

**Tutorial:**  
**Computable Model Theory and**  
**Differential Algebra**

**Russell Miller,**  
**Queens College & Graduate Center**  
**C.U.N.Y.**

**April 12, 2007**

Workshop in Differential Algebra  
and Related Topics  
Rutgers University, Newark, NJ

## Computability Facts

Computability theory = recursion theory.

A function from  $\mathbb{N}$  to  $\mathbb{N}$  is *computable* if it is computed by some Turing machine ( $\equiv$  computer) using some finite program. This includes *partial functions*, whose domains may be proper subsets of  $\mathbb{N}$ .

So  $f(n) = m$  iff the computer, when given  $n$  as an input, *halts* within a finite number of steps and outputs  $m$ .

## **$k$ -ary Functions**

There exist computable bijections:

$$\pi_k : \mathbb{N}^k \rightarrow \mathbb{N}$$

$$\pi : (\cup_k \mathbb{N}^k) \rightarrow \mathbb{N}.$$

A  $k$ -ary (partial) computable function is a function of the form  $\varphi \circ \pi_k$ , for any unary (partial) computable  $\varphi$ .

We can list the partial computable functions as

$$\varphi_0, \varphi_1, \dots$$

so that there is a single partial computable binary function  $\varphi$  with

$$\varphi(e, n) = \varphi_e(n).$$

## Noncomputable Sets

A set is *computable* if its characteristic function is computable.

A set is *computably enumerable* (or *c.e.*) if it is empty or the range of a computable function whose domain is all of  $\mathbb{N}$ .

**Kleene-Post Theorem:** A set  $A \subseteq \mathbb{N}$  is computable iff both  $A$  and  $\overline{A}$  are c.e.

**Fact:** There exists a noncomputable c.e. set  $K$ , known as the *Halting Problem*.

## Computable Fields

**Defn.:** A *presentation* of a (countable) field  $F$  is a listing  $a_0, a_1, a_2, \dots$  of the elements of  $F$ . The presentation is *computable* if the functions  $f$  and  $g$  defined by addition and multiplication in  $F$ :

$$a_i + a_j = a_{f(i,j)} \quad a_i \cdot a_j = a_{g(i,j)}$$

are computable functions.

Then subtraction and division are also computable functions, and we can locate the identity elements of  $F$  on the list.

For differential fields, we would also require that each derivation  $\delta$  be given by a computable (unary) function  $h$ :

$$\delta(a_i) = a_{h(i)}.$$

Very little is known about computable differential fields!

## Early Examples

The rationals  $\mathbb{Q}$  form a computable field.

Enumerate them as follows:

$$\frac{0}{1}, \frac{1}{1}, -\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, -\frac{1}{2}, -\frac{2}{1}, \frac{1}{3}, \frac{3}{1}, \dots$$

So the numerator & denominator of  $a_i$  are computable from  $i$ , and conversely. Use this to define addition and multiplication.

Similar results for fields  $\mathbb{Q}(X)$ ,  $\mathbb{Q}(X_0, \dots, X_n)$ ,  $\mathbb{Q}(X_0, X_1, \dots)$ ,  $\mathbb{Q}(\sqrt{2})$ ,  $\mathbb{Q}(\sqrt{p_n} | n \geq 0)$ , etc.  
( $p_n$  = the  $n$ -th prime number.)

## Noncomputable Fields

Computability is not preserved under isomorphisms of fields! We must say that a particular *presentation* of a field  $F$  is computable, not that the isomorphism type of  $F$  is computable.

Example: There are uncountably many ways of enumerating the elements of  $\mathbb{Q}$ . Only countably many can have computable operations.

**Proposition:** All infinite fields have noncomputable presentations. No finite field does.

## Specific Examples

$F_{\overline{K}} = \mathbb{Q}(\sqrt{p_n} | n \notin K)$  has no computable presentation. If it did, we could use that presentation to enumerate  $\overline{K}$ .

$F_K = \mathbb{Q}(\sqrt{p_n} | n \in K)$  *does* have a computable presentation. However, it has no splitting algorithm!

