A lower degree bound for the Real Nullstellensatz and pseudo-densities with minimal norm

Sebastian Gruler

doctoral student
supervised by Markus Schweighofer

University of Konstanz, Germany

Workshop on Positive Semidefinite Rank

Institute for Matheical Sciences
National University of Singapore

February 05, 2016

Outline

Given a set of polynomials $f_1, \ldots, f_s \in \mathbb{R}[\underline{X}] := \mathbb{R}[X_1, \ldots, X_n]$.
The system $f_1 = 0, \ldots, f_r = 0$ has a Real Nullstellensatz refutation (RNR), if there exist $g_1, \ldots, g_s, h_1, \ldots, h_t \in \mathbb{R}[\underline{X}]$ with

$$\sum_{i=1}^{s} f_i g_i = 1 + \sum_{j=1}^{t} h_j^2.$$

Given a set of polynomials $f_1,\dots,f_s \in \mathbb{R}[\underline{X}] := \mathbb{R}[X_1,\dots,X_n]$.
The system $f_1 = 0,\dots,f_r = 0$ has a Real Nullstellensatz refutation (RNR), if there exist $g_1,\dots,g_s,h_1,\dots,h_t \in \mathbb{R}[\underline{X}]$ with

$$\sum_{i=1}^{s} f_i g_i = 1 + \sum_{j=1}^{t} h_j^2.$$

Such a RNR certify, that the system

$$f_1 = 0,\dots,f_s = 0$$

has no solution in $\mathbb{R}^n$.

Given a set of polynomials $f_1, \dots, f_s \in \mathbb{R}[\underline{X}] := \mathbb{R}[X_1, \dots, X_n]$.
The system $f_1 = 0, \dots, f_r = 0$ has a Real Nullstellensatz refutation (RNR), if there exist $g_1, \dots, g_s, h_1, \dots, h_t \in \mathbb{R}[\underline{X}]$ with

$$\sum_{i=1}^{s} f_i g_i = 1 + \sum_{j=1}^{t} h_j^2.$$

Such a RNR certify, that the system

$$f_1 = 0, \dots, f_s = 0$$

has no solution in $\mathbb{R}^n$. The degree of such a RNR is defined as

$$\max_{\substack{1 \le i \le s \\ 1 \le j \le t}} \{\deg f_i g_i, 2 \cdot \deg h_j\}$$

Consider the system

$$f = X_1 + \ldots + X_n - r = 0, \quad f_i = X_i^2 - X_i = 0, \ 1 \leq i \leq n \tag{1}$$

with $0 < r < n$ and $r \notin \mathbb{N}$.

Consider the system

$$f = X_1 + \ldots + X_n - r = 0, \quad f_i = X_i^2 - X_i = 0, \ 1 \leq i \leq n \tag{1}$$

with $0 < r < n$ and $r \notin \mathbb{N}$.

Theorem (Grigoriev, 2001)

Let $0 \leq k$ be an integer with $k < r < n - k$. Then the degree of any RNR of (1) is at least $d := \min\{2k+4, n+1\}$

Sketch of the proof:

Sketch of the proof:
Assume there is a RNR with degree $< d$. Then there exist $g, g_1, \dots, g_n, \in \mathbb{R}[\underline{X}],\ h \in \sum \mathbb{R}[\underline{X}]^2$ with $\deg g \leq n-1,\ \deg h \leq \min\{2k+2, n-1\}$ with

$$fg + \sum_{i=1}^{n} f_i g_i = 1 + h. \tag{2}$$

Sketch of the proof:
Assume there is a RNR with degree $< d$. Then there exist $g, g_1, \ldots, g_n, \in \mathbb{R}[\underline{X}],\ h \in \sum \mathbb{R}[\underline{X}]^2$ with $\deg g \leq n-1,\ \deg h \leq \min\{2k+2, n-1\}$ with

$$fg + \sum_{i=1}^{n} f_i g_i = 1 + h. \tag{2}$$

As Grigoriev, we construct a linear functional $L : \mathbb{R}[\underline{X}] \to \mathbb{R}$, that applied to the left-hand side of (2) evalates to 0 and with $L(1) = 1$ and $L(h) \geq 0$.

Sketch of the proof:
Assume there is a RNR with degree $< d$. Then there exist $g, g_1, \ldots, g_n, \in \mathbb{R}[\underline{X}],\ h \in \sum \mathbb{R}[\underline{X}]^2$ with $\deg g \leq n-1,\ \deg h \leq \min\{2k+2, n-1\}$ with

$$fg + \sum_{i=1}^{n} f_i g_i = 1 + h. \tag{2}$$

As Grigoriev, we construct a linear functional $L : \mathbb{R}[\underline{X}] \to \mathbb{R}$, that applied to the left-hand side of (2) evalates to 0 and with $L(1) = 1$ and $L(h) \geq 0$.

