

PROPER DIVISIBILITY IN COMPUTABLE RINGS

NOAM GREENBERG AND ALEXANDER MELNIKOV

ABSTRACT. We study divisibility in computable integral domains. We develop a technique for coding Σ_2^0 binary trees into the divisibility relation of a computable integral domain. We then use this technique to prove two theorems about non-atomic integral domains.

In every atomic integral domain, the divisibility relation is well-founded. We show that this classical theorem is equivalent to ACA_0 over RCA_0 .

In every computable non-atomic integral domain there is a Δ_3^0 infinite sequence of proper divisions. We show that this upper bound cannot be improved to Δ_2^0 in general.

1. INTRODUCTION

Throughout most of the 19th century algebra was algorithmic; existence proofs were given by explicit constructions. Kronecker’s elimination theory stands in contrast with the later abstract development led by Dedekind, Kummer and Hilbert; however all of mathematics up to that point was as constructive [22]. *Computable algebra* aims to unearth the effective content of algebraic objects and constructions, revealing that aspect of mathematics which is lost when using the axiomatic, set-theoretic approach.

There has been much work considering fields. Early work concerning splitting algorithms in fields (Herrman [17], van der Waerden [32]) was later made precise (for example Fröhlich and Shepherdson [14]) using the tools of computability theory, developed by Gödel, Church, Turing and Kleene (e.g., [30, 31]). These tools allow us to rigorously define, for example, what is a computable field, and what operations on fields are computable. For example, Rabin [23] showed that every computable field can be computably embedded into a computable algebraically closed field; however the image of the embedding of the field into its algebraic closure may not always be computable, indeed to identify it sometimes extra computational power is required, such as the halting problem. Rabin’s construction is not identical to Steinitz’s original construction of algebraic closure [28]; in the absence of a splitting algorithm, an alternative approach is necessary, presenting the algebraic closure as the quotient of a polynomial ring by a computable ideal.

Computability theory allows us not only to differentiate the computable from that which is not, but also compare different noncomputable objects, using *relative computability*. This captures the intuitive concepts of relative complexity, or information content: what it means for one object to be more complicated than

Greenberg was supported by a Rutherford Discovery Fellowship, by the Marsden Fund, and by a Turing Research Fellowship “Mind, Mechanism and Mathematics” from the Templeton Foundation. We thank Damir Dzhafarov and Dan Turetsky for some useful conversations. We thank Valentin Bura, whose Master’s thesis [4] contains an outline of Theorem 1.1, for allowing us to include material from his thesis. Valentin Bura declined co-authorship of this paper.

another, or one problem to be easier to solve than another. For example, Friedman, Simpson and Smith showed [13] that in general, constructing a maximal ideal in a commutative ring is more complicated than constructing a prime ideal, but neither can be done computably. A yardstick for measuring complexity is given by iterations of Turing’s jump operator, defined by taking the relative halting problem. For example, the full power of the halting problem is required to construct maximal ideals in all rings, but is not necessary for building prime ideals.

There is a fundamental connection between computability and foundational questions formalised in second order arithmetic. The project of reverse mathematics attempts to pin-point the proof-theoretic power of mathematical facts and theorems. It finds the number-theoretic axioms required to prove these theorems. Those axioms are often formalised as set existence axioms. Examples for the connection are the system RCA_0 of “recursive comprehension”, which in terms of set existence corresponds to relative computability; and the system ACA_0 of “arithmetic comprehension”, which corresponds to the Turing jump. Using this correspondence, the effective results from [13] mentioned above yield a proof that the statement “every ring has a maximal ideal” is equivalent to ACA_0 , but that the statement “every ring has a prime ideal” is strictly weaker. We remark though that computable algebra and reverse mathematics are complementary approaches for measuring the complexity of objects and theorems. Unlike reverse mathematics, computable algebra does not give any information about the amount of induction required to prove a theorem. On the other hand, in terms of set existence, computable algebra makes finer distinctions; for example, reverse mathematics cannot distinguish between one or two iterations of the Turing jump.

The groundwork for computable algebra was laid by Rabin [23] and Mal’cev [19] and continued by Metakides and Nerode [21, 20] and Ershov [12] and his school (for example [11]). While there has been much work on groups [18], fields [11] and vector spaces [20], relatively little is known about rings. Other than the work by Friedman, Simpson and Smith mentioned above, investigations were made into algorithms of ideal membership (see [29] for a survey), the complexity of radicals [9], Euclidean domains [25, 8], the proof-theoretic strength of the statement “every Artinian ring is Noetherian” [5], and the complexity of primes [10]. In this paper we consider a couple of basic facts regarding unique factorisation.

1.1. Results. It is well-known that every Euclidean domain is a principal ideal domain, and that every principal ideal domain is a unique factorisation domain. Underlying the latter implication is the following characterisation of unique factorisation:

Theorem A. *An integral domain R is a unique factorisation domain if and only if:*

- (1) *every irreducible element of R is prime; and*
- (2) *the divisibility relation in R is well-founded.*

An integral domain satisfying (1) is sometimes called an AP-domain; property (2) is abbreviated as “accp”, because the condition is equivalent to the ascending chain condition for principal ideals. One half of one direction of this equivalence is:

Theorem B. *If R is an integral domain satisfying accp, then every element of R is the product of irreducible elements of R .*

A ring satisfying the conclusion of Theorem B is called *atomic*. We remark that the converse of Theorem B fails [16]. In this paper we determine the proof-theoretic strength of these theorems:

Theorem 1.1. *Both Theorem A and Theorem B are equivalent to ACA_0 over RCA_0 .*

In terms of computability we consider the complexity of a witness for the contrapositive of Theorem B. An infinite sequence $\langle a_n \rangle$ of elements of an integral domain R witnesses the failure of accp if for all n , a_{n+1} properly divides a_n . We call such a sequence an *infinite chain of proper divisibility*. If the accp fails, how much computational power do we need to find such a chain? As mentioned above, results in reverse mathematics often utilise constructions from effective mathematics. In our example, the proof of Theorem 1.1 is an adaptation to second-order arithmetic of the following:

Theorem 1.2. *There is a computable integral domain R which is not atomic, such that every infinite chain of proper divisibility in R computes the halting problem \emptyset' .*

That is, the halting problem is sometimes necessary for finding witnessing sequences. It is important to note that while Theorem 1.1 gives a complete answer for the proof-theoretic content of Theorems A and B, in terms of computability, Theorem 1.2 is not optimal. A crude upper bound for the complexity of a sequence witnessing the failure of accp (in non-atomic rings) is \emptyset'' , the second iteration of the Turing jump. We can show that \emptyset' is not enough:

Theorem 1.3. *There is a computable integral domain R which is not atomic, such that \emptyset' does not compute any infinite chain of proper divisibility in R .*

We note that our method seems insufficient for a coding of \emptyset'' into the proper divisibility relation of a computable domain: we leave open the question whether there is a non-atomic computable integral domain in which every chain of proper divisibility computes \emptyset'' . We also remark that we expect that in *atomic* rings in which accp fails, witnessing sequences may need to have much higher complexity, all the way up the hyperarithmetic hierarchy.

1.2. A new technique. To prove Theorems 1.2 and 1.3 we employ a technique of coding binary trees into integral domains. In terms of complexity we can translate Σ_2^0 (computably enumerable relative to \emptyset') binary trees T into computable integral domains \mathcal{Q}_T . The coding is not injective on isomorphism types. Nonetheless, properties of the resulting ring \mathcal{Q}_T are controlled by the originating tree T in a way that allows us to separate much of the algebra from the computability-theoretic constructions. For example we will ensure that:

- T is finite if and only if \mathcal{Q}_T is atomic.

In our coding we will identify the nodes (vertices) of T as elements of \mathcal{Q}_T , which in some sense generate \mathcal{Q}_T . Much of our work will be to show that witnesses to the failure of accp in \mathcal{Q}_T essentially come from infinite decreasing sequences in T . More precisely, by multiplying their elements we can view multisets of nodes of T as elements of \mathcal{Q}_T ; a sequence $\langle M_n \rangle$ of multisets is *properly decreasing* if the corresponding sequence of elements of \mathcal{Q}_T witnesses the failure of accp . However, it is crucial that this relation on multisets can be read off the tree T without the need to consult the ring \mathcal{Q}_T . Thus, we can work directly with Σ_2^0 trees without worrying about algebra. We will show (Corollary 3.36):

- Suppose that T is infinite. Every sequence of elements of \mathcal{Q}_T which witnesses the failure of accp computes a properly decreasing sequence of multisets of T .

We note that coding ideas were used in the context of computable abelian groups [7, 3, 1] where divisibility plays an important role, and also in Boolean algebras [15]. We believe that such codings of trees into the divisibility relation have never been seriously studied/applied in computable ring theory. We expect that our coding will have applications beyond those presented in this paper. On the other hand, if there is a way to improve our theorems to code \emptyset'' into descending sequences (we encourage the reader to try, so as to get an idea of the complications involved), we suspect that different coding techniques will be required.

1.3. The structure of the paper. In Section 2 we give more detailed background and necessary definitions. In Section 3 we describe the coding of Σ_2^0 trees into rings and prove various technical lemmas about the coding. In Section 4 we prove Theorems 1.1 and 1.2. In Section 5 we prove Theorem 1.3.

2. PRELIMINARIES

2.1. Computability theory. The main notions of computability are partial computable functions and computably enumerable sets. While the formal definitions are involved (see for example [24]) the main idea is that a function f is partial computable if there is an algorithm (for example implemented by a Turing machine) which given an input n halts after finitely many steps and outputs $f(n)$ in case $n \in \text{dom } f$, and never halts otherwise. A set A is computably enumerable if there is an algorithm which runs indefinitely and outputs the elements of A . A set A is computable if membership in A can be decided by an algorithm (formally, if its characteristic function is partial computable). A *computable* function is a partial computable function whose domain is a computable set. A set is computable if and only if it and its complement are computably enumerable. A function is partial computable if and only if its graph is computably enumerable.

A key notion is relative computability. Given a set (or function) B , we say that a set (or function) A is *B-computable* if A is computable by a machine which is given access to information about B (as a “black box”). We write $A \leq_T B$ and say that A is *Turing reducible* to B . Informally, this says that B contains at least as much information as A . Turing reducibility \leq_T is a pre-partial ordering; the equivalence classes are known as the *Turing degrees*. Similarly, a set is computably enumerable relative to B if there is an algorithm with access to B which enumerates the elements of A .

The *halting problem* relative to a set B , denoted B' , is the collection of algorithms with access to B which terminate (after finitely many steps). It is a universal B -computably enumerable set. B' computes B but not vice-versa. The relative halting problem induces an increasing map on Turing degrees, which is known as the *Turing jump*.

There is a close connection between computability and definability in arithmetic. The semi-ring $(\mathbb{N}, +, \cdot)$ is analysed using first-order logic. Formulas in the language of semi-rings are put in a hierarchy of complexity based on alteration of quantifiers. For example a formula is Σ_1^0 if it contains a single unrestricted existential quantifier, Σ_2^0 if it is of the form $\exists\forall$, and so on. A set of numbers is Σ_n^0 if it is definable by a

Σ_n^0 formula. A set is Δ_n^0 if it and its complement are Σ_n^0 . A set is computable if and only if it is Δ_1^0 , c.e. if and only if it is Σ_1^0 , computable from \emptyset' if and only if it is Δ_2^0 , c.e. in \emptyset' if and only if it is Σ_2^0 , computable from \emptyset'' if and only if it is Δ_3^0 , and so on.

For more on computability, a standard reference is [27].

2.2. Computable algebra. As mentioned above, using the notion of Turing computable sets and functions, Rabin [23] and independently Mal'cev [19] gave the first general definition of computable structures. For rings we obtain the following.

Definition 2.1. A *computable ring* is a ring $(R, +_R, \cdot_R)$ such that R is a computable subset of \mathbb{N} and $+_R$ and \cdot_R are computable functions from R^2 to R .

More generally, we ask how much external computational power we need to construct all objects that are used in the proof of a theorem that we have in mind. The answer will, in a way, measure how “constructive” the theorem is. As mentioned above, Friedman, Simpson and Smith [13] constructed a computable ring in which every maximal ideal computes \emptyset' . On the other hand they showed that every computable ring contains a prime ideal which is computationally significantly weaker than \emptyset' ; however they did construct a computable ring which has no computable prime ideal.

For more on effective algebra see for example [2, 11].

2.3. Reverse mathematics. Reverse mathematics [13] studies subsystems of second-order arithmetic. We fix a relatively weak base theory; a standard choice is RCA_0 , which contains the usual semi-ring axioms together with Σ_1^0 induction and Δ_1^0 comprehension (set existence). The standard models of RCA_0 are those whose second-order part induces an ideal in the Turing degrees. On the other hand, since we use limited induction, in analysing RCA_0 we need to take into account non-standard models in which there are “infinite” natural numbers. Informally, RCA_0 is the weakest system which allows the formalisation of relative computability.

