Serdica J. Computing **8** (2014), No 1, 29–46

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

STURM SEQUENCES AND MODIFIED SUBRESULTANT POLYNOMIAL REMAINDER SEQUENCES

Alkiviadis G. Akritas, Gennadi I. Malaschonok*, Panagiotis S. Vigklas

Abstract. In 1971 using *pseudo*-divisions — that is, by working in $\mathbb{Z}[x]$ — Brown and Traub computed Euclid's polynomial remainder sequences (prs's) and (proper) subresultant prs's using `sylvester1`, the most widely known form of Sylvester's matrix, whose determinant defines the resultant of two polynomials.

In this paper we use, for the first time in the literature, the Pell-Gordon Theorem of 1917, and `sylvester2`, a little known form of Sylvester's matrix of 1853 to initially compute Sturm sequences in $\mathbb{Z}[x]$ *without* pseudo-divisions — that is, by working in $\mathbb{Q}[x]$. We then extend our work in $\mathbb{Q}[x]$ and, despite the fact that the absolute value of the determinant of `sylvester2` equals the absolute value of the resultant, we construct *modified* subresultant prs's, which may differ from the proper ones only in sign.

ACM Computing Classification System (1998): F.2.1, G.1.5, I.1.2.

Key words: Polynomials, real roots, Sturm sequences, Sylvester's matrices, matrix triangularization.

*This author is partly supported by project 2476 of the Government Task of the Russian Ministry of Education and Science (No. 2014/285) and by project 12-07-00755 of Russian Foundation for Basic Research.

1. Introduction. The Sturm sequence of a polynomial $p(x) \in \mathbb{Z}[x]$ or $p(x) \in \mathbb{Q}[x]$, of degree $n \geqslant 2$, is the sequence of functions $f_0(x), f_1(x), \ldots, f_k(x)$, $k \leqslant n$, where $f_0(x) = p(x)$, $f_1(x) = p'(x)$, and, for $2 \leqslant j \leqslant k$, $f_j(x)$ is the *negative* remainder obtained on dividing $f_{j-2}(x)$ by $f_{j-1}(x)$.

In other words, the Sturm sequence of $p(x)$ is obtained by *negating* the remainders obtained in the process of finding the greatest common divisor of $p(x)$ and $p'(x)$ using the Euclidean algorithm.

If $k = n$, the Sturm sequence is called *complete*, whereas if $k < n$, it is called *incomplete*.

Therefore, we see that obtaining polynomial remainders is the major operation in computing Sturm sequences and, since 1836, *pseudo*-division (explained below) has been the only method used to keep these computations in $\mathbb{Z}[x]$.

For example, the Sturm sequence in $\mathbb{Z}[x]$ of $p(x) = x^3 + 3x^2 - 7x + 7$ is shown below and was obtained with the `sturm` function of the freely available Computer Algebra System (CAS) `Xcas`:[1]

```
> sturm(x^3+3x^2-7x+7)[1]
```

$$[[1, 3, -7, 7], [3, 6, -7], [60, -84], -2912]$$

Here, to obtain the first remainder, $60x - 84$, we had to pseudo-divide; in other words, we premultiplied the divident by 3^2, that is, by the leading coefficient of the divisor raised to the power $\deg(p) - \deg(p') + 1$, and then we applied the division algorithm for polynomials. The second remainder -2912 was computed in a similar way.

However, using pseudo-division in every step of the Sturmian (Euclidean) algorithm causes exponential coefficient growth [1]. To avoid this exponential coefficient growth we can make every intermediate result *primitive*, that is, we can divide the remainders by the greatest common divisors of their coefficients, the so-called *content*. However, computing the content was (erroneously) considered to be quite expensive, especially for multivariate polynomials, and one would like to find divisors of the content without any gcd computation.

In 1853 Sylvester discovered that, for complete Sturm sequences in $\mathbb{Z}[x]$, the coefficients of the polynomial remainders can be correctly computed as determinants of submatrices of `sylvester2`, a little known form of *Sylvester*'s matrix of dimension $2n \times 2n$ [15], [5]; we call these determinants *modified subresultants* to distinguish them from the proper subresultants which are determinants of submatrices of `sylvester1`, the wel-known form of Sylvester's matrix of dimension

[1] In both CASs used in this paper, `Xcas` and `Sympy`, enumeration begins with 0. The interface to them was `TeXmacs`.

$(m+n)\times(m+n)$, which was discovered in 1840 [14]. However, Sylvester's result of 1853 did not carry over to incomplete Sturm sequences, since the signs of the coefficients could not be correctly computed.

As Sylvester pointed out, the coefficients of the polynomial remainders obtained as modified subresultants are the *smallest possible* without introducing rationals and without computing (integer) greatest common divisors. However, since it is time consuming — and tiring — to evaluate a large number of determinants, people use pseudo-division and then divide out a certain factor to reduce the coefficients to modified subresultants.

In general, given $p(x), q(x) \in \mathbb{Z}[x]$ of degrees $deg(p) = n$ and $deg(q) = m$ with $n \geq m$ their (proper) subresultant polynomial remainder sequence (prs) is a sequence of polynomials similar to the one obtained by applying Euclid's algorithm on $p(x), q(x)$. The two sequences differ in that the coefficients of each polynomial in the subresultant prs are the determinants of submatrices of `sylvester1`. The determinant of `sylvester1` itself is called the *resultant* of $p(x), q(x)$ and serves as a criterion of whether the two polynomials have common roots or not.

The problem of computing in $\mathbb{Z}[x]$ the proper subresultant prs of $p(x), q(x)$ has been extensively studied in the literature along with its relation to the prs obtained from Euclid's algorithm [12], [7], [8], [10], [11], [9].

