Глава 13

Въпрос 13: Теорема за елиминация и теорема за продължение

Да разгледаме идеал $I = \langle G \rangle \lhd k[x_1, \ldots, x_n]$ с крайна система пораждащи $G = \{g_1, \ldots, g_t\}$, $g_i \in k[x_1, \ldots, x_n]$. Тогава за всяко $1 \leq j \leq n-1$ сеченията $I_j := I \cap k[x_{j+1}, \ldots, x_n]$ се наричат елиминационни идеали на I. Аналогично, да разгледаме подмножествата $G_j := G \cap k[x_{j+1}, \ldots, x_n]$, за всяко $1 \leq j \leq n$. Ясно е, че $\langle G_j \rangle \subseteq I_j$ в $k[x_{j+1}, \ldots, x_n]$. Да означим с $V_j(G_j)$ и $V_j(I_j)$ афинните многообразия в k^{n-j}, определени от G_j, съответно, I_j. Тогава $V_j(I_j) \subseteq V_j(G_j)$. Афинното многообразие $V_{n-1}(G_{n-1}) \subseteq k$ съвпада с k за $G_{n-1} = \emptyset$. Ако G_{n-1} е непразното множество от полиноми на x_n, то $V_{n-1}(G_{n-1})$ има най-много краен брой елементи. По-нататък, естественото влагане $k[x_{j+1}, \ldots, x_n] \subset k[x_j, x_{j+1}, \ldots, x_n]$ се ограничава до включване $G_j \subseteq G_{j-1}$. Съответните афинни многообразия се оказват свързани с проекция

$$\mathrm{pr}_j : V_{j-1}(G_{j-1}) \longrightarrow V_j(G_j),$$

$$\mathrm{pr}_j(a_j, a') = a'.$$

Още повече,

$$V_{j-1}(G_{j-1}) = \{(a_j, a') \in k \times k^{n-j} \mid a' \in V_j(G_j),\ f(a_j, a') = 0 \ \text{ за } \forall f \in G_{j-1} \setminus G_j\}.$$

За $G_{j-1} = G_j$ имаме $V_{j-1}(G_{j-1}) = k \times V_j(G_j)$. Ако G_j е собствено подмножество на G_{j-1}, то слоевете на $\mathrm{pr}_j : V_{j-1}(G_{j-1}) \to V_j(G_j)$ са крайни.
Затова интерес представляват такива пораждащи системи G на $I = \langle G \rangle$, за които $\langle G_j \rangle = I_j$ при всички $1 \leq j \leq n-1$. Така наречената Теорема за елиминация 9 установява, че базисите на Грьобнер G на $I = \langle G \rangle$ относно лексикографската наредба имат това свойство. Преди да докажем тази Теорема да разгледаме следния

Пример 13.1. *Нека $I \lhd \mathbb{C}[x, y, z]$ е идеалът, породен от полиномите*

$$g_1 = x + y + z^2 - 1,$$

$$g_2 = y^2 - y - z^2 + z,$$

$$g_3 = 2yz^2 + z^4 - z^2,$$

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2.$$

Тогава

$$V_2(G_2) = V_2(g_4) = \{0,\ 1,\ -1 - \sqrt{2},\ -1 + \sqrt{2}\} \subset \mathbb{C},$$

$$V_1(G_1) = \{(0,0),\ (1,0),\ (0,1),\ (-1 - \sqrt{2}, -1 - \sqrt{2}),\ (-1 + \sqrt{2}, -1 + \sqrt{2})\} \subset \mathbb{C}^2,$$

а $V(G) = V(I)$ се състои от петте точки

$$(1,0,0), \quad (0,1,0), \quad (0,0,1),$$

$$(-1 - \sqrt{2}, -1 - \sqrt{2}, -1 - \sqrt{2}), \quad (-1 + \sqrt{2}, -1 + \sqrt{2}, -1 + \sqrt{2}).$$

Многообразието $V(I) = V(g_1, \ldots, g_4)$ се състои от решенията на системата уравнения

$$\left| \begin{array}{l} g_1 = 0 \\ \quad \ldots \\ g_4 = 0 \end{array} \right.$$

