Computable tree presentations of continuum-size structures

Russell Miller

Queens College & CUNY Graduate Center

Computable Structure Theory and Interactions
Technische Universität Wien
16 July 2024

Presenting automorphism groups

Let $\mathcal S$ be a computable structure, with domain ω , in a relational signature (R_0,R_1,\ldots) . We begin building the *automorphism tree* $T_{\operatorname{Aut}(\mathcal S)}$ of $\mathcal S$, which by definition contains all nodes $\tau=(\rho\oplus\lambda)\in\omega^{<\omega}$ with any length $n=|\rho|=|\lambda|$ satisfying:

• $\sigma := \rho \cup (\lambda^{-1})$ is a partial injective function; and

Presenting automorphism groups

Let $\mathcal S$ be a computable structure, with domain ω , in a relational signature (R_0,R_1,\ldots) . We begin building the *automorphism tree* $T_{\operatorname{Aut}(\mathcal S)}$ of $\mathcal S$, which by definition contains all nodes $\tau=(\rho\oplus\lambda)\in\omega^{<\omega}$ with any length $n=|\rho|=|\lambda|$ satisfying:

- $\sigma := \rho \cup (\lambda^{-1})$ is a partial injective function; and
- $(\forall i < n)(\forall (x_1, \ldots, x_k) \in (\mathsf{dom}(\sigma))^{\mathsf{arity}(R_i)})$

$$\mathcal{S} \models R_i(x_1, \dots, x_k) \iff \mathcal{S} \models R_i(\sigma(x_1), \dots, \sigma(x_k)).$$

In general $T_{\operatorname{Aut}(\mathcal{S})}$ is an infinite-branching computable subtree of $\omega^{<\omega}$, with terminal nodes, whose paths are in bijection with the elements of $\operatorname{Aut}(\mathcal{S})$. For a path P, the corresponding automorphism is

$$f = \{(n, \rho(n)) : (\exists \tau) (\rho \oplus \tau) \in P\} \in Aut(S).$$

We can compute composition and inversion on these automorphisms.

Examples

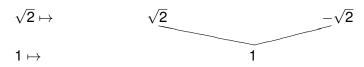
•
$$S = (\mathbb{Q}, <)$$
.

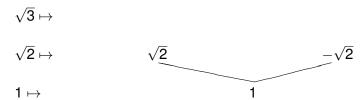
Examples

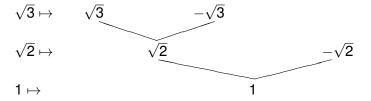
- $S = (\mathbb{Q}, <)$.
- $S = (\mathbb{Z}, <)$.

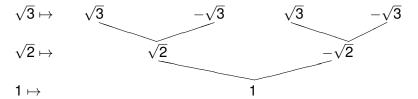
Examples

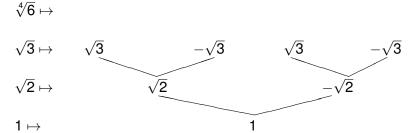
- $S = (\mathbb{Q}, <)$.
- $S = (\mathbb{Z}, <)$.
- $S = Gal(\overline{\mathbb{Q}}/\mathbb{Q}) = Aut(\overline{\mathbb{Q}})$, the absolute Galois group of the field \mathbb{Q} .
- Other Galois groups!

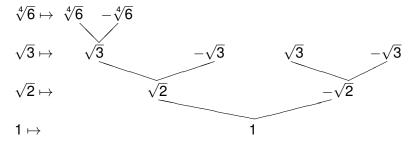


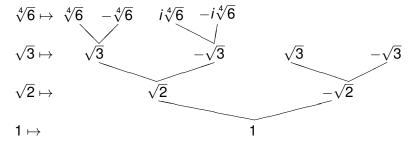


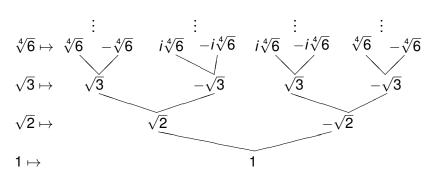












It is even cleaner to replace $\sqrt[4]{6}$ by a primitive generator of the Galois extension generated by $\sqrt{2}$, $\sqrt{3}$, and $\sqrt[4]{6}$. Then that level lists each automorphism of that Galois extension exactly once.

Comparing these examples

In these examples, $T_{Aut(S)}$ can be presented with no terminal nodes.

