Computable Fields and their Algebraic Closures

Russell Miller

Queens College & CUNY Graduate Center
New York, NY.

Workshop on Computability Theory
Universidade dos Açores
Ponta Delgada, Portugal, 6 July 2010

Slides available at
qc.edu/~rmiller/slides.html

Classical Algebraic Closures

Theorem

Every field F has an algebraic closure $\overline{F}$: a field extension of F which is algebraically closed and algebraic over F. This *algebraic closure* of F is unique up to F-isomorphism.

Classical Algebraic Closures

Theorem

Every field F has an algebraic closure $\overline{F}$: a field extension of F which is algebraically closed and algebraic over F. This *algebraic closure* of F is unique up to F-isomorphism.

The theory Th(ACF$_m$) of algebraically closed fields of characteristic m is κ-categorical for every uncountable κ, and has countable models

$$\overline{\mathbb{F}_m} \prec \overline{\mathbb{F}_m(X_0)} \prec \overline{\mathbb{F}_m(X_0, X_1)} \prec \cdots \prec \overline{\mathbb{F}_m(X_0, X_1, X_2, \ldots)}.$$

So ACF's of characteristic m are indexed by their transcendence degrees. (Here $\mathbb{F}_0 = \mathbb{Q}$ and $\mathbb{F}_p = \mathbb{Z}/(p\mathbb{Z})$ for prime p.)

Classical Algebraic Closures

Theorem

Every field F has an algebraic closure $\overline{F}$: a field extension of F which is algebraically closed and algebraic over F. This *algebraic closure* of F is unique up to F-isomorphism.

The theory $\mathrm{Th}(\mathrm{ACF}_m)$ of algebraically closed fields of characteristic m is κ-categorical for every uncountable κ, and has countable models

$$\overline{\mathbb{F}_m} \prec \overline{\mathbb{F}_m(X_0)} \prec \overline{\mathbb{F}_m(X_0, X_1)} \prec \cdots \prec \overline{\mathbb{F}_m(X_0, X_1, X_2, \ldots)}.$$

So ACF's of characteristic m are indexed by their transcendence degrees. (Here $\mathbb{F}_0 = \mathbb{Q}$ and $\mathbb{F}_p = \mathbb{Z}/(p\mathbb{Z})$ for prime p.)

Fact

All countable ACF's are computably presentable.

Splitting Algorithms

Theorem (Kronecker, 1882)

- The field $\mathbb{Q}$ has a splitting algorithm: it is decidable which polynomials in $\mathbb{Q}[X]$ have factorizations in $\mathbb{Q}[X]$.
- Let F be a computable field of characteristic 0 with a splitting algorithm. Every primitive extension $F(x)$ of F also has a splitting algorithm, which may be found uniformly in the minimal polynomial of x over F (or uniformly knowing that x is transcendental over F).

Recall that for $x \in E$ algebraic over F, the *minimal polynomial* of x over F is the unique monic irreducible $p(X) \in F[X]$ with $p(x) = 0$.

Splitting Algorithms

Theorem (Kronecker, 1882)

- The field $\mathbb{Q}$ has a splitting algorithm: it is decidable which polynomials in $\mathbb{Q}[X]$ have factorizations in $\mathbb{Q}[X]$.
- Let F be a computable field of characteristic 0 with a splitting algorithm. Every primitive extension $F(x)$ of F also has a splitting algorithm, which may be found uniformly in the minimal polynomial of x over F (or uniformly knowing that x is transcendental over F).

Recall that for $x \in E$ algebraic over F, the *minimal polynomial* of x over F is the unique monic irreducible $p(X) \in F[X]$ with $p(x) = 0$.

Corollary

For any algebraic computable field F, every finitely generated subfield $\mathbb{Q}(x_1, \ldots, x_n)$ or $\mathbb{F}_p(x_1, \ldots, x_n)$ has a splitting algorithm, uniformly in the tuple $\langle x_1, \ldots, x_d \rangle$.

