A Univalent Formalization of Affine Schemes in `Cubical Agda`

Anders Mörtberg, **Max Zeuner**

University of Stockholm

HoTTEST, 20.10.2022

Set-level (constructive) mathematics in `Cubical Agda`

- Equality by paths ($x \equiv_A y$) as functions

$$p : \mathrm{I} \to A \quad \text{with} \quad p(\mathrm{i}_0) = x \quad \& \quad p(\mathrm{i}_1) = y$$

Moreover *dependent paths* over lines $B : \mathrm{I} \to \mathsf{Type}$
and *transport* along (dependent) paths

Set-level (constructive) mathematics in `Cubical Agda`

- Equality by paths ($x \equiv_A y$) as functions

$$p : \mathbb{I} \to A \quad \text{with} \quad p(i_0) = x \quad \& \quad p(i_1) = y$$

  Moreover *dependent paths* over lines $B : \mathbb{I} \to \text{Type}$
  and *transport* along (dependent) paths
- Supports *higher inductive types*
  $\Rightarrow$ *set-quotients & propositional truncations*

Set-level (constructive) mathematics in Cubical Agda

- Equality by paths ($x \equiv_A y$) as functions

$$p : \mathsf{I} \to A \quad \text{with} \quad p(\mathsf{i}_0) = x \quad \& \quad p(\mathsf{i}_1) = y$$

  Moreover *dependent paths* over lines $B : \mathsf{I} \to \mathsf{Type}$
  and *transport* along (dependent) paths

- Supports *higher inductive types*
  ⇒ *set-quotients* & *propositional truncations*
- Supports *univalence* ⇒ *structure identity principle*

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

Set-level (constructive) mathematics in `Cubical Agda`

- Equality by paths ($x \equiv_A y$) as functions

$$p : \mathsf{I} \to A \quad \text{with} \quad p(\mathsf{i}_0) = x \quad \& \quad p(\mathsf{i}_1) = y$$

  Moreover *dependent paths* over lines $B : \mathsf{I} \to \mathsf{Type}$
  and *transport* along (dependent) paths

- Supports *higher inductive types*
  ⇒ *set-quotients* & *propositional truncations*

- Supports *univalence* ⇒ *structure identity principle*

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

- Everything computes!

Set-level (constructive) mathematics in `Cubical Agda`

- Equality by paths ($x \equiv_A y$) as functions

$$p : \mathbb{I} \to A \quad \text{with} \quad p(i_0) = x \quad \& \quad p(i_1) = y$$

  Moreover *dependent paths* over lines $B : \mathbb{I} \to \text{Type}$
  and *transport* along (dependent) paths
- Supports *higher inductive types*
  ⇒ *set-quotients & propositional truncations*
- Supports *univalence* ⇒ *structure identity principle*

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

- Everything computes!

⇒ Great for univalent formalization of set-level constructive mathematics in the spirit of Voevodsky [2015]

A brief history of formalizing schemes

Schemes are a natural continuation of Voevodsky [2015],
but also an interesting benchmark in general (apparently)

A brief history of formalizing schemes

Schemes are a natural continuation of Voevodsky [2015], but also an interesting benchmark in general (apparently)

Existing work in:

- `Coq`
- `lean-mathlib`
- `Isabelle/HOL`
- `UniMath`

A brief history of formalizing schemes

Schemes are a natural continuation of Voevodsky [2015],
but also an interesting benchmark in general (apparently)

Existing work in:

- `Coq`
- `lean-mathlib`
- `Isabelle/HOL`
- `UniMath`

All use non-constructive "Hartshorne" approach...

$\Rightarrow$ Formalize constructive "lift from basis" approach in `Cubical Agda` (following Coquand et al. [2009] with crucial help from univalence)

Structure sheaf on the Zariski lattice (over R)

classically: compact open sets
$U \subseteq \mathrm{Spec}(R) = \{\mathfrak{p} \text{ prime ideal}\}$

