Algebra computazionale
Dott. Massimo Caboara

Stefano Maggiolo
http://poisson.phc.unipi.it/~maggiolo/
maggiolo@mail.dm.unipi.it

2006–2007

Indice

1 Fattorizzazione

07.03.2007

1.1 Introduzione

In una variabile, si definisce l'*anello dei polinomi* come $R[x] \coloneqq \{ (a_i) \mid (\exists k)(\forall i > k) a_i = 0 \} \subseteq R[[x]]$. Per esempio, $x^3+2x+1 = (1, 2, 0, 1, 0, \ldots)$.

Una definizione equivalente si può dare a partire da quella di *monomio*, che non è altro che un coefficiente moltiplicato per una variabile elevata a un certo esponente, e definendo un polinomio come somma, differenza e prodotto finiti di monomi. In questo contesto, la definizione è sintattica: $x + x \neq 2x$. Il secondo si dice posto in *forma canonica*.

In una variabile, gli ordinamenti dei termini compatibili con il prodotto sono solo quelli per grado crescente e per grado decrescente.

I polinomi in più variabili si possono descrivere analogamente a quanto fatto prima, oppure si può dare una definizione ricorsiva: $R[x_1, \ldots, x_n] \coloneqq R[x_1][x_2, \ldots, x_n]$, anche se questa rappresentazione non è ottimale per l'implementazione al computer. Quella che si usa, invece, è un'altra rappresentazione: $R[x_1, \ldots, x_n]$ è l'insieme delle successioni definitivamente nulle di elementi di $(R, \mathbb{N}^n)$ ordinate secondo un certo ordinamento σ. Il fatto di avere un ordinamento non è strettamente necessario, ma permette di velocizzare le operazioni di confronto.

1.2 Operazioni sui polinomi

08.03.2007

Le operazioni naturali sui polinomi sono le seguenti.

1. Prodotto per $c \in K$ o per $t \in T^n$ (dove T^n indica l'insieme dei monomi in n variabili con coefficiente unitario); è un'operazione con complessità lineare.

2. Somma e differenza di polinomi: per polinomi densi si riduce a fare la somma di due vettori (complessità lineare); se però si sommano due polinomi di dimensione molto diversa, questo procedimento intuitivo è molto inefficiente; per ottimizzare l'operazione si possono usare i *geobucket*: si partiziona il polinomio in un certo numero di polinomi corrispondenti ai vari bucket; la somma dei sottopolinomi è il polinomio originale e i bucket hanno grandezza crescente; la somma di due polinomi viene eseguita sommando il polinomio più piccolo e un bucket di dimensione simile, ed eventualmente riportando sul bucket successivo.

3. Prodotto di polinomi: se $f, g \in R[x]$, $\partial f = \partial g = n$, utilizzando la moltiplicazione standard il costo è $\mathrm{O}(n^2)$, ma si può fare di meglio, in due modi: l'algoritmo di Karatsuba ha complessità $\mathrm{O}(n^{1.59})$, mentre l'algoritmo di Schonhagen-Strassen $\mathrm{O}(n \log n \log \log n)$, usando la FFT. Quest'ultimo però è di difficile implementazione ed è raro vederlo implementato in un sistema di algebra computazionale.

4. Divisione con resto: se si è su $K[x]$ esiste la divisione con resto, infatti l'anello dei polinomi è un anello euclideo, PID e UFD. Invece, $\mathbb{Z}[x]$ o su $K[\underline{x}]$ non sono PID, quindi nemmeno euclidei. Tuttavia nell'ultimo caso si può comunque dividere: invece di richiedere un elemento canonico in ${}^{K[x]}\!/_{(f)}$, si richiede un elemento canonico in ${}^{K[\underline{x}]}\!/_{I}$, con I generato, a priori, da un

insieme arbitrario di elementi; poiché non è un anello euclideo, la divisione non sarà univoca. Per quanto riguarda il gcd, invece, si può fare usando la regola naïf di prendere i fattori comuni col minimo esponente, oppure, su un anello euclideo, con l'algoritmo di Euclide. Se $\partial f = n$, $\partial g = m$, l'algoritmo euclideo standard ha costo $O(nm)$; usandolo, si possono calcolare l'inverso di un elemento in ${}^{K[x]}/_{(f)}$; effettuare operazioni su ideali (intersezione, quoziente, radicale); risolvere equazioni diofantee o sistemi (usando una variante dell'algoritmo di Gauss-Jordan che non effettua divisioni).

5. Valutazione di un polinomio su un elemento $a \in R$: se il polinomio non ha grado molto basso, questa operazione è infattibile in analisi numerica, perché l'eventuale errore si amplifica troppo.

1.3 Algoritmo di Karatsuba

Se si deve calcolare $(ax+b)(cx+d)$, si può usare l'algoritmo naïf, che si riduce a calcolare $acx^2+bd+(ad+bc)x$: quattro moltiplicazioni e una somma. Altrimenti, si possono calcolare ac, bd e $(a+b)(c+d)$, ottenendo il terzo coefficiente da $(a+b)(c+d)-ac-bd$, usando solo tre moltiplicazioni e quattro somme. Usualmente, si considera il costo computazionale dell'addizione trascurabile rispetto a quello della moltiplicazione, quindi si è ottenuto un miglioramento di complessità. Più in dettaglio, l'algoritmo di Karatsuba prende in input due polinomi di grado minore di $n = 2^k$; se $n = 1$ effettua la moltiplicazione scalare, altrimenti spezza f in $f_1 x^{n/2} + f_0$ e g in $g_1 x^{n/2} + g_0$ ed effettua ricorsivamente la moltiplicazione $a \coloneqq f_0 g_0$, $b \coloneqq f_1 g_1$, $c \coloneqq (f_0 + f_1)(g_0 + g_1)$; a partire da queste, ritrova il prodotto, che è $bx^n + cx^{n/2} + a$.

Teorema 1.1. *La complessità di Karatsuba è* $O(n^{\log 3})$.

1.4 Richiami

Alcuni risultati che si danno per noti: il teorema fondamentale dell'algebra ($f \in \mathbb{C}[x]$ è irriducibile se e solo se $\partial f = 1$); $f \in \mathbb{R}[x]$ è irriducibile se e solo se $\partial f = 1$ o $\partial f = 2$ e $\Delta f < 0$; se $f \in \mathbb{Q}[x]$ e ${}^m/_n$ è radice di f allora m e n sono divisori di termine noto e coefficiente direttore, rispettivamente.

Per fattorizzare in $\mathbb{Q}[x]$ si può usare il metodo di forza bruta: per ogni grado si uguaglia il prodotto di due polinomi generici con il polinomio da fattorizzare e ci si riconduce alla risoluzione di un sistema. In realtà i migliori algoritmi di forza bruta sono meno performanti dei migliori algoritmi per fattorizzare in $\mathbb{Q}[x]$. Per il lemma di Gauss, fattorizzare su $\mathbb{Q}[x]$ è equivalente a fattorizzare su $\mathbb{Z}[x]$; questo aiuta parzialmente nel metodo di forza, ma non troppo.

Su $\mathbb{Z}_p[x]$, si può usare lo stesso metodo, ma questa volta è molto più facile trovare la soluzione del sistema; altrimenti, si può provare a dividere per tutti i polinomi di grado inferiore a quello di partenza.

Su $\mathbb{Q}[x]$, i polinomi irriducibili sono un aperto dello spazio dei polinomi, quindi sono quasi tutti; tuttavia, i criteri di irriducibilità non sono tanti, praticamente solo il criterio di Eisenstein.

Un cambiamento lineare di coordinate non cambia la riducibilità del polinomio: se $a, b \in \mathbb{Q}$, $f(x)$ è riducibile se e solo se $f(ax + b)$ è riducibile.

Esercizio 1.2. Dimostrare che $x^{p-1} + x^{p-2} + \cdots + 1$ è irriducibile.

Se $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$, allora $f(x) = g(x)h(x)$ in $\mathbb{Z}_n[x]$; questo non implica che se f è riducibile in $\mathbb{Q}[x]$ allora è riducibile su $\mathbb{Z}_n[x]$ per ogni n, perché i fattori potrebbero banalizzarsi passando a $\mathbb{Z}_n[x]$ (per esempio se $f(x) = (2x+5)(3x-1)$ in $\mathbb{Q}[x]$, questa fattorizzazione non passa a una fattorizzazione di $\mathbb{Z}_2[x]$ o $\mathbb{Z}_3[x]$). In conclusione, f si fattorizza sicuramente in $\mathbb{Z}_n[x]$ quando n non divide il coefficiente direttore. Viceversa, non si può dire nulla, come mostra la proposizione seguente.

Proposizione 1.3. *Sia $f_{a,b}(x) = x^4 + ax^2 + b^2$ con $a, b \in \mathbb{Z}$; allora:*

1. *$f_{a,b}$ è riducibile su $\mathbb{Z}_p[x]$ per ogni p primo;*
2. *esistono $a, b \in \mathbb{Z}$ tali che $f_{a,b}$ è irriducibile su $\mathbb{Z}[x]$.*

Dimostrazione. Per $p = 2$ si verifica facilmente che non esistono polinomi di quella forma irriducibili su $\mathbb{Z}_2[x]$, provando tutti i casi. Per $p > 2$, sia $a = 2s$, allora

$$\begin{aligned} f(x) = x^4 + 2sx^2 + b^2 &= (x^2+s)^2 - (s^2 - b^2) = \\ &= (x^2+b)^2 - (2b-2s)x^2 = \\ &= (x^2-b)^2 - (-2b-2s)x^2. \end{aligned}$$

Lo scopo è di mostrare che tra s^2-b^2, $2b-2s$ e $-2b-2s$ ci sia almeno un quadrato (per cui una tra le tre sarà una differenza di quadrati). Si suppone allora che $2b-2s$ e $-2b-2s$ non siano quadrati; per il teorema dell'elemento primitivo, i due sono c^t e c^k per qualche t e k dispari; allora $(2b-2s)(-2b-2s) = 4(s^2-b^2) = c^{i+k}$ è un quadrato, ma anche 4 lo è e di conseguenza anche $s^2 - b^2$.

Si vuole ora dimostrare che per $a = 2 = b$, f è irriducibile: innanzitutto, per un criterio visto in precedenza, non esistono fattori lineari. Di conseguenza, se fosse fattorizzabile, f si scriverebbe come prodotto di due fattori di secondo grado, che si possono assumere essere monici:

$$x^4 + ax^2 + b^2 = (x^2 + cx + d)(x^2 + ex + f), \text{ con } c, d, e, f \in \mathbb{Z}.$$

Si ottiene un sistema che si dimostra facilmente essere impossibile. □

14.03.2007

Esempio 1.4. Si considera il polinomio

$$\begin{aligned} x^4 + 4 = (x^2 + 2i)(x^2 - 2i) &= (x + i\sqrt{2i})(x - i\sqrt{2i})(x + \sqrt{2i})(x - \sqrt{2i}) = \\ &= (x - 1 + i)(x - 1 - i)(x + 1 + i)(x + 1 - i), \end{aligned}$$

usando $\sqrt{i} = \sqrt{2}/2 + i\sqrt{2}/2$. Per ricavare un'eventuale fattorizzazione su $\mathbb{Q}$ da quella su $\mathbb{C}$, si devono provare tutte le possibilità; però notando che il primo e il secondo fattore hanno radici coniugate, si scopre subito che

$$x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2).$$

1.5 Fattori multipli

Molti algoritmi che lavorano su polinomi funzionano meglio se applicati a polinomi senza fattori multipli o comunque, in generale, se si rimuovono i fattori multipli da un polinomio si abbassa la sua dimensione per l'algoritmo in questione. Perciò, si vuole un algoritmo efficiente che, dato un polinomio, ne restituisca uno con tutti i fattori del primo ma presi una volta sola.

Definizione 1.5. Sia $f \in K[x]$, $f = \prod f_i^{\alpha_i}$ con $f_i \in K[x]$ irriducibili; f è *square free* (SQFR) se $\alpha_i = 1$ per ogni i; si definisce $\mathrm{SQFR}(f) = \prod f_i$.

Per calcolare $\mathrm{SQFR}(f)$ usando la definizione, si deve conoscere la fattorizzazione, che è un'operazione dal costo molto alto; trovare la decomposizione square free invece è decisamente meno dispendioso.

Definizione 1.6. Un campo K si dice *perfetto* se e solo se ha caratteristica 0 o ha caratteristica positiva p e $K = K^p$ (cioè esistono tutte le radici p-esime). Per i nostri scopi si richiede che sia dato anche l'algoritmo di calcolo della radice p-esima.

Osservazione 1.7. Per il piccolo teorema di Fermat, $\mathbb{Z}_p$ è perfetto ($a^p = a$, da cui $\sqrt[p]{a} = a$), ma anche $\mathbb{F}_{p^n}$ è perfetto: se $x \in \mathbb{F}_{p^n}$, vale $x^{p^n} = x$, da cui $\sqrt[p]{x} = x^{p^{n-1}}$. Le due relazioni precedenti valgono in quanto il gruppo moltiplicativo di $\mathbb{F}_{p^n}$ ha $p^n - 1$ elementi. Un esempio di campo non perfetto è $\mathbb{F}_p(x)$: si dimostra che x non ha radice p-esima.

Teorema 1.8. *Se K è un campo perfetto, $f(x) \in K[x]$ non costante, allora:*

1. *f è square free se e solo se $(f, f') = 1$;*
2. *se $\operatorname{ch} K = 0$, $f/(f, f') = \mathrm{SQFR}(f)$;*
3. *se $\operatorname{ch} K > 0$, esiste un algoritmo[1] per trovare $\mathrm{SQFR}(f)$.*

Dimostrazione. Sia $f = \prod f_i^{\alpha_i}$; allora, assumendo senza perdita di generalità che tutti i polinomi siano monici,

$$f' = \sum_j \left(\alpha_j f_j^{\alpha_j - 1} f_j' \prod_{i \neq j} f_i^{\alpha_i} \right).$$

Da questo si mostra facilmente che se il massimo comune divisore di f e f' è diverso da 1, allora f non può essere square free. Viceversa, sia f square free, e per assurdo sia h un fattore irriducibile comune a f e f'. Allora $f = hg$ e $f' = hg' + h'g$, ma allora per l'irriducibilità di h, $h \mid h'$ o $h \mid g$. Se $h \mid g$ si ha l'assurdo perché $h^2 \mid f$, altrimenti $h \mid h'$ è ancora assurdo in caratteristica 0 (accade se e solo se $h' = 0$), mentre in caratteristica p, significa che

$$h = a_n^p (x^p)^n + \cdots + a_1^p (x^p)^1 + a_0^p = (a_n x^n + \cdots + a_1 x + a_0)^p,$$

quindi h non era irriducibile (i coefficienti si possono prendere potenze p-esime perché il campo è perfetto). □

Esempio 1.9. Sia

$$f(x) = x^4 - 8x^3 + 23x^2 - 28x + 12 = (x-1)(x-2)^2(x-3);$$

allora

$$\begin{aligned} f'(x) &= 4x^3 - 24x^2 + 46x - 28 = \\ &= (x-2)^2(x-3) + (x-1)2(x-2)(x-3) + (x-1)(x-2)^2 \end{aligned}$$

e risulta $(f, f') = (x - 2)$.

[1] Si veda [KR00]; la differenza rispetto al caso $\operatorname{ch} K = 0$ deriva dal fatto che non necessariamente $f' = 0$ implica f costante.

