# Mechanised Constructive Reverse Mathematics

## Completeness, Löwenheim-Skolem Theorem, Post's Problem

Dominik Kirst

Proofs and Algorithms Seminar
LIX, November 4th, 2024

# Constructive Reverse Mathematics

Classical reverse mathematics studies classically detectable equivalences:

- Which theorems are equivalent to the axiom of choice or similar principles?
- Which theorems are equivalent to which comprehension principles?
- Many more, see Friedman (1976) and Simpson (2009)

Constructive reverse mathematics studies constructively detectable equivalences:

- Which theorems are equivalent to excluded middle (LEM) or weaker principles?
- Which theorems are equivalent to which specific formulation of the axiom of choice?
- Many more, see Ishihara (2006) and Diener (2018)

Characterises the computational content of analysed theorems

# Some Typical Principles

Fragments of the excluded middle:

$$\begin{aligned}
\mathsf{LEM} &:= \forall P : \mathbb{P}.\, P \lor \neg P \\
\mathsf{LPO} &:= \forall f : \mathbb{N}\to\mathbb{B}.\, (\exists n.\, f\ n = \mathsf{true}) \lor (\forall n.\, f\ n = \mathsf{false}) \\
\mathsf{MP} &:= \forall f : \mathbb{N}\to\mathbb{B}.\, \neg\neg(\exists n.\, f\ n = \mathsf{true}) \to (\exists n.\, f\ n = \mathsf{true})
\end{aligned}$$

Fragments of the axioms of choice:

$$\begin{aligned}
\mathsf{AC} &:= \forall AB. \forall R : A\to B\to\mathbb{P}.\, \mathsf{tot}(R) \to \exists f : A\to B. \forall x.\, R\, x\, (f\ x) \\
\mathsf{DC} &:= \forall A.\, \mathsf{inhab}(A) \to \forall R : A\to A\to\mathbb{P}.\, \mathsf{tot}(R) \to \exists f : \mathbb{N}\to A. \forall n.\, R\, (f\ n)\, (f\ (n+1)) \\
\mathsf{CC} &:= \forall A. \forall R : \mathbb{N}\to A\to\mathbb{P}.\, \mathsf{tot}(R) \to \exists f : \mathbb{N}\to A. \forall n.\, R\, n\, (f\ n)
\end{aligned}$$

To unveil fine distinctions, we use CIC as a modest base system

# Some Typical Connections

- LEM: Every non-empty set of numbers has a minimum
- LPO: Every sequence in a compact set has a convergent subsequence
- MP: Every bi-enumerable set of numbers is decidable
- AC: Every set can be well-ordered
- DC: Every partial order without infinite descending chains is well-founded
- CC: Every sequentially continuous real-valued function is continuous

Often very subtle, we use Coq to systematically track dependencies

# Example 1: Completeness

(jww. Yannick Forster, Christian Hagemeier, Hugo Herbelin, Ian Shillito, Dominik Wehr)

# Analysing Completeness Theorems in Constructive Meta-Theory

Does $\mathcal{T} \vDash \varphi$ imply $\mathcal{T} \vdash \varphi$ constructively?

Confusing situation in the literature on first-order logic:

- Completeness equivalent to Boolean Prime Ideal Theorem (Henkin, 1954)
- Completeness requires Markov's Principle (Kreisel, 1962)
- Completeness equivalent to Weak Kőnig's Lemma (Simpson, 2009)
- Completeness equivalent to Weak Fan Theorem (Krivtsov, 2015)
- Completeness holds fully constructively (Krivine, 1996)

# Working Towards an Explanation

There are multiple dimensions at play:

- Syntax fragment (e.g., propositional, minimal, negative, full)
- Complexity of the context (e.g., finite, decidable, enumerable, arbitrary)
- Cardinality of the signature (e.g., countable, uncountable)
- Representation of the semantics (e.g., Boolean, decidable, propositional)

Ongoing systematic investigation:

- Started by Herbelin and Ilik (2016) and Forster, Kirst, and Wehr (2021)
- New observations by Hagemeier and Kirst (2022) and Kirst (2022)
- Comprehensive overview of current landscape by Herbelin (2022)
- Today: syntactic disjunction, arbitrary contexts, countable signature, prop. semantics

# Classical Outline for Intuitionistic Propositional Logic

Employing prime theories ($\varphi \lor \psi \in \mathcal{T} \to \varphi \in \mathcal{T} \lor \varphi \in \mathcal{T}$):

- Lindenbaum Extension: if $\mathcal{T} \nvdash \varphi$ then there is prime $\mathcal{T}'$ with $\mathcal{T}' \nvdash \varphi$
- Universal Model $\mathcal{U}$: consistent prime theories related by inclusion
- Truth Lemma for $\mathcal{T}$ in $\mathcal{U}$: $\varphi \in \mathcal{T} \iff \mathcal{T} \Vdash \varphi$
- Model Existence: if $\mathcal{T} \nvdash \varphi$ then there is $\mathcal{M}$ with $\mathcal{M} \Vdash \mathcal{T}$ and $\mathcal{M} \nVdash \varphi$
- Quasi Completeness: if $\mathcal{T} \Vdash \varphi$ then $\neg\neg(\mathcal{T} \vdash \varphi)$
- Completeness: if $\mathcal{T} \Vdash \varphi$ then $\mathcal{T} \vdash \varphi$