Proposition

The full orbit relation

$$\{(\overline{a}; \overline{b}) \in \cup_n(S^n \times S^n) : (\exists f \in Aut(S)) \ f(\overline{a}) = \overline{b}\}$$

is decidable if and only if there is a computable tree presentation of $\operatorname{Aut}(\mathcal{S})$ without terminal nodes.

Comparing these examples

In these examples, $T_{Aut(S)}$ can be presented with no terminal nodes.

Proposition

The full orbit relation

$$\{(\overline{a}; \overline{b}) \in \cup_n (\mathcal{S}^n \times \mathcal{S}^n) : (\exists f \in \mathsf{Aut}(\mathcal{S})) \ f(\overline{a}) = \overline{b}\}$$

is decidable if and only if there is a computable tree presentation of Aut(S) without terminal nodes.

- If $T_{Aut(S)}$ is finite-branching, then S is an algebraic structure, in the model-theoretic sense: every orbit is finite.
- For algebraic computable structures \mathcal{S} , the size of the orbits of all tuples \overline{a} is computable (uniformly in \overline{a}) if and only if $T_{\operatorname{Aut}(\mathcal{S})}$ has computable branching and no terminal nodes.

Finite non-computable branching

For an example where $\mathcal S$ is algebraic but $T_{\operatorname{Aut}(\mathcal S)}$ does not have computable branching, consider $\operatorname{Gal}(\overline F/F)=\operatorname{Aut}(\overline F_F)$ for a computable field F that has no splitting algorithm. Here $\mathcal S=\overline F_F$, the algebraically closed field $\overline F$ with constants for elements of F.

 \overline{F} contains three elements θ_0 , θ_1 , θ_2 such that all $\theta_i^3 = 2$. If $X^3 - 2$ is irreducible in F[X], then all six permutations of these roots occur in $Gal(\overline{F}/F)$. But if $X^3 - 2$ factors in F[X], then at least one θ_i is the only element of its orbit. A *splitting algorithm for F* is a decision procedure deciding irreducibility in F[X]. But not all computable fields have splitting algorithms!

If $T_{\operatorname{Aut}(\mathcal{S})}$ had computable finite branching, then F would necessarily have a splitting algorithm. Therefore, for our field F, this $T_{\operatorname{Aut}(\mathcal{S})}$ cannot have computable branching.

Finally, a formal definition

For a tree T, write [T] for the set of all paths through T.

Definition

For a structure \mathfrak{M} , in a signature \mathcal{L} with only function symbols f_i , a **d**-computable tree presentation of \mathfrak{M} consists of a **d**-computable subtree T of $\omega^{<\omega}$ and, for each f_i , a Turing functional Ψ_i such that:

- for every i (with f_i of arity m) and every tuple $(f_1, \ldots, f_m) \in [T]^m$ $\Psi_i^{\vec{f}} : \omega \to \omega$ is a total function lying in [T]; and
- there is a bijection $G: [T] \to \mathfrak{M}$ which is an \mathcal{L} -isomorphism from the \mathcal{L} -structure $([T], \Psi_1, \Psi_2, \ldots)$ onto \mathfrak{M} .

If \mathcal{L} has also constant symbols c_i , then each one is represented by a path $G^{-1}(c_i^{\mathfrak{M}}) \in [T]$. In this case **d**-computability requires that these paths be **d**-computable uniformly in *i*.

Finally, a formal definition

For a tree T, write [T] for the set of all paths through T.

Definition

For a structure \mathfrak{M} , in a signature \mathcal{L} with only function symbols f_i , a **d**-computable tree presentation of \mathfrak{M} consists of a **d**-computable subtree T of $\omega^{<\omega}$ and, for each f_i , a Turing functional Ψ_i such that:

- for every i (with f_i of arity m) and every tuple $(f_1, \ldots, f_m) \in [T]^m$ $\Psi_i^{\vec{f}} : \omega \to \omega$ is a total function lying in [T]; and
- there is a bijection $G: [T] \to \mathfrak{M}$ which is an \mathcal{L} -isomorphism from the \mathcal{L} -structure $([T], \Psi_1, \Psi_2, \ldots)$ onto \mathfrak{M} .

If \mathcal{L} has also constant symbols c_i , then each one is represented by a path $G^{-1}(c_i^{\mathfrak{M}}) \in [T]$. In this case **d**-computability requires that these paths be **d**-computable uniformly in *i*.

