Serdica J. Computing **9** (2015), No. 2, 123–138

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON THE REMAINDERS OBTAINED IN FINDING THE GREATEST COMMON DIVISOR OF TWO POLYNOMIALS

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

Abstract. In 1917 Pell[1] and Gordon used `sylvester2`, Sylvester's little known and hardly ever used matrix of 1853, to compute[2] the coefficients of a Sturmian remainder — obtained in applying in $\mathbb{Q}[x]$, Sturm's algorithm on two polynomials $f, g \in \mathbb{Z}[x]$ of degree n — in terms of the determinants[3] of the corresponding submatrices of `sylvester2`. Thus, they solved a problem that had eluded both J. J. Sylvester, in 1853, and E. B. Van Vleck, in 1900.[4]

In this paper we extend the work by Pell and Gordon and show how to compute[2] the coefficients of an Euclidean remainder — obtained in finding in $\mathbb{Q}[x]$, the greatest common divisor of $f, g \in \mathbb{Z}[x]$ of degree n — in terms of the determinants[5] of the corresponding submatrices of `sylvester1`, Sylvester's widely known and used matrix of 1840.

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

Key words: Polynomial Remainder Sequence (PRS), Sylvester's matrices, Euclidean PRS, Subresultant PRS, Sturm sequence, Modified Subresultant PRS.

*Partially supported by the Russian Foundation for Basic Research, grant No. 16-07-00420a.

[1]See the link `http://en.wikipedia.org/wiki/Anna_Johnson_Pell_Wheeler` for her biography.

[2]Both for *complete* and *incomplete* sequences, as defined in the sequel.

[3]Also known as *modified* subresultants.

[4]Using determinants Sylvester and Van Vleck were able to compute the coefficients of Sturmian remainders *only* for the case of *complete* sequences.

[5]Also known as (proper) subresultants.

1. Introduction. We begin by first describing Sylvester's two matrices. We believe both are important and deserve to be treated on their own. For that, consider the polynomials $f, g \in \mathbb{Z}[x]$ of degrees n, m, respectively, with $n > m$.

Sylvester's matrix `sylvester1` was discovered in 1840 [8] and its dimensions are $(n+m) \times (n+m)$; it consists of two groups of rows, the first one with m rows and the second one with n. Concatenation of the two groups yields the matrix `sylvester1`.

In the first row of the first group (of m rows) are the coefficients of $f(x)$ with $m-1$ trailing zeros. The second row in this group differs from the first one in that its elements have been rotated to the right by one. A total of $m-1$ rotations are needed to construct the first group of rows.

In the first row of the second group (of n rows) are the coefficients of $g(x)$ with $n-1$ trailing zeros. The second row in this group differs from the first one in that its elements have been rotated to the right by one. A total of $n-1$ rotations are needed to construct the second group of rows.

Sylvester's matrix `sylvester2` was discovered in 1853, its dimensions are $2n \times 2n$ and it consists of n pairs of rows [9]. In the first row of the first pair are the coefficients of $f(x)$ whereas in the second row of the first pair are the coefficients of $g(x)$; $n-m$ zeros have been prepended to $g(x)$ to also make it of degree n. Both rows in the first pair have $2n-(n+1)$ trailing zeros and both rows of the last pair have $2n-(n+1)$ leading zeros. The second pair of rows differs from the first one in that the elements of both rows have been rotated to the right by one. A total of $2n-(n+1)$ rotations are needed to construct `sylvester2`.

In the freely available computer algebra system `Xcas/Giac` Sylvester's matrix `sylvester1` is given by the built-in function `sylvester`, whereas Sylvester's matrix `sylvester2` is given by our own function `sylvester2`. In the (also freely available) computer algebra system `Sympy` we have written the function `sylvester`[6] which returns either matrix depending on the last optional argument; by default matrix `sylvester1` is returned.

Example 1. Take $f(x) = ax^3 + bx^2 + cx + d$ with $a > 0$ and $g(x) = 3ax^2 + 2bx + c$. Then, $S_1(f, g)$, their `sylvester1` matrix, is

[6] All `Sympy` functions mentioned in this paper can be downloaded from the link `http://inf-server.inf.uth.gr/~akritas/publications/subresultants.py`.