The other system we use is ACA_0 , arithmetic comprehension. It extends RCA_0 by adding comprehension of all arithmetic sets (first-order definable sets). It turns out that Σ_1^0 comprehension is sufficient. This implies that over RCA_0 , ACA_0 is equivalent to the existence of the Turing jump: a model M of RCA_0 is a model of ACA_0 if and only if for every set X in the second-order part of M , the Turing jump X' belongs to M as well. This means that the standard models of ACA_0 are those which induce a *jump-ideal* of the Turing degrees. Equivalently, a standard formulation is that a model of RCA_0 is a model of ACA_0 if and only if for every function f in the model, the range of f is also in the model (we say that the range of f “exists”).

Informally, when we show that a theorem of mathematics is provable in RCA_0 (for example, the intermediate value theorem, or the existence of algebraic closure), it means that it is “effective”, or algorithmic. When we show that a theorem is equivalent to ACA_0 (for example, the Bolzano-Weierstrass theorem, or the existence of maximal ideals) we show that not only the theorem is not effective, but that ACA_0 is the weakest extension of RCA_0 that can prove it: it *requires* the Turing jump.

For more, see the standard reference [26].

2.4. Accp and atomic rings. For summary we recall the properties of integral domains that we consider:

- accp, equivalent to the divisibility relation being well-founded;

- AP domain: every irreducible element is prime;
- atomic domain: every non-unit element is the product of irreducible elements;
- *unrestricted UFD* (abbreviated U-UFD): if an element is the product of irreducibles, then this factorisation is unique (up to units).

Here recall that an irreducible element is a minimal nonunit element in the divisibility relation, and that a prime element p is one satisfying $p|ab \Rightarrow p|a$ or $p|b$. Every prime is irreducible (in any integral domain).

Theorem A says that an integral domain is atomic and a U-UFD if and only if it has accp and is an AP domain. Theorem B says that the accp implies atomicity. We mentioned that this does not reverse (Grams [16]). It is also the case that every AP domain is a U-UFD; this too does not reverse [6]. The reason we do not state this as “Theorem C” is that it is not equivalent to ACA_0 ; in fact it is provable in RCA_0 .

Recall the proof of Theorem B. Let R be a non-atomic integral domain. There are two cases. If there is some non-unit $a \in R$ which has no irreducible factor, then an infinite sequence witnessing the failure of accp is constructed by taking $a_0 = a$ and a_{n+1} some proper factor of a_n . Otherwise, take any $a \in R$ which is not the product of irreducible elements. Let $a_0 = a$, and given a_n (which inductively has the same property), let $a_{n+1} = a_n/p$ for some irreducible factor p of a_n .

An examination of the definitions shows that if R is a computable ring then the divisibility relation is computably enumerable (c.e.) and hence \emptyset' -computable; it follows that the set of units is c.e. as well. The set of irreducible elements is then co-c.e. in \emptyset' (Π_2^0), and so is computable from \emptyset'' . We conclude that in the first case above, the sequence constructed can be made computable from \emptyset' ; in the second case, from \emptyset'' . Formalising this argument in second-order arithmetic shows that ACA_0 implies Theorem B; similar considerations show that ACA_0 implies Theorem A as well. We remark that the split into two cases illustrates one of the many difficulties in coding \emptyset'' into the failure of accp : in any ring witnessing such a coding, every element must have an irreducible factor.

2.5. Trees. Regarding trees, we follow terminology from combinatorics and computer science rather than computability. We will be exclusively using *full binary trees*, in which every node that is not a leaf has two children. Every tree has a designated root. If x is a node of a tree T which is not a leaf of T , then one of the children of x is designated as the left child and one is designated as the right child. For example, the infinite complete binary tree is $2^{<\omega}$ (the set of all finite binary strings) with the root being the empty string, and $\sigma^{\frown}0$ and $\sigma^{\frown}1$ being the left and right children (respectively) of a string $\sigma \in 2^{<\omega}$. Note that the relations “ x is the root of T ”, “ y is the left child of x ” and “ y is the right child of x ” completely specify the structure of a tree.

A *subtree* of a tree T is a subset $S \subseteq T$ which is closed under taking parents and which is a tree under the relations of T (so we require that S is a full binary tree). For example, the “fishbone” $\{0^n, 0^n1 : n < \omega\}$ is a subtree of $2^{<\omega}$.

3. TRANSLATING TREES TO RINGS

In this section we define the translation (coding) of Σ_2^0 -trees into computable integral domains.

3.1. An informal explanation of the translation. In our construction we will approximate a Σ_2^0 tree T by a sequence $\langle T_n \rangle$ of finite trees. We construct \mathcal{Q}_T as a sequence of extensions; \mathcal{Q}_{T_n} will be a subring of $\mathcal{Q}_{T_{n+1}}$ and $\mathcal{Q}_T = \bigcup_n \mathcal{Q}_{T_n}$.

We will set $\mathbb{A} = \mathbb{Q}[t_n, t_n^{-1} : n \in \omega]$ where the t_n are purely transcendental (algebraically independent) over \mathbb{Q} . To begin with we start with the tree T_0 consisting of a single node r (the root) and set $\mathcal{Q}_{T_0} = \mathbb{A}[r]$ (with r transcendental over \mathbb{A}). During the construction we will be adjoining new elements to the ring and declare new relations on it. We describe the two basic operations that we may apply to our ring at a later stage of the construction.

Operation 1: Factorizing a transcendental. Since we will be willing to play with proper divisibility, we might want to factorize purely transcendental elements over \mathbb{A} . For example suppose that T_1 consists of the root r and its two children a and b . In \mathcal{Q}_{T_1} we will factorise r into a and b . That is, we will set $\mathcal{Q}_{T_1} = \mathbb{A}[a, b]$ with a, b algebraically independent over \mathbb{A} , and identify r with ab . So a and b properly divide r . We could then further factorise, say a , into its two children x and y on T_2 ; we obtain the ring $\mathcal{Q}_{T_2} = \mathbb{A}[b, x, y]$, with a identified with xy . See Fig. 1.

Operation 2: Inverting a transcendental. We might later decide to change our mind about the proper division $x \mid a$ by inverting y . This happens for example if $T_3 = T_1$, that is, the leaves x and y were chopped off T_2 . Starting with $\mathcal{Q}_{T_2} = \mathbb{A}[b, x, y]$ we obtain the extension $\mathcal{Q}_{T_3} = \mathbb{A}[b, x, y, y^{-1}] = \mathbb{A}[y, y^{-1}][b, x]$. The base ring \mathbb{A} was chosen so that $\mathbb{A}[y, y^{-1}]$ is isomorphic to \mathbb{A} , and in \mathcal{Q}_{T_3} , a and x are associates; so $\mathcal{Q}_{T_3} = \mathbb{A}[y, y^{-1}][b, x] = \mathbb{A}[y, y^{-1}][a, b] \cong \mathbb{A}[a, b] = \mathcal{Q}_{T_1}$. See Fig. 2.

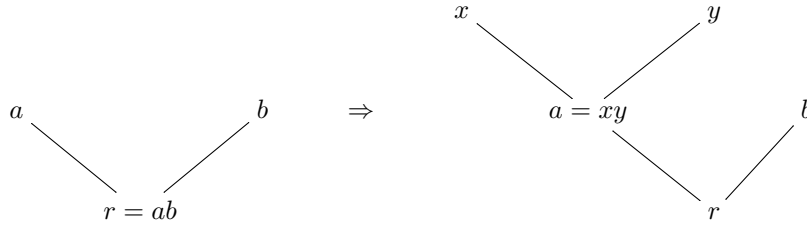


FIGURE 1. Operation 1: factorization of a into xy .

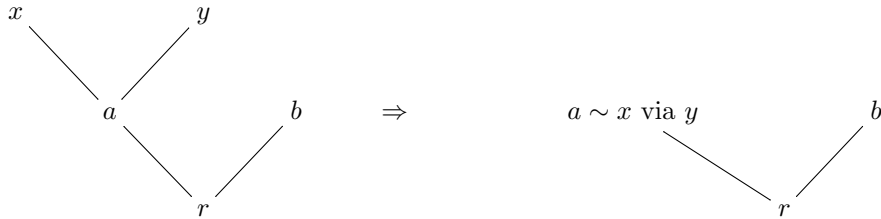


FIGURE 2. Operation 2: inverting a leaf. “ $a \sim x$ via y ” indicates that a and x are associates and y is the unit witnessing this fact.

Note that in the example above we may at a later stage factorize a again, say $a = x'y'$, and then invert or factorize y' or x' , etc.¹ The same can be said about any leaf of the finite binary tree that we have at any stage. What will we build at the end? The ring that we end up with will naturally correspond to a (perhaps infinite) binary tree consisting precisely of those nodes that are introduced but never erased. Up to isomorphism, we could start with the final tree T and define \mathcal{Q}_T by only applying operation 1: going down the levels of T , repeatedly factoring the elements of T into their children. The point is that this direct approach will only yield a computable ring if the final tree T is computable. Using the approximation for T and operation 2 as well as operation 1 allows us to construct a computable copy of \mathcal{Q}_T even if T is merely Σ_2^0 and not necessarily computable.

As mentioned, the main goal is to computably translate descending chains of proper divisibility into multisets of elements of our trees. The main step is Proposition 3.31 (and Corollary 3.36) which says that descending chains compute descending chains of *monomials*, products of nodes in our trees. The point is that when we *construct* T we can control the complexity of chains of divisibility in \mathcal{Q}_T by only considering multisets of nodes in T (and its finite approximations). We do not have to worry about general elements of \mathcal{Q}_T . Of course, to show that this reduction can be achieved, we need a detailed analysis of the structure of \mathcal{Q}_T .

Example 3.1. When working with the ring \mathcal{Q}_{T_3} above we may wonder if elements such as $x^2a + y$, $x^2y^2a^2t_3^2 - 14x^3y^{-4}a$ or $t_0x^2b^3 + 2y^{-3} + 3t_0x^2 + (1/7)t_0t_3a^2$ are involved in infinite chains of divisibility in the final ring, and it is not clear how to control the result just using the trees. In contrast, divisibility of monomials such as x^3b^2 , $a^2x^2b^2$ and yab^2 is immediate from the sequence of trees constructed so far. We can present these monomials as associates of products of leaves of T_3 and then just compare powers. For example $a^2x^2b^2 \sim a^4b^2$ and $x^3b^2 \sim a^3b^2$ and so the latter properly divides the former in \mathcal{Q}_{T_3} . If later a is inverted then the division is no longer proper.

3.2. Roadmap for this section. In the rest of this section we give the formal treatment of our transformation of trees into rings. We do it in three steps.

In Section 3.3 we define the operator $T \mapsto \mathcal{Q}_T$, defined on all binary trees T . As mentioned above this only uses operation 1. The treatment in this subsection is not effective. The direct approach allows us to gain some basic information about the algebraic structure of \mathcal{Q}_T (Proposition 3.8). We observe the algebraic properties of nodes on the tree and conclude, for example, that T is finite if and only if \mathcal{Q}_T is atomic (Corollary 3.9). We also observe how operation 1 and operation 2 affect the rings we obtain (Proposition 3.5 and Lemma 3.13).

In Section 3.4 we introduce linear systems of trees (Definition 3.15). In application, a linear system of trees will consist of the final tree we construct, together with its finite approximations. For an inductive treatment, in this section we consider both finite and infinite linear systems of trees. Using both operation 1 and operation 2 we define the ring $\mathcal{Q}_{\mathbb{L}}$ associated with a linear system of trees \mathbb{L} . This tree is isomorphic to $\mathcal{Q}_{T_{\mathbb{L}}}$, where $T_{\mathbb{L}}$ is the last tree of the system; the difference is that nodes introduced somewhere in the system but later discarded are elements

¹We note though that the labels of new children of a must be distinct from x and y ; once y has been inverted, we cannot make it transcendental again. This corresponds to condition (3) in the definition of linear systems of trees (Definition 3.15).

of $\mathcal{Q}_{\mathbb{L}}$, where they are either units or associates of nodes on the final tree $T_{\mathbb{L}}$. In this subsection we show (Proposition 3.20) that the transformation on linear systems is computable. As Σ_2^0 trees are those which can be approximated via computable linear systems, this shows that for such trees T , \mathcal{Q}_T has a computable copy.

Finally, in Section 3.5 we show how to simplify sequences witnessing the failure of accp in $\mathcal{Q}_{\mathbb{L}}$. As discussed above (and formalised in Definition 3.22), monomials are products in $\mathcal{Q}_{\mathbb{L}}$ of nodes appearing in trees along the system (both ones which are eventually discarded, and ones which survive until the final tree $T_{\mathbb{L}}$). The bulk of this subsection is devoted to an analysis of the prime elements of $\mathcal{Q}_{\mathbb{L}}$. Some of the primes are given by the leaves of $T_{\mathbb{L}}$. The others (denoted by $\mathbf{P}(\mathbb{L})$) multiplicatively generate a subset $\mathbf{wfd}(\mathbb{L})$ on which the divisibility relation is well-founded. The main technical fact is Lemma 3.25 which says that these primes are not factorized during the construction; they are either inverted or remain prime. This analysis of primes allows us to show that divisibility in $\mathcal{Q}_{\mathbb{L}}$ is in some sense a “direct sum” of divisibility in $\mathbf{wfd}(\mathbb{L})$ and in monomials (Lemma 3.26 and Corollary 3.29). Since $\mathbf{wfd}(\mathbb{L})$ is well-founded, the well-founded part of elements of a sequence $\langle a_n \rangle$ of proper divisibility in $\mathcal{Q}_{\mathbb{L}}$ stabilises. We can then divide by the stabilised value and obtain a sequence of monomials, yielding our goal, Proposition 3.31. At the end of this subsection we discuss monomial decompositions, which are multisets of nodes, and translate Proposition 3.31 to the language of multisets (Corollary 3.36)).

