وزارت علوم، تحقیقات و فناوری

دانشگاه دامغان
دانشکده ریاضی و علوم کامپیوتر

پایان‌نامه کارشناسی ارشد
ریاضی محض

اثبات جدید برای درستی الگوریتم F_5 (شبه F_5)

توسط:
فاطمه شهید

استاد راهنما:
دکتر عبدالعلی بصیری

استاد مشاور:
دکتر سجاد رحمانی

شهریورماه ۱۳۹۱


بسم الله الرحمن الرحيم

به نام خدا

اثبات جدید برای درستی الگوریتم F_5 (شبه F_5)

توسط:

فاطمه شهید

پایان‌نامه

ارائه شده به تحصیلات تکمیلی دانشگاه به عنوان بخشی از فعالیت‌های تحصیلی لازم برای اخذ درجه کارشناسی ارشد

در رشته

ریاضی محض

از دانشگاه دامغان

ارزیابی و تأیید شده توسط کمیته پایان‌نامه با درجه: **عالی**

دکتر عبدالعلی بصیری، استادیار ریاضی محض، گرایش جبر محاسباتی، دانشکده ریاضی و علوم کامپیوتر، دانشگاه دامغان (استاد راهنما)

دکتر سجاد رحمانی، استادیار ریاضی محض، گرایش جبر محاسباتی، دانشکده ریاضی و علوم کامپیوتر، دانشگاه دامغان (استاد مشاور)

دکتر مجید فرهادی، استادیار ریاضی محض، گرایش هندسه جبری، دانشکده ریاضی و علوم کامپیوتر، دانشگاه دامغان (داور اول)

دکتر سید هاشم طبسی، استادیار علوم کامپیوتر، دانشکده ریاضی و علوم کامپیوتر، دانشگاه دامغان (داور دوم)

دکتر نرگس تولایی، استادیار ریاضی محض، گرایش آنالیز هارمونیک، دانشکده ریاضی و علوم کامپیوتر، دانشگاه دامغان (نماینده تحصیلات تکمیلی)

شهریورماه ۱۳۹۱

تقدیم به

تقدیم.....

سپاسگزاری

از تمام کسانی که من را در تهیه‌ی این پایان‌نامه یاری کردند، تشکر می‌نمایم.

چکیده

اثبات جدید برای درستی الگوریتم F_5 (شبه F_5)

به وسیله‌ی:
فاطمه شهید

حل دستگاه‌های چندجمله‌ای چندمتغیره توسط پایه گروبنر، از قسمت‌های اساسی جبر محاسباتی است که توسط بوخ‌برگر در سال ۱۹۶۵ با ارائه در [۵]، وارد عرصه علمی شد. طی چند سال اخیر الگوریتم‌های مختلفی برای محاسبه‌ی پایه گروبنر ارائه شد که یکی از قویترین و کاراترین الگوریتم‌های موجود، الگوریتم F_5 است. این الگوریتم با داشتن محک‌های قوی، از محاسبات غیر ضروری (با حذف زوج‌های غیر مفید) جلوگیری می‌کند. اما گونه‌ی اصلی آن برای درک و فهم کمی مشکل است. سان و وانگ در [۳۲]، با ارائه‌ی گونه‌ی جدیدی از الگوریتم F_5 (F_5B) این مفهوم را ساده کردند، به طوری که الگوریتم جدید معادل گونه اصلی آن نیز می‌باشد. سپس در [۳۴] اثبات درستی آن را ارائه دادند. در این پایان نامه پس از ارائه‌ی الگوریتم F_5B، اثبات درستی آن که همچنین اثباتی برای درستی گونه‌ی اصلی الگوریتم F_5 است را مورد بررسی قرار می‌دهیم.

واژه های کلیدی: پایه گروبنر، الگوریتم F_5، الگوریتم F_5B.

فهرست مطالب

فهرست الگوریتم‌ها

پیشگفتار

نظریه‌ی پایه گروبنر برای اولین بار در سال ۱۹۶۵ توسط شخصی به نام برونو بوخبرگر [۱] ارائه شد. وی این پایه را حین کار بر روی پایان‌نامه‌اش، برای محاسبه‌ی پایه‌ی فضای برداری $K[x_1,\ldots,x_n]/I$ بدست آورد که در آن $K[x_1,\ldots,x_n]$ حلقه‌ی چندجمله‌ای‌های با متغیرهای $x_1,\ldots,x_n$ و I یک ایده‌آل صفربعدی [۲] دراین حلقه است.