It has been shown in the literature that using `sylvester1` the polynomials in the proper subresultant prs are proportional to those obtained by the Euclidean algorithm. Moreover, for complete sequences obtained using `sylvester1`, the proper subresultant prs is identical to the Euclidean prs, where the polynomial remainder p_{i+2} in the latter sequence has been divided by the square of the leading coefficient of the polynomial p_i [1].

In `Xcas` the function `sylvester` returns the matrix `sylvester1`. This function can be easily renamed `sylvester1` with the statement `sylvester1 := sylvester`. Then, for the polynomials $p(x) = ax^3 + bx^2 + cx + d$ with $a > 0$, and $q(x) = 3ax^2 + 2bx + c$ the 5×5 `sylvester1` matrix is given below:

```
> sylvester1(a*x^3+b*x^2+c*x+d, 3a*x^2+2b*x+c, x)
```

$$\begin{pmatrix} a & b & c & d & 0 \\ 0 & a & b & c & d \\ 3a & 2b & c & 0 & 0 \\ 0 & 3a & 2b & c & 0 \\ 0 & 0 & 3a & 2b & c \end{pmatrix}$$

Note that the entries in the above matrix are the coefficients of the two polynomials; in the first group of *two* rows are the coefficients of $p(x) = ax^3 +$

$bx^2 + cx + d$, whereas in the second (last) group of *three* rows are the coefficients of $q(x) = 3ax^2 + 2bx + c$. The proper subresultant prs of $p(x), q(x)$ has two additional polynomials, $f \cdot x + g$ and h, of degrees 1 and 0, respectively.

The constant polynomial h of degree 0 — which is the resultant of the two polynomials — is easily computed as the determinant of the 5×5 `sylvester1` matrix and is shown below

$$27 \cdot a^3 \cdot d^2 - 18 \cdot a^2 \cdot b \cdot c \cdot d + 4 \cdot a^2 \cdot c^3 + 4 \cdot a \cdot b^3 \cdot d - a \cdot b^2 \cdot c^2. \tag{1}$$

To compute the coefficients f, g of the polynomial of degree 1, we delete 1 (the last) row from each group of rows in the `sylvester1` matrix and we are left with the 3×5 matrix:

$$\begin{pmatrix} a & b & c & d & 0 \\ 3a & 2b & c & 0 & 0 \\ 0 & 3a & 2b & c & 0 \end{pmatrix}.$$

Then,

$$f = \begin{vmatrix} a & b & c \\ 3a & 2b & c \\ 0 & 3a & 2b \end{vmatrix},$$

and, after we swap the 3rd and 4th columns,

$$g = \begin{vmatrix} a & b & d \\ 3a & 2b & 0 \\ 0 & 3a & c \end{vmatrix}.$$

We have written code in `Xcas` that performs these computations easily,[2] and the reader is urged to take advantage of it in order to compute the proper subresultant prs of the polynomial $p(x) = x^6 + x^5 - x^4 - x^3 + x^2 - x + 1$ and its derivative.[3]

Using the function `subresultants` of `Sympy`, another freely available CAS, we can verify that the answer is:

$$x^6 + x^5 - x^4 - x^3 + x^2 - x + 1,$$
$$6x^5 + 5x^4 - 4x^3 - 3x^2 + 2x - 1,$$

[2]It can be downloaded from the link `http://inf-server.inf.uth.gr/~akritas/publications/subres_sylvester1`

[3]This is the same example used by Van Vleck [16].

$$
\begin{aligned}
&-17x^4 - 14x^3 + 27x^2 - 32x + 37,\\
&44x^3 - 114x^2 + 120x - 7,\\
&-516x^2 + 828x + 186,\\
&9108x - 3114,\\
&127359.
\end{aligned} \tag{2}
$$

The proper subresultant prs computed this way is identical with the prs obtained by Euclid's algorithm for polynomials and the constant 127359 is the value of the resultant of $p(x)$ and its derivative. Consequently, sequence (2) differs from the Sturm sequence of the polynomial $p(x) = x^6 + x^5 - x^4 - x^3 + x^2 - x + 1$.

Using the `Xcas` function `sturm` we see that the Sturm sequence of $p(x)$ is:

$$
\begin{aligned}
&x^6 + x^5 - x^4 - x^3 + x^2 - x + 1,\\
&6x^5 + 5x^4 - 4x^3 - 3x^2 + 2x - 1,\\
&17x^4 + 14x^3 - 27x^2 + 32x - 37,\\
&-44x^3 + 114x^2 - 120x + 7,\\
&-516x^2 + 828x + 186,\\
&9108x - 3114,\\
&-127359.
\end{aligned} \tag{3}
$$

A term by term comparison of sequences (2) and (3) reveals that:

- the absolute values of the coefficients of both sequences are the same, whereas

- the signs in the two sequences may differ.

Therefore, the proper subresultant prs computed using the `sylvester1` matrix of the polynomial $p(x) = x^6 + x^5 - x^4 - x^3 + x^2 - x + 1$ and its derivative gives us information about the prs obtained by the Euclidean algorithm and the resultant of the two polynomials.

However, there also exists a rarely used form of Sylvester's matrix, call it `sylvester2`, whose dimensions are $2n \times 2n$; that matrix was developed by Sylvester in 1853 and by Jacobi eighteen years earlier and has been used by very few authors, including the first author of this paper [16], [13], [2], [3], [4], [5], [6].

