A Formalisation of Sturm's theorem in Isabelle/HOL

Manuel Eberl

January 7, 2014

Abstract

Sturm sequences are a method of efficiently computing the number of real roots of a real polynomial inside a given interval. In this project, this fact and a number of methods to construct Sturm sequences efficiently have been formalised with the interactive theorem prover Isabelle/HOL. Building upon this, an Isabelle/HOL proof method was then implemented to prove statements about the number of roots of a real polynomial and related properties.

Contents

1 Introduction

Sturm sequences are finite sequences of polynomials with certain properties that, as shown by *Sturm's Theorem*, can be used to determine the number of roots of a real polynomial in a given interval alorithmically. This is used to prove properties about the roots of specific polynomials directly, but can also be part of other algorithms such as approximation of roots through bisection, and it forms the basis of Tarski's decision procedure for real arithmetic. Implementations of Sturm sequences for these purposes exist in a number of computer algebra systems,

There are different ways to construct Sturm sequences for a fixed polynomial P. The "canonical" Sturm sequence construction works only if P has no multiple roots, but it can be adapter to the more general case of any nonzero polynomial.

Both Sturm's Theorem and these constructions were formally proven in Isabelle/HOL in this project. This paper will give a detailed account of the formalisation, including a very explicit proof that closely follows the structure of the formal proof in Isabelle/HOL, but omits the proofs for basic lemmas about real analysis and polynomials.

Section **??** introduces some basic notation for well-known concepts that are not directly related to Sturm sequence. Section **??** then defines a number of basic concepts that are used in Sturm's theorem, in particular, the concept of a *Sturm sequence*. Section **??** contains some simple auxiliary lemmas that will be required in the main proof. Section **??** contains the main portion of the proof, as it shows that Sturm sequences can be used to count the real roots of polynomials. Section **??** then shows how Sturm sequences can be constructed in different cases and how these constructions can be applied. Finally, section **??** explains how further preprocessing can be used to automatically decide more complex, interesting properties on real polynomials.

2 Notation

In our the following proofs, we will use the following notation and terminology:

- $\mathbb{R}[X]$ denotes the set of all polynomials with real coefficients.
- P' denotes the derivative of a polynomial $P \in \mathbb{R}[X]$.
- Some property holds *in a neighbourhood* of some $x_0 \in \mathbb{R}$ if there exists an $\varepsilon > 0$ such that the property holds for all $x \in (x_0 - \varepsilon; x_0 + \varepsilon) \setminus \{x_0\}$. Note that it does *not* have to hold *at x_0 itself*.
- $\mathrm{lc}(P)$ denotes the leading coefficient of a polynomial P.

3 Proof of Sturm's theorem

3.1 Definitions

First, we define two notions that will be important in the proof of Sturm's theorem:
A *quasi-Sturm sequence*[1] is a list of polynomials $P_0, P_1, \ldots, P_{n-1} \in \mathbb{R}[X]$ that fulfils the following properties:

- $n \geq 1$, i.e. the sequence is not empty
- P_{n-1} does not change its sign, i.e. $\operatorname{sgn}(P_{n-1}(x)) = \operatorname{sgn}(P_{n-1}(y))$ for all $x, y \in \mathbb{R}$
- for any $i \in \{0, \ldots, n-3\}$ and any root x_0 of P_{i+1}, $P_i(x_0)P_{i+2}(x_0) < 0$ holds

It can easily be seen that any nonempty sequence obtained by dropping a number of elements from the beginning of a quasi-Sturm sequence is again a quasi-Sturm sequence.

A *Sturm sequence* is a quasi-Sturm sequence that fulfils the following additional properties:[2]

- $n \geq 2$, i.e. the sequence contains at least two polynomials
- for any root x_0 of P_0, $P_0(x)P_1(x)$ is negative in some sufficiently small interval $(x_0 - \varepsilon; x_0)$ and positive in some sufficiently small interval $(x_0; x_0 + \varepsilon)$[3]
- P_0 and P_1 have no common roots.

In Isabelle, these two concepts are captured in *locales* of the same name.

