A new general formula for the Cauchy Index on an interval with Subresultants

Daniel Perrucci[♭∗]   Marie-Françoise Roy[♯]

♭ Departamento de Matemática, FCEN, Universidad de Buenos Aires and IMAS UBA-CONICET,
Ciudad Universitaria, 1428 Buenos Aires, Argentina
♯ IRMAR (UMR CNRS 6625), Université de Rennes 1,
Campus de Beaulieu, 35042 Rennes Cedex, France

Abstract

We present a new formula for the Cauchy index of a rational function on an interval using subresultant polynomials. There is no condition on the endpoints of the interval and the formula also involves in some cases less subresultant polynomials.

Keywords: Cauchy Index, Subresultant Polynomials.

AMS subject classifications: 14P99, 13P15, 12D10, 26C15

1 Introduction

Let $(\mathbf{R}, \leq)$ be a real closed field and $P, Q \in \mathbf{R}[X]$ with $P \neq 0$. Already considered by Sturm and Cauchy ([8, 4]), the Cauchy index of the rational function $\dfrac{Q}{P}$ is the integer number which counts its number of *jumps* from $-\infty$ to $+\infty$ minus its number of *jumps* from $+\infty$ to $-\infty$. This value plays an important role in many algorithms in real algebraic geometry ([2, 3, 6]). For instance, the Tarski query of Q for P, defined as

$$\mathrm{TaQ}(Q,P) = \#\Big\{x \in \mathbf{R} \mid P(x) = 0,\ Q(x) > 0\Big\} \ - \ \#\Big\{x \in \mathbf{R} \mid P(x) = 0,\ Q(x) < 0\Big\},$$

is equal to the Cauchy index of the rational function $\dfrac{P'Q}{P}$ (see, for instance, [3, Proposition 2.57]). Tarski queries are used to solve the *sign determination problem*, which consists in listing the signs of a list of polynomials in $\mathbf{R}[X]$ evaluated at the roots in $\mathbf{R}$ of another polynomial in $\mathbf{R}[X]$ (see [3,

[∗]Partially supported by the Argentinian grants UBACYT 20020160100039BA and PIP 11220130100527CO CONICET

Section 10.3]). In particular, the number of real roots of a polynomial $P \in \mathbf{R}[X] \setminus \{0\}$ coincides with the Tarski query $\mathrm{TaQ}(1, P)$ and is equal to the Cauchy index of the rational function $\frac{P'}{P}$. We can also mention the role of the Cauchy index for complex roots counting (see [4, 5, 7]). For more information and references to the history of the Cauchy index see [5].

1.1 Cauchy index

Let $P, Q \in \mathbf{R}[X]$ with $P \neq 0$. The usual definition of the Cauchy index of $\frac{Q}{P}$ is made directly on intervals whose endpoints are not roots of P. In this paper we use the extended definition of the Cauchy index introduced in [5, Section 3], which is made first locally at elements in $\mathbf{R}$, and then on intervals without restriction.

Definition 1 *Let $x \in \mathbf{R}$ and $P, Q \in \mathbf{R}[X], P \neq 0$.*

- *If $Q \neq 0$, the rational function $\frac{Q}{P}$ can be written uniquely as*

$$\frac{Q}{P} = (X - x)^m \frac{\widetilde{Q}}{\widetilde{P}}$$

with $m \in \mathbb{Z}$, $\widetilde{P}, \widetilde{Q} \in \mathbf{R}[X]$, $\widetilde{P}$ monic, $\widetilde{P}$ and $\widetilde{Q}$ coprime and $\widetilde{P}(x) \neq 0, \widetilde{Q}(x) \neq 0$. For $\varepsilon \in \{+, -\}$, define

$$\mathrm{Ind}_x^{\varepsilon}\Big(\frac{Q}{P}\Big) = \begin{cases} \frac{1}{2} \cdot \mathrm{sign}\Big(\frac{\widetilde{Q}(x)}{\widetilde{P}(x)}\Big) & \text{if } \varepsilon = + \text{ and } m < 0, \\ \frac{1}{2} \cdot (-1)^m \cdot \mathrm{sign}\Big(\frac{\widetilde{Q}(x)}{\widetilde{P}(x)}\Big) & \text{if } \varepsilon = - \text{ and } m < 0. \end{cases}$$

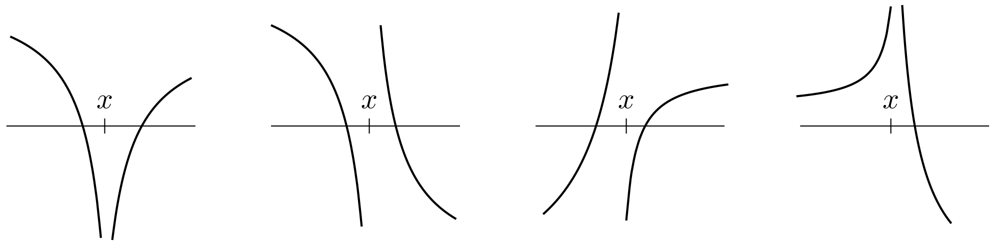
In all other cases, define

$$\mathrm{Ind}_x^{\varepsilon}\Big(\frac{Q}{P}\Big) = 0$$

- *The Cauchy index of $\frac{Q}{P}$ at x is*

$$\mathrm{Ind}_x\Big(\frac{Q}{P}\Big) = \mathrm{Ind}_x^{+}\Big(\frac{Q}{P}\Big) - \mathrm{Ind}_x^{-}\Big(\frac{Q}{P}\Big).$$

Said in other terms, when x is a pole of $\frac{Q}{P}$, we have that $\mathrm{Ind}_x^{+}\Big(\frac{Q}{P}\Big)$ is one half of the sign of $\frac{Q}{P}$ *to the right* of x, and $\mathrm{Ind}_x^{-}\Big(\frac{Q}{P}\Big)$ is one half of the sign of $\frac{Q}{P}$ *to the left* of x. Then, the Cauchy index of $\frac{Q}{P}$ at x, $\mathrm{Ind}_x\Big(\frac{Q}{P}\Big)$, is simply the difference between them. We illustrate this notion considering the graph of the function $\frac{Q}{P}$ around x in each different case.



$\mathrm{Ind}_x\Big(\dfrac{Q}{P}\Big) = 0$ $\qquad$ $\mathrm{Ind}_x\Big(\dfrac{Q}{P}\Big) = 1$ $\qquad$ $\mathrm{Ind}_x\Big(\dfrac{Q}{P}\Big) = -1$ $\qquad$ $\mathrm{Ind}_x\Big(\dfrac{Q}{P}\Big) = 0$

Definition 2 *Let $a, b \in \mathbf{R}$ with $a < b$ and $P, Q \in \mathbf{R}[X]$ with $P \neq 0$. If $Q \neq 0$, the Cauchy index of $\dfrac{Q}{P}$ on $[a, b]$ is*

$$\mathrm{Ind}_a^b\Big(\frac{Q}{P}\Big) = \mathrm{Ind}_a^+\Big(\frac{Q}{P}\Big) + \sum_{x \in (a,b)} \mathrm{Ind}_x\Big(\frac{Q}{P}\Big) - \mathrm{Ind}_b^-\Big(\frac{Q}{P}\Big),$$

where the sum is well-defined since only roots x of P in (a, b) contribute.

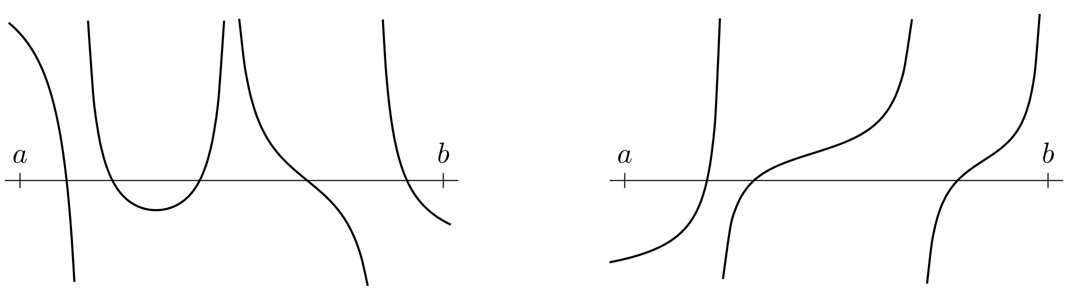
Similarly, if $Q \neq 0$, the Cauchy index of $\dfrac{Q}{P}$ on $\mathbf{R}$ is

$$\mathrm{Ind}_{\mathbf{R}}\Big(\frac{Q}{P}\Big) = \sum_{x \in \mathbf{R}} \mathrm{Ind}_x\Big(\frac{Q}{P}\Big)$$

where, again, the sum is well-defined since only roots x of P in $\mathbf{R}$ contribute.

