فرهنگ و اندیشهٔ ریاضی

شماره ۵۶ (بهار ۱۳۹۴) صص. ۶۹ تا ۸۲

نرمال‌سازی نوتر و پایهٔ گربنر

امیر هاشمی و نازنین رحمانی

چکیده

یکی از روش‌هایی که در بهبود محاسبات مربوط به ایدآل‌های حلقهٔ چندجمله‌ای‌ها مطرح است، قرار دادن یک ایدآل در موقعیتی است که یک مجموعهٔ مولد مناسب برای آن به‌دست آید. به‌عنوان مثال برای محاسبهٔ چندگونای متناظر، بعد و رادیکال یک ایدآل با قرار دادن آن در یک موقعیت مناسب به‌نام موقعیت نوتر می‌توان سرعت محاسبات را ارتقاء داد. در این مقاله، یک الگوریتم برای پیدا کردن تنک‌ترین ماتریس تغییر مختصات برای قرار دادن یک ایدآل در موقعیت نوتر معرفی می‌کنیم. برای این منظور، از مفهوم پایهٔ گربنر که ابزاری قوی در علوم محاسباتی محسوب می‌شود، استفاده می‌کنیم. در این راستا ابتدا مفهوم‌های نرمال‌سازی نوتر و پایهٔ گربنر را به‌تفصیل یادآوری و برخی از کاربردها و ارتباط‌های آن‌ها را بیان می‌کنیم. در پایان نیز الگوریتم مورد نظر را با ارائهٔ مثال‌هایی شرح می‌دهیم.

۱. مقدمه

فرض کنید K یک میدان و $R = K[x_1, \ldots, x_n]$ حلقهٔ چندجمله‌ای‌ها با متغیرهای $x_1, \ldots, x_n$ و با ضرایب در K و I یک ایدآل R باشد. برای محاسبهٔ کمیت‌های مربوط به I، شکل ارائهٔ ایدآل از اهمیت ویژه‌ای برخوردار بوده و در حجم محاسبات حائز اهمیت است. بنابراین یکی از مباحث مهم در هندسهٔ جبری و جبر محاسباتی یافتن موقعیت مناسب ایدآل I

عبارات و کلمات کلیدی. نرمال‌سازی نوتر، پایهٔ گربنر.

برای محاسبهٔ کمیت مورد نظر است. منظور از تغییر شکل ارائهٔ یک ایدآل، پیدا کردن یک موقعیت مناسب برای آن و در نتیجه یافتن یک مجموعهٔ مولد مناسب برای ایدآل است. لازم به ذکر است که برخی از کمیت‌های مربوط به یک ایدآل مانند بعد آن تحت تغییر شکل ایدآل پایا هستند. برای مثال ایدآل $I = \langle xy - ۱ \rangle \subseteq \mathbb{R}[x, y]$ را در نظر بگیرید. با جایگذاری $x + \tilde{y}$ به‌جای y در $xy - ۱$ شکل ارائهٔ ایدآل به‌صورت $\langle x^۲ + x\tilde{y} - ۱ \rangle \subseteq \mathbb{R}[x, \tilde{y}]$ خواهد بود، اما بعد ایدآل تغییر نمی‌کند. یکی از شکل‌های مناسب برای یک ایدآل، نرمال‌سازی نوتر[1] یعنی قرار دادن یک ایدآل در موقعیت نوتر[2] است. نرمال‌سازی نوتر در محاسبهٔ رادیکال یک ایدآل، بعد ایدآل و تصویر چندگونای مستوی[3] کاربرد دارد. در این مقاله روش محاسباتی کارایی برای قرار دادن یک ایدآل در موقعیت نوتر بیان می‌کنیم. در این روش به‌کمک پایهٔ گربنر[4] می‌توان یک الگوریتم قطعی برای محاسبهٔ نرمال‌سازی نوتر با تنک‌ترین ماتریس تغییر مختصات ارائه داد؛ در حالی که بقیهٔ الگوریتم‌های محاسبهٔ نرمال‌سازی نوتر از روش‌های تصادفی استفاده می‌کنند [۵]. مفهوم پایهٔ گربنر یکی از مفهوم‌های اساسی در هندسهٔ جبری و جبر محاسباتی است که حدود نیم قرن پیش توسط بوخبرگر[5] در پایان‌نامه دکترایش معرفی شد. او بعدها به احترام استاد راهنمایش این مفهوم جدید را پایهٔ گربنر نامید [۲]. با توجه به جنبه‌های محاسباتی، پایهٔ گربنر به یکی از ابزارهای مهم در علوم و مهندسی تبدیل شده است. تاکنون ۶ کتاب و بالغ بر ۳۰۰۰ مقاله در زمینهٔ پایهٔ گربنر و کاربردهای آن نگاشته شده است که نشان از اهمیت و کاربردی بودن این مفهوم دارد.

ساختار این مقاله به این صورت است که در بخش دوم مفهوم‌های نرمال‌سازی نوتر و پایهٔ گربنر را معرفی و برخی کاربردهای آن‌ها را بیان می‌کنیم. در پایان، در بخش سوم با ارائهٔ یک الگوریتم ارتباط این دو مفهوم را بیان می‌کنیم.

۲. نرمال‌سازی نوتر، پایهٔ گربنر و کاربردها

در این بخش ابتدا به بیان برخی مفهوم‌ها و اصطلاحات جبری می‌پردازیم که برای معرفی مفهوم نرمال‌سازی نوتر به آن‌ها نیاز داریم. برای مطالعهٔ کامل‌تر این مفاهیم مرجع [۸] توصیه می‌شود.

