Objects of greatest complexity in their class

André Nies

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

Is there a most complex object in a class?

The following questions arises frequently in mathematics and theoretical computer science.

We are given a class of objects and a method to compare their complexity.

- Is there a most complex object in the class?
  If so, we call it a complete object for the class.
- What are the properties of a complete object?
- Is a complete object unique in some sense?

Two basic notions of computability

A function ψ defined on a subset of $\mathbb{N}$ is called partially computable if there is a Turing machine that

- with n as an input, outputs $\psi(n)$ if defined,
- and doesn't stop otherwise.

$n \longrightarrow$ [Turing machine M] $\longrightarrow \psi(n)$ if $\psi(n)$ defined

$A \subseteq \mathbb{N}$ is called computably enumerable (c.e.) if

$$A = \{n\colon\ M(n)\ \text{halts}\}\ \text{for a Turing machine}\ M.$$

The halting problem is m-complete for c.e. sets

Definition

Let $A, B \subseteq \mathbb{N}$.
$B \leq_m A$ if $\exists f\colon \mathbb{N} \to \mathbb{N}$ computable such that $n \in B \leftrightarrow f(n) \in A$.

$M_0, M_1, \ldots$ effective listing of all Turing machines.

$\mathcal{H} = \{\langle e, n\rangle \colon M_e(n) \text{ halts}\}$ is the halting problem.

Theorem (Complete object exists; Turing 1936, Post, 1944)

$\mathcal{H}$ is $\leq_m$-complete for the class of c.e. sets.

Theorem (Uniqueness of complete object, Myhill, 1955)

Let A and B be $\leq_m$-complete for the c.e. sets. Then there is a computable permutation ρ of $\mathbb{N}$ such that $\rho(A) = B$.

The satisfiability problem SAT is complete for NP

- In complexity theory one studies sets of words over a finite alphabet.
- SAT is the set of satisfiable Boolean formulas (encoded by words). E.g. $(x \vee \neg y) \wedge (\neg x \vee y) \wedge (x \vee z) \in \texttt{SAT}$.
- NP is the class of problems of the form

$$\{w \colon \exists u \, [\, M(w\#u) \text{ accepts}]\},$$

  for a Turing machine M that stops in polynomial time relative to $|w|$. ($\#$ is a separator symbol.)

Theorem (Cook 1971; Levin 1973)

SAT *is polynomial time* $\leq_m$*-complete for* NP.
Hence $P \neq NP$ *iff* $\texttt{SAT} \notin P$.

The Berman-Hartmanis conjecture (dating from 1976) asks whether all NP-complete problems A, B are polynomial time isomorphic: $A = \rho(B)$, where ρ and ρ^{-1} are in PTIME.

Motivation

Suppose we are given a preordering $\leq$ to compare the complexity of objects in the class $\mathcal{C}$.

Why are we interested in complete objects S for a class $\mathcal{C}$?

The answer depends on whether we focus on $\mathcal{C}$, or on S.

Focussing on the class $\mathcal{C}$

- The preordering is often (but not always) simple.
- Often it is "simpler" than the objects it is supposed to compare. Computable functions compare computably enumerable sets; polytime functions compare NP sets.
- Usually $\mathcal{C}$ is downward closed under $\leq$.
- So the single object S, together with the simple preordering $\leq$, describes the whole class $\mathcal{C}$.

L'etat, c'est moi

Focussing on the complete object S

- A complete object S for $\mathcal{C}$ can be expected to be interesting.
- Reflecting Tao and others, one can ask the question: is S structured, or random?
- The halting problem and SAT are structured. Chaitin's Ω and the Rado graph are random.

The complexity of an object S can be determined by proving that S is complete for the canonical class $\mathcal{C}$ of objects it belongs to.
(How is the randomness content of S related to $\mathcal{C}$?)

More recent example: Solovay completeness

Definition

$\alpha \in \mathbb{R}$ is called c.e. from the left if

$$\{q \in \mathbb{Q}\colon\ q < \alpha\}$$

is computably enumerable. Equivalent formulation: $\alpha = \sup_s p_s$ for an increasing computable sequence $\langle p_s \rangle_{s \in \mathbb{N}}$ of rationals.