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

$$\mathcal{O} : \mathrm{ZL}_R^{op} \to \mathrm{CommRing}$$

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

generators, $f \in R$

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

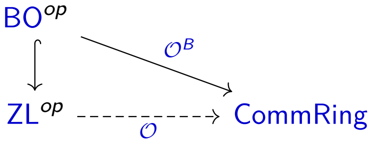
constructively: equiv. class of $\langle f \rangle$

ring of fractions
of the form r/f^n

Comparison lemma for sheaves on distributive lattices

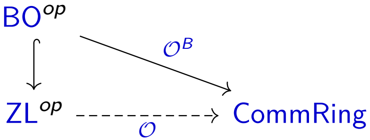
Comparison lemma for sheaves on distributive lattices

Kan-extension along inclusion of generators (basic opens)
preserves sheaf property



Comparison lemma for sheaves on distributive lattices

Kan-extension along inclusion of generators (basic opens) preserves sheaf property



For Kan-extension to exist need *small* ZL!
Construction due to Español [1983]:

$$\mathsf{ZL} = \mathsf{List}\ R\ /\ \_\!\sim\!\_$$

$$\begin{aligned} [x_1, \ldots, x_n] \sim [y_1, \ldots, y_m] \quad &= \quad \forall i.\ x_i \in \sqrt{\langle\ y_1, \ldots, y_m\ \rangle} \\ &\& \quad \forall i.\ y_i \in \sqrt{\langle\ x_1, \ldots, x_n\ \rangle} \end{aligned}$$

Well-definedness: "$D(f) \equiv D(g) \Rightarrow R[1/f] \equiv R[1/g]$"?

Well-definedness: "$D(f) \equiv D(g) \Rightarrow R[1/f] \equiv R[1/g]$"?

But basic opens (generators) are subset i.e. function $\mathsf{ZL} \to \mathsf{hProp}$ defined using propositional truncation $\|\_\|$

Well-definedness: “$D(f) \equiv D(g) \;\Rightarrow\; R[1/f] \equiv R[1/g]$”?

But basic opens (generators) are subset i.e. function ZL $\to$ hProp defined using propositional truncation $\|\_\|$

Want to define function

$$\mathcal{O}^B : \Sigma[\,\mathfrak{a} \in \mathrm{ZL}\,]\,\big(\underbrace{\exists[\,f \in R\,]\,(D(f) \equiv \mathfrak{a})}_{\text{h-prop}}\big) \;\to\; \underbrace{\mathrm{CommRing}}_{\text{h-groupoid}}$$

with $\quad \mathcal{O}^B\big(\,\mathfrak{a}\,,\,|\,f\,,\,p\,|\,\big) \;=\; R[1/f]$

Well-definedness: "$D(f) \equiv D(g) \Rightarrow R[1/f] \equiv R[1/g]$"?

But basic opens (generators) are subset i.e. function $\mathsf{ZL} \to \mathsf{hProp}$ defined using propositional truncation $\|\_\|$

Want to define function

$$\mathcal{O}^B : \Sigma[\ \mathfrak{a} \in \mathsf{ZL}\ ]\ \big(\underbrace{\exists[\ f \in R\ ]\ (D(f) \equiv \mathfrak{a})}_{\text{h-prop}}\big) \ \to\ \underbrace{\mathsf{CommRing}}_{\text{h-groupoid}}$$

with $\quad \mathcal{O}^B(\ \mathfrak{a}\ ,\ |\ f\ ,\ p\ |\ ) \ =\ R[1/f]$

"Naïve well-definedness" only enough if codomain of $\mathcal{O}^B$ was a set, we need something stronger!

Well-definedness: "$D(f) \equiv D(g) \Rightarrow R[1/f] \equiv R[1/g]$"?

But basic opens (generators) are subset i.e. function $\mathsf{ZL} \to \mathsf{hProp}$ defined using propositional truncation $\|\_\|$

Want to define function

$$\mathcal{O}^B : \Sigma[\, \mathfrak{a} \in \mathsf{ZL} \,] \left(\underbrace{\exists[\, f \in R \,]\, (D(f) \equiv \mathfrak{a})}_{\text{h-prop}} \right) \to \underbrace{\mathsf{CommRing}}_{\text{h-groupoid}}$$

with $\quad \mathcal{O}^B(\, \mathfrak{a} \,,\, |\, f \,,\, p \,|\,) \;=\; R[1/f]$

"Naïve well-definedness" only enough if codomain of $\mathcal{O}^B$ was a set, we need something stronger!

