Survo-ristikot ja polynomit

Jukka Tuomela
Fysiikan ja matematiikan laitos
Joensuun yliopisto

Survo-ristikko

Seppo Mustonen on viime aikoina eri lehdissä esitellyt Survo-ristikoita: http://www.survo.fi/ristikot/ .

Tällaiset ongelmat ratkeavat, ainakin periaatteessa, polynomien avulla.

Tarkastellaan erästä Mustosen yksinkertaista tehtävää seuraavan kaavion avulla.

$$\begin{array}{cccc} x_1 & x_2 & x_3 & b_1 \\ x_4 & x_5 & x_6 & b_2 \\ c_1 & c_2 & c_3 & \end{array}$$

Tässä siis parametrit b_1, b_2, c_1, c_2 ja c_3 ovat positiivisia kokonaislukuja, ja haluttaisiin löytää $x_1,\ldots, x_6$ siten, että

$$(1)\quad \begin{cases} x_1 + x_2 + x_3 = b_1 \\ x_4 + x_5 + x_6 = b_2 \\ x_1 + x_4 = c_1 \\ x_2 + x_5 = c_2 \\ x_3 + x_6 = c_3 \end{cases}$$

Lisäksi vaaditaan, että
(i) muuttujat x_i ovat kokonaislukuja ja
(ii) $x_i \neq x_j$ kaikilla $i \neq j$ ja
(iii) $1 \leq x_i \leq 6$.
Analysoidaan ensiksi yhtälöryhmää (1). Tämähän on lineaarinen yhtälöryhmä, jossa on 5 yhtälöä ja 6 tuntematonta. Mutta itse asiassa kaikki yhtälöt eivät ole riippumattomia. Helposti voidaan tarkistaa, että on vain 4 riippumatonta yhtälöä, ja että ratkaisu on olemassa vain jos

$$(2)\quad b_1 + b_2 = c_1 + c_2 + c_3 .$$

Jos oletetaan, että tämä yhteensopivuusehto on voimassa, niin 4 yhtälöä ja 6 tuntematonta osoittaa, että ratkaisuavaruus on 2-ulotteinen: 2 muuttujaa x_i voidaan valita mielivaltaisesti, ja muut voidaan ratkaista näitten avulla. Tässä vaiheessa ei siis ole varsinaisesti väliä mitä lukuja parametrit b_i ja c_j ovat. Geometrinen mielikuva on kuitenkin selvä: ratkaisujoukko on (2-ulotteinen) taso 6-ulotteisessa avaruudessa.

Määritellään nyt ratkaisujoukko rationaalilukujen $\mathbb{Q}$ avulla. Olkoon

$$x = (x_1, x_2, x_3, x_4, x_5, x_6) \in \mathbb{Q}^6 ,$$
$$d = (b_1, b_2, c_1, c_2, c_3) \in \mathbb{Q}^5 ,$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Tällöin yhtälöryhmä (1) voidaan yksinkertaisesti esittää muodossa $Ax = d$ ja ratkaisujoukko on siis

$$L_6 = \left\{ x \in \mathbb{Q}^6 \mid Ax = d \right\} .$$

Vastaavasti yleinen Survo-ristikko voidaan kuvata kaaviolla

$$\begin{array}{ccccc} x_1 & x_2 & \cdots & x_j & b_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{(k-1)j+1} & x_{(k-1)j+2} & \cdots & x_{jk} & b_k \\ c_1 & c_2 & \cdots & c_j & \end{array}$$

Vastaavan matriisin A kooksi tulee siis $(k+j)\times jk$ ja jätän lukijalle harjoitustehtäväksi osoittaa, että A:n rangi on $k+j-1$. Joskus Survo-ristikoissa on lisäksi annettu valmiiksi joittenkin muuttujien x_i arvot. Koska tällä ei ole varsinaisesti merkitystä tehtävän matemaattisen rakenteen kannalta, jätän tämän muunnelman lähemmän tarkastelun harjoitustehtäväksi.