We first define L on the ring $\mathbb{R}[\mathtt{x}] := \mathbb{R}[\mathtt{x}_1, \ldots, \mathtt{x}_n] := \mathbb{R}[\underline{X}] / \left(X_i^2 - X_i\right)$

We first define L on the ring $\mathbb{R}[\mathrm{x}] := \mathbb{R}[\mathrm{x}_1, \ldots, \mathrm{x}_n] := \mathbb{R}[\underline{X}] / \left(X_i^2 - X_i\right)$ and then extend it to $\mathbb{R}[\underline{X}]$ by letting $L(p) := L(\bar{p})$.

We first define L on the ring $\mathbb{R}[\mathrm{x}] := \mathbb{R}[\mathrm{x}_1, \ldots, \mathrm{x}_n] := \mathbb{R}[\underline{X}] / (X_i^2 - X_i)$ and then extend it to $\mathbb{R}[\underline{X}]$ by letting $L(p) := L(\bar{p})$. For such a $p \in \mathbb{R}[\mathrm{x}]$, we define

$$\mathrm{Sym}(p) := \frac{1}{n!} \sum_{\sigma \in S_n} p(\mathrm{x}_\sigma)$$

Fact

For every symmetric multilinear polynomial $f \in \mathbb{R}[\mathrm{x}]$ exists a unique univariate polynomial $\widetilde{f} \in \mathbb{R}[T]$ with $f(\mathrm{x}) = \widetilde{f}(\sum \mathrm{x}_i)$ and $\deg f = \deg \widetilde{f}$

So we can define

$$L(p) := \widetilde{\mathrm{Sym}(p)}(r)$$

So we can define

$$L(p) := \widetilde{\mathrm{Sym}(p)}(r)$$

$L(1) = 1$ is obvious and it is not hard to show that $L(f \cdot g) = 0$ for all $g \in \mathbb{R}[\mathrm{x}]$ with $\deg g \leq n-1$.

So we can define

$$L(p) := \widetilde{\mathrm{Sym}(p)}(r)$$

$L(1) = 1$ is obvious and it is not hard to show that $L(f \cdot g) = 0$ for all $g \in \mathbb{R}[\mathrm{x}]$ with $\deg g \leq n-1$. So it remains to show that $L(h^2) \geq$ for all $h \in \mathbb{R}[\mathrm{x}]$ with $\deg h \leq \min\{k+1, \lfloor \frac{n}{2} \rfloor\}$.

So we can define

$$L(p) := \widetilde{\mathrm{Sym}(p)}(r)$$

$L(1) = 1$ is obvious and it is not hard to show that $L(f \cdot g) = 0$ for all $g \in \mathbb{R}[\mathrm{x}]$ with $\deg g \leq n-1$. So it remains to show that $L(h^2) \geq$ for all $h \in \mathbb{R}[\mathrm{x}]$ with $\deg h \leq \min\{k+1, \lfloor \frac{n}{2} \rfloor\}$. Note that $\mathrm{Sym}(h^2)$ is a symmetric sum of squares in $\mathbb{R}[\mathrm{x}]$.

Theorem (Blekherman, 2015)

$f \in \mathbb{R}[\mathrm{x}]$ is a symmetric sum of squares of polynomials of degree at most d iff $\widetilde{f} \in \mathrm{sos}_d + T(n-T)\mathrm{sos}_{d-1} + T(T-1)(n-T)(n-1-T)\mathrm{sos}_{d-2} + \ldots + T \cdot \ldots (T-(d-1)) \cdot (n-T) \cdot \ldots \cdot (n-(d-1)-T)$, with $\mathrm{sos}_i = \sum \mathbb{R}[T]_i^2$.

So we can define

$$L(p) := \widetilde{\mathrm{Sym}(p)}(r)$$

$L(1) = 1$ is obvious and it is not hard to show that $L(f \cdot g) = 0$ for all $g \in \mathbb{R}[\mathrm{x}]$ with $\deg g \leq n-1$. So it remains to show that $L(h^2) \geq$ for all $h \in \mathbb{R}[\mathrm{x}]$ with $\deg h \leq \min\{k+1, \lfloor \frac{n}{2} \rfloor\}$. Note that $\mathrm{Sym}(h^2)$ is a symmetric sum of squares in $\mathbb{R}[\mathrm{x}]$.