For `Xcas` we have written our own function `sylvester2`[4] and for the same polynomials $p(x) = ax^3 + bx^2 + cx + d$ with $a > 0$ and $q(x) = 3ax^2 + 2bx + c$ mentioned above the 6×6 `sylvester2` matrix is:

```
> sylvester2(a*x^3+b*x^2+c*x+d, 3a*x^2+2b*x+c,x)
```

$$\begin{pmatrix} a & b & c & d & 0 & 0 \\ 0 & 3a & 2b & c & 0 & 0 \\ 0 & a & b & c & d & 0 \\ 0 & 0 & 3a & 2b & c & 0 \\ 0 & 0 & a & b & c & d \\ 0 & 0 & 0 & 3a & 2b & c \end{pmatrix}.$$

Note that the entries in the above matrix are the coefficients of the two polynomials written in 3 pairs. We can now use `sylvester2` to compute a modified subresultant prs of $p(x), q(x)$, which also has two additional polynomials, $\tilde{f} \cdot x + \tilde{g}$ and $\tilde{h}$, of degrees 1 and 0, respectively.

The constant polynomial $\tilde{h}$ of degree 0 is easily computed as the determinant of the 6×6 `sylvester2` matrix and its value — reduced by dividing out a — is shown below

$$-27 \cdot a^3 \cdot d^2 + 18 \cdot a^2 \cdot b \cdot c \cdot d - 4 \cdot a^2 \cdot c^3 - 4 \cdot a \cdot b^3 \cdot d + a \cdot b^2 \cdot c^2. \tag{4}$$

Comparing (1) and (4) we see that the determinant of `sylvester2` and the resultant have opposite signs.

To compute the coefficients $\tilde{f}, \tilde{g}$ of the polynomial of degree 1, we delete 1 pair (the last) of rows in the `sylvester2` matrix and we are left with the 4×6 matrix:

$$\begin{pmatrix} a & b & c & d & 0 & 0 \\ 0 & 3a & 2b & c & 0 & 0 \\ 0 & a & b & c & d & 0 \\ 0 & 0 & 3a & 2b & c & 0 \end{pmatrix}.$$

Then, the reduced coefficients are:

$$\tilde{f} = \begin{vmatrix} a & b & c & d \\ 0 & 3a & 2b & c \\ 0 & a & b & c \\ 0 & 0 & 3a & 2b \end{vmatrix} /a,$$

[4]It can be found in the link: `http://inf-server.inf.uth.gr/~akritas/publications/sylvester2`

and, after we swap the 4th and 5th columns,

$$\tilde{g} = \begin{vmatrix} a & b & c & 0 \\ 0 & 3a & 2b & 0 \\ 0 & a & b & d \\ 0 & 0 & 3a & c \end{vmatrix} /a.$$

The reader is asked to use the `Xcas` functions `subMat` and `colSwap` and compute the modified subresultant prs of the polynomial $p(x) = x^6 + x^5 - x^4 - x^3 + x^2 - x + 1$ and its derivative. It turns out that using the `sylvester2` matrix, the modified subresultant prs is:

$$\begin{aligned} & x^6 + x^5 - x^4 - x^3 + x^2 - x + 1, \\ & 6x^5 + 5x^4 - 4x^3 - 3x^2 + 2x - 1, \\ & 17x^4 + 14x^3 - 27x^2 + 32x - 37, \\ & -44x^3 + 114x^2 - 120x + 7, \\ & -516x^2 + 828x + 186, \\ & 9108x - 3114, \\ & -127359. \end{aligned} \tag{5}$$

Comparing sequences (2), (3) and (5) we see that:

- sequences (2) and (5) differ, which implies that the signs of the modified subresultant prs may differ from those of the proper one, and
- sequences (3) and (5) are identical (as Sylvester realized in 1853 and as is proven by equation (9) in Section 3.1), which implies that, for complete prs's, the modified subresultant prs, computed with `sylvester2`, is identical to the Sturm sequence — provided the second polynomial is the derivative of the first.

For complete Sturm sequences in $\mathbb{Z}[x]$, Van Vleck presented in 1900 a theorem and a computational method for computing the polynomial remainders of Sturm's sequences by triangularizing the `sylvester2` matrix of $p(x)$ and $p'(x)$. In his method VanVleck cleverly takes advantage of the special form of this matrix and only triangularizes matrices of 3 rows, thus making his method extremely fast and suitable even for manual computations [16], [6].

However, Van Vleck's method computes the correct sign of the coefficients *only* for complete Sturm sequences, when no pivot occurs in the triangularization

process. In all other cases the sign of the coefficients may not be correct. This was observed by Pell[5] and Gordon ([13], p. 193) and — using the `sylvester2` matrix — they presented a theorem, Theorem 1 in this paper, to correctly compute, in all cases, the coefficients of the polynomial remainders of Sturm prs's in $\mathbb{Q}[x]$, that is *without* pseudo-divisions. Theorem 1 was also used by us to construct modified subresultant prs's in $\mathbb{Z}[x]$ without pseudo-divisions; this was achieved by multiplying each remainder in $\mathbb{Q}[x]$ by a certain factor.

To compute the Sturm prs in $\mathbb{Q}[x]$ for the polynomial $p(x) = x^3 + 3x^2 - 7x + 7$ we use the function `sturm` of `Sympy` as follows:

```
Python] import sympy

Python] x = sympy.var('x')

Python] sympy.sturm(x**3+3*x**2-7*x+7)

 [x**3 + 3*x**2 - 7*x + 7, 3*x**2 + 6*x - 7, 20*x/3 - 28/3, -182/25]
```

To our knowledge, the Pell-Gordon paper was completely forgotten and has not been cited in the literature before us.[6] However, this paper is of great importance because, as it turns out, Pell and Gordon anticipated by 30 and 50 years, respectively, the main results by Habicht (1948) [12] and Brown-Collins (1966-1971) [7], [8], [10], [11].

