$\boldsymbol{d}$-Computable Categoricity for Algebraic Fields

Russell Miller[*]

April 26, 2010

Abstract

We use the Low Basis Theorem of Jockusch and Soare to show that all computable algebraic fields are $\boldsymbol{d}$-computably categorical for a particular Turing degree $\boldsymbol{d}$ with $\boldsymbol{d}' = \boldsymbol{0}''$, but that not all such fields are $\boldsymbol{0}'$-computably categorical. We also prove related results about algebraic fields with splitting algorithms, and fields of finite transcendence degree over $\mathbb{Q}$.

1 Introduction

Fields were the first mathematical structures for which the notion of computable categoricity arose. In [11], Frohlich and Shepherdson gave an example of (in their terminology; see their Corollary 5.51) two isomorphic, explicitly presented fields with no explicit isomorphism between them. This idea eventually grew into the following definition.

Definition 1.1 Let $\boldsymbol{d}$ be any Turing degree. A computable structure $\mathfrak{A}$ is $\boldsymbol{d}$-*computably categorical* if for every computable structure $\mathfrak{B}$ isomorphic to $\mathfrak{A}$, there exists a $\boldsymbol{d}$-computable isomorphism from $\mathfrak{A}$ onto $\mathfrak{B}$. If $\boldsymbol{d} = \boldsymbol{0}$, we say that $\mathfrak{A}$ is *computably categorical*.

[*] The author was partially supported by grants numbered 80209-04 12, 67182-00-36, 68470-00 37, 69723-00 38, and 61467-00 39 from The City University of New York PSC-CUNY Research Award Program, by grant #13397 from the Templeton Foundation, and by grant # DMS 0554841 from the National Science Foundation. He wishes to acknowledge useful conversations with Denis Hirschfeldt, Joseph Miller and Frank Stephan.

Much research has been devoted to characterizing the computably categorical models of various theories, including work by Dzgoev, Goncharov, Lempp, McCoy, Miller, Remmel, and Solomon. Some results are readily stated: we know that a computable linear order is computably categorical iff it has only finitely many pairs of consecutive elements, for example, and that a computable Boolean algebra is computably categorical iff it has finitely many atoms. On the other hand, the known structural characterization of computably categorical trees requires a description by recursion on the heights of finite trees. The question has been studied for a number of other theories as well, and results along these lines may be found in [12], [13], [14], [15], [16], [21], [24], [27], [30], and [31].

However, the original problem of computable categoricity for fields has defied all attempts at structural characterization. The most obvious conjecture would be that the transcendence degree of a field over its prime subfield should determine computable categoricity. For algebraically closed fields, this is indeed the case, as shown by Ershov in [7]: an ACF is computably categorical iff it has finite transcendence degree over its prime subfield. However, in the same work, Ershov built a field, algebraic over its prime subfield but not algebraically closed, which was not computably categorical. Moreover, recent work by Miller and Schoutens [28], and independent unpublished work by Kudinov and Lvov, has shown there to be a computably categorical field of infinite transcendence degree over the rationals $\mathbb{Q}$. Thus, neither implication in the naive first guess actually holds.

In this paper we restrict ourselves to the case of an algebraic field, by which we mean any subfield of any of the algebraically closed fields $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Z}_p}$. We want the field to be computably presented, and so we refer to such an object as a *CAF*: a computable algebraic field. (Sections 6 and 7 consider the cases of positive characteristic and finite transcendence degree.) Moreover, instead of trying directly to get an algebraic characterization of the computably categorical CAFs, we will ask instead how close to computable categoricity they come. Definition 1.1 generalizes the notion to arbitrary oracles. A computable structure which is $\mathbf{0}'$-computably categorical, for instance, may not be computably categorical, but it is not too far from being so: the relatively low-powered oracle $\emptyset'$ would allow us to compute isomorphisms between any two computable copies. It was shown in [24], for example, that for every n there is a computable tree (of height just $(n+3)$, in fact) which is not $\mathbf{0}^{(n)}$-computably categorical. Intuitively, this means that it can be hard to compute isomorphisms even for relatively short trees. On the other hand, the simple linear orders $(\omega, <)$ and $(\mathbb{Z}, <)$, while not computably categorical, are both $\mathbf{0}'$-computably categorical.

We will show that there exists a computable algebraic field which is not $\mathbf{0}'$-computably categorical. From experience, one is led to suspect that some CAF will therefore require at least a $\mathbf{0}''$-oracle, if not more, to compute isomorphisms. Surprisingly, though, this is not the case. The Low Basis Theorem, first proven by Jockusch and Soare in [19], allows us to show that any two isomorphic CAFs have an isomorphism f between them such that $f' \leq_T \emptyset''$. That is, the isomorphism is at least one jump below the degree $\mathbf{0}''$, although not necessarily computable in $\mathbf{0}'$. Indeed, a strong version of the Low Basis Theorem yields a Turing degree $\boldsymbol{d}$ such that $\boldsymbol{d}' = \mathbf{0}''$ and all computable CAFs are $\boldsymbol{d}$-computably categorical. Thus, the complexity of categoricity for CAFs lies in a nebulous region strictly between $\mathbf{0}'$ and $\mathbf{0}''$, closer to $\mathbf{0}'$ but not equal to either. To demonstrate that this region is indeed nebulous, we show that there is no least degree $\boldsymbol{d}$ such that all computable CAFs are $\boldsymbol{d}$-computably categorical, and likewise that many individual CAFs have no least degree $\boldsymbol{d}$ relative to which they are computably categorical.

Fields are also of interest because they remain an unknown in the context of the theorem of Hirschfeldt, Khoussainov, Shore, and Slinko, who showed in [17] that many theories are *complete* in a number of computable-model-theoretic respects. The theory of directed graphs, for example, is very much complete: for every nontrivial computable structure $\mathfrak{A}$, there is a computable graph $\mathfrak{G}$ which has the same spectrum and the same computable dimension as $\mathfrak{A}$, has relations realizing all degree spectra realized by relations on $\mathfrak{A}$, and behaves just like $\mathfrak{A}$ for persistence of computable categoricity under expansion by constants. Intuitively, this says that anything which can happen in any computable structure can happen in a computable directed graph. Although [17] did not remark it, the construction there also preserves the properties with which we are concerned here: $\mathfrak{A}$ is $\boldsymbol{d}$-computably categorical iff $\mathfrak{G}$ is, for each Turing degree $\boldsymbol{d}$.

In [17], many theories besides directed graphs were shown to have these properties, including symmetric irreflexive graphs, partial orders, rings, domains, and groups. On the other hand, certain theories have been shown not to be complete in various respects. For example, Boolean algebras cannot realize certain spectra, and neither can linear orders, by results in [5], [20], [26], and [32]. Similarly, [24] and [27] together show that trees can only realize the computable dimensions 1 and ω. Fields remain a significant unknown in all of this study. It was recently shown in [2] that the spectrum of a algebraic field can be precisely the upper cone of Turing degrees above any given degree $\boldsymbol{d}$; this sets fields apart from linear orders, Boolean algebras, and trees, for which Richter showed such a spectrum to be impossible whenever $\boldsymbol{d} >_T \mathbf{0}$ (see [32]). However, we do not know whether every possible spectrum can be realized by a field, nor whether fields can have finite computable dimension, nor much about the possible degrees of categoricity of fields (see Definition 5.7 below), and so on.

Of course, this paper only addresses algebraic fields, and thus will not give full answers to questions about fields in general, but it takes a step in the direction of such questions. The computable trees built in [24] and discussed above can have any degree $\mathbf{0}^{(n)}$ as the least degree in which they are categorical, and current work by Fokina, Kalimullin, and Miller in [9] has shown that for directed graphs, many other degrees $\boldsymbol{d}$ can be the least degree in which the graph is categorical. However, for algebraic fields, this paper will rule out that role for all degrees except the Δ^0_2 degrees, and for the specific case of algebraic fields with splitting algorithms, the only possible least degree is $\mathbf{0}$. Likewise, when the algebraic field has a splitting algorithm, we will show that its computable dimension must be either 1 or ω, so that such fields fail to be complete in that respect. Far more work than this remains to be done, of course, and the case of fields with infinite transcendence degree promises to be a good deal more complicated than that of algebraic fields. Nevertheless, the results in this paper do hold relevance for these questions, not least because they demonstrate that even when we restrict from fields to the (apparently) simpler situation of an algebraic field F, questions about categoricity of F in various Turing degrees already have nontrivial solutions, which will turn out to be related to questions about degrees of members of Π^0_1-classes. If nothing else, this paper gives computable model theorists a good excuse for not yet having figured out a criterion for computable categoricity for fields.

We describe our principal conventions for this paper. A *computable field* is a structure in the signature with addition and multiplication, whose domain is an initial segment of ω, and for which those two operations are computable. It follows that subtraction and division (when defined) are also computable, and that one can effectively pick out the two identity elements in the domain. Of course, it can cause confusion when we refer to the identity elements of the field by their usual names 0 and 1. However, every computable field is computably isomorphic to a field in which the domain element $0 \in \omega$ really is the additive identity and 1 really is the multiplicative identity. We therefore adopt this convention for our computable fields: the domain elements 0 and 1 are the identity elements for the field. At certain times we may refer to "prime numbers" p in our fields. By this we will mean the sum $(1 + \cdots + 1)$ taken p times in the field, and will trust the reader not to confuse this element with the domain element p.

Given a computable field F, we will often refer to its polynomial ring $F[X]$. This may be viewed just as the set F^* of finite tuples of elements of F, with $\langle a_0, \ldots, a_d \rangle$ identified with $\sum a_i X^i$. (For a perfect identification, ensure that if $a_d = 0$, then $d = 0$.) Likewise one builds the ring $F[X_1, \ldots, X_{n+1}]$ by taking finite tuples from $F[X_1, \ldots, X_n]$. Thus all these polynomial rings are presented uniformly in F and n.

If $g : F \to E$ is any field homomorphism, and $p(X) = \sum_i a_i X^i \in F[X]$, we will write $p^g(X)$ for the polynomial $\sum_i g(a_i) X^i \in E[X]$, the image of $p(X)$ under the map g on the coefficients. When g and the fields are computable, so is the map $p \mapsto p^g$.

Also, given a computable field F, we will treat any field extension $F(x)$ as a computable field as well. To compute it, we will need to know whether x is algebraic over F or not, and if it is, we will need its minimal polynomial $p(X)$ over F. In the latter case, one views elements of $F(x)$ as F-linear combinations over the set $\{1, x, x^2, \ldots, x^{d-1}\}$, where $d = \deg(p)$, with the obvious addition and multiplication (which requires knowledge of p, of course). In the former case, $F(x)$ is just the quotient field of the domain $F[X]$ given above; computable presentability of the quotient field is simple as long as the field F has a splitting algorithm, as described in Section 2, and in this paper we will not be taking transcendental extensions of any fields without splitting algorithms. We can iterate these extensions, even over infinitely many generators, as long as the minimal polynomial (or lack thereof) for each generator over the preceding ones is given effectively. Notice that the base field F is a computable subfield of each extension built this way.

Computability-theoretic notation is standard and can be found in [33]; we do offer a quick review here of standard algebraic definitions, since the anticipated audience is mostly logicians. The field $\mathbb{Q}$ is known to be computably categorical, and so we will often just write $\mathbb{Q}$ to denote a computable presentation of that field; similarly for $\mathbb{Z}_p$, the field of p elements, when we consider positive characteristic. A field has *characteristic* p if the sum of the multiplicative identity 1 with itself p times equals 0, the additive identity, and if p is the smallest positive integer for which this happens. Such a p must be prime. If there is no such p, we say that the field has characteristic

0. The *prime subfield* of a field F is the intersection of all subfields of F; this is also a subfield, and is isomorphic to $\mathbb{Z}_p$ if F has characteristic $p > 0$, and to $\mathbb{Q}$ otherwise. Uniformly in any computable field, the prime subfield is computably enumerable. Indeed, in any computable algebraic field, we will see that the prime subfield must be computable.

A *finite* field extension $F \subseteq E$ is an extension such that there exist finitely many elements $x_1, \ldots, x_n \in E$ for which $E = F(x_1, \ldots, x_n)$; an extension $F \subseteq E$ is called *infinite* iff it is not finite. If $F \subseteq E$ is a field extension, then an element $x \in E$ is *algebraic over* F if x is the root of some nonzero polynomial $f(X) \in F[X]$. For each such x, there is a polynomial of least degree in $F[X]$ for which x is a root; this is called the *minimal polynomial of* x *over* F, and is unique if we require the leading coefficient to be 1. This polynomial will also be *irreducible* in $F[X]$: apart from constants, it will have no factorization there.

Finite algebraic extensions of $\mathbb{Q}$ or of $\mathbb{Z}_p$ are a means for us, not an end. All such fields are quickly seen to be computably categorical. However, infinite algebraic extensions are readily viewed as infinite iterations of extensions by single elements, and so finite algebraic extensions will indeed be of importance as we study algebraic fields. Since the second part of the following definition is not standard, we state it here:

Definition 1.2 If $F \subseteq E$ are fields, then E is *algebraic over* F if every $x \in E$ is algebraic over F. When F is the prime subfield of E, we simply call E an *algebraic field.*

Thus the algebraic fields are precisely the subfields of the algebraically closed fields $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Z}_p}$. Elements of $\overline{\mathbb{Q}}$ are traditionally called *algebraic numbers*, but, by a longstanding and widely used definition, an *algebraic number field* is a finite algebraic extension of $\mathbb{Q}$, not an infinite one. Thus $\overline{\mathbb{Q}}$ itself is a field of algebraic numbers, but not an algebraic number field. We reiterate here that for us, every algebraic extension of either $\mathbb{Q}$ or $\mathbb{Z}_p$, whether finite or infinite, will be called an *algebraic field.*

An $x \in E$ is *transcendental over* F if it is not algebraic over F. A *transcendence basis* for an extension $F \subseteq E$ is a minimal set $B \subset E$ such that E is an algebraic extension of the subfield $F(b : b \in B)$. The size of a transcendence basis is an invariant of the extension, and is called the *transcendence degree* of E over F.

