Rezultante polinoma i sustavi polinomijalnih jednadžbi[†]

Tomislav Pejković

11.7.2007.

Sadržaj

1 Rezultanta dvaju polinoma

Ako su dana dva polinoma $f, g \in k[x]$ pozitivnog stupnja, npr.

$$\begin{aligned} f &= a_0x^l + \cdots + a_l, \quad a_0 \neq 0, \quad l > 0 \\ g &= b_0x^m + \cdots + b_m, \quad b_0 \neq 0, \quad m > 0. \end{aligned} \tag{1}$$

tada je *rezultanta* od f i g, u oznaci $\mathrm{Res}(f, g)$, determinanta tipa $(l+m) \times (l+m)$

$$\mathrm{Res}(f,g) = \det \begin{bmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & a_2 & \ddots & a_0 & \vdots & b_2 & \ddots & b_0 \\ a_l & \vdots & \ddots & a_1 & b_m & \vdots & \ddots & b_1 \\ & a_l & & a_2 & & b_m & & b_2 \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_l & & & & b_m \end{bmatrix}, \tag{2}$$

[†]predavanje održano na Seminaru za teoriju brojeva i algebru

gdje su na praznim mjestima nule. Kada želimo naglasiti ovisnost o x, pišemo $\mathrm{Res}(f, g, x)$ umjesto $\mathrm{Res}(f, g)$. Jedan jednostavan primjer je

$$\mathrm{Res}(x^3 + 5x - 1, 2x^2 - 3x + 6) = \begin{vmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & -3 & 2 & 0 \\ 5 & 0 & 6 & -3 & 2 \\ -1 & 5 & 0 & 6 & -3 \\ 0 & -1 & 0 & 0 & 6 \end{vmatrix} = 395 \tag{3}$$

Tri osnovna svojstva rezultante su

- (Cjelobrojni polinom) $\mathrm{Res}(f, g)$ je cjelobrojni polinom u koeficijentima od f i g.
- (Zajednički faktor) $\mathrm{Res}(f, g) = 0$ ako i samo ako f i g imaju zajednički faktor u $k[x]$.
- (Eliminacija) Postoje polinomi $A, B \in k[x]$ takvi da je $Af + Bg = \mathrm{Res}(f, g)$. Koeficijenti od A i B su cjelobrojni polinomi u koeficijentima od f i g.

Uskoro ćemo dati skicu dokaza druga dva svojstva (prvo je jasno iz definicije rezultante), ali najprije objasnimo što ova svojstva govore. Prvo svojstvo kaže da postoji polinom

$$\mathrm{Res}_{l,m} \in \mathbb{Z}[u_0, \ldots, u_l, v_0, \ldots, v_m]$$

takav da za f i g kao u (1) imamo

$$\mathrm{Res}(f, g) = \mathrm{Res}_{l,m}(a_0, \ldots, a_l, b_0, \ldots, b_m).$$

Ako radimo nad skupom kompleksnih brojeva, onda svojstvo zajedničkog faktora znači da $f, g \in \mathbb{C}[x]$ imaju zajednički korijen ako i samo ako im je rezultanta jednaka 0. Tako nam primjer u (3) pokazuje da $x^3 + 5x - 1$ i $2x^2 - 3x + 6$ nemaju isti korijen u $\mathbb{C}$ jer je $395 \neq 0$ iako ne znamo koji su korijeni tih polinoma.

Da bismo razumjeli svojstvo eliminacije, pogledajmo kako se rezultante mogu koristiti za elimininiranje varijabli iz sustava jednadžbi na jednom jednostavnom primjeru

$$\begin{aligned} f &= xy - 1 = 0 \\ g &= x^2 + y^2 - 4 = 0. \end{aligned}$$

Ovdje imamo dvije varijable, ali ako promotrimo f i g kao polinome u x čiji koeficijenti su polinomi u y, možemo izračunati rezultantu s obzirom na varijablu x:

$$\mathrm{Res}(f, g, x) = \begin{vmatrix} y & 0 & 1 \\ -1 & y & 0 \\ 0 & -1 & y^2 - 4 \end{vmatrix} = y^4 - 4y^2 + 1.$$

Prema eliminacijskom svojstvu, postoje polinomi $A, B \in k[x, y]$ takvi da je $A \cdot (xy - 1) + B \cdot (x^2 + y^2 - 4) = y^4 - 4y^2 + 1$. Slijedi da $y^4 - 4y^2 + 1$ iščezava za svako rješenje sustava $f = g = 0$. Zato rješavanjem $y^4 - 4y^2 + 1 = 0$ dobivamo y kooordinate rješenja.

Rezultante su zanimljive među ostalim i zato što se mogu izraziti na različite načine.

Propozicija 1. *Neka su polinomi f i g kao u (1) i neka su im korijeni $\xi_1, \ldots, \xi_l$ i $\eta_1, \ldots, \eta_m$, respektivno (možda u nekom većem polju). Tada vrijedi*

$$\begin{aligned} \operatorname{Res}(f,g) &= a_0^m b_0^l \prod_{i=1}^{l}\prod_{j=1}^{m}(\xi_i - \eta_j) \\ &= a_0^m \prod_{i=1}^{l} g(\xi_i) \qquad\qquad i \\ &= (-1)^{lm} b_0^l \prod_{j=1}^{m} f(\eta_j); \end{aligned} \tag{4}$$

$$\begin{aligned} \operatorname{Res}(g,f) &= (-1)^{lm} \operatorname{Res}(f,g), \\ \operatorname{Res}(f,g) &= (-1)^{lm} b_0^{l-\deg(r)} \operatorname{Res}(g,r), \end{aligned} \tag{5}$$

pri čemu je r ostatak pri dijeljenju f sa g, $f = gq + r$, $\deg(r) < \deg(g)$, a za $r = 0$ je $\operatorname{Res}(f,g) = 0$.

Sve formule navedene u (4) i (5), ali i svojstvo zajedničkog faktora vrlo jednostavno slijede iz prve, pa ćemo samo nju i dokazati. Primjetimo još da nam formule u (5) daju efikasan algoritam za računanje rezultante dvaju polinoma (postupak je kao u Euklidovom algoritmu).

Dokaz prve formule u (4) [Es 01]. Kako bismo tvrdnju dokazali sasvim općenito, promatrat ćemo f i g kao polinome s koeficijentima u prstenu $\mathbb{Z}[\xi_1, \ldots, \xi_l, \eta_1, \ldots, \eta_m]$, tj. možemo umjesto korijena polinoma f i g staviti nezavisne varijable (koje u dokazu jednako označavamo). Vrijedi

$$\begin{aligned} f &= a_0 \prod_{1 \le i \le l} (x - \xi_i) = a_0 x^l + \cdots + a_l, \\ g &= b_0 \prod_{1 \le j \le m} (x - \eta_j) = b_0 x^m + \cdots + b_m. \end{aligned}$$

Označimo za $N \in \mathbb{N}$ s $V(T_1, \ldots, T_N)$ takozvanu *Vandermondeovu determinantu* kvadratne matrice $M(T_1, \ldots, T_N)$ dimenzije N s elementima u $\mathbb{Z}[T_1, \ldots, T_N]$ kojoj je k-ti red dan sa $(T_k)^{N-1}, \ldots, (T_k)^2, T_k, 1$ $(1 \le k \le N)$. Prisjetimo se da je

$$V(T_1, \ldots, T_N) = \prod_{1 \le i < j \le N} (T_i - T_j).$$

Definirajmo sada $M = M(\eta_1, \ldots, \eta_m, \xi_1, \ldots, \xi_l)$ i neka je Δ matrica iz (2), tj. $\operatorname{Res}(f,g) = \det \Delta$. Primjetimo da je $f(\eta_j) = \sum_{0 \le k \le l} a_k (\eta_j)^{l-k}$ za $1 \le j \le m$, $f(\xi_j) = 0$ za $1 \le j \le l$, $g(\xi_j) = \sum_{0 \le k \le m} b_k (\xi_j)^{m-k}$ za $1 \le j \le l$, $g(\eta_j) = 0$ za $1 \le j \le m$.

Izračunat ćemo determinantu produkta $M\Delta$ na dva različita načina. U $\det(M\Delta)$ za $1 \le j \le m$ je $f(\eta_j)$ faktor u čitavom j-tom retku, a za $m+1 \le j \le m+l$ je $g(\xi_{j-m})$ faktor u čitavom j-tom retku, pa nakon izlučivanja tih veličina dobivamo

determinantu koju možemo izračunati kao produkt determinanti dvaju blokova, a obje ove determinante su Vandermondeove. Imamo

$$\det(M\Delta) = \prod_{1\le j\le m} f(\eta_j) \prod_{1\le i\le l} g(\xi_i) V(\xi_1,\dots,\xi_l) V(\eta_1,\dots,\eta_m).$$

Usporedimo li ovo s umnoškom $\det(M)\det(\Delta)$, dobivamo

$$\prod_{1\le j\le m} f(\eta_j) \prod_{1\le i\le l} g(\xi_i) V(\xi_1,\dots,\xi_l) V(\eta_1,\dots,\eta_m) = \mathrm{Res}(f,g) V(\eta_1,\dots,\eta_m,\xi_1,\dots,\xi_l).$$

Vrijedi

$$V(\eta_1,\dots,\eta_m,\xi_1,\dots,\xi_l) = V(\xi_1,\dots,\xi_l)V(\eta_1,\dots,\eta_m) \prod_{\substack{1\le i\le l\\ 1\le j\le m}} (\eta_j - \xi_i).$$

Zato je

$$\prod_{1\le j\le m} f(\eta_j) \prod_{1\le i\le l} g(\xi_i) = \mathrm{Res}(f,g) \prod_{\substack{1\le i\le l\\ 1\le j\le m}} (\eta_j - \xi_i).$$

Tvrdnju konačno dobivamo skratimo li prethodnu jednakost s $\prod_{\substack{1\le i\le l\\ 1\le j\le m}} (\eta_j - \xi_i)$ koristeći pri tome da je

$$f(\eta_j) = a_0 \prod_{1\le i\le l} (\eta_j - \xi_i) \quad \text{i} \quad g(\xi_i) = b_0 \prod_{1\le j\le m} (\xi_i - \eta_j).$$

□

Dokažimo sada i svojstvo eliminacije kako je ranije iskazano.

Dokaz svojstva eliminacije [La 02]. Promatramo ponovno polinome f i g kao u (1), ali nam sada $a_0,\dots,a_l,b_0,\dots,b_m$ označavaju veličine algebarski nezavisne nad $\mathbb{Z}$. (Točnije bi bilo uvesti nove polinome s novim koeficijentima koji imaju to svojstvo, a onda "stare" f i g dobivamo tako da umjesto koeficijenata "novih" f i g uvrstimo konkretne elemente $a_0,\dots,a_l,b_0,\dots,b_m$ iz k. Ipak zadržavamo stare oznake radi jednostavnosti pisanja.)