Question: what about relation symbols?

Relations as definable subsets of [T]

Notice that in a computable tree presentation of \mathfrak{M} , even equality on $[T]^2$ will in general only be Π_1^0 : f = g iff $(\forall n) f(n) = g(n)$.

Notice that we are discussing sets of reals, from ω^{ω} . Saying that a (binary) relation R is Π_1^0 means that there exists a functional Φ such that, for every $f,g\in [T]$,

$$(f,g)\in R\iff \Phi^{f\oplus g}(0)\uparrow.$$

For equality, $\Phi^{f \oplus g}(0)$ merely tests, for n = 0, 1, 2, ..., whether f(n) = g(n), and halts as soon as it finds an n with $f(n) \neq g(n)$.

Relations as definable subsets of [T]

Notice that in a computable tree presentation of \mathfrak{M} , even equality on $[T]^2$ will in general only be Π_1^0 : f = g iff $(\forall n) f(n) = g(n)$.

Notice that we are discussing sets of reals, from ω^{ω} . Saying that a (binary) relation R is Π^0_1 means that there exists a functional Φ such that, for every $f,g\in [T]$,

$$(f,g)\in R\iff \Phi^{f\oplus g}(0)\uparrow.$$

For equality, $\Phi^{f \oplus g}(0)$ merely tests, for n = 0, 1, 2, ..., whether f(n) = g(n), and halts as soon as it finds an n with $f(n) \neq g(n)$.

In a group, having finite order is Σ_2^0 . Let $\Psi^f(k,n)\downarrow$ iff $(f^k)\upharpoonright n\neq id\upharpoonright n$. Then

$$f$$
 is torsion $\iff (\exists k \forall n \forall s) \Psi_s^f(k, n) \uparrow$.

Relation symbols

In this context, the natural way to define decidability, for a subset $R \subseteq [T]^n$, is to say that R is both Σ_1^0 and Π_1^0 :

$$\exists \Phi \exists \Psi \ [R = \{\vec{f} \in [T]^n : \Phi^{\vec{f}}(0)\downarrow\} = \{\vec{f} \in [T]^n : \Psi^{\vec{f}}(0)\uparrow\}].$$

This makes R a clopen subset of $[T]^n$. In many cases – e.g., Galois groups, or other finite-branching-presentable \mathfrak{M} – this means that R is determined by some finite level of the tree. Such relations are BORING, not to mention uncommon. (Try to find a first-order definition in \mathcal{L} of a proper nonempty decidable relation!)

Relation symbols

In this context, the natural way to define decidability, for a subset $R \subseteq [T]^n$, is to say that R is both Σ_1^0 and Π_1^0 :

$$\exists \Phi \exists \Psi \ [R = \{\vec{f} \in [T]^n : \Phi^{\vec{f}}(0)\downarrow\} = \{\vec{f} \in [T]^n : \Psi^{\vec{f}}(0)\uparrow\}].$$

This makes R a clopen subset of $[T]^n$. In many cases – e.g., Galois groups, or other finite-branching-presentable \mathfrak{M} – this means that R is determined by some finite level of the tree. Such relations are BORING, not to mention uncommon. (Try to find a first-order definition in \mathcal{L} of a proper nonempty decidable relation!)

For the moment, we leave aside the question of tree presentations in signatures with relation symbols.

Quotient tree presentations

Consider the following subtree of $\mathbb{Q}^{<\omega}$:

$$T = \left\{ \sigma \in \mathbb{Q}^{<\omega} : (\forall j < k < |\sigma|) |q_j - q_k| < \frac{1}{2^j} \right\}.$$

[T] consists of

Quotient tree presentations

Consider the following subtree of $\mathbb{Q}^{<\omega}$:

$$T = \left\{ \sigma \in \mathbb{Q}^{<\omega} : (\forall j < k < |\sigma|) |q_j - q_k| < \frac{1}{2^j} \right\}.$$

[T] consists of precisely the fast-converging Cauchy sequences of rational numbers! Each $(q_0, q_1, q_2, \ldots) \in [T]$ has $(\forall j) |q_j - \lim_k q_k| \leq \frac{1}{2^j}$.