$F \subseteq E$ is a *normal* extension if every irreducible polynomial $f(X) \in F[X]$ either has no roots in E, or has its full complement of $\deg(f)$-many roots in E, counted by multiplicity. An irreducible polynomial $f(X) \in F[X]$ is *separable* if $f(X)$ has $\deg(f)$ distinct roots in some field extension of F. An algebraic extension $F \subseteq E$ is *separable* if for every $x \in E$, the minimal polynomial $f(X)$ of x over F is separable. Over a field of characteristic 0, all irreducible polynomials are separable, but in positive characteristic this can fail. A *Galois extension* is a finite normal algebraic separable extension. The *Galois group* $\mathrm{Gal}(E/F)$ of an extension $F \subseteq E$ is the group of automorphisms of E which fix F pointwise; for finite algebraic extensions, it is a finite group. For further algebraic preliminaries, many sources are useful, including [18] and [35]. In general the author does not claim any originality for the purely algebraic results in this paper; if any of them are original, it is due to their obscurity, not their difficulty.

2 Background and Results on Fields

Any discussion of computable fields of characteristic 0 should begin with the question of a splitting algorithm for $\mathbb{Q}$.

Definition 2.1 The *splitting set* for a field F is the set of reducible polynomials in $F[X]$. The *root set* of F is $\{p(X) \in F[X] : (\exists a \in F)p(a) = 0\}$.

With the splitting set as oracle, one can decompose any polynomial in $F[X]$ into its irreducible components in $F[X]$. Throughout the literature on computable fields, the phrase "F has a splitting algorithm" is used to mean that F has a *computable* splitting set. In this paper we will be concerned with the Turing degree of the splitting set, not just with its computability, so we introduce the new term to avoid conflict with the existing one. Likewise, F has a *root algorithm* if its root set is computable.

It is not obvious that $\mathbb{Q}$ must have a splitting algorithm, but Kronecker provided one. It works for every computable presentation of $\mathbb{Q}$, since $\mathbb{Q}$ is a computably categorical field. In fact, Kronecker showed that every finite extension of $\mathbb{Q}$ has a splitting algorithm, using the following theorem. Since the original paper dates to 1882, the reader may prefer to see the more recent version in [6], or Lemmas 17.3 and 17.5 of [10]. Part (c) is an obvious relativization of the argument.

Theorem 2.2 (Kronecker [23]) *(a) The splitting set of the field $\mathbb{Q}$ is computable.*

(b) *Let L be a c.e. subfield of a computable field K. If L has a splitting algorithm, then for any $x \in K$ transcendental over L, $L(x)$ also has a splitting algorithm. When $x \in K$ is algebraic over L, again $L(x)$ has a splitting algorithm, which requires knowledge of the minimal polynomial of x over L.*

(c) *More generally, for any c.e. subfield L of a computable field K and any $x \in K$ transcendental over L, the splitting set of $L(x)$ is Turing-equivalent to the splitting set for L, via reductions uniform in x. Also, if $x \in K$ is algebraic over L, $L(x)$ and L have Turing-equivalent splitting sets, uniformly in x and the minimal polynomial of x over L.* ■

The algorithms for algebraic and transcendental extensions are different, so it is essential to know whether x is algebraic. If it is, then from the splitting set for L one can determine its minimal polynomial. This yields the following.

Lemma 2.3 *For every computable field F algebraic over its prime subfield P, the splitting set for each finitely generated subfield $P[\vec{x}]$ is computable uniformly in the finite tuple $\vec{x}$ of elements of F.*

Proof. Clearly there are splitting algorithms for all finite fields, just by checking all possible factorizations. (So in fact there is a single algorithm which works in all positive characteristics.) In characteristic 0, the prime subfield of F is c.e. within F, hence computably isomorphic to a computable presentation. Kronecker's splitting algorithm works for any computable presentation of $\mathbb{Q}$, since the field $\mathbb{Q}$ is uniformly computably categorical. The lemma then follows by induction on the size of the tuple $\vec{x}$, using part (b) of Theorem 2.2. Since our F is algebraic over P, we may simply search for a polynomial $p(X)$ with root x_n and coefficients in $P[x_0, \ldots, x_{n-1}]$, and then split it, using the splitting algorithm for $P[x_0, \ldots, x_{n-1}]$ (by inductive hypothesis), until we have found the minimal polynomial of x_n over $P[x_0, \ldots, x_{n-1}]$. ■

These splitting algorithms also allow us to compute the Galois groups of the corresponding fields.

Lemma 2.4 *Let $\overline{\mathbb{Q}}$ be any computable presentation of the algebraic closure of the field of rational numbers. For every finite tuple $\langle x_0, \ldots, x_n\rangle$ of elements of $\overline{\mathbb{Q}}$, we may compute the automorphism group of the field $F = \mathbb{Q}[\vec{x}]$ – that is, the Galois group of F over $\mathbb{Q}$ – uniformly in $\vec{x}$. (Here we present an automorphism σ by giving the values $\sigma(x_0), \ldots, \sigma(x_n)$.)*

Indeed, even if we are only given the minimal polynomial of each x_i over $\mathbb{Q}[x_0, \ldots, x_{i-1}]$, we can still compute Gal$(F/\mathbb{Q})$ uniformly in those polynomials, without knowing the elements x_i themselves.

Of course, the Galois group of F over any subfield $\mathbb{Q}[\vec{y}]$ can then be computed uniformly in the finite tuple $\vec{y}$, since it contains just those $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ which fix $\vec{y}$ pointwise. This lemma should be compared to Lemma 17.13 on p. 235 of [10]. The statement there only considers Galois extensions, i.e. finite normal separable algebraic extensions (equivalently, splitting fields of single polynomials). However, we will need the result also for extensions which are not normal.

Proof. We can give a computable presentation of F just from the minimal polynomials described, and Lemma 2.3 provides splitting algorithms for all subfields of F. Therefore, in the following, we can find the minimal polynomial of any element of F over any subfield of F. For instance, to find the minimal polynomial of x_3 over $\mathbb{Q}[x_1, x_5]$, we simply search in $\mathbb{Q}[X]$ for any polynomial $p(X)$ such that $p(x_3) = 0$ in F, then apply the splitting algorithm of $\mathbb{Q}[x_1, x_5]$ to $p(X)$ to find its irreducible component there with root x_3.

Now let σ be any function with domain $\vec{x}$ and range contained in the set S of all conjugates in F over $\mathbb{Q}$ of each element x_i. (S is finite and computable uniformly in $\vec{x}$, and so is the size of S, so we have restricted ourselves here to a known finite set of σ's.) Test first whether x_0 and $\sigma(x_0)$ have the same minimal polynomial over $\mathbb{Q}$. If not, then of course $\sigma \notin \mathrm{Gal}(F/\mathbb{Q})$. If so, then $\mathbb{Q}[x_0] \cong \mathbb{Q}[\sigma(x_0)]$ via σ (extended to $\mathbb{Q}[x_0]$), and we continue by recursion. Assuming inductively that σ maps $\mathbb{Q}[x_0, \ldots, x_i]$ isomorphically onto $\mathbb{Q}[\sigma(x_0), \ldots, \sigma(x_i)]$, find the minimal polynomials $p(X)$ of x_{i+1} over $\mathbb{Q}[x_0, \ldots, x_i]$ and $q(X)$ of $\sigma(x_{i+1})$ over $\mathbb{Q}[\sigma(x_0), \ldots, \sigma(x_i)]$. If $q(X) = p^\sigma(X)$, we have $\mathbb{Q}[x_0, \ldots, x_{i+1}] \cong \mathbb{Q}[\sigma(x_0), \ldots, \sigma(x_{i+1})]$ via σ and we continue; if not, then $\sigma \notin \mathrm{Gal}(F/\mathbb{Q})$. If we eventually reach $\mathbb{Q}[x_0, \ldots, x_n] \cong \mathbb{Q}[\sigma(x_0), \ldots, \sigma(x_n)]$ via σ, then $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. ∎

We will also require Rabin's Theorem. To begin with, we give his name to the type of field embedding he considered.

Definition 2.5 Let F and E be computable fields. A function $g : F \to E$ is a *Rabin embedding* if:

- g is a homomorphism of fields; and

- E is both algebraically closed and algebraic over the image of g; and
- g is a computable function.

Theorem 2.6 (Rabin [29]) *Let F be any computable field.*

1. *There exists a computable algebraically closed field $\overline{F}$ with a Rabin embedding of F into $\overline{F}$.*
2. *For every Rabin embedding g of F (into any computable ACF E), the image of g is a computable subset of E iff F has a splitting algorithm.*

Corollary 2.7 *For any computable field F, the following are Turing equivalent:*

(i.) *the image $g(F)$ of F under any Rabin embedding g;*

(ii.) *the splitting set of F;*

(iii.) *the root set of F;*

(iv.) *the root function of F, i.e. the function with domain $F[X]$ which computes the number of distinct roots in F of any $p(X) \in F[X]$;*

(v.) *the root multiplicity function of F, i.e. the function with domain $F[X]$ which computes the number of roots in F, counted by multiplicity, of any $p(X) \in F[X]$.*

Proof. (i) and (ii) are Turing equivalent by Rabin's Theorem, the proof of which easily relativizes to the splitting set, or to the image $g(F)$, when either is not computable. With an oracle for the splitting set, we can find all irreducible factors of a given $p(X)$ and check whether any of them is linear, thereby computing the root set. (In our presentation of $F[X]$ described in Section 1, $\sum_{i\leq d} a_i X^i$ is represented by $\langle a_0, \ldots, a_d \rangle$, so we can compute the degree d of any element.) From the root set, we may determine whether a given $p(X)$ has a root and, if so, find such a root $r \in F$ and repeat the process for $\frac{p(X)}{X-r}$ until there are no more roots, thereby computing the root function. The root function and the root multiplicity function are quickly seen to compute each other. It is possible to compute the splitting set from the root function using symmetric polynomials, as shown in [11], but we give a direct computation of $g(F)$ instead, based on Rabin's proof of his theorem.

Given a Rabin embedding $g : F \hookrightarrow E$ and any $x \in E$, find any polynomial $p(X) \in F[X]$ such that $p^g(x) = 0$. (Recall that $p^g \in E[X]$ is the image of p under the map g on its coefficients.) With a root function for F, we may find all the roots $r_0, \ldots, r_n$ of p in F. Then $x \in g(F)$ iff $(\exists i \leq n) x = g(r_i)$. ■

When the field in question is an algebraic field, we have a stronger result.

Corollary 2.8 *Any two isomorphic computable algebraic fields F and $\tilde{F}$ must have Turing-equivalent splitting sets. Hence the Turing degree of each item in Corollary 2.7 is an invariant of the isomorphism type of a CAF. Moreover, the Turing reductions are uniform in F and $\tilde{F}$.*

If F and $\tilde{F}$ are isomorphic computable fields of characteristic 0 *with finite transcendence degree over their prime subfields, then they still have Turing-equivalent splitting sets, but the uniformity need no longer hold.*

Proof. We prove that the images of F and $\tilde{F}$ under Rabin embeddings $g : F \hookrightarrow E$ and $\tilde{g} : \tilde{F} \hookrightarrow \tilde{E}$ are Turing-equivalent, and then appeal to Corollary 2.7. Rabin's Theorem proves that some such g and $\tilde{g}$ must exist, of course. Since F and $\tilde{F}$ are algebraic fields, each of E and $\tilde{E}$ is algebraic over its prime subfield P and $\tilde{P}$. Therefore, given any $x \in E$, we may find a polynomial $q(X) \in P[X]$, say of degree d, such that $q(x) = 0$. We find all roots $r_1, \ldots, r_d \in \tilde{E}$ of the corresponding $\tilde{q} \in \tilde{P}[X]$, and check how many are in $\tilde{g}(\tilde{F})$, using our $\tilde{g}(\tilde{F})$-oracle. Then we enumerate $g(F)$ until that many roots of q have appeared in $g(F)$. Now $x \in g(F)$ iff x is one of those roots.

This process was uniform in F and $\tilde{F}$, since the Rabin embeddings g and $\tilde{g}$ may be built uniformly in F and $\tilde{F}$. For the case of fields in general, to make the same argument work, we must take P to be not the prime subfield of E, but rather a purely transcendental extension of the prime subfield by a transcendence basis for E. Likewise $\tilde{P}$ must be the corresponding subfield of $\tilde{E}$ under an isomorphism $(E, F) \to (\tilde{E}, \tilde{F})$. If this transcendence basis is finite, then knowing it (for a single F and $\tilde{F}$) constitutes finitely much information, and so the same argument still succeeds, but not uniformly. For a field of infinite transcendence degree, the theorem would not in general be true.