**Defn.:**  $F$  has a *splitting algorithm* if the set

$$\{\pi(a_0, \dots, a_d) : \sum_i a_i X^i \text{ irreducible in } F[X]\}$$

is computable.

## Building $F_K$

- Start building  $\mathbb{Q}$  with addition and multiplication, as previously presented, one step at a time. (Assume  $a_1$  is the unit.)
- As we build, enumerate  $K$  (computably).
- When some  $n$  appears in  $K$ , we will have put elements  $\{a_0, \dots, a_m\}$  into  $F_K$  already. Let the next element  $a_{m+1}$  have

$$a_{m+1} \cdot a_{m+1} = a_1 + a_1 + \dots + a_1 \quad (p_n \text{ times}).$$

Continue building  $F_K$ , treating  $a_{m+1}$  as  $\sqrt{p_n}$ .

So  $n \in K \iff (X^2 - p_n)$  splits.

## Transcendence Bases

A transcendence basis  $B$  (for a computable field  $F = \{a_0, a_1, \dots\}$ , over its prime field, say  $\mathbb{Q}$ ) is *computable* if  $\{n : a_n \in B\}$  is computable.

Is this possible? Let  $B$  contain all  $a_n$  such that, for all  $p \in \mathbb{Q}[X_0, \dots, X_n]$

$$p(a_0, \dots, a_n) = 0 \Rightarrow \deg(p(a_0, \dots, a_{n-1}, X_n)) = 0.$$

Then  $\overline{B}$  is c.e., but  $B$  might not be.

## No Computable Transcendence Basis

**Proposition:** There exists a computable field with no computable transcendence basis.

Sketch: Start building  $F = \mathbb{Q}(X_0, X_1, \dots)$ . If an element  $j$  enters the c.e. set  $W_e$ , and  $a_j$  appears so far to be transcendental over  $\mathbb{Q}(X_0, \dots, X_{2e})$  then make  $a_j$  satisfy some algebraic relation  $R$  over  $\mathbb{Q}$ . By choosing  $R$  to involve large numbers, we can respect all operations defined so far.

(So here  $X_i$  might turn out to be algebraic!)

## Why This Works

$\mathbb{Q}(X_0, \dots, X_{2e})$  has transcendence degree  $> e$  over  $\mathbb{Q}$ , for every  $e$ . So  $F$  has infinite tr. deg.

Possibilities for  $W_e$ :

- $W_e$  is finite.
- $W_e \subseteq \mathbb{Q}(X_0, \dots, X_{2e})$ .
- $W_e$  includes a  $j$  as above, and we made  $a_j$  algebraic over  $\mathbb{Q}$ .

So no  $W_e$  can be a transcendence basis.

## Algebraic Closure

**Proposition:** Every countable algebraically closed field has a computable presentation.

Proof uses: (Kronecker, van der Waerden)

- $\mathbb{Q}$  has a splitting algorithm.
- If  $F$  has a splitting algorithm, so does  $F(X)$ .
- If  $F$  has a splitting algorithm and we know the minimal polynomial of  $\alpha$  over  $F$ , then so does  $F(\alpha)$ .

Use these to build the algebraic closure around  $\mathbb{Q}(X_i | i \in I)$ , for  $I$  finite or  $\mathbb{N}$ .

**But wait...**

So the computable field  $F_K$  has a computable algebraic closure  $E(\cong \overline{\mathbb{Q}})$ . But then why can't we have a splitting algorithm for  $F_K$ ?

In fact,  $F_{\overline{K}}$  has a computable algebraic closure, despite not being computably presentable!

Clearly  $F_{\overline{K}}$  cannot be a computable subset, or even a c.e. subset, of any computable presentation of  $\overline{\mathbb{Q}}$ .

## Rabin's Theorem

**Thm.** (Rabin, 1960):

1. For every computable field  $F$ , there exists a computable field embedding  $\psi$  and a computable algebraically closed field  $E$  such that  $\psi : F \rightarrow E$  and  $E$  is algebraic over  $\psi(F)$ . (Hence  $F$  embeds as a c.e. subset of its computable algebraic closure.)
2. For any  $F$ ,  $E$ , and  $\psi$  as above,  $\psi(F)$  is a computable subset of  $E$  iff  $F$  has a splitting algorithm.

