La Matematica nella Società e nella Cultura

Rivista dell'Unione Matematica Italiana

Cristina Bertone

Algoritmi per la fattorizzazione di polinomi e la decomposizione di curve

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **4** (2011), n.1 (Fascicolo Tesi di Dottorato), p. 11–14.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RIUMI_2011_1_4_1_11_0>

La Matematica nella Società e nella Cultura. Rivista dell'Unione Matematica Italiana, Unione Matematica Italiana, 2011.

La Matematica nella Società e nella Cultura
Rivista dell'Unione Matematica Italiana
Serie I, Vol. IV, Aprile 2011, 11-14

Algoritmi per la fattorizzazione di polinomi e la decomposizione di curve

Cristina Bertone

Consideriamo un insieme di polinomi $\{F_1, \dots, F_s\} \subseteq \mathbb{K}[X_1, \dots, X_n]$, dove $\mathbb{K}$ è un campo, e consideriamo il suo *insieme degli zeri*

$$V(F_1, \dots, F_s) = \{P \in \overline{\mathbb{K}}^n | F_i(P) = 0, i = 1, \dots, s\}.$$

L'insieme di punti $V(F_1, \dots, F_s)$ è un *insieme algebrico* di $\overline{\mathbb{K}}^n$, dove $\overline{\mathbb{K}}$ è la chiusura algebrica di $\mathbb{K}$. In realtà, questo insieme di punti coincide con $V(\mathfrak{a})$, dove $\mathfrak{a}$ è l'ideale generato dall'insieme di polinomi $\{F_1, \dots, F_s\}$.

Un insieme algebrico è *irriducibile* se non si può esprimere come unione di due sottoinsiemi algebrici propri, altrimenti è detto *riducibile*.

Se consideriamo un insieme algebrico riducibile e lo scriviamo come unione di insiemi algebrici irriducibili, questi costituiscono le *componenti irriducibili* (o semplicemente le *componenti*).

In questa tesi consideriamo una curva algebrica (ovvero, un insieme algebrico di dimensione 1) negli spazi affini $\mathbb{C}^2$ e $\mathbb{C}^3$ e cerchiamo delle tecniche efficaci dal punto di vista computazionale per individuare le componenti irriducibili di tali curve.
In entrambi gli spazi affini, la decomposizione di una curva esiste ed è unica, nel senso che esiste un numero finito di componenti irriducibili, le quali sono univocamente determinate.

Tuttavia, a prima vista, la situazione in $\mathbb{C}^3$ è notevolmente differente dalla situazione di $\mathbb{C}^2$.

$\mathbb{C}^2$: una curva $\mathcal{C}$ è un insieme algebrico di dimensione 1, quindi è definito da un ideale principale: $V(\mathfrak{a}) = \mathcal{C}$ con $\mathfrak{a} = (f(X, Y)) \subseteq \mathbb{C}[X, Y]$.
Perciò $\mathcal{C}$ è irriducibile se e solo se $f(X, Y)$ è irriducibile in $\mathbb{C}[X, Y]$. Il problema di decomporre $\mathcal{C}$ nelle sue componenti irriducibili $\mathcal{C}_1, \dots, \mathcal{C}_s$ è quindi equivalente al problema di calcolare la fattorizzazione di $f(X, Y)$ in $\mathbb{C}[X, Y]$.

$\mathbb{C}^3$: una curva $\mathcal{C}$ non è definita da un singolo polinomio, ne occorrono almeno 2. In questo caso, la decomposizione di $\mathcal{C}$ in $\mathcal{C}_1, \dots, \mathcal{C}_s$ è equivalente alla decomposizione primaria dell'ideale $\mathfrak{a}$, tale che $V(\mathfrak{a}) = \mathcal{C}$.

In questa tesi ci limitiamo al caso della decomposizione di curve definite da polinomi a coefficienti razionali.

Per quel che riguarda la decomposizione in $\mathbb{C}^2$, il problema della fattorizzazione assoluta (e della fattorizzazione razionale) è stato studiato da numerosi autori, che

hanno proposto algoritmi sempre più performanti (si può vedere Kaltofen(1990) e Kaltofen (1992) per un quadro d'insieme sulla ricerca in questo ambito).

Anche il problema di calcolare la decomposizione primaria di un ideale $\mathfrak{a}$ in un anello polinomiale è stato attaccato con tecniche diverse (si può vedere per esempio Decker et al. (1999) e i riferimenti in esso contenuti) e la ricerca in questo campo è in continuo sviluppo (ad esempio, il caso degli ideali 0-dimensionali, Durvye (2009)). Tuttavia, non c'è ancora una strategia efficiente per il caso generale. Due delle strategie più recenti per la decomposizione di curve in $\mathbb{C}^3$ si basano sulla riduzione al caso di un insieme di punti del piano e usano calcoli numerici(Galligo et al. (2002), Sommese et al. (2001)).

