UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

CERTIFICATS DE POSITIVITAT PER POLINOMIS

Autor: Pau Anguera Salvat

Director: Dr. Carlos D'Andrea
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 10 de juny de 2025

Abstract

In this project, we focus on finding certificates of positivity for real polynomials in $\mathbb{R}[x]$. To find them, we look for representations of a polynomial f in such a way that we can assure it is non-negative for all x. Through changes of variables, we see that it's sufficient to find them for $x \in [-1, 1]$. We can also observe that in certain certificates it's necessary to choose a correct set of generators to affirm its existance. Finally, we look through certificates of positivity on curves in $\mathbb{R}^2$ and we give general conditions for certificates to exist in $\mathbb{R}^n$.

Resum

Aquest treball es centra en trobar certificats de positivitat per a polinomis reals en $\mathbb{R}[x]$. Per trobar-los, representem un polinomi f de certa manera que podem assegurar que és no negatiu per tot x. Veiem que mitjançant canvis de variables és suficient trobar-los per $x \in [-1, 1]$. Veiem també que en certs certificats és necessari trobar un conjunt de generadors adequats per afirmar la seva existència. Finalment, fem una ullada als certificats de positivitat en corbes de $\mathbb{R}^2$ i donem unes condicions generals perquè existeixin certificats en $\mathbb{R}^n$.

2020 Mathematics Subject Classification. 11G05, 11G10, 14G10

Agraïments

Voldria agrair al meu tutor, Carlos d'Andrea, per tot l'acompanyament que m'ha fet al llarg del treball, per haver-me recomanat el tema i haver-me ajudat i assistit en tots els problemes i preocupacions que he anat trobant durant el procés.

Gràcies als meus amics i a tota la meva família, per ser-hi sempre que els necessito.

Gràcies en especial al meu pare Lluís, la meva germana Bruna i sobretot, gràcies a la meva mare Mercè, per assegurar-se que sempre vaig pel camí correcte, pel seu recolzament en totes les decisions que prenc i el seu amor incondicional.

Gràcies al Miquel, el Marc, l'Albert i l'Iris, pel seu suport emocional, que ens hem vist créixer, i espero que segueixi així fins l'últim dels nostres dies.

Gràcies al Pol Gasch, que no ens hem separat des de l'inici de la carrera i a l'Eudald, el Xavier, el Ramón, la Berta i el Pol Plans, per donar-me els millors anys de la vida a la universitat.

A l'Alba, per haver-me recomanat el tutor, haver-me motivat a fer un bon tfg i perquè em feia de psicòloga cada vegada que anàvem al gimnàs.

A la Júlia, l'Alex i la Marina, per el nostre grup d'estudi i per tots els exàmens que hem aprovat estudiant junts i explicant-nos el temari els uns als altres, que sense ells no hauria estat possible treure'm la carrera.

Al Guillem, el Xavi, l'Adrià, el Jaume i l'Àlex, per estar sempre preparats per fer-me perdre el temps jugant al Valorant o parlant de tonteries.

A les fades, per proveir un espai d'esbarjo i confiança sempre que necessitava descansar en algun moment, i a la Sandra i la Maria, per ser unes grans companyes de pis i no crear mai mal ambient.

A la Maria, la Sofía, la Nadia, la Núria, la Sílvia, el Marc, el Miguel, l'Abril. A les meves cosines Aina, Anna, Emma i Mireia. A la Cèlia que, des de ben petits, jugàvem junts quan venia a veure la meva germana a casa. A l'Héctor i el Lluís, un per introduir-me al Twilight Imperium i l'altre per deixar-se guanyar sempre. A la Clàudia, que amb les seves dots d'ensenyament ha aconseguit explicar-me assignatures i fer-me aprovar exàmens que després ella suspèn. A l'Aina, la Lola i el Guillem, per acompanyar-me al gimnàs sempre que ho necessitava. A la Laia, la Bruna, el Manuel, la Teresa, el Dídac, la Cinta, l'Ester i la Paula, per estar sempre a la universitat i fer bona companyia. A l'Òscar i l'Elna, per recordar-me quan tenim provetes a algorísmica.

Al Gerard, els bons moments a la pista de bàsquet i no ser capaç de guanyar-me cap u contra u, al Jerez, per ser el meu jove carnisser, al encara més jove Pablo, per pujar a ajudar l'equip quan el necessitàvem de jugador o d'entrenador, als meus entrenadors Nacho i Biel, al Martí per donar-me forces per seguir endavant cada entrenament i partit, al Bonis, per ser un gran base i acompanyar-me després de cada entreno a casa, al Moncunill, per ensenyar-me que és el compromís amb un equip. A la Maria per ser molt positiva amb les meves funcions. A la Clàudia i el Jordi per creure en mi. Al Maxim per jugar amb mi al Go i als escacs i a l'Irina, la Lucía i el Guerau, per animar-me a fer uns agraïments ben complets.

Índex

1 Introducció

Si un polinomi f en els reals amb n variables pot ser escrit com una suma de quadrats, llavors aquest polinomi clarament només té valors no negatius en tot $\mathbb{R}^n$. Aquesta afirmació tan simple ens porta a un ampli món teòric i computacional de mètodes que busquen relacionar polinomis positius i sumes de quadrats.

Una representació explícita de f com a suma de quadrats es coneix com un certificat de positivitat. Arribar a trobar una representació de f que sigui suma de quadrats et garanteix immediatament la positivitat de f en $\mathbb{R}$. Per exemple, si considerem

$$f(x, y) = y^4 + 4x^2 - y^2 - 4xy + 1$$

Aquest polinomi és no negatiu per qualsevol valor de $\mathbb{R}^2$, però no es veu clarament a primera vista. En canvi, quan aconseguim trobar la representació adequada,

$$f(x, y) = (y^2 - 1)^2 + (2x - y)^2$$

queda molt més evident la seva positivitat.

La pregunta sobre si sempre existeix un certificat de positivitat per a un polinomi f que és positiu per tot $\mathbb{R}^n$ es remunta al segle XIX, en les obres de Hilbert. En un dels articles que va publicar, va demostrar que existeix un polinomi $f \geq 0$ en tot $\mathbb{R}^n$ que no pot ser escrit com a suma de quadrats de polinomis. Seguidament va plantejar si existien certificats de positivitat quan permetíem sumes de quadrats de funcions racionals, o sigui, quocients de polinomis. Al 1927, Artin va respondre afirmativament la pregunta.

Els certificats de positivitat tenen utilitats en múltiples branques de les matemàtiques, com ara les matemàtiques aplicades, les enginyeries o la ciència de dades. Les més famoses són les aplicacions en el problema dels moments d'anàlisi funcional i en l'optimització de polinomis. Concretament, hi ha una gran quantitat d'aplicacions de sumes de quadrats i polinomis positius per trobar polinomis mínims en subconjunts tancats de $\mathbb{R}^n$, normalment conjunts definits per equacions polinòmiques no estrictes finites. La raó per la qual es fan servir certificats de positivitat per aquests tipus de problemes d'optimització és simple: per un polinomi f i un subconjunt $K \subseteq \mathbb{R}^n$, el problema de trobar el mínim de $f(x)$ per tot $x \in K$ equival a trobar el màxim $\lambda \in \mathbb{R}$ tal que $f - \lambda \geq 0$ en K. Això porta a algoritmes per minimitzar polinomis en K.

Al 2021, Victòria Powers va publicar el llibre "Certificates of Positivity for Real Polinomials"[1], on recollia la teoria envers dels certificats de positivitat en polinomis reals, juntament amb algorismes computacionals per trobar-los. Les demostracions que apareixen són elementals, i la major part del llibre es centra més en divulgar informació que en demostrar-la. Aquest treball es basa en un capítol d'aquest llibre, concretament el 8, que parla de certificats de positivitat de polinomis positius en conjunts bàsics semialgebraics tancats de $\mathbb{R}$. L'objectiu principal del treball ha estat ampliar aquest capítol, escrivint les demostracions que no hi són i afegir-ne d'altres de necessàries.

La part principal d'aquest treball és centra en els certificats de positivitat en polinomis a la recta real. Al contrari de les situacions amb moltes dimensions, els certificats de positivitat en $\mathbb{R}$ per a polinomis positius en conjunts semialgebraics bàsics tancats quasi sempre existeixen. Mirarem diversos certificats de positivitat, buscant diferents representacions de f, la representació com a suma de polinomis quadrats $f = g^2 + h^2$ o $f = \sigma_1 + \sigma_2 g$ on σ_1, σ_2 són polinomis de sumes de quadrats. Estudiarem principalment en

els intervals on x pertany a $[-1,1]$ o $[0,\infty)$, ja que veurem que amb aquests dos podem determinar certificats de positivitat per tot $\mathbb{R}$ mitjançant canvis de variables. Veurem que l'única complicació és la tria del conjunt de generadors, ja que l'existència d'alguns certificats de positivitat depèn d'ella, i els resultats no sempre seran certs per qualsevol conjunt de generadors.

Finalment parlarem dels certificats de positivitat en polinomis sobre corbes, que són conjunts algebraics de dimensió 1. Denotem una corba plana com el conjunt no buit

$$\left\{(x,y) \in \mathbb{R}^2 \mid p(x,y) = 0\right\}$$

Per una corba plana C, ens interessa la qüestió de si una funció $f \geq 0$ pot ser escrita com a suma de quadrats en l'anell de coordenades de C, $R[C]$. Començarem estudiant què passa a $\mathbb{R}^2$, mirant el cercle unitat. Després estudiarem com canvien les condicions que han de complir les corbes depenent de si són racionals o no i, finalment, estudiarem quines condicions ha de complir una corba reductible en $\mathbb{R}^n$ perquè tot polinomi $f \geq 0$ pugui ser una suma de quadrats en $R[C]$.

2 Conceptes preliminars

2.1 Notació

Al llarg del treball farem servir la següent notació:

- Farem servir $\mathbb{Z}$ per denotar els nombres enters, $\mathbb{Q}$ per als racionals $\mathbb{R}$ per als reals, $\mathbb{C}$ per als complexos i $\mathbb{N}$ per els naturals, és a dir, els enters estrictament positius.
- Usarem $\mathbb{Z}_{\geq 0}$ per els enters no negatius, $\mathbb{Q}_{\geq 0}$ per els racionals no negatius i $\mathbb{R}_{\geq 0}$ per els reals no negatius.
- Denotarem com a $\mathbb{Q}_+$ els racionals estrictament positius i com a $\mathbb{R}_+$ els nombres reals estrictament positius.
- Denotarem per $\mathbb{F}$ un cos, que pot ser $\mathbb{R}$ o $\mathbb{Q}$ i que alguna vegada serà $\mathbb{C}$.
- En la secció de corbes, denotarem per R a un cos real tancat, en general serà $\mathbb{R}^n$.
- Si tenim un conjunt no buit U i $n \in \mathbb{N}$, denotarem com a U^n el producte cartesià $U \times \cdots \times U$ de n copies de U. Concretament, $\mathbb{R}^n$ denota el n-espai euclidià de dimensió n.
- Per qualsevol vector $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, denotarem com $\|x\|$ la distància euclidiana de x fins l'origen, és a dir, $\|x\| = \sqrt{x_1^2 + \cdots + x_n^2}$.
- Per un polinomi f, denotarem per $\|f\|_1$ el màxim dels coeficients de f en valor absolut.
- i denota $\sqrt{-1}$ en $\mathbb{C}$.
- Per qualsevol $a \in \mathbb{R}$, denotarem com a $\lceil a \rceil$ el següent enter més pròxim a a, és a dir, l'enter m més petit tal que $a \leq m$.
- Per qualsevol $a \in \mathbb{R}$, denotarem com a $\lfloor a \rfloor$ el anterior enter més pròxim a a, és a dir, l'enter m més gran tal que $a \geq m$.
- En termes generals, A serà un anell commutatiu amb el 1 i denotarem per I un ideal de A.
- Per qualsevol conjunt $T \subseteq A$, T^2 són els quadrats de T: $T^2 = \{t^2 \mid t \in T\}$.
- Per qualsevol conjunt $T \subseteq A$, expressarem $T + T = \{t_1 + t_2 \mid t_1, t_2 \in T\}$ i $T - T = \{t_1 - t_2 \mid t_1, t_2 \in T\}$.
- Per qualsevol conjunt $T \subseteq A$, expressarem $TT = \{t_1 * t_2 \mid t_1, t_2 \in A\}$.

2.2 Definicions

Definició 2.1. *Un conjunt $X \subseteq \mathbb{R}$ és semialgebraic si pot ser definit per un conjunt finit d'inequacions polinòmiques en $\mathbb{R}$.*

Definició 2.2. *Un conjunt $X \subseteq \mathbb{R}$ és bàsic semialgebraic tancat si tots els seus elements estan definits per un nombre finit d'inequacions a $\mathbb{R}$ amb desigualtat no estricte ($\leq$).*

Definició 2.3. *Prenem A un anell commutatiu amb 1.*

1. *$T \subseteq A$ és un preprimer si $T + T \subseteq T$, $TT \subseteq T$, i $\mathbb{Q}_{\geq 0} \subseteq T$.*
2. *Un preprimer T és generador si $T - T = A$.*
3. *Si T és preprimer, $M \subseteq A$ és un T-mòdul si $M + M \subseteq M$, $TM \subseteq M$ i $1 \in M$.*
4. *Un T-mòdul és arquimedià si $\forall a \in A$ existeix una $k \in \mathbb{N}$ tal que $k - a \in M$.*

Definició 2.4. *Anomenem transformada de Goursat d'un polinomi f de grau d a un canvi de variables denotat com $\hat{f}$ i definit com*

$$\hat{f}(x) = (1+x)^d f\left(\frac{1-x}{1+x}\right).$$

Podem observar que $\hat{f}$ és, efectivament, un polinomi, el grau de $\hat{f} \leq d$ i el coeficient de x^d en $\hat{f}$ és $f(-1)$, per tant el grau de f i $\hat{f}$ són iguals si i només si $f(-1) \neq 0$.

Podem observar també que

$$\hat{\hat{f}} = (1+x)^d \hat{f}\left(\frac{1-x}{1+x}\right) = (1+x)^d \left(1 + \frac{1-x}{1+x}\right)^d f\left(\frac{1 - \frac{1-x}{1+x}}{1 + \frac{1-x}{1+x}}\right) = 2^d f(x).$$

que ens serà útil més endavant.