U sustavu linearnih jednadžbi

$$\begin{aligned}
x^{m-1}f(x) &= a_0x^{l+m-1} + a_1x^{l+m-2} + \cdots + a_lx^{m-1}\\
x^{m-2}f(x) &= \qquad a_0x^{l+m-2} + \ \cdots\ + a_lx^{m-2}\\
&\ \ \vdots\\
f(x) &= \qquad\qquad\qquad a_0x^{l} + \ \cdots\qquad + a_l\\
x^{l-1}g(x) &= b_0x^{l+m-1} + b_1x^{l+m-2} + \cdots + b_mx^{l-1}\\
x^{l-2}g(x) &= \qquad b_0x^{l+m-2} + \ \cdots\ + b_mx^{l-2}\\
&\ \ \vdots\\
g(x) &= \qquad\qquad\qquad b_0x^{m} + \ \cdots\qquad + b_m
\end{aligned}$$

označimo s C vektor stupac na lijevoj strani, a sa $C_0, \ldots, C_{l+m}$ stupčane vektore koeficijenata. Našu jednadžbu tada možemo zapisati

$$C = x^{l+m-1}C_0 + \cdots + 1 \cdot C_{l+m}.$$

Primjenimo sad Cramerovo pravilo na zadnji koeficijent koji je jednak 1 i dobivamo

$$\mathrm{Res}(f,g) = \det(C_0, \ldots, C_{l+m}) = \det(C_0, \ldots, C_{l+m-1}, C).$$

Odavdje vidimo da postoje polinomi A i B u $\mathbb{Z}[a_0, \ldots, a_l, b_0, \ldots, b_m][x]$ takvi da je

$$Af + Bg = \mathrm{Res}(f,g).$$

□

Formule dane u (4) izgledaju nepraktične za upotrebu jer uključuju korijene od f i g. No, postoji jednostavan način za računanje navedenih produkata. Primjerice, formula $\mathrm{Res}(f,g) = a_0^m \prod_{i=1}^{l} g(\xi_i)$ nam govori da rezultantu možemo dobiti kao umnožak svojstvenih vrijednosti jednog linearnog preslikavanja (do na faktor a_0^m). Objasnimo ukratko o čemu se radi. Promatrajmo kvocijentni prsten $A_f = k[x]/\langle f \rangle$ i neka je preslikavanje m_g definirano na sljedeći način

$$m_g([h]) = [g] \cdot [h] = [gh] \in A_f,$$

gdje je $[h] \in A_f$ susjedna klasa od $h \in k[x]$. Ako na A_f gledamo kao na skup svih polinoma h stupnja $< l$, možemo interpretirati $m_g(h)$ kao ostatak pri dijeljenju gh s f. Takav pogled omogućuje nam sljedeći način računanja $\mathrm{Res}(f,g)$.

Propozicija 2. *$Res(f,g) = a_0^m \det(m_g : A_f \to A_f)$.*

Dokaz. v. [CLO 05, str. 74] □

Primjer. Za $f = x^3 + 5x - 1$ i $g = 2x^2 - 3x + 6$ kao u (3), gledajući na A_f preko ostataka pri dijeljenju s f i koristeći bazu $\{1, x, x^2\}$ od A_f imamo

$$\mathrm{Res}(f,g) = 1^2 \det(m_g) = \begin{vmatrix} 6 & 2 & -3 \\ -3 & -4 & 17 \\ 2 & -3 & -4 \end{vmatrix} = 395.$$

Primjetimo da je 3×3 determinanta u ovom primjeru manja od 5×5 determinante iz definicije (2). Općenito, propozicija 2 nam govori da $\mathrm{Res}(f,g)$ možemo prikazati kao $l \times l$ determinantu, dok se u definiciji rezultante koristi $(l+m) \times (l+m)$ matrica. Zamijenom f i g, vidimo da rezultantu možemo prikazati korištenjem $m \times m$ determinante.

Kako bismo mogli prijeći na rezultante više polinoma u više varijabli, moramo sada napraviti jednu malu modifikaciju u definiciji rezultante. Naime, umjesto uporabe polinoma u jednoj varijabli x, možemo koristiti *homogene* polinome u varijablama x, y. (Podsjetimo se da je polinom homogen ako mu je svaki član istog stupnja.) Ako su $F, G \in k[x,y]$ homogeni polinomi (ukupnog ili totalnog) stupnja l, m, respektivno, onda možemo pisati

$$\begin{aligned} F &= a_0x^l + a_1x^{l-1}y + \cdots + a_ly^l \\ G &= b_0x^m + b_1x^{m-1}y + \cdots + b_my^m. \end{aligned} \tag{6}$$

Primjetimo da a_0 ili b_0 (ili oba) mogu biti nula. Definiramo $\mathrm{Res}(F,G) \in k$ upotrebom iste determinante kao u (2).

Ako homogeniziramo polinome f i g iz (1) upotrebom prikladnih potencija od y, dobivamo F i G iz (6) i tada je očito $\mathrm{Res}(f,g) = \mathrm{Res}(F,G)$. Krenemo li u suprotnom smijeru, zaključivanje više nije toliko jednostavno. Ako su F i G dani sa (6), onda možemo dehomogenizirati polinome uvrštavanjem $y = 1$, no na taj način možda nećemo dobiti polinome traženog stupnja jer a_0 ili b_0 može biti nula. Usprkos tome rezultanta $\mathrm{Res}(F,G)$ i dalje zadovoljava neka osnovna svojstva.

Propozicija 3. *Neka su l i m prirodni brojevi.*

a. *Postoji polinom $\mathrm{Res}_{l,m} \in \mathbb{Z}[u_0,\ldots,u_l,v_0,\ldots,v_m]$ takav da je*

$$\mathrm{Res}(F,G) = \mathrm{Res}_{l,m}(a_0,\ldots,a_l,b_0,\ldots,b_m)$$

za sve F,G kao u (6).

b. *Nad poljem kompleksnih brojeva $\mathrm{Res}(F,G) = 0$ ako i samo ako jednadžbe $F = G = 0$ imaju rješenje $(x,y) \neq (0,0)$ u $\mathbb{C}^2$ (takvo rješenje zovemo* netrivijalno*).*

Dokaz. V. [CLO 05, str. 75] □

Primjer. Kao primjer kako se rezultante mogu koristiti za eliminiranje varijabli iz jednadžbi, promotrimo parametarske jednadžbe

$$\begin{aligned} x &= 1 + s + t + st \\ y &= 2 + s + st + t^2 \\ z &= s + t + s^2. \end{aligned}$$

Želimo eliminirati s,t iz ovih jednadžbi kako bismo dobili jednadžbu koja sadrži samo x,y,z. Stavimo

$$\begin{aligned} f &= 1 + s + t + st - x \\ g &= 2 + s + st + t^2 - y \\ h &= s + t + s^2 - z. \end{aligned}$$

Najprije eliminiramo t:

$$\begin{aligned} \mathrm{Res}(f,g,t) &= 3 + 6\,s + 3\,s^2 - 2\,x - s\,x + s^2\,x + x^2 - y - 2\,s\,y - s^2\,y \\ \mathrm{Res}(f,h,t) &= -1 + 2\,s^2 + s^3 + x - z - s\,z. \end{aligned}$$

Zatim eliminiramo s:

$$\begin{aligned} p = \mathrm{Res}(\mathrm{Res}(f,g,t),\mathrm{Res}(f,h,t),s) =& 9\,x^2 + 15\,x^3 + 13\,x^4 - 6\,x^5 + x^6 \\ & - 15\,x^2\,y - 20\,x^3\,y - x^4\,y + 7\,x^2\,y^2 + 5\,x^3\,y^2 \\ & - x^2\,y^3 - 9\,x^2\,z + 3\,x^3\,z - x^4\,z + 2\,x^5\,z \\ & + 6\,x^2\,y\,z - x^3\,y\,z - 2\,x^4\,y\,z - x^2\,y^2\,z + 9\,x^2\,z^2 \\ & + 6\,x^3\,z^2 + x^4\,z^2 - 6\,x^2\,y\,z^2 - 2\,x^3\,y\,z^2 + x^2\,y^2\,z^2. \end{aligned}$$

2 Multipolinomijalne rezultante

U prvom dijelu proučavali smo rezultante dvaju homogenih polinoma F, G u varijablama x, y. Kako bismo generalizirali ta razmatranja, pretpostavimo da imamo $n+1$ homogenih polinoma $F_0, \ldots, F_n$ u varijablama $x_0, \ldots, x_n$ i neka svaki polinom F_i ima pozitivan (ukupni) stupanj. Tada dobivamo $n+1$ jednadžbu u $n+1$ nepoznanici

$$F_0(x_0, \ldots, x_n) = \cdots = F_n(x_0, \ldots, x_n) = 0. \tag{7}$$

Budući da su F_i homogeni pozitivnog stupnja, ove jednadžbe uvijek imaju rješenje $x_0 = \cdots = x_n = 0$, koje zovemo *trivijalno* rješenje. Zato je ključno pitanje postoje li *netrivijalna* rješenja. U nastavku ćemo raditi nad poljem kompleksnih brojeva, pa su netrivijalna rješenja točke iz $\mathbb{C}^{n+1} \setminus \{(0, \ldots, 0)\}$.

Općenito, postojanje netrivijalnih rješenja ovisi o koeficijentima polinoma $F_0, \ldots, F_n$; za većinu vrijednosti koeficijenata nema netrivijalnih rješenja, a za određene specijalne vrijednosti, takva rješenja postoje.

Jedan slučaj u kojem se to lagano vidi je kad su svi polinomi F_i linearni, tj. stupnja 1. Kako su svi homogeni, jednadžbe (7) možemo napisati u sljedećem obliku

$$\begin{aligned} F_0 &= c_{00}x_0 + \cdots + c_{0n}x_n = 0 \\ &\vdots \\ F_n &= c_{n0}x_0 + \cdots + c_{nn}x_n = 0. \end{aligned} \tag{8}$$

Ovo je $(n+1) \times (n+1)$ sustav linearnih jednadžbi, pa znamo da netrivijalno rješenje postoji ako i samo ako je determinanta matrice sustava jednaka nula. Tako smo dobili *jedan* uvjet $\det(c_{ij}) = 0$ za postojanje netrivijalnih rješenja. Primjetimo da je ova determinanta polinom u koeficijentima c_{ij}.

Općenito, kad imamo $n+1$ homogenih polinoma $F_0, \ldots, F_n \in \mathbb{C}[x_0, \ldots, x_n]$, postavlja se temeljno pitanje: *Koje uvjete moraju zadovoljavati koeficijenti od $F_0, \ldots, F_n$ da bi $F_0 = \cdots = F_n = 0$ imao netrivijalno rješenje?* Kako bismo precizno odgovorili na ovo pitanje, moramo najprije uvesti neke oznake. Neka je d_i (ukupni) stupanj od F_i, tako da možemo pisati

$$F_i = \sum_{|\alpha| = d_i} c_{i,\alpha} x^\alpha. \qquad \text{(koristimo multiindekse)}$$

Za svaki par indeksā i, α, uvodimo varijablu $u_{i,\alpha}$. Ako je polinom $P \in \mathbb{C}[u_{i,\alpha}]$, onda s $P(F_0, \ldots, F_n)$ označavamo broj dobiven zamjenom svake varijable $u_{i,\alpha}$ u P s odgovarajućim koeficijentom $c_{i,\alpha}$. Ovo je značenje izraza *polinom u koeficijentima od F_i*. Sada možemo odgovoriti na naše temeljno pitanje.

Teorem 4 (Mertens 1899.)**.** *Ako fiksiramo pozitivne stupnjeve $d_0, \ldots, d_n$, tada postoji jedinstveni polinom* $\mathrm{Res} \in \mathbb{Z}[u_{i,\alpha}]$ *koji ima sljedeća svojstva:*

a. *Ako su $F_0, \ldots, F_n \in \mathbb{C}[x_0, \ldots, x_n]$ homogeni polinomi redom stupnja $d_0, \ldots, d_n$, onda sustav jednadžbi* (7) *ima netrivijalno rješenje nad $\mathbb{C}$ ako i samo ako je* $\mathrm{Res}(F_0, \ldots, F_n) = 0$.

b. $\mathrm{Res}(x_0^{d_0}, \ldots, x_n^{d_n}) = 1$.

c. Res *je ireducibilan polinom, čak i ako ga promatramo kao polinom u* $\mathbb{C}[u_{i,\alpha}]$.