# Constructive Completeness Proof?

For $\mathcal{T}$ quasi-prime ($\varphi \lor \psi \in \mathcal{T} \to \neg\neg(\varphi \in \mathcal{T} \lor \varphi \in \mathcal{T})$) and stable ($\neg\neg(\varphi \in \mathcal{T}) \to \varphi \in \mathcal{T}$):

- Lindenbaum Extension: if $\mathcal{T} \nvdash \varphi$ then there is stable quasi-prime $\mathcal{T}'$ with $\mathcal{T}' \nvdash \varphi$
- Universal Model: consistent stable quasi-prime theories related by inclusion
- Truth Lemma: fails for disjunction
- Model Existence: fails
- Quasi Completeness: fails
- Completeness: needs MP/LEM depending on theory complexity and syntax fragment

# The Issue with Disjunction

Truth Lemma case for disjunctions $\varphi \lor \psi$:

$$\begin{aligned} \varphi \lor \psi \in \mathcal{T} &\overset{?}{\iff} \mathcal{T} \Vdash \varphi \lor \psi \\ &\overset{\textit{def}}{\iff} \mathcal{T} \Vdash \varphi \;\lor\; \mathcal{T} \Vdash \psi \\ &\overset{\textit{IH}}{\iff} \varphi \in \mathcal{T} \;\lor\; \psi \in \mathcal{T} \end{aligned}$$

- So we really need prime theories to interpret disjunctions
- Primeness from Lindenbaum Extension is constructive no-go

# Quasi Completeness via WLEM

Weak law of excluded middle WLEM $:= \forall P : \mathbb{P}. \neg P \vee \neg\neg P$

**Lemma**

*Assuming WLEM, every stable quasi-prime theory is prime.*

**Proof.**

Assume $\varphi \vee \psi \in \mathcal{T}$. Using WLEM, decide whether $\neg(\varphi \in \mathcal{T})$ or $\neg\neg(\varphi \in \mathcal{T})$. In the latter case, conclude $\varphi \in \mathcal{T}$ directly by stability. In the former case, derive $\psi \in \mathcal{T}$ using stability, since assuming $\neg(\psi \in \mathcal{T})$ on top of $\neg(\varphi \in \mathcal{T})$ contradicts quasi-primeness for $\varphi \vee \psi \in \mathcal{T}$. □

Classical proof outline works again up to Quasi Completeness!

# Backwards Analysis

Is that the best we can get?

**Fact**

*Model Existence implies WLEM.*

**Proof.**

Given $P$, use model existence on $\mathcal{T} := \{x_0 \vee \neg x_0\} \cup \{x_0 \mid P\} \cup \{\neg x_0 \mid \neg P\}$. We have $\mathcal{T} \nvdash \bot$ so if $\mathcal{M} \Vdash \mathcal{T}$, then either $\mathcal{M} \Vdash x_0$ or $\mathcal{M} \Vdash \neg x_0$, so either $\neg\neg P$ or $\neg P$, respectively. □

**Fact**

*Quasi Completeness implies the following principle:* $\forall p : \mathbb{N} \to \mathbb{P}.\, \neg\neg(\forall n.\, \neg p\, n \vee \neg\neg p\, n)$

**Proof.**

Using similar tricks for $\mathcal{T} := \{x_n \vee \neg x_n\} \cup \{x_n \mid p\, n\} \cup \{\neg x_n \mid \neg p\, n\}$. □

Obvious consequence both from WLEM and DNS, maybe enough for Quasi Completeness?

# Countable Weak Excluded-Middle Shift[1]

$$\mathsf{WLEMS}_{\mathbb{N}} := \forall p : \mathbb{N} \to \mathbb{P}.\, (\forall n.\, \neg\neg(\neg p\, n \lor \neg\neg p\, n)) \to \neg\neg(\forall n.\, \neg p\, n \lor \neg\neg p\, n)$$

$$\Leftrightarrow \forall pq : \mathbb{N} \to \mathbb{P}.\, (\forall n.\, \neg\neg(\neg p\, n \lor \neg q\, n)) \to \neg\neg(\forall n.\, \neg p\, n \lor \neg q\, n)$$

**Lemma**

*Assuming $\mathsf{WLEMS}_{\mathbb{N}}$, every stable quasi-prime theory is not not prime.*

**Proof.**

Assume $\mathcal{T}$ not prime and derive a contradiction. Given the negative goal, from $\mathsf{WLEMS}_{\mathbb{N}}$ we obtain $\forall \varphi.\, \neg(\varphi \in \mathcal{T}) \lor \neg\neg(\varphi \in \mathcal{T})$. This yields exactly the instances of WLEM needed to derive that $\mathcal{T}$ is prime, contradiction. □

Already this lemma turns out to be enough for Quasi Completeness!

