حل دستگاه‌های معادلات هم‌نهشتی خطی روی برخی حلقه‌ها به‌کمک تجزیه‌هایی از مدول‌ها

محمود بهبودی[۱]، شادی عسگری[۲]، علی مرادزاده دهکردی[۳]، امیر هاشمی[۴]*
۱، ۴. دانشگاه صنعتی اصفهان، دانشکده علوم ریاضی، اصفهان
۲. پژوهشگاه دانش‌های بنیادی، پژوهشکدهٔ ریاضیات، تهران
۳. مرکز آموزش عالی شهرضا، دانشکدهٔ علوم پایه، شهرضا

دریافت ۹۶/۰۲/۰۲ پذیرش ۹۶/۱۰/۱۷

چکیده

هدف اصلی این مقاله حل دستگاه‌های معادلات هم‌نهشتی خطی روی CF- حلقه‌های جابه‌جایی است. فرض کنید R یک CF-حلقه جابه‌جایی (یعنی، هر مجموع مستقیم متناهی تولید از R-مدول‌های دوری دارای یک صورت متعارف[1] باشد) و $I_1,\ldots,I_n$ ایدآل‌هایی از حلقه R باشند. ما دستگاه معادلات هم‌نهشتی خطی

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n\equiv b_1 & (\bmod\ I_1)\\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n\equiv b_2 & (\bmod\ I_2)\\ \vdots\ \ \vdots\ \ \ \vdots\ \ \ \vdots\ \ \ \vdots\ \ \ \vdots & \ \ \vdots\\ a_{n1}x_1+a_{n2}x_2+\cdots+a_{nn}x_n\equiv b_n & (\bmod\ I_n)\end{cases}$$

را که $a_{ij},b_i\in R$ و $I_j\subseteq\bigcap_{i\neq j}(I_i:a_{ij})$، برای هر $1\le i,j\le n$، بررسی می‌کنیم. در این راستا، تکنیک‌هایی از نظریهٔ ماتریس‌های هم‌نهشتی را معرفی می‌کنیم و به‌عنوان کاربردی از این تکنیک‌ها به حل دستگاه بالا می‌پردازیم. در پایان کاربردی از تکنیک‌های جبر محاسباتی (پایه‌های گربنر[2]) در این زمینه، در حالت خاصی که $R=\mathbb{Z}$، را بررسی می‌کنیم.

واژه‌های کلیدی: دستگاه‌های هم‌نهشتی خطی، عملیات حذفی گاوسی، پایه‌های گربنر.

رده‌بندی ریاضی (۲۰۱۰): ۱۳C۰۵ و ۱۳P۱۰

۱. مقدمه

سرمنشأ نظریهٔ حل دستگاه‌های معادلات هم‌نهشتی خطی را می‌توان در کارهای ریاضی‌دان چینی سون‌زی[3] مشاهده کرد. او در کتابی با عنوان "حساب ردهٔیک[4]" که در قرن اول میلادی به چاپ رساند، قضیهٔ باقی‌مانده چینی و استفاده از آن برای حل دستگاه‌های هم‌نهشتی خطی را مطرح کرد. توجه کنید که حل چنین دستگاه‌هایی دارای کاربردهای فراوانی است که از آن جمله می‌توان به پردازش سیگنال‌ها، رمزنگاری و غیره اشاره کرد. در این مقاله، به بررسی یک شکل کلی‌تر از دستگاه‌های هم‌نهشتی خطی روی CF- حلقه‌ها می‌پردازیم که روابط هم‌نهشتی روی برخی

*نویسنده مسئول amir.hashemi@ipm.ir

1. Canonical form
2. Gröbner bases
3. Sun Zi
4. Arithmetical classic

از ایدآل‌های حلقه تعریف شده است. برای این منظور، نظریهٔ جبرخطی هم‌نهشتی را تعمیم داده و از آن برای بررسی شکل کلی‌تر دستگاه‌های هم‌نهشتی خطی استفاده می‌کنیم. در این راستا برخی از نتایج جبری به‌دست آمده زمینهٔ CF- حلقه‌ها که روی‌کرد این مقاله بر اساس آن‌ها بنا شده است را مرور می‌کنیم.

در این پژوهش همهٔ حلقه‌ها جابه‌جایی و یک‌دار و تمامی مدول‌ها یکانی هستند. طبق [۱۲]، یک CF- حلقه R، حلقه‌ای است که هر مجموع مستقیم متناهی تولید از R- مدول‌های دوری دارای یک شکل متعارف باشد (یک شکل متعارف برای R- مدول M، یک تجزیه به‌صورت $M \cong R/I_1 \oplus \cdots \oplus R/I_n$ است که $I_1 \subseteq \cdots \subseteq I_n \neq R$). هر CF- حلقه برابر با یک حاصل ضرب مستقیم از CF- حلقه‌های تجزیه‌ناپذیر[5] است. هم‌چنین CF- حلقه‌های تجزیه ناپذیر دقیقاً حلقه‌های R هستند که در این چهار خاصیت صدق کنند: ۱. R یک حلقه حسابی[6] باشد، ۲. R دارای یک ایدآل اول مینیمال منحصر به‌فرد P باشد، ۳. هر ایدآل مشمول در P با هر ایدآل دیگر R قابل مقایسه[7] باشد و ۴. R/P یک دامنه h- موضعی[8] باشد (برای جزئیات بیش‌تر به قضیهٔ ۱ [۱۲] شود).

یک حلقه R را FGC- حلقه می‌نامند اگر تمامی R- مدول‌های متناهی تولید، به‌صورت جمع مستقیمی از مدول‌های دوری باشند [۳]، [۱۲]. این حلقه‌ها دقیقاً حاصل ضرب مستقیمی از تعداد متناهی از حلقه‌های ارزیاب ماکسیمال[9]، دامنه‌های بزوی تقریباً ماکسیمال[10] و حلقه‌های تورچ[11] که ساختار چنین حلقه‌هایی را به‌صراحت مشخص می‌کند. این حقیقت در سال ۱۹۷۶، با استفاده از مفاهیم توپولوژیکی و جبر جابه‌جایی به اثبات رسیده است. اثبات این قضیهٔ ساختاری به نتایج به‌دست آمده در ۳۰ سال گذشته وابسته بوده است، که اکثر مراحل اثبات در مقاله‌ای تفسیری از ویگاند[12] [۱۳] گردآوری شده است.

کاپلانسکی[13] به بررسی تجزیه‌های متعارف پرداخت و نشان داد که تجزیه‌های متعارف در صورت وجود منحصربه‌فرد هستند [۱۰]. بنابر قضیهٔ ۹۵ از [۳]، هر مدول متناهی تولید M روی یک FGC-حلقه R، دارای تجزیه متعارف است. بنابراین هر FGC-حلقه یک CF-حلقه است. هم‌چنین، قضیهٔ اساسی برای گروه‌های آبلی بیان می‌کند که هر دامنهٔ ایدآل اصلی[14] یک FGC- حلقه است. توجه کنید که قضیهٔ اساسی برای گروه‌های آبلی از منظر تکنیک‌های جبرخطی بیان می‌کند که یک مدول متناهی تولید A روی یک دامنهٔ ایدآل اصلی دارای تجزیهٔ $A = R/Rd_1 \oplus \ldots \oplus R/Rd_n$ است که d_iها عناصر غیریکه از حلقهٔ R هستند و $d_1 | d_2$, $d_2 | d_3$,...,$d_{n-1} | d_n$.
در حالت کلی در نظریهٔ حلقه‌ها این تجزیه را تجزیهٔ متعارف می‌نامند.

فرض کنید R یک CF- حلقه باشد. برای یک ایدآل I از حلقهٔ R و $a \in R$ داریم:

$$(I : a) = \{r \in R : ra \in I\}.$$

فرض کنید $I_1, \ldots, I_n$ یک دنباله از ایدآل‌های حلقهٔ R باشند. ما دستگاه معادلات هم‌نهشتی خطی

5. Indecomposable
6. Arithmetical
7. Comparable
8. h -local domain
9. Maximal valuation
10. Almost maximal Bezout domains
11. Torch
12. Wiegand
13. Kaplansky
14. Principal ideal domain

$$(*)\quad \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 & (\mathrm{mod}\ I_1) \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 & (\mathrm{mod}\ I_2) \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots & \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \equiv b_n & (\mathrm{mod}\ I_n), \end{cases}$$

را که، برای هر $1 \le i, j \le n$، $a_{ij}, b_i \in R$ بررسی می‌کنیم.

برخی از تکنیک‌های ماتریس‌های معمولی را به‌منظور حل دستگاه‌های معادلات هم‌نهشتی خطی تعمیم می‌دهیم. این تعمیم‌ها در حالتی برقرار است که برای هر $1 \le i, j \le n$، داشته باشیم $I_j \subseteq \bigcap_{i \ne j}(I_i : a_{ij})$. به‌علاوه، در این مقاله، تکنیک پایه‌های گربنر را به‌منظور حل چنین دستگاه‌هایی در حالتی که $R = Z$ به‌کار می‌بریم. پایه‌های گربنر یک مفهوم الگوریتمی مهم در هندسهٔ جبری محاسباتی محسوب می‌شود. این مفهوم در رسالهٔ دکتری بوخبرگر[15] [۴] در سال ۱۹۶۵ معرفی شد و او در این رساله یک الگوریتم برای محاسبهٔ آن نیز طراحی کرد. روش پایه‌های گربنر ابزاری عملی برای حل ردهٔ وسیعی از مسائل در نظریهٔ ایدآل چندجمله‌ای‌ها (مانند عضویت ایدآل، برابری ایدآل‌ها، حل دستگاه‌های چندجمله‌ای و غیره) است. هم‌چنین در بسیاری از زمینه‌های تحقیقاتی علوم و مهندسی (مانند برنامه‌ریزی خطی، گرافیک کامپیوتری، پردازش سیگنال‌های دیجیتال، رباتیک و غیره) کاربرد فراوان دارد. خواننده را برای بررسی جزئیات بیش‌تر در مورد نظریهٔ پایه‌های گربنر و کاربردهایش به [۱] ارجاع می‌دهیم. لازم به ذکر است که برای اولین بار ارتباط بین پایه‌های گربنر و حل دستگاه‌های خطی روی اعداد طبیعی را کونتی[16] و تراورسو[17] مطرح کردند [۵]. برای کسب جزئیات بیش‌تر در مورد این موضوع خواننده را به صفحهٔ ۱۰۷ از مرجع [۱] ارجاع می‌دهیم. با این حال، در این مراجع، نویسندگان تنها دستگاه‌های خطی را بررسی کرده‌اند و به مطالعه و بررسی دستگاه‌های هم‌نهشتی نپرداخته‌اند.

ساختار این مقاله بدین‌شرح است: در بخش ۱، به معرفی و بررسی برخی از تکنیک‌های نظریه ماتریس‌های هم‌نهشتی می‌پردازیم. به‌منظور بهره برداری از این تکنیک‌ها روی ماتریس هم‌نهشتی $A = \left(\left(a_{ij}\right)\right)$ (تعریف ۲ .۱)، شبیه جبرخطی معمولی، نشان می‌دهیم که می‌توان یک R- درون‌ریختی متعارف

$$\varphi : R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n \to R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$$

وابسته به A تعریف کرد اگر و تنها اگر برای هر $1 \le i, j \le n$، داشته باشیم $I_j \subseteq \bigcap_{i \ne j}(I_i : a_{ij})$. در بخش ۲، به بررسی وارون پذیری ماتریس هم‌نهشتی A و کاربردهایش به‌منظور حل دستگاه بحث شده در بالا می‌پردازیم. در بخش ۳، یک روش مبتنی بر تکنیک‌های جبرخطی پیمانه‌ای به‌منظور حل یک دستگاه خطی از معادلات هم‌نهشتی مطرح می‌کنیم. برای این منظور، روش حذفی گاوس پیمانه‌ای برای انجام حذف گاوسی روی ماتریس‌های با درایه‌های صحیح به پیمانهٔ یک عدد صحیح داده شده را ارائه می‌دهیم. برخی از مثال‌های مرتبط با بخش‌های قبلی در بخش ۴ آورده شده است. هم‌چنین در فصل ۵، به بررسی کاربردهایی از تکنیک‌های جبر محاسباتی در حل دستگاه‌های معادلات هم‌نهشتی خطی، در حالتی که $R = Z$ می‌پردازیم.

