Towards a Formalization of Affine Schemes in `Cubical Agda`

Anders Mörtberg, **Max Zeuner**

University of Stockholm

TYPES 2022, 23.06.2022

Affine schemes constructively/point-free

Goal: Equip *Zariski lattice* ZL_R with a sheaf of rings,
the so-called *structure sheaf*

Affine schemes constructively/point-free

Goal: Equip *Zariski lattice* ZL_R with a sheaf of rings, the so-called *structure sheaf*

$$\mathcal{O} \;:\; \mathsf{ZL}^{op} \to \mathsf{CommRing}$$

classically: open sets $U \subseteq \{\mathfrak{p} \text{ prime ideal}\}$

constructively: f.g. ideals $\mathfrak{a}, \mathfrak{b}$ modulo $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$

Affine schemes constructively/point-free

Goal: Equip *Zariski lattice* ZL_R with a sheaf of rings, the so-called *structure sheaf*

$$\mathcal{O} \ : \ \mathsf{ZL}^{op} \ \rightarrow \ \mathsf{CommRing}$$

classically: open sets $U \subseteq \{\mathfrak{p} \text{ prime ideal}\}$

constructively: f.g. ideals $\mathfrak{a}, \mathfrak{b}$ modulo $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$

- First constructive account due to Joyal [1976]
- Above definition of ZL due to Español [1983]
- Formalization generally follows Coquand et al. [2009]

A brief history of formalizing schemes

Existing work in: `Coq`, `lean-mathlib`, `Isabelle/HOL` & `UniMath`

A brief history of formalizing schemes

Existing work in: `Coq`, `lean-mathlib`, `Isabelle/HOL` & `UniMath`

A brief history of formalizing schemes

Existing work in: `Coq`, `lean-mathlib`, `Isabelle/HOL` & `UniMath`

All use non-constructive “Hartshorne” approach...

A brief history of formalizing schemes

Existing work in: `Coq`, `lean-mathlib`, `Isabelle/HOL` & `UniMath`

All use non-constructive “Hartshorne” approach...

⇒ Formalize constructive approach in `Cubical Agda` (with crucial help from univalence)

Cubical Agda

- Equality through path-types _≡_
  Dependent paths convenient for transporting properties

Cubical Agda

- Equality through path-types _≡_
  Dependent paths convenient for transporting properties

- Supports *higher inductive types* ⇒ *set-quotients*.
  in this talk: ZL and *localizations* $R[1/f\,]$ (rings of fractions)

Cubical Agda

- Equality through path-types $\_ \equiv \_$
  Dependent paths convenient for transporting properties
- Supports *higher inductive types* $\Rightarrow$ *set-quotients*.
  in this talk: ZL and *localizations* $R[1/f]$ (rings of fractions)
- Supports univalence $\Rightarrow$ structure identity principle

$$\text{sip} \; : \; (A\ B \; : \; \text{CommRing}) \; \rightarrow \; A \cong B \; \rightarrow \; A \equiv B$$

Cubical Agda

- Equality through path-types $\_\equiv\_$
  Dependent paths convenient for transporting properties
- Supports *higher inductive types* $\Rightarrow$ *set-quotients*.
  in this talk: ZL and *localizations* $R[1/f\,]$ (rings of fractions)
- Supports univalence $\Rightarrow$ structure identity principle

$$\mathsf{sip} \;:\; (A\ B \;:\; \mathsf{CommRing}) \;\to\; A \cong B \;\to\; A \equiv B$$

- Everything computes!

Cubical Agda

- Equality through path-types $\_\equiv\_$
  Dependent paths convenient for transporting properties
- Supports *higher inductive types* $\Rightarrow$ *set-quotients*.
  in this talk: ZL and *localizations* $R[1/f]$ (rings of fractions)
- Supports univalence $\Rightarrow$ structure identity principle

$$\mathsf{sip} \;:\; (A\ B \;:\; \mathsf{CommRing}) \;\to\; A \cong B \;\to\; A \equiv B$$

- Everything computes!