ابتدا مفهوم توسیع صحیح را با ارائهٔ چند مثال معرفی می‌کنیم و در قسمت کاربردهای پایهٔ گربنر محک مهمی را برای تشخیص صحیح بودن توسیع یک حلقه ارائه می‌دهیم. فرض کنید S

[1]Noether normalization [2]Noether position [3]Affine variety [4]Groebner basis [5]Buchberger

یک حلقه جابجایی و یکدار و R زیرحلقه‌ای از آن باشد. در این صورت S را یک توسیع حلقه‌ای R گوییم و می‌نویسیم $R \subseteq S$. در ادامه، S را یک توسیع حلقه‌ای R در نظر می‌گیریم.

تعریف ۱.۲. عنصر $s \in S$ را روی R صحیح گوییم هرگاه یک چندجمله‌ای $f \in R[x]$ وجود داشته باشد به‌طوری که ضریب بزرگترین توان x برابر ۱ باشد و $f(s) = 0$.

اگر تمام اعضای S روی R صحیح باشند، S را یک توسیع حلقه‌ای صحیح R می‌نامیم.

مثال ۲.۲. برای هر $d \in \mathbb{Q}$، $\sqrt{d} \in \mathbb{R}$ روی $\mathbb{Q}$ صحیح است.

مثال ۳.۲. $\mathbb{C}$ و $\mathbb{R}$ توسیع‌های حلقه‌های $\mathbb{Q}$ و $\mathbb{Z}$ هستند، اما صحیح نیستند، زیرا $\pi \in \mathbb{C}, \mathbb{R}$ ریشهٔ هیچ چندجمله‌ای با ضرایب در $\mathbb{Q}$ یا $\mathbb{Z}$ نیست.

تعریف ۴.۲. فرض کنید R یک K-جبر مستوی باشد. در این صورت $y_1, y_2, \dots, y_n \in R$ را روی K مستقل جبری می‌نامیم هرگاه به‌ازای هر چندجمله‌ای n متغیره مانند f که $f(y_1, \dots, y_n) = 0$، داشته باشیم $f = 0$.

اکنون قضیهٔ نرمال‌سازی نوتر را (که اولین بار امی نوتر[1] ریاضیدان آلمانی در سال ۱۹۲۶ معرفی کرد) بیان می‌کنیم.

قضیه ۵.۲ (نرمال‌سازی نوتر). *فرض کنید K یک میدان، n یک عدد صحیح مثبت و I یک ایدآل سره در حلقهٔ چندجمله‌ای‌های $R = K[x_1, \dots, x_n]$ باشد. در این صورت $d \leq n$ و $y_1, \dots, y_n \in R$ وجود دارند به قسمی که*

(آ) *$\{y_1, \dots, y_n\}$ روی K مستقل جبری هستند،*

(ب) *R یک B-مدول متناهی مولد است که $B = K[y_1, \dots, y_n]$،*

(پ) *$I \cap B = \langle y_{d+1}, \dots, y_n \rangle \subseteq B$،*

(ت) *به‌علاوه اگر $|K| = \infty$ آن‌گاه $y_1, \dots, y_d$ چندجمله‌ای‌های خطی برحسب $x_1, \dots, x_n$ هستند.*

تعریف ۶.۲. اگر $I \subseteq R = K[x_1, \dots, x_n]$ یک ایدآل و $y_1, \dots, y_d \in R/I$ روی K مستقل جبری و R/I روی $K[y_1, \dots, y_d]$ صحیح باشد، آن‌گاه $K[y_1, \dots, y_d]$ را یک نرمال‌سازی نوتر برای R/I می‌نامیم.

[1] Emmy Noether

مثال ۷.۲. $K[x]$ یک نرمال‌سازی نوتر برای $K[x,y]/\langle x^۳ - y^۲\rangle$ است. واضح است که x روی K مستقل جبری است. از طرفی $x + \langle x^۳ - y^۲\rangle$ و $y + \langle x^۳ - y^۲\rangle$ به‌ترتیب ریشه‌های $X - x(۱ + \langle x^۳ - y^۲\rangle) = ۰$ و $X^۲ - x^۳(۱ + \langle x^۳ - y^۲\rangle) = ۰$ و در نتیجه روی $K[x]$ صحیح هستند. بنابراین $K[x,y]/\langle x^۳ - y^۲\rangle$ روی $K[x]$ صحیح است.

در بعضی مراجع از مفهوم موقعیت نوتر به‌جای نرمال‌سازی نوتر استفاده می‌شود که در ادامه به آن اشاره می‌کنیم. لازم به ذکر است که این مفهوم معادل نرمال‌سازی نوتر است. یادآوری می‌کنیم که طول بزرگترین زنجیر از ایدآل‌های اول حلقهٔ R که شامل ایدآل I هستند را بعد ایدآل I می‌نامیم.

تعریف ۸.۲. فرض کنید $I \subseteq K[x_۱, \ldots, x_n]$ یک ایدآل از بعد d باشد. ایدآل I را در موقعیت نوتر می‌نامیم هرگاه

(آ) $K[x_۱, \ldots, x_d] \cap I = \{۰\}$،

(ب) برای هر $i = ۱, \ldots, n - d$، یک چندجمله‌ای $h_{d+i} \in K[x_۱, \ldots, x_{d+i}] \cap I \setminus \{۰\}$ برحسب x_{d+i} وجود داشته باشد که ضریب بزرگترین توان x_{d+i} برابر ۱ باشد.