1.6 Teorema cinese del resto

15.03.2007

Teorema 1.10 (Teorema cinese del resto)**.** *Siano R un anello, $I_1, \dots, I_t$ ideali di R, allora:*

1. *$\varphi\colon {}^{R}\!/_{\bigcap I_j} \to \prod {}^{R}\!/_{I_j}$ è iniettiva;*
2. *se gli ideali sono a due a due coprimi (cioè $I_i + I_j = 1$ per ogni $i \neq j$) allora φ è un isomorfismo.*

Dimostrazione. L'iniettività è ovvia: se $\varphi(r + \bigcap I_j) = 0$, allora $r \in I_j$ per ogni j, cioè $r \in \bigcap I_j$. Per la suriettività, se gli I_j sono tra loro coprimi, si trovano $x_j \in I_j$ e $y_j \in I_t$ tali che $1 = x_j + y_j$; allora

$$1 = \prod_{i \neq t} (x_j + y_j) = \prod_{i \neq t} x_j + y \in I_1 \cdots I_{t-1} + I_t;$$

di conseguenza, $\varphi(\prod_{i \neq t} x_j) = (0, \dots, 0, 1)$; si procede allo stesso modo per gli altri generatori. □

Teorema 1.11 (Teorema cinese del resto)**.** *Siano K un campo, $a_1, \dots, a_n \in K[x]$ polinomi, $m_1, \dots, m_n \in K[x]$ polinomi a due a due coprimi, allora esiste un unico $f \in K[x]$, con $\partial f < \prod \partial m_i$ tale che $f(x) \equiv a_i(x) \ \ (m_i(x))$.*

Dimostrazione. Sia $e_i \coloneqq \prod_{j \neq i} m_j$; si risolve $1 = h_i(x)m_i(x) + k_i(x)e_i(x)$ rispetto a h e k (è un'equazione che ha sicuramente soluzione, per la coprimalità). Ora, $k_i(x)e_i(x) \equiv \delta_{i,j} \ \ (m_j(x))$, e si pone $f(x) \coloneqq \sum a_i(x)k_i(x)e_i(x)$. □

La seconda versione del teorema cinese del resto permette di trasformare un problema di congruenze nell'algebra dei polinomi in un problema di algebra lineare, grazie alla limitazione che si ha sul grado di f.

Corollario 1.12. *Siano $n_0, \dots, n_d \in K$ distinti, $s_0, \dots, s_d \in K$ distinti, allora esiste un unico $q \in K[x]$ con $\partial q \leq d$ tale che $q(n_i) = s_i$.*

Questo corollario permette di dire che la valutazione di un polinomio di grado minore o uguale a d su d punti determina il polinomio. Come ulteriore corollario, l'insieme delle funzioni $\left\{\mathbb{F}_{p^n}^k \to \mathbb{F}_{p^n}^k\right\}$ è dato solo da applicazioni polinomiali. Un altro fatto utile è $g(x) = b$ in ${}^{K[x]}\!/_{(x\,-\,a)}$ se e solo se $g(a) = b$.

1.7 Fattorizzazione con l'interpolazione di Lagrange

Sia $p \in \mathbb{Z}[x]$ con $\partial p = 2d$; siano $n_0, \dots, n_d \in \mathbb{Z}$ interi distinti e $r_i \coloneqq p(n_i)$. Si suppone che esista un fattore a di p non banale e con grado minore o uguale a ${}^{d}\!/_{2}$, e sia $p(x) = a(x)b(x)$. Allora $p(n_i) = a(n_i)b(n_i)$ e in particolare $a(n_i) \mid r_i$. Questa condizione deve essere soddisfatta da ogni fattore di p; l'idea dell'algoritmo è trovare tutti i vettori di interi $(s_0, \dots, s_d)$ che dividono $(r_0, \dots, r_d)$ e per ognuno di questi provare a dividere p con il polinomio corrispondente al vettore $(s_0, \dots, s_d)$, cioè quello di grado minimo tra i polinomi a con $a(n_i) = s_i$. Il polinomio a è detto *polinomio interpolatore di Lagrange* ed è facilmente computabile.

Esempio 1.13. Sia $p(x) = x^4 + x + 1$; si prende $(n_0, n_1, n_2) = (-1, 0, 1)$, allora $(r_0, r_1, r_2) = (1, 1, 3)$. Poiché p è monico, si possono testare solo i polinomi monici, per cui ci si riduce a quelli nella tabella 1.

(n_0, n_1, n_2)	$a(x)$
$(1, -1, -1)$	$x^2 - x - 1$
$(1, 1, -1)$	$-x^2 - x + 1$
$(-1, -1, 1)$	$x^2 + x - 1$
$(-1, 1, 1)$	$-x^2 + x + 1$
$(1, 1, 3)$	$x^2 + x + 1$
$(-1, -1, -3)$	$-x^2 - x - 1$

Tabella 1: Possibili divisori di $x^4 + x + 1$.

Alcuni di questi polinomi sono associati (si ottengono mediante moltiplicazione per un'unità), quindi si possono evitare alcuni tentativi. Rimane solo da effettuare le divisioni e controllare se c'è un divisore.

Il problema è l'evidente lunghezza del metodo, data dal grande numero di polinomi anche in un caso quasi banale. Si può leggermente ottimizzare questo algoritmo, per esempio avendo un algoritmo veloce per ottenere il polinomio a partire dal vettore, ma l'alto numero di prove da fare lo fa rimanere inutilizzabile, in quanto comunque l'operazione da fare per ogni prova non è banale.

1.8 Fattorizzazione in $\mathbb{Z}[x]$ passando per $\mathbb{Z}_p[x]$

Si suppone innanzitutto $f \in \mathbb{Z}[x]$ monico (l'irriducibilità di un polinomio non cambia per una trasformazione lineare delle coordinate, se $f(x) = ax^n + \cdots$, si considera $g(x) \coloneqq a^{n-1} f(x/a)$). Si suppone inoltre di saper fattorizzare f in $\mathbb{Z}_p[x]$. Per poter trasportare la fattorizzazione indietro, un problema è che i coefficienti dei polinomi della fattorizzazione sollevata in $\mathbb{Z}[x]$ sono identificati solo a meno di p: più è piccolo p, più è facile trovare la fattorizzazione in $\mathbb{Z}_p[x]$ e più sono le possibili fattorizzazioni in $\mathbb{Z}[x]$. Se però si ha una limitazione sul valore assoluto dei coefficienti dei possibili fattori del polinomio in $\mathbb{Z}[x]$, si può scegliere p abbastanza piccolo e avere lo stesso poche prove da fare.

Proposizione 1.14. *Siano $f \in \mathbb{Z}[x]$ monico con $\partial f = n$ e g fattore di f di grado r; se per ogni radice z di f si ha $|z| < R$, allora*

$$|g_i| \leq \max \left\{ \binom{r}{k} R^k \mid k \in \{1, \ldots, r\} \right\}.$$

Inoltre è noto che $|z| \leq \sum |f_i|$ per ogni radice z, tuttavia questo numero può essere anche molto elevato.

Proposizione 1.15. *Si ha $|z| \leq R_z$, dove*

$$R_z \coloneqq \frac{1}{2^{1/n} - 1} \max \left\{ \left(\frac{|a_{n-i}|}{\binom{n}{i}} \right)^{1/i} \mid i \in \{1, \ldots, n\} \right\}.$$

Proposizione 1.16. *Si ha $|z| \leq R_k$, dove*

$$R_k \coloneqq 2 \max \left\{ |a_{n-i}|^{1/i} \mid i \in \{1, \ldots, n\} \right\}.$$

Esempio 1.17. Sia $f(x) \coloneqq x^5 + 17x^4 - 5x^3 - 277x^2 + 144$, allora si trova che $R_z \leq 21$, mentre $R_k \leq 34$, quindi per i fattori di grado 2, $B_2 \coloneqq 882$ è il limite per i coefficienti. Il primo successivo è 883, che si può usare per fattorizzare.

1.9 Algoritmo di Berlekamp

L'algoritmo di Berlekamp è un algoritmo di fattorizzazione in $\mathbb{Z}_p[x]$, scoperto, al contrario di quello di Lagrange che è della fine del 1700, solo nel 1967. L'idea è che in $\mathbb{Z}_p[x]$ si ha la fattorizzazione $x^p - x = \prod_{i=0}^{p-1}(x-i)$.

Teorema 1.18. *Siano $f, g \in \mathbb{Z}_p[x]$ con $\partial f = d$, $1 \leq \partial g < d$ e tali che $f \mid g^p - g$. Allora $f = \gcd(f,g)\gcd(f,g-1)\cdots\gcd(f,g-(p-1))$ e questa è una fattorizzazione non banale di f, cioè almeno due dei fattori hanno grado maggiore di 0.*

Dimostrazione. Si ha $g^p - g = g(g-1)\cdots(g-(p-1))$. Per ipotesi, $f \mid g^p - g$, quindi

$$f = \gcd(f, g^p - g) = \gcd(f,g)\gcd(f,g-1)\cdots\gcd(f,g-(p-1)),$$

perché tutti i fattori $g-i$ sono coprimi. Questa è una fattorizzazione non banale perché $\partial g < d$, quindi non può esserci un unico fattore di grado d. □

Supponendo di conoscere g, il costo di questo algoritmo è $O(pd^2)$: si fanno p massimi comuni divisori, che hanno costo $O(d^2)$. Normalmente però il grado dei polinomi richiesti dalle applicazioni è basso, quindi il termine dominante sarà p, che si è visto poter essere anche molto alto.

Rimane da trovare g; si suppone $g(x) = b_0 + \cdots + b_{d-1}x^{d-1}$, con b_i incogniti e si avrà $g(x)^p = b_0 + \cdots + b_{d-1}x^{(d-1)p}$. Con l'algoritmo di Euclide si calcola $x^{ip} = q_i(x)f(x) + r_i(x)$ con $\partial r_i < d$. Allora,

$$g(x)^p - g(x) = f(x)q(x) - g(x) + (b_0 r_0(x) + \cdots + b_{d-1}r_{d-1}(x)).$$

Si ha che $f(x) \mid g(x)^p - g(x)$ se e solo se l'ultima parte è 0, perché questa ha grado minore di d. Si ottiene quindi un sistema quadrato con d equazioni, $(Q - I_d)^t b = 0$ dove l'i-esima righe di Q sono i coefficienti di r_i. In tutto, l'algoritmo di Berlekamp costa $O(d^3 + pd^2)$, che si può approssimare a $O(pd^2)$ in quasi tutti i casi pratici. In particolare, questo algoritmo è molto più efficiente del provare a dividere per tutti i polinomi di grado inferiore a d.

1.10 Trucco di Kronecker

Il trucco di Kronecker consiste nel codificare in un unico intero diversi interi, provvisto che si abbia un limite sulla grandezza di questi interi. Lo stesso si può fare con gli esponenti dei polinomi multivariati, per esempio si può trasformare $x^i y^j$ in $z^{100*i+j}$; fattorizzando il polinomio monovariato ottenuto si ottiene anche una fattorizzazione del polinomio multivariato originale, più alcuni termini spurii.

1.11 Sollevamento henseliano e teorema cinese del resto

Ora si ha un algoritmo per fattorizzare in $\mathbb{Z}_p[x]$, ma rimane il problema sulla grandezza di p. Ci sono due possibili approcci: il primo è sfruttare il sollevamento henseliano, il secondo è fattorizzare in tanti primi piccoli e usare il teorema cinese del resto per combinare i risultati.

Teorema 1.19 (Hensel lifting)**.** *Se $f \in \mathbb{Z}[x]$ è monico, $f \equiv g_1 h_1 \ (q)$ e g_1, h_1 sono monici e coprimi modulo q, allora esistono $g_2, h_2 \in \mathbb{Z}[x]$ tali che g_2 e h_2 sono coprimi modulo q^2, $g_2 \equiv g_1 \ (q)$, $h_2 \equiv h_1 \ (q)$ e $f \equiv g_2 h_2 \ (q^2)$. Inoltre, g_2 e h_2 sono unici modulo q^2.*

Questo teorema si può applicare iterativamente, con un costo sostanzialmente basso, sia perché trovare g_2 e h_2 non costa molto, sia perché procedendo per quadrati si supera il limite richiesto molto velocemente.

Si suppone di sapere che $f \equiv g_1 h_1 \ (q)$; si vuole trovare uno spezzamento $f \equiv g_2 h_2 \ (q^2)$. Dallo spezzamento originale si trova in tempo lineare che $f \equiv g_1 h_1 + q k_1 \ (q^2)$. Si risolve l'equazione diofantea $k_1 \equiv g_1 H_1 + h_1 G_1 \ (q)$, con $\partial G_1 < \partial g_1$ e $\partial H_1 < \partial h_1$ e si ottiene la fattorizzazione con $g_2 = g_1 + qG_1$ e $h_2 = g_2 + qG_2$.

Esempio 1.20. Sia $f \coloneqq x^4 + 1$; f si scompone come $(x^2 + x - 1)(x^2 - x - 1)$ in $\mathbb{Z}_3[x]$: questo garantisce che f non ha fattori lineari su $\mathbb{Q}$, altrimenti, dato che 3 non divide il coefficiente di testa, li avrebbe anche in $\mathbb{Z}_3[x]$. Il limite è 4, quindi partendo dalla fattorizzazione in $\mathbb{Z}_3$ basta arrivare a 3^2. Si calcola il sollevamento di Hensel:

$$k_1 \equiv x^2 \equiv (x^2 + x - 1)(ax + b) + (x^2 - x - 1)(cx + d) \quad (3),$$

dove i termini H_1 e G_1 sono lineari per la condizione sui loro gradi. Questa equazione può essere risolta sia come un sistema lineare in 4 incognite che con l'algoritmo euclideo. Risolvendolo, $H_1 = 4x$ e $G_1 = -4x$, quindi

$$\begin{aligned} g_2 &= (x^2 + x - 1) + 3(4x) = x^2 + 4x - 1, \\ h_2 &= (x^2 - x - 1) + 3(-4x) = x^2 - 4x - 1. \end{aligned}$$

Effettivamente, $(x^2 + 4x - 1)(x^2 - 4x - 1) \equiv x^4 + 1 \ (9)$. Provando a dividere $x^4 + 1$ per h_2 e g_2, si scopre che nessuno dei due lo divide, perciò $x^4 + 1$ non è fattorizzabile in $\mathbb{Q}[x]$, dato che $9 > 4$.

Si vede ora lo stesso esempio usando però il teorema cinese del resto.

Esempio 1.21. Sia sempre $f \coloneqq x^4 + 1$; si ha

$$f \equiv (x^2 - x - 1)(x^2 + x - 1) \quad (3) \qquad \text{e} \qquad f \equiv (x^2 + 2)(x^2 - 2) \quad (5).$$

Si cerca un fattore H di f in $\mathbb{Q}[x]$, $H(x) = x^2 + ax + b$ (senza perdita di generalità si può assumere che sia monico); allora si provano tutte le combinazioni di fattori: la prima è

$$x^2 + ax + b \equiv x^2 + x - 1 \quad (3) \qquad \text{e} \qquad x^2 + ax + b \equiv x^2 + 2 \quad (5),$$

cioè

$$\begin{cases} a \equiv 1 \quad (3) \\ a \equiv 0 \quad (5) \end{cases} \qquad \text{e} \qquad \begin{cases} b \equiv -1 \quad (3) \\ b \equiv 2 \quad (5) \end{cases}.$$

Il polinomio candidato è quindi $x^2 + 10x + 2$. Provando tutte le altre combinazioni di fattori, si ottengono diversi polinomi che devono essere provati tutti.

Questo algoritmo sembra meno efficiente (perché si devono provare tutte le combinazioni), ma può rivaleggiare nella pratica con il sollevamento henseliano.

1.12 Decomposizione grado per grado

Si sa che in $\mathbb{Z}_p[x]$, $x^{p^r} - x = \prod f(x)$ dove il prodotto varia sui polinomi $f \in \mathbb{Z}_p[x]$ irriducibili con $\deg f \mid r$. Questo implica che il massimo comune divisore di f e $x^p - x$ è il prodotto dei fattori lineari irriducibili di f, e così via il massimo comune divisore di f e $x^{p^r} - x$ è il prodotto di tutti i fattori di grado minore o uguale di r. Per ottenere i fattori di grado r, basta dividere $\gcd(f, x^{p^r} - x)$ per i massimi comuni divisori relativi ai gradi inferiori che dividono r. Questo algoritmo permette di spezzare il polinomio se ha fattori di gradi diversi, altrimenti troverà solo una fattorizzazione banale; tuttavia per il suo costo molto piccolo viene spesso provato prima di un qualsiasi altro algoritmo di fattorizzazione.

Esempio 1.22. Sia $f(x) = x^9 - 1 \in \mathbb{Z}_5[x]$; allora si ha $\gcd(f(x), x^5 - x) = x - 1$: $x - 1$ è l'unico fattore di grado 1 nella fattorizzazione di $f(x)$ in $\mathbb{Z}_5[x]$. Proseguendo, $\gcd(f(x), x^{25} - 1) = x^3 - 1$, che diviso per $x - 1$ fa $x^2 + x + 1$, che l'unico fattore di grado 2; $\gcd(f(x), x^{125} - x) = x - 1$, $\gcd(f(x), x^{625} - x) = x^3 - 1$. Non esistono fattori di grado 3 e 4 (quindi nemmeno di grado 5), allora la fattorizzazione è data da $x - 1$, $x^2 + x + 1$ e $f(x)/x^3 - 1$.