$\Rightarrow$ Great for constructive and univalent formalization
of set-level mathematics in the spirit of Voevodsky [2015]

Outline of Construction

Define $\mathcal{O} : \mathsf{ZL}^{op} \to \mathsf{CommRing}$ on generators $D(f) \in \mathsf{ZL}$ for $f \in R$:

Outline of Construction

Define $\mathcal{O} : \mathsf{ZL}^{op} \to \mathsf{CommRing}$ on generators $D(f) \in \mathsf{ZL}$ for $f \in R$:

$$D(f) \mapsto R[1/f]$$

classically: $\{\mathfrak{p} \mid f \notin \mathfrak{p}\}$

constructively: equiv. class of $\langle f \rangle$

ring of fractions of the form r/f^n

Outline of Construction

Define $\mathcal{O} : \mathsf{ZL}^{op} \to \mathsf{CommRing}$ on generators $D(f) \in \mathsf{ZL}$ for $f \in R$:

$$D(f) \mapsto R[1/f]$$

classically: $\{\mathfrak{p} \mid f \notin \mathfrak{p}\}$

constructively: equiv. class of $\langle f \rangle$

ring of fractions of the form r/f^n

Check well-defined: "$D(f) \equiv D(g) \Rightarrow R[1/f] \equiv R[1/g]$"

Outline of Construction

Define $\mathcal{O} : \mathsf{ZL}^{op} \to \mathsf{CommRing}$ on generators $D(f) \in \mathsf{ZL}$ for $f \in R$:

$$D(f) \mapsto R[1/f]$$

classically: $\{\mathfrak{p} \mid f \notin \mathfrak{p}\}$

constructively: equiv. class of $\langle f \rangle$

ring of fractions of the form r/f^n

Check well-defined: "$D(f) \equiv D(g) \;\Rightarrow\; R[1/f] \equiv R[1/g]$"

Also need (wip):

- Proof of sheaf property
- Extension to ZL preserves sheaf property

Where does univalence help?

1. Well-definedness stated with $\_ \equiv \_$ not provable without univalence
2. In proof of the sheaf property, need $R[1/f][1/g] \equiv R[1/fg]$

Where does univalence help?

1. Well-definedness stated with $\_\equiv\_$ not provable without univalence
2. In proof of the sheaf property, need $R[1/f][1/g] \equiv R[1/fg]$

But: `lean-mathlib-team` was not convinced:

> *"However, univalence does not solve the problem [...]*
> *the lion's share of the work still needs to done"*

- Buzzard et al. [2021]

Where does univalence help?

1. Well-definedness stated with $\_\equiv\_$ not provable without univalence
2. In proof of the sheaf property, need $R[1/f][1/g] \equiv R[1/fg]$

But: `lean-mathlib-team` was not convinced:

> *"However, univalence does not solve the problem [...]*
> *the lion's share of the work still needs to done"*

- Buzzard et al. [2021]

Buuut: can *actually* employ univalence through a simple algebraic trick

The "algebra trick"

Observation: factor $\mathcal{O} : \mathsf{ZL}^{op} \to \mathsf{R\text{-}Alg} \to \mathsf{CommRing}$

The "algebra trick"

Observation: factor $\mathcal{O} : \mathsf{ZL}^{op} \to \mathsf{R\text{-}Alg} \to \mathsf{CommRing}$

$$D(f) \leq D(g) \quad \Leftrightarrow \quad \mathsf{isContr}\left(Hom_R(R[1/g], R[1/f])\right)$$

The "algebra trick"

Observation: factor $\mathcal{O} : \mathsf{ZL}^{op} \to \mathsf{R\text{-}Alg} \to \mathsf{CommRing}$

$$D(f) \leq D(g) \quad \Leftrightarrow \quad \mathsf{isContr}\left(Hom_R(R[1/g], R[1/f\,])\right)$$

And by using univalence/the SIP:

$$D(f) \equiv D(g) \quad \Rightarrow \quad \mathsf{isContr}\,(R[1/f\,] \equiv_{\mathsf{R\text{-}Alg}} R[1/g])$$

The "algebra trick"

Observation: factor $\mathcal{O} : \mathsf{ZL}^{op} \to \mathsf{R\text{-}Alg} \to \mathsf{CommRing}$

$$D(f) \leq D(g) \quad \Leftrightarrow \quad \mathsf{isContr}\left(Hom_R(R[1/g], R[1/f])\right)$$

And by using univalence/the SIP:

$$D(f) \equiv D(g) \quad \Rightarrow \quad \mathsf{isContr}\left(R[1/f] \equiv_{\mathsf{R\text{-}Alg}} R[1/g]\right)$$

- What we *actually* need for constructing the presheaf
- Lets us avoid cumbersome diagram chases in proof of sheaf property

Summary

We presented the outline of a formalization of affine schemes that:

- Uses a synthetic description of Zariski lattice but follows (& elaborates) the textbook strategy $D(f) \mapsto R[1/f]$
- Uses a simple algebraic observation and univalence to make the construction work *out of the box*!