Definició 2.5. *Un mòdul quadràtic és un subconjunt $T \subseteq A$ amb $1 \in T$, que està tancat amb la suma i la multiplicació de quadrats. $1 \in T$, $T + T \subseteq T$, $A^2 T \in T$.*

Definició 2.6. *Un mòdul quadràtic és un preordre de A si també és tancat en la multiplicació.*

Definició 2.7. *Un polinomi f és definit semipositivament si $f(x) \geq 0$ $\forall x \in \mathbb{R}$. De forma similar, és definit positivament si $f(x) > 0$ $\forall x \in \mathbb{R}$.*

Definició 2.8. *Sigui $S = \{g_1, \ldots, g_k\}$ on $g_1, \ldots, g_k \in \mathbb{R}[x]$, denotarem com a K_S el conjunt generat per S. Llavors definim K_S com*

$$K_S := \{x \in \mathbb{R} \mid g_1 \geq 0, \ldots, g_k \geq 0\}.$$

Definició 2.9. *El preordre generat per un conjunt S, expressat com P_S, és el preordre més petit que conté S.*

Podem veure que $f \in P_S$ si i només si f es pot escriure com

$$f = \sum_{\epsilon = \{\epsilon_1, \ldots, \epsilon_k\} \in \{0,1\}^k} \sigma_\epsilon g_1^{\epsilon_1} \cdots g_k^{\epsilon_k},$$

on $\sigma_\epsilon \in \sum \mathbb{R}[x]^2$.

Definició 2.10. *Sigui $S = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[x]$. El mòdul quadràtic generat per S, M_S, és el mòdul quadràtic més petit que conté S.*

Podem veure que el mòdul quadràtic consisteix en totes les $f \in \mathbb{R}[x]$ tals que

$$f = \sigma_0 + \sigma_1 g_1 + \cdots + \sigma_k g_k,$$

per alguns $\sigma_0, \ldots, \sigma_s \in \sum \mathbb{R}[x]^2$.

Observació 2.11. Veiem que sempre es compleix que $M_S \subseteq P_S$ i si $\#S = 1$ llavors $M_S = P_S$, però si $\#S > 1$ en general no es compleix la igualtat ja que hi poden haver combinacions de sumes de quadrats que no estiguin al preordre, però hi ha algunes excepcions.

Exemple 2.12. Si prenem $S = \{1 - x, 1 + x\}$ on $\#S = 2$ llavors en $\mathbb{R}[x]$ tenim

$$(1 + x)(1 - x) = \frac{1}{2}(1 - x)^2(1 + x) + \frac{1}{2}(1 + x)^2(1 - x)$$

per tant $(1 - x)(1 + x) \in M_S$ i en aquest cas sí que es compleix $M_S = P_S$.

Definició 2.13. *$f \in \mathbb{R}[x]$ és suma de quadrats si existeixen $g_1, \ldots, g_k \in \mathbb{R}[x]$ tals que*

$$f = g_1^2 + \cdots + g_k^2.$$

Definició 2.14. *Un preordre P_S és saturat si quan $f \geq 0$ en K_S implica que $f \in P_S$. El mateix passa amb un mòdul quadràtic M_S, si quan $f \geq 0$ en K_S llavors $f \in M_S$ i M_S és saturat.*

Si tenim $S \subseteq \mathbb{R}[x]$, podem definir quatre propietats relacionades als certificats de positivitat de K_S. Ja que l'existència de certificats de positivitat pot dependre de S, aquestes propietats són de S no de K_S. Les propietats són les següents:

$$\begin{aligned}
(\geq) \quad & f \geq 0 \text{ en } K_S \Rightarrow f \in P_S \\
(>) \quad & f > 0 \text{ en } K_S \Rightarrow f \in P_S \\
(\geq)_M \quad & f \geq 0 \text{ en } K_S \Rightarrow f \in M_S \\
(>)_M \quad & f > 0 \text{ en } K_S \Rightarrow f \in M_S
\end{aligned}$$

Definició 2.15. *Preneu un subconjunt no buit V d'un espai vectorial E sobre $\mathbb{F}$. Anomenarem a V varietat lineal sobre E si per tot f, g de V i tot α, β de $\mathbb{F}$, $\alpha f + \beta g$ està en V.*

Definició 2.16. *Sigui $(\mathbb{A}, E, \phi)$ l'espai afí definit sobre $\mathbb{F}$. Diem que $V \subset \mathbb{A}$ és una varietat afí si (V, E, ϕ') també és un espai afí definit sobre cert espai vectorial $F \subseteq E$ i amb certa aplicació ϕ'.*

Definició 2.17. *Un polinomi trigonomètric és un polinomi que s'expressa de la forma $w(e^{i\theta}) = \sum_{j=-n}^{n} c_j e^{ji\theta}$ en $\mathbb{C}[x]$.*

Definició 2.18. *Donat un anell A, un ideal de A és un subconjunt I de A tal que*

1. *$(I, +)$ és subgrup de $(A, +)$;*
2. *$ax \in I$, per a tot parell d'elements $a \in A$, $x \in I$.*

Definició 2.19. *Un ideal I d'un anell A es diu ideal primer si és un ideal propi i, per a $a, b \in A$, es compleix*

$$ab \in I \implies a \in I \text{ o } b \in I.$$

Definició 2.20. *Anomenem anell noetherià a un anell commutatiu i unitari que satisfà que la cadena d'ideals és estacionària. És a dir, donada una cadena d'ideals:*

$$I_1 \subseteq \cdots \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq \cdots$$

existeix un n tal que:

$$I_n = I_{n+1} = \cdots .$$

Definició 2.21. *Un morfisme d'anells és una aplicació $f : A_1 \to A_2$ que compleix*

$$f(a+b) = f(a) + f(b) \ i \ f(ab) = f(a)f(b)$$

Definició 2.22. *Considerem un morfisme d'anells $f : A_1 \to A_2$ on A_1 i A_2 són anells amb el 1.*

$$\tilde{f} : \frac{\mathbb{F}[x_1, \ldots, x_n]}{I(A_2)} \to \frac{\mathbb{F}[x_1, \ldots, x_n]}{I(A_1)}$$

és un isomorfisme d'anells que indueix a f. Existeix una aplicació lineal $g : A_2 \to A_1$ tal que $f \circ g = Id_{A_2}$ i $g \circ f = Id_{A_1}$,

Definició 2.23. *Considerem A un anell. Denotem* $\operatorname{Sper} A$ *al espectre real de A, és a dir, al espai topològic que consisteix en tots els parells $\alpha = (\mathfrak{p}, \omega)$ on $\mathfrak{p} \in \operatorname{Sper} A$ i ω és un cos residual ordenat del quocient $(A/\mathfrak{p})$ de $\mathfrak{p}$.*

Definició 2.24. *Si V és una R-varietat afí, escrivim l'anell de coordenades com $R[V]$. Un anell de coordenades és un anell associat a un conjunt de funcions polinòmiques definides en una varietat afí. Altrament dit,*

$$R[V] = \frac{R[x_1, \ldots, x_n]}{I(V)}$$

on $I(V)$ és l'ideal de V.

Definició 2.25. *Sigui V una varietat algebraica i sigui $p \in V$ un punt. L'espai tangent a V en p, denotat per T_pV, és el subespai vectorial definit com:*

$$T_pV := \left\{ v \in \mathbb{F}^n \;\middle|\; \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p) v_i = 0 \right\}$$

Definició 2.26. *Sigui $A = \mathbb{F}[x_1, \ldots, x_n]/I$ l'anell de coordenades d'una varietat afí V.*

La dimensió algebraica de V, denotada $\dim V$*, és la longitud màxima d'una cadena estrictament creixent d'ideals primers en A, és a dir:*

$$\dim V = \dim A = \sup \{ r \in \mathbb{N} \mid \exists\, \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r \text{ ideals primers en } A \}$$

Definició 2.27. *Donat un subconjunt $S \subseteq \mathbb{F}[x]$, la varietat afí definida per S és*

$$\mathcal{Z}(S) := \{ x \in \mathbb{F}^n \mid f(x) = 0 \text{ per tot } f \in S \},$$

el conjunt zero de S.

Definició 2.28. *Anomenem ideal d'anul·lació al ideal d'un anell polinomial que donada una varietat algebraica, aquest es redueix a zero. Per un subconjunt $K \subseteq \mathbb{F}^n$, l'ideal d'anul·lació de K és*

$$I(K) = \{ f \in \mathbb{F}[x] \mid f(x) = 0 \text{ per tot } x \in K \}.$$

És fàcil veure que $I(K)$ és un ideal de $\mathbb{F}[x]$.

Definició 2.29. *Sigui A un anell commutatiu amb 1, i sigui $I \subseteq A$ un ideal.*

1. *El radical de I és*

$$\sqrt{I} = \{a \in A \mid \exists m \in \mathbb{N} \text{ tal que } a^m \in I\}.$$

2. *I és real si $a_1, \ldots, a_k \in A$ amb $a_1^2 + \cdots + a_k^2 \in I$ implica que $a_i \in I$ per $i = 1, \ldots, k$.*

3. *El radical real de I és*

$$\sqrt[\text{re}]{I} = \{a \in A \mid \exists m \in \mathbb{N},\, b_1, \ldots, b_k \in A \text{ amb } a^{2m} + b_1^2 + \cdots + b_k^2 \in I\}.$$

Definició 2.30. *Un cos és formalment real si es pot assignar una mesura d'ordre per a tenir un cos ordenat.*

Definició 2.31. *Anomenem $\sqrt[\text{re}]{(0)}$, el nilradical real de A. $\sqrt[\text{re}]{(0)}$ és la intersecció de tots els radicals primers tals que el seu cos residual és formalment real.*

Teorema 2.32. *([1] Nullstellensatz de Hilbert) Suposem I és un ideal en $\mathbb{C}[x]$, llavors*

$$I(\mathcal{Z}(I)) = \sqrt{I}.$$

Teorema 2.33. *([1] Nullstellensatz Real) Suposem que I és un ideal en $\mathbb{R}[x]$, llavors*

$$I(\mathcal{Z}(I)) = \sqrt[\text{re}]{I}.$$

És més, $\sqrt[\text{re}]{I} = I$ si i només si I és un ideal real.

Definició 2.34. *Un mapa racional és un morfisme entre varietats no buides que es pot escriure amb funcions racionals.*

Definició 2.35. *Un mapa birracional de X a Y és un mapa racional $f : X \to Y$ tal que hi ha un mapa racional $Y \to X$ invers respecte f.*

Definició 2.36. *Prenem V una R-varietat afí i sigui S un subconjunt semialgebraic de $V(R)$. Escrivim*

$$B_V(S) = \{f \in R[V] \mid \exists \lambda \in R\ \forall x \in S : |f(x)| \leq \lambda\}$$

per l'anell de funcions acotades sobre S. Principalment, ens interessarà el cas $S = V(R)$, pel qual utilitzem la notació

$$B(V) = B_V(V(R)).$$

3 Polinomis definits semipositivament i sumes de quadrats

En aquesta secció ens endinsarem en els certificats de positivitat en intervals tancats de $\mathbb{R}$. Començarem veient un teorema senzill que ens diu que tot polinomi no negatiu en $\mathbb{R}$ pot ser escrit com a suma de quadrats de polinomis. Un cop vist, només ens queden dos casos generals a analitzar; els intervals tancats i els semi-infinits.

3.1 Semipositivitat de polinomis en $\mathbb{R}$

Proposició 3.1. *[1] Si $f \in \mathbb{R}[x]$ és un polinomi definit semipositivament, llavors el coeficient principal de f és positiu i totes les arrels reals de f apareixen amb multiplicitat parella.*

Demostració: El grau de f és parell per ser definit semipositivament, per tant si el coeficient principal fos negatiu tindríem que $\lim_{x\to\infty} f(x) = -\infty$, que contradiu que $f \geq 0$. Com que f no pot canviar de signe a les arrels, tota arrel apareix amb multiplicitat parella.

□

Aquesta propietat dels polinomis definits semipositivament ens és molt útil per demostrar el següent teorema, que ens diu que existeixen els certificats de positivitat per tots els polinomis $f \geq 0$, i és la base de tota la primera meitat del treball.

Teorema 3.2. *[1] Si $f \in \mathbb{R}[x]$ és un polinomi definit semipositivament, llavors f pot ser escrit com a suma de dos quadrats de polinomis en $\mathbb{R}[x]$.*

Demostració: Per el teorema fonamental de l'Àlgebra, f pot ser factoritzat en factors lineals a $\mathbb{C}$. Com que f té tots els coeficients reals, totes les arrels en $\mathbb{C} \setminus \mathbb{R}$ venen en parelles conjugades. Per la Proposició 3.1, el coeficient principal de f és positiu, per tant és c^2 per algun $c \in \mathbb{R}$ diferent de 0. Suposem que les arrels reals de f són $a_1, \ldots, a_s$ amb multiplicitats $2u_1, \ldots, 2u_s$, i les no reals són les parelles conjugades $\{b_1 \pm ic_1, \ldots, b_t \pm ic_t\}$. Llavors tenim

$$f = c^2 \cdot \prod_{j=1}^{s} (x - a_j)^{2u_j} \cdot \prod_{k=1}^{t} (x - (b_k + ic_k))(x - (b_k - ic_k)).$$

Sigui $p(x) = c \cdot \prod_{j=1}^{s} (x - a_j)^{u_j}$. Expandint el segon producte, ho podem escriure com a $(q(x) + ih(x))(q(x) - ih(x))$, on $q(x), h(x) \in \mathbb{R}[x]$. Per tant, ens queda

$$f = (p(x))^2 \cdot (q(x) + ih(x))(q(x) - ih(x)) = (p(x)q(x))^2 + (p(x)h(x))^2.$$

□

Un cop hem vist que tot polinomi definit semipositivament es pot escriure com a suma de quadrats de polinomis, anem a aprofundir en la seva positivitat depenent de l'interval.

