Journal of Pure and Applied Algebra 225 (2021) 106687

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

Construction of the circle in *UniMath*

Marc Bezem [a,*], Ulrik Buchholtz [b], Daniel R. Grayson [c,1], Michael Shulman [d]

[a] *Department of Informatics, University of Bergen, Norway*
[b] *Department of Mathematics, Technical University of Darmstadt, Germany*
[c] *Department of Mathematics, University of Illinois at Urbana-Champaign, United States of America*
[d] *Department of Mathematics, University of San Diego, United States of America*

ARTICLE INFO

Article history:
Received 15 October 2019
Received in revised form 18 November 2020
Available online 11 January 2021
Communicated by E. Riehl

MSC:
03B15; 03B70; 55U35; 03G30

ABSTRACT

We show that the type T$\mathbb{Z}$ of $\mathbb{Z}$-torsors has the dependent universal property of the circle, which characterizes it up to a unique homotopy equivalence. The construction uses Voevodsky's Univalence Axiom and propositional truncation, yielding a stand-alone construction of the circle not using higher inductive types.

Contents

* Corresponding author.
E-mail addresses: marc.bezem@uib.no (M. Bezem), ulrikbuchholtz@gmail.com (U. Buchholtz), danielrichardgrayson@gmail.com (D.R. Grayson), shulman@sandiego.edu (M. Shulman).
URLs: https://www.ae-info.org/ae/Member/Bezem_Marc (M. Bezem), https://www2.mathematik.tu-darmstadt.de/~buchholtz/ (U. Buchholtz), http://dangrayson.com/ (D.R. Grayson), http://www.sandiego.edu/~shulman/ (M. Shulman).
[1] *Current address:* 2409 S. Vine St., Urbana, Illinois 61801, USA.

https://doi.org/10.1016/j.jpaa.2021.106687

1. Introduction

In the standard set-theoretic foundations of mathematics, the sets have elements, which are themselves sets. A set has no additional structure connecting its various elements to each other. An equation between two sets is always a proposition, and equality between two elements of a set is independent of the ambient set. By contrast, in homotopy type theory and in Voevodsky's univalent foundations, the *types* are the fundamental objects, serving to classify the objects of mathematics. They have elements. Equations are used only to compare two elements of the same type, and the equations are not always propositions. Types thus behave much like spaces, viewed from the point of view of homotopy theory, due to the promotion of isomorphisms between objects of the same type to equalities (true equations), together with the intuition that an equality between two objects of the same type is like a path between two points in the same space.

Synthetic homotopy theory is the study of the homotopy theoretic properties of types. It is a fruitful one, because it turns out that many of the most basic results of standard homotopy theory have true analogues for types. This is true even though the framework is based purely on logical principles, rather than implemented like traditional homotopy theory in terms of topological spaces and continuous maps or combinatorial structures such as simplicial sets and fibrant replacement.

In standard homotopy theory it is well known that the *classifying space* of the group $\mathbb{Z}$ of integers is homotopy equivalent to the circle. We aim to reproduce that result in synthetic homotopy theory in a way that doesn't presuppose the existence of a circle.

The traditional algebraic notion of $\mathbb{Z}$-torsor yields a category whose objects are the $\mathbb{Z}$-torsors. Moreover, this category is a groupoid (all arrows are isomorphisms), and one specific object—namely $\mathbb{Z}$ itself—is the trivial $\mathbb{Z}$-torsor, whose automorphism group is $\mathbb{Z}$, and to which every other object is merely isomorphic. In univalent type theory, this category is thus completely captured by the type $\mathrm{T}\mathbb{Z}$ of all $\mathbb{Z}$-torsors, which is a connected pointed 1-type whose fundamental group is $\mathbb{Z}$; we may call it the *classifying type* of $\mathbb{Z}$. In this paper we show that $\mathrm{T}\mathbb{Z}$ behaves the way a circle ought to behave, by establishing that maps from it to other types (or families of types) are freely determined by the destinations of the base point and the canonical loop at the base point (corresponding to the element 1 of $\mathbb{Z}$). The proof is constructive, in that it does not appeal to the axiom of choice or the law of the excluded middle.

There are various types equivalent to the type of $\mathbb{Z}$-torsors, and thus they also provide constructions of circles: all one needs is a connected pointed type whose automorphism groups are isomorphic to $\mathbb{Z}$. For example, if one arising from geometry is desired, one may consider the type consisting of all frieze patterns in a Euclidean plane[2] formed from a linear collection of evenly spaced copies of the letter F.

$$\cdots FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF\cdots$$

We have formalized the result in *UniMath*, a name which refers both to Voevodsky's (univalent) foundation of mathematics based on a formal type theoretic language and to a particular repository [21] of formalized proofs, initiated by him, encoded in the language of the proof assistant *Coq*. See [20] for an overview by Voevodsky of it.

The other standard way to construct a circle in type theory uses *higher inductive types*, where one posits a new type $\mathbb{S}^1$, an element $\mathrm{pt} : \mathbb{S}^1$, a path $\circlearrowleft : \mathrm{pt} = \mathrm{pt}$, an induction principle (for defining functions from it), and nothing more. Adding higher inductive types to the system would give another construction of the circle,

[2] We say *a* Euclidean plane instead of *the* Euclidean plane to indicate that the type is actually the type of pairs consisting of a Euclidean plane and such a frieze pattern in it.

equivalent to the one described above. Voevodsky chose not to include higher inductive types, nor inductive types,[3] in *UniMath* for two chief reasons. Firstly, it was (and still is) not clear how to specify precisely what a definition of a higher inductive type consists of: see [3,5] for two approaches. Secondly, Voevodsky planned to prove consistency of *UniMath* in a series of papers[4] and realized that adding inductive types and higher inductive types to the system would dramatically increase the length of the series and the burden of writing them; as it was, he died before completing the project. At his death the series was well underway but far from complete: [16,12,13,17,18,14,19]. His approach in the series is to interpret each of the basic constructions of the formal system as a traditional mathematical construction: a context is interpreted as a fibrant simplicial set, a type in a context is interpreted as a fibration of fibrant simplicial sets, an element of a type in a context is interpreted as a section of such a fibration, and so on.

More recent work [1,2], unpublished but formalized, has established the initiality principle for the type theory used in *UniMath*, which Voevodsky had emphasized as a crucial unproven step. That, together with the simplicial set model described in [4], may arguably be regarded as establishing the consistency result that Voevodsky sought.

We turn now to the content of this paper.

As a prerequisite we require, of the reader, a working knowledge of homotopy type theory as described in, for example, the first four chapters of [11]. In the next Section 2, more precisely in Eq. (2.6), we give a precise formulation of the main result.

Preparing for the proof of the main result, we give in Section 3 some auxiliary results that are not in the first four chapters of [11]. The full proof of the main result can be found in Section 4, more precisely in Section 4.2. In Section 5 we discuss the interpretation of the main result in higher toposes, before we conclude in Section 6.

2. Precise formulation and discussion

2.1. Preview of the type of $\mathbb{Z}$-torsors

Recall that for a group G, a *G-torsor* consists of a nonempty set X and a left action of G on it that is free and transitive. This means that for all $x, y \in X$ there is a unique $g \in G$ such that $g \cdot x = y$. Any element $x_0 \in X$ yields a bijection $e : G \to X$ given by $g \mapsto g \cdot x_0$. If the operation in the group G is written additively, we'll echo that by writing the torsor operation additively: $g + x$.

In the case where G is $\mathbb{Z}$, then since $\mathbb{Z}$ is a free group with one generator, an action of $\mathbb{Z}$ on a set X is completely determined by the action of the integer 1—it is a bijection $X \xrightarrow{\cong} X$ which we denote by f. Fixing $x_0 \in X$, the corresponding bijection $e : \mathbb{Z} \to X$ then satisfies $e(s(n)) = (1+n)+x_0 = 1+(n+x_0) = f(e(n))$ for all integers n. So the following diagram commutes.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow[s]{\cong} & \mathbb{Z} \\ {\scriptstyle e}\downarrow{\scriptstyle \cong} & & {\scriptstyle e}\downarrow{\scriptstyle \cong} \\ X & \xrightarrow[f]{} & X \end{array}$$

Conversely, we get a unique $\mathbb{Z}$-torsor from any pair (X, f), where X is a nonempty set and $f : X \to X$ is a function, such that there merely exists a bijection e that makes the diagram above commute, by

[3] *UniMath* accepts just a few specific types and type formers that can be introduced as inductive types, namely: the finite types of cardinality at most 2, the natural numbers, binary coproducts, sums of families of types, and identity types.

[4] Early work [4] with Kapulkin and Lumsdaine to establish consistency left him unsatisfied, so he embarked on his own series of papers, to be realized with more details exposed.

transporting the structure of $\mathbb{Z}$ as a trivial $\mathbb{Z}$-torsor along e, thereby expressing e as an isomorphism of $\mathbb{Z}$-torsors. Independence of the structure on X from the choice of e is established by observing that $n + x_0 = f^n(x_0)$ for all $n \in \mathbb{Z}$. Alternatively, one could use the existence of e to show that f is a bijection and X is nonempty, define an action of $\mathbb{Z}$ on X by setting $n + x := f^n(x)$ for any $n \in \mathbb{Z}$, and then use the existence of e again to show that the action is free and transitive.

With the above considerations in mind, and recalling that, in the presence of univalence, isomorphisms correspond to identities, we consider pairs (X, f) of type $\sum_{X:\mathcal{U}}(X \to X)$ and introduce *the pointed type of $\mathbb{Z}$-torsors* by adopting the following definitions (cf. Definition 4.1).

$$\mathrm{T}\mathbb{Z} :\equiv \sum_{(X,f)} \|(\mathbb{Z}, s) = (X, f)\|$$

$$\mathrm{pt} :\equiv ((\mathbb{Z}, s), |\mathrm{refl}_{(\mathbb{Z},s)}|) : \mathrm{T}\mathbb{Z}$$

We claim that the type $\mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}$ is equivalent to $\mathbb{Z}$. To see that, begin by observing that every function $f : \mathbb{Z} \to \mathbb{Z}$ commuting with s is propositionally equal to $s^{f(0)}$. The first projection acting on $p : \mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}$ gives a path $\mathrm{pr}_1(p) : \mathbb{Z} = \mathbb{Z}$ such that the corresponding transport function $\mathrm{pr}_1(p)_* : \mathbb{Z} \to \mathbb{Z}$ is a bijection commuting with s. We evaluate this bijection at 0. Let $\mathrm{ev}_0(p) :\equiv \mathrm{pr}_1(p)_*(0)$ for all $p : \mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}$, then $\mathrm{ev}_0 : (\mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}) \to \mathbb{Z}$. Combining these observations and using the univalence axiom, one proves that ev_0 is an equivalence.

Since $\mathbb{Z}$ is a set, it follows that the underlying set of the fundamental group of $(\mathrm{T}\mathbb{Z}, \mathrm{pt})$ is equivalent to $\mathbb{Z}$, and with a bit more work, that the fundamental group of $(\mathrm{T}\mathbb{Z}, \mathrm{pt})$ is isomorphic to $\mathbb{Z}$. However, we do not need this fact here.

We define $1 :\equiv s(0)$. The preimage of 1 under the equivalence ev_0 is a natural generating path of $\mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}$, so we define $\circlearrowleft :\equiv \mathrm{ev}_0^{-1}(1)$, which we call the *loop* of $\mathrm{T}\mathbb{Z}$. Alternatively, we could have obtained $\circlearrowleft$ directly from $s : \mathbb{Z} \simeq \mathbb{Z}$ by applying the univalence axiom (with some easy add-ons, e.g., proving that s commutes with itself).

