Topos-theoretic aspect of the degrees of unsolvability

Takayuki Kihara

Nagoya University, Japan

NUS logic seminar, March 22, 2023

- Hyland (1982) introduced the *effective topos* Eff, "the world of computable mathematics."
- Eff has the smallest subtopos (the degenerated topos), "the world of inconsistent mathematics."
- Eff has the second smallest subtopos Set, "the world of set-theoretic mathematics."

 For each α ∈ 2^ω Hyland found a subtopos Eff[α] of Eff, "the world of α-relatively computable mathematics." α ≤_T β ⇔ Eff[β] is a subtopos of Eff[α]

- (Idea) smaller topos ≈ stronger theory
- Let us examine the structure of all subtoposes of a topos!
 - ▷ non-degenerated subtoposes of Eff ≈ all worlds between "the computable world" and "the set-theoretic world".
- (Key Idea) "a subtopos of Eff" ≈ "Eff relative to an oracle".
 - An oracle changes a world / model / semantics.

Table of contents:

- Kripke-like semantics
- Grothendieck / Lawvere-Tierney topology
- Oracle vs. LT-topology
- Observe theory

Kleene's realizability interpretation (1945)

- A proof of $A \wedge B$ is a pair of proofs of A and B.
- A proof of $A \lor B$ is a pair of a tag indicating which of A or B is correct and a proof of the formula for the correct side.
- A proof of A → B is (a code of) a computable function that, given a proof of A, outputs a proof of B.
- A proof of ∃x ∈ I. A(x) is a pair of a code of a witness c ∈ I of the existence and a proof of the formula A(c).
- A proof of ∀x ∈ I. A(x) is (a code of) a computable function that, given a code of an element c ∈ I, outputs a proof of A(c).
- This interpretation can obviously be made relative to an oracle.
 - ▷ Given an oracle α , replace "computable" with " α -computable".
 - An oracle α is not necessarily single-valued;
 e.g. Lifschitz realizability (realizability relative to Π⁰₁ classes)
 - ▷ An oracle changes semantics.
- Factors causing changes in semantics:
 - ► Coverage: factor causing changes in Kripke semantics
 - Oracle: factor causing changes in realizability interpretation

KRIPKE SEMANTICS FOR INTUITIONISTIC LOGIC

 Intuitionistic Kripke model is a preorder (P, ≤) with an assignment of which atomic propositions φ are valid at which positions p ∈ P.

- ▷ If φ is true at $p \in P$ then we write $p \Vdash \varphi$.
- ▷ Moreover we assume that $q \le p \Vdash \varphi$ implies $q \Vdash \varphi$.



In intuitionistic model, in order to claim that $\varphi \lor \psi$ is valid at a position $p \in P$, one must determine whether φ or ψ is valid at the position p.

•
$$p \Vdash \varphi \land \psi \iff p \Vdash \varphi$$
 and $p \Vdash \psi$

• $p \Vdash \varphi \lor \psi \iff p \Vdash \varphi \text{ or } p \Vdash \psi$.

• $p \Vdash \varphi \rightarrow \psi \iff (\forall q \le p) [q \Vdash \varphi \text{ implies } q \Vdash \psi].$

BETH SEMANTICS

- To deepen our understanding of models of semi-constructive mathematics, it is also useful to have a model that
 - does not "immediately decide which is valid"
 - ▶ but rather "postpones the decision of which is valid".
- In the Beth model, to assert that "φ V ψ is valid at position p" is to know that "no matter what path α we take beyond position p, at some point along α either φ or ψ will be determined to be valid".



• $p \Vdash \varphi \land \psi \iff p \Vdash \varphi$ and $p \Vdash \psi$.