Next, we define the notion of *sign changes*. Let $P_0, \ldots, P_{n-1} \in \mathbb{R}[X]$ be a sequence of polynomials and $x \in \mathbb{R}$. By evaluating the P_i at x, we obtain a sequence of real numbers $y_0, \ldots, y_{n-1}$. We now traverse this sequence from left to right and count how often the sign changes, i. e. how often we see a positive number and the last nonzero number in the sequence was negative (or vice versa). This is called the number of *sign changes* of the sequence $P_0, \ldots, P_{n-1}$ at the position x and is denoted as $\sigma(P_0, \ldots, P_{n-1}; x)$.
In Isabelle, this is realised by evaluating the P_i at x, deleting all zeros from the list, applying the *remdups_adj* operation on the list and taking the length of the remaining list minus one as the result. The *remdups_adj* function simply deletes equal adjacent elements in the list, e. g. it turns $[1, 2, 2, 1, 1, 1]$ into $[1, 2, 1]$.
A related notion are the sign changes "at infinity". For this, we compute the sequences

$$\left(\operatorname{sgn}\left(\lim_{x \to -\infty} P_i(x)\right)\right)_{0 \leq i < n} \quad \textit{and} \quad \left(\operatorname{sgn}\left(\lim_{x \to \infty} P_i(x)\right)\right)_{0 \leq i < n}$$

and count the sign changes in these sequences in the same way as before. The number of sign changes is called $\sigma(P_0, \ldots, P_{n-1}; -\infty)$ and $\sigma(P_0, \ldots, P_{n-1}; \infty)$, respectively. Note that the signs of these limits for a P_i can be determined by taking the sign of the leading coefficient of P_i.[4]

[1] This term is, to our knowledge, not used in any of the literature. It was "invented" solely for the purpose of this formal proof, since we need to perform explicit induction on the sequence, which does not preserve the Sturm sequence property, but does preserve the weaker notion of quasi-Sturm sequence

[2] This definition was adapted from [**sag**] as it has the virtue of being very general, allowing us to easily generalise the canonical construction later.

[3] In Isabelle/HOL, this is expressed as "eventually, the property $\operatorname{sgn}(P_0P_1(x)) = \textsf{if } x > x_0 \textsf{ then } 1 \textsf{ else } -1$ holds at x_0".

[4] For ∞ in general and for $-\infty$ and even degree, it is simply the sign of the leading coefficient; for $-\infty$ and odd degree, it is the opposite of the sign of the leading coefficient.

3.2 Important auxiliary lemmas

The first auxiliary lemma concerns the behaviour of polynomials at infinity and will be important for counting roots in intervals of infinite length.

Lemma 1. *Let $P \in \mathbb{R}[X] \setminus \{0\}$. Then there exist $l, u \in \mathbb{R}$ such that $l < u$, all roots of P are in $(l; u)$ and*

$$\forall x \leq l.\ \mathrm{sgn}(P(x)) = \mathrm{sgn}\left(\lim_{x \to -\infty} P(x)\right)$$
$$\forall x \geq u.\ \mathrm{sgn}(P(x)) = \mathrm{sgn}\left(\lim_{x \to \infty} P(x)\right)$$

Proof. Obviously, the limit of $P(x)$ at $-\infty$ (resp. ∞) is either ∞ or $-\infty$. Therefore, there exists an l (resp. a u) such that for all $x \leq l$ (resp. $x \geq u$), $P(x)$ increases above every bound in the case of the limit ∞ or falls below every bound in case of the limit $-\infty$. In particular, if we choose 0 as the bound, we see that $P(x)$ will be positive for all values beyond some point in the case of ∞ or negative in the case of $-\infty$, which implies $\mathrm{sgn}(P(x)) = \mathrm{sgn}(\lim_{x \to -\infty} P(x))$ (resp. $\mathrm{sgn}(P(x)) = \mathrm{sgn}(\lim_{x \to \infty} P(x))$) for all x beyond that point. Therefore, bounds l and u that fulfil the last two requirements exist.
Also, since the $P(x)$ is positive or negative for all x below l (resp. above u), it has no roots outside the interval $(l; u)$. Lastly, should $l < u$ not hold already, we can simply increase u until it does. □

Since Sturm's theorem is based on counting sign changes, a crucial part in proving it is to formalise the counting of sign changes in a way that is convenient for subsequent proofs. In this proof, this was done by proving that under certain conditions, the computation of the number of sign changes of a sequence can be "decomposed".

