Università di Pisa

Dipartimento di Matematica
Corso di Laurea Triennale in Matematica

Algebra lineare su moduli e algoritmo di Buchberger

Relatore:
Prof. Massimo Caboara

Presentata da:
Letizia D'Achille

Anno Accademico 2020/2021

A Francesco
e ai miei genitori

Indice

Introduzione

L'algoritmo di Buchberger [2], una procedura per il calcolo di speciali sistemi di generatori di ideali e moduli su anelli di polinomi, detti basi di Gröbner , è uno strumento fondamentale in algebra computazionale. Tale algoritmo ha estese applicazioni e diverse efficienti implementazioni [7, 9, 12]. Un esame della letteratura ha portato alla luce diverse analogie tra l'algoritmo di Buchberger e gli algoritmi di Gauss ed euclideo. Queste sono rese particolarmente evidenti dall'uso della notazione matriciale per i moduli. Tali considerazioni non vengono generalmente formalizzate nei testi.
In questo contesto il presente lavoro ha l'obiettivo di analizzare le forme normali di un modulo e le procedure per la loro computazione, mettendo a confronto i calcoli effettuati dall'algoritmo di Buchberger con quelli eseguiti dall'algoritmo di Gauss e dall'algoritmo euclideo. Alcune analogie facilmente osservabili portano a concludere che l'algoritmo di Buchberger è una diretta generalizzazione degli altri due.
Considerando una specifica classe di ordinamenti di modulo, gli ordinamenti lessicografici sulle componenti, si nota che la forma matriciale di una base di Gröbner, opportunamente riordinata, contiene blocchi di zeri che conferiscono alla matrice una struttura a scalini. Questa forma normale, particolarmente semplice, risulta utile al computo delle operazioni di base tra moduli. È infatti sufficiente determinare le basi di Gröbner di moduli associati a specifiche matrici a blocchi e studiare le sottomatrici in corrispondenza dei pivot della matrice risultante per poter effettuare queste operazioni. Sono stati approfonditi diversi algoritmi che sfruttano questo approccio, analizzando anche la loro efficienza rispetto alle procedure standard.
Più in generale, gli ordinamenti lessicografici sulle componenti appartengono alla classe degli ordinamenti di eliminazione delle componenti di modulo, per i quali vale una proposizione analoga al noto teorema di eliminazione delle indeterminate.
Le osservazioni fatte sulle forme normali portano naturalmente al confronto sistematico dell'algoritmo di Buchberger con l'algoritmo di Gauss. Questo è stato condotto considerando ideali generati da polinomi lineari, ed allargandosi poi a moduli più generali.
Si è cercato di ricondurre ogni operazione dell'algoritmo di Gauss ad un'operazione effettuata dall'algoritmo di Buchberger; alcuni passi possono essere tradotti direttamente, mentre per altri l'interpretazione è meno immediata. Il raffronto viene esteso alle forme normali che si ottengono dai due algoritmi, riprendendo e spiegando le analogie osservate in precedenza. Per estensione dall'algoritmo di eliminazione di Gauss, si è successivamente preso in esame il calcolo della matrice inversa mediante il metodo dell'affiancamento della matrice identità, che con considerazioni simili è stato ricondotto ad un caso particolare dell'applicazione dell'algoritmo di Buchber-

ger esteso.
In seguito, sempre analizzando le singole operazioni effettuate dalle diverse procedure, si è eseguito un confronto tra l'algoritmo di Buchberger e l'algoritmo euclideo. In particolare, si è esplicitato il legame tra il massimo comun divisore di due polinomi e la base di Gröbner dell'ideale generato da essi generato. In questo contesto l'algoritmo di Buchberger esteso è stato messo in relazione con il rispettivo algoritmo euclideo esteso per il calcolo dell'identità di Bezout. Questo ha suggerito l'utilizzo della teoria sulle basi di Gröbner come alternativa per trattare il problema dell'esistenza delle soluzioni e della loro determinazione per sistemi di equazioni diofantee a variabili polinomiali.
Considerando infine gli aspetti computazionali degli algoritmi di Gauss ed euclideo, sulla base delle analogie individuate, si è studiato tramite alcuni esempi come i problemi di instabilità numerica caratteristici di tali algoritmi si ripercuotano sul comportamento dell'algoritmo di Buchberger.
Al fine di mantenere la tesi quanto più possibile auto-contenuta, nel primo capitolo si introducono brevemente la teoria e la notazione necessari. I prerequisiti e le relative dimostrazioni basilari di algebra commutativa si possono trovare in [7, 9, 12, 3]. Da questi testi sono stati tratti i risultati e le definizioni presentati nel primo capitolo.
Nel secondo capitolo si introducono gli ordinamenti di eliminazione delle componenti di modulo ed i conseguenti risultati riguardanti il calcolo esplicito delle operazioni tra moduli. Il materiale presentato è stato tratto da [4, 5, 3, 12], rielaborando le dimostrazioni per semplificarle ed uniformare la notazione al resto del testo.
Il terzo capitolo comprende infine i confronti dell'algoritmo di Buchberger con l'algoritmo di Gauss e l'algoritmo euclideo. Le nozioni di analisi numerica menzionate si possono trovare in [8]. La tesi è completata da alcune brevi conclusioni che riassumono i risultati principali e si espongono possibili approfondimenti e ampliamenti futuri al lavoro presentato.
La trattazione è completata da numerosi esempi, che chiariscono le notazioni e le procedure presentate. Le computazioni sono state eseguite utilizzando il sistema di algebra computazionale CoCoA, sviluppato all'Università di Genova [1]. In appendice sono stati riportati due esempi di codici CoCoA, selezionando i più significativi. Sono state utilizzate entrambe le versioni CoCoA 4.7.5 e CoCoA 5.3.2 poiché, pur essendo CoCoA 5.3.2 la versione più aggiornata e fruibile, è ancora parzialmente incompleta. Non sono implementati per esempio gli ordinamenti di eliminazione delle componenti di moduli, presenti invece in CoCoA 4.7.5.

Capitolo 1

Moduli e basi di Gröbner

Nel presente capitolo si esporranno definizioni e proprietà computazionali di base dell'anello di polinomi $R = k[x_1, \ldots, x_n]$ con k campo e di R-moduli liberi $M \subseteq R^r$, utili alla comprensione dei capitoli successivi.

A tale scopo è necessario introdurre il metodo di implementazione dei moduli che verrà usato nel seguito[1]. Dato un R-modulo $M \subseteq R^r$ si considererà la sua rappresentazione matriciale: ciascun elemento $m \in M$ è visto in maniera naturale come vettore di R^r. Dato quindi $\{g_1, \ldots, g_s\} \subseteq R^r$ un insieme di generatori di M, quest'ultimo si scrive sotto forma di matrice come segue

$$\mathcal{M} = \begin{pmatrix} g_1 & \vert & \ldots & \vert & g_s \end{pmatrix} \in R^{r \times s}$$

Viceversa, data una matrice $\mathcal{M}$, il modulo M ad essa associato è il modulo generato dalle colonne di $\mathcal{M}$.

Esempio 1.0.1. Dati $r = 3$ e $R = \mathbb{Q}[x_1, x_2, x_3]$, sia $M \subseteq R^3$ un R-modulo generato dai vettori $\{[x_1, x_2, 1], [0, x_1^2 + 1, x_2], [x_1x_2, 0, x_1]\}$. La sua rappresentazione sotto forma di matrice è

$$\mathcal{M} = \begin{pmatrix} x_1 & 0 & x_1x_2 \\ x_2 & x_1^2 + 1 & 0 \\ 1 & x_2 & x_1 \end{pmatrix}$$

1.1 Ordinamenti di modulo

Si inizia richiamando alcune definizioni di base utili per introdurre e caratterizzare gli ordinamenti di modulo.

Definizione 1.1.1. Un polinomio $f \in k[x_1, \ldots, x_n]$ della forma $f = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ con $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ è detto termine. Si denota l'insieme di tutti i termini di $k[x_1, \ldots, x_n]$ con T^n.

Definizione 1.1.2. Si definisce logaritmo la mappa $\log : T^n \to \mathbb{N}^n$ che manda $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mapsto (\alpha_1, \ldots, \alpha_n)$.

[1] Esistono altre implementazioni canoniche, che possono risultare anche più efficienti, che tuttavia sono meno immediate e pertanto sono state omesse per maggior chiarezza. Si veda [3].

Definizione 1.1.3. Dato $r \geq 1$ e $M = R^r$ l'R-modulo libero con base canonica $\{e_1, \ldots, e_r\}$, allora un termine di M è un elemento della forma te_i dove $t \in T^n$ e $1 \leq i \leq r$. Si denota l'insieme di tutti i termini di M con $MT(M)$.

A questo punto si possono introdurre le nozioni di ordinamento per anelli e moduli.

Definizione 1.1.4. Dato $k[x_1, \ldots, x_n]$, un ordinamento totale τ su T^n tale che

- sia compatibile con l'operazione di monoide, ovvero dati $t_1, t_2, t_3 \in T^n$ si ha

$$t_1 \geq_\tau t_2 \implies t_1 \cdot t_3 \geq_\tau t_2 \cdot t_3$$

- $t \geq_\tau 1 \quad \forall t \in T^n$

è detto ordinamento di termini.

Osservazione 1.1.1. Un ordinamento di termini τ è tale che ogni catena strettamente decrescente di termini è stazionaria.

Osservazione 1.1.2. C'è una corrispondenza biunivoca tra un ordinamento di termini su T^n e un ordinamento di monoide su $\mathbb{N}^n$, data dall'isomorfismo di monoidi $\log : T^n \to \mathbb{N}^n$. Inoltre ogni ordinamento di monoide su $\mathbb{N}^n$ si estende in modo univoco a un ordinamento di monoide su $\mathbb{Z}^n$: dato $v \in \mathbb{Z}^n$, siano $v_1, v_2 \in \mathbb{N}^n$ tali che $v = v_1 - v_2$, allora si pone $v \leq_{\tau_\mathbb{Z}} 0$ se e solo se $v_1 \leq_{\tau_\mathbb{N}} v_2$; dati $v, w \in \mathbb{Z}^n$ si definisce quindi $v \leq_{\tau_\mathbb{Z}} w$ se e solo se $v - w \leq_{\tau_\mathbb{Z}} 0$. La buona definizione e l'unicità seguono dalla proprietà di compatibilità dell'ordinamento con le operazioni di monoide.

Si presenta un primo esempio di ordinamento di termini su T^n.

Definizione 1.1.5. Dati $t_1, t_2 \in T^n$ si pone $t_1 \geq_{lex} t_2$ se e solo se $t_1 = t_2$ o la prima componente non nulla di $\log(t_1) - \log(t_2)$ è positiva. L'ordinamento di termini così definito è detto lex o lessicografico.

Esempio 1.1.1. Usando l'ordinamento lex, si ha che le indeterminate sono ordinate in maniera decrescente, ovvero $x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n$. Inoltre, dato $n \geq 3$, si ha per esempio $x_1x_2^2x_3 >_{lex} x_1x_2x_3^3$, infatti la prima componente non nulla di $(1, 2, 1) - (1, 1, 3) = (0, 1, -2)$ è positiva.

Definizione 1.1.6. Dati $v_1, \ldots, v_n \in \mathbb{Z}^n$ vettori linearmente indipendenti, sia V la matrice la cui i-esima riga è v_i. Allora si può definire il seguente ordinamento su T^n: per $t_1, t_2 \in T^n$ si ha $t_1 \geq_\tau t_2$ se $t_1 = t_2$ o se la prima coordinata non nulla del vettore $V \cdot (\log(t_1) - \log(t_2))$ è positiva.

Osservazione 1.1.3. V come sopra definisce un ordinamento di termini se e solo se il primo elemento non nullo di ogni colonna di V è positivo.

Esempio 1.1.2. L'ordinamento lex è rappresentato dalla matrice identità:

$$V = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & \cdots \\ \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Questo segue direttamente confrontando la definizione dell'ordinamento e la costruzione della matrice V. Inoltre il primo elemento non nullo di ogni colonna è positivo, e in effetti si ha che lex è un ordinamento di termini.

Si presentano altri due classici esempi di ordinamenti di termini su T^n.

Definizione 1.1.7. Dati $t_1, t_2 \in T^n$ si pone $t_1 \geq_{deglex} t_2$ se e solo se $\deg(t_1) > \deg(t_2)$, o se $\deg(t_1) = \deg(t_2)$ e $t_1 \geq_{lex} t_2$. L'ordinamento di termini così definito è detto deglex. È rappresentato dalla seguente matrice:

$$V = \begin{pmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ \cdots & 0 & 1 & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

Esempio 1.1.3. Usando l'ordinamento deglex, come per l'ordinamento lex, si ha che $x_1 >_{deglex} x_2 >_{deglex} \cdots >_{deglex} x_n$. Inoltre, dato $n \geq 3$, si ha per esempio $x_1x_2^2x_3 <_{deglex} x_1x_2x_3^3$, infatti $\deg(x_1x_2^2x_3) = 4 < 5 = \deg(x_1x_2x_3^3)$. Si avrebbe invece $x_1^2x_2x_3^2 >_{deglex} x_1x_2^3x_3$ poiché i due termini hanno uguale grado e vale $x_1^2x_2x_3^2 >_{lex} x_1x_2^3x_3$.

Definizione 1.1.8. Dati $t_1, t_2 \in T^n$ si pone $t_1 \geq_{degrevlex} t_2$ se e solo se $\deg(t_1) > \deg(t_2)$, o se $\deg(t_1) = \deg(t_2)$ e l'ultima componente non nulla di $\log(t_1) - \log(t_2)$ è negativa, o se $t_1 = t_2$. L'ordinamento di termini così definito è detto degrevlex. È rappresentato dalla seguente matrice:

$$V = \begin{pmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & 0 & -1 \\ 0 & 0 & \cdots & -1 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & -1 & 0 & \cdots & 0 \end{pmatrix}$$

Esempio 1.1.4. Usando l'ordinamento degrevlex, come per i precedenti, si ha che $x_1 >_{degrevlex} x_2 >_{degrevlex} \cdots >_{degrevlex} x_n$. Inoltre, dato $n \geq 3$, si ha di nuovo che $x_1x_2^2x_3 <_{degrevlex} x_1x_2x_3^3$, infatti $\deg(x_1x_2^2x_3) = 4 < 5 = \deg(x_1x_2x_3^3)$. Si avrebbe invece $x_1^2x_2x_3^2 <_{degrevlex} x_1x_2^3x_3$ poiché i due termini hanno uguale grado e l'ultima componente non nulla di $(2,1,2) - (1,3,1) = (1,-2,1)$ è positiva.

Definizione 1.1.9. Dato un termine $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in T^n$ si introduce il grado di t, ovvero il naturale $\deg(t) = \alpha_1 + \cdots + \alpha_n$.

Definizione 1.1.10. Un ordinamento di termini τ su T^n è detto compatibile con il grado se dati $t_1, t_2 \in T^n$, $t_1 \geq_\tau t_2$ implica $\deg(t_1) \geq \deg(t_2)$.

Osservazione 1.1.4. Gli ordinamenti deglex e degrevlex sono compatibili con il grado per definizione, mentre lex non lo è. Si è infatti già visto che $x_1x_2^2x_3 >_{lex} x_1x_2x_3^3$, ma $\deg(x_1x_2^2x_3) < \deg(x_1x_2x_3^3)$.

Si estende ora la nozione di ordinamento di termini a moduli liberi.

Definizione 1.1.11. Dato $r \geq 1$, siano $M = R^r$ l'R-modulo libero con base canonica $\{e_1, \ldots, e_r\}$ e τ un ordinamento di termini su T^n, un ordinamento totale μ su $MT(M)$ tale che

- sia compatibile con le operazioni di modulo, ovvero dati $t_1, t_2 \in T^n$ e $m, n \in MT(M)$ si ha

$$t_1 \geq_\tau t_2 \implies t_1 m \geq_\mu t_2 m \qquad m \geq_\mu n \implies t_1 m \geq_\mu t_1 n$$

$$t_1 e_i \geq_\mu t_2 e_i \implies t_1 e_j \geq_\mu t_2 e_j$$

- $te_1 \geq_\mu e_1 \quad \forall t \in T^n$

è detto ordinamento di termini di M.

Osservazione 1.1.5. Come per gli ordinamenti di termini su T^n, anche ogni ordinamento di termini di M è tale che ogni catena strettamente decrescente di termini è stazionaria o, equivalentemente, è un buon ordinamento.

Seguono alcuni tra i più importanti esempi di ordinamenti di termini di M.

Definizione 1.1.12. Sia τ un ordinamento di termini su T^n, e sia $M = R^r$ R-modulo libero. Dati $t_1 e_i, t_2 e_j \in MT(M)$ tali che $t_1, t_2 \in T^n$ e $i, j \in \{1, \ldots, r\}$ si pone

- $t_1 e_i \geq_{ToPos} t_2 e_j \iff t_1 >_\tau t_2$ o $t_1 = t_2$ e $i \leq j$
  L'ordinamento di termini di M così definito è detto ToPos.

- $t_1 e_i \geq_{PosTo} t_2 e_j \iff i < j$ o $i = j$ e $t_1 \geq_\tau t_2$
  L'ordinamento di termini di M così definito è detto PosTo.

Definizione 1.1.13. Dato μ un ordinamento di termini di M e dato $m \in M$, sia $m = \sum_{i=1}^{s} c_i t_i e_{\gamma_i}$ la sua rappresentazione unica con $t_1 e_{\gamma_1} >_\mu \cdots >_\mu t_s e_{\gamma_s}$, dove $c_i \in R \setminus \{0\}$, $t_i \in T^n$ e $\gamma_i \in \{1, \ldots, r\}$. Il termine $t_1 e_{\gamma_1}$ è detto *leading term* di m rispetto a μ, e si denota con $\mathrm{LT}_\mu(m)$. Il coefficiente c_1 è detto *leading coefficient* di m rispetto a μ, e si denota con $\mathrm{LC}_\mu(m)$. Infine $c_1 t_1 e_{\gamma_1}$ è detto *leading monomial* di m rispetto a μ, e si denota con $\mathrm{LM}_\mu(m)$.

Si introducono infine due classi di ordinamenti più generali che saranno utili in seguito.

Definizione 1.1.14. Siano $L \subseteq \{x_1, \ldots, x_n\}$ e $\hat{R} = k[x_i | x_i \notin L]$. Dato $r \geq 1$, sia $M = R^r$ R-modulo libero. Un ordinamento di termini di M μ è detto ordinamento di eliminazione di L se ogni elemento $m \in M$ tale che $\mathrm{LT}_\mu(m) \in \hat{R}^r$ è contenuto in $\hat{R}^r$.

