Formalising the GAGA theorem

Jujian Zhang

Imperial College London

Introduction

This project is to formalise the famous GAGA theorem by Jean-Pierre Serre in his *Géometrie Algébrique et Géométrie Analytique* [8]. The process of formalising mathematics is to use an interactive theorem prover to verify mathematical proofs. In this project, we will be using Lean.

Why formalising The first reason is to validate mathematical proofs. Undoubtedly, mathematics is hard, so hard that sometimes even top experts cannot agree what the correct answer should be. For example, the two articles in *Annals of mathematics* [4, 7] give two different answers to the same question. Because we couldn't perform experiments to validate mathematical proofs and mathematicians make mistakes, so we need other tools to help us check mathematics. The second reason is that, by formalising more and more mathematics, we will build a larger and larger database of mathematical proofs which could potentially be utilised by modern machine learning algorithms so that machine not only can verify mathematical proofs, it can prove theorems on its own, see this paper [6] and the IMO grand challenge where AI will attempt to solve IMO problem on its own [1].

Why GAGA Very roughly speaking, algebraic geometry "uses only polynomials to cut shapes" while analytic geometry "uses holomorphic functions to cut shapes" and the two geometries have very different topology, one has the Zariski topology while the other has the analytic topology. Intuitively, a statement in analytic geometry might not be true in algebraic geometry. However, the two geometries are still closely related, prior to GAGA theorem, Chow's theorem states that analytic subspace of complex projective space that is closed (in the ordinary topological sense) is an algebraic subvariety, i.e. closed in Zariski topology as well [3]. The GAGA theorem is a stronger theorem from which Chow's theorem immediately follows. The GAGA theorem very roughly states that under some conditions, the two geometries are "equivalent", for more details see below. Besides the interesting contents of GAGA, its importance lies in the fact that it is used in the proof of Fermat Last Theorem. So if one wants to formalise Fermat Last theorem, one need to unavoidably formalise the GAGA theorem.

Statement of GAGA[5]

The following is the statement of GAGA:

1. Let $(X, \mathcal{O}_X)$ be a scheme of locally finite type over $\mathbb{C}$, then the closed points of X forms a topological space denoted by X^{an} such that the inclusion map $\lambda_X : X^{an} \hookrightarrow X$ is continuous. The topology of X^{an} is very different from subspace topology from X.
2. If $\phi : X \to Y$ is a morphism between schemes of locally finite type over $\mathbb{C}$, then there is a morphism $\phi^{an} : X^{an} \to Y^{an}$ such that the following square commutes:

$$\begin{array}{ccc} X & \xrightarrow{\phi} & Y \\ \big\downarrow \lambda_X & & \big\downarrow \lambda_Y \\ X^{an} & \xrightarrow{\phi^{an}} & Y^{an}. \end{array}$$

3. There is a sheaf $\mathcal{O}_X^{an}$ of X^{an}, such that $\lambda : (X, \mathcal{O}_X) \to (X^{an}, \mathcal{O}_X^{an})$ induced by the inclusion map is a map between ringed space. This is the "analyfication" of $(X, \mathcal{O}_X)$.
4. A coherent sheaf of modules $\mathcal{F}$ over $(X, \mathcal{O})$ also has analyfication $\mathcal{F}^{an}$, defined as the kernel of map ϕ^{an} in the following diagram:

$$\begin{array}{ccccc} (X^{an}, \mathcal{O}^{an}) & \xrightarrow{(1,\phi^{an})} & (X^{an}, (\mathcal{O} \oplus \mathcal{F})^{an}) & \xrightarrow{(1,\psi^{an})} & (X^{an}, \mathcal{O}^{an}) \\ \big\downarrow & & \big\downarrow & & \big\downarrow \\ (X, \mathcal{O}) & \xrightarrow{(1,\phi)} & (X, \mathcal{O} \oplus \mathcal{F}) & \xrightarrow{(1,\psi)} & (X, \mathcal{O}) \end{array}$$

