The Fundamental Theorem of Algebra in ACL2

Ruben Gamboa and John Cowles

Department of Computer Science
University of Wyoming
Laramie, Wyoming 82071

{ruben,cowles}@uwyo.edu

ACL2 Workshop 2018
Austin, TX

UNIVERSITY OF WYOMING

Outline

The Theorem

Theorem

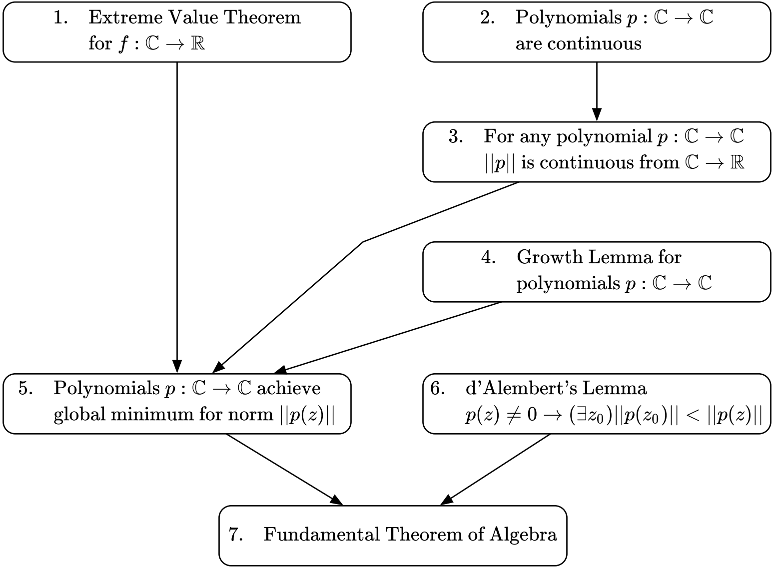
Suppose p is a non-constant, complex polynomial with complex coefficients, then there is some complex number z such that $p(z) = 0$.

The Theorem

```
(defun-sk polynomial-has-a-root (poly)
  (exists (z)
          (equal (eval-polynomial poly z) 0)))

(defthm fundamental-theorem-of-algebra-sk
  (implies (and (polynomial-p poly)
                (not (constant-polynomial-p poly)))
           (polynomial-has-a-root poly))
  :hints ...)
```

Proof Outline



Outline

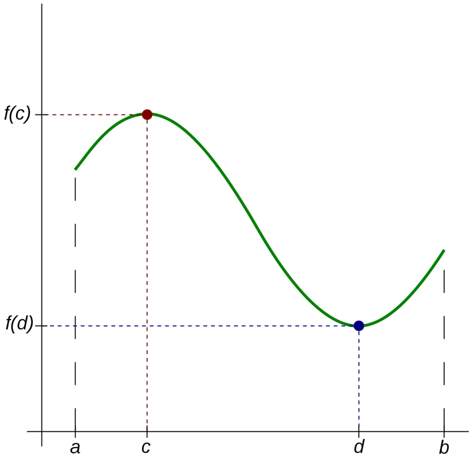
- Overview
- Extreme Value Theorem
- Continuity
- Growth Lemma for Polynomials
- D'Alembert's Lemma
- Conclusion

Extreme Value Theorem (Reals)

Theorem

Suppose f is a real function that is continuous on the interval $[a, b]$. Then there exists some $d \in [a, b]$ such that $(\forall x \in [a, b])(f(d) \leq f(x))$.