• $p \Vdash \varphi \lor \psi \iff (\forall \alpha \ni p \text{ path})(p \ge \exists q \in \alpha) [q \Vdash \varphi \text{ or } q \Vdash \psi].$

• $p \Vdash \varphi \rightarrow \psi \iff (\forall q \le p) [q \Vdash \varphi \text{ implies } q \Vdash \psi].$

BETH SEMANTICS

- $p \Vdash \varphi \land \psi \iff p \Vdash \varphi$ and $p \Vdash \psi$.
- $p \Vdash \varphi \lor \psi \iff (\forall \alpha \ni p \text{ path})(p \ge \exists q \in \alpha) [q \Vdash \varphi \text{ or } q \Vdash \psi].$
- $p \Vdash \varphi \rightarrow \psi \iff (\forall q \le p) [q \Vdash \varphi \text{ implies } q \Vdash \psi].$

(Observation) $p \Vdash \varphi \lor \psi \iff (\exists B \text{ bar for } p)(\forall b \in B) [b \Vdash \varphi \text{ or } b \Vdash \psi]$



COVERING SEMANTICS

- There is also a type of model that asserts that "φ ∨ ψ is globally valid" if it is locally determined whether φ or ψ is valid.
- E.g., for a topological space, use the complete lattice (*O*(*X*), ⊆) of open sets in *X* as a base of Kripke-like model.
- $A \Vdash \varphi \land \psi \iff A \Vdash \varphi$ and $A \Vdash \psi$.
- $A \Vdash \varphi \lor \psi \iff (\exists \mathcal{U} \text{ open cover of } A)(\forall V \in \mathcal{U}) \lor V \Vdash \varphi \text{ or } V \Vdash \psi.$
- $A \Vdash \varphi \rightarrow \psi \iff (\forall B \subseteq A) [B \Vdash \varphi \text{ implies } B \Vdash \psi].$



In general, for a complete lattice L, a cover of $a \in L$ is a set $U \subseteq L$ s.t. $a \leq \bigvee U$.

(WEAK) FORCING SEMANTICS

• Another type of model, with slightly looser conditions than Beth semantics, requires that the truth need not be determined along all paths, but only that it should be determined along any generic path.

•
$$p \Vdash \varphi \land \psi \iff p \Vdash \varphi$$
 and $p \Vdash \psi$.

•
$$p \Vdash \varphi \lor \psi \iff (\forall q \le p)(\exists r \le q) [r \Vdash \varphi \text{ or } r \Vdash \psi].$$

• $p \Vdash \varphi \rightarrow \psi \iff (\forall q \ge p) [q \Vdash \varphi \text{ implies } q \Vdash \psi].$

(Observation) $p \Vdash \varphi \lor \psi \iff (\exists D \text{ dense below } p)(\forall q \in D) [q \Vdash \varphi \text{ or } q \Vdash \psi]$

UNIFYING VARIOUS KRIPKE-LIKE SEMANTICS

There are many different definitions of $a \Vdash \varphi \lor \psi$:

- (Kripke) $a \Vdash \varphi$ or $a \Vdash \psi$.
- (Beth) $(\exists B \text{ bar for } a)(\forall b \in B) [b \Vdash \varphi \text{ or } b \Vdash \psi].$
- (Covering) $(\exists U \text{ cover of } a)(\forall b \in U) [b \Vdash \varphi \text{ or } b \Vdash \psi].$
- (Forcing) ($\exists D$ dense below a)($\forall b \in D$) [$b \Vdash \varphi$ or $b \Vdash \psi$].

All these examples can be unified by giving some assignment $a \mapsto J_a$:

•
$$(\exists V \in J_a)(\forall b \in V) \ [b \Vdash \varphi \text{ or } b \Vdash \psi].$$

 \triangleright Without loss of generality, one may assume that J_a is downward closed.

$$\begin{split} J_a^{Kr} &= \{\downarrow a\}; \qquad \qquad J_a^{Be} = \{\downarrow B : B \text{ bar for } a\}; \\ J_a^{Cov} &= \{\downarrow U : U \text{ cover of } a\}; \qquad J_a^{Fo} = \{\downarrow D : D \text{ dense below } a\}. \end{split}$$

If an assignment $a \mapsto J_a$ satisfies a certain condition, then it is called a *Grothendieck topology* (on an underlying poset).

(Example) J^{Kr} , J^{Be} , J^{Cov} , J^{Fo} are Grothendieck topologies.