Palataan sitten esimerkkiin (1), ja halutaan löytää sellainen ratkaisu, joka lisäksi toteuttaisi ehdot (i), (ii) ja (iii). Tarkastellaan tapausta, jossa parametrit b_i ja c_i on annettu seuraavasti:

$$\begin{array}{cccc} x_1 & x_2 & x_3 & 7 \\ x_4 & x_5 & x_6 & 14 \\ 9 & 8 & 4 & \end{array}$$

Merkitään edelleen

$$\mathbb{N}_6 = \{1,2,3,4,5,6\}.$$

Mahdollisten ratkaisujen joukko voidaan näin ollen tulkita joukon $\mathbb{N}_6$ permutaatioiden joukoksi, joten ratkaisukandidaattien lukumäärä on 6! = 720. Olkoon edelleen

$$(3)\quad V_6 = \{p^1, \ldots, p^{720}\} \subset \mathbb{Q}^6,$$

missä p^i on jokin joukon $\mathbb{N}_6$ permutaatioista, tulkittuna avaruuden $\mathbb{Q}^6$ pisteenä. Survo-ristikon (1) ratkaisu on siis

$$R_6 = L_6 \cap V_6.$$

Näemme siis, että Survo-ongelma on geometrinen: ratkaisu on kahden *varieteetin* leikkaus.

Varieteetti

Varieteetilla tarkoitetaan jonkin polynomisysteemin ratkaisujoukkoa. Siis esimerkiksi $J = \{1,2\} \subset \mathbb{R}$ ja yksikkökehä $S^1 \subset \mathbb{R}^2$ ovat varieteetteja, koska J on polynomin $p = (x-1)(x-2)$ ja S^1 polynomin $q = x^2 + y^2 - 1$ nollakohtien joukko. Sen sijaan suljettu väli $[0,1] \subset \mathbb{R}$ ei ole varieteetti.

L_6 on selvästi (lineaarinen) varieteetti: systeemin (1) yhtälöt ovat (ensimmäisen asteen) polynomeja. Mutta entäpä V_6, minkä systeemin nollakohtien joukko se on?

Tarkastellaan selvyyden vuoksi ensin kolmen muuttujan tapausta. Olkoon $\mathbb{Q}[x_1, x_2, x_3]$ muuttujien x_1, x_2 ja x_3 rationaalikertoimisten polynomien joukko. Kolmen olion permutaatioita vastaava varieteetti on

$$V_3 = \{(1,2,3),(1,3,2),(2,1,3),(2,3,1),(3,1,2),(3,2,1)\} \subset \mathbb{Q}^3.$$

Koska x_i on joko 1, 2 tai 3, niin selvästi täytyy päteä

$$(x_i - 1)(x_i - 2)(x_i - 3) = x_i^3 - 6x_i^2 + 11x_i - 6 = 0$$

kaikilla *i*. Siis jos määritellään

$$\tilde{V}_3 = \{(x_1, x_2, x_3) \mid x_i^3 - 6x_i^2 + 11x_i - 6 = 0, i = 1,2,3\},$$

niin selvästi $\tilde{V}_3$ on varieteetti ja $V_3 \subset \tilde{V}_3$. Varieteetissa $\tilde{V}_3$ on 27 pistettä, joten se on liian iso; tarvitaan lisää yhtälöitä, jotta päästään varieteettiin V_3. Pieni miettiminen johtaa yhtälöön $x_1 + x_2 + x_3 - 6 = 0$, mutta tämäkään ei vielä riitä. Jätän lukijalle harjoitustehtäväksi laskea kuinka monta pistettä on varieteetissa

$$\begin{cases} x_1^3 - 6x_1^2 + 11x_1 - 6 = 0 \\ x_2^3 - 6x_2^2 + 11x_2 - 6 = 0 \\ x_3^3 - 6x_3^2 + 11x_3 - 6 = 0 \\ x_1 - x_2 + x_3 - 6 = 0 \end{cases}.$$

Tarvitaan siis vielä lisää informaatiota. Jätän taas lukijalle harjoitustehtäväksi osoittaa, että seuraava systeemi antaa oikean varieteetin:

$$(4)\quad V_3 : \begin{cases} x_1^3 - 6x_1^2 + 11x_1 - 6 = 0 \\ x_1^2 - x_1x_2 + x_2^2 - 6(x_1 + x_2) + 11 = 0. \\ x_1 + x_2 + x_3 - 6 = 0 \end{cases}$$

Huomattakoon, että tehtävän symmetriasta johtuen muuttujia voidaan permutoida ylläolevassa systeemissä varieteetin pysyessä samana. Siis eri polynomisysteemeillä voi olla sama varieteetti. Tämän takia varieteetteja onkin parasta tutkia *ideaalien* avulla.