در ادامه، مفهوم پایهٔ گربنر را معرفی می‌کنیم و سپس به بیان برخی از کاربردهای مرتبط با موضوع این مقاله می‌پردازیم. برای توضیحات تکمیلی به [۱، ۳] مراجعه کنید. فرض کنید $\mathbb{M}$ مجموعهٔ تمام تک‌جمله‌ای‌ها در $R = K[x_۱, \ldots, x_n]$ باشد. یک ترتیب تک‌جمله‌ای روی R یک ترتیب کلی $\prec$ روی $\mathbb{M}$ است که در شرایط زیر صدق کند:

(آ) برای هر $m_۱, m_۲, m_۳ \in \mathbb{M}$ که $m_۱ \prec m_۲$ داشته باشیم $m_۱m_۳ \prec m_۲m_۳$،

(ب) به‌ازای هر $m \in \mathbb{M}$، $۱ \prec m$.

مثال مهمی از ترتیب تک‌جمله‌ای ترتیب الفبایی است. فرض کنید $\alpha, \beta \in \mathbb{N}^n$ و x^α و x^β دو تک‌جمله‌ای باشند. x^α را نسبت به ترتیب الفبایی از x^β بزرگتر گوییم (و می‌نویسیم $x^\alpha \succ_{lex} x^\beta$) هرگاه سمت چپ‌ترین مؤلفهٔ ناصفر $\alpha - \beta$ مثبت باشد. برای هر $f \in R$ بزرگترین تک‌جمله‌ای f نسبت به ترتیب $\prec$ را تک‌جمله‌ای پیشرو، ضریبش را ضریب پیشرو و حاصلضرب آن‌ها را جملهٔ پیشرو می‌نامیم و به‌ترتیب با نمادهای $LM(f)$ ، $LC(f)$ ، $LT(f)$ نمایش می‌دهیم. فرض کنید $I \subseteq R$ یک ایدآل و $\prec$ یک ترتیب تک‌جمله‌ای روی R باشد. ایدآل پیشروی I را با نماد $LT(I)$ نمایش می‌دهیم و به‌صورت زیر تعریف می‌کنیم:

$$LT(I) = \langle LT(f) \mid f \in I\rangle.$$

تعریف ۹.۲. فرض کنید $I \subseteq R$ یک ایدآل و $\succ$ یک ترتیب تک‌جمله‌ای روی R باشد. زیرمجموعهٔ متناهی $G = \{g_1, \dots, g_s\} \subseteq I$ را یک پایهٔ گربنر I نسبت به $\succ$ می‌نامیم هرگاه $LT(I) = \langle LT(g_1), \dots, LT(g_s)\rangle$.

تعریف ۱۰.۲ (ایدآل حذفی). فرض کنید $I \subseteq R$ یک ایدآل و $0 \leq l < n$ یک عدد صحیح باشد. l−امین ایدآل حذفی I عبارت است از $I_l = I \cap K[x_{l+1}, \dots, x_n]$.

قضیه ۱۱.۲ (قضیه حذف). *اگر $I \subseteq R$ یک ایدآل و G یک پایهٔ گربنر برای I نسبت به ترتیب $x_1 \succ_{lex} x_2 \succ_{lex} \cdots \succ_{lex} x_n$ باشد، آن‌گاه برای هر $0 \leq l < n$ مجموعهٔ $G_l = G \cap K[x_{l+1}, \dots, x_n]$ یک پایهٔ گربنر برای ایدآل حذفی I_l است.*

به‌عنوان کاربردی از قضیهٔ حذف یک روش محاسباتی برای حذف متغیرها از دستگاه معادلات چندجمله‌ای برای یافتن جواب دستگاه ارائه می‌کنیم. در ادامه با یک مثال این روند را معرفی می‌کنیم.

مثال ۱۲.۲. دستگاه زیر را در نظر بگیرید:

$$\begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases}$$

ایدآل متناظر با این دستگاه، یعنی $I = \langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1\rangle$ را در نظر می‌گیریم. در این صورت پایهٔ گربنر I نسبت به ترتیب $x \succ_{lex} y \succ_{lex} z$ مجموعهٔ چندجمله‌های زیر خواهد بود:

$$g_1 = x + y + z^2 - 1, \qquad g_2 = y^2 - y - z^2 - z,$$
$$g_3 = 2yz^2 + z^4 - z^2, \qquad g_4 = z^6 - 4z^4 + 4z^3 - z^2.$$

از طرفی جواب‌های دستگاه مورد نظر همان جواب‌های دستگاه بالا است. همان طور که مشاهده می‌شود، g_4 یک چندجمله‌ای برحسب z است. با حل معادلهٔ $z^6 - 4z^4 + 4z^3 - z^2 = 0$ مقدار z را $0, 1, -1 \pm \sqrt{2}$ به‌دست می‌آوریم. با جایگزینی این مقادیر در g_3 و g_2 جواب‌های ممکن

برای y و در آخر نیز با جایگزینی مقادیر y و z در $g_۱$، مقدار x را به‌دست می‌آوریم. به این ترتیب مجموعهٔ زیر جواب دستگاه معادلات خواهد بود:

$$\{(۱, ۰, ۰), (۰, ۱, ۰), (۰, ۰, ۱), (-۱ + \sqrt{۲}, -۱ + \sqrt{۲}, -۱ + \sqrt{۲}), \\ (-۱ - \sqrt{۲}, -۱ - \sqrt{۲}, -۱ - \sqrt{۲})\}$$

در حالت کلی جواب‌های یک دستگاه معادلات را به‌کمک دو مرحلهٔ زیر می‌توانیم به‌دست آوریم.

