Localizzazione delle soluzioni di un sistema polinomiale zero-dimensionale in aritmetica esatta

Candidato:
Leonardo Landi

Relatore:
Prof. Giorgio Ottaviani

UNIVERSITÀ
DEGLI STUDI
FIRENZE

22 Luglio 2014

Ideali zero-dimensionali

Problema: Sia dato il sistema nelle incognite x,y:

$$\begin{cases} 9x^2 - 19xy + 8y^2 + 21x - 12y = 0 \\ 3x^2 - 7xy + 2y^2 + 9x - 6 = 0 \end{cases}$$

- Quante sono le soluzioni reali distinte del sistema?
- Quante di esse sono contenute in un dato rettangolo del piano?
- Quale è la loro molteplicità?
- Siamo in grado di approssimarle?

Ideali zero-dimensionali

Dato un sistema di equazioni polinomiali

$$f_1 = f_2 = \cdots = f_m = 0$$

nelle variabili $x_1, \ldots, x_n$ a coefficienti in $\mathbb{C}$, sia I l'ideale di $\mathbb{C}[x_1, \ldots, x_n]$ generato da $f_1, \ldots, f_m$.

Definizione (Ideale zero-dimensionale)

L'ideale I si dice zero-dimensionale se la varietà delle soluzioni

$$\mathcal{V}(I) = \{(a_1 \ldots a_n) \in \mathbb{C}^n \mid f(a_1 \ldots a_n) = 0,\ \forall f \in I\}$$

consiste di un numero finito di punti.

Un criterio di zero-dimensionalità

Teorema

Sia I ideale di $\mathbb{C}[x_1, \ldots, x_n]$. $\mathcal{V}(I)$ è finito $\iff$ $\mathbb{C}[x_1, \ldots, x_n]/I$ ha dimensione finita come spazio vettoriale su $\mathbb{C}$.

Denotiamo con $\mathcal{A}$ l'algebra $\mathbb{C}[x_1, \ldots, x_n]/I$ sul campo $\mathbb{C}$. Una base monomiale $\mathcal{B}$ è data da $\{[x^\alpha] \mid x^\alpha \notin LT(I)\}$.

Esempio: Sia I ideale di $\mathbb{C}[x]$. Una base di $\mathcal{A}$ è $\mathcal{B} = \{[1], [x], \ldots, [x^{d-1}]\}$, dove d è il grado del polinomio generatore di I.

Esempio: $I = (x^3 - xy, y^2 - 1) \subset \mathbb{C}[x, y]$. Una base di $\mathcal{A}$ è data da $\mathcal{B} = \{[1], [x], [x^2], [x^2y], [xy], [y]\}$.

Esempio: $I = (x^3 - xy, y^2 - 1) \subset \mathbb{C}[x, y, z]$ non è zero-dimensionale, infatti una base di $\mathcal{A}$ contiene le classi $[z^i]$ $\forall i \in \mathbb{N}$.

Un criterio di zero-dimensionalità

Teorema

Sia I ideale di $\mathbb{C}[x_1, \ldots, x_n]$. $\mathcal{V}(I)$ è finito $\iff$ $\mathbb{C}[x_1, \ldots, x_n]/I$ ha dimensione finita come spazio vettoriale su $\mathbb{C}$.

Denotiamo con $\mathcal{A}$ l'algebra $\mathbb{C}[x_1, \ldots, x_n]/I$ sul campo $\mathbb{C}$. Una base monomiale $\mathcal{B}$ è data da $\{[x^\alpha] \mid x^\alpha \notin LT(I)\}$.

Esempio: Sia I ideale di $\mathbb{C}[x]$. Una base di $\mathcal{A}$ è $\mathcal{B} = \{[1], [x], \ldots, [x^{d-1}]\}$, dove d è il grado del polinomio generatore di I.

Esempio: $I = (x^3 - xy, y^2 - 1) \subset \mathbb{C}[x, y]$. Una base di $\mathcal{A}$ è data da $\mathcal{B} = \{[1], [x], [x^2], [x^2y], [xy], [y]\}$.

Esempio: $I = (x^3 - xy, y^2 - 1) \subset \mathbb{C}[x, y, z]$ non è zero-dimensionale, infatti una base di $\mathcal{A}$ contiene le classi $[z^i]$ $\forall i \in \mathbb{N}$.

Un criterio di zero-dimensionalità

Teorema

Sia I ideale di $\mathbb{C}[x_1, \ldots, x_n]$. $\mathcal{V}(I)$ è finito $\iff$ $\mathbb{C}[x_1, \ldots, x_n]/I$ ha dimensione finita come spazio vettoriale su $\mathbb{C}$.

Denotiamo con $\mathcal{A}$ l'algebra $\mathbb{C}[x_1, \ldots, x_n]/I$ sul campo $\mathbb{C}$. Una base monomiale $\mathcal{B}$ è data da $\{[x^\alpha] \mid x^\alpha \notin LT(I)\}$.

Esempio: Sia I ideale di $\mathbb{C}[x]$. Una base di $\mathcal{A}$ è $\mathcal{B} = \{[1], [x], \ldots, [x^{d-1}]\}$, dove d è il grado del polinomio generatore di I.

Esempio: $I = (x^3 - xy, y^2 - 1) \subset \mathbb{C}[x, y]$. Una base di $\mathcal{A}$ è data da $\mathcal{B} = \{[1], [x], [x^2], [x^2y], [xy], [y]\}$.

Esempio: $I = (x^3 - xy, y^2 - 1) \subset \mathbb{C}[x, y, z]$ non è zero-dimensionale, infatti una base di $\mathcal{A}$ contiene le classi $[z^i]$ $\forall i \in \mathbb{N}$.

Un criterio di zero-dimensionalità

Teorema

Sia I ideale di $\mathbb{C}[x_1, \ldots, x_n]$. $\mathcal{V}(I)$ è finito $\iff$ $\mathbb{C}[x_1, \ldots, x_n]/I$ ha dimensione finita come spazio vettoriale su $\mathbb{C}$.

Denotiamo con $\mathcal{A}$ l'algebra $\mathbb{C}[x_1, \ldots, x_n]/I$ sul campo $\mathbb{C}$. Una base monomiale $\mathcal{B}$ è data da $\{[x^\alpha] \mid x^\alpha \notin LT(I)\}$.

Esempio: Sia I ideale di $\mathbb{C}[x]$. Una base di $\mathcal{A}$ è $\mathcal{B} = \{[1], [x], \ldots, [x^{d-1}]\}$, dove d è il grado del polinomio generatore di I.

Esempio: $I = (x^3 - xy, y^2 - 1) \subset \mathbb{C}[x, y]$. Una base di $\mathcal{A}$ è data da $\mathcal{B} = \{[1], [x], [x^2], [x^2y], [xy], [y]\}$.

Esempio: $I = (x^3 - xy, y^2 - 1) \subset \mathbb{C}[x, y, z]$ non è zero-dimensionale, infatti una base di $\mathcal{A}$ contiene le classi $[z^i]$ $\forall i \in \mathbb{N}$.

Matrici compagne

Definizione (Matrici compagne)

Le applicazioni

$$M_{x_i} : \mathcal{A} \to \mathcal{A}$$

$$[g] \mapsto [gx_i]$$

indotte dalla moltiplicazione per x_i in $\mathcal{A}$ si dicono matrici compagne di I.

Analogamente M_h denota l'applicazione indotta dalla moltiplicazione per h nell'algebra $\mathcal{A}$.

Le applicazioni di questo tipo soddisfano le consuete proprietà di linearità all'interno di un'algebra.

