



HAL
open science

Observational Equality: Now For Good

Loïc Pujet, Nicolas Tabareau

► **To cite this version:**

Loïc Pujet, Nicolas Tabareau. Observational Equality: Now For Good. POPL, Jan 2022, Philadelphie, United States. hal-03367052v1

HAL Id: hal-03367052

<https://inria.hal.science/hal-03367052v1>

Submitted on 6 Oct 2021 (v1), last revised 10 Nov 2021 (v4)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Observational Equality: Now For Good

LOÏC PUJET, Inria, France

NICOLAS TABAREAU, Inria, France

Building on the recent extension of dependent type theory with a universe of definitionally proof-irrelevant types, we introduce TT^{obs} , a new type theory based on the setoidal interpretation of dependent type theory. TT^{obs} equips every type with an identity relation that satisfies function extensionality, propositional extensionality, and definitional uniqueness of identity proofs (UIP). Compared to other existing proposals to enrich dependent type theory with these principles, our theory features a notion of reduction that is normalizing and provides an algorithmic canonicity result, which we formally prove in AGDA using the logical relation framework of Abel et al. Our paper thoroughly develops the meta-theoretical properties of TT^{obs} , such as the decidability of the conversion and of the type checking, as well as consistency. We also explain how to extend our theory with quotient types, and we introduce a setoidal version of Swan’s Id types that turn it into a proper extension of MLTT with inductive equality.

CCS Concepts: • **Theory of computation** → **Type theory**.

Additional Key Words and Phrases: type theory, dependent types, rewriting theory, confluence, termination

1 INTRODUCTION

Dependent type theories and in particular MLTT, as originally developed by [Martin-Löf \[1975\]](#), provide an adequate framework for developing constructive mathematics and certifying software. A core aspect of MLTT is the coexistence of two distinct notions of equality: a *definitional* equality that records the equations automated by the system, and a *propositional* equality that is a type internal to the system and thus can be used to do equational reasoning. However, the propositional equality of MLTT lacks some extensionality principles that pervade mathematical reasoning, such as function extensionality (funext). Since they are generally considered desirable, these principles are sometimes added as axioms, but doing so results in a system with weaker computational properties.

Throughout the years, several options to obtain a more extensional version of propositional equality while preserving computation have been explored. The most successful lines of work can be roughly divided into two groups: the ones using an observational equality, and the ones using a cubical equality. Both notions build on the following fundamental idea: in order to obtain sufficient extensionality principles, the behavior of equality in a given type should be explicitly specified for every type instead of using a single definition that is parametric over the types.

The work on observational equality originated from the study of the setoid model of type theory [Altenkirch \[1999\]](#); [Hofmann \[1995\]](#), and a first attempt at a proper type theory that supports an observational equality satisfying funext has been proposed in [Altenkirch et al. \[2007\]](#). In these systems, observational equality equips every type with a setoid structure. This setoidal equality satisfies the uniqueness of identity proofs (UIP), that states that all proofs of an equality are equal; in other words, equality is proof irrelevant.

The other line of work is more recent and takes its roots in the formulation of the univalence axiom [Kapulkin et al. \[2012\]](#), that gives a new meaning to the equality between types: two types are equal when they equivalent. This can be understood as an extensionality principle for the universe of types. In their search for a computational interpretation of univalence, [Cohen et al. \[2015\]](#)

50 developed a notion of cubical equality, which satisfies funext and univalence, but is incompatible
51 with UIP.

52 Thus, observational equality and cubical equality are two diverging directions for providing
53 propositional equality with more extensionality. [Altenkirch et al. \[2016\]](#); [Capriotti \[2017\]](#); [Voevodsky
54 \[2013\]](#) advocates that the two solutions are actually complementary and can be integrated to a
55 single system with two universe hierarchies, one that satisfies univalence and the other that satisfies
56 UIP. While cubical type theory has been thoroughly investigated and even implemented in the
57 AGDA proof assistant [Vezzosi et al. \[2019\]](#), observational equality has not reached a comparable
58 level of maturity. Recent attempts to design a type theory based on observational equality are
59 either extensional [Sterling et al. \[2019\]](#), thus lacking an algorithm for type checking, or restricted
60 to a single universe and having computational properties only up to a conjecture [Altenkirch et al.
61 \[2019\]](#). Indeed, the latter relies on computation in an enriched version of MLTT that features a
62 universe of definitionally proof-irrelevant types (noted hereafter Ω_i) as recently proposed by [Gilbert
63 et al. \[2019\]](#), along with a proof-irrelevant identity type that supports a strong eliminator. This
64 theory has not been justified yet, and it has even been shown not to be normalizing in presence of
65 impredicativity [Abel and Coquand \[2020\]](#).

66 In this paper, we define TT^{obs} , the first extension of $\text{MLTT} + \Omega_i$ with an observational equality
67 which satisfies UIP, funext and propext, and supports quotient types and countably many universes
68 —with a proof of normalization and canonicity formalized in AGDA.¹ Firstly, we remark that this
69 theory can only be derived in a system with some level of cumulativity, as it is required for certain
70 computation rules to be well-typed. This makes explicit some difficulties that do not show up in
71 previous works. Second, we remark that our version of observational equality can be equipped
72 with two elimination principles: a notion of type cast (or coercion) for proof relevant types, and
73 the standard eliminator of MLTT for proof irrelevant types, thus making all the setoidal structure
74 derivable from the standard eliminator. Funext and propext are obtained by specifying the right
75 computation rules for observational equality whereas UIP is obtained for free by interpreting
76 observational equality in Ω .

77 The proof of normalization and canonicity is based on the use of logical relations defined in
78 AGDA using induction-recursion as initially developed by [Abel et al. \[2018\]](#) and later extended
79 to Ω by [Gilbert et al. \[2019\]](#). Compared to previous work on formalized normalization proofs,
80 we have added the support for a cumulative hierarchy with two universes, and we make a clear
81 distinction between inhabitants of proof-irrelevant types, which have no computational behavior,
82 and inhabitants of proof relevant types, which do. This key change allows us to add new principles
83 in Ω without having to supply them with a computational behavior, trivializing for instance the
84 management of higher coherences of the cubical interpretation. In counterpart for this added
85 flexibility, normalization does not directly implies canonicity anymore, and a separate proof of
86 consistency of the theory is required to derive canonicity. This proof is done by defining a model
87 for TT^{obs} , but as consistency is the only consequence that we need from the existence of a model,
88 the model can be defined in an extensional setting.

89 To illustrate the simplicity of extending $\text{MLTT} + \Omega$ to TT^{obs} , we have implemented a simple version
90 in AGDA using rewrite rules, as recently introduced by [Cockx et al. \[2021\]](#), which is available in the
91 anonymous supplementary material (file [\[setoid_rr.agda\]](#)).

92
93 *Plan of the paper.* In Section 2, we present the syntax and typing rules of TT^{obs} , focusing on its
94 notions of conversion and reduction. Then in Section 3, we develop the logical relation framework,
95 and the model from which we derive consistency. This shows normalization, canonicity and
96 decidability of typechecking for TT^{obs} . In Section 4, we explain how to extend TT^{obs} to support

97 ¹Formalization available as anonymous material, references to a particular file are done using [\[myfolder/myfile.agda\]](#).

99	s	$::= \mathcal{U} \mid \Omega$	Relevances
100	i, j	$\in \mathbb{N}$	Universe levels
101	Γ, Δ	$::= \bullet \mid \Gamma, x : s_i^i A$	Contexts
102	t, u, m, n, e, A, B	$::= x \mid s_i$	Variables and Universes
103		$\mid \lambda(x : A). t \mid t u \mid \Pi_{s,i}^j(x : A). B$	Dependent products
104		$\mid 0 \mid S t \mid \mathbb{N}\text{-elim}(P, t, u, n) \mid \mathbb{N}$	Natural numbers
105		$\mid \langle t, u \rangle \mid \text{fst}(t) \mid \text{snd}(t) \mid \exists_i^j(x : A). B$	Existential types
106		$\mid \perp\text{-elim}(A, t) \mid \perp$	Empty type
107		$\mid * \mid \top$	Singleton type
108		$\mid t \sim_A u \mid \text{refl}(t) \mid \text{transp}(t, B, u, t', e)$	Observational equality
109		$\mid \text{cast}(A, B, e, t) \mid \text{castrefl}(A, t)$	Type cast

Fig. 1. Syntax of $\mathbb{T}\mathbb{T}^{\text{obs}}$

quotient types, box types and squash types, as well as the standard identity type of MLTT, while preserving meta-theoretical properties.

2 A TYPE THEORY WITH OBSERVATIONAL EQUALITY

$\mathbb{T}\mathbb{T}^{\text{obs}}$ has two cumulative hierarchies of universes. The first one, that we write \mathcal{U}_i (where i is a natural number), is the usual universe hierarchy of Martin-Löf type theory. The second family, that we write Ω_i , is the family of *definitionally proof-irrelevant types*, which means that any two inhabitants of a type $A : \Omega_i$ are convertible. This corresponds to the two hierarchies presented in Gilbert et al. [2019] and implemented in AGDA, except that we also introduce some cumulativity features that will prove useful when interpreting equality in the universe of propositions and for dependent function types. Having a proof-irrelevant hierarchy of types seems to be crucial to interpret an extensional equality which satisfies UIP. Indeed, it trivializes all of the higher coherences that naturally arise when considering proofs of equality between equalities, and provides a canonical inhabitant for the type that encodes UIP, which is simply given by reflexivity.

2.1 Syntax of $\mathbb{T}\mathbb{T}^{\text{obs}}$

The syntax of the sorts, contexts, terms and types of $\mathbb{T}\mathbb{T}^{\text{obs}}$ is specified in Fig. 1. The theory features cumulative dependent functions (noted $\Pi_{s,i}^j(x : A). B$) with η -equality, natural numbers, as well as proof-irrelevant dependent sums (noted $\exists(x : A). B$), a proof-irrelevant empty type (noted \perp) and unit type (noted \top). When B does not depend on A , we will write $A \rightarrow B$ instead of $\Pi(x : A). B$, and $A \wedge B$ instead of $\exists(x : A). B$. The capture-avoiding substitution of a variable x in a term A by the term t is noted $B[x := t]$. $\mathbb{T}\mathbb{T}^{\text{obs}}$ can also be extended with more primitives such as quotients or general inductive types, but we defer the treatment of those to Section 4 to better focus on the treatment of equality in the theory.

Compared to MLTT with proof irrelevant types, there are two fundamental new ingredients in $\mathbb{T}\mathbb{T}^{\text{obs}}$. The first is a proof-irrelevant observational equality type $t \sim_A u$ which encodes equality of t and u at type A , together with a term $\text{refl}(t)$ that witnesses reflexivity of this equality. The second is an operation that casts a term t from a type A to another type B according to a proof of equality e between A and B , which is noted $\text{cast}(A, B, e, t)$. This operation comes with a witness $\text{castrefl}(A, t)$ that casting between a type A and itself does nothing. Note that since observational equality is proof irrelevant, any proof of equality between A and A is convertible to $\text{refl}(A)$. The theory also features a generic transport $\text{transp}(t, B, u, t', e)$ when A and B are proof irrelevant.

Observational equality is quite different from the usual Martin-Löf Identity Type, which is an inductive type that computes via the J -eliminator. Instead, observational equality $t \sim_A u$ should be understood as an eliminator that reduces the type A to its weak head normal form, and then reduces by pattern-matching on it, much like the path type from Cubical Type Theory. In particular, the reduction rules for observational equality between two dependent products, or two types in Ω_i provide us with function extensionality and propositional extensionality by definition.

2.2 Typing Rules of \mathbb{T}^{obs}

The typing rules of \mathbb{T}^{obs} are presented in Fig. 2. They are based four kinds of judgments: $\vdash \Gamma$ (well-formedness of a context), $\Gamma \vdash t :^{s,i} A$ (typing of a term), $\Gamma \vdash t \equiv u :^{s,i} A$ (convertibility of terms), and $\Gamma \vdash t \Rightarrow u :^i A$ (weak-head reduction of relevant terms). To avoid clutter, we will omit the s,i annotations that denote the sort and level of a type as that can generally be inferred from the context.² Similarly, we will often omit the annotations on the dependent function type and simply write $\Pi(x : A). B$; except when the annotations are explicitly required to understand a rule. In all the judgments, s denotes either \mathcal{U} or Ω .

Generic rules and universes. Rules **CTX-NIL**, **CTX-CONS** and **VAR** describe the usual formation of contexts and typing of variables. Rule **CONV** stipulates that type checking is done modulo conversion of types. The formation rule for universes (Rule **UNIV**) states that both \mathcal{U}_i and Ω_i are relevant types. It is natural for Ω to be proof-relevant, since its inhabitants are types which are not convertible to one another despite being proof-irrelevant.

Dependent products. The formation of dependent products between a domain and a codomain that have different sorts and universe levels is allowed. The resulting type has the same relevance as the codomain, and a universe level that is higher than both the level of the domain and the level of the codomain (Rule **PI-FORM**). The sort of the domain and the levels of both the domain and the codomain are collected as annotation to the dependent function type for the convenience of the type checking algorithm. Note that the introduction of cumulativity in the formation of dependent products is a necessary complication of \mathbb{T}^{obs} as the rules that provide us with propositional extensionality and function extensionality can only be well-typed in the presence of cumulativity.

Rules **FUN** and **APP** are the usual rules of λ -abstraction and application. Note that the sort and level annotation are implicit as they can be inferred from the premises.

Existential types. \mathbb{T}^{obs} features proof-irrelevant dependent sums. They are required to describe the behavior of observational equality between two dependent functions types. We do not need them to be cumulative so we keep the formation rule as simple as possible (**\exists -FORM**).

We give a negative presentation of dependent sums with one introduction rule (Rule **PAIR**) and two projections (Rules **FST** and **SND**). Note that because of proof irrelevance, the negative and positive presentations are completely equivalent, and we do not need any rule to account for the computational behavior of projections, nor η -equality. This is because any well-typed equality between two inhabitants of a proof-irrelevant type is proven by reflexivity (modulo Rule **CONV**).

Natural numbers. Strictly speaking, all inductive types could be excluded from the core of \mathbb{T}^{obs} , and be considered as extensions. However, we decided to treat the example of natural numbers as we feel it is both very simple and a good illustration.

The type \mathbb{N} comes with a formation rule **N-FORM**, constructors **0** (Rule **ZERO**) and **S** (Rule **SUC**) and an elimination/induction principle given by Rule **N-ELIM**. Since we do not require cumulativity for the type of natural numbers, we decided to only allow it in the lowest universe \mathcal{U}_0 , but it could

²The interested reader may look at the AGDA formalization where all annotations have been made explicit.

