Cauchy-Schwarz in ACL2(r) Abstract Vector Spaces[*]

Carl Kwan
Department of Computer Science
The University of Texas at Austin
Austin, TX, USA
carlkwan@cs.utexas.edu

Yan Peng Mark R. Greenstreet
Department of Computer Science
University of British Columbia
Vancouver, BC, Canada
{yanpeng, mrg}@cs.ubc.ca

We present a proof of the Cauchy-Schwarz inequality for ACL2(r) abstract vector spaces. Moreover, our proof uses `Smtlink`, an ACL2 book that uses the SMT solver Z3 at the backend, and requires little user-guidance beyond stating the basic inner-product and vector-space properties. By necessity, we also present a formal theory of abstract vector spaces. The proof and theory are based on our previous work on real vector spaces in ACL2(r). Abstraction is obtained via encapsulation, but reasoning about abstract vectors involved building `Smtlink` support for Z3's theory of uninterpreted functions and sorts, which we also discuss. To our knowledge, this is the first formal proof of Cauchy-Schwarz for abstract vector spaces in a first-order logic.

Let $(V,\mathbb{R})$ be a vector space and $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{R}$ an inner product. For any $u,v \in V$, the Cauchy-Schwarz inequality states

$$|\langle u,v\rangle|^2 \leq \langle u,u\rangle \cdot \langle v,v\rangle. \tag{Cauchy-Schwarz}$$

Proof. (sketch) Suppose $u,v \neq 0$. Let $\alpha = \langle v,v\rangle^{-1}\langle u,v\rangle \in \mathbb{R}$ and observe

$$0 \leq \|u-\alpha v\|^2 = \langle u,u\rangle - 2\alpha\langle u,v\rangle + \alpha^2\langle v,v\rangle = \langle u,u\rangle - (2\alpha-\alpha)\langle u,v\rangle = \langle u,u\rangle - \langle v,v\rangle^{-1}\langle u,v\rangle^2. \quad (1)$$

Rearranging produces Cauchy-Schwarz. For the full proof and statement of the theorem, see [2]. □

This extended abstract presents two novel contributions: (a) an ACL2(r) formalisation of abstract vector spaces over $\mathbb{R}$ by way of encapsulation; and, (b) a highly-automated `Smtlink`-leveraged proof of the Cauchy-Schwarz inequality (including square-rooted statements and equality conditions) for such abstract spaces. Previously, we only proved Cauchy-Schwarz for $V = \mathbb{R}^n$. Here, we encapsulate the definitions of the basic functions (e.g. vector addition, etc.) for $(\mathbb{R}^n, \mathbb{R}, \langle\cdot,\cdot\rangle)$ thus suppressing the real properties of $\mathbb{R}^n$ but exporting the inner-product space axioms. As discussed later, we require the co-domain of inner-product to be $\mathbb{R}$. The subsequent theorems (e.g. Cauchy-Schwarz, etc.) only depend on the inner-product space axioms and do not assume that the vectors are real.

We will focus the rest of our discussion on (b), our proof using `Smtlink`. In [2], the ACL2(r) proof of Cauchy-Schwarz involved "hand"-substituting α and guiding the theorem prover through each step of the algebraic manipulation via instantiating the appropriate properties of the inner product and vector space operations. This was onerous. The current proof offloads nearly all algebraic manipulations to the Z3 SMT solver using the `Smtlink` [3, 4] package for ACL2. While ACL2 excels at induction, rewriting, and reasoning about complex systems, the intricate algebraic manipulations involving inequalities that consistently appear in the proof of Cauchy-Schwarz (as well as other "mathematical" theorems in, e.g. applied analysis) are more efficiently performed by SMT solvers. By introducing user-defined structures with finite rules or axioms and proving theorems over them, we have thematically delved into the realm of SMT solvers wherein an extensive body of quality research has developed procedures and heuristics for finding satisfiable outcomes given some finite number of assumptions. Thus, it is natural to exploit SMT techniques for problems where the reasoning is largely "algebraic".

[*] An Extended Abstract on Abstract Types for Reasoning in Abstract Spaces

G. Passmore, R. Gamboa (Eds.): ACL2 Workshop 2020
EPTCS ??, 2020, pp. 1–3, doi:10.4204/EPTCS.??.??

From a user's point of view, the proof of Cauchy-Schwarz essentially amounts to stating the basic properties of the inner product as hypotheses to Smtlink. Prior to the statement of the main theorem, there are only three lemmas involved in algebraic manipulations! The application of inner product space axioms to prove the desired hypotheses are automatically verified by ACL2(r) itself. The proof in ACL2(r) follows easily and directly from a pencil-and-paper proof of Cauchy-Schwarz.