Описанието на $V(I)$ ще започнем с намиране на $V_2(G_2) = V_2(g_4) \subset \mathbb{C}$. След изнасяне на общ множител z^2 забелязваме, че $\frac{g_4}{z^2}$ има двоен корен $1 \in \mathbb{C}$ и разлагаме

$$g_4 = z^2(z-1)^2(z^2+2z-1).$$

Следователно

$$V_2(g_4) = \{0, \quad 1, \quad z_{3,4} = -1 \mp \sqrt{2}\}.$$

По-нататък, $G_1 = \{g_1, \ldots, g_4\} \cap \mathbb{C}[y,z] = \{g_2, g_3, g_4\}$, така че

$$V_1(G_1) = \{(y,z) \in \mathbb{C}^2 \mid z \in V_2(g_4), \quad g_2(y,z) = 0, \quad g_3(y,z) = 0\}.$$

По-точно, $g_2(y,0) = y(y-1) = 0$ и $g_3(y,0) = 0$ дават $(0,0), (1,0) \in V_1(G_1)$. Аналогично, $g_2(y,1) = y(y-1) = 0$ и $g_3(y,1) = 2y = 0$ определят $(0,1) \in V_1(G_1)$. За $z_i^2 = -2z_i + 1$, $3 \leq i \leq 4$ пресмятаме $g_3(y, z_i) = 2z_i^2(y - z_i) = 0$ и проверяваме, че $g_2(z_i, z_i) = 0$ за да стигнем до заключението, че $(z_i, z_i) \in V_1(G_1)$. По този начин,

$$V_1(G_1) = \{(0,0),\ (1,0),\ (0,1),\ (-1-\sqrt{2}, -1-\sqrt{2}),\ (-1+\sqrt{2}, -1+\sqrt{2})\}.$$

Сега описанието на

$$V(I) = \{(x,y,z) \in \mathbb{C}^3 \mid (y,z) \in V_1(G_1),\ g_1(x,y,z) = 0\}$$

се свежда до решаването на уравнението $x = -y - z^2 + 1$ за $\forall (y,z) \in V_1(G_1)$.

Теорема 9. *Нека G е базис на Грьобнер на идеала $I = \langle G \rangle \lhd k[x_1, \ldots, x_n]$ относно лексикографската наредба $>_{\text{lex}}$. Тогава за всяко $1 \leq j \leq n-1$ сечението*

$$G_j = G \cap k[x_{j+1}, \ldots, x_n]$$

е базис на Грьобнер на j-тия елиминационен идеал

$$I_j = I \cap k[x_{j+1}, \ldots, x_n].$$

В частност, $I_j = \langle G_j \rangle$.

Доказателство: След евентуална пермутация на елементите $g_1, \ldots, g_t$ на базиса на Грьобнер G на I можем да считаме, че $G_j = \{g_1, \ldots, g_r\}$ за произволно фиксирано $1 \leq j \leq n-1$. Първо ще докажем, че G_j поражда I_j. Доколкото $\langle G_j \rangle \subseteq I_j$, достатъчно е да установим, че всеки полином $f \in I_j$ има нулев остатък при деление с G_j. За целта да отбележим, че f принадлежи на идеала I с базис на Грьобнер G, така че $\overline{f}^G = 0$. С други думи, $f(x_{j+1}, \ldots, x_n) = \sum_{i=1}^{t} g_i h_i$ за някакви полиноми $h_i \in k[x_1, \ldots, x_n]$. Твърдим, че $h_{r+1} = \ldots = h_t = 0$ и $h_1, \ldots, h_r \in k[x_{j+1}, \ldots, x_n]$. Това се дължи на факта, че $g_{r+1}, \ldots, g_t \notin k[x_{j+1}, \ldots, x_n]$, така че старшите членове $LT(g_{r+1}), \ldots, LT(g_t)$ се делят на поне една от променливите $x_1, \ldots, x_j$. При първата стъпка от делението, нито един моном на f не се дели на $LT(g_{r+1}), \ldots, LT(g_t)$, така че текущите частни са нулеви. При деление на $f \in k[x_{j+1}, \ldots, x_n]$ с някой от полиномите $g_1 \ldots, g_r \in k[x_{j+1}, \ldots, x_n]$, частното е моном от $k[x_{j+1}, \ldots, x_n]$. В резултат, текущото делимо се модифицира до полином от $k[x_{j+1}, \ldots, x_n]$ и горното разсъждение продължава да е в сила. По този начин, при деление на $f \in I_j$ с G получаваме $f = \sum_{i=1}^{r} g_i h_i$ за подходящи полиноми $h_i \in k[x_{j+1}, \ldots, x_n]$. С други думи, делението на f с G в $k[x_1, \ldots, x_n]$ съвпада с делението на f с G_j в $k[x_{j+1}, \ldots, x_n]$ и $f \in \langle G_j \rangle$. Това установява, съвпадението $I_j = \langle G_j \rangle$.

