Journal of Symbolic Computation 47 (2012) 942–953

Contents lists available at SciVerse ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Sylvester's double sums: An inductive proof of the general case

Teresa Krick [a,1], Agnes Szanto [b]

[a] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires and IMAS, CONICET, 1428 Buenos Aires, Argentina

[b] Department of Mathematics, North Carolina State University, Raleigh NC 27695, USA

ARTICLE INFO

Article history:
Received 23 June 2011
Accepted 17 January 2012
Available online 30 January 2012

Keywords:
Sylvester's double sums
Subresultants

ABSTRACT

In 1853, Sylvester introduced a family of double sum expressions for two finite sets of indeterminates and showed that some members of the family are essentially the polynomial subresultants of the monic polynomials associated with these sets. In 2009, in a joint work with C. D'Andrea and H. Hong we gave the complete description of all the members of the family as expressions in the coefficients of these polynomials. More recently, M.-F. Roy and A. Szpirglas presented a new and natural inductive proof for the cases considered by Sylvester. Here we show how induction also allows to obtain the full description of Sylvester's double-sums.

1. Introduction

Let A and B be non-empty finite lists (ordered sets) of distinct indeterminates over a field k. In Sylvester (1853), Sylvester introduced for each $0 \le p \le |A|$ and $0 \le q \le |B|$ the following univariate polynomial in the variable x and coefficients in the field $k(\alpha, \beta; \alpha \in A, \beta \in B)$, of degree $\le p+q$, called the *double sum expression* in A and B:

$$\mathrm{Sylv}^{p,q}(A,B) := \sum_{\substack{A' \subset A,\ B' \subset B \\ |A'|=p,\ |B'|=q}} R(x,A')\,R(x,B')\,\frac{R(A',B')\,R(A-A',B-B')}{R(A',A-A')\,R(B',B-B')},$$

E-mail addresses: krick@dm.uba.ar (T. Krick), aszanto@ncsu.edu (A. Szanto).
URLs: http://mate.dm.uba.ar/~krick (T. Krick), http://www4.ncsu.edu/~aszanto (A. Szanto).
1 Tel.: +54 11 4576 3335; fax: +54 11 4576 3335.

0747-7171/$ – see front matter
doi:10.1016/j.jsc.2012.01.003

where for sets Y, Z of indeterminates,

$$R(Y,Z) := \prod_{y\in Y, z\in Z}(y-z), \qquad R(y,Z) := \prod_{z\in Z}(y-z)$$

and by convention $R(Y,\emptyset) = 1$.

Let now f, g be the monic univariate polynomials in $k(\alpha, \beta; \alpha \in A, \beta \in B)$, defined as

$$f = \prod_{\alpha\in A}(x-\alpha) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \quad \text{and}$$
$$g = \prod_{\beta\in B}(x-\beta) = x^n + b_{n-1}x^{n-1} + \cdots + b_0,$$

where $m := |A| \geq 1$ and $n := |B| \geq 1$. The *k-th subresultant* of the polynomials f and g is defined, for $0 \leq k < \min\{m,n\}$ or $k = \min\{m,n\}$ when $m \neq n$, as the polynomial

$$\mathrm{Sres}_k(f,g) := \det \begin{array}{c} \overbrace{\qquad\qquad\qquad\qquad}^{m+n-2k} \\ \left|\begin{array}{cccccc} a_m & \cdots & & \cdots & a_{k+1-(n-k-1)} & x^{n-k-1}f(x) \\ & \ddots & & & \vdots & \vdots \\ & & a_m & \cdots & a_{k+1} & x^0 f(x) \\ \hline b_n & \cdots & & \cdots & b_{k+1-(m-k-1)} & x^{m-k-1}g(x) \\ & \ddots & & & \vdots & \vdots \\ & & b_n & \cdots & b_{k+1} & x^0 g(x) \end{array}\right| \begin{array}{c} \\ \\ \\ n-k \\ \\ \\ \\ m-k \end{array} \end{array} \tag{1}$$

with $a_\ell = b_\ell = 0$ for $\ell < 0$. Subresultant polynomials were also introduced by Sylvester in Sylvester (1853). They became an important tool in polynomial computer algebra after G. Collins revisited them in Collins (1967), and some of their properties are still mysterious. See for instance Geddes et al. (1992), von zur Gathen and Gerhard (2003) or Apéry and Jouanolou (2005) for more references on the subject.

For $k = 0$, $\mathrm{Sres}_0(f,g)$ coincides with the resultant:

$$\mathrm{Res}(f,g) = \prod_{\alpha\in A} g(\alpha) = (-1)^{mn}\prod_{\beta\in B} f(\beta). \tag{2}$$

Also, for instance,

$$\mathrm{Sres}_m(f,g) = f \quad \text{for } m < n \quad \text{and} \quad \mathrm{Sres}_n(f,g) = g \quad \text{for } n < m. \tag{3}$$

Relating Sylvester's double sums with the polynomials f and g, it is immediate that

$$\mathrm{Sylv}^{0,0}(A,B) = R(A,B) = \mathrm{Res}(f,g), \tag{4}$$
$$\mathrm{Sylv}^{m,0}(A,B) = R(x,A) = f \quad \text{and} \quad \mathrm{Sylv}^{0,n}(A,B) = R(x,B) = g, \tag{5}$$
$$\mathrm{Sylv}^{m,n}(A,B) = R(x,A)\,R(x,B)\,R(A,B) = \mathrm{Res}(f,g)\,f\,g. \tag{6}$$

More generally, for every $0 \leq p \leq m$ and $0 \leq q \leq n$, the polynomial $\mathrm{Sylv}^{p,q}(A,B)$, which is symmetric in the α's and in the β's, can be expressed as a polynomial in x whose coefficients are rational functions in the a_i's and the b_j's. Sylvester in Sylvester (1853) gave this rational expression for the following values of (p,q):

(1) If $0 \leq k := p+q < m \leq n$ or if $k = m < n$, then Sylvester (1853, Art. 21):

$$\mathrm{Sylv}^{p,q}(A,B) = (-1)^{p(m-k)}\binom{k}{p}\,\mathrm{Sres}_k(f,g).$$

(2) If $p+q = m = n$, then Sylvester (1853, Art. 22):

$$\mathrm{Sylv}^{p,q}(A,B) = \binom{m-1}{q} f + \binom{m-1}{p} g.$$

(3) If $m < p+q < n-1$, then Sylvester (1853, Arts. 23 & 24):
$$\mathrm{Sylv}^{p,q}(A,B) = 0.$$

(4) If $m < p+q = n-1$, then Sylvester (1853, Art. 25): $\mathrm{Sylv}^{p,q}(A,B)$ is a "numerical multiplier" of f, but the ratio is not established.