2.2. The type of circles

In order to explain our main result, that $\mathrm{T}\mathbb{Z}$ behaves like the circle understood as a higher inductive type with constructors $\mathrm{pt} : \mathrm{T}\mathbb{Z}$ and $\circlearrowleft : pt = \mathrm{pt}$, we introduce, following [10], the type of *circle algebras*, consisting of a type together with a point and a loop at that point.

$$\mathbb{S}\text{-Alg} :\equiv \sum_{C:\mathcal{U}} \sum_{c:C} c = c.$$

The type of *fibered circle algebras* over a circle algebra $\mathcal{C} \equiv (C, c, s)$ is defined to be the dependent version thereof.

$$\mathbb{S}\text{-Fib-Alg}(\mathcal{C}) :\equiv \sum_{A:C\to\mathcal{U}} \sum_{a:A(c)} a =_s^A a.$$

As explained and proved in [10, Thm. 50], given a circle algebra $\mathcal{C} \equiv (C, c, s)$, there are various equivalent ways to state that it behaves like the circle, including[5]:

Homotopy initiality The type of algebra homomorphisms from $\mathcal{C}$ to any other circle algebra $\mathcal{A} \equiv (A, a, p)$ is contractible, where this type of algebra homomorphisms is

[5] The dependent universal property is not discussed in [10], however, it is easily seen to be equivalent to the induction principle.

$$\mathbb{S}\text{-hom}(\mathcal{C},\mathcal{A}) :\equiv \sum_{f:C\to A} \sum_{r:f(c)=a} \mathrm{ap}_f(s) =_r^{\tilde{A}} p, \tag{2.1}$$

where $\tilde{A}(y) :\equiv (y = y)$ for $y : A$. We recall the basics of paths over a path, and the accompanying operations, in Section 3.1 below. (The type $\mathbb{S}\text{-hom}(\mathcal{C},\mathcal{A})$ is equivalent to the type

$$\sum_{f:C\to A} (f(c), \mathrm{ap}_f(s)) = (a, p),$$

where the pairs are regarded as elements of $\sum_{y:A} \tilde{A}(y)$.)

Universal property For any type $A : \mathcal{U}$, the map that evaluates a function $f : C \to A$ at c and s,

$$(C \to A) \to \sum_{a:A} a = a, \qquad f \mapsto (f(c), \mathrm{ap}_f(s)), \tag{2.2}$$

is an equivalence.

Induction principle Any fibered circle algebra $\mathcal{A} \equiv (A, a, p)$ over $\mathcal{C}$ has an algebra section, where the type of algebra sections is

$$\mathbb{S}\text{-sect}(\mathcal{A}) :\equiv \sum_{f:\prod_{z:C} A(z)} \sum_{r:f(c)=a} \mathrm{apd}_f(s) =_r^{\tilde{A}} p, \tag{2.3}$$

where $\tilde{A}(y) :\equiv (y =_s^A y)$ for $y : A(c)$. (Here apd is as defined in [11, 2.3]; the type $\mathbb{S}\text{-sect}(\mathcal{A})$ is equivalent to the type

$$\sum_{f:\prod_{z:C} A(z)} (f(c), \mathrm{apd}_f(s)) = (a, p),$$

where the pairs are regarded as elements of $\sum_{y:A(c)} \tilde{A}(y)$.)

Dependent universal property For any type family $A : C \to \mathcal{U}$, the map that evaluates a function $f : \prod_{z:C} A(z)$ at c and s,

$$\left(\prod_{z:C} A(z)\right) \to \sum_{a:A(c)} a =_s^A a, \qquad f \mapsto (f(c), \mathrm{apd}_f(s)), \tag{2.4}$$

has a section.

From the equivalence of the types encoding the four principles above, it also follows that the type of induction terms for $\mathcal{C}$,

$$\prod_{A:C\to\mathcal{U}} \prod_{a:A(c)} \prod_{p:a=_s^A a} \mathbb{S}\text{-sect}(A, a, p), \tag{2.5}$$

which is equivalent to the type of sections of (2.4) for all families A, is a proposition.

The type of circles, then, is the subtype of $\mathbb{S}$-Alg corresponding to any of these definitions. As in [11, Sec. 9.8], we can prove a structure identity principle for circle algebras and circles, viz., for circle algebras $\mathcal{C} \equiv (C, c, s)$ and $\mathcal{C}' \equiv (C', c', s')$, the canonical function

$$(\mathcal{C} =_{\mathbb{S}\text{-Alg}} \mathcal{C}') \to \sum_{f:C\to C'} \sum_{r:f(c)=c'} (\mathrm{ap}_f(s) =_r^{\tilde{C}'} s') \times \mathrm{isEquiv}(f),$$

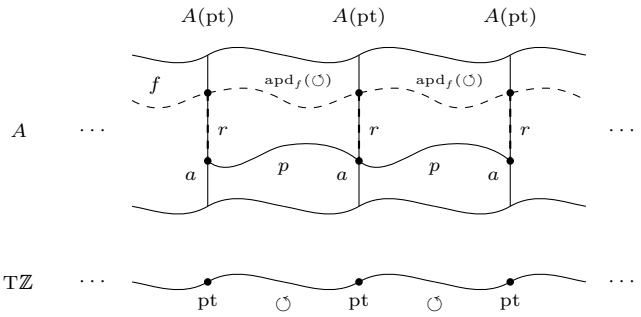

Fig. 1. A visualization of circle induction principle.

where $\tilde{C}'(y) :\equiv (y = y)$ for $y : C'$, is an equivalence. By homotopy initiality for circles, it then follows straightforwardly that the type of circles is a proposition, i.e., independently of whether there are any circles, any two circles are uniquely identifiable.

2.3. $\mathrm{T}\mathbb{Z}$ *is a circle*

With this in hand, we can outline our route to proving that the circle algebra $(\mathrm{T}\mathbb{Z}, \mathrm{pt}, \circlearrowleft)$ is a circle.

As a warm-up, we first prove in Section 4.1 the *recursion principle*, which states that, given a type A, an element a of A and a path $p : a =_A a$, one can construct a function $f : \mathrm{T}\mathbb{Z} \to A$ with a path $r : f(\mathrm{pt}) = a$ such that $\mathrm{ap}_f(\circlearrowleft) =_r^{\tilde{A}} p$, or, equivalently, $\mathrm{ap}_f(\circlearrowleft) = r*(p*r^{-1})$. This construction was formalized by Grayson in 2014, see [21, Circle.v].[6] This however only proves *weak* initiality, or equivalently, only gives a *section* of the evaluation map in (2.2).

In Section 4.2 we then prove the induction principle, in which A is not a type but a type family over $\mathrm{T}\mathbb{Z}$. On the basis of Grayson's construction of the recursion principle, Shulman sketched an approach to the induction principle, see [8]. Independently of this, but also departing from Grayson's proof of the recursion principle, Buchholtz and Bezem found the construction presented in this paper, which has subsequently been formalized by Grayson [21, Circle2.v, Theorem circle_induction] in *UniMath*.

Spelling out the induction principle, we have to construct a function of the following type:

$$\prod_{A:\mathrm{T}\mathbb{Z}\to\mathcal{U}} \prod_{a:A(\mathrm{pt})} \prod_{p:a=^{A}_{\circlearrowleft}a} \sum_{f:\prod_{z:\mathrm{T}\mathbb{Z}} A(z)} \sum_{r:f(\mathrm{pt})=a} \mathrm{apd}_f(\circlearrowleft) =_r^{\tilde{A}} p \tag{2.6}$$

(Recall that $\tilde{A}(y) \equiv (y =^{A}_{\circlearrowleft} y)$ for $y : A(\mathrm{pt})$.)

The type in Eq. (2.6) is illustrated in Fig. 1. We think of $\mathrm{T}\mathbb{Z}$ as a circle (and prove that it is), but we illustrate it (and objects depending on it) as periodically recurring, in order to make clearer diagrams. We draw the type family A as a periodic fibration over this circle, and the goal is then to produce from the point a and the path p over $\circlearrowleft$, the section f, the path r, and a final element inhabiting the type $\mathrm{apd}_f(\circlearrowleft) =_r^{\tilde{A}} p$, which corresponds to filling the inside of the curvilinear quadrilateral in Fig. 1. (This will be made precise in course of the argument below, in terms of compositions of paths over paths.)

Our construction uses the propositional truncation operation $\|\_\|$, as in [11, 6.9], but we do not require that the dependent eliminator witnessing the induction principle of $\|\_\|$ computes judgmentally on the point constructor $|\_| : X \to \|X\|$. In the *UniMath* formalization, propositional truncation is constructed as (the propositional resizing of)

[6] Our construction here uses the same basic idea but manages the computations involved in establishing the induction principle differently.

$$\|X\| :\equiv \prod_{P:\mathrm{Prop}} ((X \to P) \to P), \tag{2.7}$$

where Prop is the type of all propositions (in a chosen universe). Using this construction, the corresponding non-dependent eliminator will compute judgmentally on the point constructor, but the dependent eliminator will not. As we explain below, this has the consequence that in *UniMath*, the non-dependent circle eliminator that we construct for T$\mathbb{Z}$ will then compute judgmentally on pt, but the dependent one will not.

If the underlying type theory has propositional truncation with a dependent eliminator that computes judgmentally on the point constructor, as in [11, 6.9], then our construction for the induction principle in Eq. (2.6) simplifies. Its application to A, a, p of appropriate types is a triple (f, r, q) where f is a section of A and $r : f(\mathrm{pt}) = a$. In this case, $f(\mathrm{pt}) \equiv a$, but in general we won't have $r \equiv \mathrm{refl}_a$. However, the type $\mathrm{apd}_f(\circlearrowleft) =^{\tilde{A}}_{\bar{r}} p$ makes sense for all $\bar{r} : a = a$, and we'll have that $r = \mathrm{refl}_a$, so we may transport q to obtain an element of type $\mathrm{apd}_f(\circlearrowleft) =^{\tilde{A}}_{\mathrm{refl}_a} p$. This type is judgmentally equal to $\mathrm{apd}_f(\circlearrowleft) = p$.

In a type theory where higher inductive types are admitted, one can introduce a circle $\mathbb{S}^1$ as a higher inductive type, as in [11, 6.1], and this will easily be shown to be equivalent to T$\mathbb{Z}$, without relying on the results of our paper. The equivalence can be established by observing that T$\mathbb{Z}$ and $\mathbb{S}^1$ are pointed connected types with loop spaces equivalent to $\mathbb{Z}$. (For the interested reader: apply [11, Lemma 7.6.2] with $n = -2$ to reduce to action on paths. Then use connectedness to strengthen this result from embeddings to equivalences. Finally, again using connectedness, reduce to the loop spaces of the respective points, and show they are equivalent to $\mathbb{Z}$ and thus to each other.) The induction principle Eq. (2.6) for T$\mathbb{Z}$ then follows directly.

