Tímarit um raunvísindi og stærðfræði
1. árg. 2. hefti 2003 – raust.is/2003/2/13

Notkun á tölvum við rannsóknir í víxlinni algebru

Freyja Hreinsdóttir

Raunvísindastofnun Háskólans

Vefútgáfa: 24. október 2003

Ágrip Tölvunotkun við rannsóknir innan víxlinnar algebru er mjög útbreidd. Við lýsum hér nokkrum grundvallaratriðum varðandi þessa notkun og sýnum dæmi þar sem tölvureikningar gáfu af sér tilgátu sem síðan var sönnuð með hefðbundnum aðferðum. Við gerum skil helstu forritapökkum sem í notkun eru og bendum á nýjustu bækur innan sviðsins.

1. Inngangur

Hér verður stuttlega lýst hvernig nota má tölvur við rannsóknir í víxlinni algebru og svipalgebru. Efninu eru á engan hátt gerð tæmandi skil enda afar víðfeðmt.

Við byrjum á að rekja þá þróun sem átt hefur sér stað innan víxlinnar algebru með tilkomu tölvualgebru og nefnum nokkur dæmi um hvað hægt er að reikna. Við lýsum svokölluðum Gröbner-grunnum, sem eru bakjarl flestra forrita sem notuð eru í víxlinni algebru, og sýnum dæmi um hagnýtingar þeirra. Við skoðum því næst dæmi úr eigin rannsóknum höfundar þar sem tölvureikningar leiddu til tilgátu, sem síðan var hægt að sanna með hefðbundnum aðferðum svipalgebru. Við sýnum með dæmi hvernig notkun á einum forritapakka, Macaulay2, fer fram og að lokum bendum við á helstu bækur og forritapakka sem notaðir eru við reikninga í víxlinni algebru.

2. Þróun og saga

Um miðjan sjöunda áratug síðustu aldar komu Gröbner-grunnar fram á sjónarsviðið. Þeir voru uppgötvaðir af H. Hironaka [11], sem kallaði þá staðalgrunna, og óháð honum af B. Buchberger [5] sem kallaði þá *Gröbner-grunna* eftir leiðbeinanda sínum W. Gröbner. Hófst þá þróun nýs rannsóknasviðs sem kalla mætti *víxlna reikni-algebru* (e. Computational Commutative Algebra) og sem einkum fæst við hvernig og hvaða fyrirbæri víxlinnar algebru sé hægt að reikna á viðunandi löngum tíma.

Á áttunda áratugnum betrumbætti Buchberger hugmyndir sínar, gerði þær aðgengilegri og forritaði reiknirit sín. Um svipað leyti urðu tölvur nothæfari og fólk sem stundaði rannsóknir í víxlinni algebru gat nú reiknað dæmi sem áður var einungis hægt að láta sig dreyma um. Þetta hefur síðan vakið upp margar nýjar spurningar. Reikniritið hefur þótt áhugavert út frá sjónarhorni algebru og rúmfræði, og það kemur víða við sögu þar sem beitt er algebrulegum aðferðum við lausnir á hagnýtum verkefnum.

3. Hvað er hægt að reikna?

Þau verkefni innan víxlinnar algebru þar sem tölvur geta komið að góðum notum eru margvísleg. Við nefnum hér nokkur atriði og förum gegnum helstu skilgreiningar sem þarf.

Hilbert-röð: Baugur R kallast *stigaður* (e. graded) ef skrifa má hann sem beina summu, $R = \bigoplus_{i\in\mathbb{N}} R_i$, þannig að $R_iR_j \subset R_{i+j}$ fyrir öll i, j. Stak í R_j kallast *einsleitt* (e. homogeneous) stak af stigi j. Íðal í R er *einsleitt* ef það er spannað af einsleitum stökum. Stigaður mótull yfir R er mótull M ásamt liðun $M = \bigoplus_{i\in\mathbb{Z}} M_i$, þannig að $R_iM_j \subset M_{i+j}$ fyrir öll i, j.

Dæmi um stigaðan baug er víxlni margliðubaugurinn $P = k[x_1, \ldots x_n]$, þar sem k er svið. Við getum skrifað P sem beina summu $P = P_0 \oplus P_1 \oplus \cdots$, þar sem P_j er mengi allra einsleitra margliða af stigi j (einsleit margliða af stigi j er summa einliða af stigi j). Ef I er einsleitt íðal þá er P/I stigaður mótull yfir P.

Ef við látum M vera endanlega spannaðan mótul yfir P þá er *Hilbert-fall* M skilgreint sem $H_M(s) := \dim_k M_s$, þ.e.a.s. vídd M_s sem vektorrúms yfir k. Hilbert sýndi að til er einkvæmt ákvörðuð margliða $P_M(s)$, af stigi $\leq n$, þannig að fyrir stór s er $H_M(s) = P_M(s)$. Þessi margliða kallast *Hilbert-margliða* M. Við skilgreinum *Hilbert-röð* mótulsins M sem $h_M(t) = \sum_{i \geq 0} \dim_k M_i t^i$. Sýna má að Hilbert-röðina má skrifa sem rætt fall $f(t)/(1-t)^n$, þar sem $f(t)$ er margliða með heiltölustuðlum.