Esempio 1.1.5. Dato $1 \leq j < n$ e $r = 1$, l'ordinamento lessicografico su T^n è un ordinamento di eliminazione di $L = \{x_1, \ldots, x_j\}$, ovvero per le prime j indeterminate. Si può notare infatti che, dati due termini t_1, t_2 tali che t_1 contiene un'indeterminata con indice minore rispetto a tutte le indeterminate contenute in t_2, allora vale $t_1 >_{lex} t_2$. Da questo segue che, dato $f \in R$, se $\mathrm{LT}_{lex}(f)$ contiene solo le ultime $n - j$ indeterminate, allora anche gli altri termini di f devono soddisfare tale proprietà. Dato $n \geq 5$, sia per esempio $f = x_4^2 x_5 + x_3 x_4^2 + 4x_3^3 x_5$. Si ha $\mathrm{LT}_{lex}(f) = x_3^3 x_5 \in \{x_3, \ldots, x_n\}$, e vale in effetti $f \in \{x_3, \ldots, x_n\}$.

Definizione 1.1.15. Sia $r \geq 1$, e sia $M = R^r$ R-modulo libero. Fissato $1 \leq t < r$, un ordinamento di termini di M μ è detto ordinamento di eliminazione delle prime t componenti se ogni elemento $m \in M$ tale che $\mathrm{LT}_\mu(m) \in \mathbf{0}_t \oplus R^{r-t}$ è contenuto in $\mathbf{0}_t \oplus R^{r-t}$. Se μ è un ordinamento di eliminazione delle prime t componenti per ogni $1 \leq t < r$, si dice che μ è un ordinamento lessicografico sulle componenti.

Esempio 1.1.6. Dato $1 \leq t < r$, l'ordinamento di termini di M PosTo è un ordinamento di eliminazione delle prime t componenti. In realtà PosTo è un ordinamento lessicografico sulle componenti. Dalla definizione dell'ordinamento segue infatti che, dato $m \in R^r$, se $\mathrm{LT}_{PosTo}(m)$ ha solo le ultime $r - t$ componenti non nulle, allora anche gli altri termini di m devono soddisfare tale proprietà. Dato $r = 3$ e fissato $\tau =$ lex l'ordinamento di termini su T^n, sia per esempio $m = [0, x_2^2 + x_1^2 x_2 x_3, x_1 x_2^2]$. Si ha $\mathrm{LT}_{PosTo}(m) = [0, x_1^2 x_2 x_3, 0] = x_1^2 x_2 x_3 \cdot e_2 \in \mathbf{0}_1 \oplus R^2$, e vale in effetti $m \in \mathbf{0}_1 \oplus R^2$.

1.2 Basi di Gröbner e algoritmo di Buchberger

Si introduce ora il concetto di basi di Gröbner di moduli, specifici sistemi di generatori utili alla computazione di operazioni tra moduli.

Definizione 1.2.1. Dato $r \geq 1$, sia $M \subseteq R^r$ un R-modulo e μ un ordinamento di termini di M. Il modulo $\mathrm{LT}_\mu(M) = \langle \mathrm{LT}_\mu(m) | m \in M \setminus \{0\} \rangle$ è detto *leading term module* di M rispetto a μ. Se $r = 1$, l'ideale $\mathrm{LT}_\mu(M) \subseteq R$ è anche detto *leading term ideal* di M rispetto a μ.

Definizione 1.2.2. Dato $r \geq 1$, sia $M \subseteq R^r$ un R-modulo e μ un ordinamento di termini di M. Allora $G = \{g_1, \ldots, g_s\} \subseteq R^r \setminus \{0\}$ è detta base di Gröbner di M rispetto a μ se $\mathrm{LT}_\mu(M) = \langle \mathrm{LT}_\mu(g_1), \ldots, \mathrm{LT}_\mu(g_s) \rangle$.

Esempio 1.2.1. Siano $r = 2$, $R = \mathbb{Q}[x_1, x_2]$, e sia $M = \langle [x_1^2, 1], [x_1 x_2, 0] \rangle \subseteq R^2$. Dato $\mu =$ lexPos ordinamento su M, si osserva che $G = \{[x_1^2, 1], [x_1 x_2, 0]\}$ non è una base di Gröbner di M, infatti $m = x_2 \cdot [x_1^2, 1] - x_1 \cdot [x_1 x_2, 0] = [0, x_2] \in M$ è tale che $\mathrm{LT}_\mu(m) = [0, x_2] \notin \langle [x_1^2, 0], [x_1 x_2, 0] \rangle = \langle \mathrm{LT}_\mu([x_1^2, 1]), \mathrm{LT}_\mu([x_1 x_2, 0]) \rangle$. Per ottenere una base di Gröbner basta aggiungere l'elemento $[0, x_2]$.

Per calcolare la base di Gröbner di un modulo a partire da un insieme di suoi generatori si utilizza l'algoritmo di Buchberger. Si presentano ora i concetti necessari alla comprensione dell'algoritmo e quindi il suo pseudo-codice.

È necessario introdurre la nozione di divisibilità tra termini. Mentre è intuitivo il significato di "t_1 divide t_2" per $t_1, t_2 \in T^n$ e così anche il risultato di t_1/t_2, meno ovvia è la definizione di divisibilità tra due termini in $MT(M)$.

Definizione 1.2.3. Sia $M \subseteq R^r$ un R-modulo. Dati $t_1 e_i, t_2 e_j \in MT(M)$ tali che $t_1, t_2 \in T^n$ e $i, j \in \{1, \ldots, r\}$, si dice che $t_1 e_i$ divide $t_2 e_j$ se $i = j$ e t_1 divide t_2 come termini di T^n. In tal caso si pone $\frac{t_1 e_i}{t_2 e_i} = \frac{t_1}{t_2} e_i$.

Definizione 1.2.4. Dato $r \geq 1$, sia $M \subseteq R^r$ un R-modulo, e μ un ordinamento di termini di M. Dati $f, g \in R^r$, siano $\mathrm{LT}_\mu(f) = t_1 e_i$ e $\mathrm{LT}_\mu(g) = t_2 e_j$ i leading term

dei vettori rispetto a μ. Se $i = j$ si può definire il vettore

$$\mathrm{S}(f,g) = \frac{\mathrm{lcm}(\mathrm{LT}_\mu(f), \mathrm{LT}_\mu(g))}{\mathrm{LM}_\mu(f)} f - \frac{\mathrm{lcm}(\mathrm{LT}_\mu(f), \mathrm{LT}_\mu(g))}{\mathrm{LM}_\mu(g)} g$$

detto S-vettore di f e g. Se $r = 1$ è anche detto S-polinomio di f e g.

Definizione 1.2.5. Dato $r \geq 1$, sia $M \subseteq R^r$ un R-modulo. Dati $m, n \in M \setminus \{0\}$ si dice che m riduce a $g \in M$ modulo n se esiste un monomio $t_j e_{\gamma_j}$ di m tale che $\mathrm{LT}(n) | t_j e_{\gamma_j}$ e $g = m - \frac{c_j t_j e_{\gamma_j}}{\mathrm{LM}(n)} \cdot n$. Dato $g \in M$ si dice che g è ridotto rispetto a $G = \{g_1, \ldots, g_s\} \subset R^r \setminus \{0\}$ se $g = 0$ oppure se $\forall i$ $\mathrm{LT}(g_i)$ non divide alcun elemento del supporto di r.

La procedura che segue calcola una forma ridotta g di un elemento m di un modulo rispetto a un insieme di elementi dello stesso $G = \{g_1, \ldots, g_s\}$ e ad un ordinamento di termini del modulo μ fissato. Inoltre, la procedura ritorna un insieme di vettori $\{f_1, \ldots, f_s\}$ tale che $m = f_1 g_1 + \cdots + f_s g_s + g$.

Algoritmo di Divisione

Procedure NR
Input $m \in R^r \setminus \{0\}$, $G = \{g_1, \ldots, g_s\} \subset R^r \setminus \{0\}$
Output $g \in R^r, \{f_1, \ldots, f_s\} \subset R^r$

1: $g \coloneqq 0$;
2: $f_1 \coloneqq 0; \ldots; f_s \coloneqq 0$;
3: **while** $m \neq 0$ **do**
4: **while** $\exists j$ tale che $\mathrm{LT}_\mu(g_j) | \mathrm{LT}_\mu(m)$ **do**
5: $i \coloneqq \min\{ j : \mathrm{LT}_\mu(g_j) | \mathrm{LT}_\mu(m)\}$;
6: $f_i \coloneqq f_i + \frac{\mathrm{LM}_\mu(m)}{\mathrm{LM}_\mu(g_i)}$;
7: $m \coloneqq m - \frac{\mathrm{LM}_\mu(m)}{\mathrm{LM}_\mu(g_i)} \cdot g_i$;
8: **endwhile**;
9: $g \coloneqq g + \mathrm{LM}_\mu(m)$;
10: $m \coloneqq m - \mathrm{LM}_\mu(m)$;
11: **endwhile**;
12: **return** $g, f_1, \ldots, f_s$;

La terminazione dell'algoritmo segue dal fatto che ad ogni iterazione dell'algoritmo, in particolare nell'eseguire i passi 7 e 10, il $\mathrm{LT}_\mu(m)$ decresce rispetto all'ordinamento μ in quanto viene sostituito da $\mathrm{LT}_\mu(m - \mathrm{LT}_\mu(m))$. Basta quindi ricordare che μ è un buon ordinamento dall'Osservazione 1.1.5.

Si enuncia ora un criterio che è alla base della costruzione dell'algoritmo di Buchberger.

Teorema 1.2.1. *(Criterio di Buchberger) Dato $r \geq 1$, sia $M \subseteq R^r$ un R-modulo generato da $G = \{g_1, \ldots, g_s\} \subseteq R^r \setminus \{0\}$ e sia μ un ordinamento di termini di M. Allora sono equivalenti:*

- *G è base di Gröbner di M rispetto a μ;*
- *per ogni coppia $f, g \in G$, si ha $NR_{\mu,G}(S(f,g)) = 0$.*

Esempio 1.2.2. Si vuole mostrare che dati i vettori $g_1 = [x_1^2, 1]$, $g_2 = [x_1x_2, 0]$ e $g_3 = [0, x_2]$ dall'Esempio 1.2.1, allora $G' = \{g_1, g_2, g_3\}$ è una base di Gröbner di M. In effetti, dato che (g_1, g_2) è l'unica coppia di vettori con leading term sulla stessa componente, basta calcolare $\mathrm{S}(g_1, g_2) = [0, x_2] = g_2$ la cui forma ridotta rispetto a G' è uguale a 0.

Osservazione 1.2.1. Dall'esempio precedente si osserva che computare gli S-vettori tra sole coppie di termini relativi alla stessa componente sia vantaggioso dal punto di vista computazionale. In generale è in effetti importante ridurre il numero di S-vettori calcolati trovando in particolare dei criteri che permettano di predire se un S-vettore sarà ridotto a 0. Molto efficienti a questo scopo sono i criteri di Gebauer-Möller [10]. Un possibile criterio più intuitivo si ottiene invece constatando che se due elementi f, g hanno leading term coprimi tra loro, allora vale $\mathrm{NR}_{\mu,\{f,g\}}(\mathrm{S}(f, g)) = 0$, si veda [7] per una dimostrazione.

Definizione 1.2.6. Dato $r \geq 1$, sia $M \subseteq R^r$ un R-modulo e μ un ordinamento di termini di M. Allora una base di Gröbner $G = \{g_1, \ldots, g_s\} \subseteq R^r \setminus \{0\}$ di M rispetto a μ è detta ridotta se $\forall i = 1, \ldots, s$ valgono le seguenti condizioni:

- $\mathrm{LC}_\mu(g_i) = 1$
- $\mathrm{LT}_\mu(g_i) \notin \mathrm{LT}_\mu(G \setminus \{g_i\})$
- $\mathrm{NR}_{\mu, G\setminus\{g_i\}}(g_i) = g_i$

Osservazione 1.2.2. Dalla definizione è facilmente deducibile l'algoritmo per ridurre una base di Gröbner, che sarà di seguito denominato *Reduce*.

Teorema 1.2.2. *Dato $r \geq 1$, sia $M \subseteq R^r$ un R-modulo e μ un ordinamento di termini di M. Allora la base di Gröbner ridotta di M rispetto a μ è unica.*

L'algoritmo di Buchberger calcola una base di Gröbner ridotta di un modulo a partire da un insieme di suoi generatori rispetto ad un ordinamento di termini del modulo μ fissato. Nell'algoritmo che segue si scrivono $\mathrm{LT}_\mu(g_i) = t_i e_{\gamma_i}$ con $c_i \in R\setminus\{0\}$, $t_i \in T^n$ e $\gamma_i \in \{1, \ldots, r\}$ per $i = 1, \ldots, s'$.

Algoritmo di Buchberger

Procedure GB
Input $G = \{g_1, \ldots, g_s\} \subset R^r \setminus \{0\}$
Output $G = \{g'_1, \ldots, g'_{s'}\} \subset R^r$

1: $s' = s$;
2: $L \coloneqq \{\, (i, j) \,:\, 1 \leq i < j \leq s, \gamma_i = \gamma_j\}$;
3: **while** $L \neq \emptyset$ **do**
4: choose $(i, j) \in L$;
5: $L \coloneqq L \setminus (i, j)$;
6: $(p, \cdot, \ldots, \cdot) \coloneqq \mathrm{NR}_{\mu,G}(\mathrm{S}(g_i, g_j))$;
7: **if** $p \neq 0$ **then**
8: $s' = s' + 1$;
9: $L \coloneqq L \cup \{\, (i, s') \,:\, 1 \leq i < s', \gamma_i = \gamma_{s'}\}$;
10: $G \coloneqq G \cup \{p\}$;
11: **endif**;
12: **endwhile**;
13: **return** Reduce(G);

La correttezza dell'algoritmo segue dal Teorema 1.2.1, in quanto alla fine dell'esecuzione si ha che si riducono a 0 tutti gli S-vettori tra coppie di elementi della base, ed è possibile dimostrarne la terminazione.

È prima necessario enunciare il risultato che segue.

Teorema 1.2.3. *(Teorema della base di Hilbert) Sia A un anello noetheriano, allora $A[x_1, \ldots, x_n]$ è noetheriano.*

A questo punto è possibile provare la terminazione dell'algoritmo di Buchberger.

Dimostrazione. L'algoritmo termina nel momento in cui viene soddisfatta la condizione $L = \emptyset$. Si può notare che ad ogni ciclo viene cancellata una coppia da L nel passo 4. Inoltre l'insieme L viene ampliato solo al passo 7, ma ogni volta che questo accade viene aggiunto a G un elemento che non si riduce a 0 rispetto agli elementi precedenti in G. Se L venisse ampliato infinite volte, si otterrebbe quindi una catena ascendente infinita di moduli

$$\langle \mathrm{LT}_\mu(g_1), \ldots, \mathrm{LT}_\mu(g_s) \rangle \subset \langle \mathrm{LT}_\mu(g_1), \ldots, \mathrm{LT}_\mu(g_{s+1}) \rangle \subset \ldots$$

che è assurdo per la noetherianità di R. Il fatto che $R = k[x_1, \ldots, x_n]$ sia noetheriano segue dal Teorema 1.2.3 e dal fatto che k è un campo, perciò noetheriano. L'insieme L viene quindi ampliato finite volte, e l'algoritmo termina in finiti passi. □

Esempio 1.2.3. Siano $r = 2$, $R = \mathbb{Q}[x_1, x_2]$, e sia $M \subseteq R^2$ il sottomodulo generato da $g_1 = [x_1^2, 1]$ e $g_2 = [x_1x_2 + x_2^2, 0]$. Si vuole calcolare un base di Gröbner di M tramite l'algoritmo di Buchberger, rispetto a $\mu =$ lexPos ordinamento su M.

- Sia $G = \{g_1, g_2\}$, $s' = 2$ e $L = \{(1, 2)\}$. Si sceglie $(1, 2) \in L$ e si pone $L = \emptyset$.
- Si calcola $\mathrm{S}(g_1, g_2) = [-x_1x_2^2, x_2]$ e quindi $\mathrm{NR}_{\mu,G}([-x_1x_2^2, x_2]) = [x_2^3, x_2] \neq 0$.
- Siano quindi $s' = 3$, $g_3 = [x_2^3, x_2]$, $L = \{(1, 3), (2, 3)\}$, e $G = \{g_1, g_2, g_3\}$.
- Si sceglie $(2, 3) \in L$ e si pone $L = \{(1, 3)\}$.
- Si calcola $\mathrm{S}(g_2, g_3) = [x_2^4, -x_1x_2]$, poi $\mathrm{NR}_{\mu,G}([x_2^4, -x_1x_2]) = [0, -x_1x_2 - x_2^2] \neq 0$.
- Siano quindi $s' = 4$, $g_4 = [0, -x_1x_2 - x_2^2]$ e $G = \{g_1, g_2, g_3, g_4\}$.

Si noti in particolare che non vengono aggiunte altre coppie a L in quanto non si computano S-vettori tra elementi che hanno leading term su componenti diverse.

- Si sceglie $(1, 3) \in L$ e si pone $L = \emptyset$.
- Si calcola $\mathrm{S}(g_1, g_3) = [0, x_2^3 - x_1^2x_2]$ e quindi $\mathrm{NR}_{\mu,G}([0, x_2^3 - x_1^2x_2]) = [0, 0]$.

Dato che $L = \emptyset$ l'algoritmo termina e ritorna $G = \{g_1, g_2, g_3, g_4\}$ base di Gröbner ridotta.

Si può costruire una versione estesa dell'algoritmo di Buchberger in cui si ottiene una matrice $\mathcal{A}$ le cui colonne costituiscono le rappresentazioni dei vettori della base di Gröbner rispetto all'insieme di generatori iniziale. Questo significa che se $G = \{g_1, \ldots, g_s\}$ è l'insieme di generatori di partenza e $G' = \{g'_1, \ldots, g'_{s'}\}$ è la base di Gröbner in output, allora $\mathcal{A} = (a_{ij}) \in R^{s \times s'}$ è tale che $g_j = a_{1j}g_1 + \cdots + a_{sj}g_s$ per $j = 1, \ldots, s'$. Nell'algoritmo che segue si denotano con $a_1, \ldots, a'_s$ le colonne della matrice $\mathcal{A}$.