۲. مبانی جبرخطی هم‌نهشتی

فرض کنید R یک حلقه و $\beta = (I_1, \ldots, I_n)$ یک دنباله از ایدآل‌های R باشد. در این بخش ما به بیان تکنیک‌هایی برای حل دستگاه‌های هم‌نهشتی خطی

---

15. Buchberger
16. Conti
17. Traverso

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{I_1} \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 \pmod{I_2} \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \equiv b_n \pmod{I_n}, \end{cases}$$

می‌پردازیم که در آن، برای هر $1 \le i, j \le n$، داریم $I_j \subseteq \bigcap_{i \neq j}(I_i : a_{ij})$.

به‌منظور ارائه تکنیک‌های جبرخطی مد نظر ما، ابتدا چند تعریف و نتیجه برای نمایش ماتریسی دستگاه بالا بیان می‌کنیم. مجموعه ماتریس‌های $n \times m$ روی حلقه R را با نماد $M_{n\times m}(R)$ نمایش می‌دهیم.

تعریف ۱.۲ فرض کنیم R یک حلقه باشد. رابطهٔ $\approx$ روی $M_{n\times m}(R)$ را بدین‌صورت تعریف می‌کنیم. برای $A = (a_{ij})$ و $A' = (a'_{ij})$ در $M_{n\times m}(R)$،

$$A \approx A' \Leftrightarrow a_{ij} - a'_{ij} \in I_i$$

واضح است که رابطهٔ $\approx$ یک رابطهٔ هم‌ارزی است و یک ردهٔ هم‌ارزی از $A = (a_{ij})_{n\times m}$ را با نماد $\left(\left(a_{ij}\right)\right)$ نمایش می‌دهیم.

حال قرار می‌دهیم $R^{\beta} = \left\{\left(\left(a_i\right)\right)_{n\times 1} \mid 1 \le i \le n, a_i \in R\right\}$. واضح است که R^{β} یک R- مدول با جمع معمولی و ضرب

$$\cdot : R \times R^{\beta} \to R^{\beta}$$
$$\left(r, \left(\left(\alpha_i\right)\right)_{n\times 1}\right) \mapsto \left(\left(r\alpha_i\right)\right)_{n\times 1}$$

است. هم‌چنین، نگاشت $\psi : \oplus_{i=1}^{n} R/I_i \to R^{\beta}$ با ضابطهٔ

$$\psi\left(r_1 + I_1, r_2 + I_2, \ldots, r_n + I_n\right) = \left(\left(r_i\right)\right)_{n\times 1}$$

یک یک‌ریختی R- مدولی است. برای راحتی به‌ازای هر $1 \le i \le n$ داریم:

$$e_i = (0, \ldots, 0, 1 + I_i, 0, \ldots, 0).$$

فرض کنیم $\varphi : \oplus_{i=1}^{n} R/I_i \to \oplus_{i=1}^{n} R/I_i$ یک R- درون‌ریختی باشد. بنابراین عناصر a_{ij} از حلقه R موجود است به طوری‌که $\varphi(e_j) = \Sigma_{i=1}^{n} a_{ij}e_i$. ما $[\varphi]_{\beta}$ را با ماتریس $\left(\left(a_{ij}\right)\right)_{n\times n}$ نمایش می‌دهیم. برای هر $x \in I_j$، داریم $\Sigma_{i=1}^{n} x a_{ij} e_i = 0$. بنابراین برای هر $1 \le i, j \le n$ ماتریس $[\varphi]_{\beta}$ در خاصیت $I_j \subseteq \bigcap_{i\neq j}(I_i : a_{ij})$ صدق می‌کند.

برعکس، فرض کنید $(a_{ij})_{n\times n}$ یک ماتریس در $M_{n\times n}(R)$ باشد. نگاشت $\theta : R^{\beta} \to R^{\beta}$ را با ضابطهٔ $\theta\left(\left(\left(r_i\right)\right)_{n\times 1}\right) = \left(\left(A\left(r_i\right)\right)\right)_{n\times 1}$ تعریف می‌کنیم. حال گزارهٔ زیر را داریم.

گزاره ۲.۲ *نگاشت θ خوش تعریف است اگر و تنها اگر $I_j \subseteq \bigcap_{i\neq j}(I_i : a_{ij})$ برای هر $1 \le i, j \le n$. در نتیجه، ماتریس $(a_{ij})_{n\times n}$ یک R- درون‌ریختی متعارف از $\oplus_{i=1}^{n} R/I_i$ القا می‌کند اگر و تنها اگر برای هر $1 \le i, j \le n$ داشته باشیم $I_j \subseteq \bigcap_{i\neq j}(I_i : a_{ij})$.*

اثبات. فرض کنید θ خوش تعریف باشد و $\alpha_j \in I_j$. اگر $(b_{k1})_{n\times 1} \approx (c_{k1})_{n\times 1}$، جایی‌که برای هر $k \neq i$، $b_{i1} = 1 = c_{i1}$، $c_{j1} = \alpha_j$، $b_{k1} = 0$ و برای هر $k \neq i, j$، $c_{k1} = 0$. بنابراین

$$(a_{ij})_{n\times n}(b_{k1})_{n\times 1} \approx (a_{ij})_{n\times n}(c_{k1})_{n\times 1}$$

و این ایجاب می‌کند که

$$\begin{pmatrix} a_{1i} \\ . \\ . \\ . \\ a_{ii} \\ . \\ . \\ . \\ a_{ni} \end{pmatrix} \approx \begin{pmatrix} a_{1j}\alpha_j + a_{1i} \\ . \\ . \\ . \\ a_{ij}\alpha_j + a_{ii} \\ . \\ . \\ . \\ a_{nj}\alpha_j + a_{ni} \end{pmatrix}.$$

حال با بررسی سطر i-ام، داریم $a_{ij}\alpha_j \in I_i$. بنابراین، برای هر $1 \le j \ne i \le n$، داریم $I_j \subseteq (I_i : a_{ij})$، از این‌رو، $I_j \subseteq \bigcap_{i \ne j}(I_i : a_{ij})$. اثبات برعکس ساده است.

لم ۲. ۳ *فرض کنیم* $A = (a_{ij})$ *و* $A' = (a'_{ij})$ *دو ماتریس در* $M_{n\times n}(R)$ *باشند به طوری‌که* $A \approx A'$. *اگر برای هر* i, j، $I_j \subseteq \bigcap_{i \ne j}(I_i : a_{ij})$، *آن‌گاه* $I_j \subseteq \bigcap_{i \ne j}(I_i : a'_{ij})$.

اثبات. بنابر فرض، برای هر $i \ne j$، داریم $a_{ij} - a'_{ij} \in I_i$ و $a_{ij} I_j \subseteq I_i$. هم‌چنین، این روابط نتیجه می‌دهد که $(a_{ij} - a'_{ij}) I_j \subseteq I_i$ که این ایجاب می‌کند $a'_{ij} I_j \subseteq I_i$ و لذا $I_j \subseteq \bigcap_{i \ne j}(I_i : a'_{ij})$.

نتیجه ۲. ۴ *فرض کنید* $A = (a_{ij})_{n\times n}$ *و* $B = (b_{ij})_{n\times n}$ *دو ماتریس در* $M_{n\times n}(R)$ *باشند به‌طوری‌که* $I_j \subseteq \bigcap_{i \ne j}(I_i : a_{ij})$. *اگر* $A \approx B$ *و* $X = (\alpha_{i1})_{n\times 1} \approx (\beta_{i1})_{n\times 1} = Y$، *آن‌گاه* $AX \approx BY$.

حال بر اساس بحث بالا، تعریف زیر را ارائه می‌دهیم.

تعریف ۲. ۵ مجموعۀ $M_n(R; I_1, I_2, \ldots, I_n)$ را مجموعه‌ای از ماتریس‌های هم‌نهشتی با درایه‌ها در R و به پیمانۀ $I_1, \ldots, I_n$ تعریف می‌کنیم. در واقع:

$$M_n(R; I_1, I_2, \ldots, I_n) := \left\{ \left((a_{ij}) \right) \middle| I_j \subseteq \bigcap_{i \ne j} (I_i : a_{ij}), 1 \le \mathrm{i},\ \mathrm{j} \le \mathrm{n} \right\}$$

گزارۀ ۲. ۶ نشان می‌دهد که $M_n(R; I_1, I_2, \ldots, I_n)$ با جمع و ضرب ماتریسی تشکیل حلقه می‌دهد.

گزاره ۲. ۶ *مجموعۀ* $M_n(R; I_1, I_2, \ldots, I_n)$ *با جمع و ضرب زیر تشکیل حلقه می‌دهد*

$$\left((a_{ij})\right) + \left((b_{ij})\right) = \left((a_{ij} + b_{ij})\right), \quad \left((a_{ij})\right)\left((b_{ij})\right) = \left((c_{ij})\right)$$

جایی‌که $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.

اثبات. ما فقط خوش تعریفی عملگر ضرب را نشان می‌دهیم و بررسی بقیه خواص به سادگی امکان‌پذیر است. برای این منظور، فرض کنید $\left((a_{ij})\right) \approx \left((a'_{ij})\right)$ و $\left((b_{ij})\right) \approx \left((b'_{ij})\right)$ جایی که

$$\left((a_{ij})\right), \left((b_{ij})\right), \left((a'_{ij})\right), \left((b'_{ij})\right) \in M_n(R; I_1, I_2, \ldots, I_n).$$

بنابراین کافی است نشان دهیم $\left((c_{ij})\right) \approx \left((c'_{ij})\right)$ جایی‌که $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$ و $c'_{ij} = \sum_{k=1}^{n} a'_{ik} b'_{kj}$. برای راحتی تنها $c_{11} - c'_{11} \in I_1$ را چک می‌کنیم و بقیه موارد مشابه با آن به‌دست می‌آید. داریم:

$$\begin{aligned}c_{11}-c'_{11} &= a_{11}b_{11}+a_{12}b_{21}+\cdots+a_{1n}b_{n1}-a'_{11}b'_{11}-a'_{12}b'_{21}-\cdots-a'_{1n}b'_{n1}\\ &= a_{11}b_{11}+a_{12}b_{21}+\cdots+a_{1n}b_{n1}-(b_{11}a'_{11}+b_{21}a'_{12}+\cdots+b_{n1}a'_{1n})\\ &\quad +(b_{11}a'_{11}+b_{21}a'_{12}+\cdots+b_{n1}a'_{1n})-a'_{11}b'_{11}-a'_{12}b'_{21}-\cdots-a'_{1n}b'_{n1}\\ &= b_{11}(a_{11}-a'_{11})+b_{21}(a_{12}-a'_{12})+\cdots+b_{n1}(a_{1n}-a'_{1n})\\ &\quad -a'_{11}(b_{11}-b'_{11})-a'_{12}(b_{21}-b'_{21})-\cdots-a'_{1n}(b_{n1}-b'_{n1}).\end{aligned}$$

از این‌که $\left(\left(a_{ij}\right)\right)\approx\left(\left(a'_{ij}\right)\right)$، نتیجه می‌گیریم که $a_{1k}-a'_{1k}\in I_1$ و بنابراین $b_{k1}(a_{1k}-a'_{1k})\in I_1$ برای هر $1\le k\le n$. هم‌چنین، از $\left(\left(b_{ij}\right)\right)\approx\left(\left(b'_{ij}\right)\right)$ نتیجه می‌گیریم که برای هر $1\le k\le n$ داریم $b_{k1}-b'_{k1}\in I_k$. اگر $k=1$، آن‌گاه $a'_{11}(b_{11}-b'_{11})\in I_1$. در غیر این‌صورت، $a'_{1k}(b_{k1}-b'_{k1})\in I_k$، زیرا $I_k\subseteq\bigcap_{k\neq1}(I_1:a'_{1k})$. بنابراین، $c_{11}-c'_{11}\in I_1$.

