دانشگاه شهرکرد

دانشکده علوم پایه

پایان‌نامه‌ی کارشناسی ارشد رشته‌ی ریاضی گرایش جبر

کدگشایی کدهای تصحیح کننده خطا با فاصله کراندار با استفاده از پایه‌های گروبنر

استاد راهنما:

دکتر علیرضا نقی‌پور

استاد مشاور:

دکتر محمد غلامی

پژوهشگر:

فریبا قاسمی فلاورجانی

دی ماه ۱۳۹۰

من در قعر ضمیر خود احساسی دارم، چون گواهی گوارا و مبهمی که گاه به گاه بر دل می‌گذرد و آن این است که رسالت ایران به پایان نرسیده است و شکوه و خرمی او، به او باز خواهد گشت. من یقین دارم که ایران می‌تواند قد راست کند، کشوری نام‌آور و زیبا و سعادتمند گردد و آن‌گونه که در خور تمدن و فرهنگ و سالخوردگی اوست، نکته‌های بسیاری به جهان بیاموزد....

ایران سزاوار آن است که خوشبخت و سرفراز باشد، و برای آن‌که خوشبخت و سرفراز گردد، باید هم به خود وفادار بماند و هم به استیلای علم بر جهان کنونی ایمان بیاورد و در آموختن آنچه نمی‌داند، غفلت نورزد. ما فرزندان کنونی ایران، موهبت آن را یافته‌ایم که در یکی از دوران‌های رستاخیز این کشور زندگی کنیم، این امر هم موهبتی است و هم مسئولیتی گران بر شانه ما می‌نهد. نخستین نشانه توجه به این مسئولیت آن است که امیدوار بمانیم و صبور باشیم. این گفته تولستوی را از یاد نبریم: «نیرویی برتر از نیروی این دو جنگاور نیست: یکی زمان و دیگری شکیبایی.»

محمد علی اسلامی ندوشن

تقدیم به بهترین های زندگانیم :

پدر و مادر عزیزم .

تشکر و قدردانی

خدایا تو را سپاس که مرا در دایره امکان نهادی و نقش علم را بر دفتر اندیشه‌ام کشیدی و چشمه سار زلال دانش و معرفت را ارزانی‌ام داشتی تا در برهوت نادانی سیراب گر وجودم باشد.

در ابتدا از اولین و بزرگترین معلمان زندگیم، **پدر و مادر بزرگوارم** که مرا به جان پروردند و امید رسیدن به افق‌های روشن را در دلم شکوفا ساختند، از صمیم قلب تشکر می‌کنم.

بر خود لازم می‌دانم به پاس زحمات استاد راهنمای گرامی‌ام، **جناب آقای دکتر علیرضا نقی پور** که با سعه‌ی صدر و دقت نظرشان باعث هرچه پربار شدن این پایان نامه شدند، نهایت تشکر و قدردانی را داشته باشم.

همچنین از استاد مشاور گرامی‌ام، **جناب آقای دکتر محمد غلامی** که با نظرات و رهنمودهای ارزشمند خود مرا یاری نمودند، سپاسگزارم.

از **جناب آقای دکتر تفضلیان** و **جناب خانم دکتر آهنجیده** که زحمت باز خوانی و داوری این پایان نامه را بر عهده گرفتند، تشکر می‌کنم.

چکیده

در این پایان‌نامه کدگشایی کدهای خطی دلخواه را از طریق حل یک دستگاه از معادلات درجه ۲ که با کمک الگوریتم بوخبرگر برای یافتن پایه گروبنر صورت می‌گیرد، انجام می‌دهیم. این روش بر پایه تبدیل یک مسئله ابتدایی به حل یک دستگاه معادلات به روی یک میدان متناهی می‌باشد. یکی از خصوصیات ویژه این دستگاه این است که برای کدگشایی حداکثر نیمی از کمترین فاصله، جوابی منحصربفرد به روی بستار جبری میدان متناهی مفروض داریم، در حالی‌که نیازی به اضافه کردن معادلات میدان به این دستگاه نداریم. تجربه ما نشان می‌دهد، این کدگشایی از کدگشایی فیتزگرید و لکس بسیار سریع‌تر می‌باشد و از دیگر دستاوردهای این روش کارآیی بالای آن نسبت به روش مشخصه عمومی برای بعضی از مقادیر پارامترها می‌باشد.