Quotient tree presentations

Consider the following subtree of $\mathbb{Q}^{<\omega}$:

$$T = \left\{ \sigma \in \mathbb{Q}^{<\omega} : (\forall j < k < |\sigma|) |q_j - q_k| < \frac{1}{2^j} \right\}.$$

[T] consists of

precisely the fast-converging Cauchy sequences of rational numbers! Each $(q_0, q_1, q_2, ...) \in [T]$ has $(\forall j) |q_j - \lim_k q_k| \le \frac{1}{2^j}$.

So we can give a *tree quotient presentation* of the field \mathbb{R} , using this T. +, \cdot , and - are all computable on FC Cauchy sequences, and \div is a Π_1^0 relation. Moreover, equality, which is now defined by

$$(q_0, q_1, \ldots) \sim (r_0, r_1, \ldots) \iff \lim_k q_k = \lim_k r_k,$$

is also Π_1^0 . So this computable quotient tree presentation has the same complexity as an ordinary computable tree presentation!

Other tree-presentable structures

The *p*-adic integers \mathbb{Z}_p are the sequences $(n_1, n_2, n_3, \ldots) \in \mathbb{Z}^{\omega}$ satisfying

$$(\forall j)(\forall k>j) \ n_j\equiv n_k \ \mathsf{mod} \ p^j.$$

Example: the following sequence lies in Z_{10} :

For standard form, one chooses each $n_k \in \{0,1,\ldots,p^k-1\}$. With this form, these are very obviously the paths through a computable subtree T_p of $\omega^{<\omega}$. This T_p has finite computable branching and no terminal nodes, and the ring operations on \mathbb{Z}_p are computable by Turing functionals on the paths, so we have a computable tree presentation of the ring \mathbb{Z}_p .

Why the group \mathbb{Z}_p^+ is nice

A formula in the additive group \mathbb{Z}_p^+ , say $(\exists G)$ $a_1F_1 + a_2F_2 = bG$ (with $a_1, a_2, b \in \mathbb{Z}$), may be satisfiable for some parameters \vec{f} and not for others. Two questions arise:

- What is the complexity (as a set of reals) of the set $\{\vec{F} \in (\mathbb{Z}_p^+)^2 : (\exists G) \ a_1F_1 + a_2F_2 = bG\}$ it defines?
- ② For those \vec{f} for which the formula holds, can we compute (uniformly in \vec{f}) an instantiation $g \in \mathbb{Z}_p^+$?

Why the group \mathbb{Z}_p^+ is nice

A formula in the additive group \mathbb{Z}_p^+ , say $(\exists G)$ $a_1F_1 + a_2F_2 = bG$ (with $a_1, a_2, b \in \mathbb{Z}$), may be satisfiable for some parameters \vec{f} and not for others. Two questions arise:

- What is the complexity (as a set of reals) of the set $\{\vec{F} \in (\mathbb{Z}_p^+)^2 : (\exists G) \ a_1F_1 + a_2F_2 = bG\}$ it defines?
- ② For those \vec{f} for which the formula holds, can we compute (uniformly in \vec{f}) an instantiation $g \in \mathbb{Z}_p^+$?

For \mathbb{Z}_p^+ , the set defined by this formula is decidable, provided $b \neq 0$. If p^e is the greatest power of p dividing b, one need only examine \vec{f} up to the (e+1)-st term. (If b=0 and $a_1a_2 \neq 0$, the set $\{(f_1,f_2): (\exists G) \ a_1f_1 + a_2f_2 = 0 \cdot G\}$ is Π_1^0 but undecidable!)

When the formula does hold (and $b \neq 0$), the witness is unique and can be computed uniformly in \vec{f} . We say that in \mathbb{Z}_p^+ this formula has a computable Skolem function.

Bounds on the computability of Skolem functions

We claim that no Φ computes a Skolem function for this formula:

$$(\exists G)[(F_0=G \land F_1=G) \lor (F_2=G \land F_3 \neq G)].$$

Bounds on the computability of Skolem functions

We claim that no Φ computes a Skolem function for this formula:

$$(\exists G)[(F_0=G \land F_1=G) \lor (F_2=G \land F_3 \neq G)].$$

Proof: Given Φ , run it on the tuple (h_0, h_0, h_1, h_1) , where $h_0(n) \neq h_1(n)$ (for some n). The formula holds for these parameters, with unique witness h_0 , so for some use u, $\Phi^{(h_0 \oplus h_0 \oplus h_1 \oplus h_1)|u}(n) = h_0(n)$. Now choose $h'_0 \neq h_0$ and $h'_1 \neq h_1$, but with $h_i \upharpoonright u = h'_i \upharpoonright u$. Thus

$$\Phi^{(h_0 \oplus h'_0 \oplus h_1 \oplus h'_1)|u}(n) = \Phi^{(h_0 \oplus h_0 \oplus h_1 \oplus h_1)|u}(n) = h_0(n).$$

