



**HAL**  
open science

# On the set of bad primes in the study of Casas-Alvero Conjecture

Daniel Schaub, Mark Spivakovsky

► **To cite this version:**

Daniel Schaub, Mark Spivakovsky. On the set of bad primes in the study of Casas-Alvero Conjecture. 2023. hal-04158876v1

**HAL Id: hal-04158876**

**<https://univ-angers.hal.science/hal-04158876v1>**

Preprint submitted on 11 Jul 2023 (v1), last revised 26 Nov 2024 (v3)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# On the set of bad primes in the study of the Casas–Alvero conjecture

Daniel Schaub, Univ Angers, CNRS, LAREMA, SFR MATHSTIC  
F-49000 Angers, France  
email: daniel.schaub@univ-angers.fr

Mark Spivakovsky, Univ Paul Sabatier, CNRS, IMT UMR 5219  
F-31062 Toulouse, France and  
CNRS, LaSol UMI 2001, UNAM.  
email: mark.spivakovsky@math.univ-toulouse.fr

July 11, 2023

## Abstract

The Casas–Alvero conjecture predicts that every univariate polynomial over a field of characteristic zero having a common factor with each of its derivatives  $H_i(f)$  is a power of a linear polynomial. One approach to proving the conjecture is to first prove it for polynomials of some small degree  $d$ , compile a list of bad primes for that degree (namely, those primes  $p$  for which the conjecture fails in degree  $d$  and characteristic  $p$ ) and then deduce the conjecture for all degrees of the form  $dp^\ell$ ,  $\ell \in \mathbb{N}$ , where  $p$  is a good prime for  $d$ . In this paper we calculate certain distinguished monomials appearing in the resultant  $R(f, H_i(f))$ . As a corollary, we obtain a (non-exhaustive) list of bad primes for every degree  $d \in \mathbb{N} \setminus \{0\}$ .

## 1 Introduction

In the year 2001 Eduardo Casas–Alvero published a paper on higher order polar germs of plane curve singularities [1]. His work on polar germs inspired him to make the following conjecture (according to the testimony of José Manuel Aroca, E. Casas communicated the problem orally well before 2001).

Let  $K$  be a field,  $d$  a strictly positive integer and  $f = x^d + a_1x^{d-1} + \dots + a_{d-1}x + a_d$  a monic univariate polynomial of degree  $d$  over  $K$ . Let

$$H_i(f) = \binom{d}{i}x^{d-i} + \binom{d-1}{i}a_1x^{d-i-1} + \dots + \binom{i}{i}a_{d-i}$$

be the  $i$ -th Hasse derivative of  $f$ .

**Definition 1** *The polynomial  $f$  is said to be a **Casas–Alvero polynomial** if for each  $i \in \{1, \dots, d-1\}$  it has a non-constant common factor with its  $i$ -th Hasse derivative  $H_i(f)$ .*

Note that, by definition, a Casas–Alvero polynomial  $f$  has a common root with  $H_{d-1}(f)$ , in particular, it has at least one root  $b \in K$ , regardless of whether or not  $K$  is algebraically closed. Making the change of variables  $x \rightsquigarrow x - b$ , we may assume that 0 is a root of  $f$ , in other words,  $a_d = 0$ . In the sequel, we will always make this assumption without mentioning it explicitly.

**Conjecture 1** Assume that  $\text{char } K = 0$ . If  $f \in K[x]$  is a Casas-Alvero polynomial of degree  $d$  with  $a_d = 0$ , then  $f(x) = x^d$ .

