MAP,14-19 dec 2009, Monastir
Sylvester double sums and subresultants

Marie-Françoise Roy
Université de Rennes 1

Aviva Szpirglas
Université de Poitiers

Sylvester double sums versus subresultants
given two polynomials A and B
first notion symmetric expression of the roots of two polynomials
second notion defined through the coefficients polynomials

main result of the lecture
these two notions are very closely related
(idea due to Sylvester [S])
see details and complete proofs in [RS].

1 Definitions and main result.

A and B two finite families of elements of a field K.
The *resultant of A and B* is

$$R(A,B) := \prod_{a\in A, b\in B} (a-b).$$

$$R(A,\emptyset) = 1.$$

If $A\cap B \neq \emptyset$,

$$R(A,B) = 0,$$

$$R(X,A) := \prod_{a\in A} (X-a) \in K[X], \quad R(X,B) := \prod_{b\in B} (X-b) \in K[X],$$

$$R(X, A\cap B) = \gcd(R(X,A), R(X,B)).$$

1.1 Sylvester double sums

A finite, C subset of A with cardinality p, denoted $C \subset_p A$.
A, B finite sets, p, q two natural numbers $p+q \leq \min(\#B, \#A)$,
Sylvester double sum with exponent (p,q), denoted $\mathrm{Sylv}^{p,q}$

$$\mathrm{Sylv}^{p,q}(A,B)(X) = \sum_{\substack{C\subset_p A\\ D\subset_q B}} R(X,C)R(X,D)\frac{R(C,D)R(A\setminus C, B\setminus D)}{R(C,A\setminus C)R(D,B\setminus D)}$$

Remark 1.

1. degree of $\mathrm{Sylv}^{p,q}(A,B)(X)$ with respect to X $\leq p+q$.
2. $\mathrm{Sylv}^{0.0}(A,B)(X) = R(A,B)$.
3. a non zero Sylvester double sum of smallest possible degree is a gcd of $R(X,\ A)$ and $R(X,\ B)$. More precisely, if j is the number of elements of $A\cap B$,
   a. for every p, q such that $j = p+q$,
      $\mathrm{Sylv}^{p,q}(A,B)(X) = \gcd(R(X,A), R(X,B))$,
   b. for every p, q such that $j > p+q$,
      $\mathrm{Sylv}^{p,q}(A,B)(X) = 0$.

Properties 1 and 2 follow from the definition. Properties 3(a) and 3(b) follow from the fact that if $\sharp(C) = p, \sharp(D) = q$,

- if $p+q = \sharp(A\cap B)$, $C\cup D = A\cap B$,
  $$R(X,C)R(X,D) = R(X, A\cap B) = \gcd(R(X,A), R(X,B)),$$
- if $p+q < \sharp(A\cap B)$ or if ($p+q = \sharp(A\cap B)$ and $C\cup D \neq A\cap B$)
  $$R(A\setminus C, B\setminus D) = 0,$$
  since $(A\setminus C)\cap(B\setminus D)\neq\emptyset$.

1.2 Subresultants.

abusing notation, $A = R(X,A)$ and $B = R(X,B)$, $n \leqslant m$

$$A = \sum_{k=0}^{m} \alpha_k X^{m-k} \quad B = \sum_{k=0}^{n} \beta_k X^{n-k}.$$

$j \leq n-1$, $\mathrm{Sylv}_j(A,B)$ matrix whose rows are the coordinates of the polynomials $X^{n-1-j}A$, ..., A, B, ..., $X^{m-1-j}B$ (in this order) in the basis $\{X^{m+n-j-1}, ..., 1\}$; matrix of dimension $(m+n-2j) \times (m+n-j)$.

$\mathrm{Sres}_j(A,B)(X)$, *the subresultant of index* j of A and B: determinant of the matrix $M_j(A,B)$, whose $(m+n-2j-1)$ first columns are the columns of $\mathrm{Sylv}_j(A,B)$, and the last column (the $(m+n-2j)$-th one) has elements $X^{n-1-j}A$, ..., A, B, ..., $X^{m-1-j}B$ (in this order).

$$\mathrm{Sres}_j(A,B)(X) = \begin{vmatrix} 1 & \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{m+n-2j-2} & X^{n-j-1}A \\ 0 & 1 & \alpha_1 & \alpha_2 & \cdots & \alpha_{m+n-2j-3} & X^{n-j-2}A \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \bullet & \bullet & \bullet & \bullet & \cdots & \alpha_{m-j-1} & A \\ \bullet & \bullet & \bullet & \bullet & \cdots & \beta_{n-j-1} & B \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & \beta_1 & \beta_2 & \cdots & \beta_{m+n-2j-3} & X^{m-j-2}B \\ 1 & \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_{m+n-2j-2} & X^{m-j-1}B \end{vmatrix}$$

with the convention: $\alpha_i = 0$ for $i > m$ and $\beta_i = 0$ for $i > n$.