Algoritmo di Buchberger esteso

Procedure GBE
Input $G = \{g_1, \ldots, g_s\} \subset R^r \setminus \{0\}$
Output $G = \{g'_1, \ldots, g'_{s'}\} \subset R^r, \mathcal{A} \in R^{s \times s'}$

1: $\mathcal{A} = \mathcal{I}_s$;
2: $s' = s$;
3: $L \coloneqq \{\, (i,j) \,:\, 1 \leq i < j \leq s, \gamma_i = \gamma_j \}$;
4: **while** $L \neq \emptyset$ **do**
5: choose $(i,j) \in L$;
6: $L \coloneqq L \setminus (i,j)$;
7: $(p, f_1, \ldots, f_{s'}) \coloneqq \mathrm{NR}_{\mu,G}(\mathrm{S}(g_i, g_j))$;
8: **if** $p \neq 0$ **then**
9: $s' = s' + 1$;
10: $L \coloneqq L \cup \{\, (i,s') \,:\, 1 \leq i < s', \gamma_i = \gamma_{s'} \}$;
11: $G \coloneqq G \cup \{p\}$;
12: $a_{s'} = \frac{\mathrm{lcm}(\mathrm{LT}_\mu(g_i), \mathrm{LT}_\mu(g_j))}{\mathrm{LM}_\mu(g_i)} a_i - \frac{\mathrm{lcm}(\mathrm{LT}_\mu(g_i), \mathrm{LT}_\mu(g_j))}{\mathrm{LM}_\mu(g_j)} a_j - f_1 a_1 - \cdots - f_{s'-1} a_{s'-1}$;
13: $\mathcal{A} = (\, \mathcal{A} \,|\, a_{s'} \,)$;
14: **endif**;
15: **endwhile**;
16: **return** G, $\mathcal{A}$;

Esempio 1.2.4. Si consideri l'Esempio 1.2.3 volendo applicare ora l'algoritmo di Buchberger esteso. Nel calcolo di $\mathrm{NR}_{\mu,G}(\mathrm{S}(g_1, g_2))$ si ottiene $f_2 = -x_2$ da cui

$$a_3 = x_2 a_1 - x_1 a_2 + x_2 a_2 = [x_2, x_2 - x_1]$$

Nel calcolo di $\mathrm{NR}_{\mu,G}(\mathrm{S}(g_2, g_3))$ si ottiene $f_3 = x_2$ da cui

$$a_4 = x_2^2 a_2 - x_1 a_3 - x_2 a_3 = [-x_1 x_2 - x_2^2, x_1^2]$$

L'algoritmo dà quindi in output la matrice

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & x_2 & -x_1 x_2 - x_2^2 \\ 0 & 1 & x_2 - x_1 & x_1^2 \end{pmatrix}$$

1.3 Sizigie

Definizione 1.3.1. Dati $r \geq 1$, $M \subseteq R^r$ un R-modulo e $\mathcal{G} = (g_1, \ldots, g_s)$ una tupla di elementi di M. Una sizigia di $\mathcal{G}$ è un vettore $[f_1, \ldots, f_s] \in R^s$ tale che $\sum_{i=1}^{s} f_i g_i = 0$.

L'insieme di tutte le sizigie di $\mathcal{G} = (g_1, \ldots, g_s)$ forma un R-modulo, detto modulo delle sizigie di $\mathcal{G}$, e denotato $\mathrm{Syz}(\mathcal{G})$.

Esempio 1.3.1. Dall'Esempio 1.2.3 siano $r = 2$, $R = \mathbb{Q}[x_1, x_2]$, e $M \subseteq R^2$ il sottomodulo generato da $g_1 = [x_1^2, 1]$ e $g_2 = [x_1x_2 + x_2^2, 0]$. Si consideri quindi la coppia $\mathcal{G} = (g_1, g_2)$. Il modulo delle sizigie di $\mathcal{G}$ è

$$\mathrm{Syz}(\mathcal{G}) = \left\{ [f_1, f_2] \in R^2 \,:\, f_1 \begin{bmatrix} x_1^2 \\ 1 \end{bmatrix} + f_2 \begin{bmatrix} x_1x_2 + x_2^2 \\ 0 \end{bmatrix} = 0 \right\}$$

Sono ovvie sizigie i multipli dell'elemento $[g_2, -g_1]$.

Osservazione 1.3.1. Se si considera R^s l'R-modulo con base canonica $\{e_1, \ldots, e_s\}$, e il morfismo di moduli

$$\begin{array}{rccl} \phi: & R^s & \to & R^r \\ & e_i & \mapsto & g_i \quad \forall i = 1, \ldots, s \end{array}$$

ovvero il morfismo rappresentato dalla matrice $\mathcal{G}$, allora si ha $\ker(\phi) = \mathrm{Syz}(\mathcal{G})$.

Capitolo 2

Operazioni lineari su moduli

Nel capitolo che segue si considerano ordinamenti lessicografici sulle componenti. In questi casi particolari, la rappresentazione matriciale di un modulo e in particolare di una sua base di Gröbner, risulterà utile per la computazione di operazioni elementari tra moduli.

2.1 Ordinamento di eliminazione

Gli ordinamenti di eliminazione delle componenti godono di una proprietà analoga al teorema di eliminazione, che vale per ordinamenti di eliminazione delle indeterminate.

Proposizione 2.1.1. *Dato $r \geq 1$, sia $M \subseteq R^r$ un R-modulo e μ un ordinamento di eliminazione di M delle prime t componenti per un dato $1 \leq t < n$. Allora gli elementi di una base di Gröbner di M rispetto a μ che appartengono a $\mathbf{0}_t \oplus R^{r-t}$ sono una base di Gröbner di $M \cap \mathbf{0}_t \oplus R^{r-t}$ rispetto a $\mu|_{\mathbf{0}_t \oplus R^{r-t}}$.*

Dimostrazione. Siano $\hat{R}_t = \mathbf{0}_t \oplus R^{r-t}$ e $\mu_t = \mu|_{\hat{R}_t}$, e sia $G = \{g_1, \ldots, g_s\}$ una base di Gröbner di M. Basta dimostrare che $\mathrm{LT}_{\mu_t}(G \cap \hat{R}_t) = \mathrm{LT}_{\mu_t}(M \cap \hat{R}_t)$. In particolare vale in maniera ovvia $\mathrm{LT}_{\mu_t}(G \cap \hat{R}_t) \subseteq \mathrm{LT}_{\mu_t}(M \cap \hat{R}_t)$. Dato invece $m \in M \cap \hat{R}_t$ si ha che esiste $i = 1, \ldots, s$ tale che $\mathrm{LT}_\mu(g_i)$ è multiplo di $\mathrm{LT}_\mu(m)$, in quanto $m \in M$. Inoltre, dato che $m \in \hat{R}_t$, segue che $\mathrm{LT}_\mu(m) \in \hat{R}_t$ e quindi anche $\mathrm{LT}_\mu(g_i) \in \hat{R}_t$. Dal fatto che μ è un ordinamento di eliminazione di M delle prime t componenti, si può concludere che $g_i \in G \cap \hat{R}_t$, quindi $\mathrm{LT}_{\mu_t}(m) \in \mathrm{LT}_{\mu_t}(G \cap \hat{R}_t)$. □

Osservazione 2.1.1. Dalla proposizione segue che, in forma matriciale, la base di Gröbner di un R-modulo rispetto a un ordinamento lessicografico sulle componenti assume la forma sottostante, dove $I_1, \ldots, I_r$ sono opportuni ideali di R e gli asterischi sono blocchi costituiti da opportuni polinomi.

$$\mathrm{GB}_\mu(M) = \begin{pmatrix} \mathrm{GB}_{\mu|_R}(I_1) & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ * & \mathrm{GB}_{\mu|_R}(I_2) & \cdots & \cdots & \cdots \\ \cdots & * & \cdots & \mathbf{0} & \cdots \\ \cdots & \cdots & \cdots & \mathrm{GB}_{\mu|_R}(I_{r-1}) & \mathbf{0} \\ * & * & \cdots & * & \mathrm{GB}_{\mu|_R}(I_r) \end{pmatrix}$$

Per mostrarlo basta considerare $m_{t,1}, \ldots, m_{t,k}$, i soli elementi di $\mathrm{GB}_\mu(M)$ appartenenti a $\mathbf{0}_t \oplus R^{r-t}$ con $(t+1)$-esima componente non nulla. Denotando con $f_{t,j}$ la $(t+1)$-esima componente di $m_{t,j}$ per $j = 1, \ldots, k$, e definendo $I_{t+1} = \langle f_{t,1}, \ldots, f_{t,k} \rangle$ si trova che $G = \{f_{t,1}, \ldots, f_{t,k}\}$ è una base di Gröbner per I_{t+1}. Infatti se per assurdo $\exists f \in I_{t+1}$ tale che $\mathrm{LT}(f) \notin \mathrm{LT}(f_{t,1}, \ldots, f_{t,k})$, con $f = a_1 f_{t,1} + \cdots + a_k f_{t,k}$, allora considerando $m = a_1 m_{t,1} + \cdots + a_k m_{t,k} \in \mathbf{0}_t \oplus R^{r-t} \cap M$ si ha che $\mathrm{LT}(m) \notin \mathrm{LT}(m_{t,1}, \ldots, m_{t,k})$. Usando il fatto che μ è un ordinamento lessicografico sulle componenti, si conclude che gli elementi di $\mathrm{GB}_\mu(M)$ che appartengono a $\mathbf{0}_t \oplus R^{r-t}$ non sarebbero una base di Gröbner di $M \cap \mathbf{0}_t \oplus R^{r-t}$.

2.2 Operazioni elementari tra moduli

2.2.1 Nucleo di morfismi di moduli

Proposizione 2.2.1. *Sia $\phi : R^s \to R^r$ un morfismo di moduli definito dalla matrice $\mathcal{M}$, e M il sottomodulo di R^r generato dalle colonne di $\mathcal{M}$. Sia M' il sottomodulo di R^{r+s} descritto dalla matrice*

$$\mathcal{M}' = \begin{pmatrix} \mathcal{M} \\ \mathcal{I}_s \end{pmatrix}$$

e sia μ un ordinamento lessicografico sulle componenti su R^{r+s}. Allora la base di Gröbner di M' rispetto a μ è della forma

$$GB_\mu(M') = \begin{pmatrix} GB_{\mu|_{R^r}}(M) & \mathbf{0} \\ \mathcal{A} & GB_{\mu|_{R^s}}(\ker(\phi)) \end{pmatrix}$$

dove $\mathcal{A}$ è la matrice le cui colonne sono le rappresentazioni dei vettori di $GB_{\mu|_{R^r}}(M)$ rispetto alle colonne di $\mathcal{M}$.

Dimostrazione. Sia $G = \{g_1, \ldots, g_s\}$, dove g_i per $i = 1, \ldots, s$ sono le colonne di $\mathcal{M}$. Come si è già osservato vale $\ker(\phi) = \mathrm{Syz}(\mathcal{M})$ dove $\mathcal{M}$ è vista come tupla di vettori non nulli ($\mathcal{M} = (g_1, \ldots, g_s)$). Quindi la tesi è equivalente a dimostrare che

$$\mathrm{GB}_\mu(M') = \begin{pmatrix} \mathrm{GB}_{\mu|_{R^r}}(M) & \mathbf{0} \\ \mathcal{A} & \mathrm{GB}_{\mu|_{R^s}}(\mathrm{Syz}(\mathcal{M})) \end{pmatrix}$$

Inoltre si osserva che applicare l'algoritmo di Buchberger esteso a G corrisponde ad applicare l'algoritmo di Buchberger alle colonne di $\mathcal{M}'$ denominando $\mathcal{A} = \mathcal{I}_s$, interrompendolo prima di considerare gli S-vettori tra coppie di elementi che hanno leading term in $\mathbf{0}_r \oplus R^s$ (o equivalentemente scartando tali coppie durante l'esecuzione). Come unica differenza si ha che nel secondo algoritmo si aggiungono alla matrice $\mathcal{A}$ delle colonne in corrispondenza di vettori nulli nel blocco sovrastante. Da questa analogia si può dedurre che il blocco che si ottiene in alto a sinistra coincide con $\mathrm{GB}_{\mu|_{R^r}}(M)$, mentre il blocco in basso a sinistra è la matrice $\mathcal{A}$ data in output dall'algoritmo di Buchberger esteso, ovvero la matrice delle rappresentazioni come voluto. Si ha quindi

$$\mathrm{GB}_\mu(M') = \begin{pmatrix} \mathrm{GB}_{\mu|_{R^r}}(M) & \mathbf{0} \\ \mathcal{A} & \mathcal{N} \end{pmatrix}$$

per una certa matrice $\mathcal{N}$. Si mostra ora che se N è il sottomodulo di R^s generato dalle colonne di $\mathcal{N}$, allora $N = \mathrm{Syz}(\mathcal{M})$. Ripercorrendo l'algoritmo di Buchberger si nota che le colonne di $\mathcal{N}$, per costruzione, sono vettori appartenenti a $\mathrm{Syz}(\mathcal{M})$, in quanto corrispondenti a vettori nulli nel blocco superiore. Da questo segue $N \subseteq \mathrm{Syz}(\mathcal{M})$. Sia $[f_1, \ldots, f_s] \in \mathrm{Syz}(\mathcal{M})$, cioè $\sum_{i=1}^{s} f_i g_i = 0$. Dato che $[\sum_{i=1}^{s} f_i g_i, f_1, \ldots, f_s] \in M'$ in quanto combinazione lineare delle colonne di $\mathcal{M}'$, segue che

$$\begin{bmatrix} 0 \\ f_1 \\ \ldots \\ f_s \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{s} f_i g_i \\ f_1 \\ \ldots \\ f_s \end{bmatrix} \in M'$$

Per la Proposizione 2.1.1 gli elementi di $\mathrm{GB}_\mu(M')$ che appartengono a $M' \cap \mathbf{0}_r \oplus R^s$, ovvero le colonne del blocco $\begin{pmatrix} \mathbf{0} \\ \mathcal{N} \end{pmatrix}$, sono una base di Gröbner di $M' \cap \mathbf{0}_r \oplus R^s$. Ma per quanto detto si ha $[0, f_1, \ldots, f_s] \in M' \cap \mathbf{0}_r \oplus R^s$, da cui si conclude che $[f_1, \ldots, f_s] \in N$ essendo un vettore generato dalle colonne di $\mathcal{N}$. Da questo segue $N \supseteq \mathrm{Syz}(\mathcal{M})$, quindi la tesi. □

2.2.2 Sistemi di equazioni lineari su R

Si prende in esame un sistema di equazioni lineari su R del tipo

$$\mathcal{A}\mathcal{X} + \mathcal{B} = 0 \tag{2.1}$$

dove $\mathcal{A} \in R^{r \times s}$ e $\mathcal{B} \in R^{r \times t}$.
È possibile considerare come insieme di soluzioni di questo sistema una coppia $(\mathcal{X}_1, X_2)$ dove $\mathcal{X}_1 \in R^{s \times t}$ è detta soluzione particolare del sistema, e $X_2 \subseteq R^s$ è il nucleo del morfismo descritto dalla matrice $\mathcal{A}$ (coincide quindi con l'insieme delle soluzioni del sistema omogeneo associato) ed è detto modulo delle soluzioni generali del sistema.

Proposizione 2.2.2. *Siano A e B sottomoduli di R^r descritti rispettivamente dalle matrici $\mathcal{A} \in R^{r \times s}$ e $\mathcal{B} \in R^{r \times t}$. Sia M' il sottomodulo di R^{r+t+s} descritto dalla matrice*

$$\mathcal{M}' = \begin{pmatrix} \mathcal{B} & \mathcal{A} \\ \mathcal{I}_t & \boldsymbol{0} \\ \boldsymbol{0} & \mathcal{I}_s \end{pmatrix}$$

e sia μ un ordinamento lessicografico sulle componenti su R^{r+t+s}. Allora la base di Gröbner di M' rispetto a μ è della forma

$$GB_\mu(M') = \begin{pmatrix} GB_{\mu|_{R^r}}(A+B) & \mathbf{0} & \mathbf{0} \\ * & GB_{\mu|_{R^t}}(C) & \mathbf{0} \\ * & \mathcal{D} & GB_{\mu|_{R^s}}(E) \end{pmatrix}$$

dove gli asterischi sono blocchi costituiti da opportuni polinomi, e $C \subseteq R^t$, $D, E \subseteq R^s$ sono opportuni R-moduli con D rappresentato dalla matrice $\mathcal{D}$. Inoltre, se $GB_{\mu|_{R^t}}(C) = \mathcal{I}_t$, allora $\mathcal{D}$ è la soluzione particolare del sistema (2.1), ed E è il modulo delle soluzioni generali dello stesso. In caso contrario, il sistema non ha soluzioni.