Table of contents:

- Kripke-like semantics
- Grothendieck / Lawvere-Tierney topology
- Oracle vs. LT-topology
- Observe theory

 $j(\mathcal{U}) := \{A : A \subseteq \bigcup \mathcal{U}\}$ "the collection of all sets covered by \mathcal{U} "

(inflationary) If $A \in \mathcal{U}$ then A is covered by \mathcal{U} : $\mathcal{U} \subseteq \mathfrak{j}(\mathcal{U})$ (downward closed) For $A \subseteq B$, if B is covered by \mathcal{U} , then so is A: $A \subseteq B \in i(\mathcal{U}) \implies A \in i(\mathcal{U})$ (monotone) For $\mathcal{U} \subseteq \mathcal{V}$, if \mathcal{U} covers A, then so does \mathcal{V} : $\mathcal{U} \subseteq \mathcal{V} \implies j(\mathcal{U}) \subseteq j(\mathcal{V})$ (idempotent) If A is covered by \mathcal{U} , and every $B \in \mathcal{U}$ is covered by \mathcal{V} , then A is covered by \mathcal{V} : $i \circ i(\mathcal{U}) \subseteq i(\mathcal{U})$ **(local)** If \mathcal{U} covers A, then so does $\mathcal{U} \upharpoonright A := \{U \cap A : U \in \mathcal{U}\}$. Indeed, if \mathcal{U} covers $A \in \mathcal{V}$, then so does $\{U \cap V : U \in \mathcal{U}, V \in \mathcal{V}\}$: $i(\mathcal{U}) \cap \mathcal{V} = i(\mathcal{U} \cap \mathcal{V}) \cap \mathcal{V}$ (for downward closed \mathcal{U}, \mathcal{V})

- (inflationary) + (monotone) + (idempotent) = a closure operator.
- A coverage ≈ a local closure operator on downward closed sets.

The downward closed sets form a complete Heyting algebra under ⊆.

▶ Let Ω be a complete Heyting algebra:

A map $j: \Omega \rightarrow \Omega$ is *nucleus* if:

- (monotone) $x \le y \implies j(x) \le j(y)$.
- 2 (inflationary) $x \leq j(x)$.
- (idempotent) $j \circ j(x) \leq j(x)$.
- (local) $j(x) \land y = j(x \land y) \land y$.
 - A nucleus is a local closure operator on Ω .
 - (local) $\iff (x \leftrightarrow y) \le (j(x) \leftrightarrow j(y))$
 - (mon.) + (local) = (locally monotone) $(x \to y) \le (j(x) \to j(y))$ \triangleright (:.) nucleus \iff (loc. mon.) + (infl.) + (idem.)
 - nucleus \implies (\land -preserving) $j(x \land y) = j(x) \land j(y)$
 - ▷ (::) A nucleus is a \wedge -preserving closure operator on Ω .

• Kripke semantics:

the semantics of the topos $\mathbf{Set}^{P^{op}}$ of presheaves over a poset *P*.

- A nucleus *j* on the downward closed sets Ω in *P* ≈ a Grothendieck topology *J* on *P*.
- The collection of *J*-sheaves over *P* again forms a topos Sh_J(*P*), which is a subtopos of Set^{*P*^{op}}, and indeed:

► A subtopos of $\operatorname{Set}^{P^{op}} \approx$ a nucleus on $\Omega \approx$ a Gro. topology on *P*

- Kripke semantics relative to coverage / nucleus / Gro. topology J (a.k.a. Kripke-Joyal semantics): the semantics of the topos Sh_I(P) of J-sheaves over a poset P.
- A Grothendieck topology (coverage) is a factor that causes changes in a presheaf topos.
- What is a factor that causes changes in a topos other than a presheaf topos?
 - ▶ It is a Lawvere-Tierney topology.
 - ▶ A subtopos of a topos $\mathcal{E} \approx$ a Lawvere-Tierney topology on \mathcal{E}

A map $j: \Omega \to \Omega$ on a complete Heyting algebra Ω is *nucleus* if:

- (locally monotone) $x \to y \le j(x) \to j(y)$.
- (inflationary) $x \leq j(x)$.
- (idempotent) $j \circ j(x) \leq j(x)$.

A Grothendieck topology on a poset $P \approx A$ nucleus on downsets in $P \approx A$ Lawvere-Tierney topology on the presheaf topos $\mathbf{Set}^{P^{op}}$.