Notation 2. *Define* $\varepsilon_k = (-1)^{[k/2]} = (-1)^{k(k-1)/2}$.

Remark 3. The subresultants have the following properties

1. $\mathrm{Sres}_j(A,B)(X)$ polynomial of degree $\leq j$.
2. $\mathrm{Sres}_0(A,B)(X) = \varepsilon_m R(A,B)$.
3. The non zero subresultant with smallest index is a gcd of A and B.

similar to the properties of Sylvester double sums given in the preceeding paragraph, classical [BPR].

1.3 Main result.

equality, up to a multiplicative constant

Theorem 4. *Let $j \leq n < m$; for all p, q such that $p + q = j$,* $\mathrm{Sres}_j(A, B)(X)$ *and* $\mathrm{Sylv}^{p,q}(A, B)(X)$ *are equal u p to a multiplicative constant. More precisely,*

$$(-1)^{p(m-j)}\varepsilon_{m-j}\begin{pmatrix} j \\ p \end{pmatrix}\mathrm{Sres}_j(A,B)(X) = \mathrm{Sylv}^{p,q}(A,B)(X).$$

stated by Sylvester [S],
proved in [LP] Schur functions and their properties
new proof by [AHKS] based on matrix manipulations
here : a simple proof by induction on n

Note that for Sylvester double sums, when two different choices of p, q are made, the equality is not obvious ! But both are equal to subresultants !!

2 Two properties of Sylvester double sums.

A a finite subset of a field, $a \in A$, $A \setminus a := A \setminus \{a\}$, $a := \{a\}$.

A univariate polynomial, $c_j(A)$ coefficient of the term of degree j of A (convention $c_j(A) = 0$ when $j > \deg(A)$).

Proposition 5. *Let $j < n < m$; for every p, q such that $j = p + q$, and $b \in B$;*

$$\mathrm{Sylv}^{p,q}(A,B)(b) = (-1)^{m-j}A(b)\, c_j(\mathrm{Sylv}^{p,q}(A, B \setminus b)(X))$$

Proof.

•

$$\begin{aligned} & \mathrm{Sylv}^{p,q}(A,B)(b) \\ = & \sum_{\substack{C \subset_p A \\ D \subset_q B}} R(b,C)R(b,D)\frac{R(C,D)R(A\setminus C, B\setminus D)}{R(C, A\setminus C)R(D, B\setminus D)} \end{aligned}$$

$$= (-1)^{m-j}A(b) \sum_{\substack{C \subset_p A \\ D \subset_q B\setminus b}} \frac{R(C,D)R(A\setminus C, (B\setminus b)\setminus D)}{R(C, A\setminus C)R(D, (B\setminus b)\setminus D)}$$

Indeed, if $b \in D$, all the terms containing $R(b, D)$ are null; and if $b \notin D$, then

$$\begin{aligned} R(b,C)R(A \setminus C, B \setminus D) &= (-1)^{m-p} A(b) R(A \setminus C, (B \setminus b) \setminus D), \\ \frac{R(b,D)}{R(D, B \setminus D)} &= (-1)^q \frac{1}{R(D, (B \setminus b) \setminus D)} \end{aligned}$$

also

$$c_j(\mathrm{Sylv}^{p,q}(A, B \setminus b)(X) = \sum_{\substack{C \subset_p A \\ D \subset_q B \setminus b}} \frac{R(C,D)R(A \setminus C, (B \setminus b) \setminus D)}{R(C, A \setminus C)R(D, (B \setminus b) \setminus D).}$$

□

Proposition 6.