In Lascoux and Pragacz (2003, Th.0.1 and Prop. 2.9), A. Lascoux and P. Pragacz presented new proofs for the cases covered by Items (1) and (2). More recently, in a joint work with C. D'Andrea and H. Hong, (D'Andrea et al., 2009, Th.2.10), we introduced a unified matrix formulation that allowed us to give an explicit formula for all possible values of (p,q), i.e. for $0 \le p \le m$, $0 \le q \le n$. The proofs there were elementary though cumbersome. In their recent work, M.-F. Roy and A. Szpirglas, were able to produce in Roy and Szpirglas (2011, Main theorem) a new and natural inductive proof also for the cases covered by Item (1) and (2). The aim of this note is to give, inspired by Roy and Szpirglas (2011), a new elementary inductive proof for all the cases. We furthermore show how the cases (3) and (4), when $p+q > m$, which seem somehow less natural since there is no known counterpart in Computer Algebra associated to them yet, immediately yield other known crucial cases, as for instance the cases $p+q = m < n$ and $p+q = m = n$.

All these identities, and the ones proved in this paper, behave well when the different indeterminates in A and B are specialized to elements in k, provided that the denominators in the double sum expressions do not vanish. In particular they specialize well when the indeterminates in A are specialized to distinct elements in k, as well as those in B. In other words, the same identities hold for polynomials $f, g \in k[x]$ with simple roots. In the case of repeated elements (or polynomials with multiple roots), there is not even a right notion of how the double sum expressions should be defined. The main motivation of our investigation is to explore the applicability of the inductive proof method techniques. The ultimate goal of this investigation is to tackle the important open problem concerning the extension of the definition of Sylvester's double sums to the case of multiple roots and their connection to subresultants, which is an ongoing project of the authors. Expressions of subresultants in terms of Sylvester's single and double sums have applications for example in rational Cauchy interpolation (see Ilyuta (2005)), and extensions of these results to the multiple roots case would be a significant development. Inductive proofs have been successfully used for example in Kós and Rónyai (2011) in extending Alon's Nullstellensatz to the multiset case.

Let us now introduce the necessary notation to formulate our main result.
As in D'Andrea et al. (2009), we split the last column of the matrix in (1) to write $\mathrm{Sres}_k(f,g)$ as the sum of two determinants, obtaining an expression

$$\mathrm{Sres}_k(f,g) = F_k(f,g)\,f + G_k(f,g)\,g \tag{7}$$

where the polynomials $F_k(f,g)$ and $G_k(f,g)$ in $k(\alpha,\beta;\alpha \in A, \beta \in B)$ are defined for $0 \le k < \min\{m,n\}$ or $k = \min\{m,n\}$ when $m \ne n$ as the determinants of the $(m+n-2k)$-matrices:

$$F_k(f,g) := \det \begin{array}{|cccccc|c} a_m & \cdots & & \cdots & a_{k+1-(n-k-1)} & x^{n-k-1} & \\ & \ddots & & & \vdots & \vdots & n-k \\ & & a_m & \cdots & a_{k+1} & x^0 & \\ \hline b_n & \cdots & & \cdots & b_{k+1-(m-k-1)} & 0 & \\ & \ddots & & & \vdots & \vdots & m-k \\ & & b_n & \cdots & b_{k+1} & 0 & \end{array},$$

$$G_k(f.g) := \det \begin{array}{|cccccc|c} a_m & \cdots & & \cdots & a_{k+1-(n-k-1)} & 0 & \\ & \ddots & & & \vdots & \vdots & n-k \\ & & a_m & \cdots & a_{k+1} & 0 & \\ \hline b_n & \cdots & & \cdots & b_{k+1-(m-k-1)} & x^{m-k-1} & \\ & \ddots & & & \vdots & \vdots & m-k \\ & & b_n & \cdots & b_{k+1} & x^0 & \end{array}.$$

As recently pointed out to us by D'Andrea, Sylvester himself in Sylvester (1853, Art. 29) already looked at the factors $F_k(f,g)$ and $G_k(f,g)$ and proposed the formulas we can derive from Lemma 6 (see the remark following it).

We observe that when $k < \min\{m,n\}$, $\deg F_k(f,g) \le n-k-1$ and $\deg G_k(f,g) \le m-k-1$. Also

$$\begin{aligned} &F_m(f,g)=1, \qquad G_m(f,g)=0 \quad \text{for } m<n \quad \text{and} \quad F_n(f,g)=0,\\ &G_n(f,g)=1 \quad \text{for } n<m \end{aligned} \tag{8}$$

$$G_{m-1}(f,g)=1 \quad \text{for } m\le n \quad \text{and} \quad F_{n-1}(f,g)=(-1)^{m-n+1} \quad \text{for } n\le m. \tag{9}$$

We finally introduce the following notation that we will keep all along in this text. Given $m, n \in \mathbb{N}$, $p, q \in \mathbb{Z}$ such that $0 \le p \le m$, $0 \le q \le n$ and $k = p+q$, we set

$$\overline{p} := m-p, \qquad \overline{q} := n-q \quad \text{and} \quad \overline{k} := \overline{p}+\overline{q}-1 = m+n-k-1.$$

Sylvester's double sums, for k "too big" w.r.t. m and n, will be expressed in our result in terms of the polynomials $F_{\overline{k}}(f,g)$ and $G_{\overline{k}}(f,g)$, well-defined since the condition $n-1 \le k \le m+n-1$ for $m<n$ is equivalent to $0 \le \overline{k} \le m$, and the condition $m \le k \le 2m-1$ for $m=n$ is equivalent to $0 \le \overline{k} \le m-1$.