Soluzioni approssimate

Lemma

Dato un insieme finito di punti $\{p_1, \ldots, p_k\} \subset \mathbb{C}^n$ *e un polinomio* $h \in \mathbb{C}[x_1, \ldots, x_n]$*, i valori* $h(p_i)$ *coincidono con gli autovalori di* M_h*.*

Teorema (Stickelberger)

Sia I *un ideale zero-dimensionale.*

$(\lambda_1, \ldots, \lambda_n) \in \mathcal{V}(I) \iff \exists\, v$ *autovettore comune a tutte le matrici compagne* $M_{x_1}, \ldots, M_{x_n}$ *con autovalori* $\lambda_1, \ldots, \lambda_n$ *rispettivamente.*

Soluzioni approssimate

Lemma

Dato un insieme finito di punti $\{p_1, \ldots, p_k\} \subset \mathbb{C}^n$ *e un polinomio* $h \in \mathbb{C}[x_1, \ldots, x_n]$*, i valori* $h(p_i)$ *coincidono con gli autovalori di* M_h*.*

Teorema (Stickelberger)

Sia I *un ideale zero-dimensionale.*

$(\lambda_1, \ldots, \lambda_n) \in \mathcal{V}(I) \iff \exists\, v$ *autovettore comune a tutte le matrici compagne* $M_{x_1}, \ldots, M_{x_n}$ *con autovalori* $\lambda_1, \ldots, \lambda_n$ *rispettivamente.*

Forma traccia e decomposizione di $\mathcal{A}$

Definizione

Definiamo la forma traccia come l'applicazione bilineare $B_h : \mathcal{A} \times \mathcal{A} \longrightarrow \mathbb{R}$ *tale che* $B_h(a, b) = Tr(M_{hab})$.

Teorema (Lasker-Noether, 1905)

Sia $\mathcal{V}(I) = \{p_1 \dots p_k\}$ *e* $h(x) \in \mathbb{C}[x_1, \dots, x_n]$ *che assume valori distinti sui punti di* $\mathcal{V}(I)$.

Sia $\mathcal{A}_i = \cup_{n \in \mathbb{N}} \ker(M - \lambda_i I)^n$ *l'autospazio generalizzato di* $M_{h(x)}$ *relativo all'autovalore* λ_i, *per* $i = 1 \dots k$.

Allora $\mathcal{A} = \oplus_{i=1}^{k} \mathcal{A}_i$.

Forma traccia e decomposizione di $\mathcal{A}$

Definizione

Definiamo la forma traccia come l'applicazione bilineare $B_h : \mathcal{A} \times \mathcal{A} \longrightarrow \mathbb{R}$ *tale che* $B_h(a, b) = Tr(M_{hab})$.

Teorema (Lasker-Noether, 1905)

Sia $\mathcal{V}(I) = \{p_1 \dots p_k\}$ *e* $h(x) \in \mathbb{C}[x_1, \dots, x_n]$ *che assume valori distinti sui punti di* $\mathcal{V}(I)$.

Sia $\mathcal{A}_i = \cup_{n \in \mathbb{N}} \ker(M - \lambda_i I)^n$ *l'autospazio generalizzato di* $M_{h(x)}$ *relativo all'autovalore* λ_i, *per* $i = 1 \dots k$.

Allora $\mathcal{A} = \oplus_{i=1}^{k} \mathcal{A}_i$.

Il teorema di Sylvester-Hermite

Teorema (Sylvester-Hermite, 1853)

Sia I ideale di $\mathbb{R}[x_1, \ldots, x_n]$ e $h(x) \in \mathbb{R}[x_1, \ldots, x_n]$. Allora:

- *Il numero di punti distinti (reali o complessi) $p \in \mathcal{V}(I)$ tali che $h(p) \neq 0$ è uguale al rango di B_h.*

Inoltre, se $h(x)$ assume valori non nulli sulle coppie di punti complessi coniugati di $\mathcal{V}(I)$:

- *Il numero di punti reali distinti $p \in \mathcal{V}(I)$ tali che $h(p) > 0$ ($h(p) < 0$) è uguale al numero di autovalori positivi (negativi) di B_h meno il numero di autovalori negativi di B_1.*

Numero di radici distinte in un intervallo

Algoritmo (numero di radici reali distinte in un intervallo)

1. *Scelgo il polinomio* $h(x)$*:*

$$h(x) = \begin{cases} -(x-a) & se\ \mathcal{I} = (-\infty, a) \\ x - a & se\ \mathcal{I} = (a, +\infty) \\ -(x-a)(x-b) & se\ \mathcal{I} = (a, b) \end{cases}$$

2. *Calcolo le matrici* B_h *e* B_1 *e le loro segnature*
3. *Il numero di radici reali e distinte di* $f(x)$ *è dato dalla differenza tra il numero di autovalori positivi e negativi di* B_1
4. *Il numero di radici reali e distinte di* $f(x)$ *in* $\mathcal{I}$ *è dato dal numero di autovalori positivi di* B_h *meno il numero di autovalori negativi di* B_1

Calcolo delle molteplicità

Con metodi di bisezione si può sempre ricavare un intervallo (a, b) di ampiezza ϵ $(\forall \epsilon > 0)$ che contenga una sola soluzione.

L'algoritmo per il calcolo della molteplicità agisce su un intervallo contenente una sola soluzione e ne restituisce la relativa molteplicità. Esso si avvale del noto principio:

Lemma

Un polinomio f ha radici distinte $\iff MCD(f, f') = 1$

Nella fattorizzazione di $\tilde{f} = MCD(f, f')$ in irriducibili i termini relativi a radici di molteplicità $m \geq 1$ compaiono con grado minore di 1 rispetto al grado che avevano in f.

Calcolo delle molteplicità

Con metodi di bisezione si può sempre ricavare un intervallo (a, b) di ampiezza ϵ $(\forall \epsilon > 0)$ che contenga una sola soluzione.

L'algoritmo per il calcolo della molteplicità agisce su un intervallo contenente una sola soluzione e ne restituisce la relativa molteplicità. Esso si avvale del noto principio:

Lemma

Un polinomio f ha radici distinte $\iff MCD(f, f') = 1$

Nella fattorizzazione di $\tilde{f} = MCD(f, f')$ in irriducibili i termini relativi a radici di molteplicità $m \geq 1$ compaiono con grado minore di 1 rispetto al grado che avevano in f.

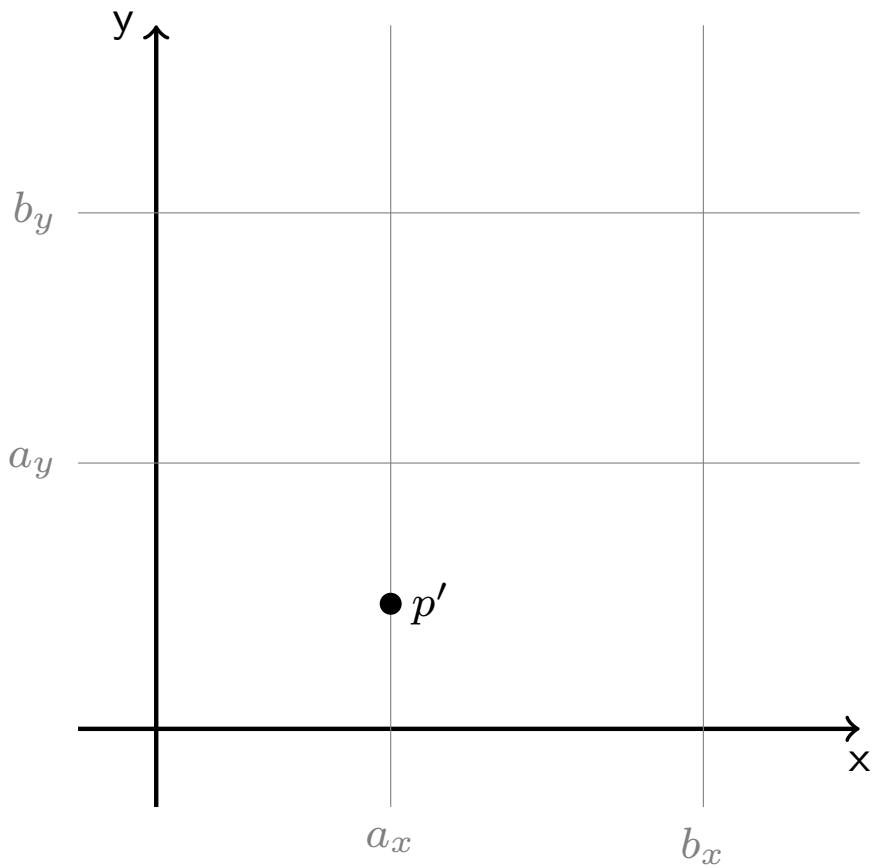
Calcolo delle molteplicità

Algoritmo (calcolo delle molteplicità)

