Oracle modalities

Andrew W Swan

University of Ljubljana

June 12, 2024

What is an oracle?

Definition (Turing '39)

An *oracle Turing machine* is a computer program that can query information from an outside source, represented as a function $\chi : \mathbb{N} \to 2$ (an *oracle*).

We say a partial function $f : \mathbb{N} \rightharpoonup \mathbb{N}$ is *computable relative to* $\chi : \mathbb{N} \to 2$ if we can compute f using χ as an oracle.

Definition

Turing reducibility defines an preorder on functions $\mathbb{N} \to 2$. We say χ' is *Turing reducible* to χ and write $\chi' \leq_T \chi$ if χ' is computable relative to χ. We refer to the poset reflection as the *Turing degrees*.

Theorem (Turing '39)

For every χ, there is χ' not Turing reducible to χ.

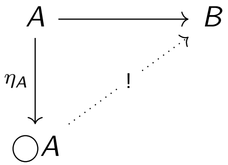
Proof.

$$\chi'(n) = \begin{cases} \varphi_e^\chi(e) + 1 & \text{if } \varphi_e^\chi \downarrow \\ 0 & \text{otherwise} \end{cases} \qquad \square$$

What is a modality?

Definition (Rijke-Shulman-Spitters)

A *reflective subuniverse* is a subtype $\mathcal{U}_{\bigcirc}$ of $\mathcal{U}$ together with $\bigcirc : \mathcal{U} \to \mathcal{U}$ and $\eta : \prod_{A:\mathcal{U}} A \to \bigcirc A$ such that $\bigcirc A \in \mathcal{U}_{\bigcirc}$ and for all $B : \mathcal{U}_{\bigcirc}$, the canonical map $B^{\bigcirc A} \to B$ is an equivalence.



Reflective subuniverses are characterised by the operator $\bigcirc : \mathcal{U} \to \mathcal{U}$. When $\mathcal{U}_{\bigcirc}$ is closed under Σ we refer to such operators as *modalities*.

What is an oracle modality?

Definition

A type A is $\bigcirc$-*connected* if $\bigcirc A = 1$.

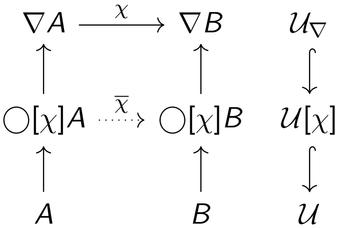
Definition (Rijke-Shulman-Spitters)

Given two modalities $\bigcirc$ and $\bigcirc'$, we write $\bigcirc \leq_T \bigcirc'$ if every $\bigcirc$-connected type is $\bigcirc'$-connected, or equivalently if $\mathcal{U}_{\bigcirc'} \subseteq \mathcal{U}_{\bigcirc}$.

Definition

Fix a modality ∇. For $A, B : \mathcal{U}$ and $\chi : \nabla A \to \nabla B$, the *oracle* modality on χ is the smallest modality $\bigcirc[\chi]$, whose reflective subuniverse contains χ, i.e. there is a unique $\overline{\chi}$ making a commutative square.

We write the reflective subuniverse as $\mathcal{U}[\chi]$.



Theorem (Hyland '82)

The Turing degrees embed in the lattice of local operators in the effective topos.

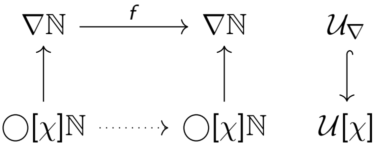
Definition

We define ∇ to be the modality of $\neg\neg$-sheafification, i.e. the smallest modality such that if P is a proposition and $\neg\neg P$ is true, then P is ∇-connected.

Theorem (S)

1. *The subcategory of* $\mathbf{Asm}^{\square^{\mathrm{op}}}$ *of* ∇*-modal, 0-truncated types is equivalent to* **Set**.
2. *We can show using axioms holding in* $\mathbf{Asm}^{\square^{\mathrm{op}}}$ *that a map* $f : \nabla\mathbb{N} \to \nabla\mathbb{N}$ *factors through* $\bigcirc[\chi]\mathbb{N}$ *precisely if it can be computed from* χ *using an "abstract oracle machine."*

We update Hyland's results using modalities and cubical assemblies (cubical sets constructed internally to assemblies).



