resultant_lcm.mws

Math 262a, Fall 1999, Glenn Tesler
LCM, GCD of commutative and noncommutative polynomials using resultants
11/11/99

```
> restart;
  with(linalg):  # maple linear algebra package
  with(Ore_algebra): # Chyzak's Ore algebra package
Warning, new definition for norm
Warning, new definition for trace
```

(Misc. routines -- hidden)

Compute the LCM of two polynomials by using the Sylvester matrix

```
> p := expand(((x-1)*(x-2))^2); degp := degree(p,x);
  q := expand(((x^2-1)*(x-3))^2); degq := degree(q,x);
```

$$p := x^4 - 6\,x^3 + 13\,x^2 - 12\,x + 4$$

$$degp := 4$$

$$q := x^6 - 6\,x^5 + 7\,x^4 + 12\,x^3 - 17\,x^2 - 6\,x + 9$$

$$degq := 6$$

Ordinary computation first:

```
> lcm(p,q),factor(lcm(p,q)); gcd(p,q),factor(gcd(p,q));
```

$$x^8 - 10\,x^7 + 35\,x^6 - 40\,x^5 - 37\,x^4 + 110\,x^3 - 35\,x^2 - 60\,x + 36,$$
$$(x-1)^2\,(x-2)^2\,(x-3)^2\,(x+1)^2$$

$$x^2 - 2\,x + 1,\ (x-1)^2$$

Form a Sylvester matrix.

```
> s := -1; pcols := 1..(degq+s+1); qcols :=
  (degq+s+2)..(degp+degq+2*s+2);
  maxrow := degp+degq+s+1; pqrows := 1..maxrow;
  S := sylv(p,q,x,s): 'S' = illsylv(p,q,x,s); # show
  row/column titles
```

$$s := -1$$

$$pcols := 1\,..\,6$$

$$qcols := 7\,..\,10$$

$$maxrow := 10$$

$$pqrows := 1 .. 10$$

$$S = \begin{bmatrix} & P & x\,P & x^2\,P & x^3\,P & x^4\,P & x^5\,P & Q & x\,Q & x^2\,Q & x^3\,Q \\ coef.\ of\ \ x^0 & 4 & 0 & 0 & 0 & 0 & 0 & 9 & 0 & 0 & 0 \\ coef.\ of\ \ x^1 & -12 & 4 & 0 & 0 & 0 & 0 & -6 & 9 & 0 & 0 \\ coef.\ of\ \ x^2 & 13 & -12 & 4 & 0 & 0 & 0 & -17 & -6 & 9 & 0 \\ coef.\ of\ \ x^3 & -6 & 13 & -12 & 4 & 0 & 0 & 12 & -17 & -6 & 9 \\ coef.\ of\ \ x^4 & 1 & -6 & 13 & -12 & 4 & 0 & 7 & 12 & -17 & -6 \\ coef.\ of\ \ x^5 & 0 & 1 & -6 & 13 & -12 & 4 & -6 & 7 & 12 & -17 \\ coef.\ of\ \ x^6 & 0 & 0 & 1 & -6 & 13 & -12 & 1 & -6 & 7 & 12 \\ coef.\ of\ \ x^7 & 0 & 0 & 0 & 1 & -6 & 13 & 0 & 1 & -6 & 7 \\ coef.\ of\ \ x^8 & 0 & 0 & 0 & 0 & 1 & -6 & 0 & 0 & 1 & -6 \\ coef.\ of\ \ x^9 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The definition of the resultant is Res(p,q,x) = det(Syl(p,q,x))

