pair, otherwise put c, d as leaves descending from b.
Note that at any stage we are bound to find children of some leaf, since otherwise the leaves constitute an irreducible factorization for a. By relativized KL, T has an infinite path, which witnesses the failure of ACCP.

□

The Theorem

second proof.

Let R be a computable non-Atomic integral domain. There are two cases to consider.

Case 1: there is some $a \in R$ with no irreducible factor. Recursively define a sequence $\langle a_i \rangle_{i \in \omega}$ with $a_0 = a$ and a_{n+1} some proper factor of a_n. By induction, a_n has no irreducible factor, so is reducible itself. $\emptyset'$ can identify such a_{n+1}, so the sequence $\langle a_i \rangle_{i \in \omega}$ is computable from $\emptyset'$. Since this is an infinite descending chain in divisibility, it is a counter-example to ACCP.

Case 2: every $b \in R$ has an irreducible factor, but some $a \in R$ is not the product of irreducible elements. Recursively define a sequence $\langle a_i \rangle_{i \in \omega}$ with $a_0 = a$ and a_{n+1} a proper factor of a_n such that there is some irreducible $p_n \in R$ with $a_n = a_{n+1} \cdot_R p_n$. By induction, a_n is not the product of irreducible elements, and since p_n is irreducible, this implies a_{n+1} does not have an irreducible factorization. $\emptyset''$ can identify an irreducible factor of a_n and so the sequence $\langle a_i \rangle_{i \in \omega}$ is computable from $\emptyset''$. This sequence is a counter-example to ACCP.

□

Note

An important thing to note here:

Both proofs presented require the oracle $\emptyset''$.

In the first proof, the labels of the tree don't have a $\emptyset'$-computable bound. Hence we need the relativised KL rather than WKL, which is equivalent to $\emptyset''$.
For the second proof, identifying an irreducible factor uses $\emptyset''$.

We currently know of no proof that requires an oracle weaker than $\emptyset''$.

Reversal proof

Theorem

There exists a computable integral domain Q, not Atomic, such that any sequence $\langle c_i \rangle_{i \in \omega}$ from Q, with c_{k+1} properly dividing c_k for all k, computes $\emptyset'$.

Corollary

The statement "if an integral domain satisfies the ACCP, then it is Atomic" implies ACA_0.

Proof.

Let M be a model of RCA_0+ the statement. Let $X \in M$, we show $X' \in M$. Note that M is closed under Turing reducibility. In M, from the proposition above, obtain an X-computable ring Q which is non-Atomic and if $\langle c_i \rangle_{i \in \omega}$ from Q with $\forall k \ c_{k+1} \mid c_k$ and they do not associate then $X \oplus \langle c_i \rangle \geq_T X'$.
By the statement, there is such a sequence in M. So $X' \in M$. $\square$

Proof outline

We construct in stages, from an enumeration of $\emptyset'$, a set of strings which (informally) encodes a binary branching computable tree T whose unique infinite path computes $\emptyset'$.

Construction

Let $\sigma_1 = \lambda$ and $T_1 = \{\sigma_1\}$.
Step k, for $k \geq 1$: If there exists $n \in \omega$ with $n < |\sigma_k|$ such that $\sigma_k(n) = 0$ and $n \in \emptyset'_{k+1}$, then $\sigma_{k+1} = \sigma_k^-$ and $T_{k+1} = T_k$. Otherwise put $n = |\sigma_k|$ and let

$$\sigma_{k+1} = \begin{cases} \sigma_k{}^\frown 0, & \text{if } n \notin \emptyset'_{k+1} \\ \sigma_k{}^\frown s, & \text{where } n \in \emptyset'_{k+1} \text{ and } n \in \emptyset'_s \setminus \emptyset'_{s-1} \end{cases}$$

with $T_{k+1} = T_k \cup \{\sigma_{k+1}\}$.
Finally, let $T = \bigcup_{n \in \omega} T_n$.

Proof outline

Next, we encode T by divisibility chains in some computable integral domain Q.