Summary

We presented the outline of a formalization of affine schemes that:

- Uses a synthetic description of Zariski lattice but follows (& elaborates) the textbook strategy $D(f) \mapsto R[1/f]$
- Uses a simple algebraic observation and univalence to make the construction work *out of the box*!

There is still some work to be done:

- Finish the construction of the structure sheaf (Extension of sheaves & sheaf property for general covers) Then sanity-check: $\mathcal{O}\big(D(1)\big) \equiv R$
- Future work: Define (spectral) schemes & projective schemes

Thank You

Sheaves

Presheaf $\mathcal{F} : L^{op} \to \mathcal{C}$ is *sheaf on distributive lattice* L if:

- $\mathcal{F}(\bot)$ is the terminal object in $\mathcal{C}$
- $\forall\, x, y \in L$ the following is a pullback square

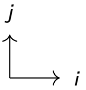
$$\begin{array}{ccc} \mathcal{F}(x \vee y) & \longrightarrow & \mathcal{F}(x) \\ \downarrow & \lrcorner & \downarrow \\ \mathcal{F}(y) & \longrightarrow & \mathcal{F}(x \wedge y) \end{array}$$

Action of the structure sheaf on objects

$$\Sigma[\, \mathfrak{a} \in \mathrm{ZL} \,] \left(\underbrace{\exists[\, f \in R \,]\, (D(f) \equiv \mathfrak{a})}_{\text{h-prop}} \right) \to \underbrace{\text{R-Alg}}_{\text{h-groupoid}}$$

we need for each $f, g, h \in R$ with $D(f) \equiv D(g) \equiv D(h)$,
a filler of the square by a result due to Kraus [2015]

$$\begin{array}{ccc} R[1/f] & \xrightarrow{\text{sip } \varphi_{fh} \ i} & R[1/h] \\ \| & & \uparrow {\scriptstyle \text{sip } \varphi_{gh} \ j} \\ R[1/f] & \xrightarrow{\text{sip } \varphi_{fg} \ i} & R[1/g] \end{array}$$



$$\Leftrightarrow \quad \text{sip } \varphi_{fh} \equiv \text{sip } \varphi_{fg} \bullet \text{sip } \varphi_{gh}$$

The sheaf property for binary covers

Lemma: $\langle f, g \rangle = A \Rightarrow$ pullback square

$$
\begin{array}{ccc}
A & \longrightarrow & A[1/g] \\
\downarrow & \lrcorner & \downarrow \\
A[1/f] & \longrightarrow & A[1/fg]
\end{array}
$$

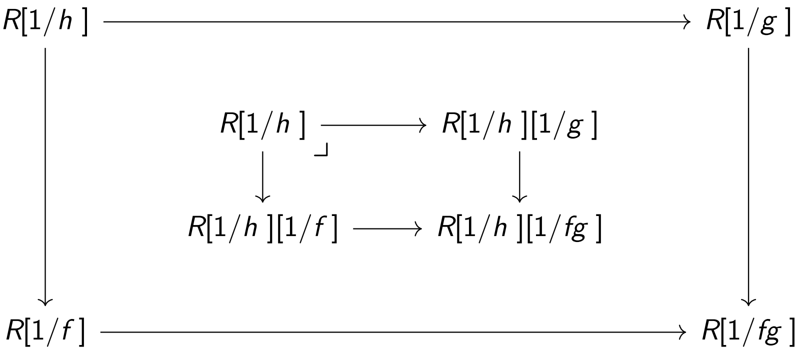
The sheaf property for binary covers

$D(h) \equiv D(f) \vee D(g) \;\Rightarrow\; \langle f/1, g/1 \rangle = R[1/h\,]$

$$
\begin{array}{ccc}
R[1/h\,] & \longrightarrow & R[1/h\,][1/g\,] \\
\downarrow & \lrcorner & \downarrow \\
R[1/h\,][1/f\,] & \longrightarrow & R[1/h\,][1/fg\,]
\end{array}
$$