If $Q = 0$, both the Cauchy index of $\dfrac{Q}{P}$ on $[a, b]$ and the Cauchy index of $\dfrac{Q}{P}$ on $\mathbf{R}$ are defined as 0.

In the following picture we consider again the graph of the function $\dfrac{Q}{P}$, this time in $[a, b]$.



$\mathrm{Ind}_a^b\Big(\dfrac{Q}{P}\Big) = 1 + 0 + 1 = 2$ $\qquad$ $\mathrm{Ind}_a^b\Big(\dfrac{Q}{P}\Big) = -1 - 1 - \dfrac{1}{2} = -\dfrac{5}{2}$

Note that with this extended definition of the Cauchy index, the Cauchy index of a rational function on an interval belongs to $\frac{1}{2}\mathbb{Z}$ and it is not necessarily an integer number.

1.2 Sturm sequences and Cauchy index

Definition 3 *Let $P, Q \in \mathbf{R}[X], P \neq 0$. Define $S_0 = P$ and, if $Q \neq 0$,*

$$\begin{aligned} S_1 &= Q, \\ S_2 &= -\mathrm{Rem}(S_0, S_1), \\ &\vdots \\ S_{i+1} &= -\mathrm{Rem}(S_{i-1}, S_i), \\ &\vdots \\ S_{s+1} &= -\mathrm{Rem}(S_{s-1}, S_s) = 0, \end{aligned}$$

with $S_1, S_2, \ldots, S_s \neq 0$, where Rem *is the remainder in the euclidean division in $\mathbf{R}[X]$ of the first polynomial by the second polynomial.*

The Sturm sequence of P and $Q \neq 0$ is $(S_0, \ldots, S_s)$ and the Sturm sequence of P and 0 is S_0, with $s = 0$. We denote by $(d_0, \ldots, d_s)$ the degrees of $(S_0, \ldots, S_s)$.

Example 4 *Let $\alpha, \beta \in \mathbf{R}$ and $P = X^5 + \alpha X + \beta \in \mathbf{R}[X]$. If $\alpha \neq 0$ and $256\alpha^5 + 3125\beta^4 \neq 0$, the Sturm sequence of P and P' is (S_0, S_1, S_2, S_3) with*

$$\begin{aligned} S_0 &= P = X^5 + \alpha X + \beta, \\ S_1 &= P' = 5X^4 + \alpha, \\ S_2 &= \tfrac{-4\alpha}{5} X - \beta \\ S_3 &= \tfrac{-(256\alpha^5 + 3125\beta^4)}{256\alpha^4}. \end{aligned}$$

In this case, $d_0 = 5, d_1 = 4, d_2 = 1, d_3 = 0$.

Extending the classical results by Sturm ([8]) and recent results by [5], we now explain that the Sturm sequence of P and Q gives a formula for the general definition of the Cauchy index on an interval $[a, b]$ under no assumptions on a and b. To do so, it is first needed to extend the notion of sign of a rational function to degenerate cases.

Definition 5 *Let $P, Q \in \mathbf{R}[X] \setminus \{0\}$. Using the same notation as in Definition 1, we define*

$$\mathrm{sign}\Big(\frac{Q}{P}, x\Big) = \begin{cases} \mathrm{sign}\big(\widetilde{Q}(x)\widetilde{P}(x)\big) \in \{-1, 1\} & \text{if } m = 0, \\ 0 & \text{otherwise}. \end{cases}$$

We define also $\mathrm{sign}\Big(\frac{Q}{P}, x\Big) = 0$ if $Q = 0$.

In other words, if x is a pole of $\frac{Q}{P}$, the sign of $\frac{Q}{P}$ at x is 0; otherwise, it is simply the sign of the continuous extension of $\frac{Q}{P}$ at x. Notice that if $Q \neq 0$, $\mathrm{sign}\Big(\frac{Q}{P}, x\Big) = \mathrm{sign}\Big(\frac{P}{Q}, x\Big)$.

We now state the general result relating the Cauchy index and the Sturm sequence, which will be proved at the end of Section 4.

Theorem 6 *Let $a, b \in \mathbf{R}$ with $a < b$ and $P, Q \in \mathbf{R}[X], P \neq 0$, $\deg Q = q < \deg P = p$. If $(S_0, \ldots, S_s)$ is the Sturm sequence of P and Q, then*

$$\mathrm{Ind}_a^b\Big(\frac{Q}{P}\Big) = \frac{1}{2}\sum_{0\leq i\leq s-1}\left(\mathrm{sign}\Big(\frac{S_{i+1}}{S_i}, b\Big) - \mathrm{sign}\Big(\frac{S_{i+1}}{S_i}, a\Big)\right).$$

Adding the condition that a and b are not common roots of P and Q, from Theorem 6 a *sign-variation-counting* formula for the Cauchy index is obtained.

Definition 7 *Let $x \in \mathbf{R}$ and $P, Q \in \mathbf{R}[X]$, we define the sign variation of (P, Q) at x by*

$$\mathrm{Var}_x(P, Q) = \frac{1}{2}\Big|\mathrm{sign}(P(x)) - \mathrm{sign}(Q(x))\Big|.$$

If $a, b \in \mathbf{R}$ with $a < b$, we denote by $\mathrm{Var}_a^b(P, Q)$ the sign variation of (P, Q) at a minus the sign variation of (P, Q) at b; namely,

$$\mathrm{Var}_a^b(P, Q) = \mathrm{Var}_a(P, Q) - \mathrm{Var}_b(P, Q).$$

Note that for $x \in \mathbf{R}$,

$$\mathrm{Var}_x(P, Q) = \begin{cases} 0 & \text{if } P(x) \text{ and } Q(x) \text{ have same sign,} \\ 1 & \text{if } P(x) \text{ and } Q(x) \text{ have opposite non-zero sign,} \\ \frac{1}{2} & \text{if exactly one of } P(x) \text{ and } Q(x) \text{ has zero sign.} \end{cases}$$

Moreover, if x is not a common root of P and Q, then

$$\mathrm{sign}\Big(\frac{Q}{P}, x\Big) = 1 - 2\mathrm{Var}_x(P, Q). \tag{1}$$

The following result then follows clearly from Theorem 6.

Theorem 8 *Let $a, b \in \mathbf{R}$ with $a < b$ and $P, Q \in \mathbf{R}[X], P \neq 0$, $\deg Q = q < \deg P = p$. If a and b are not common roots of P and Q and $(S_0, \ldots, S_s)$ is the Sturm sequence of P and Q, then*

$$\mathrm{Ind}_a^b\Big(\frac{Q}{P}\Big) = \sum_{0\leq i\leq s-1}\mathrm{Var}_a^b(S_i, S_{i+1}).$$

Theorem 8 is a generalization of the classical Sturm theorem [8, 3], since a or b can be root of P or Q (but not of both).

1.3 Subresultant polynomials

Subresultant polynomials are polynomials which are proportional to the ones in the Sturm sequence, but enjoy better properties since their coefficients belong to the ring generated by the coefficients of P and Q. We include definitions and properties concerning subresultant polynomials. We refer the reader to [3] for proofs and details.

Let $\mathbf{D}$ be a domain and let $\mathrm{ff}(\mathbf{D})$ be its fraction field.