(مرحله حذف): در این مرحله همهٔ متغیرها را جز یکی حذف می‌کنیم تا یک چندجمله‌ای تک‌متغیره به‌دست آوریم.

(مرحله توسیع) : در این مرحله ابتدا ریشهٔ چندجمله‌ای تک‌متغیره را به‌دست می‌آوریم. سپس با جایگزینی هر یک از این جواب‌ها در معادلات دیگر، مقدار بقیهٔ متغیرها را به‌دست می‌آوریم.

همان طور که در بخش قبل گفتیم با استفاده از پایهٔ گربنر محکی برای تشخیص صحیح بودن یک توسیع حلقه‌ای ارائه می‌دهیم. فرض کنید K یک میدان، $I \subseteq R = K[x_۱, \dots, x_n]$ یک ایدآل و $f_۱, \dots, f_k$، k چندجمله‌ای در R باشد. برای هر $۱ \leq i \leq k$ قرار می‌دهیم $\bar{f_i} = f_i + I$ و تعریف می‌کنیم $B = K[\bar{f_۱}, \dots, \bar{f_k}]$. در این صورت واضح است که B یک زیرحلقهٔ R/I است. اکنون می‌خواهیم بررسی کنیم در چه صورت چندجمله‌ای $h \in R$ روی $K[f_۱, \dots, f_k]$ به پیمانهٔ I صحیح است یا به عبارت دیگر، در چه صورت $h + I$ روی B صحیح است؟ محک زیر به این سؤال پاسخ می‌دهد.

گزاره ۱۳.۲ (محک صحیح بودن). *فرض کنید* $h, f_۱, \dots, f_k \in R$،

$$I = \langle g_۱, \dots, g_s \rangle \subseteq R,$$

یک ایدآل و $t, y_۱, \dots, y_k$ *متغیرهای کمکی باشند. ایدآل*

$$J = \langle t - h, y_۱ - f_۱, \dots, y_k - f_k, g_۱, \dots, g_s \rangle,$$

را در نظر می‌گیریم. فرض کنید $\succ$ *یک ترتیب تک‌جمله‌ای به‌صورت*

$$x_۱ \succ_{lex} \cdots \succ_{lex} x_n \succ_{lex} t \succ_{lex} y_۱ \succ_{lex} \cdots \succ_{lex} y_k,$$

روی $K[x_1,\ldots,x_n,t,y_1,\ldots,y_k]$ و G یک پایهٔ گربنر برای J نسبت به این ترتیب باشد. در این صورت h روی $K[f_1,\ldots,f_k]$ به پیمانهٔ I صحیح است اگر و تنها اگر یک $g \in G$ وجود داشته باشد به‌طوری که تک‌جمله‌ای پیشروی آن به‌صورت $LM(g) = t^p$ باشد که در آن، $p > 0$. به‌علاوه g یک چندجمله‌ای صحیح برای h روی $K[f_1,\ldots,f_k]$ به پیمانهٔ I تعریف می‌کند.

مثال ۱۴.۲. فرض کنید $K = \mathbb{Q}$، $I = \langle x_1^2 - x_3^2 \rangle \subseteq K[x_1,x_2,x_3,x_4]$، $f_1 = x_3^2 - 1$ و $f_2 = x_1^2 x_2$. می‌خواهیم صحیح بودن x_3 و x_4 را روی $K[f_1,f_2]$ به پیمانهٔ I بررسی کنیم. ایدآل‌های

$$I_1 = \langle t - x_3, y_1 - f_1, y_2 - f_2, I \rangle, \quad \text{و} \quad I_2 = \langle t - x_4, y_1 - f_1, y_2 - f_2, I \rangle,$$

را در $K[x_1,\ldots,x_4,t,y_1,y_2]$ در نظر می‌گیریم. پایهٔ گربنر این ایدآل‌ها نسبت به ترتیب

$$x_1 \succ_{lex} \cdots \succ_{lex} t \succ_{lex} \cdots \succ_{lex} y_2,$$

مجموعه‌های

$$G_1 = \{t^2 - y_1 - 1, x - 3 - t, x_2^4 - y_2, x_1^2 - x_2^3\},$$
$$G_2 = \{x_4 - t, x_2^4 - y_2, x_3^2 - y_1 - 1, x_1^2 - x_2^3\}$$

است. بنابراین با توجه به گزارهٔ قبل، چون t^2 تک‌جمله‌ای پیشروی $t^2 - y_1 - 1$ است، پس x_3 روی $K[f_1,f_2]$ به پیمانهٔ I با $x_3^2 - f_1 - 1$ صحیح است در حالی که x_4 روی $K[f_1,f_2]$ به پیمانهٔ I صحیح نیست.

اکنون با توجه به تعریفی که برای بعد ایدآل بیان می‌کنیم، به‌کمک پایهٔ گربنر آن را محاسبه می‌کنیم.

تعریف ۱۵.۲. فرض کنید $I \subseteq R$ یک ایدآل باشد. بعد ایدآل I را می‌توان به‌صورت زیر تعریف کرد:

$$\dim(I) = \max\{|u| \mid u \subseteq \{x_1,\ldots,x_n\},\ I \cap K[u] = \{0\}\}.$$

برای محاسبهٔ بعد یک ایدآل I با استفاده از این تعریف، برای هر زیر مجموعهٔ $u \subseteq \{x_1,\ldots,x_n\}$ یک ترتیب $u \prec_{lex} \{x_1,\ldots,x_n\} \setminus u$ تعریف می‌کنیم و با استفاده

از این ترتیب، پایهٔ گربنر G_u را برای ایدآل I به‌دست می‌آوریم. در این صورت اندازهٔ بزرگترین زیرمجموعهٔ $u \subseteq \{x_1, \ldots, x_n\}$ که $G_u \cap K[u] = \{0\}$ بعد ایدآل I است. این تعریف از بعد ایدآل با تعریفی که قبلاً از آن ارائه کردیم، معادل است (برای توضیحات بیشتر به مرجع [۴] قضیه ۱-۵-۳ مراجعه کنید).