The reader may wonder whether our result can be generalized to higher spheres. The answer is no. One can construct models of type theory with univalent universes and propositional resizing (viz., essentially of *UniMath*) that do not have higher inductive types, not even suspensions. We can take any model and restrict the nth universe, $n = 0, 1, \ldots$, to consist of homotopy n-types: the new zeroth universe $\mathcal{U}'_0$ consists of the sets of the old universe $\mathcal{U}_0$, the new universe $\mathcal{U}'_1$ consists of the groupoids of $\mathcal{U}_1$ (hence including $\mathcal{U}'_0$), etc. This construction keeps all the propositions, so it preserves propositional resizing. By our construction, $\mathcal{U}'_1$ will contain a circle T$\mathbb{Z}$, but it cannot contain the 2-sphere (the suspension of the circle), as this is not a groupoid. Because the 2-sphere in topology is not an n-type for any n, the new model will not contain a 2-sphere. The restricted model also shows that one cannot construct a circle in the lowest universe in *UniMath*.

3. Auxiliary results

In this section we present some additional results that are needed in the sequel.

3.1. Identifying elements in members of families of types

All proofs in this subsection are by (nested) induction as indicated in the text, and can moreover be found in [21, PathsOver.v].

Let $A : \mathcal{U}$, $B : A \to \mathcal{U}$, $a_i : A$, $b_i : B(a_i)$ for $i = 1, 2$, and $p : a_1 = a_2$. We are interested in identifications of b_1 and b_2 relative to this data. We cannot in general form the type $b_1 = b_2$ as their types may be different. There are several ways to solve this problem. One of them is to transport b_1 along p and form an identity type in $B(a_2)$. Another way would be to consider identifications $(a_1, b_1) = (a_2, b_2)$ in $\sum_{x:A} B(x)$ and require that the action of the first projection on such identifications is equal to p. These two ways are equivalent. The former way is easier to work with and will be the one we choose here.

Definition 3.1. Let $A : \mathcal{U}$, $B : A \to \mathcal{U}$, $a_i : A$, $b_i : B(a_i)$ for $i = 1, 2$, and $p : a_1 = a_2$. Define the transport function $\mathrm{trp}_{B,p} : B(a_1) \to B(a_2)$ by induction on p, setting $\mathrm{trp}_{B,\mathrm{refl}_{a_1}}(b_1) :\equiv b_1$. This is indeed well-typed

since $B(a_1) \equiv B(a_2)$ in this case. Now define the type $b_1 =^B_p b_2$ as $\mathrm{trp}_{B,p}(b_1) = b_2$. An element of $b_1 =^B_p b_2$ is called a *path* from b_1 to b_2 *over* p. Note that $(b_1 =^B_{\mathrm{refl}_{a_1}} b_2) \equiv (b_1 =_{B(a_1)} b_2)$.

Many of the operations on paths have their counterpart for paths over paths. We define the unit path over a path, composition of paths over paths, and reversal of paths over paths.

Definition 3.2. Let $A : \mathcal{U}$, $B : A \to \mathcal{U}$, $a_i : A$, $b_i : B(a_i)$ for $i = 1, 2, 3$, and $p_i : a_i = a_{i+1}$ for $i = 1, 2$. We define:

(1) *Unit* $\mathrm{refl}_{b_1} : b_1 =^B_{\mathrm{refl}_{a_1}} b_1$;
(2) *Composition of paths over paths* $*_{\mathrm{o}} : b_1 =^B_{p_1} b_2 \to b_2 =^B_{p_2} b_3 \to b_1 =^B_{p_1 * p_2} b_3$, defined by induction first on p_2 and then on $r : b_2 = b_3$, by setting $q *_{\mathrm{o}} \mathrm{refl}_{b_2} :\equiv q$ for all $q : b_1 =^B_{p_1} b_2$;
(3) *Reversal of paths over paths* $(\_)^{-\mathrm{o}} : b_1 =^B_{p_1} b_2 \to b_2 =^B_{(p_1)^{-1}} b_1$, defined by induction first on p_1 and then on $r : b_1 = b_2$, by setting $\mathrm{refl}^{-\mathrm{o}}_{b_1} :\equiv \mathrm{refl}_{b_1}$.

These operations on paths over paths satisfy many of the laws satisfied by the corresponding operations on paths, after some modification. We illustrate the modification required to treat composition. Suppose we have elements $a_i : A$ for $1 \le i \le 4$, paths $p_i : a_i = a_{i+1}$ for $1 \le i \le 3$, elements $b_i : B(a_i)$ for $1 \le i \le 4$, and paths $q_i : b_i =^B_{p_i} b_{i+1}$ over p_i for $1 \le i \le 3$. Then we the following two paths over paths.

$$q_1 *_{\mathrm{o}} (q_2 *_{\mathrm{o}} q_3) : b_1 =^B_{p_1 * (p_2 * p_3)} b_4$$
$$(q_1 *_{\mathrm{o}} q_2) *_{\mathrm{o}} q_3 : b_1 =^B_{(p_1 * p_2) * p_3} b_4$$

Since they are of different types, they cannot be compared directly, but there is an equivalence ε of type $\left(b_1 =^B_{p_1 * (p_2 * p_3)} b_4\right) \simeq \left(b_1 =^B_{(p_1 * p_2) * p_3} b_4\right)$ constructed from the associativity law for paths of type $p_1 * (p_2 * p_3) = (p_1 * p_2) * p_3$. The associativity law for composition of paths over paths is an easily constructed identity of type $\varepsilon(q_1 *_{\mathrm{o}} (q_2 *_{\mathrm{o}} q_3)) = (q_1 *_{\mathrm{o}} q_2) *_{\mathrm{o}} q_3$. For more information we refer the reader to the repositories with formalized proofs [21, Circle2.v].

In the rest of this section we work in a context with $A : \mathcal{U}$, $B : A \to \mathcal{U}$, $a_i : A$, $b_i : B(a_i)$ for $i = 1, 2, 3$, $p_i : a_i = a_{i+1}$ for $i = 1, 2$,

Lemma 3.3. *For every* $q : b_1 =^B_{p_1} b_2$*, the function*

$$q *_{\mathrm{o}} (\_) : (b_2 =^B_{p_2} b_3) \to (b_1 =^B_{p_1 * p_2} b_3)$$

is an equivalence.

The proof is by induction on first p_1, and then q, and finally p_2. Then conclude by reflexivity.

If $p = q$, then we can transport paths over p to paths over q.

Definition 3.4. For every $p, q : a_1 = a_2$ and 2-dimensional path $\alpha : p = q$, transport along α induces an equivalence $\mathrm{cp}_\alpha : (b_1 =^B_p b_2) \simeq (b_1 =^B_q b_2)$. The function cp_α is called *change path*, and is defined by induction on α, setting $\mathrm{cp}_{\mathrm{refl}_p} :\equiv \mathrm{id}_{b_1 =^B_p b_2}$.

Lemma 3.5. *For every* $p, q, r : a_1 = a_2$ *and 2-paths* $\alpha : p = q$*,* $\beta : q = r$*, we have* $\mathrm{cp}_{\alpha * \beta} = \mathrm{cp}_\beta \circ \mathrm{cp}_\alpha$.

The proof is by induction on β (for right-recursive composition).

Lemma 3.6. *For every* $p, q : a_1 = a_2$ *and 2-path* $\alpha : p = q$*, taking* $\alpha^- :\equiv \mathrm{ap}_{(\_)^{-1}}(\alpha)$*, we have* $(\mathrm{cp}_\alpha(\hat{p}))^{-\mathrm{o}} = \mathrm{cp}_{\alpha^-}(\hat{p}^{-\mathrm{o}})$ *for every* $\hat{p} : b_1 =^B_p b_2$.

The proof is by induction on α.

Lemma 3.7. *For every $p : a_1 = a_2$ define $\iota(p) : p^{-1} * p = \mathrm{refl}_{a_2}$ by induction on p, by setting $\iota(\mathrm{refl}_{a_1}) :\equiv \mathrm{refl}_{\mathrm{refl}_{a_1}}$. Then we have $\mathrm{cp}_{\iota(p)}(\hat{p}^{-\mathrm{o}} *_{\mathrm{o}} \hat{p}) = \mathrm{refl}_{b_2}$ for every $\hat{p} : b_1 =^B_p b_2$.*

Lemma 3.8. *For every $p : a_1 = a_2$ define $\gamma(p) : \mathrm{refl}_{a_1} * p = p$ by induction on p, setting $\gamma(\mathrm{refl}_{a_1}) :\equiv \mathrm{refl}_{\mathrm{refl}_{a_1}}$. Then we have $\mathrm{cp}_{\gamma(p)}(\mathrm{refl}_{b_1} *_{\mathrm{o}} \hat{p}) = \hat{p}$ for every $\hat{p} : b_1 =^B_p b_2$.*

The proof is in both cases by induction on first p, and then on $\hat{p}$.

Definition 3.9. For every $p, p' : a_1 = a_2$, $q, q' : a_2 = a_3$ and 2-paths $\alpha : p = p'$, $\beta : q = q'$, define $\mathrm{ap}_*(\alpha, \beta) : (p * q) = (p' * q')$ by induction first on β and then on q, setting $\mathrm{ap}_*(\alpha, \mathrm{refl}_{\mathrm{refl}_{a_2}}) :\equiv \alpha$. (This is well-typed for right-recursive composition.)

Lemma 3.10. *For every $p, p' : a_1 = a_2$, $q, q' : a_2 = a_3$ and 2-paths $\alpha : p = p'$, $\beta : q = q'$, we have $\mathrm{cp}_{\mathrm{ap}_*(\alpha,\beta)}(\hat{p} *_{\mathrm{o}} \hat{q}) = \mathrm{cp}_\alpha(\hat{p}) *_{\mathrm{o}} \mathrm{cp}_\beta(\hat{q})$, for every $\hat{p} : b_1 =^B_p b_2$ and $\hat{q} : b_2 =^B_q b_3$.*

The proof is by induction first on β, then on q, and finally on $\hat{q}$.

3.2. Dependent elimination for propositional truncation

One extra piece of knowledge we need is the *dependent* elimination principle for propositional truncation, mentioned in [11, 6.9], and qualified as 'not really useful'.[7] We use this principle in Lemma 4.2, and it plays an essential role in the proof of the induction principle for T$\mathbb{Z}$.

Recall that we assume the presence of a propositional truncation operation $\|\_\|$ (mapping each universe to the propositions therein) equipped with maps $|\_| : X \to \|X\|$ exhibiting $\|\_\|$ as a reflection into propositions, i.e., for any proposition P, precomposition with $|\_|$ induces an equivalence $(\|X\| \to P) \simeq (X \to P)$. If the inverse map sends $g : X \to P$ to $\bar{g} : \|X\| \to P$ such that $\bar{g}(|x|) \equiv g(x)$ for all $x : X$, then we say the propositional truncation operation satisfies the judgmental computation rule for the non-dependent eliminator (JNE). This can be achieved either by having $\|\_\|$ defined as a higher inductive type or using the impredicative encoding (2.7), as we verify below.

Lemma 3.11. *If A is a type and $B(x)$ is a family of propositions indexed by the elements x of $\|A\|$, and we are given $g : \prod_{a:A} B(|a|)$, then there is a function $f : \prod_{x:\|A\|} B(x)$.*

Proof. The function g induces a function $h : A \to \sum_{x:\|A\|} B(x)$ by setting $h(a) :\equiv (|a|, g(a))$. Since the codomain of h is a proposition, we get an induced map $\|A\| \to \sum_{x:\|A\|} B(x)$, which is automatically a section of $\mathrm{pr}_1 : \sum_{x:\|A\|} B(x) \to \|A\|$. By the equivalence between sections of first projections and dependent functions, we then get the required f. □

Note that the resulting function f automatically satisfies $f(|a|) = g(a)$, for each $a : A$, since each type $B(|a|)$ is a proposition. If we can achieve a judgmental equality here, then we say that the propositional truncation operation satisfies the judgmental computation rule for the dependent eliminator (JDE).