Per a $a, b \in \mathbb{R}$ amb $a < b$, considerem el canvi de variables

$$x \to \left(\frac{b-a}{2}\right) x + \frac{b+a}{2}$$

Veiem que $f \geq 0$ en $[a, b]$ si i només si $\tilde{f} \geq 0$ en $[-1, 1]$, considerant $\tilde{f}$ com el polinomi f després del canvi de variables. Això ens és útil ja que per qualsevol interval $[a, b]$ podem

aplicar un canvi de variables per arribar al interval $[-1,1]$ i, per tant, tots els resultats que trobem per $[-1,1]$ podran ser generalitzats a qualsevol interval tancat.

Hom podria pensar que sembla més natural agafar l'interval tancat $[0,1]$ com l'interval de referència. Això va ser així pels primers teoremes que van donar Bernstein i Hausdorff, però més tard va ser canviat a $[-1,1]$ pels analistes, que volien saber quins polinomis p complien la propietat que el polinomi trigonomètric $p(cos\theta)$ només tenia valors no negatius.

Un cop trobat que tot interval tancat es pot reduir al cas $[-1,1]$ ens queda veure els intervals semi-infinits. Amb un canvi de variables semblant, podem veure que tot interval es pot reduir al cas $[0,\infty)$. Finalment, veiem que mitjançant la transformada de Goursat (Definició 2.4)

$$\hat{f}(x) = (1+x)^d f\left(\frac{1-x}{1+x}\right),$$

podem trobar una relació entre els dos intervals.

Proposició 3.3. *[1] Suposem $f \in \mathbb{R}[x]$ amb grau $f = d$. Llavors $f \geq 0$ en $[-1,1]$ si i només si $\hat{f} \geq 0$ en $[0,\infty)$, i $f > 0$ en $[-1,1]$ si i només si $\hat{f} > 0$ en $[0,\infty)$ i grau $\hat{f} = d$.*

Demostració: Per $x \in (-1,1]$, agafem $y = (1-x)/(1+x) \in [0,\infty)$. Com que $(1+x)^d > 0$, tenim per definició $f(x) > 0$ si i només si $\hat{f}(y) > 0$ (respectivament amb les desigualtats estrictes). Per la transformada de Goursat, grau de $\hat{f} = d$ si i només si $f(-1) \neq 0$. Tenim per tant que $f > 0$ en $[-1,1]$ si i només si $\hat{f} > 0$ en $[0,\infty)$ i grau de $\hat{f} = d$. Si $f > 0$ en $(-1,1]$, llavors tenim que $f(-1) \geq 0$ per continuïtat, per tant $f \geq 0$ en $[-1,1]$ si i només si $\hat{f} \geq 0$ en $[0,\infty)$.

□

Resulta que la positivitat en $[-1,1]$ i en $[0,\infty)$ està fortament relacionada i, per tant, podem trobar teoremes amb qualsevol dels dos intervals i derivar-ho al mateix resultat per l'altre.

3.2 Representació de Bernstein i acotació

Un cop vist que podem veure si un polinomi és definit semipositivament en un interval només estudiant com es comporten en $[-1,1]$ després d'un canvi de variable, podem començar a fer preguntes sobre certificats de positivitat en intervals tancats i acotats. El primer que va preguntar va ser Hermite, que al 1894, en el primer volum del diari de problemes francès *Interméd des math*, va preguntar-se si que $f > 0$ en $[-1,1]$ implicava que f pot ser escrita com a

$$f(x) = \sum_{i+j \leq d} c_{ij}(1-x)^i(1+x)^j,$$

on d és el grau de f i c_{ij} són nombres reals no negatius. La resposta a aquesta pregunta ca venir un temps després, quan Goursat, Sadier i Franel van demostrar que no, cada un d'ells d'una manera diferent. Més tard, al 1915, Bernstein va demostrar que, si relaxàvem la condició del grau $i + j \leq d$, podíem trobar una representació de la forma desitjada.

En aquesta secció veurem com es pot trobar la representació relaxant la condició del grau a $i + j \leq m$ amb $m \in \mathbb{N}$ i ens centrarem en trobar una cota per al grau màxim d'aquesta representació.

Proposició 3.4. *[3] [4] Suposem $q(x_1, \ldots, x_n)$ és un polinomi homogeni real de grau d, on els coeficients de q estan acotats superiorment en valor absolut per L i que $q(u) \geq \lambda > 0$ per $u \in \Delta = \{(u_1, \ldots, u_n) \mid u_j \geq 0, \sum_j u_j = 1\}$.*

Si

$$r \geq \frac{Lnd^2}{\lambda} + nd \geq \frac{Ld(d-1)}{2\lambda} - d,$$

llavors $(\sum_j x_j)^r q(x_1, \ldots, x_m)$ té tots els coeficients positius.

Demostració: Prenem $t \in \mathbb{R}_+$ i $m \in \mathbb{Z}_{\geq 0}$ i definim $(x)_t^m \in \mathbb{R}[x]$ com

$$(x)_t^m = x(x-t)\ldots(x-(m-1)t) = \prod_{i=0}^{m-1}(x-it).$$

Sigui d = grau de q, $\alpha = (\alpha_1, \ldots, \alpha_n)$ i $|\alpha| = \alpha_1 + \cdots + \alpha_n$. Escrivim q com a $q = \sum_{|\alpha|=d} a_\alpha x^\alpha \in \mathbb{R}[x]$, i assumim $q > 0$ en Δ. El cas $d = 1$ és trivial, així que assumim $d > 1$. Donat $N \in \mathbb{N}$, expressem el polinomi com

$$(x_1 + \cdots + x_n)^N q = \sum_{|\beta|=N+d} b_\beta x^\beta.$$

Fent uns càlculs computacionals podem trobar el valor de b_β com a

$$b_\beta = \frac{N!(N+d)^d}{\beta_1! \ldots \beta_n!} \sum_{|\alpha|=d} a_\alpha \cdot \left(\frac{\beta_1}{N+d}\right)_{(N+d)^{-1}}^{\alpha_1} \cdots \left(\frac{\beta_n}{N+d}\right)_{(N+d)^{-1}}^{\alpha_n}. \tag{3.1}$$

Per $t \in \mathbb{R}_+$, podem definir

$$f_t = f_t(y_1, \ldots, y_n) = \sum_{|\alpha|=d} a_\alpha (x_1)_t^{\alpha_1} \ldots (x_n)_t^{\alpha_n} \in \mathbb{R}[x].$$

Com que quan $t \to 0$, $(x)_t^{\alpha_i} \to x^{\alpha_i}$, llavors $f_t \to f$ uniformement a Δ. Com que $f > 0$ en Δ per hipòtesi, podem trobar una t prou petita tal que $f_t > 0$ en Δ. Triem ara un $N \in \mathbb{N}$ tal que $q_{(N+d)^{-1}} > 0$ a Δ, llavors per alguna $\beta \in \mathbb{N}^n$ tal que $|\beta| = N + d$, tenim que

$$\left(\frac{\beta_1}{N+d}, \ldots, \frac{\beta_n}{N+d}\right) \in \Delta.$$

Tenim per (3.1) que $b_\beta > 0$ per a tot $|\beta| = N + d$. Amb això veiem que tots els coeficients de $(x_1 + \cdots + x_n)^N q$ són estrictament positius.

Ara generalitzem el treball de Pólya per a trobar la $N \in \mathbb{N}$. Deixem anar el factor constant a 3.1 i fixem

$$t = \frac{1}{N+d}, \quad y_k = \frac{\beta_k}{N+d},$$

recordem que $\sum y_k = 1$. Tenim per tant,

$$f_t(y_1, \ldots, y_n) = f(y_1, \ldots, y_n) - \sum_{|\alpha|=d} a_\alpha (y_1^{\alpha_1} \cdots y_n^{\alpha_n} - (y_1)_t^{\alpha_1} \ldots (y_n)_t^{\alpha_n}).$$

Usant la informació que tenim sobre f, veiem que

$$f_t(y_1,\dots,y_n) \geq \lambda - L\sum_{|\alpha|=d}\frac{d!}{\alpha_1!\cdots\alpha_n!}|y_1^{\alpha_1}\cdots y_n^{\alpha_n} - (y_1)_t^{\alpha_1}\dots(y_n)_t^{\alpha_n}|. \tag{3.2}$$

Si $\alpha_k > \beta_k$, llavors $(y_k)_t^{\alpha_k} = 0$, per tant, $y_k^{\alpha_k} \geq (y_k)_t^{\alpha_k} \geq 0$ per a tot k així que podem treure el valor absolut de l'equació.

Pel Teorema Multinomial,

$$\sum_{|\alpha|=d}\frac{d!}{\alpha_1!\cdots\alpha_n!}y_1^{\alpha_1}\cdots y_n^{\alpha_n} = (y_1+\cdots+y_n)^d = 1.$$

Per la identitat iterada de Vandermonde–Chu (la demostrarem més endavant):

$$\sum_{|\alpha|=d}\frac{d!}{\alpha_1!\cdots\alpha_n!}(y_1)_t^{\alpha_1}\cdots(y_n)_t^{\alpha_n} = (y_1+\cdots+y_n)_t^d = \prod_{k=0}^{d-1}(1-kt).$$

Per 3.2 només hem de veure que

$$\lambda - L(1-(1-t))\cdots(1-(d-1)t) \geq 0,$$

i queda demostrat.

Suposem ara que

$$t = \frac{1}{N+d} < \frac{2}{d(d-1)}\cdot\frac{\lambda}{L}.$$

Veiem fàcilment per inducció que quan $0 \leq w_j \leq 1$, llavors $\prod(1-w_j) \geq 1-\sum w_j$. Com que $\lambda \leq f(1,0,\dots,0) \leq L$ i $d \geq 2$, tenim

$$t < \frac{1}{d(d-1)}$$

i, per tant,

$$(1-(1-t)\cdots(1-(d-1)t)) < (1+2+\cdots+(d-1))t = \frac{(d-1)d}{2}t < \frac{\lambda}{L}.$$

Finalment, només ens queda veure la identitat iterada de Vandermonde-Chu,

$$\sum_{|\alpha|=d}\frac{d!}{\alpha_1!\cdots\alpha_n!}(x_1)_t^{\alpha_1}\cdots(x_n)_t^{\alpha_n} = (x_1+\cdots+x_n)_t^d. \tag{3.3}$$

Veiem primer 3.3 de forma combinatòria en el cas concret on $t=1$ i $x_k = y_k$ és un enter no negatiu

$$\sum_{|\alpha|=d}\frac{d!}{\alpha_1!\cdots\alpha_n!}(y_1)_1^{\alpha_1}\cdots(y_n)_1^{\alpha_n} = (y_1+\cdots+y_n)_1^d.$$

Considerem n conjunts $S_1,\dots,S_n$ d'elements no iguals, on $|S_k| = y_k$, i $S = \bigcup S_k$. Aleshores el nombre de d-tuples d'elements diferents de S és

$$y(y-1)\cdots(y-(d-1)),$$

on $y = \sum y_k$, que és la part de la dreta de l'equació. Comptem el nombre de d-tuples d'una altra manera. Per a cada n-tupla α amb $|\alpha| = d$, considerem el nombre de d-tuples on on hi ha α_k elements diferents de S_k, $1 \leq k \leq n$. Hi ha $\binom{y_k}{\alpha_k} = \frac{(y_k)_1^{\alpha_k}}{\alpha_k!}$ maneres d'escollir-los, amb $d!$ maneres de distribuir-los, per tant ens queden

$$d! \prod_{k=1}^{n} \frac{(y_k)_1^{\alpha_k}}{\alpha_k!} = \frac{d!}{\alpha_1! \cdots \alpha_n!} (y_1)_1^{\alpha_1} \cdots (y_n)_1^{\alpha_n}$$

d-tuples. Amb totes les tries de α completem la part esquerra de l'equació, per tant queda demostrat el cas concret on els y_k són enters no negatius. Però els dos costats de l'equació són polinomis en els y_k, i la seva diferència és un polinomi que s'anul·la en $\mathbb{N}^n$. Per tant, s'anul·la idènticament, i aquest cas especial passa a ser un reflex per tots els y_k reals. Finalment, prenem $y_k = x_k/t$ i multipliquem per t^d tenint en compte la definició de $(y)_t^d$ ens queda demostrat 3.3.

□

Ara, si tenim una funció definida semipositivament $g(x) = \sum_{j=0}^{m} c_j x^j$, $g(x) > 0$ per tot $x \geq 0$, la funció homogènia $G(x, y) = \sum_{j=0}^{m} c_j x^j y^{m-j}$ compleix que quan $x \geq 0, y \geq 0$, $x + y = 1$ llavors $G(x, y) \geq 0$ i quan $y = 1$, $G(x, 1) = g(x)$.

Per la proposició 3.4 tenim que existeix un r que fa que $(1 + x)^r g(x)$ tingui tots els coeficients positius i és definida semipositiva ja que $x \geq 0$ per tant $(1 + x)^r g(x) \geq 0$.

Definició 3.5. *Prenem $g(x)$ definida positivament en $[0, \infty)$. Definim $\hat{r}(g)$ com l'enter d més petit tal que $(1 + x)^d g(x)$ té coeficients no negatius.*

Prenem $f(x)$ una funció qualsevol, de grau d definida positiva en $x \in [-1, 1]$. Quan li apliquem la transformada de Goursat $\hat{f}(x)$, com que és definida positiva en $[0, \infty)$ tenim que existeix una r tal que $(1 + x)^r \hat{f}(x) = \sum_{j=0}^{r+d} d_j x^j$ té tots els seus coeficients postius. Podem aplicar la transformada de Goursat de grau d a la nova funció i ens queda

$$\frac{2}{(1+x)^r}(1+x)^d \hat{f}\left(\frac{1-x}{1+x}\right) = \sum_{j=0}^{r+d} d_j \left(\frac{1-x}{1+x}\right)^j \frac{2}{(1+x)^r} = \frac{2^{d+1}}{(1+x)^r} f(x).$$

$$f(x) = \sum_{j=0}^{r+d} \frac{d_j}{2^d} (1+x)^j (1-x)^{r+d-j}$$

Per tant, com 2^d és positiu, no canvia la positivitat dels coeficients i podem representar $f(x)$ com a un polinomi amb tots els coeficients positius.