در پایان این بخش، برخی از کاربردهای نرمال‌سازی نوتر را به‌طور مختصر بیان می‌کنیم. ابتدا به کاربرد آن در محاسبهٔ رادیکال یک ایدآل اشاره می‌کنیم (برای توضیحات بیشتر به [۶] مراجعه کنید). فرض کنید $I = \langle G \rangle \subseteq K[x_1, \ldots, x_n]$ یک ایدآل از بعد d و G پایهٔ گربنر ایدآل I باشد. فرض کنید I در موقعیت نوتر باشد. ضرایب چندجمله‌ای‌های G را در $K[x_1, \ldots, x_d]$ در نظر می‌گیریم. $\mu = LCM(LC(g) \mid g \in G)$ را کوچکترین مضرب مشترک ضرایب پیشروی چندجمله‌ای‌های G و $I : \mu^*$ را

$$\{f \in K[x_1, \ldots, x_n] \mid \exists N \in \mathbb{N} \ : \ \mu^N f \in I\},$$

تعریف می‌کنیم. چندجمله‌ای‌های ناصفر $h_{d+i} \in K[x_1, \ldots, x_d, x_{d+i}]$ که $1 \leq i \leq n-d$ را در I به‌صورت

$$h_{d+i} = cont(h_{d+i}).pp(h_{d+i}),$$

در نظر می‌گیریم که در آن $cont(h_{d+i}) \in K[x_1, \ldots, x_d]$ محتوای h_{d+i} (بزرگترین مقسوم علیه مشترک ضرایب h_{d+i}) و $pp(h_{d+i})$ چندجمله‌ای اولیهٔ h_{d+i} (چندجمله‌ای که بزرگترین مقسوم علیه مشترک ضرایب آن یک است) باشد. فرض کنید $L_{d+i} = sqfr(pp(h_{d+i}))$ چندجمله‌ای خالی از مربع $pp(h_{d+i})$ باشد. قرار می‌دهیم $P_{d+i} = cont(h_{d+i})L_{d+i}$. اگر $P = \{P_{d+1}, \ldots, P_n\}$ آن‌گاه

$$\sqrt{I} = \sqrt{I + \langle P, \mu \rangle} \cap (I + \langle P \rangle) : \mu^*,$$

رادیکال ایدآل I خواهد بود. با توجه به تعریف μ و P، ایدآل $I + \langle P, \mu \rangle$ یک ایدآل از بعد صفر خواهد بود و در این صورت طبق لم سیدنبرگ[1] [۴] اگر برای هر $1 \leq i \leq n$ یک چندجمله‌ای خالی از مربع f_i که $(I + \langle P, \mu \rangle) \cap K[x_i] = \langle f_i \rangle$ را به ایدآل اضافه کنیم، آن‌گاه رادیکال ایدآل به‌دست می‌آید. برای مثال، اگر ایدآل $I = \langle x^4 y - 2x^2 y + y, y^2 - y \rangle \subseteq K[x, y]$ را در نظر بگیریم با توجه به این که I از بعد یک است $I = \langle x^4 y - 2x^2 y + y, y^2 - y \rangle \cap K[x] = \{0\}$

[1] Seidenberg

و $y^۲ - y$ یک چندجمله‌ای تکین برحسب y است، طبق تعریف،I در موقعیت نوتر است. اگر $\mu = x^۴ - ۲x^۲ + ۱$ را در نظر بگیریم، آن‌گاه

$$I + \langle P, \mu \rangle = \langle x^۴y - ۲x^۲y + y, y^۲ - y, x^۴ - ۲x^۲ + ۱\rangle,$$

یک ایدآل از بعد صفر است و در نتیجه

$$\sqrt{I + \langle P, \mu\rangle} = \langle x^۴y - ۲x^۲y + y, y^۲ - y, x^۴ - ۲x^۲ + ۱, x^۲ - ۱, y^۲ - ۱\rangle.$$

در این صورت خواهیم داشت

$$\begin{aligned}\sqrt{I} &= \sqrt{I + \langle P, \mu\rangle} \cap (I + \langle P\rangle) : \mu^* \\ &= \langle x^۴y - ۲x^۲y + y, y^۲ - y, x^۴ - ۲x^۲ + ۱, x^۲ - ۱, y^۲ - ۱\rangle \cap \langle y\rangle \\ &= \langle y^۲ - y, xy^۲ - y\rangle.\end{aligned}$$

کاربرد دیگر نرمال‌سازی نوتر در تصویر چندگونای مستوی است. می‌دانیم که تصویر یک چندگونای مستوی تحت نگاشت تصویر الزاماً یک مجموعهٔ بستهٔ جبری نیست. اما اگر ایدآل در موقعیت نوتر باشد، تصویر آن یک مجموعهٔ بستهٔ ضربی خواهد بود. برای مثال، ایدآل

$$I = \langle xy - ۱\rangle \subseteq \mathbb{R}[x, y],$$

و نگاشت تصویر $\pi_۱ : \mathbb{R}^۲ \longrightarrow \mathbb{R}$ با ضابطهٔ $(x, y) \mapsto y$ را در نظر می‌گیریم. مشاهده می‌کنیم که تصویر مجموعهٔ جبری $V(I)$ تحت $\pi_۱$ مجموعهٔ $\pi_۱(V(I)) = \mathbb{R} \setminus \{۰\}$ است که یک مجموعهٔ جبری نیست. اما با جایگذاری $x + \tilde{y}$ به‌جای y در $xy - ۱$ ایدآل

$$\langle x^۲ + x\tilde{y} - ۱\rangle \subseteq \mathbb{R}[x, \tilde{y}],$$

را خواهیم داشت و در این صورت $\pi_۱(V(x^۲ + x\tilde{y} - ۱)) = \mathbb{R}$ یک مجموعهٔ جبری است.