Definition 9 *Let $P = a_pX^p + \cdots + a_0, Q = b_qX^q + \cdots + b_0 \in \mathbf{D}[X] \setminus \{0\}$ with $\deg P = p \geq 1$ and $\deg Q = q < p$. For $0 \leq j \leq q$, the j-th subresultant polynomial of P and Q, $\mathrm{sResP}_j(P,Q) \in \mathbf{D}[X]$ is*

$$\det \underbrace{\begin{pmatrix} a_p & a_{p-1} & \cdots & & & & & X^{q-j-1}P \\ 0 & a_p & a_{p-1} & \cdots & & & & X^{q-j-2}P \\ & \ddots & \ddots & \ddots & & & & \vdots \\ & & 0 & a_p & a_{p-1} & \cdots & & P \\ & & & 0 & b_q & b_{q-1} & \cdots & Q \\ & & \iddots & \iddots & \iddots & & & \vdots \\ & \iddots & \iddots & \iddots & & & & \vdots \\ 0 & b_q & b_{q-1} & \cdots & & & & X^{p-j-2}Q \\ b_q & b_{q-1} & \cdots & & & & & X^{p-j-1}Q \end{pmatrix}}_{p+q-2j} \in \mathbf{D}[X].$$

By convention, we extend this definition with

$$\begin{aligned} \mathrm{sResP}_p(P,Q) &= P \in \mathbf{D}[X], \\ \mathrm{sResP}_{p-1}(P,Q) &= Q \in \mathbf{D}[X], \\ \mathrm{sResP}_j(P,Q) &= 0 \in \mathbf{D}[X] \qquad \textit{for } q < j < p-1. \end{aligned}$$

We also define $\mathrm{sResP}_p(P,0) = P, \mathrm{sResP}_j(P,0) = 0, j = 0, \dots, p-1$.

Note that in the matrix above, all the entries in the first $p+q-2j-1$ columns are elements in $\mathbf{D}$, and all the entries in the last column are elements in $\mathbf{D}[X]$. Doing column operations, it is easy to prove that for $0 \leq j \leq p$,

$$\deg \mathrm{sResP}_j(P,Q) \leq j.$$

Note also that in the case $q = p-1$, we have given two definitions for $\mathrm{sResP}_q(P,Q)$, both equal to Q so that there is no ambiguity.

Definition 10 *Let $P, Q \in \mathbf{D}[X] \setminus \{0\}$ with $\deg P = p \geq 1$ and $\deg Q = q < p$.*

- *For $0 \le j \le q$, the j-th subresultant coefficient of P and Q, $\mathrm{sRes}_j(P,Q) \in \mathbf{D}$ is the coefficient of X^j in $\mathrm{sResP}_j(P,Q)$. By convention, we extend this definition with*

$$\begin{array}{rcll} \mathrm{sRes}_p(P,Q) & = & 1 \ \in \mathbf{D} & \textit{(even if } P \textit{ is not monic)}, \\ \mathrm{sRes}_j(P,Q) & = & 0 \ \in \mathbf{D} & \textit{for } q < j \le p-1. \end{array}$$

- *For $0 \le j \le p$, $\mathrm{sResP}_j(P,Q)$ is said to be*
  - **defective** *if* $\deg \mathrm{sResP}_j(P,Q) < j$ *or, equivalently, if* $\mathrm{sRes}_j(P,Q) = 0$,
  - **non-defective** *if* $\deg \mathrm{sResP}_j(P,Q) = j$ *or, equivalently, if* $\mathrm{sRes}_j(P,Q) \neq 0$.

We refer the reader to [1, Chapitre 9] for another definition of subresultant polynomials and coefficients, which differs possibly in a sign.

We illustrate Definitions 9 and 10 with the following example.

Example 11 *Let $\alpha, \beta \in \mathbf{R}$ and $P = X^5 + \alpha X + \beta \in \mathbf{R}[X]$, then $P' = 5X^4 + \alpha$ as in Example 4. We have* $\mathrm{sResP}_5(P,P') = P, \mathrm{sResP}_4(P,P') = P'$

$$\mathrm{sResP}_3(P,P') = \det \begin{pmatrix} 1 & 0 & X^5+\alpha X+\beta \\ 0 & 5 & 5X^4+\alpha \\ 5 & 0 & 5X^5+\alpha X \end{pmatrix} = -5(4\alpha X+5\beta)$$

$$\mathrm{sResP}_2(P,P') = \det \begin{pmatrix} 1 & 0 & 0 & 0 & X^6+\alpha X^2+\beta X^1 \\ 0 & 1 & 0 & 0 & X^5+\alpha X+\beta \\ 0 & 0 & 5 & 0 & 5X^4+\alpha \\ 0 & 5 & 0 & 0 & 5X^5+\alpha X^1 \\ 5 & 0 & 0 & 0 & 5X^6+\alpha X^2 \end{pmatrix} = 0,$$

$$\mathrm{sResP}_1(P,P') = \det \begin{pmatrix} 1 & 0 & 0 & 0 & \alpha & \beta & X^7+\alpha X^3+\beta X^2 \\ 0 & 1 & 0 & 0 & 0 & \alpha & X^6+\alpha X^2+\beta X^1 \\ 0 & 0 & 1 & 0 & 0 & 0 & X^5+\alpha X+\beta \\ 0 & 0 & 0 & 5 & 0 & 0 & 5X^4+\alpha \\ 0 & 0 & 5 & 0 & 0 & 0 & 5X^5+\alpha X^1 \\ 0 & 5 & 0 & 0 & 0 & \alpha & 5X^6+\alpha X^2 \\ 5 & 0 & 0 & 0 & \alpha & 0 & 5X^7+\alpha X^3 \end{pmatrix} = 80\alpha^2(4\alpha X+5\beta),$$

$$\mathrm{sResP}_0(P,P') = \det \begin{pmatrix} 1 & 0 & 0 & 0 & \alpha & \beta & 0 & 0 & X^8+\alpha X^4+\beta X^3 \\ 0 & 1 & 0 & 0 & 0 & \alpha & \beta & 0 & X^7+\alpha X^3+\beta X^2 \\ 0 & 0 & 1 & 0 & 0 & 0 & \alpha & \beta & X^6+\alpha X^2+\beta X^1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \alpha & X^5+\alpha X+\beta \\ 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 5X^4+\alpha \\ 0 & 0 & 0 & 5 & 0 & 0 & 0 & \alpha & 5X^5+\alpha X^1 \\ 0 & 0 & 5 & 0 & 0 & 0 & \alpha & 0 & 5X^6+\alpha X^2 \\ 0 & 5 & 0 & 0 & 0 & \alpha & 0 & 0 & 5X^7+\alpha X^3 \\ 5 & 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 5X^8+\alpha X^4 \end{pmatrix} = 256\alpha^5+3125\beta^4.$$

Note that $\mathrm{sResP}_5(P,P')$ *and* $\mathrm{sResP}_4(P,P')$ *are non-defective while* $\mathrm{sResP}_3(P,P')$ *and* $\mathrm{sResP}_2(P,P')$ *are defective. Finally,* $\mathrm{sResP}_1(P,P')$ *is defective if and only if* $\alpha = 0$*, and* $\mathrm{sResP}_0(P,P')$ *is defective if and only if* $256\alpha^5 + 3125\beta^4 = 0$*.*

The following Structure Theorem is a key result in the theory of subresultants, stating the connection between subresultants and remainders. To state it, we need to introduce a notation.

Notation 12 *For* $n \in \mathbb{Z}$*, we denote* $\epsilon_n = (-1)^{\frac{1}{2}n(n-1)}$*.*

Note that $\epsilon_n = 1$ if the remainder of n in the division by 4 is 0 or 1 and $\epsilon_n = -1$ if the remainder of n in the division by 4 is 2 or 3; this implies that for $k \in \mathbb{Z}$

$$\epsilon_{2k+n} = (-1)^k \epsilon_n = \epsilon_{2k}\epsilon_n. \tag{2}$$

Theorem 13 (Structure Theorem of Subresultants) *Let* $P, Q \in \mathbf{D}[X] \setminus \{0\}$ *with* $\deg P = p \geq 1$ *and* $\deg Q = q < p$*. Let* $(d_0, \ldots, d_s)$ *be the sequence of degrees of the Sturm sequence of* P *and* Q *in decreasing order and let* $d_{-1} = p + 1$ *(note that* $d_0 = p$ *and* $d_1 = q$*).*

- *For* $1 \leq i \leq s$*,*

  $$\mathrm{sResP}_{d_{i-1}-2}(P,Q) = \cdots = \mathrm{sResP}_{d_i+1}(P,Q) = 0 \in \mathbf{D}[X]$$

  and $\mathrm{sResP}_{d_{i-1}-1}(P,Q)$ *and* $\mathrm{sResP}_{d_i}(P,Q)$ *are proportional. More precisely, for* $1 \leq i \leq s$*, denote*

  $$\begin{aligned} T_i &= \mathrm{sResP}_{d_{i-1}-1}(P,Q) \ \in \mathbf{D}[X], \\ t_i &= \mathrm{lc}(T_i) \ \in \mathbf{D} \end{aligned}$$

