Oracles and relativization

Peter Mayr

Computability Theory, October 23, 2023

Idea: Measure the hardness of a problem P by considering the problems that can be solved using P as oracle.

An **oracle** is a black box that solves

- decision problems: Is $x \in A$?

or

- function problems: What is $f(x)$? for a total function f?

Oracle machines

We use the definition from

- Van Melkebeek, Randomness and Completeness in Computational Complexity, 2000.

Definition

An **oracle TM** M^0 (for $O = A, f$) is a DTM with additional oracle tape and two special states `query`, `response`.
Computation is as usual except in `query`:

- Then the content of the oracle tape is considered as input x for the oracle O: Is $x \in A$? What is $f(x)$?
- x is replaced by the answer: $0/1, f(x)$
- M^o changes to `response`.

Hence an instance of O is solved in a single step of M^O.

Alternative definition for oracle machines

- Soare, Turing computability: theory and applications, 2016.

Alternative Definition

For $A \subseteq \mathbb{N}$ an **oracle TM** M^A is a DTM with additional oracle tape that is read-only and contains the characteristic function χ_A as sequence over $\{0, 1\}$.

Note

- Here M^A can look up whether $x \in A$ on the oracle tape in $\sim x$ steps.
- Recall: (The graph of) a function $f : \mathbb{N} \to \mathbb{N}$ encodes as a subset of $\mathbb{N}$,
$$A := \{2^x 3^{f(x)} \ : \ x \in \mathbb{N}\}.$$
Conversely subsets encode as characteristic functions. Hence M^f and M^A have the same computational power.
- The difference in the two definitions is relevant only for analysing their different computational complexity.

Convention

We will only consider oracles $A \subseteq \mathbb{N}$ in the following.

(No restriction and makes notation easier and concrete)

Note

- Every oracle TM M^A can be coded as an ordinary DTM (independent of A) by some $e \in \mathbb{N}$.
- If the oracle TM M_e^A on input x halts with output y, write

$$\varphi_e^A(x) = y.$$

$\varphi_e^{(k),A} \colon \mathbb{N}^k \to_p \mathbb{N}$ is the partial function computed by M_e^A.

Computations with oracles

Definition

Fix $A \subseteq \mathbb{N}$.

1. $f : \mathbb{N}^k \to_p \mathbb{N}$ is **computable in** A if there exists e such that

$$f = \varphi_e^A$$

   $P \subseteq \mathbb{N}^k$ is **computable in** A if its characteristic function is.

2. $g : \mathbb{N}^k \to_p \mathbb{N}$ is **recursive in** A if g is obtained by composition, primitive recursion and search μ from 0, successor, projections and the characteristic function χ_A of A.
   $P \subseteq \mathbb{N}^k$ is **recursive in** A if its characteristic function is.

Theorem

A function f is computable in A iff f is recursive in A.

Proof.

Relativization of the proof that computable $=$ recursive. □

Example

- If A is computable, then computable in A is just computable.
- Every c.e. set is computable in K.
  If $f : A \to K$ is a many-one reduction, then $\chi_A = \chi_K \circ f$.

Basic results relativized to A

Our current theory for computable functions can be relativized to functions that are computable in A.

Relativized Enumeration Theorem

There exists $z \in \mathbb{N}$ such that for all $A \subseteq \mathbb{N}$ and all $x, y \in \mathbb{N}$

$$\varphi_x^A(y) = \varphi_z^A(x, y).$$

Relativized S^m_n-Theorem

For every $m, n \geq 1$ there exists an injective computable function s^m_n such that for all $A \subseteq \mathbb{N}$ and all $x \in \mathbb{N}, \bar{y} \in \mathbb{N}^m, \bar{z} \in \mathbb{N}^n$

$$\varphi^A_{s^m_n(x,\bar{y})}(\bar{z}) = \varphi^A_x(\bar{y}, \bar{z}).$$

Proof sketch

- $M_{s(x,y)}$ on input z simulates M_x on input (y, z), which makes $s(x, y)$ computable and independent of A.
- s can be made injective (e.g. by setting the accept state of $M_{s(x,y)}$ as $2^x 3^y$).

Relativized Recursion Theorem

For all $A \subseteq \mathbb{N}$ and all $x, y \in \mathbb{N}$, if $f(x, y)$ is computable in A, then there is a computable function $n(y)$ such that

$$\varphi^A_{n(y)} = \varphi^A_{f(n(y),y)}.$$

Furthermore $n(y)$ does not depend on A.

Proof sketch

n is obtained from the computable (independent of A) $d(x, y)$ obtained from the S^m_n-Theorem.