Theorem (Blekherman, 2015)

$f \in \mathbb{R}[\mathrm{x}]$ is a symmetric sum of squares of polynomials of degree at most d iff $\widetilde{f} \in \mathrm{sos}_d + T(n-T)\mathrm{sos}_{d-1} + T(T-1)(n-T)(n-1-T)\mathrm{sos}_{d-2} + \ldots + T \cdot \ldots (T-(d-1)) \cdot (n-T) \cdot \ldots \cdot (n-(d-1)-T)$, with $\mathrm{sos}_i = \sum \mathbb{R}[T]_i^2$.

Together with $k < r < n-k$, this theorem applied to $\mathrm{Sym}(h^2)$, easily shows $L(h^2) = \widetilde{\mathrm{Sym}(h^2)}(r) \geq 0$.

Definition

A degree-d pseudo density is a function $D : \{0,1\}^m \to \mathbb{R}$ such that $\mathbb{E}_x D(x) = 1$ and $\mathbb{E}_x D(x) p(x)^2 \geq 0$ for all $p \in \mathbb{R}[\mathtt{x}_1, \ldots, \mathtt{x}_m]$ with $\deg(p) \leq d$.

Definition

A degree-d pseudo density is a function $D : \{0,1\}^m \to \mathbb{R}$ such that $\mathbb{E}_x D(x) = 1$ and $\mathbb{E}_x D(x) p(x)^2 \geq 0$ for all $p \in \mathbb{R}[\mathrm{x}_1, \ldots, \mathrm{x}_m]$ with $\deg(p) \leq d$.

Theorem (LRS, 2015)

For any $m, d \geq 1$ the following holds. Let $f : \{0,1\}^m \to [0,1]$ be a nonngegative function with $d := \deg_{sos}(f) - 1$ and let $D : \{0,1\}^m \to \mathbb{R}$ a degree-d pseudo-density with $\mathbb{E}_x D(x) f(x) < -\varepsilon$ for an $\varepsilon \in (0,1]$, then for every $n \geq 2m$, we have

$$rk_{psd}(M_n^f) \geq \left(\frac{c\varepsilon n}{dm^2 \|D\|_\infty \log n} \right)^{d/2} \left(\frac{\varepsilon}{\|D\|_\infty} \right)^{3/2} \sqrt{\mathbb{E}_x f(x)}$$

For an odd n define

$$f := \mathtt{x}_1 + \ldots + \mathtt{x}_n - \frac{n}{2}.$$

We are looking for a degree-$\lfloor \frac{n}{2} \rfloor$ pseudo density $D : \{0,1\}^n \to \mathbb{R}$ with $\mathbb{E}_x D(x) f(x)^2 = 0$ and small norm.

For an odd n define
$$f := \mathtt{x}_1 + \ldots + \mathtt{x}_n - \frac{n}{2}.$$

We are looking for a degree-$\lfloor \frac{n}{2} \rfloor$ pseudo density $D : \{0,1\}^n \to \mathbb{R}$ with $\mathbb{E}_x D(x) f(x)^2 = 0$ and small norm. So, D has to satisfy the following properties:

1. $\mathbb{E}_x D(x) = 1$
2. $\mathbb{E}_x D(x) p(x)^2 \geq 0$ f.a. $p \in \mathbb{R}[\mathtt{x}]$ with $\deg(p) \leq \lfloor \frac{n}{2} \rfloor$
3. $\mathbb{E}_x D(x) f(x)^2 = 0$

For an odd n define

$$f := \mathrm{x}_1 + \ldots + \mathrm{x}_n - \frac{n}{2}.$$

We are looking for a degree-$\lfloor \frac{n}{2} \rfloor$ pseudo density $D : \{0,1\}^n \to \mathbb{R}$ with $\mathbb{E}_x D(x) f(x)^2 = 0$ and small norm. So, D has to satisfy the following properties:

1. $\mathbb{E}_x D(x) = 1$
2. $\mathbb{E}_x D(x) p(x)^2 \geq 0$ f.a. $p \in \mathbb{R}[\mathrm{x}]$ with $\deg(p) \leq \lfloor \frac{n}{2} \rfloor$
3. $\mathbb{E}_x D(x) f(x)^2 = 0$

Every Function $D : \{0,1\}^n \to \mathbb{R}$, that satisfies this three properties, is called feasible.