  (note that $T_1 = Q$*), and extend this notation with* $T_0 = P$ *and* $t_0 = 1 \in \mathbf{D}$ *(even if* P *is not monic). Then*

  $$\mathrm{sRes}_{d_i}(P,Q) \cdot T_i = t_i \cdot \mathrm{sResP}_{d_i}(P,Q) \in \mathbf{D}[X]$$

  with

  $$\mathrm{sRes}_{d_i}(P,Q) = \epsilon_{d_{i-1}-d_i} \cdot \frac{t_i^{d_{i-1}-d_i}}{\mathrm{sRes}_{d_{i-1}}(P,Q)^{d_{i-1}-d_i-1}} \in \mathbf{D}. \tag{3}$$

  This implies $\deg T_i = d_i \leq d_{i-1} - 1$*.*

- *For* $1 \leq i \leq s-1$*,*

  $$t_{i-1} \cdot \mathrm{sRes}_{d_{i-1}}(P,Q) \cdot T_{i+1} = -\mathrm{Rem}\left(t_i \cdot \mathrm{sRes}_{d_i}(P,Q) \cdot T_{i-1}, T_i\right) \in \mathbf{D}[X] \tag{4}$$

  (where Rem *is the remainder in the euclidean division in* $\mathrm{ff}(\mathbf{D})[X]$ *of the first polynomial by the second polynomial) and the quotient belongs to* $\mathbf{D}[X]$*.*

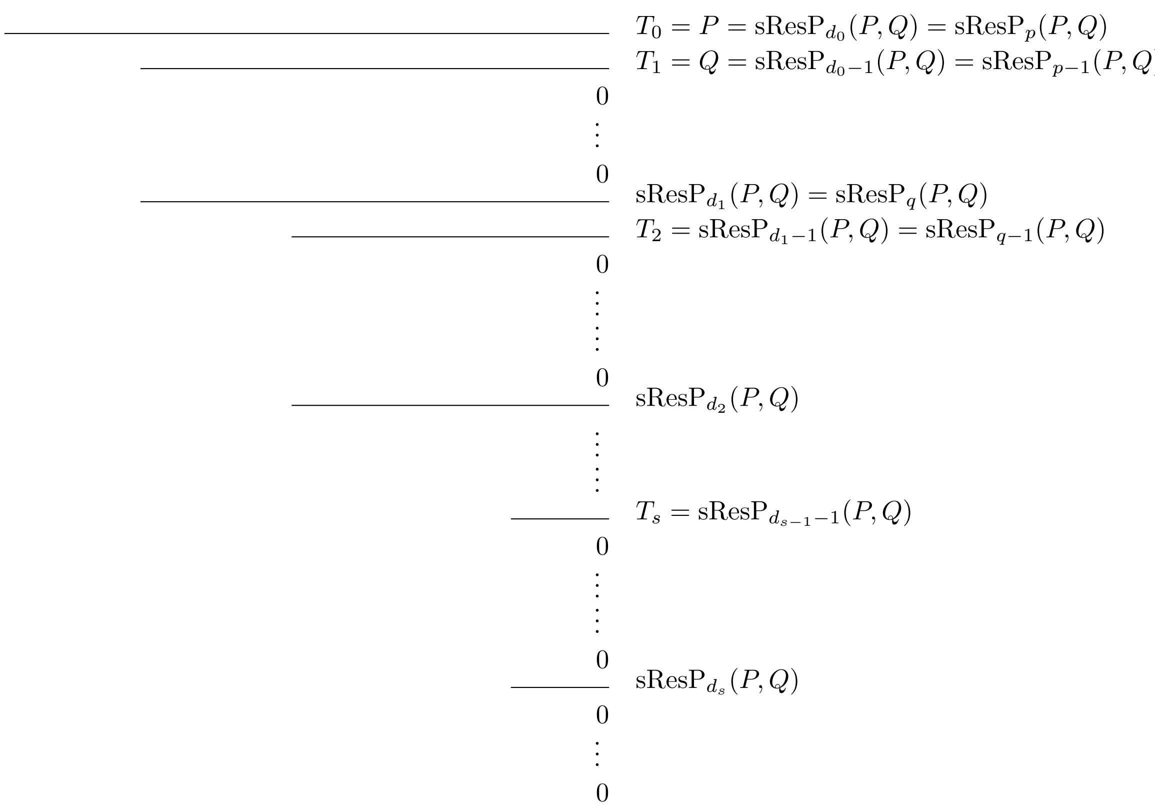
- *Both* $T_s \in \mathbf{D}[X]$ *and* $\mathrm{sResP}_{d_s}(P,Q) \in \mathbf{D}[X]$ *are greatest common divisors of* P *and* Q *in* $\mathrm{ff}(\mathbf{D})[X]$ *and they divide* $\mathrm{sResP}_j(P,Q)$ *for* $0 \leq j \leq p$*. In addition, if* $d_s > 0$ *then*

  $$\mathrm{sResP}_{d_s-1}(P,Q) = \cdots = \mathrm{sResP}_0(P,Q) = 0 \in \mathbf{D}[X].$$

Proof: See [3, Chapter 8]. □

Note that Theorem 13 (Structure Theorem of Subresultants) gives a method for computing the subresultant polynomials using remainders which is more efficient than using their definition as determinants. However we are not concerned with subresultant polynomials computations in the current paper. We are only concerned with a formula for the Cauchy index using the subresultant polynomials.

Theorem 13 (Structure Theorem of Subresultants) can be illustrated by the following picture.



As a corollary to Theorem 13, all subresultant polynomials are either 0 or proportional to polynomials in the Sturm sequence. More precisely, for $1 \le i \le s$, the subresultant polynomial T_i is proportional to S_i in the Sturm sequence.

Remark 14 *In the case where all the subsresultant polynomials are non-defective, there are no pairs of proportional polynomials in the sequence of subresultant polynomials, the degrees of the polynomials S_i in the Sturm sequence decrease one by one, and the coefficient of proportionality between T_i and S_i is a square (see [3, Corollary 8.37]).*

Example 15 (Continuation of Example 4 and Example 11) *Let us take as before $P = X^5 + \alpha X + \beta$ and suppose $\alpha \neq 0$ and $256\alpha^5 + 3125\beta^4 \neq 0$.*

Looking at Example 11, we observe that, as expected given the Structure Theorem, the degrees of the non-defective subresultant polynomials are $d_0 = 5, d_1 = 4, d_2 = 1,\ d_3 = 0$*, i.e. the degrees of the polynomials in the Sturm sequence given in Example 4. Moreover* $\mathrm{sResP}_2(P,P') = 0$*, while* $\mathrm{sResP}_3(P,P')$ *is proportional to* $\mathrm{sResP}_1(P,P')$ *and, also, to* S_2 *given in Example 4.*

Using the notation from Theorem 13, we have

$$
\begin{array}{ll}
T_0 = \mathrm{sResP}_5(P,P') = P = X^5 + \alpha X + \beta, & t_0 = 1, \\
T_1 = \mathrm{sResP}_4(P,P') = P' = 5X^4 + \alpha, & t_1 = 5, \\
T_2 = \mathrm{sResP}_3(P,P') = -20\alpha X - 25\beta, & t_2 = -20\alpha, \\
T_3 = \mathrm{sResP}_0(P,P') = 256\alpha^5 + 3125\beta^4, & t_3 = 256\alpha^5 + 3125\beta^4.
\end{array}
$$

1.4 Main results

In order to state our results we introduce the following notation.

Notation 16 *Using the notation from Theorem 13, for* $0 \le i \le s$*, let*

$$\mathrm{p}(i) = \max\{j \mid 0 \le j \le i,\ d_{j-1} - d_j \text{ is odd}\}$$

($\mathrm{p}(i)$ *is well-defined since* $d_{-1} - d_0 = (p+1) - p = 1$ *is odd).*

We are ready now to state our main result, which is a new formula for $\mathrm{Ind}_a^b\left(\frac{Q}{P}\right)$ using only the polynomials T_i in the sequence of the subresultant polynomials.