Il problema apparente di questo algoritmo è che gli esponenti del polinomio $x^{p^r} - 1$ crescono in modo esponenziale. Però questo non è molto influente: se $\partial g \gg \partial f$, allora $\gcd(f, g) = \gcd(f, qf + r)$ dividendo g per f; ma allora questo è $\gcd(f, r)$. Inoltre, si può sfruttare il fatto che g è molto sparso.

1.13 Algoritmi di preprocessing

Si sono visti due algoritmi (decomposizione square free e decomposizione grado per grado) per abbassare il grado del polinomio da fattorizzare al prezzo di un costo irrisorio; si è anche considerato $a^{n-1} f(x/a)$ per avere un polinomio monico. Tuttavia, al contrario dei primi due algoritmi, questo metodo può avere effetti collaterali.

Esempio 1.23. Sia $f(x) \coloneqq 2x^4 + 3x^3 + 5x^2 + 3x + 2$ e si pone $g(x) \coloneqq 2^3 f(x/2) = x^4 + 3x^3 + 10x^2 + 12x + 16$. I coefficienti del polinomio monico ottenuto a partire da f sono molto più alti, quindi anche i limiti per gli algoritmi sono peggiori.

Esercizio 1.24. Fattorizzare sui razionali (senza usare gli algoritmi specifici per i razionali) il polinomio $f(x) \coloneqq 2x^6 + 7x^5 + 13x^4 + 16x^3 + 13x^2 + 7x + 2$. Provare poi sostituendo un parametro come coefficiente del termine di quarto grado.

1.14 Fattorizzazione nei campi finiti

22.03.2007

La fattorizzazione in $\mathbb{F}_{p^n}[x]$ non è molto diversa da quella in $\mathbb{F}_p[x]$, dato che il polinomio $x^{p^n} - x$ è uguale a $\prod_{s \in \mathbb{F}_{p^n}} (x - s)$. Sapendo questo, si può usare lo stesso algoritmo di Berlekamp che si usava su $\mathbb{F}_p[x]$. L'uguaglianza dei due polinomi si ottiene osservando che $a^{p^n - 1} = 1$ per ogni $a \in \mathbb{F}_{p^n}^\star$, cioè $a^{p^n} = a$ per ogni $a \in \mathbb{F}_{p^n}$. Allora ogni $a \in \mathbb{F}_{p^n}$ è radice di $x^{p^n} - x$.

Il problema nell'usare questo metodo è che $g(x)^{p^n} - g(x)$ può arrivare a gradi molto alti, e anche dividendo una prima volta per il polinomio da fattorizzare rimane una cosa spiacevole. Un algoritmo alternativo più efficiente è quello di Cantor-Zassenhaus, anche se ha il problema di essere probabilistico.

Se si vuole fattorizzare un polinomio a coefficienti in un'estensione algebrica di un campo finito, si osserva che $\mathbb{F}_{p^n}[\alpha] \cong \mathbb{F}_{p^n}[x]/(F(x))$, è ancora un campo finito

del tipo $\mathbb{F}_{p^k}$. La fattorizzazione allora si compie con gli stessi algoritmi che si usano nei campi finiti.

1.15 Estensioni algebriche

Definizione 1.25. Sia $F \subseteq K$ un'estensione di campi, $\alpha \in K$; α si dice algebrico su F se esiste $f \in F[x]$ tale che $f(\alpha) = 0$.

Alcuni fatti: gli elementi di K algebrici su F formano un campo; la chiusura algebrica di un campo esiste ed è unica (a meno di isomorfismi) e ha sempre cardinalità infinita; se $|K| = \infty$, allora $|K| = \left|\bar{K}\right|$. Da queste osservazioni si deduce che $\bar{\mathbb{Q}}$ è numerabile (ovviamente $\mathbb{Q}$ non è algebricamente chiuso). Si dimostra che $\bar{\mathbb{F}_p} = \bigcup_{k>0} \mathbb{F}_{p^k}$.

Si sa che $K[\alpha] \cong {}^{K[x]}\!/_{(p(x))}$, dove $p(x)$ è un qualsiasi polinomio irriducibile con α come radice; nell'isomorfismo, α corrisponde a $\bar{x}$. Di conseguenza, ogni elemento di $K[\alpha]$ può essere scritto nella forma $a_{d-1}\alpha^{d-1} + \cdots + a_0$, dove d è il grado di p. Altrimenti, essendo $K[\alpha]$ un K-spazio vettoriale, si può identificare l'elemento con la d-upla $(a_{d-1}, \ldots, a_0) \in K^d$.

Sia $\beta \in K[\alpha]$, si vuole trovare il polinomio minimo di β; le potenze di β appartengono a $K[\alpha]$, ma $K[\alpha]$ è uno spazio vettoriale di dimensione d, quindi $\beta^0, \ldots, \beta^d$ sono linearmente dipendenti su K. Sia $b_0\beta^0 + \cdots + b_d\beta^d = 0$ una relazione che realizza la dipendenza. I b_i si possono trovare tramite un sistema di equazioni lineari; allora il polinomio minimo di β divide $b_0 + \cdots + b_d x^d$.

Esempio 1.26. Sia $\mathbb{Z}_3[\alpha] = {}^{\mathbb{Z}_3[x]}\!/_{(x^3+2x+1)}$; si cerca il polinomio minimo di $\beta \coloneqq \alpha^2 + 1$. Si ottengono[2]

$$\begin{aligned} \beta^0 &= 1, & \beta^2 &= \alpha^4 + 2\alpha^2 + 1 = -\alpha + 1, \\ \beta^1 &= \alpha^2 + 1, & \beta^3 &= -\alpha^3 + \alpha^2 - \alpha + 1 = \alpha^2 + \alpha - 1. \end{aligned}$$

Perciò si cerca una combinazione lineare non banale del tipo

$$0 = b_0 + b_1(\alpha^2 + 1) + b_2(-\alpha + 1) + b_3(\alpha^2 + \alpha - 1),$$

che si trova[3] essere, per esempio, $(b_0, \ldots, b_3) = (1, -1, 1, 1)$.

All'interno di $K[\alpha]$, somma prodotto e differenza di elementi si fanno come tra i polinomi; l'inverso si fa tramite l'algebra lineare: si equaglia il prodotto del polinomio per un polinomio incognito a 1, risolvendo come un sistema dato che oltre un certo grado non si può andare.

Teorema 1.27. *Siano F un campo di caratteristica 0, α e β algebrici su F; allora esiste γ algebrico tale che $F(\alpha, \beta) = F(\gamma)$.*

Dimostrazione. Si considerano f e g polinomi minimi di α e β, con grado m e n. Si considera K, il campo di spezzamento di f e g. Si sa che esistono $a_1, \ldots, a_m, b_1, \ldots, b_n \in K$ radici dei polinomi f e g, ma gli a_i sono tutti distinti (i polinomi non square free nei campi di caratteristica 0 non sono irriducibili), così come i β_i. Si scrive $a_i + \lambda b_j \neq a_1 + \lambda b_1$: sicuramente esiste $\lambda \in K$ tale che questa disequazione è verificata per ogni $i \neq j$. Il resto della dimostrazione prova che $F(a_1 + \lambda b_1) = F(\alpha, \beta)$. □

[2] In `Cocoa` si utilizza la funzione `NR`$(f(x), [g_1(x), \ldots, g_r(x)])$, che dà un rappresentante canonico del primo polinomio rispetto ai secondi.

[3] In `Cocoa` si può usare `ReducedGBasis(Ideal`$(f_1, \ldots, f_k)$`)`.

Dal punto di vista computazionale, costruire il campo di spezzamento non è facile; però una volta ottenuto, il problema diventa banale: basta scegliere λ che eviti un numero finito di valori, cioè si sceglie casualmente λ, che con probabilità 1 andrà bene. Nel caso dei razionali, si hanno dei limiti sulle radici, quindi si può cercare un λ al di fuori del limite per $(a_i - a_j)/(b_j - b_i)$. Alternativamente, si può testare il λ scelto a caso, costruendo il polinomio minimo di $\alpha+\lambda\beta$ e verificando che abbia grado mn (se questo accade, necessariamente $F(\alpha + \lambda\beta) = F(\alpha, \beta)$, dato che c'è un contenimento e i gradi sono uguali). La complessità nel caso pessimo è di $\mathrm{O}(m^5n^5)$, ma nel caso medio questa si riduce molto perché il test deve essere eseguito una volta sola.

1.16 Calcolo del massimo comun divisore

04.04.2007

Esempio 1.28. Siano

$$A \coloneqq x^8 + x^6 - 3x^4 - 3x^3 + x^2 + 2x - 5, \qquad B \coloneqq 3x^6 + 5x^4 - 4x^2 - 9x + 21;$$

calcolando il massimo comun divisore di questi due polinomi con l'algoritmo euclideo, si trovano polinomi intermedi con gradi alti, cosa che peggiora notevolmente il costo dell'algoritmo. Lavorando in $\mathbb{Z}_5[x]$, si ottiene che $(A_5(x), B_5(x)) = 1$, quindi il massimo comun divisore in $\mathbb{Q}[x]$ è congruo a 1 modulo 5. Infine, poiché il coefficiente direttore del massimo comun divisore divide il coefficiente direttore di entrambi i polinomi, deve necessariamente essere $(A(x), B(x)) = 1$ in $\mathbb{Q}[x]$, altrimenti il coefficiente direttore dovrebbe essere ± 1 e il polinomio non sarebbe più uguale a 1 modulo 5.

L'idea quindi è quella di calcolare il massimo comun divisore in $\mathbb{Z}_p[x]$ per diversi primi p e ricostruire la soluzione con il teorema cinese del resto. Tuttavia ci sono dei problemi: per esempio, $(x+2, x-3) = 1$ in $\mathbb{Q}[x]$, ma $(x+2, x-3) = x - 2$ in $\mathbb{Z}_5[x]$.

Definizione 1.29. Dati $f, g \in \mathbb{Z}[x]$, si dice che $p \in \mathbb{Z}$ primo è *bad* rispetto a f e g se $\gcd(f_p, g_p) \neq \gcd(f, g)_p$.

Teorema 1.30. *Dati $f, g \in \mathbb{Z}[x]$, i primi bad sono in numero finito.*

Osservazione 1.31. La complessità media di questo algoritmo è polinomiale con esponente basso, anche se teoricamente, nel caso peggiore, la complessità è esponenziale.

1.17 Massimo comun divisore per polinomi multivariati

Gli anelli di polinomi multivariati non sono anelli euclidei, ma si possono pensare come $K[x_1, \ldots, x_n] \subseteq K(x_1, \ldots, x_{n-1})[x_n]$, cioè immersi in un anello euclideo, dove si può calcolare normalmente il massimo comun divisore.

Corollario 1.32 (al lemma di Gauss)**.** *Siano $f, g \in R[x]$, con R dominio di integrità. Allora la parte primitiva di* $\gcd(f, g)$ *è il* gcd *delle parti primitive, e così per il contenuto.*

Esempio 1.33. Se si hanno

$$A \coloneqq (y^2 - y - 1)x^2 + (y^2 - 2)x + (y^2 + y + 1),$$
$$B \coloneqq (y^2 - y + 1)x^2 - (y^2 + 2)x + (y^2 + y + 2)$$

si verifica lo stesso fenomeno visto in precedenza, se si calcola il massimo comun divisore con l'algoritmo euclideo.

Nel caso dei polinomi multivariati, si può valutare una variabile, cioè porre $y = a$ (che è equivalente a quozientare l'anello per $(y - a)$). Si ha in particolare che se $A = PQ$ in $K[x, y]$ allora $A = PQ$ in $K[x,y]/(y-a)$, ma non è vero il viceversa. In particolare, se $A(x, a)$ è irriducibile, allora lo è anche $A(x, y)$.

La complessità teorica di questo approccio è $\mathrm{O}(d^{2n+1}k^3)$, dove d è il massimo dei gradi e n il numero di variabili; però si dimostra che, valutando in numeri grandi, la probabilità di riuscire a fattorizzare è alta.

2 Basi di Gröbner

18.04.2007

2.1 Ordinamenti

Si lavora in $K[\underline{x}]$, un UFD dove si possono calcolare tutti i massimi comuni divisori. In particolare, si lavorerà con $K \in \{\mathbb{Q}, \mathbb{F}_{p^n}\}$. L'anello dei polinomi multivariati non è euclideo, ma ci si può chiedere se esiste qualcosa di simile alla divisione euclidea che si ha in $K[x]$. Per affrontare questo problema si deve avere un ordinamento dei termini.

Definizione 2.1. Si definisce $O(T^n)$, l'insieme degli ordinamenti totali su T^n : $= \{x_1^{\alpha_1} \cdots x_n^{\alpha_n}\}$ che siano compatibili con il prodotto.

Definizione 2.2. Se $\sigma \in O(T^n)$ è tale che $x_i > 1$ per ogni i, allora σ è detto *term-ordering*. L'insieme di questi σ si denota con $\mathrm{TO}(T^n)$.

Esempio 2.3. Si usano spesso i seguenti ordinamenti: lessicografico (Lex): $x > y > z$; DegLex: $t_1 > t_2$ se e solo se $\partial t_1 > \partial t_2$ o $\partial t_1 = \partial t_2$ e $t_1 > t_2$ lessicograficamente.

2.2 Rappresentanti canonici

In una variabile, esiste un rappresentante canonico per un elemento di $K[x]/(f(x))$, dato dalla divisione euclidea: se $g \in K[x]$, $g = qf + r$ e il rappresentante è r.

Esempio 2.4. Sia $g \coloneqq xy \in K[x, y]$ e sia $I \coloneqq (x - z)$. Allora $xy - y(x - z) = yz$. Però se si cambia ordinamento e si considera $I = (z - x)$, xy non si riduce, dato che la divisione viene fatta tra i termini di grado massimo: cambiando l'ordinamento è cambiato il rappresentante.

Esempio 2.5. Siano $g \coloneqq x^2y^2$, $I \coloneqq (x^2y + 1, xy^2 + 1)$; allora si può scrivere sia $g - y(x^2y + 1) = -y$ che $g - x(xy^2 + 1) = -x$: il rappresentante cambia a seconda della scelta della riduzione. Però se si scelgono come rappresentanti dell'ideale i polinomi $x - y$ e $y^3 + 1$, si può mostrare che si riesce a trovare, con il procedimento di riduzione, un rappresentante canonico per ogni polinomio.

2.3 Ordinamenti da matrici

Definizione 2.6. Si definisce la mappa $\log\colon T^n \to \mathbb{N}^n$ che associa al termine $\prod x_i^{\alpha_i}$ la n-upla $(\alpha_1, \ldots, \alpha_n)$ e la sua inversa $T\colon \mathbb{N}^n \to T^n$.

Definizione 2.7. Data una matrice $M \in \mathscr{M}_n(\mathbb{Z})$ con $\det M \neq 0$, si ha un ordinamento σ_M definito da $t_1 > t_2$ se e solo se $M \log t_1 > M \log t_2$ con l'ordinamento lessicografico.

Il σ_M così definito è un elemento di $O(T^n)$; in particolare, $\sigma_M \in \mathrm{TO}(T^n)$ se e solo se il primo elemento non nullo per ogni colonna di M è positivo.

Esempio 2.8. Ci si pone in $\mathbb{Q}[x, y, z]$; sia

$$M \coloneqq \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

allora $x^\alpha y^\beta z^\gamma >_{\sigma_M} x^a y^b z^c$ se e solo se $\alpha + \beta + \gamma > a + b + c$ (cioè $\partial f > \partial g$), o $\partial f = \partial g$ e $\alpha > a$, o $\partial f = \partial g$, $\alpha = a$ e $\gamma > c$. In particolare se $M = \left(\begin{smallmatrix} 1 & 1 \\ I_{n-1} & 0 \end{smallmatrix}\right)$, σ_M è l'ordinamento DegLex, mentre se $M = I_n$, σ_M è l'ordinamento Lex.

Osservazione 2.9. Matrici diverse possono dare lo stesso ordinamento: per esempio se si somma alla seconda riga la prima, l'ordinamento che ne segue è uguale.

Definizione 2.10. Si definisce l'ordinamento DegRevLex come l'ordinamento associato alla matrice $M = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -J_{n-1} \end{smallmatrix}\right)$, dove J_{n-1} è la matrice di dimensione $n-1$ con 1 sull'antidiagonale e 0 altrove.