Theorem 1 (*See also D'Andrea et al. (2009, Th.2.10)*). *Set $1 \le m \le n$, and let $0 \le p \le m$, $0 \le q \le n$ and $k = p+q$.*
Then, for $(p,q) \ne (m,n)$:

– *when $m < n$:*

$$\mathrm{Sylv}^{p,q}(A,B) = \begin{cases} (-1)^{p(m-k)}\binom{k}{p}\mathrm{Sres}_k(f,g) & \text{for} \quad 0 \le k \le m \\ 0 & \text{for} \quad m+1 \le k \le n-2 \text{ when } m \le n-3 \\ (-1)^c\left(\binom{\overline{k}}{\overline{p}}F_{\overline{k}}(f,g)f - \binom{\overline{k}}{\overline{q}}G_{\overline{k}}(f,g)g\right) & \text{for} \quad n-1 \le k \le m+n-1 \end{cases}$$

– *when $m = n$:*

$$\mathrm{Sylv}^{p,q}(A,B) = \begin{cases} (-1)^{p(m-k)}\binom{k}{p}\mathrm{Sres}_k(f,g) & \text{for} \quad 0 \le k \le m-1 \\ (-1)^c\left(\binom{\overline{k}}{\overline{p}}F_{\overline{k}}(f,g)f - \binom{\overline{k}}{\overline{q}}G_{\overline{k}}(f,g)g\right) & \text{for} \quad m \le k \le 2m-1, \end{cases}$$

where $c := \overline{p}\,\overline{q} + n - p - 1 + nq$;

and for $(p,q) = (m,n)$:

$$\mathrm{Sylv}^{m,n}(A,B) = \mathrm{Res}(f,g)\,f\,g.$$

Theorem 1 can be written in a more uniform manner instead of being split in cases: by Identity (7), for $0 \le k \le m$ when $m < n$ and for $0 \le k < m$ when $m = n$,

$$\mathrm{Sylv}^{p,q}(A,B) = (-1)^{p(m-k)}\left(\binom{k}{p}F_k(f,g)f + \binom{k}{q}G_k(f,g)g\right),$$

or for $0 \le \overline{k} \le m$ when $m < n$ and for $0 \le \overline{k} < m$, when $m = n$,

$$\begin{aligned} \mathrm{Sylv}^{p,q}(A,B) &= (-1)^c\left(\binom{\overline{k}}{\overline{p}}\mathrm{Sres}_{\overline{k}}(f,g) - \binom{\overline{k}+1}{\overline{q}}G_{\overline{k}}(f,g)\,g\right) \\ &= (-1)^c\left(\binom{\overline{k}+1}{\overline{p}}F_{\overline{k}}(f,g)f - \binom{\overline{k}}{\overline{q}}\mathrm{Sres}_{\overline{k}}(f,g)\right). \end{aligned} \tag{10}$$

The cases "in between", for $m+1 \le k \le n-2$ when $m \le n-3$, are the cases when neither $0 \le k \le m$ nor $0 \le \overline{k} \le m$, i.e. the cases when the corresponding matrices F_k, G_k and $F_{\overline{k}}$, $G_{\overline{k}}$ are not defined (or could be defined as 0 for uniformity).

We also note that the case $k = m = n-1$ is covered twice: $\mathrm{Sres}_m(f,g) = f = F_m(f,g)f - G_m(f,g)g$ since $\overline{k} = m$, $F_m = 1$ and $G_m = 0$. Finally the case $p = m$, $q = n$ is Identity (6).

The proof of Theorem 1 is based, as the proof in Roy and Szpirglas (2011), on specialization properties.

2. Specialization properties

In the sequel, given a polynomial h in a single variable x, we denote by $\mathbf{c}_k(h)$ its coefficient of order k, i.e. the coefficient corresponding to the monomial x^k.

The following specialization properties of Sylvester's double sums were previously proved in Lascoux and Pragacz (2003, Lemma 2.8) and in Roy and Szpirglas (2011, Prop.3.1), where they were used as one of the key ingredients of their inductive proof for the cases $k \le m < n$ and $k < m = n$. We repeat the proof here for the sake of completeness.

Lemma 2. *For any $\alpha \in A$ and $\beta \in B$,*

- $\mathrm{Sylv}^{p,q}(A,B)(\alpha) = (-1)^p\, \mathbf{c}_{p+q}\big(\mathrm{Sylv}^{p,q}(A-\alpha,B)\big)\, R(\alpha,B)$ *for* $0 \le p < m$ *and* $0 \le q \le n$,
- $\mathrm{Sylv}^{p,q}(A,B)(\beta) = (-1)^{q+\bar{p}}\, \mathbf{c}_{p+q}\big(\mathrm{Sylv}^{p,q}(A,B-\beta)\big)\, R(\beta,A)$ *for* $0 \le p \le m$ *and* $0 \le q < n$.

Proof.

$$\begin{aligned}
\mathrm{Sylv}^{p,q}(A,B)(\alpha) &= \sum_{\substack{A'\subset A-\alpha,\ B'\subset B\\ |A'|=p,\ |B'|=q}} R(\alpha,A')\,R(\alpha,B')\,\frac{R(A',B')\,R(A-A',B-B')}{R(A',A-A')\,R(B',B-B')}\\
&= (-1)^p\,R(\alpha,B) \sum_{\substack{A'\subset A-\alpha,\ B'\subset B\\ |A'|=p,\ |B'|=q}} \frac{R(A',B')\,R((A-\alpha)-A',B-B')}{R(A',(A-\alpha)-A')\,R(B',B-B')}\\
&= (-1)^p\,\mathbf{c}_{p+q}\big(\mathrm{Sylv}^{p,q}(A-\alpha,B)\big)\,R(\alpha,B).
\end{aligned}$$

The second identity is a consequence of the fact that

$$\mathrm{Sylv}^{p,q}(A,B) = (-1)^{pq}\,(-1)^{\bar{p}\,\bar{q}}\,\mathrm{Sylv}^{q,p}(B,A). \quad \square$$

Next result replaces the specialization properties of subresultants in Roy and Szpirglas (2011, Prop. 4.1) by specialization properties of the polynomials $F_k(f,g)$ and $G_k(f,g)$. This will allow a more uniform and simpler proof of our main theorem, covering all cases of p and q.