ریاضیدانان با مطالعه‌ی بیشتر پایه گروبنر [۳] به نتایج و کاربردهای مهمی از آن دست یافته‌اند. به عنوان مثال، می‌توان به حل دستگاه‌های چندجمله‌ای چندمتغیره در رباتیک، بیوشیمی، رمزنگاری و غیره اشاره کرد. در حقیقت با استفاده از پایه گروبنر، برای هر دستگاه چندجمله‌ای چندمتغیره، می‌توان دستگاهی معادل آن یافت که ویژگی‌های بهتری نسبت به دستگاه اصلی دارد.

اولین گام برای محاسبه‌ی پایه گروبنر، ارائه‌ی الگوریتم بوخبرگر توسط برونو بوخبرگر در [۵] بود. اما از آنجا که این الگوریتم از لحاظ اجرایی دارای پیچیدگی زمانی بالایی می‌باشد، تلاش‌هایی در جهت بهبود آن صورت گرفت. از جمله‌ی این تلاش‌ها ارائه‌ی دو محک، توسط بوخبرگر در سال ۱۹۷۹ در [۶] می‌باشد که تا حدود زیادی از محاسبه‌ی کاهش به صفرهای غیر ضروری در این الگوریتم جلوگیری می‌کنند.

بعد از الگوریتم بوخبرگر الگوریتم‌های دیگری نیز در [۶، ۱۴، ۱۵، ۱۹، ۲۵، ۲۲، ۲۰] ارائه شدند.

---

[۱] Bronu Bouchberger

[۲] I را صفربعدی گوئیم هرگاه پایه‌ی فضای برداری $K[x_1,...,x_n]/I$ متناهی البعد بدست آید.

[۳] بوخبرگر این پایه را به افتخار استاد راهنمایش ولفگانگ گروبنر، در سال ۱۹۷۹ رسما گروبنر نام نهاد.

در بین الگوریتم‌های ارائه شده برای این منظور، الگوریتم‌های XL، که توسط کورتز و همکارانش [۴] در [۱۰] و F_4 و F_5 نیز که توسط فوژر [۵] به ترتیب در سال‌های ۱۹۹۹ و ۲۰۰۲ در مقاله‌های [۱۴] و [۱۵] منتشر شدند، مشهورترین الگوریتم‌ها هستند.

الگوریتم F_5 با بکارگیری دو محک قوی به نام محک بازنویسی و محک سیزیجی تقریبا از محاسبه‌ی همه‌ی کاهش به صفرهای غیر ضروری جلوگیری می‌کند. از آنجا که این الگوریتم از چندین تابع و زیرالگوریتم تشکیل شده است، هم از لحاظ اجرایی و هم از جهت فهم و درک کمی مشکل به نظر می‌آید. به همین دلیل برخی در صدد ساده کردن آن بر آمدند و گونه‌های متفاوتی از این الگوریتم را معرفی کردند. به عنوان مثال ادر [۶] و پری [۷] در [۲۷] گونه‌ای به نام F_5C و باردت [۸] در [۳] گونه‌ای به نام F_5M ارائه کردند.

در این پایان‌نامه یک الگوریتم جدید، به نام F_5B ارائه می‌دهیم که معادل با گونه‌ی اصلی الگوریتم F_5 است، اما مفهومی ساده‌تر دارد و از لحاظ اجرایی نیز راحت‌تر است. [۹] الگوریتم F_5B و گونه‌ی اصلی الگوریتم F_5، در تکنیک انتخاب زوج‌های بحرانی تفاوت دارند (رجوع کنید به [۳۲]).