Computable Algebraic Closures

We want a presentation of $\overline{F}$ with F as a recognizable subfield.

Defn.

For a computable field F, a *Rabin embedding* of F consists of a computable field E and a field homomorphism $g : F \to E$ such that:

- E is algebraically closed;
- E is algebraic over the image $g(F)$; and
- g is a computable function.

Computable Algebraic Closures

We want a presentation of $\overline{F}$ with F as a recognizable subfield.

Defn.

For a computable field F, a *Rabin embedding* of F consists of a computable field E and a field homomorphism $g : F \to E$ such that:

- E is algebraically closed;
- E is algebraic over the image $g(F)$; and
- g is a computable function.

Rabin's Theorem (1960); see also Frohlich & Shepherdson (1956)

Every computable field F has a Rabin embedding. Moreover, for every Rabin embedding $g : F \to E$, the following are Turing-equivalent:

- the image $g(F)$, as a subset of E;
- the *splitting set* $S_F = \{p \in F[X] : p \text{ factors nontrivially in } F[X]\}$;
- the *root set* $R_F = \{p \in F[X] : p \text{ has a root in } F\}$.

Proof of Rabin's Theorem

$R_F \leq_T S_F$

Given $p(X)$, an S_F-oracle allows us to find the irreducible factors of p in $F[X]$. But $p \in R_F$ iff p has a linear factor.

Proof of Rabin's Theorem

$R_F \leq_T S_F$

Given $p(X)$, an S_F-oracle allows us to find the irreducible factors of p in $F[X]$. But $p \in R_F$ iff p has a linear factor.

$S_F \leq_T g(F)$

Given a monic $p(X) \in F[X]$, find all its roots $r_1, \ldots, r_d \in E$. Factorizations of its image p^g in $E[X]$ are all of the form

$$p^g(X) = h(X) \cdot j(X) = (\Pi_{i \in S}(X - r_i)) \cdot (\Pi_{i \notin S}(X - r_i))$$

for some $S \subsetneq \{1, \ldots, d\}$. Check if any of these factors lies in $g(F)[X]$.

Proof of Rabin's Theorem

$R_F \leq_T S_F$

Given $p(X)$, an S_F-oracle allows us to find the irreducible factors of p in $F[X]$. But $p \in R_F$ iff p has a linear factor.

$S_F \leq_T g(F)$

Given a monic $p(X) \in F[X]$, find all its roots $r_1, \ldots, r_d \in E$. Factorizations of its image p^g in $E[X]$ are all of the form

$$p^g(X) = h(X) \cdot j(X) = (\Pi_{i \in S}(X - r_i)) \cdot (\Pi_{i \notin S}(X - r_i))$$

for some $S \subsetneq \{1, \ldots, d\}$. Check if any of these factors lies in $g(F)[X]$.

$g(F) \leq_T R_F$

Given $x \in E$, find some $p(X) \in F[X]$ for which $p^g(x) = 0$. Find all roots of p in F: if $p \in R_F$, find a root $r_1 \in F$, then check if $\frac{p(X)}{X - r_1} \in R_F$, etc. Then $x \in g(F)$ iff x is the image of one of these roots.

Different Presentations of F

Theorem

Let $F \cong \tilde{F}$ be two computable presentations of the same field. Assume that F is *algebraic* (over its prime subfield $\mathbb{Q}$ or $\mathbb{F}_p$). Then $R_F \equiv_T R_{\tilde{F}}$.

Proof: Given $p(X) \in F[X]$, find $q(X) \in \mathbb{F}_m[X]$ divisible by $p(X)$. Use $R_{\tilde{F}}$ to find all roots of $h(q)(X)$ in $\tilde{F}$. Then find the same number of roots of $q(X)$ in F, and check whether any one is a root of $p(X)$.

$$\begin{array}{cccc} & F & \cong & \tilde{F} \\ & \cup\!| & & \cup\!| \\ h: & \mathbb{F}_m & \to & \tilde{\mathbb{F}}_m \end{array}$$

Comparing R_F, S_F, and $g(F)$

We know that $R_F \equiv_T S_F \equiv_T g(F)$. Is there any way to distinguish the complexity of these sets?