Dimostrazione. La forma della base di Gröbner di M' è data dall'Osservazione 2.1.1. Per la Proposizione 2.2.1 si ha che il blocco in alto a sinistra è la base di Gröbner del modulo generato dalle colonne di $\begin{pmatrix}\mathcal{B} & \mathcal{A}\end{pmatrix}$, ovvero $\mathrm{GB}_{\mu|_{R^r}}(A+B)$ come voluto. Siano ora $\mathcal{C}, \mathcal{E}$ rispettivamente le matrici $\mathrm{GB}_{\mu|_{R^t}}(C)$ e $\mathrm{GB}_{\mu|_{R^s}}(E)$. Di nuovo per la Proposizione 2.2.1 si ha che

$$\mathcal{A}\mathcal{X}+\mathcal{B}=0 \iff \begin{pmatrix}\mathcal{B} & \mathcal{A}\end{pmatrix}\begin{pmatrix}\mathcal{I}_t \\ \mathcal{X}\end{pmatrix}=0 \iff \begin{pmatrix}\mathcal{I}_t \\ \mathcal{X}\end{pmatrix} \in \ker(\begin{pmatrix}\mathcal{B} & \mathcal{A}\end{pmatrix}) = \begin{pmatrix}\mathcal{C} & \mathbf{0} \\ \mathcal{D} & \mathcal{E}\end{pmatrix} \quad (2.2)$$

Si supponga senza perdere generalità che le basi di Gröbner calcolate siano ridotte. In questo caso dato un ideale $I \subset R$, se $1 \in I$ allora $I = R$ e quindi $\mathrm{GB}_{\mu|_R}(I) = \{1\}$. Sfruttando induttivamente questa proprietà sulle righe di $\mathcal{C}$, sotto le ipotesi equivalenti (2.2), si ottiene che tale matrice deve contenere i vettori della base canonica di R^t e quindi riordinando le colonne si conclude $\mathcal{I}_t = \mathcal{C}$. Di conseguenza $\mathcal{X} = \mathcal{D} + \mathcal{K}$ per una certa matrice $\mathcal{K}$, in quanto ciascuna colonna di $\mathcal{C}$ corrisponde a una colonna di $\mathcal{D}$. Infine $\mathcal{K}$ deve essere costituita da colonne che sono combinazione lineare di colonne di $\mathcal{E}$. In conclusione si ha

$$\begin{pmatrix}\mathcal{I}_t \\ \mathcal{X}\end{pmatrix} \in \ker(\begin{pmatrix}\mathcal{B} & \mathcal{A}\end{pmatrix}) = \begin{pmatrix}\mathcal{C} & \mathbf{0} \\ \mathcal{D} & \mathcal{E}\end{pmatrix} \iff \begin{cases}\mathcal{C} = \mathcal{I}_t \\ \mathcal{X} = \mathcal{D} + \mathcal{K}\end{cases}$$

con $\mathcal{K} \in E$, ovvero la tesi. □

Esempio 2.2.1. Si vuole calcolare la soluzione del sistema $\mathcal{A}\mathcal{X} + \mathcal{B} = 0$ con $A = \langle [x_1, x_2], [x_2, x_1], [1, 0] \rangle$ e $B = \langle [x_1x_2, x_2^2], [x_1x_2, x_1^2] \rangle$ sottomoduli di $\mathbb{Q}[x_1, x_2]^2$. Si considera la matrice

$$\begin{pmatrix} \begin{bmatrix} x_1x_2 & x_1x_2 \\ x_2^2 & x_1^2 \end{bmatrix} \begin{bmatrix} x_1 & x_2 & 1 \\ x_2 & x_1 & 0 \end{bmatrix} \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{matrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{pmatrix}$$

e si computa una sua base di Gröbner rispetto a $\mu =$ Poslex ordinamento su M. Si ottiene

$$\begin{pmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & x_1 & x_2 \end{bmatrix} \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} \\ \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & -x_2 & -x_1 \end{matrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{matrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{matrix} \\ \begin{bmatrix} -x_2 & 0 \\ 0 & -x_1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ -x_2 \\ -x_1^2 + x_2^2 \end{bmatrix} \end{pmatrix}$$

perciò per la proposizione si ha

$$\mathcal{X} = \left(\begin{bmatrix} -x_2 \\ 0 \\ 0 \end{bmatrix} + \lambda_1 \begin{bmatrix} x_1 \\ -x_2 \\ -x_1^2 + x_2^2 \end{bmatrix} \middle| \begin{bmatrix} 0 \\ -x_1 \\ 0 \end{bmatrix} + \lambda_2 \begin{bmatrix} x_1 \\ -x_2 \\ -x_1^2 + x_2^2 \end{bmatrix} \right)$$

Si consideri ora un sistema di equazioni lineari su R del tipo

$$\mathcal{A}\mathcal{X} + \mathcal{B} = 0 \mod N \tag{2.3}$$

dove $\mathcal{A} \in R^{r\times s}$, $\mathcal{B} \in R^{r\times t}$ e $N \subseteq R^r$ è un R-modulo.

Proposizione 2.2.3. *Nelle ipotesi della Proposizione 2.2.2, sia M' il sottomodulo di R^{r+t+s} descritto dalla matrice*

$$\mathcal{M}' = \begin{pmatrix} \mathcal{N} & \mathcal{B} & \mathcal{A} \\ \boldsymbol{0} & \mathcal{I}_t & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \mathcal{I}_s \end{pmatrix}$$

e sia $N \subseteq R^r$ è il modulo generato dalle colonne di $\mathcal{N}$. Allora la base di Gröbner di M' rispetto a μ è della forma

$$GB_\mu(M') = \begin{pmatrix} GB_{\mu|_{R^r}}(A+B+N) & \mathbf{0} & \mathbf{0} \\ * & GB_{\mu|_{R^t}}(C) & \mathbf{0} \\ * & \mathcal{D} & GB_{\mu|_{R^s}}(E) \end{pmatrix}$$

e le soluzioni descritte da $\mathcal{D}$ ed E come nella Proposizione 2.2.2 sono soluzioni dell'equazione (2.3).

Dimostrazione. Trovare $\mathcal{X}$ tale che $\mathcal{A}\mathcal{X} + \mathcal{B} = 0 \mod N$ è equivalente a trovare $\mathcal{X}$ tale che esista $\mathcal{K}$ con $\mathcal{A}\mathcal{X} + \mathcal{B} = \mathcal{N}\mathcal{K}$. Si osservi che

$$\mathcal{A}\mathcal{X} + \mathcal{B} = \mathcal{N}\mathcal{K} \iff \mathcal{A}\mathcal{X} - \mathcal{N}\mathcal{K} + \mathcal{B} = 0 \iff \begin{pmatrix} \mathcal{A} & \mathcal{N} \end{pmatrix} \begin{pmatrix} \mathcal{X} \\ -\mathcal{K} \end{pmatrix} + \mathcal{B} = 0$$

Applicando la proposizione precedente, è possibile calcolare le soluzioni di questo sistema trovando la base di Gröbner del sottomodulo descritto dalla matrice

$$\begin{pmatrix} \mathcal{B} & \mathcal{A} & \mathcal{N} \\ \mathcal{I}_t & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathcal{I}_s & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathcal{I}_n \end{pmatrix}$$

dove n è il numero di colonne di $\mathcal{N}$. Dato che ai fini della tesi non è importante conoscere i valori assunti da $\mathcal{K}$, è possibile omettere la computazione di tali valori rimuovendo la matrice $\mathcal{I}$ sotto al blocco $\mathcal{N}$. Questo è possibile in quanto il calcolo di $\mathcal{K}$ non influisce sul calcolo degli altri blocchi come è possibile notare ripercorrendo la dimostrazione della Proposizione 2.2.2. Di conseguenza riordinando le colonne si ottiene esattamente la matrice in ipotesi, e calcolando la sua base di Gröbner si otterranno unicamente i valori di $\mathcal{X}$ come voluto. □

Note sull'efficienza

Esiste un metodo più ovvio per la risoluzione dei sistemi lineari come quello nell'equazione (2.1). Basta infatti verificare se le colonne di $\mathcal{B}$ appartengono ad A sottomodulo descritto dalla matrice $\mathcal{A}$, e in tal caso individuare una soluzione particolare e la soluzione generale del sistema di equazioni lineari.

Per fare questo basta applicare la Proposizione 2.2.1 e calcolare la base di Gröbner del modulo descritto dalla matrice $\begin{pmatrix}\mathcal{A}\\ \mathcal{I}_s\end{pmatrix}$ in modo da ottenere

$$\begin{pmatrix}\mathrm{GB}_{\mu|_{R^r}}(A) & \mathbf{0}\\ \mathcal{A}' & \mathrm{GB}_{\mu|_{R^s}}(\mathrm{Syz}(\mathcal{A}))\end{pmatrix}$$

dove $\mathcal{A}'$ è la matrice le cui colonne sono le rappresentazioni dei vettori di $\mathrm{GB}_{\mu|_{R^r}}(A)$ rispetto ai generatori iniziali di A, ovvero $\mathrm{GB}_{\mu|_{R^r}}(A) = \mathcal{A}' \cdot \mathcal{A}$.
A questo punto per verificare se i generatori di B appartengono ad A basta ridurli rispetto a $\mathrm{GB}_{\mu|_{R^r}}(A)$ ottenendone anche una rappresentazione $\mathcal{R}$ (ovvero tale che $\mathcal{B} = \mathcal{R} \cdot \mathrm{GB}_{\mu|_{R^r}}(A)$) grazie alla procedura NR.
Una soluzione particolare si trova quindi moltiplicando la matrice delle relazioni per $\mathcal{A}'$, infatti dalle relazioni precedenti si ottiene $\mathcal{B} = (\mathcal{R} \cdot \mathcal{A}') \cdot \mathcal{A}$.
Infine la soluzione generale $\mathcal{X}$ tale che $\mathcal{A}\mathcal{X} = 0$ è data esattamente da un insieme di generatori del modulo $\mathrm{Syz}(\mathcal{A})$ per definizione.

Per un algoritmo migliore, dato che non è necessaria una base di Gröbner del modulo $\mathrm{Syz}(\mathcal{A})$ ma solo un suo insieme di generatori generico, basta applicare l'algoritmo di Buchberger esteso tenendo nota delle sizigie individuate senza proseguire calcolandone una base di Gröbner, come invece previsto dalla Proposizione 2.2.1.

Questo secondo metodo risulta di poco più efficiente del metodo proposto nella Proposizione 2.2.2, poiché evita computazioni non necessarie come la costruzione delle basi di Gröbner delle matrici nei blocchi superiori. Inoltre, utilizzando l'algoritmo di Buchberger esteso, si evita la notazione matriciale del problema.

Il problema dell'efficienza ridotta può essere compensato modificando l'algoritmo opportunamente, in modo che i due procedimenti risultino infine equivalenti.
La prima ottimizzazione possibile consiste nel troncare la computazione nel momento in cui, dal calcolo delle componenti $r+1, \ldots, r+t$, risulti evidente che non può comparire un'identità, e quindi il sistema risulti anticipatamente senza soluzioni.
Una seconda ottimizzazione prevede di sostituire il procedimento con l'applicazione dell'algoritmo di Buchberger esteso alle sole prime r componenti della matrice nella Proposizione 2.2.2, ovvero al modulo generato dalle colonne di

$$\begin{pmatrix}\mathcal{B} & \mathcal{A}\end{pmatrix}$$

Come sopra, questo basta in quanto è sufficiente un insieme di generatori del modulo delle soluzioni generali. Inoltre, in questo modo, viene nuovamente rimossa la notazione matriciale.

2.2.3 Preimmagine tramite morfismi di moduli

Proposizione 2.2.4. *Sia $\phi : R^s \to R^r$ un morfismo di moduli definito dalla matrice $\mathcal{M}$, e M il sottomodulo di R^r generato dalle colonne di $\mathcal{M}$. Sia $\mathcal{N} \in R^{r\times t}$ e N il sottomodulo di R^r generato dalle colonne di $\mathcal{N}$. Sia M' il sottomodulo di R^{r+s} descritto dalla matrice*

$$\mathcal{M}' = \begin{pmatrix} \mathcal{N} & \mathcal{M} \\ \boldsymbol{0} & \mathcal{I}_s \end{pmatrix}$$

e sia μ un ordinamento lessicografico sulle componenti su R^{r+s}. Allora la base di Gröbner di M' rispetto a μ è della forma

$$GB_\mu(M') = \begin{pmatrix} GB_{\mu|_{R^r}}(N+M) & \mathbf{0} \\ * & GB_{\mu|_{R^s}}(\phi^{-1}(N)) \end{pmatrix}$$

dove l'asterisco è un blocco costituito da opportuni polinomi.

Dimostrazione. Basta osservare che

$$\begin{aligned}\phi^{-1}(N) &= \{\, v \in R^s \mid \phi(v) \in N\} = \{\, v \in R^s \mid \mathcal{M}v \in N \,\} = \\ &= \{\, v \in R^s \mid \mathcal{M}v = 0 \mod N \,\}\end{aligned}$$

ovvero gli elementi di $\phi^{-1}(N)$ sono tutte e solo le soluzioni di $\mathcal{M}\mathcal{X} = 0 \mod N$. La tesi segue dalla Proposizione 2.2.3. □

2.2.4 Intersezione

Proposizione 2.2.5. *Siano M e N sottomoduli di R^r descritti rispettivamente dalle matrici $\mathcal{M} \in R^{r\times s}$ e $\mathcal{N} \in R^{r\times t}$. Sia M' il sottomodulo di R^{2r} descritto dalla matrice*

$$\mathcal{M}' = \begin{pmatrix} \mathcal{M} & \mathcal{N} \\ \boldsymbol{0} & \mathcal{N} \end{pmatrix}$$

e sia μ un ordinamento lessicografico sulle componenti su R^{2r}. Allora la base di Gröbner di M' rispetto a μ è della forma

$$GB_\mu(M') = \begin{pmatrix} GB_{\mu|_{R^r}}(M+N) & \mathbf{0} \\ * & GB_{\mu|_{R^r}}(M \cap N) \end{pmatrix}$$

dove gli asterischi sono blocchi costituiti da opportuni polinomi.

Dimostrazione. Trovare un vettore v tale che $v \in M \cap N$ è equivalente a trovare v tale che $v \in M$ e $v \in N$, ovvero tale che esista $\mathcal{X}$ tale che $\mathcal{N}\mathcal{X} = v \in M$. Quindi per trovare $v \in M \cap N$ basta risolvere il sistema $\mathcal{N}\mathcal{X} = 0 \mod M$ per poi moltiplicare le soluzioni per $\mathcal{N}$. Per la Proposizione 2.2.3 basterebbe trovare la base di Gröbner del sottomodulo descritto dalla matrice

$$\begin{pmatrix} \mathcal{M} & \mathcal{N} \\ \mathbf{0} & \mathcal{I}_r \end{pmatrix}$$

e quindi moltiplicare le soluzioni calcolate come nella Proposizione 2.2.2 per $\mathcal{N}$, ma è possibile eseguire la moltiplicazione anticipatamente, facendo il prodotto tra $\mathcal{N}$ e il blocco $\mathcal{I}_r$ sotto a $\mathcal{N}$, ottenendo la tesi. □

Esempio 2.2.2. Si vuole calcolare l'intersezione tra i due sottomoduli di $\mathbb{Q}[x_1, x_2]^2$ $M = \langle [x_1^2, 1],\ [x_1x_2 + x_2^2, 0] \rangle$ e $N = \langle [x_2^2, 1], [x_1x_2, 0] \rangle$. Si considera la matrice

$$\begin{pmatrix} \begin{bmatrix} x_1^2 & x_1x_2 + x_2^2 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x_2^2 & x_1x_2 \\ 1 & 0 \end{bmatrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \quad \begin{bmatrix} x_2^2 & x_1x_2 \\ 1 & 0 \end{bmatrix} \end{pmatrix}$$

e si computa una sua base di Gröbner rispetto a $\mu =$ Poslex ordinamento su M. Si ottiene

$$\begin{pmatrix} \begin{bmatrix} x_1^2 & x_1x_2 & x_2^2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} \\ \begin{matrix} -x_1x_2 - x_2^2 & x_1x_2 & -x_1x_2 & x_1x_2 + x_2^2 \\ -1 & 0 & 0 & 1 \end{matrix} & \begin{bmatrix} x_1^2x_2 + x_1x_2^2 & x_2^3 & 0 \\ 0 & x_2 & x_1^2x_2 + x_1x_2^2 \end{bmatrix} \end{pmatrix}$$

perciò per la proposizione si ha $M \cap N = \langle [x_1^2x_2 + x_1x_2^2, 0], [x_2^3, x_2], [0, x_1^2x_2 + x_1x_2^2] \rangle$. È riportato il codice in CoCoA in Appendice in Figura A.1.

2.2.5 Quoziente per un vettore

Proposizione 2.2.6. *Sia M un sottomodulo di R^r descritto dalla matrice $\mathcal{M} \in R^{r \times s}$, e sia $v \in R^r$ un vettore. Sia M' il sottomodulo di R^{r+1} descritto dalla matrice*

$$\mathcal{M}' = \begin{pmatrix} \mathcal{M} & v \\ \boldsymbol{0} & 1 \end{pmatrix}$$

e sia μ un ordinamento lessicografico sulle componenti su R^{r+1}. Allora la base di Gröbner di M' rispetto a μ è della forma

$$GB_\mu(M') = \begin{pmatrix} GB_{\mu|_{R^r}}(M + \langle v \rangle) & \mathbf{0} \\ * & GB_{\mu|_R}(M : \langle v \rangle) \end{pmatrix}$$

dove gli asterischi sono blocchi costituiti da opportuni polinomi.

Dimostrazione. Trovare un vettore w tale che $w \in M : \langle v \rangle$ è equivalente a trovare w tale che $v \cdot w \in M$. Quindi per trovare un tale vettore basta risolvere il sistema $v \cdot w = 0 \mod M$ ovvero, per la Proposizione 2.2.3, trovare la base di Gröbner del sottomodulo descritto dalla matrice presentata nell'enunciato. □

2.3 Composizione di operazioni

In questa sezione saranno presentati alcuni esempi di composizione di operazioni elementari tra moduli, in particolare per il calcolo di oggetti interessanti dal punto di vista algebrico come intersezioni multiple e quoziente generico tra moduli.

2.3.1 Intersezioni multiple

Si vogliono intersecare $M_1, \dots, M_t$ sottomoduli di R^r. Un possibile algoritmo consiste nel considerare il sottomodulo di $R^{r(t+1)}$ descritto dalla matrice

$$\begin{pmatrix} \mathcal{I}_r & \mathcal{M}_1 & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots & \cdots \\ \mathcal{I}_r & \mathbf{0} & \cdots & \mathcal{M}_t \\ \mathcal{I}_r & \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix}$$

dove $\mathcal{M}_i$ descrive il sottomodulo M_i, e calcolarne una base di Gröbner rispetto a un ordinamento lessicografico sulle componenti. Usando la Proposizione 2.2.1 si ha infatti che questo consente di calcolare le prime r componenti del nucleo del morfismo ϕ definito dalla matrice

$$\begin{pmatrix} \mathcal{I}_r & \mathcal{M}_1 & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots & \cdots \\ \mathcal{I}_r & \mathbf{0} & \cdots & \mathcal{M}_t \end{pmatrix}$$

Basta quindi osservare che

$$[f_0, f_1, \dots, f_t] \in \ker(\phi) \iff \begin{cases} \mathcal{M}_1 f_1 = -f_0 \\ \vdots \\ \mathcal{M}_t f_t = -f_0 \end{cases} \iff f_0 \in M_1 \cap \cdots \cap M_t$$

dove $f_0 \in R^r$.

Osservazione 2.3.1. Lo stesso algoritmo si può applicare all'intersezione elementare tra due moduli M e N calcolando una base di Gröbner del sottomodulo descritto dalla matrice

$$\begin{pmatrix} \mathcal{I}_r & \mathcal{M} & \mathbf{0} \\ \mathcal{I}_r & \mathbf{0} & \mathcal{N} \\ \mathcal{I}_r & \mathbf{0} & \mathbf{0} \end{pmatrix}$$

Confrontando con l'algoritmo presentato nella Proposizione 2.2.5, è immediato chiedersi quindi quale tra i due sia più efficiente dal punto di vista computazionale. Allo stesso modo, per il calcolo di intersezioni multiple, si potrebbero mettere a confronto questo algoritmo con l'ovvia procedura che consiste nell'applicare più volte l'algoritmo di intersezione della Proposizione 2.2.5. Non saranno presentate qui maggiori considerazioni sul problema, che in generale dipende fortemente dagli oggetti dati in input, ma potrebbe essere interessante approfondire.