Recall that in *UniMath*, $\|A\| :\equiv \prod_{P:\mathrm{Prop}}((A \to P) \to P)$, and the function $|\_| : A \to \|A\|$ is defined by $|a|(P, f) :\equiv f(a)$ for all $P : \mathrm{Prop}$, $f : A \to P$, and $a : A$. Thus we naturally get a recursion principle: if $P : \mathrm{Prop}$, then any $g : A \to P$ defines an $f : \|A\| \to P$ by setting $f(x) :\equiv x(P, g)$. Clearly f satisfies $f(|a|) \equiv |a|(P, g) \equiv g(a)$, for all $a : A$.

[7] The dependent elimination principle appears to be used later in [11, Lemma 7.3.3], though.

For induction the situation is different: if $B : \|A\| \to \mathrm{Prop}$, then from any $g : \prod_{a:A} B(|a|)$ we can construct a function $f : \prod_{x:\|A\|} B(x)$, as in the proof of Lemma 3.11. Unwinding the proof, there will be a transport involved in converting the section to a dependent function, and we won't have $f(|a|) \equiv g(a)$, as the path of type $|a| = |a|$ coming from the proof that $\|A\|$ is a proposition need not be the path given by reflexivity.

There are several other ways of defining f, but none we are aware of satisfies the computation rule $f(|a|) \equiv g(a)$. It is currently unknown whether it is possible to define in *UniMath* a propositional truncation with an induction principle that satisfies the computation rule.

3.3. The integers

For convenience we give a direct inductive definition of the set of integers, and we give an alternative induction principle in Section 3.4. Thus we get a set of integers $\mathbb{Z}$, a constant $0 : \mathbb{Z}$, and a successor function $s : \mathbb{Z} \to \mathbb{Z}$ that is an equivalence.

Definition 3.12. Let $\mathbb{Z}$ be the inductive type with the following three constructors:
(1) $\mathrm{zero} : \mathbb{Z}$ for the integer number zero, $0 :\equiv \mathrm{zero}$;
(2) $\mathrm{pos} : \mathbb{N} \to \mathbb{Z}$ for positive integers, $1 :\equiv \mathrm{pos}(0), \ldots$;
(3) $\mathrm{neg} : \mathbb{N} \to \mathbb{Z}$ for negative integers, $-1 :\equiv \mathrm{neg}(0), \ldots$.

The *embedding* function $i : \mathbb{N} \to \mathbb{Z}$ is defined by induction, setting $i(0) :\equiv \mathrm{zero}$, $i(S(n)) :\equiv \mathrm{pos}(n)$. Like the type $\mathbb{N}$, the type $\mathbb{Z}$ is a set with decidable equality and ordering relations, and we denote its elements often in the usual way as $\ldots, -1, 0, 1, \ldots$.

One well-known equivalence is *negation* $- : \mathbb{Z} \to \mathbb{Z}$, also called *complement*, inductively defined by setting $-\,\mathrm{zero} :\equiv \mathrm{zero}$, $-\,\mathrm{pos}(n) :\equiv \mathrm{neg}(n)$, $-\,\mathrm{neg}(n) :\equiv \mathrm{pos}(n)$. Negation is its own inverse.

The *successor* function $s : \mathbb{Z} \to \mathbb{Z}$ is defined inductively setting $s(\mathrm{zero}) :\equiv \mathrm{pos}(0)$, $s(\mathrm{pos}(n)) :\equiv \mathrm{pos}(S(n))$, $s(\mathrm{neg}(n)) :\equiv -i(n)$. For example, we have $s(-1) \equiv s(\mathrm{neg}(0)) \equiv -i(0) \equiv \mathrm{zero} \equiv 0$. Denoting the successor function on $\mathbb{N}$ by S, by induction on $n : \mathbb{N}$ one proves $s(i(n)) = i(S(n))$, so that one can say that s extends S on the i-image of $\mathbb{N}$. From now on we will identify $i(n) : \mathbb{Z}$ with n, and $-i(n) : \mathbb{Z}$ with $-n$, for all $n : \mathbb{N}$.

The successor function s is an equivalence. The inverse s^{-1} of s is called the *predecessor* function. We denote the n-fold iteration of s as s^n, and the n-fold iteration of s^{-1} as s^{-n}.

Addition of integers is defined inductively by setting $z + \mathrm{zero} :\equiv z$, $z + \mathrm{pos}(n) :\equiv s^{n+1}(z)$, $z + \mathrm{neg}(n) :\equiv s^{-(n+1)}(z)$. From addition and unary $-$ one can define a binary *substraction* function setting $z - y :\equiv z + (-y)$.

Recall the equivalence $\mathrm{ev}_0 : (\mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}) \to \mathbb{Z}$ from Section 2.1, which sends p to $\mathrm{pr}_1(p)_*(0)$. We have $\mathrm{refl}_{\mathrm{pt}} : \mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}$, as well as the operations of *path reversal* and *path composition* as defined in [11, 2.1]. These satisfy the laws as stated and proved in [11, Lemma 2.1.4], equipping $\mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}$ with a group structure. The equivalence ev_0 maps $\mathrm{refl}_{\mathrm{pt}}$ via $\mathrm{id}_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$ to 0. As explained above, ev_0 maps any $p : \mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}$ via $s^k : \mathbb{Z} \to \mathbb{Z}$ to some $k : \mathbb{Z}$. Since $(s^k)^{-1} = s^{-k}$ and $s^k \circ s^l = s^{k+l}$, ev_0 transports path reversal and path composition to negation and addition, respectively. This means that the entire group structure of $\mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}$ is transported to the usual group structure on $\mathbb{Z}$, including all the proofs of the group laws in $\mathbb{Z}$. (The fact that we do not have to reprove the group laws is one of the benefits of the univalent approach.)

3.4. Some induction principles for the integers

The definition of $\mathbb{Z}$ yields the following induction principle. Given $P : \mathbb{Z} \to \mathcal{U}$, to construct elements $h(z) : P(z)$ for every $z : \mathbb{Z}$, it suffices to give $h(0) : P(0)$ and functions $f : \prod_{n:\mathbb{N}}(P(n) \to P(n+1))$ and $g : \prod_{n:\mathbb{N}}(P(-n) \to P(-n-1))$, as illustrated in Fig. 2.

The function $h : \prod_{z:\mathbb{Z}}(P(z))$ defined in this way satisfies $h(n+1) \equiv f(n, h(n))$ and $h(-n-1) \equiv g(n, h(-n))$ for all $n : \mathbb{N}$.

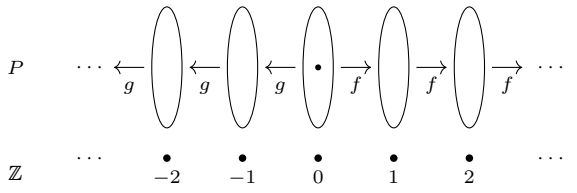

Fig. 2. Asymmetric integer induction principle.

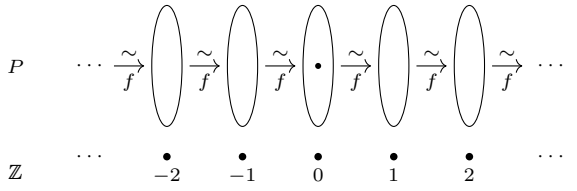

Fig. 3. Symmetric integer induction principle.

It is possible to give a more symmetric, but less general induction principle, if we assume that the functions are equivalences. In that case we can reorient the g's to point in the same direction as the f's, allowing us to combine them into a single family $f : \prod_{z:\mathbb{Z}} P(z) \simeq P(z+1)$ of equivalences, as illustrated in Fig. 3.

We shall need that in this case, giving an element $h : \prod_{z:\mathbb{Z}} P(z)$ together with identities of type $h(z+1) = f_z(h(z))$ for all $z : \mathbb{Z}$ is equivalent to giving the single element $h(0)$. We formulate this precisely as follows.

Theorem 3.13. *Let $P : \mathbb{Z} \to \mathcal{U}$ and $f : \prod_{z:\mathbb{Z}} P(z) \simeq P(z+1)$. The function*

$$\varphi : \left(\sum_{h:\prod_{z:\mathbb{Z}} P(z)} \prod_{z:\mathbb{Z}} h(z+1) = f_z(h(z)) \right) \to P(0)$$

that sends (h, q) to $h(0)$ is an equivalence.

See [21, AffineLine.v, Definition ℤBi-Recursion_weq] for the formalization of the proof, and see [21, AffineLine.v, Definition ℤTorsorRecursion_weq] for the formalization of a version for arbitrary ℤ-torsors.

Proof. We prove that the fiber over any $p : P(0)$ is contractible. We simplify notations a bit by leaving out the types of h and q. The fiber $\sum_{(h,q)} h(0) = p$ consists of triples (h, q, r) with $r : h(0) = p$. By case distinction, h can (equivalently) be split in three parts (h_-, h_0, h_+) with $h_0 : P(0)$, $h_+ : \prod_{n:\mathbb{N}} P(n+1)$, and $h_- : \prod_{n:\mathbb{N}} P(-n-1)$. Since $h(0) = p$ only depends on h_0 the pair (h_0, r) with $r : h_0 = p$ contracts away, so we're left with the type

$$\varphi^{-1}(p) \simeq \psi_+(p) \times \psi_-(p),$$

where $\psi_+(p)$ and $\psi_-(p)$ are defined as follows.

$$\psi_+(p) :\equiv \sum_{h_+:\prod_{n:\mathbb{N}} P(n+1)} \big((h_+(0) = f_0(p)) \times \prod_{n:\mathbb{N}} h_+(n+1) = f_n(h_+(n))\big)$$

$$\psi_-(p) :\equiv \sum_{h_-:\prod_{n:\mathbb{N}} P(-n-1)} \big((h_-(0) = f_{-1}^{-1}(p)) \times \prod_{n:\mathbb{N}} h_-(n+1) = f_{-n-2}^{-1}(h_-(n))\big)$$

The type $\varphi^{-1}(p)$ is contractible, because $\psi_+(p)$ and $\psi_-(p)$ are contractible. They are contractible because each specifies a certain function, namely h_+ or h_-, specifies that this function has a certain value at 0, and

prescribes the value of the function at all successors. Such a specification is unique by the universal property (induction) of $\mathbb{N}$. □

Let us spell out the inverse function produced in the proof. It maps $p : P(0)$ to a pair whose first component is the function that takes $z : \mathbb{Z}$ to $f^z(p) : P(z)$, where

$$\begin{aligned} f^0(p) &\equiv p, \\ f^{n+1}(p) &\equiv f_n(f^n(p)), && \text{for } n : \mathbb{N}, \\ f^{-n-1}(p) &\equiv f_{-n-1}^{-1}(f^{-n}(p)), && \text{for } n : \mathbb{N}. \end{aligned}$$

4. Main results

In this section, pairs (X, f) will be of type $\sum_{X:\mathcal{U}}(X \to X)$. Moreover, nested pairs will be written as tuples. With these notational simplifications, we rephrase some definitions from Section 2.1. The formalization of Section 4.1 can be found in [21, Circle.v], and that of Section 4.2 can be found in [21, Circle2.v].