Textbook-argument: $D(f) = D(g) \Rightarrow$ *canonical iso* $R[1/f] \cong R[1/g]$

The "algebra trick"

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

The "algebra trick"

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

$$D(f) \leq D(g) \;\Leftrightarrow\; \sqrt{\langle\, f \,\rangle} \subseteq \sqrt{\langle\, g \,\rangle} \;\Leftrightarrow\; g \in R[1/f]^{\times}$$

$$\Leftrightarrow\; \exists!\, \varphi : R[1/g] \to R[1/f] \text{ s.t. } \varphi(x/1) = x/1 \text{ for } x \in R$$

$$\Leftrightarrow\; \mathsf{isContr}\, \Big(Hom_R\big(R[1/g], R[1/f]\big)\Big)$$

The "algebra trick"

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

$$D(f) \leq D(g) \;\Leftrightarrow\; \sqrt{\langle\, f \,\rangle} \subseteq \sqrt{\langle\, g \,\rangle} \;\Leftrightarrow\; g \in R[1/f]^{\times}$$

$$\Leftrightarrow\; \exists!\, \varphi : R[1/g] \to R[1/f] \text{ s.t. } \varphi(x/1) = x/1 \text{ for } x \in R$$

$$\Leftrightarrow\; \mathsf{isContr}\ \Big(Hom_R\big(R[1/g], R[1/f]\big)\Big)$$

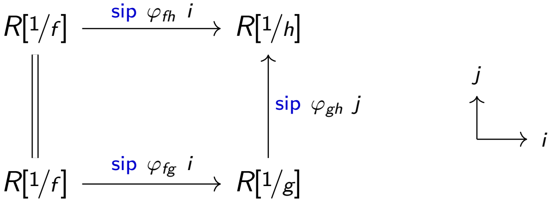
And by using univalence/the SIP for R-Alg:

$$D(f) \equiv D(g) \quad\Rightarrow\quad \mathsf{isContr}\ \big(R[1/f] \equiv R[1/g]\big)$$

(center of contraction: sip applied to unique iso $\varphi_{fg} : R[1/f] \cong R[1/g]$)

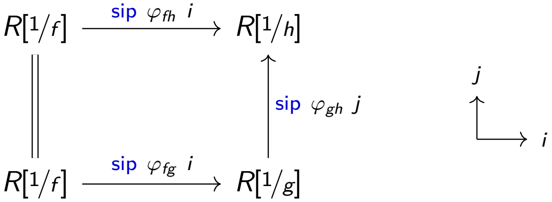
Overcoming the h-level mismatch (in R-Alg)

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



Overcoming the h-level mismatch (in R-Alg)

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



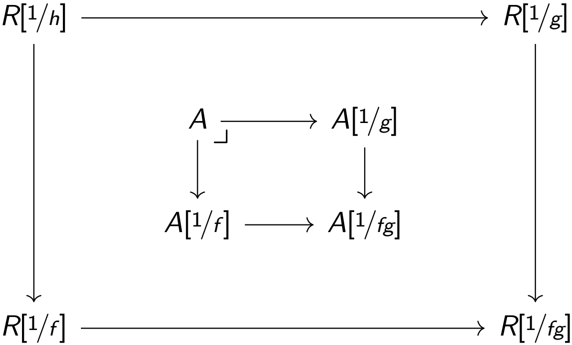
Proof: This is equivalent to giving a path

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

Sheaf property for binary cover $D(h) \equiv D(f) \vee D(g)$

Goal: outer square is pullback

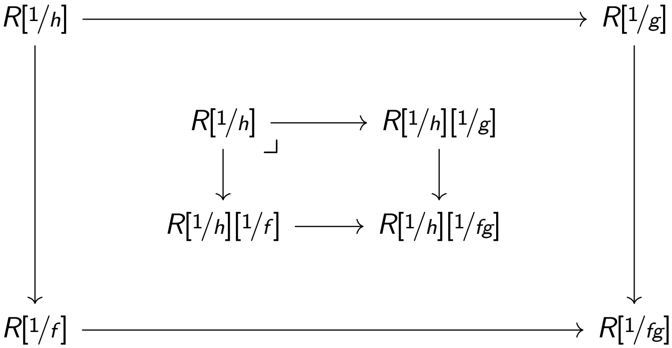
Lemma: $\langle f, g \rangle = A \Rightarrow$ pullback square