Esempio 2.3.1. Si consideri l'Esempio 2.2.2. Calcolando ora la base di Gröbner di

$$\begin{pmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_1^2 & x_1x_2 + x_2^2 \\ 1 & 0 \end{bmatrix} & 0 & 0 \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 0 & 0 & \begin{bmatrix} x_2^2 & x_1x_2 \\ 1 & 0 \end{bmatrix} \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 0 & 0 & 0 & 0 \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 0 & 0 & 0 & 0 \end{pmatrix}$$

si ottiene la matrice

$$\begin{pmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & x_1^2 & x_2^2 & x_1x_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} & & \mathbf{0} \\ & * & \\ & & \begin{bmatrix} x_1^2x_2 + x_1x_2^2 & x_2^3 & 0 \\ 0 & x_2 & x_1^2x_2 + x_1x_2^2 \end{bmatrix} \end{pmatrix}$$

da cui si ha nuovamente $M \cap N = \langle [x_1^2x_2 + x_1x_2^2, 0], [x_2^3, x_2], [0, x_1^2x_2 + x_1x_2^2] \rangle$. In questo semplice caso non si evidenziano differenze tra i due algoritmi nei tempi di computazione[1]. È riportato il codice in CoCoA in Appendice in Figura A.1.

2.3.2 Quoziente tra moduli

Si vuole calcolare il quoziente tra M e N sottomoduli di R^r. Per ricondursi ai risultati precedenti si può usare il fatto che, se $N = \langle g_1, \ldots, g_t \rangle$, allora

$$M : N = \bigcap_{i=1}^{t} (M : \langle g_i \rangle)$$

Più in generale, dati $M_1, \ldots, M_t$ sottomoduli di R^r e $g_1, \ldots, g_t \in R^r$, si vuole calcolare $\bigcap_{i=1}^{t} (M_i : \langle g_i \rangle)$. A questo scopo basta calcolare la base di Gröbner rispetto a un ordinamento lessicografico sulle componenti del sottomodulo di R^{rt+1} descritto dalla matrice

$$\begin{pmatrix} \mathcal{M}_1 & \cdots & \mathbf{0} & g_1 \\ \cdots & \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathcal{M}_t & g_t \\ \mathbf{0} & \cdots & \mathbf{0} & 1 \end{pmatrix}$$

dove $\mathcal{M}_i$ descrive il sottomodulo M_i. Si conclude grazie alla Proposizione 2.2.6[2].

Osservazione 2.3.2. Come nel caso delle intersezioni, potrebbe risultare interessante confrontare l'algoritmo presentato con la procedura che consiste nel calcolare prima i singoli quozienti, e quindi la loro intersezione.

Esempio 2.3.2. Si vuole calcolare il quoziente tra i moduli $M = \langle [x_1, x_2], [x_2, x_1] \rangle$ e $N = \langle [x_1^2, x_2^2], [x_2^2, x_1^2] \rangle$ di $\mathbb{Q}[x_1, x_2]^2$. A tale scopo si considera la matrice

$$\begin{pmatrix} \begin{bmatrix} x_1 & x_2 \\ x_2 & x_1 \end{bmatrix} & 0 & 0 & \begin{bmatrix} x_1^2 \\ x_2^2 \end{bmatrix} \\ 0 & 0 & \begin{bmatrix} x_1 & x_2 \\ x_2 & x_1 \end{bmatrix} & \begin{bmatrix} x_2^2 \\ x_1^2 \end{bmatrix} \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

[1] I tempi sono stati calcolati a partire da implementazioni ad alto livello. I confronti sono quindi utili per una prima valutazione degli algoritmi ma non devono essere considerati fortemente rilevanti.

[2] In alternativa è possibile utilizzare l'algoritmo presentato per le intersezioni multiple combinato con l'algoritmo per i quozienti elementari, ma la matrice risulterebbe nettamente più grande. Si veda [3] per approfondire.

e si computa una sua base di Gröbner rispetto a μ = Poslex ordinamento su M. Si ottiene

$$\begin{pmatrix} \begin{bmatrix} x_1 & x_2 & 0 & 0 & 0 & 0 & 0 \\ x_2 & x_1 & 0 & 0 & 0 & x_1^2 - x_2^2 & x_1x_2 - x_2^2 \\ 0 & 0 & x_1 & x_2 & 0 & 0 & 0 \\ 0 & 0 & x_2 & x_1 & x_1^2 - x_2^2 & 0 & x_1x_2 - x_2^2 \end{bmatrix} & \begin{matrix} 0 \\ 0 \\ 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{matrix} & \begin{bmatrix} x_1 + x_2 \end{bmatrix} \end{pmatrix}$$

da cui si ha $M : N = \langle x_1 + x_2 \rangle$.

2.3.3 Intersezione di preimmagini

Può essere utile calcolare l'intersezione delle preimmagini di un sottomodulo $N \subseteq R^r$ rispetto a diverse mappe $\phi_1, \ldots, \phi_t : R^s \to R^r$ definite da matrici $\mathcal{M}_1, \ldots, \mathcal{M}_t$. Si può però notare che essa coincide con la preimmagine di N^t rispetto alla mappa $(\phi_1, \ldots, \phi_t) : R^s \to R^{rt}$. Per la Proposizione 2.2.4 basta quindi considerare il sottomodulo di R^{rt+s} descritto dalla matrice

$$\begin{pmatrix} \mathcal{N} & \mathcal{M}_1 \\ \cdots & \cdots \\ \mathcal{N} & \mathcal{M}_t \\ \mathbf{0} & \mathcal{I}_s \end{pmatrix}$$

dove $\mathcal{N}$ rappresenta il modulo N, e calcolarne la base di Gröbner rispetto a un ordinamento lessicografico sulle componenti.

Capitolo 3

Parallelismi tra Buchberger e altri algoritmi classici

Nelle pagine precedenti sono state presentate nozioni e procedure relative al calcolo di basi di Gröbner, e ne sono state esibite applicazioni per operare su moduli sotto molti aspetti. È tuttavia possibile dare altre interpretazioni all'algoritmo di Buchberger, quest'ultimo può quindi avere ripercussioni anche su ambiti differenti rispetto alla pura algebra computazionale.

3.1 Algoritmo di eliminazione di Gauss

La prima procedura con cui è possibile fare un confronto è il noto algoritmo di eliminazione di Gauss per il calcolo di una forma a scalini di una matrice e della sua inversa. L'idea della similitudine nasce dalla forma a blocchi presentata nell'Osservazione 2.1.1, che è appunto paragonabile a una forma a scalini, anche se non equivalente come si vedrà nel seguito.

Prima di guardare più in generale all'algoritmo di Buchberger applicato a moduli senza uno specifico ordinamento, è utile osservare alcuni casi più particolari in cui l'analogia tra i due diversi algoritmi risulta più forte.

L'algoritmo di riduzione di Gauss in effetti è essenzialmente un caso particolare dell'algoritmo di Buchberger applicato ad ideali specifici. Per capire meglio quest'asserzione, conviene chiarire con un esempio.

Esempio 3.1.1. Si supponga di voler risolvere il seguente sistema di equazioni lineari

$$\begin{cases} 3x_1 - 2x_2 + 4x_3 + 5x_4 = 0 \\ x_1 - x_2 + 3x_4 = 0 \\ 2x_1 + 8x_3 - 2x_4 = 0 \end{cases}$$

Usando l'algoritmo di Gauss si porta la matrice dei coefficienti nella sua forma a scalini come segue

$$\begin{pmatrix} 3 & -2 & 4 & 5 \\ 1 & -1 & 0 & 3 \\ 2 & 0 & 8 & -2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & -1 & 0 & 3 \\ 0 & 1 & 4 & -4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

da cui si otterrebbe il sistema ridotto

$$\begin{cases} x_1 - x_2 + 3x_4 = 0 \\ x_2 + 4x_3 - 4x_4 = 0 \end{cases}$$

Si consideri invece il seguente ideale

$$I = \langle 3x_1 - 2x_2 + 4x_3 + 5x_4, x_1 - x_2 + 3x_4, 2x_1 + 8x_3 - 2x_4 \rangle \subseteq k[x_1, x_2, x_3, x_4]$$

generato dai polinomi presenti nel sistema di equazioni iniziale. Dato $\tau = \text{lex}$ come ordinamento su T^n, si può osservare usando il Teorema 1.2.1 che l'insieme $G = \{x_1 - x_2 + 3x_4, x_2 + 4x_3 - 4x_4\}$ dato dal sistema finale è un insieme di generatori di I e ne è una base di Gröbner. In particolare è una base di Gröbner minimale, cioè tale che $\forall g \in G\ \text{LT}_\tau(g) \notin \text{LT}_\tau(G \setminus \{g\})$. Portando invece la matrice dei coefficienti nella sua forma a scalini ridotta si ottiene

$$\begin{pmatrix} 1 & 0 & 4 & -1 \\ 0 & 1 & 4 & -4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

da cui l'insieme di polinomi $G = \{x_1 + 4x_3 - x_4, x_2 + 4x_3 - 4x_4\}$ che è in particolare una base di Gröbner ridotta di I. In effetti l'algoritmo di Buchberger applicato all'insieme

$$G = \{3x_1 - 2x_2 + 4x_3 + 5x_4, x_1 - x_2 + 3x_4, 2x_1 + 8x_3 - 2x_4\}$$

trova che l'S-polinomio dei primi due generatori è $x_2 + 4x_3 - 4x_4$, che viene aggiunto a G, mentre i successivi vengono ridotti a 0. Effettuando la riduzione si ottiene quindi la base di Gröbner precedente.

Osservazione 3.1.1. Dall'esempio si osserva che ogni operazione dell'algoritmo di eliminazione corrisponde ad un'operazione compiuta dall'algoritmo di Buchberger: la moltiplicazione di una riga della matrice per uno scalare equivale alla sostituzione di uno dei generatori della base con un suo multiplo scalare; la somma di una riga ad un'altra equivale alla sostituzione di un generatore con la somma di altri due; lo scambio di due righe equivale allo scambio di due generatori. In tutti i casi l'operazione in Buchberger ha senso in quanto si sta operando solo con prodotti per scalari nel campo k, quindi dopo le sostituzioni i vettori nella base continuano a generare l'ideale di partenza.

Osservazione 3.1.2. L'analogia si può estendere a ideali generati da polinomi contenenti un termine costante, la matrice $\mathcal{A}$ associata ai generatori dell'ideale avrà $n+1$ colonne di cui l'ultima conterrà i termini noti dei generatori.

Osservazione 3.1.3. Non è necessario restringersi a $\tau = \text{lex}$. Si possono ripetere le medesime osservazioni fatte considerando un qualsiasi ordinamento di termini τ su T^n tale che $x_1 \geq_\tau x_2 \geq_\tau \cdots \geq_\tau x_n$. Anche l'osservazione precedente ha significato in quanto dalla Definizione 1.1.4 segue sempre $x_n \geq_\tau 1$.

È possibile quindi enunciare il risultato generale che segue.

Proposizione 3.1.1. [12] *Sia* $\mathcal{A} = (a_{ij}) \in k^{s\times n}$ *e siano* $\forall i = 1, \dots, s$ $g_i = \sum_{j=1}^{n} a_{ij}x_j$ *i polinomi lineari determinati dalle righe di* $\mathcal{A}$*. Si consideri quindi l'ideale* $I = \langle g_1, \dots, g_s\rangle \subseteq k[x_1, \dots, x_n]$*. Sia ora* $\mathcal{B} = (b_{ij}) \in k^{s'\times n}$ *la forma a scalini di* $\mathcal{A}$ *e siano* $\forall i = 1, \dots, s'$ $g'_i = \sum_{j=1}^{n} b_{ij}x_j$ *i polinomi determinati dalle righe di* $\mathcal{B}$*. Allora* $G = \{\, g'_i : 1 \le i \le s', g'_i \neq 0 \,\}$ *è una base di Gröbner minimale di* I *rispetto a un ordinamento* τ *su* $k[x_1, \dots, x_n]$ *tale che* $x_1 \ge_\tau x_2 \ge_\tau \cdots \ge_\tau x_n$*. Inoltre, se* $\mathcal{B}$ *è una forma a scalini ridotta, allora* G *è una base di Gröbner ridotta.*

Dimostrazione. Il fatto che l'insieme di polinomi G continui a generare I segue da quanto visto nell'Osservazione 3.1.1. Si mostra ora che G è una base di Gröbner usando il Teorema 1.2.1. Basta quindi verificare che $\mathrm{NR}_{\tau,\{g'_i,g'_j\}}(\mathrm{S}(g_i, g_j)) = 0$ $\forall i, j = 1, \dots, s'$ $i \neq j$. Questo è vero per il criterio enunciato nell'Osservazione 1.2.1 in quanto g_i e g_j hanno leading term che corrispondono ai pivot ottenuti nella forma ridotta della matrice, che si traducono in indeterminate distinte e perciò coprime. La base di Gröbner è minimale, cioè $\mathrm{LT}_\mu(g_i) \notin \mathrm{LT}(G \setminus \{g_i\})$, si nuovo perché i leading term dei polinomi contengono indeterminate distinte. Nel caso di una forma a scalini ridotta i polinomi in G soddisfano ovviamente $\mathrm{LC}_\tau(g_i) = 1$, e come sopra vale $\mathrm{LT}_\tau(g_i) \notin \mathrm{LT}_\tau(G \setminus \{g_i\})$. Infine vale $\mathrm{NR}_{\tau,G\setminus\{g_i\}}(g_i) = g_i$ infatti, per come si determinano i polinomi a partire dalla matrice ridotta che ha elementi nulli in alto e in basso rispetto ai pivot, si osserva che i termini di g_i non contengono indeterminate presenti nei leading term dei polinomi in $G \setminus \{g_i\}$. Quindi G è una base di Gröbner ridotta di I. □

Osservazione 3.1.4. Questa interpretazione dell'algoritmo di Buchberger permette nello specifico di vedere l'unicità della forma a scalini ridotta di una matrice come un caso particolare dell'unicità della base di Gröbner ridotta enunciata nel Teorema 1.2.2.

Osservazione 3.1.5. Si potrebbe enunciare una proposizione analoga alla Proposizione 3.1.1 considerando, piuttosto che i polinomi associati alle matrici, i vettori corrispondenti alle righe di $\mathcal{A}$ e $\mathcal{B}$. Di conseguenza, invece dell'ideale I nell'enunciato, si potrebbe considerare il modulo $M \subseteq k^n$ generato dai vettori associati a $\mathcal{A}$, e l'insieme di generatori G costituito dai vettori associati a $\mathcal{B}$. Allora G è una base di Gröbner ridotta di M rispetto all'unico ordinamento[1] μ di moduli su k^n tale che $e_1 \ge_\mu e_2 \ge_\mu \cdots \ge_\mu e_n$.
Si è visto quindi che nel caso di ideali generati da polinomi di grado minore o uguale a 1, l'algoritmo di Buchberger si può tradurre automaticamente nell'algoritmo di riduzione di Gauss. Nel caso di ideali generici non è difficile generalizzare la costruzione della matrice $\mathcal{A}$ associata ai generatori dell'ideale, per esempio facendo corrispondere a ciascuna colonna un termine disponendole rispetto all'ordinamento posto su T^n, ma non si potrebbero ripetere gli stessi argomenti usati nella proposizione. È possibile però trovare un caso notevole per gli ideali generati da polinomi omogenei. Nel seguito sarà presentato solo un esempio, ma sarebbe possibile enunciare un risultato simile alla Proposizione 3.1.1 approfondendo la teoria sugli ideali omogenei [7, 11].

Esempio 3.1.2. Si consideri τ = lex ordinamento su T^n e $I \subseteq k[x_1, x_2, x_3]$ l'ideale generato da $\{x_1^2 - 2x_2^2 - 2x_2x_3 - x_3^2, -x_1x_2 + 2x_2x_3 + x_3^2, -x_1^2 + x_1x_2 + x_1x_3 + x_3^2\}$.

[1] L'unicità segue dalla Definizione 1.1.11.

Con l'algoritmo di Buchberger si trova che una sua base di Gröbner è l'insieme $G = \{x_1^2 - 2x_2^2 - 2x_2x_3 - x_3^2,\ x_1x_2 - 2x_2x_3 - x_3^2, x_1x_3 - 2x_2^2 + x_3^2, x_2^3 - \frac{3}{2}x_2x_3^2 - \frac{1}{2}x_3^3\}$. Se si ordinano i termini presenti nei generatori iniziali di I rispetto all'ordinamento τ, si può scrivere la matrice dei coefficienti e quindi ridurla nella sua forma a scalini come segue.

$$\begin{pmatrix} 1 & 0 & 0 & -2 & -2 & -1 \\ 0 & -1 & 0 & 0 & 2 & 1 \\ -1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & -2 & -2 & -1 \\ 0 & 1 & 0 & 0 & -2 & -1 \\ 0 & 0 & 1 & -2 & 0 & 1 \end{pmatrix}$$

Costruendo i polinomi corrispondenti, si ottengono i primi tre generatori della base di Gröbner di I trovata, ovvero i generatori omogenei di grado 2. Per trovare il polinomio omogeneo di grado 3, detti $\{g_1, g_2, g_3\}$ i generatori iniziali di I, si deve invece considerare la matrice dei coefficienti dell'insieme

$$\begin{aligned} \{&x_1g_1, x_2g_1, x_3g_1, \\ &x_1g_2, x_2g_2, x_3g_2, \\ &x_1g_3, x_2g_3, x_3g_3\} \end{aligned}$$

di nuovo con i termini ordinati rispetto a τ, e trovarne la forma ridotta. È riportato il codice in CoCoA in Appendice in Figura A.2.

Osservazione 3.1.6. L'insieme considerato per trovare i polinomi omogenei di grado 3 della base di Gröbner è in effetti l'insieme di tutti i polinomi omogenei di grado 3 ottenibili da $\{g_1, g_2, g_3\}$. Il procedimento è generalizzabile per trovare i polinomi omogenei di grado n della base di Gröbner di un ideale.

Dal caso particolare degli ideali generati da polinomi omogenei si vede come l'algoritmo di Gauss applicato a una determinata matrice non sia sempre conclusivo per trovare un base di Gröbner per l'oggetto che si sta considerando. Tuttavia, nei casi considerati, sono stati sempre ottenuti elementi contenuti nella base trovata con Buchberger, anche se parzialmente.