Lemma 3. *For any root α of f and any root β of g, we have*

- $F_k(f,g)(\beta) = -\,\mathbf{c}_{n-k-1}\left(F_{k-1}\left(f,\dfrac{g}{x-\beta}\right)\right)$ *for* $1 \le k \le \min\{m,n\}-1$,
- $G_k(f,g)(\alpha) = (-1)^{m-k-1}\,\mathbf{c}_{m-k-1}\left(G_{k-1}\left(\dfrac{f}{x-\alpha},g\right)\right)$ *for* $1 \le k \le \min\{m,n\}-1$.

Proof. Given a root β of g, we set

$$\frac{g}{x-\beta} := x^{n-1} + b'_{n-2}x^{n-2} + \cdots + b'_0.$$

The following relationship between the coefficients of g and of $\frac{g}{x-\beta}$ is straightforward:

$$b_i = b'_{i-1} - \beta b'_i \quad \text{for } 1 \le i \le n-1 \quad \text{and} \quad b_0 = -\beta b'_0. \tag{11}$$

(Here $b_n = b'_{n-1} = 1$.)

First consider

$$\mathbf{c}_{n-k-1}\left(F_{k-1}\left(f,\frac{g}{x-\beta}\right)\right)=\mathbf{c}_{n-k-1}\left(\det\begin{array}{|cccccc|}\hline a_m&\cdots&&\cdots&a_{k-(n-k-1)}&x^{n-k-1}\\ &\ddots&&&\vdots&\vdots\\ &&a_m&\cdots&a_k&x^0\\ \hline b'_{n-1}&\cdots&&\cdots&b'_{k-(m-k)}&0\\ &\ddots&&&\vdots&\vdots\\ &&b'_{n-1}&\cdots&b'_k&0\\ \hline\end{array}\right)$$

$$=(-1)^{m+n}\det\begin{array}{|cccccc|}\hline 0&a_m&\cdots&&\cdots&a_{k-(n-k-2)}\\ &&\ddots&&&\vdots\\ &&&a_m&\cdots&a_k\\ \hline b'_{n-1}&\cdots&\cdots&&\cdots&b'_{k-(m-k)}\\ &\ddots&&&&\vdots\\ &&b'_{n-1}&\cdots&&b'_k\\ \hline\end{array}\begin{array}{l}\\ \\ n-1-k\\ \\ \\ m-k+1\end{array}$$

$$=(-1)^{m-k+1}\det\begin{array}{|cccccc|}\hline a_m&\cdots&&\cdots&a_{k-(n-k-2)}&\\ &\ddots&&&\vdots&\\ &&a_m&\cdots&a_k&\\ \hline b'_{n-1}&\cdots&&\cdots&b'_{k-(m-k-1)}&\\ &\ddots&&&\vdots&\\ &&b'_{n-1}&\cdots&b'_k&\\ \hline\end{array}\begin{array}{l}\\ \\ n-1-k\\ \\ \\ m-k\end{array}.$$

We apply elementary column operations on the matrix above, replacing the j-th column C_j by $C_j-\beta C_{j-1}$ starting from the last column $C_{n+m-2k-1}$ up to the second column C_2, and using the relations in (11):

$$\mathbf{c}_{n-k-1}\left(F_{k-1}\left(f,\frac{g}{x-\beta}\right)\right)$$

$$=(-1)^{m-k+1}\det\begin{array}{|cccccc|}\hline a_m&a_{m-1}-\beta a_m&\cdots&&\cdots&a_{k-(n-k-2)}-\beta a_{k+1-(n-k-2)}\\ &\ddots&&&\vdots&\\ &&a_m&a_{m-1}-\beta a_m&\cdots&a_k-\beta a_{k+1}\\ \hline b_n&b_{n-1}&\cdots&&\cdots&b_{k+1-(m-k-1)}\\ &\ddots&&&\vdots&\\ &&b_n&b_{n-1}&\cdots&b_{k+1}\\ \hline\end{array}\begin{array}{l}\\ \\ n-1-k\\ \\ \\ m-k\end{array}. \tag{12}$$

Next consider

$$F_k(f,g)(\beta)=\det\begin{array}{|ccccc|}\hline a_m&\cdots&&\cdots&a_{k+1-(n-k-1)}&\beta^{n-k-1}\\ &\ddots&&&\vdots&\vdots\\ &&a_m&\cdots&a_{k+1}&\beta^0\\ \hline b_n&\cdots&&\cdots&b_{k+1-(m-k-1)}&0\\ &\ddots&&&\vdots&\vdots\\ &&b_n&\cdots&b_{k+1}&0\\ \hline\end{array}\begin{array}{l}\\ \\ n-k\\ \\ \\ m-k\end{array}.$$

We apply elementary row operations on the matrix above, replacing the i-th row R_i by $R_i - \beta R_{i+1}$, starting from the first row R_1 up to row R_{n-k-1}:

$$F_k(f,g)(\beta) = \det \left[\begin{array}{cccccc|c}
a_m & a_{m-1}-\beta a_m & & & \cdots & a_{k+1-(n-k-1)}-\beta a_{k+2-(n-k-1)} & 0 \\
 & \ddots & & & & \vdots & \vdots \\
 & & a_m & a_{m-1}-\beta a_m & \cdots & a_{k+2}-\beta a_{k+1} & 0 \\
 & & & a_m \quad a_{m-1} & \cdots & a_{k+1} & 1 \\
\hline
b_n & \cdots & & & \cdots & b_{k+1-(m-k-1)} & 0 \\
 & \ddots & & & & \vdots & \vdots \\
 & & b_n & \cdots & & b_{k+1} & 0
\end{array}\right] \begin{array}{c} \\ \\ n-k \\ \\ \\ m-k \end{array}$$

$$= (-1)^{m-k} \det \left[\begin{array}{cccc|c}
a_m & a_{m-1}-\beta a_m & \cdots & a_{k+1-(n-k-1)}-\beta a_{k+2-(n-k-1)} & \\
 & \ddots & & \vdots & n-k-1 \\
 & a_m \quad a_{m-1}-\beta a_m & \cdots & a_{k+2}-\beta a_{k+1} & \\
\hline
b_n & \cdots & \cdots & b_{k+1-(m-k-1)} & \\
 & \ddots & & \vdots & m-k \\
 & b_n & \cdots & b_{k+1} &
\end{array}\right] . \tag{13}$$