Comparing R_F, S_F, and $g(F)$

We know that $R_F \equiv_T S_F \equiv_T g(F)$. Is there any way to distinguish the complexity of these sets?

Recall: $A \leq_1 B$ if there is a 1-1 computable f such that:

$$(\forall x)[x \in A \iff f(x) \in B].$$

$A \leq_{\text{wtt}} B$ if there are Φ_e and a computable bound g with:

$$(\forall x)\Phi_e^{B \upharpoonright g(x)}(x) \downarrow = \chi_A(x).$$

Comparing R_F, S_F, and $g(F)$

We know that $R_F \equiv_T S_F \equiv_T g(F)$. Is there any way to distinguish the complexity of these sets?

Recall: $A \leq_1 B$ if there is a 1-1 computable f such that:

$$(\forall x)[x \in A \iff f(x) \in B].$$

$A \leq_{\text{wtt}} B$ if there are Φ_e and a computable bound g with:

$$(\forall x)\Phi_e^{B \restriction g(x)}(x) \downarrow = \chi_A(x).$$

Theorem (M, 2010)

For all algebraic computable fields F, $S_F \leq_1 R_F$. However, there exists such a field F with $R_F \not\leq_1 S_F$.

Problem: Given a polynomial $p(X) \in F[X]$, compute another polynomial $q(X) \in F[X]$ such that

$$p(X) \text{ splits} \iff q(X) \text{ has a root}.$$

$p(X)$ splits $\iff$ $q(X)$ has a root.

Let F_t be the subfield $\mathbb{F}_m[a_0, \ldots, a_{t-1}]$. So every F_t has a splitting algorithm.

For a given $p(X)$, find an t with $p \in F_t[X]$. Check first whether p splits there. If so, pick its $q(X)$ to be a linear polynomial. If not, find the splitting field K_t of $p(X)$ over F_t, and the roots $r_1, \ldots, r_d$ of $p(X)$ in K_t.

$p(X)$ splits $\iff$ $q(X)$ has a root.

Let F_t be the subfield $\mathbb{F}_m[a_0, \ldots, a_{t-1}]$. So every F_t has a splitting algorithm.

For a given $p(X)$, find an t with $p \in F_t[X]$. Check first whether p splits there. If so, pick its $q(X)$ to be a linear polynomial. If not, find the splitting field K_t of $p(X)$ over F_t, and the roots $r_1, \ldots, r_d$ of $p(X)$ in K_t.

Proposition

For $F_t \subseteq L \subseteq K_t$, $p(X)$ splits in $L[X]$ iff there exists $\emptyset \subsetneq S \subsetneq \{r_1, \ldots, r_d\}$ such that L contains all elementary symmetric polynomials in S.

$p(X)$ splits $\iff$ $q(X)$ has a root.

Let F_t be the subfield $\mathbb{F}_m[a_0, \ldots, a_{t-1}]$. So every F_t has a splitting algorithm.

For a given $p(X)$, find an t with $p \in F_t[X]$. Check first whether p splits there. If so, pick its $q(X)$ to be a linear polynomial. If not, find the splitting field K_t of $p(X)$ over F_t, and the roots $r_1, \ldots, r_d$ of $p(X)$ in K_t.

Proposition

For $F_t \subseteq L \subseteq K_t$, $p(X)$ splits in $L[X]$ iff there exists $\emptyset \subsetneq S \subsetneq \{r_1, \ldots, r_d\}$ such that L contains all elementary symmetric polynomials in S.

Effective Theorem of the Primitive Element

Each finite algebraic field extension is generated by a single element, which we can find effectively.