197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245

$$\begin{array}{c}
\text{CTX-NIL} \\
\frac{}{\vdash \bullet} \\
\text{CTX-CONS} \\
\frac{\vdash \Gamma \quad \Gamma \vdash A : s_i}{\vdash \Gamma, x : A} \\
\text{VAR} \\
\frac{\vdash \Gamma \quad x : A \in \Gamma}{\Gamma \vdash x : A} \\
\text{CONV} \\
\frac{\Gamma \vdash t : A \quad \Gamma \vdash A \equiv B : s_i}{\Gamma \vdash t : B} \\
\text{UNIV} \\
\frac{\vdash \Gamma}{\Gamma \vdash s_i : \mathcal{U}_j} \quad i < j \\
\text{II-FORM} \\
\frac{\Gamma \vdash A : s_i \quad \Gamma, x : A \vdash B : s'_j}{\Gamma \vdash \Pi_{s_i}^j(x : A). B : s'_k} \quad \begin{array}{l} i \leq k \\ j \leq k \end{array} \\
\text{III-FORM} \\
\frac{\Gamma \vdash A : \Omega_i \quad \Gamma, x : A \vdash B : \Omega_i}{\Gamma \vdash \exists(x : A). B : \Omega_i} \\
\text{FUN} \\
\frac{\Gamma \vdash A : s_i \quad \Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda(x : A). t : \Pi(x : A). B} \\
\text{APP} \\
\frac{\Gamma \vdash t : \Pi(x : A). B \quad \Gamma \vdash u : A}{\Gamma \vdash t u : B[x := u]} \\
\text{PAIR} \\
\frac{\Gamma \vdash t : A \quad \Gamma \vdash u : B[x := t]}{\Gamma \vdash \langle t, u \rangle : \exists(x : A). B} \\
\text{FST} \\
\frac{\Gamma \vdash t : \exists(x : A). B}{\Gamma \vdash \text{fst}(t) : A} \\
\text{SND} \\
\frac{\Gamma \vdash t : \exists(x : A). B}{\Gamma \vdash \text{snd}(t) : B[x := \text{fst}(t)]} \\
\text{N-FORM} \\
\frac{\vdash \Gamma}{\Gamma \vdash \mathbb{N} : \mathcal{U}_0} \\
\text{ZERO} \\
\frac{\vdash \Gamma}{\Gamma \vdash 0 : \mathbb{N}} \\
\text{SUC} \\
\frac{\Gamma \vdash n : \mathbb{N}}{\Gamma \vdash S n : \mathbb{N}} \\
\text{N-ELIM} \\
\frac{\Gamma \vdash A : \mathbb{N} \rightarrow s_i \quad \Gamma \vdash t_0 : A \mathbf{0} \quad \Gamma \vdash t_S : \Pi(n : \mathbb{N}). A n \rightarrow A (S n) \quad \Gamma \vdash n : \mathbb{N}}{\Gamma \vdash \mathbf{N-elim}(A, t_0, t_S, n) : A n} \\
\text{I-FORM} \\
\frac{\vdash \Gamma}{\Gamma \vdash \perp : \Omega_i} \\
\text{I-ELIM} \\
\frac{\Gamma \vdash A : s_i \quad \Gamma \vdash t : \perp}{\Gamma \vdash \perp\text{-elim}(A, t) : A} \\
\text{T-FORM} \\
\frac{\vdash \Gamma}{\Gamma \vdash \top : \Omega_i} \\
\text{T-INTRO} \\
\frac{\vdash \Gamma}{\Gamma \vdash * : \top} \\
\text{EQ-FORM} \\
\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash u : A}{\Gamma \vdash t \sim_A u : \Omega_i} \\
\text{REFL} \\
\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A}{\Gamma \vdash \text{refl}(t) : t \sim_A t} \\
\text{TRANSPORT-}\Omega \\
\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash B : \Pi(x : A). t \sim_A x \rightarrow \Omega_j \quad \Gamma \vdash u : B t \quad \Gamma \vdash t' : A \quad \Gamma \vdash e : t \sim_A t'}{\Gamma \vdash \text{transport}(t, B, u, t', e) : B t' e} \\
\text{CAST} \\
\frac{\Gamma \vdash A : s_i \quad \Gamma \vdash B : s_i \quad \Gamma \vdash e : A \sim_s B \quad \Gamma \vdash t : A}{\Gamma \vdash \text{cast}(A, B, e, t) : B} \\
\text{CAST-REFL} \\
\frac{\Gamma \vdash A : s_i \quad \Gamma \vdash t : A \quad \Gamma \vdash e : A \sim_s A}{\Gamma \vdash \text{castrefl}(A, t) : t \sim_A \text{cast}(A, A, e, t)}
\end{array}$$

Fig. 2. \mathbb{T}^{obs} Typing Rules

be made to inhabit all relevant universes without added difficulty. Extensions to other inductive types and quotient types are presented in Section 4.

Empty and Unit type. To encode respectively the true equalities and the absurd equalities, \mathbb{T}^{obs} features the unit type \top and the empty type \perp . Besides its formation rule (Rule \perp -FORM), the empty type comes with an elimination principle (Rule \perp -ELIM) that can eliminate it into both proof-irrelevant and proof-relevant types. In MLTT with a proof irrelevant universe hierarchy, this constitutes the unique connection between the proof-irrelevant and relevant types. This means

$\frac{\text{REFL}}{\Gamma \vdash t : A} \quad \Gamma \vdash t \equiv t : A$	$\frac{\text{SYM}}{\Gamma \vdash t \equiv u : A} \quad \Gamma \vdash u \equiv t : A$	$\frac{\text{TRANS}}{\Gamma \vdash t \equiv u : A} \quad \Gamma \vdash t \equiv t' : A \quad \Gamma \vdash t' \equiv u : A$	$\frac{\text{RED-CONV}}{\Gamma \vdash t \equiv u : A} \quad \Gamma \vdash t \Rightarrow u : A$
$\frac{\eta\text{-EQ}}{\Gamma \vdash t \equiv u : \Pi(x : A). B} \quad \Gamma \vdash t, u : \Pi(x : A). B \quad \Gamma, x : A \vdash t x \equiv u x : B$	$\frac{\text{PROOF-IRRELEVANCE}}{\Gamma \vdash t \equiv u : A} \quad \Gamma \vdash A : \Omega_i \quad \Gamma \vdash t : A \quad \Gamma \vdash u : A$		

Fig. 3. \mathbb{T}^{obs} Conversion Rules (except congruence)

that the only way to use information from a proof-irrelevant term to build a proof-relevant term is by using a proof of \perp , which amounts to proving that actually we are in an inaccessible branch or impossible case. In \mathbb{T}^{obs} however, there is another very different way of using proof irrelevant information to build a proof relevant term, by transporting (or casting) along a proof of equality.

The unit type on the other hand only requires a formation rule (Rule **T-FORM**) and a constructor $*$ (Rule **T-INTRO**). It does not require an eliminator, since the usual one can be derived from proof irrelevance. Equivalently, we could have defined the unit type as $\perp \rightarrow \perp$. Note that both the unit type and the empty types are made cumulative, this is because there are used as terminal cases for the computation of observational equality which can live at any level.

Setoid equality and Type Casts. A central feature of \mathbb{T}^{obs} is that every proof-relevant type comes equipped with a proof-irrelevant equality type, noted $t \sim_A u$ (Rule **EQ-FORM**) and a canonical way to inhabit it, by the reflexivity term $\text{refl}(t)$ (Rule **REFL**). It is not necessary to equip proof-irrelevant types with a propositional equality, as two terms would always be propositional equal by reflexivity. As we will see in the definition of reduction above, the equality type of \mathbb{T}^{obs} should not be seen as a type constructor like the identity type of MLTT, but rather as a type eliminator that computes on its type argument and possibly on its two end points.

For this equality type to be of any use, we need to be able to eliminate it as well. The usual J -eliminator defined in MLTT can be defined in our context, but if the predicate is proof-relevant, there will be no hope for the eliminator to compute on reflexivity: since equality types are proof irrelevant, there is no reduction of equality proofs, and we cannot do pattern matching on the equality proof either. In order to avoid this issue, we restrict the use of J to proof-irrelevant predicates only, and note it **transp** (Rule **TRANSPORT- Ω**). Note that in this setting, the non-dependent version of the eliminator would be enough, as one can prove the contractibility of singletons for free thanks to proof-irrelevance [**Univalent Foundations Program 2013**]. Using **transp**, we can derive the usual groupoid laws provided by the J eliminator, and we note e^{-1} for the inverse of e , $e \cdot e^{-1}$ for the transitivity, and **ap** $f e$ for the preservation of equality by non-dependent function.

To deal with elimination of equality in a proof relevant context, we introduce a cast primitive that handles transport between two propositionally equal relevant types. Note that our cast operation also applies to proof-irrelevant types (Rule **CAST**). This is unnecessary as Rule **TRANSPORT- Ω** subsumes this case, but it will allow us to write more uniform reduction rules. The term **cast**(A, B, e, t) is an eliminator that reduces the types A and B in weak-head normal form, then reduces by pattern-matching on their head constructors. This will be explained in more detail in the next section. When applied to reflexivity, **cast** does not compute to the identity function, but this equality is propositionally admissible as witnessed by **castrefl** (Rule **CAST-REFL**).

2.3 Conversion and Reduction to Weak-Head Normal Forms

Conversion (Fig. 3) subsumes reduction (**RED-CONV**), η -equality of functions (Rule **η -EQ**), and proof-irrelevance (Rule **PROOF-IRRELEVANCE**). It is also closed under reflexivity, symmetry, transitivity and congruence. Note that η -equality does not need to be defined when the codomain is in Ω , because of proof-irrelevance. Congruence rules are standard and presented in Appendix A, Fig. 9.

Fig. 4 describes the reduction in TT^{obs} . Note that since reduction is typed, one needs to add a rule for type conversion (Rule **CONV-RED**). Reduction features the usual notion of β -reduction (Rule **β -RED**), which corresponds to the computation rule of application (the eliminator of dependent functions) applied to a λ -term (the constructor of dependent functions). Similarly, rules **\mathbb{N} -ELIM-ZERO** and **\mathbb{N} -ELIM-SUC** describe the two computation rules of the eliminator of \mathbb{N} , one for each constructor of \mathbb{N} .

As mentioned previously, the equality type and type cast operation of TT^{obs} are eliminators, and thus must come with their computation rules. Since $t \sim_A u$ is an eliminator for the universe, it needs rules for every type constructor. Rule **EQ-FUN** is the computation rule for dependent functions which stipulates that two functions are equal when they are pointwise equal, thus naturally providing TT^{obs} with function extensionality. Rule **EQ- Ω** says that two proof irrelevant types are equal when they are logically equivalent, thus providing TT^{obs} with propositional extensionality. Note that cumulativity is required for this reduction rule to preserve typing, as the types A and B live in a universe below $A \sim_{\Omega_i} B$.

There are three reduction rules for equality in \mathcal{U} . Rule **EQ-UNIV** stipulates that when the two endpoints are both \mathbb{N} or the same universe, the equality holds, which is captured by the fact that it reduces to the unit type. Rule **EQ-UNIV- \neq** says that when the two endpoints do not have the same head hd , the equality does not hold, which is captured by the fact that it reduces to the empty type. The function $\text{hd } A$ is simply equal to \mathbb{N} or s_i when A is the type of natural numbers or a universe respectively, and is defined as (Π, s, i, j) when A is the type $\Pi_{s,i}^j (x : A). B$. The third rule (Rule **EQ- Π**) says that two dependent function types are equal when their domain are equal, and their codomain are pointwise equal (as type families) up to the equality on their domain. As for Rule **EQ- Ω** , this rule is well-typed only in presence of cumulativity.

There are four rules for equality in \mathbb{N} , corresponding to every possible normal forms of the endpoints. Equality holds when both endpoints are 0 (Rule **EQ-ZERO**), computes to the equality of arguments when both endpoints are successors (Rule **EQ-SUC**), and does not hold otherwise (Rules **EQ-ZERO-SUC** and **EQ-SUC-ZERO**). This concludes the reduction rules for equality.

We can now turn to the description of the computation rules for type cast, which only need to be defined when the types are compatible—otherwise the cast will be stuck.³ Casting from \mathbb{N} to \mathbb{N} is defined by recursion to be the identity on constructors (Rules **CAST-ZERO** and **CAST-SUC**, and casting a type from a universe to the the same universe is the identity⁴ (Rule **CAST-UNIV**). Finally, casting between two dependent products is more involved: it produces a new function by casting back and forth the argument and return value of the original function (Rule **CAST- Π**).

For our definition of reduction to be complete, we need to add rules that reduce the scrutinees of eliminators to *weak-head normal form* (whnf), so the eliminator can then reduce by case analysis on the whnf. Weak-head normal forms correspond to relevant terms that can *not* be reduced (Fig. 5). They are either terms with a constructor in head position, or a neutral term, which correspond to the stuck terms that cannot exist in an empty context. Neutral terms are either variables, eliminators

³The cast could also reduce to an elimination on the proof of equality which in this case has type \perp , which will result in a stuck term.