   where vertical arrows are inclusion and $\phi : \mathcal{O} \to \mathcal{O} \oplus \mathcal{F}$ is $r \mapsto r \oplus 0$ and $\psi : \mathcal{O} \oplus \mathcal{F} \to \mathcal{O}$ is $r \oplus s \mapsto r$.
5. Assume that X^{an} is Hausdorff and compact. If $\mathcal{F}$ and $\mathcal{G}$ are two coherent algbraic sheaves over $(X, \mathcal{O}_X)$ and $f : \mathcal{F}^{an} \to \mathcal{G}^{an}$ is a morphism of $\mathcal{O}_X^{an}$-modules, then f is induced by some $\phi : \mathcal{F} \to \mathcal{G}$, i.e. $f = \phi^{an}$.
6. If $\mathcal{A}$ is a coherent analytic sheaf of modules over $(X^{an}, \mathcal{O}_X^{an})$, then $\mathcal{A} \cong \mathcal{A}'^{an}$ where $\mathcal{A}'$ is a coherent algebraic sheaf over $(X, \mathcal{O}_X)$.

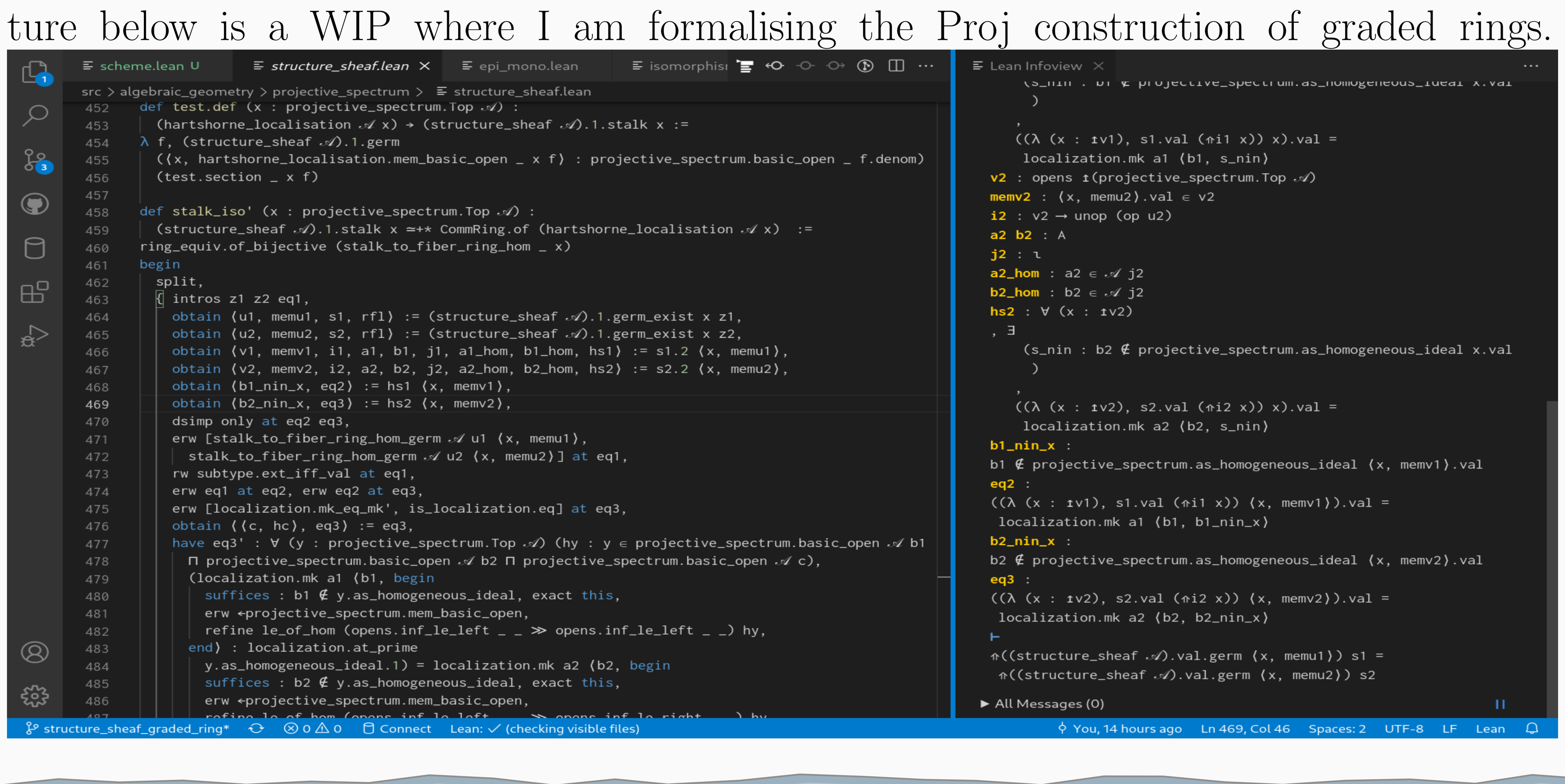
Statement 1,2 and 3 is the analyfication functor. In simple words, the idea is that given an algebraic object with Zariski topology, the functor gives back an anlytic object with analytic topology and given a map between two algebraic objects, the functor gives back a map between the two corresponding analytic object. The punchline of GAGA is that this anlytification process induces an equivalence of category between algebraic coherent sheaves and analytic coherent sheaves. The equivalence is in the following sense: algebraic coherent sheaves give analytic coherent sheaves (statement 4) and analytic coherent sheaves come from algebraic sheaves (statement 6); maps between algebraic coherent sheaves give maps between corresponding analytic coherent sheaves and maps (statement 4) between analytic sheaves come from maps between algebraic coherent sheaves (statement 6).

