The Complexity of Classifications and Descriptions

Matthew Harrison-Trainor

Victoria University of Wellington

Maltsev Meeting 2019

In 2002, S. Goncharov and J. Knight published the paper *Computable Structure and Non-Structure Theorems* in *Algebra and Logic*.

It introduced into computable structure theory a systematic framework for analysing classification and characterization problems.

This talk will introduce the general framework and then we will explain a variety of different recent results using this framework.

Often in mathematics we have some property P that we are interested in. We want to characterize P by showing that it is equivalent to some simpler property Q. For example, you might think of P as being the property of vector spaces of being isomorphic, and Q as having the same dimension.

If we have a characterization Q of P, how do we know whether Q is the simplest possible characterization? Or if we cannot find a characterization, can we show that there is no possible characterization?

These are the sorts of questions that the methods in this talk will allow us to answer.

Outline

1. General framework
2. Applications to group theory
3. Applications to decidability and presentations of structures

Outline

1. General framework
2. Applications to group theory
3. Applications to decidability and presentations of structures

Fix your favourite programming language (e.g. C, Java, Assembly, Haskell, ...).

A function $f : \mathbb{N}^n \to \mathbb{N}^m$ is computable if there is a computer program that on input $\bar{a}$ computes $f(\bar{a})$.

A relation $R \subseteq \mathbb{N}^n$ is computable if there is a computer program that on input $\bar{a}$ outputs 1 if $\bar{a} \in R$ and 0 otherwise.

A computable structure is a structure with domain $\mathbb{N}$ with various (uniformly) computable functions, relations, and constants on $\mathbb{N}$.

For example, a computable group is a group with domain $\mathbb{N}$ and whose group operation is a computable function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Using a universal Turing machine, we can make a computale list $(\mathcal{A}_i)_{i \in \mathbb{N}}$ of all of the computable structures in a given language. Essentially, $\mathcal{A}_i$ takes the ith computer program and tries to interpret it as a structure. Some of the $\mathcal{A}_i$ might be partial because the ith computer program does not halt on certain inputs.

Given a property P, define the index set of the computable structures with property P:

$$I_P := \{i : \mathcal{A}_i \text{ has property } P\}.$$

The idea is to measure the complexity of property P by measuring the computational complexity of the index set I_P.

We use complexity classes from the arithemetic, (hyperarithemtic), and projective hierarchies. We make comparisons using many-one reductions.

If you are unfamiliar with these, but familiar with computational complexity theory, this is analogous to complexity classes such as P, NP, and $EXPTIME$ and polynomial-time reductions.

Definition

$A \leq_m B$ (A is many-one reducible to B) if there is a computable function f such that

$$n \in A \iff f(n) \in B.$$

We can decide membership in A using membership in B; so A is simpler than B.

The arithmetical sets are those which can be expressed using quantification only over $\mathbb{N}$ (e.g., over elements of the structures). These are divided into a hierarchy based on the alternations of quantifiers:

- a set is Σ_n^0 if it is definable using n alternating quantifiers, starting with an existential quantifier;
- a set is Π_n^0 if it is definable using n alternating quantifiers, starting with a universal quantifier.

We can use multiples of the same quantifier in a row, counting only as one quantifier. For example, a set defined by

$$\exists x \exists y \ \forall a \ \exists b \ \ R(\cdots, x, y, a, b)$$

where R does not involve any quantifiers is Σ_3.

A relation is Σ^1_1 if it is definable using only existential quantifiers over sets and functions, and any quantifiers over natural numbers.

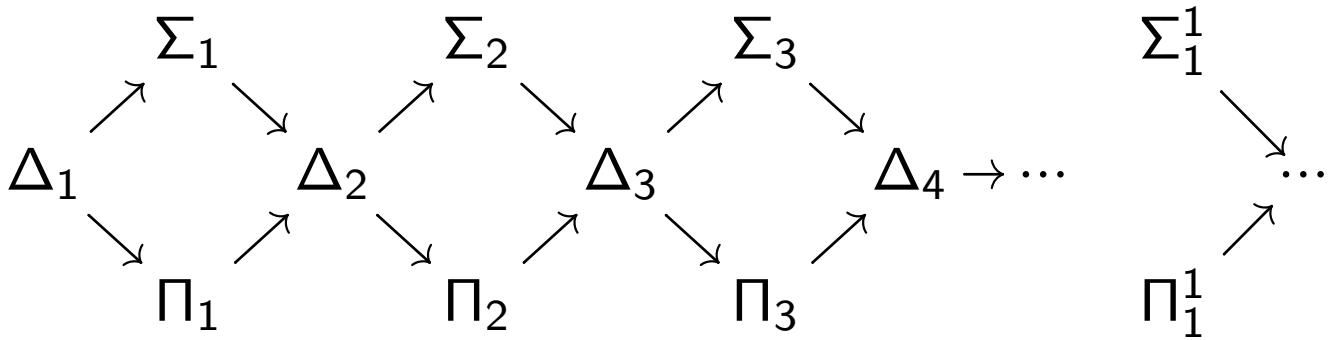
A relation is Π^1_1 if it is definable using only universal quantifiers over sets and functions, and any quantifiers over natural numbers.