⁴We could also define it by recursion on the argument. It is not clear whether these two options have any significant difference.

$$\begin{array}{c}
344 \quad \beta\text{-RED} \\
345 \quad \frac{\Gamma, x : A \vdash t : B \quad \Gamma \vdash u : A}{\Gamma \vdash (\lambda(x : A). t) u \Rightarrow t[x := u] : B[x := u]} \\
346 \\
347 \\
348 \quad \text{CONV-RED} \\
349 \quad \frac{\Gamma \vdash t \Rightarrow u : A \quad \Gamma \vdash A \equiv B : s_i}{\Gamma \vdash t \Rightarrow u : B} \\
350 \\
351 \\
352 \quad \text{N-ELIM-ZERO} \\
353 \quad \frac{\Gamma \vdash A : \mathbb{N} \rightarrow \mathcal{U}_i \quad \Gamma \vdash t_0 : A \mathbf{0} \quad \Gamma \vdash t_S : \Pi(n : \mathbb{N}). A n \rightarrow A (\mathbf{S} n)}{\Gamma \vdash \mathbf{N}\text{-elim}(A, t_0, t_S, \mathbf{0}) \Rightarrow t_0 : A \mathbf{0}} \\
354 \\
355 \quad \text{N-ELIM-SUC} \\
356 \quad \frac{\Gamma \vdash A : \mathbb{N} \rightarrow \mathcal{U}_i \quad \Gamma \vdash t_0 : A \mathbf{0} \quad \Gamma \vdash t_S : \Pi(n : \mathbb{N}). A n \rightarrow A (\mathbf{S} n) \quad \Gamma \vdash n : \mathbb{N}}{\Gamma \vdash \mathbf{N}\text{-elim}(A, t_0, t_S, \mathbf{S} n) \Rightarrow t_S \mathbf{N}\text{-elim}(A, t_0, t_S, n) : A (\mathbf{S} n)} \\
357 \\
358 \quad \text{EQ-FUN} \\
359 \quad \frac{\Gamma \vdash f : \Pi(x : A). B \quad \Gamma \vdash g : \Pi(x : A). B}{\Gamma \vdash f \sim_{\Pi A B} g \Rightarrow \Pi(x : A). f x \sim_B g x : \Omega_i} \\
360 \\
361 \quad \text{EQ-}\Omega \\
362 \quad \frac{\Gamma \vdash A : \Omega_i \quad \Gamma \vdash B : \Omega_i}{\Gamma \vdash A \sim_{\Omega_i} B \Rightarrow (A \rightarrow B) \wedge (B \rightarrow A) : \Omega_j}^{i < j} \\
363 \\
364 \quad \text{EQ-UNIV} \\
365 \quad \frac{\vdash \Gamma \quad A \in \{\mathbb{N}, s_i\}}{\Gamma \vdash A \sim_{\mathcal{U}_j} A \Rightarrow \top : \Omega_k}^{i < j < k} \\
366 \\
367 \quad \text{EQ-UNIV-}\neq \\
368 \quad \frac{\vdash \Gamma \quad A, B \in \{\mathbb{N}, \Pi A. B, s_i\} \quad \text{hd } A \neq \text{hd } B}{\Gamma \vdash A \sim_{\mathcal{U}_j} B \Rightarrow \perp : \Omega_k}^{i < j < k} \\
369 \\
370 \quad \text{EQ-}\Pi \\
371 \quad \frac{\Gamma \vdash A, A' : s_i \quad \Gamma, x : A \vdash B : s'_j \quad \Gamma, x : A' \vdash B' : s'_j \quad a := \text{cast}(A', A, \text{fst}(e)^{-1}, a')}{\Gamma \vdash \frac{\Pi(x : A). B \sim_{\mathcal{U}_k} \Pi(x : A'). B' \Rightarrow \exists(e : A \sim_{\mathcal{U}_i} A'). \Pi(a' : A'). B[x := a] \sim_{\mathcal{U}_j} B'[x := a']}{: \Omega_i}}^{i \leq k, j \leq k}} \\
372 \\
373 \quad \text{EQ-ZERO} \\
374 \quad \frac{\vdash \Gamma}{\Gamma \vdash \mathbf{0} \sim_{\mathbb{N}} \mathbf{0} \Rightarrow \top : \Omega_i} \\
375 \\
376 \quad \text{EQ-ZERO-SUC} \\
377 \quad \frac{\Gamma \vdash n : \mathbb{N}}{\Gamma \vdash \mathbf{0} \sim_{\mathbb{N}} \mathbf{S} n \Rightarrow \perp : \Omega_i} \\
378 \\
379 \quad \text{EQ-SUC-ZERO} \\
380 \quad \frac{\Gamma \vdash n : \mathbb{N}}{\Gamma \vdash \mathbf{S} n \sim_{\mathbb{N}} \mathbf{0} \Rightarrow \perp : \Omega_i} \\
381 \\
382 \quad \text{EQ-SUC} \\
383 \quad \frac{\Gamma \vdash n : \mathbb{N} \quad \Gamma \vdash m : \mathbb{N}}{\Gamma \vdash \mathbf{S} m \sim_{\mathbb{N}} \mathbf{S} n \Rightarrow m \sim_{\mathbb{N}} n : \Omega_i} \\
384 \\
385 \quad \text{CAST-ZERO} \\
386 \quad \frac{\Gamma \vdash e : \mathbb{N} \sim_{\mathcal{U}} \mathbb{N}}{\Gamma \vdash \text{cast}(\mathbb{N}, \mathbb{N}, e, \mathbf{0}) \Rightarrow \mathbf{0} : \mathbb{N}} \\
387 \\
388 \quad \text{CAST-SUC} \\
389 \quad \frac{\Gamma \vdash e : \mathbb{N} \sim_{\mathcal{U}} \mathbb{N} \quad \Gamma \vdash n : \mathbb{N}}{\Gamma \vdash \text{cast}(\mathbb{N}, \mathbb{N}, e, \mathbf{S} n) \Rightarrow \mathbf{S} \text{cast}(\mathbb{N}, \mathbb{N}, e, n) : \mathbb{N}} \\
390 \\
391 \quad \text{CAST-UNIV} \\
392 \quad \frac{\Gamma \vdash e : \mathcal{U}_i \sim_{\mathcal{U}} \mathcal{U}_i \quad \Gamma \vdash A : \mathcal{U}_i}{\Gamma \vdash \text{cast}(\mathcal{U}_i, \mathcal{U}_i, e, A) \Rightarrow A : \mathcal{U}_i} \\
393 \\
394 \quad \text{CAST-}\Pi \\
395 \quad \frac{\Gamma \vdash e : \Pi(x : A). B \sim_{\mathcal{U}} \Pi(x : A'). B' \quad \Gamma \vdash f : \Pi(x : A). B \quad a := \text{cast}(A', A, \text{fst}(e)^{-1}, a')}{\Gamma \vdash \frac{\text{cast}(\Pi(x : A). B, \Pi(x : A'). B', e, f) \Rightarrow \lambda(a' : A'). \text{cast}(B[x := a], B'[x := a'], \text{snd}(e) a', f a)}{: \Pi(x : A'). B'}}}
\end{array}$$

Fig. 4. $\mathbb{T}\mathbb{T}^{\text{obs}}$ Reduction Rules (except substitutions)

applied to another neutral term, or obtained from an inhabitant of \cdot . In $\mathbb{T}\mathbb{T}^{\text{obs}}$, inhabitant of a proof-irrelevant type are never considered as whnf, as there is no notion of reduction of proof-irrelevant terms.

The substitution rules that implement reduction of scrutinees to weak-head normal form are described in Appendix A, Fig. 10.

```

393     whnf      w ::= ne |  $\Pi(x : A). B$  |  $s_i$  |  $\exists(x : A). B$  |  $\mathbb{N}$  |  $\perp$  |  $\top$  |  $\lambda(x : A). t$  |  $0$  |  $S n$ 
394     neutral   ne ::=  $x$  |  $ne t$  |  $\perp$ -elim( $A, e$ ) |  $\mathbb{N}$ -elim( $P, t, u, ne$ )
395             |  $t \sim_{ne} u$  |  $ne \sim_{\mathbb{N}} m$  |  $0 \sim_{\mathbb{N}} ne$  |  $S m \sim_{\mathbb{N}} ne$ 
396             |  $ne \sim_{\mathcal{U}_i} B$  |  $\mathbb{N} \sim_{\mathcal{U}_i} ne$  |  $\Pi(x : A). B \sim_{\mathcal{U}_i} ne$  | cast( $\mathbb{N}, \mathbb{N}, e, ne$ )
397             | cast( $ne, B, e, t$ ) | cast( $\mathbb{N}, ne, e, t$ ) | cast( $\Pi(x : A). B, ne, e, t$ )
398             | cast( $w, w', e, t$ ) (where  $w, w' \in \{\mathbb{N}, \Pi A. B, s_i\}$ ,  $hd w \neq hd w'$ )

```

Fig. 5. Weak-head normal and neutral forms

3 METATHEORETICAL PROPERTIES

In order for a type theory to be a reasonable candidate for implementation in a proof assistant, it is desirable to have some control over its behavior and its semantics. There is a wide variety of properties we can ask of type theory ; we will describe four of them and prove they apply to TT^{obs} .

Consistency. A theory is called consistent if it is impossible to use it to derive a contradiction. It goes without saying that this property is of utmost importance if one wants to build interesting mathematics. When proving a theory consistent, one should pay some attention to the meta-theory where reasoning takes place, as a consistency result is really a reduction of the consistency of the theory to the consistency of the meta-theory.

Normalization. If a type theory features reduction rules, one may want to make sure that by repeatedly applying said rules, all terms eventually reach a normal form that cannot be reduced further. One says that the reduction strategy is normalizing.

Canonicity. A term belonging to a type is called canonical when it can be explicitly built up using the constructors of that type. For instance, an inhabitant of the type \mathbb{N} of natural numbers is canonical if it is an explicit numeral. If all terms of type \mathbb{N} in an empty context normalize to a canonical form, then the theory is said to enjoy canonicity for natural numbers.

Decidability of Type Checking. Finally, in order to implement a type theory in a proof assistant, it is desirable to have an algorithm that, given a context Γ and terms t and A , decides whether t is an inhabitant of A in context Γ . This ensures users that when they found a proof for a statement, the proof assistant can automatically check that their proof is correct.

In this section, we will prove these four properties for TT^{obs} . We first present our extension of the logical relations framework developed by Abel et al. [2018] and later extended to Ω by Gilbert et al. [2019]. The framework provides a proof of normalization and canonicity from consistency, as well as decidability of conversion and thus decidability of type checking. It has been formalized in the anonymous AGDA development. Then, to get consistency and therefore canonicity, we develop a model of TT^{obs} in a constructive set theory that supports inductive-recursive definitions and one Grothendieck universe.

3.1 Normalization and Canonicity from Consistency

We now explain the proof by reducibility as initially formalized in AGDA by Abel et al. [2018] and extended to Ω by Gilbert et al. [2019]. The proof starts from untyped syntax [Definition/Untyped.agda], with syntactical operations such as weakening and substitution, that are used to define typing judgements [Definition/Typed.agda]. Abel et al. [2018] also identify the weak head normal forms: define a neutral term to be term that has a variable in head position, which blocks reduction. Weak head normal forms are then defined to be either neutral terms or terms that have a constructor in head position. This is the notion that we extended to TT^{obs} in Fig. 5.

From there, Abel et al. [2018] use induction-recursion to define a Kripke logical relation that exhibits the structure and properties of well-typed terms, and implies weak-head normalization.

442	$\Gamma \Vdash_{\ell} A$	A is a reducible type at level ℓ in context Γ
443	$\Gamma \Vdash_{\ell} A \equiv B$	A and B are reducibly equal types at level ℓ in context Γ
444	$\Gamma \Vdash_{\ell} t : A$	t is a reducible term at level ℓ of type A in context Γ
445	$\Gamma \Vdash_{\ell} t \equiv u : A$	t and u are reducibly equal terms at level ℓ of type A in context Γ

Fig. 6. The four judgments of the logical relation

The proof builds up to the *fundamental lemma*, which states that any well-typed term is reducible by induction on the typing derivation. [Abel et al. \[2018\]](#) prove this for a dependent type theory with dependent functions, natural numbers and one universe. [Gilbert et al. \[2019\]](#) extends it with one universe of definitionally proof irrelevant types.

In our work, we added support for two cumulative universe levels, existential types, proof irrelevant axioms, setoid equality and cast. This doubles the size of the proof, getting it up to 20,000 lines of Agda code.

Our most novel contribution to the proof is our treatment of proof-irrelevant types. Even though the theory studied by [Gilbert et al. \[2019\]](#) features proof-irrelevant types, their reducibility proof extends reduction rules to the inhabitants of these types, and the normalization result applies to them too. From this, [Gilbert et al. \[2019\]](#) derives an easy proof of consistency: any proof of \perp in an empty context will reduce to a weak head normal form, and the only weak head normal forms that can inhabit \perp are neutral terms. But since there are no variables in the empty context, neutral terms cannot exist, so \perp has no inhabitants in the empty context.

However, this strategy is not applicable in our setting: it seems difficult to devise reduction rules for some terms that we postulated, such as `castrefl`, so that they reduce to a normal form. Therefore we have dropped the notion of reduction rules for inhabitants of proof-irrelevant types in \mathbb{T}^{obs} , and only prove normalization for proof-relevant types. We argue that this is more faithful to the philosophy of proof irrelevance, and results in a proof that is completely agnostic about the proof irrelevant content of the theory—we could postulate any proof-irrelevant axiom and the normalization proof would carry through.

Of course, this means that consistency and canonicity do not follow from normalization anymore. The reason is simple: since we gave up any kind of control on the proof-irrelevant terms, we are forced to consider them as neutral. This also adds neutrals to the proof-*relevant* world, as \perp -elim can build inhabitants of proof-relevant types from inhabitants of \perp . Therefore, we need consistency of our theory to show canonicity.

3.2 Definition of the Logical Relation

In this section, we define the (Kripke) logical relation that we used [[Definition/LogicalRelation.agda](#)], closely following [Abel et al. \[2018\]](#). For pedagogical reasons, will present a somewhat informal version of the logical relation, and refer the interested reader to the formalization. The logical relation is indexed by a level ℓ , on which we do induction to define the judgements. While our formal proof only features three levels, we will describe a full proof with levels that range over \mathbb{N} as this does not add significant complexity to the argument. The logical relation features four kinds of judgements presented in Fig. 6.

As is customary in reducibility proofs [[Girard 1972](#)], these judgements imply normalization, are closed under weak head expansion, and are verified by all neutral terms. The judgement $\Gamma \Vdash_{\ell} A$ is defined inductively, while the three other are simultaneously defined by recursion on a derivation of $\Gamma \Vdash_{\ell} A$. Thus, these judgements technically depend on the specific derivation of $\Gamma \Vdash_{\ell} A$, but since two different derivations will give rise to equivalent judgements we freely ignore this dependence.

We now present the six cases in the inductive definition $\Gamma \Vdash_\ell A$, together with the definition of the other three judgments.

Neutral Types.

$$\frac{\Gamma \vdash A \Rightarrow^* N : s_i \quad \text{neutral } N}{\Gamma \Vdash_\ell A}$$

This rule states that A is reducible to a neutral type: $\Gamma \vdash A \Rightarrow^* N : s_i$ means that A reduces to a neutral term N in a finite number of steps (possibly zero), and that both A and N are of type s_i in context Γ . When A is reducible to a neutral type, we define:

- $\Gamma \Vdash_\ell A \equiv B$ if there is a neutral term M such that $\Gamma \vdash B \Rightarrow^* M : s_i$ and $\Gamma \vdash N \equiv M : s_i$.

If A is a proof-relevant type, then we also define:

- $\Gamma \Vdash_\ell t : A$ if there is a neutral term n such that $\Gamma \vdash t \Rightarrow^* n : N$.
- $\Gamma \Vdash_\ell t \equiv u : A$ if there are neutral terms n, m such that $\Gamma \vdash t \Rightarrow^* n : N$ and $\Gamma \vdash u \Rightarrow^* m : N$, and $\Gamma \vdash n \equiv m : N$.

If A is a proof-irrelevant type, then we define instead:

- $\Gamma \Vdash_\ell t : A$ if $\Gamma \vdash t : A$.
- $\Gamma \Vdash_\ell t \equiv u : A$ if $\Gamma \vdash t : A$ and $\Gamma \vdash u : A$.

More generally, inhabitant of proof-irrelevant types are always reducible when they are well-typed.

Universes.

$$\frac{\Gamma \vdash A \Rightarrow^* s_i : \mathcal{U}_{j \substack{i < \ell \\ i < j}}}{\Gamma \Vdash_\ell A}$$

When A is reducible to a universe, we define:

- $\Gamma \Vdash_\ell A \equiv B$ if $\Gamma \vdash B \Rightarrow^* s_i : \mathcal{U}_j$.
- $\Gamma \Vdash_\ell t : A$ if there is a normal form t' such that $\Gamma \vdash t \Rightarrow^* t' : s_i$, and $\Gamma \Vdash_i t$ (which is already defined by induction hypothesis, since $i < \ell$).
- $\Gamma \Vdash_\ell t \equiv u : A$ if there are normal forms t', u' such that $\Gamma \vdash t \Rightarrow^* t' : s_i$ and $\Gamma \vdash u \Rightarrow^* u' : s_i$, and $\Gamma \Vdash_i t, \Gamma \Vdash_i u$, and $\Gamma \Vdash_i t \equiv u$.