Let $Q_0 \cong \mathbb{Q}$, $Q_1 = Q_0[a_\lambda] \cdots$.
At *step* k, we have computable ring $Q_k = R_k[a_{\sigma_k}, b_{\sigma_k \upharpoonright n}]_{n=1,2\cdots|\sigma_k|}$, where R_k is a computable subring of Q_k and the elements presented are algebraically independent over R_k.
At *step* $k+1$, if $T_{k+1} = T_k$ make b_{σ_k} a unit of Q_{k+1}, we let $R_{k+1} = R_k[b_{\sigma_k}, b_{\sigma_k}^{-1}]$ and $Q_{k+1} = R_{k+1}[a_{\sigma_{k+1}}, b_{\sigma_{k+1} \upharpoonright n}]$.
Otherwise, if $T_{k+1} = T_k \cup \{\sigma_{k+1}\}$, let $R_{k+1} = R_k$ and define $Q_{k+1} = (R_{k+1}[a_{\sigma_k}, b_{\sigma_k \upharpoonright n}])[a_{\sigma_{k+1}}, b_{\sigma_{k+1}}]$ and impose the condition $a_{\sigma_k} = a_{\sigma_{k+1}} \cdot b_{\sigma_{k+1}}$.
Finally, let $Q_\omega = \bigcup_{k \in \omega} Q_k$.

Proof outline

We can prove the following:

- No a_σ in Q_ω is a unit or irreducible. Hence a_λ does not have an irreducible factorization.
- Q_ω is a non-Atomic integral domain.
- By the Theorem we study, it must have infinite descending chains in proper divisibility.
- Any infinite divisibility descending sequence of Q_ω whose terms do not have an a_σ factor must stabilize.
- Any infinite descending chain in divisibility of Q_ω computes $\emptyset'$.

Therefore, we have shown the Theorem under study implies ACA_0.

Open question

We have shown:

There exists a computable integral domain Q_ω, not Atomic, such that any sequence $\langle c_i \rangle_{i\in\omega}$ from Q_ω, with c_{k+1} properly dividing c_k for all k, computes $\emptyset'$.

Question

Is this true if we replace $\emptyset'$ by $\emptyset''$?

The direct proofs we have use $\emptyset''$.So the question seems natural: either we can improve on these proofs and use a weaker oracle or answer the question above in the affirmative.

Open question

Fact

There exists an infinitely-branching computable tree with a unique infinite path that computes $\emptyset''$.

Construction

Consider an enumeration of the oracle machines $\phi_0, \phi_1, \phi_2 \ldots$ We construct the tree S whose unique path encodes $\emptyset''$. Run the construction from before.

If we back-track in the construction, leave S unchanged. For each new σ_k, with $1 \leq i \leq k$, run $\phi_i^{\sigma_k}(i)$ for k steps and put the string $s_1 s_2 \ldots s_k$ into S, where $s_i = 0$ if $\phi_i^{\sigma_k}(i) \uparrow$ and $s_i = s$ if $\phi_i^{\sigma_k}(i) \downarrow$ at step s.

Open question

In the enumeration of $\emptyset''$, elements can enter S more than one time.
As a consequence, it is possible that we backtracked from some element $\sigma \in S$ and then σ reappears at a later stage.
This creates a problem for coding the tree into a ring: once an element is made a unit in a ring, it cannot be un-inverted.
In technical terms, the terminal elements of the tree are not c.e. (Σ_1) , they are $\emptyset'$-c.e. (Σ_2).

References

Bura (2013)
Reverse Mathematics of Divisibility in Integral Domains
Victoria University of Wellington Master Thesis.

Friedman et al. (1983)
Countable Algebra and Set Existence Axioms
Annals of Pure and Applied Logic 25, 141 – 181.

Simpson (2010)
Subsystems of Second Order Arithmetic
Cambridge University Press 2nd edition.

Solomon (1998)
Reverse Mathematics and Ordered Groups
Cornell University PhD Thesis.