No known analogue for differential fields!

## Rabin Proof

Part 1. Hard! Even uses some elimination theory, building a computable ring  $R = F[x_0, x_1, \dots]$  and a maximal proper ideal  $U$ , computable as a subset of  $R$ , such that  $R/U$  is the algebraic closure of (the image of)  $F$ .

$\psi(F)$  computable  $\implies$  splitting algorithm for  $F$ :  
Given  $p \in F[X]$ , we can split  $(\psi \circ p)(X)$  into linear factors in  $E$ . Ask whether any proper product of these factors has all its coefficients in the computable set  $\psi(F)$ .

## Rabin Proof II

Splitting algorithm for  $F \implies \psi(F)$  computable:  
Fix  $y \in E$ .

- Since  $\psi(F)$  is c.e., we can find a  $q \in (\psi(F))[X]$  s.t.  $q(y) = 0$ . Pull  $q$  back to  $p \in F[X]$ , and check whether  $p$  is reducible there. ( $F$  has a splitting algorithm!)
- If so, find a proper factor of  $q$  in  $(\psi(F))[X]$  with root  $y$ . Repeat until we find the minimal polynomial of  $y$ .
- If  $q$  is of degree 1, then  $y \in \psi(F)$ .
- Else  $y \notin \psi(F)$ .

So the splitting algorithm for  $F$  lets us compute  $\psi(F)$  inside  $E$ .

## Uncountable Fields

Some notions exist for computable functions  $F$  on  $\mathbb{R}$ .

- Bitmap model: use the binary expansion of  $r \in \mathbb{R}$  as an *oracle* to compute bits of the binary expansion of  $F(r)$ . Works for countable sequences of bits (or naturals) only.
- Blum-Shub-Smale model: assume that addition and multiplication on  $\mathbb{R}$  are computable. Defines certain other functions to be computable as well.
- Models of infinite-time computability: Hamkins, Koepke, Lewis, etc.

## Local Computability

**Defn.(M.):** A field  $F$  has a *computable simple cover* if every finitely generated subfield of  $F$  has a computable presentation.

(This rules out nothing!)

**Defn:** A *uniformly computable simple cover* of  $F$  is a computably presented list of all finitely generated subfields of  $F$ , up to isomorphism, ignoring multiplicity, allowing repetitions:

$$\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2, \dots$$

with every  $\mathcal{A}_i$  a computable field, uniformly in  $i$ .

## Fitting the Pieces Together

**Defn.:** A uniformly computable cover  $\mathfrak{A}$  of  $F$  consists of a u.c. simple cover  $\{\mathcal{A}_0, \mathcal{A}_1, \dots\}$ , along with computably presented sets  $I_{ij}^{\mathfrak{A}}$  of embeddings  $\mathcal{A}_i \hookrightarrow \mathcal{A}_j$ , such that every  $f \in I_{ij}^{\mathfrak{A}}$  lifts to an inclusion in  $F$ , and every inclusion  $\mathcal{B} \subseteq \mathcal{C}$  is the lift of an  $f$  in some  $I_{ij}^{\mathfrak{A}}$ :

$$\begin{array}{ccc}
 \mathcal{B} & \xrightarrow{\subseteq} & \mathcal{C} \\
 \beta \uparrow \cong & & \gamma \uparrow \cong \\
 \mathcal{A}_i & \xrightarrow{f} & \mathcal{A}_j
 \end{array}$$

with  $\gamma \circ f = \beta$ .

Both  $\mathbb{C}$  and  $\mathbb{R}$  have uniformly computable covers.