Съгласно Теорема 5, пораждащата система G_j на I_j е базис на Грьобнер на този идеал тогава и само тогава, когато $\overline{S(g_p,g_q)}^{G_j}=0$ за всички $1\leq p<q\leq r$. Доколкото G е базис на Грьобнер на $I=\langle G\rangle$, остатъците $\overline{S(g_p,g_q)}^{G}=0$ за всички $1\leq p<q\leq r$. С други думи, $S(g_p,g_q)=\sum_{i=1}^{t}g_ih_i^{(p,q)}$ за подходящи полиноми $h_i^{(p,q)}\in k[x_1,\ldots,x_n]$. Както при доказателството на $I_j\subseteq\langle G_j\rangle$, частните $h_i^{(p,q)}=0$ се анулират за $r+1\leq i\leq t$, а частните $h_1^{(p,q)},\ldots,h_r^{(p,q)}\in k[x_{j+1},\ldots,x_n]$ не зависят от $x_1,\ldots,x_j$, така че $S(g_p,g_q)=\sum_{i=1}^{r}g_ih_i^{(p,q)}$ съвпада с резултата от делението на $S(g_p,g_q)$ с G_j в $k[x_{j+1},\ldots,x_n]$. По този начин, $\overline{S(g_p,g_q)}^{G_j}=0$ за всички $1\leq p<q\leq r$ и G_j се оказва базис на Грьобнер на I_j относно $>_{\text{lex}}$, Q.E.D.

Точките $a=(a_1,\ldots,a_n)\in V(I)$ се наричат пълни решения на идеала $I\lhd k[x_1,\ldots,x_n]$ или на произволна система от негови пораждащи. За всяко $1\leq j\leq n-1$ казваме, че точките $(a_{j+1},\ldots,a_n)\in V_j(I_j)$ са частични решения на I. Теоремата за пордължение дава достатъчни условия за продължимост на $(a_{j+1},\ldots,a_n)\in V_j(I_j)$ до $(a_j,a_{j+1},\ldots,a_n)\in V_{j-1}(I_{j-1})$. Без ограничение на общността можем да считаме, че $j=1$ и да формулираме теоремата като условие за продължимост на частично решение $(a_2,\ldots,a_n)\in V_1(I_1)$ до пълно решение $(a_1,a_2,\ldots,a_n)\in V(I)$. Преди да разгледаме Теоремата за продължение, да се спрем на следния

Пример 13.2. *Нека I е идеалът в $\mathbb{C}[x,y,z]$, породен от полиномите $f=xy-1$ и $g=xz-1$. Тогава*

$$V_1(I_1)=\{(a,a)\,|\,a\in\mathbb{C}\}$$

и частичните решения $(a,a)\in V_1(I_1)$ с $a\in\mathbb{C}^*$ се продължават до пълни решения $\left(\frac{1}{a},a,a\right)\in V(I)$, докато частичното решение $(0,0)\in V_1(I_1)$ не се продължава до пълно решение.