The rest of the paper is organised as follows:

In Section 2 we state the Pell-Gordon Theorem ([13], pp. 190, 193) for two polynomials A, B and present a modification of it along with an example of its use. The modification concerns: (a) the leading coefficient of A, (b) the degree difference between the polynomial remainders in case of incomplete Sturm sequences, and (c) the number of leading zero coefficients in the second polynomial.

In Section 3 we first compute Sturm sequences in $\mathbb{Z}[x]$ using polynomial divisions in $\mathbb{Q}[x]$ and the formula (7) of the Pell-Gordon Theorem without taking into consideration the signs involved. Once this is accomplished, we use the signs involved in formula (7) to compute modified subresultant prs's in $\mathbb{Z}[x]$ corresponding to `sylvester2`, Sylvester's matrix of 1853. Codes in `Sympy` are provided for both cases.

Finally, in Section 4 we state our conclusions.

---

[5] See the link `http://en.wikipedia.org/wiki/Anna_Johnson_Pell_Wheeler` for a biography of Anna Johnson Pell Wheeler.

[6] Panagiotis S. Vigklas discovered it while reviewing scientific data bases.

2. The Pell-Gordon Theorem for Polynomials in $\mathbb{Q}[x]$. As mentioned in the Introduction, Anna Johnson Pell Wheeler and R. L. Gordon realized the flaw in Van Vleck's theorem when the Sturm sequence is incomplete. Using `sylvester2`, the same form of Sylvester's matrix as Van Vleck, they stated and proved the following [13]:

Theorem 1. *Let*

$$A = a_0x^n + a_1x^{n-1} + \cdots + a_n$$

and

$$B = b_0x^n + b_1x^{n-1} + \cdots + b_n$$

be two polynomials of the n-th degree. Modify the process of finding the highest common factor of A and B by taking at each stage the negative of the remainder. Let the i-th modified remainder be

$$R^{(i)} = r_0^{(i)}x^{m_i} + r_1^{(i)}x^{m_i-1} + \cdots + r_{m_i}^{(i)}$$

where (m_i+1) *is the degree of the preceeding remainder, and where the first* (p_i-1) *coefficients of* $R^{(i)}$ *are zero, and the* p_i*th coefficient* $\varrho_i = r_{p_i-1}^{(i)}$ *is different from zero. Then for* $k = 0, 1, \ldots, m_i$ *the coefficients* $r_k^{(i)}$ *are given by*[7]

$$r_k^{(i)} = \frac{(-1)^{u_{i-1}}\,(-1)^{u_{i-2}}\cdots(-1)^{u_1}\,(-1)^{v_{i-1}}}{\varrho_{i-1}^{p_{i-1}+1}\,\varrho_{i-2}^{p_{i-2}+p_{i-1}}\cdots\varrho_1^{p_1+p_2}\,\varrho_0^{p_1}} \cdot \mathrm{Det}\,(i,k)\,, \tag{6}$$

where $u_{i-1} = 1 + 2 + \cdots + p_{i-1}$, $v_{i-1} = p_1 + p_2 + \cdots + p_{i-1}$ *and*

$$\mathrm{Det}\,(i,k) = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & \cdot & \cdot & \cdots & a_{2v_{i-1}} & a_{2v_{i-1}+1+k} \\ b_0 & b_1 & b_2 & \cdots & \cdot & \cdot & \cdots & b_{2v_{i-1}} & b_{2v_{i-1}+1+k} \\ 0 & a_0 & a_1 & \cdots & \cdot & \cdot & \cdots & a_{2v_{i-1}-1} & a_{2v_{i-1}+k} \\ 0 & b_0 & b_1 & \cdots & \cdot & \cdot & \cdots & b_{2v_{i-1}-1} & b_{2v_{i-1}+k} \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & a_0 & a_1 & \cdots & a_{v_{i-1}} & a_{v_{i-1}+1+k} \\ 0 & 0 & 0 & \cdots & b_0 & b_1 & \cdots & b_{v_{i-1}} & b_{v_{i-1}+1+k} \end{vmatrix}.$$

P r o o f. The proof by induction of this theorem depends on two Lemmas and can be found in the original paper of Pell and Gordon.

As demonstrated in Example 1 that follows below,[8] we use a modification of formula (6) to compute the coefficients of the Sturm sequence. In our case

[7] It is understood in (6) that $\varrho_0 = b_0$, $p_0 = 0$, and that $a_i = b_i = 0$ for $i > n$.

[8] Since there are no examples in [13] we believe our Example 1 is quite useful.

$p_0 = \deg(A) - \deg(B) = 1$, since B is the derivative of A and, hence, the modified formula is shown below with the changes appearing in bold:

$$r_k^{(i)} = \frac{(-1)^{u_{i-1}}(-1)^{u_{i-2}}\cdots(-1)^{u_1}(-1)^{u_0}(-1)^{v_{i-1}}}{\varrho_{i-1}^{\boldsymbol{p_{i-1}+p_i-\mathbf{degDiffer}}}\varrho_{i-2}^{p_{i-2}+p_{i-1}}\cdots\varrho_1^{p_1+p_2}\varrho_0^{\boldsymbol{p_0}+p_1}}\cdot\frac{\mathrm{Det}(i,k)}{\boldsymbol{\varrho_{-1}}}, \tag{7}$$

where `degDiffer` is the difference between the expected degree m_i and the actual degree of the remainder and $\varrho_{-1} = a_0$, the leading coefficient of A.