The somewhat surprising observation underlying this paper is that SMT techniques offer dramatic benefits even when the theorems to be proven are statements over abstract domains. Z3 is a many-sorted logic whereas ACL2 is untyped. For the proof of Cauchy-Schwarz in $(\mathbb{R}^n, \mathbb{R})$, this is a largely benign issue because Z3 supports reasoning over the reals. The exception is when functions act on objects outside their intended domains. For example, many functions in ACL2(r) on $\mathbb{R}^n$ are fixed to return zero on non-real inputs, but analogous functions in Z3 will return an arbitrary value of the appropriate type. Given the correct hypotheses in the ACL2(r) theorem statement, e.g. (implies (real-vec-p x) ...), this problem is mitigated. For abstract Cauchy-Schwarz, on the other hand, we require the proof to be type-independent, or the hypotheses to be otherwise free of assumptions on the particular domain in which the vectors live. The challenge is that Smtlink requires type-recognisers for each free variable in the hypothesis, discharges the trivial cases when a variable has a value of a "wrong" type, and invokes Z3 to discharge the intended case.

Smtlink supports abstract types by using Z3 theories of uninterpreted sorts and functions. These allow users to define functions (and constants as nullary functions) over abstract types and, given some assumptions about the model, reason about them. Instead of writing the type-recogniser (real-vec-p v), we now may provide Smtlink with a recogniser for an abstract type (a-vec-p v) for which the definition is encapsulated (within the encapsulation, (a-vec-p v) is functionally equivalent to (real-vec-p v)). Theorems dependent on manipulations of inequalities involving functions over abstract algebraic structures are automatically proven with Smtlink. Here is the ACL2(r) proof of Cauchy-Schwarz above:

```
(local (defthm cs1-when-v-not-zero
   (implies (and (a-vec-p u) (a-vec-p v) (vector-compatible u v) (not (vector-zero-p v)))
            (b* ((uu (inner-prod u u)) (uv (inner-prod u v)) (vv (inner-prod v v)))
                (<= (* uv uv) (* uu vv))))
   :hints
   (("Goal" :smtlink(:abstract (a-vec-p)
                     :functions((vector-add :formals ((u a-vec-p) (v a-vec-p))
                                            :returns ((sum a-vec-p))
                                            :level 0) ... ) ;; elided functions
                     :hypotheses( ...                       ;; elided hypotheses
                      ((equal (inner-prod (vector-add u (scalar-vector-prod (- (aa u v)) v))
                                          (vector-add u (scalar-vector-prod (- (aa u v)) v)))
                              (+ (inner-prod u u)
                                 (* (- 2) (aa u v) (inner-prod u v))
                                 (* (aa u v) (aa u v) (inner-prod v v)))))))))))
```

Another form of introducing abstraction into ACL2 is via monoids [1]. However, encapsulating the type-recogniser for abstract vectors was more amenable to leveraging Smtlink, which greatly simplified the proof of Cauchy-Schwarz. Regarding our choice of $\mathbb{R}$ as the co-domain of inner-prod: Cauchy-Schwarz typically only deals with vector spaces over $\mathbb{R}$ or $\mathbb{C}$, and an ordered subfield is necessary for inequalities to be well-defined. This immediately excludes finite fields and the usual induced norm by taking the square root of the inner product eliminates the last conventional candidate for fields, $\mathbb{Q}$. In the case of $\mathbb{C}$, supporting complex numbers in Z3 would require representing constants as uninterpreted nullary functions, which significantly increases the number of hypotheses to Smtlink. Nevertheless, we leave the ACL2 proof of Cauchy-Schwarz for $(V, \mathbb{C})$ as ongoing research.

References

[1] Sebastiaan J. C. Joosten, Bernard van Gastel & Julien Schmaltz (2013): *A Macro for Reusing Abstract Functions and Theorems*. *Electronic Proceedings in Theoretical Computer Science* 114, p. 2941, doi:`10.4204/eptcs.114.3`.

[2] Carl Kwan & Mark R. Greenstreet (2018): *Real Vector Spaces and the Cauchy-Schwarz Inequality in ACL2(r)*. *Electronic Proceedings in Theoretical Computer Science* 280, p. 111127, doi:`10.4204/eptcs.280.9`.

[3] Yan Peng & Mark Greenstreet (2015): *Extending ACL2 with SMT Solvers*. *Electronic Proceedings in Theoretical Computer Science* 192, p. 6177, doi:`10.4204/eptcs.192.6`.

[4] Yan Peng & Mark R. Greenstreet (2018): *Smtlink 2.0*. *Electronic Proceedings in Theoretical Computer Science* 280, p. 143160, doi:`10.4204/eptcs.280.11`.