Относно лексикографската наредба, най-малкото общо кратно

$$LCM(LM(f),LM(g))=LCM(xy,xz)=xyz,$$

така че S-полиномът

$$S(f,g)=z(xy-1)-y(xz-1)=y-z\in\langle f,g\rangle\cap\mathbb{C}[y,z]=I_1.$$

Следователно $\langle y-z\rangle\subseteq I_1$ и $V_1(y-z)=\{(a,a)\,|\,a\in\mathbb{C}\}\supseteq V_1(I_1)$. От друга страна,

$$V(I)=V(f,g)=\left\{\left(\frac{1}{a},a,a\right)\,\middle|\,a\in\mathbb{C}^*\right\}$$

се проектира във $V_1(I_1)$, откъдето следва, че $V_1(I_1)\supseteq V_1(y-z)\setminus\{(0,0)\}$. Доколкото $V_1(y-z)$ и $V_1(I_1)$ са афинни многообразия, а $V_1(y-z)\setminus\{(0,0)\}$ не е афинно многообразие, стигаме до извода, че $V_1(y-z)=V_1(I_1)$. В частичните решения $(a,a)\in V_1(I_1)$ с $a\in\mathbb{C}^*$ полиномите $f(x,a,a)=ax-1$ и $g(x,a,a)=ax-1$ имат ненулеви старши коефициенти и имат общ корен $x=\frac{1}{a}$. Това дава пълното решение $\left(\frac{1}{a},a,a\right)\in V(I)$. Полиномите $f(x,0,0)=-1$ и $g(x,0,0)=-1$ не се анулират в нито едно комплексно число, така че частичното решение $(0,0)\in V_1(I_1)$ не се продължава до пълно решение.

Сега ще докажем Теоремата за продължение:

Теорема 10. *Нека k е алгебрично затворено поле,*

$$f_i=\sum_{j=0}^{N_i}f_{i,j}x_1^j\in k[x_1,x_2,\ldots,x_n]$$

са полиноми на x_1 *от степен* $N_i \in \mathbb{N}$ *относно* x_1 *с коефициенти* $f_{i,j} \in k[x_2, \ldots, x_n]$, $f_{i,N_i} \not\equiv 0$ *за* $1 \leq i \leq s$. *Ако* $I_1 = I \cap k[x_2, \ldots, x_n]$ *е първият елиминационен идеал на* $I = \langle f_1, \ldots, f_s \rangle \lhd k[x_1, x_2, \ldots, x_n]$, *то всяко частично решение*

$$c = (c_2, \ldots, c_n) \in V_1(I_1) \setminus V(f_{i,N_i} \,|\, 1 \leq i \leq s)$$

се продължава до пълно решение

$$(c_1, c) = (c_1, c_2, \ldots, c_n) \in V(I).$$

Доказателство: Вземайки предвид, че $\langle f_1 \rangle = \langle f_1, f_1, f_1 \rangle$ и $\langle f_1, f_2 \rangle = \langle f_1, f_2, f_2 \rangle$, можем да считаме, че идеалът $I = \langle f_1, \ldots, f_s \rangle$ се поражда от $s \geq 3$ полинома. За всяко $c \in V_1(I_1) \setminus V(f_{i,N_i} \,|\, 1 \leq i \leq s)$ трябва да установим съществуването на решение $c_1 \in k$ на системата полиномиални уравнения

$$\left| \begin{array}{l} f_1(x_1, c) = 0 \\ \quad \ldots \\ f_s(x_1, c) = 0 \end{array} \right. \tag{13.1}$$

Съгласно $c \notin V(f_{i,N_i} \,|\, 1 \leq i \leq s)$ можем да считаме, че $f_{1,N_1}(c) \neq 0 \in k$, след евентуална пермутация на полиномите $f_1, f_2, \ldots, f_s$. Да въведем нови променливи $u_2, \ldots, u_s$ и да разгледаме резултантата

$$h(u_2, \ldots, u_s, x_2, \ldots, x_n) := \operatorname{Res}\left(f_1, \sum_{i=2}^{s} u_i f_i, x_1\right) \in k[u_2, \ldots, u_s, x_2, \ldots, x_n]$$

относно x_1. Съгласно Твърдение 12.3, съществуват полиноми

$$A, B \in \mathbb{Z}[f_{1,j}, \sum_{i=2}^{s} u_i f_{i,j}][x_1] \subseteq k[u_2, \ldots, u_s, x_2, \ldots, x_n][x_1],$$

така че

$$Af_1 + B\left(\sum_{i=2}^{s} u_i f_i\right) = h.$$

Представяме

$$A = \sum_{\alpha \in P} A_\alpha u^\alpha, \quad B = \sum_{\beta \in Q} B_\beta u^\beta, \quad h = \sum_{\mu \in M} h_\mu u^\mu$$