It is possible to prove this corollary without appealing to Rabin's Theorem. Given $q(X) = \sum a_i X^i \in F[X]$, the root function for $\tilde{F}$ will give the number of roots in $\tilde{F}$ of polynomials of the form $\sum \tilde{b}_i X^i$ with each $\tilde{b}_i$ P-conjugate to a_i. Then one finds an equal number of roots of such polynomials in $F[X]$, and checks how many are roots of q, thus computing the root function on q. ■

Of course, finite extensions of the prime field are not the only algebraic extensions with splitting algorithms; $\overline{\mathbb{Q}}$ itself is an infinite extension of the prime field which nevertheless has a (very simple!) splitting algorithm. We also give a more interesting example, which will be used in Theorem 3.4.

Lemma 2.9 *Let F be the quadratic closure of $\mathbb{Q}$, i.e. the field we get by starting with $\mathbb{Q}$ and repeatedly closing under square roots (equivalently, under roots of quadratic polynomials). Then F is computably presentable and has a splitting algorithm.*

Proof. F is easily enumerated as a subfield of $\overline{\mathbb{Q}}$, hence is computably presentable. For the splitting algorithm, we appeal to Rabin's Theorem. To compute whether an arbitrary $x \in \overline{\mathbb{Q}}$ lies in F, find the minimal polynomial $p(X)$ of x over $\mathbb{Q}$, and let $K \subset \overline{\mathbb{Q}}$ be its splitting field, with Galois group G, which we determine using Lemma 2.4. The subfields between $\mathbb{Q}$ and K are precisely the fixed fields of subgroups of G, so we may determine all of them, find generators for each, and determine the degree of each over each of its own subfields. But x lies in the quadratic closure iff there is a sequence of subfields $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n = K$ such that $[K_{i+1} : K_i] = 2$ for all $i < n$. ■

Next we consider some field-theoretic facts which will be needed for our constructions.

Lemma 2.10 *For a field F algebraic over its prime subfield P, every endomorphism (i.e. every homomorphism from F into itself) is an automorphism.*

Proof. Since fields have no nontrivial ideals, every endomorphism g is one-to-one. So for any $y \in F$, the set of the finitely many P-conjugates of y in F must be mapped one-to-one into itself by g, forcing $y \in \text{range}(g)$. ■

Lemma 2.11 *If $F \subseteq E \subseteq K$ are finite field extensions, then their indices satisfy $[K : F] = [K : E] \cdot [E : F]$. Hence if E_1 and E_2 are finite extensions of F within a larger field, and $[E_1 : F]$ is relatively prime to $[E_2 : F]$, then $E_1 \cap E_2 = F$.*

Lemma 2.12 *In a finite normal algebraic extension $F \subseteq L$, each root in L of an irreducible $p(X) \in F[X]$ can be mapped to each other root of $p(X)$ in L by an element of Gal(L/F). In fact, $p(X)$ is irreducible in $F[X]$ iff the Galois group of the splitting field of $p(X)$ over F acts transitively on the roots of $p(X)$.*

Proof. These are standard results; see for instance [18], p. 215, Thm. 4.2 and Lemma 4.14. ■

The next results lead up to Proposition 2.15, which will be the key to our theorems in Sections 3 and 4 about fields which are not computably categorical.

Lemma 2.13 *Fix any prime p. In the ring $\mathbb{Z}[\sqrt{p}]$, an element $a + b\sqrt{p}$ is a unit (i.e. has a multiplicative inverse) iff $a^2 - pb^2 = \pm 1$.*

Proof. The norm map $N(a+b\sqrt{p}) = |a^2 - pb^2|$ is multiplicative on $\mathbb{Z}[\sqrt{p}]$, with values in ω. Since 1 is the only unit in ω, all units have norm 1. Conversely, if $a^2 - pb^2 = 1$, then $(a + b\sqrt{p}) \cdot (a - b\sqrt{p}) = 1$, and if $a^2 - pb^2 = -1$, then $(a + b\sqrt{p}) \cdot (-a + b\sqrt{p}) = 1$. ■

It follows that the element $\sqrt{p}$ itself is irreducible in $\mathbb{Z}[\sqrt{p}]$, i.e. has no factorization there except by units. In unique factorization domains, irreducible elements are always prime, but this is not true for domains in general. Nevertheless, we do have at least one prime in this ring.

Lemma 2.14 *In the ring $\mathbb{Z}[\sqrt{p}]$ (for p a prime in $\mathbb{Z}$), the element $\sqrt{p}$ itself is always prime. That is, if $x, y \in \mathbb{Z}[\sqrt{p}]$ and $\sqrt{p}$ divides the product (xy), then $\sqrt{p}$ must divide either x or y in $\mathbb{Z}[\sqrt{p}]$.*

Proof. Suppose that $\sqrt{p}$ divides the product (xy) in $\mathbb{Z}[\sqrt{p}]$, and use the norm map N defined above. The norm $p = N(\sqrt{p})$ divides $N(x)N(y)$ in ω, and since p is prime there, it must (without loss of generality) divide $N(x)$. Say $x = a + b\sqrt{p}$ with $a, b \in \mathbb{Z}$. Then p divides $|a^2 - pb^2|$, so p divides a^2, so p divides a, say $a = pc$, with $c \in \mathbb{Z}$. But then $x = \sqrt{p} \cdot (b + c\sqrt{p})$, so $\sqrt{p}$ divides x in $\mathbb{Z}[\sqrt{p}]$. ■

For any nonzero element $x \in \mathbb{Q}[\sqrt{p}]$, we define the *content of x* to be the greatest power $k \in \mathbb{Z}$ of $\sqrt{p}$ such that $\frac{x}{\sqrt{p}^k} = \frac{y}{n}$ for some $y \in \mathbb{Z}$ and some $n \in \mathbb{N}$ such that $p \nmid n$. (Intuitively, this is the number of powers of $\sqrt{p}$ dividing x.) We regard 0 as having (positive) infinite content. The content is nonnegative when $x \in \mathbb{Z}[\sqrt{p}]$, but may be negative when $x \in \mathbb{Q}[\sqrt{p}]$. For a polynomial, the content is the minimum of the contents of its coefficients, as suggested by the intuitive definition.

When $h(X)$ is a polynomial with coefficients in $\mathbb{Q}[\sqrt{p}]$, we will write $h^-(X)$ to denote the image of this polynomial when $\sqrt{p}$ is mapped to $-\sqrt{p}$. That is, coefficients of the form $(a + b\sqrt{p})$ in h become $(a - b\sqrt{p})$ in h^-. If $h(X) \in \mathbb{Q}[X]$, then of course $h^- = h$.

Proposition 2.15 *For any fixed prime p, let F be the field $\mathbb{Q}[\sqrt{p}]$. Then for every odd prime number d, there exists a polynomial $h(X) \in F[X]$ of degree d with the following properties.*

- *h and h^- are both irreducible in the polynomial ring $F[X]$.*
- *The splitting field of h over F has Galois group isomorphic to S_d, the symmetric group on the d roots of h, and the same holds for h^-. (Since S_d acts transitively on the roots, this implies the preceding condition.)*
- *The splitting field of $h(X)$ over the splitting field of $h^-(X)$ also has Galois group isomorphic to S_d (and vice versa). In particular, each of $h(X)$ and $h^-(X)$ is irreducible over the splitting field of the other.*

Moreover, uniformly in p, d, and any computable presentation of F, it is computable whether an arbitrary $h(X) \in F[X]$ satisfies these properties.

Proof. The final remark about computability follows readily from Lemma 2.4, along with basic facts which allow one to determine the number of real roots. So we only need prove existence of some such polynomial $h(X)$. In fact, though, we give a moderately detailed description of one such $h(X)$. To begin, fix p and d, and let

$$h_0(X) = d! \cdot \sum_{k=0}^{\frac{d-1}{2}} \frac{(-1)^k \cdot X^{2k+1}}{(2k+1)!}$$

be the monic scalar multiple of the Taylor polynomial of degree d for the sine function. The relevant facts are that h_0 is monic of degree d in $\mathbb{Q}[X]$ with d distinct real roots, one of which is 0, and with distinct y-coordinates at its critical points; any polynomial with these properties would suffice. For this h_0, the distinctness of y-coordinates at critical points follows from the increasing error margin between $h_0(x)$ and $\sin x$ as x moves further from 0.

Write $h_0(X) = \sum_{i \leq d} c_i X^i$. Now for each $\epsilon > 0$ there exists a $\delta > 0$ such that for every $h_1(X) \in \mathbb{R}[X]$ of degree d with each coefficient within

δ of the corresponding coefficient c_i, the roots of $h_1(X)$ are within ϵ of the corresponding roots of h_0, and the y-coordinates of critical points of h_1 are within ϵ of those of the corresponding critical points of h_0. We choose our particular $h_1(X) \in \mathbb{Q}[\sqrt{p}][X]$ to be monic with constant term 0 and such that all its other coefficients have content 2, as defined above, and lie within δ of the corresponding c_i, where δ corresponds to an ϵ less than half the difference between any two roots of h_0, and less than half the difference between any y-coordinates of critical points of h_0. Therefore h_1 also has d distinct real roots, and there is a unique critical point of h_1 whose y-coordinate y_0 lies closest to 0. (Since h_1 has no repeated roots, no critical point can have y-coordinate equal to 0.) Also, $h_1^-(X) = h_1(X)$, since all nonzero coefficients have even content.

Finally, to get the polynomial $h(X)$ from $h_1(X)$, we just add $\pm b\sqrt{p}$, where b is a rational number with content 0 such that $|y_0| < b\sqrt{p}$, but $b\sqrt{p}$ is less than all other absolute values of y-coordinates of critical points of h_1. If $y_0 > 0$, let $h(X) = h_1(X) + b\sqrt{p}$, so that $h^-(X) = h_1(X) - b\sqrt{p}$; whereas if $y_0 < 0$, we do the opposite: $h(X) = h_1(X) - b\sqrt{p}$ and $h^-(X) = h_1(X) + b\sqrt{p}$. Thus $h(X)$ has the same number of real roots as $h_1(X)$, namely d, since no critical point of h_1 crossed the x-axis when we added the constant term. However, the one critical point of $h_1^-(X)$ closest to the x-axis does cross that axis when we create $h^-(X)$, and so $h^-(X)$ has exactly two fewer real roots than $h_1^-(X) = h_1(X)$. We let $r_1, \ldots, r_d \in \mathbb{R}$ be all roots of h, and $r_1^-, \ldots, r_d^-$ all roots of h^-, ordered so that $r_1^-, \ldots, r_{d-2}^-$ are real.

We now wish to appeal to Gauss's Lemma and Eisenstein's Theorem (see [35]). The usual versions of these may not apply, since they concern only unique factorization domains and their fraction fields. (It is unknown for exactly which primes p, or even for how many primes, the ring $\mathbb{Z}[\sqrt{p}]$ is a UFD.). However, knowing that $\sqrt{p}$ is a prime in $\mathbb{Z}[\sqrt{p}]$, we may adapt those results as follows.

Lemma 2.16 *If two polynomials $f(X), g(X) \in \mathbb{Z}[\sqrt{p}][X]$ both have content* 0*, then so does their product. (In Gauss's terminology, the product of* primitive *polynomials is also primitive.)*

Proof. Let a_iX^i and b_jX^j be the lowest-degree terms of $f(X)$ and $g(X)$, respectively, such that $\sqrt{p}$ divides neither a_i nor b_j. Then the coefficient of X^{i+j} in the product polynomial is the sum of a_ib_j with terms divisible by $\sqrt{p}$. Since $\sqrt{p}$ is prime, it cannot divide a_ib_j, hence does not divide this coefficient. ■

Lemma 2.17 *For any prime degree $d > 2$ and any prime p, these polynomials $h(X)$ and $h^{-}(X)$ are irreducible in the polynomial ring $\mathbb{Q}[\sqrt{p}][X]$.*

Proof. Suppose $h(X) = f(X) \cdot g(X)$ were a factorization of h in $\mathbb{Q}[\sqrt{p}][X]$. First we write all coefficients of f and g in the form $\frac{a+b\sqrt{p}}{p^n \cdot c}$, with $a, b, c \in \mathbb{Z}$, $n \geq 0$, and p not dividing c in $\mathbb{Z}$. Then we multiply by the highest power p^n of p occurring in any denominator of those coefficients, and collect the denominators: $\sqrt{p}^k h(X) = \frac{1}{m} f_0(X) \cdot g_0(X)$, where now $f_0, g_0 \in \mathbb{Z}[\sqrt{p}][X]$, $k = 2n$, and $m \in \mathbb{N}$ with $p \nmid m$. By Lemma 2.16, if $k > 0$, then either f_0 or g_0 has content > 0, so we may divide f_0 or g_0 by $\sqrt{p}$ and still have a polynomial of the same form. By induction, therefore, we may assume that $k = 0$. So now

$$f_0(X) \cdot g_0(X) = m \cdot h(X).$$

Write $f_0(X) = \sum a_i X^i$ and $g_0(X) = \sum b_i X^i$, and fix $c = \deg(f_0)$, so $0 < c < d$ and $d - c = \deg(g_0)$. In $mh(X)$ the constant term has content 1, the lead term has content 0, and all other terms have content 2, by our construction of $h(X)$, since $p \nmid m$. Multiplying out, we see that $a_0 \cdot b_0$ equals the constant term of $mh(X)$, hence has content 1. Without loss of generality, then, $\sqrt{p} \mid a_0$ and $\sqrt{p} \nmid b_0$ in $\mathbb{Z}[\sqrt{p}]$. But now the coefficient of X in $mh(X)$ equals $(a_0 b_1 + a_1 b_0)$ and is divisible by $\sqrt{p}$, so $\sqrt{p} \mid a_1$ by Lemma 2.14. Likewise, for each i with $1 < i \leq c$ in turn, we see that the coefficient of X^i in $mh(X)$ is divisible by $\sqrt{p}$ (since $i \leq c < d$) and is equal to $a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$. By induction $\sqrt{p} \mid a_j$ for all $j < i$, while still $\sqrt{p} \nmid b_0$, forcing $\sqrt{p} \mid a_i$ in $\mathbb{Z}[\sqrt{p}]$. (If $c > d - c$, then those b_j with $j > d - c$ are defined to be 0 here, of course.) Thus f_0 has content > 0, and g_0 has all coefficients in $\mathbb{Z}[\sqrt{p}]$, yet the lead term X^d in $mh(X)$ has coefficient $m = a_c b_{d-c}$ and $\sqrt{p} \nmid m$, a contradiction. Hence $h(X)$ was irreducible in $\mathbb{Q}[\sqrt{p}][X]$ as desired, and the same argument works for $h^{-}(X)$. ∎

Let K and K^{-} be the splitting fields of $h(X)$ and $h^{-}(X)$ over $F = \mathbb{Q}[\sqrt{p}]$. By irreducibility of h^{-}, the field $F[r^{-}]$ generated by any single root r^{-} of h^{-} must have vector-space dimension d over F, and so that dimension d divides $[K^{-} : F]$, which equals the order of $\mathrm{Gal}(K^{-}/F)$. Since d is prime, the Sylow Theorems show that $\mathrm{Gal}(K^{-}/F)$ contains an element of order d. Also, complex conjugation defines an element of $\mathrm{Gal}(K^{-}/F)$, which transposes the two non-real roots of h^{-} and fixes all the others. But by a lemma from group theory (see [18], p. 268; we are following the larger construction given there) a permutation group on a prime number d of elements which contains both a transposition and an element of order d can only be the symmetric group S_d on those d elements. Thus $\mathrm{Gal}(K^-/F) \cong S_d$.