Definition 4.1. The pointed type of $\mathbb{Z}$-torsors is defined by

$$\begin{aligned} \mathrm{T}\mathbb{Z} &:\equiv \sum_{(X,f)} \|(\mathbb{Z}, s) = (X, f)\|, \\ \mathrm{pt} &:\equiv (\mathbb{Z}, s, |\mathrm{refl}_{(\mathbb{Z},s)}|) : \mathrm{T}\mathbb{Z}. \end{aligned}$$

The variables X, Y, Z will be used for elements of $\mathrm{T}\mathbb{Z}$, as well as, by an abuse of notation, for their the first components. The equivalence ev_0 is defined by

$$\begin{aligned} \mathrm{ev}_0 : (\mathrm{pt} =_{\mathrm{T}\mathbb{Z}} \mathrm{pt}) &\to \mathbb{Z} \\ p &\mapsto \mathrm{pr}_1(p)_*(0). \end{aligned}$$

The loop of $\mathrm{T}\mathbb{Z}$ is defined as $\circlearrowleft :\equiv \mathrm{ev}_0^{-1}(1)$, satisfying $\mathrm{pr}_1(\circlearrowleft)_* = s$.

The type $\mathrm{T}\mathbb{Z}$ is equivalent to the more traditionally defined type of $\mathbb{Z}$-torsors, but is more parsimonious.[8] (Traditionally, a $\mathbb{Z}$-torsor is defined as a nonempty set upon which the group $\mathbb{Z}$ acts freely and transitively.) Another way to think of it is as the type of Cayley diagrams for $\mathbb{Z}$ with respect to the generator 1.

We remark that the pointed type $\mathrm{T}\mathbb{Z}$ is connected, that is, $\|\mathrm{pt} = Z\|$ for all $Z : \mathrm{T}\mathbb{Z}$.

Lemma 4.2. *If $P(Z)$ is a proposition for all $Z : \mathrm{T}\mathbb{Z}$, then $P(\mathrm{pt})$ implies that $P(Z)$ holds for all $Z : \mathrm{T}\mathbb{Z}$.*

Proof. Let $P(Z)$ be a proposition for all $Z : \mathrm{T}\mathbb{Z}$, and assume we have a proof $p : P(\mathrm{pt})$. Let $(X, f, t) : \mathrm{T}\mathbb{Z}$, then $t : \|(\mathbb{Z}, s) = (X, f)\|$. Since $P(X, f, t)$ is a proposition, it suffices by Lemma 3.11 to prove $P(X, f, |e|)$ for all $e : (\mathbb{Z}, s) = (X, f)$. By induction on e we reduce the task to proving $P(\mathbb{Z}, s, |\mathrm{refl}_{(\mathbb{Z},s)}|)$, which is the same as $P(\mathrm{pt})$, so p provides the proof. □

The proof $q : \prod_{Z:\mathrm{T}\mathbb{Z}} P(Z)$ constructed above has the property that $q(\mathrm{pt}) \equiv p$ if the computation rule for the induction principle for propositional truncation holds.

[8] Our formalization, however, uses the traditional definition.

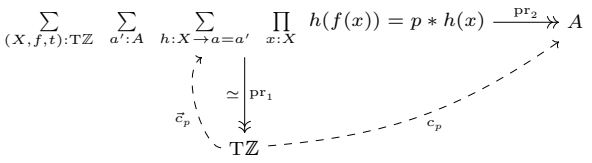

Fig. 4. Mapping torsors to A.

Recall that the aim of this section is to show that $\mathrm{T}\mathbb{Z}$ satisfies the induction principle Eq. (2.6) for the circle. The recursion principle is the non-dependent version of the induction principle, namely that there is a function of the following type:

$$\prod_{A:\mathcal{U}} \prod_{a:A} \prod_{p:a=_A a} \sum_{f:\mathrm{T}\mathbb{Z}\to A} \sum_{r:f(\mathrm{pt})=a} \mathrm{ap}_f(\circlearrowleft) =_r^{\tilde{A}} p. \tag{4.1}$$

Although the same method works to derive both the recursion and the induction principles, we opt to do the recursion principle first, as it is slightly simpler, and prepares the way for the more complicated induction principle.

4.1. Recursion in $\mathrm{T}\mathbb{Z}$

Fix $A : \mathcal{U}$, $a : A$ and $p : a =_A a$. We want to construct a function f from $\mathrm{T}\mathbb{Z}$ to A that maps pt to a, as witnessed by some $r : f(\mathrm{pt}) = a$, such that $\mathrm{ap}_f(\circlearrowleft) =_r^{\tilde{A}} p$. As mentioned in Section 2.3, the last requirement is equivalent to $\mathrm{ap}_f(\circlearrowleft) = r * (p * r^{-1})$. This is because $\mathrm{trp}_{\tilde{A},r^{-1}}(p) = r * (p * r^{-1})$, which in turns follows from the groupoid law $p = \mathrm{refl} * p$ upon induction on r.

All input data is present in p and its type. When defining types and functions depending on the input data, we use p in various denotations to express this dependence.

To be able to apply Lemma 4.2, we need to find a suitable proposition. The idea is to find a correspondence[9] from $\mathrm{T}\mathbb{Z}$ to A whose first projection is an equivalence, thereby yielding a map from $\mathrm{T}\mathbb{Z}$ to A, cf. Fig. 4.

Definition 4.3. For every (X, f), define

$$Q_p(X, f) :\equiv \sum_{a':A} \sum_{h:X\to a=a'} \prod_{x:X} h(f(x)) = p * h(x).$$

Lemma 4.4. *The type $Q_p(X, f)$ is contractible for all $(X, f, t) : \mathrm{T}\mathbb{Z}$.*

Proof. By Lemma 4.2 it suffices to prove that $Q_p(\mathbb{Z}, s)$ is contractible. Note that $Q_p(\mathbb{Z}, s)$ is the total space of the family $R_p : A \to \mathcal{U}$ defined by

$$R_p(a') :\equiv \sum_{h:\mathbb{Z}\to a=a'} \prod_{z:\mathbb{Z}} h(z + 1) = p * h(z).$$

Note furthermore that $\sum_{a':A} a = a'$ is contractible with center (a, refl_a). Thus, to show that $Q_p(\mathbb{Z}, s)$ is contractible, it suffices to define an equivalence

$$\varphi_{a'} : \left(\sum_{h:\mathbb{Z}\to a=a'} \prod_{z:\mathbb{Z}} h(z + 1) = p * h(z) \right) \xrightarrow{\sim} (a = a')$$

[9] A *correspondence* (or *span*) from a type T to a type T' is a type C with projections $\mathrm{pr}_1 : C \to T$ and $\mathrm{pr}_2 : C \to T'$.

for each $a' : A$. The intention is now to invoke Theorem 3.13. Indeed, let us define the constant type family $P_{a'}(z) :\equiv (a = a')$ over $\mathbb{Z}$. Also, define $f_{a'}(z) : P_{a'}(z) \to P_{a'}(z+1)$ by $f_{a'}(z)(q) :\equiv p * q$ for all $z : \mathbb{Z}$ and $q : a = a'$. Then each $f_{a'}(z)$ is an equivalence (with inverse $q \mapsto p^{-1} * q$). Thus, applying Theorem 3.13 shows that $\varphi_{a'}$ is an equivalence, where $\varphi_{a'}(h, q) :\equiv h(0)$. □

A relevant observation at this point is that $Q_p(X, f)$ does not depend on $t : \|(\mathbb{Z}, s) = (X, f)\|$. This means that we actually apply in the proof above the non-dependent version of Lemma 4.2, for which the computation rule holds also in *UniMath*. For $Z \equiv (X, f, t) : \mathrm{T}\mathbb{Z}$, let $\vec{c}_p(Z)$ denote the center of contractibility of $Q_p(X, f)$ as constructed in the proof above. We introduce the notation $(c_p(Z), \tilde{c}_p(Z), \hat{c}_p(Z)) :\equiv \vec{c}_p(Z)$ for its components. The value of $\vec{c}_p(\mathrm{pt})$ can be uncovered by a careful analysis of the steps of the proof. First, the center of $\sum_{a':A} a = a'$ is (a, refl_a). This center is pulled back by φ_a to a center (a, c) of $Q_p(\mathbb{Z}, s)$, where c is the center of $\varphi_a^{-1}(\mathrm{refl}_a)$ coming from the proof that φ_a is an equivalence. The latter proof is the above instance of Theorem 3.13. Unraveling this instance, and using the remark at the end of the proof of Theorem 3.13, tells us that c is a pair (h, q) with $h(z) \equiv p^z$ for all $z : \mathbb{Z}$. Indeed, $\varphi_a(h, q) = h(0) \equiv \mathrm{refl}_a$. Moreover, q has type $\prod_{z:\mathbb{Z}} h(z+1) = p * h(z)$. Wrapping up, $\vec{c}_p(\mathrm{pt}) = (a, h, q)$, with judgmental equality if (JNE) holds.

The analysis in the previous paragraph means we have achieved one of our goals, namely that the function c_p from $\mathrm{T}\mathbb{Z}$ to A maps pt to a, definitionally if (JNE) holds. In any case, let $r :\equiv \tilde{c}_p(\mathrm{pt}, 0)^{-1} : c_p(\mathrm{pt}) = a$, which reduces under (JNE) to refl_a. We will now deal with the other goal, namely that c_p acting on $\circlearrowleft$ yields $r * (p * r^{-1})$.

Lemma 4.5. *For all $X, Y : \mathrm{T}\mathbb{Z}$, $e : X = Y$ and $x : X$ we have $\mathrm{ap}_{c_p}(e) = \tilde{c}_p(X, x)^{-1} * \tilde{c}_p(Y, \tilde{e}(x))$, where $\tilde{e} :\equiv \mathrm{pr}_1(e)_* : X \to Y$.*

Proof. By using induction on e we only have to check the case where $X \equiv Y$ and $e \equiv \mathrm{refl}_X$. In this case $\mathrm{ap}_{c_p}(e)$ is $\mathrm{refl}_{c_p(X)}$. On the right-hand side we get $\tilde{e}(x) \equiv x$, and hence this side simplifies to a reflexivity path of the correct type, as $\tilde{c}_p(X, x)$ has type $a = c_p(X)$. □

We apply the above lemma with $X \equiv Y \equiv \mathrm{pt}$ and $e \equiv \circlearrowleft : \mathrm{pt} = \mathrm{pt}$. Then we have $\tilde{e}(z) = s(z) = z + 1$. Note that $\hat{c}_p(\mathrm{pt}, 0) : \tilde{c}_p(\mathrm{pt}, 1) = p * \tilde{c}_p(\mathrm{pt}, 0)$. Hence, taking $z :\equiv 0$ in Lemma 4.5, it follows that

$$\mathrm{ap}_{c_p}(\circlearrowleft) = \tilde{c}_p(\mathrm{pt}, 0)^{-1} * \tilde{c}_p(\mathrm{pt}, 1) = r * (p * r^{-1}).$$

This means we have achieved our second goal as well, and we've produced an element of the type (4.1).

4.2. Induction in $\mathrm{T}\mathbb{Z}$

Fix $A : \mathrm{T}\mathbb{Z} \to \mathcal{U}$, $a : A(\mathrm{pt})$, and $p : a =^A_{\circlearrowleft} a$. On the basis of this input data, we will construct a function f of type $\prod_{Z:\mathrm{T}\mathbb{Z}} A(Z)$ that maps pt to a, as witnessed by some $r : f(\mathrm{pt}) = a$, such that $\mathrm{apd}_f(\circlearrowleft) =^{\tilde{A}}_r p$. We follow the pattern of the non-dependent case in Section 4.1, but keep in mind that A is now not constant and p is a *path over a path*. We make extensive use of the functions and lemmas from Section 3.1.