The sheaf property for binary covers

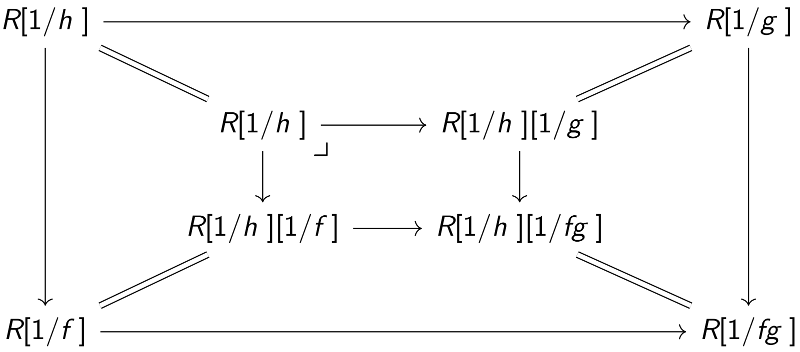
$D(h) \equiv D(f) \vee D(g)$ want: outer square is pullback



The sheaf property for binary covers

$D(h) \equiv D(f) \vee D(g)$ want: outer square is pullback

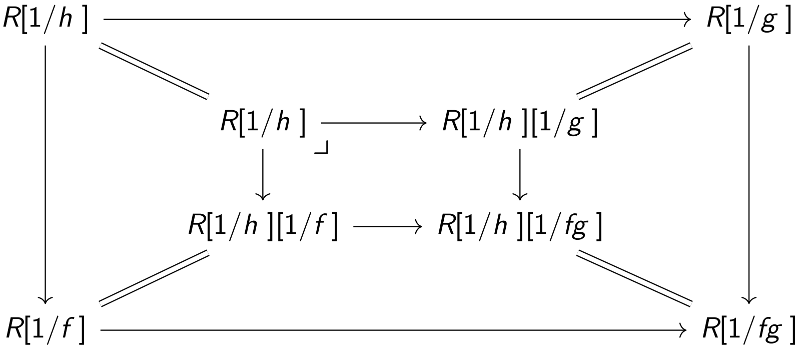
- Transport along paths of rings



The sheaf property for binary covers

$D(h) \equiv D(f) \vee D(g)$ want: outer square is pullback

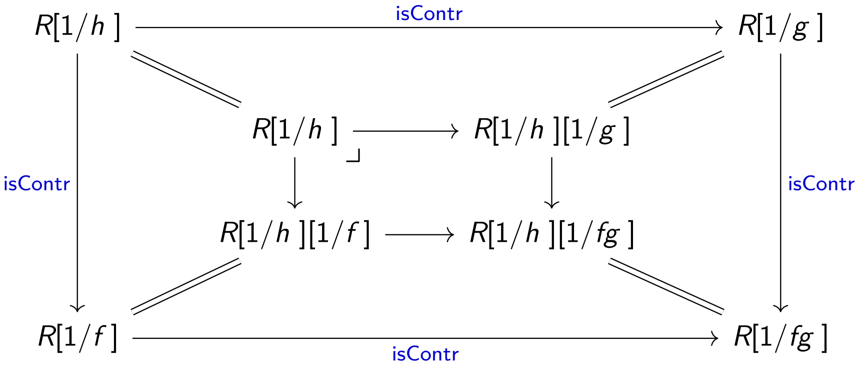
- Transport along paths of rings
- Provide dependent paths between morphisms



The sheaf property for binary covers

$D(h) \equiv D(f) \vee D(g)$ want: outer square is pullback

- Transport along paths of rings
- Provide dependent paths between morphisms
  - by contractibillity of R-homs



Links to library

- The Zariski lattice
- General construction of presheaf and lemma for sheaf property (line 268)
- Key lemma from univalence
(line 299)

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. URL https://doi.org/10.1080/10586458.2022.2062073.

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. URL https://doi.org/10.1080/10586458.2021.1983489.

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.

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

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/.

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

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. ISBN 978-3-939897-88-0. doi: http://dx.doi.org/10.4230/LIPIcs.TYPES.2014.111. URL http://drops.dagstuhl.de/opus/volltexte/2015/5494.

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.