یادآوری می‌کنیم که، برای یک R- مدول M، مجموعهٔ تمام R- درون‌ریختی‌ها از M، $\mathrm{E}nd_R(M)$، تشکیل یک حلقه می‌دهد. در حالتی‌که $I_1=\cdots=I_n=0$، حلقهٔ $M_n(R;I_1,I_2,\ldots,I_n)$ با $M_{n\times n}(R)$ یک‌سان و با $\mathrm{E}nd_R(\oplus_{i=1}^nR)$ یک‌ریخت است. قضیهٔ ۲. ۷ این نتیجه را برای حالت غیربدیهی تعمیم می‌دهد.

قضیه ۲. ۷ *به‌عنوان هم‌ریختی حلقه‌ها داریم* $M_n(R;I_1,I_2,\ldots,I_n)\cong\mathrm{E}nd_R(\oplus_{i=1}^nR/I_i)$.

اثبات. فرض کنید $\varphi:\oplus_{i=1}^nR/I_i\to\oplus_{i=1}^nR/I_i$ یک R- درون‌ریختی باشد و نگاشت

$$\psi:\mathrm{E}nd_R(\oplus_{i=1}^nR/I_i)\to M_n(R;I_1,I_2,\ldots,I_n)$$

را با ضابطهٔ $\psi(\varphi)=[\varphi]_\beta$ تعریف می‌کنیم. ادعا می‌کنیم که نگاشت ψ یک یک‌ریختی حلقه‌ای است. ابتدا، نشان می‌دهیم که ψ، خوش تعریف است. فرض کنیم $\varphi\in\mathrm{E}nd_R(\oplus_{i=1}^nR/I_i)$. از این‌که $\{\mathbf{e}_1,\ldots,\mathbf{e}_n\}$ یک مجموعهٔ مولد برای $\oplus_{i=1}^nR/I_i$ است، آن‌گاه برای هر j، $\varphi(\mathbf{e}_j)=\Sigma_{i=1}^na_{ij}\mathbf{e}_i$ جایی‌که $a_{ij}\in R$. اگر برای هر j، $\varphi(\mathbf{e}_j)=\Sigma_{i=1}^na'_{ij}\mathbf{e}_i$ جایی‌که $a'_{ij}\in R$، آن‌گاه $\Sigma_{i=1}^n(a_{ij}-a'_{ij})\mathbf{e}_i=0\in\oplus_{i=1}^nR/I_i$. بنابراین، برای هر $1\le i,j\le n$، داریم $a_{ij}-a'_{ij}\in I_i$ ، از این‌رو، $(a_{ij})_{n\times n}\approx(a'_{ij})_{n\times n}$. بنابراین، ψ خوش تعریف است و بنابر گزارهٔ ۲. ۲، $[\varphi]_\beta\in M_n(R;I_1,I_2,\ldots,I_n)$.

حال نشان می‌دهیم که ψ یک هم‌ریختی حلقه‌ای است. فرض کنید $\varphi_1,\varphi_2\in\mathrm{E}nd_R(\oplus_{i=1}^nR/I_i)$. در این‌صورت عناصر $a_{ik},a'_{kj}\in R$ موجودند به‌طوری‌که، برای هر $1\le k,j\le n$، $\varphi_1(\mathbf{e}_k)=\Sigma_{i=1}^na_{ik}\mathbf{e}_i$ و $\varphi_2(\mathbf{e}_j)=\Sigma_{k=1}^na'_{kj}\mathbf{e}_k$. برای هر $1\le j\le n$،

$$\begin{aligned}(\varphi_1\circ\varphi_2)(\mathbf{e}_j)&=\varphi_1(\varphi_2(\mathbf{e}_j))=\varphi_1(\Sigma_{k=1}^na'_{kj}\mathbf{e}_k)=\Sigma_{k=1}^na'_{kj}\varphi_1(\mathbf{e}_k)\\&=\Sigma_{k=1}^na'_{kj}(\Sigma_{i=1}^na_{ik}\mathbf{e}_i)=\Sigma_{i=1}^n(\Sigma_{k=1}^na_{ik}a'_{kj})\mathbf{e}_i.\end{aligned}$$

بنابراین

$$\psi(\varphi_1 o\varphi_2)=[\varphi_1 o\varphi_2]_\beta=\left(\left(\sum_{k=1}^na_{ik}a'_{kj}\right)\right)_{n\times n}=\left(\left(a_{ij}\right)\right)_{n\times n}\left(\left(a'_{ij}\right)\right)_{n\times n}=\psi(\varphi_1)\psi(\varphi_2).$$

هم‌چنین، به‌وضوح $\psi(\varphi_1+\varphi_2)=\psi(\varphi_1)+\psi(\varphi_2)$ و $\psi(1_{\mathrm{E}nd_R(\oplus_{i=1}^nR/I_i)})=1_{M_n(R;I_1,I_2,\ldots,I_n)}$.

به‌کمک گزارهٔ ۲. ۲، هم‌ریختی حلقه‌ای ψ پوشا است. هم‌چنین، ψ یک به یک است، زیرا اگر

$$\psi(\varphi_1)=\psi(\varphi_2)$$

جایی‌که $\varphi_1(\mathbf{e}_j)=\Sigma_{i=1}^na_{ij}\mathbf{e}_i$ و $\varphi_2(\mathbf{e}_j)=\Sigma_{i=1}^na'_{ij}\mathbf{e}_i$، ($1\le j\le n$)، آن‌گاه $[\varphi_1]_\beta=[\varphi_2]_\beta$ و بنابراین $\left(\left(a_{ij}\right)\right)_{n\times n}\approx\left(\left(a'_{ij}\right)\right)_{n\times n}$. از این‌رو، $a_{ij}-a'_{ij}\in I_i$ و $\Sigma_{i=1}^n(a_{ij}-a'_{ij})\mathbf{e}_i=0$. این ایجاب می‌کند که $\varphi_1=\varphi_2$.

فرض کنید R یک CF- حلقه باشد. دستگاه هم‌نهشتی خطی (۱) را در نظر بگیرید:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 & (\text{mod } I_1) \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 & (\text{mod } I_2) \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots & \quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \equiv b_n & (\text{mod } I_n) \end{cases} \tag{۱}$$

جایی‌که n یک عدد صحیح مثبت، $a_{ij}, b_i \in R$ و $I_j \subseteq \bigcap_{i \neq j}(I_i : a_{ij})$ ($1 \leq i, j \leq n$).

در ادامه نشان می‌دهیم که حل دستگاه هم‌نهشتی خطی (۱) را می‌توان به‌حالتی‌که $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$ محدود نمود. برای این منظور، فرض کنید $A = (a_{ij})$ نمایش ماتریس ضرایب دستگاه بالا باشد. به‌کمک گزارهٔ ۲. ۲، ماتریس A،
R- درون‌ریختی

$$\varphi : R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n \to R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$$

را القا می‌کند. هم‌چنین، بنابر [۱۲]، R- مدول $R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$ دارای یک صورت متعارف است. بنابراین یک‌ریختی

$$\psi : R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n \cong R/J_1 \oplus R/J_2 \oplus \cdots \oplus R/J_n$$

موجود است به‌طوری‌که J_i یک ایدآل از R و $J_1 \subseteq J_2 \subseteq \cdots \subseteq J_n$. بنابراین، نمودار زیر را در نظر می‌گیریم

$$\begin{array}{ccc} R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n & \xleftarrow{\varphi} & R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n \\ \psi \downarrow & & \psi^{-1} \uparrow \\ R/J_1 \oplus R/J_2 \oplus \cdots \oplus R/J_n & \xleftarrow{h} & R/J_1 \oplus R/J_2 \oplus \cdots \oplus R/J_n \end{array}$$

جایی‌که $h = \psi\varphi\psi^{-1}$. بنابراین، به‌کمک گزارهٔ ۲. ۲، R- درون‌ریختی h یک ماتریس مانند $C = (c_{ij})$ القا می‌کند که در شرط $J_j \subseteq \bigcap_{i \neq j}(J_i : c_{ij})$ صدق می‌کند.

حال برای حل دستگاه هم‌نهشتی خطی (۱)، ابتدا دستگاه هم‌نهشتی خطی (۲) را حل می‌کنیم:

$$\begin{cases} c_{11}x_1 + c_{12}x_2 + \cdots + c_{1n}x_n \equiv d_1 & (\text{mod } J_1) \\ c_{21}x_1 + c_{22}x_2 + \cdots + c_{2n}x_n \equiv d_2 & (\text{mod } J_2) \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots & \quad \vdots \\ c_{n1}x_1 + c_{n2}x_2 + \cdots + c_{nn}x_n \equiv d_n & (\text{mod } J_n) \end{cases} \tag{۲}$$

جایی‌که $(d_1 + J_1, d_2 + J_2, \ldots, d_n + J_n) := \psi(b_1 + I_1, b_2 + I_2, \ldots, b_n + I_n)$. بنابراین، $(x_1, x_2, \ldots, x_n)$ یک جواب از دستگاه (۲) است اگر و تنها اگر $(y_1, y_2, \ldots, y_n)$ یک جواب از دستگاه (۱) باشد به‌طوری‌که

$$\psi^{-1}(x_1 + J_1, x_2 + J_2, \ldots, x_n + J_n) = (y_1 + I_1, y_2 + I_2, \ldots, y_n + I_n).$$

از این رو، با توجه به مباحث بالا، کافی است تنها دستگاه‌های هم‌نهشتی خطی با شرط $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$ را بررسی کنیم. هدف ما در بخش بعدی این است که تکنیک‌های جبرخطی هم‌نهشتی را برای حل چنین دستگاه‌هایی تعمیم دهیم.

۳. وارون‌پذیری ماتریس‌های هم‌نهشتی

در این بخش، مفهوم وارون‌پذیری در $M_n(R; I_1, I_2, \ldots, I_n)$ را جایی‌که $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$ تعریف و بررسی می‌کنیم. به‌علاوه، از این مفهوم برای حل دستگاه‌های هم‌نهشتی خطی استفاده می‌کنیم.

تعریف ۳. ۱ فرض کنید R یک حلقه و $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$ یک زنجیر از ایدآل‌های سره R باشد. هم‌چنین، فرض کنید $A = ((a_{ij})) \in M_n(R; I_1, I_2, \ldots, I_n)$. دترمینان A را با نماد $\det(A)$ نمایش و بدین‌صورت تعریف

می‌شود:

$$\det(A) \equiv \sum_{\delta\in S_n} sgn(\delta) a_{1\delta(1)} a_{2\delta(2)} \ldots a_{n\delta(n)} \ (mod\ I_n)$$

جایی‌که S_n نمایش مجموعهٔ تمام جای‌گشت‌ها روی n و $sgn(\delta)$ نمایش علامت $\delta\in S_n$ باشد. بنابراین، اگر δ زوج باشد، آن‌گاه $sgn(\delta)=1$ و اگر δ فرد باشد، آن‌گاه $sgn(\delta)=-1$.

تذکر ۳. ۲ فرض کنید R یک حلقه باشد و $I_1\subseteq I_2\subseteq\ldots\subseteq I_n$ یک زنجیر از ایدآل‌های R باشد. اگر $A=\left(\left(a_{ij}\right)\right)\approx\left(\left(b_{ij}\right)\right)=B$ دو ماتریس در $M_n(R;I_1,I_2,\ldots,I_n)$ باشند، آن‌گاه به‌راحتی می‌توان دید که $\det(A)=\det(B)$. بنابراین تعریف بالا خوش تعریف است.