Hilbert-röð og Hilbert-margliða baugs R fela í sér mikilvægar algebrulegar upplýsingar um bauginn (t.d. Krullvídd og Betti-tölur) sem og rúmfræðilegar upplýsingar um mótsvarandi víðerni (t.d. vídd og gráðu). Það er því mjög áhugavert að geta reiknað þær út.

Dæmi: Látum $P = k[x, y, z]$ og I vera íðalið spannað af x^2, xy, yz, xz^2, y^3 og z^4. Þá er I einsleitt íðal svo P/I er stigaður mótull yfir P. Með því að telja einliður af hverju stigi sést að $h_{P/I}(t) = 1 + 3t + 3t^2 + 1$.

Okstöðumótull: Fyrir íðal I, spannað af $f_1, \ldots, f_s$, viljum við reikna *okstöðumótul* (e. syzygy module) íðalsins, þ.e.a.s. P-mótulinn

$$\mathrm{Syz}_P(f_1, \ldots, f_s) = \{(g_1, \ldots, g_s) \in P^s \mid g_1 f_1 + \cdots + g_s f_s = 0\}.$$

Frjáls uppleysing: Fyrir mótul M skilgeinum við *frjálsa uppleysingu* á M sem fleygaða lest af frjálsum mótlum

$$\mathcal{F} : \cdots \to F_i \to \cdots \to F_1 \to F_0 \to M \to 0$$

Ef M er mótull yfir P er alltaf til endanleg frjáls uppleysing en ef M er mótull yfir P/I er uppleysingin óendanleg. Í fyrra tilvikinu felur uppleysingin í sér ýmsa algebrulega eiginleika M, svo sem dýpt yfir R, ef gefin er stysta uppleysingin getum við t.d. skorið úr um hvort mótull er Cohen-Macaulay, ef viss samhverfa kemur fram í víddum frjálsu mótlanna $F_0, \ldots$ þá er mótullinn Gorenstein eða hugsanlega fullkomið snið (e. complete intersection). Í báðum tilvikum er frjáls uppleysing notuð til að reikna svipgrúpur og hjásvipfræðigrúpur (Tor og Ext). Víddir frjálsu mótlanna $F_0, \ldots$ kallast *Betti-tölur* mótulsins M. Ef frjáls uppleysing er þekkt má lesa stuðla margliðunnar f (sem er teljari Hilbert-raðar) út úr Betti-tölum.

Viss hugtök úr víxlinni algebru eru ekki skilgreind hér að ofan. Við bendum lesanda á kennslubækur í faginu, t.d. [7], án þess þó að það sé skilyrði fyrir að skilja framhaldið.

Ein grundvallarforsenda þess að geta reiknað í $R = P/I$ er að við höfum leið til að skera úr um hvenær tvö stök h og g í P/I eru sama stakið, þ.e.a.s. að skera úr um hvort $h - g \in I$:

- Gefið $f \in P$, hvernig getum við ákvarðað hvort $f \in I$? (*Ideal Membership Problem*)

Dæmi: Er $x^2y^2z^3 + y^2z^5$ í íðalinu $I = \langle x^2 + xz, xy + y^2, yz + z^2 \rangle$?

Við vitum að sérhvert íðal í margliðubaugnum er endanlega spannað, þ.e. til eru $f_1, \ldots, f_s$ þannig að $I = (f_1, \ldots, f_s)$. Svo að spurninguna má umorða sem:

- Eru til $h_1, \ldots, h_s \in P$ þannig að $f = f_1 h_1 + \cdots + f_s h_s$?

Fyrir margliður í einni breytistærð er einfalt að skera úr um hvort stak sé í íðali. Baugurinn $k[x]$ er höfuðíðalabaugur svo sérhvert íðal I er á forminu $I = \langle g(x) \rangle$ og því

$$f(x) \in I \text{ þþaa } g(x) \mid f(x)$$

og við göngum úr skugga um þetta með venjulegri margliðudeilingu. Þetta gefur einnig einkvæmt ákvarðaða framsetningu á stökunum í $k[x]/I$, þ.e.a.s. við getum skrifað sérhvert $f \in k[x]/I$ sem $f = g \cdot q + r$ þar sem

$r = 0$ eða $\deg r < \deg g$. Eins og flestum er kunnugt þá deilum við þeim lið í g af hæsta stigi í þann lið f sem hefur hæsta stig, þ.e.a.s. reikniritið byggir á því að við getum *raðað* liðunum í bæði f og g eftir stigi.

Fyrir margliður í mörgum breytistærðum útvíkkum við deilingarreikniritið og reiknum svokallaðan *Gröbner-grunn* fyrir íðalið I. Til þess að það sé hægt þurfum við röðun á liðunum í hverri margliðu.