Definició 3.6. *Definim $\mathcal{P}_d$ com*

$$\mathcal{P}_d := \left\{ \sum_{i+j \leq d} c_{ij} (1-x)^i (1+x)^j \mid c_{ij} \geq 0 \right\}.$$

Definició 3.7. *El grau de Bernstein d'una funció f definida positivament en $[-1, 1]$, escrit com a $r(f)$, és l'enter més petit n tal que $f \in \mathcal{P}_n$.*

Corol·lari 3.8. *([2], Corol·lari 5) Suposem* $g(x) = \sum_{j=0}^{d} b_j x^j$ *definit positivament en* $[0, \infty)$, $|b_j| \leq L$ *i*

$$\lambda = \min \left\{ \sum_{j=0}^{d} b_j t^j (1-t)^{d-j} \mid t \in [0,1] \right\}.$$

Llavors

$$\hat{r}(g) \leq 2d + \left\lceil \frac{2d^2 L}{\lambda} \right\rceil.$$

Demostració: Sigui $q(x,y) = \sum_{j=0}^{d} b_j x^j y^{d-j}$, apliquem la proposició 3.4 a q, amb $m = 2$ i substituïm a y per $1-t$ per a que ens quedi una representació de $g(x)$. Observem que $\lambda = \inf\{(1-t)^d g\left(\frac{t}{1-t}\right) \mid t \in [0,1)\}$.

□

Un cop vist tot això, podem passar al teorema principal, on aconseguim acotar el grau m de la representació en funció, principalment, dels coeficients de f.

Teorema 3.9. *([2], Teorema 6) Suposem que* $f(x) > 0$ *en* $[-1,1]$. *Prenem* $d =$ *grau de* f *i* λ *com el mínim de* f *en* $[-1,1]$. *Llavors existeixen nombres reals positius* c_{ij} *i* $m \in \mathbb{Z}_{\geq 0}$ *tals que:*

$$f(x) = \sum_{i+j \leq m} c_{ij} (1-x)^i (1+x)^j,$$

i

$$m \leq 3d + \left\lceil \frac{2d^2 \|f\|_1}{\lambda} \right\rceil.$$

Demostració:

Ja hem vist amb les proposicions i definicions anteriors que $f(x)$ pot ser representat com

$$f(x) = \sum_{j=0}^{r+d} c_j (1+x)^j (1-x)^{m-j}$$

que és el mateix que dir que la podem representar com a

$$f(x) = \sum_{i+j \leq m} c_{ij} (1-x)^i (1+x)^j.$$

per alguna m.

Anem a comprovar ara que quan $f \in \mathcal{P}_m$ llavors m està acotada com a

$$m \leq 3d + \left\lceil \frac{2d^2 \|f\|_1}{\lambda} \right\rceil.$$

Per començar suposem $m = \hat{r}(\hat{f})$, de manera que

$$(1+x)^{m+d} f\left(\frac{1-x}{1+x}\right) = (1+x)^m \hat{f}(x) = \sum_{k=0}^{m+d} b_k x^k,$$

amb $b_k \geq 0$. Si apliquem la transformada de Goursat de grau $m+d$ a les dues igualtats llavors obtindrem

$$2^{m+d} f(x) = \sum_{k=0}^{m+d} b_k (1-x)^k (1+x)^{m+d-k}.$$

i

$$f(x) = \sum_{k=0}^{m+d} \hat{b}_k (1-x)^k (1+x)^{m+d-k}.$$

Per tant, veiem que $r(f) \leq m+d = \hat{r}(\hat{f}) + d$.

Anem a comprovar ara que $r(f) \geq \hat{r}(\hat{f}) + d$ i, per tant, que són iguals. Observem que la representació de $f(x)$

$$f(x) = \sum_{i+j \leq d} c_{ij} (1-x)^i (1+x)^j$$

amb $c_{ij} \geq 0$ pot ser escrita com:

$$f(x) = \sum_{i+j \leq r} c_{ij} (1-x)^i (1+x)^j \left(\frac{1-x}{2} + \frac{1+x}{2} \right)^{r-(i+j)}$$

$$= \sum_{i+j \leq r} c_{ij} (1-x)^i (1+x)^j \frac{1}{2^{r-(i+j)}} \sum_{\ell=0}^{r-(i+j)} \binom{r-(i+j)}{\ell} (1-x)^\ell (1+x)^{r-(i+j)-\ell}$$

$$:= \sum_{k=0}^{r} c_k (1-x)^k (1+x)^{r-k},$$

i si $c_{ij} \geq 0$ per tot i, j, llavors també tenim que $c_k \geq 0$ per tot k. Per tant, sempre podem aconseguir $r(f)$ usant una representació equivalent de f.

Fent servir aquesta representació de f amb $c_k \geq 0$, podem aplicar la transformada de Goursat de grau $r \geq d$, i obtenim

$$(1+x)^r f\left(\frac{1-x}{1+x} \right) = (1+x)^{r-d} \hat{f}(x) = 2^r \sum_{k=0}^{r} c_k x^k$$

i per tant tenim que $\hat{r}(\hat{f}) \leq r(f) - d$ i veiem $r(f) \geq \hat{r}(\hat{f}) + d$, que usant el resultat que hem trobat anteriorment concloem que $r(f) = \hat{r}(\hat{f}) + d$. Ara només ens fa falta aplicar el corol·lari 3.8. Veiem que

$$\hat{r}(\hat{f}) = r(f) - d \leq \left\lceil \frac{2Ld^2}{\lambda} \right\rceil + 2d$$

$$m \leq 3d + \left\lceil \frac{2d^2 \|f\|_1}{\lambda} \right\rceil.$$

ja que $\|f\|_1 = |c_k| \leq L$ i al principi hem suposat $\hat{r}(\hat{f}) = m$.

□

3.3 Mòdul quadràtic i preordre

En la majoria dels casos, els certificats de positivitat de polinomis en conjunts semialgebraics venen d'objectes algebraics associats al conjunt. Dos dels més importants són els mòduls quadràtics i els preordres.

Pólya i Szegő van ser dels primers en veure i demostrar que quan $f \geq 0$ en $[-1,1]$ llavors f pertany al mòdul quadràtic generat per x. Per veure-ho, primer hem de trobar una manera de representar f com $f = \sigma + \tau x$ smb σ, τ suma de quadrats.

Teorema 3.10. *[1] Suposem $f \in \mathbb{R}[x]$ amb el grau de $f = d$ i amb $f \geq 0$ en $[0,\infty)$. Llavors existeixen $\sigma, \tau \in \sum \mathbb{R}[x]^2$ amb grau de σ, $\tau x \leq d$ tals que $f = \sigma + \tau x$.*

Demostració: Suposem $f_1 = \sigma_1 + \tau_1 x$ i $f_2 = \sigma_2 + \tau_2 x$, on $\sigma_1, \sigma_2, \tau_1, \tau_2 \in \sum \mathbb{R}[x]^2$ amb els graus de σ_i, $\tau_i x \leq$ grau de f_i. Llavors tenim que

$$f_1 \cdot f_2 = (\sigma_1 + \tau_1 x)(\sigma_2 + \tau_2 x) = (\sigma_1\sigma_2 + \tau_1\tau_2 x^2) + (\sigma_1\tau_2 + \sigma_2\tau_1)x,$$

que és de la forma $\sigma + \tau x$ on els graus dels polinomis σ, $\tau x \leq$ grau $f_1 f_2$. Per tant, és suficient escriure f com a producte de factors que satisfan la conclusió del teorema.

Factoritzem f en factors lineals de $\mathbb{C}$. Com que $f \geq 0$ en $[0,\infty)$, qualsevol arrel real positiva de f és de grau parell i les arrels complexes són parelles de conjugats que corresponen a factors definits semipositivament. Per tant, podem factoritzar f com a $p \cdot x^a \cdot \prod(x + b_i)$, on p està definit semipositivament, $a \in \{0,1\}$, i cada $b_i > 0$. Com que això compleix la representació de f com a suma de polinomis quadrats, queda demostrat.

□

Gràcies a aquest teorema podem demostrar que existeixen certificats de positivitat en un mòdul quadràtic per $f \geq 0$ en $[-1,1]$, amb una certa informació del grau de f.

Teorema 3.11. *[1] Sigui $S = \{1 - x^2\}$ i $U = \{1 - x, 1 + x\}$, observem que $K_S = K_U = [-1,1]$. Llavors tenim*

1. *$M_S = M_U$.*
2. *Suposem que $f \in \mathbb{R}[x]$ amb $f \geq 0$ a $[-1,1]$ i que el grau de $f = d$. Llavors $f \in M_S = M_U$. Més concretament, si d és parell, llavors $f = \sigma + \tau(1 - x^2)$, on σ, τ són sumes de quadrats amb els graus de $\sigma, (1 - x^2)\tau \leq d$. Si d és imparell, llavors $f = \sigma(1+x) + \tau(1-x)$, on σ, τ són sumes de quadrats amb els graus de $\sigma, \tau \leq d-1$.*

Demostració:

(1) Podem veure amb les igualtats

$$1 \pm x = \frac{(1 \pm x)^2}{2} + \frac{1 - x^2}{2}$$

que $M_U \subseteq M_S$. Tenint en compte que $1 - x^2 = (1 + x)(1 - x)$ podem veure que $M_S \subseteq P_U$. Per l'exemple 2.12 $P_U = M_U$. Per tant, $M_S = M_U$.

(2) Per la proposició 3.3 $\hat{f} \geq 0$ a $[0,\infty)$, on $\hat{f}$ és la transformada de Goursat de f. Tenim que, per el Teorema 3.10 fent servir que tot polinomi que és suma de quadrats ho és com a maxim de dos quadrats, podem veure que

$$\hat{f} = g_1^2 + g_2^2 + (h_1^2 + h_2^2)x,$$

on $r_i :=$ grau de $g_i \leq d/2$ i $s_i :=$ grau de $h_i \leq (d-1)/2$. Si tornem a aplicar la transformada de Goursat obtenim

$$2^d f = \sum_{i=1,2} (1+x)^{d-2r_i} (\hat{g_i})^2 + (1-x) \sum_{i=1,2} (1+x)^{d-1-2s_i} (\hat{h_i})^2.$$

En el cas on d és parell, el primer terme és una suma de quadrats amb un grau màxim d, i el segon terme pot ser escrit com $(1-x^2)\sigma$, on σ és suma de quadrats de grau $\sigma \leq d-2$. Per altra banda, si d és senar, el primer terme és $(1+x)\sigma$ amb σ suma de quadrats del grau pertinent i el segon terme és $(1-x)\tau$ amb τ suma de quadrats del grau pertinent. □

Finalment, veiem un cas especial del teorema de Schmüdgen ([1] capítol 7). El teorema de Schmüdgen ens diu que si K_S és compacte, llavors per tot $f \in \mathbb{R}[x]$ tal que $f > 0$ en K_S, $f \in P_S$. Nosaltres ens limitarem al cas on S està format per un únic polinomi, $\#S = 1$, i $K_S = [-1, 1]$. Quan $f > 0$, llavors construïm polinomis reals definits semipositivament s i t tals que

$$f = s + th.$$

Abans de poder escriure s i h com a suma de quadrats de polinomis, hem de demostrar el teorema següent:

Teorema 3.12. *([2], Teorema 7) Prenem $\epsilon > 0$, i $h(x) = (1-x^2)^r q(x)$ amb r senar, on $0 < \alpha \leq q(x)$ per a $x \in (-\infty, -1] \cup [1, \infty)$ i $0 \leq q(x) \leq \beta$ per a $x \in [-1, 1]$.*

Llavors prenem

$$A = \frac{1}{r 2^r \epsilon^{r-1} \alpha}, \quad i \quad m = \left\lfloor \frac{r}{2\epsilon} \left(\frac{\beta}{r\alpha} \right)^{\frac{1}{r}} \right\rfloor,$$

si agafem $F(x)$ com a $F(x) = 1 + \epsilon + x - Ax^{2m} h(x)$ aquesta és definida semipositiva.

Observació 3.13. Observem que aquest teorema ens implica que F és suma de quadrats, per tant $1 + \epsilon + x = F + Ax^{2m} h$ pertany al preordre de h.

Prenem $\bar{h}(x) = h(-x)$, llavors agafant els mateixos valors de α, β, A i M, tenim que $1 + \epsilon + x \in P(\bar{h})$; fent el canvi $x \to -x$, veiem que $1 + \epsilon - x \in P(h)$.

Per tant, tenim,

$$1 + \epsilon \pm x = F_\pm(x) + G_\pm(x) h(x),$$

on $F_\pm, G_\pm$ són suma de quadrats, i $\deg F_\pm, \deg G_\pm h$ estan acotats superiorment per

$$\left\lfloor \frac{r}{\epsilon} \left(\frac{\beta}{r\alpha} \right)^{\frac{1}{r}} \right\rfloor + \deg h \leq \frac{r}{\epsilon} \left(\frac{\beta}{r\alpha} \right)^{\frac{1}{r}} + \deg h.$$

Demostració: Volem veure que $F(x) \geq 0$ per tot $x \in \mathbb{R}$ i notem que $1 + \epsilon + x \geq 0$ si $x \geq -1 - \epsilon$ i $-Ax^{2m} h(x) \geq 0$ si $|x| \geq 1$. Per tant només hem d'observar què passa quan $x \in (-\infty, -1 - \epsilon) \cup (-1, 1)$.

Per parts, podem començar escrivint $x \in (-\infty, -1-\epsilon)$ com $x = -1-\epsilon-y$, amb $y > 0$. Per tant podem escriure $F(x)$ com

$$F(x) = -y - A(1 + \epsilon + y)^{2m} (1 - (1 + \epsilon + y)^2)^r q(-1 - \epsilon - y) \geq 0.$$

Sabem que s'ha de complir que $(1+\epsilon+y)^{2m} \geq 1$ i $q(-1-\epsilon-y) \geq \alpha$ per hipòtesi, i com que r és senar, utilitzant igualtats notables trobem

$$(1-(1+\epsilon+y)^2)^r = (2+\epsilon+y)^r(\epsilon+y)^r \geq 2^r(r\epsilon^{r-1}y).$$

La desigualtat ve donada del fet que $\epsilon, y \geq 0$ i d'agafar un terme de l'expansió binomial de $(\epsilon+y)^r$ i un de l'expansió de $(2+\epsilon+y)^r$. Amb això en tenim suficient com per veure

$$-y + A2^r r\epsilon^{r-1}y\alpha \geq y(A2^r r\epsilon^{r-1}\alpha - 1) \geq 0,$$

que és cert per definició de A.