Certainly the columns of S0 below are linearly dependent because there are more columns than rows!
Any dependence S0 * [a b]^t (where length(a)=# columns of S with multiples of p, length(b)=same for q)
yields   a*(first cols of S0) =-b*(rest of cols) = common multiple of p and q.

```
S0 := sylv(p,q,x,0);
```

$$S0 := \begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 9 & 0 & 0 & 0 & 0 \\ -12 & 4 & 0 & 0 & 0 & 0 & 0 & -6 & 9 & 0 & 0 & 0 \\ 13 & -12 & 4 & 0 & 0 & 0 & 0 & -17 & -6 & 9 & 0 & 0 \\ -6 & 13 & -12 & 4 & 0 & 0 & 0 & 12 & -17 & -6 & 9 & 0 \\ 1 & -6 & 13 & -12 & 4 & 0 & 0 & 7 & 12 & -17 & -6 & 9 \\ 0 & 1 & -6 & 13 & -12 & 4 & 0 & -6 & 7 & 12 & -17 & -6 \\ 0 & 0 & 1 & -6 & 13 & -12 & 4 & 1 & -6 & 7 & 12 & -17 \\ 0 & 0 & 0 & 1 & -6 & 13 & -12 & 0 & 1 & -6 & 7 & 12 \\ 0 & 0 & 0 & 0 & 1 & -6 & 13 & 0 & 0 & 1 & -6 & 7 \\ 0 & 0 & 0 & 0 & 0 & 1 & -6 & 0 & 0 & 0 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

But we’ll use the square matrix S that’s just a little smaller. If (p,q) are relatively prime then S is invertible and we fail to find the common multiple p*q, but in all other cases, we do find the least common multiple.

```
> Nul_S := nullspace(S);
```

$$Nul\_S := \{[-9, -12, 2, 4, -1, 0, 4, -4, 1, 0], [-36, -57, -4, 18, 0, -1, 16, -12, 0, 1]\}$$

Any vector in the nullspace has two parts,
    v = [a b]^transpose,

where the first deg(p) columns of S &* a
= - last deg(q) columns of S &* b
= coefficient vector of a common multiple of p and q.
Because we have arranged the columns of S in the order we did, the vector v with the most trailing 0's is the one producing the least degree common multiple.

(function to find the vector with most leading 0's)

```
> bestv := getbestv(Nul_S):
  bestv0 := bestv[2]: bestv := bestv[1]:
  print(‘nullspace vector giving LCM is‘,bestv,‘
  with‘,bestv0-1,‘trailing 0’s‘);
```

nullspace vector giving LCM is, [-9, -12, 2, 4, -1, 0, 4, -4, 1, 0], *with*, 1, *trailing 0's*

(function to take selected columns of S * same selected components of vector, and then express the resulting vector as the polynomial it encodes)

Compute the LCM using the first part of the vector:

```
> infolevel[halfcombo] := 1;
  lcm_pq := halfcombo(S,bestv,pcols,x);
```

$$infolevel_{halfcombo} := 1$$

```
halfcombo:
```

$$\begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 \\ -12 & 4 & 0 & 0 & 0 & 0 \\ 13 & -12 & 4 & 0 & 0 & 0 \\ -6 & 13 & -12 & 4 & 0 & 0 \\ 1 & -6 & 13 & -12 & 4 & 0 \\ 0 & 1 & -6 & 13 & -12 & 4 \\ 0 & 0 & 1 & -6 & 13 & -12 \\ 0 & 0 & 0 & 1 & -6 & 13 \\ 0 & 0 & 0 & 0 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \&* \begin{bmatrix} -9 \\ -12 \\ 2 \\ 4 \\ -1 \\ 0 \end{bmatrix} = \begin{bmatrix} -36 \\ 60 \\ 35 \\ -110 \\ 37 \\ 40 \\ -35 \\ 10 \\ -1 \\ 0 \end{bmatrix}, \text{--->}$$

$$lcm\_pq := -36 + 60\,x + 35\,x^2 - 110\,x^3 + 37\,x^4 + 40\,x^5 - 35\,x^6 + 10\,x^7 - x^8$$

and the second part:

```
> halfcombo(S,bestv,qcols,x);
halfcombo:
```

$$\begin{bmatrix} 9 & 0 & 0 & 0 \\ -6 & 9 & 0 & 0 \\ -17 & -6 & 9 & 0 \\ 12 & -17 & -6 & 9 \\ 7 & 12 & -17 & -6 \\ -6 & 7 & 12 & -17 \\ 1 & -6 & 7 & 12 \\ 0 & 1 & -6 & 7 \\ 0 & 0 & 1 & -6 \\ 0 & 0 & 0 & 1 \end{bmatrix} \&* \begin{bmatrix} 4 \\ -4 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 36 \\ -60 \\ -35 \\ 110 \\ -37 \\ -40 \\ 35 \\ -10 \\ 1 \\ 0 \end{bmatrix}, --->$$