[1] Mentioned in systematic study by Umezawa (1959) but absent from the literature otherwise

# Quasi Completeness via $\mathsf{WLEMS}_{\mathbb{N}}$

Refined proof outline using $\mathsf{WLEMS}_{\mathbb{N}}$:

- Lindenbaum Extension: if $\mathcal{T} \nvdash \varphi$ then there is stable not not prime $\mathcal{T}'$ with $\mathcal{T}' \nvdash \varphi$
- Universal Model $\mathcal{U}$: consistent stable prime theories related by inclusion
- Truth Lemma for $\mathcal{T}$ in $\mathcal{U}$: $\varphi \in \mathcal{T} \iff \mathcal{T} \Vdash \varphi$
- Quasi Model Existence: if $\mathcal{T} \nvdash \varphi$ then there not not is $\mathcal{M}$ with $\mathcal{M} \Vdash \mathcal{T}$ and $\mathcal{M} \nVdash \varphi$
- Quasi Completeness: if $\mathcal{T} \Vdash \varphi$ then $\neg\neg(\mathcal{T} \vdash \varphi)$
- Completeness: needs MP/LEM depending on theory complexity and syntax fragment

# Consequences and Ongoing Work

Consequences:

- WLEM and Model Existence are equivalent
- $\mathrm{WLEMS}_{\mathbb{N}}$, Quasi Model Existence, and Quasi Completeness are equivalent
- Completeness for enumerable $\mathcal{T}$ follows from $\mathrm{WLEMS}_{\mathbb{N}} + \mathrm{MP}$

Generalisation:

- Classical propositional logic
- Classical first-order logic, maybe intuitionistic first-order logic
- Classical and intuitionistic modal logics
- Bi-intuitionistic logic (depending on exclusion semantics)

# Example 2: Löwenheim-Skolem Theorems

(jww. Haoyi Zeng)

# The Downwards Löwenheim-Skolem Theorem[2]

## Definition (Elementary Submodels)

Given first-order models $\mathcal{M}$ and $\mathcal{N}$, we call $h : \mathcal{M} \to \mathcal{N}$ an elementary embedding if

$$\forall \rho : \mathbb{N} \to \mathcal{M}.\, \forall \varphi.\, \mathcal{M} \vDash_\rho \varphi \leftrightarrow \mathcal{N} \vDash_{h \circ \rho} \varphi.$$

If such an elementary embedding $h$ exists, we call $\mathcal{M}$ an elementary submodel of $\mathcal{N}$.

## Theorem (DLS)

*Every model has a countable elementary submodel.*

What is the constructive status of the DLS theorem?

[2] Löwenheim (1915); Skolem (1920)

# Classical Reverse Mathematics of DLS[3]

$$\begin{aligned} \mathsf{DC}_A &:= \forall R : A \to A \to \mathbb{P}.\, \mathsf{tot}(R) \to \exists f : \mathbb{N} \to A. \forall n.\, R\,(f\ n)\,(f\,(n+1)) \\ \mathsf{CC}_A &:= \forall R : \mathbb{N} \to A \to \mathbb{P}.\, \mathsf{tot}(R) \to \exists f : \mathbb{N} \to A. \forall n.\, R\, n\,(f\ n) \end{aligned}$$

## Theorem

*The* DLS *theorem is equivalent to* DC.

## Sketch.

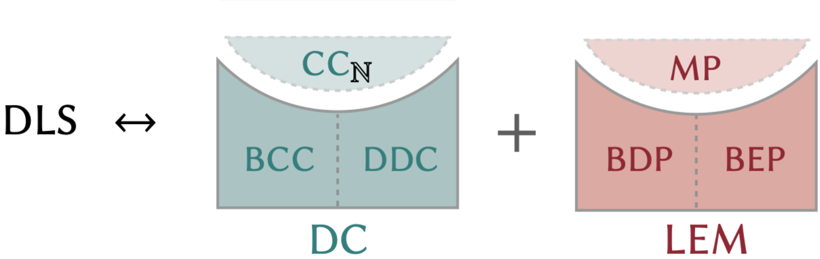
- To prove DLS from DC, arrange the iterative construction such that a single application of DC yields a path through all possible extensions that induces the resulting submodel.
- Starting with a total relation $R : A \to A \to \mathbb{P}$, consider $(A, R)$ a model. Applying DLS, obtain an elementary submodel $(\mathbb{N}, R')$ so in particular $R'$ is still total. Apply $\mathsf{CC}_{\mathbb{N}}$ to obtain a choice function for $R'$ that is reflected back to $A$ as a path through $R$. □

[3] Boolos et al. (2002); Espíndola (2012); Karagila (2014)

# Constructive Reverse Mathematics of DLS?

Over a base theory like the Calculus of Inductive Constructions of the Coq Proof Assistant:

1. Does the DLS theorem still follow from DC alone or is there some contribution of LEM?
2. Does the DLS theorem still imply DC or is there some contribution of CC?



# DLS using Henkin Environments

## Definition (Henkin Environment)

Given a model $\mathcal{M}$, we call $\rho : \mathbb{N} \to \mathcal{M}$ a Henkin environment if for all $\varphi$:

$$\exists n.\, \mathcal{M} \vDash_\rho \varphi[\rho\, n] \;\rightarrow\; \mathcal{M} \vDash_\rho \dot{\forall}\varphi$$
$$\exists n.\, \mathcal{M} \vDash_\rho \dot{\exists}\varphi \;\rightarrow\; \mathcal{M} \vDash_\rho \varphi[\rho\, n]$$

## Lemma

*Every model with a Henkin environment has a countable elementary submodel.*

## Proof.

Given a model $\mathcal{M}$ and a Henkin environment $\rho$, we obtain a countable elementary submodel as the syntactic model $\mathcal{N}$ constructed over the domain $\mathbb{T}$ of terms by setting

$$f^{\mathcal{N}}\, \vec{t} \;:=\; f\, \vec{t} \qquad \text{and} \qquad P^{\mathcal{N}}\, \vec{t} \;:=\; P^{\mathcal{M}}\, (\hat{\rho}\, \vec{t}). \quad \square$$

