The Theory of Fields is Complete for Isomorphisms

Russell Miller

Queens College & CUNY Graduate Center

Workshop on Computable Model Theory Banff International Research Station 7 November 2013

(Joint work with Jennifer Park, Bjorn Poonen, Hans Schoutens, and Alexandra Shlapentokh.)

Completeness for Isomorphisms

Theorem (Hirschfeldt-Khoussainov-Shore-Slinko 2002)

For every automorphically nontrivial, countable structure \mathcal{A} , there exists a countable graph G which has the same spectrum as \mathcal{A} , the same *d*-computable dimension as \mathcal{A} (for each *d*), and the same categoricity properties as \mathcal{A} under expansion by a constant, and which realizes every DgSp_{\mathcal{A}}(R) (for every relation R on \mathcal{A}) as the spectrum of some relation on G.

Moreover, this holds not only of graphs, but also of partial orderings, lattices, rings, integral domains of arbitrary characteristic, commutative semigroups, and 2-step nilpotent groups.

Given \mathcal{A} , they built a graph $G = \mathscr{G}(\mathcal{A})$ such that the isomorphisms from \mathcal{A} onto any \mathcal{B} correspond bijectively with the isomorphisms from $\mathscr{G}(\mathcal{A})$ onto $\mathscr{G}(\mathcal{B})$, by a map $f \mapsto \mathscr{G}(f)$ which preserves the Turing degree of f.

Incompleteness for Isomorphisms

The following classes of structures are known not to be complete in this way, by results of Richter, Dzgoev and Goncharov, Remmel, and many others:

- Inear orders
- Boolean algebras
- trees (as partial orders, or under the meet function)
- abelian groups
- real closed fields
- algebraically closed fields
- fields of finite transcendence degree over Q.

From Graphs to Fields

Theorem (MPPSS)

For every countable graph *G*, there exists a countable field $\mathscr{F}(G)$ with the same computable-model-theoretic properties as *G*, as in the HKSS theorem. Indeed, \mathscr{F} may be viewed as an effective, fully faithful functor from the category of countable graphs (under monomorphisms) into the class of fields, with an effective inverse functor (on its image).

Full faithfulness means that each field homomorphism $\mathscr{F}(G) \to \mathscr{F}(G')$ comes from a unique monomorphism $G \to G'$. Isomorphisms $g: G \to G'$ will map to isomorphisms $\mathscr{F}(g) : \mathscr{F}(G) \to \mathscr{F}(G')$.

We do not claim that every $F' \cong \mathscr{F}(G)$ lies in the image of \mathscr{F} . This situation will require attention.

Construction of $\mathscr{F}(G)$

We use two curves X and Y, defined by integer polynomials:

$$X: p(u, v) = u^4 + 16uv^3 + 10v^4 + 16v - 4 = 0$$

$$Y: q(T, x, y) = x^4 + y^4 + 1 + T(x^4 + xy^3 + y + 1) = 0$$

Let $G = (\omega, E)$ be a graph. Set $K = \mathbb{Q}(\prod_{i \in \omega} X)$ to be the field generated by elements $u_0 < v_0 < u_1 < v_1, \ldots$, with $\{u_i : i \in \omega\}$ algebraically independent over \mathbb{Q} , and with $p(u_i, v_i) = 0$ for every *i*. The element u_i in $K \subseteq \mathscr{F}(G)$ will represent the node *i* in *G*.

Next, adjoin to *K* elements x_{ij} and y_{ij} for all i > j, with $\{x_{ij} : i > j\}$ algebraically independent over *K*, and with

$$q(u_iu_j, x_{ij}, y_{ij}) = 0 \text{ if } (i,j) \in E$$
$$q(u_i + u_j, x_{ij}, y_{ij}) = 0 \text{ if } (i,j) \notin E.$$

We write Y_t for the curve defined by q(t, x, y) = 0 over $\mathbb{Q}(t)$. So the process above adjoins the function field of either $Y_{u_iu_j}$ or $Y_{u_i+u_j}$, for each i > j. $\mathscr{F}(G)$ is the extension of K generated by all x_{ij} and y_{ij} .