$$x^8 - 10\,x^7 + 35\,x^6 - 40\,x^5 - 37\,x^4 + 110\,x^3 - 35\,x^2 - 60\,x + 36$$

```
> factor(");
```

$$(x-1)^2\,(x-2)^2\,(x-3)^2\,(x+1)^2$$

To compute a GCD, we want a linear combination a(x)*p(x) + b(x)*q(x) = g(x) <> 0 with as many high powers of x having 0 coefficient as possible.
Specifically, deg(p) + deg(q) = deg(lcm) + deg(gcd)
gives the required degree of the gcd, and all higher powers should be annihilated.

```
> S_top := submatrix(S, bestv0+1-s..maxrow,
                    1..(degp+degq+2*s+2));
```

$$S\_top := \begin{bmatrix} -6 & 13 & -12 & 4 & 0 & 0 & 12 & -17 & -6 & 9 \\ 1 & -6 & 13 & -12 & 4 & 0 & 7 & 12 & -17 & -6 \\ 0 & 1 & -6 & 13 & -12 & 4 & -6 & 7 & 12 & -17 \\ 0 & 0 & 1 & -6 & 13 & -12 & 1 & -6 & 7 & 12 \\ 0 & 0 & 0 & 1 & -6 & 13 & 0 & 1 & -6 & 7 \\ 0 & 0 & 0 & 0 & 1 & -6 & 0 & 0 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

These vectors will kill the coefficients of the top powers of x: (This is the right nullspace, vectors v with M v = 0.. These are properly column vectors, but Maple turns them into row vectors.)

```
> Nul_S_top := nullspace(S_top);
```

$$Nul\_S\_top := \left\{\left[\frac{-27}{4}, -9, \frac{-15}{2}, -1, \frac{5}{4}, 0, 0, 1, \frac{-5}{4}, 0\right], [-27, -27, -18, -6, 1, 1, 0, 0, -1, -1], [-9, -12, -7, 0, 1, 0, 1, 0, -1, 0]\right\}$$

Note Nul_S_top contains Nul_S as a subspace, and is one dimension higher.
All vectors v in Nul_S_top give rise to linear combinations a(x)*p(x) + b(x)*q(x) that annihilate the necessary high degree coefficients of x. If v is in Nul_S as well, this linear combination is 0; otherwise it is a nonzero scalar multiple of the gcd. So we just need one vector in Nul_S_top \ Nul_S.

```
> infolevel[halfcombo] :=0:
  for vec in Nul_S_top do
     g :=
  halfcombo(S,vec,pcols,x)+halfcombo(S,vec,qcols,x):
     print(evalm(vec),‘--->‘,expand(g)=factor(g))
  od:
```

$$[-9, -12, -7, 0, 1, 0, 1, 0, -1, 0], --->, -27+54\,x-27\,x^2=-27\,(x-1)^2$$

$$[-27, -27, -18, -6, 1, 1, 0, 0, -1, -1], --->, -108+216\,x-108\,x^2=-108\,(x-1)^2$$

$$\left[\frac{-27}{4}, -9, \frac{-15}{2}, -1, \frac{5}{4}, 0, 0, 1, \frac{-5}{4}, 0\right], --->, -27+54\,x-27\,x^2=-27\,(x-1)^2$$