# The Drinker Paradox

In every bar, one can identify a person such that,
if they drink, then the whole bar drinks

$$\mathsf{DP}_A := \forall P : A \to \mathbb{P}.\, \exists x.\, P\,x \to \forall y.\, P\,y$$
$$\mathsf{EP}_A := \forall P : A \to \mathbb{P}.\, \exists x.\, (\exists y.\, P\,y) \to P\,x$$

## Fact (contrasting Warren and Diener (2018))

DP *and* EP *are equivalent to* LEM*.*

## Proof.

To derive LEM from DP, given $p : \mathbb{P}$ use DP for $A := \{b : \mathbb{B} \mid b = \mathsf{false} \lor (p \lor \neg p)\}$ and $P : A \to \mathbb{P}$ defined by $P\,(\mathsf{true}, \_) := \neg p$ and $P\,(\mathsf{false}, \_) := \top$. □

# DLS assuming DC and LEM

**Theorem**

*Assuming* DC *and* LEM, *the* DLS *theorem holds.*

**Proof.**

Construct a Henkin environment in three steps:

1. Given some environment $\rho$, we know by DP and EP that, relative to $\rho$, Henkin witnesses for all formulas exist.
2. Applying CC we can simultaneously choose from these witnesses at once and therefore extend to some environment $\rho'$.
3. This describes a total relation on environments, through which DC yields a path that can be merged into a single environment, and that then must be Henkin. □

# Reverse Analysis

**Theorem**

*Assuming* $\mathrm{CC}_{\mathbb{N}}$, *the* DLS *theorem implies* DC.

**Proof.**

Following the outline from the beginning, using the assumption of $CC_{\mathbb{N}}$ to obtain a choice function in the countable elementary submodel. □

So over $\mathrm{CC}_{\mathbb{N}}$ and LEM, the DLS theorem is equivalent to DC.

# DLS using Blurred Henkin Environments

## Definition (Henkin Environment)

Given a model $\mathcal{M}$, we call $\rho : \mathbb{N} \to \mathcal{M}$ a blurred Henkin environment if or all $\varphi$:

$$(\forall n.\, \mathcal{M} \vDash_\rho \varphi[\rho\, n]) \;\to\; \mathcal{M} \vDash_\rho \dot{\forall} \varphi$$

$$\mathcal{M} \vDash_\rho \dot{\exists} \varphi \;\to\; (\exists n.\, \mathcal{M} \vDash_\rho \varphi[\rho\, n])$$

## Lemma

*Every model with a blurred Henkin environment has a countable elementary submodel.*

## Proof.

Given a model $\mathcal{M}$ and a blurred Henkin environment $\rho$, we obtain a countable elementary submodel as the same syntactic model $\mathcal{N}$ constructed over the domain $\mathbb{T}$ from before. □

# The Blurred Drinker Paradox (BDP)

In every bar, there is an at most countable group such that, if all of them drink, the the whole bar drinks

$$\begin{aligned} \mathsf{BDP}_A &:= \forall P : A \to \mathbb{P}. \exists f : \mathbb{N} \to A. (\forall n. P\,(f\,n)) \to \forall x. P\,x \\ \mathsf{BEP}_A &:= \forall P : A \to \mathbb{P}. \exists f : \mathbb{N} \to A. (\exists x. P\,x) \to \exists n. P\,(f\,n) \end{aligned}$$

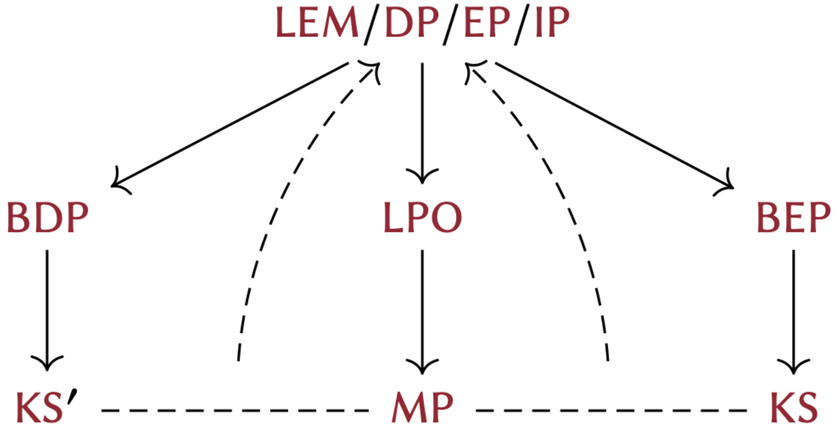
**Fact**

LEM *decomposes into* $\mathsf{BDP} + \mathsf{DP}_{\mathbb{N}}$ *and even* $\mathsf{BDP} + \mathsf{MP}$*, similarly for* BEP*.*

**Proof.**

The first decomposition is trivial. The latter follows since BDP implies Kripke's schema (KS) which is known to imply LEM in connection to MP. □

# Classification of BDP



# DLS assuming DC and BDP

**Theorem**

*Assuming* DC *and* BDP/BEP, *the* DLS *theorem holds.*

**Proof.**

Construct a blurred Henkin environment in three steps:

1. Given some environment $\rho$, we know by BDP/BEP that, relative to $\rho$, blurred Henkin witnesses for all formulas exist.
2. Applying CC we can simultaneously choose from these witnesses at once and therefore extend to some environment $\rho'$.
3. This describes a total relation on environments through which DC yields a path, that can be merged into a single environment, and that then must be blurred Henkin. □

# Reverse Analysis

**Theorem**

*The* DLS *theorem implies* BDP *and* BEP*.*

**Proof.**

Using the same pattern as in the previous analysis, basically DLS reduces BDP to the trivially provable $\mathrm{BDP}_{\mathbb{N}}$, respectively BEP to the trivially provable $\mathrm{BEP}_{\mathbb{N}}$. □

So over $\mathrm{CC}_{\mathbb{N}}$, the DLS theorem decomposes into DC+BDP+BEP.

# Blurred Choice Axioms

$$\begin{aligned}\mathsf{BCC}_A &:= \forall R : \mathbb{N}\to A\to\mathbb{P}.\, \mathsf{tot}(R) \to \exists f : \mathbb{N}\to A. \forall n.\exists m.\, R\, n\, (f\; m)\\ \mathsf{DDC}_A &:= \forall R : A\to A\to\mathbb{P}.\, \mathsf{dir}(R) \to \exists f : \mathbb{N}\to A.\, \mathsf{dir}(R\circ f)\end{aligned}$$

**Lemma**

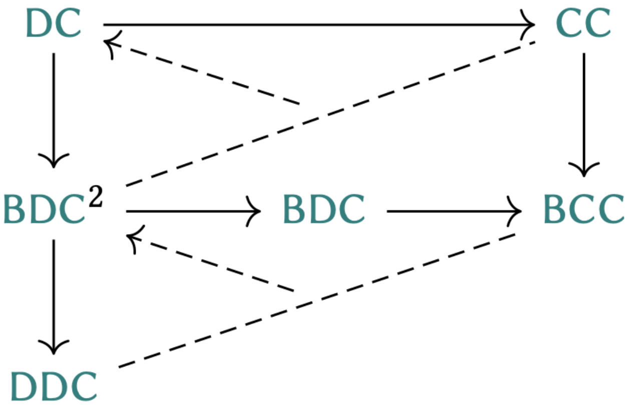
CC *decomposes into* BCC + $\mathsf{CC}_{\mathbb{N}}$ *and* DC *decomposes into* DDC + CC.

$$\mathsf{BDC}^2_A := \forall R : A^2\to A\to\mathbb{P}.\, \mathsf{tot}(R) \to \exists f : \mathbb{N}\to A.\, \mathsf{tot}(R\circ f)$$

**Lemma**

$\mathsf{BDC}^2$ *decomposes into* BCC + DDC.

# Classification of Blurred Choice Axioms



# DLS assuming BDC and BDP

## Theorem

*Assuming* $\mathsf{BDC}^2$ *and* BDP/BEP, *the* DLS *theorem holds.*

## Proof.

Construct a blurred Henkin environment in three steps:

1. Given some environment $\rho$, we know by BDP/BEP that, relative to $\rho$, blurred Henkin witnesses for all formulas exist.
2. Applying BCC we can simultaneously choose from these witnesses at once and therefore extend to some environment $\rho'$.
3. This describes a directed relation on environments, through which DDC yields a path that can be merged into a single environment, and that then must be blurred Henkin. □

# Reverse Analysis

**Theorem**

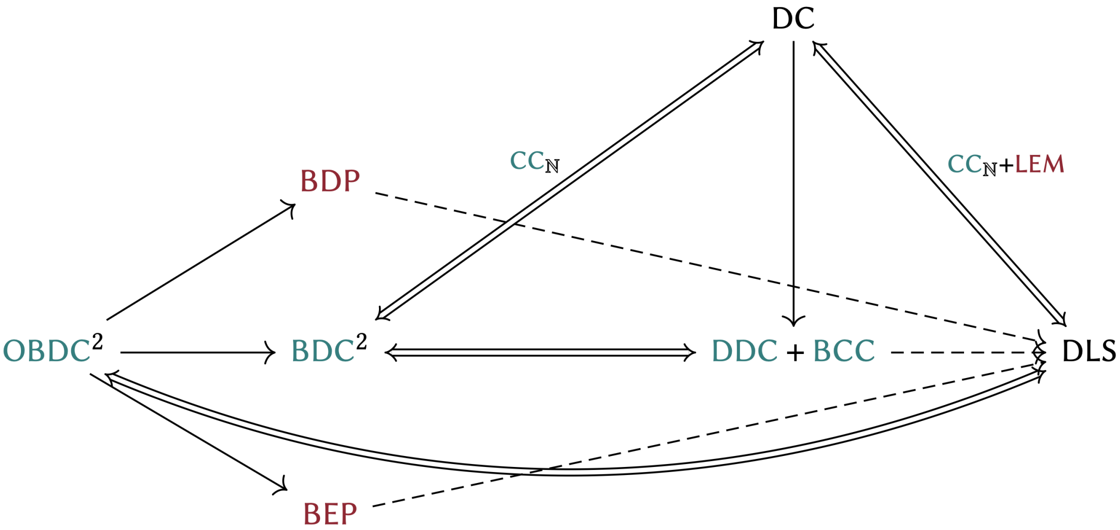
*The* DLS *theorem implies* $\mathsf{BDC}^2$ *and therefore also* BCC *and* DDC.