Now let E be the field generated by K and K^- together, i.e. the splitting field over $\mathbb{Q}$ of the product polynomial $(h \cdot h^-)$. All of the following field extensions are normal: $\mathbb{Q} \subset F$, $F \subset K$, $F \subset K^-$, $K \subset E$, $K^- \subset E$, and $\mathbb{Q} \subset E$. So the nontrivial element $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, which has $\sigma(\sqrt{p}) = -\sqrt{p}$, extends to some $\overline{\sigma} \in \mathrm{Gal}(E/\mathbb{Q})$. Since this $\overline{\sigma}$ maps $h(X)$ to $h^-(X)$, it must map K onto K^- and vice versa. Indeed, by normality, the map $\tau \mapsto \overline{\sigma}^{-1}\tau\overline{\sigma}$ is an isomorphism of $\mathrm{Gal}(K/F)$ onto $\mathrm{Gal}(K^-/F)$, so the former is also isomorphic to S_d. Moreover, since $\mathrm{Gal}(K^-/F) \cong S_d$, we have:

Lemma 2.18 *For every permutation π of the set $\{1, \ldots, d\}$, there exists some $\tau \in Gal(E/\mathbb{Q})$ with $\tau(r_i) = r^-_{\pi(i)}$ for every i.* ■

Now fix any $i, j \leq d$. This lemma yields a $\tau \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\tau(r_i) = r^-_{d-1}$, and $\tau(r_j) = r^-_d$. Let $\zeta \in \mathrm{Gal}(E/\mathbb{Q})$ be complex conjugation, which is indeed an automorphism of E because E is the splitting field of the product polynomial $((X^2 - p) \cdot h(X) \cdot h^-(X)) \in \mathbb{Q}[X]$. Hence ζ interchanges r^-_{d-1} with r^-_d and fixes all other roots of h and h^-, and so we have:

$$\begin{aligned}
(\tau^{-1} \circ \zeta \circ \tau)(r_i) &= \tau^{-1}(\zeta(r^-_{d-1})) = \tau^{-1}(r^-_d) = r_j \\
(\tau^{-1} \circ \zeta \circ \tau)(r_j) &= \tau^{-1}(\zeta(r^-_d)) = \tau^{-1}(r^-_{d-1}) = r_i \\
(\tau^{-1} \circ \zeta \circ \tau)(r_k) &= \tau^{-1}(\tau(r_k)) = r_k \quad (\text{for all } k \notin \{i, j\}) \\
(\tau^{-1} \circ \zeta \circ \tau)(r^-_k) &= \tau^{-1}(\tau(r^-_k) = r^-_k \quad (\text{for all } k \leq d),
\end{aligned}$$

with the last two lines holding because $\tau(r_k)$ and $\tau(r^-_k)$ are real numbers, hence fixed by ζ. This shows that $\mathrm{Gal}(E/K^-)$ contains the automorphism transposing r_i with r_j and fixing all other r_k, and since $i, j \leq d$ were arbitrary, $\mathrm{Gal}(E/K^-)$ acts as the symmetric group S_d on the roots of $h(X)$. Conjugating by $\overline{\sigma}$ shows that $\mathrm{Gal}(E/K)$ likewise acts as S_d on the roots of $h^-(X)$. This completes the proof of Proposition 2.15. ■

3 Computable Categoricity

We start considering categoricity with a result first proven by Frohlich and Shepherdson in [11], the computable categoricity of normal algebraic extensions, which is easily extended (as stated here) to extensions which have only "finitely much" transcendence or non-normality.

Proposition 3.1 *Let F be a computable field of characteristic 0 with prime subfield P, and assume there exist elements $x_1, \ldots, x_n \in F$ such that F is a normal algebraic extension of $P(x_1, \ldots, x_n)$. Then F is computably categorical. Moreover, the same holds for computable fields F of characteristic p if we assume that each x_i is algebraic over P.*

Proof. We will handle all characteristics simultaneously. Suppose that $\tilde{F}$ is another computable field, and that $\varphi : F \to \tilde{F}$ is an isomorphism between them. We build a computable isomorphism $f : F \to \tilde{F}$, which will be the union of compatible partial isomorphisms f_s, each with domain $D_s \subset F$. We start by setting $D_0 = \{0, 1, x_1, \ldots, x_n\}$ and defining $f_0(0) = 0$, $f_0(1) = 1$, and $f_0(x_i) = \varphi(x_i)$ for all i.

At stage $s + 1$, we extend f_s to the element $s \in F$. By assumption the field F_s generated by D_s is computably enumerable, and so is the polynomial ring $F_s[X]$. Moreover, by Theorem 2.2, we have a splitting algorithm for $F_s[X]$, uniformly in s. (In the case where $\chi(F) \neq 0$, this is why we require all x_i to be algebraic over P.) Therefore, we can search until we find a polynomial in $F_s[X]$ with root s, and then factor it until we have the minimum polynomial $p_s(X)$ of s over F_s. (Here we use the fact that F is algebraic over $P(x_1, \ldots x_n)$.) Now f_s is uniquely (and computably) extendible to an isomorphism from F_s onto a subfield $\tilde{F}_s$ of $\tilde{F}$ containing the range $\tilde{D}_s$ of f_s, and applying this map to the coefficients in $p_s(X)$ gives a polynomial $\tilde{p}_s(X) \in \tilde{F}_s[X]$. Find the least root r of $\tilde{p}_s$ in $\tilde{F}$, and set $f_{s+1}(s) = r$. This completes the construction.

To see that $f = \cup_s f_s$ is an isomorphism, we need the following standard result. (See, for example, [18] for a proof.)

Sublemma 3.2 *Given any countable fields $L \subseteq K \subseteq E$ such that K/L is a Galois extension and E/L a normal separable (but possibly infinite) extension, every element of Gal(K/L) extends to an element of Gal(E/L).*

Sublemma 3.3 *At each stage s of this construction, the map f_s can be extended to an isomorphism from F onto $\tilde{F}$.*

Proof. For $s = 0$, f_s is the restriction of the isomorphism φ to D_0. Proceeding by induction on s, we suppose that f_s extends to an isomorphism ψ. Then $f_{s+1}(s)$ and $\psi(s)$ will both be roots of the polynomial $\tilde{p}(X)$. Now F is normal over $P(x_1, \ldots, x_n)$, and the normality is preserved by the isomorphism ψ, so $\tilde{F}$ must contain a splitting field $\tilde{K}$ of $\tilde{p}(X)$ over $\tilde{F}_s$. By Lemma 2.12, there is an automorphism σ of this splitting field which fixes $\tilde{F}_s$ pointwise and maps $\psi(s)$ to $f_{s+1}(s)$. Moreover, Sublemma 3.2 allows us to extend σ to an automorphism ρ of $\tilde{F}$. But $(\sigma \circ \psi)\restriction D_{s+1} = f_{s+1}$ since σ is the identity on the subset $f_s(D_s)$ of $\tilde{F}_s$, and $\sigma(\psi(s)) = f_{s+1}(s)$. Thus $\rho \circ \psi$ is the desired isomorphism extending f_{s+1}. ■

Therefore, $f = \cup_s f_s$ is a monomorphism of fields. Moreover, f and φ are equal on the domain $P(x_1, \ldots, x_n)$, and every $\tilde{a} \in \tilde{F}$ is algebraic over the image of $P(x_1, \ldots, x_n)$. If $\tilde{p}(X)$ is the minimum polynomial for $\tilde{a}$, then eventually all the roots of the corresponding polynomial in $P(x_1, \ldots, x_n)[X]$ will enter the domain of f, and one of these roots must be mapped to $\tilde{a}$. Therefore the range of f is $\tilde{F}$, and f is the computable isomorphism we needed. ■

The key here was Lemma 2.12, which allowed us to choose $f_{s+1}(s)$ to be the first element we found in $\tilde{F}$ satisfying the appropriate polynomial there, knowing that this was the correct choice up to an automorphism of $\tilde{F}$ over the image of f_s.

However, in the case where the extension is algebraic but not normal, it is possible for computable categoricity to fail. This was proven in [7], but here we construct an example which introduces the techniques we will use in subsequent results. Begin by using the even integers to construct identical computable copies F_0 and $\tilde{F}_0$ of the field $\mathbb{Q}[\sqrt{p_e} : e \in \omega]$, where $p_0, p_1, \ldots$ are the primes. Write w_e and v_e for the two square roots in F_0 of the e-th prime (i.e. of the number $1 + 1 + \cdots 1$, added p_e times), and $\tilde{w}_e$ and $\tilde{v}_e$ for the same two square roots in $\tilde{F}_0$. At each stage $s + 1$, we check whether there exists $e \leq s$ such that $\varphi_{e,s}(w_e)$ converges to either $\tilde{w}_e$ or $\tilde{v}_e$. If not, we end the stage. If so, then for the least such e, we adjoin to F_s half of the remaining odd integers, in such a way as to adjoin two square roots of v_e, and we adjoin to $\tilde{F}_s$ the same odd integers, but now adjoining two square roots of $\varphi_e(w_e)$. Having done so, we end the stage.

Clearly the fields F and $\tilde{F}$ thus constructed are computable and isomorphic. However, if any φ_e were an isomorphism from F onto $\tilde{F}$, then $\varphi_e(w_e)$ would have to converge to either $\tilde{v}_e$ or $\tilde{w}_e$, and when we saw this convergence, we would have destroyed the isomorphism φ_e, since w_e would have no square root in F, yet $\varphi_e(w_e)$ would have a square root in $\tilde{F}$. (To prove the absence of square roots of w_e in F, notice that we may view F as a subfield of the reals, by thinking of each v_e as the positive square root of p_e. Hence F has no more than two fourth roots of any of its elements. Since the square roots of v_e are fourth roots of p_e, w_e cannot have any square roots of its own. Moreover, since F and $\tilde{F}$ are isomorphic, the square roots of $\varphi_e(w_e)$ are the only fourth roots of $(\tilde{v}_e)^2$ in $\tilde{F}$.)

Since we must perform this diagonalization at infinitely many stages, the field F does not satisfy Proposition 3.1: F is an algebraic extension of its prime subfield P, the rationals, but it is certainly not a normal extension, even over any finite subfield $P[x_1, \ldots x_n]$. In particular, for every e such that we diagonalized against φ_e, the irreducible polynomial $X^4 - (w_e)^2$ in $P[X]$ has exactly two roots in F. (Recall that $(w_e)^2$ represents the e-th prime number, with the integers viewed as a subring of P.) If we extended F and $\tilde{F}$ to include all four roots of these polynomials, then they would become normal over their prime subfields, but the diagonalization would no longer hold.

A more interesting result, requiring more technical results from field theory, concerns our ability to avoid computable categoricity even while preserving a splitting algorithm. The preceding construction failed to do so: a splitting algorithm for that F would allow one to decide whether $(X^2 - v_e)$ has any roots in F, from which we could determine immediately whether or not $\varphi_e(v_e)$ and $\varphi_e(w_e)$ will ever converge to $\tilde{v}_e$ and $\tilde{w}_e$, which is not a decidable question.

Theorem 3.4 *There exists a computable algebraic field F which is not computably categorical, yet possesses a splitting algorithm.*

Proof. We build isomorphic computable fields F and $\tilde{F}$ of characteristic 0, diagonalizing against any computable isomorphism between them, yet retaining a root algorithm. By Corollary 2.7, this will suffice.