3.3. The ring associated with a binary tree. We emphasize again that all trees we discuss are full binary trees (finite or countable) with a designated root and designated left and right children for all non-leaves.

Notation 3.2. Let $\{t_n : n < \omega\}$ be a set of indeterminates. We let

$$\mathbb{A} = \mathbb{Q}[t_n, t_n^{-1} : n < \omega].$$

Remark 3.3. \mathbb{A} is a localization of $\mathbb{Q}[t_n : n < \omega]$. The latter is a unique factorization domain, and so \mathbb{A} is a unique factorization domain.

Definition 3.4. Let T be a tree. Considering the elements of T as indeterminates over \mathbb{A} , we let I_T be the ideal of $\mathbb{A}[T]$ generated by the polynomials $x - yz$, where $x, y, z \in T$ and y, z are the children of x . We let $\mathcal{Q}_T = \mathbb{A}[T]/I_T$.

We identify the elements of T with their images in \mathcal{Q}_T .

3.3.1. Extension. We show that if S is a subtree of T then \mathcal{Q}_S is canonically a subring of \mathcal{Q}_T . This means that the identity map on $\mathbb{A} \cup S$ induces an embedding of \mathcal{Q}_S into \mathcal{Q}_T , equivalently that $I_T \cap \mathbb{A}[S] = I_S$.

Proposition 3.5.

- (1) *If S is a subtree of T then \mathcal{Q}_S is canonically a subring of \mathcal{Q}_T .*
- (2) *If $T = \bigcup_{k < \omega} T_k$ where each T_k is a subtree of T_{k+1} , then $\mathcal{Q}_T = \bigcup_{k < \omega} \mathcal{Q}_{T_k}$.*

Proof. The proof is based on the the following lemma.

Lemma 3.6. *Let S be a subtree of a tree T , and suppose that $T = S \cup \{y, z\}$ where y and z are the children on T of a node x which is a leaf of S . Then $\mathcal{Q}_T \cong \mathcal{Q}_S[y, z]/(x - yz)$, and \mathcal{Q}_S is canonically a subring of \mathcal{Q}_T . In \mathcal{Q}_T , y and z are transcendental over \mathcal{Q}_S .*

We first prove the proposition using the lemma, and then we prove the lemma. Let S be a subtree of T . If there is a finite sequence $S = S_0 \subset S_1 \subset \cdots \subset S_m = T$ with each S_{k+1} extending S_k by adding two children to a leaf of S_k then we obtain our result by applying Lemma 3.6 m times. In particular, if T is finite then \mathcal{Q}_S is canonically a subring of \mathcal{Q}_T .

Suppose that $T = \bigcup_{k < \omega} T_k$ with each T_k finite and T_k a subtree of T_{k+1} . Since $I_T = \bigcup_{k < \omega} I_{T_k}$ and $I_{T_m} \cap \mathbb{A}[T_k] = I_{T_k}$ for all $k < m$, it follows that for all $k < \omega$, $I_T \cap \mathbb{A}[T_k] = I_{T_k}$. So each \mathcal{Q}_{T_k} is canonically a subring of \mathcal{Q}_T , and $\mathcal{Q}_T = \bigcup_{k < \omega} \mathcal{Q}_{T_k}$.

This also implies that even if T is infinite and S is any subtree of T , \mathcal{Q}_S is canonically a subring of \mathcal{Q}_T . \square

Proof of Lemma 3.6. Let $J = (I_S)_{\mathbb{A}[T]}$ be the ideal of $\mathbb{A}[T]$ generated by I_S . Since $\mathbb{A}[T] = \mathbb{A}[S][y, z]$ (with y, z algebraically independent over $\mathbb{A}[S]$),

$$\mathbb{A}[T]/J \cong (\mathbb{A}[S]/I_S)[y, z] = \mathcal{Q}_S[y, z]$$

by an isomorphism which is the identity on $\mathbb{A} \cup T$. We have $I_T = (I_S \cup \{x - yz\})_{\mathbb{A}[T]}$ and so

$$\mathcal{Q}_T \cong (\mathbb{A}[T]/J)/(x - yz) \cong \mathcal{Q}_S[y, z]/(x - yz).$$

Since $x - yz$ is a nonconstant polynomial over \mathcal{Q}_S , $(x - yz) \cap \mathcal{Q}_S = \{0\}$ and so \mathcal{Q}_S is a subring of \mathcal{Q}_T .

Let f be a polynomial with coefficients in \mathcal{Q}_S . If $f(y) = 0$ in \mathcal{Q}_T then $f(y) \in (x - yz)$ as an element of $\mathcal{Q}_S[y, z]$, but again since $x - yz$ is a nonconstant polynomial over $\mathcal{Q}_S[y]$, this means that $f = 0$, and so y is transcendental over \mathcal{Q}_S in \mathcal{Q}_T ; the same holds for z . \square

Remark 3.7. Let R be an integral domain. Then $R[x, y, z]/(x - yz) \cong R[y, z]$ canonically (i.e. by the map which is the identity on R, y and z). The point is that this map from $R[y, z]$ to $R[x, y, z]/(x - yz)$ is injective: no polynomial $f \in R[y, z]$ can be divisible by $x - yz$ since in $R[x, y, z]$, x is transcendental over $R[y, z]$.

3.3.2. *Algebraic properties.* In the following, $\text{leaves}(T)$ stands for the set of leaves of a tree T .

Proposition 3.8. *Let T be a tree.*

- (1) \mathbb{A} is (canonically) a subring of \mathcal{Q}_T .
- (2) If T is finite then $\mathcal{Q}_T = \mathbb{A}[\text{leaves}(T)]$, where $\text{leaves}(T)$ is algebraically independent over \mathbb{A} .
- (3) \mathcal{Q}_T is an integral domain.
- (4) No $x \in T$ is a unit of \mathcal{Q}_T .
- (5) If x is a leaf of T then x is prime in \mathcal{Q}_T . If $x \in T$ is not a leaf then x is reducible in \mathcal{Q}_T .

Proof. We first prove the proposition in the case when T is finite. The proof is an induction on the number of nodes in T . For $T = \{r\}$ (the tree whose only node is its root), $\mathcal{Q}_T = \mathbb{A}[r]$ by definition (I_T is trivial). Let T be a finite tree with more than one node. Choose any leaf y of T , and let x be the parent of y on T , and let z be the child of x other than y . Let $S = T \setminus \{y, z\}$. So S is a subtree of T and x is a leaf of S .

By Lemma 3.6, \mathcal{Q}_S is a subring of \mathcal{Q}_T . By induction, \mathbb{A} is a subring of \mathcal{Q}_S , so it is a subring of \mathcal{Q}_T . Let $L = \text{leaves}(S)$. By induction, $\mathcal{Q}_S = \mathbb{A}[L]$, and

so in \mathcal{Q}_S , x is transcendental over $\mathbb{A}[L \setminus \{x\}]$. By Remark 3.7, in \mathcal{Q}_T , $\{y, z\}$ is algebraically independent over $\mathbb{A}[L \setminus \{x\}]$. This shows that $\mathcal{Q}_T = \mathbb{A}[L \cup \{y, z\} \setminus \{x\}] = \mathbb{A}[\text{leaves}(T)]$ with $\text{leaves}(T)$ algebraically independent over \mathbb{A} . This is certainly an integral domain. Every $x \in T$ is the product of irreducible elements (namely the leaves that extend x) and so is not a unit. Every leaf of T is prime, the other nodes are products of several primes.

Suppose that T is an infinite tree. We can write $T = \bigcup_{k < \omega} T_k$, where each T_k is finite and a subtree of T_{k+1} . Proposition 3.5 says that $\mathcal{Q}_T = \bigcup_{k < \omega} \mathcal{Q}_{T_k}$. The properties (1), (2) and (4) carry over to T . Let $x \in T$. If x is a leaf of T then x is prime in every \mathcal{Q}_{T_k} such that $x \in T_k$ and so is prime in \mathcal{Q}_T . Otherwise, $x = yz$ in \mathcal{Q}_T where y and z are the children of x on T , and y and z are nonunits in \mathcal{Q}_T . \square

Corollary 3.9. *For any tree T , \mathcal{Q}_T satisfies the ascending chain condition for principal ideals if and only if T is finite. In fact:*

- (1) *If T is finite then \mathcal{Q}_T is a unique factorization domain.*
- (2) *If T is infinite then \mathcal{Q}_T is not atomic.*

Proof. If T is finite then \mathcal{Q}_T is a polynomial ring over \mathbb{A} , which is a unique factorization domain. By Gauss's lemma, it is a unique factorization domain.

If T is infinite then by König's lemma there is an infinite path $\langle x_n \rangle_{n < \omega}$ in T . Let y_n be the child of x_{n-1} other than x_n . Then $x_{n-1} = x_n y_n$. As y_n is not a unit of \mathcal{Q}_T , x_n properly divides x_{n-1} in \mathcal{Q}_T .

To see that \mathcal{Q}_T is not atomic, we show that the root r of T is not the product of irreducible elements. For let A be a finite multiset of elements of \mathcal{Q}_T such that $r = \prod A$. As in the proof of Proposition 3.8, write $T = \bigcup_{k < \omega} T_k$ as the union of an increasing sequence of finite subtrees. Let k be sufficiently large so that every element of A is in \mathcal{Q}_{T_k} . In \mathcal{Q}_{T_k} , $L = \text{leaves}(T_k)$ is the unique irreducible factorization of r , so (up to association) each element of A is a product of leaves of T_k , and each leaf appears exactly once. Since $T \neq T_k$ we can take some $x \in L$ which is not a leaf of T , and find some $a \in A$ which is divisible by x (in \mathcal{Q}_{T_k} , and so in \mathcal{Q}_T). Then in \mathcal{Q}_T , a is divisible by x and x is a reducible element of \mathcal{Q}_T , and so a is a reducible element of \mathcal{Q}_T . \square

3.3.3. *Pruning.* When we chop off the children of some node on a tree (recall operation 2), we want to invert the left child, making the right child an associate of the parent.

Definition 3.10. Let T be a tree and let Y be a set disjoint from T . Considering Y as a set of indeterminates over $\mathbb{A}[T]$, we let

$$\mathcal{Q}_T^Y = \mathcal{Q}_T[Y, Y^{-1}] = \mathcal{Q}_T[y, y^{-1} : y \in Y].$$

We note that letting $\mathbb{A}^Y = \mathbb{A}[Y, Y^{-1}]$ and $I_T^Y = (I_T)_{\mathbb{A}^Y[T]}$ we have $\mathcal{Q}_T^Y = \mathbb{A}^Y[T]/I_T^Y$ (canonically). Since $\mathbb{A} \cong \mathbb{A}^Y$ and $I_T \cap \mathbb{A} = \{0\}$, we have:

Lemma 3.11. $\mathcal{Q}_T^Y \cong \mathcal{Q}_T$ by an isomorphism which is the identity on T .

The isomorphism though is not canonical since it is not the identity on \mathbb{A} ; there is no canonical way to choose an isomorphism between \mathbb{A} and \mathbb{A}^Y . The combination of Proposition 3.8 and Lemma 3.11 (and the analysis preceding it) gives:

Proposition 3.12. Let T be a tree and Y be a set disjoint from T .

- (1) \mathbb{A}^Y is canonically a subring of \mathcal{Q}_T^Y .

- (2) If T is finite and $L = \text{leaves}(T)$ then $\mathcal{Q}_T^Y = \mathbb{A}^Y[L]$, with L algebraically independent over \mathbb{A}^Y .
- (3) \mathcal{Q}_T^Y is an integral domain.
- (4) No $x \in T$ is a unit of \mathcal{Q}_T^Y .
- (5) If x is a leaf of T then x is prime in \mathcal{Q}_T^Y . If $x \in T$ is not a leaf then x is reducible in \mathcal{Q}_T^Y .
- (6) If T is finite then \mathcal{Q}_T^Y is a unique factorization domain. Otherwise it is not atomic.

And of course, every element of Y is a unit of \mathcal{Q}_T^Y .

Lemma 3.13. *Let T be a subtree of a tree S , and suppose that $S = T \cup \{y, z\}$ where y and z are the children on S of a node x which is a leaf of T . Then $\mathcal{Q}_T^y = \mathcal{Q}_S[y^{-1}]$.*

Thus $\mathcal{Q}_S[y^{-1}] \cong \mathcal{Q}_T$ via an isomorphism which is the identity on T .