4. Raðanir á einliðum og Gröbner-grunnar

Táknum einliðu (*e. monomial*) í $k[x_1, \ldots, x_n]$ með $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ þar sem $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.

Skilgreining: *Einliðuröðun* á $k[x_1, \ldots, x_n]$ er röðun $>$ á mengi einliða x^α í $k[x_1, \ldots, x_n]$ sem uppfyllir:

a. Röðunin $>$ er línuleg.
b. Ef $x^\alpha > x^\beta$ og x^γ er einliða, þá er $x^{\alpha+\gamma} > x^{\beta+\gamma}$.
c. Röðunin $>$ er velröðun þ.e. sérhvert ekki tómt mengi af einliðum hefur minnsta stak.

Í $k[x]$ er röðun með tilliti til stigs eina einliðuröðunin, þ.e.a.s.

$$\cdots > x^{n+1} > x^n > \cdots > x^3 > x^2 > x > 1.$$

Fyrir margliðubauga í mörgum breytistærðum eru til margar mismunandi einliðuraðanir. Við skoðum hér tvær slíkar. Byrjum á að ákveða að

$$x_1 > x_2 > \cdots x_n.$$

Gefið þetta val skilgreinum við:
Stafrófsröðun (e. lexicographic order): $x^\alpha >_{lex} x^\beta$ ef í mismuninum $\alpha - \beta \in \mathbb{Z}^n$ þá er það stak, sem er lengst til vinstri af þeim sem eru frábrugðin 0, stærra en 0.

Öfug stiguð stafrófsröðun (e. graded reverse lexicographic order): $x^\alpha >_{grevlex} x^\beta$ ef $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$ eða ef $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ og í mismuninum $\alpha - \beta \in \mathbb{Z}^n$ þá er það stak, sem er lengst til hægri af þeim sem eru frábrugðin 0, minna en 0.

Til dæmis í $k[x, y, z]$, með $x > y > z$, þá er

$$x^3yz^2 >_{lex} x^2y^3z \quad \text{og} \quad x^2y^3z >_{grevlex} x^3yz^2$$

Látum nú $f \in k[x_1, \ldots, x_n]$ og $>$ vera einliðuröðun. Þá má skrifa $f = \sum_1^s c_i m_i$ þar sem $m_1 > m_2 \cdots > m_s$ eru einliður og $c_i \neq 0$, $i = 1, \ldots, s$. Þá kallast $c_1 m_1$ *forystuliður* f m.t.t. $>$, táknað $LT_>(f)$ og m_1 kallast *forystueinliða* f, táknað $LM_>(f)$.

Til dæmis er $LT_{>_{lex}}(3x^3z^2 + x^2y^2z) = 3x^3z^2$ og $LT_{>_{grevlex}}(3x^3z^2 + x^2y^2z) = x^2y^2z$.

Við fáum nú deilingarreiknirit fyrir $k[x_1, \ldots, x_n]$, þ.e.a.s. fyrir gefnar margliður $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ og gefna einliðuröðun $>$ þá má skrifa sérhvert $f \in k[x_1, \ldots, x_n]$ sem

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

þar sem $a_i, r \in k[x_1, \ldots, x_n], \forall i$ og annað hvort er $r = 0$ eða r er samantekt af einliðum sem ekki eru deilanlegar með $LT_>(f_1), \ldots, LT_>(f_s)$. Við köllum r *afgang* við deilingu með $(f_1, \ldots, f_s)$.

Skilgreining: Látum $>$ vera einliðuröðun á $k[x_1, \ldots, x_n]$ og $I \subseteq k[x_1, \ldots, x_n]$ vera gefið íðal. *Gröbner-grunnur* fyrir I, með tilliti til röðunarinnar $>$, er mengi spönnuða $G = \{g_1, \ldots, g_t\}$ fyrir I, þannig að fyrir sérhvert $f \in I$ gildir að $LT(f)$ er deilanlegt með $LT(g_i)$ fyrir eitthvert i.

Fyrir $f \in k[x_1, \ldots, x_n]$ er afgangurinn r við deilingu með Gröbner-grunninum einkvæmt ákvarðaður og kallast *staðalframsetning f mátað við I* (*e. normal form of f modulo I*), táknað $\bar{f}$. Við sjáum að $f \in I$ þá og því aðeins að $\bar{f} = 0$.

5. Reiknirit Buchbergers

Nú lýsum við hvernig reikna má Gröbner-grunn fyrir gefið íðal.

Látum f og g vera margliður í $k[x_1, \ldots, x_n]$. *S-margliðan* af f og g er skilgreind sem

$$S(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g$$

þar sem $x^\gamma = \mathrm{MSF}(\mathrm{LM}(f), \mathrm{LM}(g))$, $\mathrm{LE}(f)$ er forystueinliða f og MSF er minnsta samfeldi.

Látum $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ vera íðal. Þá má ákvarða Gröbner-grunn I í endanlega mörgum skrefum (sjá t.d. kafla 3 í [8]) með eftirfarandi reikniriti:

Inn: $F = (f_1, \ldots, f_s)$ (lágmarksspönnuðir)
Út: Gröbner-grunnur $G = (g_1, \ldots, g_t)$ fyrir I með $F \subseteq G$.