Proposizione 2.11. *Sia $\sigma \in \mathrm{TO}(T^n)$; allora sono equivalenti:*

1. *σ è l'ordinamento Lex;*
2. *$f \in K[\underline{x}]$, $\mathrm{LT}_\sigma(f) \in K[x_i, \dots, x_n]$ implica $f \in K[x_i, \dots, x_n]$.*

Proposizione 2.12. *Sia $\sigma \in \mathrm{TO}(T^n)$ compatibile col grado; allora sono equivalenti:*

1. *σ è l'ordinamento DegRevLex;*
2. *$f \in K[\underline{x}]$ omogeneo, $\mathrm{LT}_\sigma(f) \in (x_i, \dots, x_n)$ allora $f \in (x_i, \dots, x_n)$.*

Osservazione 2.13. Si può definire il grado di un termine t come il prodotto della prima riga della matrice dell'ordinamento per $\log(t)$: per esempio, se la prima riga della matrice è $(1, 2, 4)$, allora $\partial x = 1$, $\partial y = 2$ e $\partial z = 4$. Analogamente si può definire il grado come la k-upla data dal prodotto delle prime k righe della matrice per il logaritmo del termine.

19.04.2007

Dato T^n, per ogni $M \in \mathscr{M}_n(\mathbb{Z})$ con $\det M \neq 0$, sia $\sigma_M \in O(T^n)$ dato da $t_1 >_{\sigma_M} t_2$ se e solo se $M(\log(t_1) - \log(t_2)) > 0$. La prima entrata non nulla di ogni colonna di M è maggiore di 0 se e solo se $\sigma_M \in \mathrm{TO}(T^n)$ se e solo se per ogni $i \in \{1, \dots, n\}$, $x_i > 1$.

Esempio 2.14. Si è visto l'ordinamento Lex, con $M = I_n$, l'ordinamento DegLex, con $M = \left(\begin{smallmatrix} 1 & 1 \\ I_{n-1} & 0 \end{smallmatrix}\right)$, l'ordinamento DegRevLex, con $M = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -J_{n-1} \end{smallmatrix}\right)$.

Esempio 2.15. Sia

$$M \coloneqq \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 2 & 3 & 2 \end{pmatrix}$$

e sia $t_1 \coloneqq x^2yz$. Si cercano i $t_2 \coloneqq x^a y^b z^c$ che siano non comparabili con t_1 rispetto a σ_M. Allora

$$M(\log(t_1) - \log(t_2)) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

cioè

$$M \begin{pmatrix} 2-a \\ 1-b \\ 1-c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

che dà come soluzioni, per esempio, $a = b = 1$, $c = 2$. Questo accade perché $\det M = 0$: se M fosse non singolare, l'unico termine non confrontabile con t_1 sarebbe t_1 stesso.

Osservazione 2.16. Sia $M \in \mathscr{M}_n(\mathbb{Z})$ con determinante non nullo. Se E è una matrice triangolare superiore con elementi sulla diagonale positivi, allora $\sigma_{EM} = \sigma_M$. Questo permette di semplificare la matrice di definizione dell'ordinamento, anche se spesso non è necessario.

Esercizio 2.17. Si suppone di avere una matrice generica. Si vuole un modo di rappresentare i termini in modo che sia efficiente l'operazione di confronto tra due polinomi, in particolare più efficiente che la moltiplicazione delle matrici.

2.4 Notazioni

Definizione 2.18. Sia $f = \sum c_i t_i \in A[\underline{x}]$, con A anello; siano i $t_i \in T^n$; il *supporto* di f è $\operatorname{Supp}(f) \coloneqq \{\, t_i \in T^n \mid c_i \neq 0 \,\}$. Il *leading term* di f è $\operatorname{LT}_\sigma(f) = \{\, t \in \operatorname{Supp}(f) \mid (\forall t' \in \operatorname{Supp}(f)) t' \leq t \,\}$; analogamente si definisce il *leading coefficient*, $\operatorname{lc}_\sigma(f)$ e il *leading monomial*, $\operatorname{LM}_\sigma(f)$. Dato un ideale $I \leq A[\underline{x}]$, si definisce $\operatorname{LT}_\sigma(I) \coloneqq (\{\, \operatorname{LT}_\sigma(f) \mid f \in I \,\})$.

Esempio 2.19. L'ideale $\operatorname{LT}_\sigma(I)$ non è facile da calcolare. Siano $I \coloneqq (x^2-1, y^2-1)$ e $J \coloneqq (x^2-1, y^2-1, xy+x)$ e sia σ l'ordinamento DegLex. Si ottiene che $\operatorname{LT}_\sigma(I) = (x^2, y^2)$, ma non è vero che $\operatorname{LT}_\sigma(J) = (x^2, y^2, xy)$, in quanto $y + 1 = (-y-1)(x^2-1) + x(xy+x)$, quindi $y \in \operatorname{LT}_\sigma(J)$. In particolare, non è possibile calcolare LT_σ a partire dai generatori dell'ideale. Il poterlo fare, come nel caso di I, è una prima caratterizzazione delle basi di Gröbner. Per esempio, $J = (x^2-1, y+1)$ e questa è una base di Gröbner. In particolare la cosa che dà fastidio in una base non di Gröbner è poter scrivere un elemento dell'ideale con una cancellazione dei termini di testa, in modo che il primo termine non nullo non sia contenuto nell'ideale generato dai termini di testa della base.

2.5 Notherianità

Per rappresentare un ideale nel calcolatore non ci sono problemi quando l'ideale è finitamente generato; si sa che $K[x]$ è un PID, quindi non pone problemi. Per $K[\underline{x}]$ si deve dimostrare che ogni ideale è finitamente generato.

Definizione 2.20. Sia A un anello; A si dice *noetheriano* se si verifica almeno una tra:

1. ogni successione crescente di ideali è stazionaria;

2. ogni insieme non vuoto di ideali di A, ammette un elemento massimale;

in particolare si dimostra che le due condizioni sono equivalenti.

Proposizione 2.21. *Sia A un anello; A è noetheriano se e solo se ogni suo ideale è finitamente generato.*

Dimostrazione. $\Rightarrow$ Sia I un ideale di A; per assurdo, se I non è finitamente generato, sia $\Sigma \coloneqq \{\, I' \subseteq I \mid I' \leq A \text{ finitamente generato} \,\}$; Σ è non vuoto in quanto $(0) \in \Sigma$, quindi esiste $I_0 \in \Sigma$ massimale. Si vuole dimostrare che $I = I_0$: per assurdo, sia $x \in I \setminus I_0$, allora $I_0 \subsetneq (I_0, x) \subseteq I$ ed è finitamente generato, assurdo.

$\Leftarrow$ Se si ha una catena $I_0 \subseteq I_1 \subseteq \cdots$ di ideali in A; si considera $I \coloneqq \bigcup I_i$: è un ideale di A, quindi è finitamente generato per ipotesi, cioè $I = (a_1, \ldots, a_k)$. Ognuno di questi elementi appartiene agli ideali della catena a partire da un certo indice; una volta che tutti i generatori appartengono alla catena, questa si è stabilizzata. □

Esempio 2.22. Tutti i PID sono noetheriani; se A e B sono noetheriani e $I \leq A$, $A \oplus B$ e A/I sono noetheriani.

Teorema 2.23 (della base di Hilbert)**.** *Se A è un anello noetheriano, allora $A[x]$ è notheriano. In particolare, $K[\underline{x}]$ è noetheriano.*

Dimostrazione. Sia $I \leq A[x]$ un ideale; si vuole dimostrare che è finitamente generato. Si pone $\sigma \in \mathrm{TO}(T^1)$ l'usuale ordinamento dei polinomi in una variabile, per grado. Sia $f_0 \in I$ un polinomio di grado minimale in I; ancora, sia $f_1 \in I \setminus (f_0)$ di grado minimale, e così via. Per assurdo, se I non è finitamente generato, si può costruire in questo modo una successione infinita in I e una corrispondente successione $(a_0 \coloneqq \mathrm{lc}_\sigma(f_0), \ldots)$ in A. Come ideale, questo è uguale a $(a_0, \ldots, a_k)$ per un certo k, poiché A è noetheriano.

Si considera f_{k+1}: $a_{k+1} = \sum b_i a_i$ perché $a_{k+1} \in (a_0, \ldots, a_k)$ e si pone $g \coloneqq f_{k+1} - \sum b_i x^{\gamma_i} f_i \in I \setminus (f_0, \ldots, f_k)$, con i γ_i appropriati in modo che si abbia la cancellazione del termine di testa di g, cioè $\gamma_i = (\partial f_{k+1} - \partial f_i)$. Quindi $\partial g < \partial f_{k+1}$, assurdo per la minimalità di f_{k+1}. □

Corollario 2.24. *L'ideale $\mathrm{LT}_\sigma(I)$ è finitamente generato per ogni ideale I; un ideale monomiale J di $K[\underline{x}]$ è finitamente generato da termini.*

Si dimostra che anche $K[[\underline{x}]]$ è noetheriano. Esistono anche anelli non noetheriani, come per esempio $K[x_1, \ldots]$.

2.6 Basi di Gröbner

Si cerca di caratterizzare delle basi di ideali di $K[\underline{x}]$ in modo che vengano agevolate le computazioni.

Proposizione 2.25. *Siano $I \leq K[\underline{x}]$ un ideale non nullo, $X = (f_1, \ldots, f_k)$ una lista di elementi di I non nulli e $\sigma \in \mathrm{TO}(T^n)$; allora sono equivalenti (condizioni A):*

1. *per ogni $f \in I$ non nullo, esistono $g_1, \ldots, g_k \in K[\underline{x}] \setminus \{0\}$ tali che $f = \sum g_i f_i$ e $\mathrm{LT}_\sigma(f) \geq \mathrm{LT}_\sigma(f_i)\,\mathrm{LT}_\sigma(g_i)$ per ogni i;*

2. *per ogni* $f \in I$ *non nullo, esistono* $g_1, \ldots, g_k \in K[\underline{x}] \setminus \{0\}$ *tali che* $f = \sum g_i f_i$ *e* $\mathrm{LT}_\sigma(f) = \max\{\mathrm{LT}_\sigma(f_i)\,\mathrm{LT}_\sigma(g_i)\}$.

Un sistema di generatori che soddisfa le condizioni si dice base di Gröbner *di* I. *Le condizioni sopra sono equivalenti anche alle due seguenti (condizioni B):*

1. $\mathrm{LT}_\sigma(I) = (\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_k))$;
2. *la stessa cosa come monoidi in* T^n.

26.04.2007

Lemma 2.26. *Sia* $\underline{x}^{\underline{\alpha}_1} \geq \underline{x}^{\underline{\alpha}_2} \geq \cdots$ *una successione decrescente di elementi di* T^n. *Allora la successione è definitivamente stazionaria.*

Dimostrazione. La dimostrazione è una conseguenza del teorema della base di Hilbert: sia $I \coloneqq (\underline{x}^{\underline{\alpha}_1}, \underline{x}^{\underline{\alpha}_2}, \ldots)$; per il teorema della base, esistono $i_1 \geq \cdots \geq i_k$ tali che $I = (\underline{x}^{\underline{\alpha}_{i_1}}, \ldots, \underline{x}^{\underline{\alpha}_{i_k}})$. Se $\underline{x}^{\underline{\alpha}_j}$ è un elemento della successione con $j > i_k$ (da cui $\underline{x}^{\underline{\alpha}_j} \leq \underline{x}^{\underline{\alpha}_{i_k}}$), allora $\underline{x}^{\underline{\alpha}_j} \in I$, perciò $\underline{x}^{\underline{\alpha}_j} = \sum f_{i_t} \underline{x}^{\underline{\alpha}_{i_t}}$; ma allora ogni termine della somma moltiplica un generatore, e tutti i generatori sono maggiori o uguali a $\underline{x}^{\underline{\alpha}_j}$, che di conseguenza non può essere strettamente minore di $\underline{x}^{\underline{\alpha}_{i_k}}$. □

Esempio 2.27. Siano $f \coloneqq x^5y^3$ e $A \coloneqq \left\{ x^\alpha y^\beta \in T^2 \mid x^\alpha y^\beta \leq_\sigma x^5y^3 \right\}$; se σ è DegLex, $|A| < \infty$, però se è Lex questo non è più vero, la cardinalità di A può essere infinita. Il lemma assicura che una catena discendente deve essere finita. Questo è cruciale per le procedure che lavorano riducendo il termine di testa a ogni passo (come per esempio la divisione): il lemma assicura che la procedura termini.

Proposizione 2.28. *Le condizioni A e B viste in precedenza sono equivalenti.*

Definizione 2.29. Siano E un insieme, $r \subseteq E \times E$ una relazione su E; la *chiusura riflessiva transitiva* di r è la relazione che associa gli elementi f e g se e solo se esiste una catena di elementi (eventualmente vuota) che parte da f e arriva a g e tali che ogni coppia successiva è il relazione tramite r; si indica con $f \to g$. La *chiusura di equivalenza* di r è una relazione che associa f e g se e solo se esiste una successione di elementi che parte da f e arriva a g e tale che ogni coppia successiva di elementi (in un qualche ordine) è in relazione per la chiusura riflessiva transitiva di r e si indica $f \leftrightarrow g$.

Proposizione 2.30. *Siano* $f, g, r, s \in K[\underline{x}]$ *e si denotino con* $\to$ *e* $\leftrightarrow$ *rispettivamente la chiusura riflessiva transitiva e di equivalenza di* $\xrightarrow{(f_1,\ldots,f_k)}$, *che indica una riduzione mediante i polinomi* $f_1, \ldots, f_k$. *Allora:*

1. $0 \to f$ *implica* $f = 0$;
2. $f \to g$ *implica* $tf \to tg$ *per ogni* $t \in T^n$;
3. *se* $f \to g$ *e* $g \to f$ *allora* $f = g$;
4. *se* $f \xrightarrow{f_1} g$, *allora per ogni* $r \in K[\underline{x}]$ *esiste* $h \in K[\underline{x}]$ *tale che* $f + r \to h$ *e* $g + r \to h$;
5. *se* $f \leftrightarrow g$ *e* $r \leftrightarrow s$ *allora* $f + r \leftrightarrow g + s$;
6. *se* $f \leftrightarrow g$ *allora* $hf \leftrightarrow hg$ *per ogni* $h \in K[\underline{x}]$;

7. $\to$ *è noetheriana;*

8. *se* $\mathscr{F} \coloneqq \{f_1, \dots, f_k\} \subseteq K[\underline{x}] \setminus \{0\}$ *allora:*

   (a) $f \in (\mathscr{F}) \Leftrightarrow f \leftrightarrow 0$*;*

   (b) $f - g \in (\mathscr{F}) \Leftrightarrow f \leftrightarrow g$*.*

Dimostrazione. I primi punti si dimostrano facilmente. Se $f \overset{\mathscr{F}}{\longleftrightarrow} 0$, allora esiste una successione $h_1, \dots, h_n$ che comincia in f e termina in 0 con frecce orientate arbitrariamente. Per induzione, partendo da 0, se dopo la i-esima freccia si arriva a un polinomio $h_i \coloneqq \sum_{j=1}^{i} c_j t_j f_{k_j} \in (\mathscr{F})$, ci sono due possibilità: se $h_{i-1} \to h_i$, allora $h_i = h_{i-1} - c_i t_i f_{k_i}$ e $h_{i-1} = h_i + c_i t_i f_{k_i} \in (\mathscr{F})$; altrimenti se $h_{i-1} \leftarrow h_i$, si ha $h_{i-1} = h_i - c_i t_i f_{k_i} \in (\mathscr{F})$; di conseguenza se $f \to 0$, $f \in (\mathscr{F})$; il viceversa è ovvio. □

Proposizione 2.31. *Siano* $\mathscr{F} = \{f_1, \dots, f_k\} \subseteq K[\underline{x}] \setminus \{0\}$, $\sigma \in \mathrm{TO}(T^n)$, $f, g \in K[\underline{x}]$*. Allora sono equivalenti:*

1. $f \in (\mathscr{F})$ *se e solo se* $f \to 0$*;*

2. f *è irriducibile secondo* $\mathscr{F}$ *e* $f \in (\mathscr{F})$ *implica* $f = 0$*;*

3. *per ogni* $g \in K[\underline{x}]$*, esiste unico* $h \in K[\underline{x}]$ *irriducibile tale che* $g \to h$*;*

4. $\to$ *è* confluente *(cioè se* $f \to h_1$ *e* $f \to h_2$ *allora esiste* h *tale che* $h_1 \to h$ *e* $h_2 \to h$*).*

Inoltre queste condizioni equivalenti (condizioni C) sono equivalenti alla definizione di base di Gröbner.