Ideaali

Matematiikan ala, joka tutkii varieteettien yleisiä ominaisuuksia, on nimeltään *algebrallinen geometria*; varieteetit ovat geometrisia olioita ja ideaalit ovat niitten algebrallisia vastineita.

Tarkastellaan polynomirengasta $\mathbb{Q}[x_1, \ldots, x_n]$. Rengas on joukko, jonka alkioille on määritelty sekä yhteen- että kertolasku. Renkaan $\mathbb{Q}[x_1, \ldots, x_n]$ osajoukko $\mathcal{I}$ on *ideaali*, jos

(1) $0 \in \mathcal{I}$,
(2) $f \in \mathcal{I}, g \in \mathcal{I} \Rightarrow f + g \in \mathcal{I}$,
(3) $f \in \mathbb{Q}[x_1, \ldots, x_n], g \in \mathcal{I} \Rightarrow fg \in \mathcal{I}$.

Ideaalien hyödyllisyys perustuu siihen, että ne (lähes) vastaavat yksikäsitteisesti tiettyjä varieteetteja. Tässä ei ole mahdollista muotoilla tätä tarkemmin, mutta kirjassa *Ideals, varieties and algorithms* [1] asia käsitellään perusteellisesti ja ymmärrettävästi. Todettakoon vain, että tämän kirjoituksen kannalta voidaan ajatella, että tiettyä varieteettia vastaa yksikäsitteinen ideaali, ja vastaavasti tiettyä ideaalia vastaa yksikäsitteinen varieteetti.

Tarkastellaan vaikkapa varieteettia V_3 ja sitä vastaavaa polynomisysteemiä (4). Merkitään edelleen

$f_3 = x_1^3 - 6x_1^2 + 11x_1 - 6,$
$f_2 = x_1^2 + x_1x_2 + x_2^2 - 6(x_1 + x_2) + 11$ ja
$f_1 = x_1 + x_2 + x_3 - 6.$

Tällöin varieteettia V_3 vastaava ideaali on

$$\mathcal{I}_3 = \{ f \in \mathbb{Q}[x_1, x_2, x_3] \mid f = a_1 f_1 + a_2 f_2 + a_3 f_3,\ a_i \in \mathbb{Q}[x_1, x_2, x_3] \}.$$

Sanotaan, että $\mathcal{I}_3$ on polynomien f_i virittämä ideaali, ja tälle käytetään usein merkintää $\mathcal{I}_3 = \langle f_1, f_2, f_3 \rangle$. Tälle ideaalille on toinenkin "luonnollinen" virittäjäjoukko eli *kanta*. Olkoon $g_1 = f_1,\ g_2 = x_1^2 + x_2^2 + x_3^2 - 14$ ja $g_3 = x_1^3 + x_2^3 + x_3^3 - 36;$ voidaan osoittaa, että

$$\mathcal{I}_3 = \langle f_1, f_2, f_3 \rangle = \langle g_1, g_2, g_3 \rangle.$$

Samanlainen tulos pätee yleisestikin. Ensin tarvitaan kuitenkin muutama merkintä. Olkoon

$$\mathbb{N}_n = \{1, 2, \ldots, n\}.$$

Tarkastellaan varieteettia

$$V_n = \{ p^1, \ldots, p^{n!} \} \subset \mathbb{Q}^n,$$

missä siis jokainen p^i vastaa tiettyä joukon $\mathbb{N}_n$ permutaatiota. Edelleen määritellään kertoimet $a_{k,n}$ seuraavasti:

$$(x-1)\cdots(x-n) = \sum_{k=0}^{n} a_{k,n} x^k.$$

Erityisesti siis $a_{n,n} = 1,\ a_{n-1,n} = -\sum_{i=1}^{n} i = -n(n+1)/2$ ja $a_{0,n} = (-1)^n n!$. Olkoon nyt M_r^s summa kaikista monomeista, jotka ovat kertalukua *s* ja joissa esiintyy muuttujia $x_1, \ldots, x_r$. Siis esimerkiksi

$$M_4^1 = x_1 + x_2 + x_3 + x_4,$$
$$M_2^3 = x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3.$$