In effetti è vantaggioso dal punto di vista computazionale risolvere il problema passando da un insieme algebrico di dimensione 1 in $\mathbb{C}^3$ a un insieme algebrico di dimensione 0 in $\mathbb{C}^2$ (ovvero, considerare una generica sezione piana). Al contrario, passare da una curva in $\mathbb{C}^3$ a una curva in $\mathbb{C}^2$ richiede spesso calcoli molto pesanti (proiettare la curva su un generico piano equivale a un'eliminazione di variabili).
Tuttavia, questo è esattamente quello che facciamo in questa tesi: studiamo il caso "base" della decomposizione di una curva in $\mathbb{C}^2$ e cerchiamo poi di ricondurre la decomposizione di una curva in $\mathbb{C}^3$ al caso base già noto.
Una volta studiato un algoritmo di fattorizzazione assoluta per polinomi in 2 variabili, utilizziamo le stesse tecniche per una curva in $\mathbb{C}^3$ mediante proiezione su un piano generico; la tecnica di proiezione e fattorizzazione assoluta è "classica", ma siamo in grado di accelerare di molto i calcoli perché utilizziamo tecniche modulari.

Nella prima parte della tesi, affrontiamo quindi il problema per $n = 2$, ovvero ci occupiamo del calcolo della fattorizzazione assoluta di un polinomio razionale. Questo problema è stato intensivamente studiato negli ultimi anni (tra gli altri, Galligo, Chèze, Rupprecht, Lecerf, Sommese e loro coautori) con tecniche diverse. Il punto di partenza del nostro studio è un algoritmo esistente, l'algoritmo Trager-Traverso. Seguiamo la stessa procedura di questo algoritmo, ma ne miglioriamo l'efficienza di esecuzione cercando dei risultati più fini di quelli dell'algoritmo originale.

L'algoritmo di fattorizzazione assoluta costruisce l'estensione algebrica di $\mathbb{Q}$ di grado minimo contenente i coefficienti dei fattori assoluti del polinomio. Per fare ciò è necessaria la scelta di un primo p che assicuri l'esistenza in $\mathbb{Q}_p$ (campo dei numeri p-adici) di un elemento primitivo dell'estensione algebrica che stiamo cercando. Possiamo inoltre affermare che per genericità il primo scelto assicura una buona riduzione di $f(X, Y)$, cioè la fattorizzazione di $f(X, Y)$ modulo p ha lo stesso numero di fattori della fattorizzazione di $f(X, Y)$ in $\overline{\mathbb{Q}}[X, Y]$. Possiamo quindi usare l'Hensel lifting per ottenere un'approssimazione p-adica più precisa dell'elemento primitivo. Infine costruiamo il polinomio univariato che definisce l'estensione algebrica; per fare questo usiamo l'algoritmo *LLL* di riduzione per reticoli interi.

Iniziamo la seconda parte della tesi evidenziando le somiglianze tra il caso della curva nel piano e quello della curva nello spazio affine tridimensionale. Definiamo quindi per il caso tridimensionale la decomposizione primaria di un ideale, la funzione di Hilbert affine, le componenti razionali, algebriche e coniugate della decomposi-

zione primaria. Usando la funzione di Hilbert, otteniamo anche la definizione di grado e molteplicità di una componente primaria.

L'obiettivo che ci poniamo è la costruzione di un polinomio *separatore* per ogni componente algebrica della curva: è un polinomio che definisce una superficie algebrica di $\mathbb{C}^3$ che contiene una componente irriducibile della curva ma non contiene nessuna delle altre. Il primo problema da risolvere è quello di trovare una limitazione al grado di un polinomio separatore; se potessimo calcolare tale limitazione, potremmo utilizzare un algoritmo numerico di decomposizione evitando calcoli superflui e costosi.

Ci concentriamo quindi su limitazioni per il grado del polinomio separatore ottenibili usando invarianti di geometria algebrica e argomenti esistenti in letteratura: il Lifting Problem, la regolarità e il generico ideale iniziale.

Il Lifting Problem in codimensione 2 è un problema classico in geometria algebrica. Anche se il caso delle curve nello spazio tridimensionale (proiettivo) è completamente risolto, il problema è ancora aperto in dimensione più alta. Il lemma trisecante di Laudal e i miglioramenti successivi ottenuti da vari autori, forniscono un bound inferiore sul grado di un polinomio separatore, ottenuto calcolando la generica sezione piana. In questa parte della tesi, riguardo al Lifting problem vengono anche brevemente riassunti alcuni risultati originali riguardanti la positività della seconda classe di Chern di un fascio riflessivo ottenuti in collaborazione con Margherita Roggero; lo studio della seconda classe di Chern di un fascio riflessivo è infatti una delle direzioni di ricerca per la dimostrazione della congettura di Emilia Mezzetti per il caso generale del Lifting Problem.