We obtain the first identity of the statement by comparing (12) and (13).
For the second identity, we have

$$\begin{aligned}
G_k(f,g)(\alpha) &= (-1)^{(n-k)(m-k)} F_k(g,f)(\alpha) \\
&= (-1)^{(n-k)(m-k)+1} \mathbf{c}_{m-k-1} \left(F_{k-1}\left(g, \frac{f}{x-\alpha}\right)\right) \\
&= (-1)^{(n-k)(m-k)+1} (-1)^{(m-k)(n-k+1)} \mathbf{c}_{m-k-1} \left(G_{k-1}\left(\frac{f}{x-\alpha}, g\right)\right) \\
&= (-1)^{m-k-1} \mathbf{c}_{m-k-1} \left(G_{k-1}\left(\frac{f}{x-\alpha}, g\right)\right). \quad \square
\end{aligned}$$

As an immediate consequence we obtain the following important specialization properties of subresultants, which seem to have been stated and proved for the first time in Roy and Szpirglas (2011, Prop. 4.1).

Corollary 4. *For any root α of f, any root β of g and any $0 \le k < \min\{m,n\}$, we have*

- $Sres_k(f,g)(\beta) = (-1)^{m-k}\, \mathbf{c}_k \left(Sres_k\left(f\,,\, \frac{g}{x-\beta}\right)\right) f(\beta)$,
- $Sres_k(f,g)(\alpha) = \mathbf{c}_k \left(Sres_k\left(\frac{f}{x-\alpha}\,,\, g\right)\right) g(\alpha)$.

Proof. It is sufficient to prove the first identity, since the second identity is a consequence of

$$\mathrm{Sres}_k(g,f) = (-1)^{(m-k)(n-k)} \mathrm{Sres}_k(f,g).$$

By (7) and the previous lemma,

$$\mathrm{Sres}_k(f,g)(\beta) = F_k(f,g)(\beta) f(\beta) = -\,\mathbf{c}_{n-k-1} \left(F_{k-1}\left(f, \frac{g}{x-\beta}\right)\right) f(\beta).$$

Now it is immediate to verify by the definition of the principal scalar subresultant of order k that

$$\mathbf{c}_{n-k-1} \left(F_{k-1}\left(f, \frac{g}{x-\beta}\right)\right) = (-1)^{m-k-1} \mathbf{c}_k \left(\mathrm{Sres}_k\left(f, \frac{g}{x-\beta}\right)\right). \quad \square$$

3. Proof of Theorem 1

It turns out that the cases of Theorem 1 where k is "big" are easy to prove by induction and will be used later in the other cases. That is why we start with this case first in the following proposition. The proof will use a lemma for the extremal cases (p, n) and (m, q), which is given after the proposition. We recall that $\overline{p} = m - p$, $\overline{q} = n - q$, and $\overline{k} = m + n - k - 1$.

Proposition 5. *Set $1 \le m \le n$ and let $0 \le p \le m$, $0 \le q \le n$ and $k = p + q$ be such that $n - 1 \le k \le m + n - 1$, i.e. $0 \le \overline{k} \le m$, when $m < n$ or $m \le k \le 2m - 1$, i.e. $0 \le \overline{k} \le m - 1$, when $m = n$. Then*

$$\mathrm{Sylv}^{p,q}(A, B) = (-1)^{\overline{p}\,\overline{q}+n-p-1+nq}\left(\binom{\overline{k}}{\overline{p}} F_{\overline{k}}(f, g) f - \binom{\overline{k}}{\overline{q}} G_{\overline{k}}(f, g)\, g\right).$$

Proof. By induction on $\overline{k} \ge 0$:
The case $\overline{k} = 0$ implies $(p, q) = (m - 1, n)$ or $(p, q) = (m, n - 1)$ and will follow from Lemma 6 below.

Now set $\overline{k} > 0$.
– For $p = m$ and $q < n$ or $p < m$ and $q = n$, also by Lemma 6,

$$\mathrm{Sylv}^{m,q}(A, B) = (-1)^{n-m-1+nq} F_{\overline{q}-1}(f, g) f \quad \text{and} \quad \mathrm{Sylv}^{p,n}(A, B) = (-1)^{p} G_{\overline{p}-1}(f, g) g$$

accordingly, which matches the statement since in these cases $\binom{\overline{k}}{\overline{q}}$ or $\binom{\overline{k}}{\overline{p}}$ equals 0.
– For $p < m$ and $q < n$, we specialize $\mathrm{Sylv}^{p,q}(A, B)$ of degree $k \le m + n - 2$ in the $m + n$ elements of $A \cup B$ by means of Lemma 2 and the inductive hypothesis:

$$\begin{aligned}\mathrm{Sylv}^{p,q}(A, B)(\alpha) &= (-1)^{p}\, \mathbf{c}_k\big(\mathrm{Sylv}^{p,q}(A - \alpha, B)\big)\, g(\alpha) \\ &= (-1)^{c'+p}\, \mathbf{c}_k\left(\binom{\overline{k}-1}{\overline{p}-1} \mathrm{Sres}_{\overline{k}-1}\left(\frac{f}{x-\alpha}, g\right) - \binom{\overline{k}}{\overline{q}} G_{\overline{k}-1}\left(\frac{f}{x-\alpha}, g\right) g\right) g(\alpha),\end{aligned}$$

by Identity (10). Here $c' = (\overline{p} - 1)\overline{q} + n - p - 1 + nq$.
Note that we are looking for the coefficient of degree k of the expression between brackets; the condition $\overline{k} - 1 \le m - 1 < n - 1 \le k$ in case $m < n$ and $\overline{k} - 1 \le m - 2 < k$ in case $m = n$ imply in both cases that $\deg(\mathrm{Sres}_{\overline{k}-1}(\frac{f}{x-\alpha}, g)) \le \overline{k} - 1 < k$. Then

$$\mathrm{Sylv}^{p,q}(A, B)(\alpha) = (-1)^{c'+p}\, \mathbf{c}_k\left(-\binom{\overline{k}}{\overline{q}} G_{\overline{k}-1}\left(\frac{f}{x-\alpha}, g\right) g\right) g(\alpha).$$