Dokaz. Dokaz pogledajte u [GKZ 94], usp. i [S 82, Sch 76]. □

Izraz $\mathrm{Res}(F_0, \ldots, F_n)$ zovemo *rezultanta* od $F_0 \ldots, F_n$. Ponekad pišemo $\mathrm{Res}_{d_0,\ldots,d_n}$ umjesto Res kako bismo eksplicitno naglasili ovisnost o stupnjevima. U ovim oznakama, ako je svaki $F_i = \sum_{j=0}^{n} c_{ij}x_j$ linearan komentar nakon sustava (8) pokazuje da je

$$\mathrm{Res}_{1,\ldots,1}(F_0, \ldots, F_n) = \det(c_{ij}).$$

Drugi primjer o kojemu smo dosta govorili je rezultanta dvaju polinoma. U ovom slučaju znamo da je $\mathrm{Res}(F_0, F_1)$ dana determinantom (2). Teorem 4 povlači da je ova determinanta ireducibilni polinom u koeficijentima od F_0, F_1.

2.1 Jednadžba parametarski zadane plohe

Navedimo u kratkim crtama jedan primjer korisnosti multipolinomijalne rezultante. Promotrimo *problem implicitizacije* u kojemu se traži jednadžba parametarski zadane krivulje ili plohe. Radi određenosti, uzmimo da je ploha zadana parametarski jednadžbama

$$\begin{aligned} x &= f(s,t) \\ y &= g(s,t) \\ z &= h(s,t), \end{aligned} \tag{9}$$

gdje su $f(s,t)$, $g(s,t)$, $h(s,t)$ polinomi (koji nisu nužno homogeni) stupnjeva d_0, d_1, d_2. Postoji nekoliko metoda pronalaženja jednadžbe $p(x,y,z) = 0$ plohe opisane s (9), primjerice upotreba Gröbnerovih baza. Mi ćemo pokazati da je u mnogim slučajevima moguće koristiti multipolinomijalne rezultante.

Najprije moramo homogenizirati gornje jednadžbe s obzirom na treću varijablu u. Primjerice, ako je

$$f(s,t) = f_{d_0}(s,t) + f_{d_0-1}(s,t) + \cdots + f_0(s,t),$$

gdje je f_j homogen (ukupnog) stupnja j u s, t, onda je

$$F(s,t,u) = f_{d_0}(s,t) + f_{d_0-1}(s,t)u + \cdots + f_0(s,t)u^{d_0},$$

a to je homogeni polinom u s, t, u stupnja d_0. Slično se $g(s,t)$ i $h(s,t)$ homogeniziraju u $G(s,t,u)$ i $H(s,t,u)$, a jednadžbe (9) postaju

$$F(s,t,u) - xu^{d_0} = G(s,t,u) - yu^{d_1} = H(s,t,u) - zu^{d_2} = 0. \tag{10}$$

Primjetimo da x, y, z promatramo kao koeficijente u ovim jednadžbama. Sada problem implicitizacije za (9) možemo riješiti na sljedeći način.

Propozicija 5. *Uz prethodne oznake, pretpostavimo da sustav homogenih jednadžbi*

$$f_{d_0}(s,t) = g_{d_1}(s,t) = h_{d_2}(s,t) = 0$$

ima samo trivijalna rješenja. Tada, za trojku $(x,y,z) \in \mathbb{C}^3$*, sustav jednadžbi* (9) *ima rješenje* $(s,t) \in \mathbb{C}^2$ *ako i samo ako je*

$$\mathrm{Res}_{d_0,d_1,d_2}(F - xu^{d_0}, G - yu^{d_1}, H - zu^{d_2}) = 0.$$

Dokaz. Prema teoremu 4, rezultanta iščezava ako i samo ako (10) ima netrivijalno rješenje (s,t,u). Ako je $u \neq 0$, onda je $(s/u, t/u)$ rješenje od (9). Ako je pak $u = 0$, onda je (s,t) netrivijalno rješenje $f_{d_0}(s,t) = g_{d_1}(s,t) = h_{d_2}(s,t) = 0$, što je u suprotnosti s našom pretpostavkom. Zato se ne može dogoditi $u = 0$. Za drugi smjer je dovoljno opaziti da rješenje (s,t) od (9) povlači netrivijalno rješenje $(s,t,1)$ od (10). □

Kako je rezultanta polinom u koeficijentima, slijedi da je

$$p(x,y,z) = \mathrm{Res}_{d_0,d_1,d_2}(F - xu^{d_0}, G - yu^{d_1}, H - zu^{d_2}) \tag{11}$$

polinom u x, y, z koji prema propoziciji 5 iščezava *točno* na slici parametrizacije. To posebno znači da parametrizacija pokriva *čitavu* plohu $p(x,y,z) = 0$, što naravno nije slučaj u svim polinomijalnim parametrizacijama; ovdje je pretpostavka da $f_{d_0}(s,t) = g_{d_1}(s,t) = h_{d_2}(s,t) = 0$ ima samo trivijalna rješenja od ključne važnosti.

2.2 Kompaktan zapis $\mathrm{Res}_{2,2,2}$

Jedna od većih poteškoća s multipolinomijalnim rezultantama je što su to obično *jako* veliki izrazi. Primjerice, promotrimo sustav jednadžbi zadan sa 3 kvadratne forme u 3 varijable:

$$\begin{aligned}
F_0 &= c_{01}x^2 + c_{02}y^2 + c_{03}z^2 + c_{04}xy + c_{05}xz + c_{06}yz = 0\\
F_1 &= c_{11}x^2 + c_{12}y^2 + c_{13}z^2 + c_{14}xy + c_{15}xz + c_{16}yz = 0\\
F_2 &= c_{21}x^2 + c_{22}y^2 + c_{23}z^2 + c_{24}xy + c_{25}xz + c_{26}yz = 0.
\end{aligned}$$

Ovo je sustav tri ternarne kvadrike. Prema teoremu 4 rezultanta $\mathrm{Res}_{2,2,2}(F_0, F_1, F_2)$ iščezava upravo onda kad sustav ima netrivijalno rješenje u x, y, z.

Polinom $\mathrm{Res}_{2,2,2}$ je vrlo velik: ima 18 varijabli (po jednu za svaki koeficijent c_{ij}), a uskoro ćemo vidjeti da mu je (ukupni) stupanj 12. Potpuno raspisan, $\mathrm{Res}_{2,2,2}$ ima 21894 članova. Zato je za rad s ovom rezultantom potrebno znati kompaktniji način za njeno predstavljanje. Navest ćemo sada jednu interesantnu formulu za $\mathrm{Res}_{2,2,2}$.

Najprije sa J označimo Jacobijan od F_0, F_1, F_2:

$$J = \begin{vmatrix}
\dfrac{\partial F_0}{\partial x} & \dfrac{\partial F_0}{\partial y} & \dfrac{\partial F_0}{\partial z}\\[2ex]
\dfrac{\partial F_1}{\partial x} & \dfrac{\partial F_1}{\partial y} & \dfrac{\partial F_1}{\partial z}\\[2ex]
\dfrac{\partial F_2}{\partial x} & \dfrac{\partial F_2}{\partial y} & \dfrac{\partial F_2}{\partial z}
\end{vmatrix},$$

koji je kubni homogeni polinom u x, y, z. To znači da su parcijalne derivacije od J kvadrike, pa ih možemo zapisati na sljedeći način

$$\begin{aligned}
\frac{\partial J}{\partial x} &= b_{01}x^2 + b_{02}y^2 + b_{03}z^2 + b_{04}xy + b_{05}xz + b_{06}yz\\
\frac{\partial J}{\partial y} &= b_{11}x^2 + b_{12}y^2 + b_{13}z^2 + b_{14}xy + b_{15}xz + b_{16}yz\\
\frac{\partial J}{\partial z} &= b_{21}x^2 + b_{22}y^2 + b_{23}z^2 + b_{24}xy + b_{25}xz + b_{26}yz.
\end{aligned}$$

Primjetite da je svaki b_{ij} kubni polinom u c_{ij}. Tada je prema klasičnoj Salmonovoj formuli (usp.[CLO 05]), rezultanta tri ternarne kvadrike dana sa 6×6 determinantom

$$\text{Res}_{2,2,2}(F_0,F_1,F_2)=\frac{-1}{512}\begin{vmatrix} c_{01} & c_{02} & c_{03} & c_{04} & c_{05} & c_{06}\\ c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16}\\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26}\\ b_{01} & b_{02} & b_{03} & b_{04} & b_{05} & b_{06}\\ b_{11} & b_{12} & b_{13} & b_{14} & b_{15} & b_{16}\\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25} & b_{26}\end{vmatrix}. \tag{12}$$

Napomena.

a. Iz (12) je jasno da je $\text{Res}_{2,2,2}$ stupnja 12 u varijablama $c_{01},\ldots,c_{26}$.

b. Razlomak $-1/512$ pojavljuje se u formuli radi normalizacije (svojstvo b u teoremu 4).

Primjer. Upotrijebimo prethodnu formulu za računanje jednadžbe plohe definirane u primjeru na kraju §1:

$$\begin{aligned} x &= 1+s+t+st\\ y &= 2+s+st+t^2\\ z &= s+t+s^2. \end{aligned}$$

Primjetimo da $st=st+t^2=s^2=0$ ima samo trivijalno rješenje, pa ovdje možemo primjeniti propoziciju 5. Stavimo

$$\begin{aligned} f_0 &= 1+s+t+st-x\\ f_1 &= 2+s+st+t^2-y\\ f_2 &= s+t+s^2-z, \end{aligned}$$

pa nakon homogeniziranja (ovdje su nam s,t,u varijable) dobivamo

$$\begin{aligned} F_0 &= (1-x)u^2+st+su+tu\\ F_1 &= t^2+(2-y)u^2+st+su\\ F_2 &= s^2-zu^2+su+tu. \end{aligned}$$

Izračunamo Jacobijan od F_0, F_1, F_2:

$$J=\det\begin{pmatrix} \frac{\partial F_0}{\partial s} & \frac{\partial F_0}{\partial t} & \frac{\partial F_0}{\partial u}\\ \frac{\partial F_1}{\partial s} & \frac{\partial F_1}{\partial t} & \frac{\partial F_1}{\partial u}\\ \frac{\partial F_2}{\partial s} & \frac{\partial F_2}{\partial t} & \frac{\partial F_2}{\partial u}\end{pmatrix}= \begin{aligned} &-6\,s^2\,t-2\,s\,t^2+2\,t^3+6\,s^2\,u-10\,s\,t\,u\\ &+10\,s\,u^2-6\,t\,u^2+2\,u^3+4\,s^2\,u\,x+8\,s\,t\,u\,x\\ &+2\,s\,u^2\,x+2\,t\,u^2\,x-2\,u^3\,x-4\,s^2\,u\,y\\ &-6\,s\,u^2\,y+2\,t\,u^2\,y-4\,t^2\,u\,z-2\,t\,u^2\,z+2\,u^3\,z \end{aligned}$$

i nastavimo dalje račun

$$\begin{aligned} \frac{\partial J}{\partial s} &= 0\cdot s^2-2t^2+(2x-6y+10)u^2-12st+(8x-8y+12)su+(8x-10)tu\\ \frac{\partial J}{\partial t} &= -6s^2+6t^2+(2x+2y-2z-6)u^2-4st+(8x-10)su-8ztu\\ \frac{\partial J}{\partial u} &= \begin{aligned}[t](4x-4y+6)s^2-4zt^2+(-6x+6z+6)u^2+(8x-10)st\\ +(4x-12y+20)su+(4x+4y-4z-12)tu.\end{aligned} \end{aligned}$$