For example, a group G is free if and only if there exists a set $B \subseteq G$ that generates G such that there are no non-trivial relations on B and every element of G is generated by elements of B. So

$$I_{free} = \{i : \mathcal{G}_i \text{ is a free group}\}$$

is Σ^1_1. But it might be (and it is) simpler!

The hierarchy we have defined is proper. It consists of more classes than the ones we have defined, but these are all that we will need.



Let Γ be one complexity classes just defined. Let $A \subseteq \mathbb{N}^n$.

Definition

A is Γ-complete if

- $A \in \Gamma$, and
- whenever $B \in \Gamma$, $B \leq_m A$.

If A is Γ-complete, then A is as complicated as possible for a set in Γ.

In practice, usually what we do to show that A is Γ-complete is to take a known set B that is Γ-complete, and show that $B \leq_m A$. This implies that A is Γ-complete.

We have easy-to-work-with examples of complete sets at many levels.

We will employ the following general strategy for a particular property P:

1. Give a characterization C for P which shows that I_P is in Γ.
2. Prove that I_P is Γ-complete.

This will show that C is the simplest possible characterization for P; indeed, if there was a simpler characterization, then I_P would have a lower complexity than Γ, and so could not be Γ-complete.

It is particularly good when we can apply these techniques to a question that has already been asked in another area of mathematics.

Let $\mathbb{C}$ be a class of structures. Let

$$I_{\mathbb{C}} = \{(i,j) : \mathcal{A}_i, \mathcal{A}_j \in \mathbb{C} \text{ and } \mathcal{A}_i \cong \mathcal{A}_j\}$$

We call $I_{\mathbb{C}}$ the isomorphism problem for $\mathbb{C}$.

We can do the same analysis here to determine how hard it is to tell whether or not two structures in $\mathbb{C}$ are isomorphic.

Outline

1. General framework
2. Applications to group theory
3. Applications to decidability and presentations of structures

Until otherwise mentioned, all groups are abelian. Two groups $G = (\omega, +_G)$ and $H = (\omega, +_G)$ are isomorphic if and only if there exists a function $f : \omega \to \omega$ satisfying

- for all $x, y \in \omega$, if $f(x) = f(y)$ then $x = y$;
- for all $y \in \omega$, there is $x \in \omega$ such that $f(x) = y$;
- for all $x, y \in \omega$, $f(x) +_H f(y) = f(x +_G y)$.

So letting $\mathcal{A}_i$ be an effective list of the abelian groups,

$$I_{AGroup} = \{(i, j) : \mathcal{A}_i \cong \mathcal{A}_j\}$$

is Σ^1_1.

Theorem (Downey, Montalbán)

I_{AGroup} is Σ^1_1-complete.

Theorem (Walker, Cohn)

If $\mathbb{Z} \oplus G \cong \mathbb{Z} \oplus H$, *then* $G \cong H$.

Definition

We say that A has the cancelation property if whenever $A \oplus G \cong A \oplus H$, $G \cong H$.

Example

$\mathbb{Q}$ has the cancellation property.

The dyadic rationals do not have the cancellation property.

$\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$ does not have the cancellation property.

Theorem (Fuchs-Loonstra)

Let G be a rank 1 torsion-free abelian group. Then G has the cancellation property if and only if $G \cong \mathbb{Z}$ or $E(G)$ has 1 is in the stable range:

> *whenever $f_1, f_2, g_1, g_2 \in E(G)$ satisfy $f_1 g_1 + f_2 g_2 = 1$, there is $h \in E(G)$ such that $f_1 + f_2 h$ is a unit of $E(G)$.*

Estes and Ohm: "the problem of a complete classification of overrings of $\mathbb{Z}$ having 1 in the stable range remains open".

Arnold: "rings with 1 in the stable range are not easily characterized".