Every feasible D corresponds to a linear functional $L_D : \mathbb{R}[\mathrm{x}] \to \mathbb{R}$, via $L_D(p) = \mathbb{E}_x D(x)p(x)$, with

- $L(1) = 1$
- $L(p^2) \geq 0$ f.a. $p \in \mathbb{R}[\mathrm{x}]$ with $\deg(p) \leq \lfloor \frac{n}{2} \rfloor$
- $L(f^2) = 0$

Every feasible D corresponds to a linear functional $L_D : \mathbb{R}[\mathrm{x}] \to \mathbb{R}$, via $L_D(p) = \mathbb{E}_x D(x)p(x)$, with

- $L(1) = 1$
- $L(p^2) \geq 0$ f.a. $p \in \mathbb{R}[\mathrm{x}]$ with $\deg(p) \leq \lfloor \frac{n}{2} \rfloor$
- $L(f^2) = 0$

A small trick shows, that such a L also satiesfies

$$L(fq) = 0 \text{ f.a. } q \in \mathbb{R}[\mathrm{x}] \text{ with } \deg(q) \leq \lfloor \frac{n}{2} \rfloor.$$

$L((af + bq)^2) \geq 0$ f.a. $a, b \in \mathbb{R}$

$L((af+bq)^2) \geq 0$ f.a. $a,b \in \mathbb{R}$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0 \quad \text{f.a } a,b \in \mathbb{R}$$

$L((af+bq)^2) \geq 0$ f.a. $a,b \in \mathbb{R}$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0 \quad \text{f.a } a,b \in \mathbb{R}$$

$$\begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \succeq 0$$

$L((af+bq)^2) \geq 0$ f.a. $a,b \in \mathbb{R}$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0 \quad \text{f.a } a,b \in \mathbb{R}$$

$$\begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \succeq 0$$

$$L(f^2)L(q^2) - L(fq)^2 \geq 0$$

$L((af+bq)^2) \geq 0$ f.a. $a, b \in \mathbb{R}$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0 \quad \text{f.a } a, b \in \mathbb{R}$$

$$\begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \succeq 0$$

$$-L(fq)^2 \geq 0$$

$L((af+bq)^2) \geq 0$ f.a. $a,b \in \mathbb{R}$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0 \quad \text{f.a } a,b \in \mathbb{R}$$

$$\begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \succeq 0$$

$$L(fq) = 0$$

$L((af+bq)^2) \geq 0$ f.a. $a,b \in \mathbb{R}$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0 \quad \text{f.a } a,b \in \mathbb{R}$$

$$\begin{pmatrix} L(f^2) & L(fq) \\ L(fq) & L(q^2) \end{pmatrix} \succeq 0$$

$$L(fq) = 0$$

Remark: Grigorievs linear functional even satisfies

$$L(fq) = 0 \text{ f.a. } q \in \mathbb{R}[\mathrm{x}] \text{ with } \deg(q) \leq n-1.$$

We call a pseudo density symmetric, if

$$D(x) = D(y) \text{ f.a. } x, y \in \{0,1\}^n \text{ with } |x| = |y|.$$

We call a pseudo density symmetric, if

$$D(x) = D(y) \text{ f.a. } x,y \in \{0,1\}^n \text{ with } |x| = |y|.$$

Observations:

- For every feasible function, there exists a feasible symmetric function with smaller norm.

We call a pseudo density symmetric, if

$$D(x) = D(y) \text{ f.a. } x, y \in \{0,1\}^n \text{ with } |x| = |y|.$$

Observations:

- For every feasible function, there exists a feasible symmetric function with smaller norm. So it is sufficient to look only for symmetric pseudo densities and we consider a pseudo density D as a function $D : \{0, \ldots, n\} \to \mathbb{R}$.

We call a pseudo density symmetric, if

$$D(x) = D(y) \text{ f.a. } x,y \in \{0,1\}^n \text{ with } |x| = |y|.$$

Observations:

- For every feasible function, there exists a feasible symmetric function with smaller norm. So it is sufficient to look only for symmetric pseudo densities and we consider a pseudo density D as a function $D : \{0,\dots,n\} \to \mathbb{R}$.
- If D is a feasible function, than $\widetilde{D} : \{0,\dots,n\} \to \mathbb{R}$, $\widetilde{D}(i) := D(n-i)$ is also feasible.

We call a pseudo density symmetric, if

$$D(x) = D(y) \text{ f.a. } x,y \in \{0,1\}^n \text{ with } |x| = |y|.$$

Observations:

- For every feasible function, there exists a feasible symmetric function with smaller norm. So it is sufficient to look only for symmetric pseudo densities and we consider a pseudo density D as a function $D : \{0,\ldots,n\} \to \mathbb{R}$.
- If D is a feasible function, than $\widetilde{D} : \{0,\ldots,n\} \to \mathbb{R}$, $\widetilde{D}(i) := D(n-i)$ is also feasible.
- If D is a feasible function, than $\hat{D} := \frac{1}{2} \cdot (D + \widetilde{D})$ is also a feasible function with smaller norm and $\hat{D}(i) = \hat{D}(n-i)$ f.a. $0 \leq i \leq n$.