Now do the same thing to find the left LCM or right GCD of noncommutative polynomials.

```
> A := shift_algebra([Sn,n]); # Chyzak’s Sn = our En:  Sn
  f(n) = f(n+1)
```

$$A := Ore\_algebra$$

```
> p := skew_product(  n*Sn^2,n*Sn-1,A); degp :=
  degree(p,Sn);
  q := skew_product(n*Sn^3+1,n*Sn-1,A); degq :=
  degree(q,Sn);
```

$$p := (n^2+2\,n)\,Sn^3-n\,Sn^2$$

$$degp := 3$$

$$q := -1-n\,Sn^3+(n^2+3\,n)\,Sn^4+n\,Sn$$

$$degq := 4$$

Form a Sylvester matrix

```
> s := -1: pcols := 1..(degq+s+1); qcols :=
  (degq+s+2)..(degp+degq+2*s+2);
  maxrow := degp+degq+s+1; pqrows := 1..maxrow;
  S := sylv(p,q,Sn,s,A): ’S’ = illsylv(p,q,Sn,s,A); # show
  row/column titles
```

$$pcols := 1\,..\,4$$

$$qcols := 5\,..\,7$$

$$maxrow := 7$$

$$pqrows := 1\,..\,7$$

$$S = \begin{bmatrix} , & P, & Sn\,P, & Sn^2\,P, & Sn^3\,P, & Q, & Sn\,Q, & Sn^2\,Q \\ coef.\ of\ \ Sn^0, & 0, & 0, & 0, & 0, & -1, & 0, & 0 \\ coef.\ of\ \ Sn^1, & 0, & 0, & 0, & 0, & n, & -1, & 0 \\ coef.\ of\ \ Sn^2, & -n, & 0, & 0, & 0, & 0, & n+1, & -1 \\ coef.\ of\ \ Sn^3, & n^2+2\,n, & -1-n, & 0, & 0, & -n, & 0, & n+2 \\ coef.\ of\ \ Sn^4, & 0, & 4\,n+3+n^2, & -2-n, & 0, & n^2+3\,n, & -1-n, & 0 \\ coef.\ of\ \ Sn^5, & 0, & 0, & 6\,n+8+n^2, & -n-3, & 0, & 5\,n+4+n^2, & -2-n \\ coef.\ of\ \ Sn^6, & 0, & 0, & 0, & n^2+8\,n+15, & 0, & 0, & n^2+7\,n+10 \end{bmatrix}$$

```
> Nul_S := nullspace(S);
```

$$Nul\_S := \left\{\left[1, 0, 0, \frac{n\,(n+2)}{n+3}, 0, 0, -n\right]\right\}$$

```
> bestv := getbestv(Nul_S):
  bestv0 := bestv[2]: bestv := bestv[1]:
  print(‘nullspace vector giving LCM is‘,bestv,‘
  with‘,bestv0-1,‘trailing 0’s‘);
```

$$nullspace\ vector\ giving\ LCM\ is, \left[1, 0, 0, \frac{n\,(n+2)}{n+3}, 0, 0, -n\right],\ with, 0, trailing\ 0's$$

Compute the LCM using the first part of the vector:

```
> infolevel[halfcombo] := 1;
  lcm_pq := halfcombo(S,bestv,pcols,Sn);
```

$$infolevel_{halfcombo} := 1$$

```
halfcombo:
```

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -n & 0 & 0 & 0 \\ n^2+2\,n & -1-n & 0 & 0 \\ 0 & 4\,n+3+n^2 & -2-n & 0 \\ 0 & 0 & 6\,n+8+n^2 & -n-3 \\ 0 & 0 & 0 & n^2+8\,n+15 \end{bmatrix} \&* \begin{bmatrix} 1 \\ 0 \\ 0 \\ \frac{n\,(n+2)}{n+3} \end{bmatrix} =$$

$$\left[\begin{array}{c} 0 \\ 0 \\ -n \\ n^2+2n \\ 0 \\ \frac{(-n-3)\,n\,(n+2)}{n+3} \\ \frac{(n^2+8n+15)\,n\,(n+2)}{n+3} \end{array}\right], \text{--->}$$