واژه‌های کلیدی: *کد، کمترین فاصله، ماتریس بررسی توازن کد، مشخصه، کدگشایی مشخصه معین، کدگشایی مشخصه نامعین، توابع ابتدایی متقارن، لگاریتم زیخ.*

فهرست مطالب

فهرست نمادها

حلقه چندجمله‌ای‌ها روی میدان $\mathbb{F}$	$\mathbb{F}[x_1, \cdots, x_n]$
ترتیب الفبایی	$\prec_{\text{lex}}$
ترتیب الفبایی مدرج	$\prec_{\text{dlex}}$
ترتیب الفبایی وارون مدرج	$\prec_{\text{drl}}$
درجه کلی f	$\deg(f)$
جمله پیشرو f	$\text{LT}(f)$
تک‌جمله‌ای پیشرو f	$\text{LM}(f)$
ضریب پیشرو f	$\text{LC}(f)$
پایه گروبنر	G
شکل متعارف f نسبت به G	$\overline{f}^G$
S-چندجمله‌ای f و g	$\text{Spoly}(f, g)$
الفبای کد	$\mathcal{A}$
کد بلوکی	C
طول کد	n
اندازه کد	M
نرخ کد	R
فاصله همینگ رشته‌های $\mathbf{x}$ و $\mathbf{y}$	$d(\mathbf{x}, \mathbf{y})$
کمترین فاصله کد C	$d(C)$
کره به شعاع r و به مرکز $\mathbf{x}$	$S_q(\mathbf{x}, r)$
حجم کره به شعاع r	$V_q(n, r)$

شعاع فشردگی	$\mathrm{pr}(C)$
شعاع پوششی	$\mathrm{cr}(C)$
بزرگترین اندازه یک کد بلوکی	$A_q(n,d)$
بعد کد	k
کد خطی	L
دوگان یک کد خطی	$L^{\perp}$
ماتریس بررسی توازن یک کد خطی	H
مشخصه رشته $\mathbf{x}$	$\mathbf{c}(\mathbf{x})$
هم‌دسته یک کد خطی	$\mathbf{x}+L$
چندجمله‌ای مولد کد دوری	$g(x)$
کد تکراری q تایی	$\mathrm{Rep}(n)$
کد همینگ از مرتبه r	$\mathcal{H}_q(r)$
کدهای گلی دودویی	$\mathcal{G}_{۲۳}, \mathcal{G}_{۲۴}$
کدهای گلی سه تایی	$\mathcal{G}_{۱۱}, \mathcal{G}_{۱۲}$
مجموعه باقیمانده‌های مربعی	QR
مجموعه باقیمانده‌های غیر مربعی	NQR
چندجمله‌ای کمین	$m_i(x)$
i امین هم‌دسته دوری	C_i
کد باقیمانده مربعی روی میدان $\mathbb{F}_{q^p}$	$\mathcal{Q}(p)$
مجموعه کامل صفرهای یک کد دوری	$\mathcal{Z}$
ماتریس واندرموند بر پایه عناصر $\alpha_۱، \cdots، \alpha_n$ از میدان $\mathbb{F}$	$V(\alpha_۱, \cdots, \alpha_n)$
توسیع کد C به روی میدان $\mathbb{F}_{q^m}$	$\tilde{C}$
مشخصه بردار $\mathbf{y}$ برحسب ماتریس بررسی توازن H	$\mathbf{s}(H,\mathbf{y})$
دوگان یک کد خطی	$\mathcal{L}(\mathbf{y},C)$
ایدآل تولید شده توسط توابع خطی $h_i(E)$	$E(\mathbf{y})$
ایدآل تولید شده توسط اشتراک $< E_{j_۱}, \cdots, E_{j_{n-t}} >$ برای $n-t$ تایی‌های افزایشی	$J(t,n)$
ایدآل تولید شده توسط $E(\mathbf{y})$ و $J(t,n)$	$E(t,\mathbf{y})$