Theorem (Fuchs-Loonstra)

Let G be a rank 1 torsion-free abelian group. Then G has the cancellation property if and only if $G \cong \mathbb{Z}$ or $E(G)$ has 1 is in the stable range:

> *whenever $f_1, f_2, g_1, g_2 \in E(G)$ satisfy $f_1 g_1 + f_2 g_2 = 1$, there is $h \in E(G)$ such that $f_1 + f_2 h$ is a unit of $E(G)$.*

Each endomorphism f of G can be identified with $f(1) \in G$.

The characterization can then be expressed in $\mathcal{L}_{\omega_1\omega}$, and the complexity of the resulting sentence is Π_4.

Estes and Ohm: "the problem of a complete classification of overrings of $\mathbb{Z}$ having 1 in the stable range remains open".

Arnold: "rings with 1 in the stable range are not easily characterized".

Theorem (HT-Ho)

The index set of rank 1 torsion-free abelian groups with the cancellation property is Π^0_4*-complete.*

What about arbitrary groups (not of rank 1)?

Let

$$I_{canc} = \{\mathcal{G}_i : \mathcal{G}_i \text{ has the cancellation property.}$$

We actually have no upper bound on I_{canc} (other than Π_2 in V).

For example, we do not know that if a group G cancels with every countable group, then it cancels with every group. If this was the case, then the index set would be Π^1_2.

The best result we have is:

Theorem (HT-Ho)

The index set I_{canc} is Σ^1_1-hard.

What this means is that for every Σ^1_1 set A, $A \leq_m I_{canc}$, but it might not be that I_{canc} itself is Σ^1_1.

Theorem (HT-Ho)

The index set I_{canc} is Σ^1_1-hard.

It is true for all groups $\mathcal{G}$ of any rank that having 1 in the stable range of $E(\mathcal{G})$ implies the cancellation proerty.

The proof uses this fact together with the fact that a group of the form

$$G \cong H \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$$

does not have the cancellation property, as

$$G \oplus \mathbb{Z} = G \oplus \{e\}.$$

Given a Σ^1_1 set A, we build a computable function f such that if $n \in A$, then $\mathcal{G}_{f(n)}$ is of this form (hence not cancellable), and if $n \notin A$, then $\mathcal{G}_{f(n)}$ has 1 in the stabel range (and hence is cancellable).

The technique we used came from a result of Riggs.

Definition

A group G is decomposable if it can be written non-trivially as $G = A \oplus B$.

This is Σ^1_1.

Theorem (Riggs)

I_{decomp} is Σ^1_1-complete.

We now consider non-abelian groups. Let

$$I_{free} = \{i : \mathcal{G}_i \text{ is a free group}\}.$$

This is, on the face of it, Σ^1_1: $\mathcal{G}$ is free if and only if there is a set $B \subseteq \mathcal{G}$ such that there is no non-trivial relation among the elements of B, and B generates all of $\mathcal{G}$.

However, Nielson transformations yield a better understanding of when a group is free.

Theorem (CHKLMMMQW, McCoy-Wallbaum)

The set I_{free} is Π^0_4-complete.

Outline

1. General framework
2. Applications to group theory
3. Applications to decidability and presentations of structures

Recall that the atomic diagram of a structure $\mathcal{A}$ is

$$D_{at}(\mathcal{A}) = \{(\bar{a}, \varphi) : \varphi \text{ is quantifier-free and } \mathcal{A} \vDash \varphi(\bar{a})\}.$$

The elementary diagram of $\mathcal{A}$ is

$$D_{el}(\mathcal{A}) = \{(\bar{a}, \varphi) : \varphi \text{ is quantifier-free and } \mathcal{A} \vDash \varphi(\bar{a})\}.$$

Definition (Chubb, R. Miller, Solomon)

An elementary first-order theory T is relatively decidable if for every $\mathcal{A} \vDash T$,

$$D_{at}(\mathcal{A}) \geq D_{el}(\mathcal{A}).$$

Which theories T are relatively decidable?