Proof. \mathcal{Q}_T is a subring of \mathcal{Q}_S . In \mathcal{Q}_S , y is transcendental over \mathcal{Q}_T (Lemma 3.6), and so in $\mathcal{Q}_S[y^{-1}]$, $\mathcal{Q}_T^y = \mathcal{Q}_T[y, y^{-1}]$. Since $\mathcal{Q}_S[y^{-1}]$ is generated over \mathcal{Q}_T by y, z and y^{-1} , and since $x \in \mathcal{Q}_T$ and $z = y^{-1}x$ in $\mathcal{Q}_S[y^{-1}]$ we obtain the desired equality. \square

Corollary 3.14. *Let T be a subtree of a finite tree S . Let N be the collection of nodes in $S \setminus T$ which are the left child of their parent. Then \mathcal{Q}_T^N is canonically isomorphic to $\mathcal{Q}_S[N^{-1}]$.*

3.4. Linear systems of trees and the associated rings.

3.4.1. Linear systems of trees.

Definition 3.15. A *linear system of trees* is a sequence (either finite or infinite) of finite trees $\langle T_i \rangle$ such that:

- (1) $T_0 = \{r\}$ is the tree with one node;
- (2) For each i , $T_{i-1} \cap T_i$ is a subtree of both T_{i-1} and of T_i ; and
- (3) For each i , the set $T_{i-1} \setminus T_i$ is disjoint from $\bigcup_{j \geq i} T_j$.

If $\mathbb{L} = \langle T_0, T_1, \dots, T_n \rangle$ is a finite linear system of trees then we let $\ell(\mathbb{L}) = n$ be the *length* of \mathbb{L} . If $\mathbb{L} = \langle T_0, T_1, \dots \rangle$ is an infinite sequence then we let $\ell(\mathbb{L}) = \omega$.

If $\mathbb{L} = \langle T_i \rangle$ is an infinite linear system of trees then we let

$$T_\omega = \lim \mathbb{L} = \bigcup_{i < \omega} \bigcap_{j \geq i} T_j.$$

This is in a sense the direct limit of the system \mathbb{L} . The elements of $T_{i-1} \setminus T_i$ are the ones which are discarded at step i , and the elements of T_ω are the ones which “survive” from the step at which they are introduced. Property (3) says that once an element is discarded, it cannot be later reintroduced.

We can append the limit tree T_ω to the sequence and so write $\mathbb{L} = \langle T_i \rangle_{i \leq \ell(\mathbb{L})}$ even when $\ell(\mathbb{L}) = \omega$. For any system (finite or infinite) we write $T_{\mathbb{L}}$ for $T_{\ell(\mathbb{L})}$, the last tree in the system \mathbb{L} .

Example 3.16. Let $S \subseteq 2^{<\omega}$ be a Σ_2^0 subtree of $2^{<\omega}$, and let $\langle S_n \rangle_{n < \omega}$ be an effective approximation of S . Thus, each S_n is a finite subtree of $2^{<\omega}$, the sequence $\langle S_n \rangle$ is computable, and $S = \liminf_{n \rightarrow \infty} S_n = \bigcup_{n < \omega} \bigcap_{m \geq n} S_m$. The sequence $\langle S_n \rangle$ can

be made to satisfy properties (1) and (2) of Definition 3.15 but does not naturally satisfy property (3): usually we change our minds about whether $\sigma \in 2^{<\omega}$ is an element of S or not finitely or even infinitely many times. However a natural relabelling of the elements of S_n by adding the stage number at which they are introduced yields a sequence $\langle T_n \rangle$ canonically isomorphic to $\langle S_n \rangle$ satisfying the definition.

Notation 3.17. Let $\mathbb{L} = \langle T_i \rangle$ be a linear system of tress. We let

$$\text{all}(\mathbb{L}) = \bigcup_{i \leq \ell(\mathbb{L})} T_i$$

be the collection of all nodes which appear along the system, both the discarded ones and the ones which survive until the last tree $T_{\mathbb{L}}$. Let

$$\text{dead}(\mathbb{L}) = \bigcup_{i < \ell(\mathbb{L})} T_i \setminus T_{i+1} = \text{all}(\mathbb{L}) \setminus T_{\mathbb{L}}.$$

be the collection of nodes which are discarded at some step. We let $\text{inv}(\mathbb{L})$ be the collection of elements of $\text{dead}(\mathbb{L})$ which are the left child of their parent.

For a directed system of trees \mathbb{L} we let $\mathcal{Q}_{\mathbb{L}} = \mathcal{Q}_{T_{\mathbb{L}}}^{\text{inv}(\mathbb{L})}$. If $y \in \text{dead}(\mathbb{L}) \setminus \text{inv}(\mathbb{L})$ then inductively (on the height of y) we identify y with the element $z^{-1}x$ of $\mathcal{Q}_{\mathbb{L}}$, where x is the parent of y (y is the right child of x) and z is the left child of x (on any T_i which contains y). As $z \in \text{inv}(\mathbb{L})$, it is already identified with an element of $\mathcal{Q}_{\mathbb{L}}$. Thus we can identify any element of $\text{all}(\mathbb{L})$ with an element of $\mathcal{Q}_{\mathbb{L}}$. By induction we can see:

Lemma 3.18. *In $\mathcal{Q}_{\mathbb{L}}$, every element of $\text{inv}(\mathbb{L})$ is a unit. Every element of $\text{dead}(\mathbb{L})$ is either a unit or an associate of an element of $T_{\mathbb{L}}$.*

The point of this is to enable canonical embeddings corresponding to extending the system of trees. If $\mathbb{L} = \langle T_i \rangle$ is a linear system of trees, and $\beta \leq \ell(\mathbb{L})$, then we let $\mathbb{L} \upharpoonright_{\beta} = \langle T_i \rangle_{i \leq \beta}$. We let $\mathbb{S} \preceq \mathbb{L}$ if $\mathbb{S} = \mathbb{L} \upharpoonright_{\beta}$ for some $\beta \leq \ell(\mathbb{L})$. Certainly if $\mathbb{S} \preceq \mathbb{L}$ then $\text{all}(\mathbb{S}) \subseteq \text{all}(\mathbb{L})$.

Lemma 3.19. *If $\mathbb{S} \preceq \mathbb{L}$ then $\mathcal{Q}_{\mathbb{S}}$ is canonically a subring of $\mathcal{Q}_{\mathbb{L}}$ (the identity map on $\mathbb{A} \cup \text{all}(\mathbb{S})$ induces an embedding of $\mathcal{Q}_{\mathbb{S}}$ into $\mathcal{Q}_{\mathbb{L}}$). If $\ell(\mathbb{L}) = \omega$ then $\mathcal{Q}_{\mathbb{L}} = \bigcup_{n < \omega} \mathcal{Q}_{\mathbb{L} \upharpoonright_n}$.*

Proof. We prove the lemma by induction on $\ell(\mathbb{L})$. We first suppose that $n = \ell(\mathbb{L})$ is finite; by induction, it suffices to treat the case $\mathbb{S} = \mathbb{L} \upharpoonright_{n-1}$. Let $S = T_{n-1} \cap T_n$. Then $N = \text{inv}(\mathbb{L}) \setminus \text{inv}(\mathbb{S})$ is the set of nodes in $T_{n-1} \setminus S$ which are the left child of their parent. By Corollary 3.14, $\mathcal{Q}_{\mathbb{S}}[N^{-1}]$ is canonically isomorphic to $\mathcal{Q}_{\mathbb{S}}^{\text{inv}(\mathbb{L})}$. By Proposition 3.5, $\mathcal{Q}_{\mathbb{S}}^{\text{inv}(\mathbb{L})}$ is canonically a subring of $\mathcal{Q}_{\mathbb{L}}$. Of course $\mathcal{Q}_{\mathbb{S}}$ is canonically a subring of its localisation $\mathcal{Q}_{\mathbb{S}}[N^{-1}]$.

Now suppose that $\ell(\mathbb{L}) = \omega$. For $k < \omega$ let $S_k = T_k \cap T_{\omega}$. Let $R_k = \mathcal{Q}_{S_k}$ and let $Q_k = \mathcal{Q}_{S_k}^{\text{inv}(\mathbb{L}) \upharpoonright_k}$; for brevity we let $N_k = \text{inv}(\mathbb{L}) \upharpoonright_k$, so $Q_k = R_k[N_k, (N_k)^{-1}]$. We have just argued that (canonically) we have

$$\mathcal{Q}_{\mathbb{L} \upharpoonright_0} \subseteq \mathcal{Q}_0 \subseteq \mathcal{Q}_{\mathbb{L} \upharpoonright_1} \subseteq \mathcal{Q}_1 \subseteq \dots$$

so $\bigcup_k \mathcal{Q}_{\mathbb{L} \upharpoonright_k} = \bigcup_k Q_k$, and $\bigcup_k Q_k = (\bigcup_k R_k)[N_{\omega}, (N_{\omega})^{-1}]$ (where $N_{\omega} = \text{inv}(\mathbb{L}) = \bigcup_k N_k$). Since $T_{\omega} = T_{\mathbb{L}} = \bigcup_k S_k$ with each S_k a subring of S_{k+1} , by Proposition 3.5,

$\mathcal{Q}_{T_{\mathbb{L}}} = \bigcup_k R_k$, and so

$$\mathcal{Q}_{\mathbb{L}} = \mathcal{Q}_{T_{\mathbb{L}}}[N_{\omega}, (N_{\omega})^{-1}] = \bigcup_k Q_k = \bigcup_k \mathcal{Q}_{\mathbb{L}_k}$$

(and each $\mathcal{Q}_{\mathbb{L}_k}$ is canonically a subring of $\mathcal{Q}_{\mathbb{L}}$.) \square

3.4.2. Effectiveness of the transformation. We note that if \mathbb{L} is a computable directed system of trees then $\text{all}(\mathbb{L})$ is naturally a computably enumerable set. However in our constructions we can label the new elements of T_k by an extra label k , which makes the set $\text{all}(\mathbb{L})$ computable; we assume this is the case from now. Note though that $\text{dead}(\mathbb{L})$ is c.e. (and $T_{\mathbb{L}}$ is co-c.e.) but not necessarily computable. For this reason, the ring $\mathcal{Q}_{\mathbb{L}}$ as presented above is not computable. By approximating $\mathcal{Q}_{\mathbb{L}}$ with $\mathcal{Q}_{\mathbb{L}_n}$ we can find a computable copy of $\mathcal{Q}_{\mathbb{L}}$.

Proposition 3.20. *Let $\mathbb{L} = \langle T_k \rangle$ be a computable directed system of trees. There is a computable ring Q and an isomorphism $\varphi: \mathcal{Q}_{\mathbb{L}} \rightarrow Q$ such that $\varphi \upharpoonright_{\text{all}(\mathbb{Q})}$ is computable.*

We will identify the computable ring given by the proposition with $\mathcal{Q}_{\mathbb{L}}$.

Proof. By recursion on $n < \omega$ we construct (uniformly) a computable copy Q_n of $\mathcal{Q}_{\mathbb{L}_n}$, such that each Q_n is a computable subset of Q_{n+1} . Further, letting $L_n = \text{leaves}(T_n)$ and $Y_n = \text{inv}(\mathbb{L} \upharpoonright_n)$, we will find a computable subring R_n of Q_n isomorphic to \mathbb{A}^{Y_n} , so $Q_n = R_n[L_n]$ (with L_n algebraically independent over R_n), and the function $n \mapsto L_n$ is computable.

We start with some computable copy Q_0 of $\mathbb{A}[r] = \mathcal{Q}_{\mathbb{L}_0}$ and let $R_0 = \mathbb{A}$. To carry out the construction we first peel off nodes from T_k and then add nodes to $T_k \cap T_{k+1}$ to obtain T_{k+1} . In terms of constructing the rings, it then suffices to show the following.

Claim 3.21. *Let R be a computable subring of a computable unique factorization domain Q , with $Q = R[L]$ where L is finite and algebraically independent over R . Let $x \in L$.*

- (1) *There is a computable presentation A of $Q[x^{-1}]$ such that both Q and $R[x, x^{-1}]$ are computable subsets of A .*
- (2) *There is a computable presentation B of $Q[y, z]/(x - yz)$ such that both R and Q are computable subsets of B .*

Further, all operations are uniform given L , x and computable indices for R and Q .

Proof. For (1), a computable copy A of $Q[x^{-1}]$ is built in a standard way as equality of two presentations of a fraction is a computable relation. However we also note that the collection of pairs $(k, a) \in \omega \times Q$ such that x^k divides a in Q is computable: by a search, we can find the unique polynomial $f \in R[X]$ such that $a = f(L)$ and verify that x^k divides each of its monomials. This shows that Q is a computable subset of A .

We compute membership in $R[x, x^{-1}]$ inside A . The argument above shows that $R[x]$ is a computable subset of Q and so of A . Given $a \in A$ we can effectively find $b \in Q$ and $k < \omega$ such that $a = b/x^k$ and x does not divide b in Q . Then $a \in R[x, x^{-1}]$ if and only if $b \in R[x]$: for if $a \in R[x, x^{-1}]$, say $a = c/x^m$ for some $c \in R[x]$ and $m < \omega$, with x not dividing c ; from $cx^k = bx^m$ and the fact that Q is a unique factorization domain we conclude that $c = b$.

For (2), let $K = R[L \setminus \{x\}]$. As above, K is a computable subset of Q . We can use Remark 3.7 to let $B = K[y, z]$; the embedding of Q into B has a computable range: the polynomials of the form $f(yz)$. The embedding is the identity on K ; since R is a computable subset of Q , it is a computable subset of K and of B .