Olkoon vielä

$$b_{k,n} = 1^k + 2^k + \cdots + n^k$$

ja määritellään seuraavat polynomit:

$$f_k = M_{n-k+1}^k + a_{n-1,n} M_{n-k+1}^{k-1} + \cdots + a_{n-k+1,n} M_{n-k+1}^1 + a_{n-k,n} = 0,$$
$$k = 1, \ldots, n,$$
$$g_k = \sum_{i=1}^{n} x_i^k - b_{k,n},\ k = 1, \ldots, n.$$

Erityisesti $f_1 = g_1$ ja $f_n = (x_1 - 1)\cdots(x_1 - n)$. Systeemin (4) kanta voidaan nyt yleistää mielivaltaisen monen muuttujan tapaukseen seuraavasti:

Lause 1. Varieteettia V_n vastaava ideaali on
$\mathcal{I}_n = \langle f_1, \ldots, f_n \rangle = \langle g_1, \ldots, g_n \rangle$.

Itse asiassa en ole tätä lausetta oikeasti todistanut, enkä tiedä mistä todistuksen voisi löytää. Jätänkin lauseen todistamisen haasteeksi lukijalle. Kuitenkin laskut, joilla olen Survo-tehtäviä ratkonut, ovat perustuneet tähän lauseeseen; tarkemmin sanoen olen käyttänyt polynomien f_i avulla määriteltyä kantaa. Lause on siis tullut todistettua esimerkin avulla. Sivulta http://www.maths.uwa.edu.au/~berwin/humour/invalid.proofs.html löytyy monia muita hyödyllisiä todistustekniikoita.

Palataan sitten tehtävään (1) ja siihen mikä on systeemiä (3) vastaava ideaali. Soveltamalla lausetta tapauksessa $n = 6$ saadaan polynomit

$$f_6 = x_1^6 - 21x_1^5 + 175x_1^4 - 735x_1^3 + 1624x_1^2 - 1764x_1 + 720,$$
$$f_5 = M_2^5 - 21M_2^4 + 175M_2^3 - 735M_2^2 + 1624M_2^1 - 1764,$$
$$f_4 = M_3^4 - 21M_3^3 + 175M_3^2 - 735M_3^1 + 1624,$$
$$f_3 = M_4^3 - 21M_4^2 + 175M_4^1 - 735,$$
$$f_2 = M_5^2 - 21M_5^1 + 175,$$
$$f_1 = g_1 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 - 21,$$
$$g_2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 - 91,$$
$$g_3 = x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 + x_6^3 - 441,$$
$$g_4 = x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4 + x_6^4 - 2275,$$
$$g_5 = x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_5^5 + x_6^5 - 12201,$$
$$g_6 = x_1^6 + x_2^6 + x_3^6 + x_4^6 + x_5^6 + x_6^6 - 67171.$$

Merkitään edelleen systeemissä (1) olevia polynomeja symboleilla $q_1, \ldots, q_5$. Siis varieteettia L_6 vastaava ideaali on

$$\mathcal{I}_{L_6} = \langle q_1, q_2, q_3, q_4, q_5 \rangle.$$

Koska ratkaisuvarieteetti on kahden varieteetin *leikkaus*, niin pienen miettimisen jälkeen voimme päätellä, että ratkaisuvarieteettia vastaavan ideaalin kanta saadaan *yhdistämällä* komponenttien kannat:

$$(5)\quad \mathcal{I}_{R_6} = \langle q_1, q_2, q_3, q_4, q_5, f_1, f_2, f_3, f_4, f_5, f_6 \rangle.$$

On siis saatu muotoiltua tehtävä siten, että ratkaisua kuvaa ideaali, jonka kannassa on yksitoista kuuden muuttujan polynomia. Päällisin puolin näyttäisi siltä, että tehtävä on muotoiltu oudolla tavalla uudelleen, mutta itse tehtävän ratkaiseminen ei ole juurikaan edistynyt. Mutta toisaalta tiedetään, että tehtävällä on yksikäsitteinen ratkaisu, eli varieteetti R_6 on yksi piste. Mutta tällöinhän

$$(6)\quad \mathcal{I}_{R_6} = \langle x_1 - a_1, x_2 - a_2, x_3 - a_3, x_4 - a_4, x_5 - a_5, x_6 - a_6 \rangle,$$

missä vakiot a_i antavat tehtävän ratkaisun. Pitäisi siis jotenkin lähteä liikkeelle kannasta (5) ja päätyä kantaan (6), josta ratkaisu voidaan suoraan lukea. Tämä vaikuttaa edelleen hankalalta, mutta 60-luvulla **Buchberger** löysi algorit-

min, jolla jokaiselle ideaalille voidaan laskea *Gröbner-kanta* (**Gröbner** oli Buchbergerin väitöskirjan ohjaaja).