We are looking for linear functions $L : \mathbb{R}[\mathrm{x}]^{S_n} \to \mathbb{R}$ with

1. $L(1) = 1$
2. $L(p^2) \geq 0$ f.a. $p \in \mathbb{R}[\mathrm{x}]$ with $\deg(p) \leq \lfloor \frac{n}{2} \rfloor$
3. $L(f^2) = 0$
4. $L(p(\mathrm{x}_1, \ldots, \mathrm{x}_n)) = L(p(1 - \mathrm{x}_1, \ldots, 1 - \mathrm{x}_n))$

We are looking for linear functions
$L : \mathbb{R}[T]/(T \cdot (T-1) \cdot \ldots \cdot (T-n)) \to \mathbb{R}$ with

We are looking for linear functions
$L : \mathbb{R}[T]/(T \cdot (T-1) \cdot \ldots \cdot (T-n)) \to \mathbb{R}$ with

1. $L(1) = 1$

We are looking for linear functions
$L : \mathbb{R}[T]/(T \cdot (T-1) \cdot \ldots \cdot (T-n)) \to \mathbb{R}$ with

1. $L(1) = 1$
2. $L(q) \geq 0$

   f.a. $q \in \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \text{sos}_{\lfloor \frac{n}{2} \rfloor - i} \left(\prod_{j=0}^{i-1} (T-j)(n-j-T) \right)$

We are looking for linear functions
$L : \mathbb{R}[T]/(T \cdot (T-1) \cdot \ldots \cdot (T-n)) \to \mathbb{R}$ with

1. $L(1) = 1$
2. $L(q) \geq 0$
   f.a. $q \in \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \mathrm{sos}_{\lfloor \frac{n}{2} \rfloor - i} \left(\prod_{j=0}^{i-1} (T-j)(n-j-T) \right)$
3. $L((T - \frac{n}{2})^2) = 0$

We are looking for linear functions
$L : \mathbb{R}[T]/(T \cdot (T-1) \cdot \ldots \cdot (T-n)) \to \mathbb{R}$ with

1. $L(1) = 1$
2. $L(q) \geq 0$
   f.a. $q \in \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \text{sos}_{\lfloor \frac{n}{2} \rfloor - i} \left(\prod_{j=0}^{i-1} (T-j)(n-j-T) \right)$
3. $L((T - \frac{n}{2})^2) = 0$
4. $L(p(T)) = L(p(n-T))$

We are looking for linear functions
$L : \mathbb{R}[T]/(T \cdot (T-1) \cdot \ldots \cdot (T-n)) \to \mathbb{R}$ with

1. $L(1) = 1$
2. $L(q) \geq 0$
   f.a. $q \in \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \text{sos}_{\lfloor \frac{n}{2} \rfloor - i} \left(\prod_{j=0}^{i-1} (T-j)(n-j-T) \right)$
3. $L((T - \frac{n}{2})^2) = 0$
4. $L(p(T)) = L(p(n-T))$

Proposition

There is a unique linear functional
$L : \mathbb{R}[T]/(T \cdot (T-1) \cdot \ldots \cdot (T-n)) \to \mathbb{R}$ with the above properties. In detail, it is the linear functional $L(T^k) = \left(\frac{n}{2}\right)^k$.

Observation:
From $L(p(T)) = L(p(n - T))$ we immediately get $L(T) = \frac{n}{2}$.

Observation:
From $L(p(T)) = L(p(n-T))$ we immediately get $L(T) = \frac{n}{2}$. This, together with $L((T-\frac{n}{2})^2) = 0$, leads to $L(T^2) = \left(\frac{n}{2}\right)^2$. From an earlier observation, we get $L((T-\frac{n}{2})^2 \cdot T^k) = 0$ for all $k \leq \lfloor \frac{n}{2} \rfloor$,

Observation:
From $L(p(T)) = L(p(n-T))$ we immediately get $L(T) = \frac{n}{2}$. This, together with $L((T-\frac{n}{2})^2) = 0$, leads to $L(T^2) = \left(\frac{n}{2}\right)^2$. From an earlier observation, we get $L((T-\frac{n}{2})^2 \cdot T^k) = 0$ for all $k \leq \lfloor \frac{n}{2} \rfloor$, what easily shows $L(T^k) = \left(\frac{n}{2}\right)^k$ for all $k \leq \lfloor \frac{n}{2} \rfloor + 1$.

Observation:
From $L(p(T)) = L(p(n-T))$ we immediately get $L(T) = \frac{n}{2}$. This, together with $L((T-\frac{n}{2})^2) = 0$, leads to $L(T^2) = \left(\frac{n}{2}\right)^2$. From an earlier observation, we get $L((T-\frac{n}{2})^2 \cdot T^k) = 0$ for all $k \leq \lfloor \frac{n}{2} \rfloor$, what easily shows $L(T^k) = \left(\frac{n}{2}\right)^k$ for all $k \leq \lfloor \frac{n}{2} \rfloor + 1$.