$G := F$
ENDURTAKIÐ
  $G' := G$
  FYRIR öll $\{p, q\}$, $p \neq q$ í G' GERIÐ
    $S := \overline{S(p,q)}^{G'}$
    EF $S \neq 0$ ÞÁ $G := G \cup \{S\}$
ÞAR TIL $G = G'$

Þar sem $\overline{S(p,q)}^{G'}$ er $S(p,q)$ mátað við stökin í G'.

Sérhver S-margliða, sem ekki verður núll mátað við stök sem fyrir eru, gefur nýja einliðu LT(S), sem ekki er í íðalinu sem spannað er af LT(g) fyrir $g \in G$. Þetta gefur vaxandi keðju af einliðuíðulum sem verður að stöðvast því P er Noetherskur. Reikniritið er því samleitið. Sönnun þess að reikniritið gefi Gröbner-grunn er nokkuð löng, sjá t.d. kafla 2.6 í [6].

Dæmi Látum $P = k[x,y]$ og $I = (f_1, f_2) = (x^2, xy - y^2)$ og reiknum Gröbner-grunninn með tilliti til stafrófsröðunnar (lex). Byrjum með $G = (f_1, f_2)$. Reiknum

$$S(f_1, f_2) = y \cdot f_1 - x \cdot f_2 = x^2 y - x^2 y + xy^2 = xy^2$$

Mátum xy^2 við G, sjáum að $LT(f_1) = x^2$ gengur ekki upp í xy^2 en það gerir hins vegar $LT(f_2) = xy$, svo við mátum við f_2 og fáum

$$xy^2 = yf_2 + y^3.$$

Nú er $y^3 < LT(f_i)$ fyrir $i = 1, 2$ svo að $\overline{S(f_1,f_2)}^{G} = y^3 \neq 0$ og þar með $G := (f_1, f_2, y^3)$.

Nú förum við í gegnum reikniritið aftur og reiknum $S(f_1, y^3)$ og $S(f_2, y^3)$. Fáum

$$S(f_1, y^3) = y^3 \cdot x^2 - x^2 \cdot y^3 = 0 \quad \text{og} \quad S(f_2, y^3) = y^2 \cdot (xy - y^2) - x \cdot y^3 = -y^4$$

og y^4 mátað við $G := (f_1, f_2, y^3)$ gefur 0. Þar með er Gröbner-grunnurinn (f_1, f_2, y^3).

Almennt er ljóst að flækjustig þessa reiknirits er mjög hátt, 2^{2^n} (sjá kafla 21 í [17]). Mörg dæmi eru hins vegar rýr á einhvern hátt eða hafa einhvers konar samhverfu eða mynstur sem gerir það að verkum að reiknitíminn er miklu minni en ætla mætti. Mjög afgerandi fyrir bæði reiknitíma og stærð Gröbner-grunns er hvaða röðun á breytum er valin. Bayer og Stillman [3] hafa sýnt að í flestum tilfellum er öfug stiguð stafrófsröðun (grevlex) best. Þetta er þó ekki algilt, sjá til dæmis [12].

6. Hagnýtingar Gröbner-grunna innan víxlinnar algebru

Í þessum kafla skoðum við hvernig nota má Gröbner-grunna við útreikninga í víxlinni algebru. Við skoðum einnig hvernig nota má Gröbner-grunna til að leysa ólínuleg jöfnuhneppi.

Við sjáum að gefinn G, Gröbner-grunnur íðals I, getum við ákvarðað staðalframsetningu $f \in P$ mátað við G. Við höfum að $f \in I$ þá og því aðeins að $\overline{f}^G = 0$ og $f = g$ í $R = P/I$ þá og því aðeins að $\overline{f-g}^G = 0$.

Sem aukaafurð úr reikniriti Buchberger fáum við okstöðumótulinn fyrir I. Þetta gerist þannig að sérhver $S-$margliða sem verður 0 gefur spönnuð í okstöðumótlinum.

Dæmi: Í dæminu hér á undan fengum við $\overline{S(f_1, y^3)}^G = 0$. Þetta gefur:

$$\begin{aligned} 0 = S(f_1, y^3) &= y^3 \cdot f_1 - x^2 \cdot y^3 \\ &= y^3 f_1 - x^2(xy^2 - y \cdot f_2) \\ &= y^3 f_1 - x^2((y \cdot f_1 - x \cdot f_2) - y \cdot f_2) \\ &= f_1(y^3 - x^2 y) + f_2(x^3 + x^2 y) \end{aligned}$$

Þar með höfum við fengið spönnuð $(y^3 - x^2y, x^3 + x^2y)$ í okstöðumótlinum og sýna má fram á að allir spönnuðir mótulsins fáist með þessum hætti.