Natural Numbers.

$$\frac{\Gamma \vdash A \Rightarrow^* \mathbb{N} : \mathcal{U}_i}{\Gamma \Vdash_\ell A}$$

When A is reducible to \mathbb{N} , we define:

- $\Gamma \Vdash_\ell A \equiv B$ if $\Gamma \vdash B \Rightarrow^* \mathbb{N} : \mathcal{U}_i$.
- $\Gamma \Vdash_\ell t : A$ if there is a normal form t' such that $\Gamma \vdash t \Rightarrow^* t' : \mathbb{N}$ and $\Gamma \Vdash \mathbb{N} t'$, which is inductively defined by

$$\frac{}{\Gamma \Vdash \mathbb{N} 0} \quad \frac{\Gamma \Vdash \mathbb{N} t}{\Gamma \Vdash \mathbb{N} S t} \quad \frac{\Gamma \vdash n : \mathbb{N} \quad n \text{ is neutral}}{\Gamma \Vdash \mathbb{N} n}$$

- $\Gamma \Vdash_\ell t \equiv u : A$ if there are normal forms t', u' such that $\Gamma \vdash t \Rightarrow^* t' : \mathbb{N}$ and $\Gamma \vdash u \Rightarrow^* u' : \mathbb{N}$, and $\Gamma \Vdash \mathbb{N} t' \equiv u'$, which is inductively defined by

$$\frac{}{\Gamma \Vdash \mathbb{N} 0 \equiv 0} \quad \frac{\Gamma \Vdash \mathbb{N} t \equiv u}{\Gamma \Vdash \mathbb{N} S t \equiv S u} \quad \frac{\Gamma \vdash n \equiv m : \mathbb{N} \quad n, m \text{ are neutral}}{\Gamma \Vdash \mathbb{N} n \equiv m}$$

- $\Gamma \Vdash_\ell t : A$ if $\Gamma \vdash t : \exists(x : F). G$.
- $\Gamma \Vdash_\ell t \equiv u : A$ if $\Gamma \vdash t : \exists(x : F). G$ and $\Gamma \vdash u : \exists(x : F). G$.

Empty type.

$$\frac{\Gamma \vdash A \Rightarrow^* \perp : \Omega_i}{\Gamma \Vdash_\ell A}$$

When A is reducible to the empty type, we define:

- $\Gamma \Vdash_\ell A \equiv B$ if $\Gamma \vdash B \Rightarrow^* \perp : \Omega_i$.
- $\Gamma \Vdash_\ell t : A$ if $\Gamma \vdash t : \perp$.
- $\Gamma \Vdash_\ell t \equiv u : A$ if $\Gamma \vdash t : \perp$ and $\Gamma \vdash u : \perp$.

We do not have to add a case for \top , since it can be encoded as $\perp \rightarrow \perp$. There is no case for $t \sim_A u$ either, this is because setoid equality is not a type constructor, but rather a type eliminator that does pattern matching on A and its two end points t and u . Consequently, the only whnfs of the form $t \sim_A u$ are neutral, and are handled by the rule for proof-irrelevant neutral types.

Embedding.

$$\frac{\Gamma \Vdash_\ell A}{\Gamma \Vdash_{\ell'} A} \ell < \ell'$$

This case ensures that the logical relation is monotonic with respect to the level.

3.3 The fundamental lemma

Before stating the fundamental lemma for the logical relation, which basically amounts to completeness of the logical relation with respect to the typing relation, we establish the correctness of logical relation, which is called the escape lemma by [Abel et al. \[2018\]](#).

LEMMA 3.1 (ESCAPE LEMMA). *Given $\Gamma \Vdash_\ell A$,*

- (1) $\Gamma \vdash A : s$.
- (2) *If $\Gamma \Vdash_\ell A \equiv B$ then $\Gamma \vdash A \equiv B : s$.*
- (3) *If $\Gamma \Vdash_\ell t : A$ then $\Gamma \vdash A : s$.*
- (4) *If $\Gamma \Vdash_\ell t \equiv u : A$ then $\Gamma \vdash t \equiv u : A$.*

PROOF. Straightforward induction on the logical relation. □

We can now state the completeness of the logical relation, a.k.a. the fundamental lemma [[Definition/LogicalRelation/Fundamental.agda](#)]. We state it here in a simple form but the proof, done by induction on the typing derivation, requires to generalize the induction hypothesis to consider reducibility under an arbitrary reducible substitution. This is achieved, in [Abel et al. \[2018\]](#) as well as in our formalization [[Definition/LogicalRelation/Substitution.agda](#)], by defining the notion of validity, but we deliberately ignore this technicality in the rest of the section.

LEMMA 3.2 (FUNDAMENTAL LEMMA).

- (1) *If $\Gamma \vdash t : A$, then there is a ℓ such that $\Gamma \Vdash_\ell A$ and $\Gamma \Vdash_\ell t : A$.*
- (2) *If $\Gamma \vdash t \equiv u : A$, then there is a ℓ such that $\Gamma \Vdash_\ell A$ and $\Gamma \Vdash_\ell t \equiv u : A$.*

The fundamental lemma will be proved by induction on the typing derivations. For most of the rules, the proof is roughly the same as in [[Abel et al. 2018](#); [Gilbert et al. 2019](#)]—with simplified proofs for inhabitants of proof-irrelevant types. The proof relies heavily on reflexivity, symmetry and transitivity of the reducible equality, stability of reducibility under reducible type conversion, reducibility of neutral terms, and the fact that reducibility is stable by weak-head expansion. Our extension to a cumulative hierarchy of universes and to proof-irrelevant existential quantification

requires numerous changes, but these do not pose any major difficulty—albeit the proof is by no means trivial, as the arguments have to be spelled out in excruciating detail. We now focus on the two main typing derivation introduced by TT^{obs} , Rules **EQ-FORM** and **CAST**. Those two cases are the consequence of the following lemmas.

LEMMA 3.3 (REDUCIBILITY OF CAST). *For all levels $\ell_1, \ell_2, \ell_3, \ell_4$, in a well formed context Γ , if:*

- (1) $\Gamma \Vdash_{\ell_1} A$ and $\Gamma \Vdash_{\ell_2} A'$ and $\Gamma \Vdash_{\ell_1} A \equiv A'$
- (2) $\Gamma \Vdash_{\ell_3} B$ and $\Gamma \Vdash_{\ell_4} B'$ and $\Gamma \Vdash_{\ell_3} B \equiv B'$
- (3) $\Gamma \vdash e : A \sim_s B$ and $\Gamma \vdash e' : A' \sim_s B'$
- (4) $\Gamma \Vdash_{\ell_1} t : A$ and $\Gamma \Vdash_{\ell_2} t' : A'$ and $\Gamma \Vdash_{\ell_1} t \equiv t' : A$

then $\Gamma \Vdash_{\ell_3} \text{cast}(A, B, e, t) : B$ and $\Gamma \Vdash_{\ell_3} \text{cast}(A, B, e, t) \equiv \text{cast}(A', B', e', t') : B$.

PROOF. The proof is by case analysis on the reducibility proofs of A, A', B, B' . If one of them is introduced by embedding, then we recursively apply the lemma on the embedded proof. Thus, it suffices to prove it when all reducibility proofs correspond to a normal form. From the proofs of reducible equality, one obtains that the reducibility proofs of A and A' (resp. B and B') are introduced by the same rule. Then, if one of the normal forms is neutral, or if the normal forms of A and B have different head constructor, then $\text{cast}(A, B, e, t)$ and $\text{cast}(A', B', e', t')$ are neutral and easily seen to be reducible. Therefore, it suffices to prove the lemma when all the reducibility proofs are introduced by the same rule. We will detail the case of dependent products, as it is the most interesting.

We know that A reduces to a term of the form $\Pi(x : F_A). G_A$, as do A', B, B' . Therefore, we know that $\text{cast}(A, B, e, t)$ reduces to $\lambda(a' : F_B). \text{cast}(G_A[x := a], G_B[x := a'], \text{snd}(e) a', t a)$ where a is a shorthand for $\text{cast}(F_B, F_A, \text{fst}(e)^{-1}, a')$, and $\text{cast}(A', B', e', t')$ reduces similarly. By the weak head expansion lemma, it suffices to prove that these normal forms are reducible, and reducibly equal at type $\Pi(x : F_B). G_B$ —that is, applying them to a reducible term a' under any weakening results in reducible terms that are reducibly equal, and that applying the first to two reducibly equal terms produce new reducibly equal terms.

To prove the first obligation, we first recursively apply the lemma to $\text{cast}(F_B, F_A, \text{fst}(e)^{-1}, a')$ so that we obtain reducibility of a , and then recursively applying it to $\text{cast}(G_A[x := a], G_B[x := a'], \text{snd}(e) a', t a)$. The other two obligations are proved in the exact same manner. \square

LEMMA 3.4 (REDUCIBILITY OF ID IN THE UNIVERSE). *For all levels $\ell_1, \ell_2, \ell_3, \ell_4$, in a well formed context Γ , if:*

- (1) $\Gamma \Vdash_{\ell_1} A$ and $\Gamma \Vdash_{\ell_2} A'$ and $\Gamma \Vdash_{\ell_1} A \equiv A'$
- (2) $\Gamma \Vdash_{\ell_3} B$ and $\Gamma \Vdash_{\ell_4} B'$ and $\Gamma \Vdash_{\ell_3} B \equiv B'$

then $\Gamma \Vdash_{\ell_{\max}} A \sim_s B$ and $\Gamma \Vdash_{\ell_{\max}} A \sim_s B \equiv A' \sim_s B'$.

PROOF. The proof is by case analysis on the reducibility proofs of A, A', B, B' . As we did in the proof of 3.3, we reduce the proof to introduction rules that correspond to the same kind of normal form. Most cases are straightforward, the difficult case being again the dependent products.

From reducibility proofs, we know that A reduces to a term of the form $\Pi(x : F_A). G_A$, as do A', B, B' . Thus, we know that $A \sim_s B$ reduces to $\exists(e : F_A \sim_{\mathcal{U}} F_B). \Pi(a' : F_B). G_A[x := a] \sim_{\mathcal{U}} G_B[x := a']$ where a is a shorthand for $\text{cast}(F_B, F_A, \text{fst}(e)^{-1}, a')$, and $A' \sim_s B'$ reduces similarly. By the weak head expansion lemma, it suffices to prove that the first normal form is reducible, and reducibly equal to the second one.

We do this by applying reducibility of **cast** to get reducibility of a , and then doing recursive calls on $F_A \sim_{\mathcal{U}} F_B$ and $G_A[x := a] \sim_{\mathcal{U}} G_B[x := a']$ under the appropriate weakenings and substitutions. \square

LEMMA 3.5 (REDUCIBILITY OF ID). *For all levels ℓ_1, ℓ_2 , in a well formed context Γ , if:*

- 687 (1) $\Gamma \Vdash_{\ell_1} A$ and $\Gamma \Vdash_{\ell_2} A'$ and $\Gamma \Vdash_{\ell_1} A \equiv A'$
 688 (2) $\Gamma \Vdash_{\ell_1} t : A$ and $\Gamma \Vdash_{\ell_2} t' : A'$ and $\Gamma \Vdash_{\ell_1} t \equiv t' : A$
 689 (3) $\Gamma \Vdash_{\ell_1} u : A$ and $\Gamma \Vdash_{\ell_2} u' : A'$ and $\Gamma \Vdash_{\ell_1} u \equiv u' : A$

690 then $\Gamma \Vdash_{\ell_1} t \sim_A u$ and $\Gamma \Vdash_{\ell_1} t \sim_A u \equiv t' \sim_A u'$.

691 PROOF. By case analysis on A and A' . The most difficult case is the universe, and is handled by
 692 lemma 3.4. The case of dependent products requires doing recursive calls on the domain and the
 693 codomain, as in the previous lemmas. \square

694
 695 These lemmas constitute the bulk of the proof: they occupy approximately 5,000 lines of Agda
 696 code and most of the time required to check the whole proof is spent on them.

697 COROLLARY 3.6 (NORMALIZATION). *A direct consequence of the fundamental lemma is that any*
 698 *well-typed term has a weak-head normal form.*

700 Another direct consequence of the fundamental lemma is that any closed term of type \mathbb{N} re-
 701 duces to a whnf of type \mathbb{N} . Thus, to conclude canonicity, we just need to know that there is
 702 no neutral term of type \mathbb{N} in an empty context. Unfortunately, as the notion of reduction is
 703 absent for terms of proof-irrelevant types, and in particular for the empty type, this cannot
 704 be proven by induction on the syntax of the neutral terms. However, assuming consistency of
 705 $\mathbb{T}\mathbb{T}^{\text{obs}}$, or in other words that there is no closed term of type \perp , we can derive canonicity of
 706 $\mathbb{T}\mathbb{T}^{\text{obs}}$ [Definition/Typed/Consequences/Canonicity.agda].

707 Section 3.5 is devoted to the definition of a model to prove consistency of $\mathbb{T}\mathbb{T}^{\text{obs}}$.

708 3.4 Decidability of typing

709 In order get decidability of typing, we first need to show decidability of conversion. This is done by
 710 defining an algorithmic version of the conversion of two terms t and u which basically amounts
 711 to computing the whnf of t and u , comparing their head, and apply the algorithm recursively if
 712 necessary. Correctness of algorithmic conversion is easy as the rules used are particular cases of
 713 typed conversion. Then, we can show that this algorithmic conversion is also complete by replaying
 714 the fundamental lemma with a definition of the logical relation using algorithmic conversion
 715 instead of typed conversion. Actually, the formalization of [Abel et al. 2018] factors the two proofs
 716 of the fundamental lemma by defining a generic interface for both algorithmic conversion and
 717 typed conversion, and uses this interface in the definition of the logical relation instead. While
 718 our formalization is also based on a generic interface for conversion, we have not formalized the
 719 definition of algorithmic conversion yet.

720 Then, to get decidability of type checking, we can simply rely on the work of Lennon-Bertrand
 721 [2021] on bidirectional type-checking, which defines an algorithmic version of type-checking
 722 provided that the theory enjoys subject reduction and decidability of conversion.