پس از معرفی پیش‌نیازها و تعاریف مورد نیاز در فصل یک و دو، الگوریتم F_5B را ارائه می‌دهیم. در فصل سه نیز گونه‌ی بازبینی شده‌ی آن، تحت عنوان F_5M را مطرح می‌کنیم که بر اساس آن هدف اصلی این پایان‌نامه یعنی اثبات قضیه‌ی درستی الگوریتم F_5B دنبال می‌شود. این اثبات را می‌توان اثباتی برای درستی الگوریتم F_5 نیز در نظر گرفت، زیرا تکنیک جدیدی که در ارائه‌ی این اثبات استفاده می‌شود، به شیوه‌ی انتخاب زوج‌های بحرانی بستگی ندارد([۳۴]). به عنوان مبحث پایانی این پایان‌نامه، تاثیر تغییر ترتیب مدولی به کار رفته در الگوریتم F_5 (شبه F_5) را مورد بررسی قرار می‌دهیم. در فصل چهار نیز کد الگوریتم F_5B موجود در این پایان‌نامه را ارائه می‌کنیم.

---

[۴] Courtois et al.

[۵] Faugere

[۶] Eder

[۷] Perry

[۸] Bardet

[۹] لازم به ذکر است که کارایی اصلی الگوریتم F_5 را ندارد. تنها برای ارائه‌ی اثبات درستی الگوریتم F_5 به کار می‌رود.

فصل ۱

معرفی پایه گروبنر

در این فصل به بیان مطالب و مفاهیمی می‌پردازیم که در سرتاسر پایان‌نامه مورد استفاده قرار می‌گیرد. از آنجا که انتظار می‌رود خواننده با این مطالب آشنایی داشته باشد، از بیان بعضی از اثبات‌ها و جزئیات خودداری می‌کنیم. اکثر مطالب این فصل از کتاب‌های [۹، ۴] استخراج شده است.

۱-۱ ترتیب‌های تک‌جمله‌ای

تک‌جمله‌ای‌ها و چندجمله‌ای‌های چندمتغیره مفاهیم بنیادی در ساختار پایه گروبنر هستند که در این بخش آن‌ها را مورد بررسی قرار می‌دهیم.

فرض کنیم $\alpha_1, ..., \alpha_n$ اعدادی صحیح و نامنفی باشند، آن‌گاه یک تک‌جمله‌ای [۱] برحسب متغیرهای $x_1, ..., x_n$، حاصل‌ضرب توانی [۲] از این متغیرهاست و آن را به شکل $x^\alpha = x^{\alpha_1}...x^{\alpha_n}$ نمایش می‌دهیم که در آن $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. درجه‌ی این تک‌جمله‌ای را نیز به صورت $|\alpha| = \sum_{i=1}^n \alpha_i$ تعریف می‌کنیم.

اگر $\alpha = (0, ..., 0)$ آن‌گاه $x^\alpha = 1$ و درجه آن نیز برابر صفر خواهد بود.

---

[۱] Monomial

[۲] Power product

تعریف ۱.۱.۱. فرض کنیم K یک میدان باشد. یک چندجمله‌ای f برحسب متغیرهای $x_1, ..., x_n$ با ضرایب درK یک ترکیب خطی از تک‌جمله‌ای‌ها می‌باشد که آن را به صورت $f = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} a_\alpha x^\alpha$ نمایش می‌دهیم.

هر جمعوند $a_\alpha x^\alpha$ از چندجمله‌ای f را یک جمله می‌نامیم که در آن $a_\alpha \neq 0$ ضریب تک‌جمله‌ای x^α نامیده می‌شود. درجه‌ی f را با $deg(f)$ نشان می‌دهیم و به صورت زیر تعریف می‌کنیم

$$deg(f) = max\{|\alpha| \mid \alpha \in \mathbb{Z}^n_{\geq 0}, a_\alpha \neq 0\}.$$

مجموعه تمام چندجمله‌ای‌های بر حسب $x_1, ..., x_n$ و با ضرایب در K را در نظر بگیرید. این مجموعه با عمل جمع و ضرب چندجمله‌ای، تشکیل یک حلقه می‌دهد. این حلقه را با نماد $K[X]$ نمایش می‌دهیم که در آن $X = x_1, ..., x_n$.

فرض کنیم $K[X]$ حلقه‌ی چندجمله‌ای‌های با ضرایب در K از متغیرهای $x_1, ..., x_n$ باشد و $\mathbb{N}$ نیز مجموعه‌ی اعداد طبیعی باشد. آن‌گاه مجموعه‌ی

$$PP(X) = \{X^\alpha | x^\alpha = x^{\alpha_1} ... x^{\alpha_n}, \alpha_i \in \mathbb{N}, i = 1, ..., n\}$$

را مجموعه‌ی تک‌جمله‌ای‌های با متغیرهای $x_1, ..., x_n$ می‌نامیم که اعضای آن تک‌جمله‌ای هستند.