Sheaf property for binary cover $D(h) \equiv D(f) \vee D(g)$

Goal: outer square is pullback

Lemma with $\langle f/1, g/1 \rangle = R[1/h] \Rightarrow$ pullback square

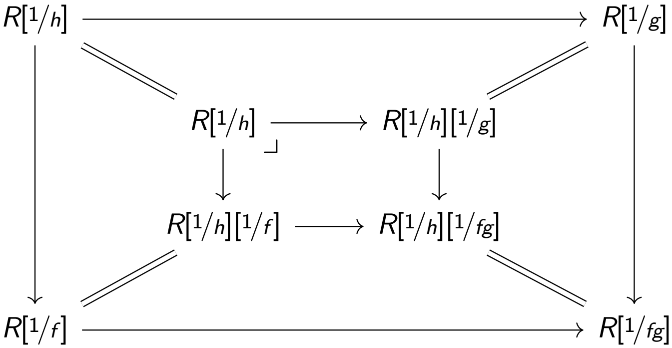


Sheaf property for binary cover $D(h) \equiv D(f) \vee D(g)$

Goal: outer square is pullback

Lemma with $\langle f/1, g/1 \rangle = R[1/h] \Rightarrow$ pullback square

- transport along paths of rings, e.g. $R[1/h][1/f] \equiv R[1/hf] \equiv R[1/f]$

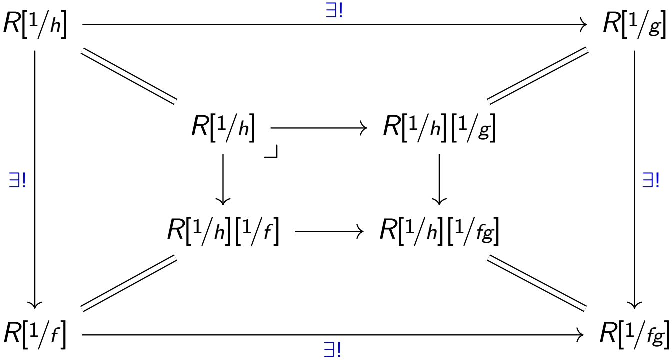


Sheaf property for binary cover $D(h) \equiv D(f) \vee D(g)$

Goal: outer square is pullback

Lemma with $\langle f/1, g/1 \rangle = R[1/h] \Rightarrow$ pullback square

- transport along paths of rings, e.g. $R[1/h][1/f] \equiv R[1/hf] \equiv R[1/f]$
- get dependent paths between morphisms for free

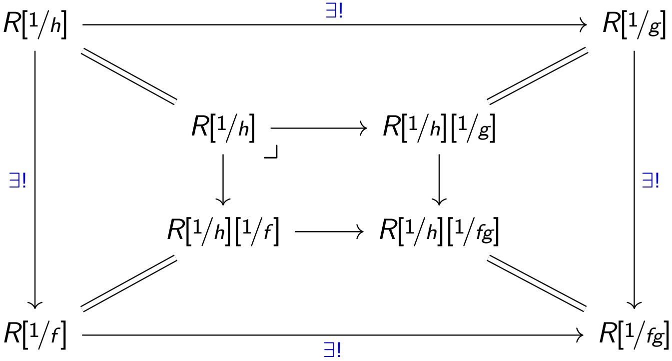


Sheaf property for binary cover $D(h) \equiv D(f) \vee D(g)$

Goal: outer square is pullback

Lemma with $\langle f/1, g/1 \rangle = R[1/h] \Rightarrow$ pullback square

- transport along paths of rings, e.g. $R[1/h][1/f] \equiv R[1/hf] \equiv R[1/f]$
- get dependent paths between morphisms for free
- forgetful functor pres. limits $\Rightarrow$ pullback square in comm. rings



Summary & future work

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

- uses a point-free, constructive 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*! (sort of)

What lies ahead:

- define (spectral) schemes as ringed lattice
- show that classically those are actually *quasi-compact, quasi-separated schemes*
- projective schemes

Thank You

Sheaves

Idea: restrict sheaf definition for locales to finite covers.

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

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

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

Links to library

- The Zariski lattice
- General construction of presheaf and lemma for sheaf property
  (lines 532 & 633)
- Key lemma from univalence
  (line 298)

Or just click your way through, starting here (def. of the structure sheaf)

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.