For  $i \in \{1, \dots, d-1\}$ , let  $R_i = R(f, H_i(f)) \in K[a_1, \dots, a_{d-1}]$  be the resultant of  $f$  and  $H_i(f)$ . The polynomials  $f$  and  $H_i(f)$  have a common factor if and only if  $R_i = 0$ . Thus  $f$  is Casas-Alvero if and only if the point  $(a_1, \dots, a_{d-1}) \in V(R_1, \dots, R_{d-1}) \subset K^{d-1}$ . In those terms the Conjecture can be reformulated as follows:

**Conjecture 2** Let  $V = V(R_1, \dots, R_{d-1}) \subset K^{d-1}$ . Then  $V = \{0\}$ . In other words,

$$\sqrt{(R_1, \dots, R_{d-1})} = (a_1, \dots, a_{d-1}) \quad (1)$$

or, equivalently ,

$$a_i^N \in (R_1, \dots, R_{d-1}) \text{ for all } i \in \{1, \dots, d-1\} \text{ and some } N \in \mathbb{N}. \quad (2)$$

If  $\text{char } K = p > 0$ , the Conjecture is false in general. The simplest counterexample is the polynomial  $f(x) = x^{p+1} - x^p$ .

**Remark 2** Let  $K \subset K'$  be a field extension. The induced extension

$$K[a_1, \dots, a_{d-1}] \subset K'[a_1, \dots, a_{d-1}]$$

is faithfully flat. Since the polynomials  $R_1, \dots, R_{d-1}$  have coefficients in  $\mathbb{Z}$ , (2) holds in  $K[a_1, \dots, a_{d-1}]$  if and only if it holds in  $K'[a_1, \dots, a_{d-1}]$ . Hence the truth of the conjecture depends only on the characteristic of  $K$ , but not on the choice of the field  $K$  itself.

**Remark 3** Formulae (1) and (2) can be interpreted in terms of Gröbner bases. Namely, (1) and (2) are equivalent to saying that for any choice of monomial ordering and Gröbner basis  $(f_1, \dots, f_N)$  of  $(R_1, \dots, R_{d-1})$ , after renumbering the  $f_j$ , the leading monomial of  $f_j$  is a power of  $a_j$ .

We will write  $\text{CA}_{d,p}$  for the statement ‘‘The Casas-Alvero conjecture holds for polynomials of degree  $d$  over fields of characteristic  $p$ ’’.

The following equivalences are known for each  $d$  ([5], [6]) :

$\text{CA}_{d,0}$  holds  $\iff$   $\text{CA}_{d,p}$  holds for some prime number  $p$   $\iff$   $\text{CA}_{d,p}$  holds for all but finitely many primes  $p$ .

**Definition 4** A prime number  $p$  is said to be a **bad prime for  $d$**  if  $\text{CA}_{d,p}$  is false. If  $p$  is not a bad prime for  $d$ , we will say that  $p$  is a **good prime for  $d$** .

**Proposition 5** ([6], Propositions 2.2 and 2.6) Take a strictly positive integer  $d$ , a prime number  $p$  and a non-negative integer  $\ell$ . Assume that  $\text{CA}_{d,p}$  holds. Then so do  $\text{CA}_{dp^\ell, p}$  and  $\text{CA}_{dp^\ell, 0}$ .

This result suggests the following general approach to the problem :

- (1) prove the conjecture for a small number  $d$ ;
- (2) compile lists of good and bad primes for  $d$ ;
- (3) conclude that  $\text{CA}_{dp^\ell, 0}$  holds for all the primes  $p$  that are known to be good for  $d$ .

In particular, this shows the importance of knowing which primes are good or bad for a given degree  $d$ .

The above approach has been carried out up to  $d \leq 7$  ([2], [3], [4], [5], [6]). Some integers cannot be written in the form  $dp^\ell$  where  $p$  is a good prime for  $d$ . For example,

$$12 = 2^2 \cdot 3, \quad 20 = 2^2 \cdot 5, \quad 24 = 2^3 \cdot 3, \quad 28 = 2^2 \cdot 7, \quad 30 = 2 \cdot 3 \cdot 5, \quad 36 = 2^2 \cdot 3^2, \quad 40 = 2^3 \cdot 5, \dots$$

$CA_{12,0}$  has been proved by [2] with the aid of a computer, by using a very clever strategy to cut down the computation of resultants and Gröbner basis. Thus the smallest degree  $d$  for which  $CA_{d,0}$  is not known is  $d = 20$ .