Extreme Value Theorem (Reals)

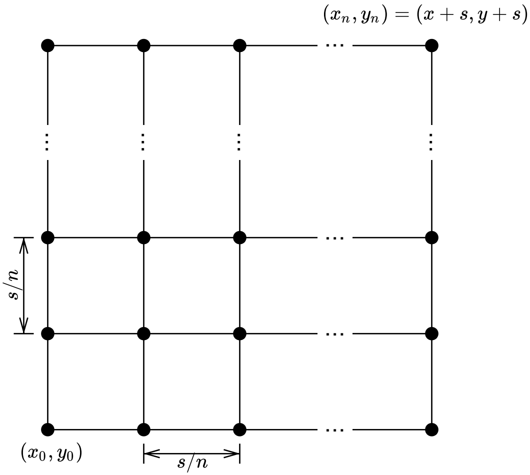


Extreme Value Theorem (Complex $\to$ Reals)

Theorem

Suppose f is a real-valued, complex function that is continuous on a closed, bounded region A. Then there exists some $d \in A$ such that $(\forall x \in A)(f(d) \leq f(x))$.

Extreme Value Theorem (Complex $\to$ Reals)



The Extreme Value Theorem

```
(defthm minimum-point-in-region-theorem-sk
  (implies (and (acl2-numberp z0)
                (realp s)
                (< 0 s)
                (inside-region-p z0 (crvcfn-domain))
                (inside-region-p (+ z0 (complex s s)) (crvcfn-domain)))
           (achieves-minimum-point-in-region context z0 s))
  :hints ...)
```

The Extreme Value Theorem

```
(defun-sk achieves-minimum-point-in-region (context z0 s)
  (exists (zmin)
          (implies (and (acl2-numberp z0)
                        (realp s)
                        (< 0 s))
                   (and (inside-region-p
                               zmin
                               (cons (interval (realpart z0)
                                               (+ s (realpart z0)))
                                     (interval (imagpart z0)
                                               (+ s (imagpart z0)))))
                        (is-minimum-point-in-region context
                                                    zmin z0 s)))))
```

The Extreme Value Theorem

```
(defun-sk is-minimum-point-in-region (context zmin z0 s)
  (forall (z)
      (implies (and (acl2-numberp z)
                    (acl2-numberp z0)
                    (realp s)
                    (< 0 s)
                          (inside-region-p
                            z
                              (cons (interval (realpart z0)
                                              (+ s (realpart z0)))
                                    (interval (imagpart z0)
                                              (+ s (imagpart z0))))))
               (<= (crvcfn context zmin) (crvcfn context z)))))
```

Outline

Continuity

Definition

A function f is continuous at a **standard** point x_0 if $f(x_0)$ is close to $f(x)$ whenever x_0 is close to x.

Continuity

Definition

A function f is continuous at a **standard** point x_0 in a **standard** context if $f(context, x_0)$ is close to $f(context, x)$ whenever x_0 is close to x.

Polynomials

- We use lists of coefficients to represent polynomials, e.g., `'(C B A)` to represent the polynomial $Ax^2 + Bx + C$
- The function `eval-polynomial` is used to interpret polynomials

Polynomials

- We use lists of coefficients to represent polynomials, e.g., `'(C B A)` to represent the polynomial $Ax^2 + Bx + C$
- The function `eval-polynomial` is used to interpret polynomials

- `(eval-polynomial poly x)` is continuous at x, using `poly` as the "context"

Minimum Value for Polynomials

- If p is a polynomial, then the function $||p(z)||$ from $\mathbb{C}$ to $\mathbb{R}$ is continuous
- By the EVT, it achieves its minimum value on any closed, bounded region

Outline

- Overview
- Extreme Value Theorem
- Continuity
- **Growth Lemma for Polynomials**
- D'Alembert's Lemma
- Conclusion

A Useful Bound

- Suppose $p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n$, where $a_n \neq 0$
- Then for large enough z:

$$\begin{aligned} ||p(z)|| &= ||a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n|| \\ &\leq ||a_0|| + ||a_1 z|| + ||a_2 z^2|| + \cdots + ||a_n z^n|| \\ &\leq ||a_0|| + ||a_1||\,||z|| + ||a_2||\,||z^2|| + \cdots + ||a_n||\,||z^n|| \\ &\leq A\left(||z^0|| + ||z^1|| + ||z^2|| + \cdots + ||z^n||\right) \\ &\leq A(n+1)||z^n|| \\ &\leq K||z^{n+1}|| \end{aligned}$$