1. *Calcolo* $\tilde{f} = MCD(f, f')$
2. *Se* $\tilde{f} = 1$ *mi fermo, perché* f *ha radici distinte*
3. *Se* $\tilde{f} \neq 1$ *ridefinisco l'algebra* $\tilde{\mathcal{A}} = \mathbb{R}[x]/(\tilde{f})$ *e controllo quante radici di* $\tilde{f}$ *ci sono in* (a, b)
4. *Se c'è ancora una radice riparto dal punto 1 con* $f = \tilde{f}$
5. *Se non ci sono radici mi fermo. Il numero di volte che ho ripetuto la procedura dal passo 1 indica la molteplicità della radice*

Numero di soluzioni distinte in un rettangolo

1. Controlliamo che le rette che individuano il rettangolo non cadano su soluzioni del sistema.

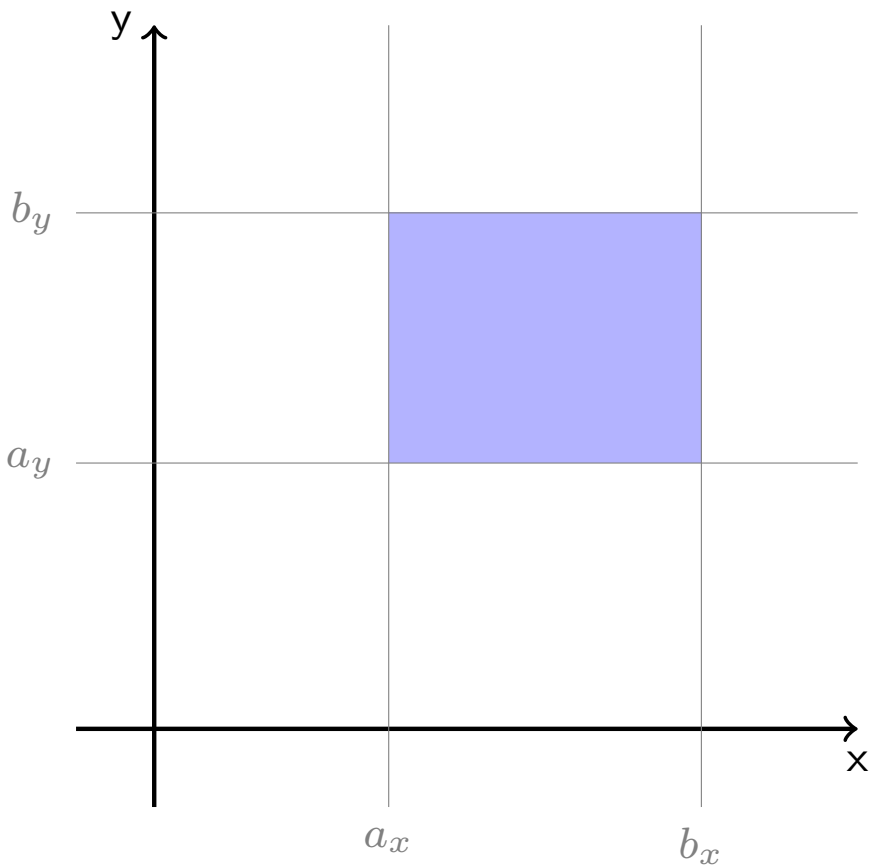


Il conteggio ha efficacia solo se non si verifica questo fenomeno.

Tale controllo può essere fatto sostituendo a_x e b_x nel generatore dell'ideale di eliminazione I_x e a_y e b_y nel generatore dell'ideale di eliminazione I_y.

Numero di soluzioni distinte in un rettangolo

2. Dividiamo il piano in quattro zone e indichiamo il numero delle soluzioni in ogni zona come in figura:



$\alpha =$ numero delle soluzioni nel rettangolo

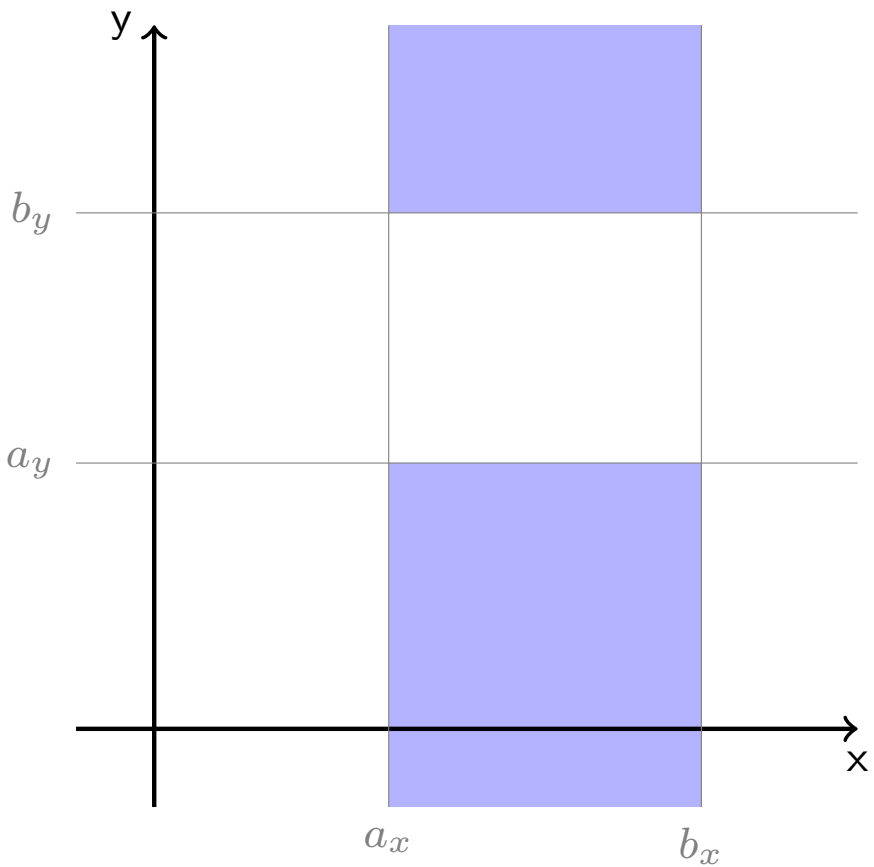
$\beta =$ numero delle soluzioni nelle strisce verticali esterne

