Machine-Checked Mathematics formalization projects

July 14, 2023

1 Recurrence and minimality on metric spaces

Guillaume Dubach, Marco Lenci, Marcello Seri

Leren Leiden zonder te klagen

In this project we defined recurrent sets of discrete dynamical systems over metric spaces and proved some basic properties and relations with the omega limit sets already in Mathlib. The result of our efforts can be seen here.

While we made much progress and learned a great deal about Lean and Mathlib, it will require more work both to generalize our definitions and proofs to the case in which Filters are used and to get to our long-term goal, Birkhoff's Ergodic Theorem.

The project, while painful as promised, was a whole lot of fun and we are grateful to Sébastien Goüezel and all the other expert participants to the workshop for their friendliness and extreme availability, in spite of our constant stream of newbie questions.

2 The Hasse-Minkowski Theorem

Alex Best, Kevin Buzzard, Marco Streng, Hanneke Wiersema, Rosa Winter

In this project we aim to formalize the Hasse-Minkowski Theorem. This theorem states that a quadratic form over $\mathbb{Q}$ has solutions in $\mathbb{Q}$ (rational points) if and only if it has solutions in all p-adic completions of $\mathbb{Q}$ and the reals (it is locally soluble). We follow the proof by Serre in A Course in Arithmetic, which splits the proof into cases $n = 2$, $n = 3$, $n = 4$ and n at least 5 (where n is the dimension of the vector space on which the quadratic form is defined). So far we stated the theorem, and are almost done with proving the trivial $n = 0$ and $n = 1$. We are in the middle of cutting the $n = 2$ case into smaller lemmas. Defining the basechange of a quadratic form already turns out to be challenging!

3 Octonions

Filippo Nuccio, Matthieu Piquerez

Octonions is a non-associative real algebra with division of dimension 8 with an involution. We want to formalize the definition in mathlib, but giving the explicit multiplication on a basis would be too painful. Hopefully, the Cayley-Dickson construction let you define quite easily octonions from quaternions, quaternions from complex numbers and complex numbers from real ones.

Some structure is preserved by the construction, but we loose some (total order, commutativity, associativity, etc.) We have been able to prove that most important structures are preserved (algebra structure, inversion (currently in progress...), involution), and isomorphism with existing definition of complex numbers and quaternions has been proven. It would be good to define norms in a clean way, to generalize the implemented Cayley-Dickson construction in order to get variants of quaternions and octonions, to have more structure-preserving theorem (e.g. if you are commutative then the Cayley-Dickson construction is associative) and to give some applications.

The main difficulty we encounter is that some structures in Mathlib are only defined for associative structure, though they have a meaning in more generality, hence we have to define new structures or to make a complicated mix of mixins.

4 Formally real fields

Mahoor Alavioun, Riccardo Brasca, Maryam Emamjomeh Zadeh, Ignasi Sánchez Rodríguez, Florent Schaffhauser

We have been working on Formally real fields, with the goal of proving formally that such fields are orderable.

We proved it by applying Zorn's lemma, to show that a formally real field contains a maximal positive cone, and that the latter defines a total positive cone in the sense of mathlib. And then it is proved in mathlib that such a cone defines an ordering.

The next step is to define real-closed fields and (possibly combining this with Antoine Chambert-Loir and Cyril Cohen's implementation of Sturm's theorem?) to prove the real Nullstellensatz.

5 The Cyclotomic Character

Jennifer Balakrishnan, Alex Best, Kevin Buzzard, Marco Streng, Hanneke Wiersema, Rosa Winter

In this project we aim to define the cyclotomic character. This is a character of the absolute Galois group of the rationals into $\mathbb{Z}_p^*$ - roughly it gives the Galois action on roots of unity. The project consists of two steps - and we are currently trying to complete the first one. The first step is to define the mod p^n cyclotomic character: a character from $G_{\mathbb{Q}}$ to $\mathbb{Z}/p^n\mathbb{Z}$. The second step will then assemble these mod p^n characters to a character from $G_{\mathbb{Q}}$ into $\mathbb{Z}_p^*$. Kevin says that we could use pro categories to prove continuity.

6 Computing the Reduced Row Echelon Form

Mohanad Ahmed, Anne Baanen, Sudhir Murthy, Wessel de Weijer

We worked on implementing a function that computes the Reduced Row Echelon normal form given a `Matrix (Fin m) (Fin n) K` where `K` is a `Field` with `DecidableEq` (and computable operations). We found out that default matrices provided by Mathlib, while easy to use in proofs, have terrible performance. Therefore, we use `Array` under the hood and define two new types: `ArrayVec` (`Array` with a specific length) and `ArrayMat` (an `ArrayVec` of length $m * n$). While our algorithm is still inefficient (optimization will complicate the correctness proof), it works well in practice.

We also made an outline of the proof of correctness which would allow us to connect it to the existing `Matrix` theory.

The project can be found at `https://github.com/wdeweijer/LorentzRREF`.

7 Fuchsian Groups

Jana Göken, Bhavik Mehta, Oliver Nash

We implemented Fuchsian Groups, which are discrete subgroups of orientation-preserving isometries on the hyperbolic plane. Addintionally, we defined the `SMul` action of $\mathsf{PSL}(2, R)$ on the upper half-plane and showed that it is acting isometrically.

8 Skew Polynomial Rings and Drinfeld Modules

María Inés de Frutos Fernández, Carlos Caralps, Xavier Généreux, Benoît Guillemet, Nandagopal Ramachandran

The aim of this project is to formalise Skew Polynomials Rings and, ultimately, Drinfeld Modules. After defining Skew Polynomials we worked on adapting multiple small lemmas from the Polynomial file found on Mathlib. With the minimal infrastructure in place, we prove that the Skew Polynomials form a ring. For Drinfeld modules, we focus our attention to the base case of $\mathbb{F}_q[t]$ - Drinfeld modules.

9 Properties of scheme morphisms

Amelia Livingston, Wim Nijgh, Torger Olson, Jonas van der Schaaf

The aim of this project is to formalize some properties of schemes morphisms. In particular we focused on defining closed immersions, as these are central to concepts such as separatedness and proper morphisms. We proved some very basic properties of closed immersions and that the canonical example of closed immersions (quotients of rings) are in fact closed immersions. We defined (but did not prove) the valuative criterion of separatedness as well.

10 Moebius sum, Brouckner-Wallis algorithm

Sam van Gool, Harald Helfgott

We formalized exercise 1 of Harald (a proof that the sum of $\mu(n)/n$ is at most 1 in absolute value) and started formalizing the correctness of the Brouckner-Wallis algorithm for solving Pell's equation. Got help on various occasions from Bhavik, Floris and Filippo.

11 Goppa codes

D. J. Bernstein

Objective is to formalize the `https://cr.yp.to/papers.html#goppadecoding` survey. Didn't really get down to work on this until yesterday, so nothing interesting to report yet, but a few hundred lines of warmup theorems went smoothly.

12 Resultants

Sander Dahmen, Dimitrios Mitsios, Qizheng Yin

We aimed to define the resultant and prove some basic properties. We defined a version for lists that is better for computations, and based on this we defined the usual version for polynomials. We also defined the linear map that gives rise to the Sylvester matrix. We stated some properties but didn't have time to prove them.

The project can be found at `https://github.com/alainchmt/resultants`