Let F_0 and $\tilde{F}_0$ be identical computable copies of the quadratic closure of the field $\mathbb{Q}$, as defined in Lemma 2.9. We will use $\sqrt{p_e}$ to diagonalize against the partial computable function φ_e, so that it cannot be an isomorphism. The strategy is much the same as above: at each stage s, find all $e \leq s$ such that $\varphi_{e,s}(\sqrt{p_e})\downarrow = \pm\sqrt{\tilde{p}_e}$ (and such that we have not already acted against φ_e at a previous stage). For each such e in turn, fix the least odd prime number $d_e > s + 1$ which is larger than any prime yet used in the construction. We search until we find a polynomial $h_e(X)$ of degree d_e, with coefficients in the subfield $\mathbb{Q}[\sqrt{p_e}]$ of F_0, which satisfies the conditions of Proposition 2.15 for d_e and p_e. (We will not actually use all of these conditions here; it is

Theorem 4.1 below which demands the full strength of the proposition.) Set $F_{s+1} = F_s[r_e]$, where r_e is any root of $h_e(X)$. If $\varphi_e(\sqrt{p_e}) = -\sqrt{\tilde{p}_e}$, then let $\tilde{F}_{s+1} = \tilde{F}_s[\tilde{r}_e]$, where $\tilde{r}_e$ is a root of $h_e(X)$ (with coefficients now in $\tilde{F}_0$, of course); but if $\varphi_e(\sqrt{p_e}) = \sqrt{\tilde{p}_e}$, then let $\tilde{F}_{s+1} = \tilde{F}_s[\tilde{r}_e^-]$, where $\tilde{r}_e^-$ is a root of $h_e^-(X)$, the image of $h_e(X)$ when the automorphism σ of $\mathbb{Q}[\sqrt{p_e}]$ with $\sigma(\sqrt{p_e}) = -\sqrt{p_e}$ is applied to the coefficients of $h_e(X)$. This completes the construction, and we let $F = \cup_s F_s$ and $\tilde{F} = \cup_s \tilde{F}_s$.

First we point out that when the diagonalization happens, $h_e(X)$ really is irreducible over F_s, not just over $\mathbb{Q}[\sqrt{p_e}]$. We know by Lemma 2.11 that $h_e(X)$ is irreducible over every repeated quadratic extension of $\mathbb{Q}[\sqrt{p_e}]$, hence also over F_0. Recall that $F_{s+1} = F_s[r_e]$, with r_e chosen to be any root of $h_e(X)$. Since h_e is irreducible over F_0, we know that $[F_0[r_e] : F_0] = d_e$, which (by induction and choice of d_e) is a prime not dividing $[F_s : F_0]$. But $[F_0[r_e] : F_0]$ must divide $[F_{s+1} : F_0]$, hence must divide $[F_{s+1} : F_s]$. On the other hand, $[F_{s+1} : F_s] \leq d_e$ because r_e satisfies a polynomial of degree d_e over F_s, and so in fact $[F_{s+1} : F_s] = d_e$. This implies that $h_e(X)$ really is the minimal polynomial of r_e over F_s, and so $h_e(X)$ was irreducible over F_s. It follows from Lemma 2.12 that it does not matter which root r_e we chose: we will always have $F_s[r_e] \cong F_s[X]/(h_e(X))$. So the construction above is well-defined.

It now follows that F_s and $\tilde{F}_s$ are isomorphic for every s. At stage 0 there are 2^ω-many possible isomorphisms f_0 from F_0 onto $\tilde{F}_0$, with each $\sqrt{p_e}$ being mapped to either of $\pm\sqrt{\tilde{p}_e}$. When we diagonalize against some φ_e at a stage $s+1$, there will still be one (but now only one) possible value for $f_{s+1}(\sqrt{p_e})$, namely $-\varphi_e(\sqrt{p_e})$, because $h_e(X)$ now has a root in F_{s+1}, while $h_e^-(X)$ does not, and exactly one of $h_e(X)$ and $h_e^-(X)$ has a root in $\tilde{F}_{s+1}$, with the choice made so that φ_e mapped $\sqrt{p_e}$ to the wrong element. Thereafter, all further extensions of F_{s+1} are of larger degrees prime to d_e, and so no more roots of h_e or h_e^- ever appear in either F or $\tilde{F}$, by Lemma 2.11. So for each stage $s+1$ at which we diagonalize, half of the isomorphisms from F_s to $\tilde{F}_s$ extend to isomorphisms from F_{s+1} to $\tilde{F}_{s+1}$, namely those with the correct value for $\sqrt{p_e}$. φ_e is not one of that half, so it cannot be an isomorphism. Thus $F \cong \tilde{F}$, but they are not computably isomorphic.

The root algorithm for F is straightforward. F_0 has a root algorithm, by Lemma 2.9, and therefore so do all the (finite) extensions F_s of F_0, uniformly in s, by Theorem 2.2. Given any $p(X) \in F[X]$, find an $n \geq \deg(p(X))$ such that $p(X) \in F_n[X]$, and check whether F_n contains any roots of $p(X)$. If not, then $p(X)$ has no root in F: for $s \geq n$, either $F_{s+1} = F_s$ or $[F_{s+1} : F_s]$ is a prime $d > s \geq n$, in which case all elements of $(F_{s+1} - F_s)$ have degree d over F_s, hence cannot be roots of $p(X)$. ■

4 $\mathbf{0}'$-Computable Categoricity

We now build a computable algebraic field F which is not even $\mathbf{0}'$-categorical. This construction requires the full strength of Proposition 2.15.

Theorem 4.1 *There exists a computable algebraic field F which is not $\mathbf{0}'$-categorical.*

The author is grateful to Joseph Miller and Frank Stephan for pointing out an error in his original construction of F. The new proof is as follows.

Proof. The object is to build isomorphic CAFs F and $\tilde{F}$ satisfying the requirements:

$$\mathcal{R}_e : \quad g_e(x) = \lim_t \varphi_e(x, t) \text{ is not an isomorphism from } F \text{ onto } \tilde{F}.$$

Here $g_e(x)$ is defined iff the given limit converges. All $\mathbf{0}'$-computable functions can be represented as such limits, so these requirements are all that is necessary to prove the theorem.

The idea is to use the square roots $\sqrt{p_e}$ and $-\sqrt{p_e}$ of the e-th prime number p_e as witnesses for $\mathcal{R}_e$. If $g_e(\sqrt{p_e})\downarrow= \pm\sqrt{\tilde{p}_e}$, the corresponding roots in $\tilde{F}$, then for all sufficiently large t we have $\varphi_e(\sqrt{p_e}, t)\downarrow= \pm\sqrt{\tilde{p}_e}$. At each stage $s+1$, for the largest t such that $\varphi_{e,s}(\sqrt{p_e}, t)\downarrow= \pm\sqrt{\tilde{p}_e}$, Proposition 2.15 allows us to adjoin to F_s a single root r^- of a polynomial h_s^-, of some large prime degree d, and meanwhile to adjoin to $\tilde{F}_{s+1}$ a single root of either of the corresponding polynomials $\tilde{h}_s$ or $\tilde{h}_s^-$, so that the only isomorphisms from F_{s+1} onto $\tilde{F}_{s+1}$ map $\sqrt{p_e}$ to $-\varphi_e(\sqrt{p_e}, t)$. If at some subsequent stage $s'+1$ we find that $\varphi_e(\sqrt{p_e}, t')\downarrow= -\varphi_e(\sqrt{p_e}, t)$ for some $t' > t$ (so that the current approximation to g_e has reversed itself to the correct value), then we may adjoin a single root of h_s to F and the same for $\tilde{F}$; now the Galois group of F allows $\sqrt{p_e}$ to be mapped to either $\pm\sqrt{p_e}$, and so we will appeal again to Proposition 2.15 for a new $h_{s'}(X)$ of a new larger prime degree which we can now use to diagonalize against the new approximation $\varphi_e(\sqrt{p_e}, t')$ in the same way. In short, the process of building a computable field (without a splitting algorithm) allows us to retract our earlier commitment against $\varphi_e(\sqrt{p_e}, t)$ if necessary, without removing any elements from F; we simply adjoin new elements to make F symmetric with respect to $\sqrt{p_e}$ and $-\sqrt{p_e}$ again, regaining the freedom to diagonalize against the new approximation. Of course, the approximation $\varphi_e(\sqrt{p_e}, t)$ could change its value for infinitely many t, but in this case $\mathcal{R}_e$ will clearly be satisfied, since g_e will not even be total, and our fields F and $\tilde{F}$ will still be isomorphic, with a unique root of each h_s and each h_s^- in F and of each $\tilde{h}_s$ and each $\tilde{h}_s^-$ in $\tilde{F}$. Finally, using new prime degrees d for each new diagonalization will ensure that the new elements we adjoin will not upset our diagonalizations on behalf of any other requirements $\mathcal{R}_i$; the key here is Lemma 2.11, along with the primality of the degrees $[F_{s+1} : F_s]$.

We start the construction by setting $F_0 = \tilde{F}_0 = \mathbb{Q}$. The initial isomorphism f_0 is just the identity map from F_0 onto $\tilde{F}_0$.

At a stage $s + 1 = \langle e, 0\rangle + 1$, we take our *initial action* on behalf of the requirement $\mathcal{R}_e$. Fix the least prime p_e such that $\sqrt{p_e} \notin F_s$, and let $\tilde{p}_e$ be the same prime in $\tilde{F}_s$; there must be such a p_e, since (by induction) $[F_s : \mathbb{Q}]$ is finite. (In fact p_e will always be the e-th prime number.) Let $F_s' = F_s[\sqrt{p_e}]$ and $\tilde{F}_s' = \tilde{F}_s[\sqrt{\tilde{p}_e}]$, with the names $\sqrt{p_e}$ and $\sqrt{\tilde{p}_e}$ staying affixed to these elements at all subsequent stages. and let d_{s+1} be the least prime number $> d_s$. Find a polynomial $h_{s+1}(X) \in \mathbb{Z}[\sqrt{p_e}][X] \subset F_s'[X]$ of degree d_{s+1} satisfying the properties given in Proposition 2.15. Let r_{s+1}^- be a root of the corresponding $h_{s+1}^-(X)$, and define $F_{s+1} = F_s'[r_{s+1}^-]$. Similarly, let $\tilde{h}_{s+1}(X) \in \tilde{F}_s'[X]$ be the same polynomial, with its coefficients now interpreted in $\tilde{F}$ (using $\sqrt{\tilde{p}_e}$ in the same role as $\sqrt{p_e}$ in F_s). Define $\tilde{F}_{s+1} = \tilde{F}_s'[\tilde{r}_{s+1}^-]$, where r_{s+1}^- is a root of $\tilde{h}_{s+1}^-$. For convenience we write $\varphi_e(\sqrt{p_e}, -1) = -\sqrt{\tilde{p}_e}$, and define f_{s+1} to extend f_s by setting $f_{s+1}(\sqrt{p_e}) = \sqrt{\tilde{p}_e}$ and $f_{s+1}(r_{s+1}^-) = \tilde{r}_{s+1}^-$. Thus f_{s+1} really is an isomorphism, assuming that f_s was.

At a stage $s + 1 = \langle e, i + 1\rangle + 1$, we define $s' = \langle e, j\rangle + 1$ (with $j \leq i$) to have been the last stage at which we took action on behalf of $\mathcal{R}_e$. (Since we took initial action on its behalf at stage $\langle e, 0\rangle + 1$, this must be defined.) Let t_{s+1} be the greatest $t \leq s$ such that $\varphi_{e,s}(\sqrt{p_e}, t') \downarrow$ for every $t' \leq t$ (allowing $t_{s+1} = -1$). If $\varphi_e(\sqrt{p_e}, t_{s+1}) \neq f_s(\sqrt{p_e})$, then we set $d_{s+1} = d_{s'}$, change nothing else, and take no action at this stage. (This includes the case $t_{s+1} = t_{s'}$, of course.) Otherwise, the approximation to the function g_e has changed its guess and now appears correct, so we respond with a *subsequent action* on behalf of $\mathcal{R}_e$. At stage s', we had adjoined a root $r_{s'}^-$

of the polynomial $h^-_{s'}(X)$ to F. Now we adjoin a root $r_{s'}$ of $h_{s'}(X)$ to F_s to create $F'_s = F_s[r_{s'}]$. Likewise, either $\tilde{h}_{s'}(X)$ or $\tilde{h}^-_{s'}(X)$ (but not both) has a root in $\tilde{F}$, and we adjoin a root of the other one to $\tilde{F}_s$ to create $\tilde{F}'_s$. Each of these four polynomials will now have exactly one root in its field, as we prove below.

Also, we choose d_{s+1} to be the least prime number $> d_s$, and find a polynomial $h_{s+1}(X) \in \mathbb{Q}[\sqrt{p_e}][X] \subset F'_s[X]$ of degree d_{s+1} satisfying the properties given in Proposition 2.15. Let r^-_{s+1} be a root of the corresponding $h^-_{s+1}(X)$, and define $F_{s+1} = F'_s[r^-_{s+1}]$. Similarly, let $\tilde{h}_{s+1}(X) \in \tilde{F}'_s[X]$ be the same polynomial, with its coefficients now interpreted in $\mathbb{Q}[\sqrt{\tilde{p}_e}] \subseteq \tilde{F}'_s$. If $\varphi_e(\sqrt{p_e}, t_{s+1}) = \sqrt{\tilde{p}_e}$, then we define $\tilde{F}_{s+1} = \tilde{F}'_s[\tilde{r}_{s+1}]$, where $\tilde{r}_{s+1}$ is a root of $\tilde{h}_{s+1}$; we also define $f_{s+1}(\sqrt{p_e}) = -\sqrt{p_e}$ and $f_{s+1}(r^-_{s+1}) = \tilde{r}_{s+1}$. If not, then $\varphi_e(\sqrt{p_e}, t_{s+1}) = -\sqrt{\tilde{p}_e}$, and we define $\tilde{F}_{s+1} = \tilde{F}'_s[\tilde{r}^-_{s+1}]$, $f_{s+1}(\sqrt{p_e}) = \sqrt{p_e}$, and $f_{s+1}(r^-_{s+1}) = \tilde{r}^-_{s+1}$, where $\tilde{r}^-_{s+1}$ is a root of $\tilde{h}^-_{s+1}$. This completes stage $s+1$ of the construction, and F and $\tilde{F}$ are the fields built during all these stages.