وزن بردار $\mathbf{e}$	$\mathrm{wt}(\mathbf{e})$
ایدآل تولید شده توسط $E_{i_1}, \cdots, E_{i_{t+1}}$ برای $t+1$ تایی‌های افزایشی	$I(t,n)$
مشخصه نامعین بردار $\mathbf{e}$ بر حسب ماتریس B	$\mathbf{u}(B,\mathbf{e})$
ماتریس رید سولمون	$B(\alpha)$
ماتریس مشخصه نامعین	$\mathcal{U}$
زیرفضا خطی تولید شده توسط ستون‌های $\mathbf{b}'_{i_1}, \cdots, \mathbf{b}'_{i_t}$ برای t تایی‌های افزایشی	$L(\mathbf{i})$
ایدآل شامل توابعی که هر $\mathbf{u}$ در $L(\mathbf{i})$ را صفر می‌کند	$I(\mathbf{i})$
ایدآل تولید شده توسط کهادهای $t+1 \times t+1$ از زیرماتریس $\mathcal{V}_{l,t+1}$	$I(t,\mathcal{V})$
چندگونای ایدآل $I(t,\mathcal{V})$	$Z(t,\mathcal{V})$
ایدآل تولید شده توسط $\sum_{j=1}^{t} U_{ij}V_j - U_{i,t+1}$	$I(t,\mathcal{U},\mathcal{V})$
چندگونای ایدآل $I(t,\mathcal{U},\mathcal{V})$	$Z(t,\mathcal{U},\mathcal{V})$
سطر i ام ماتریس H	$\mathbf{h}_i$
سطر i ام ماتریس B	$\mathbf{b}_i$
درایه واقع در سطر i ام و ستون j ام ماتریس $\mathcal{U}$	$\mathbf{u}_{ij}$
مجموعه پایه	S
توابع ابتدیی متقارن	σ_i
لگاریتم زیخ	$\mathbf{z}(x)$

مقدمه

با پیشرفت وسایل اکترونیکی و تکنولوژی و میسر شدن ارتباطات از فواصل دور از طریق ماهواره، ارتباطاتی که در قدیم فقط به صورت مکالمه‌ی حضوری یا از طریق مکاتبه انجام می‌گرفت، به طور کلی دگرگون شد. ارتباطات صوتی و تصویری نیز مطرح گردیده و در نتیجه ارتباطات از حساسیت بسیار برخوردار شد. به تدریج نیاز به طراحی سیستم‌هایی جهت انتقال داده‌ها مورد بررسی قرار گرفت و در این راستا مشکلات جدیدی در کنترل و تصحیح خطاهای رخ داده به روی داده‌ها در انتقال از کانال ارتباطی مطرح شد. اینجا بود که نظریه‌ی کدگذاری به منظور انتقال سریع، آسان و صحیح اطلاعات از کانال‌های ارتباطی عنوان شد.

در ارسال پیام دو مسئله حائز اهمیت است. یک مسئله مهم، چگونگی فشرده‌سازی اطلاعات به منظور ارسال سریع و یا ذخیره اقتصادی آن می‌باشد. این مسئله را می‌توان با کاهش افزونگی انجام داد که موضوع مورد مطالعه نظریه اطلاعات است. مسئله مهم دیگر چگونگی کشف و اصلاح خطا در پیام‌های دریافتی است. یک پیام مخابره شده توسط پدیده‌های پارازیتی متنوعی مانند خراش روی دیسک یا یک اختلال در دستگاه، با خطا همراه می‌شود. این گونه خطاها با افزایش افزونگی بررسی می‌شوند. در نظریه کدگذاری کانال، هدف امکان کشف و تصحیح چنین خطاهایی است که با کمک کدهای تصحیح کننده خطا برآورده می‌شود. مبنا و اساس عمل این کدها به این صورت است که بیت‌های پیام را به همراه بیت‌های اضافی دیگر ارسال می‌کنیم به طریقی که این بیت‌های اضافی باعث تقویت و حفاظت پیام می‌شود. این بیت‌ها را به اصطلاح افزونگی می‌گوییم. پس می‌توان نظریه اطلاعات و کدگذاری را دانش انتقال امن و اقتصادی داده‌ها از نقطه‌ای به نقطه دیگر یا از زمانی به زمان دیگر تعریف کرد.

در اواسط جنگ جهانی دوم چند ریاضی‌دان بزرگ و در رأس آن‌ها کلود شانون[1] بررسی جامعی را درباره اصول ارتباطات شروع کردند. حاصل این بررسی در سال ۱۹۴۸ طی مقاله‌ای [۳۹] منتشر شد و انقلابی در علم ارتباطات پدید آورد و از نظر شانون «مسئله اصلی ارتباطات، بازسازی دقیق یا تقریبی پیامی است که در نقطه‌ای دیگر ارسال شده است». شانون ادعا کرد که اگر نرخ ارسال اطلاعات کمتر از ظرفیت کانال باشد،