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

whereas $S_2(f,g)$, their `sylvester2` matrix, is

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

For the sequences of polynomial remainders examined in this paper the following definitions are needed:

Definition 1. *The* ***sign sequence*** *of a polynomial remainder sequence (prs) is the sequence of signs of the leading coefficients of its polynomials.*

Definition 2. *A polynomial remainder sequence (prs) is called* ***complete*** *if the degree difference between any two consecutive polynomials is* 1*; otherwise, it called* ***incomplete****.*

Given $f(x), g(x) \in \mathbb{Z}[x]$ of degrees $deg(f) = n$ and $deg(g) = m$ with $n \geq m$ their (proper) *subresultant* prs is a sequence of polynomials similar to the *Euclidean* prs, the sequence obtained by applying in $\mathbb{Q}[x]$[7] Euclid's polynomial gcd algorithm on $f(x), g(x)$.[8] The two sequences differ in that the coefficients of each polynomial in the subresultant prs are the determinants, or *subresultants*, of specially chosen sub-matrices of `sylvester1` [4]. For *complete* prs's the two sign sequences are identical and the coefficients of the Euclidean prs are easily computed with the help of the corresponding subresultants [1].

The determinant of `sylvester1` itself is called the *resultant* of $f(x), g(x)$ and serves as a criterion of whether the two polynomials have common roots or not.

[7] Or in $\mathbb{Z}[x]$, if we use our `Sympy` function `euclid_PG(p, q, x, method = 0)`; see also footnote 6.

[8] A formal definition of a subresultant prs can be found in almost all references (see for example the one by Kerber, [6]) and hence it is omitted in this paper.

For the same polynomials $f(x), g(x) \in \mathbb{Z}[x]$ mentioned above, their *modified subresultant* prs [4] is a sequence of polynomials similar to the *Sturmian* prs, the sequence obtained by applying in $\mathbb{Q}[x]$[9] Sturm's algorithm on $f(x), g(x)$. The two sequences differ in that the coefficients of each polynomial in the modified subresultant prs are the determinants, or *modified subresultants*, of specially chosen sub-matrices of `sylvester2` [4]. For *complete* prs's the two sign sequences are identical and the coefficients of the Sturmian prs are easily computed with the help of the corresponding modified subresultants [1].

The determinant of `sylvester2` itself is called the *modified resultant* of $f(x), g(x)$ and it also can serve as a criterion of whether the two polynomials have common roots or not.

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.

The determinants of the two matrices `sylvester1` and `sylvester2` — as well as the corresponding subresultants and modified subresulrtants — generally differ in sign.[10] Indeed, for the polynomials of Example 1 the determinant of $S_1(f,g)$ is

$$27 \cdot a^3 \cdot d^2 - 18 \cdot a^2 \cdot b \cdot c \cdot d + 4 \cdot a^2 \cdot c^3 + 4 \cdot a \cdot b^3 \cdot d - a \cdot b^2 \cdot c^2,$$

whereas the determinant of $S_2(f,g)$ is

$$\frac{\det(S_2(f,g))}{a} = -\det(S_1(f,g)).$$

1.1. Incomplete prs's. If an *incomplete* prs is obtained from $f(x)$, $g(x) \in \mathbb{Z}[x]$, then the following problems are encountered:

(i) the polynomials in the subresultant prs generally differ in *sign* from those of the Euclidean prs, and — unlike the case of complete prs's — it is not at all obvious how to compute the coefficients of the polynomials in the latter sequence with the help of the corresponding subresultants;

(ii) the polynomials in the modified subresultant prs generally differ in *sign* from those of the Sturmian prs, and — unlike the case of complete prs's — it is

[9] Or in $\mathbb{Z}[x]$, if we use our `Sympy` function `sturm_PG(p, q, x)`; see also footnote 6.

[10] That is, the absolute value of any modified subresultant (obtained from `sylvester2`) divided by the (positive) leading coefficient of f raised to the power $n-m$ is equal to the absolute value of the corresponding subresultant (obtained from `sylvester1`).

not at all obvious how to compute the coefficients of the polynomials in the latter sequence with the help of the corresponding modified subresultants.

These problems are best illustrated with the following example:

Example 2. Consider the storied polynomials $f = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$ and $g = 3x^6 + 5x^4 - 4x^2 - 9x + 21$ whose incomplete prs has degrees $8, 6, 4, 2, 1, 0$. These polynomials — and the computer algebra system `Sympy` — will be used throughout this paper.