Theorem 17 *Let* $a, b \in \mathbf{R}$ *with* $a < b$ *and* $P, Q \in \mathbf{R}[X] \setminus \{0\}$ *with* $\deg P = p \ge 1$ *and* $\deg Q = q < p$*. Then*

$$\mathrm{Ind}_a^b\left(\frac{Q}{P}\right) = \frac{1}{2} \sum_{0 \le i \le s-1} \epsilon_{d_{\mathrm{p}(i)-1} - d_i} \cdot \mathrm{sign}(t_{\mathrm{p}(i)}) \cdot \mathrm{sign}(t_i) \cdot \left(\mathrm{sign}\left(\frac{T_{i+1}}{T_i}, b\right) - \mathrm{sign}\left(\frac{T_{i+1}}{T_i}, a\right) \right).$$

As we will see in Section 2, the main advantage of the formula in Theorem 17 in comparison with previously known related formulas is that there is no assumption on the endpoints a and b of the interval, and, more importantly, potentially less subresultant polynomials (i.e. only te T_i) are involved.

If we add the condition that a and b are no roots of P and Q, from Theorem 17 we obtain a *sign-variation-counting* formula.

Theorem 18 *Let* $a, b \in \mathbf{R}$ *with* $a < b$ *and* $P, Q \in \mathbf{R}[X] \setminus \{0\}$ *with* $\deg P = p \ge 1$ *and* $\deg Q = q < p$*. If* a *and* b *are not common roots of* P *and* Q*, then*

$$\mathrm{Ind}_a^b\left(\frac{Q}{P}\right) = \sum_{0 \le i \le s-1} \epsilon_{d_{\mathrm{p}(i)-1} - d_i} \cdot \mathrm{sign}(t_{\mathrm{p}(i)}) \cdot \mathrm{sign}(t_i) \cdot \mathrm{Var}_a^b(T_i, T_{i+1}).$$

Finally, for the Cauchy index on $\mathbf{R}$, we obtain the following result.

Theorem 19 *Let $P, Q \in \mathbf{R}[X] \setminus \{0\}$ with $\deg P = p \geq 1$ and $\deg Q = q < p$. If the leading coefficient of P is positive or if $d_0 - d_1 = p - q$ is even, then*

$$\mathrm{Ind}_{\mathbf{R}}\left(\frac{Q}{P}\right) = \sum_{\substack{0 \leq i \leq s-1, \\ d_i - d_{i+1}\, odd}} \epsilon_{d_{\mathrm{p}(i)-1} - d_i} \cdot \mathrm{sign}(t_{\mathrm{p}(i)}) \cdot \mathrm{sign}(t_{i+1}).$$

If the leading coefficient of P is negative and $d_0 - d_1 = p - q$ is odd, then

$$\mathrm{Ind}_{\mathbf{R}}\left(\frac{Q}{P}\right) = -\mathrm{sign}(t_1) + \sum_{\substack{1 \leq i \leq s-1, \\ d_i - d_{i+1}\, odd}} \epsilon_{d_{\mathrm{p}(i)-1} - d_i} \cdot \mathrm{sign}(t_{\mathrm{p}(i)}) \cdot \mathrm{sign}(t_{i+1}).$$

Example 20 (Continuation of Examples 4, 11 and 15) *Following Notation 16, for $0 \leq i \leq 3$ we have $\mathrm{p}(i) = i$. Therefore, by Theorem 19, when we fix $(\alpha, \beta) \in \mathbf{R}^2$ with $\alpha \neq 0$ and $256\alpha^3 + 3125\beta^4 \neq 0$, the number of roots of P in $\mathbf{R}$ is given by*

$$\mathrm{Ind}_{\mathbf{R}}\left(\frac{P'}{P}\right) = 1 - \mathrm{sign}(\alpha) + \mathrm{sign}(\alpha) \cdot \mathrm{sign}(256\alpha^5 + 3125\beta^4).$$

The rest of the paper is organized as follows. In Section 2 we comment the differences between our results and previously known related formulas. In Section 3 we review some useful properties of Cauchy index. In Section 4, we recall the notion of (σ, τ)-chain and their connection with Cauchy index. Finally, in Section 5 we prove Theorem 17 using (σ, τ)-chains, and Theorems 18 and 19 as consequences of Theorem 17.

2 Comparison with previous Cauchy index formulas using subresultants

There is a previously known formula for the Cauchy index $\mathrm{Ind}_a^b\left(\frac{Q}{P}\right)$ by means of subresultant polynomials which is as follows (see [3, Chapter 9]).

Definition 21 Let s be a finite sequence of n elements in $\mathbf{R}$ of type

$$s = (s_n, \underbrace{0, \ldots, 0}_{n-m-1}, \underbrace{\qquad s' \qquad}_{m \text{ elements}},)$$

with $s_n \neq 0$ and s' a finite sequence of m elements in $\mathbf{R}$ with $0 \leq m \leq n-1$, which is either empty (this is, $m = 0$) or $s' = (s_m, \ldots, s_1)$ with $s_m \neq 0$. The **modified number of sign variations** in s is defined inductively as follows

$$\mathrm{MVar}(s) = \begin{cases} 0 & \text{if } s' = \emptyset, \\ \mathrm{MVar}(s') + 1 & \text{if } s_n s_m < 0, \\ \mathrm{MVar}(s') + 2 & \text{if } s_n s_m > 0 \text{ and } n - m = 3, \\ \mathrm{MVar}(s') & \text{if } s_n s_m > 0 \text{ and } n - m \neq 3. \end{cases}$$

In other words, the usual definition of the number of sign variations is modified by counting two sign variations for the groups: $+, 0, 0, +$ and $-, 0, 0, -$. If there are no zeros in the sequence s, $\mathrm{MVar}(s)$ is just the classical number of sign variations in the sequence.

Let $\mathcal{P}$ be a sequence $(P_0, P_1, \ldots, P_d)$ of polynomials in $\mathbf{R}[X]$ and let x be an element of $\mathbf{R}$ which is not a root of the gcd of $(P_0, P_1, \ldots, P_d)$, which we call $\mathrm{gcd}(\mathcal{P})$. Then $\mathrm{MVar}(\mathcal{P}; x)$, the **modified number of sign variations** of $\mathcal{P}$ at x, is the number defined as follows:

- delete from $\mathcal{P}$ those polynomials that are identically 0 to obtain the sequence of polynomials $\mathcal{Q} = (Q_0, \cdots, Q_s)$ in $\mathbf{D}[X]$,
- define $\mathrm{MVar}(\mathcal{P}; x)$ as $\mathrm{MVar}(Q_0(x), \cdots, Q_s(x))$.

Let a and b be elements of $\mathbf{R}$ which are not roots of $\mathrm{gcd}(\mathcal{P})$. The difference between the number of modified sign variations in $\mathcal{P}$ at a and b is denoted by

$$\mathrm{MVar}(\mathcal{P}; a, b) = \mathrm{MVar}(\mathcal{P}; a) - \mathrm{MVar}(\mathcal{P}; b).$$

Denoting by $\mathrm{SResP}(P, Q)$ the list of subresultant polynomials of P and Q, the following result is known (see [3, Chapter 9]).

Proposition 22 *Let $a, b \in \mathbf{R}$ with $a < b$ and $P, Q \in \mathbf{R}[X] \setminus \{0\}$ with $\deg P = p \geq 1$ and $\deg Q = q < p$. If a and b are not roots of P, then*

$$\mathrm{Ind}_a^b\left(\frac{Q}{P}\right) = \mathrm{MVar}(\mathrm{SResP}(P, Q); a, b).$$

Our new formula for $\mathrm{Ind}_a^b\left(\frac{Q}{P}\right)$ given in Theorem 17 improves on the one from Proposition 22 in several aspects:

a.i) Theorem 17 is general, there are no restrictions on a and b.

a.ii) More importantly, there are cases when less subresultant polynomials are involved in this new formula. The Structure Theorem of Subresultants (Theorem 13) states that in the subresultant polynomial sequence, some polynomials appear only once and other polynomials appear exactly twice (up to scalar multiples). In addition, if a polynomial appears twice, its first appearance, T_i, is defined as the polynomial determinant of a matrix of smaller size (in comparison with its second appearance), so that it is more suitable in computations. Our formula involves only the T_i, i.e. the first appearance(up to scalar multiples) of each polynomial in the subresultant polynomial sequence.