Procedure to Compute $q(X)$

For each intermediate field $F_t \subsetneq L_S \subsetneq K_t$ generated by the elementary symmetric polynomials in S, let x_S be a primitive generator. Let $q(X)$ be the product of the minimal polynomials $q_S(X) \in F_t[X]$ of each x_S.

Procedure to Compute $q(X)$

For each intermediate field $F_t \subsetneq L_S \subsetneq K_t$ generated by the elementary symmetric polynomials in S, let x_S be a primitive generator. Let $q(X)$ be the product of the minimal polynomials $q_S(X) \in F_t[X]$ of each x_S.

$\Rightarrow$: If $p(X)$ splits in $F[X]$, then F contains some L_S. But then $x_S \in F$, and $q_S(x_S) = 0$.

Procedure to Compute $q(X)$

For each intermediate field $F_t \subsetneq L_S \subsetneq K_t$ generated by the elementary symmetric polynomials in S, let x_S be a primitive generator. Let $q(X)$ be the product of the minimal polynomials $q_S(X) \in F_t[X]$ of each x_S.

$\Rightarrow$: If $p(X)$ splits in $F[X]$, then F contains some L_S. But then $x_S \in F$, and $q_S(x_S) = 0$.

$\Leftarrow$: If $q(X)$ has a root $x \in F$, then some $q_S(x) = 0$, so x is F_t-conjugate to some x_S. Then some $\sigma \in \mathrm{Gal}(K_t/F_t)$ maps x_S to x. But σ permutes the set $\{r_1, \ldots, r_d\}$, so x generates the subfield containing all elementary symmetric polynomials in $\sigma(S)$. Then F contains the subfield $L_{\sigma(S)}$, so $p(X)$ splits in $F[X]$.

Thus $S_F \leq_1 R_F$.

No Reverse Reduction

Theorem (Steiner, 2010)

There exists a computable algebraic field F with $R_F \not\leq_{\text{wtt}} S_F$.

No Reverse Reduction

Theorem (Steiner, 2010)

There exists a computable algebraic field F with $R_F \not\leq_{\mathrm{wtt}} S_F$.

Proof uses the following distinction between R_F and S_F:

Facts

For every Galois extension $L \supseteq \mathbb{Q}$ and all intermediate fields F_0 and F_1:

$$R_{F_0} \cap \mathbb{Q}[X] = R_{F_1} \cap \mathbb{Q}[X] \quad \iff \quad \exists \sigma \in \mathrm{Gal}(L/\mathbb{Q})[\sigma(F_0) = F_1].$$

But there exist such $L \supseteq F_1 \supsetneq F_0 \supseteq \mathbb{Q}$ for which

$$S_{F_0} \cap \mathbb{Q}[X] = S_{F_1} \cap \mathbb{Q}[X].$$

What about the Rabin Image $g(F)$?

Theorem (Steiner 2010)

Among the reducibilities $\leq_T$, $\leq_{\text{wtt}}$, $\leq_m$, and $\leq_1$, the following are the strongest which hold for all computable algebraic fields F:

$$\begin{array}{ccc} S_F \leq_1 R_F & S_F \leq_{\text{wtt}} g(F) & R_F \leq_{\text{wtt}} g(F) \\ R_F \leq_T S_F & g(F) \leq_T S_F & g(F) \leq_{\text{wtt}} R_F \end{array}$$

So S_F is, relatively, the easiest to compute. R_F and $g(F)$ appear the same – except that we have a field F with $S_F \leq_1 R_F$ and $S_F \not\leq_1 g(F)$. So R_F is stronger, in a subtle way.

What about the Rabin Image $g(F)$?

Theorem (Steiner 2010)

Among the reducibilities $\leq_T$, $\leq_{\text{wtt}}$, $\leq_m$, and $\leq_1$, the following are the strongest which hold for all computable algebraic fields F:

$$\begin{array}{ccc} S_F \leq_1 R_F & S_F \leq_{\text{wtt}} g(F) & R_F \leq_{\text{wtt}} g(F) \\ R_F \leq_T S_F & g(F) \leq_T S_F & g(F) \leq_{\text{wtt}} R_F \end{array}$$

So S_F is, relatively, the easiest to compute. R_F and $g(F)$ appear the same – except that we have a field F with $S_F \leq_1 R_F$ and $S_F \not\leq_1 g(F)$. So R_F is stronger, in a subtle way.