Si consideri ora l'algoritmo di Buchberger su moduli. Sia quindi $M \subseteq R^r$ un R-modulo. In questo caso non è più possibile convertire i generatori in una matrice a valori in un campo. Ci si concentra perciò sulla rappresentazione matriciale dei moduli presentata all'inizio del Capitolo 1. La matrice $\mathcal{M}$ associata al modulo è a valori nell'anello di polinomi $R = k[x_1, \ldots, x_n]$. Di nuovo, si guardi ad un esempio per capire cosa succede nel caso generale.

Esempio 3.1.3. Siano $r = 3$, $R = \mathbb{Q}[x_1, x_2]$, e sia $M \subseteq R^3$ modulo generato da $\{[x_1x_2, x_1, x_2], [x_2^2 + x_2, x_1 + x_2^2, x_1], [-x_1, x_2, x_1], [x_2^2, x_2, x_1]\}$. Sia μ = lexPos ordinamento su M. Il primo passo dell'algoritmo di Buchberger calcola l'S-vettore tra il primo e il terzo generatore ottenendo

$$\begin{bmatrix} x_1x_2 \\ x_1 \\ x_2 \end{bmatrix} + x_2 \cdot \begin{bmatrix} -x_1 \\ x_2 \\ x_1 \end{bmatrix} = \begin{bmatrix} 0 \\ x_1 + x_2^2 \\ x_1x_2 + x_2 \end{bmatrix}$$

che si riduce a $g_4 = [-x_2^3 - x_2, -x_2^2 + x_2, x_2]$. Il vettore g_4 viene quindi aggiunto alla base di partenza. Dal punto di vista delle matrici associate si ha il seguente

passaggio

$$\begin{pmatrix} x_1x_2 & x_2^2+x_2 & -x_1 & x_2^2 \\ x_1 & x_1+x_2^2 & x_2 & x_2 \\ x_2 & x_1 & x_1 & x_1 \end{pmatrix} \longrightarrow \begin{pmatrix} x_1x_2 & x_2^2+x_2 & -x_1 & x_2^2 & -x_2^3-x_2 \\ x_1 & x_1+x_2^2 & x_2 & x_2 & -x_2^2+x_2 \\ x_2 & x_1 & x_1 & x_1 & x_2 \end{pmatrix}$$

ovvero si ha l'aggiunta di una nuova colonna.

Osservazione 3.1.7. A differenza dei casi precedenti, per i moduli saranno considerati l'algoritmo di eliminazione di Gauss rispetto alle colonne e la corrispondente forma a scalini (ridotta), in quanto nella matrice associata al modulo i generatori sono disposti per colonne.

Dall'esempio si osserva che l'algoritmo di Buchberger non è una diretta trasposizione dell'algoritmo di Gauss, in quanto prevede l'aggiunta di generatori. Si è in effetti già visto, per esempio nell'Esempio 3.1.2 nel caso di ideali, che la base di Gröbner ridotta ha in generale più elementi dell'insieme di generatori di partenza.

Malgrado questo, tutte le operazioni compiute dall'algoritmo di Buchberger possono comunque essere interpretate come operazioni di colonna compiute dall'algoritmo di Gauss. Il calcolo dell'S-vettore è in effetti la somma di multipli di due colonne, e la sua riduzione è di nuovo la somma di multipli di tutte le colonne della matrice. La colonna risultante però non viene sostituita a una delle colonne precedenti, ma viene aggiunta alla fine della matrice. Questo accade ad ogni ciclo dell'algoritmo di Buchberger.
Nel caso di ideali generati da polinomi di primo grado si è però osservato che non risultavano colonne aggiunte. Questo si spiega con la riduzione della base che avviene alla fine dell'algoritmo, come si vede proseguendo con l'esempio.

Esempio 3.1.4. Nell'Esempio 3.1.3 l'algoritmo di Buchberger prosegue calcolando la seguente base di Gröbner.

$$\begin{pmatrix} x_1x_2 & x_2^2+x_2 & -x_1 & x_2^2 & -x_2^3-x_2 & -x_2^2 & x_2^2-2x_2 \\ x_1 & x_1+x_2^2 & x_2 & x_2 & -x_2^2+x_2 & -x_2^3 & -x_2^2+2x_2 \\ x_2 & x_1 & x_1 & x_1 & x_2 & x_2^3 & x_2^5-x_2^4-3x_2^3+x_2^2+2x_2 \end{pmatrix}$$

Si conclude infine con l'algoritmo di riduzione ottenendo la matrice che segue.

$$\begin{pmatrix} x_2 & x_1+x_2^2 & x_2^2 & x_2^3+x_2 & x_2^2 & x_2^2-2x_2 \\ x_1+x_2^2-x_2 & 0 & x_2 & x_2^2-x_2 & x_2^3 & -x_2^2+2x_2 \\ 0 & 0 & x_1 & -x_2 & -x_2^3 & x_2^5-x_2^4-3x_2^3+x_2^2+2x_2 \end{pmatrix}$$

Sono stati in effetti rimossi i generatori superflui e i rimanenti sono stati ridotti rispetto al resto della base.

La riduzione dei generatori è, come già osservato, un'operazione di somma di una colonna a multipli delle altre colonne.
Tuttavia si osserva anche la rimozione di generatori in eccesso. Se la riduzione venisse effettuata ad ogni passo dell'algoritmo di Buchberger, essa sarebbe più facilmente interpretabile rispetto all'algoritmo di Gauss come somma di una colonna ad un multiplo di un'altra colonna. In generale, tuttavia, il vettore aggiunto non può

essere sostituito a uno dei generatori precedenti, da cui si osserva l'aumento del numero di colonne, incompatibile con le operazioni dell'eliminazione di Gauss.

Viceversa, come già notato nell'Osservazione 3.1.1, l'applicazione dell'algoritmo di Gauss all'insieme di generatori di partenza è interpretabile come una parte dei passi dell'algoritmo di Buchberger. I due algoritmi risulterebbero nella stessa computazione se nell'algoritmo di Buchberger si omettesse il calcolo degli S-vettori. Si ricorda che nel caso generale si deve far attenzione al fatto che si sta operando su una matrice a coefficienti in un anello.

Esempio 3.1.5. Applicando dei passi ammissibili della riduzione di Gauss per colonne alla matrice dei coefficienti dell'Esempio 3.1.3, si produce la matrice che segue.

$$\begin{pmatrix} x_2 & x_1+x_2^2 & x_2^2 & -x_2^3-x_2 \\ x_1+x_2^2-x_2 & 0 & x_2 & -x_2^2+x_2 \\ 0 & 0 & x_1 & x_2 \end{pmatrix}$$

In effetti si ritrovano alcuni dei generatori presenti nella base di Gröbner ridotta individuata.

Osservazione 3.1.8. Nel caso generale il metodo di eliminazione di Gauss perde in realtà di significato, in quanto la riduzione in forma a scalini della matrice risulta compatibile con un ordinamento lessicografico sulle componenti. Nel caso di altri ordinamenti, come nell'esempio precedente, in effetti l'algoritmo di Gauss non effettuerebbe operazioni compatibili con l'ordinamento, ma che mirerebbero a ridurre inizialmente i polinomi nelle prime componenti.

Dall'osservazione precedente segue che il paragone assume significato considerando un ordinamento lessicografico sulle componenti. Si prende perciò in esame il caso dell'Osservazione 2.1.1, dove in effetti è maggiormente visibile la forma a scalini, in cui però non tutti gli elementi di una riga possono essere ridotti a zero rispetto al primo, a differenza di quanto accade in matrici a valori in un campo.

Dati i risultati ottenuti nell'Osservazione 2.1.1 per questa specifica classe di ordinamenti, si può però concludere che se R fosse un PID, si otterrebbe un'effettiva forma a scalini analoga alla forma ottenuta tramite l'algoritmo di eliminazione di Gauss, in quanto le $\mathrm{GB}_{\mu|_R}(I)$ sarebbero composte da un solo elemento.
Nel caso particolare di $R = k[x_1]$, per esempio, si avrebbe quindi una forma normale completamente affine.

Esempio 3.1.6. Siano $r = 3$, $R = \mathbb{Q}[x_1]$, e sia $M \subseteq R^3$ modulo generato da $\{[x_1^2+2, 2x_1, -x_1^3+4x_1], [x_1^2, x_1, x_1], [x_1^2+x_1, x_1^2+x_1, x_1], [x_1+1, x_1^2, x_1]\}$. Si consideri $\mu =$ Poslex ordinamento su M. La base di Gröbner di M posta in forma di matrice si presenta come segue.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & x_1 & 0 \\ x_1 & -x_1^3+x_1 & x_1^4-2x_1^2 \end{pmatrix}$$

È evidente la forma a scalini, seppure i pivot non si possono ridurre a 1 in quanto tali elementi non sono invertibili in R.

3.1.1 Calcolo della matrice inversa

Dall'analogia dell'algoritmo di Buchberger con l'algoritmo di Gauss è possibile trarre delle considerazioni anche riguardo l'algoritmo di Buchberger esteso.

In effetti la costruzione della matrice $\mathcal{A}$ delle rappresentazioni della base di Gröbner rispetto ai generatori iniziale può essere vista come l'applicazione delle stesse operazioni di colonna (o riga se si è nel caso di ideali) sia sui vettori della base, sia a una matrice identità.
Per questo motivo se $\mathcal{G}$ è la matrice associata all'insieme G dei generatori di partenza, e $\mathcal{G}'$ è la matrice associata a G' base di Gröbner in output, la matrice $\mathcal{A}$ ottenuta dall'algoritmo di Buchberger esteso è tale che $\mathcal{G}\mathcal{A} = \mathcal{G}'$.

Allo stesso modo porre sotto alla matrice $\mathcal{G}$ l'identità e applicare l'algoritmo di Gauss, produce una matrice $\begin{pmatrix} \mathcal{F} \\ \mathcal{B} \end{pmatrix}$ che ha tenuto traccia delle operazioni di colonna compiute, cioè di nuovo tale che $\mathcal{G}\mathcal{B} = \mathcal{F}$.
Nel caso in cui la matrice $\mathcal{G}$ è invertibile e, tramite operazioni di colonna, si ottiene $\mathcal{F} = \mathcal{I}$, allora come è noto si ha $\mathcal{B} = \mathcal{G}^{-1}$.

Se le computazioni dei due algoritmi coincidono, si avrà $\mathcal{A} = \mathcal{B}$.

Esempio 3.1.7. Nell'Esempio 3.1.1 l'algoritmo di Gauss coincide con l'algoritmo di Buchberger, e la matrice delle relazioni prodotta è la seguente.

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & \frac{1}{2} \\ 1 & -2 & -\frac{1}{2} \end{pmatrix}$$

In questo caso la matrice è stata prodotta tramite operazioni di riga.

3.1.2 Aspetti computazionali

Dal punto di vista computazionale, grazie al parallelismo tra i due algoritmi, la stabilità numerica del metodo di eliminazione Gaussiana si ripercuote sulla stabilità numerica dell'algoritmo di Buchberger. Ci si concentra quindi in particolare sull'analisi del caso di ideali generati da polinomi di grado al più 1.

È noto che l'algoritmo di Gauss applicato il maniera diretta non ha un buon comportamento numerico, in quanto l'errore in aritmetica floating point dipende dal modulo dei coefficienti della matrice e l'algoritmo produce in generale l'esplosione di tali elementi. Per questo si introducono le strategie del massimo pivot parziale e del massimo pivot totale, utili a limitare la crescita riducendo gli elementi rispetto a quello che ha modulo massimo.

Nel caso di Buchberger la strategia del massimo pivot totale non è applicabile, in quanto richiederebbe di ridurre i polinomi rispetto al termine che ha coefficiente più grande in modulo, tuttavia questo non sarebbe in generale compatibile con l'ordinamento imposto sui termini.
Ha invece senso considerare la strategia del massimo pivot parziale, che consiste nello

scegliere il generatore che ha leading term con coefficiente in modulo più grande per ridurre gli altri. In questo modo i coefficienti per cui si andrà a moltiplicare saranno in modulo limitati da 1. Tuttavia, questa strategia non è vantaggiosa come quella del massimo pivot totale, in quanto la limitazione dei coefficienti rimane comunque esponenziale. È possibile produrre esempi di casi problematici in questo senso.

Esempio 3.1.8. Si consideri l'ideale associato alla matrice che segue, la cui costruzione avviene come nell'Esempio 3.1.1.

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ -1 & 1 & 0 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$

La strategia del massimo pivot parziale non è utile in questo caso. La sequenza di operazioni dell'algoritmo di Gauss (e quindi di Buchberger) produce la seguente sequenza di matrici.

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & -1 & 1 & 2 \\ 0 & -1 & -1 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & -1 & 4 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 8 \end{pmatrix}$$

L'elemento posto in basso a destra aumenta ad ogni operazione come 2^n.

In generale, comunque, casi come questo sono fortemente artificiali e la strategia del massimo pivot parziale per l'algoritmo di Gauss è considerata numericamente stabile per matrici in generale.

Un'altra possibile strategia è evitare errori in aritmetica floating point effettuando i calcoli in aritmetica esatta. Questo è possibile rappresentando i razionali come coppie di interi. In questo caso nasce però il problema della dimensione degli interi usati: nel caso peggiore, quando si effettuano operazioni del tipo

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

con $a, b, c, d \in \mathbb{Z}$, il numeratore potrebbe non semplificarsi con il denominatore, e il denominatore potrebbe avere un numero di cifre pari alla somma delle cifre di b e d. Di nuovo, è facile trovare un esempio in cui si presenta il problema.

Esempio 3.1.9. Sia $I = \langle 3x_1 - 2x_2 - 7x_3, 5x_1 - 7x_2 + 6x_4, 2x_1 - 5x_2 - 2x_3 - 5x_4 \rangle$. L'algoritmo di Buchberger produce la computazione che segue.

$$\begin{pmatrix} 3 & -2 & -7 & 0 \\ 5 & -7 & 0 & 6 \\ 2 & -5 & -2 & -5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & \frac{431}{99} \\ 0 & 1 & 0 & \frac{223}{99} \\ 0 & 0 & 1 & \frac{11}{9} \end{pmatrix}$$

ovvero la base di Gröbner $G = \{x_1 + \frac{431}{99}x_4, x_2 + \frac{223}{99}x_4, x_3 + \frac{11}{9}x_4\}$.

3.2 Algoritmo euclideo

È possibile effettuare un paragone anche con l'algoritmo euclideo per il calcolo del massimo comun divisore tra polinomi. L'idea del paragone nasce dal risultato che segue.

Proposizione 3.2.1. [12] *Siano R un dominio a ideali principali, e $f_1, \ldots, f_s \in R \backslash 0$. Allora se si considera l'ideale $I = \langle f_1, \ldots, f_s \rangle$, si ha che $I = \langle \gcd(f_1, \ldots, f_s) \rangle$.*

Dimostrazione. Vale $f_i \in \langle \gcd(f_1, \ldots, f_s) \rangle \ \forall i = 1, \ldots, s$ in quanto $\gcd(f_1, \ldots, f_s) | f_i$ $\forall i = 1, \ldots, s$. Vale perciò $\langle f_1, \ldots, f_s \rangle \subseteq \langle \gcd(f_1, \ldots, f_s) \rangle$. Viceversa, sia $f \in R$ tale che $\langle f_1, \ldots, f_s \rangle = \langle f \rangle$ (esiste perché R è un dominio a ideali principali). Dato che $f | f_i$ $\forall i = 1, \ldots, s$ segue che $f | \gcd(f_1, \ldots, f_s)$, perciò $\gcd(f_1, \ldots, f_s) \in \langle f \rangle = \langle f_1, \ldots, f_s \rangle$. Si ha quindi $\langle f_1, \ldots, f_s \rangle \supseteq \langle \gcd(f_1, \ldots, f_s) \rangle$. □

Nella sezione che segue si prenderà quindi in considerazione $R = k[x_1]$ dominio a ideali principali. In particolare si studieranno ideali del tipo $I = \langle f_1, f_2 \rangle$ in quanto l'algoritmo euclideo è mirato al calcolo del massimo comun divisore tra due polinomi (anche se per iterazione può essere usato per calcolare il massimo comun divisore tra più polinomi).

In effetti si può osservare che anche l'algoritmo euclideo può essere visto come un caso particolare dell'algoritmo di Buchberger considerato in questo contesto specifico.

Corollario 3.2.1. *L'applicazione dell'algoritmo di Buchberger all'ideale $I = \langle f_1, f_2 \rangle$ produce la base $G = \{\gcd(f_1, f_2)\}$, con $\gcd(f_1, f_2)$ monico.*

Dimostrazione. Dalla Proposizione 3.2.1, si ha che $G = \{\gcd(f_1, f_2)\}$ è un insieme di generatori per l'ideale $I = \langle f_1, f_2 \rangle$, in particolare ne è una base di Gröbner minimale. Se $\gcd(f_1, f_2)$ è monico, allora si ha una base di Gröbner ridotta, e per l'unicità data dal Teorema 1.2.2 si ha che l'algoritmo di Buchberger produrrà esattamente tale base. □

Osservazione 3.2.1. Si noti che in questo caso la base di Gröbner ridotta non dipende dall'ordinamento scelto. In realtà, se $R = k[x_1]$, i possibili termini sono solo della forma $f = x_1^{\alpha_1}$ con $\alpha_1 \in \mathbb{N}$. Per la Definizione 1.1.4, si ha che l'unico ordinamento di termini possibile su R è quello tale che $1 < x_1 < x_1^2 < x_1^3 < \ldots$. Nel seguito tale ordinamento sarà denominato τ.

Di nuovo, si vuole ripercorrere un esempio per approfondire il paragone.