$\gamma =$ numero delle soluzioni nelle strisce orizzontali esterne

$\delta =$ numero delle soluzioni nei quattro angoli

Numero di soluzioni distinte in un rettangolo

2 Dividiamo il piano in quattro zone e indichiamo il numero delle soluzioni in ogni zona come in figura:



$\alpha =$ numero delle soluzioni nel rettangolo

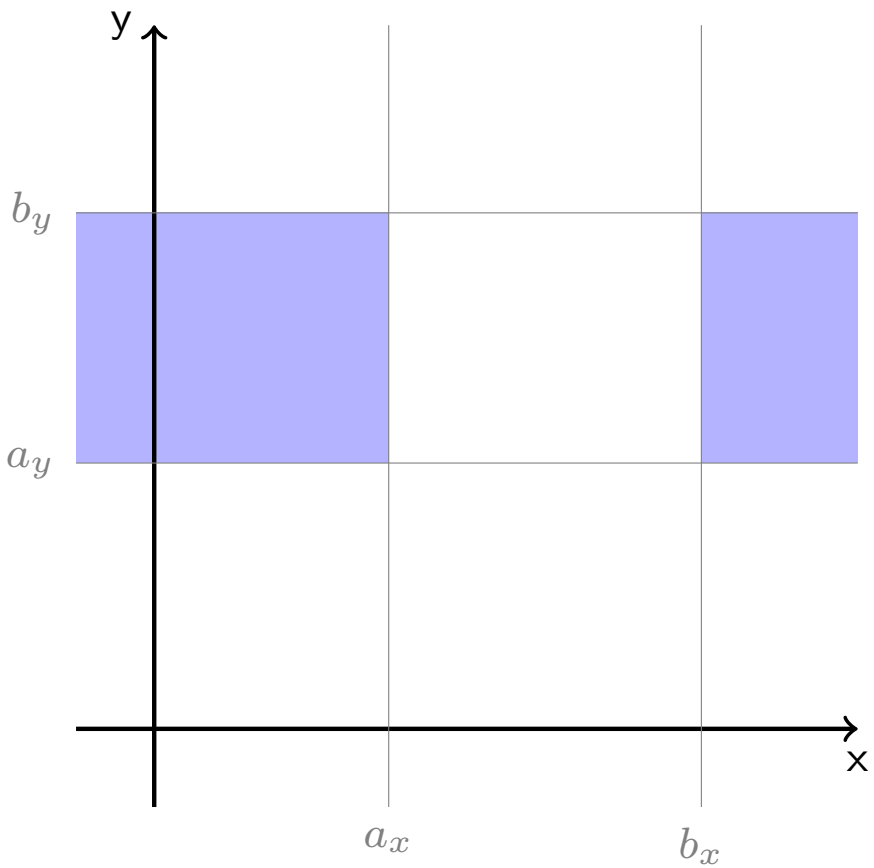
$\beta =$ numero delle soluzioni nelle strisce verticali esterne

$\gamma =$ numero delle soluzioni nelle strisce orizzontali esterne

$\delta =$ numero delle soluzioni nei quattro angoli

Numero di soluzioni distinte in un rettangolo

2 Dividiamo il piano in quattro zone e indichiamo il numero delle soluzioni in ogni zona come in figura:



α = numero delle soluzioni nel rettangolo

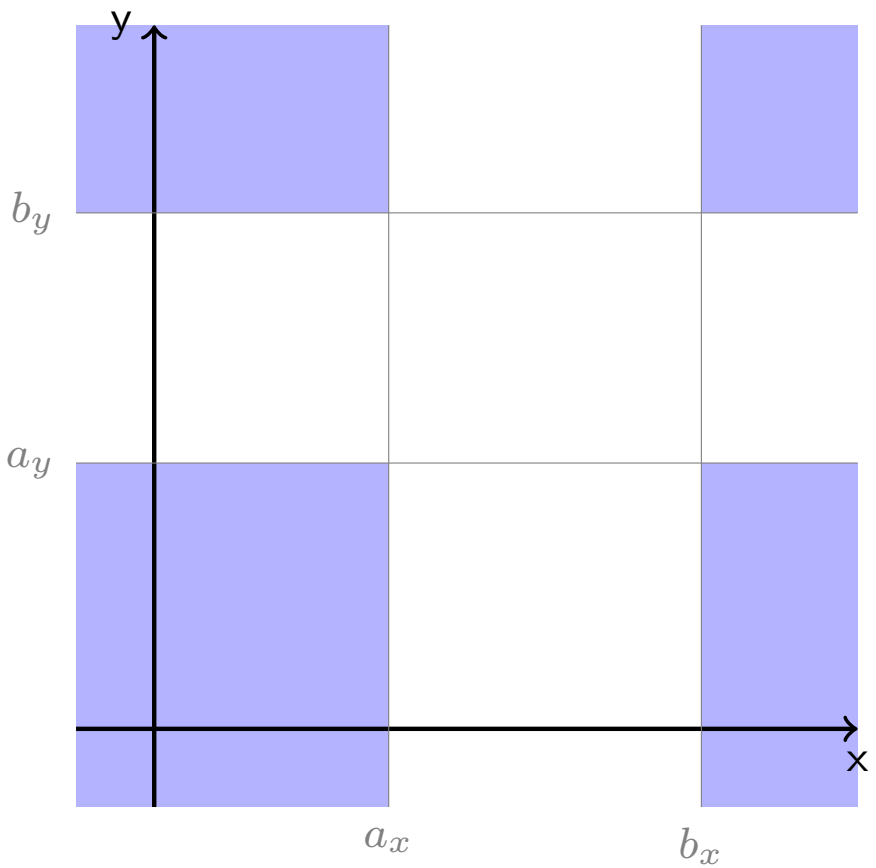
β = numero delle soluzioni nelle strisce verticali esterne

γ = numero delle soluzioni nelle strisce orizzontali esterne

δ = numero delle soluzioni nei quattro angoli

Numero di soluzioni distinte in un rettangolo

2 Dividiamo il piano in quattro zone e indichiamo il numero delle soluzioni in ogni zona come in figura:



$\alpha =$ numero delle soluzioni nel rettangolo

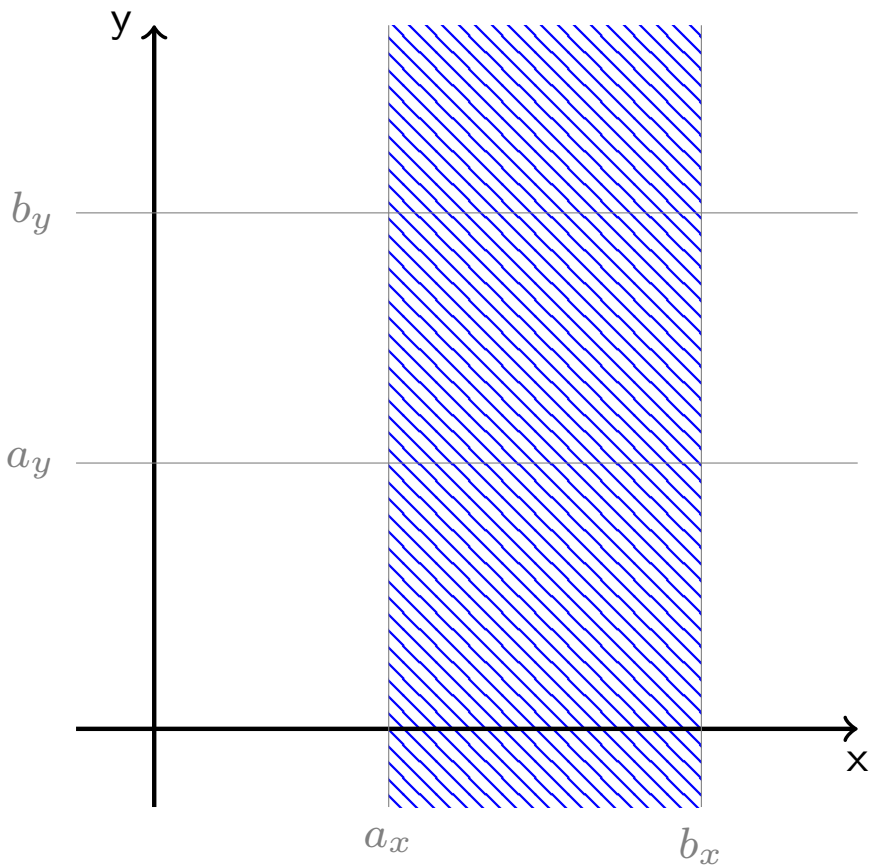
$\beta =$ numero delle soluzioni nelle strisce verticali esterne