Ara seguim veient el cas $x \in (-1,1)$. Fent ús del càlcul veiem que si a i b són positius i $0 \leq t \leq 1$, llavors tenim $t^a(1-t)^b \leq \frac{a^a b^b}{(a+b)^{a+b}}$. Fent servir aquesta desigualtat juntament amb $t = x^2$, trobem

$$F(x) = 1+\epsilon+x-A(x^2)^m(1-x^2)^r q(x) \geq \epsilon - A\frac{m^m r^r}{(m+r)^{m+r}}\beta.$$

Però tenim $\frac{m}{m+r} < 1$, i com que $m+r > \frac{r}{2\epsilon}\left(\frac{\beta}{r\alpha}\right)^{1/r}$, llavors ens queda

$$\epsilon - A\frac{m^m r^r}{(m+r)^{m+r}}\beta > \epsilon - A\beta\left(\frac{r}{m+r}\right)^r = \epsilon\left(1-\frac{\beta}{r\alpha}\left(\frac{r}{2\epsilon(m+r)}\right)^r\right) \geq 0.$$

□

Un cop demostrat aquest teorema, ens és fàcil trobar l'acotació dels graus del teorema següent.

Teorema 3.14. *([2], Corol·lari 8) Suposem que $g(x) = (1-x^2)^r h(x)$ amb r senar, tal que $0 \leq h(x) \leq v$ per a $|x| \leq 1$ i que $h(x) \geq w > 0$ per a $|x| \geq 1$. Suposem també $f \in \mathbb{R}[x]$ amb grau de $f = d$ estrictament positiu en l'interval tancat $[-1,1]$ i que té s arrels reals u_j, amb $|u_j| \geq u > 1$. Llavors, existeixen polinomis $\sigma_1, \sigma_2 \in \sum \mathbb{R}[x]^2$, tals que*

$$f = \sigma_1 + \sigma_2 g,$$

on els graus de les σ_i estan acotats superiorment per

$$s\left(\frac{r}{2(u-1)}\left(\frac{v}{w}\right)^{1/r} + \textit{grau } g\right) + d - s.$$

Demostració: Factoritzem f en factors lineals de $\mathbb{R}[x]$ de la forma $x-u_j$ i en factors irreductibles quadràtics $q_k \in \sum \mathbb{R}[x]^2$. Per tant, tenim que $|u_j| \geq u > 1$. Observem que $\pm(x-u_j) = |u_j| - \operatorname{sgn}(u_j)x$, amb el signe escollit per tal que sigui positiu en $[-1,1]$; llavors,

$$f(x) = \prod_{j=1}^{s}(|u_j| - \operatorname{sgn}(u_j)x)\prod_{k=1}^{\frac{d-s}{2}} q_k(x).$$

Fem servir l'observació 3.13 per escriure $|u_j| - \operatorname{sgn}(u_j)x = \sigma_{1j} + h\sigma_{2j}$, que tenen els graus acotats per

$$\frac{r}{(|u_j|-1)}\left(\frac{v}{rw}\right)^{\frac{1}{r}} + \text{grau } g \leq \frac{r}{2(|u_j|-1)}\left(\frac{v}{w}\right)^{\frac{1}{r}} + \text{grau } g \leq \frac{r}{2(u-1)}\left(\frac{v}{w}\right)^{\frac{1}{r}} + \text{grau } g,$$

hem utilitzat $\epsilon = |u_j| - 1$ i el fet que $\left(\frac{1}{r}\right)^{\frac{1}{r}} \geq \frac{1}{2} \implies 2^r \geq r$ per tot r i substituïm a $f(x)$ per a trobar els graus dels multiplicadors i per tant l'acotació.

□

Per una observació en [2] podem veure que es pot generalitzar a tota $S = \{g\}$ que compleixi $K_S = [-1, 1]$. Així queda demostrat aquest cas concret del teorema de Schmüdgen, que ens dona un certificat de positivitat.

4 Subconjunts semialgebraics tancats bàsics de $\mathbb{R}$

En els resultats que hem vist ara, hem trobat que hi ha un mòdul quadràtic saturat associat a un interval tancat de $\mathbb{R}$, sempre que triem el conjunt de generadors correcte. Marshall i Kuhlmann van precisar una mica més. Van observar que per un conjunt semialgebraic bàsic tancat de $\mathbb{R}$ l'afirmació és certa no només pel mòdul quadràtic, sinó també pel preordre. És més, van trobar que el preordre associat P_S estava saturat si S contenia un conjunt concret de de generadors.

4.1 Conjunt natural de generadors

Si K és un conjunt semialgebraic tancat bàsic de $\mathbb{R}$, llavors K és una unió finita d'intervals tancats i punts. Per tant, podem definir un conjunt de generadors de K que anomenarem conjunt natural de generadors.

Definició 4.1. *Prenent un conjunt bàsic semialgebraic tancat $K \subseteq \mathbb{R}$. Anomenem conjunt natural de generadors de K a un conjunt finit $S \subseteq \mathbb{R}[x]$ que compleix $K_S = K$ i ve definit de la forma:*

- *Si $K = \emptyset$, llavors $S = \{-1\}$.*
- *Si K té un element tal que és el mínim (l'anomenarem a), llavors $x - a \in S$.*
- *Si K té un element tal que és el màxim (l'anomenarem b), llavors $b - x \in S$.*
- *Si $a, b \in K$ i $(a, b) \cap K = \emptyset$, llavors $(x - a)(x - b) \in S$.*

S no conté més elements que aquests.

Observem que per $K = [-1, 1]$, el conjunt natural de generadors és $\{1 - x, 1 + x\}$ i no $\{1 - x^2\}$. Però no és cap problema ja que hem vist al exemple 2.12 que tenen el mateix preordre.

Lema 4.2. *[1] Siguin $a, b, c, d \in \mathbb{R}$ que compleixen $a \neq b$ i $(c, d) \subseteq (a, b)$, és a dir $a \leq c \leq d \leq b$. Llavors $(x - c)(x - d)$ està en el preordre generat per $(x - a)(x - b)$.*

Demostració: És suficient demostrar-ho per $a = -1$, $b = 1$ fent ús de canvi de variables. Si assumim $-1 \leq c \leq d \leq 1$, hem de demostrar que existeix un $k \in \mathbb{R}$ positiu tal que

$$h_k := (x - c)(x - d) - k(x^2 - 1)$$

és semidefinit positivament, i ja en tindrem suficient ja que implica que h_k és suma de quadrats.

Per $c + d = 0$, amb $k = 1$ ja ho tenim. Assumim $c + d \neq 0$. Llavors per $k \in (0, 1)$, el mínim de h_k és

$$m(k) := cd + k - \frac{1}{1 - k}\left(\frac{c + d}{2}\right)^2.$$

Per tant necessitem un $k \in (0, 1)$ tal que $m(k) \geq 0$. Si prenem

$$k = 1 \pm \frac{c + d}{2},$$

llavors $m(k) = (1 \pm c)(1 \pm d) \geq 0$. Quan $(c+d)/2 \in (0,1)$, prenem $k = 1-(c+d)/2 \in (0,1)$ i quan $(c+d)/2 \in (-1,0)$, prenem $k = 1+(c+d)/2 \in (0,1)$, per tant queda demostrat per tot $c + d \neq 0$.

□

Usarem ara aquest lema per demostrar el següent teorema, que relaciona el conjunt natural de generadors amb un preordre saturat, essencial per a trobar certificats de positivitat, ja que és computacionalment més òptim.

Teorema 4.3. *[1] Suposem que K és un conjunt semialgebraic tancat no buit en $\mathbb{R}$ i S conté el conjunt natural de generadors de K. Llavors per qualsevol $f \in \mathbb{R}[x]$, $f \geq 0$ en K tenim que $f \in P_S$ o, altrament dit, P_S és saturat.*

Demostració: Primer suposem $f \geq 0$ en K i demostrarem que $f \in P_S$ per inducció en el grau de f. Si $\deg f = 0$, llavors $f \in P_S$ clarament. Assumim $\deg f > 0$ i que el teorema és cert per tot $h \in \mathbb{R}[x]$ amb $\deg h < \deg f$. Si f està semidefinit positivament, llavors tenim que f és suma de quadrats i per tant $f \in P_S$. Si f no està semidefinit positivament, llavors existeix alguna constant $c \in \mathbb{R}$ que fa que $f(c) < 0$. $c \notin K$ perquè hem dit que $f \geq 0$ en K, per tant hi ha tres casos possibles: $c < x$ per tot $x \in K$, $c > x$ per tot $x \in K$ o que existeixen a, b tals que $a < c < b$ i $(a,b) \cap K = \emptyset$.

Prenem que es compleix que $c < x$ per tot $x \in K$. Llavors K té un element que és el mínim, l'anomenarem a, i f té la seva arrel més petita en $(c,a]$, l'anomenarem d. Per tant podem expressar f com $f = (x-d)g$ per alguna g. Tenim que $x - a \in S$ i per tant $x - d = (x-a) + (a-d) \in P_S$. Com que $f \geq 0$ en K i $x - d \geq 0$ en K, llavors $g \geq 0$ en K. Tenim per hipòtesi d'inducció que $g \in P_S$ i per tant $f \in P_S$. Per altra banda, si es compleix $c > x$ per tot $x \in K$, llavors K té un element que és el màxim b i f té la seva arrel més gran en $[b,c)$, l'anomenarem d, i fem servir el mateix argument que en el cas anterior. Finalment, si tenim que existeixen a, b tals que $a < c < b$ i $(a,b) \cap K = \emptyset$, llavors f té la seva arrel més gran en $[a,c)$, l'anomenem d, i la seva arrel més petita en $(c,b]$, l'anomenem e. Per tant podem representar f com $f = (x-d)(x-e)g$ amb $g \geq 0$ on K. Per el lema 4.2, tenim que $(x-d)(x-e) \in P_S$ i per hipòtesi d'inducció $g \in P_S$, per tant $f \in P_S$.

□

4.2 Dependència de la compacitat de K_S

4.2.1 Cas on K_S és compacte

Veurem més endavant que quan K_S no és compacte, S conté el conjunt natural de generadors si i només si P_S està saturat. Això no passa en el cas compacte, ja que és possible tenir un preordre saturat sense que S contingui el conjunt natural de generadors. Per demostrar-ho necessitem introduir primer el teorema de Scheiderer.

Recordem que un mòdul quadràtic $M \subset A$ és arquimedià si per tot $f \in A$ existeix un $N \in \mathbb{N}$ tal que $N - f \in M$.

Teorema 4.4. *([8], Teorema de Scheiderer) Si $S \subseteq \mathbb{R}[x]$ és finit i K_S compacte, llavors $M_S = P_S$.*

Demostració: Com que S és finit i K_S compacte, el mòdul quadràtic M_S és arquimedià. Això ho sabem ja que per compacitat, existeix una constant $N > 0$ tal que per

tot $x \in K_S$, tenim que $\sum x_i^2 \leq N$ i per tant $N - \sum x_i^2 \in M_S$.

Per el Positivstellensatz de Putinar ([9] Teorema 4), si M_S és arquimedià, llavors qualsevol polinomi $f \in \mathbb{R}[x]$ estrictament positiu en K_S pertany a M_S, és a dir,

$$f > 0 \text{ en } K_S \quad \Rightarrow \quad f \in M_S.$$

Com que tot element de P_S és no negatiu en K_S, i P_S està generat per sumes de quadrats multiplicades per productes d'elements de S, tenim que tot element de P_S està en M_S. Per tant,

$$P_S \subseteq M_S.$$

Com que per definició tenim $M_S \subseteq P_S$, podem concloure que

$$M_S = P_S.$$

□

Aquest teorema ens és necessari per trobar la saturació del preordre en els conjunts compactes. Però abans de passar al teorema i a la seva demostració que ens dóna aquesta relació, és necessari definir què és l'anell de la sèrie formal de potències en un punt.

Definició 4.5. *Denotem $\mathbb{R}[[x-a]]$ com a l'anell de la sèrie formal de potències en un punt $a \in \mathbb{R}$. Els elements de $\mathbb{R}[[x-a]]$ són les sumes formals*

$$g = b_0 + b_1(x-a) + b_2(x-a)^2 + \cdots, \quad b_i \in \mathbb{R},\ i = 0, 1, \ldots$$

Teorema 4.6. *[10] Suposem $S = \{g_1, \ldots, g_k\}$ amb K_S compacte. Escrivim K_S com a unió disjunta d'intervals $[a_j, b_j], a_j \leq b_j$, per $j = 1, \ldots, r$. Llavors P_S és saturat si i només si es compleixen les següents condicions:*

1. *per cada extrem a_j, existeix un índex i tal que $g_i(a_j) = 0$ i $g_i'(a_j) > 0$.*
2. *per cada extrem b_j, existeix un índex i tal que $g_i(b_j) = 0$ i $g_i'(a_j) < 0$.*

Demostració: Sigui P_c el preordre de $\mathbb{R}[[x-c]]$ generat per S. Prenem l'extrem de l'esquerra a_j i agafem $f = (x - a_j + \epsilon)(x - a_j) = \epsilon(x - a_j) + (x - a_j)^2$, amb $\epsilon > 0$ pròxim al zero. Llavors $f \geq 0$ en K. Si $f \in P_S$, llavors $f \in P_{a_j}$. Com que $x - a_j + \epsilon$ és una unitat i un quadrat en $\mathbb{R}[[x - a_j]]$, això implica que $x - a_j \in P_{a_j}$. Sabent això, com a mínim un g_i ha de tenir una expansió de la forma $g_i = c_0 + c_1(x - a_j) + \cdots + c_d(x - a_j)^d$ amb $c_0 = 0$ i $c_1 > 0$. Com que $c_0 = g_i(a_j)$ i $c_1 = g_i'(a_j)$, això implica $g_i(a_j) = 0$ i $g_i'(a_j) > 0$. Així veiem que si P_S està saturat, llavors es compleix (1). Si fem servir el mateix argument però amb l'extrem dret, veiem que si P_S està saturat, es compleix (2).