Gröbner-kannat

Ideaaliteorian yhteydessä kannalla tarkoitetaan mitä tahansa ideaalin virittävää joukkoa; Gröbner-kanta täyttää lisäksi eräitä muita kriteerejä, joihin nyt ei voi sen tarkemmin puuttua. Tarkastellaan kuitenkin erästä ongelmaa, jossa Gröbner-kantojen hyödyllisyys tulee esille. Eräs laskennallisen ideaaliteorian perustehtävä on selvittää kuuluuko annettu polynomi ideaaliin $I = \langle f_1, \ldots, f_m \rangle$. Keskeinen tulos on, että tämä voidaan algoritmisesti testata, jos $\{f_1, \ldots, f_m\}$ on Gröbner-kanta. Koska Buchbergerin algoritmilla voidaan puolestaan laskea Gröbner-kanta, niin ongelma voidaan ratkaista, vaikka ideaalia ei alunperin olisi annettu Gröbner-kannassa. Vastaavasti monissa muissakin laskennallisen ideaaliteorian, tai ehkä pikemminkin laskennallisen algebrallisen geometrian ongelmissa, Gröbner-kannat ovat erittäin hyödyllisiä.

Huomattakoon, että annetun ideaalin Gröbner-kanta ei ole yksikäsitteinen, vaan riippuu valitusta *monomijärjestyksestä.* Tässä ei kuitenkaan voida mennä sen syvemmälle näihin järjestyksiin; niihin voi perehtyä jo edellä mainitun kirjan *Ideals, varieties and algorithms* avulla [1].

Nykyään yleiskäyttöisissä symbolisen laskennan ohjelmistoissa on jo jonkinlainen Gröbner-kantojen toteutus, mutta jos haluaa enemmän tehoja ja mahdollisuuksia, niin on olemassa myös useita ohjelmistoja, jotka ovat erikoistuneet polynomilaskentaan. Seuraavissa laskuissa olen käyttänyt Singular-ohjelmistoa [2], [3].

Kun nyt määritellään Singularissa ideaali (5), ja lasketaan Gröbner-kanta tietyn monomijärjestyksen suhteen, niin vastaus on

$$\mathcal{I}_{R_6} = \langle x_1 - 4, x_2 - 2, x_3 - 1, x_4 - 5, x_5 - 6, x_6 - 3 \rangle.$$

Gröbner-kanta on siis haluttua muotoa (6), josta vastaus voidaan lukea suoraan!

Kun sitten siirrytään vaikeampiin tehtäviin, niin tarvittavien polynomien kertoimet, siis parametrit $a_{k,n}$, kasvavat varsin nopeasti. Lisäksi Gröbner-kantojen laskennassa välituloksissa esiintyvät polynomien kertoimet saattavat kasvaa arvaamattoman paljon. Kannattaa siis siirtyä *äärellisiin kuntiin*.

Äärelliset kerroinkunnat

Servo-ongelmissa on se laskennallisesti miellyttävä ominaisuus, että etukäteen tiedetään jokin ylä- ja alaraja ratkaisulle. Tätä voidaan hyödyntää seuraavasti. Olkoon

$$\mathbb{Z}_p = \{0, 1, \ldots, p-1\},$$

missä p on alkuluku. Laskutoimitukset $\mathbb{Z}_p$:ssä määritellään modulo p: siis jos yhteen- tai kertolaskun tulos on suurempi kuin $p - 1$, niin jaetaan p:llä ja otetaan jakojäännös. Siis esimerkiksi

$$\mathbb{Z}_7 : 3 \cdot 5 = 1,$$
$$\mathbb{Z}_{11} : 4 \cdot 8 = 10.$$

Näinhän voidaan määritellä vaikka p ei olisikaan alkuluku. Alkulukuominaisuutta tarvitaan, jos halutaan määritellä käänteisalkio. Jos p on alkuluku, niin kaikille $0 \neq a \in \mathbb{Z}_p$ on olemassa $a^{-1} \in \mathbb{Z}_p$ siten, että $aa^{-1} = 1$; esimerkiksi 3 ja 5 ovat toistensa käänteisalkioita $\mathbb{Z}_7$.