Zato je konačno

$$\mathrm{Res}_{2,2,2}(F_0,F_1,F_2) =$$

$$\frac{-1}{512}\begin{vmatrix} 0 & 0 & 1-x & 1 & 1 & 1 \\ 0 & 1 & 2-y & 1 & 1 & 0 \\ 1 & 0 & -z & 0 & 1 & 1 \\ 0 & -2 & 2x-6y+10 & -12 & 8x-8y+12 & 8x-10 \\ -6 & 6 & 2x+2y-2z-6 & -4 & 8x-10 & -8z \\ 4x-4y+6 & -4z & -6x+6z+6 & 8x-10 & 4x-12y+20 & 4x+4y-4z-12 \end{vmatrix}$$

$$\begin{aligned} &= 9 + 15\,x + 13\,x^2 - 6\,x^3 + x^4 \\ &- 15\,y - 20\,x\,y - x^2\,y + 7\,y^2 + 5\,x\,y^2 \\ &- y^3 - 9\,z + 3\,x\,z - x^2\,z + 2\,x^3\,z \\ &+ 6\,y\,z - x\,y\,z - 2\,x^2\,y\,z - y^2\,z + 9\,z^2 \\ &+ 6\,x\,z^2 + x^2\,z^2 - 6\,y\,z^2 - 2\,x\,y\,z^2 + y^2\,z^2, \end{aligned}$$

pa vidimo da je polinom koji smo dobili kada smo prvi put gledali ovu plohu

$$p = x^2\,\mathrm{Res}_{2,2,2}(F_0,F_1,F_2).$$

3 Svojstva rezultanti

Vidjeli smo u teoremu 4 da rezultanta $\mathrm{Res}(F_0,\ldots,F_n)$ iščezava ako i samo ako $F_0 = \cdots = F_n = 0$ ima netrivijalno rješenje te da je rezultanta ireducibilna nad $\mathbb{C}$ kad je promatramo kao polinom u koeficijentima od F_i. Ova svojstva karakteriziraju rezultantu do na konstantu, ali time nikako nisu iscrpljena sva svojstva ovog iznimnog polinoma. U ovom dijelu govorit ćemo o još nekim važnijim svojstvima rezultante. Dokaze nećemo navoditi, a upute za odgovarajuću literaturu potražite u [CLO 05].

U ovome dijelu fiksirajmo stupnjeve $d_0,\ldots,d_n > 0$ i neka je $\mathrm{Res} = \mathrm{Res}_{d_0,\ldots,d_n} \in \mathbb{Z}[u_{i,\alpha}]$ rezultantni polinom iz prethodnog odjeljka. Započnimo s tvrdnjom o stupnju rezultante

Teorem 6. *Za fiksirani j između 0 i n,* Res *je homogen u varijablama $u_{j,\alpha}$, $|\alpha| = d_j$ stupnja $d_0\cdots d_{j-1}d_{j+1}\cdots d_n$. To znači da je*

$$\mathrm{Res}(F_0,\ldots,\lambda F_j,\ldots,F_n) = \lambda^{d_0\cdots d_{j-1}d_{j+1}\cdots d_n}\,\mathrm{Res}(F_0,\ldots,F_n).$$

Nadalje, ukupni stupanj od Res *je $\sum_{j=0}^{n} d_0\cdots d_{j-1}d_{j+1}\cdots d_n$.*

U nastavku proučavamo simetričnost i multiplikativnost rezultante.

Teorem 7.

a. *Ako je $i < j$, onda je*

$$\mathrm{Res}(F_0,\ldots,F_i,\ldots,F_j,\ldots,F_n) = (-1)^{d_0\cdots d_n}\,\mathrm{Res}(F_0,\ldots,F_j,\ldots,F_i,\ldots,F_n),$$

gdje je druga rezultanta za stupnjeve $d_0,\ldots,d_j,\ldots,d_i,\ldots,d_n$.

b. *Ako je* $F_j = F_j' F_j''$ *produkt homogenih polinoma stupnjeva* d_j' *i* d_j''*, onda je*

$$\mathrm{Res}(F_0, \ldots, F_j, \ldots, F_n) = \mathrm{Res}(F_0, \ldots, F_j', \ldots, F_n) \cdot \mathrm{Res}(F_0, \ldots, F_j'', \ldots, F_n),$$

gdje su zadnje dvije rezultante za stupnjeve $d_0, \ldots, d_j', \ldots, d_n$ *i* $d_0, \ldots, d_j'', \ldots, d_n$.

I za općenite rezultante vrijedi analogon propozicije 2. Za homogene polinome $F_0, \ldots, F_n \in \mathbb{C}[x_0, \ldots, x_n]$ stupnjeva $d_0, \ldots, d_n$, uvodimo sljedeće polinome

$$\begin{aligned} f_i(x_0, \ldots, x_n) &= F_i(x_0, \ldots, x_{n-1}, 1) \\ \overline{F}_i(x_0, \ldots, x_n) &= F_i(x_0, \ldots, x_{n-1}, 0). \end{aligned} \tag{13}$$

Primjetimo da su $\overline{F}_0, \ldots, \overline{F}_{n-1}$ homogeni polinomi iz $\mathbb{C}[x_0, \ldots, x_{n-1}]$ stupnjeva $d_0, \ldots, d_{n-1}$.

Teorem 8. *Ako je* $\mathrm{Res}(\overline{F}_0, \ldots, \overline{F}_{n-1}) \neq 0$*, tada je kvocijentni prsten* $A = \mathbb{C}[x_0, \ldots, x_{n-1}]/\langle f_0, \ldots, f_{n-1} \rangle$ *dimenzije* $d_0 \cdots d_{n-1}$ *kao vektorski prostor nad* $\mathbb{C}$ *i*

$$\mathrm{Res}(F_0, \ldots, F_n) = \mathrm{Res}(\overline{F}_0, \ldots, \overline{F}_{n-1})^{d_n} \det(m_{f_n} : A \to A),$$

gdje je $m_{f_n} : A \to A$ *linearno preslikavanje koje odgovara množenju sa* f_n.

4 Računanje rezultanti

U nastavku ovog predavanja pogledat ćemo neke metode za računanje rezultanti. Iako nam teorem 8 omogućuje da rezultantu računamo induktivno, korisno je imati i druge alate za rad s rezultantama. U ovom odjeljku navest ćemo još neke formule za rezultantu i onda kratko komentirati praktične aspekte računanja $\mathrm{Res}_{d_0,\ldots,d_n}$. Započnimo s jednim primjerom u kojem ćemo naći formulu za $\mathrm{Res}_{1,1,2}$ i koji će nam kasnije ilustrirati općenitu metodu pronalaženja rezultante.

Primjer. Promotrimo sljedeći sustav od tri homogene jednadžbe u tri varijable:

$$\begin{aligned} F_0 &= a_1 x + a_2 y + a_3 z = 0 \\ F_1 &= b_1 x + b_2 y + b_3 z = 0 \\ F_2 &= c_1 x^2 + c_2 y^2 + c_3 z^2 + c_4 xy + c_5 xz + c_6 yz = 0. \end{aligned} \tag{14}$$

Budući su F_0 i F_1 linearni, a F_2 kvadratni, rezultanta koju računamo je $\mathrm{Res}_{1,1,2}(F_0, F_1, F_2)$. Dobivamo sljedeću formulu za tu rezultantu.

Propozicija 9. $\mathrm{Res}_{1,1,2}(F_0, F_1, F_2)$ *je dana polinomom*

$$\begin{aligned} &a_1^2 b_2^2 c_3 - a_1^2 b_2 b_3 c_6 + a_1^2 b_3^2 c_2 - 2a_1 a_2 b_1 b_2 c_3 + a_1 a_2 b_1 b_3 c_6 + a_1 a_2 b_2 b_3 c_5 - a_1 a_2 b_3^2 c_4 \\ &+ a_1 a_3 b_1 b_2 c_6 - 2a_1 a_3 b_1 b_3 c_2 - a_1 a_3 b_2^2 c_5 + a_1 a_3 b_2 b_3 c_4 + a_2^2 b_1^2 c_3 - a_2^2 b_1 b_3 c_5 + a_2^2 b_3^2 c_1 \\ &- a_2 a_3 b_1^2 c_6 + a_2 a_3 b_1 b_2 c_5 + a_2 a_3 b_1 b_3 c_4 - 2a_2 a_3 b_2 b_3 c_1 + a_3^2 b_1^2 c_2 - a_3^2 b_1 b_2 c_4 + a_3^2 b_2^2 c_1. \end{aligned}$$

Dokaz. Označimo gornji polinom s R i pretpostavimo da imamo netrivijalno rješenje (x, y, z) od (14). Najprije ćemo pokazati da mala modifikacija od R mora iščeznuti. Točnije, promatrajmo šest jednadžbi

$$x \cdot F_0 = y \cdot F_0 = z \cdot F_0 = y \cdot F_1 = z \cdot F_1 = 1 \cdot F_2 = 0, \tag{15}$$

koje možemo i ovako zapisati

$$\begin{array}{ccccccccccccc} a_1x^2 & + & 0 & + & 0 & + a_2xy & + a_3xz & + & 0 & = 0 \\ 0 & + a_2y^2 & + & 0 & + a_1xy & + & 0 & + a_3yz & = 0 \\ 0 & + & 0 & + a_3z^2 & + & 0 & + a_1xz & + a_2yz & = 0 \\ 0 & + b_2y^2 & + & 0 & + b_1xy & + & 0 & + b_3yz & = 0 \\ 0 & + & 0 & + b_3z^2 & + & 0 & + b_1xz & + b_2yz & = 0 \\ c_1x^2 & + c_2y^2 & + & c_3z^2 & + & c_4xy & + & c_5xz & + & c_6yz & = 0. \end{array}$$

Ako promatramo x^2, y^2, z^2, xy, xz, yz kao "nepoznanice", onda ovaj sustav šest linearnih jednadžbi ima netrivijalno rješenje, što znači da je determinanta matrice sustava D jednaka nula. Upotrebom računala, lako provjerimo da je determinanta $D = -a_1R$.

Razmišljajući geometrijski, dokazali smo da u 12-dimenzionalnom prostoru $\mathbb{C}^{12}$ kojemu su $a_1, \ldots, c_6$ koordinate, polinom D iščezava na skupu

$$\{(a_1, \ldots, c_6) : (14) \text{ ima netrivijalno rješenje}\} \subset \mathbb{C}^{12}. \tag{16}$$

No, prema teoremu 4, posjedovanje netrivijalnog rješenja je ekvivalentno iščezavanju rezultante, pa D iščezava na skupu

$$\mathbf{V}(\mathrm{Res}_{1,1,2}) \subset \mathbb{C}^{12}.$$

To znači da je $D \in \mathbf{I}(\mathbf{V}(\mathrm{Res}_{1,1,2})) = \sqrt{\langle \mathrm{Res}_{1,1,2} \rangle}$, pri čemu je zadnja jednakost posljedica (Hilbertovog) Nullstellensatza. Ali $\mathrm{Res}_{1,1,2}$ je ireducibilan, što očito povlači $\sqrt{\langle \mathrm{Res}_{1,1,2} \rangle} = \langle \mathrm{Res}_{1,1,2} \rangle$. Time smo dokazali da je $D \in \langle \mathrm{Res}_{1,1,2} \rangle$, pa je $D = -a_1R$ višekratnik od $\mathrm{Res}_{1,1,2}$. Ireducibilnost povlači da $\mathrm{Res}_{1,1,2}$ dijeli a_1 ili R. Prema teoremu 6 znamo da je $\mathrm{Res}_{1,1,2}$ ukupnog stupnja 5, pa slijedi da $\mathrm{Res}_{1,1,2}$ dijeli R, a zbog činjenice da je i R (ukupnog) stupnja 5, zaključujemo da je R jednak $\mathrm{Res}_{1,1,2}$ pomnoženom s nekom konstantom. Evaluiramo li oba polinoma za $(F_0, F_1, F_2) = (x, y, z^2)$, vidimo da ta konstanta mora biti 1, čime smo dokazali da je $R = \mathrm{Res}_{1,1,2}$ što smo i htjeli. □

Osnovna ideja ovog primjera je bila da pomnožimu svaku jednadžbu s prikladnim monomom da bismo dobili kvadratnu matricu kojoj onda možemo računati determinantu.