□_{3.21,3.20}

3.5. Simplifying chains of divisibility in $\mathcal{Q}_{\mathbb{L}}$.

3.5.1. *Monomials and other primes.* Let \mathbb{L} be a linear system of trees.

Definition 3.22. A *monomial* of $\mathcal{Q}_{\mathbb{L}}$ is an associate of a product of elements from $\text{all}(\mathbb{L})$. We let $\text{mon}(\mathbb{L})$ be the collection of monomials in $\mathcal{Q}_{\mathbb{L}}$.

Since every element of $\text{all}(\mathbb{L})$ is either a unit or an associate of an element of $T_{\mathbb{L}}$, a monomial in $\mathcal{Q}_{\mathbb{L}}$ is an associate of a product of elements of $T_{\mathbb{L}}$.

The following is clear:

Lemma 3.23. *If $\mathbb{S} \preceq \mathbb{L}$, then $\text{mon}(\mathbb{S}) \subseteq \text{mon}(\mathbb{L})$. If $\ell(\mathbb{L}) = \omega$ then $\text{mon}(\mathbb{L}) = \bigcup_{k < \omega} \text{mon}(\mathbb{L} \upharpoonright_k)$.*

We will see below that the notion is absolute: $\text{mon}(\mathbb{S}) = \text{mon}(\mathbb{L}) \cap \mathcal{Q}_{\mathbb{S}}$. This is not immediate because theoretically we could have an element of $\mathcal{Q}_{\mathbb{S}} \setminus \text{mon}(\mathbb{S})$ which after some inversions becomes an associate of a product of elements of $T_{\mathbb{L}}$. To give a smooth proof of this absoluteness, we need to examine the other prime elements of $\mathcal{Q}_{\mathbb{L}}$.

Notation 3.24. We let $\text{P}(\mathbb{L})$ be the collection of prime elements of $\mathcal{Q}_{\mathbb{L}}$ which are not associates of leaves of $T_{\mathbb{L}}$, and we let $\text{wfd}(\mathbb{L})$ be the multiplicative subset of $\mathcal{Q}_{\mathbb{L}}$ generated by $\text{P}(\mathbb{L})$.

We note that elements of $\text{P}(\mathbb{L})$ are not divisible (in $\mathcal{Q}_{\mathbb{L}}$) by any element of $T_{\mathbb{L}}$; see Proposition 3.12(5)).

Lemma 3.25. *For each $\mathbb{S} \preceq \mathbb{L}$, $\text{P}(\mathbb{S}) \subseteq \text{P}(\mathbb{L})$.*

Proof. Suppose that $\ell(\mathbb{L}) = \omega$ and that the lemma is known for all systems of finite length. Let $\mathbb{S} = \mathbb{L} \upharpoonright_n$ for some $n < \omega$, and let $p \in \text{P}(\mathbb{S})$. Since $\mathcal{Q}_{\mathbb{L}} = \bigcup_{k \geq n} \mathcal{Q}_{\mathbb{L} \upharpoonright_k}$ and p is prime in each $\mathcal{Q}_{\mathbb{L} \upharpoonright_k}$, p is prime in $\mathcal{Q}_{\mathbb{L}}$ (being prime is an $\forall \exists$ property). Similarly if p is divisible in $\mathcal{Q}_{\mathbb{L}}$ by some $x \in T_{\mathbb{L}}$ then for sufficiently large k , p is divisible in $\mathcal{Q}_{\mathbb{L} \upharpoonright_k}$ by some $x \in T_k = T_{\mathbb{L} \upharpoonright_k}$ (recall that $T_{\omega} = T_{\mathbb{L}} \subseteq \bigcup_{k < \omega} T_k$).

For the finite case, by induction, it suffices to consider the two basic steps of constructing the rings. Let R be a unique factorization domain and let L be a finite set algebraically independent over R . Let $p \in R[L]$ be prime in $R[L]$, which is not an associate of any element of L . Let $x \in L$. We need to show that:

- (1) p is prime in $R[L, x^{-1}]$, and is not an associate of any element of $L \setminus \{x\}$ in $R[L, x^{-1}]$.
- (2) p is prime in $R[L, y, z]/(x - yz)$, and is not an associate of any element of $L \cup \{y, z\} \setminus \{x\}$ in that ring.

For (1), we note that x is the only prime of $R[L]$ which is a unit in $R[L, x^{-1}]$; association classes of elements of $R[L]$ which are not divisible by x are not collapsed in the localisation $R[L, x^{-1}]$.

Property (2) requires more work. Let $Q = R[L \setminus \{x\}]$. By Remark 3.7, $\{y, z\}$ is algebraically independent over Q in $R[L, y, z]/(x - yz)$ and $R[L, y, z]/(x - yz) = Q[y, z]$. Of course $R[L] = Q[x]$. The units of $Q[y, z]$ equal the units of $Q[x]$ equal Q^* , so p is not an associate of any element of $L \setminus \{x\}$ in $Q[y, z]$. Since $p \in Q[x]$ and $y, z \notin Q[x]$, p cannot be an associate of y or of z in $Q[y, z]$. It remains to show that p is prime in $Q[y, z]$. Since $Q[y, z]$ is a unique factorization domain, it suffices to show that p is irreducible in $Q[y, z]$. Recall that we assume that x does not divide p in $Q[x]$. Thus, as a polynomial in x with coefficients from Q , the constant coefficient of p is nonzero, i.e. $p(0) \neq 0$.

Let $g, h \in Q[y, z]$ and suppose that $p = gh$. We need to show that one of g or h is a unit of $Q[y, z]$. Again we think of g and of h as polynomials in y and z : $p(x) = p(yz) = g(y, z)h(y, z)$.

We deal with several cases.

First, suppose that $\deg_x p = 0$, i.e., that $p \in Q$. In this case, g dividing p implies that $g \in Q$, and similarly $h \in Q$. Since p is irreducible in $Q[x]$ (and so in Q), one of g or h is a unit of Q , and so a unit of $Q[y, z]$.

Suppose that $\deg_z g = \deg_y h = 0$, i.e., that $g \in Q[y]$ and $h \in Q[z]$. We substitute $z = 0$. Since $x = yz$ this implies that $x = 0$, so we obtain $0 \neq p(0) = g \cdot h(0)$. It follows that $g \in Q$, and similarly $h \in Q$, so $p \in Q$, which returns us to the first case.

Thus, without loss of generality, we can assume that $d = \deg_y g > 0$ and $e = \deg_y h > 0$. We claim that this case is impossible. Aiming for a contradiction, we write h and g as elements of $C[z][y]$:

$$g = \sum_{i \leq d} g_i(z)y^i \quad \text{and} \quad h = \sum_{i \leq e} h_i(z)y^i.$$

The ring \mathbb{A} contains infinitely many units. So we can choose some nonzero $\alpha \in \mathbb{A}$ such that $g_d(\alpha) \neq 0$ and $h_e(\alpha) \neq 0$. Consider the polynomial

$$\bar{g} = g(x/\alpha, \alpha) = \sum_{i \leq d} \alpha^{-i} g_i(\alpha) x^i;$$

then $\deg_x \bar{g} = d > 0$. Similarly, $\deg_x \bar{h} = e > 0$ where $\bar{h} = h(x/\alpha, \alpha)$. On the other hand $p = p(x/\alpha \cdot \alpha) = \bar{g} \cdot \bar{h}$, and so in $Q[x]$ we see that p is the product of two nonconstant polynomials, neither of which can be a unit of $Q[x]$; this contradicts the assumption that p is irreducible in $Q[x]$. \square

Lemma 3.26. *Every element of $\mathcal{Q}_{\mathbb{L}}$ is the product of a monomial $m \in \text{mon}(\mathbb{L})$ and an element of $\text{wfd}(\mathbb{L})$.*

Proof. If \mathbb{L} is finite then the lemma follows from $\mathcal{Q}_{\mathbb{L}}$ being a unique factorization domain, and the fact that the irreducible elements of $\mathcal{Q}_{\mathbb{L}}$ are partitioned into $\text{P}(\mathbb{L})$ and the leaves of $T_{\mathbb{L}}$.

If \mathbb{L} is infinite, then the lemma follows from the finite case using the upward absoluteness of the monomials and the other primes (Lemmas 3.23 and 3.25) using of course the fact that $\mathcal{Q}_{\mathbb{L}} = \bigcup_{k < \omega} \mathcal{Q}_{\mathbb{L}_k}$. \square

Corollary 3.27. *Every irreducible element of $\mathcal{Q}_{\mathbb{L}}$ is prime (that is, $\mathcal{Q}_{\mathbb{L}}$ is an AP-domain).*

As mentioned in Section 2, this implies that $\mathcal{Q}_{\mathbb{L}}$ is a U-UFD: while some elements may not have an irreducible factorization, an element which does have one has a unique one up to association.

Proof. Let $p \in \mathcal{Q}_{\mathbb{L}}$ be irreducible. By Lemma 3.26, either $p \in \mathbf{wfd}(\mathbb{L})$ or p is a monomial of $\mathcal{Q}_{\mathbb{L}}$. In the first case p is a product of prime elements, and so is prime. In the second case p must be a leaf of T , and so is prime (Proposition 3.12(5)). \square

Lemma 3.28. *Suppose that $\ell(\mathbb{L}) = \omega$. Then $\mathbf{wfd}(\mathbb{L}) = \bigcup_{k < \omega} \mathbf{wfd}(\mathbb{L} \upharpoonright_k)$.*

Proof. We first show that $\mathbf{P}(\mathbb{L}) = \bigcup_{k < \omega} \mathbf{P}(\mathbb{L} \upharpoonright_k)$. We take $p \in \mathbf{P}(\mathbb{L})$ and need to show that $p \in \mathbf{P}(\mathbb{L} \upharpoonright_k)$ for some $k < \omega$. Let $i < \omega$ such that $p \in \mathcal{Q}_{\mathbb{L} \upharpoonright_i}$. By Lemma 3.26, $p = cm$ where $c \in \mathbf{wfd}(\mathbb{L} \upharpoonright_i)$ and $m \in \mathbf{mon}(\mathbb{L} \upharpoonright_i)$. By Lemma 3.23, $m \in \mathbf{mon}(\mathbb{L})$. However no proper monomial of $\mathcal{Q}_{\mathbb{L}}$ divides p in $\mathcal{Q}_{\mathbb{L}}$, and so m is a unit of $\mathcal{Q}_{\mathbb{L}}$. In other words, $p \sim c$ in $\mathcal{Q}_{\mathbb{L}}$.

We observe that $c \in \mathbf{P}(\mathbb{L} \upharpoonright_i)$: let C be a prime factorization of c in $\mathcal{Q}_{\mathbb{L} \upharpoonright_i}$. Each element of C is prime in $\mathcal{Q}_{\mathbb{L}}$. Since p is irreducible in $\mathcal{Q}_{\mathbb{L}}$, $|C| = 1$.

There is some $k \geq i$ such that m is a unit of $\mathcal{Q}_{\mathbb{L} \upharpoonright_k}$. By Lemma 3.25, $c \in \mathbf{P}(\mathbb{L} \upharpoonright_k)$, and $p \sim c$ in $\mathcal{Q}_{\mathbb{L} \upharpoonright_k}$, as required.

Now we prove the lemma. Let $c \in \mathbf{wfd}(\mathbb{L})$; $c = \prod C$ where C is a (finite) multiset of elements of $\mathbf{P}(\mathbb{L})$. There is some $k < \omega$ such that each $p \in C$ is in $\mathbf{P}(\mathbb{L} \upharpoonright_k)$. Then $c \in \mathbf{wfd}(\mathbb{L} \upharpoonright_k)$. \square

Corollary 3.29. *Let $m, m' \in \mathbf{mon}(\mathbb{L})$, $c, c' \in \mathbf{wfd}(\mathbb{L})$, and suppose that mc divides $m'c'$ in $\mathcal{Q}_{\mathbb{L}}$. Then m divides m' and c divides c' (in $\mathcal{Q}_{\mathbb{L}}$). Hence, the presentation of an element of $\mathcal{Q}_{\mathbb{L}}$ as the product of a monomial and an element of $\mathbf{wfd}(\mathbb{L})$ is unique up to association.*

Proof. If \mathbb{L} is finite, then this again follows from the fact that $\mathcal{Q}_{\mathbb{L}}$ is a unique factorization domain. If $\ell(\mathbb{L}) = \omega$ then by Lemmas 3.23 and 3.28, $m, m' \in \mathbf{mon}(\mathbb{L} \upharpoonright_k)$ and $c, c' \in \mathbf{wfd}(\mathbb{L} \upharpoonright_k)$ for some $k < \omega$. If k is sufficiently late then mc divides $m'c'$ in $\mathcal{Q}_{\mathbb{L} \upharpoonright_k}$. We then apply the finite case. \square

It follows that in $\mathcal{Q}_{\mathbb{L}}$, no non-unit monomial can divide a non-unit element of $\mathbf{wfd}(\mathbb{L})$, and vice-versa.