تعریف ۳. ۳ ماتریس $A\in M_n(R;I_1,I_2,\ldots,I_n)$ را در $M_n(R;I_1,I_2,\ldots,I_n)$ وارون‌پذیر می‌نامیم، هرگاه ماتریس $B\in M_n(R;I_1,I_2,\ldots,I_n)$ موجود باشد به‌طوری‌که $AB\approx I$ جایی‌که I ماتریس همانی است.

یادآوری می‌کنیم که یک حلقهٔ R را موضعی می‌نامیم، هرگاه دارای یک ایدآل ماکسیمال منحصر به فرد باشد. در این‌جا، $adj(A)$ نمایش ماتریس الحاقی از یک ماتریس مربعی $n\times n$، A است. از جبرخطی می‌دانیم که $A\,adj(A)=adj(A)A=\det(A)I$ جایی‌که I ماتریس همانی است.

قضیهٔ ۳. ۴ *فرض کنیم R یک حلقهٔ موضعی با ایدآل ماکسیمال M و $I_1\subseteq I_2\subseteq\cdots\subseteq I_n$ یک زنجیر از ایدآل‌های R باشد. در این صورت ماتریس $A\in M_n(R;I_1,I_2,\ldots,I_n)$ وارون‌پذیر است اگر و تنها اگر عنصر $u\in R$ موجود باشد به‌طوری‌که $\det(A)u\equiv 1(mod\ M)$.*

اثبات. فرض کنید A وارون‌پذیر باشد. بنابراین ماتریس $B\in M_n(R;I_1,I_2,\ldots,I_n)$ موجود است به‌طوری‌که $AB\approx I$. بنابر تعریف ۳. ۱، داریم $\det(A)\det(B)\equiv 1(mod\ I_n)$ و این ایجاب می‌کند که $\det(A)\det(B)\equiv 1(mod\ M)$، از این‌که $I_n\subseteq M$.

برعکس، فرض کنید عنصر $u\in R$ موجود باشد به‌طوری‌که $\det(A)u\equiv 1(mod\ M)$. بنابراین، $1-\det(A)u\in M$، از این رو، $\det(A),u\notin M$ و بنابر گزارهٔ ۱۵.۱۵ [۲]، u و $\det(A)$ عناصر یکه در R هستند. این ایجاب می‌کند که عنصر $l\in R$ موجود است به‌طوری‌که $lu.\det(A)=1$. از این‌که $A\,adj(A)\cong\det(A)I$، نتیجه می‌گیریم که

$$A\left(lu\left(adj\left(A\right)\right)\right)\approx lu.\det(A)I\approx I.$$

بنابراین ماتریس A وارون‌پذیر است.

گزاره ۳. ۵ *فرض کنید R یک حلقه، I_i یک ایدآل از R $(1\le i\le n)$ باشد و $A\in M_n(R;I_1,I_2,\ldots,I_n)$. اگر عنصر $u_i\in R$ موجود باشد به‌طوری‌که، برای هر $1\le i\le n$، $\det(A)u_i\equiv 1(mod\ I_i)$، آن‌گاه ماتریس A وارون‌پذیر است. هم‌چنین، $A^{-1}=adj(A)\,diag(u_1,u_2,\ldots,u_n)$*

اثبات. قرار دهید $B\approx adj(A)\,diag(u_1,u_2,\ldots,u_n)$. آن‌گاه

$$\begin{aligned}AB&\approx A.adj(A)\,diag(u_1,u_2,\ldots,u_n)=\det(A)I\ diag(u_1,u_2,\ldots,u_n)\\&=diag(\det(A)u_1,\det(A)u_2,\ldots,\det(A)u_n).\end{aligned}$$

هم‌چنین، با توجه به فرض

$$diag(\det(A)u_1,\det(A)u_2,\ldots,\det(A)u_n)\approx I$$

و بنابراین $AB\approx I$. لذا A وارون‌پذیر است و $A^{-1}=adj(A)\,diag(u_1,u_2,\ldots,u_n)$.

نتیجهٔ بعدی به‌وضوح از گزارهٔ ۳ . ۵ به‌دست می‌آید.

نتیجه ۳. ۶ *فرض کنید* R *یک حلقه و* $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$ *یک زنجیر از ایدآل‌های* R *باشد و* $A \in M_n(R; I_1, I_2, \ldots, I_n)$. *اگر عنصر* $u \in R$ *موجود باشد به‌طوری‌که* $\det(A)u \equiv 1 (mod\ I_1)$*، آن‌گاه ماتریس* A *وارون‌پذیر است.*

در پایان این بخش یک مثال ارائه می‌دهیم و نشان می‌دهیم که چگونه به‌کمک وارون‌پذیری ماتریس ضرایب از یک دستگاه هم‌نهشتی خطی می‌توان جواب‌های دستگاه را به‌دست آورد.

مثال ۳. ۷ دستگاه هم‌نهشتی خطی زیر را در نظر بگیرید

$$\begin{cases} -x_1 - 2x_2 + 6x_3 \equiv 26 & (mod\ 36\mathbb{Z}) \\ 9x_1 + 4x_2 + 3x_3 + 6x_4 \equiv 10 & (mod\ 18\mathbb{Z}) \\ 2x_1 + 3x_2 + x_3 + 2x_4 \equiv 5 & (mod\ 6\mathbb{Z}) \\ x_1 + x_2 + x_3 + x_4 \equiv 2 & (mod\ 3\mathbb{Z}). \end{cases}$$

قرار می‌دهیم $A = \begin{pmatrix} -1 & -2 & 6 & 0 \\ 9 & 4 & 3 & 6 \\ 2 & 3 & 1 & 2 \\ 1 & 1 & 1 & 1 \end{pmatrix} \in M_4(\mathbb{Z}; 36\mathbb{Z}, 18\mathbb{Z}, 6\mathbb{Z}, 3\mathbb{Z})$، و توجه کنید که $36Z \subseteq 18Z \subseteq 6Z \subseteq 3Z$. هم‌چنین، $\det(A) = 7$ و

$$\det(A)(-5) \equiv 1 (mod\ 36\mathbb{Z})$$
$$\det(A)(-5) \equiv 1 (mod\ 18\mathbb{Z})$$
$$\det(A)(1) \equiv 1 (mod\ 6\mathbb{Z})$$
$$\det(A)(1) \equiv 1 (mod\ 3\mathbb{Z}).$$

بنابراین به‌کمک گزارهٔ ۳ . ۵، ماتریس A وارون‌پذیر است و

$$A^{-1} = adj\,(A)diag\,(-5,-5,1,1) = \begin{pmatrix} 5 & 4 & 18 & -60 \\ 3 & 1 & 15 & -36 \\ 3 & 1 & 8 & -22 \\ -11 & -6 & -41 & 125 \end{pmatrix} \begin{pmatrix} -5 & 0 & 0 & 0 \\ 0 & -5 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

که نتیجه می‌دهد

$$A^{-1} \approx \begin{pmatrix} 11 & 16 & 18 & 12 \\ 3 & -5 & -3 & 0 \\ -3 & 1 & 2 & 2 \\ 1 & 0 & 1 & 2 \end{pmatrix}.$$

اگر $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$، آن‌گاه $X \approx A^{-1} \begin{pmatrix} 26 \\ 10 \\ 5 \\ 2 \end{pmatrix} \approx \begin{pmatrix} 20 \\ 13 \\ 0 \\ 2 \end{pmatrix}$. بنابراین،

$$\begin{pmatrix} 20 + 36k_1 \\ 13 + 18k_2 \\ 6k_3 \\ 2 + 3k_4 \end{pmatrix}$$

جواب کلی از دستگاه هم‌نهشتی خطی بالا می‌باشد جایی‌که $k_1,k_2,k_3,k_4\in\mathbb{Z}$.

۴. تکنیک‌های جبرخطی هم‌نهشتی

هدف از این بخش ارائه یک روش جدید بر اساس تکنیک‌های جبرخطی برای حل نوع خاصی از دستگاه‌های معادلات هم‌نهشتی خطی است. فرض کنیم R یک CF- حلقه و $I_1\subseteq I_2\subseteq\cdots\subseteq I_n$ یک دنباله از ایدآل‌های R باشد. در این بخش، به بررسی دستگاه معادلات هم‌نهشتی می‌پردازیم که ماتریس ضرایب آن متعلق به مجموعهٔ $M_n(R;I_1,I_2,\dots,I_n)$ باشد. در ادامه سه مثال ارائه خواهیم داد که نشان می‌دهند چگونه می‌توان از تکنیک‌های جبرخطی برای حل یک دستگاه معادلات هم‌نهشتی استفاده کرد. در مثال اول، حالتی را که $R=\mathbb{Z}$ و $I_1\subseteq I_2\subseteq\cdots\subseteq I_n$ بررسی می‌کنیم. در مثال دوم، حالتی را بررسی می‌کنیم که ایدآل‌ها به شکل زنجیر نیستند و در مثال آخر حالتی را بررسی می‌کنیم که $R=R[t]$ و ایدآل‌ها به شکل زنجیر نیستند.

در مثال اول، از روش حذفی گاوسی پیمانه‌ای برای انجام عملیات حذفی گاوسی روی ماتریس‌ها با درایه‌های صحیح به پیمانه یک عدد صحیح n داده شده استفاده می‌کنیم. [۷]، [۸]، [۹]. در این مقاله‌ها، نویسندگان به بحث در مورد جبرخطی پیمانه‌ای روی ماتریس‌ها با درایه‌ها در $\mathbb{Z}_n$، جایی که n یک عدد اول و یا توانی از یک عدد اول است، می‌پردازند. توجه کنید هنگامی که n یک چنین عدد صحیح‌ای نباشد، می‌توان با استفاده از قضیهٔ باقی‌ماندهٔ چینی، روش حذفی گاوسی پیمانه‌ای را به‌کار برد. برای یک روش جای‌گزین با استفاده از پایه‌های گربنر روی حلقه‌ها با مقسوم علیه صفر (مانند $\mathbb{Z}_n$) مرجع [۱۱] را مشاهده کنید. در پایان توجه کنید که نتایج این بخش را می‌توان به راحتی برای دامنه‌های ایدآل اصلی تعمیم داد. برای بررسی جزئیات بیش‌تر در مورد نظریه ماتریس‌ها با درایه‌ها در یک حلقه جابه‌جایی به [۴] مراجعه شود.

شایان ذکر است که نرم‌افزار میپل یک بسته برای جبرخطی پیمانه‌ای فراهم می‌سازد. به‌علاوه، در بستهٔ $LinearAlgebra[Modular]$، تابع $RowReduce$ موجود است که شکل سطری پلکانی کاهش یافتهٔ یک ماتریس با درایه‌های صحیح را به پیمانه یک عدد صحیح داده شده محاسبه می‌کند. در ادامه، ما یک دستگاه هم‌نهشتی که ماتریس ضرایب آن به مجموعهٔ $M_n(\mathbb{Z};I_1,I_2,\dots,I_n)$، جایی که $I_i=\mathbb{Z}_{m_i}$ و $I_1\subseteq I_2\subseteq\cdots\subseteq I_n$، تعلق داشته باشد بررسی می‌کنیم. بنابراین، $m_n\mid m_{n-1},\dots,m_2\mid m_1$. برای یک چنین دستگاهی، ما می‌توانیم $n-1$ دستگاه دیگر به‌ازای $i=n,\dots,2$ به‌دست آوریم و یک دستگاه جدید شامل i معادله اول از دستگاه اصلی به پیمانه m_i را بررسی کنیم. برای هر $i=n,\dots,2$، ما برای به‌دست آوردن مجهول i-ام از دستگاه متناظر استفاده می‌کنیم. هم‌چنین، به‌راحتی می‌توان مشاهده کرد که هر جواب مشترک از همهٔ دستگاه‌های جدید، یک جواب از دستگاه اولیه است و بالعکس. بنابراین، اگر این دستگاه‌ها را حل کنیم، آن‌گاه می‌توانیم دستگاه اولیه را نیز حل کنیم.