[1] Claude Shanoon

آن‌گاه می‌توان با استفاده از یک کدگذاری مناسب احتمال خطای کدگشایی را به اندازه کافی به صفر نزدیک نمود و اگر نرخ ارسال بیشتر از ظرفیت کانال باشد چنین کدگذاری با احتمال خطای کدگشایی نزدیک به صفر وجود ندارد. اثبات قضیه او بر پایه احتمالات بوده و روشی برای ساخت چنین کدی ارائه نشده است. برای آشنایی بیشر با نظریه شانون می‌توان به فصل دوم [۴۴] مراجعه کرد. پس از آن تلاش‌هایی زیادی برای رسیدن به کدهای مطلوب آغاز گردید. با تعریف نگاشت‌های خطی روی فضاهای برداری کدهای خطی و دوری معرفی گردید و کدهای معروفی نظیر کدهای همینگ [۲] و رید-سالومن [۳] مطرح شدند. آن‌چه یک کد را از بقیه کدهامتمایز می‌کند، کدگذاری و کدگشایی آسان و کارایی مناسب آن کد می‌باشد. در واقع مهم‌ترین قسمت در ارسال اطلاعات، کنترل خطا یا به عبارت دیگر طراحی مناسب برای کدگذاری و کدگشایی اطلاعات در کانال می‌باشد به گونه‌ای که:

(۱) بتوان اطلاعات را با سرعت خوبی، یعنی نرخ ارسال مناسب، دریک محیط پارازیت دار انتقال داد و یا ذخیره کرد.

(۲) بتوان اطلاعات را در حد قابل قبولی در خروجی کدگشایی کانال دریافت کرد.

(۳) اجرای کدگذاری و کدگشایی، هزینه‌ای تا حد ممکن پایین را داشته باشد.

تاکنون روش‌های بسیاری برای کدگشایی کدهای دوری ارائه شده است. از آن جمله می‌توان روش‌های بیان شده در مراجع [۱، ۷، ۲۵، ۳۳، ۳۶، ۳۷، ۴۲] را اشاره کرد. تمامی این روش‌ها پیچیدگی چندجمله‌ای دارند و در آزمایش‌های صورت گرفته کارآمد هستند، اما قادر به تصحیح میزان واقعی خطای رخ داده روی کد نمی‌باشند. برای برطرف کردن این مشکل از نظریه پایه‌های گروبنر استفاده می‌کنیم. کدگشایی‌هایی که تاکنون برای کدهای دوری ارائه شده است بر پایه سه روش کلی زیر می‌باشد.

(۱) **مشخصه‌های نامعین** در این روش درایه‌های مشخصه یک کد را به صورت متغیر در نظر می‌گیریم و با یک الگوریتم مناسب بردار خطای متناظر با این مشخصه را می‌یابیم و به این صورت کد را کدگشایی می‌کنیم. برای دیدن جزئیات بیشتر می‌توان به مرجع [۷] صفحات ۲۴۰-۲۳۱ و مراجع [۲۶، ۲۷، ۴۳] رجوع کرد.

(۲) **اتحادهای نیوتون:** در این روش از اتحادهای نیوتون برای کدگشایی استفاده می‌شود. این اتحادها رابطه‌ای میان مشخصه‌هاو درایه‌هایشان برقرار می‌کند و این امکان را فراهم می‌کند که مشخصه‌های

[2] Hamming

[3] Reed-Solmon

متفاوت یک کد را دریابیم. برای مطالعه بیشتر به مراجع [۲، ۳، ۴، ۵، ۱۶] رجوع شود.

(۳) **جمع‌های توانی:** با کمک جمع‌های توانی مکان‌های وقوع خطا در یک پیام دریافتی را می‌توانیم دریابیم. مراجع [۱۶، ۱۴، ۱۵، ۱۹، ۲۰، ۲۱، ۱۳، ۳۲، ۳۴] را مشاهده کنید.

کدگشایی‌های بالا را می‌توان روی کدهای خطی دلخواه تعمیم داد. نتایج این تعمیم‌ها در مراجع [۸، ۹، ۱۰، ۲۳، ۲۴، ۳۵] قابل ملاحظه است. کدگشایی که در این پایان‌نامه ارائه می‌دهیم تعمیمی از روش اول روی کدهای خطی دلخواه می‌باشد. در این کدگشایی از نظریه پایه‌های گروبنر برای بالا بردن قدرت تصحیح کنندگی کد استفاده می‌نماییم.