Reiknirit Buchbergers fyrir Gröbner-grunn íðals má útvíkka til að reikna Gröbner-grunn fyrir mótul. Fyrir okstöðumótulinn má því eftir að spönnuðir hafa verið reiknaðir, reikna Gröbner-grunn og $S-$margliður og þar með okstöðumótul okstöðumótulsins o.s.frv. Þetta gefur uppleysingu á P/I.

Fyrir utan það sem nefnt er hér að ofan þá gefur Buchberger-reikniritið af sér aðferðir til að reikna til dæmis: mengi spönnuða fyrir $I \cap J$, $(I :_P J) = \{x \in P \mid x \cdot J \subseteq I\}$, $I \cap k[x_1, \ldots x_k]$ o.s.frv. Reikningar á frjálsri uppleysingu gefa af sér reikninga á ýmsum stærðum í svipalgebru, sjá til dæmis [16].

Eins og áður sagði má nota Gröbner-grunna til að reikna Hilbert-röð P/I. Macaulay [15] sannaði árið 1927 að Hilbert-röð P/I er sú sama og Hilbert-röð

$P/\operatorname{in}(I)$ þar sem $\operatorname{in}(I)$ er íðalið af öllum forystuliðum staka í I. Þegar við höfum $G = \{g_1, \ldots, g_t\}$, Gröbner-grunn íðalsins þá vitum við að $LT(G_1), \ldots, LT(g_t)$ spanna $\operatorname{in}(I)$. Að reikna Hilbert-röð einliðuíðals er fléttufræðilegt vandamál, sjá til dæmis [4].

Að lokum skoðum við hér dæmi um hvernig nota má Gröbner-grunna til að leysa ólínuleg jöfnuhneppi. Skoðum jöfnuhneppið:

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

Látum I vera íðalið $(x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1)$. Gröbner-grunnur fyrir I með tilliti til stafrófsröðunnar er:

$$\begin{aligned} g_1 &= x + y + z^2 - 1 \\ g_2 &= y^2 - y - z^2 + z \\ g_3 &= 2yz^2 + z^4 - z^2 \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2. \end{aligned}$$

Þar sem upphaflegu jöfnurnar og Gröbner-grunnurinn gefa spönnuði fyrir sama íðalið þá eru lausnir á $g_1 = g_2 = g_3 = g_4 = 0$ þær sömu og á upphaflega jöfnuhneppinu. Lausnir á $g_4 = 0$ eru $z = 0, 1, -1 \pm \sqrt{2}$. Innsetning á þessu í jöfnuna $g_2 = 0$ gefur y og að lokum fæst x úr jöfnunni $g_1 = 0$. Allar lausnir eru: $(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2})$.

7. Dæmi úr daglegu lífi algebrukonu

Í þessum kafla verður lítilega kynnt dæmi sem snýr að rannsóknum höfundar og sýnt hvernig tölvualgebruforritið Macaulay var notað til að fá fram tilgátu sem síðan var sönnuð með aðferðum úr svipalgebru.

Látum $X = (x_{ij})$ og $Y = (y_{ij})$, $i, j = 1, \ldots, n$ vera $n \times n$ fylki og látum I vera íðalið sem stökin í $XY - YX$ spanna í margliðubaugunum $P = k[x_{11}, \ldots, x_{nn}, y_{11}, \ldots, y_{nn}]$ (sjá [14]). Fyrir $n = 2$ er $P = k[x_{11}, x_{12}, x_{21}, x_{22}, y_{11}, y_{12}, y_{21}, y_{22}]$ og $I = (x_{12}y_{21} - x_{21}y_{12}, x_{21}y_{11} - x_{11}y_{21} + x_{22}y_{21} - x_{21}y_{22}, x_{11}y_{12} - x_{12}y_{11} + x_{12}y_{22} - x_{22}y_{21})$.

Fyrir $n = 2, 3, 4$ getum við reiknað Gröbner-grunn íðalsins með því að nota Macaulay [2] og því reiknað *hluta* af uppleysingu sviðsins k yfir $R = P/I$. Við fáum eftirfarandi Betti-tölur fyrir $n = 3$ og $n = 4$:

```
 % 1% 2% betti qp
; total:      1    18   161   965  4426
; --------------------------------------
;     0:      1    18   161   962  4356
;     1:      -     -     -     3    70

% 1% 2% 3% betti qp3
; total:      1    32   511  5449
; --------------------------------
;     0:      1    32   511  5442
;     1:      -     -     -     3
;     2:      -     -     -     4
```

Tölurnar í töflunni eru víddir í stiguðu Yoneda algebrunni

$$\mathrm{Ext}^*_R(k, k).$$

Tölurnar í fyrstu röðinni svara til hlutalgebrunnar $\mathrm{Ext}^1_R(k, k)$ sem einnig kallast *Koszul-nykur* baugsins, táknað með $R^!$. Við vitum að þetta er Hopf algebra og þar með hjúpalgebra stigaðrar Lie algebru

$$R^! = U(g) = U(g_1 \oplus g_2 \oplus \ldots).$$

Vitum líka að Hilbert-röð algebrunnar má skrifa sem óendanlega margfeldið

$$R^!(t) = \sum_{i=0}^{\infty} \dim_k(R^!_i)t^i = \prod_{i=0}^{\infty} \frac{(1 + t^{2i+1})^{\eta_{2i+1}}}{(1 - t^{2i+2})^{\eta_{2i+2}}},$$

þar sem $\eta_j = \dim_k(g_j)$ svo með því að bera saman stuðla í margfeldinu við töflurnar hér að ofan fæst að fyrir $n = 3, 4$, þá er $\eta_3 = 2$, $\eta_4 = 0$ svo að g er núllvalda.