Reconstructing *G* **From** $\mathscr{F}(G)$

Lemma

Let
$$G = (\omega, E)$$
 be a graph, and build $\mathscr{F}(G)$ as above. Then:
(i) $X(\mathscr{F}(G)) = \{(u_i, v_i) : i \in \omega\}.$
(ii) If $(i, j) \in E$, then $Y_{u_i u_j}(\mathscr{F}(G)) = \{(x_{ij}, y_{ij})\}$ and $Y_{u_i + u_j}(\mathscr{F}(G)) = \emptyset.$
(iii) If $(i, j) \notin E$, then $Y_{u_i u_j}(\mathscr{F}(G)) = \emptyset$ and $Y_{u_i + u_j}(\mathscr{F}(G)) = \{(x_{ij}, y_{ij})\}.$

This is the heart of the proof. (i) says that p(u, v) = 0 has no solutions in $\mathscr{F}(G)$ except the ones we put there, so we can enumerate

$$\{u_i: i \in \omega\} = \{u \in \mathscr{F}(G): (\exists v \in \mathscr{F}(G)) p(u, v) = 0\}.$$

Similarly, (ii) and (iii) say that the equations $q(u_iu_j, x, y) = 0$ and $q(u_i + u_j, x, y) = 0$ have no unintended solutions in $\mathscr{F}(G)$. So, given *i* and *j*, we can determine from $\mathscr{F}(G)$ whether $(i, j) \in E$: search for a solution to either $q(u_iu_j, x, y) = 0$ or $q(u_i + u_j, x, y) = 0$.

$$X: u^{4} + 16uv^{3} + 10v^{4} + 16v - 4 = 0 \text{ over } \mathbb{Q}, \text{ and}$$
$$Y: x^{4} + y^{4} + 1 + T(x^{4} + xy^{3} + y + 1) = 0 \text{ over } \mathbb{Q}(T).$$

Lemma 0.1.

(1) Both X and Y are geometrically integral.

(2) We have $g_X = g_Y > 1$.

- (3) Even after base field extension, X and Y have no nontrivial birational automorphisms.
- (4) Even after base field extension, there is no birational map from Y to any curve definable over a finite extension of Q.
- (5) We have $X(\mathbb{Q}) = \emptyset$.
- (6) The set $u(X(\mathbb{R}))$ contains an open neighborhood of 0 in \mathbb{R} .
- (7) For each t in an open neighborhood of 0 in \mathbb{R} , we have $Y_t(\mathbb{R}) = \emptyset$.

Proof. The projective closure \widetilde{X} of X specializes under reduction modulo 5 to the curve

$$\widetilde{X}_5: u^4 + uv^3 + vw^3 + w^4 = 0$$

in $\mathbb{P}^2_{\mathbb{F}^5}$. The projective closure of Y specializes at T = 0 and $T = \infty$ to the curves

 $\widetilde{Y}_0: x^4 + y^4 + z^4 = 0$ and $\widetilde{Y}_\infty: x^4 + xy^3 + yz^3 + z^4 = 0$

- in $\mathbb{P}^2_{\mathbb{Q}}$, respectively. By [Poo05, Case I with n = 2, d = 4, c = 1], \widetilde{X}_5 and \widetilde{Y}_{∞} are smooth, projective, geometrically integral plane curves of genus 3 with no nontrivial birational automorphisms even after base extension. It follows that X and Y have the same properties, except not projective.
- (1) Explained above.
- (2) By the above, $g_X = g_Y = 3$.
- (3) Explained above.
- (4) If there were such a birational map, then the specializations \widetilde{Y}_0 and \widetilde{Y}_∞ would be isomorphic over $\overline{\mathbb{Q}}$. But the former has a nontrivial automorphism $(x, y, z) \mapsto (-x, y, z)$.
- (5) The given model of \widetilde{X} (viewed over \mathbb{Z}) reduces modulo 8 to $u^4 + 2v^4 + 4w^4 = 0$, which has no solutions in $\mathbb{P}^2(\mathbb{Z}/8\mathbb{Z})$.
- (6) The polynomial 10v⁴+16v−4 has a real zero between v = 0 and v = 1, and it is separable since it is 2 times an Eisenstein polynomial at 2. Thus X(ℝ) has a point with u = 0, and, by the implicit function theorem, also a point with any u-coordinate sufficiently close to 0 in ℝ.