$\gamma =$ numero delle soluzioni nelle strisce orizzontali esterne

$\delta =$ numero delle soluzioni nei quattro angoli

Numero di soluzioni distinte in un rettangolo

3 Utilizzando appropriati polinomi $h(x, y)$ calcoliamo il numero di soluzioni nelle quattro zone in figura:



$\alpha + \beta = n_1$ con il polinomio
$-(x - a_x)(x - b_x)$

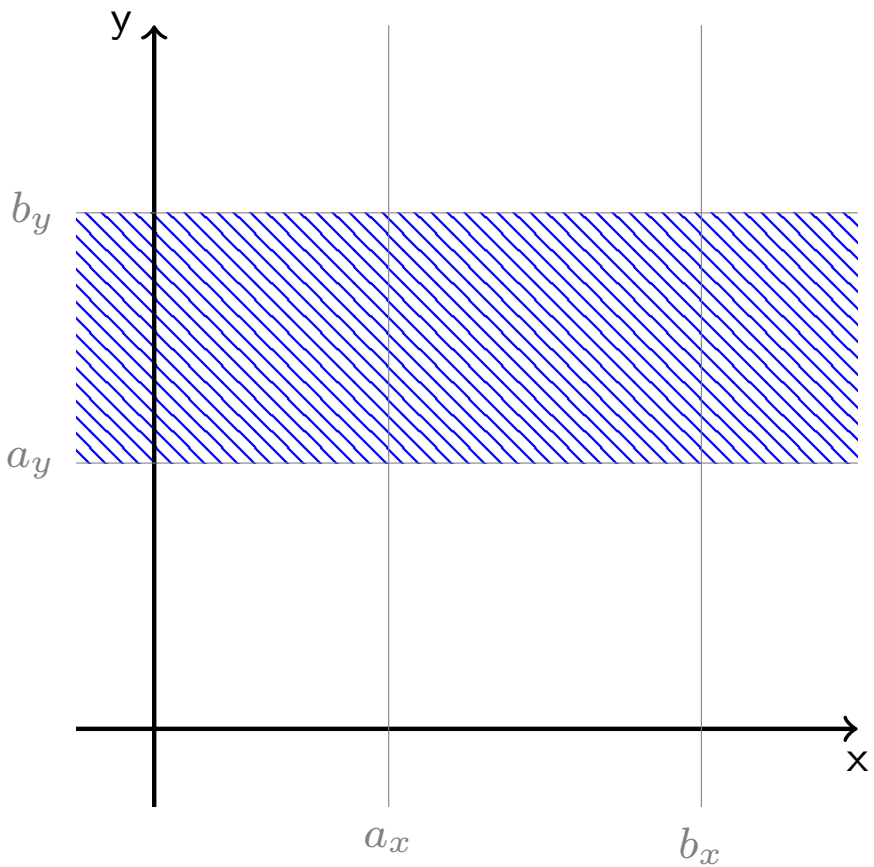
$\alpha + \gamma = n_2$ con il polinomio
$-(y - a_y)(y - b_y)$

$\alpha + \delta = n_3$ con il polinomio
$(x - a_x)(x - b_x)(y - a_y)(y - b_y)$

$\beta + \gamma = n_4$ con il polinomio
$-(x - a_x)(x - b_x)(y - a_y)(y - b_y)$

Numero di soluzioni distinte in un rettangolo

3 Utilizzando appropriati polinomi $h(x, y)$ calcoliamo il numero di soluzioni nelle quattro zone in figura:



$\alpha + \beta = n_1$ con il polinomio
$-(x - a_x)(x - b_x)$

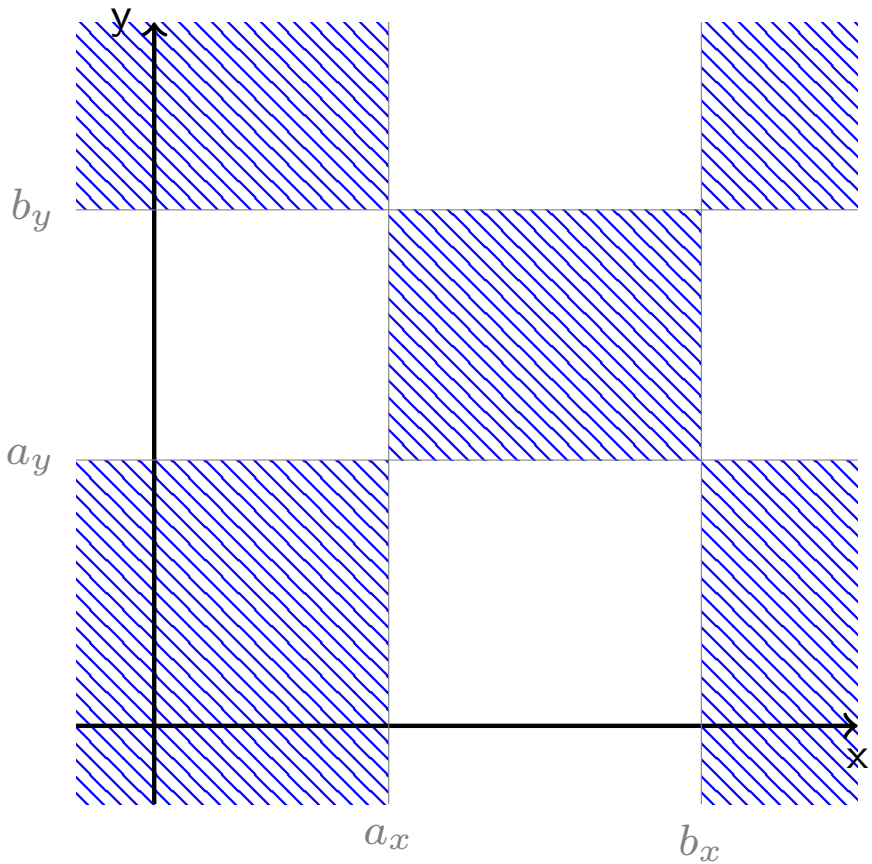
$\alpha + \gamma = n_2$ con il polinomio
$-(y - a_y)(y - b_y)$

$\alpha + \delta = n_3$ con il polinomio
$(x - a_x)(x - b_x)(y - a_y)(y - b_y)$

$\beta + \gamma = n_4$ con il polinomio
$-(x - a_x)(x - b_x)(y - a_y)(y - b_y)$

Numero di soluzioni distinte in un rettangolo

3 Utilizzando appropriati polinomi $h(x, y)$ calcoliamo il numero di soluzioni nelle quattro zone in figura:



$\alpha + \beta = n_1$ con il polinomio
$-(x - a_x)(x - b_x)$

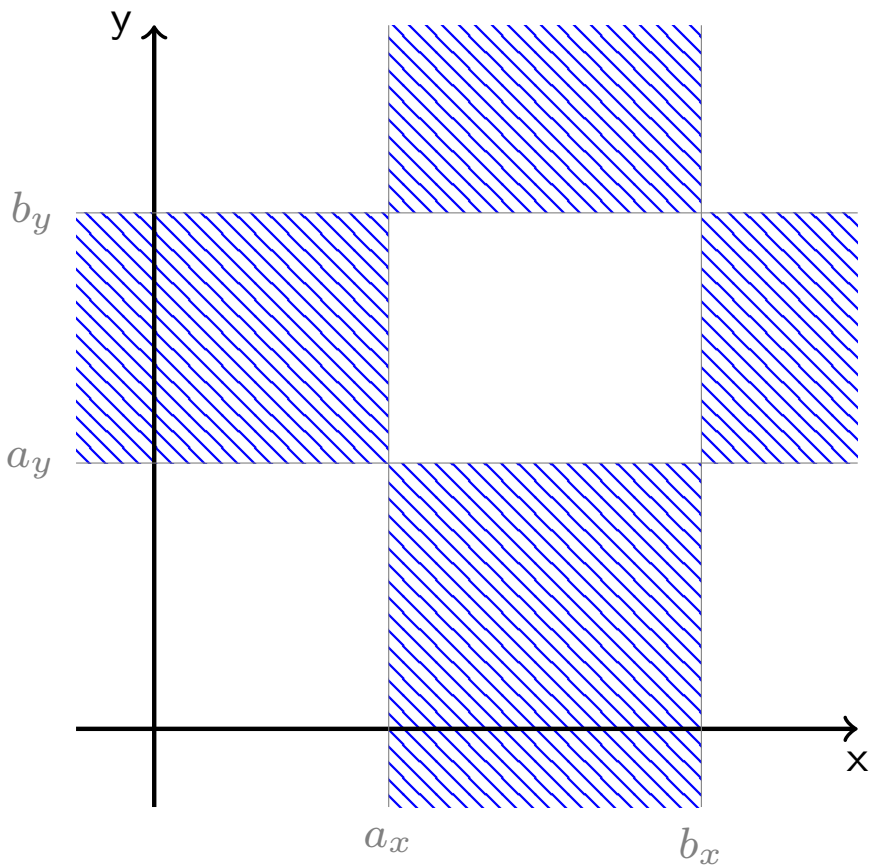
$\alpha + \gamma = n_2$ con il polinomio
$-(y - a_y)(y - b_y)$