An Lawvere-Tierney topology on Eff can be explicitly described as:

A map $j: \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ is a *Lawvere-Tierney topology* on Eff if all of the following formulas are realizable (uniformly in x, y):

- (locally monotone) $(x \to y) \to (j(x) \to j(y))$.
- (inflationary) $x \rightarrow j(x)$.
- (idempotent) $j \circ j(x) \rightarrow j(x)$.
 - This notion should give all the subtoposes of Eff.
 - How on earth does this notion relate to oracles?

Table of contents:

- Kripke-like semantics
- Grothendieck / Lawvere-Tierney topology
- Oracle vs. LT-topology
- Observe theory

Factors causing changes in semantics:

- Coverage: factor causing changes in Kripke semantics
- ▶ Oracle: factor causing changes in realizability interpretation

The key point is to notice that the following two are similar:

- A sieve *U* is a *j*-cover of an object *p*.
- With the help of an oracle *j*, an algorithm *p* can solve a problem *U*.

Factors causing changes in semantics:

- ▷ Coverage: factor causing changes in Kripke semantics
- ▶ Oracle: factor causing changes in realizability interpretation

The key point is to notice that the following three are similar:

- A sieve *U* is a *j*-cover of an object *p*.
- Under a theory j, a formula provable from any assumption $\varphi \in U$ is also provable from the assumption of a formula p.
- With the help of an oracle j, an algorithm p can solve a problem U.

With the help of an oracle F, an algorithm p can solve a problem U.

- $p \in j_F^1(U)$: $\iff p$ is a program that solves a problem Uby making exactly one guery to an oracle F.
- $p \in j_F^{\leq 1}(U)$: $\iff p$ is a program that solves a problem U by making at most one query to an oracle F.
- $p \in j_F(U)$: $\iff p$ is a program that solves a problem Uby making at most finitely many queries to an oracle F.

Under a suitably generalized notion of "oracle" (to be explained later), one can prove the following:

Theorem (K.)

- $j \equiv j_F^1$ for some "oracle" $F \iff$ (locally monotone) for j is realizable.
- $j \equiv j_F^{\leq 1}$ for some "oracle" $F \iff$ (locally monotone)

and (inflationary) for *j* are realizable.

• $j \equiv j_F$ for some "oracle" $F \iff$ (locally monotone), (inflationary) and (idempotent) for j are realizable; that is, j is an LT-topology.

Relative computability with exactly one query

Relative computability with at most one query

Relative computability with finitely many queries

locally monotone $(x \rightarrow y) \rightarrow (j(x) \rightarrow j(y))$

loc. mon. + inflationary $x \rightarrow j(x)$

loc. mon. + infl. + idempotent (Lawvere-Tierney topology) $j \circ j(x) \rightarrow j(x)$

Table of contents:

- Kripke-like semantics
- Grothendieck / Lawvere-Tierney topology
- Oracle vs. LT-topology
- Observe theory

- (Key Idea) "a subtopos of Eff" ≈ "Eff relative to an oracle".
 - ▶ Here, oracle need not be a decision problem (a total function).
- Turing degrees: degrees for decision problems (total functions)
- partial degrees: degrees for partial functions
- Medvedev degrees: degrees for mass problems
- Weihrauch degrees: degrees for partial multifunctions
- Hyland (1982): The Turing degrees embed into the subtoposes of Eff, by α → Eff[α].
- Faber-van Oosten (2014): The partial degrees (in a certain sense) correspond to the realizability subtoposes of Eff.
 - ▶ Note: there are a lot of non-realizability subtoposes of Eff.
 - (A realizability topos is the ex/reg-completion of the category of assemblies over a partial combinatory algebra.)

USING A PARTIAL FUNCTION AS AN ORACLE

[Hereafter, a function f from some $D \subseteq X$ to Y is written as $f :\subseteq X \rightarrow Y$]

Turing-like reducibility for partial functions $f \subseteq \mathbb{N} \to \mathbb{N}$:

- The major ones are Kleene-style (1952) and Sasso-style (1971).
 - [Point] Since an oracle is only partially defined, when making a query to the oracle, the response may not be returned forever!
- Kleene-style: One can access multiple parts of the oracle in parallel.
- Sasso-style: Once we have made a query to the oracle, we have to wait for a response from the oracle.
- Kleene's partial degrees ~ the enumeration degrees of the graphs.