تذکر ۲.۱.۱. هر تک‌جمله‌ای یک جمله است اما عکس آن برقرار نیست.

در ادامه به بیان مفهوم ترتیب روی تک‌جمله‌ای‌ها می‌پردازیم.

تذکر ۳.۱.۱. فرض کنیم مجموعه A یک زیر مجموعه متناهی از $\mathbb{Z}^n_{\geq 0}$ باشد، در این صورت رابطه‌ی $<$ یک رابطه‌ی کلی خواهد بود هرگاه به ازای $a, b, c \in A$ خواص زیر برقرار باشد

۱. دارای خاصیت انعکاسی باشد. یعنی به ازای هر $a \in A$ داشته باشیم $a < a$

۲. پاد متقارن باشد. یعنی اگر $a < b$ و $b < a$ آن‌گاه $a = b$.

۳. تعدی یا تراگذر باشد. یعنی اگر $a < b$ و $b < c$ آن‌گاه $a < c$.

تعریف ۴.۱.۱. ترتیب $<$ را روی حلقه چندجمله‌ای‌های $K[X]$ یک ترتیب تک‌جمله‌ای می‌نامیم هرگاه به ازای هر $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ داشته باشیم

۱. $<$ روی $\mathbb{Z}_{\geq 0}^n$ یک رابطه کلی باشد.

۲. اگر $\alpha < \beta$ آن‌گاه به ازای $\gamma \in \mathbb{Z}_{\geq 0}^n$ دارشته باشیم $\alpha + \gamma < \beta + \gamma$.

۳. $<$ روی $\mathbb{Z}_{\geq 0}^n$ خوش‌ترتیب باشد. (به عبارتی هر زیر مجموعه متناهی از $\mathbb{Z}_{\geq 0}^n$ دارای عضو مینیمم باشد).

به عنوان معادل شرط سوم در تعریف فوق اینطور نیز می‌توان نوشت که،

"به ازای هر $1 \neq x^\alpha \in K[X]$ داشته باشیم $x^\alpha > 1$."

تذکر ۱.۱.۵. مجموعه تمام تک‌جمله‌ای‌های به صورت $x^\alpha = x_1^{\alpha_1} ... x_n^{\alpha_n}$ را در نظر بگیرید. اگر توان هر یک از این تک‌جمله‌ای‌ها را به صورت n-تایی $(\alpha_1, ..., \alpha_n)$ فرض کنیم، آن‌گاه می‌توان با در نظر گرفتن یک ترتیب تک‌جمله‌ای، بین این ترتیب روی این مجموعه‌ها و مجموعه $\mathbb{Z}_{\geq 0}^n$ یک تناظر یک به یک برقرار کرد. بنابراین

$$\alpha < \beta \iff x^\alpha < x^\beta \qquad (1.1)$$

که در آن $x^\alpha, x^\beta \in K[X]$.

در ادامه به چند نمونه از ترتیب‌هایی که روی تک‌جمله‌ای‌ها به کار می‌روند، اشاره می‌کنیم. از این ترتیب‌ها در سرتاسر این پایان نامه استفاده می‌شود.

تعریف ۱.۱.۶. فرض کنید $\alpha = (\alpha_1, ..., \alpha_n), \beta = (\beta_1, ..., \beta_n), \gamma = (\gamma_1, ..., \gamma_n) \in \mathbb{Z}_{\geq 0}^n$ در این صورت گوئیم

۱. (ترتیب الفبایی) $\alpha <_{lex} \beta$ اگر و تنها اگر اولین مؤلفه از سمت چپ در $\beta - \alpha$ غیر صفر باشد. رابطه $<_{lex}$ ترتیب الفبایی نامیده می‌شود.

۲. (ترتیب الفبایی مدرج) $\alpha <_{grlex} \beta$ هرگاه $|\alpha| < |\beta|$ و اگر داشته باشیم $|\alpha| = |\beta|$ آن‌گاه رابطه $\alpha <_{lex} \beta$ برقرار باشد. ترتیب $<_{grlex}$ الفبایی مدرج نامیده می‌شود.