Esempio 3.2.1. Siano $f_1 = x_1^5 + x_1^3 + 4x_1^2 - 6x_1 + 12$, $f_2 = x_1^4 - x_1^3 - 3x_1 - 9$ due polinomi in $R = k[x_1]$. Si vuole calcolare $\gcd(f_1, f_2)$ utilizzando l'algoritmo euclideo.

$$
\begin{aligned}
f_1 &= (x_1 + 1) f_2 + (2x_1^3 + 7x_1^2 + 6x_1 + 21) && f_1 = q_1 f_2 + f_3 \\
f_2 &= \left(\frac{1}{2}x_1 - \frac{9}{4}\right) f_3 + \left(\frac{51}{4}x_1^2 + \frac{153}{4}\right) && f_2 = q_2 f_3 + f_4 \\
f_3 &= \left(\frac{8}{51}x_1 + \frac{28}{51}\right) f_4 && f_3 = q_3 f_4 + f_5
\end{aligned}
$$

Si ottiene $\gcd(f_1, f_2) = \frac{51}{4}x_1^2 + \frac{153}{4} \propto x_1^2 + 3$. Lo stesso polinomio è individuato dall'algoritmo di Buchberger, in accordo con il risultato teorico. Si vuole tuttavia analizzare il singolo passo. Posto $G = \{f_1, f_2\}$, il primo passo dell'algoritmo di Buchberger calcola

$$\mathrm{S}(f_1, f_2) = f_1 - x_1 \cdot f_2 = x_1^4 + x_1^3 + 7x_1^2 + 3x_1 + 12$$

quindi $\mathrm{NR}_{\tau,G}(\mathrm{S}(f_1, f_2)) = 2x_1^3+7x_1^2+6x_1+21$. Il primo resto prodotto dall'algoritmo euclideo, ovvero f_3, coincide quindi con il primo vettore aggiunto all'insieme G. Tuttavia è possibile fare delle osservazioni anche sull'S-polinomio prodotto. Si guardi alla divisione tra f_1 e f_2.

$$\begin{array}{rl|l} x_1^5 + x_1^3 + 4x_1^2 - 6x_1 + 12 & & x_1^4 - x_1^3 - 3x_1 - 9 \\ \cline{3-3} -x_1^5 + x_1^4 + 3x_1^2 + 9x_1 & & x_1 + 1 \\ \cline{1-2} x_1^4 + x_1^3 + 7x_1^2 + 3x_1 + 12 & & \\ -x_1^4 + x_1^3 + 3x_1 + 9 & & \\ \cline{1-2} 2x_1^3 + 7x_1^2 + 6x_1 + 21 & & \end{array}$$

Il polinomio ottenuto dopo il primo passo della divisione coincide con $\mathrm{S}(f_1, f_2)$. Ai passi successivi, calcolando gli S-polinomi per le coppie (f_2, f_3) e poi (f_3, f_4), si ottengono di nuovo le stesse computazioni dell'algoritmo euclideo. Infine l'algoritmo di Buchberger termina in quanto gli altri S-polinomi si riducono al polinomio nullo. Con la riduzione finale della base vengono rimossi tutti i generatori, ad eccezione del polinomio f_4, in quanto sono suoi multipli.

Dall'esempio precedente si possono ripercorrere i passi dell'algoritmo euclideo reinterpretandoli come passi dell'algoritmo di Buchberger, ponendo un accento sulle similitudini individuate.

Il primo passo della divisione euclidea tra due polinomi effettua la divisione tra il termine di grado massimo del primo e il termine di grado massimo del secondo, quindi moltiplica quanto ottenuto per il secondo polinomio e lo sottrae al primo.
Questo coincide con la computazione dell'S-polinomio tra i due a meno di costanti in quanto, considerando un anello di polinomi univariati e ricordando l'Osservazione 3.2.1, il minimo comune multiplo tra i leading term dei due polinomi sarà il termine di grado massimo. Dall'espressione per il calcolo dell'S-polinomio si ottiene quindi esattamente la differenza tra il polinomio di grado massimo e il polinomio di grado minimo moltiplicato per il rapporto tra i due leading term.

I passi successivi della divisione euclidea corrispondono invece alla riduzione dell'S-polinomio. In particolare la riduzione avviene sempre rispetto al polinomio di grado più basso tra i due da cui è stato calcolato, in quanto il suo leading term non è divisibile per il leading term del primo polinomio, infatti nel calcolo dell'S-polinomio il termine di grado più alto risulta semplificato.
Questo coincide con la divisione euclidea poiché essa mira a ridurre il risultato del primo passo andando a sottrarre multipli del divisore, ovvero del polinomio di grado più basso. A meno di costanti, la computazione risulta quindi uguale.

Risulta evidente che i procedimenti complessivamente possono coincidere esattamente solo se vengono calcolati solo gli S-polinomi delle coppie tra cui vengono effettua-

te le divisioni nell'algoritmo euclideo. È possibile in effetti far agire Buchberger in questo modo grazie al risultato che segue.

Proposizione 3.2.2. *Sia $R = k[x_1]$, e sia $I = \langle f_i, f_j \rangle \subseteq R$, con $\deg f_i \geq \deg f_j$. Allora vale anche $I = \langle f_j, NR_{\tau,\{f_i,f_j\}}(S(f_i, f_j)) \rangle$.*

Dimostrazione. Vale ovviamente $\mathrm{NR}_{\tau,\{f_i,f_j\}}(\mathrm{S}(f_i, f_j)) \in \langle f_i, f_j \rangle$. Dalle considerazioni precedenti segue che $\mathrm{S}(f_i, f_j) = (\frac{1}{\mathrm{LC}(f_i)})(f_i - g \cdot f_j)$ per qualche $g \in R$, e dato che viene ridotto solo rispetto a f_j si ha $\mathrm{NR}_{\tau,\{f_i,f_j\}}(\mathrm{S}(f_i, f_j)) = \mathrm{S}(f_i, f_j) - h \cdot f_j$ per qualche $h \in R$. Segue che

$$f_i = \mathrm{LC}(f_i)\mathrm{NR}_{\tau,\{f_i,f_j\}}(\mathrm{S}(f_i, f_j)) + (\mathrm{LC}(f_i)h + g) \cdot f_j \tag{3.1}$$

dunque $f_i \in \langle f_j, \mathrm{NR}_{\tau,\{f_i,f_j\}}(\mathrm{S}(f_i, f_j)) \rangle$. □

La proposizione, utilizzata iterativamente, suggerisce che ad ogni passo di Buchberger è possibile sostituire uno dei generatori con il nuovo polinomio calcolato, e quindi rimane un'unica scelta per la coppia di cui calcolare l'S-polinomio, che coincide con la coppia dell'algoritmo euclideo.

Osservazione 3.2.2. In effetti è possibile concludere un risultato più forte. Ad ogni passo di Buchberger, come si è visto, si può senza perdere generalità considerare la coppia (f_i, f_{i+1}). Siano g ed h sono i polinomi calcolati a partire da questa coppia di generatori come nella Proposizione 3.2.2, e q_i invece il quoziente della divisione euclidea ottenuto applicando un passo dell'algoritmo euclideo. Allora equiparando i due algoritmi si osserva che $q_i = \mathrm{LC}(f_i)h + g$, e quindi dalla relazione (3.1) confrontata con la relazione $f_i = q_i f_{i+1} + f_{i+2}$, si ottiene che $f_{i+2} = \mathrm{LC}(f_i)\mathrm{NR}_{\tau,\{f_i,f_j\}}(\mathrm{S}(f_i, f_j))$.

Osservazione 3.2.3. La Proposizione 3.2.1 può essere generalizzata all'anello $R = k[x_1, \ldots, x_n]$ nel caso di ideali $I = \langle f_1, f_2 \rangle$ principali. Le considerazioni precedenti permettono di affermare quindi che l'algoritmo di Buchberger può essere visto come una generalizzazione dell'algoritmo euclideo per il calcolo del $\gcd(f_1, f_2)$ anche nel caso di polinomi multivariati. Per lo stesso motivo osservazioni simili valgono per le sezioni che seguono.

3.2.1 Identità di Bezout

È naturale allargare il paragone all'algoritmo di Buchberger esteso e all'algoritmo euclideo esteso.

L'algoritmo euclideo esteso individua due polinomi m, n tali che

$$f_1 \cdot m + f_2 \cdot n = \gcd(f_1, f_2)$$

cioè l'identità di Bezout.

Si è visto che nell'algoritmo di Buchberger esteso viene costruita una matrice $\mathcal{A}$ tale che se $\mathcal{G} = (f_1, f_2)$ e $\mathcal{G}'$ è la matrice associata a G' base di Gröbner in output, allora $\mathcal{G}\mathcal{A} = \mathcal{G}'$. Se si suppone che G' abbia s' elementi, allora si è visto che la base di Gröbner ridotta coincide con $f_{s'} = \gcd(f_1, f_2)$.
Si denotano con a_{ij} gli elementi della matrice $\mathcal{A}$ e con a_j le sue colonne.

Dato che si vuole individuare una rappresentazione del polinomio $\gcd(f_1, f_2)$ rispetto a f_1 e f_2, basterà considerare l'ultima colonna di $\mathcal{A}$ infatti, per la relazione tra tale matrice, $\mathcal{G}$ e $\mathcal{G}'$, si avrà

$$\begin{pmatrix} f_1 & f_2 \end{pmatrix} \begin{pmatrix} a_{1,s'} \\ a_{2,s'} \end{pmatrix} = \gcd(f_1, f_2)$$

Si vuole quindi confrontare la costruzione dell'ultima colonna di $\mathcal{A}$ con la costruzione dei due polinomi m, n tramite l'algoritmo euclideo.
Si considera l'Esempio 3.2.1 per effettuare un paragone illustrativo.

Esempio 3.2.2. Per l'algoritmo euclideo, dalle equazioni ottenute tramite le divisioni euclidee successive, si ottengono le seguenti relazioni

$$\begin{aligned} f_3 &= f_1 - q_1 f_2 \\ f_4 &= f_2 - q_2 f_3 = -q_2 f_1 + (1 + q_2 q_1) f_2 \end{aligned}$$

da cui si trovano $m = -q_2 = -\frac{1}{2}x_1 + \frac{9}{4}$ e $n = 1 + q_2 q_1 = \frac{1}{2}x_1^2 - \frac{7}{4}x_1 - \frac{5}{4}$ che soddisfano $f_1 \cdot m + f_2 \cdot n = \gcd(f_1, f_2)$. D'altra parte, inizializzando $\mathcal{A} = \mathcal{I}$, l'algoritmo di Buchberger esteso produce le colonne

$$a_3 = \begin{pmatrix} 1 \\ -x_1 - 1 \end{pmatrix} \quad a_4 = \begin{pmatrix} -\frac{1}{2}x_1 + \frac{9}{4} \\ \frac{1}{2}x_1^2 - \frac{7}{4}x_1 - \frac{5}{4} \end{pmatrix}$$

che in effetti coincidono con le rappresentazioni dei polinomi f_3 e f_4 trovate utilizzando l'algoritmo euclideo.

In effetti dall'Osservazione 3.2.2 e dalle considerazioni che precedono, si possono ricavare le seguenti equazioni di ricorrenza per l'algoritmo euclideo e l'algoritmo di Buchberger rispettivamente

$$f_{i+2} = f_i - q_i f_{i+1} \qquad f_{i+2} = \frac{1}{\mathrm{LC}(f_i)}(f_i - q_i f_{i+1})$$

Per come avviene la costruzione di $\mathcal{A}$ nell'algoritmo di Buchberger esteso si ha quindi la relazione

$$a_{i+2} = \frac{1}{\mathrm{LC}(f_i)}(a_i - q_i a_{i+1}) \qquad a_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad a_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Siano invece m_i, n_i i coefficienti della rappresentazione di f_i rispetto a f_1, f_2 cioè i coefficienti tali che $f_i = f_1 \cdot m_i + f_2 \cdot n_i$. Dall'equazione di ricorrenza dell'algoritmo euclideo, si ricava

$$\begin{aligned} m_{i+2} &= m_i - q_i m_{i+1} & m_1 &= 1 & m_2 &= 0 \\ n_{i+2} &= n_i - q_i n_{i+1} & n_1 &= 0 & n_2 &= 1 \end{aligned}$$

Confrontando gli elementi in $a_{s'}$ con la coppia $(m_{s'}, n_{s'})$ si osserva che coincidono a meno di una costante. In effetti questo è in accordo con quanto visto in precedenza, in quanto i due algoritmi producono in output lo stesso polinomio a meno di una costante.

3.2.2 Equazioni diofantee

Si considerano equazione diofantee polinomiali del tipo

$$f_1 \cdot m + f_2 \cdot n = h \tag{3.2}$$

dove $f_1, f_2, h \in R = k[x]$ sono polinomi noti e $m, n \in R = k[x]$ incogniti. Per questo tipo di equazioni si ha il seguente risultato.

Teorema 3.2.1. [6] *L'equazione diofantea* (3.2) *ha soluzione se e solo se* $\gcd(f_1, f_2)$ *divide* h. *In tal caso, se* $[\overline{m}, \overline{n}]$ *è una soluzione particolare, allora tutte le altre soluzioni sono della forma* $[\overline{m} - kg_2, \overline{n} + kg_1]$, *dove* $g_1 = \frac{f_1}{\gcd(f_1,f_2)}$, $g_2 = \frac{f_2}{\gcd(f_1,f_2)}$ *e* $k \in R$.

Osservazione 3.2.4. La dimostrazione del teorema è elementare e viene qui omessa, ma la prima parte dell'enunciato può essere riletta considerando l'ideale $I = \langle f_1, f_2 \rangle$. In effetti un polinomio h può essere scritto come combinazione lineare di f_1 e f_2 se e solo se $h \in \langle f_1, f_2 \rangle = \langle \gcd(f_1, f_2) \rangle$, cioè se e solo se $\gcd(f_1, f_2)$ divide h.
Dalla precedente osservazione segue perciò che verificare se l'equazione (3.2) ha soluzione equivale a verificare se $h \in I = \langle f_1, f_2 \rangle$. In effetti si può verificare se $h \in I$ trovando una base di Gröbner G di I e controllando se $\mathrm{NR}_{\tau,G}(h) = 0$. Sapendo che applicando Buchberger a $\langle f_1, f_2 \rangle$ si trova proprio $\{\gcd(f_1, f_2)\}$, si ritrova la condizione necessaria e sufficiente di divisibilità enunciata nel teorema e si riscontra nuovamente l'analogia tra i due procedimenti dati dall'algoritmo euclideo e dall'algoritmo di Buchberger.
Allo stesso modo l'individuazione di una soluzione particolare dell'equazione (3.2) riporta all'analogia tra i rispettivi algoritmi estesi. In effetti, per individuare classicamente una soluzione particolare si utilizza l'algoritmo euclideo esteso per individuare la rappresentazione del $\gcd(f_1, f_2)$ rispetto a f_1 e f_2, moltiplicando poi la relazione individuata per $\frac{h}{\gcd(f_1,f_2)}$.

Similmente, la soluzione suggerita dall'algoritmo di Buchberger esteso è data dall'ottenere la rappresentazione di h rispetto alla base di Gröbner, che quindi sarà ovviamente $h = \frac{h}{\gcd(f_1,f_2)} \cdot \gcd(f_1, f_2)$, per poi sostituire in tale relazione la scrittura del $\gcd(f_1, f_2)$ rispetto a f_1 e f_2 data dalla matrice delle rappresentazione $\mathcal{A}$. Di conseguenza, grazie anche a quanto visto nelle sezioni precedenti, quindi, i due procedimenti sono corrispondenti.

Esempio 3.2.3. Si considerino i polinomi f_1, f_2 in $R = k[x_1]$ dell'Esempio 3.2.1, e sia $h = x_1^3 + x_1^2 + 3x_1 + 3 = (x_1^2 + 3)(x_1 + 1)$. Si vuole risolvere l'equazione diofantea $f_1 \cdot m + f_2 \cdot n = h$. Poiché $\gcd(f_1, f_2) = x_1^2 + 3$ divide h si ha che l'equazione ha soluzione. Per individuarne una soluzione particolare si deve considerare la rappresentazione del $\gcd(f_1, f_2)$ trovata nell'Esempio 3.2.2, ovvero $\gcd(f_1, f_2) = f_1 \cdot m + f_2 \cdot n$. Per quanto visto, basta sostituire questa scrittura nella rappresentazione di h, da cui si ottiene

$$\begin{aligned} h &= \frac{h}{\gcd(f_1, f_2)} \cdot \gcd(f_1, f_2) = (x_1 + 1)(f_1 \cdot m + f_2 \cdot n) = \\ &= f_1 \cdot \left(-\frac{1}{2}x_1^2 + \frac{7}{4}x_1 + \frac{9}{4} \right) + f_2 \cdot \left(\frac{1}{2}x_1^3 - \frac{5}{4}x_1^2 - 3x_1 - \frac{5}{4} \right) \end{aligned}$$

da cui $[\overline{m}, \overline{n}] = \left[-\frac{1}{2}x_1^2 + \frac{7}{4}x_1 + \frac{9}{4}, \frac{1}{2}x_1^3 - \frac{5}{4}x_1^2 - 3x_1 - \frac{5}{4} \right]$ è una soluzione particolare.

In effetti anche l'individuazione delle soluzioni dell'equazione (3.2) nella loro totalità può essere reinterpretata con l'algoritmo di Buchberger. Si ha che tutte e sole le soluzioni sono date dalla somma della soluzione particolare già individuata con le soluzioni dell'equazione omogenea associata

$$f_1 \cdot m + f_2 \cdot n = 0 \tag{3.3}$$

Dette $\mathrm{Sol}(f_1, f_2)$ le soluzioni dell'equazione (3.3), si può osservare immediatamente che $\mathrm{Sol}(f_1, f_2) = \mathrm{Syz}((f_1, f_2))$.
Si vuole perciò applicare la Proposizione 2.2.1, in quanto si è osservato che il nucleo di un morfismo di moduli si può riscrivere in termini di sizigie delle colonne della matrice associata al morfismo. Considerato quindi il morfismo di moduli descritto dalla matrice $\mathcal{M} = \begin{pmatrix} f_1 & f_2 \end{pmatrix}$ e un ordinamento lessicografico sulle componenti μ, si ha che basta applicare Buchberger alle colonne della matrice

$$\mathcal{M}' = \begin{pmatrix} f_1 & f_2 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

per ottenere una base di Gröbner delle sizigie considerando gli elementi che hanno la prima componente nulla.

Esempio 3.2.4. Si vogliono trovare tutte le soluzioni dell'equazione diofantea presentata nell'Esempio 3.2.3. Si calcola quindi una base di Gröbner del modulo generato dalle colonne di $\mathcal{M}'$ rispetto all'ordinamento $\mu = \mathrm{Poslex}$, ottenendo

$$\left(\begin{bmatrix} x_1^2 + 3 \\ -\frac{2}{51}x_1 + \frac{3}{17} \\ \frac{2}{51}x_1^2 - \frac{7}{51}x_1 - \frac{5}{51} \end{bmatrix} \begin{bmatrix} 0 \\ x_1^2 - x_1 - 3 \\ -x_1^3 + 2x_1 - 4 \end{bmatrix} \right)$$

Si osserva che in alto a sinistra si ottiene di nuovo il $\gcd(f_1, f_2)$, mentre nel blocco in basso a sinistra un multiplo scalare del vettore della rappresentazione del $\gcd(f_1, f_2)$ rispetto a f_1 e f_2 individuato nell'Esempio 3.2.2. Questo in accordo con quanto affermato dalla Proposizione 2.2.1. Nel blocco in basso a destra si trova invece un vettore che corrisponde all'elemento $\left[\frac{f_2}{\gcd(f_1,f_2)}, -\frac{f_1}{\gcd(f_1,f_2)}\right]$, ovvero esattamente un multiplo scalare della soluzione generale specificata dal Teorema 3.2.1.