مثال ۱.۴ دستگاه معادلات هم‌نهشتی خطی زیر را در نظر بگیرید

$$\begin{cases} 25x_1+3x_2+18x_3+36x_4\equiv 48 \pmod{72\mathbb{Z}}\\ 7x_1+4x_2+6x_3+12x_4\equiv 21 \pmod{24\mathbb{Z}}\\ 2x_1+3x_2+x_3+2x_4\equiv 3 \pmod{4\mathbb{Z}}\\ x_1+x_2+x_3+x_4\equiv 1 \pmod{2\mathbb{Z}}. \end{cases} \tag{۱}$$

اگر این دستگاه را در پیمانهٔ $2\mathbb{Z}$ در نظر بگیریم، داریم:

$$\begin{cases} x_1+x_2 & \equiv 0 \quad (mod\ 2\mathbb{Z}) \\ x_1 & \equiv 1 \quad (mod\ 2\mathbb{Z}) \\ x_2+x_3 & \equiv 1 \quad (mod\ 2\mathbb{Z}) \\ x_1+x_2+x_3+x_4 & \equiv 1 \quad (mod\ 2\mathbb{Z}). \end{cases}$$

این ایجاب می‌کند که $x_i \equiv 1\ (mod\ 2\mathbb{Z})$ برای $i=1,2,4$ و $x_3 \equiv 0\ (mod\ 2\mathbb{Z})$. بنابراین $x_i = 2z_i+1$ برای $i=1,2,4$ و $x_3 = 2z_3$. با جای‌گزینی x_1,x_2,x_3,x_4 در دستگاه هم‌نهشتی خطی (۱)، دستگاه (۲) به‌دست می‌آید:

$$\begin{cases} 50z_1+\ \ 6z_2+\ \ 36z_3 & \equiv 56 \quad (mod\ 72\mathbb{Z}) \\ 14z_1+\ \ 8z_2+\ \ 12z_3 & \equiv 22 \quad (mod\ 24\mathbb{Z}) \\ 4z_1+\ \ 6z_2+\ \ 2z_3 & \equiv 0 \quad (mod\ 4\mathbb{Z}). \end{cases} \tag{۲}$$

حال اگر دستگاه (۲) را در پیمانه $4\mathbb{Z}$ در نظر بگیریم، داریم:

$$\begin{cases} 2z_1+2z_2 & \equiv 0 \quad (mod\ 4\mathbb{Z}) \\ 2z_1 & \equiv 2 \quad (mod\ 4\mathbb{Z}) \\ 2z_2+2z_3 & \equiv 0 \quad (mod\ 4\mathbb{Z}), \end{cases}$$

که ایجاب می‌کند که $z_i \equiv 1\ (mod\ 2\mathbb{Z})$ برای $i=1,2,3$. بنابراین، $z_i = 2u_i+1$ برای $i=1,2,3$. از این‌رو، $x_i = 4u_i+3$ جایی‌که $i=1,2$ و $x_3 = 4u_3+2$. حال با جای‌گذاری $x_1 = 4u_1+3$، $x_2 = 4u_2+3$، $x_3 = 4u_3+2$ و $x_4 = 2z_4+1$ در معادلات اول و دوم از دستگاه هم‌نهشتی (۱) داریم:

$$\begin{cases} 28u_1+12u_2 & \equiv 36 \quad (mod\ 72\mathbb{Z}) \\ 4u_1+16u_2 & \equiv 12 \quad (mod\ 24\mathbb{Z}). \end{cases} \tag{۳}$$

حال اگر دستگاه (۳) را در پیمانه $24\mathbb{Z}$ در نظر بگیریم، داریم:

$$\begin{cases} 4u_1+12u_2 & \equiv 12 \quad (mod\ 24\mathbb{Z}) \\ 4u_1+16u_2 & \equiv 12 \quad (mod\ 24\mathbb{Z}). \end{cases}$$

و با استفاده از عملیات حذفی گاوس پیمانه‌ای، به‌دست می‌آوریم که

$$u_1 \equiv 3\ (mod\ 6\mathbb{Z}),\ u_2 \equiv 0\ (mod\ 6\mathbb{Z}).$$

بنابراین $u_1 = 6v_1+3$ و $u_2 = 6v_2$. از این‌رو، با جای‌گذاری $x_1 = 24v_1+15$، $x_2 = 24v_2+3$، $x_3 = 4u_3+2$ و $x_4 = 2z_4+1$ در معادلهٔ اول از دستگاه هم‌نهشتی (۱) داریم:

$$600v_1+336 \equiv 0\ (mod\ 72\mathbb{Z})$$

که ایجاب می‌کند که $24v_1 \equiv 24\ (mod\ 72\mathbb{Z})$. بنابراین $v_1 \equiv 1\ (mod\ 3\mathbb{Z})$، از این‌رو، $v_1 = 3w_1+1$. بنابراین $x_1 \equiv 39\ (mod\ 72\mathbb{Z})$. این ایجاب می‌کند که دستگاه (۱) دارای جواب منحصربه‌فرد

$$X = \begin{pmatrix} \begin{pmatrix} 39 \\ 3 \\ 2 \\ 1 \end{pmatrix} \end{pmatrix}$$

است.

در مثال بعدی ما در مورد حالتی که $R=\mathbb{Z}$ و ایدآل‌های $I_1,\cdots,I_n$ تشکیل زنجیر نمی‌دهند بحث می‌کنیم.

مثال ۴. ۲ دستگاه معادلات هم‌نهشتی خطی زیر را در نظر بگیرید

$$\begin{cases} 5x_1 + 2x_2 \equiv 4 \quad (mod\, 8) \\ 3x_1 + 5x_2 + 6x_3 \equiv 3 \quad (mod\, 12) \\ x_2 + x_3 \equiv 1 \quad (mod\, 2). \end{cases} \qquad (*)$$

قرار می‌دهیم $I_1 = 8\mathbb{Z},\ I_2 = 12\mathbb{Z},\ I_3 = 2\mathbb{Z}$. آن‌گاه

$$A = \begin{pmatrix} 5 & 2 & 0 \\ 3 & 5 & 6 \\ 0 & 1 & 1 \end{pmatrix} \in M_{3\times 3}(\mathbb{Z}; I_1, I_2, I_3) \ ; \ b = \left(\begin{pmatrix} 4 \\ 3 \\ 1 \end{pmatrix}\right).$$

از این‌که I_1، I_2 و I_3 تشکیل زنجیر نمی‌دهند، ابتدا یک زنجیر $J_1 \subseteq \cdots \subseteq J_n$ از ایدآل‌های $\mathbb{Z}$ می‌یابیم به‌طوری‌که مدول $N = \mathbb{Z}/J_1 \oplus \cdots \oplus \mathbb{Z}/J_n$ با مدول $M = \mathbb{Z}/I_1 \oplus \mathbb{Z}/I_2 \oplus \mathbb{Z}/I_3$ یک‌ریخت باشد. به‌وضوح کافی است ایدآل‌های زیر را بررسی کنیم

$$J_1 = 24\mathbb{Z},\ J_2 = 4\mathbb{Z},\ J_3 = 2\mathbb{Z}.$$

با استفاده از نمادهای بخش ۲، فرض کنیم $\varphi : M \to M$ نمایش نگاشت متناظر با A باشد. در زیر یک‌ریختی $\psi : M \to N$ را طوری می‌یابیم که نگاشت $h : N \to N$ برابر با $\psi\varphi\psi^{-1}$ باشد. برای این منظور، فرض کنید $\alpha : M \to \mathbb{Z}_8 \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_4) \oplus \mathbb{Z}_2$ با ضابطهٔ $\alpha(a_1,a_2,a_3) = (a_1,a_2,a_2,a_3)$ و $\beta : \mathbb{Z}_8 \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_4) \oplus \mathbb{Z}_2 \to N$ با ضابطهٔ $\beta(b_1,b_2,b_3,b_4) = (3b_1 + 8b_2, b_3, b_4)$. به‌وضوح می‌توان گفت که α و β یک‌ریختی‌های طبیعی هستند. اگر $\psi = \beta\alpha$، آن‌گاه $\psi : M \to N$ یک یک‌ریختی با ضابطهٔ $\psi(a_1,a_2,a_3) = (3a_1 + 8a_2, a_2, a_3)$ است. بنابراین ماتریس متناظر با ψ نسبت به مجموعهٔ مولد استاندارد از M و N عبارت است از:

$$[\psi] = \begin{pmatrix} 3 & 8 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

به‌طور مشابه، یک یک‌ریختی $\psi^{-1} : N \to M$ به‌دست می‌آوریم. تعریف می‌کنیم

$$\gamma : N \to (\mathbb{Z}_8 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$$

با ضابطهٔ $\gamma(c_1,c_2,c_3) = (c_1,c_1,c_2,c_3)$ و $\eta : (\mathbb{Z}_8 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \to M$
با ضابطهٔ $\eta(d_1,d_2,d_3,d_4) = (d_1, 4d_2 + 3d_3, d_4)$. به‌وضوح γ و η یک‌ریختی هستند.
اگر $\psi^{-1} = \eta\gamma$، آن‌گاه $\psi^{-1} : N \to M$ یک یک‌ریختی با ضابطهٔ $\psi^{-1}(c_1,c_2,c_3) = (c_1, 4c_1 + 3c_2, c_3)$ است.
بنابراین ماتریس متناظر با ψ^{-1} نسبت به مجموعهٔ مولد استاندارد از N و M عبارت است از:

$$[\psi^{-1}] = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

اگر $h = \psi\varphi\psi^{-1}$، آن‌گاه ماتریس متناظر با h عبارت است از:

$$B = [\psi]A[\psi^{-1}] = \begin{pmatrix} 3 & 8 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 5 & 2 & 0 \\ 3 & 5 & 6 \\ 0 & 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 223 & 138 & 48 \\ 23 & 15 & 6 \\ 4 & 3 & 1 \end{pmatrix}.$$

به‌منظور بازنویسی دستگاه جدید، هم‌چنین داریم:

$$d=\begin{pmatrix}d_1\\d_2\\d_3\end{pmatrix}=[\psi]b=\begin{pmatrix}3&8&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}4\\3\\1\end{pmatrix}=\begin{pmatrix}36\\3\\1\end{pmatrix}.$$

اما با استفاده از این حقیقت که،

$$B\approx\begin{pmatrix}7&18&0\\3&3&2\\0&1&1\end{pmatrix}\in M_{3\times3}(\mathbb{Z};J_1,J_2,J_3)\quad;\quad d\approx\left(\begin{pmatrix}12\\3\\1\end{pmatrix}\right)$$

دستگاه جدید متناظر با B و d عبارت است از

$$\begin{cases}7y_1+18y_2 &\equiv 12 \quad (mod\, 24)\\ 3y_1+3y_2+2y_3 &\equiv 3 \quad (mod\, 4)\\ \quad y_2+y_3 &\equiv 1 \quad (mod\, 2).\end{cases}\qquad (**)$$

با حل دستگاه $(**)$، جواب دستگاه $(*)$ به‌دست می‌آید. برای حل دستگاه $(**)$، ابتدا این دستگاه را به پیمانهٔ $J_3=2\mathbb{Z}$ حل می‌کنیم. ماتریس تکمیل شده از این دستگاه جدید عبارت است از

$$\left(\begin{pmatrix}1&0&0&0\\1&1&0&1\\0&1&1&1\end{pmatrix}\right)$$

با استفاده از تابع *RowReduce* از میپل، بعد از انجام اعمال عملیات حذف گاوسی، ماتریس بدین‌صورت تبدیل می‌شود:

$$\left(\begin{pmatrix}1&0&0&0\\0&1&0&1\\0&0&1&0\end{pmatrix}\right)$$

بنابراین $y_1\equiv 0(mod\,2),\ \ y_2\equiv 1(mod\,2)\ ,\ \ y_3\equiv 0(mod\,2)$ آن‌گاه $y_1=2z_1,\ \ y_2=2z_2+1\ ,\ \ y_3=2z_3$. با جای‌گذاری y_1,y_2,y_3 در معادلات اول و دوم دستگاه $(**)$، داریم

$$\begin{cases}14z_1+12z_2 \equiv 18 \qquad (mod\; 24)\\ \;2z_1+2z_2 \quad \equiv 0 \qquad (mod\; 4).\end{cases}$$

