A Univalent Formalization of Constructive Affine Schemes

Max Zeuner
Department of Mathematics, Stockholm University, Sweden

Anders Mörtberg
Department of Mathematics, Stockholm University, Sweden

Abstract

We present a formalization of constructive affine schemes in the `Cubical Agda` proof assistant. This development is not only fully constructive and predicative, it also makes crucial use of univalence. By now schemes have been formalized in various proof assistants. However, most existing formalizations follow the inherently non-constructive approach of Hartshorne's classic "Algebraic Geometry" textbook, for which the construction of the so-called structure sheaf is rather straightforwardly formalizable and works the same with or without univalence. We follow an alternative approach that uses a point-free description of the constructive counterpart of the Zariski spectrum called the Zariski lattice and proceeds by defining the structure sheaf on formal basic opens and then lift it to the whole lattice. This general strategy is used in a plethora of textbooks, but formalizing it has proved tricky. The main result of this paper is that with the help of the univalence principle we can make this "lift from basis" strategy formal and obtain a fully formalized account of constructive affine schemes.

2012 ACM Subject Classification Theory of computation → Logic and verification; Theory of computation → Constructive mathematics; Theory of computation → Type theory

Keywords and phrases Affine Schemes, Homotopy Type Theory and Univalent Foundations, Cubical Agda, Constructive Mathematics

Digital Object Identifier 10.4230/LIPIcs.TYPES.2022.14

Related Version *Full Version*: `https://arxiv.org/abs/2212.02902`

Supplementary Material *Software (Agda Source Code)*: `https://github.com/agda/cubical/blob/310a0956bb45ea49a5f0aede0e10245292ae41e0/Cubical/Papers/AffineSchemes.agda`
archived at `swh:1:cnt:beb6a5859db19530348074be6e9166c04871e6c7`

Funding This paper is based upon research supported by the Swedish Research Council (SRC, Vetenskapsrådet) under Grant No. 2019-04545. The research has also received funding from the Knut and Alice Wallenberg Foundation through the Foundation's program for mathematics.

Acknowledgements We would like to thank Thierry Coquand for his continued feedback and invaluable comments throughout this project. We are also indebted to Felix Cherubini for his comments and his work on the `Cubical Agda` library, particularly for his ring solver. Furthermore, we thank Martín Hötzel Escardó, Peter Dybjer, Peter LeFanu Lumsdaine, Egbert Rijke and the participants of the "Proof and Computation" autumn school in Fischbachau for our discussions.

1 Introduction

Algebraic geometry originated as the study of solutions of polynomials. Historically, the geometric objects of interest would be for example *complex affine varieties* – subsets of $\mathbb{C}^n$ defined by systems of polynomial equations. Starting with the pioneering work of Grothendieck in the 1960s, the scope of the discipline was drastically widened, making it one of the most pervasive in modern day mathematics. At the heart of this development are *schemes* – geometric objects that generalize from algebraically closed fields, like $\mathbb{C}$, to arbitrary commutative rings.

A point $a \in \mathbb{C}$ corresponds to the maximal ideal of the polynomial ring $\mathbb{C}[x]$ consisting of polynomials p such that $p(a) = 0$, i.e. the ideal generated by $(x - a)$. By looking not only at maximal ideals, but also at prime ideals of $\mathbb{C}[x]$, we arrive at the *spectrum* of $\mathbb{C}[x]$, denoted $\mathsf{Spec}\,\mathbb{C}[x]$. As $\mathbb{C}[x]$ has a non-maximal prime ideal, the zero-ideal, $\mathsf{Spec}\,\mathbb{C}[x]$ contains an additional point to $\mathbb{C}$ and carries a very different topology. This is called the *Zariski topology* in which the open sets are generated by *basic opens* $D(p) \subseteq \mathsf{Spec}\,\mathbb{C}[x]$ where $p \in \mathbb{C}[x]$. If $p \neq 0$, $D(p)$ corresponds to the set of points a where $p(a) \neq 0$ together with the zero-ideal. The spectrum can then be equipped with a *structure sheaf* that associates to every Zariski open set U a ring of "rational functions" definable on U. For a basic open $D(p)$, this will be the ring of function $q(x)/p(x)^n$ where q is another polynomial. This corresponds to the functions of the quotient ring $\mathbb{C}(x)$ that are definable everywhere but at the zeros of p. See Vakil's "The Rising Sea" [34, Ex. 3.2.3.1] for a more in-depth discussion of this motivating example and an illustration of $\mathsf{Spec}\,\mathbb{C}[x]$.

This construction can be carried out for any commutative ring R instead of $\mathbb{C}[x]$: the spectrum $\mathsf{Spec}\,R$ is the set of prime ideals of R and its Zariski topology is again generated by basic opens. For $f \in R$, the basic open $D(f)$ is the set of prime ideals that do *not* contain f. The structure sheaf maps $D(f)$ to the *localization* $R[1/f]$, the ring of fractions r/f^n where $r \in R$ and the denominator is a power of f. One can prove that this always defines a sheaf, i.e. is compatible with taking covers of open sets in a certain sense.

When Grothendieck introduced the general notion of (affine) schemes, he did so in a structural fashion that is typical for his work. Mathematical objects, in particular algebraic structures, are taken to be identical if they are isomorphic in some unique, or at least canonical, way. When constructing the structure sheaf, however, this leads to a problem of well-definedness: if $D(f) = D(g)$, then we better have $R[1/f] = R[1/g]$. Unfortunately, it is not difficult to come up with examples violating this. For example, we have $D(x) = D(x^2)$ in $\mathbb{C}[x]$ (both functions vanish only at 0), but formally speaking $\mathbb{C}[x][1/x]$ is not strictly the same ring as $\mathbb{C}[x][1/x^2]$ despite them clearly being isomorphic and describing the same sub-ring of the quotient ring $\mathbb{C}(x)$, as $1/x = x/x^2$.

In this paper we show how this problem can be solved with the help of univalence. In particular, we present a formalization in `Cubical Agda` [35] of constructive affine schemes following Coquand, Lombardi and Schuster [10]. In the constructive setting, the Zariski spectrum of a commutative ring is replaced by the so-called *Zariski lattice*. Elements of this lattice are *finitely* generated by formal basic opens, which allows for a completely predicative approach that does not require additional assumptions like Voevodsky's resizing axioms [38].

The definition of constructive affine schemes still works analogously to the classical definition given in most textbooks ranging from Grothendieck's authoritative classic "EGA I" [13], to more modern treatments such as "Algebraic Geometry" by Görtz and Wedhorn [15], "The Rising Sea" by Vakil [34], or Johnstone's "Stone Spaces" [18]. In either case one starts with the basic opens, on which the structure sheaf is defined and proved to be a sheaf. Using abstract categorical machinery this is then lifted to a sheaf on the whole Zariski spectrum/lattice. More precisely, one takes the right Kan extension along the inclusion of basic opens, which preserves the sheaf property.

From a constructive, predicative point of view there are two differences that make this construction work for the Zariski lattice. Predicatively, the inclusion of basic opens into the Zariski lattice is one of small categories, while the inclusion into the classical spectrum is not. Furthermore, since we are only concerned with sheaves on a distributive lattice and not on a general locale or topological space, we only have to consider finite covers. This allows for a predicative proof that the right Kan extension preserves sheaves on lattices. From a

classical point of view this is not really a restriction as $\mathsf{Spec}\, R$ is always a *coherent* space. As a result, sheaves on $\mathsf{Spec}\, R$ are in bijection to (finitary) sheaves on the Zariski lattice. For more details see e.g. Johnstone's "Stone Spaces" [18] and Section 6.1 of this paper.

Regardless of whether one formalizes the classical or constructive definitions, the main bottlenecks of the formalization are already found at the level of basic opens. First and foremost, there is the well-definedness problem described above. The second bottleneck is proving that the structure sheaf actually is a sheaf on basic opens. In fact, the problem with the textbook proof of the sheaf property is the well-definedness problem in disguise. Those two points were exactly where the most prominent formalization of schemes [4] in `Lean`'s `mathlib` [26] encountered problems. In this paper, we show that with the help of univalence it is in fact possible to overcome the issues of well-definedness and formalize the structure sheaf directly on basic opens and prove its sheaf property. Even though we work in the constructive, predicative setting using the Zariski lattice, the techniques used to overcome the problems on the level of basic opens should be applicable to a classical formalization in type theory with univalence and classical axioms added. The key insight is that localizations are not just commutative rings, but also commutative algebras over R. In R-algebras, isomorphisms, and thus also paths, between two localizations are unique, which ensures well-definedness of the structure sheaf.

As mentioned above, our work is completely formalized[1] in `Cubical Agda`, an extension of the `Agda` proof assistant [31] based on the cubical type theory of [7, 8] with fully constructive support of the univalence axiom and higher inductive types (HITs). However, nothing relies crucially on cubical features, or on univalence and eliminators applied to higher constructors of HITs computing definitionally, in our formalization. The only HoTT/UF features that we rely on are univalence and set quotients (from which propositional truncation follows). It would hence be possible to perform the formalization in a system implementing Book HoTT [33] or in `UniMath` [36]. Our work is thus in line with the aim of Voevodsky's Foundations library [39] of developing a library of constructive set-level mathematics based on Univalent Foundations.

Contributions

As mentioned above, the formalization presented in this paper generally follows the constructive, lattice-based approach of [10]. However, a number of design choices had to be made to ensure predicativity of our formalization and to enable us to formally prove the well-definedness of the structure sheaf. As a result some definitions and proofs deviate from the presentation in [10]. The main design choices and contributions of the paper and formalization can be summarized under the following topics:

- **Commutative algebra:** our formalization of localizations of commutative rings in Section 3.1 closely follows Atiyah and MacDonald's classic textbook [2], which works very well for our constructive approach. However, giving a predicative definition of the Zariski lattice that does not increase universe levels was more intricate. To this end, Section 3.2 contains a construction that refines the ideal-based description of [10] using ideas of Español [14].

[1] All results discussed are integrated in the `agda/cubical` library and are summarized in:
`https://github.com/agda/cubical/blob/310a0956bb45ea49a5f0aede0e10245292ae41e0/Cubical/Papers/AffineSchemes.agda`
This is a permalink to the library at the time of writing, which type-checks with `Agda` version 2.6.3.
A clickable rendered version that might be subject to change can be found here:
`https://agda.github.io/cubical/Cubical.Papers.AffineSchemes.html`

- **Category theory:** in Section 4 we present a formal notion of sheaf on a distributive lattice that closely follows [10]. However, in [10] presheaves are extended from a basis of a distributive lattice to the whole lattice in a somewhat non-standard finitary way. This is to ensure predicativity, but it actually causes problems when working in a univalent setting. We found that the point-wise right Kan extension of presheaves, as e.g. presented in MacLane's classic textbook [23], works just fine even in the constructive and predicative setting. We then give a proof that the Kan extension preserves the sheaf property. This can be seen as the main step towards a constructive and predicative "comparison lemma" that gives an equivalence of categories between sheaves on a lattice and sheaves on a basis of the lattice.
- **Constructive affine schemes:** in Section 5 we construct the structure sheaf on basic opens and extend it to the Zariski lattice. We give general heuristics for constructing presheaves (valued in R-algebras) on subsets defined using propositional truncation. The well-definedness of the presheaves thus constructed follows from univalence. The structure sheaf is a special instance of this construction with the basic opens seen as a subset of the Zariski lattice. Proving the sheaf property on basic opens can then be reduced to standard commutative algebra, again by using univalence in a way that does not require to extract the isomorphisms underlying the applications of univalence.