In the special case when a and b are not common roots of P and Q, Theorem 18 gives a *sign-variation-counting* formula which improves on the one from Proposition 22 since:

b.i) Theorem 18 imposes less restrictions on a and b.

b.ii) As in a.ii).

b.iii) The formula is more natural, since the sign-variation counting in Theorem 18 is local and needs only to consider the sign of two consecutive elements, contrarily to the modified number of sign variations which is very counter-intuitive.

Last but not least, the proofs of our results are also less technically involved than the proof of Proposition 22, which is cumbersome (see the proof in [3, Chapter 9]).

Note that, in the particular case where all subresultant polynomials are non-defective, both the formulas in Theorem 18 and in Proposition 22 become

$$\mathrm{Ind}_a^b\Big(\frac{Q}{P}\Big) = \sum_{0\le j\le p-1} \mathrm{Var}_a^b(\mathrm{sResP}_j, \mathrm{sResP}_{j+1})$$

(see [3, Chapters 2 and 9]), but the new formula extends the previous one to the case whera a and b are not common roots of P and Q.

There is also a previously known formula for the Cauchy index $\mathrm{Ind}_{\mathbf{R}}\Big(\frac{Q}{P}\Big)$ by means of subresultant coefficients which we introduce below (see [3, Chapter 4]).

Proposition 23 *Using the notation from Theorem 13, for* $0 \le i \le s$*, let* $s_i = \mathrm{sRes}_{d_i}(P,Q)$ *be the leading coefficient of the non-defective subresultant polynomial* $\mathrm{sResP}_{d_i}(P,Q)$ *(which is proportional to* T_i*). Then*

$$\mathrm{Ind}_{\mathbf{R}}\Big(\frac{Q}{P}\Big) = \sum_{\substack{0\le i\le s-1,\\ d_i-d_{i+1}\, odd}} \epsilon_{d_i-d_{i+1}}\cdot \mathrm{sign}(s_i)\cdot \mathrm{sign}(s_{i+1}).$$

Even in this special case, the new formula for $\mathrm{Ind}_a^b\Big(\frac{Q}{P}\Big)$ given in Theorem 19 improves on the one from Proposition 23. As before, the main difference between the two formulas is that the t_i are, in the defective cases, defined as determinants of matrices of smaller sizes than the s_i and therefore is more suitable in computations. On the other hand, one advantage of Proposition 23 is that it can be proved directly, using only subresultant coefficients and does not use the definition of the subresultant polynomials and the Structure Theorem of subresultants (see [3, Chapter 4]).

3 Properties of Cauchy index

In this section we include some useful properties of Cauchy index.

Lemma 24 *Let* $a, b \in \mathbf{R}$ *with* $a < b$*,* $P, Q \in \mathbf{R}[X]\setminus\{0\}$ *and* $c \in \mathbf{R}\setminus\{0\}$*. Then*

$$\mathrm{Ind}_a^b\Big(\frac{c\cdot Q}{P}\Big) = \mathrm{sign}(c)\cdot \mathrm{Ind}_a^b\Big(\frac{Q}{P}\Big).$$

Proof: Follows immediately from the definition of Cauchy index. $\square$

Lemma 25 *Let $a, b \in \mathbf{R}$ with $a < b$, $P, Q, R \in \mathbf{R}[X] \setminus \{0\}$ and $T \in \mathbf{R}[X]$ such that*

$$Q = PT + R.$$

Then

$$\mathrm{Ind}_a^b\Big(\frac{Q}{P}\Big) = \mathrm{Ind}_a^b\Big(\frac{R}{P}\Big).$$

Proof: For each $x \in [a, b]$, we first note that if

$$\frac{Q}{P} = (X - x)^m \frac{\widetilde{Q}}{\widetilde{P}}$$

with $m \in \mathbb{Z}$, $\widetilde{P}(x) \neq 0, \widetilde{Q}(x) \neq 0$ and $m < 0$, then defining

$$\widetilde{R} = \widetilde{Q} - (X - x)^{-m}\widetilde{P}T,$$

we have

$$\frac{R}{P} = (X - x)^m \frac{\widetilde{R}}{\widetilde{P}}$$

with $\widetilde{P}(x) \neq 0$ and $\widetilde{R}(x) = \widetilde{Q}(x) \neq 0$. This proves that $\mathrm{Ind}_x^{\varepsilon}\Big(\frac{Q}{P}\Big) = \mathrm{Ind}_x^{\varepsilon}\Big(\frac{R}{P}\Big)$ for every $\varepsilon \in \{-1, 1\}$. The claim follows from the definition of the Cauchy index. $\square$

The following property is known as *the inversion formula*.

Proposition 26 *Let $a, b \in \mathbf{R}$ with $a < b$ and $P, Q \in \mathbf{R}[X] \setminus \{0\}$. Then*

$$\mathrm{Ind}_a^b\Big(\frac{Q}{P}\Big) + \mathrm{Ind}_a^b\Big(\frac{P}{Q}\Big) = \frac{1}{2}\mathrm{sign}\Big(\frac{Q}{P}, b\Big) - \frac{1}{2}\mathrm{sign}\Big(\frac{Q}{P}, a\Big).$$

Proof: See [5, Theorem 3.9]. $\square$

4 (σ, τ)-chains and Cauchy index

The notion of (σ, τ)-chain was introduced in [7]. Here, we need to introduce a slight variation of this notion.

Definition 27 *Let $n \in \mathbb{Z}_{\geq 1}$ and $\sigma, \tau \in \{-1, 1\}^{n-1}$ with $\sigma = (\sigma_1, \dots, \sigma_{n-1})$ and $\tau = (\tau_1, \dots, \tau_{n-1})$. A sequence of polynomials $(P_0, \dots, P_n)$ in $\mathbf{R}[X]$ is a* special (σ, τ)-chain *if for $1 \leq i \leq n - 1$ there exist $a_i, c_i \in \mathbf{R} \setminus \{0\}$ and $B_i \in \mathbf{R}[X]$ such that*

1. $a_i P_{i+1} + B_i P_i + c_i P_{i-1} = 0,$

2. $\mathrm{sign}(a_i) = \sigma_i$,

3. $\mathrm{sign}(c_i) = \tau_i$.

As in [7], note that for $n = 1$, taking $\{-1, 1\}^0 = \{\bullet\}$, any sequence (P_0, P_1) in $\mathbf{R}[X]$ is a special $(\bullet, \bullet)$-chain.

Note also that Sturm sequences are always special $(1, \ldots, 1), (1, \ldots, 1)$ chains.

Example 28 (Continuation of Examples 4, 11, 15 and 20) *Taking* $\sigma = (1, 1)$ *and* $\tau = (1, 1)$, *then* (S_0, S_1, S_2, S_3) *is a special* (σ, τ)*-chain, with*

$$\begin{aligned} a_1 &= 1, \\ B_1 &= -\tfrac{X}{5}, \\ c_1 &= 1, \\ a_2 &= 1, \\ B_2 &= \tfrac{25(64X^3\alpha^3 - 80X^2\alpha^2\beta + 100X\alpha\beta^2 - 125\beta^3)}{256\alpha^4}, \\ c_2 &= 1. \end{aligned}$$

Taking now $\sigma = (1, 1)$ *and* $\tau = (1, -1)$, *then* (T_0, T_1, T_2, T_3) *is a special* (σ, τ)*-chain, with*

$$\begin{aligned} a_1 &= 1, \\ B_1 &= -5X, \\ c_1 &= 25, \\ a_2 &= 25, \\ B_2 &= -25(64X^3\alpha^3 - 80X^2\alpha^2\beta + 100X\alpha\beta^2 - 125\beta^3), \\ c_2 &= -6400\alpha^4. \end{aligned}$$

We will see in Section 5 how to produce special (σ, τ)*-chains using Theorem 13 (Structure Theorem of Subresultants).*

We introduce some more useful definition.