It should be noted that in the general case $p_0 = \deg(A) - \deg(B)$ and that the division $\dfrac{\mathrm{Det}(i,k)}{\varrho_{-1}}$ is possible if the leading coefficient of A is the only element in the first column of Sylvester's matrix. Moreover, if the leading coefficient of A is negative we work with the polynomial negated and at the end we reverse the signs of all polys in the sequence. □

Example 1. Take $A = 4x^5 - 3x^4 + 7$ and $B = 20x^4 - 12x^3$ and form their `sylvester2` matrix:

```
> A:=4*x^5-3*x^4+7
```

$$4\cdot x^5 - 3\cdot x^4 + 7$$

```
> B:=simplify(diff(4*x^5-3*x^4+7,x))
```

$$20\cdot x^4 - 12\cdot x^3$$

```
> S:=sylvester2(A,B,x)
```

$$\begin{pmatrix} 4 & -3 & 0 & 0 & 0 & 7 & 0 & 0 & 0 & 0 \\ 0 & 20 & -12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & -3 & 0 & 0 & 0 & 7 & 0 & 0 & 0 \\ 0 & 0 & 20 & -12 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & -3 & 0 & 0 & 0 & 7 & 0 & 0 \\ 0 & 0 & 0 & 20 & -12 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & -3 & 0 & 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 0 & 20 & -12 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & -3 & 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 & 0 & 20 & -12 & 0 & 0 & 0 \end{pmatrix}$$

All operations will be done in $\mathbb{Q}[x]$. For $i = 1$, the first remainder *negated* is of degree 3:

```
> R_1:=-rem(A,B,x)
```

$$-\frac{-9}{25}\cdot x^3 - 7$$

In the terminology of Theorem 1, here we have $p_1 - 1 = 0$ — from which we deduce $p_1 = 1$ — and $\varrho_1 = r^{(1)}_{p_1-1} = r^{(1)}_0 = \dfrac{9}{25}$.

The above information can be obtained from formula (7) if we set $\varrho_{-1} = 4$, the leading coefficient of A, $\varrho_0 = 20$, the leading coefficient of B, and $p_0 = 1$, since B is the derivative of A. Consequently, we have $u_0 = 1+2+\cdots+p_0 = p_0 = 1$ and $v_0 = p_1 + p_2 + \cdots + p_0 = p_0 = 1$, from which we compute the leading coefficient of the remainder as :

$$r^{(1)}_0 = \frac{9}{25} = \frac{(-1)^{u_0}\,(-1)^{v_0}}{\varrho_0^{p_0+p_1-\mathrm{degDiffer}}} \cdot \frac{\det(1,0)}{\varrho_{-1}} = \frac{1}{20^2} \cdot \frac{\det(1,0)}{4},$$

where degDiffer $= 3 - 3 = 0$ and $\det(1,0)$ is a submatrix of S. (degDiffer $= 0$ because we expected a remainder of degree 3 and it turns out that the remainder is indeed of degree 3.)

Since $v_0 = 1$, to compute $\det(1,0)$ we form the 4×4 submatrix M of S defined below:

```
> M:=subMat(S,0,0,3,3)
```

$$\begin{pmatrix} 4 & -3 & 0 & 0 \\ 0 & 20 & -12 & 0 \\ 0 & 4 & -3 & 0 \\ 0 & 0 & 20 & -12 \end{pmatrix}$$

and $r^{(1)}_0$ ie equal to

```
> (1/(20^2))*det(M)/4
```

$$\frac{9}{25}$$

The other three coefficients $r^{(1)}_1$, $r^{(1)}_2$, $r^{(1)}_3$ of the remainder are computed below and agree with those computed above with division. For their computation as determinants we have to successively swap in S the fourth column with the fifth, sixth and seventh columns, respectively.

For $r^{(1)}_1$ we have:

```
> M:=subMat(colSwap(S,3,4),0,0,3,3)
```

$$\begin{pmatrix} 4 & -3 & 0 & 0 \\ 0 & 20 & -12 & 0 \\ 0 & 4 & -3 & 0 \\ 0 & 0 & 20 & 0 \end{pmatrix}$$

```
> (1/(20^2))*det(M)/4
```

$$0$$

For $r_2^{(1)}$ we have:

```
> M:=subMat(colSwap(S,3,5),0,0,3,3)
```

$$\begin{pmatrix} 4 & -3 & 0 & 7 \\ 0 & 20 & -12 & 0 \\ 0 & 4 & -3 & 0 \\ 0 & 0 & 20 & 0 \end{pmatrix}$$

```
> (1/(20^2))*det(M)/4
```

$$0$$

For $r_3^{(1)}$ we have:

```
> M:=subMat(colSwap(S,3,6),0,0,3,3)
```

$$\begin{pmatrix} 4 & -3 & 0 & 0 \\ 0 & 20 & -12 & 0 \\ 0 & 4 & -3 & 7 \\ 0 & 0 & 20 & 0 \end{pmatrix}$$

```
> (1/(20^2))*det(M)/4
```

$$-7$$

For $i = 2$ the second remainder negated is of degree 1:

```
> R_2:=-rem(B,R_1,x)
```

$$-\frac{3500}{9} \cdot x - \frac{-700}{3}$$

In the terminology of Theorem 1, here we have $p_2 - 2 = 0$ — from which we deduce $p_2 = 2$ — and $\varrho_2 = r^{(2)}_{p_2-1} = r^{(2)}_1 = -\dfrac{3500}{9}$. Clearly, $r^{(2)}_0 = 0$.