۳. (ترتیب الفبایی معکوس مدرج) $\alpha <_{grevlex} \beta$ هرگاه $|\alpha| < |\beta|$ و اگر $|\alpha| = |\beta|$ آن‌گاه اولین مؤلفه ناصفر سمت راست $\beta - \alpha$ نامنفی باشد. ترتیب $<_{grevlex}$ الفبایی معکوس مدرج نامیده می‌شود.

مثال ۱.۱.۷. فرض کنید $x_1x_3, x_1x_2^2x_3, x_1^2x_3^2$ و x_2^5 تک‌جمله‌ای‌هایی در $K[X]$ باشند که $X = x_1, x_2, x_3$، اگر برای هر یک به ترتیب ۳-تایی $\alpha = (2, 0, 2), \beta = (1, 2, 1)$ و $\gamma = (0, 5, 0)$ را تشکیل دهیم، در این صورت داریم

با استفاده از ترتیب الفبایی با $x_1 <_{lex} x_2 <_{lex} x_3$ چون $\alpha - \gamma = (2, -5, 2)$ بنابر (۱.۱) نتیجه می‌گیریم

$$x_1^2x_3^2 >_{lex} x_2^5$$

همچنین داریم $\beta - \alpha = (1, -2, 1)$ که با توجه به (۱.۱) نتیجه می‌گیریم $x_1x_2^2x_3 >_{lex} x_1^2x_3^2$.

با استفاده از ترتیب $x_1 <_{grlex} x_2 <_{grlex} x_3$، بدست می‌آوریم $x_1^2x_3^2 <_{grlex} x_2^5$ زیرا

$$deg(x_2^5) = 5 > 4 = deg(x_1^2x_3^2).$$

همچنین برای دو تک‌جمله‌ای $x_1x_2^2x_3$ و $x_1^2x_3^2$، چون $deg(x_1x_2^2x_3) = 4 = deg(x_1^2x_3^2)$ لذا عبارت

$$\alpha - \beta = (1, -2, 1)$$

را محاسبه می‌کنیم که در آن اولین مؤلفه از سمت چپ، مثبت است. بنابراین $x_1x_2^2x_3 <_{grlex} x_1^2x_3^2$.

اکنون اگر ترتیب $x_1 <_{grevlex} x_2 <_{grevlex} x_3$ را روی حلقه‌های چندجمله‌ای‌های $K[X]++$ به کار گیریم، بدست می‌آوریم $x_2^5 <_{grevlex} x_1^2x_3^2$ زیرا

$$deg(x_2^5) = 5 > 4 = deg(x_1^2x_3^2)$$

و همچنین $x_1^2x_3^2 <_{gevrlex} x_1x_2^2x_3$ زیرا $deg(x_1^2x_3^2) = 4 = deg(x_1x_2^2x_3)$ و در عبارت

$$\beta - \alpha = (-1, 2, -1)$$

اولین مؤلفه از سمت راست، مثبت است.

فرض کنید $>$ یک ترتیب تک‌جمله‌ای دلخواه باشد که آن را روی حلقه‌ی چندجمله‌ای‌های $K[X]$ در نظر می‌گیریم. هر چندجمله‌ای $f \in K[X]$، یک نمایش منحصر بفردی مانند

$$f = c_1x^{\alpha_1} + ... + c_sx^{\alpha_s}$$

دارد که در آن به ازای $i = ۱, ..., s$ داریم $۰ \neq c_i \in K[X]$ و x^{α_i}ها تک‌جمله‌ای‌هایی در $K[X]$ باشند به طوری که $x^{\alpha_۱} > ... > x^{\alpha_s}$. در این صورت تک‌جمله‌ای پیشرو، ضریب پیشرو و جمله پیشروی f را به ترتیب به صورت $x^{\alpha_۱}$، $c_۱$ و $c_۱x^{\alpha_۱}$ تعریف می‌کنیم و با نمادهای $lpp(f)$ [۳] $lc(f)$ [۴] و $lt(f)$ [۵] نمایش می‌دهیم.

به عنوان مثال فرض کنید $f = ۴xy^۲z + ۴z^۲ - ۵x^۳ + ۷x^۲z^۲$. با در نظر گرفتن ترتیب $x <_{lex} y <_{lex} z$ تک‌جمله‌ای پیشروی f برابر $x^۳$ بدست می‌آید که همان $lpp(f)$ خواهد بود. ضریب این تک‌جمله‌ای در f برابر $lc(f) = -۵$ می‌باشد. بدین ترتیب جمله پیشروی f، $lt(f) = -۵x^۳$ خواهد بود.