However, now the unique witness (for the tuple (h_0, h'_0, h_1, h'_1) is h_1 , and $h_1(n) \neq h_0(n) = \Phi^{(h_0 \oplus h'_0 \oplus h_1 \oplus h'_1)|u|}(n)$. So Φ failed on this tuple.

(All that was necessary here was the existence of two distinct elements $h_0 \neq h_1 \in \mathfrak{M}$ whose paths are non-isolated in [T].)

More non-computable Skolem functions

Theorem (Kundu-M.)

In each computable tree presentation of $Gal(\mathbb{Q})$, the formula $(\exists G) \ G \circ G = F$ has no computable Skolem function.

Proof sketch: We know that the identity map $f \in \operatorname{Gal}(\mathbb{Q})$ Given any Turing functional Φ , run Φ^{id} . If $\Phi^{\operatorname{id}|\mathcal{K}_n}(i)\!\downarrow = \pm i$ for some n, Kundu-M. have a mechanism yielding $f_0, f_1 \in \operatorname{Aut}(\overline{\mathbb{Q}})$ with

- $f_0, f_1 \in (\operatorname{Aut}(\overline{\mathbb{Q}}))^2$ with $f_0 \upharpoonright K_n = f_1 \upharpoonright K_n = \operatorname{id} \upharpoonright K_n$.
- Every $g_0 \in \operatorname{Aut}(\overline{\mathbb{Q}})$ with $g_0 \circ g_0 = f_0$ has $g_0(i) = i$.
- Every $g_1 \in \operatorname{Aut}(\overline{\mathbb{Q}})$ with $g_1 \circ g_1 = f_1$ has $g_1(i) = -i$.

So either $\Phi^{f_0}(i)$ or $\Phi^{f_1}(i)$ will be incorrect!

More non-computable Skolem functions

Theorem (Kundu-M.)

In each computable tree presentation of $Gal(\mathbb{Q})$, the formula $(\exists G) \ G \circ G = F$ has no computable Skolem function.

Proof sketch: We know that the identity map $f \in \operatorname{Gal}(\mathbb{Q})$ Given any Turing functional Φ , run Φ^{id} . If $\Phi^{\operatorname{id}|K_n}(i)\!\downarrow = \pm i$ for some n, Kundu-M. have a mechanism yielding $f_0, f_1 \in \operatorname{Aut}(\overline{\mathbb{Q}})$ with

- $f_0, f_1 \in (\operatorname{Aut}(\overline{\mathbb{Q}}))^2$ with $f_0 \upharpoonright K_n = f_1 \upharpoonright K_n = \operatorname{id} \upharpoonright K_n$.
- Every $g_0 \in \operatorname{Aut}(\overline{\mathbb{Q}})$ with $g_0 \circ g_0 = f_0$ has $g_0(i) = i$.
- Every $g_1 \in \operatorname{Aut}(\overline{\mathbb{Q}})$ with $g_1 \circ g_1 = f_1$ has $g_1(i) = -i$.

So either $\Phi^{f_0}(i)$ or $\Phi^{f_1}(i)$ will be incorrect!

In contrast, when C is the cyclotomic field, $\operatorname{Gal}(C/\mathbb{Q})$ has computable Skolem functions for every formula $(\exists \vec{G})\alpha(\vec{F}, \vec{G})$ in which α is a conjunction of literals. (Conjecture: likewise for $\exists \vec{G} \forall \vec{H} \alpha(\vec{F}, \vec{G}, \vec{H})$!)

Atomic and negated-atomic formulas in $Gal(C/\mathbb{Q})$

The procedure described above, computing Skolem functions, needs to handle $\exists G\alpha(\vec{F},G)$, where α is a conjunction of *literals*. Simple atomic formulas in functional languages are always equations, and it is Π^0_1 (in \vec{F} and G) for an equation in those variables to hold. Consequently, it is Σ^0_1 for an inequation to hold: $\sum a_i f_i \neq bg$ iff there is some level m in the tree at which $\sum a_i \cdot f_i(m) \neq b \cdot g(m)$. Once such an I appears, the inequation is guaranteed to hold in \mathfrak{M} . Equations define Π^0_1 classes (i.e., closed sets), while inequations define open sets.