Remark 3.30. If $\mathbb{S} \preccurlyeq \mathbb{L}$ then $\mathbf{mon}(\mathbb{S}) = \mathbf{mon}(\mathbb{L}) \cap \mathcal{Q}_{\mathbb{S}}$. To see this, note that any divisor of $a \in \mathcal{Q}_{\mathbb{S}}$ in $\mathbf{wfd}(\mathbb{S})$ is a non-unit divisor of a in $\mathbf{wfd}(\mathbb{L})$.

Note however that it is quite likely that there are $a \in \mathbf{wfd}(\mathbb{L}) \cap \mathcal{Q}_{\mathbb{S}}$ which are not in $\mathbf{wfd}(\mathbb{S})$; some monomial of $\mathcal{Q}_{\mathbb{S}}$ divides a in $\mathcal{Q}_{\mathbb{S}}$, but that monomial is a unit of $\mathcal{Q}_{\mathbb{L}}$.

3.5.2. Monomials and the failure of accp. Recall that an *infinite chain of proper divisions* in an integral domain R is a sequence a_0, a_1, \dots of elements such that each a_{n+1} properly divides a_n . In other words it is a counter example to the ascending chain condition for principal ideals.

Proposition 3.31. *Let \mathbb{L} be a computable linear system of trees. Every sequence of proper divisions in $\mathcal{Q}_{\mathbb{L}}$ computes a sequence of proper divisions consisting of monomials.*

Proof. Let $\langle a_n \rangle$ be a sequence of proper divisions in $\mathcal{Q}_{\mathbb{L}}$. For each $n < \omega$ we write $a_n = c_n m_n$, where $c_n \in \mathbf{wfd}(\mathbb{L})$ and m_n is a monomial of $\mathcal{Q}_{\mathbb{L}}$.

By Corollary 3.29, $c_{n+1} \mid c_n$ for all n . The divisibility relation of $\mathcal{Q}_{\mathbb{L}}$ restricted to $\mathbf{wfd}(\mathbb{L})$ is well-founded as each element of $\mathbf{wfd}(\mathbb{L})$ is a product of primes. Hence there is some n^* such that for all $n \geq n^*$, $c_n \sim c_{n^*}$. It follows that for all $n \geq n^*$, m_{n+1} properly divides m_n . The desired sequence is $\langle a_n/c_{n^*} \rangle_{n \geq n^*}$. \square

3.5.3. *Monomial decompositions.* Recall that multisets are sets which record multiplicities. We only consider finite multisets (and so finite multiplicities).

Definition 3.32. Let \mathbb{L} be a linear system of trees, and let $m \in \mathbf{mon}(\mathbb{L})$. A *monomial decomposition* (or *factorization*) of m is a multiset M of elements of $\mathbf{all}(\mathbb{L})$ such that $m \sim \prod M$.

We emphasize that a monomial factorization of a monomial m is far from unique, even if we restrict ourselves to nodes from $T_{\mathbb{L}}$. Given $m \in \mathbf{mon}(\mathbb{L})$ we can effectively find *some* monomial decomposition M of m , by enumerating multisets and waiting for a unit witnessing that $m \sim \prod M$.

Definition 3.33. Let \mathbb{L} be a linear system of trees; let M and N be multisets of elements of $\mathbf{all}(\mathbb{L})$. We write $M \preceq_{\mathbb{L}} N$ if $\prod M$ divides $\prod N$ in $\mathcal{Q}_{\mathbb{L}}$. We write $M \prec_{\mathbb{L}} N$ if $M \preceq_{\mathbb{L}} N$ but $N \not\preceq_{\mathbb{L}} M$.

Lemma 3.34. *If \mathbb{L} is finite then the relation $\preceq_{\mathbb{L}}$ is computable, uniformly in \mathbb{L} . If \mathbb{L} is infinite then the relation $\preceq_{\mathbb{L}}$ is c.e. in \mathbb{L} .*

Proof. If \mathbb{L} is finite then we let L be the set of leaves of $T_{\mathbb{L}}$. Given any multiset M of elements of $\mathbf{all}(\mathbb{L})$ we can effectively find a multiset \bar{M} of elements of L such that $\prod \bar{M} \sim \prod M$. If M and N are multisets of elements of L then $M \preceq_{\mathbb{L}} N$ if and only if $M \subseteq N$ (multiset inclusion, which means the multiplicity of any element $x \in L$ in M is no greater than its multiplicity in N .)

Suppose that \mathbb{L} is infinite, and let M and N be multisets of elements of $\mathbf{all}(\mathbb{L})$. Then $M \preceq_{\mathbb{L}} N$ if and only if there is some $k < \omega$ such that all the elements of M and N are from $\mathbf{all}(\mathbb{L} \upharpoonright_k)$ and $M \preceq_{\mathbb{L} \upharpoonright_k} N$. \square

Again we emphasize that it is possible that M and N are multisets of elements of $\mathbf{all}(\mathbb{L} \upharpoonright_k)$, that $M \preceq_{\mathbb{L}} N$ but that $M \not\preceq_{\mathbb{L} \upharpoonright_k} N$. The reason is that M may contain elements which later become units.

Definition 3.35. Let \mathbb{L} be an infinite linear system of trees. A sequence $\langle M_n \rangle$ of multisets of elements of $\mathbf{all}(\mathbb{L})$ is *properly decreasing* if for all n , $M_{n+1} \prec_{\mathbb{L}} M_n$.

Proposition 3.31 and the observation that from a monomial we can obtain *some* decomposition yield:

Corollary 3.36. *Let \mathbb{L} be a computable linear system of trees. Every sequence of proper divisions in $\mathcal{Q}_{\mathbb{L}}$ computes a properly decreasing sequence of multisets of elements of $\mathbf{all}(\mathbb{L})$.*

Corollary 3.36 is the final step in our programme to hide the algebra in our constructions. When building systems \mathbb{L} we never make reference to the ring $\mathcal{Q}_{\mathbb{L}}$; rather, we control the complexity of properly decreasing sequences of multisets.

4. THE HARDNESS RESULT

In this section we prove Theorems 1.1 and 1.2. We start with coding \emptyset' .

Proof of Theorem 1.2. Let f be a computable function whose range is \emptyset' .

Define a linear system of trees $\mathbb{L} = \langle T_k \rangle$ by letting each T_s be the “fishbone” tree of length s ; $f(s)$ is the length of agreement between T_s and T_{s+1} . In detail, T_s will consist of the root $a_{0,s}$ and nodes $a_{k,s}$ and $b_{k,s}$ for $k \in [1, \dots, s]$, with $a_{k+1,s}$ being the right child of $a_{k,s}$ and $b_{k+1,s}$ being the left child of $a_{k,s}$. For $k < f(s)$ we let $a_{k,s+1} = a_{k,s}$ and $b_{k,s+1} = b_{k,s}$; for $k \geq f(s)$, $a_{k,s+1}$ and $b_{k,s+1}$ will be new elements not used before. In other words $T_s \cap T_{s+1}$ consists of the first $f(s)$ many levels of T_s . In ring terms, the elements $b_{k,s}$ for $k \geq f(s)$ are inverted in $\mathcal{Q}_{\mathbb{L} \upharpoonright_{s+1}}$, and so $a_{s,s}$ becomes associate with $a_{f(s)-1,s}$ in that ring.

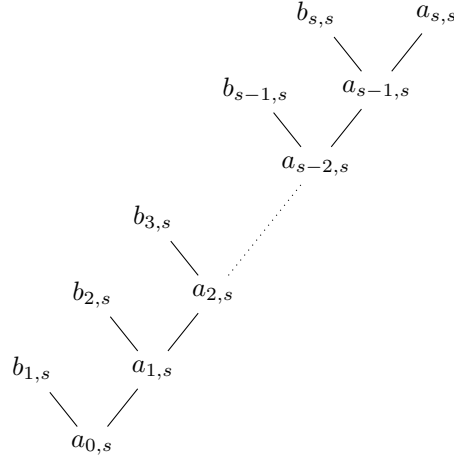


FIGURE 3. The fishbone T_s .

We claim that the ring $\mathcal{Q}_{\mathbb{L}}$ is as required. We first analyse multisets of elements of $\text{all}(\mathbb{L})$.

Let M be such a multiset. For sufficiently large s , every element of M is in $\text{all}(\mathbb{L} \upharpoonright_s)$. For such s we let $M[s]$ be the unique multiset of leaves of T_s such that $\prod M \sim \prod M[s]$. As mentioned in the proof of Lemma 3.34, it is easy to compute $M[s]$ given M . The leaves of T_s are $a_{s,s}$ and $b_{k,s}$ for $k = 1, \dots, s$. To obtain $M[s+1]$ from $M[s]$ we first extract every copy of $a_{s,s}$ and $b_{k,s}$ for $k \geq f(s)$; and then add copies of $a_{s+1,s+1}$ and $b_{k,s+1}$ for $k = f(s), \dots, s+1$; with multiplicities all equaling the multiplicity of $a_{s,s}$ in $M[s]$. In particular the multiplicity of $a_{s,s}$ in $M[s]$ does not depend on s ; we denote this multiplicity by $m(M)$.

Let $k \geq 1$ and let $s^* = s^*(M)$ be the least s such that $M[s]$ is defined. Let $k^* = k^*(M) = \min \{f(t) : t \geq s^*\}$. Let $t \geq s^*$ such that $f(t) = k^*$. Then for all $s > t$, the multiplicity of $b_{k,s}$ in $M[s]$ is $m(M)$. For $k < k^*$, the multiplicity of $b_{k,s}$ in $M[s]$ is constant for all $s \geq s^*$. We denote this constant value by $b_k(M)$.

Say N is another such multiset and $N \preceq_{\mathbb{L}} M$. Then for all sufficiently late s , $N[s] \subseteq M[s]$. This implies that $m(N) \leq m(M)$. If $m(N) < m(M)$ then $N \prec_{\mathbb{L}} M$. Suppose that $m(N) = m(M)$ and that $N \prec_{\mathbb{L}} M$. Then there must be some $k < k^*(M), k^*(N)$ such that $b_k(N) < b_k(M)$.

Let $\langle M_n \rangle$ be a properly decreasing sequence of multisets of elements of $\text{all}(\mathbb{L})$. Since $m(M_{n+1}) \leq m(M_n)$, the sequence $m(M_n)$ eventually stabilizes. By taking a final segment of the sequence, we may assume that $m(M_n)$ is constant for all n .

For each n , find some sufficiently late s such that $M_n[s]$ and $M_{n+1}[s]$ are both defined. Find the least k such that the multiplicity of $b_{k,s}$ in $M_{n+1}[s]$ is smaller than its multiplicity in $M_n[s]$. Then for all $t \geq s$, $f(t) > k$, in other words \emptyset'_s is correct up to k . To show that this allows us to compute \emptyset' we need to show that these numbers k are unbounded as we scan larger and larger n . But the numbers $b_k(M_n)$ are non-decreasing with n . So they cannot drop infinitely often for finitely many values of k . \square

4.1. Reverse mathematics.

Proof of Theorem 1.1. We show that Theorem 1.2 can be proved in RCA_0 . More precisely: in RCA_0 we show that for every function $f: \mathbb{N} \rightarrow \mathbb{N}$ there is a non-atomic integral domain R such that every infinite chain of divisibility in R computes (together with f) the range of f . This immediately implies that Theorem B implies ACA_0 over RCA_0 . Further, we observe that the domain R produced is an AP-domain; this implies that Theorem A implies ACA_0 over RCA_0 .

It is not actually the case that all of our arguments above can be carried out in RCA_0 as-is. For example, in the very first definition of \mathcal{Q}_T , even if T is computable, the ideal I_T may fail to be computable. So some care must be taken.

Working in RCA_0 , we start with a function $f: \mathbb{N} \rightarrow \mathbb{N}$. The sequence of trees $\mathbb{L} = \langle T_s \rangle_{s \in \mathbb{N}}$ defined in the proof of Theorem 1.2 certainly exists. The next step is to construct an increasing sequence $\langle Q_s \rangle$ of rings which play the role of $\mathcal{Q}_{\mathbb{L}|_s}$. We rely on the characterisation given by Proposition 3.12(2) and the construction given in Proposition 3.20. Let L_s be the set of leaves of T_s , and let $Y_s = \text{inv}(\mathbb{L}|_s) \cup \{t_n : n \in \mathbb{N}\}$. Then we let $Q_s = \mathbb{Q}[L_s, Y_s, Y_s^{-1}]$. The standard embedding of Q_s into Q_{s+1} exists and moreover its image exists, uniformly in s .

For further analysis of the rings Q_s we appeal to the well-known Schubert-Kronecker algorithm, which can be carried out in RCA_0 . The algorithm shows that the set of irreducible polynomials in $\mathbb{Q}[x_1, \dots, x_n]$ is computable, uniformly in n . Since association of polynomials is computable, the divisibility relation in these rings is computable too. A direct argument can now be made to show that each of these polynomial rings is atomic. To show that each such ring is a UFD, it now suffices to show that each such ring is an AP-domain. This is proved by induction on n , using the arguments proving Gauss's lemma. The reason that Σ_1^0 induction suffices is that irreducibility and divisibility are computable in these rings (uniformly in s). This makes the statement that $\mathbb{Q}[x_1, \dots, x_n]$ is an AP-domain Π_1^0 . We mentioned above that the standard proof that AP domains are U-UFDs can be carried out in RCA_0 .