اکنون با معرفی مفاهیم تک‌جمله‌ای‌ها و چندجمله‌ای‌های چندمتغیره و بیان ترتیب روی آن‌ها می‌توان الگوریتم تقسیم را برای چندجمله‌ای‌های چندمتغیره ارائه داد که تعمیم الگوریتم تقسیم چندجمله‌ای یک متغیره می‌باشد. در بخش بعدی این هدف را دنبال می‌کنیم.

۱-۲ الگوریتم تقسیم

الگوریتم تقسیم در حلقه‌ی $K[X]$ از مفاهیم اساسی در محاسبه‌ی پایه‌ی گروبنر بوسیله‌ی الگوریتم بوخبرگر (در بخش‌های بعدی معرفی می‌گردد) است که فرایند کاهشی بر اساس آن انجام می‌گیرد.

قضیه ۱.۲.۱. *(الگوریتم تقسیم) فرض کنید $>$ یک ترتیب تک‌جمله‌ای و $F = \{f_۱, f_۲, ..., f_s\}$ زیرمجموعه‌ای از چندجمله‌ای‌ها در $K[X]$ باشد. اگر داشته باشیم $f \in K[X]$ آن‌گاه این چندجمله‌ای را می‌توان به صورت زیر نوشت*

$$f = a_۱f_۱ + a_۲f_۲ + ... + a_sf_s + r, \qquad (۲.۱)$$

که در آن به ازای $i = ۱, ..., s$، $a_i, r \in K[X]$ و r برابر صفر است یا یک چندجمله‌ای است که هیچ جمله‌ای از آن بر هیچ یک از جمله‌های $lt(f_۱), ..., lt(f_s)$ بخش‌پذیر نیست (r باقیمانده تقسیم f بر مجموعه‌ی F نامیده می‌شود). همچنین $lt(a_if_i) \leq lt(f)$.

---

[۳] **l**eading **p**ower **p**roduct

[۴] **l**eading **c**oefficient

[۵] **l**eading **t**erm

برهان. وجود $a_1, ..., a_s, r$ را با ارائه‌ی الگوریتم زیر نشان می‌دهیم.

الگوریتم ۱-۱ تقسیم چندمتغیره

Require: A set of Polynomials $(f_1, ..., f_m) \subset K[X],$, $f \in K[X]$ and monomial order $<$.
Ensure: $a_1, ..., a_s, r$
  $a_1, ..., a_s, r := 0$
  $p := f$
  while $p \neq 0$ **do**
    $i := 1$
    $sw := false$
    while $i \leq s$ and $sw = false$ **do**
      if $lt(f_i) \mid lt(p)$ **then**
        $a_i := a_i + \dfrac{lt(p)}{lt(f_i)}$
        $p := p - (\dfrac{lt(p)}{lt(f_i)}) f_i$
        $sw := true$
      else
        $i := i + 1$
      end if
    end while
    if $sw = false$ **then**
      $r := r + lt(p)$
      $p := p - lt(p)$
    end if
  end while
  return $(a_1, ..., a_s, r)$

قبل از اثبات قضیه، ابتدا به نکته‌ی زیر اشاره می‌کنیم.

در هر بار اجرای حلقه‌ی $while$، دقیقا یکی از حالت‌های زیر رخ می‌دهد.

- (گام تقسیم) اگر اندیسی مانند $i \in \{۱, ..., s\}$ وجود داشته باشد به طوری که $lt(f_i)|lt(p)$، آن‌گاه الگوریتم ادامه می‌یابد.
- (گام باقیمانده) اگر هیچ یک از $lt(f_i)$ها به ازای $i = ۱, ..., s$، $lt(p)$ را عاد نکند، آن‌گاه $lt(p)$ به باقیمانده اضافه می‌شود.

اکنون با توجه به نکته‌ی فوق، درستی و پایان‌پذیری الگوریتم را نشان می‌دهیم.