Anem a suposar ara que (1) i (2) es compleixen. Per cada extrem esquerra a_j, $x - a_j \in P_{a_j}$ i per cada extrem dret b_j, $-(x - b_j) \in P_{b_j}$. Prenem un polinomi $f \neq 0$ que satisfà $f \geq 0$ en K. Si c és un zero de f i, per tant, un punt interior de K, llavors $f \geq 0$ en algun entorn de c. Per tant f és de la forma $f = t_k(x-c)^k + t_{k+1}(x-c)^{k+1} + \ldots$ on $t_k > 0$ i k és parell, o sigui que f és un quadrat de $\mathbb{R}[[x - c]]$. Per veure $f \in P_S$, per el Teorema 9.2.1 de [10], només hem de veure que per cada j, $f(a_j) = 0 \Rightarrow f \in P_{a_j}$ i $f(b_j) = 0 \Rightarrow f \in P_{b_j}$. Si $f(a_j) = 0$ llavors f es pot escriure com $f = t_k(x - a_j)^k + t_{k+1}(x - a_j)^{k+1} + \ldots$ amb $t_k \neq 0$, $k \geq 1$. Si a_j no és un punt aïllat de K llavors que $f \geq 0$ en K implica que $t_k > 0$. Si k és parell, llavors f és un quadrat de $\mathbb{R}[[x - a_j]]$ i per tant $f \in P_{a_j}$. Si k és senar, llavors $f \in P_{a_j}$ ja que $x - a_j \in P_{a_j}$. Si a_j és un punt aïllat de K, llavors $a_j = b_j$ per tant

també tenim $-(x-b_j) = -(x-a_j) \in P_{a_j}$, per tant $(x-a_j) \subseteq P_{a_j}$. Per tant $f \in P_{a_j}$ també es compleix. Podem fer servir el mateix argument per els extrems drets i queda demostrat.

□

4.2.2 Cas on K_S no és compacte

És natural preguntar-se què passa amb el mòdul quadràtic quan K_S no és compacte. Per aquest cas, tenim el següent teorema que són el Teorema 2.1 i 2.5 de [6].

Teorema 4.7. *Si tenim un subconjunt finit $S \subseteq \mathbb{R}[x]$ tal que K_S no és compacte, denotem com $\tilde{S}$ el conjunt natural de generadors de K_S. Es compleix que*

1. *P_S està saturat (la propietat $(\geq)$ es manté en S) si i només si $(>)$ es manté en S.*
2. *M_S és saturat (la propietat $(\geq)_M$ es manté en S) si i només si la propietat $(>)_M$ es manté en S.*
3. *P_S està saturat si i només si $\tilde{S} \subseteq S$.*
4. *M_S està saturat si i només si $\tilde{S} \subseteq S$ i es compleix que $|\tilde{S}| \leq 1$ o $|\tilde{S}| = 2$ i K_S té un punt aïllat.*

5 Estudi de la positivitat de les corbes

Abans de començar amb la secció de corbes, s'han de definir uns conceptes bàsics necessaris per entendre la secció al complet.

Definició 5.1. *Una corba és una varietat algebraica de dimensió* 1.

Definició 5.2. *Una corba C és reductible si pot ser expressada com a $C = C_1 \cup C_2$ on C_1, C_2 són corbes que compleixen $C_i \neq C$. Si no es pot, llavors C és irreductible.*

Definició 5.3. *Una corba C en $\mathbb{R}^n$ és racional si pot ser parametritzada amb funcions racionals d'una sola variable, o sigui, si existeixen funcions racionals $a_1(t), \ldots, a_n(t) \in \mathbb{R}(t)$ tal que per tot $x = (x_1, \ldots, x_n) \in C$ excepte una quantitat finita de punts, existeix $t \in \mathbb{R}$ tal que $a_i(t) = x_i$ per tota i.*

Exemple 5.4. La parametrització més coneguda és potser la del cercle unitat. El cercle unitat $\{1 - x^2 - y^2 = 0\}$ es pot parametritzar com

$$x(t) = \frac{1 - t^2}{1 + t^2}, \qquad y(t) = \frac{2t}{1 - t^2}.$$

Definició 5.5. *Anomenem P punt singular d'una corba C a un punt que compleix $T_P(C) \geq 2$, és a dir, un punt tal que l'espai tangent a la corba no està definit de forma regular en P. Un punt d'una corba que no és singular s'anomena punt regular.*

Definició 5.6. *Es diu que una corba C és no singular si tots els seus punts són regulars.*

Definició 5.7. *Anomenem bucle en una corba C a un camí tal que el seu punt inicial i el seu punt final són els mateixos.*

Definició 5.8. *Sigui C una corba, escrivim $C(\mathbb{R})$ com el conjunt de punts reals de la corba.*

Definició 5.9. *Una corba C s'anomena virtualment compacte si existeix una funció no constant acotada en C, és a dir, $h \in \mathbb{R}[x, y]$ tal que existeix $N \in \mathbb{N}$ on $|h(x, y)| \leq N$ per a tot $(x, y) \in C$, i $\bar{h} \in \mathbb{R}[C]$ no és una funció constant.*

Exemple 5.10. Tenim per definició que tota corba compacte és virtualment compacte.

Un exemple de corba virtualment compacte que no és compacte podria ser $C = \{x^3 + xy^2 + 1 = 0\}$. Podem veure que per tot $(x, y) \in C$, $-1 \leq x < 0$ per tant $f(x, y) = x$ està acotada i $\bar{f}$ no és constant.

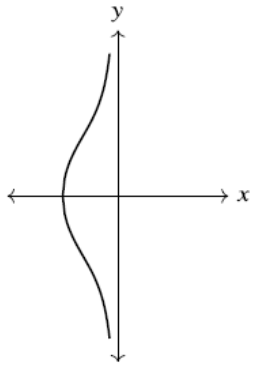

Figura 1: $\{x^3 + xy^2 + 1 = 0\}$

Definició 5.11. *Si tenim C una corba plana, escriurem com a $\mathbb{R}[C]$ l'anell de coordenades que conté el conjunt d'elements $f+\langle p\rangle$ on $\langle p\rangle$ és l'ideal principal generat per p i $f \in \mathbb{R}[x,y]$. Escriurem com a $\bar{f}$ l'element $f + \langle p\rangle$.*

5.1 Corbes en el pla

En aquesta secció, discutirem la positivitat de les corbes. Sigui V una varietat lineal i $\mathbb{R}[V] = \mathbb{R}[x]/I$ l'anell de coordenades, considerem que $f + I$ és una suma de quadrats en $\mathbb{R}[V]$ si existeixen $g1, \ldots, g_k \in \mathbb{R}[x]$ i $u \in I$ tals que

$$f = g_1^2 + \cdots + g_k^2 + u, \tag{5.1}$$

i diem que f és definit semipositivament si $f(x) \geq 0$ per tot $x \in V$. Observem que 5.1 és un certificat de positivitat en V. Al llarg d'aquesta secció ens preguntarem si quan f és definit semipositivament, aquest pot ser escrit com una suma de quadrats.

Anomenem una corba plana al conjunt no buit

$$C = \left\{(x,y) \in \mathbb{R}^2 \mid p(x,y) = 0\right\}$$

on $p \in \mathbb{R}[x,y]$. Sempre assumirem que p no té quadrats, o sigui, no existeix $g \in \mathbb{R}[x,y]$ tal que g^2 divideix a p. Per tant, tota corba plana pot ser escrita com a polinomi lliure de quadrats. També assumim que p canvia de signe en $\mathbb{R}^2$ per evitar casos degenerats com $\{x^2 + y^2 = 0\}$.

5.1.1 El cercle unitat

Començarem veient si tot $f \geq 0$ és suma de quadrats en el cercle unitat. Començarem anomenant i demostrant el teorema de Fejér-Riesz, que necessitarem per poder treballar amb polinomis trigonomètrics i tenir una forma simple de trobar quadrats en ells.

Teorema 5.12. *([11] Teorema de Fejér-Riesz)*

Sigui

$$w(e^{i\theta}) = \sum_{j=-n}^{n} c_j e^{ji\theta} \tag{5.2}$$

un polinomi trigonomètric amb coeficients reals, que és no negatiu per a tot nombre real θ. Llavors existeix un polinomi $p(z) = \sum_{j=0}^{n} a_j z^j$

tal que

$$w(e^{i\theta}) = |p(e^{i\theta})|^2. \tag{5.3}$$

A més, el polinomi $p(z)$ es pot escollir de manera que no tingui arrels en $D = \{z \in \mathbb{C} : |z| < 1\}$ i és únic excepte per constants multiplicatives de mòdul 1.

Demostració: Per demostrar aquest teorema hem d'observar que quan els valors d'un polinomi trigonomètric són reals per tot θ real, llavors els coeficients satisfan $c_{-j} = \overline{c_j}$ per a tot j. Hem d'observar també que en

$$w(z) = \sum_{j=-n}^{n} c_j z^j$$

es satisfà $w\left(\frac{1}{z}\right) = \overline{w(z)}$ per a tot z en els complexos. Si $c_{-n} \neq 0$, llavors $q(z) = z^n w(z)$ és un polinomi de grau $2n$ amb $q(0) \neq 0$. Les arrels de $q(z)$ de mòdul $\neq 1$ venen en parelles recíproques $\alpha, 1/\overline{\alpha}$ amb la mateixa multiplicitat. Les arrels amb mòdul 1 tenen multiplicitat parella. Per tant, usant el teorema fonamental de l'àlgebra, podem factoritzar com

$$w(z) = c \prod_{j=1}^{r} \left[(z - \alpha_j)(z^{-1} - \overline{\alpha_j})\right],$$

on $\alpha_1, \ldots, \alpha_r$ tenen mòdul ≥ 1 i c és una constant positiva. Finalment, obtenim el resultat desitjat amb

$$p(z) = \sqrt{c} \prod_{j=1}^{r} (z - \alpha_j).$$

□

Un cop demostrat el teorema, podem procedir a veure que existeix un certificat de positivitat per a tot polinomi $f \geq 0$ en el cercle unitat. Ho demostrarem passant a polinomis trigonomètrics, i usarem el teorema de Fejér-Riesz per trobar els quadrats pertinents.

Teorema 5.13. *[1] Prenem C el cercle unitat $\{1 - x^2 - y^2 = 0\}$. Llavors tot $f \geq 0$ en C és suma de quadrats. De forma més precisa, si $f \geq 0$ en C, llavors f és la suma de dos quadrats en $\mathbb{R}[C]$.*

Demostració: Prenem un $f \in \mathbb{R}[x, y]$ tal que $f \geq 0$ en C, i considerem $p(\theta) := f(\cos\theta, \sin\theta)$. Escrivim $p(\theta)$ com a un polinomi trigonomètric en els reals i com que $f \geq 0$ en C, tenim que $p(\theta) \geq 0$ per qualsevol θ.

Com que $p(\theta)$ és un polinomi trigonomètric real no negatiu per tot θ, llavors pel Teorema 5.12 sabem que existeix un polinomi en els complexos $q(x) \in \mathbb{C}[x]$ tal que $p(\theta) = |q(e^{i\theta})|^2$. Podem escriure $q(e^{i\theta}) = p_1(\theta) + ip_2(\theta)$, on p_1, p_2 són polinomis trigonomètrics reals i per tant existeixen $f_j \in \mathbb{R}[x, y]$ tals que $p_j(\theta) = f_j(\cos\theta, \sin\theta)$. Per tant tenim

$$f(\cos\theta, \sin\theta) = |q(e^{i\theta})|^2 = p_1(\theta)^2 + p_2(\theta)^2 = f_1(\cos\theta, \sin\theta)^2 + f_2(\cos\theta, \sin\theta)^2.$$

Això és cert per tota θ, per tant $f = f_1^2 + f_2^2$ en $\mathbb{R}[C]$ ja que $f - (f_1^2 + f_2^2) = 0$ en C.

□

5.1.2 Corbes racionals i no racionals

Ara estudiarem la positivitat depenent de si la corba és racional o no en $\mathbb{R}^2$. Començant amb el cas racional, veiem que es pot reduir a estudiar la positivitat en $\mathbb{R}$ i al cercle unitat. Convenientment, ja tenim demostrats els dos casos en aquest treball, ho veiem:

Proposició 5.14. *[12] Suposem que C és una corba racional no-singular. Llavors qualsevol $f \geq 0$ és suma de quadrats en $\mathbb{R}[C]$.*

Demostració: Com que C és una corba racional no singular, existeix una aplicació racional birracional

$$\varphi : \mathbb{P}^1 \dashrightarrow C$$

definida sobre $\mathbb{R}$. Aquesta aplicació indueix un isomorfisme d'anells:

$$\mathbb{R}[C] \cong \mathbb{R}[t] \quad \text{o bé} \quad \mathbb{R}[x,y]/(x^2+y^2-1),$$

depenent de si el morfisme és dominat per la recta real o pel cercle unitat.

És a dir, qualsevol corba racional no singular C és (birracionalment) isomorfa a la recta real $\mathbb{R}$ o al cercle unitat S^1. Per tant, podem reduir la demostració a aquests dos casos coneguts.

El cas on $C = \mathbb{R}$ està demostrat en el Teorema 3.2 i el cas $C = S^1$ altrament escrit com $\mathbb{R}[C] = \mathbb{R}[x,y]/(x^2+y^2-1)$ és el cas del Teorema 5.13

Així doncs, qualsevol corba racional no-singular és birracionalment equivalent a un d'aquests dos casos, i la propietat de ser suma de quadrats es preserva sota isomorfismes d'anells. Per tant, tot element $f \in \mathbb{R}[C]$ tal que $f \geq 0$ a $C(\mathbb{R})$ és suma de quadrats a $\mathbb{R}[C]$.

□

El cas no racional ja és més complicat. Scheiderer ens dóna una demostració. Es basa, principalment, en donar una classificació completa de corbes afins, restringida a les corbes irreductibles, que compleixen que tot $f \geq 0$ es pot escriure com a suma de quadrats a la corba. Amb això i algunes propietats que es poden trobar al llarg de l'article [13] s'acaba demostrant el següent teorema, que ens dóna les condicions per a tenir una representació de suma de quadrats.