Definition 29 *Let* $a, b \in \mathbf{R}$, $n \in \mathbb{Z}_{\geq 1}$, $(P_0, \ldots, P_n)$ *in* $\mathbf{R}[X] \setminus \{0\}$ *and* $\sigma, \tau \in \{-1, 1\}^{n-1}$. *We define* $\theta(\sigma, \tau)_0 = 1$, *for* $1 \leq i \leq n - 1$,

$$\theta(\sigma, \tau)_i = \prod_{1 \leq j \leq i} \sigma_j \tau_j$$

and

$$W(\sigma, \tau)_a^b(P_0, \ldots, P_n) = \frac{1}{2} \sum_{0 \leq i \leq n-1} \theta(\sigma, \tau)_i \cdot \left(\mathrm{sign}\Big(\frac{P_{i+1}}{P_i}, b\Big) - \mathrm{sign}\Big(\frac{P_{i+1}}{P_i}, a\Big) \right).$$

Using the ideas of the proof of [5, Theorem 3.11], we obtain the following result for special (σ,τ)-chains. Note that no assumption on a and b is made.

Proposition 30 *Let $a,b\in\mathbf{R}$ with $a<b$, $n\in\mathbb{Z}_{\geq 1}$ and $\sigma,\tau\in\{-1,1\}^{n-1}$. If $(P_0,\dots,P_n)$ in $\mathbf{R}[X]\setminus\{0\}$ is a special (σ,τ)-chain then*

$$\mathrm{Ind}_a^b\Big(\frac{P_1}{P_0}\Big)+\theta(\sigma,\tau)_{n-1}\cdot\mathrm{Ind}_a^b\Big(\frac{P_{n-1}}{P_n}\Big)=W(\sigma,\tau)_a^b(P_0,\dots,P_n).$$

Proof: We proceed by induction in n. If $n=1$, the result follows from Proposition 26 (Inversion Formula).

Suppose now that $n\geq 2$. Taking a_1,B_1,c_1 as in Definition 27, by Lemmas 24 and 25 we have

$$\begin{aligned}
& \mathrm{Ind}_a^b\Big(\frac{P_0}{P_1}\Big)+\sigma_1\cdot\tau_1\cdot\mathrm{Ind}_a^b\Big(\frac{P_2}{P_1}\Big)\\
=\ & \mathrm{Ind}_a^b\Big(\frac{-a_1P_2-B_1P_1}{c_1P_1}\Big)+\sigma_1\cdot\tau_1\cdot\mathrm{Ind}_a^b\Big(\frac{P_2}{P_1}\Big)\\
=\ & -\mathrm{sign}(a_1)\cdot\mathrm{sign}(c_1)\cdot\mathrm{Ind}_a^b\Big(\frac{P_2}{P_1}\Big)+\sigma_1\cdot\tau_1\cdot\mathrm{Ind}_a^b\Big(\frac{P_2}{P_1}\Big)\\
=\ & 0.
\end{aligned}$$

We consider $\sigma'=(\sigma_2,\dots,\sigma_{n-1})$, $\tau'=(\tau_2,\dots,\tau_{n-1})$ and we apply the inductive hypothesis to the special (σ',τ')-chain $(P_1,\dots,P_n)$. For $1\leq i\leq n-1$ we have that $\theta(\sigma,\tau)_i=\sigma_1\cdot\tau_1\cdot\theta(\sigma',\tau')_{i-1}$. Finally, using Proposition 26 (Inversion Formula) and the inductive hypothesis,

$$\begin{aligned}
& \mathrm{Ind}_a^b\Big(\frac{P_1}{P_0}\Big)+\theta(\sigma,\tau)_{n-1}\cdot\mathrm{Ind}_a^b\Big(\frac{P_{n-1}}{P_n}\Big)\\
=\ & \mathrm{Ind}_a^b\Big(\frac{P_1}{P_0}\Big)+\mathrm{Ind}_a^b\Big(\frac{P_0}{P_1}\Big)+\sigma_1\cdot\tau_1\cdot\mathrm{Ind}_a^b\Big(\frac{P_2}{P_1}\Big)+\sigma_1\cdot\tau_1\cdot\theta(\sigma',\tau')_{n-2}\cdot\mathrm{Ind}_a^b\Big(\frac{P_{n-1}}{P_n}\Big)\\
=\ & -\frac{1}{2}\mathrm{sign}\Big(\frac{P_1}{P_0},a\Big)+\frac{1}{2}\mathrm{sign}\Big(\frac{P_1}{P_0},b\Big)+\sigma_1\cdot\tau_1\cdot W(\sigma',\tau')_a^b(P_1,\dots,P_n)\\
=\ & W(\sigma,\tau)_a^b(P_0,\dots,P_n)
\end{aligned}$$

as we wanted to prove. □

Corollary 31 *Let $a,b\in\mathbf{R}$ with $a<b$, $n\in\mathbb{Z}_{\geq 1}$ and $\sigma,\tau\in\{-1,1\}^{n-1}$. If $(P_0,\dots,P_n)$ in $\mathbf{R}[X]\setminus\{0\}$ is a special (σ,τ)-chain and P_n divides P_{n-1}, then*

$$\mathrm{Ind}_a^b\Big(\frac{P_1}{P_0}\Big)=W(\sigma,\tau)_a^b(P_0,\dots,P_n).$$

As mentioned in the Introduction, Theorem 6 can be deduced from Corollary 31.

Proof of Theorem 6 : Theorem 6 is a special case of Corollary 31 taking $\sigma=(1,\dots,1)$ and $\tau=(1,\dots,1)$, since the Sturm sequence is a special $((1,\dots,1),(1,\dots,1))$-chain and S_s divides S_{s-1}. □

5 Proof of the main results

We fix the notation we will use from this point.

Notation 32 *Let $P, Q \in \mathbf{R}[X] \setminus \{0\}$ with $\deg P = p \geq 1$ and $\deg Q = q < p$. Let $(d_0, \dots, d_s)$ be the sequence of degrees of the non-defective subresultant polynomials of P and Q in decreasing order and let $d_{-1} = p + 1$.*

- *Using the notation from Theorem 13, for $1 \leq i \leq s-1$, let*

$$\begin{aligned} a_i &= t_{i-1} \cdot \mathrm{sRes}_{d_{i-1}}(P, Q) \ \in \mathbf{R}, \\ B_i &= -\mathrm{Quot}\left(t_i \cdot \mathrm{sRes}_{d_i}(P, Q) \cdot T_{i-1}, T_i\right) \ \in \mathbf{R}[X], \\ c_i &= t_i \cdot \mathrm{sRes}_{d_i}(P, Q) \ \in \mathbf{R}. \end{aligned}$$

- *For $1 \leq i \leq s-1$, let*

$$\begin{aligned} \sigma_i &= \mathrm{sign}(a_i) \ \in \{-1, 1\}, \\ \tau_i &= \mathrm{sign}(c_i) \ \in \{-1, 1\}, \end{aligned}$$

  and let $\sigma = (\sigma_1, \dots, \sigma_{s-1})$ and $\tau = (\tau_1, \dots, \tau_{s-1})$.

Lemma 33 *$(T_0, \dots, T_s)$ is a special (σ, τ)-chain. In addition, T_s divides all its elements.*

Proof: Recall that $T_0 = P$ and $T_1 = Q$. Also, by the Structure Theorem of Subresultants (Theorem 13), we have that for $1 \leq i \leq s-1$,

$$a_i T_{i+1} + B_i T_i + c_i T_{i-1} = 0.$$

The claim follows from the definition of σ, τ. □

The following lemma explores the relation between the signs of the leading coefficients of the subresultants polynomials.