(7) This follows from
$$Y_0(\mathbb{R}) = \emptyset$$
 and compactness.

Lemma 0.2. Fix G. Consider X and all the curves $Y_{u_iu_j}$ and $Y_{u_i+u_j}$. Even after base field extension, the only nonconstant rational maps between these curves are the identity maps from one of them to itself.

Proof. By (2), all the curves have the same genus. By (3) and Lemma 0.5, it suffices to show that no two distinct curves in this list are birational even after base field extension. By (4), this is already true for X and Y_t for any transcendental t. If t, t' are algebraically independent over \mathbb{Q} , and Y_t and $Y_{t'}$ become birational after base field extension, then we can specialize t' to an element of $\overline{\mathbb{Q}}$ while leaving t transcendental, contradicting (4). The previous two sentences apply in particular to any t and t' taken from the $u_i u_j$ and the $u_i + u_j$.

Lemma 0.3. Let G = (V, E) be a graph. Let $x_{ij}, y_{ij} \in \mathscr{F}(G)$ correspond to the rational functions x, y on $Z_{\{i,j\}}$.

(i) We have $X(\mathscr{F}(G)) = \{(u_i, v_i) : i \in V\}.$

- (ii) If $\{i, j\} \in E$, then $Y_{u_i u_j}(\mathscr{F}(G)) = \{(x_{ij}, y_{ij})\}$ and $Y_{u_i + u_j}(\mathscr{F}(G)) = \emptyset$.
- (iii) If $\{i, j\} \notin E$, then $Y_{u_i u_j}(\mathscr{F}(G)) = \emptyset$ and $Y_{u_i + u_j}(\mathscr{F}(G)) = \{(x_{ij}, y_{ij})\}$.

Proof.

(i) By definition, 𝔅(G) is the direct limit of F(Z), where Z ranges over finite products of the Z_{i,j}. Thus, by Lemma 0.4, each point in X(𝔅(G)) corresponds to a rational map from some Z to X_F. By Lemmas 0.6 and 0.2 every such rational map is constant. In other words, X(𝔅(G)) = X(F).

Similarly, by Lemma 0.4, each point in X(F) corresponds to a rational map from some finite power of X to X. By (5), the rational map is nonconstant. By Lemmas 0.6 and 0.2 it is the *i*th projection for some *i*. The corresponding point in X(F) is (u_i, v_i) .

(ii) Suppose that $\{i, j\} \in E$. The same argument as for (i) shows that $Y_{u_i u_j}(\mathscr{F}(G)) = Y_{u_i u_j}(F) \cup \{(x_{ij}, y_{ij})\}$, the last point coming from the identity $Z_{\{i,j\}} \to Y_{u_i u_j}$. By (6), we may embed F in \mathbb{R} so that the u_i are mapped to algebraically independent real numbers so close to zero that $Y_{u_i u_j}(\mathbb{R}) = \emptyset$ by (7). Thus $Y_{u_i u_j}(F) = \emptyset$. So $Y_{u_i u_j}(\mathscr{F}(G)) = \{(x_{ij}, y_{ij})\}$. The argument for $Y_{u_i + u_j}(\mathscr{F}(G)) = \emptyset$ is the same, except now that $Z_{\{i,j\}}$ is not birational to $Y_{u_i u_j}$. The argument for (iii) is the same as for (ii).

Lemma 0.4. If V and W are varieties over a field k, and W is integral, then V(k(W)) is in bijection with the set of rational maps $W \dashrightarrow V$.

Proof. The description of a point in V(k(W)) involves only finitely many elements of k(W), and there is a dense open subvariety $U \subseteq W$ on which they are all regular.

Lemma 0.5. Let k be a field of characteristic 0. Let C and D be geometrically integral curves over k such that $g_C = g_D > 1$. Every nonconstant rational map $C \dashrightarrow D$ is a birational map.

Π

Proof. This is a well known consequence of Hurwitz's formula.