Example: $\alpha = \sum_{n \in A} 2^{-n}$ for a c.e. set A.

Solovay reducibility

Definition (Solovay-reducibility)

$\beta \leq_S \alpha$ if $\beta = \sup_s q_s$ for a computable sequence of rationals such that $\beta - q_s = O(\alpha - p_s)$.

Theorem (Kučera and Slaman, 2001)

Let $\alpha \in [0, 1]$ be c.e. from the left. Then:

$$\alpha \text{ is } \leq_S\text{-complete} \Leftrightarrow \alpha \text{ is Martin-Löf random.}$$

Examples of $\leq_S$-complete reals:

- $\alpha = \sum_e 2^{-e}\alpha_e$, for an effective list $\langle \alpha_e \rangle$ of the c.e. from the left reals;
- Chaitin's Ω (the probability that a universal prefix-free machine halts).

Random sets and K-trivial sets

An infinite bit sequence $B = z_1, z_2, \ldots$ is Martin-Löf random if its initial segments $z_1, \ldots, z_n$ are only compressible by a constant b:

$\exists b \, \forall n \, [K(z_1, \ldots, z_n) \geq n - b]$,
where K denotes prefix-free Kolmogorov-complexity.

At the opposite end of initial segment compressibility, B is called K-trivial (Chaitin/Solovay 1975) if

$K(z_1, \ldots, z_n) \leq K(0^n) + \text{const.}$

Even more recent example: ML-completeness

Bienvenu, Greenberg, Kučera, N., Turetsky, JEMS ta, introduced the following.

$B \leq_{\mathrm{ML}} A$ (B is Martin-Löf reducible to A) if all Martin-Löf random oracles that compute A also compute B.

(At present we don't know if this is an arithmetical relation.)

Theorem

Some c.e. set A is $\leq_{\mathrm{ML}}$-complete for the class of c.e. sets B such that $B <_{\mathrm{ML}} \mathcal{H}$ (the halting problem).

The c.e. sets B such that $B \leq_{\mathrm{ML}} A$ are exactly the c.e. K-trivials. A is called a "smart K-trivial".

We can remove c.e. ness of B: by a result of Day and Miller, for each non-K-trivial B there is ML-random $Z \not\geq_T \mathcal{H}$ that is not above B; also they show that Z is not OW-random, and hence $Z \geq_T A$.

Embedding relation among countable structures

Embedding of countable structures

Let $\mathcal{C}$ be a class of countable structures. For instance:

- graphs,
- linear orders
- Abelian groups,
- all groups.

$B \preceq A$ if there is an injective $f\colon B \to A$ that preserves relations and functions in both directions. E.g. $\mathbb{Z} \preceq \mathbb{Q}$ as abelian groups.

Question: Is there a $\preceq$-complete countable structure?

- graphs yes
- linear orders yes
- Abelian groups yes
- all groups NO

An extra condition might ensure that a complete structure is unique: The Rado graph is the unique homogeneous $\preceq$–complete countable graph. The same holds for the Fraisse limit of the finitely generated abelian groups.

Computable reducibility of structures

- The embedding relation $\preceq$ is not necessarily simpler than the structures it is about.
- Suppose the domain of the structures is $\mathbb{N}$ (or an initial segment of $\mathbb{N}$).

$B \preceq_{c,1} A$ if there is a computable injective $f\colon B \to A$ that preserves relations and functions in both directions.
We still have $\mathbb{Z} \preceq_{c,1} \mathbb{Q}$ as abelian groups.

For instance: let E, F be equivalence relations on $\mathbb{N}$. Define

$$E \preceq_{c,1} F \text{ if } \forall u \forall v\, Euv \leftrightarrow Fh(u)h(v)$$

for a computable injective function $h\colon \mathbb{N} \to \mathbb{N}$.