(i) Using the built-in function `subresultants` we obtain the polynomial remainder sequence (1) in $\mathbb{Z}[x]$, which is the (proper) subresultant prs,

$$\begin{aligned}(1)\quad & x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21,\\ & \qquad 15x^4 - 3x^2 + 9, 65x^2 + 125x - 245, 9326x - 12300, 260708.\end{aligned}$$

The coefficients of the polynomials in the second row of (1) are all determinants of submatrices of `sylvester1`.

On the other hand, using the built-in function `rem`, we obtain the polynomial remainder sequence (2) in $\mathbb{Q}[x]$, which is the Euclidean prs,

$$\begin{aligned}(2)\quad & x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21,\\ & \qquad -5x^4/9 + x^2/9 - 1/3, -117x^2/25 - 9x + 441/25,\\ & \qquad 233150x/19773 - 102500/6591, -1288744821/543589225.\end{aligned}$$

How can we compute the coefficients of the polynomials in the Euclidean prs (2) from the corresponding subresultants of the subresultant prs (1) and vice-versa?

(ii) Using our own function `modified_subresultants_PG` we obtain the polynomial remainder sequence (3) in $\mathbb{Z}[x]$, which is the modified subresultant prs,

$$\begin{aligned}(3)\quad & x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21,\\ & \qquad -15x^4 + 3x^2 - 9, 65x^2 + 125x - 245, -9326x + 12300, 260708.\end{aligned}$$

The coefficients of the polynomials in the second row of (3) are all determinants of submatrices of `sylvester2`.

On the other hand, using `-rem`, we obtain the polynomial remainder sequence (4) in $\mathbb{Q}[x]$, which is the Sturmian prs,

$$(4)\quad x^8+x^6-3x^4-3x^3+8x^2+2x-5, 3x^6+5x^4-4x^2-9x+21, \\ 5x^4/9-x^2/9+1/3, 117x^2/25+9x-441/25, \\ 233150x/19773-102500/6591, -1288744821/543589225.$$

How can we compute the coefficients of the polynomials in the Sturmian prs (4) from the corresponding modified subresultants of the modified subresultant prs (3) and vice-versa?

These problems were extremely difficult to tackle and eluded both Sylvester (1853) and Van Vleck (1900) [11]. As Sylvester put it ([9], p. 419) "... the same explicit method might be applied to show, that if the first divisor were e degrees instead of being only one degree lower than the first divident, α^{e+1} would be contained in every term of the second residue;[11] the difficulty, however, of the proof by this method augments with the value of e" [1]. For his part, Van Vleck considered *only* complete Sturm sequences, and stated ([11], p. 4) "... the degree of each succeeding polynomial, respectively remainder is, *in general*,[12] one less than that of the preceding."

It was in 1917 that Pell and Gordon [7] "modified" Van Vleck's theorem and, hence, solved the problem of computing the coefficients of a Sturmian remainder via modified subresultants. Their paper went unnoticed for about 100 years, until one of us (P. S. Vigklas) discovered it in the journal archives.

1.2. Outline of the Paper. In this paper we present a solution to the problem of computing the coefficients of an Euclidean remainder via subresultants. A graphical representation of our solution is given in Figure 1 — follow the double arrows.

In Section 2 we present the relationship that exists between Sturmian remainders and modified subresultant prs's — branch $\mathcal{PG}$ in Figure 1. This relationship is described in the remarkable theorem by Pell and Gordon, which is stated here for completion along with an example on how to compute the coefficients of the polynomials in the Sturmian prs from the corresponding modified subresultants of the modified subresultant prs.