Proof:
We show $L(T^k) = \left(\frac{n}{2}\right)^k$ for all $1 \leq k \leq n$ by induction on k.

Observation:
From $L(p(T)) = L(p(n-T))$ we immediately get $L(T) = \frac{n}{2}$. This, together with $L((T-\frac{n}{2})^2) = 0$, leads to $L(T^2) = \left(\frac{n}{2}\right)^2$. From an earlier observation, we get $L((T-\frac{n}{2})^2 \cdot T^k) = 0$ for all $k \leq \lfloor \frac{n}{2} \rfloor$, what easily shows $L(T^k) = \left(\frac{n}{2}\right)^k$ for all $k \leq \lfloor \frac{n}{2} \rfloor + 1$.

Proof:
We show $L(T^k) = \left(\frac{n}{2}\right)^k$ for all $1 \leq k \leq n$ by induction on k. The base clause is already done.

Observation:
From $L(p(T)) = L(p(n-T))$ we immediately get $L(T) = \frac{n}{2}$. This, together with $L((T-\frac{n}{2})^2) = 0$, leads to $L(T^2) = \left(\frac{n}{2}\right)^2$. From an earlier observation, we get $L((T-\frac{n}{2})^2 \cdot T^k) = 0$ for all $k \leq \lfloor \frac{n}{2} \rfloor$, what easily shows $L(T^k) = \left(\frac{n}{2}\right)^k$ for all $k \leq \lfloor \frac{n}{2} \rfloor + 1$.

Proof:
We show $L(T^k) = \left(\frac{n}{2}\right)^k$ for all $1 \leq k \leq n$ by induction on k. The base clause is already done. For the induction step we distinguish the cases k odd and k even.

Case 1: k odd

Case 1: k odd

$$\begin{aligned} L(T^k) &= L((n-T)^k) \\ &= L\left(\sum_{i=0}^{k} \binom{k}{i} n^{k-i} (-T)^i\right) \end{aligned}$$

Case 1: k odd

$$\begin{aligned} L(T^k) &= L((n-T)^k) \\ &= L\left(\sum_{i=0}^{k-1} \binom{k}{i} n^{k-i}(-T)^i\right) - L(T^k) \end{aligned}$$

Case 1: k odd

$$
\begin{aligned}
L(T^k) &= L((n-T)^k) \\
&= L\left(\sum_{i=0}^{k-1}\binom{k}{i} n^{k-i}(-T)^i\right) - L(T^k) \\
2L(T^k) &= \sum_{i=0}^{k-1}\binom{k}{i} n^{k-i}(-1)^i L(T^i)
\end{aligned}
$$

Case 1: k odd

$$
\begin{aligned}
L(T^k) &= L((n-T)^k) \\
&= L\left(\sum_{i=0}^{k-1}\binom{k}{i} n^{k-i}(-T)^i\right) - L(T^k) \\
2L(T^k) &= \sum_{i=0}^{k-1}\binom{k}{i} n^{k-i}(-1)^i \left(\frac{n}{2}\right)^i
\end{aligned}
$$

Case 1: k odd

$$
\begin{aligned}
L(T^k) &= L((n-T)^k) \\
&= L\left(\sum_{i=0}^{k-1}\binom{k}{i} n^{k-i}(-T)^i\right) - L(T^k) \\
2L(T^k) &= \sum_{i=0}^{k-1}\binom{k}{i} n^{k-i}\left(-\frac{n}{2}\right)^i
\end{aligned}
$$

Case 1: k odd

$$L(T^k) = L((n-T)^k)$$
$$= L\left(\sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}(-T)^i\right) - L(T^k)$$
$$2L(T^k) = \sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}\left(-\frac{n}{2}\right)^i$$
$$2L(T^k) = \sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}\left(-\frac{n}{2}\right)^i + \left(-\frac{n}{2}\right)^k - \left(-\frac{n}{2}\right)^k$$

