A Formalisation of Sturm Chains in Isabelle/HOL

Manuel Eberl

September 9, 2013

1 Background

Isabelle/HOL is an interactive theorem proving environment based on *Higher Order Logic*. The Isabelle/HOLlibrary already contains a theory of univariate polynomials, including, in particular, differentiability. Furthermore, all basic analysis, such as limits and the intermediate and mean value theorem, are also available. Thus, most of the basic ingredients to formalise Sturm's theorem are available.

To explain the statement of Sturm's theorem in its most special case, we will first introduce the notion of a Sturm sequence of a polynomial.
Let $p \in \mathbb{R}[X]$ that has no multiple real roots. The *Sturm sequence*, or *Sturm chain*, of p is then defined as the sequence $p_0, p_1, \ldots p_n$ where:

$$\text{where} \quad p_i = \begin{cases} p & \text{for } i = 0 \\ p' & \text{for } i = 1 \\ -p_{i-2} \bmod p_{i-1} & \text{otherwise} \end{cases}$$

$$\text{and} \quad n = \min\{i \in \mathbb{N} \mid \text{degree}(p_i) \leq 0\}$$

Further, let $\sigma(x)$ denote the number of sign changes in the sequence $p_0(x), p_1(x), \ldots, p_n(x)$ for any $x \in \mathbb{R}$. By "sign change", we mean that a sign at one position is -1 and at the next position, skipping all zeroes, the sign is 1, or vice versa.

Sturm's theorem now states that for $a, b \in \mathbb{R}$ with $a \leq b$, the number of real roots of p in the interval $(a; b]$ is $\sigma(a) - \sigma(b)$.[1]

Based on this, a number of generalisations can be used to count roots of polynomials with multiple roots as well, and furthermore, the total number of real roots can be determined by using $\lim_{x \to \pm\infty} \sigma(x)$, which can be determined by looking at the leading coefficients of the polynomials in the chain.

2 Goal

The goal is to formulise Sturm's theorem and its aforementioned generalisations in *Isabelle/HOL*. The result should be an executable function for determining the number of roots of a polynomial. Such a function can be exported to a programming language such as ML or Haskell using Isabelle's code generator, or it can be used to implement a decision procedure fo the number of roots of a polynomial directly in Isabelle.

[1] Since p was assumed to not have multiple roots, multiplicity is not relevant for counting here.

One example for which such a decision procedure would be useful is the formalisation of algorithms for numerical approximation; for instance, there exists a formalisation of an algorithm for approximating the $\exp$ function that requires the fact that the polynomial

$$\frac{1}{120}x^5 + \frac{1}{24}x^4 + \frac{1}{6}x^3 - \frac{49}{16777216}x^2 - \frac{17}{2097152}x$$

has exactly three roots in the interval $(-0.010831, 0.010831)$. In Isabelle, this is written as:

lemma"$\mathrm{card}\ \{x :: \mathrm{real}. -0.010831 < x\ \wedge\ x < 0.010831\ \wedge$
$\mathrm{poly}\ [:0, -17/2097152, -49/16777216, 1/6, 1/24, 1/120:]\ x\ =\ 0\} = 3$"

This fact is readily checkable with any computer algebra system, but was, so far, unfeasible to prove in Isabelle. We aim to be able to prove statements like these with our proof method derived from our formalisation of Sturm chains.

3 Work outline

We estimate that the work to be done is the following:

- Define, with enough generality to allow for later generalisations and optimisations, what properties a general Sturm chain must fulfil
- Prove that a chain fulfilling these requirements can indeed be used to count roots
- Prove that the various canonical and non-canonical sturm chains fulfil these requirements
- Prove that one can determine the signs of polynomials for sufficiently large arguments by looking at the leading coefficients (this may require extension of the Polynomial library, since no lemmas about limits of polynomials exist so far)
- Use these definitions and proofs to implement a decision procedure as described above and integrate it with Isabelle