2 Background

Here we give the necessary background for the paper. We first sketch the constructive approach to schemes of [10]. We then continue with an introduction to the concepts of `Cubical Agda` needed for the paper.

2.1 Affine schemes constructively

Recall that, classically, the spectrum of a commutative ring R is the set of its prime ideals $\mathsf{Spec}\, R = \{\mathfrak{p} \subseteq R \mid \mathfrak{p} \text{ prime}\}$ equipped with the Zariski topology. The open sets of this topology are generated by basic opens $D(f) = \{\mathfrak{p} \mid f \notin \mathfrak{p}\}$ for $f \in R$. Constructively, there are two issues with this. First, the notion of prime ideal is not really well-behaved. One of the main reasons for this is that the central notion of *localizing* at a prime ideal $\mathfrak{p}$ actually uses the set-theoretic complement $R \setminus \mathfrak{p}$, which does not work well constructively without additional decidability assumptions.[2] To remedy this, one can define the notion of a *prime filter* on R and check that classically those are exactly the complements of prime ideals.

The second issue concerns the point-set definition of a topological space itself. For a constructive development of algebraic geometry it is preferable to avoid this definition and instead characterize the *locale* of open sets of $\mathsf{Spec}\, R$ in a direct, point-free way. This can be done by observing that the closed sets of the Zariski topology admit a direct algebraic characterization. Every closed set is of the form $V(\mathfrak{a}) = \{\mathfrak{p} \mid \mathfrak{a} \subseteq \mathfrak{p}\}$, where $\mathfrak{a}$ is a *radical ideal*. An ideal $\mathfrak{a} \subseteq R$ is radical if $\mathfrak{a} = \sqrt{\mathfrak{a}}$, where

$$\sqrt{\mathfrak{a}} = \left\{ x \in R \mid \exists n > 0 : x^n \in \mathfrak{a} \right\}$$

The *locale of Zariski opens* can thus be characterized by the set of radical ideals of R. The join and meet operation can be defined using addition and multiplication of ideals.

[2] See e.g. the discussion by Mines, Richman and Ruitenberg in their standard textbook on constructive algebra [27, Section III.3].

From a predicative viewpoint this is still unsatisfactory. Predicatively, the ideals of a ring form a proper class and consequently the Zariski locale is not a set in such a setting. However, by restricting to the *lattice of compact open sets* of the Zariski topology these size issues can be avoided.[3] Classically, the objects of this lattice are finite unions of basic opens $D(f_1) \cup \cdots \cup D(f_n)$ and the join and meet operation are just union $\cup$ and intersection $\cap$. Note that for the meet this only works because basic opens are closed under intersections, i.e. we have $D(f) \cap D(g) = D(fg)$ for any $f, g \in R$.

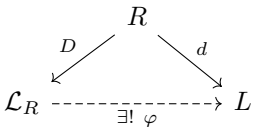
As with the locale of Zariski opens, this so-called *Zariski lattice* $\mathcal{L}_R$ of a commutative ring R can be described in a point-free way. This was first done by Joyal [19], using the observation that the Zariski lattice has a certain universal property. The lattice itself can be defined as the free distributive lattice generated by *formal symbols* $D(f)$, $f \in R$, satisfying the following relations:

$$D(1) = \top \quad \text{and} \quad D(0) = \bot \tag{1}$$

$$\forall f, g \in R : \; D(fg) = D(f) \wedge D(g) \tag{2}$$

$$\forall f, g \in R : \; D(f + g) \leq D(f) \vee D(g) \tag{3}$$

The induced map $D : R \to \mathcal{L}_R$ is universal in the following sense: for any distributive lattice L and *support* map $d : R \to L$, i.e. any map d such that conditions (1)-(3) above hold for d (in place of D), there is a unique lattice homomorphism $\varphi : \mathcal{L}_R \to L$ such that the following commutes



Using the correspondence of Zariski opens with radical ideals, the elements of $\mathcal{L}_R$ can also be described as the *radicals of finitely generated ideals*. For two finitely generated ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$, the join and meet of the radicals are then given by

$$\sqrt{\mathfrak{a}} \vee \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a} + \mathfrak{b}} \qquad \text{and} \qquad \sqrt{\mathfrak{a}} \wedge \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a}\mathfrak{b}}$$

using the fact that addition and multiplication of two finitely generated ideals is again finitely generated. The support $D : R \to \mathcal{L}_R$ maps $f \in R$ to the radical of the principal ideal $\sqrt{\langle f \rangle}$ and for any support $d : R \to L$, the unique morphism $\varphi : \mathcal{L}_R \to L$ is given by

$$\varphi\big(\sqrt{\langle f_1, \ldots, f_n \rangle}\,\big) \;=\; d(f_1) \vee \cdots \vee d(f_n)$$

In Section 3.2, we will show how to formalize this Zariski lattice of radicals of finitely generated ideals and prove its universal property while avoiding size issues.

The lattice theoretic approach does require a notion of a sheaf on a distributive lattice. Recall that a sheaf on a topological space X is just a sheaf on the locale of open sets of X. By restricting the definition of sheaf on a locale to finite covers one obtains sheaves on a distributive lattice. This means that for any distributive lattice L, a presheaf $\mathcal{F} : L^{op} \to \mathcal{C}$, valued e.g. in commutative rings (i.e. $\mathcal{C} = \mathsf{CommRing}$), is a sheaf if for all $x_1, \ldots, x_n \in L$ the following is an equalizer diagram

[3] Through a more careful analysis one might be able to define the structure sheaf on the large Zariski locale in predicative univalent foundations, as long as one uses a small type of basic opens. See the recent work by de Jong and Hötzel Escardó [11] and by Tosun and Hötzel Escardó [32] for results of this kind. For the development of constructive and predicative scheme theory however, it seems certainly advantageous to work with the small Zariski lattice.

$$\mathcal{F}\Big(\bigvee_{i=1}^{n} x_i\Big) \to \prod_{i=1}^{n} \mathcal{F}(x_i) \rightrightarrows \prod_{i<j} \mathcal{F}(x_i \wedge x_j)$$

A basis of a distributive lattice is a subset $B \subseteq L$ containing $\top$ and closed under meets, such that for any $x \in L$ there exists a finite list $b_1, \dots, b_n \in B$ such that $x = \bigvee_{i=1}^{n} b_i$. In Section 4, we describe how to obtain sheaves on L from sheaves on B. This works analogous to the special case of the so-called *comparison lemma* for topological spaces. For the structure sheaf, the idea is to map $D(f)$ to the ring $R[1/f]$, the *localization of R away from f*. Recall that for a subset $S \subseteq R$ containing 1 and being closed under multiplication, the localization $S^{-1}R$ is defined as the ring of fractions r/s where $r \in R$ and $s \in S$. Equality of fractions is given by

$$\frac{r_1}{s_1} = \frac{r_2}{s_2} \quad \text{iff} \quad \exists u \in S : \; u(r_1 s_2 - r_2 s_1) = 0$$

$R[1/f]$ is defined by localizing with $S = \{1, f, f^2, f^3, \dots\}$. Its elements are thus fractions r/f^n where the denominator is a power of f and equality can be rephrased as

$$\frac{r}{f^n} = \frac{r'}{f^m} \quad \text{iff} \quad \exists k \in \mathbb{N} : \; f^{k+m} r = f^{k+n} r'$$

Verifying that the presheaf defined by sending $D(f)$ to $R[1/f]$ is indeed a sheaf on the basis $\mathcal{B}_R \subseteq \mathcal{L}_R$ of basic opens proceeds the same way in any constructive or classical account. As indicated in the introduction, there are some issues to be overcome when formalizing the construction of the structure sheaf. In this paper we discuss what a solution to these problems can look like in a univalent setting.[4]

2.2 Set-level univalent mathematics in Cubical Agda

We will now briefly discuss the concepts needed from `Cubical Agda` for this paper, for more details see [35]. Our notation is inspired by `Agda` syntax and the `agda/cubical` library, but we have taken some liberties when typesetting, e.g. shortening notations and omitting some projections and universe levels whenever possible. We write `Type ℓ` for universes (at level ℓ) and `Σ[ x ∈ A ] B x` for dependent pair types over a family $B : A \to$ `Type ℓ`. The major difference when working in `Cubical Agda` compared to vanilla `Agda` or Book HoTT is that the primary identity type is changed from Martin-Löf's inductive construction [25] to a primitive *path*-type. The identification $x \equiv y$ is captured by `Path A x y`, the type of functions $p :$ `I` $\to A$, where `I` is a primitive interval type, restricting definitionally to x and y at the endpoints `i0` and `i1` of `I`. `Cubical Agda` also has a dependent path type, `PathP`. Given a line of types $B :$ `I` $\to$ `Type`, which we may think of as B(`i0`) $\equiv B$(`i1`), and $x : B$(`i0`), $y : B$(`i1`), the type `PathP` $B\ x\ y$ expresses that x and y may be identified relative to B. The regular path type `_≡_` is, by definition, `PathP` $(\lambda\ i \to A)$, i.e. the special case of a constant line of types.

`Cubical Agda` also comes with a function `ua` : $A \simeq B \to A \equiv B$ which promotes equivalences (or isomorphisms) of types to paths between these types. The fact that this map is an equivalence itself is a way to formulate Voevodsky's univalence axiom. A reasonable question to ask in a univalent setting is whether an equivalence of types can be promoted to

[4] A solution that is e.g. taken in [10], is to map $D(f)$ to $S_f^{-1}R$, the ring of fractions whose denominators are elements of the *saturation* $S_f = \{g \mid D(f) \subseteq D(g)\}$. It is immediate to see that if $D(f) = D(g)$, then $S_f^{-1}R = S_g^{-1}R$, but it is not as natural to work with these rings. Usually, one still wants to appeal to the "canonical isomorphism" between $R[1/f]$ and $S_f^{-1}R$, as in e.g. [13, Sect. 1.3].

an equality of structured types, such as groups or rings. The *Structure Identity Principle (SIP)* [33, Sect. 9.8] is an informal principle which attempts to answer this: given two structured types (A, S_A) and (B, S_B) and an equivalence of underlying types $A \simeq B$ which is a homomorphisms with respect to the structure in question, we get a path of structured types $(A, S_A) \equiv (B, S_B)$. For instance, an isomorphism of rings R and S induces a path $R \equiv S$. This has been implemented in `agda/cubical` using the cubical SIP of Angiuli, Cavallo, Mörtberg and Zeuner [1]. For this paper we will use sip to denote the function that turns isomorphisms of commutative rings or R-algebras (over a ring R) into paths.

Univalence refutes *Uniqueness of Identity Proofs (UIP)*, or Streicher's axiom K [30], because it produces equality proofs in Type that are not equal [33, Ex. 3.1.9]. In the presence of univalence, it is therefore important to keep track of which types satisfy UIP or related principles expressing the complexity of a type's equality relation. In the terminology of HoTT/UF, a type satisfying UIP is called an *h-set* (*homotopy set*, henceforth simply *set*), while a type whose elements are all equal is called an *h-proposition* (henceforth *proposition*).