Lemma 2. *Let $P_0, \ldots, P_{n-1}$ be a sequence of polynomials and $i \in \{0, \ldots, n-1\}$ and $x \in \mathbb{R}$. Furthermore, assume $P_i(x) \neq 0$. Then $\sigma(P_0, \ldots, P_{n-1}; x) = \sigma(P_0, \ldots, P_i; x) + \sigma(P_i, \ldots, P_{n-1}; x)$*

Proof. For our informal definition of sign changes, this is obvious; for the Isabelle definition using list operation, it can be proven using simple properties of the *remdups_adj* and *filter* functions. □

Lemma 3. *Let $P, Q, R \in \mathbb{R}[X]$ and $x \in \mathbb{R}$ with $P(x) \neq 0$ and $\mathrm{sgn}(R(x)) = -\mathrm{sgn}(P(x))$. Then $\sigma(P, Q, R; x) = 1$*

Proof. By case distinction □

Lemma 4. *Let $P_0, \ldots, P_{n-1} \in \mathbb{R}[X]$, $Q_0 \ldots, Q_{n-1} \in \mathbb{R}[X]$ be two sequences of polynomials and $x \in \mathbb{R}$. Assume $\mathrm{sgn}(P_i(x_1)) = \mathrm{sgn}(Q_i(x_2))$ for all i. Then $\sigma(P_0, \ldots, P_{n-1}; x_1) = \sigma(Q_0, \ldots, Q_{n-1}; x_2)$.*

Proof. Trivial. □

Later, we will also require some algebraic properties of polynomials, such as squarefree decomposition of polynomials.

Lemma 5. *Let $P \in \mathbb{R}[X] \setminus \mathbb{R}$, i.e. a nonconstant real polynomial. Let $D := \gcd(P, P')$. Then the following holds:*

1. *$\gcd(P/D, P'/D) = 1$, i. e. P/D and P'/D are coprime*
2. *$\forall x \in \mathbb{R}.\ (P/D)(x) = 0 \iff P(x) = 0$, i. e. P and P/D have the same roots, disregarding multiplicity*

3.3 Relating roots and Sturm sequences

We will now show how Sturm sequences can be used to determine the number roots of polynomials in a given interval. To this end, we will first explore how the number of sign changes of a Sturm sequence behaves in the neighbourhood of non-roots and roots of the polynomial.

Lemma 6. *Let $P_0, \ldots, P_{n-1}$ be a quasi-Sturm sequence and $x_0 \in \mathbb{R}$. Assume $P_0(x_0) \neq 0$. Then $\sigma(P_0, \ldots, P_{n-1}; x_0)$ is constant in the neighbourhood of x_0.*

Proof. By induction over the length of the sequence

- if the sequence has length 1, the number of sign changes is, of course, 0 at any position.
- if the sequence has length 2, we know that P_1 does not change its sign anywhere by definition of a quasi-Sturm sequence. Furthermore, since $P_0(x_0) \neq 0$, the sign of P_0 does not change in the neighbourhood of x_0. By Lemma **??**, the number of sign changes of the sequence P_0, P_1 also remains constant in the neighbourhood of x_0.
- if the sequence has length ≥ 3 and $P_1(x_0) \neq 0$, Lemma **??** implies

  $$\sigma(P_0, \ldots, P_{n-1}; x_0) = \sigma(P_0, P_1; x_0) + \sigma(P_1, \ldots, P_{n-1}; x_0)$$

  Since $P_0(x_0) \neq 0$ and $P_1(x_0) \neq 0$, the signs of P_0 and P_1 do not change in the neighbourhood of x_0 and therefore $\sigma(P_0, P_1; x_0)$ is constant in the neighbourhood of x_0. Also, the sequence $P_1, \ldots, P_{n-1}$ is again a quasi-Sturm sequence with $P_1(x_0) \neq 0$, i. e. the induction hypothesis can be applied and we can conclude that $\sigma(P_1, \ldots, P_{n-1}; x_0)$ is also constant in the neighbourhood of x_0.
- if the sequence has length ≥ 3 and $P_1(x_0) = 0$, we have $P_0(x_0)P_2(x_0) < 0$ by the definition of a quasi-Sturm sequence and thus $P_0(x_0) \neq 0$, $P_2(x_0) \neq 0$, and $\operatorname{sgn}(P_2(x_0)) = -\operatorname{sgn}(P_0(x_0))$. With Lemma **??**, we have:

  $$\sigma(P_0, \ldots, P_{n-1}; x_0) = \sigma(P_0, P_1, P_2; x_0) + \sigma(P_2, \ldots, P_{n-1}; x_0)$$

  Furthermore, since $P_0(x_0) \neq 0$ and $P_2(x_0) \neq 0$, $\operatorname{sgn}(P_2(x)) = -\operatorname{sgn}(P_0(x))$ holds in the entire neighbourhood of x_0 as the signs of P_0 and P_2 do not change in the neighbourhood of x_0, and with Lemma **??**, we then have $\sigma(P_0, P_1, P_2; x) = 1$ (i. e. constant) in the entire neighbourhood of x_0. As for the second summand, we know that $P_2, \ldots, P_{n-1}$ is again a quasi-Sturm sequence and $P_2(x_0) \neq 0$, so we can apply the induction hypothesis and obtain that $\sigma(P_2, \ldots, P_{n-1}; x_0)$, too, is constant in the neighbourhood of x_0.

