Quantifier elimination with Sturm sequences

The seminar showed that you can use Sturm sequences to transform a formula $\exists X. S(X, T)$ to a system of equations and inequalities only depending on $T$. Here now an example similar to Exercise 6.4 with a polynomial in $x$ and depending on parameters $a$ and $c$. We want to eliminate the existential quantifier from the formula $\exists x. x^4 + ax^3 + c$. We start with building the Sturm sequence.

\[
P = P_0 = x^4 + ax^3 + c \\
P_1 = P' = 4x^3 + 3ax^2 \\
P_2 = \text{negative remainder of the division of } P_0 \text{ by } P_1 \\
P_2 = -(P_0 \mod P_1) = \frac{1}{16}(3a^2x^2 - 16c) \triangleq 3a^2x^2 - 16c
\]

We can multiply polynomials in the Sturm sequence with positive real numbers to get nicer looking integer coefficients. This works because it doesn’t change the sign and the divisibility/roots of the polynomial (regarding division in $\mathbb{R}[X]$).

Since we look at the limits at $-\infty$ and $\infty$ it’s necessary to do a case distinction on the leading coefficients. In our example the leading coefficient of $P_2$ is depending on $a$ and can become 0:

Case 1: $a = 0$

Then $P_0 = x^4 + c$, $P_1 = 4x^3$ and $P_2 = -16c$. The leading coefficient of $P_2$ is now $c$. We need another case distinction.

Case 1.1: $a = 0$, $c = 0$

Then $P_0 = x^4$, $P_1 = 4x^3$ and $P_2 = 0$. By having a look at the sign changes at $-\infty$ and $\infty$ we see that $P$ has one root. If a polynomial evaluates to zero in the Sturm algorithm, we simply ignore it.

\[
\begin{array}{c|cc}
  & -\infty & \infty \\
P_0 & + & + \\
P_1 & - & + \\
P_2 & 0 & 0 \\
\end{array}
\]

Case 1.2: $a = 0$, $c \neq 0$

Then $P_0 = x^4 + c$, $P_1 = 4x^3$ and $P_2 = -16c$.

\[
\begin{array}{c|cc}
  & -\infty & \infty \\
P_0 & + & + \\
P_1 & - & + \\
P_2 & -\text{sign}(c) & -\text{sign}(c) \\
\end{array}
\quad
\begin{array}{c|cc}
  & -\infty & \infty \\
P_0 & + & + \\
P_1 & - & + \\
P_2 & - & - \\
\end{array}
\quad
\begin{array}{c|cc}
  & -\infty & \infty \\
P_0 & + & + \\
P_1 & - & + \\
P_2 & + & + \\
\end{array}
\]

So $P$ has two roots for $a = 0$ and $c < 0$ and no roots for $a = 0$ and $c > 0$.

Case 2: $a \neq 0$

\[
P_3 = \frac{1}{3a^3}(-64cx - 48ac) \triangleq -64cx - 48ac
\]

Looking at the leading coefficient leads to another case distinction.

Case 2.1: $a \neq 0$, $c = 0$

Then $P_0 = x^4 + ax^3$, $P_1 = 4x^3 + 3ax^2$, $P_2 = 3a^2x^2$ and $P_3 = 0$. 

So for \( a \neq 0 \) and \( c = 0 \) \( P \) has two roots. As you can easily see those are 0 and \(-a\) since \( x^4 + ax^3 = x^3(x + a) \).

**Case 2.2: \( a \neq 0, c \neq 0 \)**

\[
P_4 = \frac{1}{256}(-27a^4 + 256c) \leq -27a^4 + 256c
\]

Hey, how about a case distinction?

**Case 2.2.1: \( a \neq 0, c \neq 0, P_4 = 0 \)**

Then \( P_0 = x^4 + ax^3 + c, P_1 = 4x^3 + 3ax^2, P_2 = 3a^2x^2 - 16c, P_3 = -64cx - 48ac \) and \( P_4 = 0 \).

\[
\begin{array}{c|cc}
\text{ } & -\infty & \infty \\
P_0 & + & + \\
P_1 & - & + \\
P_2 & + & + \\
P_3 & \text{sign}(c) & -\text{sign}(c) \\
P_4 & 0 & 0 \\
\end{array}
\]

So \( P \) has one real roots if \( c > 0 \) and three roots if \( c < 0 \). But the case \( c < 0 \) is in contradiction to \(-27a^4 + 256c = 0 \iff c = \frac{27}{256}a^4\). We can ignore this case.

**Case 2.2.2: \( a \neq 0, c \neq 0, P_4 \neq 0 \)**

Then \( P_0 = x^4 + ax^3 + c, P_1 = 4x^3 + 3ax^2, P_2 = 3a^2x^2 - 16c, P_3 = -64cx - 48ac \) and \( P_4 = -27a^4 + 256c \).

\[
\begin{array}{c|cc}
\text{ } & -\infty & \infty \\
P_0 & + & + \\
P_1 & - & + \\
P_2 & + & + \\
P_3 & \text{sign}(P_4) & \text{sign}(P_4) \\
P_4 & 0 & 0 \\
\end{array}
\]

\[
\begin{array}{cc|cc|cc|cc}
\text{ } & \text{ } & \text{ } & c > 0 & P_4 > 0 & c > 0 & P_4 < 0 & c < 0 & P_4 > 0 & c < 0 & P_4 < 0 \\
\text{ } & \text{ } & \text{ } & -\infty & \infty & -\infty & \infty & -\infty & \infty & -\infty & \infty \\
P_0 & + & + & P_0 & + & + & P_0 & + & + & P_0 & + & + \\
P_1 & - & + & P_1 & - & + & P_1 & - & + & P_1 & - & + \\
P_2 & + & + & P_2 & - & - & P_2 & + & + & P_2 & + & + \\
P_4 & + & + & P_4 & + & + & P_4 & + & + & P_4 & + & + \\
\text{ } & \text{ } & \text{ } & 0 \text{ roots} & 2 \text{ roots} & 4 \text{ roots} & 2 \text{ roots} & \text{ } & \text{ } & \text{ } & \text{ } \\
\end{array}
\]

The third case \( c < 0 \) and \( P_4 > 0 \) is a contradiction and can be ignored in the final formula.

**Conclusion**

By gathering all cases where \( P \) has roots, we can now eliminate the existential quantifier. We can also negate the cases where \( P \) has no roots to get an also equivalent formula.
\[ \exists x. x^4 + a \cdot x^3 + c = 0 \]
\[ \iff \]
\[ (a = 0 \land c = 0) \lor (a = 0 \land c < 0) \lor (a \neq 0 \land c > 0 \land -27a^4 + 256c = 0) \lor (a \neq 0 \land c > 0 \land -27a^4 + 256c < 0) \lor (a \neq 0 \land c < 0 \land -27a^4 + 256c < 0) \]
\[ \iff \neg((a = 0 \land c > 0) \land (a \neq 0 \land c > 0 \land -27a^4 + 256c > 0)) \]

The above formula could of course be further simplified.

What to take from all of this:

- You can multiply all polynomials in the Sturm sequence with positive real numbers without changing the result of the algorithm (even \( P_0 \)).
- You have to make a case distinction if the leading coefficient of a Sturm polynomial contains a parameter.
- Avoid doing long division on complex polynomials by hand. It’s cumbersome and error prone.