Theorem (Definition / Theorem)

T is model complete if and only if for every formula φ, there is an existential formula θ such that

$$T \vDash \varphi \longleftrightarrow \theta.$$

If T is decidable and model complete, then T is relatively decidable. Let $\mathcal{A} \vDash T$. We show how to compute $D_{el}(\mathcal{A})$ using $D_{at}(\mathcal{A})$. Given a formula φ and $\bar{a} \in \mathcal{A}$, we want to decide whether $\mathcal{A} \vDash \varphi(\bar{a})$. Find an existential formulas $\exists \bar{x} \theta$ and $\exists \bar{y} \theta'$ such that

$$T \vDash \varphi \longleftrightarrow \exists \bar{x} \theta \qquad \text{and} \qquad T \vDash \neg\varphi \longleftrightarrow \exists \bar{y} \theta'.$$

We can search simultaneously to witnesses for both $\exists \bar{x} \theta(\bar{a}, \bar{x})$ and $\exists \bar{y} \theta'(\bar{a}, \bar{y})$. We will find witnesses for one of these, and thus decide whether $\mathcal{A} \vDash \varphi(\bar{a})$.

This idea generalizes:

Theorem (Chubb, R. Miller, Solomon)

Let T be a c.e. theory. Then T is relatively decidable if and only if for every $\mathcal{A} \models T$, there is $\bar{a} \in \mathcal{A}$ such that $Th(\mathcal{A}, \bar{a})$ is model complete.

This is a nice theorem, but we really want a characterization that talks only about the theory T, and not about tuples in models. For example, in the paper where this theorem was proved, the authors suggested that perhaps a characterization of the following form was possible:

Conjecture (Chubb, R. Miller, Solomon)

Let T be a complete decidable theory. Then T is relatively decidable if and only if there is a formula φ such that $T \models \exists \bar{x} \varphi(\bar{x})$ and $T \cup \{\varphi(\bar{c})\}$ is model complete, where $\bar{c}$ is a new set of constants.

Let $(T_i)_{i\in\mathbb{N}}$ list the complete decidable theories. Consider the index set

$$I_{rd} = \{T_i : T_i \text{ is relatively decidable.}\}.$$

This is clearly Π^1_1: T is relatively decidable if for every model $\mathcal{A} \vDash T$, there is a Turing reduction $D_{el}(\mathcal{A}) \leq_T D_{at}(\mathcal{A})$.

If the conjecture was true, then it would be Σ^0_3.

Theorem (HT)

I_{rd} is Π^1_1 complete.

Question (Goncharov)

Classify the structures which are isomorphic to a decidable structure.

Theorem (HT)

The index set

$$I_{decpres} = \{i : \mathcal{A}_i \text{ has a decidable presentation}\}$$

is Σ^1_1*-complete.*

Alexander Melnikov talked yesterday about primitive recursive structures. He stated the following theorem:

Theorem (Bazhenov, HT, Kalimullin, Melnikov, Ng)

The index set of structures with punctual (resp. polynomial-time, automatic) presentations is Σ^1_1*-complete.*

Since he talked about primitive recursive structures yesterday, we will focus on automatic structures today.

Automatic structures are defined using deterministic finite automata (DFA).

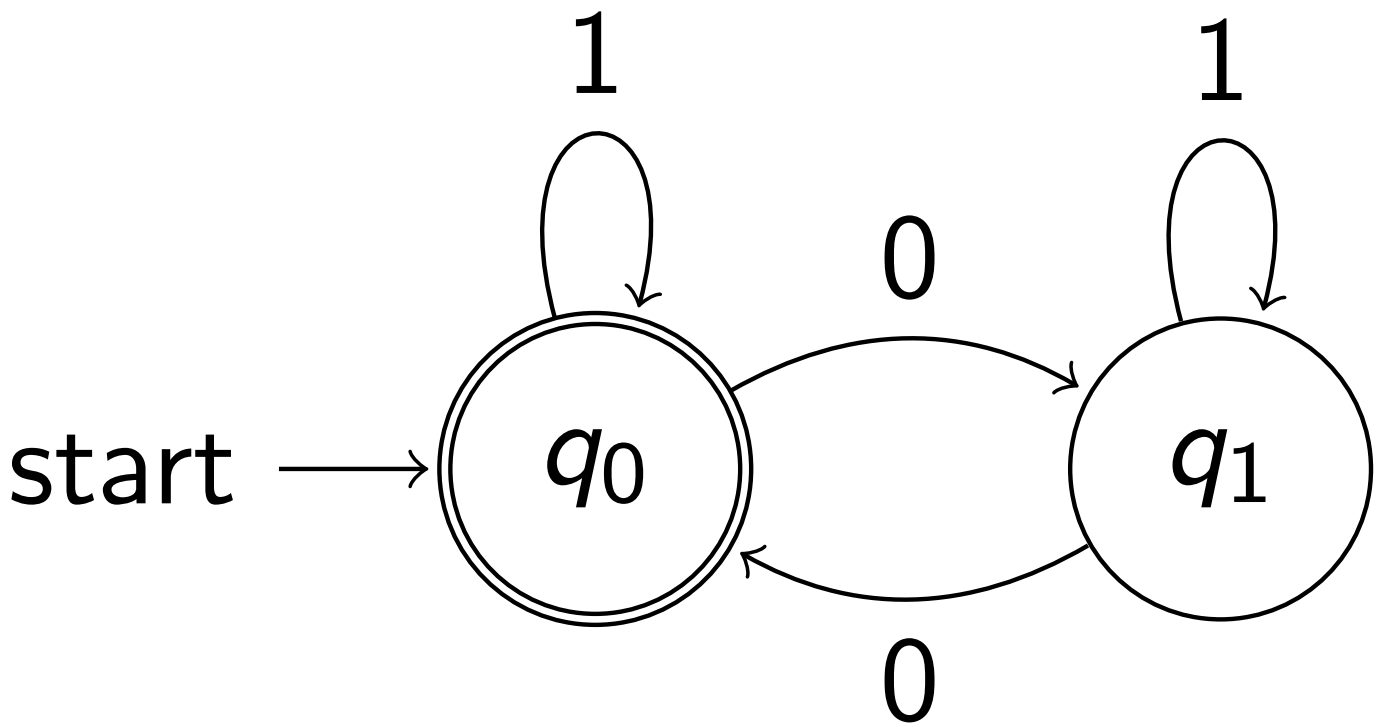
A DFA consists of:

- states Q,
- a language Σ,
- an initial state $q_0 \in Q$,
- accepting states $F \subseteq Q$,
- and a transition function $\delta : Q \times \Sigma \to Q$.

A DFA accepts a string $\sigma \in \Sigma^*$ if, reading σ and starting at q_0, it ends in an accepting state.

A subset $L \subseteq \Sigma^*$ is called regular if there is a DFA that accepts exactly L.

The set of strings with an even number of 0's is regular. Take $Q = \{q_0, q_1\}$, $\Sigma = \{0, 1\}$, and $F = \{q_0\}$. The transition function δ is defined as follows:



Given $x_1, \ldots, x_n \in \Sigma^*$, define the convolution $\mathrm{conv}(x_1, \ldots, x_n)$ to be the string

$$x_1(1), x_2(1), \ldots, x_n(1), x_1(2), x_2(2), \ldots$$

where $x_i = \langle x_i(1), x_i(2), \ldots \rangle$. Pad this with a new symbol $\diamond$ to even out the lengths.

Given a set $R \subseteq (\Sigma^*)^n$ define the convolution of R to be

$$\mathrm{conv}(R) = \{\mathrm{conv}(x_1, \ldots, x_n) : (x_1, \ldots, x_n) \in R\}.$$

R is called regular if the convolution of R is regular;

A structure $\mathcal{A} = (A, R_1, R_2, \ldots, R_n)$ is automatic if the domain is a regular language and each of the relations R_i is regular.

Presburger arithmetic is automatic presentable. Its automatic presentation $(\{0,1\}^*, 1, +, \leq\}$ uses binary representation, with the least significant bit first. The standard method of adding two numbers in binary uses a single carry bit and is thus automatic.

Theorem (Khoussainov, Nerode)

An automatic structure is decidable: There is an algorithm that, given an automatic structure $\mathcal{A}$, an elementary first-order formula $\varphi(\bar{x})$, and a tuple $\bar{a}$, decides whether $\mathcal{A} \models \varphi(\bar{a})$.

This can be very useful. For example, consider the game of infinite chess, played on an infinite board with finitely many pieces.

Theorem (Brumleve, Hamkins, Schlicht)

There is an algorithm to decide, for a given position in infinite chess, whether white achieves checkmate within n moves.

The proof is to present game tree as an automatic structure.

A fundamental question is:

Question (Khoussainov, Nerode)

How do we tell whether a given structure has an automatic presentation?

Theorem (Bazhenov, HT, Kalimullin, Melnikov, Ng)

The index set

$$I_{autpres} = \{i : \mathcal{A}_i \text{ has an automatic presentation}\}$$

is Σ^1_1*-complete.*

At the beginning of the talk, we asked: If we have a characterization Q of P, how do we know whether Q is the simplest possible characterization? Or if we cannot find a characterization, can we show that there is no possible characterization?

We have seen that index sets provide a formal framework for answering such questions and seen many examples of the method in action.