□

Lemma 7. *Let $P_0, \ldots, P_{n-1}$ be a Sturm sequence and $x_0 \in \mathbb{R}$. Assume $P_0(x_0) = 0$. Then for x in the neighbourhood of x_0, we have $\sigma(P_0, \ldots, P_{n-1}; x) = \sigma(P_0, \ldots, P_{n-1}; x_0) + 1$ if $x < x_0$ and $\sigma(P_0, \ldots, P_{n-1}; x) = \sigma(P_0, \ldots, P_{n-1}; x_0)$ if $x \geq x_0$.*

Proof. From the definition of a Sturm sequence, we know that $P_0(x_0) = 0$ implies $P_1(x_0) \neq 0$. Therefore, $P_1(x_0)$ has the same nonzero sign in a neighbourhood of x_0. Moreover, in a neighbourhood of x_0, we have $P_0(x)P_1(x) < 0$ if $x < x_0$ and $P_0(x)P_1(x) > 0$ if $x > x_0$. With Lemma **??**, we have:

$$\sigma(P_0, \ldots, P_{n-1}; x) = \sigma(P_0, P_1; x) + \sigma(P_1, \ldots, P_{n-1}; x) \qquad \text{in a NH of } x_0$$

Since $P_1(x_0) \neq 0$ in a neighbourhood of x_0, we can apply Lemma **??** and obtain:

$$\sigma(P_1, \ldots, P_{n-1}; x) = \sigma(P_1, \ldots, P_{n-1}; x_0) \qquad \text{in a NH of } x_0$$

Of course, since $P_0(x_0) = 0$, we also have:

$$\sigma(P_1, \ldots, P_{n-1}; x_0) = \sigma(P_0, \ldots, P_{n-1}; x_0)$$

In summary, we have shown so far that:

$$\sigma(P_0, \ldots, P_{n-1}; x) = \sigma(P_0, P_1; x) + \sigma(P_0, \ldots, P_{n-1}; x_0) \qquad \text{in a NH of } x_0$$

Therefore, what remains to be shown is that $\sigma(P_0, P_1; x) = 1$ for $x < x_0$ and $\sigma(P_0, P_1; x) = 0$ for $x > x_0$ for all x in a neighbourhood of x_0. This is a simple consequence of $P_0(x)P_1(x) < 0$ for $x < 0$ and $P_0(x)P_1(x) > 0$ for $x > 0$ and the fact that P_1 has the same sign in the entire neighbourhood of x_0. □

To express it in a less formal way: when passing through the real numbers in increasing order and tracking the number of sign changes of a Sturm sequence of a real polynomial P, that number increases by 1 every time one passes a root of P and remains constant otherwise. Intuitively, it should now be clear that Sturm sequences can be used to count the number of roots of a polynomial in a given interval. We will now prove this formally.

Lemma 8. *Let $P_0, \ldots, P_{n-1}$ be a Sturm sequence with $P_0 \neq 0$ and $x_0 \in \mathbb{R}$. Fix $a, b \in \mathbb{R}$ with $a \leq b$. Then the following holds:*

$$\sigma(P_0, \ldots, P_{n-1}; a) - \sigma(P_0, \ldots, P_{n-1}; b) = |\{x \in (a; b] \mid P_0(x) = 0\}|$$

Proof. By induction over $k := |\{x \in (a; b].\ P_0(x) = 0\}|$ for arbitrary a, b.

- if $k = 0\}| = 0$, we have $P_0(x) \neq 0$ for all $x \in (a; b]$. We now distinguish two cases:
  - if $P_0(a) \neq 0$, we have $P_0(x) \neq 0$ for all $x \in [a; b]$. Lemma **??** then implies that $\sigma(P_0, \ldots, P_{n-1})$ is constant in the neighbourhood of all $x \in [a; b]$ and must therefore be constant in the entire interval $[a; b]$ as polynomials are continuous.
  - if $P_0(a) = 0$, we know from Lemma **??** that

    $$\sigma(P_0, \ldots, P_{n-1}; x) = \sigma(P_0, \ldots, P_{n-1}; a)$$

    for all $x \in (a; a + \varepsilon)$ for some $\varepsilon > 0$, i. e. $\sigma(P_0, \ldots, P_{n-1})$ is constant in the right neighbourhood of a. Furthermore, using $P_0(x) \neq 0$ for all $x \in (a; b]$ and Lemma **??**, that $\sigma(P_0, \ldots, P_{n-1})$ is constant in the neighbourhood of every $x \in (a; b]$. Therefore, $\sigma(P_0, \ldots, P_{n-1})$ is constant on the entire interval $[a; b]$.