## Correspondence Systems

**Defn.:** If  $\mathfrak{A} = \{\mathcal{A}_0, \mathcal{A}_1, \dots\}$  is a uniformly computable cover of  $F$ , a *correspondence system*  $M$  is a set of isomorphisms  $\beta : \mathcal{A}_i \hookrightarrow \mathcal{B}$  identifying various  $\mathcal{A}_i \in \mathfrak{A}$  with various subfields  $\mathcal{B} \subseteq F$  in a very strong way:

- $(\forall j \forall f \in I_{ij}^{\mathfrak{A}})(\exists \gamma \in M)$  [ $f$  lifts to the inclusion  $\mathcal{B} \subseteq \mathcal{C} = \gamma(\mathcal{A}_j)$  via  $\beta$  and  $\gamma$ ].
- $(\forall \mathcal{C} \supseteq \mathcal{B})(\exists \gamma \in M \exists j \exists f \in I_{ij}^{\mathfrak{A}})$  [ $f$  lifts to the inclusion  $\mathcal{B} \subseteq \mathcal{C} = \gamma(\mathcal{A}_j)$  via  $\beta$  and  $\gamma$ ].

$$\begin{array}{ccc}
 \mathcal{B} & \xrightarrow{\subseteq} & \mathcal{C} \\
 \beta \uparrow \cong & & \gamma \uparrow \cong \\
 \mathcal{A}_i & \xrightarrow{f} & \mathcal{A}_j
 \end{array}$$

$\mathbb{C}$  has a u.c. cover with a correspondence system;  
 $\mathbb{R}$  does not!

## Advantages

Existential questions about  $F$ , even over parameters, reduce to existential questions about the cover  $\mathfrak{A}$ , which is computably presented. So we can ask about the possibility of algorithms for  $F$ , using  $\mathfrak{A}$  as a “presentation” of  $F$ .

To do this uniformly over different parameter sets, we adopt the convention of “naming” a parameter  $p \in F$  by giving its representation  $\alpha^{-1}(p)$  in some  $\mathcal{A}_i$ , under some  $\alpha$  in the correspondence system, with  $\text{dom}(\alpha) = \mathcal{A}_i$ .

Example: is there an algorithm which accepts  $(a_0 \in \mathcal{A}_{i_0}, \dots, a_d \in \mathcal{A}_{i_d})$  as input, and decides whether the corresponding

$$\beta_0(a_0) + \beta_1(a_1) \cdot X + \dots + \beta_d(a_d) \cdot X^d$$

is irreducible in  $F$ ?

## New Theorems

**Thm.:** Suppose  $F$  has a uniformly computable cover and a correspondence system. Then the  $\Sigma_n$ -theory of  $F$  over parameters  $p_0, \dots, p_m \in F$  is arithmetically a  $\Sigma_n$  set.

(A  $\Sigma_n$ -formula  $\varphi$  is of the form

$$(\exists x_n \forall x_{n-1} \exists x_{n-1} \cdots x_0) \theta(x_0, \dots, x_n, p_0, \dots, p_m).$$

The  $\Sigma_n$ -theory contains those  $\varphi$  true in  $F$ .)

**Thm.:** A countable structure  $F$  is computably presentable iff  $F$  is perfectly locally computable ( $\equiv F$  is u.l.c. and has a correspondence system with one additional property).

## Computable Simulations

**Thm.** (M.-Mulcahey): Every perfectly locally computable field  $F$  has a *computable simulation*  $\mathcal{B}$ , i.e. a computably presentable elementary subfield which realizes the same finitary types as  $\mathcal{S}$ .

Indeed, given any countable parameter set  $P \subseteq F$ ,  $\mathcal{B}$  is isomorphic to an elementary subfield  $\mathcal{B}_P \preceq F$  with  $P \subseteq \mathcal{B}_P$ , such that  $\mathcal{B}_P$  and  $F$  realize the same types over each finite  $P_0 \subseteq P$ .

The same holds for other types of structures, including differential fields.

## References

V.S. Harizanov, Pure Computable Model Theory, *Handbook of Recursive Mathematics*, vol. 1 (Amsterdam: Elsevier, 1998), 3-114.

L. Harrington, Recursively Presentable Prime Models, *Journal of Symbolic Logic* **2** (1974), 305-309.

R. Miller, Locally Computable Structures, to appear in *Computation and Logic in the Real World - Third Conference of Computability in Europe, CiE 2007*, Springer-Verlag LNCS 4497, ed. B. Cooper, B. Löwe, & A. Sorbi.

M.O. Rabin, Computable Algebra, General Theory, and Theory of Computable Fields, *Transactions of the A.M.S.* **95** (1960), 341-360.