Case 1: k odd

$$
\begin{aligned}
L(T^k) &= L((n-T)^k) \\
&= L\left(\sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}(-T)^i\right) - L(T^k)
\end{aligned}
$$

$$2L(T^k) = \sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}\left(-\frac{n}{2}\right)^i$$

$$2L(T^k) = \sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}\left(-\frac{n}{2}\right)^i + \left(-\frac{n}{2}\right)^k - \left(-\frac{n}{2}\right)^k$$

$$2L(T^k) = \left(n-\frac{n}{2}\right)^k + \left(\frac{n}{2}\right)^k$$

Case 1: k odd

$$
\begin{aligned}
L(T^k) &= L((n-T)^k) \\
&= L\left(\sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}(-T)^i\right) - L(T^k)
\end{aligned}
$$

$$2L(T^k) = \sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}\left(-\frac{n}{2}\right)^i$$

$$2L(T^k) = \sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}\left(-\frac{n}{2}\right)^i + \left(-\frac{n}{2}\right)^k - \left(-\frac{n}{2}\right)^k$$

$$2L(T^k) = 2\left(\frac{n}{2}\right)^k$$

Case 1: k odd

$$
\begin{aligned}
L(T^k) &= L((n-T)^k) \\
&= L\left(\sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}(-T)^i\right) - L(T^k) \\
2L(T^k) &= \sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}\left(-\frac{n}{2}\right)^i \\
2L(T^k) &= \sum_{i=0}^{k-1}\binom{k}{i}n^{k-i}\left(-\frac{n}{2}\right)^i + \left(-\frac{n}{2}\right)^k - \left(-\frac{n}{2}\right)^k \\
2L(T^k) &= 2\left(\frac{n}{2}\right)^k \\
L(T^k) &= \left(\frac{n}{2}\right)^k
\end{aligned}
$$

Case 2: k even ($k \geq 4$)

Case 2: k even $(k \geq 4)$
$L\left(\left(aT^{k/2-1}+bT^{k/2}\right)^2\right) \geq 0$ f.a. $a,b \in \mathbb{R}$

Case 2: k even ($k \geq 4$)
$L\left(\left(aT^{k/2-1} + bT^{k/2}\right)^2\right) \geq 0$ f.a. $a,b \in \mathbb{R}$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L(T^{k-2}) & L(T^{k-1}) \\ L(T^{k-1}) & L(T^k) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0 \text{ f.a } a,b \in \mathbb{R}$$

$$\begin{pmatrix} L(T^{k-2}) & L(T^{k-1}) \\ L(T^{k-1}) & L(T^k) \end{pmatrix} \succeq 0$$

Case 2: k even $(k \geq 4)$

$L\left(\left(aT^{k/2-1} + bT^{k/2}\right)^2\right) \geq 0$ f.a. $a,b \in \mathbb{R}$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L(T^{k-2}) & L(T^{k-1}) \\ L(T^{k-1}) & L(T^k) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0 \text{ f.a } a,b \in \mathbb{R}$$

$$\begin{pmatrix} \left(\frac{n}{2}\right)^{k-2} & \left(\frac{n}{2}\right)^{k-1} \\ \left(\frac{n}{2}\right)^{k-1} & L(T^k) \end{pmatrix} \succeq 0$$

Case 2: k even $(k \geq 4)$
$L\left(\left(aT^{k/2-1} + bT^{k/2}\right)^2\right) \geq 0$ f.a. $a,b \in \mathbb{R}$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L(T^{k-2}) & L(T^{k-1}) \\ L(T^{k-1}) & L(T^k) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0 \text{ f.a } a,b \in \mathbb{R}$$

$$\begin{pmatrix} \left(\frac{n}{2}\right)^{k-2} & \left(\frac{n}{2}\right)^{k-1} \\ \left(\frac{n}{2}\right)^{k-1} & L(T^k) \end{pmatrix} \succeq 0$$

$$\left(\frac{n}{2}\right)^{k-2} L(T^k) - \left(\frac{n}{2}\right)^{2k-2} \geq 0$$

Case 2: k even $(k \geq 4)$
$L\left(\left(aT^{k/2-1} + bT^{k/2}\right)^2\right) \geq 0$ f.a. $a,b \in \mathbb{R}$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L(T^{k-2}) & L(T^{k-1}) \\ L(T^{k-1}) & L(T^k) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0 \text{ f.a } a,b \in \mathbb{R}$$

$$\begin{pmatrix} \left(\frac{n}{2}\right)^{k-2} & \left(\frac{n}{2}\right)^{k-1} \\ \left(\frac{n}{2}\right)^{k-1} & L(T^k) \end{pmatrix} \succeq 0$$

$$\left(\frac{n}{2}\right)^{k-2} L(T^k) - \left(\frac{n}{2}\right)^{2k-2} \geq 0$$

$$L(T^k) \geq \left(\frac{n}{2}\right)^k$$

$$L\left(T \cdot (n - T) \cdot \left(aT^{k/2-2} + bT^{k/2-1}\right)^2\right) \geq 0 \text{ f.a. } a,b \in \mathbb{R}$$