How can computer verify mathematics

Traditionally, computers are really good at questions like "what are the first 1000 prime numbers", but they cannot answer "are there infinitely many primes"; the former needs only computation while the latter requires a proof. The answer is dependent type theory. The idea is to encode mathematical proposition as types and proof as terms of a type. For example given two propositions A and B, to express the idea of A implying B, we use function type: suppose A is represented by type α (β resp.) so terms of α (β resp.) are proofs of A (B resp.), then the type of function $\alpha \to \beta$ represents $A \implies B$; because such a function will output a term of β given input of a term α, i.e. output a proof of B given a proof of A. The dependent part in dependent type theory makes universal quantification and existential quantification expressible. Let's now see the aforementioned example of proving infinitude of primes using Lean.

```
example (n : ℕ) :  (p : ℕ), n ≤ p ∧ p.prime :=
begin
  let N := n.factorial + 1,
  have N_ne_1 : N ≠ 1 := ne_of_gt (nat.succ_lt_succ (nat.factorial_pos n)),
  let p := N.min_fac,
  have p_prime : nat.prime p := nat.min_fac_prime N_ne_1,
  have n_le_p : n ≤ p,
  { apply le_of_not_ge,
    intros rid,
    have h : p ∣ n.factorial := nat.dvd_factorial (nat.min_fac_pos _) rid,
    have h : p ∣ 1 := (nat.dvd_add_iff_right h).2 (nat.min_fac_dvd _),
    exact p_prime.not_dvd_one h, },
  use p,
  split,
  exact n_le_p,
  exact p_prime,
end
```

For more details, see [2]. The above example does not capture the interactive nature of formalising mathematics. In fact, at every line, one can click anywhere to view what is currently know and what is required to be proven etc. The picture below is a WIP where I am formalising the Proj construction of graded rings.



References

References

[1] Imo grand challenge. `https://imo-grand-challenge.github.io/`, 2020.

[2] Jeremy Avigad, Leonardo de Moura, and Soonho Kong. Theorem proving in lean, 2015.

[3] Wei-Liang Chow. On compact complex analytic varieties. *American Journal of Mathematics*, 71(4):893–914, 1949.

[4] János Kollár. Non-quasi-projective moduli spaces. *Annals of mathematics*, pages 1077–1096, 2006.

[5] Amnon Neeman. *Algebraic and analytic geometry*. Number 345. Cambridge University Press, 2007.

[6] Stanislas Polu and Ilya Sutskever. Generative language modeling for automated theorem proving. *arXiv preprint arXiv:2009.03393*, 2020.

[7] Georg Schumacher and Hajime Tsuji. Quasi-projectivity of moduli spaces of polarized varieties. *Annals of mathematics*, pages 597–639, 2004.

[8] Jean-Pierre Serre. Géométrie algébrique et géométrie analytique. In *Annales de l'institut Fourier*, volume 6, pages 1–42, 1956.