The following lemma follows from the fact that $\mathbb{Z}$ is a set and $s : \mathbb{Z} \to \mathbb{Z}$ is an equivalence.

Lemma 4.6. *Suppose $q : (\mathbb{Z}, s) = (X, f)$. Then X is a set and $f : X \to X$ is an equivalence. Morever, with $\tilde{q} :\equiv \mathrm{pr}_1(q)_*$ the equivalence induced by q, we have $f^n(x) = (\tilde{q} \circ s^n \circ \tilde{q}^{-1})(x) = \tilde{q}(\tilde{q}^{-1}(x) + n)$, for all $n : \mathbb{Z}$ and $x : X$.*

Note that for fixed $x : X$ the expression $\tilde{q}^{-1}(x) + n$ can be seen as the function shifting $n : \mathbb{Z}$ by $\tilde{q}^{-1}(x)$ positions, indeed an equivalence. Hence $f^n(x)$ as a function of n is an equivalence from $\mathbb{Z}$ to X. Recall that we may denote $f^n(x)$ by $n + x$, as X is a $\mathbb{Z}$-torsor via f.

Definition 4.7. For every $Z :\equiv (X, f, t) : \mathrm{T}\mathbb{Z}$ and $x : X$, define $s^Z_x : \mathrm{pt} =_{\mathrm{T}\mathbb{Z}} Z$ by the equivalence $e_x(n) :\equiv f^n(x)$ using the univalence axiom. Indeed, $f \circ e_x = e_x \circ s$, as both functions map n to $f^{n+1}(x)$.

Applying Theorem 3.13, we will need two auxiliary results about the paths s^{pt}_x, one for $x = 0$ and the other for the (symmetric) induction step. In Definition 4.7, if $Z \equiv \mathrm{pt}$ and $x = 0$, we get $e_0 = \mathrm{id}$. Applying the univalence axiom gives thus the first result.

Lemma 4.8. *There is a path* $\gamma_0 : \mathrm{refl}_{\mathrm{pt}} = s^{\mathrm{pt}}_0$.

For the second result, note that prefixing s^Z_x by $\circlearrowleft$ amounts to precomposing the equivalence e_x with s. We have $(e_x \circ s)(n) = e_x(n+1) = f^{n+1}(x) = f^n(f(x)) = e_{f(x)}(n)$, so $e_x \circ s = e_{1+x}$. Applying the univalence axiom we get:

Lemma 4.9. *For every* $Z :\equiv (X, f, t) : \mathrm{T}\mathbb{Z}$ *and* $x : X$, *we have a path* $\delta^Z_x : \circlearrowleft * s^Z_x = s^Z_{1+x}$.

Now we are ready to derive the induction principle using the same technique as for the recursion principle. We reuse notations as much as possible, but take care that all types are different.

Definition 4.10. For every $Z :\equiv (X, f, t) : \mathrm{T}\mathbb{Z}$, define

$$Q_p(Z) :\equiv \sum_{a' : A(Z)} \sum_{h : \prod_{x:X} a =^A_{s^Z_x} a'} \prod_{x:X} h(f(x)) = \mathrm{cp}_{\delta^Z_x}(p *_{\mathrm{o}} h(x)),$$

where δ^Z_x comes from Lemma 4.9.

Note that, unlike the Q_p from Definition 4.3, this version depends crucially on the t-component of Z through both s^Z and δ^Z.

Lemma 4.11. *For every* $Z : \mathrm{T}\mathbb{Z}$, *the type* $Q_p(Z)$ *is contractible.*

Proof. By Lemma 4.2 it suffices to prove that $Q_p(\mathrm{pt})$ is contractible. We have $Q_p(\mathrm{pt}) \equiv \sum_{a' : A(\mathrm{pt})} R(a')$ for $R : A(\mathrm{pt}) \to \mathcal{U}$ defined by

$$R_p(a') :\equiv \sum_{h : \prod_{z:\mathbb{Z}} a =^A_{s^{\mathrm{pt}}_z} a'} \prod_{z:\mathbb{Z}} h(z+1) = \mathrm{cp}_{\delta^{\mathrm{pt}}_z}(p *_{\mathrm{o}} h(z)).$$

We show that $\sum_{a' : A(\mathrm{pt})}(a =^A_{s^{\mathrm{pt}}_0} a')$ is contractible. Let refl_a be the reflexivity path at a over $\mathrm{refl}_{\mathrm{pt}}$. Note that $\sum_{a' : A(\mathrm{pt})}(a =^A_{\mathrm{refl}_{\mathrm{pt}}} a') \equiv \sum_{a' : A(\mathrm{pt})}(a = a')$ is contractible with center (a, refl_a). By Lemma 4.8 $\sum_{a' : A(\mathrm{pt})}(a =^A_{s^{\mathrm{pt}}_0} a')$ is contractible with center $(a, \mathrm{cp}_{\gamma_0}(\mathrm{refl}_a))$.

Thus, to show that $Q_p(\mathrm{pt})$ is contractible, it suffices to define an equivalence

$$\varphi_{a'} : R_p(a') \xrightarrow{\sim} (a =^A_{s^{\mathrm{pt}}_0} a')$$

for each $a' : A(\mathrm{pt})$. We again invoke Theorem 3.13, this time with the family $P_{a'} : \mathbb{Z} \to \mathcal{U}$ given by $P_{a'}(z) :\equiv (a =^A_{s^{\mathrm{pt}}_z} a')$ and the equivalences $f_{a'} : \prod_{z:\mathbb{Z}} P_{a'}(z) \simeq P_{a'}(z+1)$ given by $f_{a'}(z) :\equiv \mathrm{cp}_{\delta^{\mathrm{pt}}_z}(p *_{\mathrm{o}} (\_))$. Thus, applying Theorem 3.13 shows that $\varphi_{a'}$ is an equivalence, where $\varphi_{a'}(h, q) :\equiv h(0)$. □

To simplify notations, we will now use variables $X, Y : \mathrm{T}\mathbb{Z}$, and also write $X, Y : \mathcal{U}$ for the underlying types.

Let $\vec{c}_p(X)$ denote the center of contraction of $Q_p(X)$ for $X : \mathrm{T}\mathbb{Z}$. Again, we write $(c_p(X), \tilde{c}_p(X), \hat{c}_p(X)) :\equiv \vec{c}_p(X)$ for the components, where

$$\begin{aligned} c_p &: \prod_{X:\mathrm{T}\mathbb{Z}} A(X), \\ \tilde{c}_p &: \prod_{X:\mathrm{T}\mathbb{Z}} \prod_{x:X} a =^A_{s^X_x} c_p(X), \\ \hat{c}_p &: \prod_{X:\mathrm{T}\mathbb{Z}} \prod_{x:X} \tilde{c}_p(X, 1+x) = \mathrm{cp}_{\delta^X_x}(p *_{\mathrm{o}} \tilde{c}_p(X, x)). \end{aligned}$$

In particular, $q :\equiv \tilde{c}_p(\mathrm{pt}, 0) : a =^A_{s^{\mathrm{pt}}_0} c_p(\mathrm{pt})$, so we can define $r :\equiv \mathrm{cp}_{(\gamma_0^{-1})^-}(q^{-\mathrm{o}}) : c_p(\mathrm{pt}) = a$ (recall Lemma 3.6).

We now proceed to establish that $\mathrm{apd}_{c_p}(\circlearrowleft) =^{\tilde{A}}_r p$. Again we work be elaborating $\mathrm{apd}_{c_p}(\circlearrowleft)$.

Lemma 4.12. *For all $X, Y : \mathrm{T}\mathbb{Z}$, $e : X = Y$ and $x : X$ we have a path $\varepsilon_{e,x} : (s^X_x)^{-1} * s^Y_{\tilde{e}(x)} = e$, where $\tilde{e} :\equiv \mathrm{pr}_1(e)_* : X \to Y$.*

Proof. By induction on e it suffices to give $\varepsilon_{\mathrm{refl}_X,x} : (s^X_x)^{-1} * s^X_x = \mathrm{refl}_X$, since $\mathrm{pr}_1(\mathrm{refl}_X)_*(x) \equiv x$. Hence we set $\varepsilon_{\mathrm{refl}_X,x} :\equiv \iota(s^X_x)$, with ι as in Lemma 3.7. □

Lemma 4.13. *For all $X, Y : \mathrm{T}\mathbb{Z}$, $e : X = Y$ and $x : X$ we have $\mathrm{apd}_{c_p}(e) = \mathrm{cp}_{\varepsilon_{e,x}}(\tilde{c}_p(X, x)^{-\mathrm{o}} *_{\mathrm{o}} \tilde{c}_p(Y, \tilde{e}(x)))$, where $\tilde{e}$ is as above.*

Proof. Induction on e reduces the proof to the case $e \equiv \mathrm{refl}_X : X = X$, which follows from Lemma 3.7 and Lemma 4.12. It remains to check that the general statement of the lemma is well-typed. We have the following paths over paths.

$$\begin{aligned} \mathrm{apd}_{c_p}(e) &: c_p(X) =^A_e c_p(Y) \\ \tilde{c}_p(Y, \tilde{e}(x)) &: a =^A_{s^Y_{\tilde{e}(x)}} c_p(Y) \\ \tilde{c}_p(X, x)^{-\mathrm{o}} &: c_p(X) =^A_{(s^X_x)^{-1}} a \\ \tilde{c}_p(X, x)^{-\mathrm{o}} *_{\mathrm{o}} c_p(Y, \tilde{e}(x)) &: c_p(X) =^A_{(s^X_x)^{-1} * s^Y_{\tilde{e}(x)}} c_p(Y) \end{aligned}$$

In order to make ends meet between the first and the fourth typing we invoke Lemma 4.12 and Definition 3.4. □

We're now ready to calculate $\mathrm{apd}_{c_p}(\circlearrowleft)$. A great simplification is obtained by using that $\mathrm{T}\mathbb{Z}$ is a groupoid: all 2-paths having the same endpoints are equal. Hence the functions cp_α only depend on the path-type of α. Also, as $\mathrm{cp}_{\mathrm{refl}}$ is the identity, so is any cp_α when the endpoints of α are definitionally equal. We make extensive use of this simplification.