حال، این دستگاه را به پیمانهٔ $J_2=4\mathbb{Z}$ حل می‌کنیم. برای این منظور، ماتریس تکمیل شده از این دستگاه عبارت است از :

$$\left(\begin{pmatrix}2&0&2\\2&2&0\end{pmatrix}\right).$$

اگر اعمال حذفی گاوس را روی این ماتریس انجام دهیم، این ماتریس به‌دست می‌آید:

$$\left(\begin{pmatrix}2&0&2\\0&2&2\end{pmatrix}\right)$$

بنابراین $2z_1\equiv 2\ (mod\ 4),\ 2z_2\equiv 2\ (mod\ 4)$. از این‌رو، $z_1\equiv 1\ (mod\ 2),\ z_2\equiv 1\ (mod\ 2)$، یعنی $z_1=2u_1+1\ \ ,\ z_2=2u_2+1$. بنابراین $y_1=4u_1+2\ ,\ \ y_2=4u_2+3$، همچنین $y_2\equiv 3(mod\ 4)$. آن‌گاه با جای‌گذاری y_1 و y_2 در معادلهٔ اول دستگاه $(**)$، داریم

$$4u_1\equiv 16\ \ (\mathrm{mod}\ \ 24)\ \Rightarrow u_1\equiv 4\ \ (\mathrm{mod}\ \ 6)\ \Rightarrow y_1\equiv 18\ \ (\mathrm{mod}\ \ 24)$$

بنابراین دستگاه $(**)$ دارای جواب منحصربه‌فرد $\left(\begin{pmatrix}18\\3\\0\end{pmatrix}\right)$ است. از این‌رو، $\begin{pmatrix}18\\3\\0\end{pmatrix}[\psi^{-1}]$ که با $\left(\begin{pmatrix}2\\9\\0\end{pmatrix}\right)$ هم‌ارز است، جواب منحصربه‌فرد دستگاه $(*)$ است.

در مثال بعدی ما در مورد حالتی که $R=\mathbb{R}[t]$ و ایدآل‌های $I_1,\cdots,I_n$ تشکیل زنجیر نمی‌دهند بحث می‌کنیم.

مثال ۴. ۳ فرض کنیم $R=\mathbb{R}[t]$، حلقهٔ چندجمله‌ای‌ها با ضرایب در $\mathbb{R}$ باشد. این دستگاه را در نظر می‌گیریم:

$$(\star)\quad \begin{cases} -t\,x_1 + t(t+1)\,x_2 - 2(t+1)\,x_3 \equiv 2(t-1) \pmod{t^2(t+1)R} \\ (t-1)\,x_1 + tx_2 \equiv 0 \pmod{t(t-1)R} \\ t\,x_1 - t\,x_2 + x_3 \equiv -2t+1 \pmod{t^2R}. \end{cases}$$

قرار می‌دهیم:

$$.I_1=t^2(t+1)R,\quad I_2=t(t-1)R,\quad I_3=t^2R$$

از این‌که I_1، I_2، I_3 تشکیل زنجیر نمی‌دهند، ابتدا یک زنجیر از ایدآل‌های $J_1\subseteq\cdots\subseteq J_n$ از R می‌یابیم که $N=R/J_1\oplus\cdots\oplus R/J_n$ با $M=R/I_1\ \ m\oplus\ \ R/I_2\oplus\ \ R/I_3$ یک‌ریخت باشد. برای این منظور کافی است قرار دهیم:

$$J_1=t^2(t+1)(t-1)R,\quad J_2=t^2R,\quad J_3=tR.$$

با استفاده از نمادهای بخش ۲، فرض کنیم $\varphi:M\to M$ نمایش نگاشت متناظر با A باشد. در زیر یک‌ریختی $\psi:M\to N$ را طوری می‌یابیم که نگاشت $h:N\to N$ برابر با $\psi\varphi\psi^{-1}$ باشد. برای این منظور، فرض کنید $\alpha:M\to L$ با ضابطهٔ $\alpha(f_1,f_2,f_3)=(f_1,f_2,f_2,f_3)$ جایی‌که

$$L=R/t^2(t+1)R\oplus R/(t-1)R\oplus R/tR\oplus R/t^2R$$

و $\beta:L\to N$ با ضابطهٔ $\beta(g_1,g_2,g_3,g_4)=((t-1)g_1+t^2(t+1)g_2,g_4,g_3)$. به‌وضوح می‌توان گفت که α و β یک‌ریختی‌های طبیعی هستند. اگر $\psi=\beta\alpha$، آن‌گاه $\psi::M\to N$ یک یکریختی با ضابطهٔ $\psi(f_1,f_2,f_3)=((t-1)f_1+t^2(t+1)f_2,f_3,f_2)$ است. بنابراین ماتریس متناظر با ψ نسبت به مجموعهٔ مولد استاندارد از M و N عبارت است از:

$$[\psi]=\begin{pmatrix} t-1 & t^2(t+1) & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}.$$

به‌طور مشابه، یک یک‌ریختی $\psi^{-1}:N\to M$ به‌دست می‌آوریم. هم‌ریختی $\gamma:N\to L$ با ضابطهٔ

$$\gamma(p_1,p_2,p_3)=(p_1,p_1,p_3,p_2)$$

و هم‌ریختی $\eta:L\to M$ با ضابطهٔ

$$\eta(q_1,q_2,q_3,q_4)=(q_1,tq_2+(t-1)q_3,q_4)$$

را تعریف می‌کنیم. به‌وضوح γ و η یک‌ریختی هستند. اگر $\psi^{-1}=\eta\gamma$، آن‌گاه $\psi^{-1}:N\to M$ یک یک‌ریختی با ضابطهٔ $\psi^{-1}(p_1,p_2,p_3)=(p_1,tp_1+(t-1)p_3,p_2)$ است. بنابراین ماتریس متناظر با ψ^{-1} نسبت به مجموعهٔ مولد استاندارد از N و M عبارت است از:

$$[\psi^{-1}]=\begin{pmatrix}1 & 0 & 0\\ t & 0 & t-1\\ 0 & 1 & 0\end{pmatrix}.$$

اگر A ماتریس ضرایب دستگاه $(\star)$ باشد و $B=[\psi]A[\psi^{-1}]$، آن‌گاه

$$B\approx\left(\begin{pmatrix} t(t^2+1) & -2(t^2-1) & -t(t^2-1)\\ t & 1 & t\\ -1 & 0 & 0\end{pmatrix}\right)\in M_{3\times 3}(R;J_1,J_2,J_3).$$

هم‌چنین اگر $b=\begin{pmatrix}2(t-1)\\ 0\\ -2t+1\end{pmatrix}$، آن‌گاه

$$d=\begin{pmatrix}d_1\\ d_2\\ d_3\end{pmatrix}=[\psi]b\approx\left(\begin{pmatrix}2(t-1)^2\\ -2t+1\\ 0\end{pmatrix}\right).$$

دستگاه متناظر با B و $[\psi]b$ عبارت است از

$$(\star\star)\quad\begin{cases} t(t^2+1)y_1 - 2(t^2-1)y_2 - t(t^2-1)y_3 \equiv 2(t-1)^2 \pmod{J_1}\\ ty_1 + y_2 + ty_3 \equiv -2t+1 \pmod{J_2}\\ -y_1 \equiv 0 \pmod{J_3}.\end{cases}$$

با حل دستگاه $(\star\star)$، جواب دستگاه $(\star)$ به‌دست می‌آید. برای حل دستگاه $(\star\star)$، ابتدا این دستگاه را به پیمانهٔ $J_3=tR$ حل می‌کنیم. ماتریس تکمیل شده از این دستگاه جدید عبارت است از:

$$\left(\begin{pmatrix}0 & 2 & 0 & 2\\ 0 & 1 & 0 & 1\\ -1 & 0 & 0 & 0\end{pmatrix}\right)\in M_{3\times 4}(R;J_3,J_3,J_3).$$

آن‌گاه با انجام اعمال سطری مقدماتی $r_1\leftrightarrow r_3, -r_1\mapsto r_1, r_3-2r_2\mapsto r_3$ داریم:

$$\left(\begin{pmatrix}0 & 2 & 0 & 2\\ 0 & 1 & 0 & 1\\ -1 & 0 & 0 & 0\end{pmatrix}\right)\to\left(\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 1\\ 0 & 0 & 0 & 0\end{pmatrix}\right)$$

و بنابراین $y_1\equiv 0 \pmod{J_3},\ y_2\equiv 1 \pmod{J_3}$ و y_3 یک متغیر دل‌خواه در پیمانه J_3 است. آن‌گاه با جای‌گذاری $y_1=tz_1$ و $y_2=tz_2+1$ در معادلهٔ اول و دوم دستگاه $(\star\star)$ داریم:

$$\begin{cases} t^2(t^2+1)z_1 - 2(t^2-1)(tz_2+1) - t(t^2-1)y_3 \equiv 2(t-1)^2 \pmod{J_1}\\ t^2z_1 + tz_2+1 + ty_3 \equiv -2t+1 \pmod{J_2}.\end{cases}$$

حال، این دستگاه را در پیمانهٔ $J_2=t^2R$ حل می‌کنیم. برای این منظور، ماتریس تکمیل شده از این دستگاه عبارت است از:

$$\left(\begin{pmatrix}0 & 2t & t & -4t\\ 0 & t & t & -2t\end{pmatrix}\right).$$

بنابراین با انجام اعمال سطری مقدماتی $r_1\leftrightarrow r_2, r_2-2r_1\mapsto r_2, r_1+r_2\mapsto r_1, -r_2\mapsto r_2$، داریم:

$$\left(\begin{pmatrix}0 & 2t & t & -4t\\ 0 & t & t & -2t\end{pmatrix}\right)\to\left(\begin{pmatrix}0 & t & 0 & -2t\\ 0 & 0 & t & 0\end{pmatrix}\right).$$

بنابراین $ty_3\equiv 0 \pmod{t^2R},\ tz_2\equiv -2t \pmod{t^2R}$.

از این‌رو، $y_3\equiv 0 \pmod{tR},\ z_2\equiv -2 \pmod{tR}$، یعنی، $y_3=tu_3,\ z_2=tu_2-2$. بنابراین با

جای‌گذاری $y_1 = tz_1$، $y_2 = t^2u_2 - 2t + 1$ و $y_3 = tu_3$ در معادلهٔ اول دستگاه $(\star\star)$، داریم:

$$\begin{array}{rrcll}
& t^2(t^2+1)z_1 - 2(t^2-1)(-2t+1) & \equiv & 2(t-1)^2 & \pmod{t^2(t^2-1)R} \\
\Rightarrow & t^2(t^2+1)z_1 & \equiv & 4t^2(-t+1) & \pmod{t^2(t^2-1)R} \\
\Rightarrow & (t^2+1)z_1 & \equiv & 4(-t+1) & \pmod{(t^2-1)R} \\
\Rightarrow & (t^2-1+2)z_1 & \equiv & 4(-t+1) & \pmod{(t^2-1)R} \\
\Rightarrow & 2z_1 & \equiv & 4(-t+1) & \pmod{(t^2-1)R} \\
\Rightarrow & z_1 & \equiv & 2(-t+1) & \pmod{(t^2-1)R}.
\end{array}$$

بنابراین $z_1 = (t^2-1)f(t) + 2(-t+1)$، از این‌رو،

$$y_1 = t(t^2-1)f(t) + 2t(-t+1) \pmod{t^2(t^2-1)R}$$

جایی‌که $f(t)$ یک عنصر دل‌خواه از R است. بنابراین دستگاه $(\star\star)$ دارای جواب

$$\left(\begin{pmatrix} t(t^2-1)f(t) + 2t(-t+1) \\ -2t+1 \\ 0 \end{pmatrix}\right)$$

است. از این‌رو،

$$[\psi^{-1}]\left(\begin{pmatrix} t(t^2-1)f(t) + 2t(-t+1) \\ -2t+1 \\ 0 \end{pmatrix}\right) \approx \left(\begin{pmatrix} t(t^2-1)f(t) + 2t(-t+1) \\ 0 \\ -2t+1 \end{pmatrix}\right)$$

تمام جواب‌های دستگاه $(\star)$ است.