The above information can be also obtained from formula (7) if we consider that we now have $u_1 = 1 + 2 + \cdots + p_1 = p_1 = 1$ and $v_1 = p_0 + p_1 + \cdots + p_1 = p_0 + p_1 = 2$ from which we compute the leading coefficient of the remainder as:

$$r^{(2)}_1 = -\frac{3500}{9} = \frac{(-1)^{u_1}\,(-1)^{u_0}\,(-1)^{v_1}}{\varrho_1^{p_1+p_2-\mathrm{degDiffer}}\,\varrho_0^{p_0+p_1}} \cdot \frac{\det(2,1)}{\varrho_{-1}} = \frac{1}{\left(\frac{9}{25}\right)^2 20^2} \cdot \frac{\det(2,1)}{4},$$

where degDiffer $= 2 - 1 = 1$ and $\det(2,1)$ is a submatrix of S. (degDiffer $= 1$ because we expected a remainder of degree 2 and it turns out that the remainder is of degree 1.) Notice that $\dfrac{9}{25}$ is now raised to the power 2 instead of to the power 3.

Since $v_1 = 2$, we compute $\det(2,1)$ from a 6×6 submatrix M of S. Notice, however, that since the first coefficient is $r_0^{(2)} = 0$ the determinant of the submatrix M below is 0.

```
> M:=subMat(S,0,0,5,5)
```

$$\begin{pmatrix} 4 & -3 & 0 & 0 & 0 & 7 \\ 0 & 20 & -12 & 0 & 0 & 0 \\ 0 & 4 & -3 & 0 & 0 & 0 \\ 0 & 0 & 20 & -12 & 0 & 0 \\ 0 & 0 & 4 & -3 & 0 & 0 \\ 0 & 0 & 0 & 20 & -12 & 0 \end{pmatrix}$$

```
> det(M)
```

$$0$$

Subsequently, for $r_1^{(2)}$ and $r_2^{(2)}$ we swap in S column 5 with columns 6 and 7, respectively.

For $r_1^{(2)}$ we have:

```
> M:=subMat(colSwap(S,5,6),0,0,5,5)
```

$$\begin{pmatrix} 4 & -3 & 0 & 0 & 0 & 0 \\ 0 & 20 & -12 & 0 & 0 & 0 \\ 0 & 4 & -3 & 0 & 0 & 7 \\ 0 & 0 & 20 & -12 & 0 & 0 \\ 0 & 0 & 4 & -3 & 0 & 0 \\ 0 & 0 & 0 & 20 & -12 & 0 \end{pmatrix}$$

```
> (1/((9/25)^2*20^2))*det(M)/4
```

$$\frac{-3500}{9}$$

For $r_2^{(2)}$ we have:

```
> M:=subMat(colSwap(S,5,7),0,0,5,5)
```

$$\begin{pmatrix} 4 & -3 & 0 & 0 & 0 & 0 \\ 0 & 20 & -12 & 0 & 0 & 0 \\ 0 & 4 & -3 & 0 & 0 & 0 \\ 0 & 0 & 20 & -12 & 0 & 0 \\ 0 & 0 & 4 & -3 & 0 & 7 \\ 0 & 0 & 0 & 20 & -12 & 0 \end{pmatrix}$$

```
> (1/((9/25)^2*20^2))*det(M)/4
```

$$\frac{700}{3}$$

For $i = 3$ the third remainder negated is of degree 0:

```
> R_3:=-rem(R_1,R_2,x)
```

$$\frac{21632}{3125}$$

In the terminology of Theorem 1, here we have $p_3 - 1 = 0$ — from which we deduce $p_3 = 1$ — and $\varrho_3 = r^{(3)}_{p_3-1} = r^{(3)}_0 = \dfrac{21632}{3125}$.

The above information can be also obtained from formula (7) if we consider that we now have $u_2 = 1+2+\cdots+p_2 = 1+p_2 = 3$ and $v_2 = p_0+p_1+p_2+\cdots+p_2 = p_0 + p_1 + p_2 = 4$, from which we compute

$$r^{(3)}_0 = \frac{(-1)^{u_2}\,(-1)^{u_1}\,(-1)^{u_0}\,(-1)^{v_2}}{\varrho_2^{p_2+p_3-\text{degDiffer}}\,\varrho_1^{p_1+p_2}\,\varrho_0^{p_1+p_0}} \cdot \frac{\det(3,0)}{\varrho_{-1}} = \frac{-1}{\left(-\frac{3500}{9}\right)^3\left(\frac{9}{25}\right)^3 20^2} \cdot \frac{\det(3,0)}{4},$$

where degDiffer $= 0-0 = 0$ and $\det(3,0)$ is a submatrix of S. (degDiffer $=$ 0 because we expected a remainder of degree 0 and it turns out that the remainder is indeed of degree 0.)

Since $v_2 = 4$, to compute $\det(3,0)$ we take the whole 10×10 matrix S and have:

```
> (-1/((-3500/9)^3*(9/25)^3*20^2))*det(S)/4
```

$$\frac{21632}{3125}$$

3. Sturm Sequences in $\mathbb{Z}[x]$ and Modified Subresultant PRS's Using Polynomial Divisions in $\mathbb{Q}[x]$. The goal of this section is to use equation (7) of the Pell-Gordon Theorem in order to develop an algorithm for computing modified subresultant prs's in $\mathbb{Z}[x]$ by doing polynomial divisions in $\mathbb{Q}[x]$. This will be achieved in two steps:

- Using the absolute value of the denominator of the first fraction in the modified Pell-Gordon equation (7), we first develop an algorithm to compute Sturm sequences in $\mathbb{Z}[x]$ doing divisions in $\mathbb{Q}[x]$. If the Sturm sequence is complete, then we have computed the modified subresultant prs as well.
- For the general case, using the exact value of the fraction in the modified Pell-Gordon equation (7), we develop an algorithm to compute modified subresultant prs's.