این پایان‌نامه شامل چهار فصل است. در فصل اول با تعریف ترتیب تک‌جمله‌ای، الگوریتم تقسیم را ارائه می‌دهیم سپس پایه گروبنر را معرفی می‌کنیم و الگوریتم بوخبرگر[۴] را برای محاسبه پایه گروبنر یک ایدآل از حلقه‌ی چندجمله‌ای‌ها می‌آوریم. فصل دوم را با تعریف کد بر فضای برداری آغاز می‌کنیم و در ادامه به معرفی کدهای خطی و دوری و بیان خصوصیات ویژه آن‌ها می‌پردازیم. چند نوع کد خطی مانند کدهای همینگ و گلی[۵] را معرفی می‌کنیم و سعی می‌کنیم به طور خلاصه یک کدگشایی برای هر کدام از آن‌ها ارائه دهیم. در فصل ۳ که فصل اصلی پایان‌نامه است، کدگشایی کدهای تصحیح کننده خطا [۱۲] بررسی می‌کنیم. در این فصل با تعریف ایدآل دترمینانی خاص و تعریف ایدآل‌های دیگر به بررسی روابط میان چندگوناهای ایدآل‌ها می‌پردازیم و در نهایت با به‌دست آوردن ایدآل $J(t, \mathbf{y})$ و یافتن پایه گروبنر این ایدآل کد C را کدگشایی می‌کنیم. در فصل ۴ با بیان کدگشایی هیگس[۶] و هامفرز[۷] [۲۸]، سعی می‌کنیم کدگشایی فصل ۳ را با بهره‌گیری از این کدگشایی انجام داده و به این طریق کدگشایی [۱۲] را تایید کنیم.

[4] Buchberger
[5] Golay
[6] Higgs
[7] Hamphreys

فصل ۱

مفاهیم مقدماتی از پایه گروبنر

۱.۱ چندجمله‌ای‌های چند متغیره

در این بخش ابتدا مقدمات لازم برای توصیف پایه گروبنر[1] را فراهم می‌کنیم. از جمله این مقدمات تعریف چندجمله‌ای‌های چند متغیره و ترتیب‌های موجود بر این چندجمله‌ای‌ها می‌باشد. سپس قضایای مربوط به تقسیم چندجمله‌ای‌ها را بیان می‌کنیم.

با مفهوم حلقه‌ی چندجمله‌ای‌های تک متغیره روی میدان $\mathbb{F}$ (که با نماد $\mathbb{F}[x]$ نمایش داده می‌شود.) و مفاهیم پیرامون آن در جبر آشنا شده‌ایم. از آن‌جا که چندجمله‌ای‌هایی که در علوم ریاضی کاربرد فراوان دارند، چندجمله‌ای‌های چند متغیره هستند، در این بخش برآنیم که حلقه‌ی چندجمله‌ای‌های چند متغیره و مفاهیم پیرامون آن را به اختصار معرفی و بررسی کنیم.

تعریف ۱.۱.۱. یک تک‌جمله‌ای برحسب $x_1، \cdots، x_n$ عبارت است از حاصل‌ضربی به شکل $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ که در آن $\alpha_1, \cdots, \alpha_n \in \mathbb{N} \cup \{0\}$. این تک‌جمله‌ای را با نماد x^α که $\alpha = (\alpha_1, \cdots, \alpha_n)$ نمایش می‌دهیم.

تعریف ۱.۱.۲. میدان $\mathbb{F}$ را در نظر می‌گیریم. چندجمله‌ای f برحسب $x_1، \cdots، x_n$ باضرایب در میدان $\mathbb{F}$ را به صورت یک ترکیب خطی متناهی از تک‌جمله‌ای‌ها تعریف می‌کنیم. به عبارت دیگر یک چندجمله‌ای بر حسب $x_1، \cdots، x_n$ عبارت است از $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ که در آن $a_\alpha \in \mathbb{F}$ و A یک زیرمجموعه متناهی از $(\mathbb{N} \cup \{0\})^n$ است، به هر یک از $a_\alpha x^\alpha$ ها یک جمله گوییم.

[1] Groebner basis

تعریف ۳.۱.۱. مجموعه‌ی همه چندجمله‌ای‌ها برحسب $x_1, \cdots, x_n$ با ضرایب در میدان $\mathbb{F}$ را حلقه‌ی چندجمله‌ای‌ها روی $\mathbb{F}$ نامیده و با $R = \mathbb{F}[x_1, \cdots, x_n]$ نمایش می‌دهیم.

