Computably Categorical Fields
via Fermat’s Last Theorem

Russell Miller,
Queens College &
Graduate Center, CUNY

Hans Schoutens,
NYC College of Technology
& Graduate Center, CUNY

May 22, 2009
Computable Categoricity

**Defn.**: A computable structure $\mathcal{A}$ is *computably categorical* if for each computable $\mathcal{B} \cong \mathcal{A}$ there is a computable isomorphism from $\mathcal{A}$ to $\mathcal{B}$.

**Examples**: (Dzgoev, Goncharov; Remmel; Lempp, McCoy, M., Solomon)

- A linear order is computably categorical iff it has only finitely many adjacencies.
- A Boolean algebra is computably categorical iff it has only finitely many atoms.
- An ordered Abelian group is computably categorical iff it has finite rank (≡ basis as $\mathbb{Z}$-module).
- For trees, the known criterion is recursive in the height and not easily stated!
Computably Categorical Fields

**Thm.** (Frohlich-Shepherdson): All normal algebraic extensions of \( \mathbb{Q} \) and of \( \mathbb{Z}/(p) \) are computably categorical. However, there does exist a computable field which is not c.c.

**Thm.** (Ershov, 1977): An algebraically closed field is computably categorical iff it has finite transcendence degree over its prime subfield.

Natural conjecture: this holds for fields in general. But:

**Thm.** (Ershov, 1977): There exists a computable field, algebraic over \( \mathbb{Q} \), which is not c.c.

**Thm.** (Miller-Schoutens, 2009): There exists a computable field of infinite transcendence degree over \( \mathbb{Q} \) which is c.c.
Infinite Transcendence

Basic distinction for computable fields: finite vs. infinite transcendence degree.

- For finite tr.deg. $n$, use $Q(x_1, \ldots, x_n)$ in place of the prime subfield $Q$, and constructions for algebraic fields go through.

- For infinite tr.deg., very hard just to identify a basis!

Prop.: If a computable field $F$ contains the algebraic closure of its prime subfield $Q$, and has infinite tr.deg. over $Q$, then $F$ is not c.c.

Proof: Use $\Delta_2$ guessing to identify a basis $B$ in $F$. Build $\tilde{F} \cong F$, with a corresponding basis $\tilde{B}_s$. But when $\varphi_e$ maps $b \in B$ to a transcendental $\varphi_e(b)$ in $\tilde{F}$, we reconfigure $\tilde{F}$ and make $\varphi_e(b)$ algebraic instead. The algebraic closure allows this to work: there must be an embedding of $\tilde{F}_s$ into $\tilde{F}_s \cup \overline{Q}$ with $\varphi_e(b)$ mapping into $\overline{Q}$. 
Tagging a Basis Element

Idea: make basis elements recognizable, by making them part of solutions to certain polynomials. Start with \( \mathbb{Q}(x_0, x_1, x_2, \ldots) \) purely transcendental, and then adjoin (e.g.) \( y_0 \) satisfying

\[
x_0^5 + y_0^5 = 1.
\]

The hope is that, in other computable copies of this field, we can recognize the pair \( \{x_0, y_0\} \) as the unique solution to \( X^5 + Y^5 = 1 \).

- By Fermat’s Theorem, the only solutions in \( \mathbb{Q} \) are \( (0, 1) \) and \( (1, 0) \).
- Need to show that there are no other solutions in our field.
- Then we need to tag other \( x_i \), adding other \( y_i \), without adjoining any more solutions of \( X^5 + Y^5 = 1 \).
This calls for **algebraic geometry**!

**Prop.** Let $k$ be a field of char. 0 and let $C$ be a curve over $k$ of genus $g \geq 2$. Then the function field $K = k(C)$ of $C$ is generated by the coordinates of any $K$-rational point $P$ of $C$ which is not $k$-rational. So for any $P \in C(K) \setminus C(k)$, the natural inclusion $k(P) \subseteq K$ is an equality.

Take $k = \mathbb{Q}$, $C$ a Fermat curve, so $K = \mathbb{Q}(x)[y]/(x^p + y^p - 1)$. The Proposition shows that every nontrivial solution of $C$ within $K$ generates $K$. So such solutions correspond to automorphisms of $K$. 

