Formalising Linear Algebra

Holden Lee

Computer Laboratory, University of Cambridge

What is formal verification?

Mathematics is "knowledge built upon an absolute foundation" because it is built on logic, which has set rules for how a statement can be deduced from previous statements. Practically speaking, however, we write mathematics using a mixture of formal symbols and natural language, skip over details of proofs, and introduce errors from oversight—especially as the mathematics becomes more complex.

Isabelle, a formal verification system based on higher-order logic, allows us to interactively check complex proofs using a computer. It has been used to check proofs that are difficult to referee, such as the Kepler conjecture, and hence places mathematics back on a firm foundation.

Project Goal

I formalise basic linear algebra (up to the rank-nullity theorem) over an arbitrary field.

Why linear algebra?

- Although several impressive results have been proved using Isabelle, Isabelle's library of basic abstract algebra is incomplete.
- A reasonable verification system must be able to deal with abstract algebra in full generality. I generalise previous developments of linear algebra to arbitrary fields.
- Linear algebra over non-real fields—namely finite fields—is essential for cryptography.

Acknowledgements

I would like to thank Lawrence Paulson for supervising my project and Marjorie Batchelor for organising the PMC. This project was funded by the Post-Masters Consultancy and the Computer Laboratory.

Methods and Results

I use the locale system in Isabelle to define vector spaces and linear maps:

locale *vectorspace* =
  module: *module K V* + *field*: *field K*
  for *K* **and** *V*

I prove the Rank-Nullity Theorem via the Replacement Theorem.

theorem (**in** *linear-map*) *rank-nullity*:
  assumes *fd*: *V.fin-dim*
  shows (*vectorspace.dim K* (*W.vs imT*)) + (*vectorspace.dim K* (*V.vs kerT*)) = *V.dim*

Along the way I formalize useful definitions and facts such as function spaces, direct sums, and existence of bases. The proof for existence of bases is below; note how Isabelle's structured proofs system displays proofs in a human-readable way.

lemma (**in** *vectorspace*) *finite-basis-exists*:
  assumes *h1*: *fin-dim*
  shows ∃ *β*. *finite β* ∧ *basis β*
proof −
  from *h1* **obtain** *A* **where** *1*: *finite A* ∧ *A*⊆*carrier V* ∧ *gen-set A* **by** (*metis fin-dim-def*)
  hence *2*: ∃ *β*. *β*⊆*A* ∧ *minimal β* (λ*S*. *S*⊆*carrier V* ∧ *gen-set S*)
    apply (*intro minimal-exists*) **by** *auto*
  then obtain *β* **where** *3*: *β*⊆*A* ∧ *minimal β* (λ*S*. *S*⊆*carrier V* ∧ *gen-set S*) **by** *auto*
  hence *4*: *lin-indpt β* **apply** (*intro min-gen-is-li*) **by** *auto*
  moreover from *3* **have** *5*: *gen-set β* ∧ *β*⊆*carrier V* **apply** (*unfold minimal-def*) **by** *auto*
  moreover from *1 3* **have** *6*: *finite β* **by** (*auto simp add*: *finite-subset*)
  ultimately show *?thesis* **apply** (*unfold basis-def*) **by** *auto*
qed

The proof is as follows.

1. Because V is finite-dimensional, there is a finite generating set (we took this as our definition of finite-dimensional).
2. Hence, there is a minimal $\beta \subseteq A$ such that β generates V.
3. β is linearly independent because a minimal generating set is linearly independent.

Finally, β is a basis because it is both generating and linearly independent.

Conclusions and Further Work

My original goal was to verify the recently-proved Kakeya and Nikodym conjectures on the geometry of finite fields. Although this has not been finished, the new linear algebra development paves the way by making key steps in the proof possible, for example, interpreting $\mathbb{F}_p[X_1, \ldots, X_n]$ as a vector space over $\mathbb{F}_p$.