برای توصیف الگوریتم تقسیم چندجمله‌ای‌های تک متغیره، مفاهیمی مانند جمله پیشرو و ضریب پیشرو نیز مطرح است، به این ترتیب که جمله با بزرگترین درجه x، جمله پیشرو و ضریب این جمله، ضریب پیشرو نامیده می‌شود. در چندجمله‌ای‌های چند متغیره، مرتب کردن جمله‌ها تنها برحسب درجه امکان‌پذیر نیست. به عنوان مثال در چندجمله‌ای $f = x^3 + xy^2 + xyz$، هر سه جمله از درجه ۳ است، پس نمی‌توان گفت کدام یک جمله پیشرو است. برای این منظور لازم است یک رابطه ترتیب روی تک‌جمله‌ای‌ها تعریف کنیم تا بتوانیم بین آن‌ها تمایز قائل شویم. البته رابطه‌ای که تعریف می‌کنیم باید خصوصیاتی داشته باشد که در تعاریف زیر به آن‌ها اشاره خواهیم کرد.

تعریف ۴.۱.۱. رابطه $\leq$ را یک ترتیب کلی روی مجموعه‌ی X نامیم، هرگاه برای هر $a, b, c \in X$ داشته باشیم:

(۱) انعکاسی: برای هر a، $a \leq a$ باشد.

(۲) پادتقارنی : هرگاه $a \leq b$ و $b \leq a$، آن‌گاه $a = b$.

(۳) تعدی: هرگاه $a \leq b$ و $b \leq c$، آن‌گاه $a \leq c$.

(۴) مقایسه‌پذیری: $a \leq b$ یا $b \leq a$.

تعریف ۵.۱.۱. رابطه $\leq$ روی $\mathbb{Z}_{\geq 0}^n$ را خوش ترتیب نامیم، هرگاه هر زیرمجموعه‌ی ناتهی از $\mathbb{Z}_{\geq 0}^n$ دارای کوچکترین عضو نسبت به $\leq$ باشد.

قبل از تعریف ترتیب تک‌جمله‌ای، به تعریف دیگری نیازمندیم که در زیر آمده است.

تعریف ۶.۱.۱. یک رابطه ترتیب تک‌جمله‌ای $\leq$ روی $\mathbb{Z}_{\geq 0}^n$ رابطه‌ای است که در شرایط زیر صدق کند:

(۱) $\leq$ یک ترتیب کلی روی $\mathbb{Z}_{\geq 0}^n$ باشد.

(۲) هرگاه $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$ و $\alpha \leq \beta$، آن‌گاه $\alpha + \gamma \leq \beta + \gamma$.

(۳) $\leq$ یک رابطه خوش ترتیب باشد.

تعریف ۷.۱.۱. ترتیب تک‌جمله‌ای روی حلقه‌ی R عبارت است از یک رابطه ترتیب تک‌جمله‌ای روی $\mathbb{Z}^n_{\geq 0}$ که با استفاده از تناظر یک به یک زیر به R منتقل می‌شود.

$$\phi : \mathbb{Z}^n_{\geq 0} \longrightarrow R$$
$$\alpha \mapsto x^\alpha$$

از این به بعد یک ترتیب تک‌جمله‌ای روی R را با نماد $\prec$ نمایش می‌دهیم.

حال آماده‌ایم که انواع ترتیب‌های تک‌جمله‌ای روی R را معرفی می‌کنیم.

تعریف ۸.۱.۱. فرض می‌کنیم x^α و x^β دو تک‌جمله‌ای در R و n تایی‌های $\alpha = (\alpha_1, \cdots, \alpha_n)$ و $\beta = (\beta_1, \cdots, \beta_n)$ اعضایی از $\mathbb{Z}^n_{\geq 0}$ باشند. ترتیب الفبایی که با نماد $\prec_{\text{lex}}$ نمایش داده می‌شود، به صورت زیر تعریف می‌شود.