Teorema 5.15. *([13], Teorema 4.18) Sigui C una corba irreductible no racional en $\mathbb{R}^2$. Tota $f \geq 0$ és suma de quadrats en C si i només si es compleixen les següents condicions.*

1. *C és virtualment compacte.*
2. *C és, o bé no singular, o bé les úniques singularitats són múltiples punts ordinaris.*

No sobra remarcar que aquest teorema pot ser generalitzat en més que corbes al pla. De fet, es compleix per tota corba en $\mathbb{R}^n$.

5.2 Condicions de positivitat en corbes reductibles a $\mathbb{R}^n$

Un cop vist les corbes irreductibles, queda estudiar què passa amb les reductibles. Plaumann va demostrar a [14] com, sota certes condicions de la corba, tota funció definida semipositivament es pot escriure com a suma de quadrats en l'anell de coordenades de la corba. Aquesta secció està dedicada pràcticament sencera al article [14], ja que tot l'article està enfocat en demostrar aquest primer teorema.

Teorema 5.16. *[1] Considerem C una corba en $\mathbb{R}^n$ i C' la unió de totes les components irreductibles de C que no són virtualment compactes. Llavors, tot $f \geq 0$ en $\mathbb{R}[C]$ és suma de quadrats si i només si les següents condicions es compleixen:*

1. *Totes les singularitats de C són punts ordinaris.*
2. *Tots els punts d'intersecció amb $\mathbb{C}$ de C són reals.*
3. *Tots els components irreductibles de C' són racionals i no-singulars.*
4. *La configuració dels components irreductibles de C' no té cap bucle.*

Per demostrar aquest teorema, necessitem abans múltiples teoremes i propietats de les corbes. Al llarg del que queda del treball, ens dedicarem a citar i demostrar els teoremes necessaris per acabar demostrant el teorema 5.16 i veure així en quines corbes reductibles podem afirmar que tota funció definida semipositivament es pot escriure com a suma de quadrats.

Començarem veient quines condicions han de complir les components irreductibles de la corba, reals i no reals, per a tenir representacions en forma de suma de quadrats per $f \geq 0$.

Lema 5.17. *[12] Sigui A un anell noetherià connectat amb* $\operatorname{Sper} A \neq \emptyset$*, i suposem que A no és real reduït. Llavors existeix $f \in A$ que desapareix idènticament en* $\operatorname{Sper} A$ *però no és suma de quadrats en A.*

Demostració: Per començar observem que $I^2 \neq I$ per qualsevol ideal $(0) \neq I \neq (1)$ de A. De fet, si $I^2 = I$, el Lema de Nakayama ([15], p.8) diu que hi ha un $a \in I$ tal que $(1-a)I = 0$. Per tant $a^2 = a$, i que A estigui connectat implica que o bé $a = 0$, o bé $a = 1$, o sigui que $I = (0)$ o $I = (1)$.

Ara prenem $I = \sqrt[\text{re}]{(0)}$, el nilradical real de A. Per hipòtesi tenim que, $(0) \neq I \neq (1)$, i que $I^2 \neq I$. Qualsevol $f \in I \setminus I^2$ té la propietat que diu el Lema ja que A/I és real reduït.

□

Corol·lari 5.18. *([14], Corol·lari 2.10) Sigui V una R-varietat afí i sigui V_r la unió de totes les components irreductibles reals de V i V_{nr} la unió de les no reals. Llavors $f \geq 0$ és suma de quadrats en $R[V]$ si i només si $V_{nr}(R) = \emptyset$, $V_r \cap V_{nr} = \emptyset$, i $f \geq 0$ és suma de quadrats en $R[V_r]$.*

Demostració: $V_{nr}(R) \neq \emptyset$ o $V_r \cap V_{nr} \neq \emptyset$, les dues impliquen que existeix una component no connectada V' de V tal que V' no és real però $V'(R) \neq \emptyset$, i per tant $f \geq 0$ no és suma de quadrats en $R[V']$ pel lema anterior. Com ja hem vist, això implica que $f \geq 0$ no és suma de quadrats en $R[V]$. Contràriament, si $V_{nr}(R) = \emptyset$ i $V_r \cap V_{nr} = \emptyset$,

llavors tot element de $R[V_{nr}]$ és suma de quadrats en $R[V_{nr}]$ pel Nullstellensatz real i $R[V] \cong R[V_r] \times R[V_{nr}]$, per tant que $f \geq 0$ sigui suma de quadrats en $R[V_r]$ és suficient i necessari per dir que $f \geq 0$ és suma de quadrats en $R[V]$.

□

Prenem C una corba afí en R que té com a components irreductibles $C_1, \ldots, C_m$. Ara buscarem veure que quan $f \geq 0$ és suma de quadrats en $R[C]$, llavors també ho és en $R[C_1], \ldots, R[C_m]$. Per fer-ho, necessitarem les següents proposicions

Proposició 5.19. *(Scheiderer [13] Corol·lari 4.22) Sigui C un corba finita en R. Si C té un punt singular que no és ordinari múltiple, llavors $f \geq 0$ no és suma de quadrats en $R[C]$.*

Lema 5.20. *([14], Lema 3.2) Sigui C una corba afí en R on tots els punts d'intersecció reals són punts ordinaris múltiples. Considerem $C' \subset C$ una subcorba tancada de C. Llavors tota funció definida semipositivament en C' pot ser estesa a una funció definida semipositivament a C, és a dir, tot element de $R[C']$ és la imatge d'un element definit semipositivament en $R[C]$ en el mapa restringit $R[C] \to R[C']$.*

Demostració: Prenem f una funció definida semipositivament a C', i prenem D com la unió de totes les components irreductibles de C que no estan a C'. Sigui $Z = C' \cap D$ el esquema teòric de la intersecció. Necessitem trobar una funció definida positivament en D que concordi amb f en el subesquema tancat Z. Si Z es basa en r punts reals i s punts no reals, llavors assumir que existeixen punts d'intersecció implica que l'anell de funcions regulars $R[Z]$ de Z és un producte directe

$$R[Z] \cong \underbrace{R \times \cdots \times R}_{r} \times A_1 \times \cdots \times A_s$$

amb $R(\sqrt{-1}) \subset A_i$ per tot $i \in \{1, \ldots, s\}$. Això implica que $\sum A_i^2 = A_i$ per tot i, i com que f només té valors negatius als punts reals de Z, podem veure que la classe de f en $R[Z]$ és una suma de quadrats en $R[Z]$. Per tant pot ser ascendit a una suma de quadrats en $R[D]$ que concretament és definit semipositivament a D.

□

Proposició 5.21. *([14], Proposició 3.3) Sigui C una corba afí a R. Si $f \geq 0$ és suma de quadrats en $R[C]$, llavors també és suma de quadrats en $R[C']$ per tota subcorba C' tancada de C.*

Demostració: Si totes les singularitats de C són múltiples punts ordinaris llavors tota $f \geq 0$ en C' és pot estendre a una funció g definida semipositivament en C pel lema 5.20. Llavors g és suma de quadrats en $R[C]$ per hipòtesi, per tant f és suma de quadrats en $R[C']$. Si C té punts singulars reals que no són ordinaris múltiples llavors les funcions definides semipositivament no són suma de quadrats en $R[C]$ per la proposició 5.19, que ens porta a contradicció.

□

Proposició 5.22. *([14], Proposició 3.4) Sigui C una corba real de R, assumim que C té almenys un punt d'intersecció no real. Llavors les funcions definides positivament no són sumes de quadrats en $R[C]$.*

Demostració: Sigui C_1 i C_2 dos components irreductibles diferents de C que intersequen en un punt no real. Per la Proposició 5.21, és suficient veure que $f \geq 0$ no és suma de quadrats en $R[C_1 \cup C_2]$. Per tant, podem assumir $C = C_1 \cup C_2$.

Sigui $I_j = I_{R[C]}(C_j)$ l'ideal d'anul·lació de C_j dins de $R[C]$ $(j = 1, 2)$, i prenem Z com el subesquema tancat de C_1 determinat per l'ideal $J = (I_1 + I_2)/I_1$ de $R[C_1] = R[C]/I_1$, és a dir, Z és la intersecció teòrica esquemàtica de C_1 i C_2 dins de C_1. Escrivim $Z = S \cup T$ on S i T són subesquemes tancats de C tals que S està recolzat per punts reals i T per no reals. Sigui $I_S = I_{R[C_1]}(S)$ i $I_T = I_{R[C_1]}(T)$ els ideals d'anul·lació de S i T en $R[C_1]$, tals que $J = I_S \cap I_T$. Com que T és no buit per hipòtesi, tenim que $(0) \subsetneq I_T \subset R[C_1]$. Prenem $A = R[C_1]/I_T^2$, i triem $h \in I_T \setminus I_T^2$. Com que T té recolzament no real, tenim que $\sqrt{-1} = a \in A$,per tant tot element de A és suma de quadrats; concretament, $h + I_T^2$, la classe de h en A, és suma de quadrats en A. Per tant, l'element $(0 + I_S, h + I_T^2) \in (R[C_1]/I_S) \times A \cong R[C_1]/(I_S \cap I_T^2)$ que en conseqüència té una suma de quadrats $f = \sum F_i^2$ que es restringeix a $(0 + I_S, h + I_T^2)$ mòdul $I_S \cap I_T^2$. Com que $h \in I_T$, tenim $f \in J \subset R[C_1]$.

Ara agafem $F \in I_2 \subset R[C]$ tal que $F|_{C_1} = f$. Clarament, F no està definit semipositivament a $C(R)$. Però volem veure que F no pot ser una suma de quadrats en $R[C]$. Si ho fos, tindríem $F = \sum_{i=1}^r F_i^2$, $F_i \in R[C]$, és compliria que $F_i \in I_2$ per tot $i = 1, \ldots, r$, ja que C_2 és real. Això implicaria $f = \sum_{i=1}^r f_i^2$ amb $f_i = F_i|_{C_1}$. Llavors de $F_i \in I_2$ podem concloure que $f_i \in J$ per tot $i = 1, \ldots, r$, ja que $f \in J^2 \subset (I_S \cap I_T^2)$, i això ens porta a una contradicció en la tria de h.

□

Teorema 5.23. *([14], Teorema 3.13) Sigui C una corba afí en R amb components irreductibles $C_1, \ldots, C_m$, i assumim que $B(C_i) = R$ per tot $i = 1, \ldots, m$. Llavors $f \geq 0$ és suma de quadrats en $R[C]$ si i només si es compleixen les següents condicions:*

1. *Tot C_i és isomorf a subcorbes obertes de $\mathbb{A}^1_R$.*
2. *Tots els punts d'intersecció de C són múltiples punts ordinaris reals.*
3. *La configuració de C no té cap bucle.*

Necessitaríem escriure pràcticament la resta de l'article [14] per poder demostrar aquest teorema, així que no ho demostrarem explícitament. De totes maneres, aquest teorema és vital per la demostració del 5.16, ja que ens que les condicions (3) i (4) existeixen i són necessàries.

Lema 5.24. *([14], Lema 1.4) Si V és la unió de dues subvarietats tancades V_1, V_2 que intersequen en finits múltiples punts $P_1, \ldots, P_r$, llavors la intersecció de V_1 amb V_2 és transversal si i només si el homeomorfisme diagonal*

$$R[V] \to \{(f, g) \in R[V_1] \times R[V_2] \,|\, \forall i \in \{1, \ldots, r\} : f(P_i) = g(P_i)\}$$

donat per $f \mapsto (f|_{V_1}, f|_{V_2})$ és un isomorfisme.

Demostració: Sigui φ el mapa $R[V] \to R[V_1] \times R[V_2]$ donat per $f \mapsto (f|_{V_1}, f|_{V_2})$. Tenim $\mathcal{I}_{V_1} \cap \mathcal{I}_{V_2} = (0)$, ja que V és la unió de V_1 i V_2, per tant φ és injectiva. La imatge de φ consisteix en tots els elements $(f|_{V_1}, g|_{V_2}) \in R[V_1] \times R[V_2]$, $f, g \in R[V]$, tals que $f - g \in \mathcal{I}_{V_1} + \mathcal{I}_{V_2}$.

Per altra banda, $(f,g) \in R[V_1] \times R[V_2]$ satisfà que $f(P_i) = g(P_i)$ per tot $i \in \{1,\dots,r\}$ si i només si $f - g \in \bigcap_{i=1}^r \mathfrak{m}_{P_i}$. Per tant, la imatge de φ té la forma desitjada si i només si $\mathcal{I}_{V_1} + \mathcal{I}_{V_2} = \bigcap_{i=1}^r \mathfrak{m}_{P_i}$, per tant, l'afirmació inicial és certa.

□

Lema 5.25. *([14], Lema 1.6) Per qualsevol cos K i qualsevol $n \geq 1$, existeix un isomorfisme*

$$K[[x_1,\dots,x_n]]/(x_ix_j \mid 1 \leq i < j \leq n) \cong \{(f_1,\dots,f_n) \in K[[t_1]] \times \cdots \times K[[t_n]] \mid f_1(0) = \cdots = f_n(0)\}.$$

donat pel mapa $\varphi\colon K[[x_1,\dots,x_n]]/(x_ix_j \mid i,j) \to \prod_i K[[t_i]]$ que envia la classe de $f \in K[[x_1,\dots,x_n]]$ a

$$(f(t_1,0,\dots,0),\ f(0,t_2,0,\dots,0),\ \dots,\ f(0,\dots,0,t_n)).$$

Demostració: No és difícil veure que φ està ben definida i és injectiva. Per veure que la imatge és aquesta, prenem $(f_1,\dots,f_n)$ un element de la part de la dreta tal que $f_1(0) = \cdots = f_n(0)$. Llavors

$$\varphi(f_1(x_1) + \cdots + f_n(x_n) - (n-1)f_1(0)) = (f_1,\dots,f_n).$$

□

Un cop vistos aquests senzills lemes, els utilitzarem per trobar condicions i relacions entre subcorbes mitjançant isomorfismes i homeomorfismes amb les interseccions. Més tard ho necessitarem a la demostració principal, ja que mirem què passa en les unions i interseccions de les components irreductibles de la corba.