۵. پایه‌های گربنر و دستگاه‌های هم‌نهشتی

در این بخش به کاربرد جدیدی از پایه‌های گربنر در حل دستگاه‌های معادلات هم‌نهشتی خطی می‌پردازیم. برای این منظور، ابتدا برخی تعاریف و نتایج اصلی مرتبط با پایه‌های گربنر را بیان و به کاربرد این پایه‌ها در حل دستگاه‌های خطی روی اعداد طبیعی نیز اشاره می‌کنیم.

فرض کنیم $P = K[x_1,\ldots,x_n]$ حلقهٔ چندجمله‌ای‌ها روی میدان K با متغیرهای $x_n,\ldots,x_2,x_1$ باشد. فرض کنیم $I = \langle f_1,\ldots,f_k \rangle$ یک ایدآل P باشد که توسط چندجمله‌ایهای $f_1,\ldots,f_k \in P$ تولید می‌شود. هم‌چنین فرض کنیم $f \in P$ و $\prec$ یک ترتیب تک‌جمله‌ای روی حلقهٔ P باشد. در این صورت بزرگ‌ترین تک‌جمله‌ای f (نسبت به $\prec$) را تک‌جمله‌ای پیش‌روی f می‌نامیم و با $LM(f)$ نمایش می‌دهیم. ضریب $LM(f)$ در f را ضریب پیش‌روی f می‌نامیم و با $LC(f)$ نمایش می‌دهیم. حاصل‌ضرب $LM(f).LC(f)$ را جملهٔ پیش‌روی f می‌نامیم و آن را با $LT(f)$ نمایش می‌دهیم. ایدآل تک‌جمله‌ای $LT(I) = \langle LT(f) \mid f \in I \rangle$ را ایدآل جملهٔ پیش‌روی I می‌نامیم.

یک زیر مجموعهٔ متناهی $G = \{g_1,\ldots,g_t\} \subseteq I$ را یک پایهٔ گربنر I نسبت به $\prec$ می‌نامیم هرگاه

$$LT(I) = \langle LT(g_1),\ldots,LT(g_k) \rangle.$$

برای توضیحات بیش‌تر راجع به پایه‌های گربنر به [۱] صفحه ۳۲ مراجعه شود.

حال فرض کنیم $a_{ij}, b_i \in \mathbb{Z}$ که $i=1,\dots,m$ و $j=1,\dots,n$. می‌خواهیم با استفاده از پایه‌های گربنر جواب $(\sigma_1,\dots,\sigma_n)\in\mathbb{N}^n$ را برای دستگاه

$$\begin{cases} a_{11}\sigma_1 + a_{12}\sigma_2 + \cdots + a_{1n}\sigma_n &= b_1 \\ \vdots \\ a_{m1}\sigma_1 + a_{m2}\sigma_2 + \cdots + a_{mn}\sigma_n &= b_n \end{cases} \qquad (۳)$$

به‌دست آوریم. برای حل این دستگاه، آن را به مسالهٔ معادل در نظریهٔ ایدآل‌های چندجمله‌ای تبدیل می‌کنیم و سپس این مسالهٔ جدید را با استفاده از تکنیک پایه‌های گربنر حل می‌کنیم. برای این منظور یک متغیر جدید به‌نام ω معرفی می‌کنیم و ایدآل J را به‌صورت $J=\langle x_1\cdots x_m\omega-1\rangle$ در نظر می‌گیریم. برای هر عضو $(a_{1i},\dots,a_{mi})\in\mathbb{Z}^m$ با مؤلفه‌های منفی، می‌توان این $m-$ تایی را بدین‌صورت نوشت:

$$(a_{1i},\dots,a_{mi}) = (a'_{1i},\dots,a'_{mi}) + \alpha_i(-1,\dots,-1)$$

که در آن $(a'_{1i},\dots,a'_{mi})\in\mathbb{N}^m$ و $\alpha_i\in N$. دقت کنیم که اگر برای هر j داشته باشیم $a_{ij}\in\mathbb{N}$ آن‌گاه $\alpha_i=0$. بنابراین برای هر i داریم:

$$x_1^{a_{1i}}\cdots x_m^{a_{mi}} + J = x_1^{a'_{1i}}\cdots x_m^{a'_{mi}} + J$$

حال نگاشت چندجمله‌ای زیر را در نظر می‌گیریم:

$$\phi: K[y_1,\dots,y_n] \to K[x_1,\dots,x_m]/J$$

که در آن $\phi(y_i) = x_1^{a'_{1i}}\cdots x_m^{a'_{mi}} + J$. همچنین فرض می‌کنیم $x_1^{b_1}\cdots x_m^{b_m} + J = x_1^{b'_1}\cdots x_m^{b'_m} + J$. گزارهٔ زیر یک روش الگوریتمیک برای حل دستگاه (۳) فراهم می‌کند ([۱] صفحه ۱۰۹).

گزاره ۱.۵ *با استفاده از نمادهای بالا، دستگاه (۳) یک جواب طبیعی دارد اگر و تنها اگر* $x_1^{b'_1}\cdots x_m^{b'_m}\omega^\beta + J$ *تصویر یک تک‌جمله‌ای در* $K[y_1,\dots,y_n]$ *تحت نگاشت* ϕ *باشد. به‌علاوه، اگر*

$$x_1^{b'_1}\cdots x_m^{b'_m}\omega^\beta + J = \phi(y_1^{\sigma_1}\cdots y_n^{\sigma_n})$$

آن‌گاه $(\sigma_1,\dots,\sigma_n)$ یک جواب دستگاه (۳) است.

لازم به ذکر است که برای تشخیص این که $x_1^{b'_1}\cdots x_m^{b'_m}\omega^\beta + J$ متعلق به تصویر ϕ است یا خیر یک پایهٔ گربنر G را برای ایدآل

$$I = \langle y_1 - x_1^{a'_{11}}\cdots x_m^{a'_{m1}}\omega^{\alpha_1},\dots,y_n - x_1^{a'_{1n}}\cdots x_m^{a'_{mn}}\omega^{\alpha_n}, x_1\cdots x_m\omega-1\rangle$$

نسبت به‌ترتیب الفبایی که در آن برای هر i,j، $y_i \prec \omega \prec x_j$ محاسبه می‌کنیم. حال فرض کنیم h باقی‌ماندهٔ تقسیم $x_1^{b'_1}\cdots x_m^{b'_m}\omega^\beta$ بر G باشد. اگر $(\sigma_1,\dots,\sigma_n)\in\mathbb{N}^n$ موجود باشد که $h=y_1^{\sigma_1}\cdots y_n^{\sigma_n}$ در این صورت $(\sigma_1,\dots,\sigma_n)$ یک جواب دستگاه (۳) است و اگر چنین $(\sigma_1,\dots,\sigma_n)\in\mathbb{N}^n$ موجود نباشد آن‌گاه دستگاه جواب ندارد. برای مشاهدهٔ مثال‌های متنوعی در این زمینه به [۱] صفحات ۱۰۷-۱۱۰ مراجعه شود. در ادامه نتیجهٔ اصلی این بخش که تعمیم این گزاره برای حل دستگاه هم‌نهشتی (۱) برای حالت خاص $R=\mathbb{Z}$ را بیان می‌کنیم. در واقع چون $\mathbb{Z}$ یک دامنهٔ ایدآل اصلی است پس برای هر i، $I_i=\langle n_i\rangle$ که $n_i\in\mathbb{N}$ و در نتیجه دستگاه (۱) را می‌توان به‌صورت (۴) نوشت:

$$\begin{cases} a_{11}\sigma_1 + a_{12}\sigma_2 + \cdots + a_{1n}\sigma_n \equiv b_1 \pmod{n_1} \\ \vdots \\ a_{m1}\sigma_1 + a_{m2}\sigma_2 + \cdots + a_{mn}\sigma_n \equiv b_n \pmod{n_m}. \end{cases} \qquad (۴)$$

قرار می‌دهیم $J=\langle x_1^{n_1}-1,\dots,x_m^{n_m}-1, x_1\cdots x_m\omega-1\rangle$ و نگاشت چندجمله‌ای

$$\psi : K[y_1,\ldots,y_n] \to K[x_1,\ldots,x_m,\omega]/J$$

را با ضابطهٔ $\psi(y_i) = x_1^{a'_{1i}} \cdots x_m^{a'_{mi}} \quad \omega^{\alpha_i} + J$ در نظر می‌گیریم. بنابراین دستگاه (۴) یک جواب طبیعی دارد اگر و تنها اگر $x_1^{b'_1} \cdots x_m^{b'_m} \quad \omega^{\beta} + J$ تصویر یک تک‌جمله‌ای در $K[y_1,\ldots,y_n]$ تحت ψ باشد. به‌ویژه، اگر

$$x_1^{b'_1} \cdots x_m^{b'_m} \quad \omega^{\beta} + J = \psi(y_1^{\sigma_1} \cdots y_n^{\sigma_n})$$

آن‌گاه $(\sigma_1,\ldots,\sigma_n)$ یک جواب دستگاه (۴) است. در قضیهٔ ۵. ۲ یک روش الگوریتمیک جدید برای بررسی تعلق $x_1^{b'_1} \cdots x_m^{b'_m} \quad \omega^{\beta} + J$ در تصویر نگاشت ψ معرفی می‌کنیم.

قضیه ۵. ۲ فرض کنیم

$$I = \langle y_1 - x_1^{a'_{11}} \cdots x_m^{a'_{m1}} \omega^{\alpha_1}, \ldots, y_n - x_1^{a'_{1n}} \cdots x_m^{a'_{mn}} \omega^{\alpha_n}, x_1 \cdots x_n \omega - 1, x_1^{n_1} - 1, \ldots, x_m^{n_m} - 1 \rangle$$

و G یک پایه گربنر I نسبت به‌ترتیب تک‌جمله‌ای الفبایی که برای هر i,j داشته باشیم $y_i \prec \omega \prec x_j$، باشد. در این صورت دستگاه (۴) یک جواب طبیعی دارد اگر و تنها اگر باقی‌مانده تقسیم $x_1^{b'_1} \cdots x_m^{b'_m} \omega^{\beta}$ بر G یک تک‌جمله‌ای برحسب $y_1,\ldots,y_n$ باشد. به‌علاوه، اگر این باقی‌مانده $y_1^{\gamma_1} \cdots y_n^{\gamma_n}$ باشد، آن‌گاه $(\gamma_1,\ldots,\gamma_n)$ یک جواب طبیعی دستگاه است.