ابتدا به درستی آن می‌پردازیم. بدین منظور، ادعا می‌کنیم معادله‌ی

$$f = a_1 f_1 + ... + a_s f_s + p + r \qquad (*)$$

در هر گام الگوریتم برقرار است. برای مقادیر اولیه‌ی $a_1, ..., a_s, p$ و r این معادله بوضوح برقرار است.

با فرض برقراری معادله‌ی $(*)$ در حالت قبلی، اگر گام بعدی، گام تقسیم باشد، آن‌گاه اندیسی مانند $i \in \{1, ..., s\}$ وجود دارد که $lt(f_i)|lt(p)$ و رابطه‌ی $a_i f_i + p$ در هر گام تقسیم تغییری نخواهد کرد زیرا

$$a_i f_i + p = (a_i + \frac{lt(p)}{lt(p)}) f_i + (p - (\frac{lt(p)}{lt(f_i)}) f_i).$$

در نتیجه رابطه‌ی $(*)$ همچنان برقرار است. اما اگر گام بعدی در این مرحله، گام باقیمانده باشد، آن‌گاه $p + r$ غیر قابل تغییر خواهد بود، زیرا

$$p + r = (p - lt(p)) + (r + lt(p)),$$

که دراین حالت نیز، همچنان معادله‌ی $(*)$ برقرار است.

اکنون به اثبات پایان‌پذیری الگوریتم تقسیم می‌پردازیم.

در هر مرحله از الگوریتم اگر $p \neq 0$ باشد جمله‌ی پیشروی آن به طور مرتب کاهش می‌یابد. این کاهش را برای حالات مذکور در ابتدای اثبات بررسی می‌کنیم.

اگر در گام تقسیم باشیم، در هر مرحله بدست می‌آوریم $\acute{p} = p - \frac{lt(p)}{lt(f_i)} f_i$. بنابر رابطه‌ی

$$lt(\frac{lt(p)}{lt(f_i)} f_i) = \frac{lt(p)}{lt(f_i)} lt(f_i) = lt(p)$$

نتیجه می‌گیریم p و $\frac{lt(p)}{lt(f_i)} f_i$ دارای جمله‌ی پیشروی یکسانی هستند. پس $lt(\acute{p}) < lt(p)$.

از طرفی طی گام باقیمانده، می‌دانیم

$$\acute{p} = p - lt(p),$$

که بوضوح در آن، جمله‌ی پیشروی p کاهش می‌یابد و $lt(\acute{p}) < lt(p)$.

بنابراین در هر مرحله جمله‌ی پیشروی p کاهش می‌یابد تا اینکه به شرط توقف یعنی $p = 0$ برسیم. در این حالت

$$f = a_1 f_1 + ... + a_s f_s + r.$$

سرانجام الگوریتم متوقف می‌شود، زیرا اگر الگوریتم هرگز متوقف نشود، دنباله‌ی نزولی نامتناهی از جمله‌های پیشروی p بدست می‌آید که با فرض خوش ترتیب بودن رابطه‌ی $<$ در تناقض است. □

از کاربردهای الگوریتم تقسیم چند متغیره، تعیین مجموعه مولدهایی با ویژگی‌های خاص است که در ادامه به روش یافتن این دسته از مجموعه‌ها می‌پردازیم.

تذکر ۱.۲.۲. با تغییر ترتیب تک‌جمله‌ای و همچنین ترتیب چندجمله‌ای‌های مقسوم علیه در مجموعه‌ای مانند F، بنا به قضیه‌ی ۱.۲.۱، باقیمانده نیز تغییر می‌کند.

فرض کنیم $f_1, f_2, ..., f_s, f \in K[X]$ و I ایده‌آل تولید شده توسط $\langle f_1, f_2, ..., f_s \rangle$ باشد. در این صورت مسئله‌ی عضویت یک ایده آل یعنی تعیین عضویت f در I.

واضح است که اگر f عضو ایده‌آل I باشد آن‌گاه به صورت ترکیب خطی ار مولدهای I نوشته می‌شود، به طوری که

$$f = a_1 f_1 + ... + a_s f_s$$

در مثال بعد مسئله‌ی عضویت ایده‌آل را به ازای یک یک ایده‌آل در حلقه‌ی $K[X]$، با استفاده از الگوریتم تقسیم بررسی می‌کنیم.