Remaining work: for isomorphic computable algebraic fields $F \cong \tilde{F}$, how do these sets compare?

Noncomputable Algebraic Fields

Now let F be any field algebraic over $\mathbb{Q}$ (or over $\mathbb{F}_p$), but not necessarily computable. We wish to consider the *spectrum* of F:

$$\text{Spec}(F) = \{\text{T-degrees } \boldsymbol{d} : \exists K \cong F[\deg(K) = \boldsymbol{d}]\}.$$

Problem: Describe Spec(F).

Noncomputable Algebraic Fields

Now let F be any field algebraic over $\mathbb{Q}$ (or over $\mathbb{F}_p$), but not necessarily computable. We wish to consider the *spectrum* of F:

$$\text{Spec}(F) = \{\text{T-degrees } \boldsymbol{d} : \exists K \cong F[\deg(K) = \boldsymbol{d}]\}.$$

Problem: Describe Spec(F).
Now if $K \cong F$ and $\deg(K) = \boldsymbol{d}$, then $\boldsymbol{d}$ can enumerate $\mathbb{Q}_K \subseteq K$.
Moreover, $\boldsymbol{d}$ can compute the (unique) isomorphism from $\mathbb{Q}_F$ onto a fixed computable copy of $\mathbb{Q}$.
Moreover, every $x \in K$ has a minimal polynomial over $\mathbb{Q}$, and $\boldsymbol{d}$ can find it. (Kronecker!) Thus $\boldsymbol{d}$ can enumerate $(\mathbb{Q}[X] \cap R_F)$.

Noncomputable Algebraic Fields

Now let F be any field algebraic over $\mathbb{Q}$ (or over $\mathbb{F}_p$), but not necessarily computable. We wish to consider the *spectrum* of F:

$$\text{Spec}(F) = \{\text{T-degrees } \boldsymbol{d} : \exists K \cong F[\deg(K) = \boldsymbol{d}]\}.$$

Problem: Describe Spec(F).
Now if $K \cong F$ and $\deg(K) = \boldsymbol{d}$, then $\boldsymbol{d}$ can enumerate $\mathbb{Q}_K \subseteq K$.
Moreover, $\boldsymbol{d}$ can compute the (unique) isomorphism from $\mathbb{Q}_F$ onto a fixed computable copy of $\mathbb{Q}$.
Moreover, every $x \in K$ has a minimal polynomial over $\mathbb{Q}$, and $\boldsymbol{d}$ can find it. (Kronecker!) Thus $\boldsymbol{d}$ can enumerate $(\mathbb{Q}[X] \cap R_F)$.

Theorem (Frolov, Kalimullin, & M 2009)

For any algebraic field extension $F \supseteq \mathbb{Q}$,

$$\text{Spec}(F) = \{\boldsymbol{d} : \boldsymbol{d} \text{ can enumerate } \mathbb{Q}[X] \cap R_F\}.$$

Useful Field Fact

The proof of the inclusion $\supseteq$ uses:

Fact

For algebraic fields F and K, the following are equivalent:

- $F \cong K$.
- $F \hookrightarrow K$ and $K \hookrightarrow F$.
- Every f.g. subfield of each field embeds into the other field.

Let $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots = K$, and $f_s : K_s \to F$. By algebraicity, there are only finitely many possible embeddings of each K_s into F. So let $g_0 = f_0$ and g_s be any extension of g_{s-1} such that

$$\exists^\infty t \geq s[\, f_t \restriction K_s = g_s \,].$$

This is noneffective, but then $g = \cup_s g_s$ embeds K into F.

And for Algebraic Closures...