Lemma 0.6. Let V_1, \ldots, V_n be geometrically integral varieties over a field k. Let C be a geometrically integral curve over k such that $g_C > 1$. Then each rational map $V_1 \times \cdots \times V_n \dashrightarrow C$ factors through the projection $V_1 \times \cdots \times V_n \to V_i$ for at least one i.

Proof. By induction, we may assume that n = 2. We may assume that k is algebraically closed. A rational map $\phi: V_1 \times V_2 \dashrightarrow C$ may be viewed as an algebraic family of rational maps $V_1 \dashrightarrow C$ parametrized by (an open subvariety of) V_2 . But the de Franchis-Severi theorem [Sam66, Théorème 2] implies that there are no nonconstant algebraic families of nonconstant rational maps $V_1 \dashrightarrow C$. Thus either the rational maps in the family are all the same, in which case ϕ factors through the first projection, or each rational map in the family is constant, in which case ϕ factors through the second projection.

References

- [Poo05] Bjorn Poonen, Varieties without extra automorphisms. III. Hypersurfaces, Finite Fields Appl. 11 (2005), no. 2, 230–268, DOI 10.1016/j.ffa.2004.12.001. MR2129679 (2006e:14060) ↑(document)
- [Sam66] Pierre Samuel, Compléments à un article de Hans Grauert sur la conjecture de Mordell, Inst. Hautes Études Sci. Publ. Math. 29 (1966), 55–62 (French). MR0204430 (34 #4272) ↑(document)

Functoriality

Suppose $g: G \to G'$ is a graph monomorphism. The map $f = \mathscr{F}(g): \mathscr{F}(G) \to \mathscr{F}(G')$ uses a *g*-oracle to map

$$(u_i, v_i) \mapsto (u'_{g(i)}, v'_{g(i)})$$
 and $(x_{ij}, y_{ij}) \mapsto (x'_{g(i)g(j)}, y'_{g(i)g(j)}).$

 $(\mathscr{F}(G)$ is built by a tightly defined process, so all these elements are known.) With

$$\begin{aligned} q(u_i u_j, x_{ij}, y_{ij}) &= 0 \text{ in } \mathscr{F}(G) \iff (i, j) \in E \\ \iff (g(i), g(j)) \in E' \\ \iff q(u'_{g(i)} u'_{g(j)}, x'_{g(i)g(j)}, y'_{g(i)g(j)}) = 0 \text{ in } \mathscr{F}(G'), \end{aligned}$$

and likewise for $u_i + u_j$, this *f* extends to a field homomorphism, using oracles for $\mathscr{F}(G) (\leq_T G)$ and $\mathscr{F}(G') (\leq_T G')$. So $f \leq_T g \oplus G \oplus G'$.

Finally, *g* is an isomorphism iff $\mathscr{F}(g)$ is.

Full Faithfulness

Suppose $f : \mathscr{F}(G) \to \mathscr{F}(G')$ is an isomorphism. We identify u_0, u_1, \ldots in $\mathscr{F}(G)$ and $u'_0, u'_1 \ldots$ in $\mathscr{F}(G')$.

Now *f* must map each (u_i, v_i) to some (u'_k, v'_k) . Define $g = \mathscr{F}^{-1}(f) : G \to G'$ by g(i) = k. With *f* an isomorphism, this *g* is onto *G'* and preserves the edge relations in *G* and *G'*:

$$(i,j) \in E \iff (\exists x, y \in \mathscr{F}(G) \ q(u_i u_j, x, y) = 0$$

 $\iff (\exists x', y' \in \mathscr{F}(G') \ q(u'_{g(i)} u'_{g(j)}, x', y') = 0$
 $\iff (g(i), g(j)) \in E'.$

Indeed $g \leq_T f$, with no oracle needed for G, $\mathscr{F}(G)$, G', or $\mathscr{F}(G')$. Moreover, $\mathscr{F}(g) = f$, and so $f \leq_T g \oplus G \oplus G'$.