Since $\sigma(P_0, \ldots, P_{n-1})$ is constant on the entire interval $[a; b]$, we have

$$\sigma(P_0, \ldots, P_{n-1}; a) - \sigma(P_0, \ldots, P_{n-1}; b) = 0$$

which is exactly the number of roots of P_0 in $(a; b]$.

- if $k > 0$, we take the smallest root of P_0 in the interval $(a; b]$ and call it x_2. With Lemma **??**, we know that for all x in a sufficiently small left neighbourhood of x_2:

  $$\sigma(P_0, \ldots, P_{n-1}; x) = \sigma(P_0, \ldots, P_{n-1}; x_2) + 1$$

  Let x_1 then be some value in $(a; x_2)$ that is in this neighbourhood. We know that P_0 has no roots in the interval $(a; x_2]$ and thus, by induction hypothesis,

  $$\sigma(P_0, \ldots, P_{n-1}; a) = \sigma(P_0, \ldots, P_{n-1}; x_1) = \sigma(P_0, \ldots, P_{n-1}; x_2) + 1$$

  Furthermore, the number of roots of P_0 in the interval $(x_2; b]$ is exactly $k - 1$, so by induction hypothesis,

  $$\sigma(P_0, \ldots, P_{n-1}; x_2) - \sigma(P_0, \ldots, P_{n-1}; b) = k - 1$$

  Adding these two equations yields

  $$\sigma(P_0, \ldots, P_{n-1}; a) - \sigma(P_0, \ldots, P_{n-1}; b) = k$$

□

Lemma 9. *Let $P_0, \ldots, P_{n-1}$ be a Sturm sequence with $P_0 \neq 0$. Then the following holds:*

$$\sigma(P_0, \ldots, P_{n-1}; -\infty) - \sigma(P_0, \ldots, P_{n-1}; \infty) = |\{x \mid P_0(x) = 0\}|$$

Proof. Using Lemma **??** for every P_i and taking the smallest lower bound l and largest upper bound u, we obtain $l, u \in \mathbb{R}$ with $l < u$ such that P_0 has no roots outside the interval $(l; u)$ and for all P_i:

$$\operatorname{sgn}(P_i(l)) = \operatorname{sgn}\left(\lim_{x \to -\infty} P_i(x)\right) \quad \text{and} \quad \operatorname{sgn}(P_i(u)) = \operatorname{sgn}\left(\lim_{x \to \infty} P_i(x)\right)$$

It is then easy to see that the number of sign changes of the sequence $P_0, \ldots, P_{n-1}$ at l resp. u can be determined by considering the signs of the limits of the P_i at $\pm\infty$ instead of $P_i(u)$ and $P_i(l)$. Since all roots of P_0 lie in the interval $(l; u)$, we have thus shown that the total number of roots of P_0 can be determined in the way described above. □

Note: similar statements for the usage of σ at $\pm\infty$ to compute the number of roots $> a$, $< a$, $\geq a$, or $\leq a$ for some fixed $a \in \mathbb{R}$ can be proven analogously.

4 Constructing Sturm sequences

4.1 The canonical Sturm sequence

The canonical Sturm sequence $P_0, \ldots, P_{n-1}$ of a polynomial $P \in \mathbb{R}[X]$ is constructed as follows:

$$P_i = \begin{cases} P & \text{for } i = 0 \\ P' & \text{for } i = 1 \\ -P_{i-2} \bmod P_{i-1} & \text{otherwise} \end{cases}$$

n is chosen such that $n \geq 2$ and P_{n-1} is constant, since this will simplify formalisation. Choosing a higher value for n only results in a number of zero polynomials at the end of the sequence, which do not change the result in any way. Note that this construction always terminates as the degree of the polynomials involved strictly decreases with every step, so that one reaches a constant polynomial in finitely many steps.