اثبات. فرض کنیم $(c_1,\ldots,c_n) \in \mathbb{N}^n$ یک جواب دستگاه باشد. بنابراین اعداد صحیح $t_1,\ldots,t_m$ وجود دارند که $a_{i1}c_1 + \cdots + a_{in}c_n = b_i - t_i n_i$ برای هر i. بنابراین دستگاه

$$\begin{cases} a_{11}\sigma_1 + a_{12}\sigma_2 + \cdots + a_{1n}\sigma_n &= b_1 - t_1 n_1 \\ \vdots \\ a_{m1}\sigma_1 + a_{m2}\sigma_2 + \cdots + a_{mn}\sigma_n &= b_m - t_m n_m \end{cases}$$

دارای یک جواب طبیعی $(c_1,\ldots,c_n)$ است. بدون از دست دادن کلیت مسئله، فرض کنیم $-t_m n_m$ کم‌ترین مقدار بین $-t_i n_i$–ها باشد. دو حالت برای $-t_m n_m$ ممکن است: اگر $-t_m n_m \geq 0$ در این صورت می‌توان نوشت:

$$(b_1 - t_1 n_1, \ldots, b_m - t_m n_m) = (b'_1,\ldots,b'_m) + (-t_1 n_1, \ldots, -t_m n_m) + \beta(-1,\ldots,-1).$$

فرض کنیم G_1 یک پایهٔ گربنر برای ایدآل تولید شده به‌وسیلهٔ چند جمله‌ای‌های

$$y_1 - x_1^{a'_{11}} \cdots x_m^{a'_{m1}} \omega^{\alpha_1},\ \ldots,\ y_n - x_1^{a'_{1n}} \cdots x_m^{a'_{mn}} \omega^{\alpha_n},\ x_1 \cdots x_m \omega - 1$$

باشد. با استفاده از گزارهٔ قبلی و با توجه به این که دستگاه بالا یک جواب طبیعی دارد نتیجه می‌گیریم باقی‌ماندهٔ تقسیم $x_1^{b'_1} \cdots x_m^{b'_m} x_1^{-t_1 n_1} \cdots x_m^{-t_m n_m} \omega^{\beta}$ بر G_1 یک تک‌جمله‌ای برحسب $y_1,\ldots,y_n$ است. از طرف دیگر داریم $x_i^{n_i} - 1 \in I$ و درنتیجه باقی‌ماندهٔ تقسیم $x_1^{b'_1} \cdots x_m^{b'_m} \omega^{\beta}$ نسبت به G یک تک جمله‌ای برحسب $y_1,\ldots,y_n$ است.

حال فرض کنیم $-t_m n_m < 0$. بنابراین می‌توان نوشت

$$\begin{aligned}(b_1 - t_1 n_1, \ldots, b_m - t_m n_m) = (b'_1,\ldots,b'_m) &+ (-t_1 n_1 + t_m n_m, \ldots, -t_{m-1} n_{m-1} \\ &+ t_m n_m, 0) + (\beta + t_m n_m)(-1,\ldots,-1).\end{aligned}$$

حال با استفاده از گزارهٔ قبل، باقی‌ماندهٔ تقسیم

$$u = x_1^{b'_1} \cdots x_m^{b'_m} x_1^{-t_1 n_1 + t_m n_m} \cdots x_{m-1}^{-t_{m-1} n_{m-1} + t_m n_m} \omega^{\beta + t_m n_m}$$

نسبت به G_1 یک تک‌جمله‌ای برحسب $y_1,\ldots,y_n$ است. برای هر $i = 1,\ldots,m-1$ قرار می‌دهیم

$$s_i = x_i^{-t_i n_i + t_m n_m}.$$

ادعا می‌کنیم باقی‌ماندهٔ تقسیم s_i بر G برابر است با $x_i^{t_m n_m}$. از طرفی چون $t_i \geq 0$ ، از $x_i^{n_i} - 1 \in I$ نتیجه می‌گیریم $x_i^{n_i t_i} - 1 \in I$ و ادعای مورد نظر اثبات می‌شود. با استفاده از این ادعا، u با استفاده از G به

$$v = x_1^{b'_1} \cdots x_m^{b'_m} x_1^{t_m n_m} \cdots x_{m-1}^{t_m n_m} \omega^{\beta + t_m n_m}$$

کاهش می‌یابد. از عضویت $x_m^{n_m}-1\in I$ داریم $x_n^{t_m n^m}-1\in I$. از طرفی از $x_1\cdots x_m\omega-1\in I$ نتیجه می‌گیریم که $x_1^{t_m n^m}\cdots x_{m-1}^{t_m n^m}\omega^{t_m n^m}-1\in I$. با استفاده از این نتایج v به $x_1^{b'_1}\cdots x_m^{b'_m}\omega^{\beta}$ کاهش می‌یابد. چون باقی‌ماندهٔ تقسیم u بر G یک تک‌جمله‌ای برحسب $y_1,\ldots,y_n$ است پس باقی‌ماندهٔ تقسیم $x_1^{b'_1}\cdots x_m^{b'_m}\omega^{\beta}$ نیز بر G یک تک‌جمله‌ای برحسب $y_1,\ldots,y_n$ است و حکم مورد نظر ثابت می شود. برعکس، فرض کنیم باقی‌ماندهٔ تقسیم $x_1^{b'_1}\cdots x_m^{b'_m}\omega^{\beta}$ بر G تک‌جمله‌ای $y_1^{\gamma_1}\cdots y_n^{\gamma_n}$ باشد. از تعلق $x_1\cdots x_m\omega-1\in I$ داریم:

$$x_1^{b'_1}\cdots x_m^{b'_m}-y_1^{\gamma_1}\cdots y_n^{\gamma_n}(x_1\cdots x_m)^{\beta}\in I.$$

اگر در ایدآل I به جای y_i قرار دهیم $x_1^{a'_{1i}}\cdots x_m^{a'_{mi}}\omega^{\alpha_i}$ آن گاه

$$x_1^{b'_1}\cdots x_m^{b'_m}-(x_1^{a'_{11}}\cdots x_m^{a'_{m1}})^{\gamma_1}\cdots(x_1^{a'_{1n}}\cdots x_m^{a'_{mn}})^{\gamma_n}\,\omega^{\alpha_1\gamma_1+\cdots+\alpha_n\gamma_n}\in\langle x_1^{n_1}-1,\ldots x_m^{n_m}-1\rangle.$$

با ضرب این رابطه در $(x_1\cdots x_m)^{\alpha_1\gamma_1+\cdots+\alpha_n\gamma_n}$ داریم:

$$x_1^{b'_1}\cdots x_m^{b'_m}(x_1\cdots x_m)^{\alpha_1\gamma_1+\cdots+\alpha_n\gamma_n}-(x_1^{a'_{11}}\cdots x_m^{a'_{m1}})^{\gamma_1}\cdots(x_1^{a'_{1n}}\cdots x_m^{a'_{mn}})^{\gamma_n}(x_1\cdots x_m)^{\beta}$$

متعلق به $\langle x_1^{n_1}-1,\ldots,x_m^{n_m}-1\rangle$ است. حال اگر قرار دهیم $x_i^{n_i}=1$ در این صورت چندجمله‌ای بالا برابر صفر خواهد شد و در نتیجه برای هر i داریم

$$(a'_{i1}-\alpha_1)\gamma_1+\cdots+(a'_{in}-\alpha_n)\gamma_n\equiv b'_i-\beta\pmod{n_i}.$$

بنابراین $(\gamma_1,\ldots,\gamma_n)$ یک جواب دستگاه (۴) است و حکم مورد نظر ثابت می‌شود.

مثال ۵. ۳ دستگاه زیر را در نظر می‌گیریم

$$\begin{cases}\sigma_1-2\sigma_2+5\sigma_3\equiv -47 \pmod 4\\ 3\sigma_1+7\sigma_2-\sigma_3\equiv 12 \pmod 8\\ -4\sigma_1+\sigma_2-2\sigma_3=-7\end{cases}$$

که در آن معادلهٔ آخر یک معادلهٔ دقیق است و هم‌نهشتی نیست. قرار دهیم:

$$I=\langle y_1-x_1^5x_2^7\omega^4,\,y_2-x_2^9x_3^3\omega^2,\,y_3-x_1^7x_2\omega^2,\,x_1x_2x_3\omega-1,\,x_1^4-1,\,x_2^8-1\rangle.$$

با استفاده از تابع *Basis* از بسته *Groebner* در نرم‌افزار میپل پایهٔ گربنر B برای ایدآل I را نسبت به‌ترتیب الفبایی با ترتیب $y_3\prec y_2\prec y_1\prec\omega\prec x_3\prec x_2\prec x_1$ محاسبه می‌کنیم. از طرف دیگر، می‌توان $(-47,12,-7)$ را بدین‌صورت نوشت:

$$(-47,12,-7)=(0,59,40)+47(-1,-1,-1).$$

باقی‌ماندهٔ تقسیم $x_2^{59}x_3^{40}\omega^{47}$ نسبت به B برابر است با $y_1y_2^9y_3^6$. با استفاده از قضیه قبل نتیجه می‌گیریم $(1,9,6)$ یک جواب برای دستگاه مورد نظر است. حال اگر دستگاه

$$\begin{cases}\sigma_1-2\sigma_2+5\sigma_3=-47\\ 3\sigma_1+7\sigma_2-\sigma_3=12\\ -4\sigma_1+\sigma_2-2\sigma_3=-7\end{cases}$$

را در نظر بگیریم. برای حل آن طبق گزارهٔ قبل باید ایدآل I' را تشکیل دهیم که از ایدآل I با حذف چندجمله‌ای‌های x_1^4-1 و x_2^8-1 به‌دست می‌آید. اگر B' پایهٔ گربنر I' نسبت به‌ترتیب بالا باشد، آن گاه باقی‌ماندهٔ تقسیم $x_2^{59}x_3^{40}\omega^{47}$ بر B' چندجمله‌ای $x_3^{31}y_1y_2^7y_3\omega^{39}$ است. چون این تک‌جمله‌ای برحسب تنها y_1,y_2,y_3 نیست پس طبق گزارهٔ قبل این دستگاه هیچ جواب طبیعی ندارد.

منابع

1. Adams W. W., Loustaunau P., "An introduction to Gröbner bases", American Mathematical Society (1994).

2. Anderson F. W., Fuller K. R., "Rings and Categories of Modules", second ed., Grad. Texts in Math., Vol. 13, Springer-Verlag, Berlin (1992).

3. Brandal W., "Commutative Rings Whose Finitely Generated Modules Decompose", Lecture Notes in Mathematics, 723, Springer, Berlin (1979).

4. Buchberger B., "Ein Algorithms zum Auffinden der Basiselemente des Restklassenrings nach einem nuildimensionalen Polynomideal", PhD thesis, Universität Innsbruck (1965).

5. Conti P., Traverso C., "Buchberger algorithm and integer programming", In Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes AAECC9 (H.F. Mattson, T. Mora, and T.R.N Rao eds.), Lecture Notes in Comput. Sci., Vol. 539, Springer verlag, Berlin and New York (1991) 130-139.

6. Dumas J-G., Giorgi P., Pernet C., "Dense linear Algebra over finite fields: the FFLAS and FFPACK packages", ACM Trans. Math. Softw., Vol. 35, Number 3 (2008)1-35.

7. Dumas J-G., Pernet C., Sultan Z., "Simultaneous computation of the row and column rank profiles, Proceedings of ISSAC’13", ACM Press, New York (2013) 181-188.

8. Dumas J-G., Saunders B. D., Villard G., "On efficient sparse integer matrix Smith normal form computations", Jounal of Symbolic Computation, Vol. 32, Number 1/2 (2001) 71-99.

9. Hungerford T. W., "Algebra, Springer-Verlag", New York-Berlin (1980).

10. Kaplansky I., "Elementary divisors and modules", Trans. Amer. Math. Soc. 66, (1949) 464-491.

11. Kapur D., Cai Y., "An algorithm for computing a Gröbner basis of a polynomial ideal over a ring with zero divisors", Mathematics in Computer Science, Vol. 2, Number 4, (2009) 601-634.

12. Shores T., Wiegand R., "Decompositions of modules and matrices", Bull. Amer. Math. Soc. 79 (6) (1973) 1277-1280.

13. Wiegand R., Wiegand S., "Commutative rings whose finitely generated modules are direct sums of cyclics", Abelian group theory (Proc. Second New Mexico State Univ. Conf., Las Cruces, N.M., 1976), Lecture Notes in Math., Vol. 616, Springer, Berlin, (1977) 406-423.