We combine modalities with ideas from HoTT to give a synthetic proof of the following theorem.[1]

Theorem

If two oracles $\chi, \chi' : \mathbb{N} \to \nabla 2$ induce isomorphic permutation groups of $\mathbb{N}$ then they are Turing equivalent.

Formally: Given $\nabla(\pi_1(\mathcal{U}, \bigcirc[\chi]\mathbb{N})) = \nabla(\pi_1(\mathcal{U}, \bigcirc[\chi']\mathbb{N}))$, we can show $\neg\neg\chi \equiv_T \chi'$.

Computability: We can show internally in $\mathbf{Asm}^{\square^{op}}$ that for permutations $e, f, g : \bigcirc[\chi]\mathbb{N} \xrightarrow{\sim} \bigcirc[\chi]\mathbb{N}$ if $f \neq g$ then either $e \neq f$ or $e \neq g$, relative to χ, i.e. $\bigcirc[\chi](e \neq f + e \neq g)$.

HoTT: Every group is the homotopy group of some pointed type. It is often simpler to work with the pointed type directly instead of the group (Buchholtz, Van Doorn, Rijke). E.g. for wreath product, which is used in the proof.

[1] It can also be proved directly. Q for audience: does this already appear in the literature?

Traditional definition of wreath product $Sym(2) \wr Sym(\mathbb{N})$

```
wreath : Group
G     wreath                           = (ℕ → Bool) × (ℕ ≃ ℕ)
_*_   wreath (b , e) (c , f)           = (λ n → b n ⊕ c (equivFun e n)) , (e ·ₑ f)
id    wreath                           = (λ _ → false) , idEquiv ℕ
_⁻¹   wreath (b , e)                   = (λ n → b (invEq e n)) , invEquiv e
assoc wreath (a , e) (b , f) (c , g) = ≡-×
  (funExt (λ n → ⊕-assoc (a n) (b (equivFun e n)) (c (equivFun f (equivFun e n)))))
  (compEquiv-assoc e f g)
unit  wreath (a , e)                   = ≡-× refl (compEquivIdEquiv e)
inv   wreath (a , e)                   = ≡-× (funExt (λ n → ⊕-cancel (a (invEq e n))))
                                             (invEquiv-is-linv e)
```

Definition using homotopy groups:

```
HoTTWreath : Group
HoTTWreath = π₁ ((Σ[ A ∈ Type ] (A → Type)) , (ℕ , λ _ → Bool))
```

Theorem (Christensen-Opie-Rijke-Scoccola)

For every modality $\bigcirc$, there is a modality $\bigcirc^{(1)}$, such that $A : \mathcal{U}$ belongs to $\mathcal{U}_{\bigcirc^{(1)}}$ iff $\mathsf{Id}(a, b)$ belongs to $\mathcal{U}_{\bigcirc}$ for all $a, b : A$.

Definition

We call $\bigcirc^{(1)}$ the *suspension* of $\bigcirc$. We write $\bigcirc^{(k)}$ for the suspension iterated k times.

Idea: A only contains computable points, $\bigcirc[\chi]$ lets us construct new points using the oracle, e.g. $n = 5$ if $\varphi_e(e)\downarrow$ and $n = 2$ otherwise.

For $\bigcirc[\chi]^{(k)}A$, we can use the oracle to construct n-cells for $n \geq k$, but not for $n < k$.

Example

Apply the 3rd suspension of the halting problem to $\mathbb{S}^2$.

$$\pi_2(\bigcirc[\kappa]^{(3)}\mathbb{S}^2) = \mathbb{Z}$$

$$\pi_3(\bigcirc[\kappa]^{(3)}\mathbb{S}^2) = \bigcirc[\kappa]\mathbb{Z}$$

Some open problems:

1. Are there non trivial examples of cotopological modalities using realizability?
2. "HoTT-style" synthetic proofs of classic results in computable group theory e.g. Higman embedding theorem.
3. Higher computable structures?
4. Countable families of finite cell complexes as "higher" c.e. degrees?

Thanks for your attention!

A.W. Swan, Oracle modalities, arXiv:2406.05818

`https://github.com/awswan/oraclemodality`