Við setjum því fram eftirfarandi tilgátu:

Tilgáta: Ef $n \geq 3$ þá er Lie algebran g núllvalda af stigi 3 og $\dim g_1 = 2n^2$, $\dim g_2 = n^2 - 1$, $\dim g_3 = 2$.

Til að sanna þessa tilgátu reiknum við út (í höndunum) Koszul-nykur baugsins. Þetta er deildabaugur af *óvíxlna* margliðubaugnum $k\langle X_{ij}, Y_{ij}\rangle$ þar sem X_{ij} svarar til x_{ij} og Y_{ij} svarar til y_{ij}. Íðalið sem er mátað við í þessum óvíxlna baug fæst með lausn ákveðins jöfnuhneppis sem fæst úr upphaflega íðalinu (dæmi um spönnuði eru: $[X_{ir}, Y_{rj}] - [X_{is}, Y_{sj}]$ fyrir öll $r, s \in \{1, \ldots, n\}$). Við getum síðan sýnt beint (með því að skoða öll möguleg Lie-margfeldi) að af stigi 3 eru í mesta lagi 2 óháð stök, þ.e.a.s. $\dim g_3 \leq 2$ og að öll Lie-margfeldi af stigi > 3 eru 0 þannig að algebran er núllvalda. Til að sýna fram á að víddin er nákvæmlega 2 þá notfærum við okkur að $tr(X(XY - YX)) = 0$ og $tr(Y(XY - YX)) = 0$ gefur tvo línulega óháða spönnuði í okstöðumótli íðalsins I, svo vídd þess mótuls er að minnsta kosti 2 (sjá [13]).

8. Notkun Macaulay2

Hér fyrir neðan sýnum við dæmi um einfalda notkun MACAULAY2 [9].

Við byrjum á að skilgreina bauginn sem við reiknum í en hann er margliðubaugurinn í þremur breytistærðum yfir ræðu tölurnar $\mathbb{Q}$. Þegar við hefjum keyrslu forritsins fáum við "i1: ". Við sláum inn "R=QQ[x,y,z]". Forritið svarar með ”o1=R” og ”o1:PolynomialRing” sem þýðir að við höfum skilgreint breytuna R af gerðinni (type) margliðubaugur.

```
i1 :  R=QQ[x,y,z]

o1 = R

o1 : PolynomialRing
```

Við skilgreinum nú íðal með því að gefa spönnuði þess.

```
i2 : i=ideal(x^2+x*z, x*y+y^2, y*z+z^2)

             2              2         2
o2 = ideal (x + x*z, x*y + y , y*z + z )

o2 : Ideal of R
```

Við viljum reikna Gröbner-grunn íðalsins sem við skilgreindum. Þegar við skilgreindum bauginn í upphafi tiltókum við enga sérstaka einliðuröðun. Þá notar forritið sjálfgefnu röðunina *grevlex*. Ef við viljum nota aðra röðun t.d. *lex* þá tiltökum við hana með R=QQ[x,y,z, MonomialOrder=>Lex].

```
i3 : gb i

o3 = | yz+z2 xy+y2 x2+xz xz2-z3 y3-z3 z4 |

o3 : GroebnerBasis
```

Við sjáum að Gröbner-grunnurinn inniheldur upphaflegu spönnuðina og tvö stök af stigi 3 og eitt af stigi 4. Við reiknum næst uppleysingu íðalsins i.

```
i4 : F=res i

       1      3      3      1
o4 = R  <-- R  <-- R  <-- R  <-- 0

      0      1      2      3      4

o4 : ChainComplex
```

Við fáum víddir mótlanna í uppleysingunni. Við viljum líka sjá varpanirnar og gerum því

```
i5 : F.dd

           1                            3
o5 = 0 : R  <------------------------- R  : 1
               | x2+xz xy+y2 yz+z2 |

           3                                      3
  1 : R  <----------------------------------- R  : 2
             {2} | xy+y2  -yz-z2      0      |
```

```
            {2} | -x2-xz -yz-z2      -yz-z2 |
            {2} | 0      x2+xy+y2+xz xy+y2  |

          3                                        1
  2 : R  <---------------------------------- R  : 3
            {4} | 1/2yz+1/2z2              |
            {4} | 1/2xy+1/2y2              |
            {4} | -1/2x2-1/2xy-1/2y2-1/2xz |

          1
  3 : R  <----- 0 : 4
                0
```

```
o5 : ChainComplexMap
```