U općem slučaju, neka su $F_0 \ldots, F_n \in \mathbb{C}[x_0, \ldots, x_n]$ stupnjeva $d_0, \ldots, d_n$. Tada definiramo

$$d = \sum_{i=0}^{n} (d_i - 1) + 1 = \sum_{i=0}^{n} d_i - n.$$

U prethodnom primjeru smo imali $(d_0, d_1, d_2) = (1, 1, 2)$, pa dobivamo $d = 2$. Primjetite da je to upravo stupanj monoma na lijevoj strani jednadžbi koje slijede iz (15).

Podijelimo sada monome $x^\alpha = x_0^{a_0} \cdots x_n^{a_n}$ (ukupnog) stupnja d u $n+1$ skupova na sljedeći način:

$$\begin{aligned} S_0 &= \{x^\alpha : |\alpha| = d,\ x_0^{d_0} \text{ dijeli } x^\alpha\} \\ S_1 &= \{x^\alpha : |\alpha| = d,\ x_0^{d_0} \text{ ne dijeli } x^\alpha,\ \text{ali } x_1^{d_1} \text{ dijeli}\} \\ &\vdots \\ S_n &= \{x^\alpha : |\alpha| = d,\ x_0^{d_0}, \ldots, x_{n-1}^{d_{n-1}} \text{ ne dijeli } x^\alpha,\ \text{ali } x_n^{d_n} \text{ dijeli}\}. \end{aligned}$$

Svaki monom stupnja d je djeljiv s $x_i^{d_i}$ za barem jedan i između 0 i n (Dirichletov princip), pa leži u jednom od skupova $S_0, \ldots, S_n$. Primjetimo, usto, da su ti skupovi disjunktni. U nastavku ćemo koristiti jedno očito opažanje:

$$\text{ako je } x^\alpha \in S_i, \text{ onda možemo pisati } x^\alpha = x_i^{d_i} \cdot x^\alpha / x_i^{d_i},$$

a jasno je da je $x^\alpha/x_i^{d_i}$ monom stupnja $d - d_i$ jer je $x^\alpha \in S_i$. Trebat će nam i činjenica da u skupu S_n ima točno $d_0 \cdots d_{n-1}$ monoma (slijedi iz toga što za dane cijele brojeve $a_0, \ldots, a_{n-1}$ za koje je $0 \le a_i \le d_i - 1$, postoji jedinstveni a_n takav da je $x_0^{a_0} \cdots x_n^{a_n} \in S_n$).

Sada možemo napisati sustav jednadžbi koji poopćuje (15):

$$\begin{aligned} x^\alpha/x_0^{d_0} \cdot F_0 &= 0 \quad \text{za sve } x^\alpha \in S_0 \\ &\vdots \\ x^\alpha/x_n^{d_n} \cdot F_n &= 0 \quad \text{za sve } x^\alpha \in S_n. \end{aligned} \tag{17}$$

Kako je F_i stupnja d_i, to je $x^\alpha/x_i^{d_i} \cdot F_i$ stupnja d. Zato svaki polinom na lijevoj strani od (17) možemo zapisati kao linearnu kombinaciju monoma (ukupnog) stupnja d. Takvih monoma ima $N = \binom{d+n}{n}$[‡]. Zapažamo da je ukupan broj jednadžbi jednak broju elemenata u $S_0 \cup \cdots \cup S_n$, a taj je također N. Dakle, gledamo li na monome stupnja d kao na nepoznanice, dobivamo sustav od N linearnih jednadžbi u N nepoznanica.

Definicija 10. *Determinantu $N \times N$ matrice sustava jednadžbi danih u* (17) *označavamo s D_n.*

Primjer. Vratimo se ponovno na primjer koji smo malo prije detaljno analizirali. Imamo tri jednadžbe (v. (14)):

$$\begin{aligned} F_0 &= a_1x + a_2y + a_3z = 0 \\ F_1 &= b_1x + b_2y + b_3z = 0 \\ F_2 &= c_1x^2 + c_2y^2 + c_3z^2 + c_4xy + c_5xz + c_6yz = 0. \end{aligned}$$

Ovdje je $(d_0, d_1, d_2) = (1, 1, 2)$, pa je $d = 2$ i $S_0 = \{x^2, xy, xz\}$ (svi monomi stupnja 2 koji su djeljivi s x^1), $S_1 = \{y^2, yz\}$ (monomi stupnja 2 koji nisu djeljivi s x, ali su djeljivi s y^1), $S_2 = \{z^2\}$ (monomi stupnja 2 koji nisu djeljivi s x ni s y, ali su djeljivi sa z^2, ovdje su to svi preostali monomi). Jednadžbe

$$x \cdot F_0 = y \cdot F_0 = z \cdot F_0 = y \cdot F_1 = z \cdot F_1 = 1 \cdot F_2 = 0,$$

su upravo jednadžbe (17) primjenjene u ovoj situaciji, pa ako raspišemo te jednadžbe

$$\begin{array}{rcrcrcrcrcl} a_1x^2 & + & 0 & + & 0 & + a_2xy + & a_3xz & + & 0 & = 0 \\ 0 & + & a_2y^2 & + & 0 & + a_1xy + & 0 & + & a_3yz & = 0 \\ 0 & + & 0 & + & a_3z^2 & + & 0 & + & a_1xz + a_2yz & = 0 \\ 0 & + & b_2y^2 & + & 0 & + b_1xy + & 0 & + & b_3yz & = 0 \\ 0 & + & 0 & + & b_3z^2 & + & 0 & + & b_1xz + b_2yz & = 0 \\ c_1x^2 & + & c_2y^2 & + & c_3z^2 & + & c_4xy & + & c_5xz + c_6yz & = 0 \end{array}$$

[‡]To je broj d-kombinacija u skupu od $n+1$ elemenata s ponavljanjem. Imamo $n+1$ pretinac i d kuglica ili drugim riječima n jedinica (pregrade) i d nula.

iz dobivenog sustava dobivamo za $x^2, y^2, z^2, xy, xz, yz$ kao nepoznanice determinantu

$$D_2 = \begin{vmatrix} a_1 & 0 & 0 & a_2 & a_3 & 0 \\ 0 & a_2 & 0 & a_1 & 0 & a_3 \\ 0 & 0 & a_3 & 0 & a_1 & a_2 \\ 0 & b_2 & 0 & b_1 & 0 & b_3 \\ 0 & 0 & b_3 & 0 & b_1 & b_2 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \end{vmatrix}.$$

Primjer. Kada imamo polinome $F_0, F_1 \in \mathbb{C}[x, y]$ kao u (6), tj.

$$\begin{aligned} F_0 &= a_0 x^l + a_1 x^{l-1} y + \cdots + a_l y^l \\ F_1 &= b_0 x^m + b_1 x^{m-1} y + \cdots + b_m y^m, \end{aligned}$$

onda je $d = l + m - 1$, pa je

$$\begin{aligned} S_0 &= \{x^{l+m-1}, x^{l+m-2} y, \ldots, x^l y^{m-1}\}, \\ S_1 &= \{x^{l-1} y^m, x^{l-2} y^{m+1}, \ldots, y^{l+m-1}\}. \end{aligned}$$

Ovdje sustav (17) izgleda ovako

$$\begin{aligned} x^{l+m-1}/x^l \cdot F_0 = \quad & x^{m-1} \cdot F_0 = 0 \\ x^{l+m-2} y/x^l \cdot F_0 = \; & x^{m-2} y \cdot F_0 = 0 \\ & \vdots \\ x^l y^{m-1}/x^l \cdot F_0 = \quad & y^{m-1} \cdot F_0 = 0 \\ \\ x^{l-1} y^m/y^m \cdot F_1 = \quad & x^{l-1} \cdot F_1 = 0 \\ x^{l-2} y^{m+1}/y^m \cdot F_1 = \; & x^{l-2} y \cdot F_1 = 0 \\ & \vdots \\ y^{l+m-1}/y^m \cdot F_1 = \quad & y^{l-1} \cdot F_1 = 0. \end{aligned}$$

pa je determinanta matrice sustava jednaka

$$D_1 = \det \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_l & & & \\ & a_0 & a_1 & a_2 & \cdots & a_l & & \\ & & \ddots & \ddots & \ddots & & \ddots & \\ & & & a_0 & a_1 & a_2 & \cdots & a_l \\ b_0 & b_1 & b_2 & \cdots & b_m & & & \\ & b_0 & b_1 & b_2 & \cdots & b_m & & \\ & & \ddots & \ddots & \ddots & & \ddots & \\ & & & b_0 & b_1 & b_2 & \cdots & b_m \end{bmatrix} = \operatorname{Res}(F_0, F_1).$$

Zaključujući slično kao u dokazu propozicije 9 dobivamo da je

$$D_n = \text{Res} \cdot \text{dodatni faktor}. \tag{18}$$

Ovaj dodatni faktor ne sadrži koeficijente od F_n, a u njemu se pojavljuju i samo neki koeficijenti od $F_0, \ldots, F_{n-1}$.

Propozicija 11. *Dodatni faktor iz* (18) *je cjelobrojni polinom u koeficijentima od* $\overline{F}_0, \ldots, \overline{F}_{n-1}$, *gdje je* $\overline{F}_i = F_i(x_0, \ldots, x_{n-1}, 0)$.

Skica dokaza. Najprije se pokaže da dodatni faktor (nazovimo ga E_n) leži kao i D_n i Res u $\mathbb{Z}[u_{i,\alpha}]$ (koeficijenti su mu iz $\mathbb{Q}$ jer je kvocijent dvaju polinoma s cjelobrojnim koeficijentima, a zbog ireducibilnosti Res u $\mathbb{Z}[u_{i,\alpha}]$ koji je faktorijalni prsten (domena jedinstvene faktorizacije), moraju koeficijenti od E_n ležati u $\mathbb{Z}$).

Budući je $D_n = \mathrm{Res} \cdot E_n$ homogen u koeficijentima od F_n, lako se vidi da Res i E_n također moraju biti homogeni u tim koeficijentima. Ali, teorem 6 i napomena o broju elemenata u S_n povlače da su i Res i D_n stupnja $d_0 \cdots d_{n-1}$ u koeficijentima od F_n. Odavdje slijedi da je E_n stupnja nula u koeficijentima od F_n, tj. ovisi samo o koeficijentima od $F_0, \ldots, F_{n-1}$.