Further we note that every irreducible element of $\mathbb{Q}[x_1, \dots, x_n]$ is irreducible also in $\mathbb{Q}[x_1, \dots, x_{n+1}]$, and by induction, in $\mathbb{Q}[x_1, x_2, \dots]$, and that no new units are added. Further, in RCA_0 we show that the localisation of a UFD is a UFD. It follows that: every ring Q_s is a UFD; divisibility and irreducibility in the rings Q_s exists (uniformly in s). The tree T_ω may not exist, but the ring Q_ω does, and is shown to be non-atomic. Hence there is a sequence $\langle a_n \rangle$ of elements of Q_ω , each a_{n+1} properly dividing a_n .

The analysis of Subsection 3.5.1 is followed verbatim. Proposition 3.31 also holds. The point is that the sets $\text{wfd}(\mathbb{L}|_s)$ and $\text{mon}(\mathbb{L}|_s)$ exist, uniformly in s . Given the sequence $\langle a_n \rangle_{n \in \mathbb{N}}$, we can, for each $n \in \mathbb{N}$, first find $s(n) \in \mathbb{N}$ such that $a_n \in Q_{s(n)}$, and then find $c_n \in \text{wfd}(\mathbb{L}|_{s(n)})$ and $m_n \in \text{mon}(\mathbb{L}|_{s(n)})$ such that $a_n = c_n m_n$. The

sequences $\langle c_n \rangle$ and $\langle m_n \rangle$ exist, and for all n , c_{n+1} divides c_n . Further, let C_n be a finite multiset of elements of $\mathcal{P}(\mathbb{L} \upharpoonright_{s(n)})$ such that $c_n = \prod C_n$. Then $|C_{n+1}| \leq |C_n|$ and if c_{n+1} divides c_n properly, then $|C_{n+1}| < |C_n|$. Since the sequence $\langle |C_n| \rangle$ exists, there is some $n^* \in \mathbb{N}$ such that for all $m \geq n$, $|C_m| = |C_n|$. After renaming, we obtain a properly decreasing sequence $\langle M_n \rangle$ of multisets of elements of $\text{all}(\mathbb{L})$.

We now join the proof of Theorem 1.2. The sequence of numbers $\langle m(M_n) \rangle$ exists and is non-increasing, and so stabilizes on a value m^* ; so we may assume that this value is constant for all $n \in \mathbb{N}$. The array $\langle M_n[s] \rangle$ exists. In RCA_0 we can show that for all n there is some $s = s(n)$ such that for some $k < n$, the multiplicity of $b_{k,s}$ in $M_{n+1}[s]$ is smaller than its multiplicity in $M_n[s]$. We let $k(n)$ be the least such k .

In RCA_0 we carry out the argument showing that for all n , for all $t \geq s(n)$, $f(t) > k(n)$. It remains to show in RCA_0 that for all $K \in \mathbb{N}$ there is some n such that $k(n) \geq K$. To do so we define a sequence of numbers $\langle n(j) \rangle_{j \in \mathbb{N}}$ such that $k(n(j)) \geq j$ by effective recursion. Given $n(j)$, let c be the sum of the multiplicities of $b_{k,s}$ in $M_n[s]$ for all $k \leq j$, where $n = n(j)$ and $s = s(n(j))$. For all $s \geq s(n(j))$, $f(s) > j$, so in the interval $(n(j), n(j) + c]$ there must be some m such that $k(m) > j$; let $n(j+1) = m$. \square

5. THE INSUFFICIENCY RESULT

In this section we prove Theorem 1.3: there is a computable, non-atomic integral domain R such that \emptyset' does not compute any infinite chain of divisibility in R .

For a tree T we define \preceq_T and \sim_T as $\preceq_{\mathbb{L}}$ and $\sim_{\mathbb{L}}$ where $\mathbb{L} = \langle T \rangle$. In other words for multisets of elements of T , multiset equivalence is generated by the operation of replacing a node with both its successors in T . This gives rise to the notion of decreasing and properly decreasing sequences of multisets of elements of T . We prove the following.

Proposition 5.1. *There is an infinite Σ_2^0 tree $T \subseteq 2^{<\omega}$ such that there is no Δ_2^0 properly decreasing sequence of multisets of elements of T .*

Proof of Theorem 1.3, assuming Proposition 5.1: We use the translation technique outlined in Example 3.16. Let T be given by the proposition, and let $\langle T_s \rangle$ be a computable semi-approximation of T ($\sigma \in T$ if and only if $\sigma \in T_s$ for almost all s). We define a linear system of trees \mathbb{L} by attaching stage number labels to nodes; if σ is added to T_s then we add (s, σ) to the s^{th} tree in \mathbb{L} . The limit tree $T_{\mathbb{L}}$ is isomorphic to T via the map $(s, \sigma) \mapsto \sigma$ which is of course the restriction to $T_{\mathbb{L}}$ of a computable map, and so is a Δ_2^0 -computable isomorphism. We claim that $\mathcal{Q}_{\mathbb{L}}$ is as required. Suppose that there is a Δ_2^0 sequence $\langle a_n \rangle$ of proper divisibility in $\mathcal{Q}_{\mathbb{L}}$. By Corollary 3.36 there is a Δ_2^0 properly decreasing sequence $\langle M_n \rangle$ of multisets of elements of $\text{all}(\mathbb{L})$. The halting problem \emptyset' can convert each multiset in $\text{all}(\mathbb{L})$ to a multiset of elements of $T_{\mathbb{L}}$, so we may assume that each $\langle M_n \rangle$ only contains elements of $T_{\mathbb{L}}$. Now applying the isomorphism from $T_{\mathbb{L}}$ to T gives a Δ_2^0 properly decreasing sequence of elements of T . \square

5.1. Discussion. We now informally discuss the proof of Proposition 5.1. We construct a computable semi-approximation $\langle T_s \rangle$ of T . Suppose that we first try to diagonalise against a computable sequence $\langle M_k \rangle$ of multisets of finite binary strings. The idea is the following. Assume that we start with $T = 2^{<\omega}$. By passing to an equivalent multiset we may assume that all strings in M_0 have some length s_0 .

We choose a string ρ_0 of length s_0 ; let m_0 be the multiplicity of ρ_0 in M_0 . We then declare that all other strings of length s_0 are terminal on T ; the construction henceforth will be limited to extensions of ρ_0 . If indeed each M_k is a multiset of strings on T , then each multiset M_k is equivalent to the multiset union (sum) $A_k + B_k$, where A_k consists of strings of length s_0 which are incomparable with ρ_0 ; and B_k of strings of some length $t_k > s_0$, all extending ρ_0 . If the sequence is decreasing then $A_{k+1} \subseteq A_k$; since A_0 is finite, the sequence $\langle A_k \rangle$ must stabilise. If the sequence $\langle M_k \rangle$ is properly decreasing, this means that eventually, some element of B_k must have multiplicity smaller than m_0 . We pick such k , declare $s_1 = t_k$, choose ρ_1 to be some element of B_k of multiplicity $m_1 < m_0$, and repeat the process by declaring that the strings in T of length s_1 other than ρ_1 are terminal on T . This process clearly must terminate: eventually we find some ρ_n for which we cannot find any M_k with elements extending ρ_n of multiplicity smaller than m_n (for example if $m_n = 0$). In this way we force $\langle M_k \rangle$ to fail to be properly decreasing. We can then move on to diagonalize against the next sequence of multisets, still restricting ourselves though to only extending ρ_n .

As described this construction works if the sequences $\langle M_k \rangle$ we are diagonalising against are computable. If $\langle M_k \rangle$ is merely Δ_2^0 then at each stage s we only have an approximation $M_{k,s}$, which may or may not stabilise to a final M_k . Of course if the approximation does not stabilise then the requirement is met vacuously. If for example we see that M_0 changed then we can cancel ρ_0 and rescind the declaration that other strings of length s_0 are terminal on T .

What is the effect on the construction if the approximation to $\langle M_k \rangle$, say even to M_0 , does not stabilise? In that case we would like the tree to be passed to the next requirement be all of $2^{<\omega}$, that is, we do not want the first requirement to exclude any string from T . This is easily achieved by requiring that each subsequent time a new definition of a string ρ_0 is made, it is made longer and longer, so that each length is eventually protected from the action for the itinerant M_0 .

We need to consider though the effect on weaker requirements. The next requirement surely needs to know what the first requirement does; if M_0 does not stabilize then it needs to know that it should not wait for a string ρ_0 below which it must work. This is achieved by a Π_2^0 / Σ_2^0 guessing procedure, so we employ a tree of strategies. Each strategy will be concerned with *one step* toward meeting a requirement, rather than fully meeting the requirement. If $\langle M_{k,s}^0 \rangle$ is the first approximation that we need to work against, then the root strategy works on defining ρ_0 ; a child $\langle \infty \rangle$ of the root strategy believes that M_0 does not stabilize, and so works for the next requirement; whereas other children of the root strategy guess a value for ρ_0 (and m_0) and try to define ρ_1 , so are still working for the first requirement. The outcome $\langle \infty \rangle$ is the stronger one — so this strategy working for the second requirement is stronger than the strategies working for the second step of the first requirement.

Consider a strategy γ extending $\alpha \hat{\infty}$ for some α , and a child δ of α (other than $\alpha \hat{\infty}$). Each strategy ϵ is working above some string $\rho(\epsilon)$ (and declares other strings on T of that length to be terminal); so both γ and δ work above the string $\rho(\alpha)$. There are two points to consider (see Fig. 4).

- It would be very bad if δ eliminated $\rho(\gamma)$ from T , in fact if γ is correct it would want $\rho(\gamma)$ and many extensions of $\rho(\gamma)$ to stay on T . This is easily achieved as discussed above, by requiring that the string $\rho(\delta)$ chosen by δ

- is longer than $\rho(\gamma)$, and in fact as we cycle through various δ 's between returning to γ , the corresponding strings $\rho(\delta)$ must get longer and longer.
- On the other hand, when searching for $\rho(\delta)$, α cannot agree to restrict the search to extensions of $\rho(\gamma)$. This is because it is possible that the drops in multiplicities above $\rho(\alpha)$ all occur away from $\rho(\gamma)$. All (sufficiently long) extensions of $\rho(\alpha)$ must be considered. From the point of view of γ , this is not a problem. When we go back to γ we simply erase the long strings not extending $\rho(\gamma)$ from T . If this happens infinitely often, these strings are not on T .

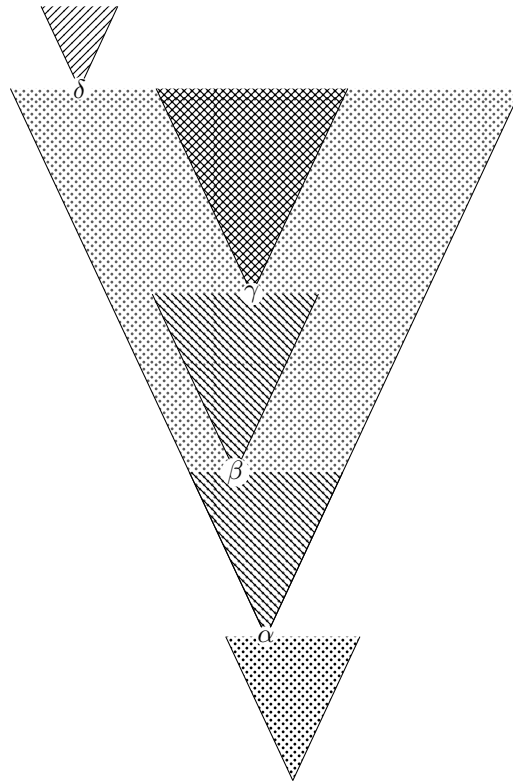


FIGURE 4. The interaction of α , γ and δ (where $\gamma \succ \beta \succ \alpha \hat{=} \infty$ but δ is another child of α). We write α for $\rho(\alpha)$ etc. The string $\rho(\delta)$ must be longer than $\rho(\gamma)$ since γ was visited before δ . The strategies α and δ work for the same requirement, as indicated by the fill pattern, as do β and γ .

5.2. **Construction.** We can now give the formal construction.

5.2.1. *The tree of strategies.* We start with the definition of the tree of strategies. For each strategy we define three parameters: (1) $e(\alpha)$, the index of the requirement for which the strategy α works; (2) $\rho(\alpha)$, the string above which α works; and (3) $m(\alpha) \leq \omega$, the multiplicity which α needs to decrease.

We start with the root (the empty string $\langle \rangle$); we set $e(\langle \rangle) = 0$, $\rho(\langle \rangle) = \langle \rangle$ and $m(\langle \rangle) = \omega$.