Lemma 10. *For all $i \in \{0, n-2\}$, we have $\gcd(P_i, P_{i+1}) = \gcd(P, P')$*

Proof. By induction on i using the fact that

$$\gcd(R, S) = \gcd(S, R \mod S) = \gcd(S, -R \mod S)$$

□

Lemma 11. *Let $P \in \mathbb{R}[X]$ with no multiple roots. Then the canonical Sturm sequence construction of P yields an actual Sturm sequence.*

Proof. We simply prove the five conditions a Sturm sequence has to satisfy:

- the sequence has at least length 2: obvious by definition
- P_{n-1} does not change its sign: obvious, since P_{n-1} is constant
- for any $i \in \{0, \ldots, n-2\}$ and any root x_0 of P_{i+1}, $P_i(x_0)P_{i+2}(x_0) < 0$ holds:
  By construction, we have $P_{i+2} = -P_i \bmod P_{i+1}$ and thus $P_i = P_{i+1}Q - P_{i+2}$ for some $Q \in \mathbb{R}[X]$. With $P_{i+1}(x_0) = 0$, this implies that $P_{i+2}(x) = -P_i(x)$, and because of Lemma **??** and the fact that P has no multiple roots, we also have $P_i(x) \neq 0$ and thus $P_i(x)P_{i+2}(x) < 0$.
- for any root x_0 of P_0, $P_0(x)P_1(x)$ is negative in some sufficiently small interval $(x_0 - \varepsilon; x_0)$ and positive in some sufficiently small interval $(x_0; x_0 + \varepsilon)$:
  Since $P_0 = P$ and $P_1 = P'$ are polynomials, there exists some neighbourhood of x_0 that does not contain any roots of either P_0 or P_1. For any $x < x_0$ in that neighbourhood, we can then apply the mean value theorem to obtain some $\xi \in [x; x_0]$ with
  $$P'(\xi)(x - x_0) = P(x) - P(x_0) = P(x)$$
  Due to $x < x_0$ $P(x)$, this implies $\operatorname{sgn}(P(x)) = -\operatorname{sgn}(P'(\xi))$. Furthermore, recall that we chose a neighbourhood of x_0 that contains no roots of P or P'; therefore, $0 \neq \operatorname{sgn}(P'(\xi)) = \operatorname{sgn}(P'(x)) = -\operatorname{sgn}(P(x))$. This directly implies $P(x)P'(x) < 0$. Similarly, for any $x > x_0$ in that neighbourhood, we can use the same argument to find that $P(x)P'(x) > 0$.
- P_0 and P_1 have no common roots:
  $P_0 = P$ and $P_1 = P'$, so if P_0 and P_1 had a common root, it would be a multiple root of P, which contradicts our assumption.

□

4.2 The case of multiple roots

Of course, one way to handle a polynomial with multiple roots is to use lemma **??** and "divide away" the "excess roots" by dividing the polynomial P by $\gcd(P, P')$. However, surprisingly, it turns out that as long as the interval bounds a and b are not multiple roots of P themselves, i.e. at least one of $P(a) \neq 0$ and $P'(a) \neq 0$ and at least one of $P(b) \neq 0$ and $P'(b) \neq 0$ holds, one can simply use the canonical Sturm sequence without any modification. To show this, we will first prove the following auxiliary result:

Lemma 12. *Let $P \in \mathbb{R}[X] \setminus \mathbb{R}$, i.e. a nonconstant real polynomial. Let $P_0, \ldots, P_{n-1}$ be the result of the canonical Sturm sequence construction of P and define $Q_i := P_i / \gcd(P, P')$. Then Q_i is a Sturm sequence and Q_0 has the same roots, disregarding multiplicity, as P.*

Proof. First, we note that $\gcd(P, P') \neq 0$, since $P' \neq 0$ by assumption. Furthermore, lemma **??** implies that $\gcd(P, P') \mid P_i$ for all i, thus $Q_i \in \mathbb{R}[X]$, i.e. the Q_i really are polynomials. This means that our definition of $Q_0, \ldots, Q_{n-1}$ is well-defined.
Now we show that the five properties for a Sturm sequence are satisfied:

- the sequence has at least length 2: obvious by construction of $Q_0, \ldots, Q_{n-1}$
- Q_{n-1} does not change its sign: obvious, since P_{n-1} is constant, so Q_{n-1} is, too.
- Q_0 and Q_1 have no common roots:
  By construction, we have $Q_0 = P / \gcd(P, P')$ and $Q_1 = P' / \gcd(P, P')$. Obviously, Q_0 and Q_1 are then coprime and cannot have any common roots.
- for any $i \in \{0, \ldots, n-1\}$ and any root x_0 of Q_{i+1}, $Q_i(x_0)Q_{i+2}(x_0) < 0$ holds:
  By construction of the canonical Sturm sequence, we have:

  $$P_{i+2} = -P_i \bmod P_{i+1}$$

  Therefore, we have:

  $$(P_i \operatorname{div} P_{i+1}) \cdot P_{i+1} - P_{i+2} = P_i$$

  Let $D := \gcd(P, P')$. Since D divides all the P_j, we have $P_i = D \cdot Q_i$, $P_{i+1} = D \cdot Q_{i+1}$, and $P_{i+2} = D \cdot Q_{i+2}$ and thus:

  $$(D \cdot Q_i \operatorname{div} D \cdot Q_{i+1}) \cdot D \cdot Q_{i+1} - D \cdot Q_{i+2} = D \cdot Q_i$$

  Cancelling D (allowed since $\mathbb{R}[X]$ is an integral domain and $D \neq 0$) yields:

  $$(Q_i \operatorname{div} Q_{i+1}) \cdot Q_{i+1} - Q_{i+2} = Q_i$$

  Since x_0 is a root of $Q_{i+1}(x_0)$, we then have:

  $$-Q_{i+2}(x_0) = Q_i(x_0)$$

  Since $\gcd(Q_i, Q_{i+1}) = 1$ and x_0 is a root of $Q_{i+1}(x_0)$, x_0 cannot be a root of Q_i and thus we have:

  $$Q_i(x_0)Q_{i+2}(x_0) = -Q_i(x_0)^2 < 0$$

- for any root x_0 of Q_0, $Q_0(x)Q_1(x)$ is negative in some sufficiently small interval $(x_0 - \varepsilon; x_0)$ and positive in some sufficiently small interval $(x_0; x_0 + \varepsilon)$:
  Let, again, $D := \gcd(P, P')$. Obtain some an $\varepsilon > 0$ such that the following two properties hold:

  1. D does not have a root in $(x_0 - \varepsilon; x_0 + \varepsilon) \setminus \{x_0\}$
  2. $P_0(x)P_1(x) < 0$ for all $x \in (x_0 - \varepsilon; x_0)$ and $P_0(x)P_1(x) > 0$ for all $x \in (x_0; x_0 + \varepsilon)$

  Then we have, for any x in $(x_0 - \varepsilon; x_0 + \varepsilon) \setminus \{x_0\}$:

  $$P_0(x)P_1(x) = Q_0(x)Q_1(x) \cdot \underbrace{D(x)^2}_{>0}$$

  This then obviously implies the property we want to show.

It remains to show that Q_0 has the same roots, disregarding multiplicity, as $P = P_0$. This is precisely the statement of lemma **??**. □

Of course, there is no reason to use this construction in practice, since if one has computed $\gcd(P, P')$ already, it is easier to compute the canonial Sturm sequence of $P/\gcd(P, P')$ directly than to compute the canonical Sturm sequence of P and then divide every polynomial in it by $\gcd(P, P')$. However, it becomes useful when combined with the following insight:

Lemma 13. *Let $P \in \mathbb{R}[X] \setminus \mathbb{R}$, i.e. a nonconstant real polynomial. Let $P_0, \ldots, P_{n-1}$ and $Q_0, \ldots, Q_{n-1}$ be as in the previous lemma. Then the following holds:*

1. $\forall x \in \mathbb{R}.\ P(x) \neq 0 \vee P'(x) \neq 0 \Longrightarrow \sigma(Q_0, \ldots, Q_{n-1}; x) = \sigma(P_0, \ldots, P_{n-1}; x)$
2. $P \neq 0 \Longrightarrow \sigma(Q_0, \ldots, Q_{n-1}; \pm\infty) = \sigma(P_9, \ldots, P_{n-1}; \pm\infty)$

Proof.

1. Let $D := \gcd(P, P')$. Consider an arbitrary $x \in \mathbb{R}$ for which $P(x) \neq 0$ or $P'(x) \neq 0$, i. e. $D(x) \neq 0$. Then we have for all i:

   $$\operatorname{sgn}(Q_i(x)) = \operatorname{sgn}(P_i(x)/D(x)) = \operatorname{sgn}(P_i(x)) \cdot \operatorname{sgn}(D(x))$$

   It is now easy to see that in both of the two cases $D(x) > 0$ and $D(x) < 0$, the number of sign changes in the two sequences is the same, since the signs in $Q_0, \ldots, Q_{n-1}$ are all either the same as in $P_0, \ldots, P_{n-1}$ or all flipped w. r. t. the signs in $P_0, \ldots, P_{n-1}$.