Another very important concept in HoTT/UF is that of *contractible* types, i.e. types with exactly one element:

```
isContr : Type → Type
isContr A = Σ[ x ∈ A ] ((y : A) → x ≡ y)
```

We can characterize propositions as types whose equality types are contractible, just as sets are types whose equality types are propositions. Thus contractible types, propositions, and sets serve as the bottom three layers of an infinite hierarchy of types introduced by Voevodsky, known as *h-levels* [37] or *n-types* [33]. This paper is about set-level mathematics, so we are mainly interested in these 3 bottom layers. However, univalence implies that collections of set-level structures (e.g. the collection of all commutative rings or R-algebras) are one level higher than sets. Types at this level are called *h-groupoids* (heceforth *groupoids*) and will be the only types of h-level higher than 2 in the paper. We write isProp A to say that A is a proposition and isSet A to say that A is a set. The "universe of propositions" hProp ℓ is defined as Σ[$A \in$ Type ℓ] (isProp A), and if isSet A, we call functions $S : A \to$ hProp ℓ a *subset* of A. For $a : A$ we denote by $a \in S$ the type of proofs that a is actually in S. It is often convenient to identify the subset S with Σ[$a \in A$] $(a \in S)$, which can be seen as a sub-type of A. With some abuse of notation we will not distinguish between subsets as functions and the corresponding Σ-type. We thus write $a : S$ for elements of S when the proof of a belonging to S can be ignored.

Another concept from HoTT/UF which `Cubical Agda` supports are higher inductive types (HITs). These allow us to define many important operations on types, such as truncations. For instance, the propositional truncation is defined by:

```
data ∥_∥ (A : Type ℓ) : Type ℓ where
  |_| : A → ∥ A ∥
  squash : isProp ∥ A ∥
```

This HIT takes a type A and forces it to be a proposition. This is a very important construction for capturing existential quantification in HoTT/UF:

$$\exists[\ x \in A\ ]\ P(x) = \| \Sigma[\ x \in A\ ]\ P(x) \|$$

In this paper, we follow the HoTT Book terminology and say that x *merely* exists when it is existentially quantified. Note that the propositional truncation in the definition is crucial. In HoTT/UF, $\Sigma\, A\, P$ without the truncation is interpreted as the total space of P, which may be highly non-trivial. For example, a subset B of a lattice L is a basis if

$$\forall\,(x : L) \to \exists[\ b_1, \ldots, b_n \in B\ ]\ (\bigvee_{i=1}^{n} b_i \equiv x)$$

Here the propositional truncation is necessary. We will see this in Section 3.2, when proving that the basic opens form a basis of $\mathcal{L}_R$.

The main HIT that we use in this paper is the *set quotient*, which quotients a type by an arbitrary relation, yielding a set. It has three constructors: [_], which includes elements of the underlying type, eq/, which equates all pairs of related elements, and squash/, which ensures that the resulting type is a set:

```
data _/_ (A : Type ℓ) (R : A → A → Type ℓ) : Type ℓ where
  [_] : (a : A) → A / R
  eq/ : (a b : A) → (r : R a b) → [ a ] ≡ [ b ]
  squash/ : isSet (A / R)
```

We can write functions out of A / R by pattern-matching; this amounts to writing a function out of A (the clause for [_]) which sends R-related elements of A to equal results (the clause for eq/), such that the image of the function is a set (the clause for squash/). Set quotients and propositional truncations have in common that the resulting type will be of a fixed h-level and this makes it very hard to map into types of higher h-levels. In fact, the higher the h-level of the target type, the more complicated the coherence conditions that need to be proved. We will see an example of this in Section 5.

3 Commutative algebra

In this section, we first discuss our formalization of localizations of rings, followed by the definition of the Zariski lattice. These objects can be described by universal properties, but may also be concretely implemented as set quotients. One of the guiding principles of this project was to work with concrete implementations and mainly use universal properties to construct equivalences and paths (via the SIP). As a result the formalization follows the usual informal treatment in the commutative algebra literature quite closely.

3.1 Localizations

Our formalization of localizations of commutative rings follows the classic textbook of Atiyah and MacDonald [2], with our main result being a path version of [2, Cor. 3.2]. Note that the definition of localization is actually the same in classical and constructive algebra.[5] For the remainder of this paper we will only consider commutative rings with a multiplicative unit (denoted by 1). Let R be such a ring and S a subset of R that contains 1 and is closed under multiplication. The formalization of localization is then straightforward:

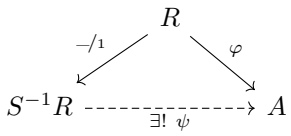
```
S⁻¹R : Type
S⁻¹R = (R × S) / _≈_
  where
  _≈_ : R × S → R × S → Type
  (r₁ , s₁ , _) ≈ (r₂ , s₂ , _) = Σ[ (u , _) ∈ S ] (u · r₁ · s₂ ≡ u · r₂ · s₁)
```

The underscores in the definition of ≈ correspond to the proofs that s_1, s_2 and s are elements of S respectively. As these are unimportant to the definition of ≈, we can safely omit them.

[5] Compare [2] with e.g. the books by Lombardi and Quitté [22] or Mines, Richman and Ruitenburg [27].

▶ Remark 1. It might be surprising that we define $\approx$ using a Σ and not an $\exists$ (as is done e.g. in [39]). However, it turns out that it does not matter whether one quotients by the truncated relation using $\exists$ or the untruncated relation using Σ, as the resulting set-quotients will be equivalent. As we do not need to prove anything about $\approx$ except it being an equivalence relation, it is more convenient to work without the truncation.

Equipping $S^{-1}R$ with the structure of a commutative ring is laborious in `Cubical Agda`, but the proofs generally proceed as in any textbook. The same holds for the universal property. Note that for this we need the canonical homomorphism $\_/1 : R \to S^{-1}R$, mapping $r : R$ to $[\ r\ ,\ 1\ ]$, the equivalence class corresponding to $r/1$. The universal property then states that for any commutative ring A with a morphism $\varphi : R \to A$, such that for all $s : S$ we have $\varphi(s) \in A^\times$ (i.e. that $\varphi(s)$ is a unit in A), there is a unique morphism $\psi : S^{-1}R \to A$, such that the following commutes



The key observation for the main results of this paper is that localizations are R-algebras via the canonical homomorphism $\_/1$. The type of R-algebras is equivalent to the Σ-type of a commutative ring A together with a ring homomorphism $\varphi : R \to A$. An homomorphism between R-algebras (A, φ) and (B, ψ) is just a ring homomorphism $\chi : A \to B$ together with a path $\chi \circ \varphi \equiv \psi$. The type of R-algebra homomorphisms will be denoted by $\mathrm{Hom}_R\big[(A, \varphi), (B, \psi)\big]$ or just $\mathrm{Hom}_R\big[A, B\big]$ if the morphisms are clear from context.

The universal property of localization then becomes a statement about R-algebras. In HoTT/UF unique existence is defined as contractibility of Σ-types, so the universal property of the localization at S becomes: *for any R-algebra (A, φ) s.t. $\varphi(S) \subseteq A^\times$, the type $Hom_R\big[S^{-1}R, (A, \varphi)\big]$ is contractible.* Combining the proof of [2, Cor. 3.2] with the SIP, we can then prove the following:[6]

▶ **Lemma 2.** *Let A be a commutative ring with a morphism $\varphi : R \to A$ satisfying*

- $\forall (s : S) \to \varphi(s) \in A^\times$
- $\forall (r : R) \to \varphi(r) \equiv 0 \to \exists[\ s \in S\ ]\ (sr \equiv 0)$
- $\forall (a : A) \to \exists[\ (r\ ,\ s) \in R \times S\ ]\ (\varphi(r)\varphi(s)^{-1} \equiv a)$

From this we can construct a path $S^{-1}R \equiv A$, which is unique as a path in R-algebras.

With this result we can transport proofs about localizations to any suitable ring and morphism pair, i.e. R-algebra, satisfying the three conditions above. Below we will see a few applications of this result that will be used for formalizing constructive affine schemes. The important case for our purpose is $R[1/f]$, the localization of R *away from* f. This can be seen as inverting a single element f in R. The subset $S = \{1, f, f^2, f^3, ...\}$ is easily defined in `Cubical Agda` as the set of $g : R$ for which we have an inhabitant of $\exists[\ n \in \mathbb{N}\ ]\ (g \equiv f^n)$.

For the remainder of this section let $f, g : R$. By the canonical homomorphism we get an element $g/1$ in $R[1/f]$. With a bit of abuse of notation we denote the localization away from this element by $R[1/f][1/g]$. This is an R-algebra by applying the canonical morphism $\_/1$ twice. We can of course also localize away from $(f \cdot g)$, thus obtaining $R[1/fg]$. Using Lemma 2, we can construct a (unique) path between these two, which will be used for the structure sheaf. Similarly, we also get other useful paths.

[6] In `Lean`'s `mathlib` *a* localization is defined to be any ring-morphism-pair satisfying the three conditions of Lemma 2. The formulation of this predicate is attributed to Neil Strickland in [4].

▶ **Lemma 3.** *We have the following paths for both commutative rings and R-algebras:*
1. $R[1/f][1/g] \equiv R[1/fg]$
2. $R[1/f] \equiv R$, *if* $f \in R^\times$
3. $R[1/f] \equiv R[1/g]$, *if* $f/1 \in R[1/g]^\times$ *and* $g/1 \in R[1/f]^\times$

3.2 The Zariski lattice

Next, we provide a definition of the Zariski lattice that does not lead to size issues, while still being convenient to work with. We have already seen that the Zariski lattice $\mathcal{L}_R$, which classically corresponds to the compact open sets of the Zariski topology, can be described as the lattice of radicals of finitely generated ideals. The meet and join of this lattice are defined using multiplication and addition of ideals. With some elementary ideal theory this should be straightforward to formalize. Unfortunately, without any form of impredicativity, like resizing axioms, this leads to size issues.

So far we have avoided being explicit about universe levels, but in this section let ℓ be the level of the base ring R, that is, the level of the universe in which the underlying type of R lives. Being precise about universe levels, subsets of R are elements of $R \to \mathsf{hProp}\ \ell$, living in $\mathsf{Type}\ (\ell + 1)$, the next bigger universe. The type of all ideals of R, which is just the Σ-type of subsets satisfying the ideal property, is hence in $\mathsf{Type}\ (\ell + 1)$. However, for technical reasons to be discussed in the next section, we need $\mathcal{L}_R : \mathsf{Type}\ \ell$. Consequently, the definition of $\mathcal{L}_R$ must not rely on the type of all ideals of R.

To avoid this issue, we use a construction due to Español [14]. Since we are only concerned with the radicals of finitely generated ideals, we can describe $\mathcal{L}_R$ in terms of generators instead of arbitrary ideals. In particular, a list of generators $\alpha = [\alpha_0, \ldots, \alpha_n]$ with $\alpha_i : R$ corresponds to the radical of the ideal generated by the α_i. In other words, we can obtain $\mathcal{L}_R$ by quotienting the type of lists with elements in R, by the relation

$$\alpha \sim \beta \quad \Leftrightarrow \quad \left(\forall\ i \to \beta_i \in \sqrt{\langle \alpha_0, \ldots, \alpha_n \rangle}\right) \text{ and } \left(\forall\ i \to \alpha_i \in \sqrt{\langle \beta_0, \ldots, \beta_m \rangle}\right)$$

Here $\langle \alpha_0, \ldots, \alpha_n \rangle$ is the ideal generated by the α_i's. As both the type of lists and $\sim$ live in $\mathsf{Type}\ \ell$ so does their quotient $\mathcal{L}_R$. It might seem more natural to quotient by the relation

$$\alpha \approxeq \beta \quad \Leftrightarrow \quad \sqrt{\langle \alpha_0, \ldots, \alpha_n \rangle} \equiv \sqrt{\langle \beta_0, \ldots, \beta_m \rangle}$$

Unfortunately the type of paths between two such radicals is large, as for any two ideals I, J we have $I \equiv J : \mathsf{Type}\ (\ell + 1)$. Still, $\sim$ is equivalent to $\approxeq$ in the sense that we have $\alpha \sim \beta$ if and only if $\alpha \approxeq \beta$. This equivalence can then be used in proofs.