724 3.5 Consistency: The Setoid Model

725 $\mathbb{T}\mathbb{T}^{\text{obs}}$ is designed to describe the behavior of constructive setoids. In order to justify this claim, we
 726 build a model of $\mathbb{T}\mathbb{T}^{\text{obs}}$ where every context and proof-relevant type is interpreted as a setoid in a
 727 constructive set theory with induction-recursion, following the seminal proof of Hofmann [1995].
 728 Then, by interpreting $\mathbb{T}\mathbb{T}^{\text{obs}}$ in this model, we can prove the following theorem, which is the central
 729 missing piece of the meta-theory of $\mathbb{T}\mathbb{T}^{\text{obs}}$:

730 THEOREM 3.7 (CONSISTENCY OF $\mathbb{T}\mathbb{T}^{\text{obs}}$). *There is no inhabitant of \perp in the empty context.*

731 We work in a constructive set theory that supports inductive-recursive definitions and one
 732 Grothendieck universe. While it would be more satisfying to use a constructive type theory, as in
 733

the normalization proof, it is significantly more challenging. This is because the interpretation of the syntax in our model is only defined on well-typed terms, but should not depend on the typing derivation. While properly establishing this in a typed context is non-trivial, the added flexibility of set theory makes the task straightforward. We will write \mathbb{N} for the set of natural numbers in our meta-theory, $(x \in A) \rightarrow B(x)$ for dependent functions and $(x \in A) \times B(x)$ for dependent products.

We define a *setoid* to be the data of a *carrier* set A and a *setoid equality* predicate on $A \times A$ that is reflexive, symmetric and transitive, which we write \approx . Alternatively, we can define setoids to be small categories such that morphism sets are subsingletons, and every morphism is invertible. We will make use of both perspectives, and use the notation $a \approx b$ to mean either the proposition or the corresponding subsingleton. Given two setoids A and B , we write $A \rightarrow_s B$ for the set of functions that preserve setoid equality. This set inherits a natural setoid structure from pointwise setoid equality. $A \leftrightarrow_s B$ denotes the set of setoid equivalences, which are pairs of setoid functions in both directions that cancel. Given $e \in A \leftrightarrow_s B$, the induced function from A to B is simply noted e , while the other direction is noted e^{-1} .

The setoid equivalence turns the (large) set of all small setoids Setoid into a *groupoid*, or in other words a category where all morphisms are invertible. Given any setoid A , this allows us to define dependent setoids as functions from A to Setoid that send setoidal equalities to setoid equivalences, in a way that is compatible with composition and identity. Then, given a setoid A and a dependent setoid $B : A \rightarrow_s \text{Setoid}$, we write $(x \in A) \rightarrow_s B(x)$ for the setoid of dependent functions, with pointwise equality. We also form a setoid Prop by using the set of subsingletons as the carrier, with logical equivalence as the equality.

The central object in the setoid model is a dual hierarchy of small setoids U_i and Ω_i , that contain codes for the setoids and propositions that can be constructed in TT^{obs} . We build these universes of codes using induction-recursion: we define the sets U_i and Ω_i by induction, and we simultaneously use recursion on them to define interpretation functions $\text{el} : U_i \rightarrow \text{Setoid}$ and $\text{val} : \Omega_i \rightarrow \text{Prop}$, setoid equality on U_i and Ω_i , as well as proofs that el and val preserve that setoid equality. All of this is done under an external induction on i and is given in Fig. 7.

We have omitted quite a few bureaucratic proofs from this definition, such as the reflexivity, symmetry and transitivity of \approx , or the fact that el-eq is compatible with reflexivity and transitivity. We also freely make use of the fact that equality is decidable on integers.

With this, we obtain two families of setoids U_i and Ω_i , along with a dependent setoid $\text{el} : U_i \rightarrow_s \text{Setoid}$ and a setoid function $\text{val} : \Omega_i \rightarrow_s \text{Prop}$. This construction turns the category of setoids and setoid functions into a *universe category* in the sense of Voevodsky [2015]. Our model is a contextual category/C-system built from this universe category. In the following, we describe the construction of the setoid model without assuming familiarity with contextual categories.

We now use U_i and Ω_i to define the types and the terms of the setoid model. From now on, we will write s to mean either U or Ω and we will also write c_Π for any of $c_{\Pi\Omega\Omega}$, $c_{\Pi\Omega U}$, $c_{\Pi U\Omega}$ and $c_{\Pi U U}$. Given a setoid Γ , a *semantic type* of level i over Γ is simply a setoid function $\Gamma \rightarrow_s s_i$. We write these sets as $\text{Ty}_{s,i} \Gamma$. Then, given a semantic type A over Γ , we define the set of *semantic terms* of type A to be the setoidal dependent product $(x \in \Gamma) \rightarrow_s \text{el } A(x)$. We note this set $\text{tm } A$.

The contexts of our model are setoids which are inductively built from the terminal setoid as sequences of types:

```

Con ::= • : Con
      |  →_• : (Γ ∈ Con) → Ty_{U,i} Γ → Con    (∀i ∈ N)
      |  →_• : (Γ ∈ Con) → Ty_{Ω,i} Γ → Con    (∀i ∈ N)

```

785	\mathbf{U}_i	$::=$	$c_N : \mathbf{U}_i$	
786		$c_{\Pi\cup\cup} : (A \in \mathbf{U}_j) \rightarrow (\text{el } A \rightarrow_s \mathbf{U}_k) \rightarrow \mathbf{U}_i$		where $j, k < i$
787		$c_{\Pi\Omega\cup} : (A \in \Omega_j) \rightarrow (\text{el } A \rightarrow_s \mathbf{U}_k) \rightarrow \mathbf{U}_i$		where $j, k < i$
788		$c_U : \{j \in \mathbb{N} \mid j < i\} \rightarrow \mathbf{U}_i$		
789		$c_\Omega : \{j \in \mathbb{N} \mid j < i\} \rightarrow \mathbf{U}_i$		
790	$\mathbf{\Omega}_i$	$::=$	$c_\perp : \mathbf{\Omega}_i$	
791		$c_{\Pi\cup\Omega} : (A \in \mathbf{U}_j) \rightarrow (\text{el } A \rightarrow_s \mathbf{\Omega}_k) \rightarrow \mathbf{\Omega}_i$		where $j, k < i$
792		$c_{\Pi\Omega\Omega} : (A \in \mathbf{\Omega}_j) \rightarrow (\text{el } A \rightarrow_s \mathbf{\Omega}_k) \rightarrow \mathbf{\Omega}_i$		where $j, k < i$
793		$c_\exists : (A \in \mathbf{\Omega}_i) \rightarrow (\text{el } A \rightarrow_s \mathbf{\Omega}_i) \rightarrow \mathbf{\Omega}_i$		
794	$\text{el} : \mathbf{U}_i \rightarrow \text{Setoid}$			
795	$\text{el } c_N$	$::=$	\mathbb{N}	$\text{val} : \mathbf{\Omega}_i \rightarrow \text{Prop}$
796	$\text{el } (c_{\Pi\cup\cup} A B)$	$::=$	$(x \in \text{el } A) \rightarrow_s \text{el } B(x)$	$\text{val } c_\perp \quad ::= \quad \perp$
797	$\text{el } (c_{\Pi\Omega\cup} A B)$	$::=$	$(x \in \text{val } A) \rightarrow \text{el } B(x)$	$\text{val } (c_{\Pi\cup\Omega} A B) \quad ::= \quad (x \in \text{el } A) \rightarrow_s \text{val } B(x)$
798	$\text{el } (c_U j)$	$::=$	\mathbf{U}_j	$\text{val } (c_{\Pi\Omega\Omega} A B) \quad ::= \quad (x \in \text{val } A) \rightarrow \text{val } B(x)$
799	$\text{el } (c_\Omega j)$	$::=$	$\mathbf{\Omega}_j$	$\text{val } (c_\exists A B) \quad ::= \quad (x \in \text{val } A) \times \text{val } B(x)$
800	$_ \approx _ : \mathbf{U}_i \rightarrow \mathbf{U}_i \rightarrow \text{Prop}$			
801	$c_N \approx c_N$	$::=$	\top	
802	$c_{\Pi\cup\cup} A B \approx c_{\Pi\cup\cup} A' B'$	$::=$	$(e \in A \approx A') \times ((x \in \text{el } A) \rightarrow_s B(x) \approx B'(\text{el-eq } e x))$	when $j = j'$ and $k = k'$
803				
804	$c_{\Pi\Omega\cup} A B \approx c_{\Pi\Omega\cup} A' B'$	$::=$	$(e \in A \approx A') \times ((x \in \text{val } A) \rightarrow B(x) \approx B'(\text{val-eq } e x))$	when $j = j'$ and $k = k'$
805				
806	$c_U j \approx c_U j'$	$::=$	$j = j'$	
807	$c_\Omega j \approx c_\Omega j'$	$::=$	$j = j'$	
808	$_ \approx _$	$::=$	\perp	otherwise
809	$_ \approx _ : \mathbf{\Omega}_i \rightarrow \mathbf{\Omega}_i \rightarrow \text{Prop}$			
810	$A \approx B$	$::=$	$\text{val } A \Leftrightarrow \text{val } B$	
811	$\text{el-eq} : (A \in \mathbf{U}_i) \rightarrow (B \in \mathbf{U}_i) \rightarrow A \approx B \rightarrow \text{el } A \leftrightarrow_s \text{el } B$			
812	$\text{el-eq } c_N c_N e$	$::=$	$(x \mapsto x, x \mapsto x)$	
813	$\text{el-eq } (c_{\Pi\cup\cup} A B) (c_{\Pi\cup\cup} A' B') e$	$::=$	$(f \mapsto (x \mapsto \text{el-eq } (e.2 (\text{el-eq}^{-1} e.1 x)) (f (\text{el-eq}^{-1} e.1 x))))$	
814			$, f \mapsto (x \mapsto \text{el-eq}^{-1} (e.2 (\text{el-eq } e.1 x)) (f (\text{el-eq } e.1 x))))$	
815	$\text{el-eq } (c_{\Pi\Omega\cup} A B) (c_{\Pi\Omega\cup} A' B') e$	$::=$	$(f \mapsto (x \mapsto \text{el-eq } (e.2 (\text{val-eq}^{-1} e.1 x)) (f (\text{val-eq}^{-1} e.1 x))))$	
816			$, f \mapsto (x \mapsto \text{el-eq}^{-1} (e.2 (\text{val-eq } e.1 x)) (f (\text{val-eq } e.1 x))))$	
817	$\text{el-eq } (c_U j) (c_U j) e$	$::=$	$(x \mapsto x, x \mapsto x)$	
818	$\text{el-eq } (c_\Omega j) (c_\Omega j) e$	$::=$	$(x \mapsto x, x \mapsto x)$	
819	$\text{val-eq} : (A \in \mathbf{\Omega}_i) \rightarrow (B \in \mathbf{\Omega}_i) \rightarrow A \approx B \rightarrow \text{val } A \Leftrightarrow \text{val } B$			
820	$\text{val-eq } A B e$	$::=$	e	
821				
822				
823				
824				
825				
826				
827				

Fig. 7. The Setoid Model

Being telescopes of setoids, inhabitants of Con have an obvious interpretation as setoids: the elements of $\Gamma \in \text{Con}$ are dependent lists of inhabitants for all of the types and propositions in Γ , and the setoid equality is inherited from pointwise setoid equality of lists.

We have all of the required blocks to get the structure of a category with families [Dybjer 1996] and thus a model of MLTT.

3.6 Interpreting $\mathbb{T}\mathbb{T}^{\text{obs}}$ in the Setoid Model

We now describe how to interpret the judgements of $\mathbb{T}\mathbb{T}^{\text{obs}}$ in the setoid model where: (i) a well-formedness judgement $\vdash \Gamma$ will be interpreted as a setoid in Con (ii) a type judgement $\Gamma \vdash A : s_i$ will be interpreted as a semantic type over the interpretation of Γ (iii) a typing judgement $\Gamma \vdash t : A$ will be interpreted as a semantic term of the corresponding semantic type (iv) a convertibility judgement $\Gamma \vdash t \equiv u : B$ will be interpreted as meta-theoretical equality of the interpretations of t and u .

Since reduction is contained in convertibility, the model will necessarily interpret reduction as equality—it is not fine enough to distinguish the two notions.

Our interpretation is defined by induction on the syntax of the terms, following Hofmann [1993]:

- The context interpretation turns a syntactical context Γ into a setoid $\llbracket \Gamma \rrbracket \in \text{Con}$.
- The type interpretation turns a syntactical context Γ and a syntactical term A into an element $\llbracket A \rrbracket_{\Gamma} \in \text{tm } \mathbf{U}_i$ for some i .
- The term interpretation turns a syntactical context Γ and a syntactical term t into an element $\llbracket t \rrbracket_{\Gamma} \in \text{tm } (\text{el} \circ \llbracket A \rrbracket_{\Gamma})$.

The reader might notice that the type interpretation is really an instance of the term interpretation. This is to be expected, since our theory features Russel-style universes, that do not separate types and terms. As we cannot hope for every syntactical term to have an interpretation, we define the interpretation as *partial* functions from the syntax to the model. In the definition by recursion, we consider that whenever a term reduces to an expression that does not make sense, the interpretation is not defined. It is possible to prove that the interpretation function is total when restricted to the well-typed terms afterwards.

The interpretation of contexts is given by:

$$\begin{aligned} \llbracket \bullet \rrbracket &:= 1 \\ \llbracket \Gamma, x : A \rrbracket &:= \llbracket \Gamma \rrbracket, \text{el} \circ \llbracket A \rrbracket_{\Gamma} \end{aligned}$$

Variables are interpreted as projections:

$$\begin{aligned} \llbracket x \rrbracket_{\Gamma, x:A} (x_1, \dots, x_n) &:= x_n \\ \llbracket x \rrbracket_{\Gamma, y:A} (x_1, \dots, x_n) &:= \llbracket x \rrbracket_{\Gamma} (x_1, \dots, x_{n-1}) \end{aligned}$$

Then, the interpretation of the basic theory is not too surprising. Since terms correspond to setoid functions, we define them by their behavior when applied to an arbitrary $x \in \llbracket \Gamma \rrbracket$. This is defined in the first part of Fig. 8. Finally, to interpret observational equality and its `cast` operation, we use the setoid structure of the universe: where e_{refl} is obtained from the reflexivity of setoid equality, and e_{id} is obtained from the behavior of `el-eq` on reflexivity.