(\therefore) It has been widely believed that the study of partial degrees can be absorbed into the theory of enumeration degrees.

This is not true for Sasso-style partial degree!

Definition (Sasso 1971, van Oosten 1997, Madore 2012)

A partial function f is *subTuring reducible* to a partial function g if there exists a Turing functional Φ which computes $\Phi^g(n) \downarrow = f(n)$ without making a query outside of **dom**(g) for any input $n \in$ **dom**(f).

- Unfortunately, none of the recursion theorists studied this.
- Translating Faber-van Oosten's work (2014) into computability-theoretic terms, it reads as follows:
 - ► The subTuring degrees ~ the realizability subtoposes of Eff.

 $f \leq_{subT} g \iff \text{Eff}[g]$ is a subtopos of Eff[f]

Theorem (K.-Ng, last week)

The subTuring degrees form a dense lattice.

Hence, the realizability subtoposes of Eff form a dense lattice.

• A partial function f is quasiminimal \iff

f is noncomputable, and every total $g \leq_{subT} f$ is computable.

• A partial function f is effectively quasiminimal $\iff f \not\leq_{subT} \emptyset$ and $\exists u \leq_{subT} f \forall total g (g \leq_{subT} f via e \implies g = \varphi_{u(e)}).$

Theorem (K.-Ng, this week)

There exists an effectively quasiminimal subTuring degree.

• CT_0 : every total relation on \mathbb{N} is computable:

 $\forall x \exists y \ A(x,y) \rightarrow \exists e \forall x \ A(x,\varphi_e(x))$

• ECT_0 : every partial function on \mathbb{N} is computable:

 $\forall x(N(x) \rightarrow \exists ! y \ A(x, y)) \rightarrow \exists e \forall x(N(x) \rightarrow A(x, \varphi_e(x)))$

where N is an almost negative formula.

Corollary (K.-Ng, this week)

There exists a realizability subtopos \mathcal{E} of Eff s.t. $\mathcal{E} \models CT_0 + \neg ECT_0!$.

Fujiwara (an expert in constructive reverse math) told me that he has never seen a model of $CT_0 + \neg ECT_0$, so this result may be new in constructive math.

- (Key Idea) "a subtopos of Eff" ≈ "Eff relative to an oracle".
 - ▶ Here, oracle need not be a decision problem (a total function).
- Turing degrees: degrees for decision problems (total functions)
- subTuring degrees: degrees for partial functions
- Medvedev degrees: degrees for mass problems
- Weihrauch degrees: degrees for partial multifunctions
- The subTuring degrees \simeq the realizability subtoposes of Eff.
 - ▶ Note: there are a lot of non-realizability subtoposes of Eff.
- To describe non-realizability subtoposes, a multifunction is needed.
 - ▷ Given a partial multifunction g on N, one can construct a subtopos Eff[g] of Eff.
- In fact, more than multifunction is needed.
 - ▷ (Bauer 2022) An extended Weihrauch predicate.
 - ▶ (K. 2023) A multifunction with "(secret) parameter"
 - ► (K. 202x) A multifunction on "N-multi-represented spaces".

 $(\text{Def.}) j \le k \iff j(x) \rightarrow k(x)$ is realizable (uniformly in x)

Theorem (K.)

The subTuring lattice is isomorphic to

the lattice of \bigcup , \bigcap -preserving LT-topologies.

exactly one query	locally monotone
at most one query	loc. mon. + inflationary
finitely many queries	loc. mon. + infl. + idempotent

Theorem (K.)

- The Weihrauch lattice is isomorphic to the lattice of ∩-preserving locally monotone maps.
- The pointed Weihrauch lattice is isomorphic to the lattice of preserving locally monotone inflationary maps.
- The generalized Weihrauch lattice is isomorphic to the lattice of ∩-preserving LT-topologies.

We need more than partial multifunctions:

- ▷ (Bauer 2022) An extended Weihrauch predicate.
- ▶ (K. 2023) A multifunction with "(secret) parameter"
- ▶ (K. 202x) A multifunction on "N-multi-represented spaces".

Theorem (K.)