Suppose that α is a strategy. The children (immediate successors) of α on the tree of strategies are: (a) $\alpha^\wedge \infty$; and (b) $\alpha^\wedge(\tau, n, k)$ where $n < m(\alpha)$, τ properly extends $\rho(\alpha)$ and $k < \omega$. The parameters for the children are defined as follows: $e(\alpha^\wedge \infty) = e(\alpha) + 1$ (we move to the next requirement), $\rho(\alpha^\wedge \infty) = \rho(\alpha)$, and $m(\alpha^\wedge \infty) = \omega$; and $e(\alpha^\wedge(\tau, n, k)) = e(\alpha)$, $\rho(\alpha^\wedge(\tau, n, k)) = \tau$, and $m(\alpha^\wedge(\tau, n, k)) = n$. The number k indicates the index of the multiset M_k^e which witnesses the multiplicity n of τ .

With each strategy α we associate a tree $T(\alpha)$ which specifies the strings which α allows to stay on T . We start with $T(\langle \rangle) = 2^{<\omega}$. Given $T(\alpha)$ we let $T(\alpha^\wedge \infty) = T(\alpha)$, while $T(\alpha^\wedge(\tau, n, k))$ is the tree obtained from $T(\alpha)$ by removing all strings longer than τ but which do not extend τ . In other words, if $\langle \rangle = \alpha_0 \prec \alpha_1 \prec \alpha_2 \prec \dots \prec \alpha_k = \alpha$ are α 's predecessors on the tree of strategies then

$$T(\alpha) = D(\rho(\alpha_0), |\rho(\alpha_1)|) \cup D(\rho(\alpha_1), |\rho(\alpha_2)|) \cup \dots \\ \cup D(\rho(\alpha_{k-1}), |\rho(\alpha_k)|) \cup D(\rho(\alpha_k), \omega)$$

where for a string σ and $n \geq |\sigma|$ we let

$$D(\sigma, n) = \{\tau \succ \sigma : |\tau| \leq n\}.$$

5.2.2. Δ_2^0 sequences of multisets. If M is a multiset of strings and τ is a string which has no proper extensions in M then we define the multiplicity of τ in M to be the number of initial segments of τ in M (with multiplicities counted of course). This of course is the multiplicity of τ in a multiset equivalent to M which does not contain other strings comparable with τ . If τ has proper extensions in M then we say that the multiplicity of τ in M is undefined (because it may be ‘fractional’).

Let $\langle M_{k,s}^e \rangle$ be a primitive recursive enumeration of finite multisets of strings such that if $\langle M_k \rangle$ is a Δ_2^0 sequence of finite multisets of strings then there is some e such that for all k , $M_k = M_{k,s}^e$ for all but finitely many s .

5.2.3. *Construction.* At stage s we define which strategies are accessible. The empty strategy is always accessible.

Suppose that a strategy α is accessible at stage s , and that $|\alpha| < s$. If s is the first stage at which α is accessible, then we let $\alpha^\wedge \infty$ be next accessible. Otherwise, let t be the previous stage at which α was accessible. Now there are two possibilities.

- (1) At stage t , $\alpha^\wedge(\tau, n, k)$ was accessible (for some τ , n and k). In this case we ask if $M_{k,s}^{e(\alpha)} = M_{k,t}^{e(\alpha)}$. If so, then we let $\alpha^\wedge(\tau, n, k)$ be accessible at stage s . Otherwise, we let $\alpha^\wedge \infty$ be accessible at stage s .
- (2) At stage t , $\alpha^\wedge \infty$ was accessible. In this case we ask if there is some $k \leq s$ and some $\tau \succ \rho(\alpha)$ of length at least t such that the multiplicity n of τ in $M_{k,s}^{e(\alpha)}$ is smaller than $m(\alpha)$. If so, then we choose the least such k and let $\alpha^\wedge(\tau, n, k)$ be accessible at stage s . Otherwise, we let $\tau^\wedge \infty$ be accessible at stage s .

The stage is stopped when we have reached an accessible strategy δ_s of length s . We then let $T_s = T(\delta_s)$.

This concludes the construction.

5.3. Verification. Define the true path δ_ω by recursion. The empty string is on the true path. If α is on the true path and $\alpha^\wedge\infty$ is accessible infinitely often, then $\alpha^\wedge\infty$ is on the true path. Otherwise there is some child $\alpha^\wedge(\tau, n, k)$ which is accessible at all but finitely many stages at which α is accessible; this child is on the true path.

In general we say that a strategy α *lies to the left* of a strategy β if $\gamma^\wedge\infty \preceq \alpha$, where γ is the longest common ancestor of α and β . If β lies on the true path then at only finitely many stages does δ_s lie to the left of β .

Let $T = \liminf_s T_s$ be the set of strings σ such that $\sigma \in T_s$ for all but finitely many stages s .

Claim 5.2. $T = \bigcap_{\alpha \in \delta_\omega} T(\alpha)$.

Proof. Let $\alpha_0 \prec \alpha_1 \prec \alpha_2 \prec \dots$ be an increasing enumeration of the true path δ_ω . Then $\bigcap_i T(\alpha_i) = \bigcup_i D(\rho(\alpha_i), |\rho(\alpha_{i+1})|)$. It thus suffices to show that if $\alpha \in \delta_\omega$, β is α 's successor on δ_ω and $\beta \neq \alpha^\wedge\infty$, then: (a) $D(\rho(\alpha), |\rho(\beta)|) \subseteq T$; and (b): all strings on T of length greater than $|\rho(\alpha)|$ extend $\rho(\alpha)$. Fix such α and β . Say $\beta = (\alpha^\wedge(\tau, n, k))$.

Let s be a stage at which β is accessible. Then all strings on $T(\delta_s)$ of length greater than $|\rho(\alpha)|$ extend $\rho(\alpha)$. This establishes (b). For (a), let t be a stage at which β is accessible, and such that for all $s \geq t$, δ_s does not lie to the left of β . We claim that for all $s \geq t$, $D = D(\rho(\alpha), |\rho(\beta)|) \subseteq T_s$. Let $s \geq t$.

If $\beta \preceq \delta_s$ then $D \subseteq T(\delta_s) = T_s$. Otherwise there is some $\gamma \prec \alpha$ such that $\alpha \succ \gamma^\wedge\infty$ but $\gamma^\wedge(\sigma, m, l) \preceq \delta_s$ for some σ, m and l . Since $\gamma^\wedge\infty$ was accessible at stage t , the outcome (σ, m, l) was chosen after stage t , so $|\sigma| > t \geq |\rho(\beta)|$. Then $D \subseteq D(\rho(\gamma), |\sigma|) \subseteq T_s$ since $\rho(\gamma) \preceq \rho(\alpha)$. \square

For the next claim, note that for every e there is some $\alpha \in \delta_\omega$ such that $e(\alpha) = e$, but only finitely many.

Claim 5.3. *The tree T does not contain properly decreasing Δ_2^0 sequences of multisets.*

Proof. Let $\langle M_k \rangle$ be a Δ_2^0 sequence of multisets of strings. Suppose, for a contradiction, that each M_k only contains elements of T and that the sequence $\langle M_k \rangle$ is decreasing; we will show it is not properly decreasing.

Find some e such that for all k , for almost all s , $M_{k,s}^e = M_k$. Let β be the longest strategy on the true path $4\delta_\omega$ such that $e(\beta) = e$ (so $\beta^\wedge\infty \in \delta_\omega$); and let α be β 's predecessor.

If $e(\alpha) = e - 1$ (or $\beta = \langle \rangle$) then let M^* be the multiset containing infinitely many copies of the empty string, let $\tau^* = \langle \rangle$ and $n^* = \omega$ (we do this just to avoid discussing two cases separately). Otherwise $\beta = \alpha^\wedge(\tau, n, k)$; in this case let $M^* = M_k$, $\tau^* = \tau$ and $n^* = n$.

Since β lies on the true path, every string on T of length greater than $|\tau^*|$ extends τ^* . On the other hand since $\beta^\wedge\infty \in \delta_\omega$, for no k does M_k contain an extension of τ^* with multiplicity smaller than n^* . Since $M_k \preceq_T M_{k^*}$ for $k \geq k^*$, for each such k we can find multisets A_k of strings such that: (a) A_k contains strings of length τ^* other than τ^* ; and (b) $M_k \sim_T A_k + (n^* \cdot [\tau^*])$ (M_k is equivalent to adding n^* many copies of τ^* to A_k). Since the elements of A_k are terminal on T , $A_{k+1} \subseteq A_k$, and so the sequence $\langle A_k \rangle$ stabilizes. We conclude that the sequence $\langle M_k \rangle$ cannot be properly decreasing. \square

REFERENCES

- [1] B. Andersen, A. Kach, A. Melnikov, and R. Solomon. Jump degrees of torsion-free abelian groups. *J. Symbolic Logic*, 77(4):1067–1100, 2012.
- [2] C. Ash and J. Knight. *Computable structures and the hyperarithmetical hierarchy*, volume 144 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, 2000.
- [3] C. Ash, J. Knight, and S. Oates. Recursive abelian p -groups of small length. Unpublished. An annotated manuscript: <https://dl.dropbox.com/u/4752353/Homepage/AK0.pdf>.
- [4] Valentin Bura. *Reverse Mathematics of Divisibility in Integral Domains*. PhD thesis, Victoria University of Wellington, New Zealand, 2013.
- [5] Chris J. Conidis. Chain conditions in computable rings. *Trans. Amer. Math. Soc.*, 362(12):6523–6550, 2010.
- [6] Jim Coykendall and Muhammad Zafrullah. AP-domains and unique factorization. *J. Pure Appl. Algebra*, 189(1-3):27–35, 2004.
- [7] R. Downey, A. Melnikov, and K. Ng. Iterated effective embeddings of abelian p -groups. *To appear in International Journal of Algebra and Computation*.
- [8] Rodney G. Downey and Asher M. Kach. Euclidean functions of computable Euclidean domains. *Notre Dame J. Form. Log.*, 52(2):163–172, 2011.
- [9] Rodney G. Downey, Steffen Lempp, and Joseph R. Mileti. Ideals in computable rings. *J. Algebra*, 314(2):872–887, 2007.
- [10] D. Dzhafarov and J. Mileti. The complexity of primes in computable UFDs. *To appear in Notre Dame Journal of Formal Logic*.
- [11] Y. Ershov and S. Goncharov. *Constructive models*. Siberian School of Algebra and Logic. Consultants Bureau, New York, 2000.
- [12] Yu. Ershov. Problems of solubility and constructive models [in russian]. Nauka, Moscow (1980).
- [13] H. Friedman, S. Simpson, and R. Smith. Countable algebra and set existence axioms. *Ann. Pure Appl. Logic*, 25(2):141–181, 1983.
- [14] A. Fröhlich and J. Shepherdson. Effective procedures in field theory. *Philos. Trans. Roy. Soc. London. Ser. A.*, 248:407–432, 1956.
- [15] S. Goncharov. *Countable Boolean algebras and decidability*. Siberian School of Algebra and Logic. Consultants Bureau, New York, 1997.
- [16] Anne Grams. Atomic rings and the ascending chain condition for principal ideals. *Proc. Cambridge Philos. Soc.*, 75:321–329, 1974.
- [17] Grete Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, 95(1):736–788, 1926.
- [18] N. Khisamiev. Constructive abelian groups. In *Handbook of recursive mathematics, Vol. 2*, volume 139 of *Stud. Logic Found. Math.*, pages 1177–1231. North-Holland, Amsterdam, 1998.
- [19] A. Mal'cev. Constructive algebras. I. *Uspehi Mat. Nauk*, 16(3 (99)):3–60, 1961.
- [20] G. Metakides and A. Nerode. Recursively enumerable vector spaces. *Ann. Math. Logic*, 11(2):147–171, 1977.
- [21] G. Metakides and A. Nerode. Effective content of field theory. *Ann. Math. Logic*, 17(3):289–320, 1979.
- [22] G. Metakides and A. Nerode. The introduction of nonrecursive methods into mathematics. In *The L. E. J. Brouwer Centenary Symposium (Noordwijkerhout, 1981)*, volume 110 of *Stud. Logic Found. Math.*, pages 319–335. North-Holland, Amsterdam, 1982.
- [23] M. Rabin. Computable algebra, general theory and theory of computable fields. *Trans. Amer. Math. Soc.*, 95:341–360, 1960.
- [24] H. Rogers. *Theory of recursive functions and effective computability*. MIT Press, Cambridge, MA, second edition, 1987.
- [25] Leonard Schrieber. Recursive properties of Euclidean domains. *Ann. Pure Appl. Logic*, 29(1):59–77, 1985.
- [26] S. Simpson. *Subsystems of second order arithmetic*. Perspectives in Logic. Cambridge University Press, Cambridge, second edition, 2009.
- [27] R. Soare. *Recursively enumerable sets and degrees*. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1987. A study of computable functions and computably generated sets.

- [28] Ernst Steinitz. *Algebraische Theorie der Körper*. Chelsea Publishing Co., New York, N. Y., 1950.
- [29] V. Stoltenberg-Hansen and J. V. Tucker. Computable rings and fields. In *Handbook of computability theory*, volume 140 of *Stud. Logic Found. Math.*, pages 363–447. North-Holland, Amsterdam, 1999.
- [30] Alan M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, 42:230–265, 1936.
- [31] Alan M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, 43:544–546, 1937.
- [32] B. van der Waerden. Eine Bemerkung über die Unzerlegbarkeit von Polynomen. *Math. Ann.*, 102(1):738–739, 1930.