$\alpha + \delta = n_3$ con il polinomio
$(x - a_x)(x - b_x)(y - a_y)(y - b_y)$

$\beta + \gamma = n_4$ con il polinomio
$-(x - a_x)(x - b_x)(y - a_y)(y - b_y)$

Numero di soluzioni distinte in un rettangolo

3 Utilizzando appropriati polinomi $h(x, y)$ calcoliamo il numero di soluzioni nelle quattro zone in figura:



$\alpha + \beta = n_1$ con il polinomio
$-(x - a_x)(x - b_x)$

$\alpha + \gamma = n_2$ con il polinomio
$-(y - a_y)(y - b_y)$

$\alpha + \delta = n_3$ con il polinomio
$(x - a_x)(x - b_x)(y - a_y)(y - b_y)$

$\beta + \gamma = n_4$ con il polinomio
$-(x - a_x)(x - b_x)(y - a_y)(y - b_y)$

Numero di soluzioni distinte in un rettangolo

4. Il problema si riduce alla risoluzione del sistema lineare nelle incognite $\alpha, \beta, \gamma, \delta$:

$$\begin{cases} \alpha + \beta & = n_1 \\ \alpha + \gamma & = n_2 \\ \alpha + \delta & = n_3 \\ \beta + \gamma & = n_4 \end{cases}$$

Il valore di α dà il numero cercato di soluzioni nel rettangolo.

Problematiche nel calcolo delle molteplicità

Non è possibile estendere con successo l'algoritmo per il calcolo delle molteplicità da una a due o più variabili.

Una tecnica che ha sempre successo per la soluzione di questo problema ha come punto di partenza l'approssimazione $\overline{p} = (\overline{x}_0, \overline{y}_0)$ dell'unica soluzione $p = (x_0, y_0)$ contenuta in un quadrato di lato 2ϵ, per un certo ϵ.

Un'approssimazione di questo tipo si può sempre trovare con metodi di bisezione, come nel caso di una sola variabile.

Problematiche nel calcolo delle molteplicità

Non è possibile estendere con successo l'algoritmo per il calcolo delle molteplicità da una a due o più variabili.

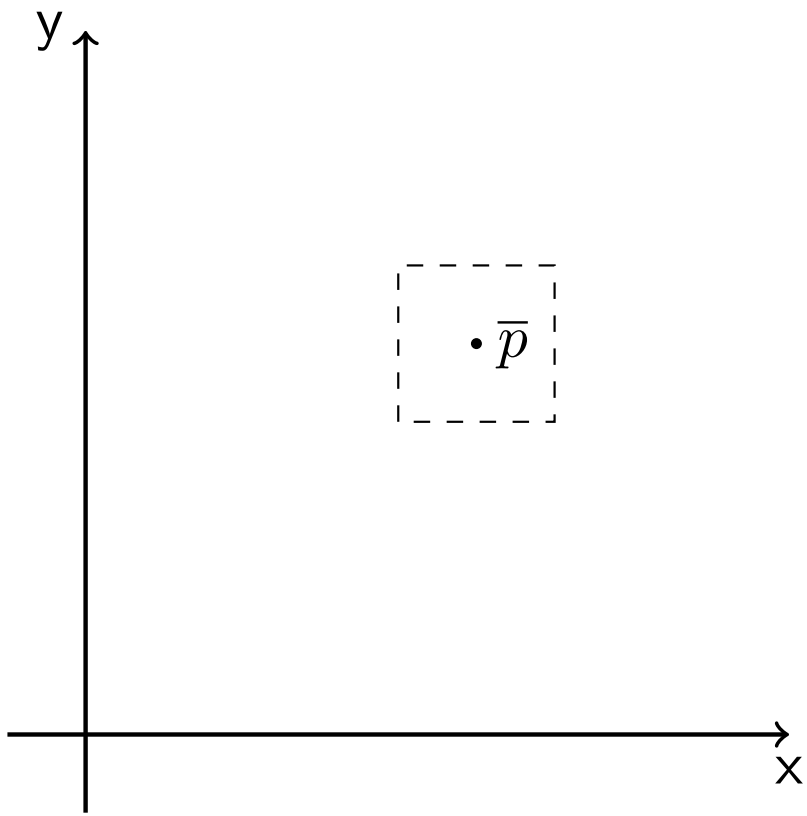
Una tecnica che ha sempre successo per la soluzione di questo problema ha come punto di partenza l'approssimazione $\overline{p} = (\overline{x}_0, \overline{y}_0)$ dell'unica soluzione $p = (x_0, y_0)$ contenuta in un quadrato di lato 2ϵ, per un certo ϵ.

Un'approssimazione di questo tipo si può sempre trovare con metodi di bisezione, come nel caso di una sola variabile.

Calcolo delle molteplicità: una tecnica di risoluzione

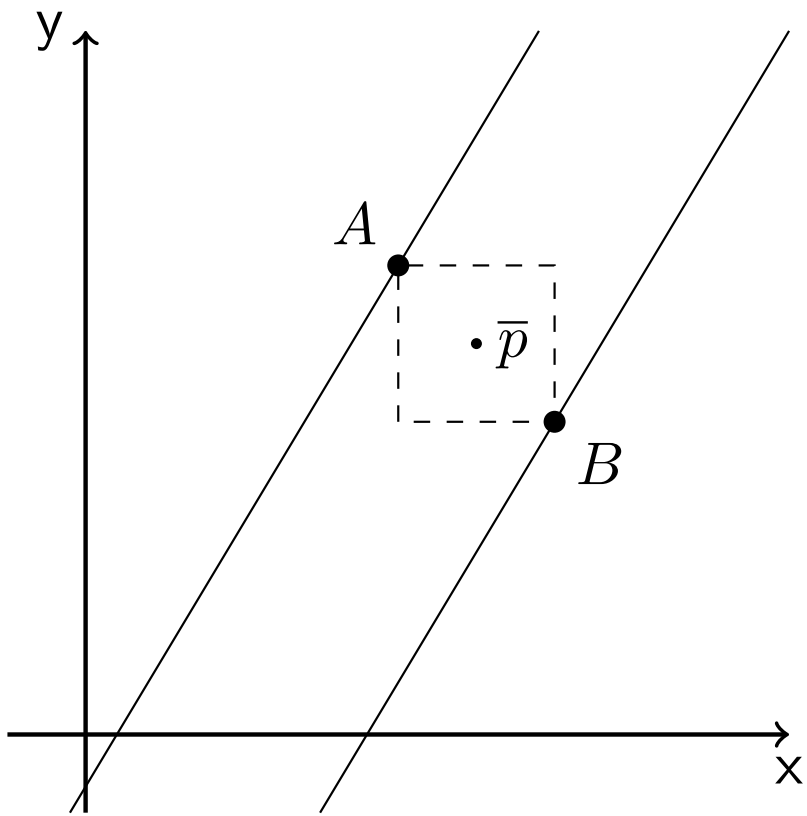
1. Determino l'approssimazione $\overline{p}$ con livello di precisione ϵ.