مثال ۱.۲.۳. فرض می‌کنیم $f_1 = xy + 1$ و $f_2 = y^2 - 1$ چندجمله‌ای‌هایی در حلقه‌ی $K[x, y]$ باشند. با در نظر گرفتن ترتیب تک‌جمله‌ای $x <_{lex} y$ و با استفاده از قضیه‌ی ۱.۲.۱، تقسیم چندجمله‌ای $f = xy^2 - x$ بر $F_1 = \{f_1, f_2\}$ نتیجه می‌گیریم

$$xy^2 - x = y.(xy + 1) + 0.(y^2 - 1) + (-x - y),$$

در حالی که تقسیم چندجمله‌ای f بر $F_2 = \{f_2, f_1\}$ برابر است با

$$xy^2 - x = X.(y^2 - 1) + 0.(xy + 1) + 00$$

تساوی دوم نشان می‌دهد که f عضو ایده‌آل است ولی از تساوی اول نمی‌توان عضویت آن را نتیجه گرفت، زیرا باقیمانده مخالف صفر است.

در مثال فوق مشاهده می‌شود که چنانچه باقیمانده تقسیم چندجمله‌ای f بر ایده‌آل تولید شده توسط $\langle f_1, f_2 \rangle$ صفر بدست آید، f عضو ایده‌آل خواهد بود. اما عکس این مطلب برقرار نیست.

توضیحات فوق و تذکر ۲.۲.۱ حاوی این نکته هستند که هر مجموعه مولدی از یک ایده‌آل در حلقه‌ی $K[X]$ نمی‌تواند شرایط مطلوب را در حل مسئله‌ی عضویت داشته باشد. برای رفع این مشکل نیاز به مجموعه‌ی مولدی مانند $F = \{f_1, ..., f_s\}$ داریم که با در نظر گرفتن یک ترتیب تک‌جمله‌ای، باقیمانده‌ی تقسیم هر چندجمله‌ای از $K[X]$ بر آن نسبت به هر ترتیبی از جایگاه‌های چندجمله‌ای‌های F، به طور یکتا بدست آید. همچنین شرط صفر بودن باقیمانده تقسیم، شرط لازم و کافی برای مسئله عضویت ایده‌آل تولید شده توسط F باشد.

در بخش بعد مفهوم جدیدی به نام پایه گروبنر را معرفی می‌کنیم که مجموعه مولدی با ویژگی‌های فوق است.

۱-۳ پایه گروبنر

در این بخش ابتدا به ایده‌آل‌های تک‌جمله‌ای و خواص آن‌ها می‌پردازیم. ساختار پایه گروبنر بر اساس این نوع از ایده‌آل‌ها بدست می‌آید.

ایده‌آل تک‌جمله‌ای

تعریف ۱.۳.۱. فرض کنیم $K[X]$حلقه‌ی چندجمله‌ای‌های برحسب متغیرهای $x_1, ..., x_n$ با ضرایب در K باشد. اگر I یک ایده‌آل در این حلقه باشد آن را ایده‌آل تک‌جمله‌ای نامیم هرگاه بوسیله مجموعه‌ای از تک‌جمله‌ای‌ها (ممکن است متناهی یا نامتناهی باشد) تولید شود.

به عنوان مثال ایده‌آل $\langle x^4y^2, x^3y^4, x^2y^2\rangle \subset K[X]$ یک ایده‌آل تک‌جمله‌ای است که در آن $X = x, y$.

ایده‌آل‌های تک‌جمله‌ای در حلقه‌ی $K[X]$ با تولید متناهی هستند. این نکته از خواص مهم ایده‌آل‌های تک‌جمله‌ای است که در این قسمت به آن می‌پردازیم. البته قبل از ارائه اثبات آن به لم‌ها و پیش‌نیازهایی احتیاج داریم که آن‌ها را در ادامه بیان می‌کنیم.

لم ۲.۳.۱. *فرض کنید $A \subset \mathbb{Z}^n_{\geq 0}$ (یک مجموعه‌ی متناهی یا نامتناهی) و I یک ایده‌آل تک‌جمله‌ای باشد که توسط $\langle x^\alpha \mid \alpha \in A\rangle$ تولید می‌شود. در این‌صورت یک تک‌جمله‌ای مانند x^β در ایده‌آل I قرار می‌گیرد اگر و تنها اگر $\alpha \in A$ وجود داشته باشد به طوری‌که $x^\beta | x^\alpha$.*