Tarkastellaan hiukan vaikeampaa Servo-tehtävää

x_1	x_2	x_3	8
x_4	x_5	x_6	15
x_7	x_8	x_9	22
11	13	21	

Tässä tapauksessa on luonnollista valita $\mathbb{Z}_{23}$, koska 23 on pienin alkuluku, joka on suurempi kuin tehtävässä annetut parametrit. Nyt varieteettia V_9 vastaavat yhtälöt tulevat paljon yksinkertaisemmiksi siinä mielessä, että kertoimet eivät ole isoja. Esimerkiksi

$$f_9 = (x_1 - 1) \cdots (x_1 - 9) = x_1^9 + x_1^8 + 19x_1^7 + 3x_1^6 + 5x_1^4 + 8x_1^3 + x_1^2 + 17x_1 + 12$$

Onneksi Gröbner-kannat ovat hyvin määriteltyjä ja Buchbergerin algoritmi toimii myös äärellisten kuntien tapauksessa, joten tehtävän ratkaisu saadaan paljon tehokkaammin kuin rationaalilukujen kunnan tapauksessa. Kun sitten muodostetaan yhtälöt tehtävälle (7) samaan tapaan kuin tapauksessa (1), niin ratkaisua kuvaa ideaali $\mathcal{I}_{R_9}$, joka on täsmälleen analoginen ideaalin $\mathcal{I}_{R_6}$ kanssa (5). Tässä tapauksessa Singular antaa Gröbner-kannaksi

$$\mathcal{I}_{R_9} = \langle x_1 - 3, x_2 - 1, x_3 - 4, x_4 - 2, x_5 - 5, x_6 - 8, x_7 - 6, x_8 - 7, x_9 - 9 \rangle.$$

Survo-tehtävät voidaan siis edellä kuvattuun tapaan ratkaista systemaattisesti. Mutta mikä on tämän ratkaisun *vaativuus*?

Laskennan vaativuus

Laskennan vaativuusanalyysissä ajatellaan, että on joukko tietyllä tavalla parametrisoituja tehtäviä, ja halutaan tietää miten tehtävän hankaluus muuttuu parametrien funktiona. Eräs perusteellisesti analysoitu tehtäväluokka ovat lineaariset yhtälöryhmät, parametrina on tuntemattomien lukumäärä n, ja tiedetään, että käytettäessä Gaussin eliminointia tarvitaan $O(n^3)$ aritmeettista operaatiota. Merkintä $O(n^3)$ tarkoittaa, että kun n kasvaa, niin operaatioit-

ten lukumäärä on $cn^3 + b(n)$, missä c on vakio ja funktio b kasvaa hitaammin kuin n^3.

Myös Survo-tehtävissä luonnollinen parametri on muuttujien määrä n. Koska V_n on äärellinen joukko, niin ratkaisu saadaan periaatteessa käymällä läpi kaikki $n!$ vaihtoehtoa; tämän algoritmin vaativuus on siis $O(n!)$. Koska funktio $n!$ kasvaa erittäin nopeasti n:n funktiona, ei tästä algoritmista ole paljoa iloa.

Mikä sitten on Gröbner-kantoja käyttävän algoritmin vaativuus? En osaa täsmällisesti vastata, mutta tunnettua on, että Gröbner-kantojen laskennan vaativuus on yleisesti ottaen huono. Tähän voidaan osittain vaikuttaa valitsemalla ”sopiva” monomijärjestys, mutta toisaalta ei osata sanoa mikä olisi kuhunkin tilanteeseen parhaiten sopiva järjestys. Gröbner-kantojen vaativuusanalyysi on siis edelleen osittain avoin ongelma. Lisäksi laskennan vaativuudessa pitäisi ottaa huomioon myös muistitilan tarve. Edellä kuvattu siirtyminen äärellisiin kuntiin auttaa oleellisesti pienentämään tätä tarvetta. Mutta myös tarvittavien monomien määrä kasvaa varsin nopeasti. Merkitään termissä M_r^s olevien monomien lukumäärää $\#M_r^s$:llä. Tällöin

$$\#M_r^s = \frac{(r+s-1)!}{s!(r-1)!}$$

ja esimerkiksi

$$\#M_9^8 = \frac{16!}{8!8!} = 12870,$$

$$\#M_{51}^{50} = \frac{50!}{25!25!} = 126410606437752 \approx 1,26 \cdot 10^{14}.$$