   La soluzione reale p sta con certezza all'interno del quadrato di centro $\overline{p}$ e lato 2ϵ.



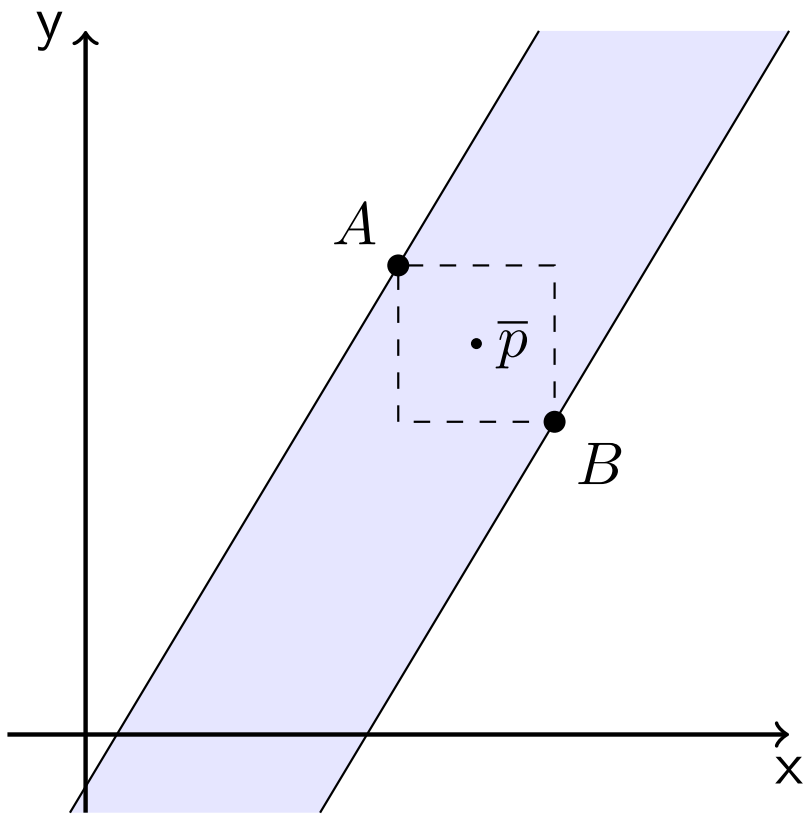
Calcolo delle molteplicità: una tecnica di risoluzione

2. Genero un valore random $a \geq 0$ e considero le due rette del piano appartenenti all'applicazione lineare $ax - y$ passanti per A e per B: queste assumeranno dei valori distinti λ_A e λ_B sui punti A e B.



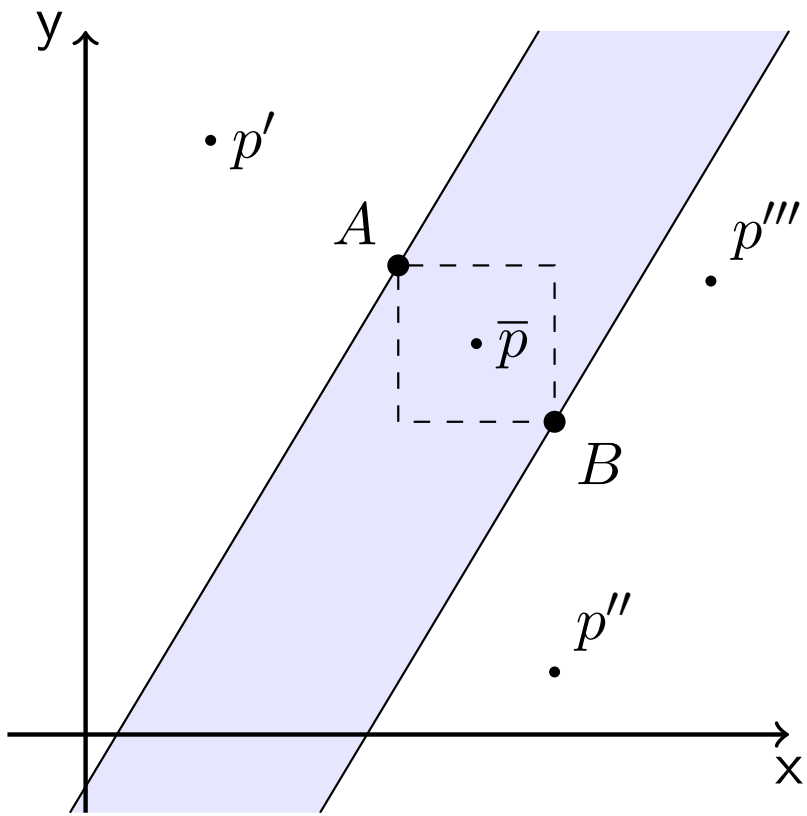
Calcolo delle molteplicità: una tecnica di risoluzione

3. Gli autovalori di M_{ax-y} sono i valori assunti da $ax - y$ sulle soluzioni di I. Con il polinomio $h(t) = -(t - \lambda_A)(t - \lambda_B)$ determino quante radici del polinomio caratteristico $f(t)$ di M_{ax-y} stanno nell'intervallo (λ_A, λ_B).



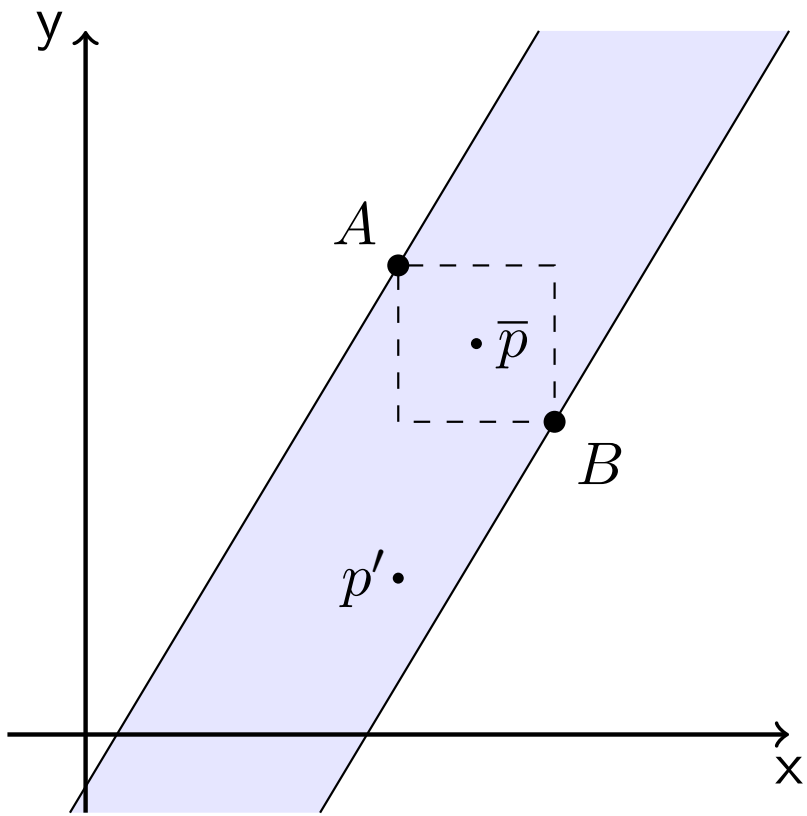
Calcolo delle molteplicità: una tecnica di risoluzione

4. Se in (λ_A, λ_B) cade una sola radice di $f(t)$ posso applicare la funzione per il calcolo della molteplicità in una variabile e determinarne la molteplicità.