като полиноми на $u_2, \ldots, u_s$ с коефициенти $A_\alpha, B_\beta \in k[x_2, \ldots, x_2][x_1]$, $h_\mu \in k[x_2, \ldots, x_n]$ и сравняваме коефициентите на u^μ в равенството

$$\left(\sum_{\alpha \in P} u^\alpha\right) f_1 + \left(\sum_{\beta \in Q} B_\beta u^\beta\right)\left(\sum_{i=2}^{s} u_i f_i\right) = \sum_{\mu \in M} h_\mu u^\mu.$$

За целта въвеждаме наредените $(s-1)$-торки e_i с единствена ненулева координата 1 на място $i-1$ и изразяваме $u_i = u^{e_i}$ за всички $2 \leq i \leq s$. Тогава

$$A\mu f_1 + \sum_{\beta + e_i} B_\beta f_i = h_\mu$$

за всяко $\mu \in M$ показва, че $h_\mu \in \langle f_1, \ldots, f_s \rangle \lhd k[u_2, \ldots, u_s, x_1, x_2, \ldots, x_n]$. Освен това, $h_\mu \in k[x_2, \ldots, x_n]$, така че $h_\mu \in I_1$ за всички $\mu \in M$. Следователно за $c \in V_1(I_1)$ получаваме, че $h_\mu(c) = 0$, откъдето

$$h(u_2, \ldots, u_s, c,) = \operatorname{Res}\left(f_1, \sum_{i=2}^{s} u_i f_i, x_1\right)(c) = 0.$$

Старшият коефициент $f_{1,N_1}(c) \neq 0$ на f_1 относно x_1 не се анулира в c. Ако $N_2 > \max(N_3, \ldots, N_s)$ и $f_{2,N_2}(c) \neq 0$, то старшият коефициент $u_2 f_{2,N_2}(c) \neq 0$ на $u_2 f_2 + \ldots + u_s f_s$ относно x_1 не се анулира и

$$\operatorname{Res}\left(f_1(x_1, c), \sum_{i=2}^{s} u_i f_i(x_1, c), x_1\right) = \operatorname{Res}\left(f_1, \sum_{i=2}^{s} u_i f_i, x_1\right)(c) = 0.$$

Следователно полиномите

$$f_1(x_1, c), \sum_{i=2}^{s} u_i f_i(x_1, c) \in k[x_1, u_2, \ldots, u_s]$$

имат общ делител $F(x_1, u_2, \ldots, u_s)$ от степен $\deg_{x_1} F \geq 1$. Още повече, $F = F(x_1)$ не зависи от $u_2, \ldots, u_s$, защото $F(x_1)$ дели $f_1(x_1, c)$. Непостоянният полином $F(x_1)$ има корен $c_1 \in k$ съгласно алгебричната затвореност на полето k. Тогава $f_1(c_1, c) = 0$ и $\sum_{i=2}^{s} u_i f_i(c_1, c) = 0$ за произволни $u_2, \ldots, u_s$. В резултат, $f_i(c_1, c) = 0$ за всички $2 \leq i \leq s$ и (13.1) има решение $x_1 = c_1$.
Ако $N_2 \leq \max(N_3, \ldots, N_s)$ или $f_{2,N_2}(c) = 0$, то заменяме полиномите $f_1, f_2, f_3, \ldots, f_s$ с $f_1, f_2 + x_1^N f_1, f_3, \ldots, f_s$ и забелязваме, че

$$I = \langle f_1, f_2, f_3, \ldots, f_s \rangle = \langle f_1, f_2 + x_1^N f_1, f_3, \ldots, f_s \rangle$$

за произволно естествено N. За достатъчно голямо N е в сила $N + N_1 > \max(N_2, N_3, \ldots, N_s)$ и старшият коефициент $f_{1,N_1}(c) \neq 0$ на $f_2 + x_1^N f_1$ относно x_1 не се анулира в c. Съгласно направените разсъждения следва съществуването на пълно решение $(c_1, c) \in V(I)$, Q.E.D.