In Section 3 we present the relationship that exists between Euclidean remainders and subresultant prs's — branches $\mathcal{AMV}$, $\mathcal{PG}$ and $\mathcal{SAM}$ in Figure

[11] α is the leading coefficient of the divisor.
[12] Our emphasis.

$$
\begin{tikzcd}
\textit{Euclidean PRS} \arrow[r, Leftrightarrow, "\mathcal{SAM}"'] \arrow[d, dash, dashed] & \textit{Sturmian PRS} \arrow[d, Leftrightarrow, "\mathcal{PG}"] \\
(\textit{proper})\ \textit{Subresultant PRS} \arrow[r, Leftrightarrow, "\mathcal{AMV}"'] & \textit{modified Subresultant PRS} \\
\textit{sylvester}1\ (1840) \arrow[u, Rightarrow] & \textit{sylvester}2\ (1853) \arrow[u, Rightarrow]
\end{tikzcd}
$$

Fig. 1. The indirect way of computing the (Euclidean) remainders — obtained in finding the greatest common divisor of two polynomials in $\mathbb{Q}[x]$ — from the (proper) subresultant prs. The latter is computed from `sylvester1`, Sylvester's matrix of 1840

1. Our main result, Theorem 4 is preceded by two auxiliary theorems: the first one establishes a relation between the signs of a subresultant prs and those of the corresponding modified subresultant prs — relation $\mathcal{AMV}$ in Figure 1 — whereas the second theorem establishes a relation between the signs of a Euclidean prs and those of the corresponding Sturmian prs — relation $\mathcal{SAM}$ in Figure 1.

Finally, in Section 4 we present our conclusions.

2. Sturmian remainders and their relationship to modified subresultant prs's. The Pell-Gordon Theorem of 1917, [7], helps us compute the coefficients of a Sturmian remainder, of a complete or incomplete sequence, with the help of modified subresultants,[13] i. e. determinants of submatrices of Sylvester's matrix `sylvester2`. The theorem is stated below but additional details can be found elsewhere [2], [3], [4].

Theorem 1 (Pell-Gordon, 1917)**.** *Let*

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

and

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

[13]That is, *without* polynomial divisions.

be two polynomials of the nth degree. Modify the process of finding the highest common factor of f and g by taking at each stage the negative of the remainder. Let the ith 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*[14]

$$(5) \qquad r_k^{(i)} = \frac{(-1)^{u_{i-1}} (-1)^{u_{i-2}} \cdots (-1)^{u_1} (-1)^{v_{i-1}}}{\varrho_{i-1}^{p_{i-1}+1} \varrho_{i-2}^{p_{i-2}+p_{i-1}} \cdots \varrho_1^{p_1+p_2} \varrho_0^{p_1}} \cdot \mathrm{Det}\,(i,k)\,,$$

where

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

and

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

Proof. See [7]. □

As indicated elsewhere [4], we use a modification of formula (5) to compute the coefficients of a polynomial in the Sturm sequence of two polynomials. In our general case $p_0 = \deg(f) - \deg(g) \geq 0$, since $deg(g) \leq deg(f)$ and, hence, the modified formula is shown below with the changes appearing in bold:

$$(6) \qquad r_k^{(i)} = \frac{(-1)^{u_{i-1}} (-1)^{u_{i-2}} \cdots (-1)^{u_1} \boldsymbol{(-1)^{u_0}} (-1)^{v_{i-1}}}{\varrho_{i-1}^{\mathrm{p}_{i-1} + \boldsymbol{p_i - \mathrm{degDiffer}}} \varrho_{i-2}^{p_{i-2}+p_{i-1}} \cdots \varrho_1^{p_1+p_2} \varrho_0^{\boldsymbol{p_0} + p_1}} \cdot \frac{\mathrm{Det}\,(i,k)}{\boldsymbol{\varrho_{-1}^{p_0}}},$$

where $\varrho_{-1} = a_0$, the leading coefficient of f and `degDiffer` is the difference between the expected degree m_i and the actual degree of the remainder. Also, note that $p_i - \mathrm{degDiffer} = 1$ for all i.

[14] It is understood in (5) that $\varrho_0 = b_0$, $p_0 = 0$, and that $a_i = b_i = 0$ for $i > n$.

It should be noted that in our (general) case the division $\dfrac{\mathrm{Det}\,(i,k)}{\varrho_{-1}^{p_0}}$ is exact. Moreover, if the leading coefficient of f is negative we work with the polynomial negated and at the end we reverse the signs of all polys in the sequence.