We claim, by induction on stages s, that every f_s is an isomorphism from F_s onto $\tilde{F}_s$, and that the degree $[F_{s+1} : F_s]$ of the extension at each stage is either $2d_{s+1}$ (for an initial action at that stage), or $(d_{s+1} \cdot d_{s'})$ (if we made a subsequent action at stage $s+1$), or 1 in all other cases. Notice that whenever we take any action, d_{s+1} is chosen to be a prime degree larger than the degree d_s used for the most recent action. In every initial action, a square root $\sqrt{p_e} \notin F_s$ is adjoined to F_s, generating an extension F'_s of degree 2. Clearly f_s extends to an isomorphism f'_s from F'_s onto $\tilde{F}'_s$. Then a root r^-_{s+1} of h^-_{s+1} is adjoined to F'_s. Now r^-_{s+1} has degree d_{s+1} over $\mathbb{Q}[\sqrt{p_e}]$, by Proposition 2.15, so d_{s+1} divides $[F_{s+1} : \mathbb{Q}]$, yet by induction $d_{s+1} \nmid [F'_s : \mathbb{Q}]$. Therefore $d_{s+1} \mid [F_{s+1} : F'_s]$. Moreover $F_{s+1} = F'_s[r^-_{s+1}]$ has degree at most d_{s+1} over F'_s, because r^-_{s+1} satisfies the polynomial $h^-_{s+1}(X) \in F'_s[X]$ of degree d_{s+1}, and so indeed $d_{s+1} = [F_{s+1} : F'_s]$ and $2d_{s+1} = [F_{s+1} : F_s]$. This also shows that $h^-_{s+1}(X)$ is the minimal polynomial of r^-_{s+1} over F'_s, because the degree of the extension $F'_s[r^-_{s+1}]$ over F'_s must be the degree of the minimal polynomial of r^-_{s+1} over F'_s. Likewise $\tilde{h}^-_{s+1}(X)$ is the minimal polynomial of $\tilde{r}^-_{s+1}$ over $\tilde{F}'_s$, and so the isomorphism f'_s does indeed extend to an isomorphism f_{s+1} from F_{s+1} onto $\tilde{F}_{s+1}$.

It remains to consider the case of a subsequent action on behalf of some $\mathcal{R}_e$ at stage $s+1$. In such an action we first build F'_s by adjoining a root $r_{s'}$ of $h_{s'}(X)$ to F_s, following an earlier action for $\mathcal{R}_e$ at a stage $s' \leq s$. By induction $d_{s'} \mid [F_s : \mathbb{Q}]$, but $(d_{s'})^2 \nmid [F_s : \mathbb{Q}]$. The final condition of

Proposition 2.15 makes clear that $[\mathbb{Q}[\sqrt{p_e}, r_{s'}^-, r_{s'}] : \mathbb{Q}[\sqrt{p_e}, r_{s'}^-]] = d_{s'}$, and so $[\mathbb{Q}[\sqrt{p_e}, r_{s'}^-, r_{s'}] : \mathbb{Q}] = 2(d_{s'})^2$. Therefore $(d_{s'})^2$ must divide $[F_{s'} : \mathbb{Q}]$, and so $d_{s'}$ must divide $[F'_s : F_s]$. As above, $[F'_s : F_s]$ actually equals $d_{s'}$, since $r_{s'}$ satisfies the polynomial $h_{s'}(X)$ of degree $d_{s'}$ over F_s, and so $h_{s'}(X)$ is the minimal polynomial of $r_{s'}$ over F_s. Then we consider the extension $F_{s+1} = F'_s[r_{s+1}^-]$. The argument there is exactly the same as the argument above for initial actions: $d_{s+1} \nmid [F'_s : \mathbb{Q}]$, but does divide $[\mathbb{Q}[r_{s+1}^-] : \mathbb{Q}]$, hence divides $[F_{s+1} : \mathbb{Q}]$, hence divides (and indeed equals) $[F_{s+1} : F'_s]$. Thus $h_{s+1}^-(X)$ is the minimal polynomial of r_{s+1}^- over F'_s, and moreover $d_{s+1} \cdot d_{s'} = [F_{s+1} : F_s]$.

Finally, parallel arguments for $\tilde{F}_{s+1}$, again using Proposition 2.15, show that $[F_{s+1} : F_s] = [\tilde{F}_{s+1} : \tilde{F}_s]$ for every s, so that the elements adjoined all have the same degrees and the corresponding minimal polynomials. The same square roots of primes are adjoined to $\tilde{F}_s$ during all initial actions, and when we adjoined a root of an h-polynomial to $\tilde{F}_{s+1}$, we had adjoined a root of another h-polynomial to F_{s+1}, such that the coefficients of the one polynomial were mapped to the coefficients of the other by f_{s+1} (as defined on F'_s or on F_s). So indeed f_{s+1} is an isomorphism from F_{s+1} onto $\tilde{F}_{s+1}$, completing the induction.

We cannot claim that $\lim_s f_s$ is an isomorphism from F to $\tilde{F}$; indeed, if it were, we would have diagonalized against it! For each e, define $\mathcal{R}_e$ to be *finitary* if we took action against it at only finitely many stages, and *infinitary* otherwise. If $\mathcal{R}_e$ is finitary, then $\lim_s f_s(\sqrt{p_e})$ converges, and we define $f(\sqrt{p_e})$ to be that limit. Otherwise $\lim_s f_s(\sqrt{p_e})$ diverges (which is why $\lim_s f_s$ fails to be an isomorphism), and we arbitrarily define $f(\sqrt{p_e}) = \sqrt{\tilde{p}_e}$, since in this case either of $\pm\sqrt{\tilde{p}_e}$ can be the image of $\sqrt{p_e}$ under an isomorphism. In either case, for the roots r_s^- and r_s adjoined at various stages s at which we acted on behalf of $\mathcal{R}_e$, we then define

$$f(r_s) = \begin{cases} \tilde{r}_s, & \text{if } f(\sqrt{p_e}) = \sqrt{\tilde{p}_e} \\ \tilde{r}_s^-, & \text{if } f(\sqrt{p_e}) = -\sqrt{\tilde{p}_e} \end{cases} \qquad f(r_s^-) = \begin{cases} \tilde{r}_s^-, & \text{if } f(\sqrt{p_e}) = \sqrt{\tilde{p}_e} \\ \tilde{r}_s, & \text{if } f(\sqrt{p_e}) = -\sqrt{\tilde{p}_e} \end{cases}$$

Since each of these roots was irreducible over the field F_s at the stage $s+1$ at which it was adjoined, and since all these roots together (including the square roots) generate F, the function f defined above extends uniquely to all of F. Moreover, the extension to each F_{s+1} from F_s is clearly an embedding into F (not necessarily into $\tilde{F}_{s+1}$, since a root $\tilde{r}_{s+1}$ or $\tilde{r}_{s+1}^-$ might only appear at a subsequent stage; but if no subsequent action is taken for this requirement, then generators of F_{s+1} over F_s do map to elements of $\tilde{F}_{s+1}$). Likewise, the inverse of this map f is seen to be an embedding with domain $\tilde{F}$, by the same argument, and so f is indeed an isomorphism.

It remains to see that all requirements have been satisfied. But this is straightforward: if $g_e = \lim_t \varphi_e(\,\cdot\,, t)$ were to be an isomorphism, then necessarily $\lim_t \varphi_e(\sqrt{p_e}, t)\downarrow = \pm\sqrt{\tilde{p}_e}$. Assume for the moment that it converged to $\sqrt{\tilde{p}_e}$, and fix the least modulus t_0 of this convergence, The construction shows that we would have acted at stage $s = \langle e, t_0\rangle + 1$ by adjoining an element r_s^- to F with $h_s^-(r_s^-) = 0$, and an element $\tilde{r}_s$ to $\tilde{F}$ with $\tilde{h}_s(\tilde{r}_s) = 0$. Write $h_s(X) = h(\sqrt{p_e}, X)$ for some polynomial $h(Y, X) \in \mathbb{Q}[Y, X] \subset F[Y, X]$, and $\tilde{h}(Y, X)$ for the corresponding polynomial with coefficients in the prime field of $\tilde{F}$. (Given the polynomials from Proposition 2.15, we can take h to be linear in Y.)

Since no further action against $\mathcal{R}_e$ was ever required, we see by the inductive argument above that $(d_s)^2 \nmid [\tilde{F}_{s_0} : \mathbb{Q}]$ for all $s_0 > s$. However, d_s does divide $[\tilde{F}_s : \mathbb{Q}]$ due to $\tilde{r}_s$, so by Proposition 2.15, any root $\tilde{r}$ of $\tilde{h}_s^-(X)$ in $\tilde{F}$ would have forced $(d_s)^2$ to divide $[\mathbb{Q}[\tilde{r}_s, \tilde{r}] : \mathbb{Q}]$, hence to divide $[\tilde{F}_{s_0} : \mathbb{Q}]$ for each stage $s_0 > s$ with $\tilde{r} \in \tilde{F}_{s_0}$. Therefore $\tilde{F}$ contains no root of $\tilde{h}_s^-(X)$. But then $\tilde{F}$ contains no root of $\tilde{h}(-\sqrt{\tilde{p}_e}, X)$, whereas in F we have $h(-\sqrt{p_e}, r_s^-) = 0$, so no isomorphism from F to $\tilde{F}$ could map $\sqrt{p_e}$ to $\sqrt{\tilde{p}_e}$. Thus g_e cannot be an isomorphism.

The case where $g_e(\sqrt{p_e}) = -\sqrt{\tilde{p}_e}$ is parallel, except that now $\tilde{F}$ contains no root of $\tilde{h}_s(X)$, whereas F still contains a root r_s^- of $h_s^-(X)$, according to the construction at stage s. Once again one sees that g_e cannot have been an isomorphism. Thus F and $\tilde{F}$, although isomorphic, are not $\mathbf{0}'$-computably isomorphic, proving the theorem. ■

The two constructions of Theorem 4.1 and Theorem 3.4 are similar: Theorem 3.4 uses a diagonalization strategy once for each requirement, and Theorem 4.1 uses the same strategy, but more than once. However, the two constructions cannot be combined. In Theorem 4.1, in order to have a root algorithm for F, we would be required to decide, when adjoining roots such as r_s and $\tilde{r}_{s+1}^-$ to F and $\tilde{F}$, whether the polynomials $h_{s+1}(X)$ and $h_{s+1}^-(X)$ have any other roots in F. If we say yes to either of these questions, then our diagonalization against φ_e fails; but if we say no, then we preclude any further chance to change our minds. So we would be unable to go back and forth between the possibilities, but could only diagonalize once, and consequently could only avoid potential computable isomorphisms, not potential $\mathbf{0}'$-computable ones.

In fact, the inability to go back also makes it hard even to code a set such as $\emptyset'$, the halting problem, into the isomorphism from F onto $\tilde{F}$ in Theorem 3.4. We can ensure that the entrance of an e into $\emptyset'$ is reflected in the isomorphism, by forcing $\sqrt{p_e}$ in F to map to $-\sqrt{p_e}$ in $\tilde{F}$ once we see e enter $\emptyset'$. However, in the situation where e never enters $\emptyset'$, isomorphisms can send the $\sqrt{p_e}$ in F to either $\pm\sqrt{p_e}$ in $\tilde{F}$, so this method does not ensure that an isomorphism will compute $\emptyset'$. $\sqrt{p_e}$ starts out with two possible images in $\tilde{F}$, but once we pin it down to one of them, we cannot unpin it without injuring the splitting algorithm. A similar comment, one jump higher, applies to Theorem 4.1: the F built there is not $\mathbf{0}'$-categorical, but it is not clear how one might code a set of degree $\mathbf{0}''$ into the isomorphisms that do exist from F onto $\tilde{F}$. We will see in the next section that such a coding is impossible.

5 $\boldsymbol{d}$-Computable Categoricity

Having shown that computable algebraic fields can fail to be $\mathbf{0}'$-categorical, and that even those with splitting algorithms need not be computably categorical, we now produce positive results stating that they must be fairly close to those levels of categoricity. First we need some mechanics. The *isomorphism tree* will have nodes corresponding to finite partial isomorphisms from F into $\tilde{F}$, and paths corresponding to full isomorphisms.