In order to prove the soundness of our interpretation, we need to extend it to weakenings and substitutions between contexts: Assume Γ and Δ are syntactical contexts, and A and t are syntactical terms. In case $\llbracket \Gamma, x : A, \Delta \rrbracket$ and $\llbracket \Gamma, \Delta \rrbracket$ are well-defined, let π_A be the projection:

$$\begin{aligned} \pi_A : \llbracket \Gamma, x : A, \Delta \rrbracket &\rightarrow_s \llbracket \Gamma, \Delta \rrbracket \\ (\vec{x}_{\Gamma}, x_A, \vec{x}_{\Delta}) &\mapsto (\vec{x}_{\Gamma}, \vec{x}_{\Delta}). \end{aligned}$$

In case $\llbracket \Gamma, \Delta[x := t] \rrbracket$ and $\llbracket \Gamma, x : A, \Delta \rrbracket$ are well-defined, we define the setoid function σ_t by:

$$\begin{aligned} \sigma_t : \llbracket \Gamma, \Delta[x := t] \rrbracket &\rightarrow_s \llbracket \Gamma, x : A, \Delta \rrbracket \\ (\vec{x}_{\Gamma}, \vec{x}_{\Delta}) &\mapsto (\vec{x}_{\Gamma}, \llbracket t \rrbracket_{\Gamma}, \vec{x}_{\Delta}). \end{aligned}$$

883		$\llbracket \mathcal{U}_i \rrbracket_{\Gamma} x$	$:=$	$c_{\cup} i$
884		$\llbracket \Omega_i \rrbracket_{\Gamma} x$	$:=$	$c_{\Omega} i$
885		$\llbracket \Pi(y : F). G \rrbracket_{\Gamma} x$	$:=$	$c_{\Pi} (\llbracket F \rrbracket_{\Gamma} x) (y \mapsto \llbracket G \rrbracket_{\Gamma, y:F} x, y)$
886		$\llbracket \lambda(y : F). t \rrbracket_{\Gamma} x$	$:=$	$y \mapsto (\llbracket t \rrbracket_{\Gamma, y:F} x, y)$
887		$\llbracket t u \rrbracket_{\Gamma} x$	$:=$	$(\llbracket t \rrbracket_{\Gamma} x) (\llbracket u \rrbracket_{\Gamma} x)$
888		$\llbracket \mathbb{N} \rrbracket_{\Gamma} x$	$:=$	$c_{\mathbb{N}}$
889		$\llbracket 0 \rrbracket_{\Gamma} x$	$:=$	0
890		$\llbracket S t \rrbracket_{\Gamma} x$	$:=$	$S (\llbracket t \rrbracket_{\Gamma} x)$
891		$\llbracket \mathbb{N}\text{-elim}(P, t_0, t_S, n) \rrbracket_{\Gamma} x$	$:=$	$\mathbb{N}\text{-elim}(\text{el} \circ (\llbracket P \rrbracket_{\Gamma} x), \llbracket t_0 \rrbracket_{\Gamma} x, \llbracket t_S \rrbracket_{\Gamma} x, \llbracket n \rrbracket_{\Gamma} x)$
892		$\llbracket \exists(y : F). G \rrbracket_{\Gamma} x$	$:=$	$c_{\exists} (\llbracket F \rrbracket_{\Gamma} x) (y \mapsto \llbracket G \rrbracket_{\Gamma, y:F} x, y)$
893		$\llbracket \langle t, u \rangle \rrbracket_{\Gamma} x$	$:=$	$(\llbracket t \rrbracket_{\Gamma} x, \llbracket u \rrbracket_{\Gamma} x)$
894		$\llbracket \text{fst}(t) \rrbracket_{\Gamma} x$	$:=$	$(\llbracket t \rrbracket_{\Gamma} x).1$
895		$\llbracket \text{snd}(t) \rrbracket_{\Gamma} x$	$:=$	$(\llbracket t \rrbracket_{\Gamma} x).2$
896		$\llbracket \perp \rrbracket_{\Gamma} x$	$:=$	c_{\perp}
897		$\llbracket \perp\text{-elim}(A, t) \rrbracket_{\Gamma} x$	$:=$	$\perp\text{-elim}(\text{el}(\llbracket A \rrbracket_{\Gamma} x), \llbracket t \rrbracket_{\Gamma} x)$
898		$\llbracket t \sim_A u \rrbracket_{\Gamma} x$	$:=$	$\llbracket t \rrbracket_{\Gamma} x \approx \llbracket u \rrbracket_{\Gamma} x \quad \text{in } \text{el}(\llbracket A \rrbracket_{\Gamma} x)$
899		$\llbracket \text{refl}(t) \rrbracket_{\Gamma} x$	$:=$	e_{refl}
900		$\llbracket \text{transp}(t, G, u, t', e) \rrbracket_{\Gamma} x$	$:=$	val-eq
901		$\llbracket \text{cast}(A, B, e, t) \rrbracket_{\Gamma} x$	$:=$	$\text{el-eq}(\llbracket A \rrbracket_{\Gamma} x, \llbracket B \rrbracket_{\Gamma} x, \llbracket e \rrbracket_{\Gamma} x, \llbracket t \rrbracket_{\Gamma} x)$
902		$\llbracket \text{castrefl}(A, t) \rrbracket_{\Gamma} x$	$:=$	e_{id}

Fig. 8. Interpretation of \mathbb{T}^{obs} in the Setoid Model

LEMMA 3.8 (WEAKENING). π_A is the semantic counterpart to the weakening of A : for all term u , when both sides are well defined, we have:

$$\llbracket u \rrbracket_{\Gamma, x:A, \Delta} = \llbracket u \rrbracket_{\Gamma, \Delta} \circ \pi_A$$

LEMMA 3.9 (SUBSTITUTION). σ_t is the semantic counterpart to the substitution by t : for all term u , when both sides are well defined, we have:

$$\llbracket u[x := t] \rrbracket_{\Gamma, \Delta[x:=t]} = \llbracket u \rrbracket_{\Gamma, x:A, \Delta} \circ \sigma_t$$

THEOREM 3.10 (SOUNDNESS OF THE SETOID MODEL).

- (1) If $\vdash \Gamma$ then $\llbracket \Gamma \rrbracket \in \text{Con}$.
- (2) If $\Gamma \vdash A : s_i$ then $\text{el} \circ \llbracket A \rrbracket_{\Gamma} \in \text{Ty}_{s,i} \Gamma$.
- (3) If $\Gamma \vdash t : A$ then $\llbracket t \rrbracket_{\Gamma} \in \text{tm}(\text{el} \circ \llbracket A \rrbracket_{\Gamma})$.
- (4) If $\Gamma \vdash t \equiv u : A$ then $\llbracket t \rrbracket_{\Gamma} = \llbracket u \rrbracket_{\Gamma}$

PROOF. By induction on the typing derivations. □

Consistency of \mathbb{T}^{obs} (Theorem 3.7) follows immediately from the soundness theorem: any inhabitant of \perp in the empty context is interpreted as a setoid function from the one-element setoid to the empty setoid, but no such function exists.

4 EXTENSIONS TO QUOTIENTS, ID TYPES AND INDUCTIVE TYPES

So far, we have defined and studied a minimal version of \mathbb{T}^{obs} . In this section, we consider several extensions of the theory. In regular MLTT, adding a type generally means giving rules for type formation, introduction, elimination and computation of the eliminator. In our case, we also need to provide computation rules for equality of types, equality of terms, and cast. Those extensions have not been formalized in the companion AGDA development.

4.1 Quotient Types

Quotients are a ubiquitous construction in mathematics, and one that is famously difficult to handle smoothly in MLTT. The usual way to handle quotients is *via* setoids, but since this structure is not built in MLTT, all the functions between setoids, all the predicates, etc... have to be supplemented with equality preservation lemmas—which appears to be quickly unmanageable.

In our theory however, every type is already a setoid and every term preserves the setoid equality by construction. This is a very comfortable setting for quotients, that can thus be added to the theory—provided the relation that induces the quotient is proof-irrelevant. This can be seen as a limitation, as noticed by [Sterling et al. \[2019\]](#), as it is generally impossible to extract proof-relevant information from equality in the quotient type. This is in contrast with the development of higher inductive types in the cubical setting [[Coquand et al. 2018](#)]. On the other hand, the positive consequence of this limitation is that the elimination principle of the quotient types is fairly easy to manipulate in \mathbb{T}^{obs} .

Quotient type are defined on a type A equipped with an equivalence relation on A

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash R : A \rightarrow A \rightarrow \Omega \quad \Gamma \vdash R_r : \Pi(x : A). R x x \quad \Gamma \vdash R_s : \Pi(x, y : A). R x y \rightarrow R y x \quad \Gamma \vdash R_t : \Pi(x, y, z : A). R x y \rightarrow R y z \rightarrow R x z}{\Gamma \vdash A/(R, R_r, R_s, R_t) : \mathcal{U}_i}$$

Since the proofs of reflexivity, symmetry and transitivity appear everywhere but are proof-irrelevant, we will generally omit them in the assumptions of our rules, and write A/R instead of $A/(R, R_r, R_s, R_t)$. The only constructor of quotient types is the canonical projection: from an element t of A , one obtains an element $\pi(t)$ of A/R which is whnf and equality between two canonical projections reduces to R .

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \pi(t) : A/R} \quad \frac{\Gamma \vdash t : A \quad \Gamma \vdash u : A}{\Gamma \vdash \pi(t) \sim_{A/R} \pi(u) \Rightarrow R t u : \Omega_i}$$

The definition of `cast` between two quotient types reduces when the casted term is a canonical projection.

$$\frac{\Gamma \vdash e : A/R \sim_{\mathcal{U}} A'/R' \quad \Gamma \vdash t : A}{\Gamma \vdash \text{cast}(A/R, A'/R', e, \pi(t)) \Rightarrow \pi(\text{cast}(A, A', \text{fst}(e), t)) : A/R'}$$

Observational equality between two quotient types reduces to equality of the (proof-relevant part of the) telescopes that define each quotient:

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash R : A \rightarrow A \rightarrow \Omega \quad \Gamma \vdash A' : \mathcal{U}_i \quad \Gamma \vdash R' : A' \rightarrow A' \rightarrow \Omega}{\Gamma \vdash A/R \sim_{\mathcal{U}} A'/R' \Rightarrow \exists(x : A \sim_{\mathcal{U}} A'). \Pi(x y : A). R x y \sim_{\Omega} R \text{cast}(A, A', e, x) \text{cast}(A, A', e, y) : \Omega_i}$$

The eliminator for quotient types encodes the universal property of quotients: to construct a function out of a quotient A/R , it suffices to give a function t_π out of A such that if $R x y$, then their images under t_π are equal.

$$\frac{\Gamma \vdash B : A/R \rightarrow s_i \quad \Gamma \vdash t_\pi : \Pi(x : A). B \pi(x)}{\Gamma \vdash t_\sim : \Pi(x, y : A). \Pi(e : R x y). (t_\pi x) \sim_{B \pi(x)} \text{cast}(B \pi(y), B \pi(x), B e^{-1}, t_\pi y) \quad \Gamma \vdash u : A/R}{\Gamma \vdash \text{Q-elim}(B, t_\pi, t_\sim, u) : B u}$$

The eliminator for quotient types has the obvious computation rule

$$\frac{\Gamma \vdash B : A/R \rightarrow s_i \quad \Gamma \vdash t_\pi : \Pi(x : A). B \pi(x)}{\Gamma \vdash t_\sim : \Pi(x, y : A). \Pi(e : R x y). (t_\pi x) \sim_{B \pi(x)} \text{cast}(B \pi(y), B \pi(x), B e^{-1}, t_\pi y) \quad \Gamma \vdash u : A}{\Gamma \vdash \text{Q-elim}(B, t_\pi, t_\sim, \pi(u)) \Rightarrow t_\pi u : B(\pi(u))}$$

There are also reduction rules that reduce terms to a weak head normal form under equality (of the form $A/R \sim_{\mathcal{U}} X$, and $x \sim_{A/R} y$, $\pi(a) \sim_{A/R} y$), and similarly for cast and quotient elimination, as well as new congruence rules as defined in Figs. 9 and 10.

We now turn to the proof that the metatheoretical properties of TT^{obs} are preserved by the addition of quotient types. More explicitly, we extend the logical relation framework and its fundamental lemma, as well as the setoid model, to quotient types. From there, we can replay our proofs of consistency, normalization, canonicity and decidability.

Reducibility. We first extend our reducibility proof to quotient types. Since they add a new family of types in normal form, we need to add a case to our logical relation:

$$\frac{\begin{array}{c} \Gamma \vdash A \Rightarrow^* A' / (R, R_r, R_s, R_t) : \mathcal{U}_i \\ \Gamma \vdash A' : \mathcal{U}_i \quad \forall \Delta \rho. \Delta \Vdash_{\ell} A'[\rho] \quad \Gamma \Vdash_{\ell} R : A' \rightarrow A' \rightarrow \Omega \quad \Gamma \vdash R_r : \Pi(x : A'). R x x \\ \Gamma \vdash R_s : \Pi(x, y : A'). R x y \rightarrow R y x \quad \Gamma \vdash R_t : \Pi(x, y, z : A'). R x y \rightarrow R y z \rightarrow R x z \end{array}}{\Gamma \Vdash_{\ell} A}$$

Given a type A reducible to a quotient type, we define:

- $\Gamma \Vdash_{\ell} A \equiv B$ if there are terms B', Q, Q_r, Q_s, Q_t such that
 - $\Gamma \vdash B \Rightarrow^* B' / (Q, Q_r, Q_s, Q_t) : \mathcal{U}_i$
 - $\forall \Delta \rho. \Delta \Vdash_{\ell} A'[\rho] \equiv B'[\rho]$
 - $\Gamma \Vdash_{\ell} R \equiv Q : A' \rightarrow A' \rightarrow \Omega$.
- $\Gamma \Vdash_{\ell} t : A$ if there is a normal form t' such that $\Gamma \vdash t \Rightarrow^* t' : A'/R$ and $\Gamma \Vdash_Q t'$, which is defined by

$$\frac{\Gamma \Vdash_{\ell} t : A' \quad \Gamma \vdash n : A'/R \quad n \text{ is neutral}}{\Gamma \Vdash_Q \pi(t) \quad \Gamma \Vdash_Q n}$$

- $\Gamma \Vdash_{\ell} t \equiv u : A$ if there are normal forms t', u' such that $\Gamma \vdash t \Rightarrow^* t' : A'/R$ and $\Gamma \vdash u \Rightarrow^* u' : A'/R$, and $\Gamma \Vdash_Q t' \equiv u'$, which is inductively defined by

$$\frac{\Gamma \Vdash_{\ell} t \equiv u : A' \quad \Gamma \vdash n \equiv m : A'/R \quad n, m \text{ are neutral}}{\Gamma \Vdash_Q \pi(t) \equiv \pi(u) \quad \Gamma \Vdash_Q n \equiv m}$$

Then, the proof of the fundamental lemma can be extended to handle the new typing rules, as well as the new cases of logical relation.

Interpretation in the Model. The type Setoid of setoids is naturally closed under quotients. Indeed, given a setoid A , providing A with a relation $R : A \times A \rightarrow_s \text{Prop}$ that is reflexive, symmetric and transitive is exactly the same thing as defining an equivalence relation on the carrier set of A that extends setoidal equality. Then, A/R is simply defined as a setoid having A for its carrier set, and the relation R as its setoidal equality. One can then easily show that A/R satisfies the universal property of a mathematical quotient, which tells us that this construction is the right candidate to interpret our quotient types.