Equipping $\mathcal{L}_R$ with the distributive lattice structure requires us to introduce operations on lists that correspond to ideal addition and multiplication. For the join we can take list concatenation $\_ +\!\!+ \_$ as this corresponds to addition of finitely generated ideals in the sense that for any two lists α, β we have that

$$\begin{aligned} \langle\ [\alpha_0, \ldots, \alpha_n] +\!\!+ [\beta_0, \ldots, \beta_m]\ \rangle &\equiv \langle \alpha_0, \ldots, \alpha_n, \beta_0, \ldots, \beta_m \rangle \\ &\equiv \langle \alpha_0, \ldots, \alpha_n \rangle + \langle \beta_0, \ldots, \beta_m \rangle \end{aligned} \tag{4}$$

When checking that $\_ +\!\!+ \_$ defines an operation on the quotient $\mathcal{L}_R$, it suffices to check that it respects $\approxeq$, which in turn follows from (4).

For the meet of $\mathcal{L}_R$ we need to define an operation $\_ \cdot\cdot \_$ on lists that corresponds to multiplication of finitely generated ideals. For two lists α, β this product $\alpha \cdot\cdot \beta$ is the list of all products of the form $\alpha_i \beta_j$. Proving the correspondence to ideal multiplication, i.e.

$$\begin{aligned}\langle\, [\alpha_0, \ldots, \alpha_n] \cdot\cdot [\beta_0, \ldots, \beta_m] \,\rangle &\equiv \langle \alpha_0\beta_0, \ldots, \alpha_n\beta_0, \ldots, \alpha_0\beta_m, \ldots, \alpha_n\beta_m \rangle \\ &\equiv \langle \alpha_0, \ldots, \alpha_n \rangle \cdot \langle \beta_0, \ldots, \beta_m \rangle \end{aligned} \tag{5}$$

is much more involved than (4), but gives us the well-definedness of $\_ \cdot\cdot \_$ on the quotient. Proving the lattice laws also proceeds by using (4) and (5), together with the equivalence of $\sim$ and $\approxeq$, thus reducing these laws to special cases of standard equalities about ideal addition/multiplication and radical ideals.

Showing the universal property of $\mathcal{L}_R$ is then relatively straightforward. Note that the basic opens are defined by the map $D : R \to \mathcal{L}_R$, sending $f : R$ to $[\,[f]\,]$, the equivalence class of the singleton list $[f]$. It then becomes straightforward to verify that for $f, g : R$

$$D(g) \leq D(f) \;\Leftrightarrow\; \sqrt{\langle g \rangle} \subseteq \sqrt{\langle f \rangle} \;\Leftrightarrow\; f \in R[1/g]^\times \;\Leftrightarrow\; \mathsf{isContr}\Big(\mathrm{Hom}_R\big[R[1/f]\,,\, R[1/g]\,\big]\Big)$$

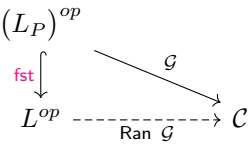
The last two logical equivalences hold by some standard commutative algebra and the universal property of localization.[7] The basic opens as a subset of $\mathcal{L}_R$ are defined as the function $\mathsf{BasicOpens} : \mathcal{L}_R \to \mathsf{hProp}$, sending $\mathfrak{a}$ to $\exists[\; f \in R \;]\; (D(f) \equiv \mathfrak{a})$. In other words $\mathfrak{a} \in \mathsf{BasicOpens}$ if there merely exists an f such that $\mathfrak{a}$ equals $D(f)$. The type of basic opens is then the type $\mathcal{B}_R = \Sigma[\; \mathfrak{a} \in \mathcal{L}_R \;]\; (\mathfrak{a} \in \mathsf{BasicOpens})$. Note that by the universal property, the only lattice morphism $\mathcal{L}_R \to \mathcal{L}_R$ commuting with D is the identity and from this it follows that for any list $\alpha = [\alpha_0, \ldots, \alpha_n]$ the equivalence class $[\,\alpha\,]$ is the finite join $\bigvee_{i=0}^{n} D(\alpha_i)$. Since being a basis is a proposition, this is enough to prove that the basic opens form a basis of $\mathcal{L}_R$.

4 Category theory

We now turn to category theory and describe the machinery needed to lift sheaves from the basis of a distributive lattice to the whole lattice. The lifting of a presheaf defined on a subset of a distributive lattice, seen as a sub-poset category, is obtained by taking the right Kan extension along the inclusion. The general theory of limits and Kan extensions in the formalization closely follows Mac Lane [23]. We will not discuss details here, but only sketch the lattice case in order to introduce notation and show where size issues enter the picture.

Note that for any category $\mathcal{C}$ and $P : \mathcal{C} \to \mathsf{hProp}$, $\mathcal{C}_P = \Sigma[\; x \in \mathcal{C} \;]\; (x \in P)$ becomes a subcategory of $\mathcal{C}$ by taking arrows between pairs to be arrows between the first projections. The projection fst induces a fully faithful embedding of $\mathcal{C}_P$ into $\mathcal{C}$. Let us now fix a distributive lattice $L : \mathsf{Type}\ \ell$. For any $P : L \to \mathsf{hProp}\ \ell$, L_P becomes a sub-poset of L.

Let $\mathcal{C}$ be an ℓ-complete category (i.e. with limits of diagrams in $\mathsf{Type}\ \ell$). The right Kan extension then exists for any $\mathcal{C}$-valued presheaf $\mathcal{G}$ on L_P:



$$\big(\mathsf{Ran}\ \mathcal{G}\big)\,(x) \;=\; \varprojlim \big\{\, \mathcal{G}(u) \to \mathcal{G}(v) \mid u, v : L_P \text{ s.t. } v \leq u \leq x \,\big\}$$

[7] As all the types above are propositions, we could also replace logical equivalence with equivalence of types $\simeq$.

Moreover, since the functor induced by fst is fully faithful, Ran $\mathcal{G}$ extends $\mathcal{G}$ in the sense that we have a natural isomorphism between $\mathcal{G}$ and $(\mathsf{Ran}\ \mathcal{G}) \circ \mathsf{fst}$. For the structure sheaf we need to consider presheaves valued in CommRing ℓ, the category of commutative rings living in the same universe as the base ring R. This category is ℓ-complete but *not* $(\ell+1)$-complete. It is precisely for this reason that we required $\mathcal{L}_R$ to be in Type ℓ.

The main result of this section is that taking the right Kan extension of a presheaf defined on the *basis* of a lattice preserves the sheaf property.[8] This requires a definition of sheaf on both distributive lattices and their bases suitable for formalization. For the remainder of this section we fix a basis B of L. When outlining the formalization, we defined sheaves on lattices by restricting the usual definition in terms of equalizer diagrams to finite covers. However, we can express these equalizers as finite limits over diagrams of a certain shape.[9] This approach is also taken by Coquand, Lombardi and Schuster in [10]. We decided to follow it as it allows one to work with special data types for the shapes of the diagrams involved, which is convenient in the formalization.

▶ **Definition 4** (Sheaf diagram shapes). *The category of the sheaf diagram shape for covers of size n, has as objects indices i, where $1 \leq i \leq n$, or pairs of indices (i, j), where $1 \leq i < j \leq n$. Arrows are either identity arrows or inclusions of singleton indices from the left $i \mapsto (i, j)$ or right $j \mapsto (i, j)$.*

In `Agda` the objects and arrows can be described as the terms of the following data types:

```
data DLShfDiagOb (n : ℕ) : Type where
  sing : Fin n → DLShfDiagOb n
  pair : (i j : Fin n) → i < j → DLShfDiagOb n

data DLShfDiagHom (n : ℕ) : DLShfDiagOb n → DLShfDiagOb n → Type where
  idAr : {x : DLShfDiagOb n} → DLShfDiagHom n x x
  singPairL : {i j : Fin n} {p : i < j} → DLShfDiagHom n (sing i) (pair i j p)
  singPairR : {i j : Fin n} {p : i < j} → DLShfDiagHom n (sing j) (pair i j p)
```

Here Fin n is the finite type of n elements from 1 to n. Composition is easily defined by case analysis as it is not possible to compose two non-identity arrows and the laws then follow directly. We denote the resulting category by DLShfDiagCat n.

▶ Remark 5. In order for this to define a category in HoTT/UF we have to prove that the hom-types are sets, i.e. that for x, y : DLShfDiagOb n we have isSet (DLShfDiagHom n x y). This follows from a retraction argument using the encode-decode method [33].

Given a list of elements $\alpha = [\alpha_1, \ldots, \alpha_n]$ with $\alpha_i : L$, we get a corresponding diagram in the form of a functor DLShfDiagCat $n \to L^{op}$ sending the singleton index i to α_i and (i, j) to $\alpha_i \wedge \alpha_j$. We call this the *diagram associated to* α. Furthermore, let $\mathcal{F} : L^{op} \to \mathcal{C}$ be a presheaf, we then have a diagram DLShfDiagCat $n \to \mathcal{C}$, obtained by composing the diagram associated to α with $\mathcal{F}$. We call this the *$\mathcal{F}$-diagram associated to* α.

The join $\bigvee_{i=1}^{n} \alpha_i$ induces a cone over the diagram associated to α and it is in fact a limiting cone because limits are least upper bounds in the opposite of a poset category. A presheaf on L is a sheaf if it preserves these limits:

[8] In fact the right Kan extension (as opposed to left Kan) establishes an equivalence of categories between sheaves on a lattice L and sheaves on a basis B of L, with its inverse being restriction to B. This is the special case of the so-called *comparison lemma* for distributive lattices.

[9] See e.g. Mac Lane [23, Thm. V.2.1].

▶ **Definition 6** (Sheaves on a distributive lattice). *We say that $\mathcal{F}$ is a sheaf on the distributive lattice L, if for all lists $\alpha = [\alpha_1, \ldots, \alpha_n]$ with $\alpha_i : L$ the induced cone of $\mathcal{F}\big(\bigvee_{i=1}^n \alpha_i\big)$ over the $\mathcal{F}$-diagram associated to α is a limiting cone. In other words $\mathcal{F}\big(\bigvee_{i=1}^n \alpha_i\big)$ is the limit of the diagram*

$$\begin{array}{ccccc} & & \mathcal{F}\big(\bigvee_{i=1}^n \alpha_i\big) & & \\ & \swarrow & \downarrow & \searrow & \\ \mathcal{F}(\alpha_i) & \longrightarrow & \mathcal{F}(\alpha_i \wedge \alpha_j) & \longleftarrow & \mathcal{F}(\alpha_j) \end{array} \qquad \text{for all} \quad 1 \leq i < j \leq n.$$

We now turn our attention to the corresponding notion for the basis B. Let $\mathcal{G} : B^{op} \to \mathcal{C}$ be a presheaf. For a list $\alpha = [\alpha_1, \ldots, \alpha_n]$ with $\alpha_i : B$, we have a diagram DLShfDiagCat $n \to \mathcal{C}$, which is obtained by composing the diagram associated to α with $\mathcal{G}$. We call this the *$\mathcal{G}$-diagram associated to α*. As B is in general not closed under finite joins, the definition of a basis-sheaf below has an extra condition, saying that limits of the associated diagrams are only preserved if they exist.