**Proof.**

Using the same pattern as in the previous analyses. □

So the DLS theorem decomposes into $\mathsf{BDC}^2 + \mathsf{BDP} + \mathsf{BEP}$.

# Overview



# Ongoing Work

- What happens with uncountable cardinalities?
  - Weaker forms of blurred drinker paradoxes, stronger forms of blurred choice principles
- Are the blurred principles weaker than the original?
  - We expect BDP $\not\to$ LEM, BCC $\not\to$ CC, and DDC $\not\to$ BCC
- What is the constructive status of the upwards Löwenheim-Skolem theorem?
  - Usual proof strategy uses compactness which is as non-constructive as completeness

# Example 3: Post's Problem

(jww. Yannick Forster, Niklas Mück, Takako Nemoto, Haoyi Zeng)

# Synthetic Computability[4]

Exploit that in constructive foundations, every definable function is computable:

$$P : X \to \mathbb{P} \text{ is decidable} := \exists d : X \to \mathbb{B}.\, \forall x.\, P\,x \leftrightarrow d\,x = \text{true}$$
$$P : X \to \mathbb{P} \text{ is semi-decidable} := \exists s : X \to \mathbb{N} \to \mathbb{B}.\, \forall x.\, P\,x \leftrightarrow (\exists n.\, s\,x\,n = \text{true})$$

Pros:

- Avoid manipulating Turing machines or equivalent model of computation
- Elegant formalisation (e.g. in CIC), feasible mechanisation (e.g. in Coq)

Cons:

- Finding a correct synthetic rendering of Turing reductions not so straightforward
- Some attempts: Bauer (2021); Forster (2021); Forster and Kirst (2022); Mück (2022)

[4] Richman (1983); Bauer (2006); Forster, Kirst and Smolka (2019)

# Synthetic Oracle Computability

**Definition (Forster, Kirst and Mück (2023))**

An oracle computation is a functional $F\colon (Q \to A \to \mathbb{P}) \to I \to O \to \mathbb{P}$ captured by a computation tree $\tau\colon I \to A^* \rightharpoonup Q + O$ and its induced interrogation relation $\tau\, i\, ; R \vdash qs ; as$ as follows:

$$\frac{}{\sigma\, ; R \vdash [\,]\, ; [\,]} \qquad \frac{\sigma\, ; R \vdash qs\, ; as \qquad \sigma\, as \triangleright \mathrm{ask}\; q \qquad R q a}{\sigma\, ; R \vdash qs \mathbin{+\!\!+} [q]\, ; as \mathbin{+\!\!+} [a]}$$

$$F\, R\, i\, o \;\leftrightarrow\; \exists qs\, as.\; \tau\, i\, ; R \vdash qs ; as \land \tau\; i\; as \triangleright \mathrm{out}\; o$$

$P \preceq_T Q \;:=\;$ there is an oracle computation $F\colon (\mathbb{N} \to \mathbb{B} \to \mathbb{P}) \to \mathbb{N} \to \mathbb{B} \to \mathbb{P}$ with $F\, Q = P$

$\mathcal{S}_Q(P) \;:=\;$ there is an oracle computation $F\colon (\mathbb{N} \to \mathbb{B} \to \mathbb{P}) \to \mathbb{N} \to \mathbb{1} \to \mathbb{P}$ with $\mathrm{dom}(F\, Q) = P$

# Enumerating Oracle Computations

We need an enumeration of oracle computations for diagonalisations / Turing jump...

For consistency (with LEM), we start from a standard axiom (Kreisel (1965); Forster (2021)):

$$\mathsf{EPF} := \exists \theta{:}\,\mathbb{N} \to (\mathbb{N} \rightharpoonup \mathbb{N}).\, \forall f{:}\,\mathbb{N} \rightharpoonup \mathbb{N}.\, \exists e{:}\,\mathbb{N}.\, \forall xv.\, \theta_e\, x \downarrow v \leftrightarrow f\, x \downarrow v$$

**Theorem (Forster, Kirst and Mück (2024))**

*There is an enumerator of functionals* $\Phi{:}\,\mathbb{N} \to (\mathbb{N} \to \mathbb{B} \to \mathbb{P}) \to \mathbb{N} \to \mathbb{B} \to \mathbb{P}$ *such that*

1. $\Phi_e$ *is an oracle computation for all* $e : \mathbb{N}$
2. *Given an oracle computation* $F$ *there is* $e : \mathbb{N}$ *such that* $\forall Rxb.\, \Phi_e^R(x) \downarrow b \leftrightarrow F\, R\, x\, b$
3. *The Turing jump* $P'\, x := \Phi_x^P(x) \downarrow \mathsf{true}$ *of* $P$ *is strictly harder than* $P$
4. *The halting problem* $H := \emptyset'$ *is undecidable*

# Post's Problem

Is there a semi-decidable yet undecidable set $S$ with $H \not\preceq_T S$?

- Left as an open problem by Post (1944)
- Positive solution by Friedberg (1957) and Muchnik (1956)
- Low simple set construction by Lerman and Soare (1980)

- Synthetic proof mechanised in Coq by Zeng et al. (2024), relying on $\Sigma_2$-LEM
- Analytic proof given by Nemoto (2024), relying only on $\Sigma_1$-LEM / LPO
- Combination yields a synthetic and mechanised proof using LPO

# Low Simple Sets and Limit Computability

**Definition (Lerman and Soare (1980) and Post (1944))**

$P : X \to \mathbb{P}$ is low if $P' \preceq_T H$ and simple if it is co-infinite, semi-decidable, and for $W_e$ being the $e$-th enumerable set we have $W_e \cap P \neq \emptyset$ whenever $W_e$ is infinite.