Now let $\overline{F}$ be a computable copy of the algebraic closure of the algebraic field F. We have another notion of the spectrum:

$$\mathrm{DgSp}_{\overline{F}}(F) = \{\deg(g(F)) : g : \overline{F} \to E \text{ is an isomorphism } \& \ E \leq_T \emptyset\}.$$

Problem: Describe $\mathrm{DgSp}_{\overline{F}}(F)$.

And for Algebraic Closures...

Now let $\overline{F}$ be a computable copy of the algebraic closure of the algebraic field F. We have another notion of the spectrum:

$$\mathrm{DgSp}_{\overline{F}}(F) = \{\deg(g(F)) : g : \overline{F} \to E \text{ is an isomorphism } \& \ E \leq_T \emptyset\}.$$

Problem: Describe $\mathrm{DgSp}_{\overline{F}}(F)$.

Theorem (Frolov, Kalimullin, & M 2009)

For any algebraic field extension $F \supseteq \mathbb{Q}$, either

$$\mathrm{DgSp}_{\overline{F}}(F) = \{\ \deg(\mathbb{Q}[X] \cap R_F)\ \}$$

or

$$\mathrm{DgSp}_{\overline{F}}(F) = \{\boldsymbol{d} : \boldsymbol{d} \text{ can compute } \mathbb{Q}[X] \cap R_F\}.$$

So we have a contrast. For F as a field, the spectrum was really an upper cone of e-degrees. For F as a relation on $\overline{F}$, the spectrum is an upper cone of Turing degrees.

Galois Groups

Bad news: the automorphism group of a countable algebraic field can be uncountable! (E.g. Aut($\overline{\mathbb{Q}}$) has size 2^ω.) So there is no hope that the Galois group of a computable field extension might always be computably presentable.

Galois Groups

Bad news: the automorphism group of a countable algebraic field can be uncountable! (E.g. $\text{Aut}(\overline{\mathbb{Q}})$ has size 2^ω.) So there is no hope that the Galois group of a computable field extension might always be computably presentable.

Idea: name elements $\sigma \in \text{Aut}(F)$ the way computable analysts name real numbers: by giving approximations $\sigma_n = \sigma\restriction\{0, 1, \ldots, n\}$. From such approximations to any $\sigma, \tau \in \text{Aut}(F)$, we can likewise approximate $(\tau \circ \sigma)$.

Galois Actions

So, to give an effective presentation of Aut(F) in this manner, we need to be able to compute (or at least enumerate) the set

$$A_F = \{\langle a_0, \ldots, a_n : b_0, \ldots, b_n \rangle : (\exists \sigma \in \mathrm{Aut}(F))(\forall i)\ \sigma(a_i) = b_i\}.$$

This is the *full Galois action* of F. Equivalently, we need to compute or enumerate the orbit relation (or *Galois action*) on F:

$$B_F = \{\langle a, b \rangle : \exists \sigma \in \mathrm{Aut}(F)\ \sigma(a) = b\}.$$

The Galois action has recently proven useful in attempts (with Shlapentokh) to characterize computable categoricity for computable algebraic fields.

Standard References on Computable Fields

- Yu.L. Ershov; Theorie der Numerierungen III, *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik* **23** (1977) 4, 289-371.
- A. Frohlich & J.C. Shepherdson; Effective procedures in field theory, *Phil. Trans. Royal Soc. London, Series A* **248** (1956) 950, 407-432.
- G. Metakides & A. Nerode; Effective content of field theory, *Annals of Mathematical Logic* **17** (1979), 289-320.
- M. Rabin; Computable algebra, general theory, and theory of computable fields, *Transactions of the American Mathematical Society* **95** (1960), 341-360.
- V. Stoltenberg-Hansen & J.V. Tucker; Computable rings and fields, in *Handbook of Computability Theory*, ed. E.R. Griffor (Amsterdam: Elsevier, 1999), 363-447.

- These slides available at `qc.edu/~rmiller/slides.html`