1. *If $n < m$ and $p + q = n$, then*

$$\mathrm{Sylv}^{p,q}(A,B)(X) = (-1)^{p(m-n)} \begin{pmatrix} n \\ p \end{pmatrix} B(X).$$

2. *If $n = m = p + q$, then*

$$\mathrm{Sylv}^{p,q}(A,B)(X) = \begin{pmatrix} n-1 \\ q \end{pmatrix} A(X) + \begin{pmatrix} n-1 \\ p \end{pmatrix} B(X).$$

- Proof of the proposition : a litte complicated
  uses the following lemma (similar in spirit to Proposition 5, more technical).

  Lemma 7.
  1. *Let $j \leq n < m$; for all p, q such that $j = p + q$, and $a \in A$;*

$$\mathrm{Sylv}^{p,q}(A,B)(a) = (-1)^p B(a)\, c_j(\mathrm{Sylv}^{p,q}(A \setminus a, B)(X))$$

  2. *Let $j = n = m$; for all p, q such that $j = p + q$, if $q \neq 0$, for all $a \in A$;*

$$\begin{aligned} &\mathrm{Sylv}^{p,q}(A,B)(a) \\ = \;& (-1)^p B(a)\, c_{j-1}(\mathrm{Sylv}^{p,q-1}(B, A \setminus a)(X)) \end{aligned}$$

  3. *Let $j = n = m$; for all p, q such that $j = p + q$, if $p \neq 0$, for all $b \in B$;*

$$\mathrm{Sylv}^{p,q}(A,B)(b) = (-1)^q A(b)\, c_{j-1}(\mathrm{Sylv}^{q,p-1}(A, B \setminus b)(X))$$

Proof.
◦ Proof of the Lemma

□

Proof. Proof of proposition 6 .
◦ The proof uses a double induction on n and m.

□

3 Two properties of the subresultants.

The subresultant have analogous properties.

Proposition 8. *If b is a root of B, then, for all $0 \leq j < n < m$,*

$$\mathrm{Sres}_j(A,B)(b) = (-1)^{m-j} A(b)\, c_j\left(\mathrm{Sres}_j\left(A, \frac{B}{X-b}\right)(X)\right).$$

Proof.
◦ Manipulations in Sylvester matrix

□

Proposition 9.

$$\mathrm{Sres}_n(A,B)(X) = \varepsilon_{m-n} B(X).$$

Immediate consequence of the definition of subresultants.

No equivalent of proposition 6, 2 : subresultants are not defined for $n = m$.

4 Proof of the theorem 4

Remark 10. From proposition 8 and proposition, two similar equalities : if $j \leq n-1$, then

$$\mathrm{Sres}_j(A,B)(b) = (-1)^{m-j} A(b)\, c_j(\mathrm{Sres}_j\left(A, \frac{B}{X-b}\right)(X)$$

$$\mathrm{Sylv}^{p,q}(A,B)(b) = (-1)^{m-j} A(b)\, c_j(\mathrm{Sylv}^{p,q}(A, B \setminus b)(X)).$$

Proof by induction on n of theorem 4 : if theorem holds for $B \setminus b$ ($n-1$ elements) for every $b \in B$, by interpolation at the n elements of B, theorem holds for B.

Remark 11.

Subresultants are a basic tool in computer algebra

1. compute gcd: last non zero in the sequence
2. (real) : compute number of real roots, Cauchy index through sign variations in the whole sequence
3. as a consequence cylindrical algebraic decomposition: quantifier elimination, Hilbert'th 17 problem ...

Proofs of facts: based on an induction on the length of the euclidean remainder sequence of two polynomials A and B

Use of Sylvester double sums

1. compute gcd
2. since they are equal to the subresultants compute the number of real roots, the Cauchy index

Proof of the equality of Sylvester double sums and subresultants: based on an induction on the degree of B

Given the lectures of this morning, formalizing these proofs should be a nice exercize. Assia already worked on the subresultants .... what about Sylvester double sums ?

5 References

[S] J. J. Sylvester. On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's function. *Trans. Roy. Soc. London*, 1853.

[LP] A. Lascoux, P. Pragacz Double Sylvester sums for subresultants and multi-Schur fonctions Prépublication submitted to Journal of Symbolic Computation

[AHKS] C. d'Andrea, H Hong, T. Krick, A. Szanto An Elementary Proof of Sylvester's Double Sums for Subresultants Prépublication submitted to Journal of Symbolic Computation

[BPR] S. Basu, R. Pollack, M.-F. Roy Algorithms in real algebraic geometry Springer 2003
[RS] M.-F. Roy, A. Szpirglas Sylvester double sums and subresultants, in preparation 2009