$$L\left(T \cdot (n - T) \cdot \left(aT^{k/2-2} + bT^{k/2-1}\right)^2\right) \geq 0 \text{ f.a. } a,b \in \mathbb{R}$$

$$\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} L((nT - T^2)(T^{k-4})) & L((nT - T^2)(T^{k-3})) \\ L((nT - T^2)(T^{k-3})) & L((nT - T^2)(T^{k-2})) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \geq 0$$

$$\begin{pmatrix} nL(T^{k-3}) - L(T^{k-2}) & nL(T^{k-2} - L(T^{k-1}) \\ nL(T^{k-2}) - L(T^{k-1}) & nL(T^{k-1}) - L(T^k) \end{pmatrix} \succeq 0$$

$$L\left(T\cdot(n-T)\cdot\left(aT^{k/2-2}+bT^{k/2-1}\right)^2\right)\geq 0 \text{ f.a. } a,b\in\mathbb{R}$$

$$\begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}L((nT-T^2)(T^{k-4})) & L((nT-T^2)(T^{k-3}))\\ L((nT-T^2)(T^{k-3})) & L((nT-T^2)(T^{k-2}))\end{pmatrix}\begin{pmatrix}a\\ b\end{pmatrix}\geq 0$$

$$\begin{pmatrix}n\cdot\left(\frac{n}{2}\right)^{k-3}-\left(\frac{n}{2}\right)^{k-2} & n\cdot\left(\frac{n}{2}\right)^{k-2}-\left(\frac{n}{2}\right)^{k-1}\\ n\cdot\left(\frac{n}{2}\right)^{k-2}-\left(\frac{n}{2}\right)^{k-1} & n\cdot\left(\frac{n}{2}\right)^{k-1}-L(T^k)\end{pmatrix}\succeq 0$$

$$L\left(T\cdot(n-T)\cdot\left(aT^{k/2-2}+bT^{k/2-1}\right)^2\right)\geq 0 \text{ f.a. } a,b\in\mathbb{R}$$

$$\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} L((nT-T^2)(T^{k-4})) & L((nT-T^2)(T^{k-3})) \\ L((nT-T^2)(T^{k-3})) & L((nT-T^2)(T^{k-2})) \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}\geq 0$$

$$\begin{pmatrix} \left(\frac{n}{2}\right)^{k-2} & \left(\frac{n}{2}\right)^{k-1} \\ \left(\frac{n}{2}\right)^{k-1} & n\cdot\left(\frac{n}{2}\right)^{k-1}-L(T^k) \end{pmatrix}\succeq 0$$

$$L\left(T\cdot(n-T)\cdot\left(aT^{k/2-2}+bT^{k/2-1}\right)^2\right)\geq 0 \text{ f.a. } a,b\in\mathbb{R}$$

$$\begin{pmatrix}a & b\end{pmatrix}\begin{pmatrix}L((nT-T^2)(T^{k-4})) & L((nT-T^2)(T^{k-3}))\\ L((nT-T^2)(T^{k-3})) & L((nT-T^2)(T^{k-2}))\end{pmatrix}\begin{pmatrix}a\\ b\end{pmatrix}\geq 0$$

$$\begin{pmatrix}\left(\frac{n}{2}\right)^{k-2} & \left(\frac{n}{2}\right)^{k-1}\\ \left(\frac{n}{2}\right)^{k-1} & n\cdot\left(\frac{n}{2}\right)^{k-1}-L(T^k)\end{pmatrix}\succeq 0$$

$$n\left(\frac{n}{2}\right)^{2k-3}-\left(\frac{n}{2}\right)^{k-2}L(T^k)-\left(\frac{n}{2}\right)^{2k-2}\geq 0$$

$$L\left(T\cdot(n-T)\cdot\left(aT^{k/2-2}+bT^{k/2-1}\right)^2\right)\geq 0 \text{ f.a. } a,b\in\mathbb{R}$$

$$\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} L((nT-T^2)(T^{k-4})) & L((nT-T^2)(T^{k-3})) \\ L((nT-T^2)(T^{k-3})) & L((nT-T^2)(T^{k-2})) \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}\geq 0$$

$$\begin{pmatrix} \left(\frac{n}{2}\right)^{k-2} & \left(\frac{n}{2}\right)^{k-1} \\ \left(\frac{n}{2}\right)^{k-1} & n\cdot\left(\frac{n}{2}\right)^{k-1}-L(T^k) \end{pmatrix}\succeq 0$$

$$n\left(\frac{n}{2}\right)^{2k-3}-\left(\frac{n}{2}\right)^{k-2}L(T^k)-\left(\frac{n}{2}\right)^{2k-2}\geq 0$$

$$L(T^k)\leq\left(\frac{n}{2}\right)^k$$