Extending automorphisms of normal algebraic fields

Matthew Harrison-Trainor

University of California, Berkeley

AMS Sectional Meeting, Charleston, SC, March 2017
This is joint work with Russell Miller and Alexander Melnikov.

I will be talking about the effective versions of the following facts about fields:

- Every embedding of a field $F$ into an algebraically closed field $K$ extends to an embedding of $\overline{F}$ into $K$.
- Every automorphism of a field $F$ extends to an automorphism of $\overline{F}$.

First we will review some effective field theory.
Let $F$ be a computable field.

**Definition**

The *splitting set* $S_F$ of $F$ is the set of all polynomials $p \in F[X]$ which are reducible over $F$. If $S_F$ is computable, we say that $F$ has a splitting algorithm.

**Theorem (Rabin’s embedding theorem)**

There is a computable algebraically closed field $\overline{F}$ and a computable field embedding $\iota: F \to \overline{F}$ such that $\overline{F}$ is algebraic over $\iota(F)$.

For any such $\overline{F}$ and $\iota$, the image $\iota(F)$ of $F$ in $\overline{F}$ is Turing equivalent to the splitting set of $F$.

**Theorem (Kronecker)**

If $F$ has a splitting algorithm, then every finite extension of $F$ has a splitting algorithm.
We want to know:

- When does a computable embedding of a field $F$ into an algebraically closed field $K$ extend to a computable embedding of $\overline{F}$ into $K$?
- When does a computable automorphism of a field $F$ extend to a computable automorphism of $\overline{F}$?

Friedman, Simpson, and Smith, and Dorais, Hirst, and Shafer analyzed these questions using Reverse Mathematics. We can state their results in terms of effective algebra.
For embeddings into algebraically closed fields:

**Theorem (Friedman-Simpson-Smith; Dorais-Hirst-Shafer)**

Let $F$ be a computable field and let $\iota: F \to \overline{F}$ be a computable embedding of $F$ into its algebraic closure.

If $F$ has a splitting algorithm, every computable embedding of $F$ into a computable algebraically closed field $K$ extends to a computable embedding of $\overline{F}$ into $K$.

Even if $F$ does not have a splitting algorithm, every computable embedding of $F$ into a computable algebraically closed field $K$ extends to a low embedding of $\overline{F}$ into $K$. 
For extensions of automorphisms:

**Theorem (Friedman-Simpson-Smith; Dorais-Hirst-Shafer)**

Let $F$ be a computable field and let $\iota: F \to \overline{F}$ be a computable embedding of $F$ into its algebraic closure.

If $F$ has a splitting algorithm, every computable automorphism of $F$ extends to a computable automorphism of $\overline{F}$.

Even if $F$ does not have a splitting algorithm, every computable automorphism of $F$ extends to a low automorphism of $\overline{F}$.

We will try to answer the question: is it necessary to have a splitting algorithm?
Theorem (HT-Miller-Melnikov)

Let $F$ be a computable field and let $\iota: F \to \overline{F}$ be a computable embedding of $F$ into its algebraic closure. The following are equivalent:

1. $F$ has a splitting algorithm.
2. Every computable embedding of $F$ into a computable algebraically closed field $K$ extends to a computable embedding of $\overline{F}$ into $K$. 

\[ \begin{array}{c} \overline{F} \xrightarrow{\beta} K \\ \uparrow \iota \\ F \xrightarrow{\alpha} K \end{array} \]
Theorem (HT-Miller-Melnikov)

Let $F$ be a computable normal algebraic extension of the prime field and let $\iota: F \to \overline{F}$ be a computable embedding of $F$ into its algebraic closure. The following are equivalent:

1. $\mathcal{F}$ has a splitting algorithm.
2. Every computable automorphism of $F$ extends to a computable automorphism of $\overline{F}$.

\[
\begin{array}{c}
\overline{F} \\ \uparrow \iota \\
\mathcal{F} \\ \alpha \rightarrow F \\
\end{array}
\quad \begin{array}{c}
\beta \rightarrow \overline{F} \\
\downarrow \\
\iota \\
\end{array}
\]
Before, we fixed the embedding of $F$ into $\overline{F}$. What happens if we let this embedding vary?

**Question**

Which fields $F$ have the following property?

- For every computable automorphism $\alpha$ of $F$, there is a computable embedding $\iota: F \rightarrow \overline{F}$ of $F$ into an algebraic closure and a computable automorphism $\beta$ of $\overline{F}$ extending $\alpha$.

We do not have a complete solution to this question, but towards a partial solution, we introduce the *non-covering property*. 
Definition
We say that a group $G$ has the **non-covering property** if for all finite index normal subgroups $M \nsubseteq N$ of $G$ and $g \in G$, there is $h \in gN$ such that for all $x \in G$, $x^{-1}hx \notin gM$.

Lemma
Let $F/E$ be a separable normal extension. The following are equivalent:

1. $\text{Gal}(F/E)$ has the non-covering property.

2. For all finite normal subextensions $K_1/E$ and $K_2/E$ with $K_2 \nsubseteq K_1$, and every pair of automorphisms $\sigma$ of $K_1$ and $\tau$ of $K_2$ fixing $E$, there is an automorphism $\alpha$ of $F$ extending $\sigma$ and incompatible with $\tau$ (i.e., $(K_2, \tau)$ does not embed into $(F, \alpha)$ as a difference field).
Theorem (HT-Miller-Melnikov)

Let $F$ be a computable normal algebraic extension of the prime field $\mathbb{F}_p$ such that $\text{Gal}(F/\mathbb{F}_p)$ has the non-covering property. The following are equivalent:

1. $F$ has a splitting algorithm.

2. For every computable automorphism $\alpha$ of $F$, there is a computable embedding $\iota: F \to \overline{F}$ of $F$ into an algebraic closure and a computable automorphism $\beta$ of $\overline{F}$ extending $\alpha$.

\[
\begin{array}{ccc}
\overline{F} & \xrightarrow{\beta} & \overline{F} \\
\uparrow & & \uparrow \\
\iota \downarrow & & \iota \downarrow \\
\downarrow & & \downarrow \\
F & \xrightarrow{\alpha} & F
\end{array}
\]
The following groups have the non-covering property:

- abelian groups,
- simple groups,
- the quaternion group.

$S_3$ does not have the non-covering property.

**Theorem (HT-Miller-Melnikov)**

Let $\{G_i : i \in I\}$ be a collection of profinite groups, each of which has the non-covering property. Then $\prod_{i \in I} G_i$ has the non-covering property.
**Theorem (HT-Miller-Melnikov)**

Let $F$ be a computable normal algebraic extension of $\mathbb{F}_p$ in characteristic $p > 0$. The following are equivalent:

1. $F$ has a splitting algorithm.
2. For every computable automorphism $\alpha$ of $F$, there is a computable embedding $\iota: F \to \overline{F}$ of $F$ into an algebraic closure and a computable automorphism $\beta$ of $\overline{F}$ extending $\alpha$.

**Proof.**

The Galois group of every normal extension $F/\mathbb{F}_p$ in characteristic $p > 0$ is abelian and hence has the non-covering property.

**Question**

Is this true in characteristic zero?