Til sð sjá víddirnar í uppleysingunni á þjöppuðu formi gefum við skipunina betti

```
i6 : betti F
```

```
o6 = total: 1 3 3 1
          0: 1 . . .
          1: . 3 . .
          2: . . 3 .
          3: . . . 1
```

Til að reikna Hilbert-röð íðalsins gerum við

```
i7 : hilbertSeries i
```

```
             2      4     6
      1 - 3$T  + 3$T  - $T
o7 = ---------------------
                    3
            (1 - $T)
```

```
o7 : Divide
```

Eins og áður sagði þá sannaði Macaulay árið 1927 að Hilbert-röð íðals I og Hilbert-röð $\mathrm{in}(I)$ væri sú sama. Við reiknum $\mathrm{in}(I)$ með

```
i8 : j=ideal(leadTerm i)
```

```
                        2     2   3   4
o8 = ideal (y*z, x*y, x , x*z , y , z )
```

```
o8 : Ideal of R
```

og sjáum að Hilbert-röðin er óbreytt

```
i9 : hilbertSeries(ideal(leadTerm i))
```

```
             2      4     6
     1 - 3$T  + 3$T  - $T
o9 = ---------------------
                    3
           (1 - $T)
```

```
o9 : Divide
```

9. Forrit og bækur

Hægt er að reikna Gröbner-grunna með ýmsum almennum tölvualgebruforritum svo sem Maple, Mathematica, Maxima, Reduce og Matlab (með því að nota útvíkkaðan táknrænan verkfærakassa). Fyrir umfangsmikla reikninga í algebru er oftast betra að notast við sérhæfðari forritapakka. Þessir eru hugsanlega ekki jafn notendavænir en hafa þann kost að vera ókeypis og hægt að nálgast þá yfir netið. Þeir eru yfirleitt skrifaðir af fólki sem stundar rannsóknir í algebru við ýmsa háskóla. Hér á eftir er upptalning af þeim helstu:

MACAULAY: Einn mest notaði forritapakkinn í víxlinni algebru hefur verið MACAULAY [2] og arftaki hans MACAULAY2 [9]. Höfundar þessara pakka eru M. Stillman, D. Bayer og D. Grayson. Einnig hefur D. Eisenbud skrifað fjölda smáforrita (scripts) sem byggja á þessum pakka og fylgja honum. Nýlega (september 2001) kom hjá Springer Verlag bókin: *Computations in Algebraic Geometry with Macaulay 2* sem ritstýrt var af David Eisenbud, Daniel R. Grayson, Michael Stillman og Bernd Sturmfels. Hægt er að nálgast bókina á http://www.math.uiuc.edu/Macaulay2/Book/.

COCOA: Við háskólann í Genoa á Ítalíu hefur verið þróaður pakkinn COCOA [1] sem fyrir reikninga í víxlinni algebru og algebrulegri rúmfræði. Bókin *Computational Commutative Algebra 1*, eftir L. Robbiano og M. Kreuzer er kennslubók í reiknialgebru sem einkum byggir á COCOA. Von er á öðru bindi árið 2004.

SINGULAR: Við háskólann í Kaiserslautern í Þýskalandi hefur pakkinn SINGULAR [10] verið skrifaður. Hér hefur líka verið skrifuð bók, *A Singular Introduction to Commutative Algebra*, eftir G.M. Greuel og Gerhard Pfister.

MAGMA: Við háskólann í Sidney í Ástralíu hefur verið skrifaður pakkinn MAGMA (http://magma.-maths.usyd.edu.au/magma/).

BERGMAN: Við Stokkhólmsháskóla hefur J. Backelin ásamt fleirum þróað forritapakkann BERGMAN sem reiknar Gröbner-grunna fyrir íðul í víxlum og óvíxlnum margliðubaugum. BERGMAN er í stöðugri þróun og er með hraðvirkari forritum. BERGMAN má nálgast á http://servus.math.su.se/bergman/.
Fyrir utan þær bækur sem eru nefndar hér fyrir ofan er, fyrir þá sem vilja kynna sér reiknialgebru, úr fjölda bóka að velja. Hér á eftir verða nefndar nokkrar slíkar, listinn er þó alls ekki tæmandi.

Grunnbækur um Gröbner-grunna
1. W. Adams og P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics 3, AMS 1994.
2. T. Becker og V. Weispfenning, *Gröbner bases. A Computational approach to commutative algebra*, Springer 1993.
3. D. Cox, J. Little og D. O'Shea, *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer 1992.
4. R. Fröberg, *An Introduction to Gröbner Bases*, Wiley and sons 1997.
Sérhæfðari bækur og hagnýtingar
5. D. Cox, J. Little og D. O'Shea, *Using Algebraic Geometry*, Springer 1998.
6. D. Cox og B. Sturmfels (ritstjórn), *Applications of Computational Algebraic Geometry*, AMS 1998.
7. B. Buchberger og F. Winkler (ritstjórn), *Gröbner Bases and Applications*, LMS 251, Cambridge 1998.
8. H. Derksen og G. Kemper, *Computational Invariant theory*, Springer 2002.
9. K. Gaterman, *Computer Algebra Methods for Equivariant Dynamical Systems*, LNS 1728, Springer 2000.
10. J. Grabmeier, E. Kaltofen og V. Weisphenning, *Computer Algebra Handbook*, Springer 2003.
11. G. Pistone, E. Riccomagno og H. Wynn, *Algebraic Statistics: Computational Algebra in Statistics*, CRC Press 2000.
12. H. Schenck, *Computational Algebraic Geometry*, LMS Student Texts 58, 2003.
13. M. Saito, B. Sturmfels og N. Takayama, *Gröbner Deformations of Hypergeometric Differential Equations*, Springer 2000.
14. B. Sturmfels, *Gröbner bases and Convex Polytopes*, AMS 1996.