Note that the first fraction in formula (6) depends only on i and is independent of k. Denote by $PG^{(i)}$ that fraction and call it the $PG^{(i)}$*-factor*; that is, we have

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

in which case, the coefficients of the Sturmian remainders are exactly

$$r_k^{(i)} = PG^{(i)} \times \frac{\mathrm{Det}\,(i,k)}{\boldsymbol{\varrho_{-1}^{p_0}}}. \tag{8}$$

Example 3. Consider again the polynomials $f = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$ and $g = 3x^6 + 5x^4 - 4x^2 - 9x + 21$, seen in Example 2. The modified subresultant prs of f, g is

$$\begin{aligned} &x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21,\\ &\qquad - 15x^4 + 3x^2 - 9, 65x^2 + 125x - 245, -9326x + 12300, 260708, \end{aligned} \tag{9}$$

where the coefficients of the last 4 polynomials in the second line of (9) are all determinants (the modified subresultants $\mathrm{Det}\,(i,k)$) of appropriate submatrices of `sylvester2`.

To compute the coefficients of the Sturmian polynomials we have to compute the $PG^{(i)}$*-factor*, $i = 1, 2, 3, 4$, for each remainder. Using (7) we find

$$PG^{(i)} = \Big\{ -\frac{1}{27}, \frac{9}{125}, -\frac{25}{19773}, -\frac{19773}{2174356900} \Big\}, \quad i = 1, 2, 3, 4, \tag{10}$$

and from (8), we obtain the Sturm sequence of f, g in $\mathbb{Q}\,[x]$,

$$\begin{aligned} &x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21,\\ &\qquad 5x^4/9 - x^2/9 + 1/3, 117x^2/25 + 9x - 441/25,\\ &\qquad\quad 233150x/19773 - 102500/6591, -1288744821/543589225. \end{aligned} \tag{11}$$

Note that the Sturmian prs (4), which was computed with polynomial divisions, is identical to the Sturmian prs (11), which was computed via modified subresultants — since, for example, the coefficient $\frac{5}{9}$ in (11) is the product $(-\frac{1}{27}) \times (-15)$, etc.

Using (6) we have developed our own function `sturm_PG`[6], which computes the Sturmian prs of f, g in $\mathbb{Z}[x]$:

$$x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21,$$
$$15x^4 - 3x^2 + 9, 65x^2 + 125x - 245, 9326x - 12300, -260708. \tag{12}$$

Note that the sign sequences in (11) and (12) are identical.

3. Euclidean remainders and their relationship to subresultant prs's. In this section we prove that once a subresultant prs has been computed then the polynomial remainders in the Euclidean prs are *uniquely* determined in sign and magnitude. The converse is also true.

As indicated in Figure 1, the proof of our result is indirect and uses the Pell-Gordon theorem (Theorem 1). Additionally, we need the following two auxiliary theorems.

Theorem 2. *Let $f, g \in \mathbb{Z}[x]$ of degrees $n = \deg(f) \geq deg(g) = m$ and let f_0 be the leading coefficient of f. Consider the ith* ***modified*** *subresultant polynomial*[15]

$$\mathcal{S}_2^{(i)} = s_0^{(i)} x^{m_i} + s_1^{(i)} x^{m_i - 1} + \cdots + s_{m_i}^{(i)},$$

where (m_i+1) is the degree of the preceding polynomial, and where the first (p_i-1) coefficients of $\mathcal{S}_2^{(i)}$ are zero, and the p_ith coefficient $\varrho_i = r_{p_i-1}^{(i)}$ is different from zero. If

$$\tilde{\mathcal{S}}_1^{(i)} = \tilde{s}_0^{(i)} x^{m_i} + \tilde{s}_1^{(i)} x^{m_i - 1} + \cdots + \tilde{s}_{m_i}^{(i)},$$

is the corresponding ***(proper)*** *subresultant polynomial*[16] *and $j_i = n - m_i$, then*

$$f_0^{n-m} \tilde{\mathcal{S}}_1^{(i)} = (-1)^{\frac{j_i(j_i-1)}{2}} \mathcal{S}_2^{(i)}. \tag{13}$$

[15] That is, its coefficients are determinants (*modified* subresultants) of submatrices obtained from `sylvester2`.

[16] That is, its coefficients are determinants (proper subresultants) of submatrices obtained from `sylvester1`.

