

Canonicity for Indexed Inductive-Recursive Types

ANONYMOUS AUTHOR(S)

We prove canonicity for a Martin-Löf type theory that supports a countable universe hierarchy where each universe supports indexed inductive-recursive (IIR) types. We proceed in two steps. First, we construct IIR types from inductive-recursive (IR) types and intensional identity types, in order to simplify the subsequent canonicity proof. The constructed IIR types support the same definitional computation rules that are available in Agda's native IIR implementation. Second, we give a canonicity proof for IR types, building on the well-known method of Artin gluing. The main idea is to encode the canonicity predicate for each IR type using a metatheoretic IIR type. In short, we reduce IIR types to IR types, then use metatheoretic IIR types to prove canonicity for IR types.

ACM Reference Format:

Anonymous Author(s). 2018. Canonicity for Indexed Inductive-Recursive Types. *J. ACM* 37, 4, Article 111 (August 2018), 3 pages. <https://doi.org/XXXXXXX.XXXXXXX>

1 Introduction

Induction-recursion (IR) was first used by Martin-Löf in an informal way [?], then made formal by Dybjer and Setzer [?], who also developed set-theoretic and categorical semantics [?]. A common application of IR is to define custom universe hierarchies inside a type theory. In the proof assistant Agda, we can use IR to define a universe that is closed under our choice of type formers:

```
mutual
data U : Set0 where
  Nat' : U
  Π'   : (A : U) → (El A → U) → U

El : U → Set0
El Nat'   = Nat
El (Π' A B) = (a : El A) → El (B a)
```

This U, unlike the ambient Set₀ universe, supports an induction principle and can be used to define type-generic functions. *Indexed induction-recursion* (IIR) additionally allows indexing U over some type, which lets us define inductive-recursive predicates [?].

One application of IR has been to develop semantics for object theories that support universe hierarchies. IR has been used in normalization proofs [?], in modeling first-class universe levels [?] and proving canonicity for them [?], and in characterizing domains of partial functions [?]. Another application is to do generic programming over universes of type descriptions [?] or data layout descriptions [?].

IIR has been supported in Agda 2 since the early days of the system [?], and it is also available in Idris 1 and Idris 2 [?]. In these systems, IR has been implemented in the “obvious” way, supporting

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2018 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM 1557-735X/2018/8-ART111

<https://doi.org/XXXXXXX.XXXXXXX>

closed program execution in compiler backends and normalization during type checking, but without any formal justification.

Our **main contribution** is to **show canonicity** for a Martin-Löf type theory that supports a countable universe hierarchy, where each universe supports indexed inductive-recursive types. Canonicity means that every closed term is definitionally equal to a canonical term. Canonical terms are built only from constructors; for instance, a canonical natural number term is a numeral. Hence, canonicity justifies evaluation for closed terms. The outline of our development is as follows.

- (1) In Section ?? we specify what it means to support IR and IIR, using Dybjer and Setzer's rules with minor modifications [?]. We use first-class signatures, meaning that descriptions of (I)IR types are given as ordinary inductive types internally.
- (2) In Section ?? we construct IIR types from IR types and other basic type formers. This allows us to only consider IR types in the subsequent canonicity proof, which is a significant simplification. In the construction of IIR types, we lose some definitional equalities when IIR signatures are neutral, but we still get strict computation for canonical signatures. This matches the computational behavior of Agda and Idris, where IIR signatures are second-class and necessarily canonical. We formalize the construction in Agda.
- (3) In Section ??, we give a proof-relevant logical predicate interpretation of the type theory, from which canonicity follows. We follow the well-known method of Artin gluing [?]. The main challenge here is to give a logical predicate interpretation of IR types. We do this by using IIR in the metatheory: from each object-theoretic signature we compute a metatheoretic IIR signature which encodes the canonicity predicate for the corresponding IR type. We formalize the predicate interpretation of IR types in Agda, using a shallow embedding of the syntax of the object theory. Hence, there is a gap between the Agda version and the fully formal construction, but we argue that it is a modest gap.

2 Specification for (I)IR types

In this section we describe the object type theory, focusing on the specification of IR and IIR types. We do not yet go into the formal details of structure of the object type theory; instead, we mostly give internal definitions in an Agda-like syntax. We give an overview of the object theory.

We have a countable hierarchy of Russell-style universes, written as U_i , where i is an external natural number. We have $U_i : U_{i+1}$. We take maxima of universe levels for sizes of type formers. For example, the Π -type $(x : A) \rightarrow B x$ is in $U_{\max(i, j)}$ when $A : U_i$ and $B : A \rightarrow U_j$. We also have a lifting operation $\text{Lift } i j : U_i \rightarrow U_j$ together with $\uparrow : A \rightarrow \text{Lift } i j A$ and $\downarrow : \text{Lift } i j A \rightarrow A$ such that \uparrow and \downarrow are definitional inverses. We have intensional identity types, as $t = u : U_i$ for $t : A : U_i$.

2.1 IR types

The IR specification is parameterized over the following data:

- The level i is the size of the IR type that is being specified.
- The level j is the size of the recursive output type.
- $O : U_j$ is the output type.

IR signatures are specified by the following inductive type:

```
data Sig : Umax(i+1, o)
  ι : O → Sig
  σ : (A : Ui) → (A → Sig) → Sig
  δ : (A : Ui) → ((A → O) → Sig) → Sig
```

Example 2.1. The Agda example on Figure [?] can be specified as follows. We assume a

3 TODO

- Small IIR paper: reduction of small IIR to IR + identity, similar to mine
- Bove-Capretta: IIR is used to model domains of partial functions.
- Canonicity metatheory: Loic, Anton say it looks OK

a

References