Fields Which *F* Missed

Fix *G* and suppose $f : F \cong \mathscr{F}(G)$. With an *F*-oracle, we can enumerate X(F), thus listing out u_0, u_1, \ldots in *F*. Define a graph *G'* on ω by

$$(i,j) \in E' \iff (\exists x, y \in F) q(u_iu_j, x, y) = 0.$$

Since $F \cong \mathscr{F}(G)$, we have $(i, j) \notin E'$ iff $(\exists x, y \in F) q(u_i + u_j, x, y) = 0$, so E' is Δ_1^F , and $G' \leq_T F$.

Therefore $F' := \mathscr{F}(G') \leq_T F$. Moreover, $u_i \mapsto u'_i$ and $v_i \mapsto v'_i$ extends to an isomorphism $f' : F \to F'$, with

$$f' \leq_T F \oplus F' \equiv F \oplus \mathscr{F}(G') \leq_T F \oplus G' \leq_T F.$$

Finally, $f' \circ f^{-1} : \mathscr{F}(G) \to \mathscr{F}(G')$ yields an isomorphism $g : G \to G'$, by full faithfulness.

Fields Which *F* Missed

Fix *G* and suppose $f : F \cong \mathscr{F}(G)$. With an *F*-oracle, we can enumerate X(F), thus listing out u_0, u_1, \ldots in *F*. Define a graph *G'* on ω by

$$(i,j) \in E' \iff (\exists x, y \in F) q(u_iu_j, x, y) = 0.$$

Since $F \cong \mathscr{F}(G)$, we have $(i, j) \notin E'$ iff $(\exists x, y \in F) q(u_i + u_j, x, y) = 0$, so E' is Δ_1^F , and $G' \leq_T F$.

Therefore $F' := \mathscr{F}(G') \leq_T F$. Moreover, $u_i \mapsto u'_i$ and $v_i \mapsto v'_i$ extends to an isomorphism $f' : F \to F'$, with

$$f' \leq_T F \oplus F' \equiv F \oplus \mathscr{F}(G') \leq_T F \oplus G' \leq_T F.$$

Finally, $f' \circ f^{-1} : \mathscr{F}(G) \to \mathscr{F}(G')$ yields an isomorphism $g : G \to G'$, by full faithfulness.

Lemma

Every *F* isomorphic to $\mathscr{F}(G)$ has an *F*-computable isomorphism onto some $\mathscr{F}(G')$, for some *F*-computable $G' \cong G$.

Consequences in Computable Model Theory

Corollary

For every countable structure A which is not automorphically trivial, there exists a field F with the same Turing degree spectrum as A:

$$Spec(\mathcal{A}) = \{ deg(\mathcal{B}) : \mathcal{B} \cong \mathcal{A} \& dom(\mathcal{B}) = \omega \} \\ = \{ deg(E) : E \cong F \& dom(E) = \omega \} \\ = Spec(F).$$

No infinite field is automorphically trivial, but some infinite structures (including graphs) are, so this case must be excluded.

Consequences: Categoricity Spectra & Dimension

Corollary

For every computable structure \mathcal{A} , there exists a computable field F with the same categoricity spectrum as \mathcal{A} and (for each Turing degree d) the same d-computable dimension as \mathcal{A} . Additionally, for every computable ordinal α , F is relatively Δ_{α}^{0} -categorical if and only if \mathcal{A} is.

That is, for every Turing degree d, A is d-computably categorical if and only if F is d-computably categorical, and moreover, the number of computable structures isomorphic to A, modulo d-computable isomorphism, is exactly the number of computable fields isomorphic to F, modulo d-computable isomorphism.

In particular, fields realize all computable dimensions $\leq \omega$.

For the relative categoricity claim, recall that every $F' \cong \mathscr{F}(G)$ is of the form $\mathscr{F}(G')$, up to F'-computable isomorphism, with $G' \cong G$.

Consequences: Computable Categoricity

Downey, Kach, Lempp, Lewis, Montalbán, and Turetsky have recently proven that computable categoricity for trees is Π_1^1 -complete.

Corollary

The property of computable categoricity for computable fields is Π^1_1 -complete. That is, the set

 $\{e \in \omega : \varphi_e \text{ computes a computably categorical field}\}$

is a Π_1^1 set, and every Π_1^1 set is 1-reducible to this set.