Proof. An analogous result has been proven in [5] (Theorem 2.1) regarding $\tilde{\mathcal{S}}_1^{(i)}$ and the subresultant polynomial obtained from Bezout's matrix. Our theorem follows immediately from the equivalence of Bezout's matrix to Sylvester's matrix `sylvester2`. $\square$

The factor $(-1)^{\frac{j_i(j_i-1)}{2}}$ in (13) helps us get the signs right along the $\mathcal{AMV}$ branch of Figure 1 and, hence, we call it the *$AMV^{(i)}$-factor*.

Example 4. Consider again the polynomials $f = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$ and $g = 3x^6 + 5x^4 - 4x^2 - 9x + 21$, seen in Examples 2 and 3. Note that $f_0 = 1$. To compute the *$AMV^{(i)}$-factors* we first compute the values of the $j_i, i = 1, 2, 3, 4$, for each remainder. In our example we have

$$j_1 = n - m_1 = 8 - 5 = 3,$$

$$j_2 = n - m_2 = 8 - 3 = 5,$$

$$j_3 = n - m_3 = 8 - 1 = 7,$$

$$j_4 = n - m_4 = 8 - 0 = 8.$$

Therefore, the *$AMV^{(i)}$-factors* are $(-1)^{\frac{j_i(j_i-1)}{2}}$, for $i = 1, 2, 3, 4$ or

$$AMV^{(i)} = \{-, +, -, +\}, \quad i = 1, 2, 3, 4. \tag{14}$$

Indeed, looking at the second row of (1) and (3), we see that the first and third polynomial remainders differ in sign.

The second auxiliary theorem is an almost unknown statement with serious ramifications as we shall see. It was proven by Akritas and Malaschonok in April, 2015, during the conference on Polynomial Computer Algebra (PCA-2015) in St. Petersburg, Russia, but both felt sure that it must have been noticed earlier. Indeed, Vigklas found out that Sylvester mentioned this as a "Remark" in ([10], p. 453).[17]

Theorem 3. *Let $f, g \in \mathbb{Z}[x]$ of degrees $n = \deg(f) \geq deg(g) = m$. Modify the process of finding the greatest common divisor of f and g by taking*

[17] We quote Sylvester: "The law evidently being that the quotients change sign alternately, i. e. in the 2nd, 4th, 6th, etc places, and remain unaltered in the 1st, 3rd, 5th, etc places; whereas the residues or excesses change their signs in the 1st and 2nd, 5th and 6th, 9th and 10th, etc and remain unaltered in the 3rd and 4th, 7th and 8th, 11th and 12th etc places."

at each stage the negative of the remainder and let the ith Sturmian remainder be $R^{(i)}$. *If* $\tilde{R}^{(i)}$ *is the corresponding Euclidean remainder obtained in finding the greatest common divisor of* f *and* g, *then it holds*

$$R^{(i)} = (-1)^{\lfloor \frac{i-1}{2} \rfloor + 1} \, \tilde{R}^{(i)}. \tag{15}$$

Proof. The proof of this theorem is quite easy and is left as an exercise for the reader. *Hint*: Use the fact that for the respective quotients we have $q^{(i)} = (-1)^{i+1} \tilde{q}^{(i)}$. □

Theorem 3 tell us that once a Sturmian prs has been determined then the signs (and values) of the corresponding Euclidean prs are *uniquely* defined. The factor $(-1)^{\lfloor \frac{i-1}{2} \rfloor + 1}$ helps us get the signs right along the $\mathcal{SAM}$ branch of Figure 1 and, hence, we call it the $SAM^{(i)}$*-factor*.

Example 5. Consider again the polynomials $f = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$ and $g = 3x^6 + 5x^4 - 4x^2 - 9x + 21$, seen in Examples 2, 3 and 4. The $SAM^{(i)}$*-factor*, $i = 1, 2, 3, 4$, for each remainder is $(-1)^{\lfloor \frac{i-1}{2} \rfloor + 1}$, or

$$SAM^{(i)} = \{-, -, +, +\}, \quad i = 1, 2, 3, 4. \tag{16}$$

Indeed, comparing the polynomials in the second row of (2) and (4), we see that they differ in sign, whereas those in the third row of (2) and (4) are identical.

