I am proving Descartes' Rule of Signs in Lean for my final project. The theorem states that if the nonzero terms of a single-variable polynomial with real coefficients are ordered by descending exponent of the variable, then the number of positive roots of the polynomial is either equal to the number of sign changes between consecutive nonzero coefficients, or is less than it by an even number.

For example, if the number of sign changes is 0 or 1, then there are exactly 0 or 1 positive roots, respectively.

A simple proof as follows comes from https://www.jstor.org/stable/4145072?origin=crossref:

Some definitions: Write the polynomial $f(x)$ as $\sum_{i=0}^{n} a_i x^{b_i}$ where we have integer powers $0 < g_0 < b_1 < \cdots < b_n$ and nonzero coefficients $a_i \neq 0$. Let $V(f)$ be the number of sign changes of the coefficients of f, meaning the number of k such that $a_k a_{k+1} < 0$. Let $Z(f)$ be the number of strictly positive roots, counting multiplicity.

Formally stating Descartes' rule as follows: Thenumber of strictly positive roots (counting multiplicity) of f is equal to the number of sign changes in the coefficients of f, minus a nonnegative even number.

If $b_0 > 0$, then we can divide the polynomial by b_0, which would not change its number of strictly positive roots. Without loss of generality, let $b_0 = 0$.

Lemma: If $a_n a_0 > 0$, then $Z(f)$ is even. If $a_n a_0 < 0$, then $Z(f)$ is odd.

Note, this concludes all cases because $a_n a_0 \neq 0$ because $a_n, a_0 \neq 0$ by definition.

Proof of Lemma: $f(x)$ starts at $f(0) = a_0 > 0$ and ends at $f(+\infty) = +\infty > 0$, so it must cross the positive x-axis an even number of times, each of which contributes to an odd number of roots, and glance without cross the positive x-axis an arbitrary number of times (each of which contributes an even number of roots). The case for the other part is done similarly in lean.

Proof of the main theorem: From the lemma, it follows that $Z(f)$ and $V(f)$ always have the same parity. We now show that $Z(f) \leq V(f)$. We induct on n. If $n = 0, 1$, the proof is straightforward, and the example was given previously. Assume $n \geq 2$. By the Induction Hypothesis, $Z(f') = V(f') - 2s$ for some $s \in \mathbb{Z}^+$. By Rolle's theorem, there exists at least one positive root of f' between any two different positive roots of f. Also, any k-multiple positive root of f is a $k-1$-multiple root of f'. Therefore, $Z(f') \geq Z(f) - 1$.

If $a_0 a_1 \geq 0$, then $V(f') = V(f)$, else $V(f') = V(f) - 1$. In either case, $V(f') \leq V(f)$.

Combining these gives us

$$Z(f) \leq Z(f') + 1 = V(f') - 2s + 1 \leq V(f) - 2s + 1 \leq V(f) + 1$$

Further, since $Z(f)$ and $V(f)$ have the same parity, we have $Z(f) \leq V(f)$.

In the next update, I'll add comments on how I properly structured my lean code to match this proof and explanations on how I used mathlib's properties to succinctly and cleanly prove this theorem.