Definition 5.1 Fix isomorphic computable algebraic fields F and $\tilde{F}$, with prime fields $\mathbb{Q}$ and $\tilde{\mathbb{Q}}$, and write $\{x_0, x_1, \ldots\}$ instead of ω for the domain of F, with $x_i = i$ for all i. (This is just to avoid confusion with $\tilde{F}$, whose domain is still ω.) For each $n \in \omega$, let $p_n(X)$ be the minimal polynomial of x_n over $\mathbb{Q}[x_0, \ldots, x_{n-1}]$, say with degree d. Now choose polynomials $r_0, \ldots, r_d \in \mathbb{Q}[X_0, \ldots, X_{n-1}]$ such that the i-th coefficient of p_n is $r_i(x_0, \ldots, x_{n-1})$, and let

$$q_n(X_0, \ldots, X_n) = \sum_{i=0}^{d} r_i(X_0, \ldots, X_{n-1}) \cdot X_n^i.$$

The *isomorphism tree for F and $\tilde{F}$* is the set

$$T_{F,\tilde{F}} = \{\sigma \in \omega^{<\omega} : (\forall n < \mathrm{lh}(\sigma))\ \tilde{q}_n(\sigma(0), \ldots, \sigma(n)) = 0 \text{ in } \tilde{F}\},$$

where each $\tilde{q}_n$ is the image of q_n with coefficients mapped from $\mathbb{Q}$ to $\tilde{\mathbb{Q}}$.

It is clear that $T_{F,\tilde{F}}$ is a subtree of $\omega^{<\omega}$. By Lemma 2.3, p_n is computable uniformly in n. By induction on the length n of $\sigma \in T_{F,\tilde{F}}$, one sees that the map $\mathbb{Q}[x_0, \ldots, x_{n-1}] \to \tilde{\mathbb{Q}}[\sigma(0), \ldots, \sigma(n-1)]$ with $x_i \mapsto \sigma(i)$ is an isomorphism for all such σ. Hence, if f is a path through $T_{F,\tilde{F}}$, then f defines an embedding of F into $\tilde{F}$, indeed an isomorphism from F onto $\tilde{F}$, by Lemma 2.10. Conversely, it is clear that every isomorphism f from F onto $\tilde{F}$ is defined by a unique path through $T_{F,\tilde{F}}$ in this way.

Intuitively, the process here is simply to line up all the elements $x_0, x_1, \ldots$ of F, and then to search for possible embeddings of each $\mathbb{Q}[x_0, \ldots, x_n]$ into $\tilde{F}$. The splitting algorithms for finite extensions of $\mathbb{Q}$ enable us to recognize such embeddings when we find them, and we make them into a tree in the obvious way, by viewing them as maps from the finite set $\{x_0, \ldots, x_n\}$ into $\tilde{F}$. Basic facts from field theory, along with the algebraicity of F, show the tree to be finite-branching, and paths through it correspond to full isomorphisms from F onto $\tilde{F}$. Of course, some nodes on the tree may be nonextendible, i.e. may not lie on any (infinite) path.

Theorem 5.2 *Any two isomorphic computable algebraic fields F and $\tilde{F}$ have an isomorphism f from F onto $\tilde{F}$ such that $f' \leq_T R'$, where R is the root set of F.*

Proof. The number of immediate successors of a node $\sigma \in T_{F,\tilde{F}}$ is just the number of roots of $q_n(\sigma(0), \ldots, \sigma(n-1), X_n)$ in $\tilde{F}$ (where $n = \mathrm{lh}(\sigma)$). This number is finite and can be computed from the root set of $\tilde{F}$, or (by Corollary 2.8) from the root set R of F. In the language of [3], this says that the computable tree $T_{F,\tilde{F}}$ is *highly R-recursive*, or *highly R-computable*. But now we can apply the Low Basis Theorem of Jockusch and Soare (from [19], or see Theorem 3.6 of [3]), relativized to an R-oracle, to conclude that there is a path through $T_{F,\tilde{F}}$ which is low relative to R. This path immediately computes the isomorphism f we desire, since the lowness means that $f' \leq_T R'$. ∎

Since the Low Basis Theorem actually yields more, we state it in full here, in a relativized form. For a proof, see also [3]. By definition, an R-computable finite-branching tree T is an R-computable subset of $\omega^{<\omega}$, closed under initial segments, with each level finite.

Theorem 5.3 (Low Basis Theorem; Jockusch & Soare [19]) *Fix any set $R \subseteq \omega$, and let $\mathcal{T}$ be the class of all those R-computable finite-branching* *trees T for which the function $s : T \to \omega$ via*

$$s(\sigma) = |\{n \in \omega : \sigma\hat{\ }\langle n\rangle \in T\}|$$

is also R-computable. Then there exists a Turing degree $\boldsymbol{d}$ with $\boldsymbol{d}' \leq_T deg(R)'$ such that every infinite $T \in \mathcal{T}$ has a $\boldsymbol{d}$-computable path. (Such a degree is known as a PA-degree relative to *R.) Indeed, there exist two PA-degrees $\boldsymbol{d}_0$ and $\boldsymbol{d}_1$ relative to R such that every degree which is both $\leq_T \boldsymbol{d}_0$ and $\leq_T \boldsymbol{d}_1$ is $\leq_T deg(R)$ as well.* ■

Applying this result to our situation, we see:

Corollary 5.4 *For every computable algebraic field F with root set R, there exists a degree $\boldsymbol{d}$ low relative to R, i.e. with $\boldsymbol{d}' \leq_T deg(R')$, such that F is $\boldsymbol{d}$-computably categorical.*

Proof. By Corollary 2.8, for all computable fields $\tilde{F} \cong F$ and every $\boldsymbol{d}$ which is a PA-degree relative to R, the isomorphism tree $T_{F,\tilde{F}}$ has a path computable in $\boldsymbol{d}$. The Low Basis Theorem provides such a $\boldsymbol{d}$ low relative to R. ■

Corollary 5.5 *There exists a degree $\boldsymbol{d}$ with $\boldsymbol{d}' \leq_T \boldsymbol{0}''$ such that every computable algebraic field F is $\boldsymbol{d}$-computably categorical. Indeed, every PA-degree relative to $\boldsymbol{0}'$ is such a $\boldsymbol{d}$.*

Proof. The root set R of F, being $\exists$-definable, always satisfies $R \leq_T \emptyset'$. ■

Corollary 5.6 *There exists a low degree $\boldsymbol{d}$ such that every computable algebraic field with a splitting algorithm is $\boldsymbol{d}$-computably categorical. Indeed, every PA-degree is such a $\boldsymbol{d}$.* ■

Thus the results in Theorems 4.1 and 3.4 were essentially as strong as we could have hoped to make them. Next we recall a definition from [9].

Definition 5.7 The *categoricity spectrum* of a computable structure $\mathfrak{A}$ is the set

$$\{\boldsymbol{d} : \mathfrak{A} \text{ is } \boldsymbol{d}\text{-computably categorical}\}.$$

The *degree of categoricity* of $\mathfrak{A}$ is the least degree in the categoricity spectrum of $\mathfrak{A}$, if such a degree exists.

Corollary 5.8 *If F is a computable algebraic field with a splitting algorithm, and F is not computably categorical, then F has no degree of categoricity. More generally, for any computable algebraic field F, the degree of categoricity of F, if it exists, must be computable from the root set R of F.*

Proof. Theorem 5.3 provides two degrees $\boldsymbol{d}_0$ and $\boldsymbol{d}_1$, both PA-degrees relative to R, such that every degree below both is computable from R. But the degree of categoricity of F must lie below all degrees in the categoricity spectrum of F, including $\boldsymbol{d}_0$ and $\boldsymbol{d}_1$, and the general result follows. In the specific case where R is computable, the degree of categoricity can only be $\mathbf{0}$, making F computably categorical. ■

Fokina, Kalimullin, and Miller proved in [9] that every c.e. degree $\boldsymbol{c}$ can be the degree of categoricity of a computable algebraic field, by building isomorphic CAFs F and $\tilde{F}$ such that F is $\boldsymbol{c}$-computably categorical, but every isomorphism from F to $\tilde{F}$ computes $\boldsymbol{c}$. More generally, the following holds.

Theorem 5.9 (adapted from [9]) *For all c.e. degrees $\boldsymbol{c} \leq_T \boldsymbol{d}$, there exists a computable algebraic field F with degree of categoricity $\boldsymbol{c}$ and with root set of degree $\boldsymbol{d}$.* ■

When $\boldsymbol{c} = \boldsymbol{d}$, this is proved in [9]. In the more general case, one divides the primes in half, using half of them for degrees of polynomials in the construction of [9], which codes an arbitrary c.e. set $W \in \boldsymbol{c}$ into all isomorphisms from F to $\tilde{F}$, and using the other half for degrees of polynomials to code a c.e. set $D \in \boldsymbol{d}$ into the root set of F. Each time an n enters D, one adjoins to F a full complement of roots of a designated *code polynomial* for n, which had no roots in F until that stage. Thus, with an oracle for the root set, one can compute whether $n \in D$, and conversely, a D-oracle lets one decide W as well, so that the entire root set is D-computable. Finally, by adding all roots of the code polynomial when n enters D, we ensure that F is categorical even in the lower degree $\boldsymbol{c}$. Of course, Corollary 5.8 shows that the construction would be impossible unless $\boldsymbol{c} \leq_T \boldsymbol{d}$.

On the other hand, the field F built in Theorem 4.1 is an example of a CAF with non-computable root set which has no degree of categoricity. If it had such a degree $\boldsymbol{c}$, then by Corollary 5.8, $\boldsymbol{c}$ would be computable in its root set, hence computable in $\mathbf{0}'$. However, this is impossible, since F is not $\mathbf{0}'$-computably categorical.

We next consider the idea of the degree of categoricity of a class of computable structures, defined in the obvious way. For algebraic fields, the answer is that it cannot exist.

Corollary 5.10 *There is no least degree $\boldsymbol{d}$ such that every computable algebraic field is $\boldsymbol{d}$-computably categorical. Likewise, there is no such least degree for CAFs with splitting algorithms.*

Proof. Such a degree $\boldsymbol{d}$ would have to lie below all PA-degrees relative to $\mathbf{0}'$, by Corollary 5.5, hence below $\mathbf{0}'$, by the Low Basis Theorem with $R = \emptyset'$. Theorem 4.1 showed this to be impossible. The same argument with $R = \emptyset$ and Theorem 3.4 shows the result for fields with splitting algorithms. ■

Corollary 5.11 *Every computable algebraic field with a splitting algorithm, or even with a low splitting set, has computable dimension either* 1 *or* ω*, and both are possible.*

Proof. Goncharov showed in [13] that if two computable structures are isomorphic via a $\mathbf{0}'$-computable isomorphism but not via any computable isomorphism, then the isomorphism type of those structures has computable dimension ω. By Corollary 5.4, this result applies to all computable fields with low splitting sets which are not computably categorical, and by Theorem 3.4, such a field exists. ■

Although it is not clear whether this result extends to computable algebraic fields in general, we do note that the field F built in the proof of Theorem 4.1 has other computable copies which are $\mathbf{0}'$-computably isomorphic to it, but not computably isomorphic to it. We omit the details, which require a finite-injury argument, but the construction of F in Theorem 4.1 allows us to "scavenge" by diagonalizing against individual computable functions when the construction diagonalizes against limits of computable functions. Hence that F does have computable dimension ω, by Goncharov's result. We also note that a different modification of the proof of Theorem 4.1 allows us to build countably many isomorphic computable algebraic fields, no two of which are $\mathbf{0}'$-computably isomorphic. Thus the $\mathbf{0}'$-computable dimension of an algebraic field can also be ω.

6 Finite Transcendence Degree

So far we have considered only algebraic fields. However, our results generally carry over to the case of a field of finite transcendence degree over its prime subfield. The difference is that with (positive) finite transcendence degree it is necessary to know a transcendence basis. This constitutes finitely much information, and so it is not a problem for an algorithm to have this information. However, it does eliminate much uniformity from our previous theorems. We have not dwelt upon uniformity until now, but in this section we specifically consider it, while extending the preceding categoricity results to fields of finite transcendence degree. For the most part, the proofs are identical to those for the original results, and will be omitted. First we recall a definition.

Definition 6.1 A computable structure $\mathfrak{A}$ is *uniformly computably categorical* if there is a Turing functional Ψ such that, whenever $S \subseteq \omega$ is the atomic diagram (under some fixed Gödel numbering) of a computable structure $\mathfrak{B}$ isomorphic to $\mathfrak{A}$, the function Ψ^S is an isomorphism from $\mathfrak{A}$ onto $\mathfrak{B}$.

For example, the computable dense linear order without end points is uniformly computably categorical: one simply goes ahead and begins the standard back-and-forth construction between any two computable copies, consulting the oracle, i.e. the atomic diagram, whenever we wish to know the ordering of domain elements m and n. On the other hand, the computable dense linear order with end points is computably categorical but not uniformly so, because there is no effective way of identifying the end points in an arbitrary computable copy. (A full proof involves the construction of a counterexample to each computable partial functional which might serve as the Ψ.) Of course, if we augment the language by adding a constant symbol for each end point, then the computable DLO with end points becomes uniformly computably categorical, since now the atomic diagram effectively picks out those end points.

Proposition 3.1 already allowed for finite transcendence degree, at least in characteristic 0. The negative results, Theorems 4.1 and 3.4, do not require consideration for uniformity, since the fields constructed there are not even computably categorical. The interesting situations are the categoricity results in Section 5. These results can readily be reproduced for fields of finite transcendence degree: the key is that, instead of using the prime subfield P of F, we fix a transcendence basis $B = \{b_1, \ldots, b_n\} \subset F$ and then use the subfield $P(b_1, \dots, b_n)$ in place of P. Of course we have a splitting algorithm over this field, just as over P, by Lemma 2.3. The catch is that in $\tilde{F}$ we cannot just arbitrarily choose a transcendence basis and extend $\tilde{P}$ by it, because such an arbitrary choice might not admit an extension to an isomorphism. (For instance, if $F = \tilde{F} = \mathbb{Q}(b_1)$, suppose we happened to choose $\{b_1^2\}$ as the transcendence basis for $\tilde{F}$.) Instead, knowing that there exists an isomorphism $\rho : F \to \tilde{F}$, we replace $\tilde{P}$ by $\tilde{P}(\rho(b_1), \dots, \rho(b_n))$ in the proofs of the results. Then eveything goes through with no trouble. However, we did allow ourselves the knowledge of the finite set $\rho(B)$, not to mention the knowledge of a transcendence basis B for F in the first place, and these things cannot in general be determined from the atomic diagram. Therefore, most uniformity in the constructions disappears when the transcendence degree becomes positive.