▶ **Definition 7** (Sheaves on a basis of a distributive lattice). *We say that $\mathcal{G}$ is a sheaf on the basis B of a distributive lattice, if for all $\alpha = [\alpha_1, \ldots, \alpha_n]$ with $\alpha_i : B$, such that $\bigvee_{i=1}^n \alpha_i$ is in B, the induced cone of $\mathcal{G}\big(\bigvee_{i=1}^n \alpha_i\big)$ over the $\mathcal{G}$-diagram associated to α is a limiting cone.*

The following lemma only holds for sheaves on the whole lattice, since it requires closure under finite joins.

▶ **Lemma 8.** *Let $\mathcal{F} : L^{op} \to \mathcal{C}$, then $\mathcal{F}$ is sheaf if and only if $\mathcal{F}(\bot)$ is terminal in $\mathcal{C}$ and for all $x, y : L$ the following is a pullback square*

$$\begin{array}{ccc} \mathcal{F}(x \vee y) & \longrightarrow & \mathcal{F}(x) \\ \downarrow & \lrcorner & \downarrow \\ \mathcal{F}(y) & \longrightarrow & \mathcal{F}(x \wedge y) \end{array}$$

Proof. We start by observing that Definition 6 also applies to the empty list []. The join over [] is just $\bot$ and the associated diagram is the "empty" diagram. So if $\mathcal{F}$ is a sheaf then $\mathcal{F}(\bot)$ is terminal. Furthermore, the pullback squares are exactly the sheaf condition for two element lists. This concludes the "only if" direction.

For the other direction, we proceed by induction on the length n. The base case $n = 0$ follows from $\mathcal{F}(\bot)$ being terminal. For the inductive step take a list $\alpha_1, \ldots, \alpha_n : L$ of length n. By assumption the following is a pullback square

$$\begin{array}{ccc} \mathcal{F}\big(\bigvee_{i=1}^n \alpha_i\big) & \longrightarrow & \mathcal{F}\big(\bigvee_{i=2}^n \alpha_i\big) \\ \downarrow & \lrcorner & \downarrow \\ \mathcal{F}(\alpha_1) & \longrightarrow & \mathcal{F}\big(\bigvee_{i=2}^n (\alpha_1 \wedge \alpha_i)\big) \end{array}$$

Now both lists $\alpha_1, \ldots, \alpha_n$ and $\alpha_1 \wedge \alpha_1, \ldots, \alpha_1 \wedge \alpha_n$ are of length $n - 1$. By applying the induction hypothesis to both, one can easily check that $\mathcal{F}\big(\bigvee_{i=1}^n \alpha_i\big)$ is the desired limit. ◀

This alternative characterization can be used to prove our "comparison lemma" for distributive lattices. For the remainder of this section, let $\mathcal{G} : B^{op} \to \mathcal{C}$ be a sheaf on the basis B. The key observation is the following technical lemma.

▶ **Lemma 9.** *For any list of elements $\alpha_1, \ldots, \alpha_k : B$, we have that*[10]

$$\big(\mathsf{Ran}\ \mathcal{G}\big)\big(\bigvee_{i=1}^{k} \alpha_i\big) \ \cong\ \varprojlim \ \big\{\, \mathcal{G}(\alpha_i) \to \mathcal{G}(\alpha_i \wedge \alpha_j) \leftarrow \mathcal{G}(\alpha_j) \mid 1 \le i < j \le k \,\big\} \tag{6}$$

Proof sketch. By definition we have

$$\big(\mathsf{Ran}\ \mathcal{G}\big)\big(\bigvee_{i=1}^{k} \alpha_i\big) \ =\ \varprojlim \ \big\{\, \mathcal{G}(u) \to \mathcal{G}(v) \mid u, v : B \text{ s.t. } v \le u \le \bigvee_{i=1}^{k} \alpha_i \,\big\}$$

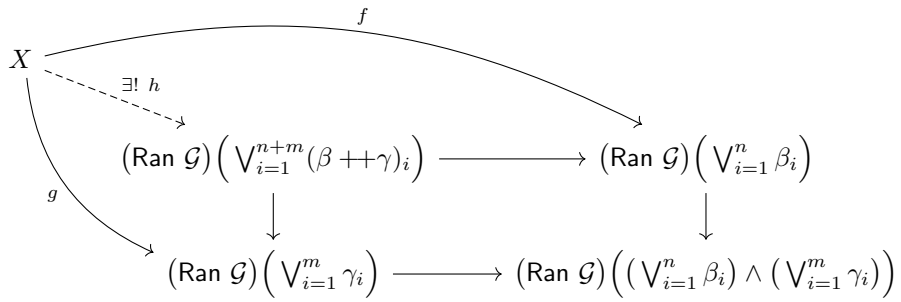
This immediately gives us the map from left to right, since we can restrict the defining diagram of $\big(\mathsf{Ran}\ \mathcal{G}\big)\big(\bigvee_{i=1}^{k} \alpha_i\big)$ to the $\mathcal{G}$-diagram associated to α.

For the inverse map we have to show that given any $X : \mathcal{C}$ with a cone based at X over the $\mathcal{G}$-diagram associated to α, we can extend this to a cone based at X over the defining diagram of $\big(\mathsf{Ran}\ \mathcal{G}\big)\big(\bigvee_{i=1}^{k} \alpha_i\big)$. Assume we have $X : \mathcal{C}$ with such a cone and let $u : B$ such that $u \le \bigvee_{i=1}^{k} \alpha_i$. Then $\bigvee_{i=1}^{k}(u \wedge \alpha_i) \equiv u$ and hence $\bigvee_{i=1}^{k}(u \wedge \alpha_i)$ is in B. This means that we can apply the assumption that $\mathcal{G}$ is a sheaf to this join. By substituting along this path, we can see $\mathcal{G}(u)$ as the limit of the $\mathcal{G}$-diagram associated to the $u \wedge \alpha_i$'s. By composing with restrictions we get a cone based at X over the $\mathcal{G}$-diagram associated to the $u \wedge \alpha_i$'s, and thus an arrow $X \to \mathcal{G}(u)$. It is not hard to show that this is functorial in u, which gives us the desired inverse arrow. The proof that the two maps are mutually inverse, is quite cumbersome and we will omit it here. ◀

The proof of the following theorem is the most technical of the entire formalization, so again we only give an outline.

▶ **Theorem 10.** $\mathsf{Ran}\ \mathcal{G}$ *is a sheaf on the distributive lattice L.*

Proof sketch. It suffices to check the terminal and pullback condition of Lemma 8. We will restrict our attention to the pullback case here. Let $x, y : L$ and note that, as being a pullback square is a proposition, we can take covers $x \equiv \bigvee_{i=1}^{n} \beta_i$ and $y \equiv \bigvee_{i=1}^{m} \gamma_i$ by base elements, i.e. $\beta_i, \gamma_j : B$ for all i and j. Substituting these covers for x and y, we have to prove the following: given $X : \mathcal{C}$ and arrows f and g such that the outer square in the diagram below commutes, then there is a unique arrow h making the whole diagram commute:



(7)

Here $(\beta +\!\!+ \gamma)$ is the list-concatenation of β and γ. Applying Lemma 9 to $(\beta +\!\!+ \gamma)$, we get such an arrow h from a cone based at X over the diagram

$$\big\{\, \mathcal{G}\big((\beta +\!\!+ \gamma)_i\big) \to \mathcal{G}\big((\beta +\!\!+ \gamma)_i \wedge (\beta +\!\!+ \gamma)_j\big) \leftarrow \mathcal{G}\big((\beta +\!\!+ \gamma)_j\big) \mid 1 \le i < j \le n + m \,\big\}$$

[10] This is actually how the extension $\big(\mathsf{Ran}\ \mathcal{G}\big)$ is defined in [10]. However, in general we cannot use concrete covers of arbitrary elements of L by base elements to construct a functor into $\mathcal{C}$ if its h-level is unknown.

To construct such a cone, we apply Lemma 9 to both β and γ and precompose the resulting limiting cones with f and g respectively. This gives us two cones based at X, one over the $\mathcal{G}$-diagram associated to β and the other one over the $\mathcal{G}$-diagram associated to γ. Note that the two cones are compatible in the following sense: for all $1 \leq i \leq n$ and $1 \leq j \leq m$ the following square commutes

$$\begin{array}{ccc} X & \longrightarrow & \mathcal{G}(\beta_i) \\ \downarrow & & \downarrow \\ \mathcal{G}(\gamma_j) & \longrightarrow & \mathcal{G}(\beta_i \wedge \gamma_j) \end{array}$$

This is because the outer square in diagram (7) commutes and it is sufficient to construct a cone based at X over the $\mathcal{G}$-diagram associated to $(\beta +\!\!+ \gamma)$.

Note that the induced h is the unique cone morphism between the cone thus constructed and the limiting cone obtained from applying Lemma 9 to $(\beta +\!\!+ \gamma)$. Moreover, f and g are the unique cone morphisms between their respective precomposition-cones based at X and the limiting cones obtained from applying Lemma 9 to β and γ respectively. From this it follows by a cumbersome diagram chase that h is the unique morphism making the two triangles in diagram (7) commute. ◀

Formalizing the gaps in the above proof sketches is quite tedious and uses involved transports. We refer the interested reader to the formalization.

5 The structure sheaf

We now have all the ingredients needed to formalize the structure sheaf. The basic opens $\mathcal{B}_R$ form a basis of $\mathcal{L}_R$ and we have seen in the previous section how sheaves can be extended along the embedding $\mathsf{fst} : \mathcal{B}_R \to \mathcal{L}_R$. What should the structure sheaf on $\mathcal{B}_R$ then look like? Focusing on the underlying presheaf and its action on objects for now, we need a function $\mathcal{B}_R \to \mathsf{CommRing}\ \ell$, which upon unfolding the definition of $\mathcal{B}_R$ becomes

$$\big(\Sigma[\ \mathfrak{a} \in \mathcal{L}_R\ ]\ \underbrace{\exists[\ f \in R\ ]\ (D(f) \equiv \mathfrak{a})}_{\text{prop. trunc.}}\big) \longrightarrow \underbrace{\mathsf{CommRing}\ \ell}_{\text{groupoid}}$$

Since membership in $\mathcal{B}_R$ is defined as a mere existence condition using propositional truncation, we can only specify the behavior of the structure sheaf in the case where we are given a point constructor of this truncation. If $\mathfrak{a} : \mathcal{L}_R$ is a basic open, such an element of the truncation consists of an element $f : R$ and a path $p : D(f) \equiv \mathfrak{a}$. In this case we know that the structure sheaf should send $(\ \mathfrak{a}\ ,\ |\ f\ ,\ p\ |\ )$ to $R[1/f]$. If the goal type were a proposition, this would be enough to specify a function. However, the type of commutative rings is a groupoid, requiring us to construct some non-trivial higher coherences.