۳. الگوریتم نرمال‌سازی نوتر

در مقدمه بیان کردیم که الگوریتم‌هایی که تاکنون برای محاسبهٔ نرمال‌سازی نوتر ارائه شده‌اند، با استفاده از روش‌های تصادفی ماتریس تغییر مختصات را پیدا می‌کنند که این مستلزم محاسبات طولانی و پیچیده است که قطعاً به زمان بیشتری نیز نیاز دارد. اما الگوریتمی که در این بخش ارائه

می‌شود با استفاده از یک روش قطعی، تغییر مختصاتی که یک ایدآل نیاز دارد که با آن در موقعیت نوتر قرار بگیرد یا به عبارت دیگر، یک ماتریس تنک‌تر (نسبت به روشهای دیگر) برای ماتریس تغییر مختصات ایدآل را محاسبه می‌کند.

الگوریتم ۱ نرمال سازی نوتر

ورودی: ایدآل $I = \langle F \rangle \subseteq R = K[x_1, \ldots, x_n]$ و متغیرهای $V = [x_1, \ldots, x_n]$.

خروجی: یک مجموعهٔ ψ از نگاشت‌های خطی طوری که $\langle \psi(I) \rangle$ در موقعیت نوتر باشد.

۱: ψ را مجموعهٔ تهی در نظر می‌گیریم.

۲: چندجمله‌ای $f \in F$ را از درجهٔ m به صورت $f = f_m + \cdots + f_0$ در نظر می گیریم که f_i از درجه i است.

۳: $b_1, \ldots, b_{n-1}$ را طوری انتخاب می‌کنیم که $f_m(b_1, \ldots, b_{n-1}, 1) \neq 0$.

۴: قرار دهید $\begin{pmatrix} y_1 \\ \vdots \\ y_{n-1} \\ x_n \end{pmatrix} \begin{pmatrix} 1 & \cdots & -b_1 \\ \vdots & \cdots & \vdots \\ \vdots & 1 & -b_{n-1} \\ 0 & \cdots & 1 \end{pmatrix}^{-1} = M$.

۵: برای هر $i = 1, \ldots, n-1$، x_i را با $M[i]$ در F جایگذاری می‌کنیم و آن را $\tilde{F}$ می‌نامیم.

۶: با استفاده از پایهٔ گربنر $\langle \tilde{F} \rangle \cap K[y_1, \ldots, y_{n-1}]$ را محاسبه می‌کنیم و آن را F' می‌نامیم.

۷: ψ را اجتماع ψ و نگاشت خطی $x_i \to x_i - b_i x_n$ برای $i = 1, \ldots, n-1$ در نظر می‌گیریم.

۸: اگر $F' \neq \{0\}$ آنگاه قرار می‌دهیم ψ برابر با اجتماع ψ و خروجی نرمال سازی نوتر روی $\langle F' \rangle$ و $[y_1, \ldots, y_{n-1}]$ باشد.

۹: ψ را برمی‌گردانیم.

روند الگوریتم ۱ به این صورت است که ابتدا $n-1$ متغیر y_i را برحسب متغیر x_n به‌صورت $y_1 = x_1 - b_1 \cdot x_n, \ldots, y_{n-1} = x_{n-1} - b_{n-1} \cdot x_n$ می‌سازیم و با جایگذاری در یک چندجمله‌ای $y_n = c x_n^m + \sum_{i=0}^{m-1} \tilde{f}_i x_n^i$ مقادیر مناسب برای b_iها را به‌دست می‌آوریم. سپس به‌کمک پایهٔ گربنر ایدآل $I' := I \cap K[y_1, \ldots, y_{n-1}]$ را محاسبه می‌کنیم و در هر مرحله یکی از تعداد متغیرها کم می‌کنیم. این روند را حداکثر $n-d$ بار که d بعد ایدآل است تکرار می‌کنیم، زیرا

در این صورت با توجه به این که بعد ایدآل d است، خواهیم داشت

$$I' = I \cap K[y_1, \ldots, y_d] = \{0\}.$$

لازم به ذکر است که بعد ایدآل با تغییر متغیر خطی تغییر نمی‌کند. از طرفی، $n-d$ چندجمله‌ای تکین روی $K[y_1, \ldots, y_d]$ در ایدآل I می‌سازیم. بنابراین با توجه به تعریف نرمال‌سازی نوتر، ایدآل مورد نظر در موقعیت نوتر قرار می‌گیرد.

اثبات درستی الگوریتم ۱ از لم نرمال‌سازی نوتر نتیجه می شود. برای اثبات پایان‌پذیری الگوریتم از نتایجی استفاده می‌کنیم که در ادامه می‌آیند.