2.7 Criterio di Buchberger

Definizione 2.32. Siano $f, g \in K[\underline{x}]$, $\sigma \in \mathrm{TO}(T^n)$ e $t \coloneqq \gcd(\mathrm{LT}_\sigma(f), \mathrm{LT}_\sigma(g))$, allora

$$S(f,g) = \frac{\mathrm{LT}_\sigma(g)}{\mathrm{LC}_\sigma(f)t} f - \frac{\mathrm{LT}_\sigma(f)}{\mathrm{LC}_\sigma(g)t} g$$

è l'*S-polinomio* di f e g.

Esempio 2.33. Dati $f \coloneqq x^2 - 1$ e $g \coloneqq y^2 - 1$,

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

Se $f \coloneqq xy^2 - 1$ e $g \coloneqq x^2 y - 1$, $S(f,g) = -x + y$. Il costo per calcolare l'S-polinomio è ridotto.

Teorema 2.34 (Criterio di Buchberger)**.** *Sia* $G \coloneqq \{g_1, \dots, g_t\} \subseteq K[\underline{x}] \setminus \{0\}$*; allora sono equivalenti:*

1. G *è una base di Gröbner;*

2. $S(g_i, g_j) \xrightarrow{G} 0$ *per ogni* $i < j$*.*

Esercizio 2.35. Se $\mathrm{LT}_\sigma(g_i)$ sono a due a due coprimi, allora $S(g_i, g_j) \xrightarrow{G} 0$.

Osservazione 2.36. Genericamente, un insieme di generatori non sono una base di Gröbner: infatti i coefficienti dei polinomi generatori devono soddisfare una condizione algebrica, quindi devono essere in un chiuso di Zariski.

Se $S(g_i, g_j) \to g$, l'idea di Buchberger è di aggiungere g nell'insieme di generatori. Si deve capire però se questo procedimento termina, dato che aggiungendo h si devono calcolare un numero lineare di nuovi S-polinomi. In effetti, ha termine per il teorema della base di Hilbert: la successione di ideali ascendente $I_i \coloneqq (\mathrm{LT}_\sigma(g_1), \dots, \mathrm{LT}_\sigma(g_t), \mathrm{LT}_\sigma(h_1), \dots, \mathrm{LT}_\sigma(h_i))$, deve stabilizzarsi, cioè a un certo punto non si riuscirà più a produrre un S-polinomio che non si riduca a 0.

Esempio 2.37. Sia $G \coloneqq \{g_1 \coloneqq x^2 - 1, g_2 \coloneqq y^2 - 1, g_3 \coloneqq xy + x\}$; si pongono $B \coloneqq \varnothing$ la base finora calcolata e $P \coloneqq ((1,2),(1,3),(2,3))$ le coppie di cui fare l'S-polinomio. La prima coppia si riduce a 0 perché le teste sono coprime; $S(g_1, g_3) = y(x^2 - 1) - x(xy + x) = -x^2 - y$ (ma si può cambiare il segno a tutto e considerare $x^2 + y$). Riducendo questo polinomio si ottiene $x^2 + y \to x^2 + y - (x^2 - 1) = y + 1$, che è irriducibile e non nullo: si aggiunge come g_4, aggiungendo le coppie $((1,4),(2,4),(3,4))$ a P. Ora, $g_2, g_3 \xrightarrow{g_4} 0$, perché g_4 li divide entrambi; d'altra parte anche $(1,4)$ si riduce a 0 per la coprimalità delle teste. Quindi si ha concluso.

Prima di iniziare, si può provare a ridurre ogni polinomio generatore con gli altri, per abbassare la complessità.

L'algoritmo è anche molto sensibile all'ordine con cui vengono valutate le coppie e importante è anche riuscire a trovare dei criteri per sapere a priori se una coppia si riduce a 0. Uno dei metodi è appunto la coprimalità dei termini di testa; ne esiste uno cambinatorio sui termini di testa molto efficace in pratica.

Osservazione 2.38. Se g_1 e g_2 sono polinomi omogenei, allora $S(g_1, g_2)$ è omogeneo e $\partial S(g_1, g_2) \geq \partial g_1, \partial g_2$. Se G è composto da polinomi omogenei, allora la riduzione di g omogeneo tramite G è un polinomio omogeneo h e $\partial g = \partial h$ (o $h = 0$). Queste osservazioni permettono di ottimizzare l'algoritmo di Buchberger, valutando le coppie per grado.

09.05.2007

Dimostrazione del criterio di Buchberger. $\Rightarrow$ Per la definizione di base di Gröbner.

$\Leftarrow$ Se $S_{i,j}$ si riduce a 0, allora $S_{i,j} = \sum h_k^{i,j} g_k$ e inoltre per ogni k,

$$\mathrm{LT}(h_k^{i,j} g_k) \leq \mathrm{LT}(S_{i,j}) < \frac{\mathrm{LT}(g_i)\,\mathrm{LT}(g_j)}{\mathrm{gcd}_{i,j}},$$

dove $\mathrm{gcd}_{i,j} \coloneqq \mathrm{gcd}(\mathrm{LT}(g_i), \mathrm{LT}(g_j))$. Per assurdo, si suppone che G non sia una base di Gröbner; allora esiste $f \in I$ tale che $\mathrm{LT}(f) \notin (\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t))$. In particolare, $f = \sum f_k g_k$ perché G è comunque un sistema di generatori e i termini di testa di quella somma si cancelleranno a vicenda.

Sia $T = \max\{\mathrm{LT}(f_k)\,\mathrm{LT}(g_k)\}$ e si scelga la scrittura $f = \sum f_k g_k$ in modo tale che T e il numero di occorrenze di T nella scrittura siano minimali (con precedenza a T). Per costruzione, esistono almeno due addendi della somma che ammettono T come termine di testa, perché si devono cancellare a vicenda. Siano i e j due degli indici che hanno come termine di

testa T. Allora

$$\mathrm{LT}(f_i) = \frac{\mathrm{LT}(f_j)\,\mathrm{LT}(g_j)}{\mathrm{LT}(g_i)} \Rightarrow \frac{\mathrm{LT}(g_j)}{\gcd_{i,j}} \mid \mathrm{LT}(f_i) \Rightarrow \mathrm{LM}(f_i) = cT'' \frac{\mathrm{LT}(g_j)}{\gcd_{i,j}}.$$

Si vuole ottenere ora una scrittura di f che violi la minimalità. Si scrive $f = \sum f_k g_k = \sum f_k g_k - cT''(S_{i,j} - \sum h_k^{i,j} g_k)$; raccogliendo i g_k, si ha $f = \sum u_k g_k$. In particolare,

$$\begin{aligned} u_i &= f_i - cT'' \left(\frac{\mathrm{LT}(g_j)}{\gcd_{i,j}} + h_i^{i,j} \right) \\ u_j &= f_j - cT'' \left(\frac{\mathrm{LT}(g_i)}{\gcd_{i,j}} + h_j^{i,j} \right) \\ u_v &= f_v - cT'' h_v^{i,j}. \end{aligned}$$

Il numero di volte in cui T compare diminuisce di due, quindi si sta violando la minimalità, dato che o dimuniscono il numero di occorrenze o diminuisce T se quelle erano le ultime due occorrenze. □

Esempio 2.39. Siano $f_1 \coloneqq x+y+z+9$, $f_2 \coloneqq x^5 - y^3 + z$, $f_3 \coloneqq x^2z^5 + xz^3 + 1$ e sia $I \coloneqq (f_1, f_2, f_3)$. Se si calcola la base di Gröbner di I rispetto all'ordinamento Lex, si ottengono sempre tre polinomi, del tipo $z^{31} + g_1(z)$, $y + g_2(z)$, $x + g_3(z)$ e con i coefficienti dei polinomi molto alti.

Esempio 2.40. Sia $C(3)$ il terzo ideale ciclico: $(x+y+z, xy+yz+zx, xyz-1)$. Con l'ordinamento DegRevLex, per trovare una base di Gröbner $C(4)$ ci si impiega un centesimo di secondo; per $C(6)$ ci si impiega mezzo secondo; per $C(9)$ cinque ore; per $C(10)$ un giorno e l'output è maggiore di un GigaByte.

In generale, e nello specifico per gli ideali ciclici, Lex è l'ordinamento che dà i risultati peggiori, cioè più grandi. Sempre in generale, su $\mathbb{Q}$ è più difficile calcolare i risultati che non in $\mathbb{Z}_p$. Ci sono esempi in cui i risultati che si ottengono lavorando sui razionali sono diversi, ma se si evitano polinomi particolari, il risultato è lo stesso che in $\mathbb{Z}_p$.

3 Usi delle basi di Gröbner

3.1 Appartenenza a un ideale

Le basi di Gröbner sono utili in molti problemi: per verificare $f \in I$, basta calcolare la base di Gröbner di I e provare a ridurre f secondo la base: se si riduce a 0, allora $f \in I$, altrimenti no.

Esempio 3.1. Si provi a verificare se $x^3y^2 + x^2y^3 + x^3y - x^2y^2 - 2xy \in (x^2y - 1, xy^2 - 1) =: I$. Una base di Gröbner dell'ideale è $(x-y, y^3-1)$. Ora, ${}^{K[x,y]}/_{I} = {}^{K[y]}/_{(y^3-1)}$, quindi $\bar{f} = y^2 + y^2 + y - y - 2y^2 = 0$, cioè $f \in I$.

3.2 Aritmetica nel quoziente di un anello polinomiale

Si può semplificare l'aritmetica in ${}^{K[\underline{x}]}/_{I}$, semplicemente considerando il rappresentante canonico alla fine di ogni operazione. *10.05.2007*

Si possono usare le basi di Gröbner per analizzare ${}^{K[\underline{x}]}/_{I}$ come K-spazio vettoriale.

Esempio 3.2. Si considera ${}^{K[x,y]}/_{I}$, con $I \coloneqq (x^2y-1, xy^2-1) = (y-x, y^3-1)$: grazie alla base di Gröbner si è riusciti a capire che quello spazio vettoriale ha dimensione finita e che ogni suo elemento si può scrivere come ay^2+by+c con $a, b, c \in K$.

Definizione 3.3. Dato $I \leq K[\underline{x}]$ con l'ordinamento σ, si definisce $N_\sigma(I) \coloneqq T^n \setminus \mathrm{LT}_\sigma(I)$.

Esempio 3.4. Nell'esempio precedente, se σ è DegRevLex, $\mathrm{LT}_\sigma(I) = (x, y^3)$. Si possono prendere i punti in $\mathbb{N}^2$ come $(a, b) \to x^a y^b$. Se si escludono i termini di testa e tutti i punti più in alto o più a destra dei termini di testa, quello che resta sono i termini che danno una base per lo spazio vettoriale quoziente, cioè $N_\sigma(I) = \{1, y, y^2\}$.

Proposizione 3.5. *Sia I un ideale non nullo di $K[\underline{x}]$. Allora $N_\sigma(I)$ è una base di ${}^{K[\underline{x}]}/_{I}$ come K-spazio vettoriale, per ogni $\sigma \in \mathrm{TO}(T^n)$. Inoltre è anche una base come K-spazio vettoriale di ${}^{K[\underline{x}]}/_{\mathrm{LT}_\sigma(I)}$ per ogni $\sigma \in \mathrm{TO}(T^n)$.*

Dimostrazione. Sicuramente gli elementi di $N_\sigma(I)$ generano, perché ogni f nel quoziente può essere ridotto a un f' che non contiene termini contenuti nell'ideale dei termini di testa.

Inoltre per le proprietà delle basi di Gröbner gli elementi di $N_\sigma(I)$ sono tutti irriducibili, quindi non possono essere ridotti l'uno all'altro. □

Corollario 3.6. *Mentre $N_\sigma(I)$ dipende da σ, la sua cardinalità è indipendente da σ, poiché è la dimensione del K-spazio vettoriale quoziente.*

Esempio 3.7. Sia $I \coloneqq (xy^3 - x^2, x^3y^2 - y)$; sia σ DegRevLex, allora $\mathrm{LT}_\sigma(I) = (x^3y^2, x^4, xy^3, y^4)$, mentre posto τ Lex, $\mathrm{LT}_\tau(I) = (y, x^{12})$. In entrambi i casi una base è composta da 12 elementi. I diagrammi che risultano considerando $\mathbb{N}^2$ si dicono *diagrammi a scala*. Si dimostra che la scala è chiusa se e solo se lo spazio vettoriale ha dimensione finita se e solo se il sistema associato all'ideale ha un numero finito di soluzioni (che contate con molteplicità nella chiusura algebrica, sono tante quante gli elementi di $N_\sigma(I)$).

Proposizione 3.8. *Siano f, g omogenei standard[4] in $K[\underline{x}]$ con l'ordinamento σ; allora sicuramente $S(f, g)$ è omogeneo. Inoltre se $F = \{f_1, \ldots, f_k\} \subseteq K[\underline{x}]$, con f_i omogenei, e si ha che $f \xrightarrow{F} h$, allora h è omogeneo dello stesso grado.*

Questa proposizione permette di dire che se si ordinano le coppie per grado, nell'algoritmo di Buchberger con ideali omogenei, l'S-polinomio ha grado maggiore o uguale dei polinomi di partenza (in realtà si dimostra che è strettamente maggiore) e riducendolo si ottiene o 0 o un polinomio dello stesso grado: si può lavorare quindi grado per grado, con la sicurezza che elaborando i polinomi di un certo grado non si produrranno polinomi di grado inferiore, anzi, solo eventuali polinomi di grado maggiore. Se si sa anche qualcosa della struttura grado per grado di ${}^{K[\underline{x}]}/_{I}$ (cioè, relazioni sulle dimensioni delle componenti omogenee), si possono sapere quante riduzioni diverse da 0 si otterranno in un certo grado, quindi una volta trovate tutte si possono evitare calcoli inutili e passare al grado successivo.

[4] Un polinomio f si dice omogeneo standard se e solo se per ogni $t \in \mathrm{Supp}(f)$, $\log(t) \cdot (1, \ldots, 1)$ è costante.

3.3 Basi di Gröbner ridotte e uguaglianza di ideali

Definizione 3.9. Sia $G = \{g_1, \ldots, g_k\} \subseteq K[\underline{x}]$; G si dice *minimale* se $(G) \neq (G \setminus \{g_i\})$ per ogni i.

Dato un insieme di polinomi, il primo passo per trovare un sottoinsieme minimale è quello di provare a ridurre ogni polinomio per i rimanenti; se si riduce a 0, sicuramente si può eliminare, ma potrebbe ridursi a 0 mediante gli S-polinomi dei rimanenti polinomi. In generale, il problema di trovare un sottoinsieme minimale è difficile. Nel caso omogeneo, però, se σ è grado-compatibile (esiste una matrice che lo descrive la cui prima riga è formata da 1), si possono ordinare per grado i generatori $f_1, \ldots, f_k$; si suppone di avere già calcolato la base di Gröbner fino al grado d e che $f_1, \ldots, f_j$ siano i polinomi di grado inferiore o uguale a d. Un elemento di grado $d+1$ se appartiene all'ideale, si riduce a 0 con i polinomi $f_1, \ldots, f_j$ uniti eventualmente ad altri polinomi di grado $d+1$. In sostanza, quello che non si riduce a 0 né per $f_1, \ldots, f_j$ né per gli altri polinomi di grado $d+1$ è parte di una base minimale.

Si sa che con le basi di Gröbner diventa facile il problema di decidere $f \in I$; si valuta ora il problema $I = J$. Si può affrontare prendendo dei generatori di I e riducendoli per una base di Gröbner di J e verificando che si riducano a 0, e poi viceversa. Si vorrebbe però avere una base di Gröbner "canonica", in modo da poter verificare $I = J$ solo guardando le basi. In generale, la base di Gröbner dipende da molte cose. La base di Gröbner ridotta però dipende solo dall'ordinamento.