When $\overline{k} - 1 < m - 1$, i.e $k \ge n$, we apply Lemma 3 and get

$$\begin{aligned}\mathrm{Sylv}^{p,q}(A, B)(\alpha) &= (-1)^{c'+p}\left(-\binom{\overline{k}}{\overline{q}}\, \mathbf{c}_{k-n}\left(G_{\overline{k}-1}\left(\frac{f}{x-\alpha}, g\right)\right) g(\alpha)\right) \\ &= (-1)^{c'+p+k-n}\left(-\binom{\overline{k}}{\overline{q}} G_{\overline{k}}(f, g)(\alpha) g(\alpha)\right) \\ &= (-1)^{\overline{p}\,\overline{q}+n-p-1+nq}\left(-\binom{\overline{k}}{\overline{q}} G_{\overline{k}}(f, g)(\alpha) g(\alpha)\right).\end{aligned}$$

When $\overline{k} - 1 = m - 1$, $G_{\overline{k}-1}\left(\frac{f}{x-\alpha}, g\right) = 0 = G_{\overline{k}}(f, g)$ and therefore we also get

$$\mathrm{Sylv}^{p,q}(A, B)(\alpha) = (-1)^{\overline{p}\,\overline{q}+n-p-1+nq}\left(-\binom{\overline{k}}{\overline{q}} G_{\overline{k}}(f, g)(\alpha) g(\alpha)\right).$$

Analogously,

$$\begin{aligned}
\mathrm{Sylv}^{p,q}(A,B)(\beta) &= (-1)^{q+\overline{p}+c''}\,\mathbf{c}_k\left(\binom{\overline{k}}{\overline{p}}F_{\overline{k}-1}\left(f,\frac{g}{x-\beta}\right)f-\binom{\overline{k}-1}{\overline{q}-1}\mathrm{Sres}_{\overline{k}-1}\left(f,\frac{g}{x-\beta}\right)\right)f(\beta)\\
&= (-1)^{q+\overline{p}+c''}\,\mathbf{c}_k\left(\binom{\overline{k}}{\overline{p}}F_{\overline{k}-1}\left(f,\frac{g}{x-\beta}\right)f\right)f(\beta)\\
&= (-1)^{q+\overline{p}+c''}\binom{\overline{k}}{\overline{p}}\,\mathbf{c}_{k-m}\left(F_{\overline{k}-1}\left(f,\frac{g}{x-\beta}\right)\right)f(\beta)\\
&= (-1)^{q+\overline{p}+c''+1}\binom{\overline{k}}{\overline{p}}F_{\overline{k}}(f,g)(\beta)f(\beta),
\end{aligned}$$

where $c''=\overline{p}\,(\overline{q}-1)+n-1-p-1+(n-1)q$. Therefore,

$$\mathrm{Sylv}^{p,q}(A,B)(\beta)=(-1)^{\overline{p}\,\overline{q}+n-p-1+nq}\binom{\overline{k}}{\overline{p}}F_{\overline{k}}(f,g)(\beta)f(\beta).$$

This concludes the proof. □

The next lemma covers the cases (p,n) and (m,q) needed in the proof of the previous result. Observe that

$$\mathrm{Sylv}^{p,n}(A,B)=g\sum_{A'\subset A,|A'|=p}R(x,A')\,\frac{R(A',B)}{R(A',A-A')}\quad\text{for } p\le m,$$

$$\mathrm{Sylv}^{m,q}(A,B)=f\sum_{B'\subset B,|B'|=q}R(x,B')\,\frac{R(A,B')}{R(B',B-B')}\quad\text{for } q\le n.$$

Lemma 6. *Set $1\le m\le n$. Then*

(1) $\mathrm{Sylv}^{p,n}(A,B)=(-1)^pG_{\overline{p}-1}(f,g)\,g$ *for* $0\le p\le m-1$, *i.e.* $1\le\overline{p}\le m$.
(2) $\mathrm{Sylv}^{m,q}(A,B)=(-1)^{n-m-1+nq}F_{\overline{q}-1}(f,g)\,f$ *for* $n-m-1\le q\le n-1$, *i.e.* $1\le\overline{q}\le m+1$, *when* $m<n$ *and for* $0\le q\le m-1$, *i.e.* $1\le\overline{q}\le m$, *when* $m=n$.

Proof. (1) By induction on $m\ge 1$.
The case $m=1$ is clear from Identities 5 and 9, since in this case $p=0$ and $\overline{p}=1$.
Now set $m>1$ and let $0\le p\le m-1$. Both $\mathrm{Sylv}^{p,n}(A,B)$ and $G_{\overline{p}-1}(f,g)\,g$ are polynomials of degree bounded by $p+n<m+n$ and we compare them by specializing them into the $m+n$ elements $\alpha\in A$ and $\beta\in B$. Clearly both expressions vanish at every $\beta\in B$ and so we only need to compare them at $\alpha\in A$.
– For $p<m-1$, we apply Lemma 2, the inductive hypothesis and Lemma 3 (and the fact that g is monic):

$$\begin{aligned}
\mathrm{Sylv}^{p,n}(A,B)(\alpha) &= (-1)^p\,\mathbf{c}_{p+n}\big(\mathrm{Sylv}^{p,n}(A-\alpha,B)\big)\,g(\alpha)\\
&= (-1)^{2p}\,\mathbf{c}_{p+n}\left(G_{(m-1)-p-1}\left(\frac{f}{x-\alpha},g\right)g\right)g(\alpha)\\
&= \mathbf{c}_p\left(G_{(m-1)-p-1}\left(\frac{f}{x-\alpha},g\right)\right)g(\alpha)\;=\;(-1)^p\,G_{\overline{p}-1}(f,g)(\alpha)\,g(\alpha).
\end{aligned}$$