**Drastic Measures**
Fermat Curves and Solutions

Thm. (Leopoldt; Tzermias): Over an algebraically closed field $K$ of characteristic 0, the automorphism group of the projective curve $X^p + Y^p = Z^p$ is the semidirect product of the symmetric group $S_3$ and the group $(\mu(p))^2$, where $\mu(p)$ is the multiplicative group of $p$-th roots of unity in $K$.

This limits the solutions of a Fermat curve $C$, and shows that the only solutions in our function field are $(x, y)$ and $(y, x)$.

(Thanks to Gunther Cornelissen!)
Different Fermat Curves

But could one Fermat curve have a solution in the function field of another Fermat curve?

Prop.: Let \( C \) be a general collection of curves over \( k \) and let \( k(C) \) be its function field. Suppose all curves in \( C \) have genus at most \( g \) and let \( D \) be an arbitrary curve of genus at least \( g \). Then the function field \( k(D) \) embeds in \( k(C) \) if and only if \( D \in C \).

Genus of the Fermat curve \( (X^p + Y^p - 1) \) is \( \frac{(p-1)(p-2)}{2} \). So no larger-degree Fermat curve has any solution in the function field of the smaller-degree curves.
No Cover Relation

Lemma: Let $C$ be a curve of genus $g \geq 2$ and let $F_p$ be the Fermat curve of degree $p$. If $p > 64g^2$, then there is no cover relation between $C$ and $F_p$.

(This follows from work of Baker, González, González-Jiménez, & Poonen.)

“No cover relation” implies no solutions to either curve in the function field of the other curve. And by choosing each $p_{i+1}$ sufficiently large, we may ensure no cover relation between any Fermat curves $F_{p_i}$ and $F_{p_j}$.

Moreover, then there is no cover relation between finite collections of such curves.
Computable Categoricity

**Thm.** (Miller-Schoutens): The function field $F$ of the collection of Fermat curves $F_{p_0}, F_{p_1}, \ldots$ is a computable, computably categorical field of infinite transcendence degree over $\mathbb{Q}$.

Specifically, $F$ is generated over $\mathbb{Q}$ by a basis \{x_0, x_1, \ldots\} and additional elements $y_i$ s.t. $x_i^{p_i} + y_i^{p_i} = 1$. The only solutions to $X^{p_i} + Y^{p_i} = 1$ in $F$ are $(x_i, y_i), (y_i, x_i), (0, 1), \& (1, 0)$. So in any $\tilde{F} \cong F$, we may find any nonzero solution $(\tilde{x}_i, \tilde{y}_i)$ and map $x_i \mapsto \tilde{x}_i$ and $y_i \mapsto \tilde{y}_i$. 
Similar Fields

This same result would apply to any function field for an infinite c.e. set \( C = \langle C_i \rangle_{i \in \omega} \) of curves of genus \( \geq 2 \) with:

- no cover relations among the curves in \( C \);
- effective Mordell-Weil: the function \( i \mapsto |C_i(\mathbb{Q})| \) must be computable (and \( |C_i(\mathbb{Q})| < \infty \)).

What other collections \( C \) might satisfy this?

- To avoid cover relations, we could take all curves to have the same genus.
- Could we just take all Fermat curves of prime degree \( \geq 5 \)?
**Restricting Automorphisms**

For the above $F$, each $x_i$ can map to either $x_i$ or $y_i$, independently of other $x_j$. So we have $2^\omega$ automorphisms of $F$, of arbitrary Turing degree.

Build the computable extension field $E \supseteq F$ by adjoining square roots:

$$E = F[\sqrt{x_i} : i \in \omega].$$

**Lemma:** No $y_i$ has a square root in $E$.

Proof: Embed $E \hookrightarrow \mathbb{R}$ with $x_i > 1$ for all $i$. Then all $y_i = \sqrt[pi]{1 - x_i^{pi}} < 0$. 

Intrinsically Computable Basis

**Defn:** A relation $R$ on a computable $\mathcal{M}$ is \textit{intrinsically computable} if, for all isomorphisms $f : \mathcal{M} \to \mathcal{A}$ with $\mathcal{A}$ computable, $f(R)$ is computable.

In $E$, the basis $B = \{x_0, x_1, \ldots\}$ is defined by a computable infinitary $\Sigma^0_1$ formula, hence is intrinsically c.e.

**Lemma:** In a computable field, every c.e. basis is computable.

So $B$ is intrinsically computable.