To circumvent this problem we use the observation that the localizations are actually R-algebras and that we could regard the structure sheaf as taking values in R-algebras. What is usually called the structure sheaf in the literature is this R-algebra-valued sheaf composed with the forgetful functor to commutative rings. In other words, the structure sheaf factors through the forgetful functor from R-algebras to commutative rings. The single reason why the situation is more well-behaved in R-algebras is the fact that

$$D(g) \leq D(f) \iff \mathsf{isContr}\Big(\mathrm{Hom}_R\big[R[1/f]\,,\ R[1/g]\,\big]\Big)$$

Contractibility is a powerful concept in HoTT/UF and we will show how this can be used to solve the coherence issues of the structure sheaf and gives rise to a reduction argument for the sheaf property. We start with two lemmas for general constructions involving propositional truncations and R-algebras. Note that these results are pretty much tailored to the situation of the structure sheaf, but should also hold for other univalent categories, which are always groupoids and even sets if they are posetal [33, Lemma 9.1.9, Ex. 9.1.14]. With a bit of abuse of notation we will use R-Alg to denote both the type and the category of R-algebras.

▶ **Lemma 11.** *Let X : Type and $\mathcal{F} : X \to R$-Alg. Assume further that for $x, y : X$ we have an isomorphism of R-algebras $\varphi_{xy} : \mathcal{F}(x) \cong \mathcal{F}(y)$ such that for $x, y, z : X$ we have a path $\varphi_{xz} \equiv \varphi_{yz} \circ \varphi_{xy}$. Then we can construct a map $\|\mathcal{F}\| : \| X \| \to R$-Alg such that for $x : X$ we have $\|\mathcal{F}\|(|\ x\ |) = \mathcal{F}(x)$ definitionally.*

Proof. Since R-Alg is a groupoid, we can apply a result by Kraus [20, Prop. 2.3]. In order to construct $\|\mathcal{F}\|$ we need a family of paths over any two elements of X satisfying a certain coherence condition. For $x, y : X$ we get a path sip $\varphi_{xy} : x \equiv y$. The corresponding coherence condition states that for $x, y, z : X$, we need a path sip $\varphi_{xz} \equiv$ sip $\varphi_{xy} \bullet$ sip φ_{yz} (where $\_\bullet\_$ is path composition). By the functoriality of sip, which follows from the functoriality of ua, this path type is equivalent to sip $\varphi_{xz} \equiv$ sip $(\varphi_{yz} \circ \varphi_{xy})$. But by assumption we have $\varphi_{xz} \equiv \varphi_{yz} \circ \varphi_{xy}$, so by applying sip to this path we are done. ◀

For the next lemma, note that for any category $\mathcal{C}$ and family $P : \mathcal{C} \to$ Type, we have the subcategory $\mathcal{C}_{\|P\|}$ of $\mathcal{C}$ induced by $\lambda\ x \to \| P(x) \| : \mathcal{C} \to$ hProp.

▶ **Lemma 12.** *Let $\mathcal{C}$ be a category with a family $P : \mathcal{C} \to$ Type and a family of R-algebras $\mathcal{F} : \big(\Sigma[\ x \in \mathcal{C}\ ]\ P(x)\big) \to R$-Alg. Assume furthermore that for $x, y : \mathcal{C}$, $p : P(x)$, $q : P(y)$ with an arrow $f : \mathcal{C}\,[x, y]$ we have*

$$\mathit{isContr}\Big(\mathit{Hom}_R\big[\mathcal{F}(y\ ,\ q)\,,\ \mathcal{F}(x\ ,\ p)\big]\Big)$$

We can then construct a "universal" presheaf

$$\mathcal{P}_u : \big(\mathcal{C}_{\|P\|}\big)^{op} \to R\text{-}\mathit{Alg}$$

such that for $x : \mathcal{C}$ with $p : P(x)$ we have

$$\mathcal{P}_u(x\ ,\ |\ p\ |) = \mathcal{F}(x\ ,\ p)$$

definitionally, and for $y : \mathcal{C}$, $q : P(y)$ with arrow $f : \mathcal{C}\,[x, y]$, $\mathcal{P}_u\,(f)$ is the unique R-algebra morphism from $\mathcal{F}(y\ ,\ q)$ to $\mathcal{F}(x\ ,\ p)$.

Proof. We first describe the action of $\mathcal{P}_u$ on objects. By currying we fix $x : \mathcal{C}$ and need to provide a function $\| P(x) \| \to R$-Alg. For this we apply Lemma 11 to $\mathcal{F}(x\ ,\ \_) : P(x) \to R$-Alg. From our contractibility assumption it follows that given $p, q : P(x)$ there are unique morphisms from $\mathcal{F}(x\ ,\ p)$ to $\mathcal{F}(x\ ,\ q)$ and vice versa, so $\mathcal{F}(x\ ,\ p) \cong \mathcal{F}(x\ ,\ q)$. It remains to check that the family of isomorphisms thus defined is closed under composition in the sense of Lemma 11. Again, this follows from contractibility.

For the action of $\mathcal{P}_u$ on morphisms, we start by proving something stronger. Given $x, y : \mathcal{C}$, $p : \| P(x) \|$, $q : \| P(y) \|$ with an arrow $f : \mathcal{C}[x, y]$, we have:

$$\mathsf{isContr}\ \Big(\mathrm{Hom}_R\ \big[\ \mathcal{P}_u(x\ ,\ p)\ ,\ \mathcal{P}_u(y\ ,\ q)\ \big]\Big)$$

As being contractible is a proposition, we can assume that $p = |\ p'\ |$ and $q = |\ q'\ |$. In this case $\mathcal{P}_u(x\ ,\ p) = \mathcal{F}(y\ ,\ p')$ and $\mathcal{P}_u(y\ ,\ q) = \mathcal{F}(y\ ,\ q')$ and we can just use our contractibility hypothesis. Since a morphism between $(x\ ,\ p)$ and $(y\ ,\ q)$ in $\mathcal{C}_{\|P\|}$ is just a morphism $f : \mathcal{C}[x, y]$, we can take $\mathcal{P}_u(f)$ to be the center of contraction of the contractible type of R-algebra morphisms above. The functoriality of $\mathcal{P}_u$ then follows immediately. ◀

We now want to apply this construction to the Zariski lattice (seen as a poset category). In the situation of Lemma 12 with $\mathcal{C} = \mathcal{L}_R$ we set, for $\mathfrak{a} : \mathcal{L}_R$:

$$P(\mathfrak{a}) \ = \ \Sigma[\ f \in R\ ]\ (D(f) \equiv \mathfrak{a}) \qquad \text{and} \qquad \mathcal{F}(\mathfrak{a}\ ,\ f\ ,\ p) \ = \ R[1/f].$$

If we are given $\mathfrak{b} \leq \mathfrak{a}$ with $D(f) \equiv \mathfrak{a}$ and $D(g) \equiv \mathfrak{b}$ then $D(g) \leq D(f)$ and the type of R-algebra morphisms from $R[1/f]$ to $R[1/g]$ is contractible. This way we obtain the desired

$$\mathcal{P}_u : (\mathcal{B}_R)^{op} \to R\text{-Alg}$$

Composing with the forgetful functor from R-algebras to commutative rings gives us the desired presheaf on basic opens, denoted by $\mathcal{O}^B$. From this we finally obtain the structure (pre-)sheaf $\mathcal{O} : (\mathcal{L}_R)^{op} \to \mathsf{CommRing}$ using the right Kan extension machinery described in Section 4. The following fact then becomes rather straightforward to verify:

▶ **Proposition 13.** *For any $f : R$ we get a path $\mathcal{O}(D(f)) \equiv R[1/f]$.*

Proof. There is a canonical proof $p_f = |\ f\ ,\ \mathsf{refl}\ |$ of $D(f)$ belonging to the basic opens. Since we have a natural isomorphism between $\mathcal{O}^B$ and $\mathcal{O} \circ \mathsf{fst}$, we can use the SIP for commutative rings to obtain a path $\mathcal{O}(D(f)) \equiv \mathcal{O}^B(D(f)\ ,\ p_f)$. But in R-algebras $\mathcal{P}_u(D(f)\ ,\ p_f)$ equals $R[1/f]$ definitionally and applying the forgetful functor to this gives us $R[1/f]$ as a commutative ring (unfortunately not by refl). ◀

As a corollary we obtain the standard sanity check:

▶ **Corollary 14.** $\mathcal{O}(\top_{\mathcal{L}_R}) \equiv \mathcal{O}(D(1)) \equiv R$.

Proof. $D(1)$ is the top element of the Zariski lattice by definition, so the first path is just refl. By Proposition 13 we get that $\mathcal{O}(D(1)) \equiv R[1/1]$. Combining this with Lemma 3.2, we get the desired path. ◀

It remains to prove that $\mathcal{O}^B$ is indeed a sheaf. At this point the standard strategy is to reduce the general case of a cover $D(h) \equiv \bigvee_{i=1}^{n} D(f_i)$ to the special case $h = 1$ and then proceed by some algebraic computations in the rings $R[1/f_i]$.[11] Informally this reduction step follows from a short argument, but it identifies certain localizations by appealing to their canonical isomorphisms. Making this formal in a system without univalence requires to take the isomorphisms at face value and results in cumbersome diagram chases. This problem is described in detail in [4]. There the ultimate breaking point was identifying the rings $R[1/f][1/g]$ and $R[1/fg]$. As the authors point out, simply providing a path between those rings does not solve the problem at hand, since what is actually needed is a path between the diagrams occurring in the sheaf condition. For the remainder of this section we want to show that we can conclude that $\mathcal{O}^B$ is a sheaf from the aforementioned special case, using the observation that the canonical morphisms are unique in R-algebras. In our formalization, the special case of covers of $D(1)$ reads as follows:

[11] See for example [15, theorem 2.33.], [13, theorem 1.3.7] or [18, theorem V.3.3]. Note that in these classical textbooks the sheaf property only has to be verified for finite covers because basic opens are quasi-compact. In contrast, we are restricted to finite covers by definition.

▶ **Lemma 15.** *For a ring A with $f_1, \dots, f_n : A$ such that $1 \in \langle f_1, \dots, f_n \rangle$, we have*

$$A \equiv \varprojlim \left\{ A[1/f_i] \to A[1/f_i f_j] \leftarrow A[1/f_j] \mid 1 \le i < j \le n \right\}$$

More precisely, the canonical cone of A over the diagram above is a limiting cone.

Proof. The proof follows closely the textbook approach, see e.g. Mac Lane and Moerdijk [24, p. 125], by some hands-on algebra in the different rings involved. It is precisely at this point that working with concrete implementations of the $A[1/f_i]$ as set quotients really simplifies the formalization. ◀

Reducing the sheaf property of $\mathcal{O}^B$ to Lemma 15 can now be done using the special nature of $\mathcal{P}_u$. We also need that the forgetful functor preserves and reflects limits and some basic results about dependent paths. In the library this is packaged up in a generalized, technical lemma, working for arbitrary diagrams, not only those needed for the sheaf property. For the sake of readability however, we proceed to prove our main result directly.