– For $p=m-1$:

$$\begin{aligned}
\mathrm{Sylv}^{p,n}(A,B)(\alpha) &= R(\alpha,A-\alpha)\,\frac{R(A-\alpha,B)}{R(A-\alpha,\alpha)}\,g(\alpha)\\
&= (-1)^{m-1}\prod_{\alpha'\in A}g(\alpha')\;=\;(-1)^{m-1}\mathrm{Res}(f,g)\;=\;(-1)^{m-1}G_0(f,g)(\alpha)g(\alpha),
\end{aligned}$$

by Identity (2) and the fact that $\mathrm{Res}(f,g) = F_0(f,g)f + G_0(f,g)g$ has degree 0 in x. Therefore $\mathrm{Sylv}^{p,n}(A,B) = (-1)^p G_{\bar{p}-1}(f,g)\,g$.

(2) By induction on $n \geq m$.
For $n = m$, by Item (1) we have that for $0 \leq q \leq m-1$,

$$\begin{aligned}\mathrm{Sylv}^{m,q}(A,B) &= (-1)^{mq}\,\mathrm{Sylv}^{q,m}(B,A) = (-1)^{mq+q} G_{\bar{q}-1}(g,f)\,f\\ &= (-1)^{mq+q}(-1)^{(m-(\bar{q}-1))(n-(\bar{q}-1))} F_{\bar{q}-1}(f,g)\,f = (-1)^{nq-1} F_{\bar{q}-1}(f,g)\,f.\end{aligned}$$

Now set $n \geq m+1$ and let $n-m-1 \leq q \leq n-1$. Both $\mathrm{Sylv}^{m,q}(A,B)$ and $F_{\bar{q}-1}(f,g)\,f$ are polynomials of degree bounded by $m+q < m+n$ and we compare them by specializing them in the $m+n$ elements $\alpha \in A$ and $\beta \in B$. Clearly both expressions vanish at every $\alpha \in A$ and so we only need to compare them at $\beta \in B$.
– For $q < n-1$, we apply Lemma 2, the inductive hypothesis and Lemma 3:

$$\begin{aligned}\mathrm{Sylv}^{m,q}(A,B)(\beta) &= (-1)^q\,\mathbf{c}_{m+q}\big(\mathrm{Sylv}^{m,q}(A,B-\beta)\big)f(\beta)\\ &= (-1)^{q+(n-1-m-1)+(n-1)q}\,\mathbf{c}_{m+q}\left(F_{(n-1)-q-1}\left(f,\frac{g}{x-\beta}\right)f\right)f(\beta)\\ &= (-1)^{(n+m-2+nq)+1}\,F_{\bar{q}-1}(f,g)(\beta)f(\beta).\end{aligned}$$

– For $q = n-1$,

$$\begin{aligned}\mathrm{Sylv}^{m,n-1}(A,B)(\beta) &= f(\beta)\,R(\beta,B-\beta)\frac{R(A,B-\beta)}{R(B-\beta,\beta)}\\ &= (-1)^{n-1+m(n-1)}\prod_{\beta'\in B} f(\beta') \;=\; (-1)^{(mn+n-m-1)+mn}\mathrm{Res}(f,g)\\ &= \;(-1)^{n-m-1}F_0(f,g)(\beta)f(\beta).\end{aligned}$$

Therefore $\mathrm{Sylv}^{m,q}(A,B) = (-1)^{n-m-1+nq}F_{\bar{q}-1}(f,g)\,f$ as wanted. □

We remark that rewriting this result in terms of $F_k(f,g)$ and $G_k(f,g)$, this gives the expressions proposed by Sylvester in Sylvester (1853, Art. 29). Namely, for $1 \leq m \leq n$,

(1) For $0 \leq k \leq m$, when $m < n$ and for $0 \leq k \leq m-1$, when $m = n$,

$$F_k(f,g) = (-1)^{n-m-1+nk}\sum_{B'\subset B,\,|B'|=n-1-k} R(x,B')\frac{R(A,B')}{R(B',B-B')}.$$

(2) For $0 \leq k \leq m-1$,

$$G_k(f,g) = (-1)^{m-1-k}\sum_{A'\subset A,\,|A'|=m-1-k} R(x,A')\,\frac{R(A',B)}{R(A',A-A')}.$$

As a particular case of Proposition 5, using Identities (8) and (9), we obtain Case (2) and a particular case of Case (4) of the introduction:

Corollary 7.

(1) *Set $1 \leq m = n$ and let $0 \leq p,\ 0 \leq q$ be such that $p+q = m$. Then*

$$\mathrm{Sylv}^{p,q}(A,B) = \binom{m-1}{q}f + \binom{m-1}{p}g.$$

(2) *Set $1 \leq m = n-2$ and let $0 \leq p \leq m$, $0 \leq q$ be such that $p+q = n-1$. Then*

$$\mathrm{Sylv}^{p,q}(A,B) = (-1)^{p+1}\binom{m}{p}f.$$

This immediately yields a simple proof for the particular cases when $p+q=m<n$, see also Lascoux and Pragacz (2003), D'Andrea et al. (2007) and Roy and Szpirglas (2011).

