A Lean tactic for normalising ring expressions with exponents

Anne Baanen

Lean Forward
Vrije Universiteit Amsterdam

IJCAR, 2 July 2020

Background

Lean is a proof assistant based on the calculus of constructions [2]. It has a simple kernel for proof checking and an elaborator with powerful tactic support.
The Lean community is developing `mathlib`, a repository of formalised classical mathematics proofs and proof automation.

The Lean Forward project aims to make proof assistants accessible to mathematicians by developing proof automation informed by users' needs.

Background

To a mathematician, the following is obvious:

$$2^{\mathrm{n}+1} - 1 = 2 * 2^{\mathrm{n}} - 1$$

Lean should do it automatically.

The previous `ring` tactic [1] uses Horner normal form: efficient for the semiring operators $+$ and $*$, but it doesn't support exponentiation $^\wedge$.

Background

To a mathematician, the following is obvious:

$$2^{n+1} - 1 = 2 * 2^{n} - 1$$

Lean should do it automatically.

The previous `ring` tactic [1] uses Horner normal form: efficient for the semiring operators $+$ and $*$, but it doesn't support exponentiation $^\wedge$.

It's not too hard to solve this manually: rewrite $a^{n+1} = a^{n} * a$ and `ring` can finish by applying commutativity.

Such rules don't work unconditionally: x^{100} should not become 100 multiplications of x.

Design overview

Goal: a practical normalising tactic for expressions with $+$, $*$ and $^\wedge$, numerals (in $\mathbb{Q}$) and variables. It should solve all goals that `ring` can and be approximately as fast.

Design overview

Goal: a practical normalising tactic for expressions with $+$, $*$ and $^\wedge$, numerals (in $\mathbb{Q}$) and variables. It should solve all goals that `ring` can and be approximately as fast.

To prove $\mathrm{a} = \mathrm{b}$, normalise a giving $\mathrm{p_a} : \mathrm{a} = \mathrm{a}'$ and normalise b giving $\mathrm{p_b} : \mathrm{b} = \mathrm{b}'$, then check a' is identical to b'. If identical, $\mathrm{p_a} \mathrm{p_b}^{-1}$ proves $\mathrm{a} = \mathrm{b}$.

Lean tactics typically construct proof terms directly (no reflection), since the elaborator is faster than the kernel.

The normal form is a syntax tree in the type family ex. The children for each node are restricted by a parameter ex_type:

```
inductive ex_type : Type
| sum | prod | exp | base
inductive ex : ex_type → Type
| zero  : ex_info →                           ex sum  -- 0
| sum   : ex_info → ex prod →  ex sum → ex sum  -- +
| coeff : ex_info →             coeff → ex prod -- rat
| prod  : ex_info → ex exp  → ex prod → ex prod -- *
| exp   : ex_info → ex base → ex prod → ex exp  -- ^
| var   : ex_info →              atom → ex base -- atom
| sum_b : ex_info →            ex sum → ex base -- (...)
```

- $(a + b) + c$ is not allowed: left argument to sum must be a product
- $a * (b + c)$ is not allowed: right argument to prod must be a product

Intricacies

Commutativity: pick a linear order $\prec$ on ex. Then sort $\mathrm{a} + \mathrm{b} + \mathrm{c} + \cdots$ so that $\mathrm{a} \prec \mathrm{b} \prec \mathrm{c} \prec \cdots$.

Intricacies

Commutativity: pick a linear order $\prec$ on ex. Then sort $a + b + c + \cdots$ so that $a \prec b \prec c \prec \cdots$.

To limit expression size, don't unfold $100 * a$ to $a + a + \cdots + a$.
This means keeping track of coefficients.
The function `add_overlap` decides when to add coefficients:

`add_overlap` $(3 * x^2)\ (7 * x^2) \quad = 10 * x^2$

`add_overlap` $(3 * x^2)\ (7 * y^2) \quad = 3 * x^2 + 7 * y^2$

`add_overlap` $(3 * x^2)\ (-3 * x^2) \quad = 0$ (not $0 * x^2$)

Intricacies

Commutativity: pick a linear order $\prec$ on ex. Then sort $a + b + c + \cdots$ so that $a \prec b \prec c \prec \cdots$.

To limit expression size, don't unfold $100 * a$ to $a + a + \cdots + a$.
This means keeping track of coefficients.
The function `add_overlap` decides when to add coefficients:

$$\begin{aligned}
&\texttt{add_overlap}\,(3 * x^2)\,(7 * x^2) &&= 10 * x^2 \\
&\texttt{add_overlap}\,(3 * x^2)\,(7 * y^2) &&= 3 * x^2 + 7 * y^2 \\
&\texttt{add_overlap}\,(3 * x^2)\,(-3 * x^2) &&= 0 \qquad \text{(not } 0 * x^2\text{)}
\end{aligned}$$

In a general semiring R, exponentiation has type $\wedge : R \to \mathbb{N} \to R$.
During execution, `ring_exp` keeps track of the current type using a reader monad transformer.

Optimisations

To be practical, the `ring_exp` tactic must be fast.
The Horner form used by the `ring` tactic is optimal for $+$ and $*$.
Optimisation is needed to achieve acceptable running time.

Optimisations

To be practical, the `ring_exp` tactic must be fast.
The Horner form used by the `ring` tactic is optimal for $+$ and $*$.
Optimisation is needed to achieve acceptable running time.

Typeclass instances and implicit arguments cost time to infer,
so they are cached as much as possible:
instances are stored with the current type in the reader monad,
implicit arguments and intermediate values in the `ex_info` field of `ex`.

Optimisations

To be practical, the `ring_exp` tactic must be fast.
The Horner form used by the `ring` tactic is optimal for $+$ and $*$.
Optimisation is needed to achieve acceptable running time.

Typeclass instances and implicit arguments cost time to infer,
so they are cached as much as possible:
instances are stored with the current type in the reader monad,
implicit arguments and intermediate values in the `ex_info` field of `ex`.

Result: on average a constant factor slowdown compared to `ring`.
Noticeably faster on problems with larger exponents
(20 times on $x^{50} * x^{50} = x^{100}$), also in practice for
$(1 + x^2 + x^4 + x^6) * (1 + x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7$.

Benjamin Grégoire and Assia Mahboubi. “Proving equalities in a commutative ring done right in Coq”. In: TPHOLs 2005. Ed. by J. Hurd and T. Melham. Vol. 3603. LNCS. Springer, Berlin, Heidelberg, 2005, pp. 98–113. DOI: 10.1007/11541868_7.

Leonardo de Moura et al. “The Lean theorem prover (system description)”. In: Automated Deduction - CADE-25. Ed. by A. P. Felty and A. Middeldorp. Vol. 9195. LNCS. Springer, Cham, 2015, pp. 378–388. DOI: 10.1007/978-3-319-21401-6_26.