However, our universe hierarchy \mathbf{U}_i is not closed under quotients, since its elements are inductively built from \mathbf{N} , universes and function types. Therefore, we need to modify our inductive-recursive definition to account for them. In the definition of \mathbf{U}_i , we add a constructor

$$\begin{array}{l} c_Q \quad : \quad (A : \mathbf{U}_i) \\ \quad \rightarrow (R : \text{el } A \rightarrow_s \text{el } A \rightarrow_s \Omega_i) \\ \quad \rightarrow (R_r : (x : \text{el } A) \rightarrow_s \text{val } (R x x)) \\ \quad \rightarrow (R_s : (x y : \text{el } A) \rightarrow_s \text{val } (R x y) \rightarrow \text{val } (R y x)) \\ \quad \rightarrow (R_t : (x y z : \text{el } A) \rightarrow_s \text{val } (R x y) \rightarrow \text{val } (R y z) \rightarrow \text{val } (R x z)) \\ \quad \rightarrow \mathbf{U}_i \end{array}$$

In the definition of el , our new constructor is handled as follows:

$$\text{el} (c_Q A R R_r R_s R_t) := (\text{el } A) / (\lambda x y. \text{val} (R x y))$$

In the definition of the setoidal equality on U_i :

$$c_Q A R R_r R_s R_t \approx c_Q A' R' R'_r R'_s R'_t := (e : A \approx A') \times ((x y : A) \rightarrow_s R x y \approx R' (\text{el-eq } e x) (\text{el-eq } e y))$$

and all of the other cases that involve c_Q and a different constructor reduce to \perp . We also need to update the definition of el-eq :

$$\text{el-eq} (c_Q A R R_r R_s R_t) (c_Q A' R' R'_r R'_s R'_t) e := (\lambda x. \text{el-eq } A A' e.1 x, \lambda x. \text{el-eq}^{-1} A A' e.1 x)$$

Finally, the reader can check that we can extend the proofs of reflexivity, symmetry and transitivity for \approx on U_i , as well as the proofs that el-eq is compatible with reflexivity and transitivity. This defines a new universe that is closed under quotient type formation. We let the reader check that the interpretation of the syntax that defines quotient can be done in this extended universe U_i .

4.2 Id Types

The reader may wonder if our theory extends Martin-Löf type theory with inductive types: that is, whether a judgement of MLTT is a judgement in the proof-relevant fragment of our theory. Our rules handle the universe hierarchy, the dependent products, and the natural numbers in the exact same way. But there are some difficulties around Martin-Löf identity type inductive equality, and more generally around indexed inductive types.

The first idea that might come to the reader's mind is to use the proof equality types of our theory to interpret the I -types of MLTT. Sure enough, proof irrelevance will provide us with more definitional equalities than what we require. However, we need to explain how we interpret the J eliminator for proof-relevant predicates.

It is not too hard to design a term that satisfies the correct typing rule, for instance, the term

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash B : \Pi(x : A). t \sim_A x \rightarrow \mathcal{U}_j \quad \Gamma \vdash b : B t \text{ refl}(t) \quad \Gamma \vdash t' : A \quad \Gamma \vdash e : t \sim_A t'}{\Gamma \vdash \text{cast}(B t \text{ refl}(t), B t' e, \text{eq}_j(A, t, u, t', e), b) : B t' e}$$

where

$$\text{eq}_j(A, t, B, u, t') e := \text{transp}(t, \lambda(x : A). \lambda(e' : t \sim x). B t \text{ refl}(A) \sim B x e', \text{refl}(B t \text{ refl}(A)), t', e).$$

But the computational behavior is not preserved: in general, this term will not reduce to u when we substitute $t' = t$ and $e = \text{refl}(t)$. It might do when B is a closed term, but it certainly won't if B is a neutral term. More generally, there is no hope to interpret I -types as proof-irrelevant types: I -types compute by doing reduction and pattern-matching on the equality proof, which cannot happen in a proof-irrelevant context.

A very similar problem was encountered by Cohen et al. [2015] in Cubical Type Theory with equality defined using the `Path` type, and solved by Swan [2016]. Following his ideas, we introduce Id-types:

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash u : A}{\Gamma \vdash \text{Id}(A, t, u) : \mathcal{U}_i} \quad \frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A}{\Gamma \vdash \text{Idrefl}(t) : \text{Id}(A, t, t)} \quad \frac{\Gamma \vdash e, e' : \text{Id}(A, t, u)}{\Gamma \vdash e \sim_{\text{Id}(A, t, u)} e' \Rightarrow \top : \Omega_i}$$

$$\frac{\Gamma \vdash B : \Pi(x : A). \text{Id}(A, t, x) \rightarrow s_j \quad \Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash u : B t \text{ Idrefl}(t) \quad \Gamma \vdash t' : A \quad \Gamma \vdash e : \text{Id}(A, t, t')}{\Gamma \vdash J(A, t, B, u, t', e) : B t' e}$$

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash B : \Pi(x : A). \text{Id}(A, t, x) \rightarrow s_j \quad \Gamma \vdash b : B \text{ t Idrefl}(t)}{\Gamma \vdash J(A, t, B, b, t, \text{Idrefl}(t)) \Rightarrow u : B \text{ t Idrefl}(t)}$$

These rules mimic the behavior of inductive I -types, that we quotiented so they contain only one inhabitant up to propositional equality. Observational equality between two identity types is defined as equality of the telescopes of arguments, as for the quotient type:

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash u : A \quad \Gamma \vdash A' : \mathcal{U}_i \quad \Gamma \vdash t' : A' \quad \Gamma \vdash u' : A'}{\Gamma \vdash \text{Id}(A, t, u) \sim_{\mathcal{U}} \text{Id}(A', t', u') \Rightarrow \exists(e : A \sim_{\mathcal{U}} A'). \text{cast}(A, A', e, t) \sim_{A'} t' \wedge \text{cast}(A, A', e, u) \sim_{A'} u' : \Omega_j}$$

We may hope to define computation rules for `cast` by simply reducing the equality proof to a weak head normal form, and then commuting `cast` with the head constructor like we did for other positive types. However, we quickly run into a problem:

$$\frac{\Gamma \vdash A, A' : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash t, u : A' \quad \Gamma \vdash e : \text{Id}(A, t, t) \sim \text{Id}(A', t', u')}{\Gamma \vdash \text{cast}(\text{Id}(A, t, t), \text{Id}(A', t', u'), e, \text{Idrefl}(t)) \Rightarrow ? : \text{Id}(A', t', u')}$$

We cannot reduce this term to `Idrefl`, because t' and u' are not convertible in general— e only provides us with a propositional equality $t' \sim_{A'} u'$. In order to fix this, we add a term `Idpath`(e) that turns any inhabitant of $e : t \sim_A u$ into an inhabitant of `Id`(A, t, u).

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash u : A \quad \Gamma \vdash e : t \sim_A u}{\Gamma \vdash \text{Idpath}(e) : \text{Id}(A, t, u)}$$

Then, the computation rule for `cast` on `Idrefl`(t) can be defined as:

$$\frac{\Gamma \vdash A, A' : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash t', u' : A' \quad \Gamma \vdash e : \text{Id}(A, t, t) \sim \text{Id}(A', t', u')}{\Gamma \vdash \text{cast}(\text{Id}(A, t, t), \text{Id}(A', t', u'), e, \text{Idrefl}(t)) \Rightarrow \text{Idpath}(\text{fst}(\text{snd}(e))^{-1} \cdot \text{snd}(\text{snd}(e))) : \text{Id}(A', t', u')}$$

We also need to account for this additional constructor in reduction rules:

$$\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash B : \Pi(x : A). \text{Id}(A, t, x) \rightarrow s_j \quad \Gamma \vdash b : B \text{ t Idrefl}(t) \quad \Gamma \vdash t' : A \quad \Gamma \vdash e : t \sim_A t'}{\Gamma \vdash J(A, t, B, b, t', \text{Idpath}(e)) \Rightarrow \text{cast}(B \text{ t Idrefl}(t), B \text{ t' Idpath}(e), \text{eq}_j(A, t, B, u, t')e, b) : B \text{ t' Idpath}(e)}$$

$$\frac{\Gamma \vdash A, A' : \mathcal{U}_i \quad \Gamma \vdash t, u : A \quad \Gamma \vdash e : t \sim_A u \quad \Gamma \vdash t', u' : A' \quad \Gamma \vdash e' : \text{Id}(A, t, t) \sim \text{Id}(A', t', u')}{\Gamma \vdash \text{cast}(\text{Id}(A, t, u), \text{Id}(A', t', u'), e', \text{Idpath}(e)) \Rightarrow \text{Idpath}(\text{fst}(\text{snd}(e'))^{-1} \cdot \text{ap}(\text{cast}(A, A', \text{fst}(e'), -)) e \cdot \text{snd}(\text{snd}(e'))) : \text{Id}(A', t', u')}$$

Along with congruence rules and reduction of the scrutinee of `J` and `cast`, these form the rules for `Id` types.

Relation with Setoid Equality. The introduction rule for `Idpath` proves that $t \sim_A u$ implies `Id`(A, t, u). Conversely, if we have an inhabitant of `Id`(A, t, u), we can get a proof of $t \sim_A u$ by combining `J` to reduce it to the case $u = t$, and `refl`(t) to inhabit $t \sim_A t$. Since both types are also contractible (for both notions of equality), they are equivalent.

1128 *Reducibility Proof.* In order to fit identity types in our normalization proof, we add another case
1129 to the logical relation:

$$1130 \quad \frac{\Gamma \vdash A \Rightarrow^* \text{Id}(A', t, u) : \mathcal{U}_i \quad \Gamma \Vdash_{\ell} A' \quad \Gamma \Vdash_{\ell} t : A' \quad \Gamma \Vdash_{\ell} u : A'}{\Gamma \Vdash_{\ell} A}$$

1133 When A is reducible to an identity type, we define:

- 1134 • $\Gamma \Vdash_{\ell} A \equiv B$ if there are terms B', t', u' such that
 - 1135 – $\Gamma \vdash B \Rightarrow^* \text{Id}(B', t', u') : \mathcal{U}_i$
 - 1136 – $\Gamma \Vdash_{\ell} A' \equiv B'$
 - 1137 – $\Gamma \Vdash_{\ell} t \equiv t' : A'$
 - 1138 – $\Gamma \Vdash_{\ell} u \equiv u' : A'$.
- 1139 • $\Gamma \Vdash_{\ell} e : A$ if there is a normal form e' such that $\Gamma \vdash e \Rightarrow^* e' : \text{Id}(A', t, u)$ and $\Gamma \Vdash \text{Id } e'$, which
1140 is defined by

$$1142 \quad \frac{}{\Gamma \Vdash \text{Id } \text{Idrefl}(t)} \quad \frac{\Gamma \vdash e : t \sim_{A'} u}{\Gamma \Vdash \text{Id } \text{Idpath}(e)} \quad \frac{\Gamma \vdash n : \text{Id}(A', t, u) \quad n \text{ is neutral}}{\Gamma \Vdash \text{Id } n}$$

- 1144 • $\Gamma \Vdash_{\ell} e \equiv f : A$ if there are normal forms e', f' such that $\Gamma \vdash e \Rightarrow^* e' : \text{Id}(A', t, u)$ and
1145 $\Gamma \vdash f \Rightarrow^* f' : \text{Id}(A', t, u)$, and $\Gamma \Vdash \text{Id } e' \equiv f'$, which is inductively defined by

$$1147 \quad \frac{\Gamma \vdash e, f : t \sim_{A'} u}{\Gamma \Vdash \text{Id } \text{Idrefl}(t) \equiv \text{Idrefl}(t)} \quad \frac{\Gamma \vdash e, f : t \sim_{A'} u}{\Gamma \Vdash \text{Id } \text{Idpath}(e) \equiv \text{Idpath}(f)}$$

$$1148 \quad \frac{\Gamma \vdash n \equiv m : \text{Id}(A', t, u) \quad n, m \text{ are neutral}}{\Gamma \Vdash \text{Id } n \equiv m}$$

1152 Again, the proof of the fundamental lemma can be extended to handle the new typing rules, as
1153 well as the new cases of logical relation.

1155 4.3 Box and Squash

1156 Box types embed the proof-irrelevant types into the proof-relevant world. They are useful for
1157 a number of constructions: for instance, from a type $A : \mathcal{U}_i$ and a proof-irrelevant predicate
1158 $P : A \rightarrow \Omega_i$, one can build a *subset type* $\Sigma(x : A). \Box(P x) : \mathcal{U}_i$ whose inhabitants come with a proof
1159 of P , but retain the computational behavior of inhabitants of A .

$$1162 \quad \frac{\Gamma \vdash A : \Omega_i}{\Gamma \vdash \Box A : \mathcal{U}_i} \quad \frac{\Gamma \vdash A : \Omega_i \quad \Gamma \vdash t : A}{\Gamma \vdash \diamond t : \Box A} \quad \frac{\Gamma \vdash t, u : \Box A}{\Gamma \vdash t \sim_{\Box A} u \Rightarrow \top : \Omega_i} \quad \frac{\Gamma \vdash A : \Omega_i \quad \Gamma \vdash t : \Box A}{\Gamma \vdash \Box\text{-elim}(t) : A}$$

$$1165 \quad \frac{\Gamma \vdash A, B : \Omega_i}{\Gamma \vdash \Box A \sim_{\mathcal{U}} \Box B \Rightarrow A \sim_{\Omega} B : \Omega_j} \quad \frac{\Gamma \vdash A, B : \Omega_i \quad \Gamma \vdash t : A \quad \Gamma \vdash e : \Box A \sim_{\mathcal{U}} \Box B}{\Gamma \vdash \text{cast}(\Box A, \Box B, e, \diamond t) \Rightarrow \diamond \text{cast}(A, B, e, t) : \Box B}$$

1167 Conversely, Squash types embed the proof-relevant world into the proof-irrelevant world.

$$1168 \quad \frac{\Gamma \vdash A : \mathcal{U}_i}{\Gamma \vdash \|A\| : \Omega_i} \quad \frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash t : A}{\Gamma \vdash |t| : \|A\|}$$

$$1171 \quad \frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash P : \|A\| \rightarrow \Omega_j \quad \Gamma \vdash t_A : \Pi(x : A). P |x| \quad \Gamma \vdash t : \|A\|}{\Gamma \vdash \text{S-elim}(P, t_A, t) : P t}$$

1174 It is not very difficult to check that we can extend the logical relation, as well as lemmas 3.3 and 3.4
1175 so that they handle Box types and Squash types. Likewise, we can extend the setoid model and its
1176

1177 interpretation function, and obtain that these addition preserve the metatheoretical properties of
 1178 \mathbb{T}^{obs} .

1179

1180 5 RELATED WORK AND CONCLUSION

1181 Compared to [Altenkirch et al. 2007], the most important ingredient in \mathbb{T}^{obs} is the use of definitional
 1182 proof irrelevance. This added flexibility in computations allows our recursors to enjoy proper
 1183 computational behavior on open terms, and it also lets us seamlessly treat universe hierarchies.
 1184 Moreover, the normalization proof for OTT relies on a normalization conjecture for a different
 1185 theory, unlike the normalization proof for \mathbb{T}^{obs} .