Definizione 3.10. Se I è un ideale non nullo e $G \coloneqq \{g_1, \ldots, g_k\}$ è una base di Gröbner di I rispetto a σ. Allora G si dice base di Gröbner ridotta se:

1. G è ridotta come insieme di polinomi;
2. $\mathrm{LC}_\sigma(g_i) = 1$ per ogni i.

Proposizione 3.11. *La base di Gröbner di un ideale, dato l'ordinamento, esiste ed è unica.*

Dimostrazione. L'esistenza è ovvia. Siano $(g_1, \ldots, g_k)$ e $(h_1, \ldots, h_t)$ basi di Gröbner ridotte di I ordinate in modo crescente per leading term; allora $\mathrm{LT}(I) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_k)) = (\mathrm{LT}(h_1), \ldots, \mathrm{LT}(h_t))$; ma $\mathrm{LT}(I)$ è un ideale monomiale, ed è facile vedere che allora $t = k$ e $\mathrm{LT}(g_i) = \mathrm{LT}(h_i)$. A questo punto, $h_1 \in I$, quindi anche $h_1 - g_1 \to 0$ tramite $(g_1, \ldots, g_k)$; ma i termini di testa si cancellano e non ci sono riduzioni possibili, perciò $h_1 = g_1$; per mostrare che $h_i = g_i$, si dice ancora che $h_i - g_i \to 0$; di conseguenza, se $h_i \neq g_i$, allora il termine di testa si ridurrebbe tramite un $h_j = g_j$ con $j < i$; ma il termine di testa sta o in h_i o in g_i, assurdo per la minimalità delle basi di Gröbner. □

3.4 Eliminazione

Esempio 3.12. Si lavora in $K[x_1, \ldots, x_5]$ con l'ordinamento

$$\sigma \coloneqq \begin{pmatrix} 1 & 1 & & 0 & \\ 0 & 1 & & & \\ & & 1 & 1 & 1 \\ & 0 & 0 & 0 & 1 \\ & & 0 & 1 & 0 \end{pmatrix}.$$

La matrice corrisponde a un ordimento di eliminazione per x_1 e x_2: un termine nelle ultime tre variabili è sicuramente più piccolo di un termine che coinvolge una delle prime due.

Dato un ideale $I \leq K[\underline{x}, \underline{y}]$, si vuole conoscere l'ideale $I \cap K[\underline{y}]$. Si dimostra che una base di Gröbner dell'intersezione è data dall'intersezione di una base di Gröbner di I con $K[\underline{y}]$, se σ è un ordinamento di eliminazione per $\underline{x}$.

Esempio 3.13. Dati $I \coloneqq (x^3 - t^3, y^5 - t^5, z^7 - t^7)$, σ di eliminazione per t, allora si cerca $I \cap K[x, y, z]$ (si sta semplicemente passando da una descrizione parametrica di una varietà a una descrizione cartesiana). L'intersezione di una base di Gröbner con $K[x, y, z]$ dà $(y^{10} - x^3z^7, x^{12} - y^5z^7, z^{14} - x^9y^5)$. La varietà associata a $I \coloneqq (x - t^3, y - t^5, z - t^7)$ è la stessa (a meno di ricambiare le variabili alla fine), solo che lavorando con ideali omogenei generalmente si semplifica la complessità (oppure si poteva lavorare con il secondo ideale con i gradi $(3, 5, 7, 1)$).

3.5 Varietà

Si vuole risolvere il problema di verificare se un sistema ha soluzioni (o equivalentemente $\mathrm{V}(I) \neq \varnothing$). Si può dimostrare che se K è algebricamente chiuso, non esistono soluzioni se e solo se esiste un ordinamento per cui 1 appartiene alla base di Gröbner di I.

Dati i generatori di I e di J, si vorrebbero trovare dei generatori per gli ideali $\mathrm{I}(\mathrm{V}(I) \cap \mathrm{V}(J))$, $\mathrm{I}(\mathrm{V}(I) \cup \mathrm{V}(J))$, $\mathrm{I}(\mathrm{V}(I) \setminus \mathrm{V}(J))$. Il primo è semplicemente dato da $\mathrm{I}\,\mathrm{V}(I + J)$, il secondo da $I \cap J$, il terzo da $I : J^\infty$.

Proposizione 3.14. *Siano I, J ideali; allora, se $J = (f_1, \ldots, f_k)$:*

1. $I : J^\infty = \bigcap_{i=1}^k I : (f_i)^\infty$;
2. $I : (f)^\infty = (I, tf + 1) \cap K[\underline{x}]$;
3. $I \cap J = (tI, (t + 1)J) \cap K[\underline{x}]$.

Esempio 3.15. Sia $I \coloneqq (y - x) \cap (x, y)^2$ (una retta con un punto triplo). Si ha $I : (y - x)^\infty = (x, y)^2$ e $I : (x, y)^\infty = (y - x)$.

Sia $I \coloneqq (x, y) \cap (y, z)$: allora $I = (t(x, y), (t + 1)(y, z)) \cap K[x, y, z] = (tx, ty, ty + y, tz + z) \cap K[x, y, z] = (y, xz)$.

Si può dimostrare che se I e J sono omogenei, allora $I \cap J$ e $I : J^\infty$ sono omogenei. Questo si può dimostrare direttamente, ma è anche chiaro dalle costruzioni mostrate sopra. Basta sostituire 1 con una variabile aggiuntiva h e considerare una base di Gröbner rispetto a un ordinamento di riduzione per t e h.

3.6 Graduazioni non standard

Una graduazione si dice grado-compatibile se la prima riga della sua matrice è composta da 1. Se su $K[x, y, z]$ si prende l'ordinamento

$$\sigma \coloneqq \begin{pmatrix} 2 & 2 & 3 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

e si dichiara che il grado di un monomio è dato dalla prima riga, allora i polinomi omogenei saranno, per esempio, $x^3 + y^3 + z^2$. Ci sono graduazioni che non ammettono termini di un certo grado (per esempio se la prima riga è fatta solo da numeri pari). Per testare se un polinomio è omogeneo o per trovare una matrice in cui un polinomio sia omogeneo, si usa solo l'algebra lineare. Si possono anche considerare graduazioni date dalle prime due righe della matrice, piuttosto che dalla prima. In questo caso, dato che le condizioni per l'omogeneità sono due, i polinomi omogenei sono in numero minore.

4 Moduli

16.05.2007

4.1 Introduzione

Definizione 4.1. Siano M un gruppo abeliano, A un anello (commutativo con identità); M si dice *A-modulo* se esiste un'applicazione $A \times M \to M$ che associa am alla coppia (a, m) e tale che:

1. $a(m + n) = am + an$;
2. $(a + b)m = am + bn$;
3. $(ab)m = a(bm)$;
4. $1m = m$.

Esempio 4.2.
1. $\mathbb{R}^n$ è un $\mathbb{R}$-modulo;
2. un gruppo abeliano G è uno $\mathbb{Z}$-modulo;
3. $K[\underline{x}]$ è un K-modulo;
4. $K[\underline{x}, \underline{y}]$ è un $K[\underline{x}]$-modulo;
5. un ideale di A è un A-modulo.

Definizione 4.3. Un A-modulo M è detto *libero* (finitamente generato) se $M \cong A^n$ per qualche $n \in \mathbb{N}$.

Definizione 4.4. Siano M e N degli A-moduli; $\varphi\colon M \to N$ è detta *lineare* se $\varphi(\lambda m + \mu n) = \lambda\varphi(m) + \mu\varphi(n)$.

Definizione 4.5. Un *A-sottomodulo* di un A-modulo M è un sottogruppo di M chiuso rispetto alla moltiplicazione.

Dati due A-moduli M e N, alcune operazioni standard che si vogliono rendere efficienti sono l'intersezione $M \cap N$ e le divisioni del tipo

$$M :_A N \coloneqq \{\, f \in A \mid fN \subseteq M \,\},$$
$$M :_N I \coloneqq \{\, n \in N \mid nI \subseteq M \,\}.$$

4.2 Algoritmo di Buchberger per moduli

Dato $M \subseteq N = K[\underline{x}]^s$, si vuole costruire una base di Gröbner di M rispetto a un ordinamento τ su $T^n(M)$. Per costruirla, si immergerà il modulo M in un anello, precisamente $K[\underline{x}, y_1, \ldots, y_s]$, associando a gli elementi della base e_i le variabili y_i. In questo modo, si ha un isomorfismo sull'immagine; si vorrebbe avere però un isomorfismo ordinato, cioè tale che se $v_1 >_\tau v_2$ allora $\varphi(v_1) >_{\tau'} \varphi(v_2)$.

Definizione 4.6. Un *ordinamento* del modulo $K[\underline{x}]^s$ è un ordinamento τ tale che:

1. $\tau_{|K[\underline{x}]} \in \mathrm{TO}(T^n)$;
2. τ è costante quando ristretto alle varie coordinate;
3. τ soddisfa le usuali regole degli ordinamenti.

Esempio 4.7. Si considera $K[x, y]^3$ e l'ordinamento PosDegLex: significa che ristretto a ogni coordinata è l'ordinamento DegLex e prima di tutto conta che la coordinata i è maggiore della coordinata j per ogni $i < j$.

Definizione 4.8. Si definisce $MT^n \coloneqq \{\, te_i \mid t \in T^n \,\}$, dove e_i è un vettore della base canonica.

Esempio 4.9. Se σ è l'ordinamento DegLex, la matrice di PosDegLex è $\left(\begin{smallmatrix} 0 & I \\ M_\sigma & 0 \end{smallmatrix}\right)$; la matrice di DegLexPos è $\left(\begin{smallmatrix} M_\sigma & 0 \\ 0 & I \end{smallmatrix}\right)$.

Infine, per far funzionare l'algoritmo di Buchberger per i moduli, bisogna inserire la coppia (f_i, f_j) se e solo se le componenti di testa dei due sono relative alla stessa posizione. Inoltre, nella riduzione, si dice che $te_i \mid se_j$ se e solo se $t \mid s$ e $i = j$.

Esempio 4.10. Sia $M \coloneqq ((x, 1), (xy, x)) \subseteq K[\underline{x}]^2$, con l'ordinamento PosDegLex. A M si associa $M' \coloneqq (xe_1 + e_2, xye_1 + xe_2) \subseteq K[x, y, e_1, e_2]$; i termini di testa sono rispettivamente xe_1 e xye_1; l'S-polinomio dei due polinomi è $xye_1 + ye_2 - xye_1 - xe_2 = (-x+y)e_2$, che è irriducibile. Non avendo altre coppie, si ha una base di Gröbner.

4.3 Sizigie

17.05.2007

Definizione 4.11. Dati $f_1, \ldots, f_k \in K[\underline{x}]$, una k-upla $a_1, \ldots, a_k \in K[\underline{x}]$ tale che $\sum a_i f_i = 0$ è detta *sizigia* di $f_1, \ldots, f_k$. L'insieme di tutte queste k-uple è detto il *modulo delle sizigie* di $f_1, \ldots, f_k$ e si denota con $\mathrm{Syz}(f_1, \ldots, f_k)$.

Teorema 4.12. *Si considera un ordinamento PosTO (dove TO è un qualsiasi term-ordering) e si calcola una base di Gröbner di* $\left(\begin{smallmatrix} f_1 & \cdots & f_k \\ & I & \end{smallmatrix}\right)$*, dove i generatori sono le colonne; allora si ottiene un insieme di generatori* $\left(\begin{smallmatrix} \mathrm{GB}(f_1,\ldots,f_k) & & 0 \\ \star & & v_1,\ldots,v_p \end{smallmatrix}\right)$ *e* $v_1, \ldots, v_p$ *generano il modulo delle sizigie di* $f_1, \ldots, f_k$.

Dimostrazione. Poiché l'ordinamento è PosTO, prima di tutto si ottiene una base di Gröbner rispetto a TO; le colonne con la prima componente a 0 sicuramente appartengono alle sizigie, perché la combinazione lineare con i f_i si annulla. Quindi $\langle v_1, \ldots, v_p \rangle \subseteq \mathrm{Syz}(f_1, \ldots, f_k)$. Il viceversa si dimostrerà in seguito. □

4.4 Graduazioni

Definizione 4.13. Siano M, N, P degli A-moduli; $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ si dice *successione esatta corta* se f è iniettiva, g è suriettiva e $\mathrm{Im}(f) = \ker(g)$.

Definizione 4.14. Siano A un anello e G un semigruppo; si considera $\{ A_d \mid d \in G \}$, con $A_d \subseteq A$ tale che $A = \bigoplus A_d$ e per ogni $a \in A_d$ e $a' \in A_{d'}$ si ha $aa' \in A_{d+d'}$; $\{A_d\}$ è detta *graduazione* di A su G e gli elementi degli A_d si dicono *omogenei* di grado d.

Esempio 4.15. Preso $A_d \coloneqq \{ f \in K[\underline{x}] \mid \partial f = d, f \text{ omogeneo} \}$, $\{A_d\}$ è una graduazione di $K[\underline{x}]$.

Altre possibili graduazioni su $K[\underline{x}]$ sono date da

$$A_d \coloneqq \{ f \in K[\underline{x}] \mid (\forall t \in \mathrm{Supp}(f)) \log(t) \cdot (a_1, \dots, a_n) = d \},$$

con $a_i \in \mathbb{Z}$.

Si possono creare delle bigraduazioni, per esempio scegliendo

$$A_{d_1,d_2} \coloneqq \{ f \in K[\underline{x}] \mid (\forall t \in \mathrm{Supp}(f))(\forall i \in \{1,2\}) \log(t) \cdot (a_{i,1}, \dots, a_{i,n}) = d_i \}.$$

Se la graduazione è non standard, si possono avere anche delle componenti graduate vuote.

Definizione 4.16. Dato un anello A graduato su G e dato un A-modulo M, M si dice *A-modulo graduato* se esiste $\{ M_d \mid d \in G \}$ con $M = \bigoplus M_d$ e $A_d M_e \subseteq M_{d+e}$.

4.5 Funzione di Hilbert e serie di Poincaré

Definizione 4.17. Dato un ideale omogeneo I di $K[\underline{x}]$, si definisce la *funzione di Hilbert* di ${}^{K[\underline{x}]}/_{I}$ come $\mathrm{HF}_{{}^{K[\underline{x}]}/_{I}} \colon \mathbb{N} \to \mathbb{N}$ che associa a d il numero $\dim_K \left({}^{K[\underline{x}]}/_{I}\right)_d$, con la graduazione standard.

Definizione 4.18. Nella stessa situazione, la *serie di Poincaré* è $\mathrm{HP}_{{}^{K[\underline{x}]}/_{I}}(\lambda) := \sum_d \mathrm{HF}_{{}^{K[\underline{x}]}/_{I}}(d)\lambda^d$.

Esempio 4.19. La serie di Poincaré di $K[x,y]$ è $\mathrm{HP}_{K[x,y]}(\lambda) = \sum_j j\lambda^j = (1-\lambda)^{-2}$.

Si può dimostrare che $\mathrm{HP}_{K[\underline{x}]}(\lambda) = (1-\lambda)^{-n}$

Definizione 4.20. Siano M e N due A-moduli; una mappa lineare $f \colon M \to N$ tale che esiste t per cui $f(M_d) \subseteq N_{d+t}$ si dice *morfismo graduato*.

Si può generalizzare il concetto di funzione di Hilbert per moduli generici.

Proposizione 4.21. *Sia* $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ *una successione esatta di* K*-moduli omogenei con* f *e* g *graduate di grado* 0*. Allora* $\mathrm{HF}_N = \mathrm{HF}_M + \mathrm{HF}_P$.

Dimostrazione. Poiché f è iniettiva, $\dim M = \dim \mathrm{Im}(f) = \dim \ker(g)$; da g suriettiva invece, $\dim P = \dim \mathrm{Im}(g)$, ma si ha anche $\dim N = \dim \ker(g) + \dim \mathrm{Im}(g)$. Queste relazioni valgono anche grado per grado, da cui la tesi. □

Proposizione 4.22. *Siano M un A-modulo graduato su G, $F \in A$ omogeneo e $t \coloneqq \partial F$; allora*

$$0 \to \left(\frac{M}{0 :_M (F)}\right)(-t) \xrightarrow{F} M \xrightarrow{\pi} \frac{M}{FM} \to 0$$

è esatta e F e π sono graduati di grado 0.

Dimostrazione. La mappa π è un epimorfismo; se $a, b \in M$ e $a - b \in 0 :_M (F)$, allora $F(a-b) = 0$, quindi F è ben definita; se $aF = 0$, significa che $a \in 0 :_M (F)$, cioè F è iniettiva. Chiaramente $\mathrm{Im}(F) = \ker(\pi)$. □

Proposizione 4.23. *Sia M un A-modulo libero finitamente generato; allora* $\mathrm{HP}_{M(-t)}(\lambda) = \lambda^t \mathrm{HP}_M(\lambda)$.