Kako bismo završili dokaz, treba još pokazati da E_n ovisi samo o koeficijentima od $\overline{F}_i$. To znači da se koeficijenti od $F_0, \ldots, F_{n-1}$ uz koje je x_n na pozitivnu potenciju ne pojavljuju u E_n. U tu svrhu definira se pojam *težine* polinoma u $u_{i,\alpha}$ (sjetimo se da su Res, D_n i E_n takvi polinomi). Težina od $u_{i,\alpha}$ je eksponent a_n od x_n (gdje je $\alpha = (a_0, \ldots, a_n)$), težina monoma $u_{i_1,\alpha_1}^{m_1} \cdots u_{i_l,\alpha_l}^{m_l}$ se definira kao zbroj težina svakog u_{i_j,α_j} pomnoženog s odgovarajućim eksponentom m_j. Konačno, polinom u $u_{i,\alpha}$ naziva se *izobarični* ako je svaki pribrojnik u tom polinomu iste težine.

Pokaže se da je D_n izobarični polinom u kojemu svaki pribrojnik ima težinu $d_0 \ldots d_n$. Također nije teško vidjeti da iz $D_n = \mathrm{Res} \cdot E_n$ slijedi da su Res i E_n izobarični i da je težina od D_n jednaka zbroju težina od Res i E_n. Zato je dovoljno pokazati da je E_n težine nula, a to pokazujemo eksplicitno nalazeći član u Res težine $d_0 \cdots d_n$, što povlači da je težina od Res jednaka težini od D_n. □

Iako se u dodatnom faktoru u (18) pojavljuje manje koeficijenata nego u rezultanti, on može imati vrlo velik stupanj. Primjerice, ako je $d_i = 2$ za $0 \leq i \leq 4$, onda je rezultanta (ukupnog) stupnja $5 \cdot 2^4 = 80$, a D_4 je stupnja $\binom{10}{4} = 210$; ako je pak $d_i = 3$ za $0 \leq i \leq 4$, onda je $\deg \mathrm{Res} = 5 \cdot 3^4 = 405$, a $\deg D_4 = \binom{15}{4} = 1365$.

Primjetimo da propozicija 11 daje metodu za računanje rezultante: faktoriziramo D_n u ireducibilne faktore i jedini ireducibilni faktor koji sadrži sve varijable je rezultanta! Nažalost, ova metoda je izrazito nepraktična zbog sporosti faktorizacije polinoma u više varijabli (posebno polinoma velikih kao D_n).

U prijašnjim razmatranjima, skupovi $S_0, \ldots, S_n$ i determinanta D_n ovisili su o tome kako su varijable $x_0, \ldots, x_n$ poredane. Štoviše, oznaka D_n izabrana je tako da naglasi da varijabla x_n dolazi zadnja. Ako fiksiramo i između 0 i $n-1$ i poredamo varijable tako da x_i bude zadnja, onda dobivamo nešto drugačije skupove $S_0, \ldots, S_n$ i drugačiji skup jednadžbi (17). Označimo s D_i determinantu ovog sustava jednadžbi. (Napomenimo da postoji mnogo različitih poredaka varijabli u kojima je x_i posljednja. Izaberemo jedan od njih kod računanja D_i.)

Prije nego iskoristimo ove determinante, uvedimo jedan prirodan pojam koji smo zapravo već implicitno rabili. Polinome

$$\mathbf{F}_i = \sum_{|\alpha|=d_i} u_{i,\alpha} x^\alpha. \qquad i = 0, \ldots, n$$

zovemo "univerzalni" polinomi. Koeficijenti uz x^α su varijable $u_{i,\alpha}$. Ako evaluiramo $\mathbf{F}_0, \ldots, \mathbf{F}_n$ u $(c_{i,\alpha}) \in \mathbb{C}^M$, dobivamo polinome $F_0, \ldots, F_n$, gdje je $F_i = \sum_{|\alpha|=d_i} c_{i,\alpha} x^\alpha$.

Sada možemo dokazati klasičnu formulu za Res.

Propozicija 12. *Ako su $\mathbf{F}_0, \ldots, \mathbf{F}_n$ univerzalni polinomi, rezultanta je najveći zajednički djelitelj polinoma $D_0, \ldots, D_n$ u prstenu $\mathbb{Z}[u_{i,\alpha}]$, tj.*

$$\mathrm{Res} = \pm \mathrm{M}(D_0, \ldots, D_n).$$

Dokaz. Za svaki i postoje mnoge mogućnosti za D_i (koje ovise o $(n-1)!$ načina na koje možemo poredati varijable tako da je x_i posljednja). Trebamo dokazati da je, neovisno o tome koji D_i izaberemo za pojedini i, najveći zajednički djelitelj od $D_0, \ldots, D_n$ (do na predznak) rezultanta.

Slično kao u dokazu propozicije 9 (primjer s $\mathrm{Res}_{1,1,2}$) pokazuje se da Res dijeli D_n, a isto očito vrijedi i za $D_0, \ldots, D_{n-1}$. Nadalje, argumenti iz dokaza propozicije 11 pokazuju da je $D_i = \mathrm{Res} \cdot E_i$, pri čemu $E_i \in \mathbb{Z}[u_{j,\alpha}]$ ne sadrži koeficijente od $\mathbf{F}_i$. Zaključujemo da je

$$\mathrm{M}(D_0, \ldots, D_n) = \mathrm{Res} \cdot \mathrm{M}(E_0, \ldots, E_n).$$

Budući da E_i ne sadrži varijable $u_{i,\alpha}$ za svaki i, najveći zajednički djelitelj na desnoj strani mora biti konstanta, tj. cijeli broj. No koeficijenti od D_n su relativno prosti (lako se vidi da je $D_n(x_0^{d_0}, \ldots, x_n^{d_n}) = \pm 1$), pa ovaj cijeli broj mora biti ± 1 i time smo gotovi s dokazom. Spomenimo da su najveći zajednički djelitelji određeni samo do na invertibilne elemente, a u $\mathbb{Z}[u_{i,\alpha}]$ jedini invertibilni elementi su ± 1. □

Iako je formula iz propozicije 12 vrlo lijepa, nije posebno upotrebljiva u praksi. Predstavit ćemo još samo jednu formulu za rezultantu koja će nam točno reći čemu je jednak dodatni faktor u (18). Ključna je ideja, koju je imao Macaulay, da je dodatni faktor zapravo minora (tj. determinanta podmatrice) od $N \times N$ matrice iz (17) (sjetimo se da smo D_n definirali kao determinantu čitave te matrice). Kako bismo opisali ovu minoru, moramo znati koje retke i stupce matrice treba obrisati. Prisjetimo se da možemo označiti retke i stupce matrice (17) upotrebom svih monoma (ukupnog) stupnja $d = \sum_{i=0}^{n} d_i - n$. Za svaki takav monom x^α znamo da $x_i^{d_i}$ dijeli x^α za barem jedan i.

Definicija 13. *Neka su $d_0, \ldots, d_n$ i d kao i prije.*

a. Monom x^α stupnja d je reduciran *ako $x_i^{d_i}$ dijeli x^α za* točno *jedan i.*

b. D'_n je determinanta podmatrice matrice sustava (17) *dobivene brisanjem svih redaka i stupaca koji odgovaraju reduciranim monomima x^α.*

Macaulay je primjetio da je dodatni faktor u (18) upravo D'_n do na predznak. Tako dolazimo do sljedeće formule u kojoj je rezultanta dana kao kvocijent dvaju determinanti.

Teorem 14. *Ako su $\mathbf{F}_0, \ldots, \mathbf{F}_n$ univerzalni polinomi, rezultanta je dana s*

$$\mathrm{Res} = \pm \frac{D_n}{D'_n}.$$

Nadalje, ako je k proizvoljno polje i $F_0, \ldots, F_n \in k[x_0, \ldots, x_n]$, onda gornja formula vrijedi za Res *čim je $D'_n \neq 0$.*

Dokaz. Jedini dokaz ove formule nalazi se u originalnom Macaulayovom članku Macaulay, F. S. *Some formulae in eliminations.* London M. S. Proc. 35, 3-27 (1903). □

Primjer. U slučaju kad je $(d_0, d_1, d_2) = (1, 1, 2)$, imamo $d = 2$ i svi monomi stupnja 2 su reducirani osim xy. Zato $D'_2 = a_1$ odgovara podmatrici matrice na str. 14 dobivenoj brisanjem svega osim 2. retka i 4. stupca.

Iako je teorem 14 primjenjiv na sve rezultante, postoje neke poteškoće. U slučaju univerzalnih polinoma zahtijeva se dijeljenje dvaju vrlo velikih polinoma, što može biti vrlo dugotrajno, a u numeričkom slučaju, može se dogoditi neobična situacija gdje i D'_n i D_n iščezavaju[§].

Zbog navedenih fenomena bilo bi lijepo ako bismo rezultantu mogli izraziti pomoću jedne determinante, kao za $\mathrm{Res}_{l,m}$. Nije poznato je li to moguće učiniti općenito, ali u mnogim specijalnim slučajevima takav prikaz postoji. Jedan primjer vidjeli smo u formuli (12) za $\mathrm{Res}_{2,2,2}$. Ovu formulu može se (na razne načine) generalizirati, primjerice da dobijemo formule za $\mathrm{Res}_{l,l,l}$ ili $\mathrm{Res}_{l,l,l,l}$ za $l \geq 2$.

4.1 Praktični aspekti računanja rezultante

Završit ćemo ovaj odjeljak komentarom nekih praktičnih aspekata računanja rezultante. Sve metode koje smo upoznali uključujue računanje determinanti ili kvocijenta determinanti. Budući da uobičajena formula za $N \times N$ determinantu uključuje $N!$ članova, potrebni su neki bolji algoritmi za računanje velikih determinanti.

Determinante mogu biti ili *numeričke* ako su im elementi brojevi ili *simboličke* ako se u elementima pojavljuju i neke varijable. Započnimo s numeričkim determinantama. U većini slučajeva, to znači da su elementi determinante racionalni brojevi, koje onda množenjem sa zajedničkim nazivnikom možemo pretvoriti u cijele brojeve. Tada je ključna ideja reduciranje modulo prost broj p i izvođenje aritmetičkih operacija nad konačnim poljem $\mathbb{F}_p$ cijelih brojeva mod p. Računanje determinante postaje jednostavno jer radimo u polju, što nam omogućuje upotrebu standardnih algoritama iz linearne algebre (operacije na retcima i stupcima) za određivanje determinante. Druga pogodnost je da ne moramo misliti na to koliko veliki brojevi se pojavljuju (jer uvijek reduciramo mod p). Dakle, determinantu mod p možemo izračunati prilično jednostavno. Učinimo to za nekoliko prostih brojeva $p_1, \ldots, p_r$ i onda upotrebom kineskog teorema o ostatcima odredimo početnu determinantu.

Ova metoda je sasvim dovoljna kad je rezultanta dana kao jedna determinanta ili kao razlomak u kojemu je nazivnik različit od nule. Ali ako se dogodi da je nazivnik jednak nuli, potrebno nam je nešto drugo. Jedan način, koji je uveo Canny, da izbjegnemo ovaj problem je da spriječimo iščezavanje determinante tako što neke od elemenata učinimo simboličkim. Neka su $F_0, \ldots, F_n \in \mathbb{Z}[x_0, \ldots, x_n]$. Determinante D_n i D'_n iz teorema 14 dolaze od matrica koje ćemo označiti s M_n i M'_n. Tako formula iz teorema postaje

$$\mathrm{Res}(F_0, \ldots, F_n) = \pm \frac{\det(M_n)}{\det(M'_n)}$$

uz uvjet da je $\det(M'_n) \neq 0$. Ako je pak $\det(M'_n) = 0$, Cannyjeva metoda se sastoji u tome da uvedemo novu varijablu u i promatramo rezultantu

$$\mathrm{Res}(F_0 - ux_0^{d_0}, \ldots, F_n - ux_n^{d_n}). \tag{19}$$

[§]Ako npr. u primjeru vezanom uz propoziciju 9 stavimo $c_1 = c_2 = c_3 = 1$, a za sve ostale koeficijente 0, očito je da ne postoji netrivijalno rješenje, a $D_2 = D'_2 = 0$. Malom modifikacijom možemo dobiti netrivijalno rješenje, a da se D_2 i D'_2 ne promjene.