3.1. Sturm Sequences in $\mathbb{Z}[x]$ Using the Pell-Gordon Theorem. In this case we are given two polynomials A, B in $\mathbb{Z}[x]$, where B is the derivative of A and want to compute in $\mathbb{Z}[x]$ the Sturm sequence of A using Theorem 1 — that is, performing divisions in $\mathbb{Q}[x]$. Our goal is achieved by multiplying, at each step, the remainder $R^{(i)} \in \mathbb{Q}[x]$ times the absolute value of the denominator of the first fraction in (7).

To wit, if we take the absolute value of the first fraction in (7) and multiply both sides of the equation by the denominator we obtain the following equation:

$$\left|\varrho_{i-1}^{p_{i-1}+\boldsymbol{p_i}-\mathbf{degDiffer}}\,\varrho_{i-2}^{p_{i-2}+p_{i-1}}\cdots\varrho_1^{p_1+p_2}\,\varrho_0^{\boldsymbol{p_0}+p_1}\right|\cdot r_k^{(i)} = \frac{\mathrm{Det}\,(i,k)}{\boldsymbol{\varrho_{-1}}}. \tag{8}$$

In equation (8) recall that $r_k^{(i)}$ is the k-th coefficient of the remainder $R^{(i)} \in \mathbb{Q}[x]$; in addition, note that the expression $\dfrac{\mathrm{Det}\,(i,k)}{\boldsymbol{\varrho_{-1}}}$ is an integer because the division is exact.[9] Moreover, we can easily infer from equation (8) that

$$\mathrm{sgn}\left(r_k^{(i)}\right) = \mathrm{sgn}\left(\frac{\mathrm{Det}\,(i,k)}{\boldsymbol{\varrho_{-1}}}\right). \tag{9}$$

Therefore, we conclude that

$$\left|\varrho_{i-1}^{p_{i-1}+\boldsymbol{p_i}-\mathbf{degDiffer}}\,\varrho_{i-2}^{p_{i-2}+p_{i-1}}\cdots\varrho_1^{p_1+p_2}\,\varrho_0^{\boldsymbol{p_0}+p_1}\right|\cdot R^{(i)} \in \mathbb{Z}[x], \tag{10}$$

that is, after we multiply the ith remainder $R^{(i)}$ by the absolute value of the denominator of the first fraction in (7), the result will be in $\mathbb{Z}[x]$, and becomes part of the Sturm sequence over the integers. Moreover, because of (9), the Sturm sequence is identical to the modified subresultant prs.

The above procedure is easily programmed. The only critical point is to effectively compute the absolute value in (10). This value is not computed anew for each remainder $R^{(i)}$; instead, a multiplication factor, `mulFac`, is being updated as new leading coefficients are included in (10). So, if the current multiplication factor is

$$\mathrm{mulFac}_i = \left|\varrho_{i-1}^{p_{i-1}+\boldsymbol{p_i}-\mathbf{degDiffer_i}}\,\varrho_{i-2}^{p_{i-2}+p_{i-1}}\cdots\varrho_1^{p_1+p_2}\,\varrho_0^{\boldsymbol{p_0}+p_1}\right|,$$

then the updated factor for the next remainder $R^{(i+1)}$ is

$$\mathrm{mulFac}_{i+1} = \left|\varrho_i^{p_i+\boldsymbol{p_{i+1}}-\mathbf{degDiffer_{i+1}}}\,\varrho_{i-1}^{\mathbf{degDiffer_i}}\cdot\mathrm{mulFac}_i\right|,$$

[9] Since $\deg(B) < \deg(A)$ the leading coefficient of A is the only element in the first column of the `sylvester2` matrix of A, B.

which means that

$$\text{mulFac}_{i+1} = \left| \varrho_i^{p_i+\boldsymbol{p_{i+1}}-\mathbf{degDiffer_{i+1}}} \varrho_{i-1}^{p_{i-1}+p_i} \cdots \varrho_1^{p_1+p_2} \varrho_0^{\boldsymbol{p_0}+p_1} \right|.$$

Our own code for `Sympy` can be found in the link `http://inf-server.inf.uth.gr/~akritas/publications/sturm_PG.py`

3.2. Modified Subresultant PRS's Using the Pell-Gordon Theorem. As mentioned above, when the Sturm sequence is incomplete it does not necessarily match the modified subresultant prs, because as Pell and Gordon observed:[10]

$$\operatorname{sgn}\left(r_k^{(i)}\right) \neq \operatorname{sgn}\left(\operatorname{Det}(i,k)\right).$$

Therefore, to form the modified subresultant prs in the general case we have to additionally compute the sign of the determinant $\operatorname{Det}(i,k)$. This is accomplished again with the help of Theorem 1 if, instead of equation (8), we now use:

$$\left| \varrho_{i-1}^{p_{i-1}+\boldsymbol{p_i}-\mathbf{degDiffer}} \varrho_{i-2}^{p_{i-2}+p_{i-1}} \cdots \varrho_1^{p_1+p_2} \varrho_0^{\boldsymbol{p_0}+p_1} \right| \cdot r_k^{(i)} = fraction \cdot \operatorname{Det}(i,k), \tag{11}$$

where

$$fraction = \\ = \frac{(-1)^{u_{i-1}} (-1)^{u_{i-2}} \cdots (-1)^{u_1} (-1)^{u_0} (-1)^{v_{i-1}}}{\operatorname{sgn}\left(\varrho_{i-1}^{p_{i-1}+\boldsymbol{p_i}-\mathbf{degDiffer}}\right) \operatorname{sgn}\left(\varrho_{i-2}^{p_{i-2}+p_{i-1}}\right) \cdots \operatorname{sgn}\left(\varrho_1^{p_1+p_2}\right) \operatorname{sgn}\left(\varrho_0^{\boldsymbol{p_0}+p_1}\right)}.$$