2. We now consider the case of $\pm\infty$. Since $P_i = Q_i \cdot D$, we obviously have $\operatorname{lc}(P_i) = \operatorname{lc}(D) \cdot \operatorname{lc}(Q_i)$. When considering the way in which σ at $\pm\infty$ can be computed using the leading coefficients, it is then again obvious that the two sign sequences are either the same or one is "flipped" w. r. t. the other; in either way, we have $\sigma(Q_0, \ldots, Q_{n-1}; \pm\infty) = \sigma(P_0, \ldots, P_{n-1}; \pm\infty)$.

□

In conclusion: if we want to count the roots of some P between bounds $a, b \in \mathbb{R} \cup \{-\infty, \infty\}$ with $a \leq b$, we use σ with a Sturm sequence of P, and such a Sturm sequence can be obtained by applying the canonical Sturm sequence construction to P if neither a nor b are roots of both P and P', or by applying it to $P/\gcd(P, P')$ if they are.

5 Applications

The statements that were proven in lemma **??** and lemma **??** were that Sturm sequences can be used to count the roots of a polynomial P in an interval of the form $(a; b]$ for $a, b \in \mathbb{R}$, $a < b$ or in the interval $(-\infty; \infty)$. However, by adding case distinctions on whether a and b are roots of P, this can easily be generalised to arbitrary open, half-closed, closed, bounded, and unbounded real intervals.
Furthermore, statements such as $\forall x \in I.\, P(x) \neq 0$ can be decided by counting the number of roots with the above method and checking whether it is zero.
By observing that for any two polynomials P and Q, we have

$$\begin{aligned} P(x) = 0 \wedge Q(x) = 0 \quad &\iff \quad \gcd(P, Q) = 0 \\ P(x) = 0 \vee Q(x) = 0 \quad &\iff \quad (P \cdot Q)(x) = 0 \end{aligned}$$

we can further generalise our method to arbitrary statements of the form

$$(\forall x \in I.\, P(x)) \quad \text{and} \quad |\{x \in I \mid Q(x)\}| = n$$

where I is an open, half-closed, or closed, bounded or unbounded real interval and P is a property consisting of the operators $\wedge$, $\vee$, $+$, $-$, $\cdot$, ^{c}, $\neq$ and Q is a property consisting of the operators $\wedge$, $\vee$, $+$, $-$, $\cdot$, ^{c}, $=$.

Independently from this, the observation that $\forall x \in I.\, P(x) > 0$ holds iff P has no roots in I and $\lim_{x\to\infty} P(x) = \infty$ also allows us to decide statements of the form

$$(\forall x \in I.\, P(x) > 0) \quad \text{and} \quad (\forall x \in I.\, P(x) < 0)$$

Concrete examples of statements that can be proved in Isabelle/HOL by the *sturm* method that implements the decision procedure we just explained are: [5]

lemma "card $\{x ::$ real. $(x-1)^2 * (x+1) = 0\} = 2$" **by** sturm
lemma "card $\{x ::$ real. $-0.010831 < x \wedge x < 0.010831 \wedge$
poly $[: 0, -17/2097152, -49/16777216, 1/6, 1/24, 1/120 :]\ x = 0\} = 3$" **by** sturm
lemma "card $\{x ::$ real. $x^3 + x = 2 * x^2 \wedge x^3 - 6 * x^2 + 11 * x = 6\} = 1$" **by** sturm
lemma "card $\{x ::$ real. $x^3 + x = 2 * x^2 \vee x^3 - 6 * x^2 + 11 * x = 6\} = 4$" **by** sturm
lemma "$(x ::$ real$)^2 + 1 > 0$" **by** sturm
lemma "$(x ::$ real$) > 0 \implies x^2 + 1 > 0$" **by** sturm
lemma "$[\![(x ::$ real$) > 0; x \leq 2/3]\!] \implies x * x \neq x$" **by** sturm
lemma "$(x ::$ real$) > 1 \implies x * x > x$" **by** sturm

For more information on the proof method, refer to the user guide [**sturm_userguide**].

[5] For readers that are not familiar with Isabelle, "card" denotes the cardinality of a set, and "poly" constructs a polynomial from a list of coefficients, the first list element being the constant coefficient, the second one being the linear coefficient and so on. Moreover, in Isabelle, free variables in statements are implicitly universally quantified by convention.