1186 In [Altenkirch et al. 2019], the authors define a setoid model in $\text{MLTT} + \Omega$. Then, they interpret
 1187 a version of MLTT with proof-irrelevant identity types that support propext and funext in their
 1188 model, thereby providing a computational interpretation of these principles. However, handling
 1189 universes in their model requires some additions to $\text{MLTT} + \Omega$, and the resulting theory is only
 1190 conjectured to be normalizing. In contrast to this, \mathbb{T}^{obs} is a full-fledged type theory and does not
 1191 require any external model to compute.

1192 Compared to XTT [Sterling et al. 2019], the strengths of \mathbb{T}^{obs} are a normalization strategy that
 1193 exhibits canonicity, as well a full proof that conversion and typing are decidable. These properties
 1194 allow us to present a concrete implementation of our system in a proof assistant. In XTT however,
 1195 Sterling et al. show that typing cannot be decidable, as there is no way to deduce $A \sim A'$ and
 1196 $B \sim B'$ from a proof of $A \times B \sim A' \times B'$. In order to fix this shortcoming, they suggest adding a
 1197 “typecase” operator to their theory, but argue against it since it forces the universe to be closed,
 1198 thereby severely constraining the possible semantics. In \mathbb{T}^{obs} , we obtain the injectivity of type
 1199 constructors from the behavior of observational equality in the universe. These rules somewhat
 1200 constrain the semantics—for instance, we cannot interpret \mathbb{T}^{obs} in set theory using a Grothendieck
 1201 universe as the interpretation of \mathcal{U} —but our universe remains open to the addition of arbitrary
 1202 types.

1203 Finally, our setoidal adaptation of Swan’s Id types [Swan 2016] turns \mathbb{T}^{obs} into a proper extension
 1204 of MLTT, that realizes UIP, funext and propext while enjoying algorithmic canonicity. To the best
 1205 of our knowledge, this is a new result.

1206

1207 REFERENCES

- 1208 Andreas Abel and Thierry Coquand. 2020. Failure of Normalization in Impredicative Type Theory with Proof-Irrelevant
 1209 Propositional Equality. *Logical Methods in Computer Science* Volume 16, Issue 2 (June 2020). [https://doi.org/10.23638/LMCS-16\(2:14\)2020](https://doi.org/10.23638/LMCS-16(2:14)2020)
- 1210 Andreas Abel, Joakim Öhman, and Andrea Vezzosi. 2018. Decidability of Conversion for Type Theory in Type Theory. *Proceedings of the ACM on Programming Languages* 2, POPL, Article 23 (Jan. 2018), 29 pages. <https://doi.org/10.1145/3158111>
- 1211 T. Altenkirch. 1999. Extensional equality in intensional type theory. In *Proceedings. 14th Symposium on Logic in Computer*
 1212 *Science (Cat. No. PR00158)*. 412–420. <https://doi.org/10.1109/LICS.1999.782636>
- 1213 Thorsten Altenkirch, Simon Boulier, Ambrus Kaposi, and Nicolas Tabareau. 2019. Setoid type theory - a syntactic translation.
 1214 In *MPC 2019 - 13th International Conference on Mathematics of Program Construction (LNCS)*, Vol. 11825. Springer, 155–196.
 1215 https://doi.org/10.1007/978-3-030-33636-3_7
- 1216 Thorsten Altenkirch, Paolo Capriotti, and Nicolai Kraus. 2016. Extending Homotopy Type Theory with Strict Equality. In
 1217 *CSL*.
- 1218 Thorsten Altenkirch, Conor McBride, and Wouter Swierstra. 2007. Observational equality, now!. In *Proceedings of the*
 1219 *Workshop on Programming Languages meets Program Verification (PLPV 2007)*. 57–68.
- 1220 Paolo Capriotti. 2017. *Models of type theory with strict equality*. Ph.D. Dissertation. University of Nottingham.
- 1221 Jesper Cockx, Nicolas Tabareau, and Théo Winterhalter. 2021. The Taming of the Rew: A Type Theory with Computational
 1222 Assumptions. *Proc. ACM Program. Lang.* 5, POPL, Article 60 (Jan. 2021), 29 pages. <https://doi.org/10.1145/3434341>
- 1223 Cyril Cohen, Thierry Coquand, Simon Huber, and Anders Mörtberg. 2015. Cubical Type Theory: a constructive interpretation
 1224 of the univalence axiom. In *21st International Conference on Types for Proofs and Programs (21st International Conference*
 1225

- 1226 on *Types for Proofs and Programs*). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Tallinn, Estonia, 262. <https://doi.org/10.4230/LIPIcs.TYPES.2015.5>
- 1227
- 1228 Thierry Coquand, Simon Huber, and Anders Mörtberg. 2018. On Higher Inductive Types in Cubical Type Theory. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science (Oxford, United Kingdom) (LICS '18)*. Association for Computing Machinery, New York, NY, USA, 255–264. <https://doi.org/10.1145/3209108.3209197>
- 1229
- 1230 Peter Dybjer. 1996. Internal type theory. In *Types for Proofs and Programs*, Stefano Berardi and Mario Coppo (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 120–134.
- 1231
- 1232 Gaëtan Gilbert, Jesper Cockx, Matthieu Sozeau, and Nicolas Tabareau. 2019. Definitional Proof-Irrelevance without K. *Proceedings of the ACM on Programming Languages* 3 (Jan. 2019), 1–28. <https://doi.org/10.1145/329031610.1145/3290316>
- 1233
- 1234 Jean-Yves Girard. 1972. Interprétation fonctionnelle et élimination des coupures dans l’arithmétique d’ordre supérieur. (1972). Thèse de Doctorat d’État, Université de Paris VII.
- 1235
- 1236 Martin Hofmann. 1993. Non Strictly Positive Datatypes in System F. Email on types mailing list. <http://www.seas.upenn.edu/~sweirich/types/archive/1993/msg00027.html>.
- 1237
- 1238 Martin Hofmann. 1995. *Extensional concepts in intensional type theory*. Ph.D. Dissertation. University of Edinburgh.
- 1239
- 1240 Chris Kapulkin, Peter LeFanu Lumsdaine, and Vladimir Voevodsky. 2012. The simplicial model of univalent foundations. *arXiv preprint arXiv:1211.2851* (2012).
- 1241
- 1242 Meven Lennon-Bertrand. 2021. Complete Bidirectional Typing for the Calculus of Inductive Constructions. In *12th International Conference on Interactive Theorem Proving (ITP 2021) (Leibniz International Proceedings in Informatics (LIPIcs))*, Liron Cohen and Cezary Kaliszyk (Eds.), Vol. 193. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. <https://doi.org/10.4230/LIPIcs.ITP.2021.24>
- 1243
- 1244 Per Martin-Löf. 1975. An Intuitionistic Theory of Types: Predicative Part. In *Logic Colloquium '73*, H.E. Rose and J.C. Shepherdson (Eds.). Studies in Logic and the Foundations of Mathematics, Vol. 80. Elsevier, 73 – 118. [https://doi.org/10.1016/S0049-237X\(08\)71945-1](https://doi.org/10.1016/S0049-237X(08)71945-1)
- 1245
- 1246 Jonathan Sterling, Carlo Angiuli, and Daniel Gratzer. 2019. Cubical Syntax for Reflection-Free Extensional Equality. In *4th International Conference on Formal Structures for Computation and Deduction (FSCD 2019) (Leibniz International Proceedings in Informatics (LIPIcs))*, Herman Geuvers (Ed.), Vol. 131. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 31:1–31:25. <https://doi.org/10.4230/LIPIcs.FSCD.2019.31>
- 1247
- 1248 Andrew Swan. 2016. An algebraic weak factorisation system on 01-substitution sets: a constructive proof. *Journal of Logic and Analysis* (2016). <https://doi.org/10.4115/jla.2016.8.1>
- 1249
- 1250 The Univalent Foundations Program. 2013. *Homotopy Type Theory: Univalent Foundations of Mathematics*. Institute for Advanced Study.
- 1251
- 1252 Andrea Vezzosi, Anders Mörtberg, and Andreas Abel. 2019. Cubical Agda: A Dependently Typed Programming Language with Univalence and Higher Inductive Types. *Proc. ACM Program. Lang.* 3, ICFP, Article 87 (July 2019), 29 pages. <https://doi.org/10.1145/3341691>
- 1253
- 1254 Vladimir Voevodsky. 2013. A simple type system with two identity types. <https://ncatlab.org/homotopytypetheory/files/HTS.pdf>
- 1255
- 1256 Vladimir Voevodsky. 2015. A C-system defined by a universe category. *Theory Appl. Categ.* 30 (2015), No. 37, 1181–1215. <http://www.tac.mta.ca/tac/volumes/30/37/30-37abs.html> <p>Prepublication versions in arXiv.</p>
- 1257
- 1258
- 1259
- 1260
- 1261
- 1262
- 1263
- 1264
- 1265
- 1266
- 1267
- 1268
- 1269
- 1270
- 1271
- 1272
- 1273
- 1274

1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372

$$\begin{array}{c}
\text{APP-SUBST} \\
\frac{\Gamma \vdash t \Rightarrow t' : \Pi(x : A). B \quad \Gamma \vdash u : A}{\Gamma \vdash t u \Rightarrow t' u : B[x := u]} \\
\\
\text{\mathbb{N}-ELIM-SUBST} \\
\frac{\Gamma \vdash A : \mathbb{N} \rightarrow s_i \quad \Gamma \vdash t_0 : A \mathbf{0} \quad \Gamma \vdash t_S : \Pi(n : \mathbb{N}). A n \rightarrow A (\mathbf{S} n) \quad \Gamma \vdash n \Rightarrow n' : \mathbb{N}}{\Gamma \vdash \mathbf{N-elim}(A, t_0, t_S, n) \Rightarrow \mathbf{N-elim}(A, t_0, t_S, n') : A n} \\
\\
\text{EQ-SUBST} \qquad \qquad \qquad \text{EQ-UNIV-SUBST} \\
\frac{\Gamma \vdash A \Rightarrow A' : \mathcal{U}_i \quad \Gamma \vdash t : A \quad \Gamma \vdash u : A}{\Gamma \vdash t \sim_A u \Rightarrow t \sim_{A'} u : \Omega_i} \qquad \frac{\Gamma \vdash A \Rightarrow A' : \mathcal{U}_i \quad \Gamma \vdash B : \mathcal{U}_i}{\Gamma \vdash A \sim_{\mathcal{U}_i} B \Rightarrow A' \sim_{\mathcal{U}_i} B : \Omega_j}^{i < j} \\
\\
\text{EQ-UNIV-\mathbb{N}-SUBST} \qquad \qquad \qquad \text{EQ-UNIV-II-SUBST} \\
\frac{\Gamma \vdash B \Rightarrow B' : \mathcal{U}_i}{\Gamma \vdash \mathbb{N} \sim_{\mathcal{U}_i} B \Rightarrow \mathbb{N} \sim_{\mathcal{U}_i} B' : \Omega_j}^{i < j} \qquad \frac{\Gamma \vdash \Pi(x : A). P : \mathcal{U}_i \quad \Gamma \vdash B \Rightarrow B' : \mathcal{U}_i}{\Gamma \vdash \Pi(x : A). P \sim_{\mathcal{U}_i} B \Rightarrow \Pi(x : A). P \sim_{\mathcal{U}_i} B' : \Omega_j}^{i < j} \\
\\
\text{EQ-\mathbb{N}-SUBST} \qquad \qquad \qquad \text{EQ-\mathbb{N}-ZERO-SUBST} \qquad \qquad \qquad \text{EQ-\mathbb{N}-SUC-SUBST} \\
\frac{\Gamma \vdash n \Rightarrow n' : \mathbb{N} \quad \Gamma \vdash m : \mathbb{N}}{\Gamma \vdash n \sim_{\mathbb{N}} m \Rightarrow n' \sim_{\mathbb{N}} m : \Omega_i} \qquad \frac{\Gamma \vdash n \Rightarrow n' : \mathbb{N}}{\Gamma \vdash 0 \sim_{\mathbb{N}} n \Rightarrow 0 \sim_{\mathbb{N}} n' : \Omega_i} \qquad \frac{\Gamma \vdash m : \mathbb{N} \quad \Gamma \vdash n \Rightarrow n' : \mathbb{N}}{\Gamma \vdash \mathbf{S} m \sim_{\mathbb{N}} n \Rightarrow \mathbf{S} m \sim_{\mathbb{N}} n' : \Omega_i} \\
\\
\text{CAST-SUBST} \\
\frac{\Gamma \vdash A \Rightarrow A' : s_i \quad \Gamma \vdash B : s_i \quad \Gamma \vdash e : A \sim_{s_i} B \quad \Gamma \vdash t : A}{\Gamma \vdash \mathbf{cast}(A, B, e, t) \Rightarrow \mathbf{cast}(A', B, e, t) : B} \\
\\
\text{CAST-\mathcal{U}-SUBST} \\
\frac{\Gamma \vdash A : \mathcal{U}_i \quad \Gamma \vdash e : \mathcal{U}_i \sim_{\mathcal{U}_j} B \quad \Gamma \vdash B \Rightarrow B' : \mathcal{U}_j}{\Gamma \vdash \mathbf{cast}(\mathcal{U}_i, B, e, A) \Rightarrow \mathbf{cast}(\mathbb{N}, B', e, A) : B}^{i < j} \\
\\
\text{CAST-\mathbb{N}-SUBST} \\
\frac{\Gamma \vdash n : \mathbb{N} \quad \Gamma \vdash e : \mathbb{N} \sim_{\mathcal{U}_i} B \quad \Gamma \vdash B \Rightarrow B' : \mathcal{U}_i}{\Gamma \vdash \mathbf{cast}(\mathbb{N}, B, e, n) \Rightarrow \mathbf{cast}(\mathbb{N}, B', e, n) : B} \\
\\
\text{CAST-II-SUBST} \\
\frac{\Gamma \vdash \Pi(x : A). P : \mathcal{U}_i \quad \Gamma \vdash f : \Pi(x : A). P \quad \Gamma \vdash e : \Pi(x : A). P \sim_{\mathcal{U}_i} B \quad \Gamma \vdash B \Rightarrow B' : \mathcal{U}_i}{\Gamma \vdash \mathbf{cast}(\Pi(x : A). P, B, e, f) \Rightarrow \mathbf{cast}(\Pi(x : A). P, B', e, f) : B} \\
\\
\text{CAST-\mathbb{N}-\mathbb{N}-SUBST} \\
\frac{\Gamma \vdash e : \mathbb{N} \sim_{\mathcal{U}} \mathbb{N} \quad \Gamma \vdash n \Rightarrow n' : \mathbb{N}}{\Gamma \vdash \mathbf{cast}(\mathbb{N}, \mathbb{N}, e, n) \Rightarrow \mathbf{cast}(\mathbb{N}, \mathbb{N}, e, n') : \mathbb{N}}
\end{array}$$

Fig. 10. TT^{obs} Reduction Rules (substitutions only)