Nije teško pokazati[¶] da je ova rezultanta jednaka

$$\mathrm{Res}(F_0 - ux_0^{d_0}, \ldots, F_n - ux_n^{d_n}) = \pm\frac{\det(M_n - uI)}{\det(M_n' - uI)}$$

jer je $\det(M_n' - uI) \neq 0$ (to je karakteristični polinom od M_n'). Zato je rezultanta $\mathrm{Res}(F_0, \ldots, F_n)$ jednaka slobodnom članu u polinomu dobivenom dijeljenjem $\det(M_n - uI)$ sa $\det(M_n' - uI)$[‖]. Zaključujemo da se problem određivanja rezultante svodi na računanje determinanti $\det(M_n - uI)$ i $\det(M_n' - uI)$.

To nas vodi u drugi dio razmatranja, računanje simboličkih determinanti. Metode koje smo malo prije opisali u numeričkom slučaju, ovdje nisu primjenjive, pa je potrebno nešto novo. Jedna od najzanimljivijih metoda uključuje interpolaciju, a osnovna ideja je da se polinom može rekonstruirati iz njegovih vrijednosti u dovoljno velikom broju točaka. Točnije, pretpostavimo da dana simbolička determinanta sadrži varijable $u_0, \ldots, u_n$. Determinanta je tada polinom $D(u_0, \ldots, u_n)$. Ako uvrstimo $u_i = a_i$, gdje je $a_i \in \mathbb{Z}$ za $0 \leq i \leq n$, dobivamo numeričku determinantu koju onda možemo izračunati prije spomenutim metodama. Nakon što odredimo $D(a_0, \ldots, a_n)$ za dovoljno velik broj točaka $(a_0, \ldots, a_n)$, možemo rekonstruirati $D(u_0, \ldots, u_n)$. Grubo govoreći, potrebni broj točaka ovisi o stupnju od D u varijablama $u_0, \ldots, u_n$. Postoji nekoliko metoda za odabir točaka $(a_0, \ldots, a_n)$ što nas vodi na različite interpolacijske sheme (Vandermondeova, gusta, rijetka, vjerojatnosna). U slučaju kad imamo samo jednu varijablu, postoji i metoda Manochae za iznalaženje determinante bez interpolacije.

Spomenimo još takozvane *rijetke rezultante* (engl. sparse resultant) koje se koriste kada je poznato da su mnogi koeficijenti polinomā za koje računamo rezultantu jednaki nula.

5 Rješavanje jednadžbi pomoću rezultanti

U posljednjem dijelu našeg predavanja pokazat ćemo kako se rezultante mogu koristiti za rješavanje sustava polinomijalnih jednadžbi. Pretpostavimo da imamo n homogenih polinoma $F_1, \ldots, F_n$ (ukupnih) stupnjeva redom $d_1, \ldots, d_n$ u varijablama $x_0, \ldots, x_n$. Želimo naći netrivijalna rješenja sustava jednadžbi

$$F_1 = \cdots = F_n = 0. \tag{20}$$

Izložit ćemo ukratko dvije metode i to prvu malo detaljnije.

5.1 u-rezultanta

Osnovna ideja van der Waerdenove *u-rezultante* je da jednadžbama iz (20) dodamo još jednu jednadžbu $F_0 = 0$ tako da imamo $n + 1$ homogenih jednadžbi u $n + 1$ varijabli. Mi ćemo koristiti

$$F_0 = u_0x_0 + \cdots + u_nx_n,$$

[¶] ako retke i stupce matrice M_n poredamo istim redosljedom prema poretku monoma ukupnog stupnja d

[‖] Ako su F i G polinomi u u takvi da je F višekratnik od G i $G = b_ru^r + \text{članovi višeg stupnja}$, gdje je $b_r \neq 0$, tada je $F = a_ru^r + \text{članovi višeg stupnja}$. Trivijalno se vidi da je slobodni član od F/G upravo kvocijent a_r/b_r.

gdje su $u_0, \ldots, u_n$ nezavisne varijable. Budući da je broj jednadžbi jednak broju varijabli, možemo formirati rezultantu

$$\mathrm{Res}_{1,d_1,\ldots,d_n}(F_0, F_1, \ldots, F_n),$$

koju zovemo *u-rezultanta*. Vidimo da je u-rezultanta polinom u $u_0, \ldots, u_n$.

Ponekad se radi u afinoj situaciji, gdje dehomogeniziramo $F_0, \ldots, F_n$ stavljajući $x_0 = 1$ i dobivamo $f_0, \ldots, f_n$. Posebno,

$$f_0 = u_0 + u_1 x_1 + \cdots + u_n x_n. \tag{21}$$

Budući da $f_0, \ldots, f_n$ i $F_0, \ldots, F_n$ imaju iste koeficijente, u ovom slučaju u-rezultantu pišemo kao $\mathrm{Res}(f_0, \ldots, f_n)$, a ne $\mathrm{Res}(F_0, \ldots, F_n)$.

Pogledajmo na jednom primjeru kako se koristi metoda u-rezultante. Treba dosta posla, ali rezultat je iznenađujući.

Primjer. Neka je

$$F_1 = x_1^2 + x_2^2 - 10x_0^2 = 0$$
$$F_2 = x_1^2 + x_1x_2 + 2x_2^2 - 16x_0^2 = 0$$

presjek kružnice i elipse u $\mathbb{P}^{2**}$. Prema Bézoutovom teoremu postoje četiri rješenja. Kako bismo ih našli, dodajmo jednadžbu

$$F_0 = u_0x_0 + u_1x_1 + u_2x_2 = 0.$$

Pomoću teorije iz prethodnog odjeljka možemo rezultantu izračunati koristeći jednu od 10×10 determinanti D_0, D_1 ili D_2. Iskoristimo li D_0, teorem 14 povlači da je

$$\mathrm{Res}_{1,2,2}(F_0, F_1, F_2) = \pm\frac{D_0}{D_0'}.$$

Ako varijable poredamo x_2, x_1, x_0, onda je

$$S_0 = \{x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1x_2\}$$
$$S_1 = \{x_0x_1^2, x_1^3, x_1^2x_2\}$$
$$S_2 = \{x_0x_2^2, x_1x_2^2, x_2^3\}.$$

**Prisjetimo se da za projektivni prostor $\mathbb{P}^n(\mathbb{C})$ koji ćemo kratko označavati s $\mathbb{P}^n$ vrijedi

- Točka u $\mathbb{P}^n$ ima homogene koordinate $(a_0, \ldots, a_n)$, gdje $a_i \in \mathbb{C}$ nisu svi nula, a drugi skup koordinata $(b_0, \ldots, b_n)$ predstavlja istu točku u $\mathbb{P}^n$ ako i samo ako postoji kompleksan broj $\lambda \neq 0$ takav da je $(b_0, \ldots, b_n) = \lambda(a_0, \ldots, a_n)$.
- Ako je $F(x_0, \ldots, x_n)$ homogen stupnja d i $(b_0, \ldots, b_n) = \lambda(a_0, \ldots, a_n)$ su dva skupa homogenih koordinata iste točke $p \in \mathbb{P}^n$, onda je

  $$F(b_0, \ldots, b_n) = \lambda^d F(a_0, \ldots, a_n).$$

  Zato ne možemo definirati vrijednost od F u p, ali je jednadžba $F(p) = 0$ potpuno smislena. Na taj način dobivamo *projektivnu mnogostrukost* $\mathbf{V}(F) \subset \mathbb{P}^n$, koja je skup točaka od $\mathbb{P}^n$ u kojima F iščezava.

Zato dobivamo $D_0 = \det(M_0)$, gdje je M_0 matrica

$$M_0 = \begin{bmatrix} u_0 & u_1 & u_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & u_0 & 0 & u_1 & u_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & u_0 & 0 & u_1 & u_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & u_0 & 0 & 0 & u_1 & u_2 & 0 \\ -10 & 0 & 0 & \boxed{1} & 0 & \boxed{1} & 0 & 0 & 0 & 0 \\ 0 & -10 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & -10 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ -16 & 0 & 0 & \boxed{1} & 1 & \boxed{2} & 0 & 0 & 0 & 0 \\ 0 & -16 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & -16 & 0 & 0 & 0 & 0 & 1 & 1 & 2 \end{bmatrix},$$

pri čemu smo stupce indeksirali monomima poredanima leksikografski

$$x_0^3,\ x_0^2x_1,\ x_0^2x_2,\ x_0x_1^2,\ x_0x_1x_2,\ x_0x_2^2,\ x_1^3,\ x_1^2x_2,\ x_1x_2^2,\ x_2^3,$$

a istaknuli smo elemente koji leže u retku i stupcu koji odgovaraju nereduciranim monomima, ovdje su to $x_0x_1^2$ i $x_0x_2^2$. Dakle,

$$D_0' = \det(M_0') = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} = 1.$$

Sada izračunamo

$$\begin{aligned} \mathrm{Res}_{1,2,2}(F_0, F_1, F_2) = \pm\,(&2u_0^4 + 16u_1^4 + 36u_2^4 - 80u_1^3u_2 + 120u_1u_2^3 \\ &- 18u_0^2u_1^2 - 22u_0^2u_2^2 + 52u_1^2u_2^2 - 4u_0^2u_1u_2. \end{aligned}$$

Faktoriziramo ovo pomoću računala pa dobivamo da je $\mathrm{Res}_{1,1,2}(F_0, F_1, F_2)$ jednako

$$(u_0 + u_1 - 3u_2)(u_0 - u_1 + 3u_2)(u_0^2 - 8u_1^2 - 2u_2^2 - 8u_1u_2)$$

do na konstantu. Zapišemo li kvadratni faktor kao $u_0^2 - 2(2u_1+u_2)^2$ (tj. faktoriziramo u proširenju $\mathbb{Q}(\sqrt{2})$), zaključujemo da je $\mathrm{Res}_{1,2,2}(F_0, F_1, F_2)$ jednako

$$(u_0 + u_1 - 3u_2)(u_0 - u_1 + 3u_2)(u_0 + 2\sqrt{2}u_1 + \sqrt{2}u_2)(u_0 - 2\sqrt{2}u_1 - \sqrt{2}u_2)$$

pomnoženo s nekom nenul konstantom.

Koeficijenti linearnih faktora od $\mathrm{Res}_{1,2,2}(F_0, F_1, F_2)$ daju četiri točke

$$(1, 1, -3),\ (1, -1, 3),\ (1, 2\sqrt{2}, \sqrt{2}),\ (1, -2\sqrt{2}, -\sqrt{2})$$

u $\mathbb{P}^2$. Ove četiri točke su upravo četiri rješenja sustava $F_1 = F_2 = 0$. Dakle, rješenja u $\mathbb{P}^2$ su upravo koeficijenti linearnih faktora od $\mathrm{Res}_{1,2,2}(F_0, F_1, F_2)$!