گوییم $x^\beta \prec_{\text{lex}} x^\alpha$، هرگاه اولین عنصر ناصفر از سمت چپ $\alpha - \beta$ مثبت باشد. ترتیب الفبایی بالا را ترتیب مدرج نامیده و با $x^\beta \prec_{\text{dlex}} x^\alpha$ نمایش می‌دهیم، هرگاه $|\beta| = \sum_{i=1}^n \beta_i < |\alpha| = \sum_{i=1}^n \alpha_i$ یا $|\alpha| = |\beta|$ بوده و همین‌طور داشته باشیم $x^\beta \prec_{\text{lex}} x^\alpha$. ترتیب تک‌جمله‌ای مهم دیگر ترتیب الفبایی وارون مدرج نام دارد که به صورت زیر معرفی می‌شود. گوییم $x^\beta \prec_{\text{drl}} x^\alpha$ ، هرگاه $|\beta| = \sum_{i=1}^n \beta_i < |\alpha| = \sum_{i=1}^n \alpha_i$ یا $|\alpha| = |\beta|$ و همین‌طور اولین عنصر ناصفر از سمت راست n تایی $\alpha - \beta$ منفی می‌باشد.
برای اثبات این‌که ترتیب‌های بالا تک‌جمله‌ای هستند به مرجع [۲۲] صفحات ۵۵ و ۵۶ مراجعه کنید.

مثال ۹.۱.۱. در $\mathbb{F}[x, y, z]$ داریم:

(۱) $x \prec_{\text{lex}} y \prec_{\text{lex}} z$ و $x \prec_{\text{dlex}} y \prec_{\text{dlex}} z$ و $x \prec_{\text{drl}} y \prec_{\text{drl}} z$. این روابط با استفاده از تساوی‌های $(۱, -۱, ۰) = (۱, ۰, ۰) - (۰, ۱, ۰)$ و $(۰, ۱, -۱) = (۰, ۱, ۰) - (۰, ۰, ۱)$ و تعاریف بالا ثابت می‌شوند.

(۲) $y^۳z^۴ \prec_{\text{lex}} xy^۲$؛ زیرا $(۱, -۱, -۴) = (۱, ۲, ۰) - (۰, ۳, ۴)$.

(۳) $xy^۲ \prec_{\text{dlex}} y^۳z^۴$؛ زیرا $۱ + ۲ < ۳ + ۴$.

(۴) $y^۲z \prec_{\text{drl}} xy^۲$؛ زیرا $(۱, ۰, -۱) = (۱, ۲, ۰) - (۰, ۲, ۱)$.

حال با استفاده از مفهوم ترتیب تک‌جمله‌ای می‌توان مفاهیمی چون جمله پیشرو، ضریب پیشرو و مانند آن را معرفی کرد.

تعریف ۱.۱.۱۰. چندجمله‌ای $f = a_\alpha x^\alpha + \cdots + a_\gamma x^\gamma \in R$ و ترتیب تک‌جمله‌ای $\prec$ روی R را در نظر می‌گیریم. هرگاه $a_\alpha \neq 0$ و $x^\gamma \prec \cdots \prec x^\alpha$، آن‌گاه:

(۱) درجه کلی f برابر است با $\deg(f) = \max\{\, |\beta| \mid a_\beta \neq 0 \,\}$.

(۲) جمله پیشرو f برابر است با $\mathrm{LT}(f) = a_\alpha x^\alpha$.

(۳) تک‌جمله‌ای پیشرو f برابر است با $\mathrm{LM}(f) = x^\alpha$.

(۴) ضریب پیشرو f برابر است با $\mathrm{LC}(f) = a_\alpha$.

یکی دیگر از مطالبی که در مورد چندجمله‌ای‌های تک متغیره مطرح می‌شود، تقسیم آن‌ها بر یکدیگر است. به عبارت دیگر هرگاه $f, g \in \mathbb{F}[x]$ دو چندجمله‌ای تک متغیره باشند، آن‌گاه $g, r \in \mathbb{F}[x]$ وجود دارند که $f = qg + r$ و $r = 0$ یا $\deg(r) < \deg(g)$. در این حالت q را خارج قسمت و r را باقیمانده f بر g گوییم. در قضیه‌ی زیر این مطلب را در مورد چندجمله‌ای‌های چند متغیره بررسی می‌کنیم.

قضیه ۱.۱.۱۱. *فرض می‌کنیم $\prec$ یک ترتیب تک‌جمله‌ای روی R و $f_1, \cdots, f_k \in R$ چندجمله‌ای باشند. دراین‌صورت هر چندجمله‌ای $f \in R$ را می‌توان به صورت $f = a_1 f_1 + \cdots + a_k f_k + r$ نوشت که در آن $r, a_i \in R$ و $r = 0$ یا این‌که هیچ جمله‌ای از r بر $\mathrm{LT}(f_1), \cdots, \mathrm{LT}(f_k)$ بخش‌پذیر نیست.*

برهان. رجوع کنید به [۲۲] قضیه ۳ صفحه ۶۱. □

حال آماده‌ایم الگوریتم تقسیم را مطرح کنیم.