Therefore, to compute some g realizing $\mathfrak{M} \models \alpha(\vec{f},g)$, we search at each level m for a node γ that makes all the inequations hold: $\sum a_i \cdot f_i(m) \neq b \cdot \gamma$. When we find one, it becomes possible to set $g(m) = \gamma$ and compute g from the equations in α . If we never find one, then $\mathfrak{M} \not\models \exists G \ \alpha(\vec{f},G)$.

More computably-tree-presentable structures

The groups \mathbb{Z}_p^+ and \mathbb{Z}_p^x arose since $Gal(C/\mathbb{Q}) \cong \prod_{\text{all primes } p} (\mathbb{Z}_p)^x$. Computing Skolem functions as above in \mathbb{Z}_p^+ , uniformly for all primes

p, enables us to do the same for $Gal(C/\mathbb{Q})$. The integral domain \mathbb{Z}_p has a computable tree presentation, built just

The integral domain \mathbb{Z}_p has a computable tree presentation, built just like those for the groups \mathbb{Z}_p^+ and \mathbb{Z}_p^\times . We have not yet studied Skolem functions for this ring. Nerode proved in 1963 that $\text{Th}(\mathbb{Z}_p)$ is decidable.

 \mathbb{Q}_p is the quotient field of \mathbb{Z}_p . Can we give a tree presentation of it? The usual approach uses $\mathbb{Z}_p \times (\mathbb{Z}_p - \{0\})$, with $(a,b) \sim (c,d)$ just if $a \cdot d = b \cdot c$. We can handle this by splicing together two copies of the tree for \mathbb{Z}_p and giving a quotient presentation. But how to ensure that the denominator is nonzero?

Back to the question of relations

The undecidability of equality is inherent in all presentations of continuum-sized structures under Turing computability. We saw above that, stemming from the undecidability of equality, all interesting atomic formulas with parameters will likewise be undecidable, even though more complex formulas with parameters may be decidable. Is there a resolution of this oddity?

Possible solution

Working definition (possibly to be refined)

A fully computable tree presentation of an \mathcal{L} -structure \mathfrak{M} consists of a computable tree presentation T of the reduct of \mathfrak{M} to the nonrelational symbols of \mathcal{L} , along with a Turing functional Θ such that, for every atomic formula $\alpha(F_1,\ldots,F_n)$ from \mathcal{L} , every $\vec{f}\in[T]^n$, and every enumeration E of the (positive) atomic diagram of the substructure $\mathfrak{M}_{\vec{f}}\subseteq\mathfrak{M}$ generated by \vec{f} ,

$$\Theta^{\vec{f} \oplus E}(\lceil \alpha \rceil) \downarrow = \begin{cases} 1, & \text{if } \mathfrak{M} \models \alpha(\vec{f}); \\ 0, & \text{if } \mathfrak{M} \models \neg \alpha(\vec{f}). \end{cases}$$

For example, if $x, y \in \mathbb{R}$, we can decide the truth of all atomic formulas involving them, given the paths of x and y (i.e., Cauchy sequences converging fast to each) and an enumeration of those polynomials $f \in \mathbb{Q}[X, Y]$ (if any!) for which f(x, y) = 0.

Elementary substructures

In a computable tree presentation T of \mathfrak{M} , for each Turing degree \boldsymbol{d} , we have a substructure

$$\mathfrak{M}_{\boldsymbol{d}} = \{ f \in [T] : \deg(f) \leq_{T} \boldsymbol{d} \}.$$

Indeed, this holds for quotient tree presentations as well, and also with an arbtrary Turing ideal I in place of the lower cone below d. If T has no dead ends, then even \mathfrak{M}_0 will be dense in [T].

Question

In what situations will \mathfrak{M}_I be an elementary substructure of \mathfrak{M} ? Or at least, elementary for certain classes of formulas (existential, $\exists \forall$, etc.)?

Examples do exist. Indeed, \mathbb{R}_0 , the field of all computable real numbers, is itself a real closed field and hence an elementary subfield of \mathbb{R} . We also know that $(\mathbb{Z}_p^+)_0$ is elementary for existential formulas (and probably more) within \mathbb{Z}_p^+ .