Propozicija 15. *Pretpostavimo da $f_1 = \cdots = f_n = 0$ imaju stupnjeve omeđene s $d_1, \ldots, d_n$, nemaju rješenja u ∞[††] i sva rješenja su jednostruke kratnosti. Ako je $f_0 = u_0 + u_1x_1 + \cdots + u_nx_n$, gdje su $u_0, \ldots, u_n$ nezavisne varijable, onda postoji nenul konstanta C takva da je*

$$\mathrm{Res}_{1,d_1,\ldots,d_n}(f_0, \ldots, f_n) = C \prod_{p \in \mathbf{V}(f_1,\ldots,f_n)} f_0(p).$$

[††]To znači da za homogene polinome $F_0, \ldots, F_n$ sustav $F_0 = \cdots = F_n = 0$ nema netrivijalnih rješenja sa $x_0 = 0$.

Da bi se jasnije vidjelo što ova propozicija govori, označimo točke od $\mathbf{V}(f_1, \ldots, f_n)$ s p_i za $1 \leq i \leq d_1 \cdots d_n$. Ako napišemo svaku točku kao $p_i = (a_{i1}, \ldots, a_{in}) \in \mathbb{C}^n$, onda (21) povlači da je

$$f_0(p_i) = u_0 + a_{i1}u_1 + \cdots + a_{in}u_n,$$

pa je prema propoziciji 15, u-rezultanta dana sa

$$\text{Res}_{1,d_1,\ldots,d_n}(f_0, \ldots, f_n) = C \prod_{i=1}^{d_1 \cdots d_n} (u_0 + a_{i1}u_1 + \cdots + a_{in}u_n). \tag{22}$$

Odavdje jasno vidimo da je u-rezultanta polinom u $u_0, \ldots, u_n$. Također, dobivamo sljedeću metodu za rješavanje $f_1 = \cdots = f_n = 0$: izračunamo $\text{Res}_{1,d_1,\ldots,d_n}(f_0, \ldots, f_n)$, faktoriziramo u linearne faktore i očitamo rješenja! Stoga, kad imamo u-rezultantu, rješavanje danog sustava svodi se na problem faktorizacije polinoma u više varijabli.

Nažalost, u-rezultanta ima neka ozbiljna ograničenja. Ponajprije, nije jednostavno izračunati simboličke determinante velike veličine kao što smo već prije komentirali. Nadalje, čak i ako nađemo determinantu, faktorizacija polinoma u više varijabli kao u (22) je jako teška, posebno zato što u većini slučajeva uključuje brojeve s pomičnom točkom.

Postoji nekoliko metoda za rješavanje ovih problema. Opišimo u nekoliko riječi jednu od njih. Osnovna ideja je specijalizacija nekih od koeficijenata u $f_0 = u_0 + u_1x_1 + \cdots + u_nx_n$. Primjerice, ako su x_n-koordinate točaka rješenja različite, pokazuje se da specijalizacija $u_1 = \cdots = u_{n-1} = 0$, $u_n = -1$ transformira (22) u formulu

$$\text{Res}_{1,d_1,\ldots,d_n}(u_0 - x_n, f_1, \ldots, f_n) = C \prod_{i=1}^{d_1 \cdots d_n} (u_0 - a_{in}), \tag{23}$$

a a_{in} su x_n-koordinate od $p_i = (a_{i1}, \ldots, a_{in}) \in \mathbf{V}(f_1, \ldots, f_n)$. Ova rezultanta je polinom u jednoj varijabli u_0 čiji korijeni su upravo x_n-koordinate rješenja od $f_1 = \cdots = f_n = 0$. U slučaju da imamo samo jednu varijablu, računanje simboličkih determinanti i faktorizacija polinoma puno su lakši. Na ovaj način možemo naći sve pojedinačne koordinate rješenjā, a pogledajmo i jednu metodu pomoću koje ih možemo spariti (tako da znamo koje koordinate pripadaju kojem rješenju).

Pretpostavimo da smo izračunali x_1- i x_2- koordinate rješenja. Kako bismo sparili ove koordinate uzimamo dva slučajno izabrana broja α i β i promatramo rezultantu

$$R_{1,2}(u) = \text{Res}_{1,d_1,\ldots,d_n}(u - (\alpha x_1 + \beta x_2), f_1, \ldots, f_n).$$

Iz (22) slijedi da je

$$R_{1,2}(u) = C' \prod_{i=1}^{d_1 \cdots d_n} \big(u - (\alpha a_{i1} + \beta a_{i2})\big),$$

gdje je C' nenul konstanta.

Slučajnost izbora α i β osigurat će da za rješenja p_i, p_j, p_k vrijedi $\alpha a_{i1} + \beta a_{j2} \neq \alpha a_{k1} + \beta a_{k2}$, osim u slučaju kad je $p_i = p_j = p_k$. Zaključujemo da uvjet

$$\alpha \cdot (\text{neka } x_1\text{-koordinata}) + \beta \cdot (\text{neka } x_2\text{-koordinata}) = \text{ korijen od } R_{1,2}(u)$$

vrijedi jedino onda kad x_1-koordinata i x_2-koordinata dolaze od istog rješenja. Na ovaj način možemo naći prve dvije koordinate svih rješenja, a onda nastavimo postupak i nakon konačno koraka dolazimo do cjelovitih rješenja.

5.2 Skrivene varijable

Jedna od poznatijih tehnika za rješavanje sustava jednadžbi je metoda *skrivenih varijabli*. Osnovna ideja je da jednu od varijabli promatramo kao konstantu i onda uzmemo rezultantu. Kako bismo ilustrirali ovu metodu, promotrimo afine jednadžbe koje dobijemo iz nedavno riješenog primjera stavljanjem $x_0 = 1$:

$$\begin{aligned} f_1 &= x_1^2 + x_2^2 - 10 = 0 \\ f_2 &= x_1^2 + x_1x_2 + 2x_2^2 - 16 = 0. \end{aligned} \tag{24}$$

Ako promatramo x_2 kao konstantu, možemo iskoristiti najjednostavniji oblik rezultante da bi dobili

$$\operatorname{Res}(f_1, f_2) = 2x_2^4 - 22x_2^2 + 36 = 2(x_2 - 3)(x_2 + 3)(x_2 - \sqrt{2})(x_2 + \sqrt{2}).$$

Dobivena rezultanta je polinom u x_2 i njezini korijeni su *upravo* x_2-koordinate rješenja jednadžbi (kako smo odredili u spomenutom primjeru).

Kako bismo poopćili ovaj primjer, najprije promatramo afini oblik rezultante. Ako je dano $n+1$ homogenih polinoma $G_0, \ldots, G_n$ stupnjeva $d_0, \ldots, d_n$ u $n+1$ varijabli $x_0, \ldots, x_n$, dobivamo $\operatorname{Res}_{d_0,\ldots,d_n}(G_0, \ldots, G_n)$. Uvrštavanje $x_0 = 1$ daje

$$g_i(x_1, \ldots, x_n) = G_i(1, x_1, \ldots, x_n),$$

a jer g_i i G_i imaju iste koeficijente, možemo pisati rezultantu kao $\operatorname{Res}_{d_0,\ldots,d_n}(G_0, \ldots, G_n)$. Tako $n+1$ polinoma $g_0, \ldots, g_n$ u n varijabli $x_1, \ldots, x_n$ ima rezultantu. Dakle, s afine točke gledišta, formiranje rezultante zahtijeva da je *broj polinoma za jedan veći od broja varijabli*.

Pretpostavimo sada da imamo n polinoma $f_1, \ldots, f_n$ stupnjeva $d_1, \ldots, d_n$ u n varijabli $x_1, \ldots, x_n$. Što se tiče rezultante, imamo krivi broj jednadžbi i varijabli. Jedna mogućnost je da dodamo novi polinom što nas vodi na u-rezultantu. Ovdje ćemo razmotriti alternativu, tj. eliminiranje jedne od varijabli. Osnovna ideja je ono što smo učinili malo prije: *sakrijemo* varijablu, primjerice x_n, promatrajući je kao konstantu. Tako dobivamo n polinoma $f_1, \ldots, f_n$ u $n-1$ varijabli $x_1, \ldots, x_{n-1}$, pa možemo formirati rezultantu. Ovu ćemo rezultantu pisati ovako

$$\operatorname{Res}^{x_n}_{d_1,\ldots,d_n}(f_1, \ldots, f_n). \tag{25}$$

Gornji indeks x_n podsjeća nas da x_n promatramo kao konstantu. Kako je rezultanta polinom u koeficijentima od f_i, (25) je polinom u x_n.

Sada možemo iskazati osnovni rezultat metode skrivene varijable

Propozicija 16. *Generički,*[‡‡] $\operatorname{Res}^{x_n}_{d_1,\ldots,d_n}(f_1, \ldots, f_n)$ *je polinom u* x_n *čiji korijeni su* x_n*-koordinate rješenja od*

$$f_1 = \cdots = f_n = 0.$$

Prednost metode skrivenih varijabli je da se pojavljuje rezultanta koja ima manje jednadžbi i varijabli od u-rezultante. Primjerice, kada smo rješavali jednadžbe $f_1 = f_2 = 0$ iz (24), za u-rezultantu $\operatorname{Res}_{1,2,2}(f_0, f_1, f_2)$ smo koristili 10×10 matricu, a $\operatorname{Res}^{x_2}_{2,2}(f_1, f_2)$ zahtijeva samo 4×4 matricu.

Naravno da nema ništa posebno u skrivanju varijable x_n — možemo sakriti bilo koju od varijabli na isti način, tako da metodom skrivenih varijabli možemo odrediti x_i-koordinate rješenja za svaki i. Jedno ograničenje ove metode je u tome da daje samo pojedinačne koordinate rješenja, ali ne i način na koji ih treba spariti.

[‡‡] tj. do na neke specijalne slučajeve koji su određeni time da tada koeficijenti f-ova zadovoljavaju neke fiksirane polinomijalne jednadžbe.

Literatura

[CLO 05] Cox, David A.; Little, John; O'Shea, Donal. – *Using algebraic geometry.* Second edition. Graduate Texts in Mathematics, 185. Springer, New York, 2005.

[Da 01] D'Andrea, Carlos. – *Fórmulas Explícitas para el Cálculo de Resultantes y Aplicaciones.* Universidad de Buenos Aires, 2001.
`http://atlas.mat.ub.es/personals/dandrea/phd.htm`

[DD 01] D'Andrea, Carlos; Dickenstein, Alicia. – *Explicit formulas for the multivariate resultant.* Effective methods in algebraic geometry (Bath, 2000). J. Pure Appl. Algebra **164** (2001), no. 1-2, 59–86.

[DL 05] Dujella, Andrej; Luca, Florian. – *Diophantine m-tuples for primes.* Int. Math. Res. Not. 2005, no. **47**, 2913–2940.

[EM 99] Emiris, Ioannis Z.; Mourrain, Bernard. – *Matrices in elimination theory.* Polynomial elimination—algorithms and applications. J. Symbolic Comput. **28** (1999), no. 1-2, 3–44.

[Es 01] Escofier, Jean-Pierre. – *Galois theory.* Translated from the 1997 French original by Leila Schneps. Graduate Texts in Mathematics, 204. Springer-Verlag, New York, 2001.

[GKZ 94] Gel'fand, I. M.; Kapranov, M. M.; Zelevinsky, A. V. – *Discriminants, resultants, and multidimensional determinants.* Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 1994.

[La 02] Lang, Serge. – *Algebra.* Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[Ma 16] Macaulay, F. S. – *The algebraic theory of modular systems.* Cambridge University Press, Cambridge, 1916.
`http://historical.library.cornell.edu/cgi-bin/cul.math/docviewer?did=05190001`

[S 82] Schinzel, Andrzej. – *Selected topics on polynomials.* University of Michigan Press, Ann Arbor, Mich., 1982.

[Sch 76] Schmidt, Wolfgang M. – *Equations over finite fields. An elementary approach.* Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin-New York, 1976.