Dimostrazione. Si ha:

$$\begin{aligned}\mathrm{HP}_{M(-t)}(\lambda) &= \sum_{d\geq 0} \mathrm{HF}_{M(-t)}(d)\lambda^d = \sum_{d\geq 0} \mathrm{HF}_M(d-t)\lambda^d = \\ &= \lambda^t \sum_{d\geq 0} \mathrm{HF}_M(d-t)\lambda^{d-t} = \lambda^t \sum_{d\geq t} \mathrm{HF}_M(d-t)\lambda^{d-t},\end{aligned}$$

dove l'ultimo passaggio è dato dal fatto che $\mathrm{HF}_M(m) = 0$ per $m < 0$; chiaramente l'ultima espressione equivale a $\lambda^t \mathrm{HP}_M(\lambda)$. □

Osservazione 4.24. Per le ultime proposizioni si ha in particolare

$$\mathrm{HF}_M(\lambda) = \mathrm{HF}_{\left(\frac{M}{0:_M(F)}\right)(-t)}(\lambda) + \mathrm{HF}_{M/FM}(\lambda) = \lambda^t \mathrm{HF}_{\frac{M}{0:_M(F)}}(\lambda) + \mathrm{HF}_{M/FM}(\lambda).$$

Se ora $M \coloneqq R/I$, si ha $M/FM = \frac{R/I}{F R/I} \cong R/(F, I)$; inoltre

$$\frac{M}{0 :_M (F)} = \frac{R/I}{I :_{R/I} (F)} \cong \frac{R}{I : (F)}.$$

Perciò si ha $\mathrm{HF}_{R/I}(\lambda) = \mathrm{HF}_{R/(I,\,F)}(\lambda) + \lambda^t \mathrm{HF}_{R/I\,:\,(F)}(\lambda)$, che viene detta *formula principale* per R/I; in particolare si ha

$$\mathrm{HF}_{R/(f_1,\,\ldots,\,f_k)}(\lambda) = \mathrm{HF}_{R/(f_2,\,\ldots,\,f_k)}(\lambda) - \lambda^{\partial f_1} \mathrm{HF}_{R/(f_2,\,\ldots,\,f_k)\,:\,(f_1)}(\lambda).$$

Lemma 4.25 (di Macaulay)**.** *Sia $I \subseteq K[\underline{x}]$ omogeneo, σ un term-ordering compatibile col grado; allora* $\mathrm{HF}_{R/I} = \mathrm{HF}_{R/\mathrm{LT}_\sigma(I)}$.

Dimostrazione. Si deve dimostrare che $\dim (R/I)_d = \dim (R/\mathrm{LT}_\sigma(I))_d$, ma $N_\sigma(I)$ è una base sia di $K[\underline{x}]/\mathrm{LT}_\sigma(I)$ che di $K[\underline{x}]/I$ come K-spazi, da cui segue la tesi. □

Per applicare questo lemma nella pratica, si deve calcolare una base di Gröbner di I rispetto a σ, per poter avere $\mathrm{LT}_\sigma(I)$.

Esempio 4.26. Per ideali monomiali, l'operatore : agisce mediante sottrazione di esponenti (avendo come ovvio limite inferiore 0). Per esempio, $(x^2y, z, xy) : (xy) = (y, z, 1) = (1)$. Perciò, se si hanno ideali monomiali, per calcolare $\mathrm{HF}_{R/(t_1,\,\ldots,\,t_r)}(\lambda)$ è comodo spezzarlo nella differenza di $\mathrm{HF}_{R/(t_2,\,\ldots,\,t_r)}(\lambda)$ e $\lambda^{\partial t_1} \mathrm{HF}_{R/(t_2,\,\ldots,\,t_r)\,:\,(t_1)}(\lambda)$.

23.05.2007

Teorema 4.27 (Hilbert-Serre)**.** *Sia $I \subseteq K[\underline{x}]$ omogeneo; allora* $\mathrm{HP}_{R/I}(\lambda) = {}^{Q(\lambda)}/_{(1-\lambda)^n}$*, con $Q(\lambda) \in \mathbb{Z}[\lambda]$.*

Dimostrazione. Si sfrutta il lemma di Maculay, osservando che se si applica la formula principale a ${}^{R}/_{I}$ con I ideale monomiale generato da t elementi, allora ci si riduce a calcolare la serie di Poincaré di ${}^{R}/_{J}$ con J generato da un numero di elementi strettamente minore di t. □

Si può dimostrare per esercizio che se $(1-\lambda)^t \mid Q(\lambda)$, allora $t \leq n$.

4.6 Regole di calcolo

Si indica il numeratore di $\mathrm{HP}_{K[\underline{x}]/I}$ con $\langle I \rangle$. Allora si ha $\langle (1) \rangle = 0$, $\langle \underline{x}^{\underline{\alpha}} \rangle = 1 - \lambda^{\partial \underline{\alpha}}$ e $\langle I, F \rangle = \langle I \rangle - \lambda^{\partial F} \langle I : (F) \rangle$.

Esercizio 4.28. Se t_1 e t_2 sono termini coprimi, allora $\langle (t_1, t_2) \rangle = (1 - \lambda^{\partial t_1})(1 - \lambda^{\partial t_2})$.

Esercizio 4.29. Se I_1 e I_2 sono ideali monomiali che coinvolgono variabili disgiunte, allora si può generalizzare l'esercizio precedente.

Esempio 4.30. Per $I \coloneqq (x^4, x^3y^2, x^2y^3, z^2)$, si ha

$$\begin{aligned}\langle I \rangle &= \left\langle x^4, x^3y^2, x^2y^3, z^2 \right\rangle = \left\langle x^3y^2, x^2y^3, z^2 \right\rangle - \lambda^4 \left\langle y^2, \cancel{y^3}, z^2 \right\rangle = \\ &= \left\langle x^3y^2, x^2y^3 \right\rangle (1 - \lambda^2) - \lambda^4 (1 - \lambda^2)^2.\end{aligned}$$

Ora, si ha $\left\langle x^3y^2, x^2y^3 \right\rangle = \left\langle x^3y^2 \right\rangle - \lambda^5 \langle x \rangle = 1 - \lambda^5 - \lambda^5(1 - \lambda)$. Questo procedimento richiede, in teoria, tempo esponenziale.

Osservazione 4.31. Da $\langle I \rangle = \langle I, F \rangle + \lambda^{\partial F} \langle I : (F) \rangle$, se si sceglie accuratamente F si possono avere dei vantaggi nel calcolo di $\langle I \rangle$.

Esempio 4.32. Con I come nell'esempio precedente, sia $F = x$; allora $\langle I \rangle = \left\langle z^2, x \right\rangle + \lambda \left\langle x^3, x^2y^2, xy^3, z^2 \right\rangle$.

Proposizione 4.33. *Sia $M \subseteq K[\underline{x}]^r$ un modulo libero finitamente generato; allora:*

1. $\mathrm{HP}_M = \mathrm{HP}_{\mathrm{LT}_\sigma(M)}$*, con σ un ordinamento per moduli che sia compatibile con il grado;*
2. $\mathrm{HP}_{M \oplus N} = \mathrm{HP}_M + \mathrm{HP}_N$ *(dalla successione esatta corta);*
3. $\mathrm{HP}_{K[\underline{x}]^r/M} = \mathrm{HP}_{K[\underline{x}]^r} - \mathrm{HP}_M$*;*
4. $\mathrm{HP}_{K[\underline{x}]^r}(\lambda) = {}^{r}/_{(1-\lambda)^n}$*;*
5. $\mathrm{HP}_{K[\underline{x}]^r/(0,\ldots,t,\ldots,0)}(\lambda) = r - {}^{\lambda^{\partial t}}/_{(1-\lambda)^n}$*, per $t \in T^n$.*

24.05.2007

Esempio 4.34. Sia $M \coloneqq \begin{pmatrix} x & 0 \\ x & y \\ 0 & x \end{pmatrix} \subseteq (K[x,y])^3$. Preso σ come PosDegLex, si ha $\mathrm{LT}_\sigma(M) = \begin{pmatrix} x & 0 \\ 0 & y \\ 0 & 0 \end{pmatrix}$. Con la notazione introdotta in precedenza, $\mathrm{LT}_1 = (x)$, $\mathrm{LT}_2 = (y)$, $\mathrm{LT}_3 = (0)$. Quindi $\mathrm{HP}_{(K[x,y])^3/M}(\lambda) = \mathrm{HP}_{K[\underline{x}]/(x)}(\lambda) + \mathrm{HP}_{K[\underline{x}]/(y)}(\lambda) + \mathrm{HP}_{K[\underline{x}]}(\lambda)$. La prima e la seconda sono ${}^{1-\lambda}/_{(1-\lambda)^2}$, mentre la terza è $(1-\lambda)^{-2}$; la somma dà ${}^{3-2\lambda}/_{(1-\lambda)^2}$. Il termine noto del numeratore è sempre il numero di componenti del modulo, perché 1 può sempre essere componente di una base del quoziente (a meno che $M = K[\underline{x}]$).

Da $\mathrm{HP}_{K[\underline{x}]^r/M} = \mathrm{HP}_{K[\underline{x}]^r} - \mathrm{HP}_M$ si può calcolare la serie di Poincaré di M.

Si può dimostrare che se d è molto maggiore di 0 e si usa una graduazione standard, allora $\mathrm{HF}_{R/I}(d) = f(d)$ con $f \in \mathbb{Z}[d]$.

Tutte le serie di Poincaré hanno la forma $Q(\lambda)/(1-\lambda)^n$. Se si semplificano tutti i fattori $1-\lambda$, si ha che l'esponente al denominatore è la dimensione nel senso della geometria algebrica della varietà associata. Questa dimostrazione è abbastanza difficile. Come esercizio, si può dimostrare che, posto $d(R/I)$ questo numero, è uguale a $d(R/\sqrt{I})$. Inoltre, il radicale di un ideale monomiale è l'ideale generato dagli stessi elementi senza esponenti. Quindi calcolare la dimensione di una varietà sapendo la base di Gröbner è facile.

4.7 Operazioni tra moduli

Proposizione 4.35. *Siano M e N dei $K[\underline{x}]$-moduli omogenei, $M \subseteq N$; se $\mathrm{HF}_M = \mathrm{HF}_N$ allora $M = N$.*

Dimostrazione. Siano G e H basi di Gröbner ridotte di M e N rispetto a un ordinamento compatibile con il grado. Per assurdo, se $G \neq H$, sia d il primo grado per cui $G_d \neq H_d$, allora $G_d = (g_1, \ldots, g_{\nu'})$ e $H_d = (g_1, \ldots, g_\nu)$ per come si costruiscono le basi di Gröbner ridotte. Ma allora le funzioni di Hilbert devono essere necessariamente diverse in d. □

Sia J un ideale di A (ciò che si dirà varrà allo stesso modo per gli A-moduli), generato da $f_1, \ldots, f_r$; allora preso un ordinamento compatibile con il grado, sia M il modulo generato dalle colonne di $\begin{pmatrix} f_1 & \cdots & f_r \\ & I & \end{pmatrix}$; si vuole dimostrare che se si calcola la base di Gröbner ridotta di M si ottiene $\begin{pmatrix} \mathrm{RGB}_\sigma(f_1,\ldots,f_r) & 0 \\ \star & \mathrm{RGB}_\sigma(\mathrm{Syz}(f_1,\ldots,f_r)) \end{pmatrix}$. Si suppone che gli f_i siano omogenei e si pone un peso particolare in modo che tutto il modulo sia omogeneo, cioè si pone grado 0 alla componente 0-esima, grado ∂f_i alla componente i-esima. Si dimostra che questa è una graduazione e si calcola la serie di Poincaré del modulo: non si può sperare che si abbia già una base di Gröbner per l'ordinamento scelto, ma se si prende un ordinamento adatto (per esempio, DegPosTO o comunque un ordinamento per cui le ultime componenti sono più grandi della prima), si può fare in modo che i termini di testa del modulo M siano $e_1, \ldots, e_r$. Allora

$$\mathrm{HP}_M = \mathrm{HP}_{K[\underline{x}]^{r+1}} - \mathrm{HP}_{K[\underline{x}]/M} = \frac{r+1}{(1-\lambda)^n} - \left(\sum_{i=1}^{r} \mathrm{HP}_{K[\underline{x}]/(e_i)} + \mathrm{HP}_{K[\underline{x}]} \right) =$$
$$= \frac{r+1}{(1-\lambda)^n} - \sum_{i=1}^{r} \frac{1-\lambda^{\partial f_i}}{(1-\lambda)^n} - \frac{1}{(1-\lambda)^n} = \frac{\sum_{i=1}^{r} \lambda^{\partial f_i}}{(1-\lambda)^n}.$$

Ma si può calcolare la serie di Poincaré anche in un altro modo: usando l'altra matrice dei generatori. Poiché la prima componente degli ultimi generatori è nulla, denotando con N il modulo generato da questi, si ha anche $\mathrm{HP}_M = \mathrm{HP}_J + \mathrm{HP}_N$ (perché si è già dimostrato che $N \subseteq \mathrm{RGB}_\sigma(\mathrm{Syz}(f_1, \ldots, f_r))$). Si considera la successione esatta corta

$$0 \to \mathrm{Syz}(f_1, \ldots, f_r) \to \bigoplus_{i=1}^{r} K[\underline{x}](-\partial f_i) \to J \to 0;$$

per l'esattezza, la serie di Poincaré dell'elemento al centro, che per quanto calcolato all'inizio è HP_M, è uguale a $\mathrm{HP}_{\mathrm{Syz}} + \mathrm{HP}_J$. Combinando, $\mathrm{HP}_N = \mathrm{HP}_{\mathrm{Syz}}$.

Il teorema sulla successione esatta corta vale anche per elementi non omogenei (si dimostrerà più avanti). Assumendo questo, si ricavano i seguenti.

1. Si possono calcolare le sizigie di M:
$$\mathrm{RGB}\begin{pmatrix} M \\ I \end{pmatrix} = \begin{pmatrix} \mathrm{RGB}(M) & 0 \\ \star & \mathrm{RGB}(\mathrm{Syz}(M)) \end{pmatrix}.$$
2. Si può calcolare $M \cap N$:
$$\mathrm{RGB}\begin{pmatrix} M & N \\ 0 & N \end{pmatrix} = \begin{pmatrix} \mathrm{RGB}(M,N) & 0 \\ \star & \mathrm{RGB}(M \cap N) \end{pmatrix}.$$
3. Si può calcolare $M : (v)$:
$$\mathrm{RGB}\begin{pmatrix} M & v \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathrm{RGB}(M,v) & 0 \\ \star & M : v \end{pmatrix}.$$
4. Per $M : (f)$:
$$\mathrm{RGB}\begin{pmatrix} M & fI \\ 0 & I \end{pmatrix} = \begin{pmatrix} \mathrm{RGB}(M,fI) & 0 \\ \star & M:(f) \end{pmatrix}.$$
5. Sia $\varphi\colon K[\underline{x}]^r \to K[\underline{x}]^r$ una mappa lineare di moduli descritta dalla matrice M_φ; allora $\ker\varphi = \mathrm{Syz}(M_\varphi)$; se $N \subseteq K[\underline{x}]^r$, si calcola $\varphi^{-1}(N)$:
$$\mathrm{RGB}\begin{pmatrix} M_\varphi & N \\ I & 0 \end{pmatrix} = \begin{pmatrix} \mathrm{RGB}(M_\varphi,N) & 0 \\ \star & \mathrm{RGB}(\varphi^{-1}(N)) \end{pmatrix}.$$
6. Se si ha un sistema $AX = B$, allora se $B = 0$, $X = \mathrm{Syz}(A)$, altrimenti si calcola
$$\mathrm{RGB}\begin{pmatrix} -B & A \\ I & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} \mathrm{RGB}(-B,A) & 0 & 0 \\ \star & C & 0 \\ \star & D & \mathrm{Syz}(A) \end{pmatrix}.$$
Esistono soluzioni se e solo se $C = I$ e se esistono, D è una soluzione particolare e $\mathrm{Syz}(A)$ è una soluzione generale.

Si possono ottimizzare i calcoli combinando più operazioni insieme. Per esempio, se si deve calcolare $(I : (g)) \cap K$, si possono combinare le due operazioni facendo la base di Gröbner di $\left(\begin{smallmatrix} I & gI & 0 \\ 0 & I & K \\ 0 & 0 & K \end{smallmatrix}\right)$. Allo stesso modo, se si vuole calcolare $I : (f_1, \ldots, f_r) = \bigcap I : f_i$, si può calcolare un'unica base di Gröbner (per esercizio). Comunque, il costo computazionale non aumenta, perché le operazioni che si effettuano sono esattamente le stesse.