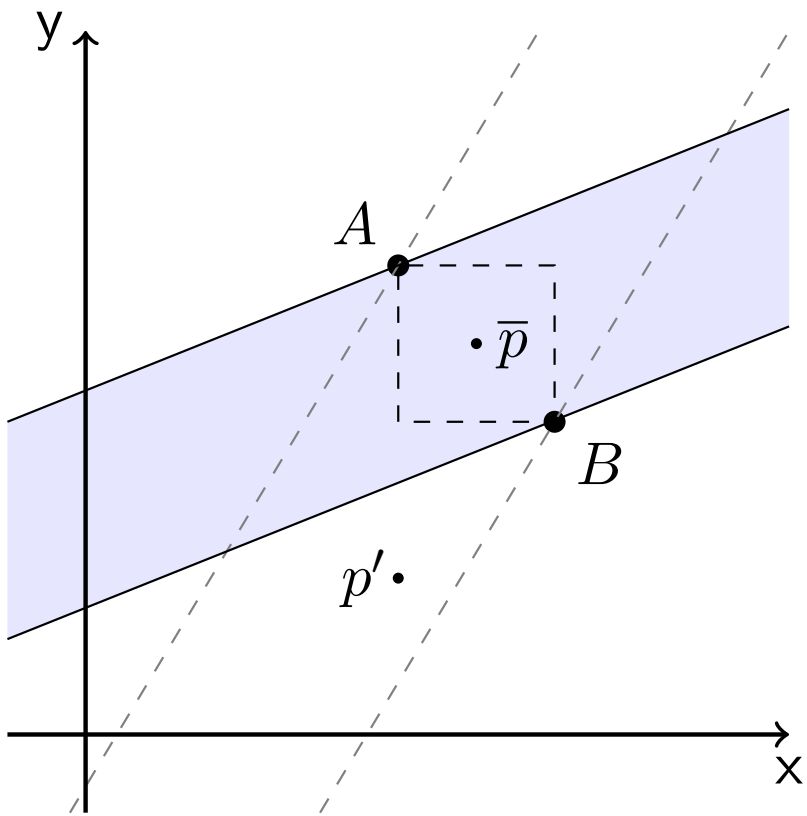
Calcolo delle molteplicità: una tecnica di risoluzione

5. Se in (λ_A, λ_B) cadono due o più radici di $f(t)$ generiamo un nuovo valore random a e ripartiamo dal punto precedente.



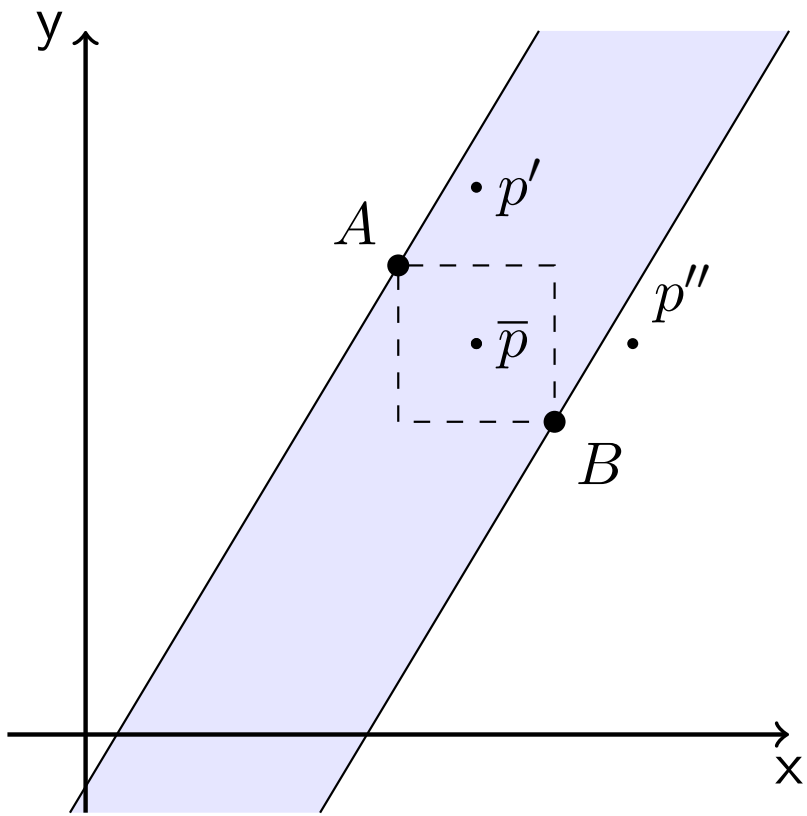
Calcolo delle molteplicità: una tecnica di risoluzione

5. Se in (λ_A, λ_B) cadono due o più radici di $f(t)$ generiamo un nuovo valore random a e ripartiamo dal punto precedente.



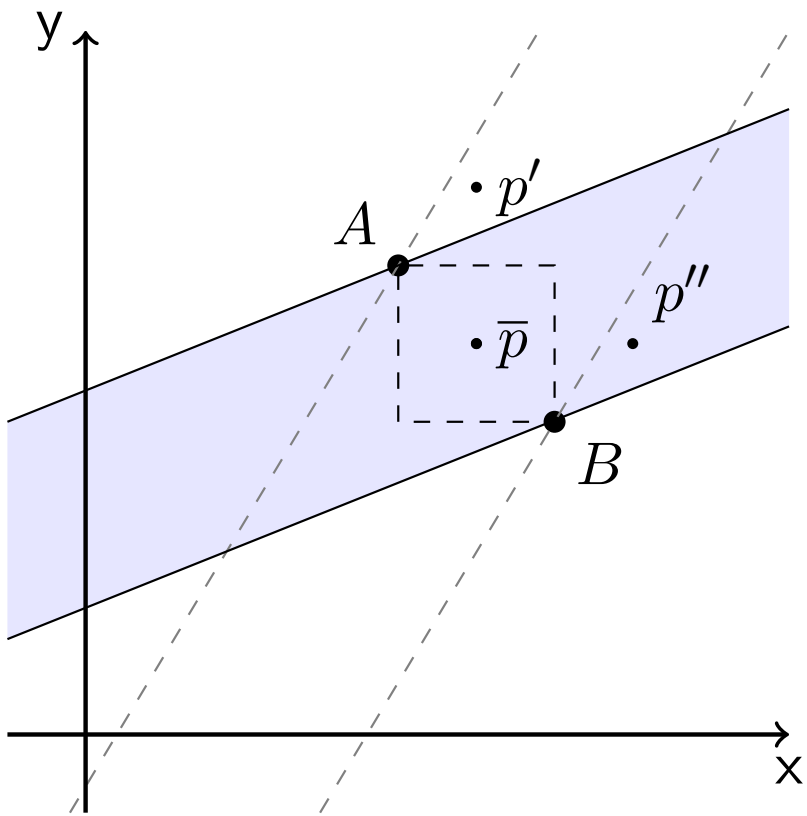
Calcolo delle molteplicità: una tecnica di risoluzione

5. Se ci sono soluzioni del sistema molto vicine al quadrato, seppure esterne, non si riesce a isolare una sola radice di $f(t)$ in (λ_A, λ_B) pur cambiando il valore di a. Occorre quindi ripartire dal punto 1), con un livello di precisione $\epsilon' < \epsilon$.



Calcolo delle molteplicità: una tecnica di risoluzione

5. Se ci sono soluzioni del sistema molto vicine al quadrato, seppure esterne, non si riesce a isolare una sola radice di $f(t)$ in (λ_A, λ_B) pur cambiando il valore di a. Occorre quindi ripartire dal punto 1), con un livello di precisione $\epsilon' < \epsilon$.



Calcolo delle molteplicità: una tecnica di risoluzione

5. Se ci sono soluzioni del sistema molto vicine al quadrato, seppure esterne, non si riesce a isolare una sola radice di $f(t)$ in (λ_A, λ_B) pur cambiando il valore di a. Occorre quindi ripartire dal punto 1), con un livello di precisione $\epsilon' < \epsilon$.