Consequences: Spectra of Relations

The *degree spectrum of a relation* R on a computable structure A is the set of all Turing degrees of images of R under isomorphisms from A onto computable structures B.

Corollary

Let A be any computable structure which is not automorphically trivial, and R an *n*-ary relation on A. Then there exists a field F and an *n*-ary relation S on F such that

 $\mathsf{DgSp}_{\mathcal{A}}(R) = \mathsf{DgSp}_{\mathcal{F}}(S).$

Consequences: Automorphism Spectra

The *automorphism spectrum* of a computable structure A is the set of all Turing degrees of nontrivial automorphisms of A. This was the subject of study by Harizanov/M/Morozov.

Corollary

For every computable structure A, there is a computable field F with the same automorphism spectrum as A.

Comparison with Algebraic Fields

In general, algebraic fields hold far less complexity than fields in general.

- For algebraic fields, computable categoricity is a Π⁰₄-complete property (Hirschfeldt-Kramer-M-Shlapentokh), not Π¹₁.
- Every algebraic field is **0**["]-categorical (and better!). Hence many categoricity spectra cannot be realized by computable algebraic fields.
- Likewise, algebraic fields have far simpler spectra (Frolov-Kalimullin-M). The spectrum of an algebraic field *F* is defined by the ability to enumerate {*p* ∈ ℚ[X] : *p* has a root in *F*}.
- The question of finite computable dimension > 1 for algebraic fields remains open.

Zeroing In on $\mathscr{F}(G)$

Every field $\mathscr{F}(G)$ can compute an order on itself. We define a field embedding *h* of $\mathscr{F}(G)$ into the computable real numbers, effectively.

- p(7, -10) < 0, so choose a countable, algebraically independent, uniformly computable set of reals near -10, to be the images $h(v_i)$, with all $p(7, h(v_i)) < 0$.
- Then we may choose $h(u_i) > 7$ in \mathbb{R} with $p(h(u_i), h(v_i)) = 0$.
- We need $q(t_{ij}, h(x_{ij}), h(y_{ij})) = 0$, with either $t_{ij} = h(u_i + u_j)$ or $t_{ij} = h(u_i u_j)$. With $t_{ij} > 14$, we know $q(t_{ij}, 0, \frac{-\sqrt[3]{t_{ij}}}{\sqrt[3]{4}}) < 0$, so we can choose the $h(y_{ij})$ all algebraically independent, uniformly computable, and close enough to $\frac{-\sqrt[3]{t_{ij}}}{\sqrt[3]{4}}$ that $q(t_{ij}, 0, h(y_{ij})) < 0$.
- This allows us to choose $h(x_{ij})$ to be a real root of $q(t_{ij}, X, h(y_{ij}))$.

Zeroing In on $\mathscr{F}(G)$

Every field $\mathscr{F}(G)$ can compute an order on itself. We define a field embedding *h* of $\mathscr{F}(G)$ into the computable real numbers, effectively.

- p(7, -10) < 0, so choose a countable, algebraically independent, uniformly computable set of reals near -10, to be the images $h(v_i)$, with all $p(7, h(v_i)) < 0$.
- Then we may choose $h(u_i) > 7$ in \mathbb{R} with $p(h(u_i), h(v_i)) = 0$.
- We need $q(t_{ij}, h(x_{ij}), h(y_{ij})) = 0$, with either $t_{ij} = h(u_i + u_j)$ or $t_{ij} = h(u_i u_j)$. With $t_{ij} > 14$, we know $q(t_{ij}, 0, \frac{-\sqrt[3]{t_{ij}}}{\sqrt[3]{4}}) < 0$, so we can choose the $h(y_{ij})$ all algebraically independent, uniformly computable, and close enough to $\frac{-\sqrt[3]{t_{ij}}}{\sqrt[3]{4}}$ that $q(t_{ij}, 0, h(y_{ij})) < 0$.

• This allows us to choose $h(x_{ij})$ to be a real root of $q(t_{ij}, X, h(y_{ij}))$. But the isomorphisms $\mathscr{F}(g)$ generally do not respect these orderings! Indeed, the archimedean ordered fields are not complete for isomorphisms, by results of Oscar Levin.

HAPPY BIRTHDAY, JULIA!