Esempio 4.36. Si vuole risolvere $(x-y)f + (x+y)g = -2x^2 - 2xy$. Si costruisce
$$M = \begin{pmatrix} 2x^2+2xy & x-y & x+y \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

e si calcola la base di Gröbner ottenendo $\begin{pmatrix} y & x & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1/2 & 1/2 & 0 & x+y \\ 1/2 & 1/2 & -2x & x-y \end{pmatrix}$. La matrice C è l'identità, quindi esistono soluzioni: quella particolare è $\begin{pmatrix} 0 \\ -2x \end{pmatrix}$, quindi in generale, $f = \lambda(x,y)(x+y)$ e $g = -2x + \lambda(x,y)(x-y)$. Anche la matrice a sinistra ha un significato nel problema, si può cercare di capire qual è.

Le proprietà esposte sopra si possono dimostrare a partire dalla proposizione sulle sizigie e dalle seguenti.

Proposizione 4.37. *Sia $M \subseteq K[\underline{x}]^r$, I ideale di $K[\underline{x}]$, $v_1 \in K[\underline{x}]^r$, $v_2 \in K[\underline{x}]^s$. Sia $M' \coloneqq \begin{pmatrix} M & Iv_1 \\ 0 & Iv_2 \end{pmatrix}$, allora $(M :_I (v_1))v_2$ sono le ultime s componenti di $\mathrm{GB}(M')$, cioè calcolando la base di Gröbner di M' si ottiene $\begin{pmatrix} \mathrm{GB}(M, Iv_1) & 0 \\ \star & \mathrm{GB}((M:_I(v_1))v_2) \end{pmatrix}$.*

Proposizione 4.38. *Siano $M, N \subseteq K[\underline{x}]^r$, $f, g \in K[\underline{x}]$, $M' \coloneqq \begin{pmatrix} M & fN \\ 0 & gN \end{pmatrix}$; allora $g(M :_N (f))$ sono le ultime r componenti di $\mathrm{GB}(M')$, cioè calcolando la base di Gröbner di M' si ottiene $\begin{pmatrix} \mathrm{GB}(M, fN) & 0 \\ \star & g(M:_N(f)) \end{pmatrix}$.*

4.8 Sizigie per ideali non omogenei

Si dimostrerà ora il teorema delle sizigie anche nel caso non omogeneo. Prima di tutto, l'immersione di $K[\underline{x}]^r$ in $K[\underline{x}, y_1, \ldots, y_r]$ può essere adattata facilmente al caso in cui si hanno degli shift di $-d_i$ nella componente i: è sufficiente dare alla variabile y_i grado d_i. Sull'altra immersione, quella in $K[\underline{x}, y]$, si può fare, ma bisogna assegnare a y^i grado d_i, e in generale questo è possibile solo tralasciando la struttura di anello graduato su $K[\underline{x}, y]$. Si può fare però con due variabili, a patto che una delle due abbia grado nullo: allora si può immergere tranquillamente qualsiasi siano gli shift (per esempio, $\partial y_1 = 0$ e $\partial y_2 = 1$). Se si hanno delle n-graduazioni, si devono aggiungere non 2 ma $n+1$ variabili.

30.05.2007

Esercizio 4.39. Sia $(x+y, xz) \in K[x,y,z]$ con l'ordinamento DegRevLex; si vogliono calcolare le sizigie. Si considera la base di Gröbner di $\begin{pmatrix} x+y \\ 1 \\ 0 \end{pmatrix}$ e $\begin{pmatrix} xz \\ 0 \\ 1 \end{pmatrix}$ (vettori 1 e 2); l'S-polinomio di questi due è $S(1,2) = z\begin{pmatrix} x+y \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} xz \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} yz \\ z \\ -1 \end{pmatrix}$. Questo vettore è irriducibile perché il suo termine di testa è yz (in PosDegRevLex). Si aggiunge questo vettore con nome 3 e si ha $S(1,3) = yz\begin{pmatrix} x+y \\ 1 \\ 0 \end{pmatrix} - x\begin{pmatrix} yz \\ z \\ -1 \end{pmatrix} = \begin{pmatrix} y^2z \\ -xz+yz \\ x \end{pmatrix}$ (nonostante le teste siano coprime, non è detto che l'S-polinomio sia 0, lo è sicuramente solo nella prima componente); $S(1,3)$ si può ridurre tramite 3 a $\begin{pmatrix} 0 \\ -xz \\ x+y \end{pmatrix}$, che diventa il vettore 4. Gli S-polinomi con 4 non sono necessari perché i termini di testa sono su componenti diverse; rimane $S(2,3) = y\begin{pmatrix} xz \\ 0 \\ 1 \end{pmatrix} - x\begin{pmatrix} yz \\ z \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ -xz \\ y+z \end{pmatrix}$ che si riduce tramite 4 a 0. Quindi i vettori da 1 a 4 formano una base di Gröbner e un generatore delle sizigie è $\begin{pmatrix} -xz \\ x+y \end{pmatrix}$, i vettori sotto lo 0 tra i vettori di una base di Gröbner.

Si ha un algoritmo per il calcolo delle sizigie di un ideale omogeneo; nel caso che l'ideale non sia omogeneo, l'idea è semplice: si rendono omogenei i polinomi, si fa il calcolo e si trasporta il risultato indietro.

Definizione 4.40. Dato un ideale $I \subseteq K[\underline{x}]$, con l'ordinamento σ', l'*ideale omogeneo corrispondente* a I è $I^h \coloneqq \left\{ f^h \mid f \in I \right\} \subseteq K[\underline{x}, h]$[5].

Osservazione 4.41. Non è vero che se $I \coloneqq (f_1, \ldots, f_r)$ allora $I^h = (f_1^h, \ldots, f_r^h)$. Per esempio, se $I \coloneqq (y^2 - x, x^2 + 1) = (x^2y + y, xy^2 + 1)$ (sono lo stesso ideale: il primo insieme di generatori è una base di Gröbner calcolata a partire dal secondo). Si prova però che $(y^2 - xh, x^2 + h^2) \neq (x^2y + yh^2, xy^2 + h^3)$, calcolando le basi di Gröbner ridotte di entrambi.

Si considera la graduazione standard e un ordinamento compatibile con il grado tale che h è più piccola di tutte le altre variabili. Tipicamente, questo ordinamento σ sarà fatto da $\begin{pmatrix} 1=\sigma'_1 & 1 \\ \sigma'_2 & 0 \\ \vdots & \vdots \\ 0 & 1 \end{pmatrix}$, dove σ'_i è la i-esima riga di σ'. Con queste ipotesi, $\mathrm{LT}_\sigma(f^h) = \mathrm{LT}_{\sigma_{|K[\underline{x}]}}(f) = \mathrm{LT}_\sigma(f)$. È indispensabile che l'ordinamento sia compatibile con il grado.

Teorema 4.42. *Sia $I \subseteq K[\underline{x}]$, con la notazione precedente; se $(f_1, \ldots, f_k)$ è una base di Gröbner rispetto a σ', allora $(f_1^h, \ldots, f_k^h)$ è una base di Gröbner di I^h rispetto a σ.*

Dimostrazione. Innanzitutto è una base di Gröbner; si deve mostrare che $S(f_1^h, f_2^h) \xrightarrow{f_1^h, \ldots, f_k^h} 0$; se si riducesse a $f \neq 0$, allora $f = g^h \in I$, con $g \neq 0$; ma g è riducibile a 0 tramite $f_1, \ldots, f_k$. Però g e f hanno lo stesso termine di testa, quindi si ha l'assurdo.

Nello stesso modo si dimostra, per esercizio, che questa base di Gröbner genera tutto I^h. □

Come corollario immediato, l'irriducibilità della base di Gröbner non cambia passando da quella non omogenea a quella omogenea.

Proposizione 4.43. *Siano $M, N \subseteq (K[\underline{x}])^r$, con $M \subseteq N$ e $M^h = N^h$, allora $M = N$.*

Questa proposizione può essere utile per esempio per calcolare le sizigie di M a partire dal fatto che calcolando la base di Gröbner di $\binom{M}{I}$ si ottiene $\begin{pmatrix} \mathrm{GB}(M) & 0 \\ \star & N \end{pmatrix}$ e risulta $N \subseteq \mathrm{Syz}(M)$; se si sa che $N^h = \mathrm{Syz}(M)^h$, si sa anche che $N = \mathrm{Syz}(M)$.

5 Sistemi di equazioni

31.05.2007

5.1 Il Nullstellensatz di Hilbert

Il Nullstellensatz forte dice che se $K = \bar{K}$ e $I \leq K[\underline{x}]$, allora $\mathrm{I}(\mathrm{V}(I)) = \sqrt{I}$. Questo avviene se e solo se per $K = \bar{K}$ e $\mathfrak{m} \leq K[\underline{x}]$ ideale massimale, allora $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ per opportuni $a_i \in K$.

Il Nullstellensatz debole invece dice che se $K = \bar{K}$, allora $\mathrm{V}(I) = \varnothing$ se e solo se $I = (1)$ se e solo se $\mathrm{RGB}_\sigma(I) = \{1\}$ per ogni $\sigma \in \mathrm{TO}(T^n)$.

Come conseguenze di questi teoremi, $\mathfrak{m} \cap K[x_1] \neq (0)$ e $K[\underline{x}]/\mathfrak{m}$ è finitamente generato come K-spazio.

[5] Si dimostra che I^h è già un ideale.

Proposizione 5.1. *Sia $\sigma \in \mathrm{TO}(T^n)$, S il sistema di equazioni associato a $I \leq K[\underline{x}]$. Allora sono equivalenti:*

1. *S ha un numero di soluzioni finito;*
2. *$I\bar{K}[\underline{x}]$ è contenuto in un numero finito di ideali massimali $\mathfrak{m}_1, \ldots, \mathfrak{m}_t \leq \bar{K}[\underline{x}]$;*
3. *$I \cap K[x_i] \neq (0)$ per ogni $i \in \{1, \ldots, n\}$;*
4. *$\dim_K {}^{K[\underline{x}]}/_I < \infty$;*
5. *$|N_\sigma(I)| < \infty$;*
6. *per ogni i, esiste α_i tale che $x_i^{\alpha_i} \in \mathrm{LT}_\sigma(I)$.*

Dimostrazione. Le implicazioni sono quasi tutte banali; quella un po' più delicata è $2 \Rightarrow 6$. Sia $\mathfrak{m}_i \coloneqq (x_1 - a_{i,1}, \ldots, x_n - a_{i,n})$, per il Nullstellensatz; sia $g_j \coloneqq \prod_{i=1}^{t}(x_j - a_{i,j})$: g_j appartiene alla varietà $\mathrm{I}(\mathrm{V}(I)) = \sqrt{I}$, il che significa che $g_j^\alpha \in I$, da cui $x_j^{t\alpha} = \mathrm{LT}_\sigma(g_j^\alpha) \in \mathrm{LT}_\sigma(I)$. Questo procedimento funziona nonostante gli ideali massimali siano in $\bar{K}[\underline{x}]$ perché l'algoritmo di Buchberger è "stabile", cioè se ha come ingresso polinomi di $K[\underline{x}]$, non incontrerà mai polinomi di $\bar{K}[\underline{x}]$. □

Definizione 5.2. Se vale una delle condizioni equivalenti della proposizione, l'ideale si dice 0-*dimensionale*.

Dato un ideale 0-dimensionale, si cerca un indizio per sapere quante soluzioni ha il sistema di equazioni associato. Per il punto 3, $I \cap K[x_i] = (g_i) \neq 0$; sicuramente il numero di soluzioni non può essere maggiore di $\prod \partial g_i$. Il problema è che in generale questo numero può essere anche molto alto. Però questo limite superiore si può migliorare.

Corollario 5.3. *Siano $f_1, \ldots, f_s \in K[\underline{x}]$, $I \coloneqq (f_1, \ldots, f_s)$ un ideale 0-dimensionale, allora $|V_{\bar{K}}(I)| \leq \dim_K {}^{K[\underline{x}]}/_I$.*

Teorema 5.4. *Sia $I \leq K[\underline{x}]$ 0-dimensionale, tale che per ogni $1 \leq i \leq n$, esiste $g_i \in I \cap K[x_i]$ con $(g_i, g_i') = 1$, allora $I = \sqrt{I}$.*

Teorema 5.5. *Sia $I \leq K[\underline{x}]$ un ideale 0-dimensionale radicale, con K un campo perfetto; allora $|V(I)| = \dim_K {}^{K[\underline{x}]}/_I$.*

Si considera ora un sistema associato a un ideale 0-dimensionale $I \coloneqq (f_1, \ldots, f_s)$; facendo la base di Gröbner rispetto a Lex, si ottiene un solo polinomio in x_n e poi blocchi di polinomi in $x_n, \ldots, x_{n-i}$: si può risolvere a partire dal basso, calcolando zeri di polinomi monovariati (che saranno singoli, perché l'anello dei polinomi in una variabile è PID). Questo procedimento funziona bene per i campi finiti, o nel caso il sistema abbia solo soluzioni razionali. Infatti il problema è nel calcolare le radici di un polinomio e se non si è nei casi precedenti, la soluzione approssimata che si può calcolare ha un errore che si amplifica mentre si risolve il sistema.

Ci sono altri modi per risolvere un sistema di equazioni: si può considerare un'applicazione lineare da ${}^{K[\underline{x}]}/_I$ in se stesso; dagli autovalori e autovettori della matrice M di f si può calcolare le soluzioni di I.

Definizione 5.6. Se I è un ideale 0-dimensionale, si dice che I è in posizione x_i-*normale* se, date due qualunque soluzioni $(a_1, \ldots, a_n)$ e $(b_1, \ldots, b_n)$ del sistema associato a I, allora $a_i \neq b_i$.

Grazie all'algoritmo visto sopra, l'essere x_i normale è equivalente a, dopo aver calcolato una base di Gröbner con l'ordinamento Lex dove x_i è la più piccola, avere il polinomio nella sola x_i senza fattori multipli.

Teorema 5.7 (Shape lemma)**.** *Sia K un campo perfetto, I un ideale 0-dimensionale radicale, x_n-normale. Allora* $\mathrm{RGB}(I) = (x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n))$ *con l'ordinamento Lex e $g_i \in K[x_n]$.*

Nell'applicare lo Shape lemma ci sono problemi: si vede subito che ∂g è uguale al numero di soluzioni del sistema, che può essere grande; la sostituzione delle radici approssimate di g_n nelle prime $n-1$ componenti amplifica l'errore. Questi sono tuttavia problemi che devono affrontare tutti gli algoritmi di questo tipo. Il vero problema intrinseco è che bisogna capire quando un ideale è x_n-regolare (o x_i-regolare, a meno di rinominare). Però, se si lavora sui reali, che un ideale sia x_n-normale è quasi certo. Per essere sicuri del fatto esiste anche un criterio.

Teorema 5.8. *Sia K un campo perfetto; siano I un ideale radicale 0-dimensionale e $(g_n) = K[x_n] \cap I$. Allora sono equivalenti:*

1. *I è x_n-normale;*
2. *$\partial g_n = \dim_K {}^{K[\underline{x}]}/_I$.*

Rimane un caso: che il polinomio non sia x_i-normale per nessuna variabile x_i. Si dimostra che solo un numero finito di trasformazioni lineari che mappano x_i in $x_i + \sum_{j \neq i} a_j x_j$ non mandano I in posizione x_i-normale. In particolare il loro numero è $\binom{\dim_K {}^{K[\underline{x}]}/_I}{2}$, quindi è sufficiente prenderne una casuale e testare.

La cosa difficile rimane la base di Gröbner Lex. Per fare questo, si può calcolare la funzione di Hilbert con l'ordinamento DegRevLex e usarla per fare la base di Gröbner Lex. Un'altra possibilità è usare l'algoritmo FLGM che trasforma una base di Gröbner in qualche ordinamento in un qualsiasi altro ordinamento.

Riferimenti bibliografici

[Chi79] Childs, Lindsay N.: *A concrete introduction to higher algebra.* Undergraduate Texts in Mathematics. Springer-Verlag, 1979.

[CLO97] Cox, David A., John B. Little e Don O'Shea: *Ideals, varieties, and algorithms.* Springer-Verlag, 1997.

[GP02] Greuel, Gert Martin e Gerhard Pfister: *A Singular introduction to commutative algebra.* Springer-Verlag, 2002.

[KR00] Kreuzer, Martin e Lorenzo Robbiano: *Computational commutative algebra 1.* Springer-Verlag, 2000.