▶ **Theorem 16.** *$\mathcal{O}^B$ is a sheaf on the basic opens.*

Proof. Again for readability, we restrict ourselves to the case of binary covers, i.e. the situation where $D(h) \equiv D(f) \vee D(g)$ for $f, g, h : R$. As described in the proof of Lemma 8, in this case the sheaf property can be reformulated as stating that sq below is a pullback.

$$\begin{array}{ccc} \mathcal{O}^B\big(D(h)\,,\,p_h\big) & \longrightarrow & \mathcal{O}^B\big(D(g)\,,\,p_g\big) \\ \downarrow & \mathsf{sq} & \downarrow \\ \mathcal{O}^B\big(D(f)\,,\,p_f\big) & \longrightarrow & \mathcal{O}^B\big(D(fg)\,,\,p_{fg}\big) \end{array} \qquad \begin{array}{ccc} R[1/h] & \longrightarrow & R[1/g] \\ \downarrow & \mathsf{sq}_R & \downarrow \\ R[1/f] & \longrightarrow & R[1/fg] \end{array}$$

Here the p's are, as in the proof of Proposition 13, the canonical proofs that the D's are in fact basic opens. Note that by definition, sq is obtained by applying the forgetful functor to sq_R and since the forgetful functor *preserves limits* (and in particular pullbacks) it suffices to prove that sq_R is a pullback in R-algebras.

The assumption $D(h) \equiv D(f) \vee D(g)$ gives us $\sqrt{\langle h \rangle} \equiv \sqrt{\langle f, g \rangle}$ and by some standard algebra $1 \in \langle f/1, g/1 \rangle$ in $R[1/h]$. This lets us apply Lemma 15 with $A = R[1/h]$ and we get that sq^* is a pullback (in rings):

$$\begin{array}{ccc} R[1/h] & \longrightarrow & R[1/h][1/g] \\ \downarrow & \mathsf{sq}^* & \downarrow \\ R[1/h][1/f] & \longrightarrow & R[1/h][1/fg] \end{array}$$

As all the vertices of sq^* are R-algebras, by the canonical morphisms coming from R, and all the edges of sq^* commute with these canonical morphisms, we can lift sq^* to a square sq^*_R in R-algebras. Since the forgetful functor *reflects limits* (and thus pullbacks), we get that sq^*_R is a pullback square as well.

All that we need is a path $\mathsf{sq}^*_R \equiv \mathsf{sq}_R$ and we are done, as we can transport *the property of being a pullback square* along this path of squares. It is immediate in `Cubical Agda` that to give a path between squares we need to give four paths between the respective vertices and four dependent paths between the morphisms over the paths of vertices. In order to see how this applies to our situation, let us first look at the left side of sq^*_R and sq_R. We get the following square where we have to provide paths at the top and bottom and a dependent path filling this square connecting the vertical arrows ψ and φ:

$$\begin{array}{ccc} R[1/h] & = & R[1/h] \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ R[1/h][1/f] & = & R[1/f] \end{array}$$

For the top path we just choose refl. For the bottom we apply Lemma 3 and get a path

$$R[1/h][1/f] \equiv R[1/hf] \equiv R[1/f]$$

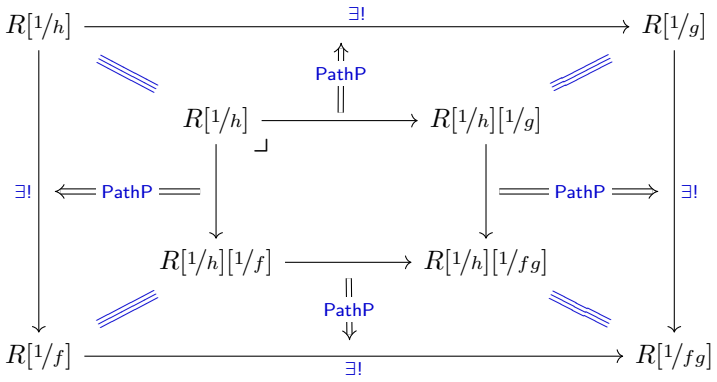
where the first path is just Lemma 3.1 and the second path is Lemma 3.2 using the fact that $D(hf) \equiv D(f)$ by absorption. Let p denote the composition of these two paths. The dependent path between ψ and φ is then of type

$$\mathsf{PathP}\ \Big(\lambda\ i \to \mathrm{Hom}_R\big[R[1/h]\,,\ p\ i\,\big]\Big)\ \psi\ \varphi$$

By a standard result about PathP, this is equivalent to the non-dependent path type

$$\mathsf{transport}\ \Big(\lambda\ i \to \mathrm{Hom}_R\big[R[1/h]\,,\ p\ i\,\big]\Big)\ \psi \equiv \varphi$$

But by definition φ is the center of contraction of the type $\mathrm{Hom}_R\big[R[1/h]\,,\ R[1/f]\,\big]$. By contractibility, we hence get a path to the transport of ψ and thus the desired dependent path. Repeating this strategy four times, as described in the diagram below, gives us the desired path $\mathsf{sq}^*_R \equiv \mathsf{sq}_R$ and finishes the proof.



◀

Combining this with Theorem 10 we get:

▶ **Corollary 17.** *$\mathcal{O}$ is a sheaf on the Zariski lattice $\mathcal{L}_R$.*

Most of the argument in the proof of Theorem 16, including the crucial transport goes through for the general $\mathcal{P}_u$ construction and cones over *arbitrary diagrams*. If we take the action of $\mathcal{P}_u$ on any cone of any shape, we only need two things for establishing that this is a limiting cone: first, a limiting cone in R-algebras of the same shape and second, a family of paths between the corresponding vertices of the two cones. In the case of structure sheaf the limiting cone is provided by Lemma 15 and the paths are provided by Lemma 3. As a matter of fact, the general case is actually easier to formalize and computationally better behaved, even though the pullback case is easier to visualize.

6 Conclusion

In this paper we presented a fully constructive and predicative formalization of the structure sheaf on the Zariski lattice in `Cubical Agda`. To this end, we gave a construction of the Zariski lattice associated to a commutative ring that does not increase the universe level even when working predicatively. We formalized the notion of sheaf on a distributive lattice and formally proved the first steps towards a "comparison lemma" for distributive lattices. In particular, we showed how to extend a sheaf defined on the basis of a lattice, and taking values in any complete category, to a sheaf on the whole lattice. Applying this to the Zariski lattice we then constructed the structure sheaf on its basis. We had to solve higher coherence conditions in order to show that this construction is well-defined. The main insight was that by essentially regarding the structure sheaf to be valued in algebras, not rings, we could use contractibility to solve the coherence issues. Furthermore, it was the same contractibility result that let us formalize the textbook proof of the sheaf property with the help of some univalent machinery.

As discussed in the introduction nothing in the paper crucially relied on cubical features, but they proved convenient in the formalization. In particular, having more things holding by refl, eliminators computing also for higher constructors, and having direct access to dependent paths in the form of PathP types simplified many of the formal proofs. We hope nevertheless that the main ideas introduced in this paper could prove useful for formalizations in other systems. For the remainder of this paper we want to make a few comments that should help putting our work into context.

6.1 Comparison to the classical definition of affine schemes

Even though the constructive, predicative approach described in this paper is similar to the standard, classical textbook approach to affine schemes in the sense that it involves a "lifting" from basic opens, it might not be immediately clear whether we loose anything by working with the Zariski lattice and finitary lattice sheaves. As mentioned in the introduction, from a classical perspective this is not the case because $\mathsf{Spec}\, R$ is a *coherent* space. A topological space X is coherent if it is *compact*, *sober* (its non-empty irreducible closed subsets are the closure of a single point), and its compact opens are closed under finite intersections and form a basis of the topology of X. A coherent map between coherent spaces X and Y is a continuous map $f : X \to Y$ such that for any compact open $K \subseteq Y$, its pre-image $f^{-1}(K)$ is compact as well. Stone's representation theorem for distributive lattices [29] states that the functor from the category of coherent spaces with coherent maps to distributive lattices, sending a coherent space to the lattice of its compact opens, is an equivalence of categories.[12] For the inverse direction we take a distributive lattice and recover the opens of the corresponding space by taking *ideals* on that lattice. We can even recover the points of the space by taking *prime filters* on the lattice. In the case of $\mathsf{Spec}\, R$ the prime filters of $\mathcal{L}_R$ are just the complements of prime ideals of R.[13]

The approach of defining $\mathcal{L}_R$ through formal generators $D(f)$ and obtaining the locale of Zariski opens as the ideals of $\mathcal{L}_R$, is taken in Johnstone's "Stone Spaces" [18, Chap. V.3]. The structure sheaf on the resulting locale of $\mathcal{L}_R$-ideals can then be constructed by only defining it on the base elements $D(f)$. In our predicative and constructive setting we only extend the

[12] Furthermore, any coherent space is coherently homeomorphic to $\mathsf{Spec}\, R$ for some ring R [17], i.e. Spec as a functor from commutative rings to coherent spaces is essentially surjective.
[13] See also the discussion by Coquand, Lombardi and Schuster in the introduction of [9].

structure sheaf construction on basic opens to $\mathcal{L}_R$. Again, classically no information is lost. Whether one considers the structure sheaf to be defined on $\mathsf{Spec}\, R$ as a topological space, on the locale of $\mathcal{L}_R$-ideals or only on $\mathcal{L}_R$, it is determined (up to unique isomorphism) by what happens at the level of basic opens.

More generally, for any coherent space X, the category of sheaves on X is equivalent to the category of (finitary) lattice-sheaves on the compact opens of X. This follows from the comparison lemma for topological spaces, which gives us an equivalence between sheaves on X and sheaves on the basis of compact opens of X. But since the compact opens are all compact we only have to consider finite covers for the sheaf property, which gives us the equivalence to lattice-sheaves on compact opens. Formalizing this classical fact would certainly be interesting in its own right. But as we are interested in the formalization of constructive mathematics, we will just see this fact as a justification that the notion of constructive affine scheme that we arrive at is not fundamentally weaker than the standard classical definition.

6.2 Existing formalizations

To our knowledge, we have presented the first constructive and predicative formalization of affine schemes. However, there are several classical formalizations of affine and general schemes in the literature by now. Examples include an early setoid-based formalization in `Coq` by Chicli [6], the aforementioned formalization in `Lean`'s `mathlib` [4], a more recent formalization in `Isabelle/HOL` [3], and a univalent `Coq` formalization in the `UniMath` library [5]. It is noteworthy that none of these formalizations define the structure sheaf on basic opens first. Instead, they follow the approach of Hartshorne's classic textbook "Algebraic Geometry" [16]. This approach directly defines the structure sheaf on arbitrary opens, but is inherently non-constructive. Assuming classical reasoning (including the axiom of choice) it is quite straightforward to formalize Hartshorne's definition. As a result, the `UniMath` formalization [5] does not actually use univalence in its definition of the structure sheaf.

It should be mentioned however, that in the beginning the `Lean` formalization [4] did use the "lift from basic opens approach". Being unable to formalize the notion of "canonical isomorphism" between localizations $R[1/f]$ in a satisfactory way, `Lean`'s `mathlib` [26] consequently adopted a non-standard take on localizations. Ultimately, the definition of the structure sheaf got completely overhauled using the Hartshorne approach. Buzzard et al. argue in [4, Sect. 3.4] that even with the structure sheaf directly defined using univalence, proving the sheaf property would run into the same problems that they encountered. As the equality/path obtained by an application of the univalence axiom would still carry around the isomorphism in question, it is a priori unclear what has actually been gained by working with paths, as opposed to working with isomorphisms directly. One of the main results of this paper is that on the contrary we can use univalence in a genuinely helpful way to construct the structure sheaf on basic opens and prove its sheaf property. This is achieved by shifting the focus to R-algebras, where the canonical isomorphisms between localizations become the center of contraction of the corresponding path spaces. Indeed, the localizations $R[1/f]$ form a full subcategory of the category of R-algebras that is posetal and equivalent to the poset of basic opens.