Our main result follows:

Theorem 4. *Let*

$$f = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

and

$$g = b_0 x^n + b_1 x^{n-1} + \cdots + b_n$$

be two polynomials of degree n. Modify the process of finding the greatest common divisor of f and g by taking at each stage the negative of the remainder.[18] *Let the ith Sturmian remainder be*

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

[18] That is, apply Sturm's algorithm on f, g.

where (m_i+1) *is the degree of the preceding remainder, and where the first* (p_i-1) *coefficients of* $R^{(i)}$ *are zero, and the* p_i*th coefficient* $\varrho_i = r^{(i)}_{p_i-1}$ *is different from zero. Then for* $k = 0, 1, \dots, m_i$ *the coefficients* $\tilde{r}^{(i)}_k$ *of the Euclidean remainder*[19]

$$\tilde{R}^{(i)} = \tilde{r}^{(i)}_0 x^{m_i} + \tilde{r}^{(i)}_1 x^{m_i-1} + \cdots + \tilde{r}^{(i)}_{m_i},$$

obtained in finding the greatest common divisor of f *and* g*, are given by*[20]

$$\tilde{r}^{(i)}_k = (-1)^{\lfloor \frac{i-1}{2} \rfloor + 1} \cdot \frac{(-1)^{u_{i-1}}\,(-1)^{u_{i-2}} \cdots (-1)^{u_1}\,(-1)^{v_{i-1}}}{\varrho^{p_{i-1}+1}_{i-1}\,\varrho^{p_{i-2}+p_{i-1}}_{i-2} \cdots \varrho^{p_1+p_2}_1\,\varrho^{p_1}_0} \cdot (-1)^{\frac{j_i(j_i-1)}{2}} \cdot \mathrm{Det}\,(i,k)\,, \tag{17}$$

where

$$u_{i-1} = 1 + 2 + \cdots + p_{i-1}, \quad v_{i-1} = p_1 + p_2 + \cdots + p_{i-1}, \quad j_i = n - m_i,$$

and

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

P r o o f. The proof follows from the previous three theorems. □

As in Section 2, we use a modification of formula (17) to compute the coefficients of an Euclidean sequence. In that case $p_0 = \deg(f) - \deg(g) \geq 0$, since $deg(g) \leq deg(f)$ and, provided the dimensions of `sylvester1` are $2 \cdot deg(f) \times 2 \cdot deg(f)$, the modified formula is shown below with the changes appearing in

[19] That is, $\tilde{R}^{(i)}$ is a member of the Euclidean sequence obtained in finding the greatest common divisor of f, g.

[20] It is understood in (17) that $\varrho_0 = b_0$, $p_0 = 0$, and that $a_i = b_i = 0$ for $i > n$.

bold:[21]

$$\tilde{r}_k^{(i)} = (-1)^{\lfloor \frac{i-1}{2} \rfloor + 1} \cdot \frac{(-1)^{u_{i-1}} (-1)^{u_{i-2}} \cdots (-1)^{u_1} \boldsymbol{(-1)^{u_0}} (-1)^{v_{i-1}}}{\varrho_{i-1}^{\mathrm{p}_{i-1} + \boldsymbol{p_i} - \mathbf{degDiffer}} \varrho_{i-2}^{p_{i-2}+p_{i-1}} \cdots \varrho_1^{p_1+p_2} \varrho_0^{\boldsymbol{p_0}+p_1}} \times (-1)^{\frac{j_i(j_i-1)}{2}} \cdot \frac{\mathrm{Det}\,(i,k)}{\boldsymbol{\varrho_{-1}^{p_0}}}, \tag{18}$$

where $\varrho_{-1} = a_0$, `degDiffer` is the difference between the expected degree m_i and the actual degree of the remainder and Det (i,k) is an appropriate submatrix of `sylvester1`. Also, note that $p_i - \text{degDiffer} = 1$ for all i.

If the leading coefficient of f is negative we work with the polynomial negated and at the end we reverse the signs of all polynomials in the sequence.

Example 6. Consider again the polynomials $f = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$ and $g = 3x^6 + 5x^4 - 4x^2 - 9x + 21$, seen in Examples 2, 3, 4 and 5. To compute the Euclidean prs (2) of f, g from the subresultant prs (1) of f, g, we do the following:

- Using the *$AMV^{(i)}$-factors* (14) we convert the subresultant prs (1) to the modified subresultant prs (3) of f, g.
- Subsequently, using (8), the *$PG^{(i)}$-factors* (10) and the determinants obtained from the modified subresultant prs (3) we compute the Sturmian prs (4) of f, g.
- Finally, using the *$SAM^{(i)}$-factors* (16) we convert the Sturmian prs (4) to the Euclidean prs (2) of f, g.