Obviously, from equation (11) it follows that

$$\operatorname{sgn}\left(r_k^{(i)}\right) = \operatorname{sgn}(fraction) \cdot \operatorname{sgn}\left(\operatorname{Det}(i,k)\right), \tag{12}$$

and from equation (12) we obtain

$$\operatorname{sgn}\left(\operatorname{Det}(i,k)\right) = \begin{cases} \operatorname{sgn}\left(r_k^{(i)}\right) & \text{if } \operatorname{sgn}(fraction) > 0, \\ -\operatorname{sgn}\left(r_k^{(i)}\right) & \text{if } \operatorname{sgn}(fraction) < 0. \end{cases} \tag{13}$$

In this subsection we use the full power of Theorem 1 and, therefore, the computer implementation is a bit more complicated.

[10] Notice than in the general case we cannot exactly divide by ϱ_{-1}.

Our own code for `Sympy` can be found in the link `http://inf-server.inf.uth.gr/~akritas/publications/sturm_Subresultants_PG.py`

4. Conclusions. We have used a forgotten theorem of 1917, by Pell and Gordon, and `sylvester2`, a rarely used form of Sylvester's matrix to compute a "new" subresultant polynomial remainder sequence of the polynomials $p(x)$ and $q(x)$ — differing from the "old" one just in the signs of the polynomials.

In the case of complete polynomial remainder sequences, and provided $q(x) = p'(x)$, this "new" subresultant prs is identical to the Sturm sequence of $p(x)$, just as the "old" subresultant prs — based on `sylvester1`, the widely used form of Sylvester's matrix — is identical to the Euclidean prs.

REFERENCES

[1] Akritas A. G. A Simple Proof of the Validity of the Reduced PRS Algorithm. *Computing*, **38** (1987), 369–372.

[2] Akritas A. G. A New Method for Computing Polynomial Greatest Common Divisors and Polynomial Remainder Sequences. *Numerische Mathematik*, **52** (1988), 119–127.

[3] Akritas A. G. Exact algorithms for the matrix-triangularization subresultant prs method. In: Proceedings of the Conference on Computers and Mathematics (Eds E. Kaltofen and S. M. Watt), Boston, Massachusetts, June, 1989, 145–155.

[4] Akritas A. G. Elements of Computer Algebra with Applications. John Wiley Interscience, New York, 1989.

[5] Akritas A. G. Sylvester's Forgotten Form of the Resultant. *Fibonacci Quarterly*, **31** (1993), 325–332.

[6] Akritas A. G., G. I. Malaschonok, P. S. Vigklas. On a Theorem by Van Vleck Regarding Sturm Sequences. *Serdica Journal of Computing*, **7** (2013), No. 4, 389–422.

[7] Brown W. S. The Subresultant PRS Algorithm. *ACM Transactions on Mathematical Software*, **4** (1978), No. 3, 237–249.

[8] Brown W. S., J. F. Traub. On Euclid's Algorithm and the Theory of Subresultants. *Journal of the Association for Computing Machinery*, **18** (1971), 505–514.

[9] Chen R. The Subresultant Polynomial Remainder Sequence Algorithm, March 23, 2013. www.math.ubc.ca/~reichst/423-project-subresultant.pdf

[10] Collins G. E. Polynomial Remainder Sequences and Determinants. *American Mathematical Monthly*, **73** (1966), No. 7, 708–712.

[11] Collins G. E. Subresultants and Reduced Polynomial Remainder Sequences. *Journal of the Association for Computing Machinery*, **14** (1967), 128–142.

[12] Habicht W. Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens. *Commentarii Mathematici Helvetici*, **21** (1948), 99–116.

[13] Pell A. J., R. L. Gordon. The Modified Remainders Obtained in Finding the Highest Common Factor of Two Polynomials. *Annals of Mathematics*, Second Series, **18** (1917), No. 4, 188–193.

[14] Sylvester J. J. A method of determining by mere inspection the derivatives from two equations of any degree. *Philosophical Magazine*, **16** (1840), 132–135.

[15] Sylvester J. J. On the Theory of Syzygetic Relations of Two Rational Integral Functions, Comprising an Application to the Theory of Sturm's Functions, and that of the Greatest Algebraical Common Measure. *Philosophical Transactions*, **143** (1853), 407–548.

[16] Van Vleck E. B. On the Determination of a Series of Sturm's Functions by the Calculation of a Single Determinant. *Annals of Mathematics*, Second Series, **1** (1899–1900), No. 1/4, 1–13.

Alkiviadis G. Akritas
Panagiotis S. Vigklas
Department of Electrical
and Computer Engineering
University of Thessaly
GR-38221, Volos, Greece
e-mail: akritas@uth.gr
pvigklas@uth.gr

Gennadi I. Malaschonok
Laboratory for Algebraic Computations
Tambov State University
Internatsionalnaya, 33
RU-392000 Tambov, Russia
e-mail: malaschonok@gmail.com

Received April 30, 2014
Final Accepted July 11, 2014