الگوریتم تقسیم

Input : $f_۱, \cdots, f_k, f \in R$.

Output : $a_۱, \cdots, a_k, r \in R \quad a_۱ := ۰, \cdots, a_k := ۰, \quad r = ۰ \quad p := f$

While $p \neq ۰$ do

$i := ۱$;

flag:= false;

While $i \neq k$ and flag = false do

If $\mathrm{LT}(f_i) \mid \mathrm{LT}(p)$ then;

$a_i := a_i + LT(p)/\mathrm{LT}(f_i)$;

$p := p + LT(p)/\mathrm{LT}(f_i) f_i$;

flag:=true;

else

$i := i + ۱$;

end if;

end while;

if flag = false then

$r := r + \mathrm{LT}(p)$;

$p := p - \mathrm{LT}(p)$;

end if

end While

Return $(a_۱, \cdots, a_k, r)$;

الگوریتم بالا را در نرم فزار میپل اجرا کرده و مثال زیر را با استفاده از آن حل می‌کنیم.

مثال ۱.۱.۱۲. فرض می‌کنیم $f = x^۲y + xy^۲ + y^۲$ و $f_۱ = xy - ۱$ و $f_۲ = y^۲ - ۱$ و $y \prec_{\mathrm{lex}} x$.

دراین صورت با استفاده از الگوریتم بالا داریم،

$$f = (x+y)f_۱ + f_۲ + x + y + ۱.$$

حال اگر ترتیب مقسوم علیه‌ها را عوض کنیم، یعنی $y_۱ = f_۲ = y^۲ - ۱$ و $y_۲ = f_۱ = xy - ۱$ آن‌گاه داریم، $f = (x+y)y_۱ + xy_۲ + x + ۲x + ۱$. در مثال بالا مشاهده می‌کنیم که باقیمانده یکتا نیست و با تغییر ترتیب مقسوم علیه‌ها و حتی تغییر ترتیب تک‌جمله‌ای، باقیمانده تغییر می‌کند. اما در مورد چندجمله‌ای‌های تک متغیره دیده‌ایم که باقیمانده یکتاست. حال سوال این است که «تحت چه شرایطی باقیمانده یکتا خواهد شد؟» اگر مجموعه‌ی مقسوم علیه‌ها پایه گروبنر باشد، آن‌گاه پاسخ مثبت است. این پایه‌ها را در بخش بعد مطالعه می‌کنیم.

۲.۱ پایه گروبنر

در این بخش ابتدا مقدمات لازم برای معرفی پایه گروبنر را فراهم کرده و سپس الگوریتمی معروف به الگوریتم بوخبرگر را برای محاسبه این پایه ارائه می‌دهیم. برای این منظور ابتدا ایدآل‌های تک‌جمله‌ای را معرفی می‌کنیم.

تعریف ۱.۲.۱. ایدآل $I \subseteq R$ را یک ایدآل تک جمله‌ای نامیم، هرگاه توسط مجموعه‌ای از تک‌جمله‌ای‌ها تولید شود.

به عنوان مثال $I =< x^۴y^۲, x^۳y^۴, x^۲y^۵ >$ یک ایدآل تک‌جمله‌ای است. حال لازم است اعضای ایدآل تک‌جمله‌ای را مشخص کنیم. لم زیر این نیاز را برآورده می‌کند.

لم ۲.۲.۱. *فرض می‌کنیم A یک زیرمجموعه از $\mathbb{Z}^n_{\geq ۰}$ و $I =< x^\alpha | \alpha \in A >$ یک ایدآل تک‌جمله‌ای باشد. دراین‌صورت:*

(۱) *تک‌جمله‌ای x^β در I است اگر و تنها اگر $\alpha \in A$ وجود داشته باشند که $x^\alpha \mid x^\beta$. به عبارت دیگر $\alpha \in A$ و $\gamma \in \mathbb{Z}^n_{\geq ۰}$ وجود داشته باشد که $\beta = \alpha + \gamma$.*

(۲) *چندجمله‌ای f در I است اگر و تنها اگر هر جمله f در I باشد.*

برهان. رجوع کنید به [۲۲] لم ۲ صفحه ۶۷. □