Abbreviate $s_0 :\equiv s^{\mathrm{pt}}_0$, $s_1 :\equiv s^{\mathrm{pt}}_1$, then $\varepsilon_{\circlearrowleft,0} : s_0^{-1} * s_1 = \circlearrowleft$. We split the latter identity in a sequence of identities:

$$s_0^{-1} * s_1 \overset{\alpha}{=} \mathrm{refl}_{\mathrm{pt}} *(\circlearrowleft * s_0) \overset{\beta}{=} \mathrm{refl}_{\mathrm{pt}} *(\circlearrowleft * \mathrm{refl}_{\mathrm{pt}}) \overset{\gamma}{=} \circlearrowleft$$

Here $\alpha :\equiv \mathrm{ap}_*((\gamma_0^{-1})^-, \delta_0^{-1})$ and $\beta :\equiv \mathrm{ap}_*(\mathrm{refl}_{\mathrm{refl}_{\mathrm{pt}}}, \mathrm{ap}_*(\mathrm{refl}_\circlearrowleft, \gamma_0^{-1}))$ are constructed with ap_* so as to enable the application of Lemma 3.10. Also, for γ we may take $\gamma(\circlearrowleft)$ from Lemma 3.8. We now calculate, recalling that $r \equiv \mathrm{cp}_{(\gamma_0^{-1})^-}(q^{-\mathrm{o}})$ and $q \equiv \tilde{c}_p(\mathrm{pt}, 0)$:

$$\begin{aligned}
\mathrm{apd}_{c_p}(\circlearrowleft) &= \mathrm{cp}_{\varepsilon_{\circlearrowleft,0}}\big(\tilde{c}_p(\mathrm{pt},0)^{-\mathrm{o}} *_{\mathrm{o}} \tilde{c}_p(\mathrm{pt},1)\big)\\
&= \mathrm{cp}_{\alpha*\beta*\gamma}\big(q^{-\mathrm{o}} *_{\mathrm{o}} \mathrm{cp}_{\delta_0}(p *_{\mathrm{o}} q)\big)\\
&= \mathrm{cp}_{\gamma}\Big(\mathrm{cp}_{\beta}\Big(\mathrm{cp}_{\alpha}\big(q^{-\mathrm{o}} *_{\mathrm{o}} \mathrm{cp}_{\delta_0}(p *_{\mathrm{o}} q)\big)\Big)\Big)\\
&= \mathrm{cp}_{\gamma}\Big(\mathrm{cp}_{\beta}\Big(r *_{\mathrm{o}} \mathrm{cp}_{\delta_0^{-1}}\big(\mathrm{cp}_{\delta_0}(p *_{\mathrm{o}} q)\big)\Big)\Big)\\
&= \mathrm{cp}_{\gamma}\Big(\mathrm{cp}_{\beta}\big(r *_{\mathrm{o}} (p *_{\mathrm{o}} q)\big)\Big)\\
&= \mathrm{cp}_{\gamma}\Big(r *_{\mathrm{o}} \big(p *_{\mathrm{o}} \mathrm{cp}_{\gamma_0^{-1}}(q)\big)\Big)\\
&= \mathrm{cp}_{\gamma}\Big(r *_{\mathrm{o}} \big(p *_{\mathrm{o}} r^{-1}\big)\Big)
\end{aligned}$$

To conclude that $\mathrm{apd}_{c_p}(\circlearrowleft) =_r^{\tilde{A}} p$, we only need a final auxiliary lemma that describes what happens when we transport p backwards along r in the family $\tilde{A}$.

Lemma 4.14. *For any $X : \mathcal{U}$, $B : X \to \mathcal{U}$, $x : X$, $b, c : B(x)$, $s : x = x$, $r : b =^B_{\mathrm{refl}_x} c$, and $q : c =^B_s c$ we have*

$$\mathrm{trp}_{\tilde{B},r^{-1}}(q) = \mathrm{cp}_{\gamma(s)}(r *_{\mathrm{o}} (q *_{\mathrm{o}} r^{-1})),$$

where $\tilde{B}(y) :\equiv (y =^B_s y)$ for $y : B(x)$, and $\gamma(s)$ is as in Lemma 3.8.

The proof is by induction on r, followed by an appeal to Lemma 3.8.

If (JDE), and not just (JNE), holds, then we see that $c_p(\mathrm{pt}) \equiv a$, and $r = \mathrm{refl}_a$, since $\vec{c}_P(\mathrm{pt})$ reduces to $\varphi_a^{-1}(a, \mathrm{cp}_{\gamma_0}(\mathrm{refl}_a))$, which is a triple (a, h, q), where $h(0) = \mathrm{cp}_{\gamma_0}(\mathrm{refl}_a)$.

5. Interpretation in higher toposes

Voevodsky's pioneering work [4] constructed interpretations of the rules of univalent foundations (but not the entire formal system [15]) in the Quillen model category of simplicial sets, which is a presentation of the fundamental $(\infty, 1)$-topos of ∞-groupoids. After a decade of further work, this interpretation has now been extended to include a class of model categories presenting all $(\infty, 1)$-toposes by Shulman [7], and made into an interpretation of the entire formal system by Brunerie, de Boer, Lumsdaine, and Mörtberg [2]. Thus, we can now say conclusively that the result of our paper yields a theorem about all $(\infty, 1)$-toposes.

However, this theorem requires a bit of unpacking to make it look familiar to higher topos theorists. In particular, since all $(\infty, 1)$-toposes are cocomplete, the more usual way to define an internal "circle object" in such a topos would be as a (homotopy) colimit: specifically, the coequalizer of two copies of the identity map of the terminal object (corresponding to the presentation of a circle as a cell complex with one 0-cell and one 1-cell). The natural theorem to expect would then be that *this* circle object is a classifier for $\mathbb{Z}$-torsors.

One way to obtain such a result from our theorem would be to observe that according to the interpretation of higher inductive types in higher toposes constructed by [5], the higher inductive $\mathbb{S}^1$ is a presentation of the above homotopy colimit. Since we have shown that our $\mathrm{T}\mathbb{Z}$ has the same induction principle that $\mathbb{S}^1$ has by definition, they must be equivalent. Thus, since our $\mathrm{T}\mathbb{Z}$ classifies $\mathbb{Z}$-torsors by construction, so does $\mathbb{S}^1$ and hence so does the circle object.

However, a more direct approach is also possible, which avoids discussing higher inductive types at all[10]: we can use our theorem to show that the interpretation of T$\mathbb{Z}$ in an $(\infty,1)$-topos has the universal property of the homotopy colimit that defines a circle object. It will then follow that since it classifies $\mathbb{Z}$-torsors, so does any other such homotopy colimit.

Theorem 5.1. *In any $(\infty,1)$-topos $\mathscr{E}$, there is a coequalizer diagram $1 \rightrightarrows 1 \to \mathrm{T}\mathbb{Z}$.*

Proof. Half of the proof takes place inside of type theory and the other half in a model category. However, the first half has already been done by Sojakova [10], as mentioned in Section 2.2. Her main theorem [10, Theorem 50] then implies that if a circle algebra $\mathcal{C} \equiv (C, c, s)$ satisfies the induction principle, then it is *homotopy-initial* in that for any other circle algebra $\mathcal{A}(A, a, p)$ the type of circle algebra homomorphisms (2.1) is contractible, i.e., there is an element of the type

$$\prod_{\mathcal{A}:\mathbb{S}\text{-Alg}} \mathrm{isContr}\big(\mathbb{S}\text{-hom}(\mathcal{C},\mathcal{A})\big).$$

It follows that our T$\mathbb{Z}$ is homotopy-initial in this sense.

For the second half of the proof, suppose we have a Quillen model category $\mathcal{E}$ that presents our $(\infty,1)$-topos $\mathscr{E}$. We must show that for any object A of $\mathscr{E}$, the diagram of hom-spaces (∞-groupoids)

$$\mathscr{E}(\mathrm{T}\mathbb{Z}, A) \to \mathscr{E}(1, A) \rightrightarrows \mathscr{E}(1, A)$$

is a homotopy equalizer, i.e., that the map from $\mathscr{E}(\mathrm{T}\mathbb{Z}, A)$ to the homotopy equalizer of two copies of the identity map of $\mathscr{E}(1, A)$ is an equivalence. It suffices to show that the homotopy fiber of this map over any point is contractible, which is to say that given any point $a : 1 \to A$ and homotopy $p : a \sim a$, the space of maps $f : \mathrm{T}\mathbb{Z} \to A$ equipped with a homotopy $r : h(\mathrm{pt}) \sim a$ and a higher homotopy $h(\circlearrowleft) * r \sim r * p$ is contractible.

Now, homotopies in the $(\infty,1)$-category $\mathscr{E}$ can always be presented by *right homotopies* in the model category $\mathcal{E}$, meaning maps into a path object. Thus, our object A of $\mathscr{E}$ with a and p can be presented by an object of $\mathcal{E}$, which we also denote A, with a point $a : 1 \to A$ in $\mathcal{E}$ and a right homotopy $p : 1 \to PA_{(a,a)}$, where PA is the path object of A and $PA_{(a,a)}$ is its pullback along $(a, a) : 1 \to A \times A$. Since path objects supply the interpretation of identity types, this corresponds to a type A with an element $a : A$ and path $p : a =_A a$, i.e., a circle algebra. By a similar argument, the homotopy fiber that we want to prove contractible is equivalent to the hom-space $\mathscr{E}(1, H_{\mathrm{T}\mathbb{Z},A})$. Thus, it suffices to observe that if B is an object with a point $1 \to \mathrm{isContr}(B)$, then B is equivalent to the terminal object (a detailed proof can be found in [9, Lemma 4.1]). □

We should also explain more carefully why our T$\mathbb{Z}$ "classifies $\mathbb{Z}$-torsors" in the $(\infty,1)$-categorical sense. Importantly, the relevant notion of "$\mathbb{Z}$-torsor" is the "local" topos- and sheaf-theoretic one: an object X of a slice $(\infty,1)$-topos $\mathscr{E}/A$ is a *$\mathbb{Z}$-torsor* if and only if there is an effective epimorphism[11] $p : B \twoheadrightarrow A$ such that p^*X is isomorphic over B to $\mathbb{Z} \times B$.

Theorem 5.2. *For any object A of an $(\infty,1)$-topos $\mathscr{E}$, the hom-space $\mathscr{E}(A, \mathrm{T}\mathbb{Z})$ is naturally equivalent to the ∞-groupoid of $\mathbb{Z}$-torsors in $\mathscr{E}/A$.*

[10] As of this writing, higher inductive types are not yet included in the work of [2]. Also the models of universes in [7] are not yet known to be closed under parametrized higher inductive types, although this is not a problem in our situation since $\mathbb{S}^1$ is not parametrized.

[11] An *effective epimorphism* is a morphism that is the quotient of its kernel. In an $(\infty,1)$-topos the relevant "kernels" are simplicial objects; see [6, Section 6.2.3].

Proof. Recall that $\mathrm{T}\mathbb{Z}$ is defined as $\sum_{X:\mathcal{U}} \sum_{f:X\to X} \|(\mathbb{Z}, s) = (X, f)\|$, so that it comes with a sequence of projections

$$\mathrm{T}\mathbb{Z} \longrightarrow \Big(\sum_{X:\mathcal{U}} (X \to X)\Big) \longrightarrow \mathcal{U}.$$

We will start by characterizing what $\mathcal{U}$ classifies, then $\sum_{X:\mathcal{U}}(X \to X)$, then finally $\mathrm{T}\mathbb{Z}$.

For the first, the univalence axiom implies that $\mathcal{U}$ is an object classifier, in the sense that $\mathscr{E}(A,\mathcal{U})$ is naturally equivalent, by pullback of the canonical map $\mathcal{U}_* \to \mathcal{U}$, to a full sub-$\infty$-groupoid of the core of $\mathscr{E}/A$ (the fiberwise "small" objects). This means that for any $f, g : A \to \mathcal{U}$, the induced map from the space of homotopies $f \sim g$ to the space of equivalences $f^*\mathcal{U}_* \simeq g^*\mathcal{U}_*$ in $\mathscr{E}/A$ is an equivalence. This holds because the former is the space of lifts of $(f, g) : A \to \mathcal{U}\times\mathcal{U}$ to the path-object $P\mathcal{U}$, while the latter is (e.g., by [9, Lemma 4.3]) the space of sections of $\mathrm{Equiv}_A(f^*\mathcal{U}_*, g^*\mathcal{U}_*)$, or equivalently the lifts of (f, g) to $\mathrm{Equiv}_{\mathcal{U}\times\mathcal{U}}(\pi_1^*\mathcal{U}_*, \pi_2^*\mathcal{U}_*)$, and the univalence axiom says precisely that $P\mathcal{U}$ is equivalent to $\mathrm{Equiv}_{\mathcal{U}\times\mathcal{U}}(\pi_1^*\mathcal{U}_*, \pi_2^*\mathcal{U}_*)$ over $\mathcal{U}\times\mathcal{U}$.