Of course, it is a bit hard to state the results of Section 5 as uniformity results anyway, since the isomorphisms produced may not be computable and hence need not be of the form φ_e to begin with. However, the construction of the tree $T_{F,\tilde{F}}$ in Theorem 5.2 is uniform in F and $\tilde{F}$, and the proof of the Low Basis Theorem from [19] provides a construction of the low path uniformly below a $\mathbf{0}'$-oracle (or, relativized to R, an R'-oracle), given an index for the computably bounded tree and an index for the computable bound itself. To get the computable bound, we need the root function for $\tilde{F}$, which can be computed from the root function (or from the root set R, or from the splitting set) for F, uniformly in the atomic diagrams of F and $\tilde{F}$, by Corollaries 2.7 and 2.8. So the whole construction gives an index for computing the low isomorphism from an R'-oracle, uniformly in the atomic diagrams of F and $\tilde{F}$. In the special case when R is computable, we can determine an index for computing the isomorphism below a $\emptyset'$-oracle, uniformly in the atomic diagrams of F and $\tilde{F}$ and the characteristic function of R.

Likewise, in Corollary 5.5, if we assume the given degree $\boldsymbol{d}$ to be $\geq_T \mathbf{0}'$, then that degree allows uniform computation below an oracle $D \in \boldsymbol{d}$ of an isomorphism between any isomorphic F and $\tilde{F}$, given only indices for the atomic diagrams of those fields. (The root set for F is $\exists$-definable, so it need not be given to us.) In 5.6, on the other hand, we require indices for the atomic diagrams and also for the root set of F; this root set is assumed to be computable, of course, but need not be quantifier-free definable (or otherwise uniformly computable) from the atomic diagram, so more information is needed to determine the isomorphism. In both of these corollaries, the uniformity is lost when we pass to the case of finite (positive) transcendence degree.

Uniform computable categoricity is studied closely in [4], which also defines a weaker version of our Definition 6.1 in which we compute the isomorphism from an index for the characteristic function of the atomic diagram, rather than using the atomic diagram itself as an oracle. Of course, since our fields satisfy the stronger version (in the foregoing formulations), they also satisfy the weaker version. In addition, [4] considers uniform computable categoricity with parameters, which is exactly the notion required for fields of finite transcendence degree: the uniformities described above for algebraic fields hold likewise for any computable field F of finite transcendence degree n after we augment the language by adding n constant symbols naming the elements of an (arbitrary) transcendence basis for F. Results from [36] and [1] show that all computable structures which are uniformly computably categorical with parameters are also relatively computably categorical (that is, every pair of isomorphic copies of the structure, both with domain ω, are isomorphic via a map computable from their Turing degrees), and it seems likely that some formulation of a kind of relative computable categoricity should be possible for fields of finite transcendence degree with splitting algorithms, and perhaps even for such fields in general. First one would need a relative version of Corollary 2.8; then the relativization would presumably involve not just the Turing degrees of the two isomorphic fields themselves, but also some (perhaps arbitrary) PA degrees relative to one or both of their root sets.

7 Characteristic p and Other Questions

Thus far we have focused on fields of characteristic 0. However, Lemma 2.3 and Corollaries 2.7 and 2.8 all hold in all characteristics. We believe, therefore, that with a few simple modifications, the results in Sections 3 and 5 hold for all computable algebraic extensions of $\mathbb{Z}_p$, for every prime $p > 0$, as well as for computable algebraic fields of characteristic 0. For instance, in Theorem 3.4, we could no longer use only square roots as the witness elements, for we need infinitely many witnesses. However, allowing q-th roots for distinct q ought to succeed, especially if these values q are themselves prime. Theorem 4.1 will require more work, from the researcher willing to tackle it, but we conjecture that fields algebraic over $\mathbb{Z}_p$ can also fail to be $\mathbf{0}'$-categorical.

Similarly, we believe that the comments in Section 6 also apply to separable fields of characteristic p with finite transcendence degree over $\mathbb{Z}_p$. The point here is that when the transcendence basis is adjoined to $\mathbb{Z}_p$, the result is an infinite field of characteristic p, and so Lemma 2.3 is not as easy for extensions of finite transcendence degree as it was for purely algebraic extensions of $\mathbb{Z}_p$. Indeed, in an inseparable finite algebraic extension of the field $\mathbb{Z}_p(b_1, \ldots, b_n)$, Kronecker's proof from [23] no longer applies. Lemma 2.3 does generalize as follows.

Lemma 7.1 *For every computable field F of any characteristic, with finite transcendence basis $\{b_1, \ldots, b_n\}$ over its prime subfield P, the splitting set for each finite* separable *extension of $P(b_i : i \in I)$ (with $I \subseteq \{1, \ldots, n\}$) by a finite tuple $\vec{x}$ is computable uniformly in I and in the finite tuple $\vec{x}$ of elements of F.*

The separability requirement, emphasized above, in no way weakens the original statement in characteristic 0, where all polynomials are separable, and allows Kronecker's algorithm to succeed even in characteristic p. Therefore, we believe that the results of Section 6 only need the added requirement of separability in order to hold in all characteristics. However, we leave the verification of these claims, as well as the investigation of the inseparable case, for another time.

Next one should ask to what extent our ideas here apply to other algebraic structures. In a theory T, such as the theory of fields, a complete 1-type $\Gamma(x)$ is *algebraic* if it is consistent with T, but no model of T realizes Γ infinitely many times. All such types are principal, and it follows from compactness that there must be some $n \in \omega$ such that T proves that at most n elements satisfy the generating formula, so that Γ cannot be realized by more than n elements in a single model. Fields are the archetype for these notions: the algebraic types are precisely those realized by algebraic elements, and a generating formula is just a statement $p(x) = 0$, for some polynomial p irreducible over the prime subfield.

In turn, a model of T is *algebraic* if it realizes only algebraic types. This cannot be stated in first-order language (unless there are only finitely many algebraic 1-types, in which case there is a finite bound on the size of algebraic models of T), but one can still ask about degrees of categoricity of such structures, just as we have done in this paper. What further requirements are necessary in order for our constructions in Section 5 to work for such a structure? For example, with fields we have an effective list of generators of all algebraic types, and without that list, the constructions would be much more daunting to attempt. We view this as a reasonable question for further investigation.

Finally, of course, the basic question remains open: which algebraic fields are computably categorical? As in the examples in Section 1, one hopes for a purely structural criterion. However, the results of Section 5 suggest that this problem may be at the level of difficulty of deciding whether a given Π^0_1-class contains a computable member. Actual bi-interpretability of these two problems is the subject of current study, but we view the results of this paper as evidence that the question of computable categoricity for fields, even with no transcendental elements present, is quantifiably a difficult problem.

References

[1] C.J. Ash, J.F. Knight, M.S. Manasse, & T.A. Slaman; Generic copies of countable structures, *Annals of Pure and Applied Logic* **42** (1989), 195-205.

[2] W. Calvert, V. Harizanov, & A. Shlapentokh; Turing degrees of the isomorphism types of algebraic objects, *Journal of London Mathematical Society* **73** (2007), 273-286.

[3] D. Cenzer; Π^0_1-classes in recursion theory, in *Handbook of Computability Theory*, ed. E.R. Griffor (Amsterdam: Elsevier, 1999) 37-85.

[4] R.G. Downey, D.R. Hirschfeldt, & B. Khoussainov; Uniformity in Computable Structure Theory, *Algebra and Logic* **42** (2003), 318-332.

[5] R.G. Downey & C.G. Jockusch, Jr.; Every low Boolean algebra is isomorphic to a recursive one, *Proceedings of the American Mathematical Society* **122** (1994), 871-880.

[6] H.M. Edwards; *Galois Theory* (New York: Springer-Verlag, 1984).

[7] Yu.L. Ershov; Theorie der Numerierungen, *Zeits. Math. Logik Grund. Math.* **23** (1977), 289-371.

[8] Y.L. Ershov & S.S. Goncharov, Constructive fields, Section 2.5 in *Constructive Models* (New York: Kluwer Academic/Plenum Press, 2000).

[9] E. Fokina, I. Kalimullin, & R.G. Miller; Degrees of categoricity of computable structures, to appear.

[10] M.D. Fried & M. Jarden, *Field Arithmetic* (Berlin: Springer-Verlag, 1986).

[11] A. Frohlich & J.C. Shepherdson; Effective procedures in field theory, *Phil. Trans. Royal Soc. London, Series A* **248** (1956) 950, 407-432.

[12] S.S. Goncharov; Autostability and computable families of constructivizations, *Algebra and Logic* **14** (1975), 647-680 (Russian), 392-409 (English translation).

[13] S.S. Goncharov; Nonequivalent constructivizations, *Proc. Math. Inst. Sib. Branch Acad. Sci.* (Novosibirsk: Nauka, 1982).

[14] S.S. Goncharov; Autostable models and algorithmic dimensions, *Handbook of Recursive Mathematics*, vol. 1 (Amsterdam: Elsevier, 1998), 261-287.

[15] S.S. Goncharov & V.D. Dzgoev; Autostability of models, *Algebra and Logic* **19** (1980), 45-58 (Russian), 28-37 (English translation).

[16] S.S. Goncharov, S. Lempp & R. Solomon; The computable dimension of ordered abelian groups, *Advances in Mathematics* **175** (2003) 1, 102-143.

[17] D.R. Hirschfeldt, B. Khoussainov, R.A. Shore, & A.M. Slinko; Degree spectra and computable dimensions in algebraic structures, *Annals of Pure and Applied Logic* **115** (2002), 71-113.

[18] N. Jacobson; *Basic Algebra I* (New York: W.H. Freeman & Co., 1985).

[19] C.G. Jockusch & R.I. Soare; Π^0_1-classes and degrees of theories, *Transactions of the American Mathematical Society* **173** (1972), 33-56.

[20] C.G. Jockusch & R.I. Soare; Degrees of orderings not isomorphic to recursive linear orderings, *Annals of Pure and Applied Logic* **52** (1991), 39-64.

[21] B. Khoussainov & R.A. Shore; Effective Model Theory: The Number of Models and their Complexity, *Models And Computability: Invited Papers from Logic Colloquium '97*, ed. S.B. Cooper & J.K. Truss, LMSLNS **259** (Cambridge: Cambridge University Press, 1999), 193-240.

[22] N. Kogabaev, O. Kudinov, & R.G. Miller; The computable dimension of I-trees of infinite height, *Algebra and Logic* **43** (2004) 6, 393-407.

[23] L. Kronecker; Grundzüge einer arithmetischen Theorie der algebraischen Größen, *J. f. Math.* **92** (1882), 1-122.

[24] S. Lempp, C. McCoy, R.G. Miller, & R. Solomon; Computable categoricity of trees of finite height, *Journal of Symbolic Logic* **70** (2005), 151-215.

[25] G. Metakides & A. Nerode; Effective content of field theory, *Annals of Mathematical Logic* **17** (1979), 289-320.

[26] R.G. Miller; The Δ_2^0-spectrum of a linear order, *Journal of Symbolic Logic* **66** (2001), 470-486.

[27] R.G. Miller; The computable dimension of trees of infinite height, *Journal of Symbolic Logic* **70** (2005), 111-141.

[28] R.G. Miller & H. Schoutens; Computably categorical fields via Fermat's Last Theorem, to appear.

[29] M. Rabin; Computable algebra, general theory, and theory of computable fields, *Transactions of the American Mathematical Society* **95** (1960), 341-360.

[30] J.B. Remmel; Recursively categorical linear orderings, *Proceedings of the American Mathematical Society* **83** (1981), 387-391.

[31] J.B. Remmel; Recursive isomorphism types of recursive Boolean algebras, *Journal of Symbolic Logic* **46** (1981), 572-594.

[32] L.J. Richter; Degrees of structures, *Journal of Symbolic Logic* **46** (1981), 723-731.

[33] R.I. Soare; *Recursively Enumerable Sets and Degrees* (New York: Springer-Verlag, 1987).

[34] V. Stoltenberg-Hansen & J.V. Tucker; Computable Rings and Fields, in *Handbook of Computability Theory*, ed. E.R. Griffor (Amsterdam: Elsevier, 1999), 363-447.

[35] B.L. van der Waerden; *Algebra*, volume I, trans. F. Blum & J.R. Schulenberger (New York: Springer-Verlag, 1970 hardcover, 2003 softcover).

[36] Y.G. Ventsov; Effective choice for relations and reducibilities in classes of constructive and positive models, *Algebra and Logic* **31** (1992), 63-73.

Department of Mathematics
Queens College – C.U.N.Y.
65-30 Kissena Blvd.
Flushing, New York 11367 U.S.A.
Ph.D. Programs in Computer Science & Mathematics
The Graduate Center of C.U.N.Y.
365 Fifth Avenue
New York, New York 10016 U.S.A.
E-mail: `Russell.Miller@qc.cuny.edu`