In particolare, dal paragone tra l'algoritmo di Buchberger applicato a $\mathcal{M}'$ e l'algoritmo di Buchberger esteso applicato a $\mathcal{M}$, si ha che si ottiene un elemento delle sizigie ogni volta che un S-polinomio tra elementi di $\mathcal{M}$ si riduce al polinomio nullo. Osservando nuovamente, grazie alla Proposizione 3.2.2, che ad ogni passo di Buchberger è possibile rimuovere uno dei generatori precedenti e quindi l'insieme degli S-vettori da calcolare ha sempre cardinalità 1, si ottiene che l'algoritmo di Buchberger termina avendo trovato che solo l'ultimo S-vettore calcolato si riduce a 0.
Infatti ad ogni passo viene trovato un elemento con f_i nella prima componente fino a quando non viene generato $f_{s'} = \gcd(f_1, f_2)$. A quel punto l'S-vettore tra le ultime due colonne si riduce a un elemento con la prima componente nulla e non si fanno ulteriori computazioni in quanto gli ultimi due vettori hanno leading term su componenti diverse.

Viene quindi generato un solo elemento con la prima componente nulla, che corrisponde con la riduzione dell'S-vettore tra le colonne corrispondenti ai due polinomi $f_{s'-1}$ e $f_{s'}$.

In effetti il vettore delle sizigie generato corrisponde con il vettore della soluzione generale presentato nel Teorema 3.2.1, ovvero

$$\begin{bmatrix} -g_2 \\ g_1 \end{bmatrix} = \begin{bmatrix} -\frac{f_2}{\gcd(f_1,f_2)} \\ \frac{f_1}{\gcd(f_1,f_2)} \end{bmatrix}$$

Questo è una diretta conseguenza del risultato che segue.

Proposizione 3.2.3. *Sia $R = k[x_1]$, e siano $f_1, f_2 \in R$. Allora se il generatore è monico $G = \left\{ \left[-\frac{f_2}{\gcd(f_1,f_2)}, \frac{f_1}{\gcd(f_1,f_2)} \right] \right\}$ è una base di Gröbner ridotta dell'R-modulo* $\mathrm{Syz}((f_1, f_2)) \subseteq R^2$.

Dimostrazione. Si vede facilmente $\left[-\frac{f_2}{\gcd(f_1,f_2)}, \frac{f_1}{\gcd(f_1,f_2)} \right] \in \mathrm{Syz}((f_1, f_2))$. Per considerazioni sulla coprimalità dei due polinomi $\frac{f_1}{\gcd(f_1,f_2)}$ e $\frac{f_2}{\gcd(f_1,f_2)}$ si può concludere che $\mathrm{Syz}((f_1, f_2)) = \left\langle \left[-\frac{f_2}{\gcd(f_1,f_2)}, \frac{f_1}{\gcd(f_1,f_2)} \right] \right\rangle$. Perciò G come nell'enunciato è una base di Gröbner minimale di $\mathrm{Syz}((f_1, f_2))$, e ne è una base di Gröbner ridotta se il generatore è monico. □

Perciò, per unicità della base di Gröbner ridotta, l'algoritmo di Buchberger deve necessariamente produrre il suddetto vettore.

Osservazione 3.2.5. La risoluzione delle equazioni diofantee può essere reinterpretata usando la Proposizione 2.2.2. Basta infatti calcolare la base di Gröbner del sottomodulo descritto dalle colonne della matrice

$$\mathcal{M}' = \begin{pmatrix} h & f_1 & f_2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

rispetto a un ordinamento lessicografico sulle componenti[2]. Se $\gcd(f_1, f_2)$ divide h, ovvero se l'equazione ha soluzione, si otterrà la seguente matrice a meno di costanti moltiplicative

$$\begin{pmatrix} \gcd(f_1, f_2) & 0 & 0 \\ 0 & 1 & 0 \\ m & \frac{h}{\gcd(f_1,f_2)} \cdot m & -\frac{f_2}{\gcd(f_1,f_2)} \\ n & \frac{h}{\gcd(f_1,f_2)} \cdot n & \frac{f_1}{\gcd(f_1,f_2)} \end{pmatrix}$$

a meno di ulteriori passi di riduzione della base. Se invece $\gcd(f_1, f_2)$ non divide h, nel posto in alto a sinistra si troverà $\gcd(f_1, f_2, h)$, mentre al posto dell'elemento unitario si avrà un polinomio non costante, il che indica che l'equazione non ha soluzione.

[2] È lo stesso procedimento utilizzato nella dimostrazione della Proposizione 2.2.3, nella quale però viene omessa la computazione di uno dei due elementi incogniti.

Esempio 3.2.5. Si vuole risolvere l'equazione diofantea dell'Esempio 3.2.3 utilizzando il metodo presentato nella precedente osservazione. Calcolando quindi una base di Gröbner del modulo generato dalle colonne di $\mathcal{M}'$ rispetto all'ordinamento $\mu = \text{Poslex}$, si ottiene

$$\begin{pmatrix} x_1^2+3 & 0 & 0 \\ 0 & 1 & 0 \\ -\frac{2}{51}x_1+\frac{3}{17} & -\frac{5}{51}x_1-\frac{1}{17} & x_1^2-x_1-3 \\ \frac{2}{51}x_1^2-\frac{7}{51}x_1-\frac{5}{51} & \frac{5}{51}x_1^2+\frac{8}{51}x_1+\frac{13}{51} & -x_1^3+2x_1-4 \end{pmatrix}$$

Si osserva che la sottomatrice ottenuta rimuovendo la seconda riga e la seconda colonna coincide con la matrice trovata nell'Esempio 3.2.4, e per le considerazioni già fatte si ha che è in accordo con quanto previsto dall'Osservazione 3.2.5. Inoltre l'elemento unitario indica che in effetti l'equazione ha soluzione. Invece i due polinomi sottostanti non coincidono con la coppia presente nella matrice nell'osservazione, ovvero $\left(\frac{h}{\gcd(f_1,f_2)}\cdot m, \frac{h}{\gcd(f_1,f_2)}\cdot n\right) = \left(-\frac{2}{51}x_1^2+\frac{7}{51}x_1+\frac{3}{17}, \frac{2}{51}x_1^3-\frac{5}{51}x_1^2-\frac{4}{17}x_1-\frac{5}{51}\right)$. Si può però osservare che sommando alla seconda colonna cambiata di segno un multiplo scalare della terza colonna, si può ottenere esattamente la coppia cercata. Questo mostra che le colonne ottenute con l'algoritmo di Buchberger corrispondono con le colonne previste dopo un passo di riduzione, come anticipato dall'osservazione.

Dall'Osservazione 3.2.5 si nota che questa modalità di risoluzione è facilmente generalizzabile a sistemi di equazioni diofantee del tipo

$$\mathcal{A}\mathcal{X} + \mathcal{B}\mathcal{Y} = \mathcal{H} \tag{3.4}$$

In effetti l'equazione (3.4) è equivalente alla seguente

$$\mathcal{A}'\mathcal{X}' = \mathcal{H} \qquad \mathcal{A}' = \begin{pmatrix}\mathcal{A} & \mathcal{B}\end{pmatrix} \quad \mathcal{X}' = \begin{pmatrix}\mathcal{X} \\ \mathcal{Y}\end{pmatrix}$$

la cui soluzione è chiaramente ottenibile tramite la Proposizione 2.2.2.

Osservazione 3.2.6. Le note sull'efficienza degli algoritmi di risoluzione per i sistemi lineari presentate alla fine della Sezione 2.2.2 si ripercuotono sull'efficienza della risoluzione delle equazioni diofantee. Di conseguenza, il procedimento presentato all'inizio della presente sezione risulta in generale più efficiente della reinterpretazione proposta nella Osservazione 3.2.5, a meno delle ottimizzazioni proposte nella Sezione 2.2.2.

3.2.3 Aspetti computazionali

Analogamente a quanto visto nel caso dell'algoritmo di Gauss nella Sezione 3.1.2, si ha che l'algoritmo euclideo non è numericamente stabile in quanto durante la computazione si produce un'esplosione dei coefficienti, dai quali dipende l'errore in aritmetica floating point.
Si può allora valutare la stessa strategia presa in considerazione per l'algoritmo di Gauss, ovvero svolgere i conti operando in aritmetica esatta. Allo stesso modo, si osserva però l'esplosione del numero di cifre di numeratore e denominatore.

Per le analogie osservate nelle sezioni precedenti, queste considerazioni si ripercuotono sull'algoritmo di Buchberger applicato a ideali del tipo $I = \langle f_1, f_2 \rangle \subseteq k[x_1]$, si veda l'esempio che segue.

Esempio 3.2.6. Sia $R = k[x_1]$ e siano $f_1 = x_1^8 + x_1^6 - 3x_1^4 - 3x_1^3 + 8x_1^2 + 2x_1 - 5$ e $f_2 = 3x_1^6 + 5x_1^4 - 4x_1^2 - 9x_1 + 21$ due polinomi in R. L'applicazione dell'algoritmo euclideo produce la seguente successione di resti.

$$\begin{aligned}
f_1 &= x_1^8 + x_1^6 - 3x_1^4 - 3x_1^3 + 8x_1^2 + 2x_1 - 5 \\
f_2 &= 3x_1^6 + 5x_1^4 - 4x_1^2 - 9x_1 + 21 \\
f_3 &= -\frac{5}{9}x_1^4 + \frac{1}{9}x_1^2 - \frac{1}{3} \\
f_4 &= -\frac{117}{25}x_1^2 - 9x_1 + \frac{441}{25} \\
f_5 &= \frac{233150}{19773}x_1 - \frac{102500}{6591} \\
f_6 &= -\frac{1288744821}{543589225}
\end{aligned}$$

Si conclude in effetti che i due polinomi sono coprimi, ma i resti prodotti per ottenere tale semplice risultato hanno progressivamente una scrittura in numero di cifre sempre più estesa. Applicando l'algoritmo di Buchberger, invece, si ottiene la seguente base di Gröbner.

$$\begin{aligned}
G = \{ & x_1^8 + x_1^6 - 3x_1^4 - 3x_1^3 + 8x_1^2 + 2x_1 - 5, \\
& 3x_1^6 + 5x_1^4 - 4x_1^2 - 9x_1 + 21, \\
& -\frac{5}{9}x_1^4 + \frac{1}{9}x_1^2 - \frac{1}{3}, \\
& -\frac{39}{25}x_1^2 - 3x_1 + \frac{147}{25}, \\
& \frac{46630}{2197}x_1 - \frac{61500}{2197}, \\
& -\frac{11014913}{21743569} \Big\}
\end{aligned}$$

Si nota nuovamente una crescita nel numero di cifre dei coefficienti, anche se i nuovi polinomi differiscono dai precedenti per una costante, come previsto dalla teoria.

Osservazione 3.2.7. Dato che i polinomi generati dall'algoritmo di Buchberger differiscono di una costante rispetto ai polinomi prodotti dall'algoritmo euclideo, ci si potrebbe chiedere se esistono casi in cui il comportamento di esplosione del numero di cifre che si verifica nell'algoritmo euclideo non si ripercuote sullo stesso comportamento nell'algoritmo di Buchberger, in quanto compensato dalle costanti moltiplicative. Dalla teoria tale costante moltiplicativa ad ogni passo è coincidente con $\mathrm{LC}(f_i)$. Si guardi al caso precedente, in cui ad ogni passo dell'algoritmo euclideo i coefficienti sono costituiti approssimativamente dal doppio delle cifre dei precedenti. In casi come questo, il prodotto per la costante data dal leading coefficient del polinomio precedente non potrebbe comunque in alcun modo compensare la crescita nel numero delle cifre. Quindi il comportamento dell'algoritmo euclideo si riflette nello stesso comportamento dell'algoritmo di Buchberger.

Conclusioni

In questa tesi si sono raccolti alcuni risultati riguardanti le forme normali dei moduli in una trattazione organica e strutturata. A partire dal teorema di eliminazione delle componenti di modulo sono stati presentati gli algoritmi per il calcolo delle principali operazioni tra moduli, mostrando che dal punto di vista computazionale possono essere resi equivalenti agli algoritmi standard. Il conseguente paragone sistematico dell'algoritmo di Buchberger con gli algoritmi di Gauss ed euclideo, ha mostrato come il primo può essere applicato per eseguire le stesse computazioni degli altri due, e si può quindi interpretare come una loro generalizzazione. Si sono estese queste stesse considerazioni alla risoluzione di equazioni diofantee. Alcuni esempi mostrano che l'algoritmo di Buchberger, generalizzazione degli algoritmi di Gauss ed euclideo, soffre di analoghi problemi di instabilità numerica.
Rimangono aperte alcune questioni di notevole interesse. In particolare, guardando allo studio delle forme normali dei moduli e degli ideali, si potrebbe approfondire il caso degli ideali omogenei, a cui è stato accennato solo con esempi, o il caso degli ordinamenti di eliminazione delle indeterminate. Potrebbe risultare interessante ampliare il confronto con l'algoritmo di Gauss con altre nozioni attinenti, studiando per esempio la trasposizione nell'algebra dei moduli della fattorizzazione LU. Infine, a partire dai rapporti con l'algebra lineare osservati, si potrebbe estendere lo studio ad altri concetti correlati, come la similitudine e la diagonalizzazione di matrici.

Appendice A

Codici in CoCoA

La sperimentazione seguente è stata condotta usando il sistema CoCoA 4.7.5. Nella stessa versione sono state effettuate tutte le verifiche relative a esempi sul calcolo di basi di Gröbner di moduli, che richiedessero un ordinamento lessicografico sulle componenti.

```
Use R ::= Q[x, y], PosTo, Lex;

G1 := [x^2, 1];
G2 := [x*y+y^2, 0];
L := [G1, G2];
M := Module(L);
A := Transposed(Mat(M));

G3 := [y^2, 1];
G4 := [x*y, 0];
L := [G3, G4];
N := Module(L);
B := Transposed(Mat(N));

//Implementazione algoritmo dell'Esempio 2.2.2

C := Transposed(BlockMatrix([[A, B], [0, B]]));
M1 := Module(C);
ReducedGBasis(M1);

//Implementazione algoritmo dell'Esempio 2.3.1

Id := Identity(2);
D := Transposed(BlockMatrix([[Id, A, 0], [Id, 0, B], [Id, 0, 0]]));
M2 := Module(D);
ReducedGBasis(M2);
```

Figura A.1: Intersezione tra moduli - Esempi 2.2.2 e 2.3.1

La sperimentazione che segue è invece stata condotta usando il sistema CoCoA 5.3.2. In questa versione non risultano ancora implementati ordinamenti su moduli differenti da ToPos, per cui è stata utilizzata per tutti gli esempi in cui non fosse richiesto un ordinamento lessicografico sulle componenti.

```
use P ::= QQ[x1, x2, x3], lex;

//Calcolo base di Grobner

I := ideal(x1^2-2*x2^2-2*x2*x3-x3^2, -x1*x2+2*x2*x3+x3^2,
    -x1^2+x1*x2+x1*x3+x3^2);
indent(ReducedGBasis(I));

//Eliminazione gaussiana su matrice dei coefficienti dei generatori

L := gens(I);
L2 := [];
for i := 1 to len(L) do
    append (ref L33, coefficients(L[i], [x1^2, x1*x2, x1*x3, x2^2, x2*x3,
    x3^2]));
endfor;

M := matrix(L2);
rref(M);

//Eliminazione gaussiana su matrice dei coefficienti dei polinomi omogenei
    di grado 3 ottenibili dai generatori

LB := [x1*(x1^2-2*x2^2-2*x2*x3-x3^2), x2*(x1^2-2*x2^2-2*x2*x3-x3^2),
    x3*(x1^2-2*x2^2-2*x2*x3-x3^2), x1*(-x1*x2+2*x2*x3+x3^2),
    x2*(-x1*x2+2*x2*x3+x3^2), x3*(-x1*x2+2*x2*x3+x3^2),
    x1*(-x1^2+x1*x2+x1*x3+x3^2), x2*(-x1^2+x1*x2+x1*x3+x3^2),
    x3*(-x1^2+x1*x2+x1*x3+x3^2)];
LB2 := [];
for i := 1 to len(LB) do
    append (ref LB2, coefficients(LB[i], [x1^3, x1^2*x2, x1^2*x3, x1*x2^2,
    x1*x2*x3, x1*x3^2, x2^3, x2^2*x3, x2*x3^2, x3^3]));
endfor;

MB := matrix(LB2);
rref(MB);
```

Figura A.2: Eliminazione gaussiana e ideali omogenei - Esempio 3.1.2

Bibliografia

[1] John Abbott, Anna M. Bigatti, and Lorenzo Robbiano. CoCoA: a system for doing Computations in Commutative Algebra. Available at `http://cocoa.dima.unige.it`.

[2] Bruno Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. *Multidimensional Systems Theory*, pages 184–232, 1985.

[3] Massimo Caboara. *Optimization of basic algorithms in Commutative Algebra.* PhD thesis, Università di Pisa, 1998.

[4] Massimo Caboara and Anna M. Perdon. Effective computations for geometric control theory. *International Journal of Control*, 79(11):1401–1417, 2006.

[5] Massimo Caboara and Carlo Traverso. Efficient algorithms for ideal operations (extended abstract). In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, ISSAC '98, page 147–152. Association for Computing Machinery, 1998.

[6] Lindsay Childs. *A Concrete Introduction to Higher Algebra.* Undergraduate Texts in Mathematics. Springer, 3th edition, 2009.

[7] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer Publishing Company, Incorporated, 4th edition, 2015.

[8] James W. Demmel. *Applied Numerical Linear Algebra.* Society for Industrial and Applied Mathematics, 1997.

[9] David Eisenbud. *Commutative Algebra*, volume 150 of *Graduate Texts in Mathematics.* Springer-Verlag, 1995.

[10] Rüdiger Gebauer and H. Michael Möller. On an installation of Buchberger's algorithm. *Journal of Symbolic Computation*, 6(2):275–286, 1988.

[11] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 2.* Springer Publishing Company, Incorporated, 2005.

[12] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1.* Springer Publishing Company, Incorporated, 2008.