6.3 Different univalent approaches to basic opens

One of the main challenges of our formalization was to solve the higher coherence issues when constructing the structure presheaf on basic opens. These coherence issues arose because the basic opens were defined as a subset of the Zariski lattice (i.e. as functions into propositions)

using propositional truncation. In constructive mathematics it is common to define subsets X as sets A with an embedding $i : A \hookrightarrow X$ and one can prove in HoTT/UF that these two notions of subsets are equivalent. This raises the question whether one could define the type of basic opens more directly, thus eliminating the coherence issues.

The basic opens can be defined as a quotient on R, equating any f and g such that $\sqrt{\langle f \rangle} = \sqrt{\langle g \rangle}$. A first, now deprecated, formalization attempt defined the structure sheaf on this type. However, in this case we need to map from a set quotient into an groupoid, which is notoriously hard. The general characterization of such maps given by Kraus and von Raumer [21, Thm. 13] is not easily applicable in this case. As a result, we ended up working in R-algebras because the contractibility of the path spaces between localizations solved the coherence issues in this case as well. Rijke has since suggested, in private communications, that the basic opens can be seen as the Rezk completion [33, Sec. 9.9] of R as a poset category with the pre-order $f \leq g$ given by inclusion $\sqrt{\langle f \rangle} \subseteq \sqrt{\langle g \rangle}$. This could potentially be used for an alternative development where coherence issues are avoided altogether.

6.4 Towards constructive quasi-compact, quasi-separated schemes

The structure sheaf, as constructed in this paper, lets us define constructive affine schemes. This is of course only the first step towards a formalization of *constructive schemes*. Schemes are classically defined as a special class of *locally ringed spaces*. However, in the constructive, predicative setting of [10] we are confined to *ringed lattices*, i.e. distributive lattices equipped with a sheaf valued in commutative rings. These correspond to ringed coherent spaces. Maps between those are maps of ringed spaces where the underlying continuous map is coherent. Morphisms of schemes, however, are just morphisms of locally ringed spaces, i.e. morpisms of ringed spaces that induce local morphisms on the stalks. In general these two types of morphisms do not coincide.

Fortunately, the situation is well-behaved for *quasi-compact, quasi-separated* schemes, a very important class of schemes that, in particular, encompasses all *Noetherian* schemes.[14] They are actually just the schemes where the underlying topological space is coherent. Furthermore, if X and Y are quasi-compact, quasi-separated schemes, for any morphism of locally ringed spaces $(f, f^\sharp) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$, the underlying continuous map f is coherent. As pointed out in [10], this was essentially already proved by Grothendieck [13, Sec. 6.1]. This makes the constructive lattice-based approach to quasi-compact, quasi-separated schemes as worked out in [10] possible.

Such an approach still needs to be able to talk about morphisms of quasi-compact, quasi-separated schemes, i.e. morphisms of locally ringed spaces. This problem is circumvented in [10] by considering *locally affine morphisms*. A locally affine morphism is induced by ring homomorphisms on affine covers and it is a standard exercise to show that for general schemes this is equivalent to a morphism of locally ringed spaces. For a formalization however, it could be advantageous to work with a constructive reformulation of morphisms of locally ringed spaces. Schuster discusses the right constructive, point-free notion of a morphism of locally ringed spaces in the setting of formal topology in [28]. Transferring this to a development based on ringed lattices could lead to a constructive account of quasi-compact, quasi-separated schemes closer to the usual classical presentation and easier to formalize.

[14] Deligne in fact argued that this class of schemes is actually sufficient for a lot of applications in algebraic geometry [12].

References

1 Carlo Angiuli, Evan Cavallo, Anders Mörtberg, and Max Zeuner. Internalizing representation independence with univalence. *Proc. ACM Program. Lang.*, 5(POPL), January 2021. doi:10.1145/3434293.

2 Michael Francis Atiyah and Ian Grant MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley-Longman, 1969.

3 Anthony Bordg, Lawrence Paulson, and Wenda Li. Simple Type Theory is not too Simple: Grothendieck's Schemes Without Dependent Types. *Experimental Mathematics*, 0(0):1–19, 2022. doi:10.1080/10586458.2022.2062073.

4 Kevin Buzzard, Chris Hughes, Kenny Lau, Amelia Livingston, Ramon Fernández Mir, and Scott Morrison. Schemes in lean. *Experimental Mathematics*, 0(0):1–9, 2021. doi:10.1080/10586458.2021.1983489.

5 Tim Cherganov. Sheaf of rings on Spec R, 2022. URL: https://github.com/UniMath/UniMath/blob/0df0949b951e198c461e16866107a239c8bc0a1e/UniMath/AlgebraicGeometry/Spec.v.

6 Laurent Chicli. Une formalisation des faisceaux et des schémas affines en théorie des types avec Coq. Technical Report RR-4216, INRIA, June 2001. URL: https://hal.inria.fr/inria-00072403.

7 Cyril Cohen, Thierry Coquand, Simon Huber, and Anders Mörtberg. Cubical Type Theory: A Constructive Interpretation of the Univalence Axiom. In Tarmo Uustalu, editor, *21st International Conference on Types for Proofs and Programs (TYPES 2015)*, volume 69 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 5:1–5:34, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.TYPES.2015.5.

8 Thierry Coquand, Simon Huber, and Anders Mörtberg. On Higher Inductive Types in Cubical Type Theory. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS 2018, pages 255–264, New York, NY, USA, 2018. ACM. doi:10.1145/3209108.3209197.

9 Thierry Coquand, Henri Lombardi, and Peter Schuster. The projective spectrum as a distributive lattice. *Cahiers de Topologie et Géométrie différentielle catégoriques*, 48(3):220–228, 2007.

10 Thierry Coquand, Henri Lombardi, and Peter Schuster. Spectral schemes as ringed lattices. *Annals of Mathematics and Artificial Intelligence*, 56(3):339–360, 2009.

11 Tom de Jong and Martín Hötzel Escardó. On Small Types in Univalent Foundations. *Logical Methods in Computer Science*, Volume 19, Issue 2, May 2023. doi:10.46298/lmcs-19(2:8)2023.

12 Pierre Deligne and Jean-François Boutot. Cohomologie étale: les points de départ. In *Cohomologie Etale*, pages 4–75, Berlin, Heidelberg, 1977. Springer Berlin Heidelberg.

13 Jean Dieudonné and Alexandre Grothendieck. *Éléments de géométrie algébrique*, volume 1. Springer Berlin Heidelberg New York, 1971.

14 Luis Español. Le spectre d'un anneau dans l'algèbre constructive et applications à la dimension. *Cahiers de Topologie et Géométrie Différentielle Catégoriques*, 24(2):133–144, 1983. URL: http://www.numdam.org/item/CTGDC_1983__24_2_133_0/.

15 Ulrich Görtz and Torsten Wedhorn. *Algebraic geometry*. Springer, 2010.

16 Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

17 Melvin Hochster. Prime ideal structure in commutative rings. *Transactions of the American Mathematical Society*, 142:43–60, 1969.

18 Peter T. Johnstone. *Stone spaces*, volume 3. Cambridge university press, 1982.

19 André Joyal. Les théoremes de chevalley-tarski et remarques sur l'algèbre constructive. *Cahiers Topologie Géom. Différentielle*, 16:256–258, 1976.

20 Nicolai Kraus. The general universal property of the propositional truncation. In Hugo Herbelin, Pierre Letouzey, and Matthieu Sozeau, editors, *20th International Conference on Types for Proofs and Programs (TYPES 2014)*, volume 39 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 111–145, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.TYPES.2014.111.

21 Nicolai Kraus and Jakob von Raumer. Coherence via well-foundedness: Taming set-quotients in homotopy type theory. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '20, pages 662–675, New York, NY, USA, 2020. Association for Computing Machinery. doi:10.1145/3373718.3394800.

22 Henri Lombardi and Claude Quitté. *Commutative Algebra: Constructive Methods: Finite Projective Modules*, volume 20. Springer, 2015.

23 Saunders Mac Lane. *Categories for the working mathematician*, volume 5. Springer Science & Business Media, 2013.

24 Saunders Mac Lane and Ieke Moerdijk. *Sheaves in geometry and logic: A first introduction to topos theory*. Springer Science & Business Media, 2012.

25 Per Martin-Löf. An Intuitionistic Theory of Types: Predicative Part. In H. E. Rose and J. C. Shepherdson, editors, *Logic Colloquium '73*, volume 80 of *Studies in Logic and the Foundations of Mathematics*, pages 73–118. North-Holland, 1975. doi:10.1016/S0049-237X(08)71945-1.

26 The mathlib Community. The lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*, CPP 2020, pages 367–381, New York, NY, USA, 2020. Association for Computing Machinery. doi:10.1145/3372885.3373824.

27 Ray Mines, Fred Richman, and Wim Ruitenburg. *A course in constructive algebra*. Springer Science & Business Media, 2012.

28 Peter Schuster. The zariski spectrum as a formal geometry. *Theoretical Computer Science*, 405(1):101–115, 2008. Computational Structures for Modelling Space, Time and Causality. doi:10.1016/j.tcs.2008.06.030.

29 Marshall Harvey Stone. Topological representations of distributive lattices and brouwerian logics. *Časopis pro pěstování matematiky a fysiky*, 67(1):1–25, 1938.

30 Thomas Streicher. *Investigations Into Intensional Type Theory*. Habilitation thesis, Ludwig-Maximilians-Universität München, 1993. URL: https://www2.mathematik.tu-darmstadt.de/~streicher/HabilStreicher.pdf.

31 The Agda Development Team. The Agda programming language. URL: http://wiki.portal.chalmers.se/agda/pmwiki.php.

32 Ayberk Tosun and Martín Hötzel Escardó. Patch locale of a spectral locale in univalent type theory, 2023. arXiv:2301.04728.

33 The Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. https://homotopytypetheory.org/book, Institute for Advanced Study, 2013.

34 Ravi Vakil. The rising sea: Foundations of algebraic geometry, 2017. draft. URL: https://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf.

35 Andrea Vezzosi, Anders Mörtberg, and Andreas Abel. Cubical agda: A dependently typed programming language with univalence and higher inductive types. *Journal of Functional Programming*, 31:e8, 2021. doi:10.1017/S0956796821000034.

36 V. Voevodsky, B. Ahrens, D. Grayson, et al. UniMath: Univalent Mathematics. Available at https://github.com/UniMath.

37 Vladimir Voevodsky. Univalent foundations, September 2010. Notes from a talk in Bonn. URL: https://www.math.ias.edu/vladimir/sites/math.ias.edu.vladimir/files/Bonn_talk.pdf.

38 Vladimir Voevodsky. Resizing rules – their use and semantic justification. slides from a talk at types, bergen, 11 september, 2011.

39 Vladimir Voevodsky. An experimental library of formalized mathematics based on the univalent foundations. *Mathematical Structures in Computer Science*, 25(5):1278–1294, 2015. doi:10.1017/S0960129514000577.