۱) فرض کنید $R = K[x_1, \ldots, x_n]$ و $f(x_1, \ldots, x_n) \in R$ به‌صورت

$$f = f_0 + \cdots + f_m,$$

باشد که در آن f_iها چندجمله‌ای‌های همگن از درجهٔ i باشند. متغیرهای جدید $\tilde{x}_1, \ldots, \tilde{x}_{n-1}$ را در نظر می‌گیریم که $\tilde{x}_i = x_i - b_i x_n$ و $b_i \in K$. در این صورت چندجمله‌ای‌های $\tilde{f}_0, \ldots, \tilde{f}_{m-1}$ در $K[\tilde{x}_1, \ldots, \tilde{x}_{n-1}]$ موجودند که

$$f(x_1, \ldots, x_n) = f_m(b_1, \ldots, b_{n-1}, 1) x_n^m + \sum_{i=0}^{m-1} \tilde{f}_i(\tilde{x}_1, \ldots, \tilde{x}_{n-1}) x_n^i.$$

۲) فرض کنید K یک میدان نامتناهی باشد و $f \in K[x_1, \ldots, x_n]$. در این صورت $f = 0$ اگر و تنها اگر برای هر $(b_1, \ldots, b_n) \in K^n$، $f(b_1, \ldots, b_n) = 0$.

۳) اگر K یک میدان نامتناهی و $0 \neq f \in K[x_1, \ldots, x_n]$ یک چندجمله‌ای همگن از درجهٔ m باشد طوری که به‌ازای هر $(b_1, \ldots, b_{n-1}, 1) \in K^n$، $f(b_1, \ldots, b_{n-1}, 1) = 0$ آن‌گاه f یک چندجمله‌ای صفر است.

برای اثبات ادعاهای ۱ و ۳ به [۸] و ادعای ۲ به [۴] صفحهٔ ۳ مراجعه کنید.

برای درک بهتر روند الگوریتم، مثال زیر را بیان می‌کنیم.

مثال ۱.۳. ایدآل

$$I = \langle y^2 z - wxy^2, xyz - wz^2, y^2 z - wx^2 yz \rangle \subseteq R = \mathbb{R}[w, x, y, z],$$

و ترتیب $z \succ_{lex} \cdots \succ_{lex} w$ را در نظر می‌گیریم. می‌خواهیم چندجمله‌ای تکینی بر حسب کوچکترین متغیر به‌دست آوریم. برای این منظور، ابتدا متغیرهای

$$w = y_1 + b_1 z, x = y_2 + b_2 z, y = y_3 + b_3 z,$$

را در یک چندجمله‌ای مانند $f = xyz - wz^2$ جایگزین می‌کنیم. با جایگذاری این تغییر متغیرها در f چندجمله‌ای زیر را خواهیم داشت:

$$(b_2 b_3 - b_1)z^3 + (y_1 b_3 + b_2 y_2 - y_1)z^2 + y_2 y_3 z.$$

حال b_1, b_2, b_3 را طوری انتخاب می‌کنیم که ضریب z^3 صفر نشود. قرار می‌دهیم $b_1 = 1$ و $b_2 = b_3 = 0$. اکنون با استفاده از روش حذفی، پایهٔ گربنر ایدآل

$$I' = I \cap \mathbb{R}[y_1, y_2, y_3] =$$

$$\langle y_2^5 y_3^2 y_1 - y_3^3 y_2 y_1, y_2^4 y_3^3 y_1 - y_2^3 y_3^3 y_1 + y_1^2 y_3^3 y_2, y_2^2 y_3^2 y_1^2 + y_3^3 y_2 y_1 - y_2^4 y_3^2 y_1 \rangle,$$

را محاسبه می‌کنیم. چون اشتراک ناتهی شد، پس طبق الگوریتم در مرحلهٔ بعد باید چندجمله‌ای تکینی برحسب y_3 بسازیم. در این مرحله نیز متغیرهای $y_1 = z_1 + b_1 y_3$ و $y_2 = z_2 + b_2 y_3$ را در $g = y_2^2 y_3^2 y_1^2 + y_3^3 y_2 y_1 - y_2^4 y_3^2 y_1$ جایگزین می‌کنیم. در این صورت g به چندجمله‌ای زیر تبدیل می‌شود:

$$\begin{aligned}
&- b_2^4 b_1 y_3^7 + (b_2^2 b_1^2 - 4 z_2 b_2^3 b_1 - b_2^4 z_1) y_3^6 \\
&+ (2 z_2 b_2 b_1^2 + 2 b_2^2 z_1 b_1 + b_2 b_1 - 6 z_2^2 b_2^2 b_1 - 4 z_2 b_2^3 z_1) y_3^5 \\
&+ (z_2^2 b_1^2 + 4 z_2 b_2 z_1 b_1 + b_2^2 z_1^2 + z_2 b_1 + b_2 z_1 - 4 z_2^3 b_2 b_1 - 6 z_2^2 b_2^2 z_1) y_3^4 \\
&+ (2 z_2^2 z_1 b_1 + 2 z_2 b_2 z_1^2 + z_2 z_1 - z_2^4 b_1 - 4 z_2^3 b_2 z_1) y_3^3 \\
&+ (z_2^2 z_1^2 - z_2^4 z_1) y_3^2.
\end{aligned}$$

در این مرحله نیز مانند مرحلهٔ قبل برای این که ضریب y_3 صفر نشود قرار می‌دهیم $b_1 = b_2 = 1$ و به‌کمک پایهٔ گربنر داریم $I'' = I' \cap \mathbb{R}[z_1, z_2] = \{0\}$. اگر تعریف کنیم

$$B = \mathbb{R}[w - y - z, x - y, f(w - y - z, x - y, y, z), g(w - y - z, x - y, y, z)],$$

آن‌گاه با توجه به این که $y_۳ = y$ و $R = B[y,z]$، B یک R -مدول متناهی مولد است. بنابراین

$$R/I = B[y,z]/\langle -y^۴ + (w-z+x)y^۳ + (z-(w-z)x)y^۲, \\ z^۳ + (-w+y)z^۲ + (x-y)yz, y^۲z - (w-y-z)(x-y)^۲yz\rangle$$

روی $B/(I\cap B) = \mathbb{R}[w-y-z, x-y]$ صحیح است. در نتیجه طبق تعریف $\mathbb{R}[w-y-z, x-y]$ یک نرمال‌سازی نوتر R/I است.