Proposició 5.26. *([14], Proposició 2.7) Sigui V una $\mathbb{R}$ varietat afí, i assumim que V és la unió de dos subvarietats tancades V_1 i V_2 amb les següents propietats:*

1. *tota $f \geq 0$ en $\mathbb{R}[V_1]$ és suma de quadrats.*
2. *$V_1(\mathbb{R})$ és compacte, o V_1 és una corba amb $V_1(\mathbb{R})$ virtualment compacte.*
3. *La intersecció de V_1 i V_2 és finita i transversal.*
4. *Tots els punts de $V_1 \cap V_2$ són reals.*

Llavors tota funció definida semipositiva $f \in \mathbb{R}[V]$ tal que $f|_{V_2}$ és suma de quadrats en $\mathbb{R}[V_2]$ també és suma de quadrats en $\mathbb{R}[V]$.

Demostració: Escrivim $V_1 \cap V_2 = \{P_1,\dots,P_r\} \subset V(\mathbb{R})$, $r \geq 0$. Fent servir el Lema 5.24, podem identificar $\mathbb{R}[V]$ amb el subanell $\mathbb{R}[V_1] \times \mathbb{R}[V_2]$ que consisteix en totes les parelles (f,g) tals que $f(P_i) = g(P_i)$ per tot $i = 1,\dots,r$. Sigui $F \in \mathbb{R}[V]$ no negatiu en $V(\mathbb{R})$ tal que $g = F|_{V_2} = g_1^2 + \cdots + g_m^2$ per algun $m \geq 1$, $g_1,\dots,g_m \in \mathbb{R}[V_2]$.

Per el Lema aplicat a $a_j^{(i)} = g_j(P_i)$, existeix $n \geq m$ i elements $f_1,\dots,f_n \in \mathbb{R}[V_1]$ tals que $f = F|_{V_1} = \sum_{j=1}^n f_j^2$, $f_j(P_i) = g_j(P_i)$ per tot $j \leq m$, i $f_j(P_i) = 0$ per tot $j > m$ $(i = 1,\dots,r)$. Per tant tenim que $F_j = (f_j, g_j)$ per $j = 1,\dots,m$ i $F_j = (f_j, 0)$ per $j = m+1,\dots,n$ són elements de $\mathbb{R}[V]$, i per tant $F = (f,g) = \sum_{j=1}^n F_j^2$.

□

Corol·lari 5.27. *([14], Corol·lari 1.7) Sigui C una corba amb components irreductibles $C_1, \ldots, C_m$ sobre un cos $\mathbb{F}$. Assumim que totes les singularitats de $C_1, \ldots, C_m$ són múltiples punts ordinaris. Les següents afirmacions són equivalents:*

1. *Totes les singularitats de C són múltiples punts ordinaris.*
2. *Les subcorbes tancades C_i i $C_i' = \bigcup_{j \neq i} C_j$ intersequen transversalment per cada $i = 1, \ldots, m$.*
3. *L'homeomorfisme diagonal $\mathbb{F}[C] \to \prod_{i=1}^m \mathbb{F}[C_i]$ donat per $f \mapsto (f|_{C_i})_{i=1,\ldots,m}$ indueix un isomorfisme entre $\mathbb{F}[C]$ i*

$$\left\{ (f_i) \in \prod_i \mathbb{F}[C_i] \mid f_i(P) = f_j(P) \ \forall P \in C_i \cap C_j,\ i, j = 1, \ldots, m \right\}$$

on $C_i \cap C_j$ és la intersecció usual de conjunts.

Demostració: La equivalència de (2) i (3) és immediata pel Lema 5.24. Assumim que (1) es compleix i escrivim φ per l'homeomorfisme diagonal $\mathbb{F}[C] \to \prod_{i=1}^m \mathbb{F}[C_i]$. Per qualsevol punt tancat $P \in C$, considerem el mapa induït $\varphi_P : \widehat{\mathcal{O}}_{C,P} \to \prod_i \widehat{\mathcal{O}}_{C_i,P}$ en anells locals complets (notem que $\widehat{\mathcal{O}}_{C_i,P} = 0$ si $P \notin C_i$). Com que P és un punt ordinari múltiple, tenim que pel Lema 5.25, φ_P és un isomorfisme. Per tant φ és un isomorfisme després de ser completat respecte qualsevol ideal maximal de $\mathbb{F}[C]$, per tant és un isomorfisme.

Per altra banda, si (3) es compleix i $P \in C$ és algun punt tancat, llavors P és un punt ordinari múltiple en cada component irreductible de C passant per P per suposició, per tant pel Lema 5.25, P ha de ser un punt ordinari múltiple de C.

□

Finalment, l'últim teorema que veurem abans de la demostració del teorema principal ens dóna condicions per a que corbes virtualment compactes tinguin representacions en forma de sumes de quadrats per $f \geq 0$. Això ho necessitarem cap al final de la demostració, on veurem que la unió de les components irreductibles és virtualment compacte, per tant podem aplicar el teorema.

Teorema 5.28. *([14], Teorema 3.7) Sigui C una corba real afí sobre $\mathbb{R}$ tal que $C(\mathbb{R})$ és virtualment compacte. Llavors $f \geq 0$ és suma de quadrats en $\mathbb{R}[C]$ si i només si les següents condicions es satisfan:*

1. *Tots els punts reals de C són múltiples punts ordinaris simples.*
2. *Tots els punts d'intersecció de C són reals.*

Demostració: Podem veure que (1) i (2) són suficients: Siguin $C_1, \ldots, C_m$ les components irreductibles de C. pel Corol·lari 5.27 tenim

$$\mathbb{R}[C] \simeq \left\{ (f_i) \in \prod_{i=1}^m \mathbb{R}[C_i] \mid f_i(P) = f_j(P) \ \forall P \in C_i \cap C_j,\ 1 \leq i, j \leq m \right\}.$$

Prenem $f = (f_1, \ldots, f_m) \in \mathbb{R}[C]$ una funció definida semipositivament. Un cop redefinida f, podem assumir que té un nombre finit de zeros en $C_1, \ldots, C_l$ i desapareix idènticament $C_{l+1}, \ldots, C_m$ per algun $0 \leq l \leq m$. Prenem $C' = \bigcup_{i=1}^l C_i$. Llavors

$g = f|_{C'}$ és suma de quadrats en $\mathbb{R}[C']$ pel teorema anterior posem $g = \sum g_i^2$, $g_i \in \mathbb{R}[C']$. Per a tot $P \in C' \cap C_j$, $j > l$, tenim $g(P) = f(P) = 0$, i com que P és real per la hipòtesi inicial, tenim que $g_i(P) = 0$ per tot i. Això implica que $f_i = (g_i|_{C_1}, \ldots, g_i|_{C_l}, 0, \ldots, 0)$ és una funció de C, per la descripció inicial de $\mathbb{R}[C]$, i per tant $f = \sum f_i^2$.

Per altra banda, la condició (1) és necessària per la Proposició 5.19 i la condició (2) per la Proposició 5.22.

□

Finalment podem demostrar el teorema 5.16, gràcies a tot el que s'ha demostrat fins ara.

Demostració: Sigui C_r la unió de totes les components irreductibles de C reals i C_{nr} la unió de les no reals. La condició (1) implica que $C_{nr}(\mathbb{R}) = \emptyset$ i la condició (2) implica que $C_r \cap C_{nr} = \emptyset$, per tant, si (1)–(4) es satisfan, que una funció $f \geq 0$ sigui suma de quadrats en $\mathbb{R}[C]$ és equivalent a que $f \geq 0$ sigui suma de quadrats en $\mathbb{R}[C_r]$ pel Corol·lari 5.18. Contràriament, si $f \geq 0$ és suma de quadrats en $\mathbb{R}[C]$, llavors $C_{nr}(\mathbb{R}) = \emptyset$ i $C_r \cap C_{nr} = \emptyset$ es compleixen pel Corol·lari 5.18, així que (1)–(4) es compleixen per C si i només si es compleixen per C_r. Per tant, podem assumir que $C = C_r$, és a dir, C és real.

Tenim que (1) és necessari que passi per la proposició 5.19, també és necessari (2) per la 5.22, i la (3) i la (4) és necessari que es compleixin pel Teorema 5.23. Per comprovar l'altre implicació, assumim que (1)–(4) es satisfan. Prenem C'' com la unió de totes les components irreductibles C_i de C tals que $B(C_i) \neq \mathbb{R}$. Llavors $C''(\mathbb{R})$ és virtualment compacte, per tant $f \geq 0$ és suma de quadrats en $\mathbb{R}[C'']$ pel Teorema 5.28. Addicionalment, $f \geq 0$ és suma de quadrats en $\mathbb{R}[C']$ pel Teorema 5.23 i per tant és suma de quadrats en $\mathbb{R}[C]$ per la Proposició 5.26.

6 Conclusions

Al llarg d'aquest treball ens hem centrat en trobar certificats de positivitat per a polinomis en $\mathbb{R}$. A través del llibre principal de Victòria Powers, hem revisat obres de matemàtics com Scheiderer, Reznick, Plaumann, Putinar, Pólya i Szegö sobre semipositivitat en polinomis i representacions de certificats de positivitat.

Hem començat veient que tot polinomi definit semipositivament en una variable es pot escriure com una suma de quadrats. Un resultat molt útil demostrat per Motzkin, ja que ens dóna el primer certificat de positivitat, el més senzill, i ens assegura que com a mínim sempre existeix un certificat de positivitat per als polinomis $f \geq 0$ en $\mathbb{R}$.

Seguidament, hem vist com podem estudiar l'existència d'altres certificats de positivitat només mirant els polinomis en els intervals $[-1, 1]$ i $[0, \infty)$ gràcies a uns canvis de variables concrets. Hermite es va preguntar si $f \geq 0$ es podria representar com a

$$f(x) = \sum_{i+j=d} c_{ij}(1-x)^i(1+x)^j,$$

amb tots els seus coeficients positius. Bernstein troba que no, però demostra que si relaxem la condició a $i + d \leq m$ sí que és possible. Addicionalment, troba una cota superior per m.

Amb el treball de Pólya i Szegö veiem els mòduls quadràtics i els preordres, que ens porten a noves representacions de polinomis per a tenir certificats de positivitat. Aquí ens n'adonem de l'importància d'escollir un conjunt correcte de generadors per a trobar els certificats.

Finalment, fem un estudi dels testos de positivitat en corbes. Concretament veiem que per trobar testos de positivitat, per una corba C hem de veure que un polinomi definit semipositivament es pot representar com a una suma de quadrats de polinomis a l'anell de coordenades $R[C]$. Amb els estudis de Scheiderer i Plaumann trobem que en dues variables l'existència de certificats dependrà de la racionalitat de la corba. També hem vist condicions necessàries per a l'existència de certificats en $\mathbb{R}^n$ depenent de si la corba és reductible o no.

A l'inici del semestre no tenia cap coneixement d'aquesta branca de l'àlgebra però un cop vaig començar el treball, li vaig agafar el gust ràpidament. M'ha sorprès veure com una pregunta aparentment simple com "quan es pot expressar una funció positiva com a suma de quadrats?" pot obrir la porta a un camp tan ric i complex. M'ha agradat aprendre sobre un tema nou de forma autodidacta, essent acompanyat pel meu tutor, qui m'ajudava amb qualsevol problema que tenia. Personalment crec que m'ha estat útil fer aquest treball, tant per els coneixements adquirits com per la capacitat de recerca i aprenentatge que he desenvolupat.

Encara que en aquest treball hem explorat gran part dels certificats de positivitat, pràcticament només ho hem estudiat en R. Sembla que sempre puguin existir, però l'extensió dels certificats de positivitat és molt més àmplia del que hem vist, i es complica molt més quan afegeixes més dimensions. No és un camp estudiat en la seva totalitat, hem vist que el llibre principal que s'ha seguit és molt recent i encara queden preguntes per respondre. Jo m'he centrat en la part més teòrica però hi ha una gran part computacional d'aplicar algorismes per trobar les representacions dels certificats de positivitat que no s'ha tocat i que és molt interessant.

Referències

[1] Powers, V. (2021). Certificates of positivity for real polynomials. Springer International Publishing.

[2] Powers, V., Reznick, B.: Polynomials that are positive on an interval. Trans. Amer. Math. Soc. **352**, 4677–4692 (2000).

[3] J. A. de Loera and F. Santos, An effective version of Pólya's theorem on positive definite forms, J. Pure Appl. Alg. **108** (1996), 231–240.

[4] Powers, V., Reznick, B.: *A new bound for Pólya's Theorem with applications to polynomials positive on polyhedra*, Journal of Pure and Applied Algebra, **164** (2001), no. 1-2, 221–229.

[5] G. Pólya and G. Szegö, Problems and Theorems in Analysis II, Springer-Verlag, New York, 1976.

[6] Kuhlmann, S., Marshall, M.: Positivity, sums of squares and the multidimensional moment problem. *Trans. Amer. Math. Soc.* **354**, 4285–4301 (2002)

[7] Reznick, B. (1995). Uniform denominators in Hilbert's seventeenth problem. *Mathematische Zeitschrift*, *220*(1), 75–97.

[8] Scheiderer, C.: Distinguished representations of non-negative polynomials. *J. Algebra* **289**, 558–573 (2005)

[9] Nie, Jiawang, and Markus Schweighofer. "On the complexity of Putinar's Positivstellensatz."Journal of Complexity 23.1 (2007): 135-150.

[10] Marshall, M.: Positive Polynomials and Sums of Squares. Mathematical Surveys and Monographs, vol. 146. American Mathematical Society, Providence (2008)

[11] Abdulmtalib Hussen, Abdelbaset Zeyani, *Fejer-Riesz Theorem and Its Generalization*, International Journal of Scientific and Research Publications, Volume 11, Issue 6, June 2021, ISSN 2250-3153.

[12] Scheiderer, C.: Sums of squares of regular functions on real algebraic varieties. *Trans. Amer. Math. Soc.* **352**, 1029–1069 (2000)

[13] Scheiderer, C.: Sums of squares on real algebraic curves. *Math. Z.* **245**, 725–760 (2003)

[14] Plaumann, D.: Sums of squares on reducible real curves. *Math. Z.* **265**, 777–797 (2010)

[15] H. Matsumura, *Commutative Algebra*, Second edition, Benjamin, Reading, Mass., 1980. MR **82i:13003**.