$\Rightarrow$ Every low simple set is a solution to Post's problem!

**Definition (Shoenfield (1959) and Gold (1965))**

$P : X \to \mathbb{P}$ is limit-computable if there exists a function $f : X \to \mathbb{N} \to \mathbb{B}$ with

$$Px \;\leftrightarrow\; \exists n.\forall m > n.\ f(x,m) = \text{true} \quad \wedge \quad \neg Px \;\leftrightarrow\; \exists n.\forall m > n.\ f(x,m) = \text{false}.$$

$\Rightarrow$ Limit-computability provides easy way to prove lowness...

# Limit Lemma

**Lemma (1)**

*If $\mathcal{S}_Q(P)$ and $\mathcal{S}_Q(\overline{P})$ then $P \preceq_T Q$.*

**Lemma (2)**

*Assuming $\Sigma_n$-LEM, if $P$ is $\Sigma_{n+1}$ and $Q$ is $\Sigma_n$, then $\mathcal{S}_Q(P)$.*

**Lemma (Limit Lemma)**

*Assuming LPO, if $P$ is limit computable, then $P \preceq_T H$.*

**Proof.**

If $P$ is limit computable, then immediately by definition both $P$ and $\overline{P}$ are $\Sigma_2$. Moreover, since the halting problem $H$ is $\Sigma_1$, Lemma 2 together with LPO yields both $\mathcal{S}_H(P)$ and $\mathcal{S}_H(\overline{P})$. From there we conclude $P \preceq_T H$ with Lemma 1. □

# The Priority Method

Fix step function $\gamma : \mathbb{N}^* \to \mathbb{N} \to \mathbb{N} \to \mathbb{P}$, approximate $S$ inductively:

$$\frac{}{0 \rightsquigarrow [\,]} \qquad \frac{n \rightsquigarrow L \quad \gamma_n^L\ x}{n+1 \rightsquigarrow x :: L} \qquad \frac{n \rightsquigarrow L \quad \forall x.\ \neg\ \gamma_n^L\ x}{n+1 \rightsquigarrow L}$$

Depending on properties of $\gamma$ we obtain for $S\,x := \exists n, L.\ n \rightsquigarrow L \land x \in L$ that:

- $\gamma$ is computable $\Rightarrow$ $S$ is semi-decidable
- $S$ satisfies $P_e :=$ $W_e$ is infinite $\to W_e \cap S \neq \emptyset$ $\Rightarrow$ $S$ is simple
- $S$ satisfies $N_e := (\exists^\infty n.\ \Phi_e^S(e)[n]\downarrow) \to \Phi_e^S(e)\downarrow$ $\Rightarrow$ $S'$ is limit computable (using LPO)

# Wall Functions

## Definition

The use function $U_e^P(x)$ approximates the continuity information of the oracle computation $\Phi_e^P(x)$ in a step-indexed way.

Define suitable $\gamma$ again relative to a wall function $\omega$ of same type:

- $\omega_n^L(e) \geq 2 \cdot e \;\Rightarrow\; S$ satisfies the requirements $P_e$
- $\omega_n^L(e) \geq \max_{e' \leq e} U_{e'}^L(e')[n] \;\Rightarrow\; S$ satisfies the requirements $N_e$ (using LPO)

## Theorem

*Assuming LPO, a low simple set exists.*

## Proof.

Choose the wall function $\omega := \max(2 \cdot e, \max_{e' \leq e} U_{e'}^L(e')[n])$. □

# Ongoing Work

Reverse analysis:

- LPO needed for limit lemma?
- LPO needed to show that $S'$ is limit computable?
- LPO needed to construct a low simple set?

Generalisation:

- Friedberg-Muchnik theorem
- Low basis theorem
- Connections to true second-order arithmetic

# Conclusion

# Topics we can discuss

- Constructive reverse mathematics
  - Analyse more theorems, identify robust base systems...
- Synthetic computability theory
  - Translate more theorems, analyse constellations of axioms...
- Development of Coq libraries
  - Extend library of first-order logic, implement more tool support...
- Models of constructive type theory
  - Study effectful realisability models, establish consistentcy of CIC+CT+LEM...
- Formalised numerical analysis
  - Mechanise singular Euler-Maclaurin expansion, explore use of proof assistants in physics...

# Bibliography I


Bauer, A. (2006). First steps in synthetic computability theory. *Electronic Notes in Theoretical Computer Science*, 155:5–31.

Bauer, A. (2021). Synthetic mathematics with an excursion into computability theory. University of Wisconsin Logic seminar.

Boolos, G. S., Burgess, J. P., and Jeffrey, R. C. (2002). *Computability and logic*. Cambridge university press.

Diener, H. (2018). Constructive reverse mathematics: Habilitationsschrift. Universität Siegen.

Espíndola, C. (2012). Löwenheim-skolem theorems and choice principles. Technical report.

Forster, Y. (2021). *Computability in Constructive Type Theory*. PhD thesis, Saarland University.