- The last inequality holds for any real constant K

An Upper Bound

- Suppose p is any polynomial
- Then for large enough z and any constant K, $||p(z)|| \leq K||z^{n+1}||$

- Consider another polynomial $q(z) = b_0 + b_1 z + b_2 z^2 + \cdots + b_n z^n$

$$\begin{aligned}
||q(z)|| &= ||b_0 + b_1 z + b_2 z^2 + \cdots + b_{n-1} z^{n-1} + b_n z^n|| \\
&\leq ||b_0 + b_1 z + b_2 z^2 + \cdots + b_{n-1} z^{n-1}|| + ||b_n z^n|| \\
&\leq K||z^n|| + ||b_n z^n|| \\
&\leq \frac{||b_n||}{2}||z^n|| + ||b_n||\,||z^n|| \\
&= \frac{3}{2}\,||b_n||\,||z^n||
\end{aligned}$$

- The last inequality comes from letting K be $\frac{||b_n||}{2}$

A Lower Bound

- Consider the polynomial $q(z) = b_0 + b_1 z + b_2 z^2 + \cdots + b_n z^n$

$$\begin{aligned}
||q(z)|| &= ||b_n z^n - (-b_0 - b_1 z - b_2 z^2 - \cdots - b_{n-1} z^{n-1})|| \\
&\geq ||b_n z^n|| - || - b_0 - b_1 z - b_2 z^2 - \cdots - b_{n-1} z^{n-1}|| \\
&= ||b_n z^n|| - ||b_0 + b_1 z + b_2 z^2 + \cdots + b_{n-1} z^{n-1}|| \\
&\geq ||b_n|| \, ||z^n|| - \frac{1}{2} ||b_n|| \, ||z^n|| \\
&= \frac{1}{2} ||b_n|| \, ||z^n||
\end{aligned}$$

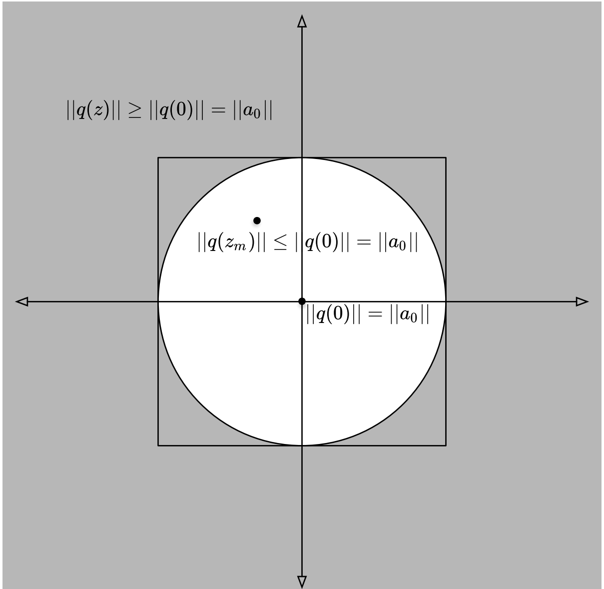
A Lower Bound

- Consider the polynomial $q(z) = b_0 + b_1 z + b_2 z^2 + \cdots + b_n z^n$

$$\frac{1}{2} ||b_n|| \, ||z^n|| \leq ||q(z)|| \leq \frac{3}{2} ||b_n|| \, ||z^n||$$

- This holds for large enough z
- The most important fact for us is that for large enough z, the value of $||q(z)||$ can't be that small

The Global Minimum of $||q(z)||$



Outline

D'Alembert's Lemma

Theorem

Suppose p is a non-constant polynomial, and $z \in \mathbb{C}$ *is such that* $p(z) \neq 0$. *Then there is some* z_0 *such that* $||p(z_0)|| < ||p(z)||$. *In particular, if* $p(z) \neq 0$ *then* z *cannot be a global minimum of* $||p(\cdot)||$.