We can now study $\preceq_{c,1}$-completeness for classes of structures of a fixed descriptive complexity, such as computable, or Σ^0_3

Complete Σ_n^0 equivalence relations

We give natural examples of Σ_n^0 equivalence relations S that are $\preceq_{c,1}$ complete. I.e., $E \preceq_{c,1} S$ for each Σ_n^0 equivalence relation E.

n=1: Equivalence of sentences under PA (Kripke and Pour-El, 1966). This is the unique "precomplete" ER.

n=2: Polynomial time Turing equivalence on exponential time sets. (Ianovski, Miller, Ng and N., JSL 2014)

n=3: Computable isomorphism of computable Boolean algebras is complete for Σ_3^0 equivalence relations (Friedman, Fokina, and N., 2012). Another example: almost equality of c.e. sets.

n=4: Turing equivalence on c.e. sets. (Ianovski, Miller, Ng and N., JSL 2014)

Completeness for Π^0_1 equivalence relations

For a binary function f let xE_fy if $\forall u\, f(x,u) = f(y,u)$.
If f is computable then E_f is Π^0_1.

Theorem (Ianovski, Miller, Ng and N., JSL 2014)

There is polynomial time computable function f such that each E_f is $\preceq_{c,1}$-complete for Π^0_1 equivalence relations.

Fix a finite alphabet $\mathbb{A}$ of size > 1. A *tree* is a nonempty subset of $\mathbb{A}^*$ closed under prefixes. Isomorphism of polynomial time trees is Π^0_1 by König's Lemma.

Given f from the theorem above, we code $f(x,.)$ into a polytime tree T_x: If $f(x,u) = k$ we add a leaf 1^u0^k to the tree. This yields:

Corollary

Isomorphism of polynomial time trees is complete for Π^0_1 equivalence relations.

Completeness for Π^0_n equivalence relations, $n \geq 2$

Theorem (Ianovski, Miller, Ng and N., 2014)

For $n \geq 2$ there is no Π^0_n and no Δ^0_n complete equivalence relation.

To prove the theorem for $n = 2$:
given a Π^0_2 equivalence relation E, we build a Δ^0_2 equivalence relation L with classes of size ≤ 2 such that $L \nleq_c E$.

Completeness in descriptive set theory and ergodic theory

$\leq_B$-completeness of orbit equivalence relations

For equivalence relations E, F on Polish spaces X, Y, $E \leq_B F$ if $Euv \leftrightarrow Fh(u)h(v)$ for a Borel measurable function $h\colon X \to Y$.

Let G Polish group, X Polish space, $G \curvearrowright X$ continuous action.

$E_G^X = \{\langle x, y\rangle \colon \exists g \in G\, [g \cdot x = y]\}$ is the corresponding orbit equivalence relation.

Theorem (Gao-Kechris '01, Sabok '13, Zielinski '14)

The following equivalence relations are $\leq_B$ complete for OER:

- *Isometry of Polish metric spaces*
- *Affine homeomorphism of Choquet simplices*
- *Homeomorphism of compact metric spaces*
- *Isomorphism of separable C^*-algebras (even restricted to the commutative ones).*

Conjugacy of ergodic transformations

- Let MPT be the group of measure preserving transformations T of the unit interval with the Lebesgue-measure μ.
- MPT is a Polish group with the Halmos metric $d(S,T) = \sum_n 2^{-n-1}[\mu(S(E_n)\Delta T(E_n)) + \mu(S^{-1}(E_n)\Delta T^{-1}(E_n))]$, where $\langle E_n \rangle_{n\in\mathbb{N}}$ is an effective list of the rational intervals.
- T is called ergodic if all measurable sets A with $T^{-1}(A) = A$ are null or conull.
- Analytic sets are the continuous projections of Borel sets.

Theorem (Foreman, Rudolph und Weiss, Annals, 2011)

Conjugacy of ergodic transformations in MPT *is analytic complete.*

Open question: Is it $\leq_B$ complete for OER?

Conclusion

- Complete objects for a class occur in a wide variety of settings in logic and CS:
  for c.e. sets, left-c.e. reals, structures of various kinds, Π^0_1 equivalence relations on $\mathbb{N}$, orbit equivalence relations.
- We can study the class via the object, and the object via the class.
- Complete objects can be structured, or random.
- Recent results connect ML-reducibility and K-triviality.