مثال ۲.۳. در سال ۲۰۰۹، روبرتز [۷] الگوریتمی مؤثر با استفاده از پایه‌های تودرتو برای محاسبهٔ نرمال‌سازی نوتر ارائه کرد. به‌عنوان مثال، ایدآل I را به‌صورت

$$\langle yz - yc - xb + ab, zc - zx - yb + ab, yc - zb + ab, xy - zx - cb + ab\rangle \\ \subseteq \mathbb{Q}[a,b,c,x,y,z],$$

در نظر می‌گیریم. الگوریتم روبرتز تغییر متغیرهای

$$a \mapsto a,\ b \mapsto b-a,\ c \mapsto c-b,\ x \mapsto x-c,\ y \mapsto y-a,\ z \mapsto z+c,$$

را برای قرار دادن I در موقعیت نوتر محاسبه می‌کند، در حالی که الگوریتم ارائه شده در این مقاله، تغییر متغیرهای

$$a \mapsto a,\ b \mapsto b,\ c \mapsto c,\ x \mapsto x-z-۲y,\ y \mapsto y,\ z \mapsto z,$$

را به‌دست می‌دهد که به‌روشنی تنک‌تر از تغییر متغیرهای ارائه شده توسط الگوریتم روبرتز است.

مثال ۳.۳. ایدآل

$$\langle x_۱x_۳ + x_۳u_۱ - x_۳u_۲ - u_۱u_۳, x_۱u_۳ - u_۱u_۳ - u_۲u_۳, \\ x_۲u_۳ + x_۳u_۱ - x_۳u_۲ - u_۱u_۳, x_۳u_۱ - x_۳u_۲ - u_۱u_۳ + u_۲u_۳, \\ x_۳u_۱u_۳ - u_۱u_۳^۲\rangle \subseteq K[u_۱,u_۲,u_۳,x_۱,x_۲,x_۳],$$

را با ترتیب $u_۱ \succ_{drl} u_۲ \succ_{drl} u_۳ \succ_{drl} x_۱ \succ_{drl} x_۲ \succ_{drl} x_۳$ در نظر بگیرید. با استفاده از الگوریتم روبرتز برای قرار دادن ایدآل بالا در موقعیت نوتر به تغییر متغیرهای زیر نیاز داریم

$$u_۱ \mapsto u_۱,\ u_۲ \mapsto u_۲,\ u_۳ \mapsto u_۳ - u_۱,\ x_۱ \mapsto x_۱ + u_۲,\ x_۲ \mapsto x_۲ - u_۱, x_۳ \mapsto x_۳ - u_۲,$$

در حالی که با الگوریتم بهبود یافتهٔ اخیر تنها با تغییر متغیرهای

$$u_۱ \mapsto u_۱,\ u_۲ \mapsto u_۲,\ u_۳ \mapsto u_۳ - u_۱,\ x_۱ \mapsto x_۱,\ x_۲ \mapsto x_۲, x_۳ \mapsto x_۳ - u_۲.$$

ایدآل در موقعیت نوتر قرار می‌گیرد که به‌روشنی تنک‌تر است.

مراجع

[۱] رشید زارع نهندی، *بوخبرگر و پایه‌های گربنر*، فرهنگ و اندیشهٔ ریاضی، شماره ۴۴، (۱۳۸۹).

[2] B. Buchberger, *An algorithm for finding the bases elements of the residue class ring. modulo a zero dimensional polynomial ideal (German),* PhD thesis, Universität Innsbruck, 1965.

[3] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms,* Springer-Verlag, New York, third edition, 2007.

[4] G.M. Greuel, and G. Pfister, *A SINGULAR introduction to commutative algebra,* Springer-Verlag, Berlin-Heidelberg, 2007.

[5] A. Hashemi, *Efficient algorithms for computing Noether normalization,* Lecture Notes in Computer Science, **5081**, (2008) 97–107.

[6] T. Krick, and A. Logar, *An algorithm for the computation of the radical of an ideal in the ring of polynomials,* AAECC9, Springer LNCS 539, (1991) 195–205.

[7] D. Robertz, *Noether normalization guided by monomial cone decompositions,* Journal of Symbolic Computation, **44** (2009) 1359–1373.

[8] R.Y. Sharp, *Steps in Commutative Algebra,* Cambridge University Press, Cambridge, 2000.

امیر هاشمی: دانشکده علوم ریاضی، دانشگاه صنعتی اصفهان، کد پستی ۸۴۱۵۶- ۸۳۱۱۱

رایانامه: Amir.Hashemi@cc.iut.ac.ir

نازنین رحمانی : دانشکده علوم ریاضی، دانشگاه صنعتی اصفهان، کد پستی ۸۴۱۵۶- ۸۳۱۱۱

رایانامه: n.rahmani@math.iut.ac.ir