Käytännössä pystyin kannettavallani varsin helposti ratkaisemaan tehtävän

x_1	x_2	x_3	x_4	24
x_5	x_6	x_7	x_8	15
x_9	x_{10}	x_{11}	x_{12}	39
21	10	18	29	

Tosin tässä en laskenut niin suoraviivaisesti kuin aiemmissa helpommissa esimerkeissä, mutta kaikki välivaiheet olivat pelkästään laskennallisen ideaaliteorian perusalgoritmien käyttöä, enkä käyttänyt mitään loogisella päättelyllä saatua lisätietoa. Sen sijaan tehtävässä

x_1	x_2	x_3	x_4	51
x_5	x_6	x_7	x_8	36
x_9	x_{10}	x_{11}	x_{12}	32
x_{13}	x_{14}	x_{15}	x_{16}	17
51	42	26	17	

kannettavani hyytyi muistin vähyyden takia. Tässä tehtävässä tarvitaan polynomia f_8, jossa on

$$1 + \#M_9^1 + \#M_9^2 + \cdots + \#M_9^8 = \frac{17!}{8!9!} = 24310$$

monomia. Nyt voisi kokeilla laskemista Lauseessa 1 mainitulla toisella kannalla; polynomien g_k termien määrähän on pieni. Valitettavasti tämä ei auta sillä välituloksissa esiintyvien polynomien monomien lukumäärä on edelleen hyvin suuri.

Mutta Survo-ongelmahan olikin oikeastaan asetettu huviksi, Sudokujen tapaan. Siis tämmöinen laskennan vaativuusanalyysi ei oikeastaan ”kuulu” alkuperäiseen tehtävänasetteluun. Kuitenkin jos jonkin tehtävän matemaattinen rakenne on liian selkeä, niin tehtävä väistämättä menettää mielenkiintoaan arvoituksena. Esimerkiksi jo hyvin kauan sitten lehdissä on ollut seuraavanlaisia tehtäviä:

(w1) Kauppiaalla on kolme purkkia. Purkkien tilavuuksien summa on 5. Ensimmäinen purkki on 2 kertaa isompi kuin toinen, ja toinen purkki on 3 kertaa isompi kuin kolmas. Mitkä ovat purkkien tilavuudet?

(w2) Kauppiaalla on kolme purkkia.

Purkkien tilavuuksien summa on $\frac{3465669}{13487}$.

Ensimmäinen purkki on $\frac{345634}{67867}$ kertaa isompi kuin toinen,

ja toinen purkki on $\frac{1299291}{4039103}$ kertaa isompi kuin kolmas.

Mitkä ovat purkkien tilavuudet?

Ensimmäisen tehtävän voisi kuvitella laskevansa päässälaskuna, mutta toinen on (ainakin minulle) liian ”vaikea”. Mutta jos on päässyt matematiikan opinnoissa siihen asti, ettei enää pelkää merkitä tuntemattomia kirjaimilla, niin heti huomaa, että molemmissa tapauksissa kyseessä on kolmen lineaarisen yhtälön ryhmä, ja tehtävät ovat siis tässä mielessä yhtä vaikeita.

Survo-ristikoilla on mielestäni samanlainen vika: kaikkien tehtävien rakenne on sama, laskennan vaativuus vain kasvaa muuttujien määrän kasvaessa.

Viitteet

[1] D. Cox, J. Little, and D. O’Shea, *Ideals, varieties and algorithms*, Springer, Berlin, 1992.

[2] G.-M. Greuel and G. Pfister, *A* **singular** *introduction to commutative algebra*, Springer-Verlag, Berlin, 2002, With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh, and UNIX).

[3] G.-M. Greuel, G. Pfister, and H. Schönemann, *Singular 3.0*, *A Computer Algebra System for Polynomial Computations*, Centre for Computer Algebra, University of Kaiserslautern, 2005, http://www.singular.uni-kl.de.