La regolarità è un invariante ben noto per ideali, che fornisce una limitazione non solo sul grado dei generatori minimali di un ideale, ma anche sul grado delle loro sizigie. Usando risultati in letteratura sulla regolarità, possiamo maggiorare il grado di un polinomio separatore in diversi modi: ad esempio, mediante il grado della componente; in casi particolari mediante la regolarità della sezione piana o ancora mediante una funzione lineare nei gradi dei generatori dell'ideale $\mathfrak{a}$; utilizziamo risultati di vari autori, quali Mumford, Chardin, Cioffi-Marinari-Ramella.

Infine, l'ideale iniziale generico è un ideale monomiale che ha caratteristiche combinatoriche che riflettono gli invarianti dell'ideale, quali la saturazione o la regolarità stessa. Il generico ideale iniziale di una componente fornisce quindi il bound desiderato sul grado del polinomio separatore.

Poiché nessuna delle limitazioni "classiche" citate sopra può fornire direttamente, usando solo dati noti dell'ideale $\mathfrak{a}$, il bound cercato, richiamiamo una strategia ben nota per calcolare la decomposizione primaria di un ideale (o almeno per calcolare le componenti primarie che sono anche prime). Questa strategia usa proiezioni generiche (metodo introdotto da Grete Hermann all'inizio del XX secolo). Le proiezioni ci permettono di ricondurre il problema della decomposizione della curva in $\mathbb{C}^3$ al problema della fattorizzazione di un polinomio in 2 variabili. Utilizzando poi la dimensione di Hilbert (per "abbinare" in maniera corretta fattori provenienti da proiezioni diverse) e ideali quoziente (per togliere punti immersi residui, che sono nel luogo singolare dell'ideale), possiamo ottenere gli ideali che definiscono le componenti prime di $\mathfrak{a}$. Nella

pratica, per avere una proiezione generica operiamo un generico cambiamento di coordi! nate e poi proiettiamo sui piani coordinati; la proiezione equivale quindi a eliminare una variabile, operazione ottenuta mediante il calcolo del risultante.

Purtroppo, questo metodo non è conveniente dal punto di vista computazionale, quindi usiamo nuovamente calcoli modulari per rendere questa strategia rapida.

Mostriamo quindi che possiamo di nuovo affidarci alla genericità (come abbiamo fatto per la fattorizzazione assoluta) per evitare primi p con un comportamento "cattivo": in altre parole, se scegliamo un primo p tale che il numero algebrico α è contenuto in $\mathbb{Q}_p$, allora siamo "quasi" certi che un ideale $\mathfrak{a}$ con generatori a coefficienti in $\mathbb{Q}(\alpha)$ può essere ridotto modulo p preservando i monomi di testa di una base di Groebner (e quindi preservando la sua funzione di Hilbert).

Questo risultato vale per ideali contenuti in anelli polinomiali a n variabili; nel nostro caso lo applichiamo a un'ideale intersezione completa generato da polinomi in $\mathbb{Q}[X, Y, Z]$. Adattiamo quindi l'algoritmo "esatto" discusso in precedenza al calcolo modulare; in particolare possiamo evitare il problema di calcolare in $\mathbb{Q}[X, Y, Z]$ risultanti e loro fattorizzazioni assolute. I calcoli modulari rendono più rapido anche il calcolo della dimensione di Hilbert e degli ideali quoziente. Come output dell'algoritmo modulare otteniamo l'ideale iniziale delle componenti prime di $\mathfrak{a}$ (e quindi maggiorazioni effettive sui gradi di polinomi separatori) e numerose informazioni sulle componenti, quali il loro numero, grado e molteplicità.

Infine, testiamo la strategia modulare su un esempio: per velocizzare ulteriormente i calcoli possiamo anche considerare la primalità dei gradi dei fattori nella fattorizzazione modulare dei risultanti, grazie alle proprietà della fattorizzazione assoluta di un polinomio razionalmente irriducibile. In questo modo possiamo evitare di usare primi diversi per ogni componente razionale delle curva e riduciamo il numero di risultanti e fattorizzazioni bivariate da calcolare.

Anche se l'algoritmo modulare non dà come output i polinomi separatori, ma al più le loro immagini modulo p, è piuttosto promettente: infatti, abbiamo provato a calcolare la decomposizione primaria dell'ideale trattato con l'algoritmo modulare mediante la routine Maple apposita, PrimaryDecomposition: Maple non è riuscito a portare a termine i calcoli a causa di problemi di allocazione della memoria, sia nel caso di una decomposizione razionale sia in quello della decomposizione assoluta.

Vista la velocità di esecuzione dell'algoritmo modulare, possiamo inoltre utilizzare il suo output come operazione preliminare per avere bound pratici che possono guidare un algoritmo di decomposizione di tipo numerico.

Dipartimento di Matematica, Università di Torino
e-mail: cristina.bertone@unito.it
Dottorato in Scienza e Alta Tecnologia, indirizzo Matematica,
con sede presso l'Università di Torino - Ciclo XXII
École Doctorale en Sciences Fondamentales et Appliqées, specialité Mathèmatiques,
con sede presso l'Università di Nizza (Francia)
Direttori di ricerca: prof. André Galligo, Università di Nizza (Francia),
prof.ssa Margherita Roggero, Università di Torino