Forster, Y. and Kirst, D. (2022). Synthetic Turing reducibility in constructive type theory. 28th International Conference on Types for Proofs and Programs (TYPES 2022).

Forster, Y., Kirst, D., and Mück, N. (2023). Oracle computability and turing reducibility in the calculus of inductive constructions. In *Asian Symposium on Programming Languages and Systems*. Springer.

Forster, Y., Kirst, D., and Mück, N. (2024). The kleene-post and post's theorem in the calculus of inductive constructions. In *32nd EACSL Annual Conference on Computer Science Logic (CSL 2024)*.

# Bibliography II


Forster, Y., Kirst, D., and Smolka, G. (2019). On synthetic undecidability in Coq, with an application to the Entscheidungsproblem. In *Proceedings of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs*.

Forster, Y., Kirst, D., and Wehr, D. (2021). Completeness theorems for first-order logic analysed in constructive type theory. *Journal of Logic and Computation*.

Friedberg, R. M. (1957). Two recursively enumerable sets of incomparable degrees of unsovlability (solution of Post's problem), 1944. *Proceedings of the National Academy of Sciences*, 43(2):236–238.

Friedman, H. M. (1976). Systems on second order arithmetic with restricted induction i, ii. *J. Symb. Logic*, 41:557–559.

Gold, E. M. (1965). Limiting recursion. *The Journal of Symbolic Logic*, 30(1):28–48.

Hagemeier, C. and Kirst, D. (2022). Constructive and mechanised meta-theory of intuitionistic epistemic logic. In *International Symposium on Logical Foundations of Computer Science*. Springer.

Henkin, L. (1954). Metamathematical theorems equivalent to the prime ideal theorem for boolean algebras. *Bulletin AMS*, 60:387–388.

Herbelin, H. (2022). Computing with gödel's completeness theorem: Weak fan theorem, markov's principle and double negation shift in action. `http://pauillac.inria.fr/~herbelin/talks/chocola22.pdf`.

# Bibliography III


Herbelin, H. and Ilik, D. (2016). An analysis of the constructive content of henkin's proof of gödel's completeness theorem.

Ishihara, H. (2006). Reverse mathematics in bishop's constructive mathematics. *Philosophia Scientiæ. Travaux d'histoire et de philosophie des sciences*, (CS 6):43–59.

Karagila, A. (2014). Downward löwenheim-skolem theorems and choice principles. Technical report.

Kirst, D. (2022). *Mechanised Metamathematics: An Investigation of First-Order Logic and Set Theory in Constructive Type Theory*. PhD thesis, Saarland University. Under review, `https://www.ps.uni-saarland.de/~kirst/thesis/`.

Kreisel, G. (1962). On weak completeness of intuitionistic predicate logic. *The Journal of Symbolic Logic*, 27(2):139–158.

Kreisel, G. (1965). Mathematical logic. In Kreisel, G., editor, *Lectures on Modern Mathematics*, pages 95–195. Wiley.

Krivine, J.-L. (1996). Une preuve formelle et intuitionniste du théorčme de complétude de la logique classique. *Bulletin of Symbolic Logic*, 2(4):405–421.

Krivtsov, V. N. (2015). Semantical completeness of first-order predicate logic and the weak fan theorem. *Studia Logica*, 103(3):623–638.

# Bibliography IV


Lerman, M. and Soare, R. (1980). $d$-simple sets, small sets, and degree classes. *Pacific Journal of Mathematics*, 87(1):135–155.

Löwenheim, L. (1915). Über möglichkeiten im relativkalkül. *Mathematische Annalen*, 76(4):447–470.

Muchnik, A. A. (1956). On the unsolvability of the problem of reducibility in the theory of algorithms. In *Dokl. Akad. Nauk SSSR*, volume 108, page 1.

Mück, N. (2022). *The Arithmetical Hierarchy, Oracle Computability, and Post's Theorem in Synthetic Computability*. Bachelor's thesis, Saarland University.

Nemoto, T. (2024). Computability theory over intuitionistic logic. Logic Colloquium 2024, European Summer Meeting of the Association for Symbolic Logic, Gothenburg, Sweden.

Post, E. L. (1944). Recursively enumerable sets of positive integers and their decision problems. *bulletin of the American Mathematical Society*, 50(5):284–316.

Richman, F. (1983). Church's thesis without tears. *The Journal of symbolic logic*, 48(3):797–803.

Shoenfield, J. R. (1959). On degrees of unsolvability. *Annals of mathematics*, 69(3):644–653.

Simpson, S. G. (2009). *Subsystems of second order arithmetic*, volume 1. Cambridge University Press.

# Bibliography V

Skolem, T. (1920). Logisch-kombinatorische untersuchungen Über die erfüllbarkeit oder bewiesbarkeit mathematischer sätze nebst einem theorem Über dichte mengen. In *Selected Works in Logic*. Universitetsforlaget.

Umezawa, T. (1959). On logics intermediate between intuitionistic and classical predicate logic. *The Journal of Symbolic Logic*, 24(2):141–153.

Warren, L., Diener, H., and McKubre-Jordens, M. (2018). The drinker paradox and its dual. *arXiv preprint arXiv:1805.06216*.

Zeng, H., Forster, Y., and Kirst, D. (2024). Post's problem and the priority method in cic. In *30th International Conference on Types for Proofs and Programs TYPES 2024–Abstracts*, page 27.