15. B. Sturmfels, *Solving Systems of Polynomial Equations*. Regional Conference Series in Mathematics 97, AMS 2002.
16. W. Vasconcelos, D. Eisenbud og J. Herzog, *Computational Methods in Commutative Algebra and Algebraic Geometry,* Springer 1997.

Summary: Computers are used extensively in research in Commutative algebra and Algebraic Geometry. This development started in the sixties with the work of Buchberger and Hironaka and the field is still expanding very rapidly. In this article we give some key definitions needed from Commutative Algebra and define Gröbner bases which are the backbone of the computations. We give a simple version of a Gröbner basis algorithm as well as examples of how this is utilized in and outside of Commutative Algebra. We show how computer results led to a conjecture that was proven by homological methods. Finally a summary of relevant software and books is given.

Heimildir

[1] J. Abbott, A. Bigatti, M. Caboara, A. Capani, M. Kreuzer, G. Niesi, D. Perkinson, A. Polverini, L. Robbiano, *CoCoA, a system for doing Computations in Commutative Algebra*, fæst á http://cocoa.dima.unige.it.
[2] D. Bayer, M. Stillman, *Macaulay: A system for computation in algebraic geometry and commutative algebra*, fæst á http://www.math.columbia.edu/˜bayer/Macaulay.
[3] D. Bayer and M. Stillman, A criterion for detecting m-regularity, *Invent. Math.* **87**, 1-11, (1987).
[4] D. Bayer and M. Stillman, Computation of Hilbert functions, *J. Symb. Comp.*, **14**, 31-50 (1992).
[5] B. Buchberger, *Ein Algorithmus zum affinden der Basielemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, doktorsritgerð Innsbruck, 1965.
[6] D. Cox, J. Little og D. O'Shea, *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, 1992.
[7] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics **150**, Springer-Verlag, 1995.
[8] R. Fröberg, *An Introduction to Gröbner Bases*, John Wiley & Sons, 1997.
[9] D. Grayson, M. Stillman, *Macaulay 2, a software system for research in algebraic geometry*, fæst á http://www.math.uiuc.edu/Macaulay2/.
[10] G.-M. Greuel, G. Pfister, H. Schönemann. SINGULAR 2.0. A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern (2001), http://www.singular.uni-kl.de.
[11] H. Hironaka, Resolution of singularities of an algebraic variety over a field of characteristic zero, *Ann. Math.*, **79**(1), I: 109-203, II:205-326 (1964).
[12] F. Hreinsdóttir, A case where choosing a product order makes the calculations of a Gröbner basis much faster, *J. Symb. Comp.*, **18**, 373-378 (1994).
[13] F. Hreinsdóttir, The Koszul dual of the ring of commuting matrices, *Comm. Alg.*, **26**, 3807-3819 (1998).
[14] F. Hreinsdóttir, *On the ring of commuting matrices*, doktorsritgerð við Stokkhólmsháskóla, 1997.
[15] F.S. Macaulay, Some properties of enumeration in the theory of modular systems, *Proc. London Math. Soc.*, 26, 531 - 555 (1927).
[16] J.E. Roos, A computer-aided study of the graded Lie-algebra of a local commutative noetherian ring, *J. Pure Appl. Algebra*, **91**, 255-315 (1994).
[17] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, 1999.

Um höfundinn: Freyja Hreinsdóttir fæddist á Raufarhöfn árið 1964. Hún lauk stúdentsprófi frá Menntaskólanum að Laugarvatni árið 1983, BS prófi í stærðfræði frá HÍ árið 1986, MS prófi í stærðfræði frá Northwestern University árið 1988 og doktorsprófi frá Stokkhólmsháskóla árið 1997. Hún starfaði við kennslu og rannsóknir við Háskóla Mälardalsins, Tækniháskólann í Stokkhólmi og Stokkhólmsháskóla á árunum 1997-2001. Hún hefur verið sérfræðingur við stærðfræðistofu Raunvísindastofnunar frá 2001. Rannsóknasvið Freyju eru víxlin algebra, reiknialgebra og svipalgebra.

Raunvísindastofnun Háskólans, Dunhaga 3, IS-107 Reykjavík
freyjah@hi.is

Móttekin: 15. ágúst 2003