- The extended Weihrauch lattice is isomorphic to the lattice of locally monotone maps.
- The pointed extended Weihrauch lattice is isomorphic to the lattice of locally monotone inflationary maps.
- The generalized extended Weihrauch lattice is isomorphic to the lattice of LT-topologies.

Sasso-style subTuring reducibility can be represented in game form.

(a.k.a. van Oosten's "dialogue" 1997):

Орр		Pro
$x_0 \in \operatorname{dom}(f)$		
	Query:	$z_0 \in \operatorname{dom}(g)$
$x_1 = g(z_0)$		
	Query:	$z_1 \in \operatorname{dom}(g)$
$x_2 = g(z_1)$		
:		•
	Query:	$z_n \in \operatorname{dom}(g)$
$x_{n+1} = g(z_n)$		A ()
	Halt:	$z_{n+1} = f(x_0)$

- Opp's moves are natural numbers x_0, x_1, x_2, \ldots
- Pro's moves are of the forms (Query, z_i) or (Halt, z_i).
 - ▶ Query is a signal to ask a query to oracle.
 - ▶ Halt is a signal to terminate the computation.
- f is subT-reducible to $g \iff$ Pro has a computable winning strategy.

A subTuring-reduction game can be considered for multifunctions.

Hirschfeldt-Jockusch's reduction game (a.k.a. Lee-van Oosten's "sight"):

Орр		Pro
$x_0 \in \operatorname{dom}(F)$		
	Query:	$z_0 \in \operatorname{dom}(G)$
$x_1 \in G(z_0)$	_	
- 6()	Query:	$z_1 \in \operatorname{dom}(G)$
$x_2 \in G(z_1)$		
•		•
	Query:	$z_n \in \operatorname{dom}(G)$
$x_{n+1} \in G(z_n)$		
	Halt:	$z_{n+1} \in F(x_0)$

- Opp's moves are natural numbers x_0, x_1, x_2, \ldots
- Pro's moves are of the forms (Query, z_i) or (Halt, z_i).
 - ▶ Query is a signal to ask a query to oracle.
 - ▶ Halt is a signal to terminate the computation.
- F is GW-reducible to $G \iff$ Pro has a computable winning strategy.

What we need is the following *reduction game* on multi-represented spaces:

Merlin	Arthur	Nimue
\mathbf{p}_0 is a name of $x_0 \in \mathbf{dom}(F)$		
	Query: \mathbf{q}_0 is a name of	$z_0 \in \operatorname{dom}(G)$
\mathbf{p}_1 is a name of $x_1 \in G(z_0)$	•	
	Query: \mathbf{q}_1 is a name of	$z_1 \in \operatorname{dom}(G)$
\mathbf{p}_2 is a name of $x_1 \in G(z_1)$		
:	•	:
	Query: \mathbf{q}_n is a name of	$z_n \in \operatorname{dom}(G)$
\mathbf{p}_{n+1} is a name of $x_n \in G(z_n)$		
	Halt: \mathbf{q}_{n+1} is a name of	$z_{n+1} \in F(x_0)$

- Merlin's move is a pair (p, x); Nimue's move is z; and Arthur's move is either (Query, q) or (Halt, q).
 - Arthur cannot see "points" and can only see "names", and Arthur can only perform computable procedures
 - ▶ Merlin and Nimue can see both "names" and "points", and Merlin and Nimue can perform any procedure.
- F is LT-reducible to G \iff Arthur-Nimue has a winning strategy where Arthur's strategy is computable.

Biliography:

- E. Faber and J. van Oosten, **More on geometric morphisms between** realizability toposes, *Theory Appl. Categ.*, 29:874–895, 2014.
- T. Kihara, Lawvere-Tierney topologies for computability theorists, Transactions of the American Mathematical Society, B, 10 (2023), 48-85.
 - T. Kihara, **Degrees of incomputability, realizability and constructive reverse mathematics**, *preprint* (2020), available at arXiv:2002.10712
- T. Kihara, Rethinking the notion of oracle, preprint (2022), 57 pages, available at arXiv:2202.00188
- T. Kihara and K. M. Ng, **The subTuring degrees**, work in progress.
- S. Lee and J. van Oosten, Basic subtoposes of the effective topos, Ann. Pure Appl. Logic, 164(9):866–883, 2013.
- S. Nakata, preprint, 2023.