Proposition 8. *Set $1\le m\le n-1$ and let $p\ge 0,\ q\ge 0$ be such that $1\le p+q=m$. Then*

$$\mathrm{Sylv}^{p,q}(A,B)=\binom{m}{p}f.$$

Proof. By induction on $n\ge m+1$, comparing the two expressions at the $n>m$ elements of B.
For $n=m+1$, by Lemma 2 and Corollary 7(1),

$$\begin{aligned}\mathrm{Sylv}^{p,q}(A,B)(\beta)&=\mathbf{c}_m\big(\mathrm{Sylv}^{p,q}(A,B-\beta)\big)f(\beta)\\&=\mathbf{c}_m\left(\binom{m-1}{q}f+\binom{m-1}{p}\frac{g}{x-\beta}\right)f(\beta)\\&=\left(\binom{m-1}{q}+\binom{m-1}{p}\right)f(\beta)\ =\ \binom{m}{p}f(\beta).\end{aligned}$$

Now set $n>m+1$,

$$\mathrm{Sylv}^{p,q}(A,B)(\beta)=\mathbf{c}_m\big(\mathrm{Sylv}^{p,q}(A,B-\beta)\big)f(\beta)=\mathbf{c}_m\left(\binom{m}{p}f\right)f(\beta)=\binom{m}{p}f(\beta).\quad\square$$

We finish the proof of Theorem 1 by splitting it into the two remaining cases to be proven. The first case is the inductive proof of Roy and Szpirglas (2011) that we repeat here for the sake of completeness.

Proposition 9. *Set $1\le m\le n$ and let $p\ge 0, q\ge 0$ and $k=p+q$ be such that $k\le m$ when $m<n$ and $k<m$ when $m=n$. Then*

$$\mathrm{Sylv}^{p,q}(A,B)=(-1)^{p(m-k)}\binom{k}{p}Sres_k(f,g).$$

Proof. By induction on $m\ge 1$:
The case $m=1$ is completely covered by Identities (4), (5), (3) and Proposition 8.
Now set $m>1$ and let $0\le k=p+q\le m$ if $m<n$ and $0\le k=p+q<m$ if $m=n$. We have
– For $0\le k\le m-1$, we compare $\mathrm{Sylv}^{p,q}(A,B)$ and $\mathrm{Sres}_k(f,g)$, which are both of degree $k<m$, by specializing them into the m elements $\alpha\in A$ by means of Lemma 2, the inductive hypothesis and Corollary 4:

$$\begin{aligned}\mathrm{Sylv}^{p,q}(A,B)(\alpha)&=(-1)^p\,\mathbf{c}_k\big(\mathrm{Sylv}^{p,q}(A-\alpha,B)\big)\,g(\alpha)\\&=(-1)^p(-1)^{p(m-1-k)}\binom{k}{p}\mathbf{c}_k\left(\mathrm{Sres}_k\left(\frac{f}{x-\alpha},g\right)\right)g(\alpha)\\&=(-1)^{p(m-k)}\binom{k}{p}\mathrm{Sres}_k(f,g)(\alpha).\end{aligned}$$

– For $k=m<n$, it is Proposition 8. $\square$

Proposition 10. *Set $1\le m\le n-3$ and let $0\le p\le m, 0\le q\le n$ be such that $m+1\le p+q\le n-2$. Then*

$$\mathrm{Sylv}^{p,q}(A,B)=0.$$

Proof. By induction on $n\ge m+3$, specializing the expression in the $n>m+1=k$ elements of B by Lemma 2.
For $n=m+3$, by Corollary 7(2):

$$\mathrm{Sylv}^{p,q}(A,B)(\beta)=-f(\beta)\mathbf{c}_{m+1}\big(\mathrm{Sylv}^{p,q}(A,B-\beta)\big)=-f(\beta)\mathbf{c}_{m+1}\left((-1)^{p+1}\binom{m}{p}f\right)=0,$$

since $\deg(f)=m<m+1$.
The case $n>m+3$ follows immediately. $\square$

Acknowledgements

T. Krick would like to thank the Mittag-Leffler Institute for hosting her in May 2011, during the preparation of this note. We also thank Carlos D'Andrea and the referees for useful comments.

Krick was partially supported by the research projects UBACyT X-113 2008–2010, CONICET PIP 2010–2012 and FonCyT BID-PICT 2010-0681 (Argentina); Szanto was partially supported by NSF grant CCR-0347506 (USA).

References

Apéry, François, Jouanolou, Jean-Pierre, 2005. Résultants et sous-résultants: le cas d'une variable, Monographie, Cours DESS 1995–1996, 322 pages.

Collins, George, 1967. Suresultants and reduced polynomial remainder sequences. J. ACM 142, 128–142.

D'Andrea, Carlos, Hong, Hoon, Krick, Teresa, Szanto, Agnes, 2007. An elementary proof of Sylvester's double sums for subresultants. J. Symbolic Comput. 42, 290–297.

D'Andrea, Carlos, Hong, Hoon, Krick, Teresa, Szanto, Agnes, 2009. Sylvester's double sums: the general case. J. Symbolic Comput. 44, 1164–1175.

von zur Gathen, Joachim, Gerhard, Jürgen, 2003. Modern Computer Algebra, Second edition. Cambridge University Press, Cambridge, UK, ISBN: 0-521-82646-2, 800 pages.

Geddes, Keith, Czapor, Stephen, Labahn, George, 1992. Algorithms for Computer Algebra. Kluwer Academic Publishers, ISBN: 0-7923-9259-0, 585 pages.

Ilyuta, G.G., 2005. Sylvester sub-resultants, rational Cauchy approximations, Thiele's continued fractions, and higher Bruhat orders. Uspekhi Mat. Nauk 60, 165–166.

Kós, Géza, Rónyai, Lajos, 2011. Alon's Nullstellensatz for multisets. arXiv:1008.2901.

Lascoux, Alain, Pragacz, Piotr, 2003. Double Sylvester sums for subresultants and multi-Schur functions. J. Symbolic Comput. 35, 689–710.

Roy, Marie-Françoise, Szpirglas, Aviva, 2011. Sylvester double sums and subresultants. J. Symbolic Comput. 46, 385–395.

Sylvester, James Joseph, 1853. On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's function and that of the greatest algebraical common measure. Philosophical Transactions of the Royal Society of London, Part III 407–548. Appears also in Collected Mathematical Papers of James Joseph Sylvester, Vol. 1, Chelsea Publishing Co. (1973) 429–586.