We slightly modified the function `sturm_PG` and developed our own function `euclid_PG`[6], which computes the Euclidean prs of f, g in $\mathbb{Z}[\mathrm{x}]$,

$$\begin{aligned} & x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5, 3x^6 + 5x^4 - 4x^2 - 9x + 21, \\ & \qquad - 15x^4 + 3x^2 - 9, -65x^2 - 125x + 245, 9326x - 12300, -260708. \end{aligned} \tag{19}$$

Note that the sign sequences in (2) and (19) are identical.

4. Conclusions.

Consider the polynomials $f, g \in \mathbb{Z}[\mathrm{x}]$. Our main result, Theorem 4, relates the Euclidean prs, obtained in finding in $\mathbb{Q}[\mathrm{x}]$ the

[21] If the dimensions of `sylvester1` are $(deg(f) + deg(g)) \times (deg(f) + deg(g))$, then the denominator $\varrho_{-1}^{p_0}$ is omitted in (18).

greatest common divisor of f, g, with the subresultant prs of f, g, as shown in Figure 1.

Together, the four theorems in our paper imply that the polynomial remainder sequence $R^{(i)}$, obtained in $\mathbb{Q}[\mathtt{x}]$ by applying Sturm's algorithm on f, g and the polynomial remainder sequence $\tilde{R}^{(i)}$, obtained in $\mathbb{Q}[\mathtt{x}]$ by applying Euclid's algorithm on f, g, are *both uniquely* defined — through equations (6), (13), (15) and (18) — either by the modified subresultant prs or by the subresultant prs; and vice-versa.

Once the polynomial remainder sequences $R^{(i)}$ and $\tilde{R}^{(i)}$ have been uniquely defined in $\mathbb{Q}[\mathtt{x}]$ then — as shown elsewhere [4] — using the same equations (6) and (18), they can be *uniquely* defined in $\mathbb{Z}[\mathtt{x}]$ as well. The signs of the coefficients in both sequences in $\mathbb{Z}[\mathtt{x}]$ are the same as those of the corresponding coefficients in $\mathbb{Q}[\mathtt{x}]$.[22]

Note added in proof. A new version of sympy (1.0) came out in March 2016. In this new version the module sumpy.polys.subresultants_qq_zz.py contains the functions referred to in this paper.

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. Three New Methods for Computing Subresultant Polynomial Remainder Sequences (PRS's). *Serdica Journal of Computing*, **9** (2015), No 1, 1–26.

[3] 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, 101–134.

[4] Akritas A. G., G. I. Malaschonok, P. S. Vigklas. Sturm Sequences and Modified Subresultant Polynomial Remainder Sequences. *Serdica Journal of Computing*, **8** (2014), No 1, 29–46.

[22] In this respect, note the caveat in `http://planetmath.org/sturmstheorem`: "Be aware that some computer algebra systems may normalize remainders from the Euclidean Algorithm which messes up the sign."

[5] Diaz–Toca G. M., L. Gonzalez–Vega. Various New Expressions for Subresultants and Their Applications. *Applicable Algebra in Engineering, Communication and Computing*, **15** (2004), 233–266.

[6] Kerber M. Division-Free computation of subresultants using Bezout matrices. Tech. Report MPI-I-2006-1-006, Saarbrucken, 2006.

[7] 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** (June, 1917), No 4, 188–193.

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

[9] 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.

[10] Sylvester J. J. On a remarkable modification of Sturm's theorem. *Philosophical Magazine and Journal of Science*, **V**, Fourth Series, (January–June, 1853), 446–456. `http://books.google.gr/books?hl=el&id=3Ov22-gFMnEC&q=sylvester#v=onepage&q&f=false`

[11] 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
Department of Electrical
and Computer Engineering
University of Thessaly
GR-38221, Volos, Greece
e-mail: `akritas@uth.gr`

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

Panagiotis S. Vigklas
Department of Electrical
and Computer Engineering
University of Thessaly
GR-38221, Volos, Greece
e-mail: `pviglas@uth.gr`

Received May 18, 2015
Final Accepted November 27, 2015