Lemma 34 *Let $P, Q \in \mathbf{R}[X] \setminus \{0\}$ with $\deg P = p \geq 1$ and $\deg Q = q < p$. Following Notation 12 and 16, for $0 \leq i \leq s$,*

$$\mathrm{sign}(\mathrm{sRes}_{d_i}(P, Q)) = \epsilon_{d_{\mathrm{p}(i)-1} - d_i} \cdot \mathrm{sign}(t_{\mathrm{p}(i)}).$$

Proof: For $i = 0$ the result is clear. For $1 \leq i \leq s$, by the Structure Theorem of Subresultants (Theorem 13),

$$\mathrm{sign}(\mathrm{sRes}_{d_i}(P, Q)) = \epsilon_{d_{i-1} - d_i} \cdot \mathrm{sign}(t_i)^{d_{i-1} - d_i} \cdot \mathrm{sign}(\mathrm{sRes}_{d_{i-1}}(P, Q))^{d_{i-1} - d_i - 1}.$$

We proceed then by induction on $i - \mathrm{p}(i)$. If $i = \mathrm{p}(i)$, then $d_{i-1} - d_i$ is odd and

$$\mathrm{sign}(\mathrm{sRes}_{d_i}(P, Q)) = \epsilon_{d_{\mathrm{p}(i)-1}-d_i} \cdot \mathrm{sign}(t_{\mathrm{p}(i)}).$$

If $i > \mathrm{p}(i)$, then $d_{i-1} - d_i$ is even, $\mathrm{p}(i) = \mathrm{p}(i-1)$ and $i - 1 - \mathrm{p}(i-1) < i - \mathrm{p}(i)$; therefore by the inductive hypothesis,

$$\mathrm{sign}(\mathrm{sRes}_{d_i}(P, Q)) = \epsilon_{d_{i-1}-d_i} \cdot \mathrm{sign}(\mathrm{sRes}_{d_{i-1}}(P, Q)) = \epsilon_{d_{i-1}-d_i} \cdot \epsilon_{d_{\mathrm{p}(i-1)-1}-d_{i-1}} \cdot \mathrm{sign}(t_{\mathrm{p}(i-1)}) =$$

$$= \epsilon_{d_{i-1}-d_i} \cdot \epsilon_{d_{\mathrm{p}(i)-1}-d_{i-1}} \cdot \mathrm{sign}(t_{\mathrm{p}(i)}) = \epsilon_{d_{\mathrm{p}(i)-1}-d_i} \cdot \mathrm{sign}(t_{\mathrm{p}(i)})$$

using equation (2). □

Now we are ready to prove Theorem 17.

Proof of Theorem 17: By Corollary 31, since $(T_0, \ldots, T_s)$ is a special (σ, τ)-chain and T_s divides T_{s-1},

$$\mathrm{Ind}_a^b\Big(\frac{Q}{P}\Big) = W(\sigma, \tau)_a^b(T_0, \ldots, T_s) = \frac{1}{2} \sum_{0 \le i \le s-1} \theta(\sigma, \tau)_i \cdot \left(\mathrm{sign}\Big(\frac{T_{i+1}}{T_i}, b\Big) - \mathrm{sign}\Big(\frac{T_{i+1}}{T_i}, a\Big)\right).$$

So, we only need to prove that for $0 \le i \le s - 1$,

$$\theta(\sigma, \tau)_i = \epsilon_{d_{\mathrm{p}(i)-1}-d_i} \cdot \mathrm{sign}(t_{\mathrm{p}(i)}) \cdot \mathrm{sign}(t_i).$$

Indeed, using Lemma 34,

$$\begin{aligned}
\theta(\sigma, \tau)_i &= \prod_{1 \le j \le i} \sigma_j \cdot \tau_j \\
&= \prod_{1 \le j \le i} \mathrm{sign}(t_{j-1}) \cdot \mathrm{sign}(\mathrm{sRes}_{d_{j-1}}(P, Q)) \cdot \mathrm{sign}(t_j) \cdot \mathrm{sign}(\mathrm{sRes}_{d_j}(P, Q)) \\
&= \mathrm{sign}(\mathrm{sRes}_{d_i}(P, Q)) \cdot \mathrm{sign}(t_i) \\
&= \epsilon_{d_{\mathrm{p}(i)-1}-d_i} \cdot \mathrm{sign}(t_{\mathrm{p}(i)}) \cdot \mathrm{sign}(t_i)
\end{aligned}$$

and we are done. □

From Theorem 17, we can easily deduce Theorem 18 as follows.

Proof of Theorem 18: Theorem 13 implies that, if for some $0 \le i \le s-1$, two consecutive polynomials T_i and T_{i+1} in the sequence $(T_0, \ldots, T_s)$ have a common root x, then every polynomial in this sequence has x as a root. So, suppose now that a and b are not common roots of $T_0 = P$ and $T_1 = Q$, therefore they are not common roots of T_i and T_{i+1} for any $0 \le i \le s - 1$.

The proof is finished using the formula from Theorem 17 for the Cauchy index $\mathrm{Ind}_a^b\Big(\frac{Q}{P}\Big)$ and the identity (1). □

Finally, we prove Theorem 19.

Proof or Theorem 19: We introduce the notation

$$\begin{aligned}
\mathrm{Var}_{+\infty}(P,Q) &= \tfrac{1}{2}\Big|\mathrm{sign}(\mathrm{lc}(P)) - \mathrm{sign}(\mathrm{lc}(Q))\Big|,\\
\mathrm{Var}_{-\infty}(P,Q) &= \tfrac{1}{2}\Big|(-1)^{\deg(P)}\mathrm{sign}(\mathrm{lc}(P)) - (-1)^{\deg(Q)}\mathrm{sign}(\mathrm{lc}(Q))\Big|,\\
\mathrm{Var}_{-\infty}^{+\infty}(P,Q) &= \mathrm{Var}_{-\infty}(P,Q) - \mathrm{Var}_{+\infty}(P,Q).
\end{aligned}$$

Note that, if $\deg(P)-\deg(Q)$ is even, then $\mathrm{Var}_{-\infty}^{+\infty}(P,Q)=0$, and if $\deg(P)-\deg(Q)$ is odd, then $\mathrm{Var}_{-\infty}^{+\infty}(P,Q)=\mathrm{sign}(\mathrm{lc}(P))\cdot\mathrm{sign}(\mathrm{lc}(Q))$.

Choosing $r\in\mathbf{R}$ big enough and applying Theorem 18,

$$\begin{aligned}
\mathrm{Ind}_{\mathbf{R}}\Big(\frac{Q}{P}\Big) &= \mathrm{Ind}_{-r}^{r}\Big(\frac{Q}{P}\Big)\\
&= \sum_{0\le i\le s-1} \epsilon_{d_{\mathrm{p}(i)-1}-d_i}\cdot\mathrm{sign}(t_{\mathrm{p}(i)})\cdot\mathrm{sign}(t_i)\cdot\mathrm{Var}_{-r}^{r}(T_i,T_{i+1})\\
&= \sum_{0\le i\le s-1} \epsilon_{d_{\mathrm{p}(i)-1}-d_i}\cdot\mathrm{sign}(t_{\mathrm{p}(i)})\cdot\mathrm{sign}(t_i)\cdot\mathrm{Var}_{-\infty}^{+\infty}(T_i,T_{i+1})\\
&= \sum_{\substack{0\le i\le s-1,\\ d_i-d_{i+1}\,\mathrm{odd}}} \epsilon_{d_{\mathrm{p}(i)-1}-d_i}\cdot\mathrm{sign}(t_{\mathrm{p}(i)})\cdot\mathrm{sign}(t_i)\cdot\mathrm{sign}(\mathrm{lc}(T_i))\cdot\mathrm{sign}(\mathrm{lc}(T_{i+1})).
\end{aligned}$$

From this identity the result can be easily proved, taking into account that for $i\ge 1$, $t_i=\mathrm{lc}(T_i)$, but there is an ad-hoc definition of $t_0=1$ (and not as the leading coefficient of $T_0=P$). $\square$

Acknowledgements: We are thankful to the anonymous referees for their helpful remarks and suggestions.

References

[1] Apéry, François; Jouanolou, Jean-Pierre. Résultant et sous-résultants : Elimination - Le Cas d'une variable. *Hermann, Paris*, 2006.

[2] Barnett, Stephen. Polynomials and linear control systems. Monographs and Textbooks in Pure and Applied Mathematics, 77. *Marcel Dekker, Inc., New York,* 1983.

[3] Basu, Saugata; Pollack, Richard; Roy, Marie-Françoise. Algorithms in real algebraic geometry. Second edition. Algorithms and Computation in Mathematics, 10. *Springer-Verlag, Berlin*, 2006.

[4] Cauchy, Augustin. Oeuvres complètes, Gauthier-Villars, Paris, 1882–1974.

[5] Eisermann, Michael. The fundamental theorem of algebra made effective: an elementary real-algebraic proof via Sturm chains. *Amer. Math. Monthly* 119 (2012), no. 9, 715–752.

[6] Henrici, Peter. Applied and computational complex analysis. Volume 1. Pure and Applied Mathematics. *Wiley-Interscience [John Wiley & Sons], New York-London-Sydney,* 1974.

[7] Perrucci, Daniel; Roy, Marie-Françoise. Quantitative Fundamental Theorem of Algebra. *Q.J.Math.* 70 (2019), no. 3, 1009–1037.

[8] Sturm, Charles. Collected Works, Edited by J.-C. Pont, Birkhuser, Basel, 2009.