$lcm\_pq :=$

$$-n\,Sn^2 + (n^2+2n)\,Sn^3 + \frac{(-n-3)\,n\,(n+2)\,Sn^5}{n+3} + \frac{(n^2+8n+15)\,n\,(n+2)\,Sn^6}{n+3}$$

```
> # The expressions get quite messy, clean them up.
  cleanpol := f -> sort(collect(expand(f),Sn,factor),Sn):

  lcm_pq := cleanpol(lcm_pq);
```

$$lcm\_pq := (n+5)\,(n+2)\,n\,Sn^6 - n\,(n+2)\,Sn^5 + n\,(n+2)\,Sn^3 - n\,Sn^2$$

and the second part:

```
> cleanpol(halfcombo(S,bestv,qcols,Sn));
halfcombo:
```

$$\left[\begin{array}{ccc} -1 & 0 & 0 \\ n & -1 & 0 \\ 0 & n+1 & -1 \\ -n & 0 & n+2 \\ n^2+3n & -1-n & 0 \\ 0 & 5n+4+n^2 & -2-n \\ 0 & 0 & n^2+7n+10 \end{array}\right] \&* \left[\begin{array}{c} 0 \\ 0 \\ -n \end{array}\right] = \left[\begin{array}{c} 0 \\ 0 \\ n \\ -n\,(n+2) \\ 0 \\ -n\,(-2-n) \\ -(n^2+7n+10)\,n \end{array}\right], \text{--->}$$

$$-(n+5)\,(n+2)\,n\,Sn^6 + n\,(n+2)\,Sn^5 - n\,(n+2)\,Sn^3 + n\,Sn^2$$

Chyzak’s LCM computation by Euclidean algorithm: annihilators(p,q,A) ---> [U,V] s.t. U*p = -V*q = LCM

```
> UV := annihilators(p,q,A):
  cleanpol(skew_product(UV[1],p,A));
```

$$n\,(n+5)\,(n+3)\,(n+2)\,Sn^6 - n\,(n+3)\,(n+2)\,Sn^5 + n\,(n+3)\,(n+2)\,Sn^3 - n\,(n+3)\,Sn^2$$

It returned (n+3) * our LCM. n+3 is in the ground field Q(n), so that’s O.K.

Compute GCD:

```
> S_top := submatrix(S, bestv0+1-s..maxrow,
                     1..(degp+degq+2*s+2));
```

$$S\_top := \begin{bmatrix} -n, & 0, & 0, & 0, & 0, & n+1, & -1 \\ n^2+2n, & -1-n, & 0, & 0, & -n, & 0, & n+2 \\ 0, & 4n+3+n^2, & -2-n, & 0, & n^2+3n, & -1-n, & 0 \\ 0, & 0, & 6n+8+n^2, & -n-3, & 0, & 5n+4+n^2, & -2-n \\ 0, & 0, & 0, & n^2+8n+15, & 0, & 0, & n^2+7n+10 \end{bmatrix}$$

These vectors will kill the coefficients of the top powers of Sn:

```
> Nul_S_top := nullspace(S_top);
```

$$Nul\_S\_top := \{\left[0, 1, 0, 0, -\frac{n+1}{n}, 0, 0\right], \left[-\frac{1}{n}, 0, 0, -\frac{n+2}{n+3}, 0, 0, 1\right]\}$$

```
> infolevel[halfcombo] :=0:
  g0 := 0:
  for vec in Nul_S_top do
     g :=
  halfcombo(S,vec,pcols,Sn)+halfcombo(S,vec,qcols,Sn):
     g := cleanpol(g):
     if g<>0 then g0 := g fi:
     print(evalm(vec),‘--->‘,cleanpol(g))
  od:
```

$$\left[0, 1, 0, 0, -\frac{n+1}{n}, 0, 0\right], \text{--->}, (-1-n)\,Sn + \frac{n+1}{n}$$

$$\left[-\frac{1}{n}, 0, 0, -\frac{n+2}{n+3}, 0, 0, 1\right], \text{--->}, 0$$

It’s hard to tell from the above that it’s just a "scalar" (independent of Sn, so it’s rational in n) multiple of n*Sn-1. But it is:

```
> factor(g0);
```

$$-\frac{(n+1)(n\,Sn-1)}{n}$$

Chyzaak’s GCD computation by Euclidean algorithm:

```
> skew_gcdex(p,q,Sn,A)[1];
```

$$-1-n+n^2\,Sn+n\,Sn$$

```
> factor(");
```

$$(n+1)(n\,Sn-1)$$

```
>
>
```