Secondly, $\sum_{X:\mathcal{U}}(X \to X)$ is the exponential in $\mathscr{E}/\mathcal{U}$ of $\mathcal{U}_*$ by itself. Thus, by the pullback-stability and universal property of exponentials, the space of lifts of $f : A \to \mathcal{U}$ to $\sum_{X:\mathcal{U}}(X \to X)$ is equivalent to the space of endomorphisms of the corresponding object $f^*\mathcal{U}_*$ of $\mathscr{E}/A$. Hence $\sum_{X:\mathcal{U}}(X \to X)$ classifies small objects equipped with an endomorphism, in that $\mathscr{E}(A, \sum_{X:\mathcal{U}}(X \to X))$ is naturally equivalent to the ∞-groupoid of small objects of $\mathscr{E}/A$ with an endomorphism.

Thirdly, for $\mathrm{T}\mathbb{Z}$ we need to consider the topos-theoretic interpretation of propositional truncation. We can ignore its particular construction in *UniMath* and focus on its universal property, which says that it is a reflection into propositions, i.e., for any proposition P we have $(\|X\| \to P) \simeq (X \to P)$. Interpreted fiberwise in an $(\infty, 1)$-topos, this says that if we represent a morphism $X \to A$ as the first projection from a dependent sum, $(\sum_{a:A} X(a)) \to A$, then the corresponding projection $(\sum_{a:A} \|X(a)\|) \to A$ is its reflection into the sub-$(\infty, 1)$-category of $\mathscr{E}/A$ consisting of the monomorphisms, i.e., maps $P \to A$ whose diagonal $P \to P \times_A P$ is an equivalence. By [6, Example 5.2.8.16 and Corollary 6.5.1.14] (in the case $n = -1$), the effective epimorphisms and monomorphisms in an $(\infty, 1)$-topos form a factorization system, and hence in particular the map $X \to (\sum_{a:A} \|X(a)\|)$ is an effective epimorphism.

Now by the definition of $\mathrm{T}\mathbb{Z}$, we have an (effective epimorphism, monomorphism) factorization $W \twoheadrightarrow \mathrm{T}\mathbb{Z} \rightarrowtail \sum_{X:\mathcal{U}}(X \to X)$, where $W = \sum_{(X,f)}(\mathbb{Z}, s) = (X, f)$ is (by arguments like those above) a classifier for small objects X equipped with an endomorphism f and a *specified* equivalence to $\mathbb{Z}$ respecting the endomorphisms. In particular, when the universal object-with-endomorphism over $\sum_{X:\mathcal{U}}(X \to X)$ is pulled back to $\mathrm{T}\mathbb{Z}$, then there exists an effective epimorphism onto $\mathrm{T}\mathbb{Z}$ (namely $W \to \mathrm{T}\mathbb{Z}$) such that when it is pulled back further along that morphism it becomes equivalent to $(\mathbb{Z}, s)$. Thus, this universal object is a $\mathbb{Z}$-torsor, and hence so is any pullback of it.

Conversely, suppose (X, f) is a $\mathbb{Z}$-torsor in $\mathscr{E}/A$, so there is an effective epimorphism $p : B \twoheadrightarrow A$ such that $p^*(X, f)$ is equivalent to $(\mathbb{Z}, s)$. Since $\mathbb{Z}$ is a small object, this implies that X has small fibers, hence is classified by some map $A \to \mathcal{U}$. Moreover, the assumption implies that when the classifying map $A \to \sum_{X:\mathcal{U}}(X \to X)$ is composed with p, it lifts to W; so we have the following diagram:

$$\begin{array}{ccc} B & \longrightarrow & W \\ \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow \\ & & \mathrm{T}\mathbb{Z} \\ & & \downarrow \\ A & \longrightarrow & \sum_{X:\mathcal{U}}(X \to X) \end{array}$$

Thus, since effective epimorphisms and monomorphisms form a factorization system, there is an essentially unique lift $A \to \mathrm{T}\mathbb{Z}$. So we have shown that an object-with-endomorphism is a $\mathbb{Z}$-torsor precisely when its

classifying map $A \to \sum_{X:\mathcal{U}}(X \to X)$ lifts to $\mathrm{T}\mathbb{Z}$. Since $\mathrm{T}\mathbb{Z} \to \sum_{X:\mathcal{U}}(X \to X)$ is a monomorphism, this means that $\mathrm{T}\mathbb{Z}$ classifies $\mathbb{Z}$-torsors. □

Combining Theorems 5.1 and 5.2, we see that any circle object in an $(\infty, 1)$-topos is equivalent to $\mathrm{T}\mathbb{Z}$ and hence classifies $\mathbb{Z}$-torsors.

6. Conclusion and future research

We have proved, for any type family $A \to \mathrm{T}\mathbb{Z}$, the induction principle of the circle for $\mathrm{T}\mathbb{Z}$:

$$\mathrm{ind}_A : \sum_{a:A(\mathrm{pt})} (a =^A_{\circlearrowleft} a) \quad \to \quad \prod_{Z:\mathrm{T}\mathbb{Z}} A(Z),$$

with ind_A mapping (a, p) to c_p satisfying $c_p(\mathrm{pt}) \equiv a$ and $\mathrm{apd}_{c_p}(\circlearrowleft) = p$.

It would be interesting to see whether our method can be generalized from $\mathrm{T}\mathbb{Z}$ to the type BG of G-torsors, where G is a free group with a set of generators, S, with decidable equality. Explicitly, we expect that it is possible in our setting to prove that BG satisfies the induction principle for a higher inductive type with a point constructor $\mathrm{pt} : BG$ and a path constructor $\circlearrowleft\_ : S \to (\mathrm{pt} =_{BG} \mathrm{pt})$,

$$\prod_{A:BG\to\mathcal{U}} \prod_{a:A(\mathrm{pt})} \prod_{p:\prod_{s:S} a=^A_{\circlearrowleft_s} a} \sum_{f:\prod_{z:BG} A(z)} \sum_{r:f(\mathrm{pt})=a} \prod_{s:S} \mathrm{apd}_f(\circlearrowleft_s) =^{\tilde{A}_s}_r p_s,$$

where $\tilde{A}_s(y) :\equiv (y =^A_{\circlearrowleft_s} y)$ for $y : A(\mathrm{pt})$.

Acknowledgements

Bezem, Buchholtz, and Grayson acknowledge the support of the Centre for Advanced Study (CAS) at the Norwegian Academy of Science and Letters in Oslo, Norway, which funded and hosted the research project Homotopy Type Theory and Univalent Foundations during the academic year 2018/19. Grayson also acknowledges the support of the Air Force Office of Scientific Research, through a grant to Carnegie Mellon University. Shulman was supported by The United States Air Force Research Laboratory under agreement number FA9550-15-1-0053. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the United States Air Force Research Laboratory, the U.S. Government, or Carnegie Mellon University.

References

[1] Guillaume Brunerie, Menno de Boer, Peter LeFanu Lumsdaine, Anders Mortberg, Initiality for Martin-Löf type theory, A formalization in Agda of the proof, https://github.com/guillaumebrunerie/initiality, 2020.
[2] Guillaume Brunerie, Menno de Boer, Peter LeFanu Lumsdaine, Anders Mortberg, Initiality for Martin-Löf type theory, Talk at HoTTEST Seminar, Sept. 10, 2020, https://www.youtube.com/watch?v=1ogUFFUfU_M.
[3] Kuen-Bang (Favonia) Hou, Implementation of higher inductive types in HoTT-Agda, https://github.com/HoTT/HoTT-Agda/blob/master/core/lib/types/HIT_README.txt.
[4] Chris Kapulkin, Peter LeFanu Lumsdaine, The simplicial model of univalent foundations (after Voevodsky), J. Eur. Math. Soc. (2012), in press, arXiv:1211.2851.
[5] Peter LeFanu Lumsdaine, Michael Shulman, Semantics of higher inductive types, Math. Proc. Camb. Philos. Soc. 169 (1) (2020) 159–208, https://doi.org/10.1017/S030500411900015X, arXiv:1705.07088.
[6] Jacob Lurie, Higher Topos Theory, Annals of Mathematics Studies, vol. 170, Princeton University Press, 2009, arXiv:math/0608040.
[7] Michael Shulman, All $(\infty, 1)$-toposes have strict univalent universes, 2019.

[8] Michael Shulman, Proof sketch of circle induction, https://groups.google.com/d/msg/homotopytypetheory/hE1eY-v_Kes/bdSoAxC9224J.
[9] Michael Shulman, The univalence axiom for elegant Reedy presheaves, Homology, Homotopy, and Applications 17 (2) (2015) 81–106, https://doi.org/10.4310/HHA.2015.v17.n2.a6, arXiv:1307.6248.
[10] Kristina Sojakova, Higher Inductive Types as Homotopy-Initial Algebras, Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. POPL '15, Association for Computing Machinery, Mumbai, India, 2015, pp. 31–42, arXiv:1402.0761.
[11] The Univalent Foundations Program, Homotopy Type Theory: Univalent Foundations of Mathematics, Institute for Advanced Study, 2013, https://homotopytypetheory.org/book.
[12] Vladimir Voevodsky, A C-system defined by a universe category, Theory Appl. Categ. 30 (37) (2015) 1181–1215, arXiv:1409.7925, http://www.tac.mta.ca/tac/volumes/30/37/30-37.pdf.
[13] Vladimir Voevodsky, C-system of a module over a Jf-relative monad, arXiv:1602.00352.
[14] Vladimir Voevodsky, C-systems defined by universe categories: presheaves, Theory Appl. Categ. 32 (3) (2017) 53–112, http://www.tac.mta.ca/tac/volumes/32/3Z32-03.pdf.
[15] Vladimir Voevodsky, HoTT is not an interpretation of MLTT into abstract homotopy theory, https://homotopytypetheory.org/2015/01/11/hott-is-not-an-interpretation-of-mltt-into-abstract-homotopy-theory/, 2015.
[16] Vladimir Voevodsky, Martin-Löf identity types in the C-systems defined by a universe category, arXiv:1505.06446, 2015.
[17] Vladimir Voevodsky, Products of families of types and (n, A)-structures on C-systems, Theory Appl. Categ. 31 (36) (2016) 1044–1094, http://www.tac.mta.ca/tac/volumes/31/36/31-36.pdf.
[18] Vladimir Voevodsky, Subsystems and regular quotients of C-systems, in: A Panorama of Mathematics: Pure and Applied; Conference on Mathematics and Its Applications, Kuwait City, 2014, in: Contemp. Math., vol. 658, Amer. Math. Soc., Providence, RI, 2016, pp. 127–137, arXiv:1406.7413.
[19] Vladimir Voevodsky, The (n, A)-structures on the C-systems defined by universe categories, Theory Appl. Categ. (ISSN 1201-561X) 32 (4) (2017) 113–121.
[20] Vladimir Voevodsky, Unimath - its present and its future, A talk, with slides and video available at https://www.newton.ac.uk/seminar/20170710113012301.
[21] Vladimir Voevodsky, Benedikt Ahrens, Daniel Grayson, et al., UniMath — a computer-checked library of univalent mathematics, http://UniMath.org.