Proof

- We prove this for a special case and only when $z = 0$:

$$\begin{aligned} p(z) &= 1 + a_1 z + a_2 z^2 + \cdots + a_n z^n \\ &= 1 + a_k z^k + z^{k+1} q(z) \end{aligned}$$

- This last equality works for <u>some</u> value of k and <u>some</u> polynomial $q(z)$

Proof

- So $||p(z)|| \leq ||1 + a_k z^k|| + ||z^{k+1} q(z)||$

- Suppose s is real with $0 < s < 1$
- We can always find a z such that $a_k z^k = -s$
- So for any s with $0 < s < 1$, we can find a z such that $||1 + a_k z^k|| = 1 - s$

Proof

$$
\begin{aligned}
||p(z)|| &\leq 1 - s + ||z^{k+1}||\,||q(z)|| \\
&= 1 - s + ||z||^{k}\,||z||\,||q(z)|| \\
&= 1 - s + \frac{s}{||a_k||}\,||z||\,||q(z)|| \\
&= 1 - s\left(1 - \frac{||z||}{||a_k||}\,||q(z)||\right)
\end{aligned}
$$

Proof

$$
\begin{aligned}
||p(z)|| &\leq 1 - s + ||z^{k+1}|| \, ||q(z)|| \\
&= 1 - s + ||z||^k \, ||z|| \, ||q(z)|| \\
&= 1 - s + \frac{s}{||a_k||} \, ||z|| \, ||q(z)|| \\
&= 1 - s \left(1 - \frac{||z||}{||a_k||} \, ||q(z)|| \right) \\
&\leq 1 - s \left(1 - \frac{||z||}{||a_k||} \, A(n+1) \right)
\end{aligned}
$$

Proof

$$\begin{aligned} ||p(z)|| &\leq 1 - s + ||z^{k+1}|| \, ||q(z)|| \\ &= 1 - s + ||z||^k \, ||z|| \, ||q(z)|| \\ &= 1 - s + \frac{s}{||a_k||} ||z|| \, ||q(z)|| \\ &= 1 - s \left(1 - \frac{||z||}{||a_k||} ||q(z)|| \right) \\ &\leq 1 - s \left(1 - \frac{||z||}{||a_k||} A(n+1) \right) \\ &\leq 1 - s \\ &< 1 \\ &= ||p(0)|| \end{aligned}$$

- We can choose a value of z such that $\frac{||z||}{||a_k||} A(n+1) < 1$
- And now we can pick the s that will result in that particular z

D'Alembert's Lemma

```
(defthm lowest-exponent-split-10
  (implies (and (polynomial-p poly)
                (equal (car poly) 1)
                (< 1 (len poly))
                (not (equal (leading-coeff poly) 0)))
           (< (norm2 (eval-polynomial
                        poly
                        (fta-bound-1 poly
                                     (input-with-smaller-value
                                        poly))))
              1))
  :hints ...)
```

Wrapping Up the Proof

- We know that $p(0) = 1$ and 0 cannot be the global minimum of $||p(\cdot)||$
- That was a special case, but we can extend it to any polynomial

- Divide by a_0, so that $p(0) \neq 0$
- Shift the polynomial, so that $p(x_0) \neq 0$
- Handle the case when the leading coefficient is 0

Outline

Wrapping Up the Main Proof

- We know that there is some x_{min} that is a global minimum of $||p(\cdot)||$
- We also know that if $p(x_{min}) \neq 0$, then x_{min} can't be a global minimum
- So $p(x_{min}) = 0$

The Fundamental Theorem of Algebra

```
(defun-sk polynomial-has-a-root (poly)
  (exists (z)
          (equal (eval-polynomial poly z) 0)))

(defthm fundamental-theorem-of-algebra-sk
  (implies (and (polynomial-p poly)
                (not (constant-polynomial-p poly)))
           (polynomial-has-a-root poly))
  :hints ...)
```