The main results of the paper are the following. First we show that for each  $i \in \{1, \dots, d-1\}$ , the monomials  $\left(1 - \binom{d}{i}\right)^{d-i} a_{d-i}^d$  and  $(-1)^{(d-1)(d-i)} \binom{d}{i}^{d-1} a_{d-1}^{d-i} a_{d-i}$  appear in the resultant  $R_i$  (unless  $i = 1$  in which case the two monomials are the same and the coefficient is  $(1-d)^{d-1}$ ). Moreover, the monomials  $a_{d-i}^d$  are the only pure powers appearing in any of the  $R_i$ . We then use these facts to compile a (non-exhaustive) list of bad primes for each  $d \in \mathbb{N}_{>0}$ , namely all the primes  $p$  for which there exists  $i \in \{1, \dots, d-1\}$  such that  $p \mid \binom{d}{i} - 1$ .

## 2 A list of bad primes

Unless otherwise specified, from now till the end of this paper we shall regard the  $R_i$  as elements of the polynomial ring  $\mathbb{Z}[a_1, \dots, a_{d-1}]$ .

**Theorem 6** *For each  $i \in \{1, \dots, d-1\}$ , the monomial  $(-1)^{d-i} \left(\binom{d}{i} - 1\right)^{d-i} a_{d-i}^d$  appears in the resultant  $R_i$ . Moreover the monomials  $a_{d-i}^d$  are the only pure powers appearing in any of the  $R_i$ .*

Proof : The polynomial  $R_i$  is the resultant of

$$f = x^d + a_{d-1}x^{d-1} + \dots + a_{d-1}x$$

and

$$H_i(f) = \binom{d}{i} x^{d-i} + \binom{d-i-1}{i} a_1 x^{d-i-1} + \dots + \binom{i+1}{i} a_{d-i-1} x + \binom{i}{i} a_{d-i}.$$

**Notation.** For  $i, j \in \{1, \dots, d-1\}$ , we denote by  $\tilde{a}_{ij}$  the element  $\binom{d-j}{i} a_j$ .

Note that for all  $i \in \{1, \dots, d-1\}$ ,  $\tilde{a}_{i,d-i} = a_{d-i}$ .

The resultant  $R_i$  equals the determinant  $D(d, i)$  of the following matrix  $M(d, i)$ :

$$\left( \begin{array}{c|c} \overbrace{\begin{array}{ccccc} 1 & a_1 & a_2 & \cdots & a_{d-i-1} \\ 0 & 1 & a_1 & \cdots & a_{d-i-2} \\ \vdots & \vdots & & & \\ 0 & \cdots & 0 & \cdots & 1 \end{array}}^{d-i} & \overbrace{\begin{array}{ccccccc} a_{d-i} & \cdots & a_{d-1} & 0 & \cdots & \cdots & 0 \\ a_{d-i-1} & a_{d-i} & \cdots & a_{d-1} & 0 & \cdots & 0 \\ & & & & & \vdots & \vdots \\ a_1 & a_2 & \cdots & a_{d-i} & \cdots & a_{d-1} & 0 \end{array}}^d \\ \hline \begin{array}{ccccc} \binom{d}{i} & \tilde{a}_{i,1} & \tilde{a}_{i,2} & \cdots & \tilde{a}_{i,d-i-1} \\ 0 & \binom{d}{i} & \tilde{a}_{i,1} & \cdots & \tilde{a}_{i,d-i-2} \\ \vdots & \vdots & & & \vdots \\ \vdots & \vdots & & & \vdots \\ \vdots & \vdots & & & \vdots \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{array} & \begin{array}{ccccccc} a_{d-i} & \cdots & 0 & 0 & \cdots & \cdots & 0 \\ \tilde{a}_{i,d-i-1} & a_{d-i} & 0 & \cdots & \cdots & \cdots & 0 \\ \tilde{a}_{i,d-i-2} & \vdots & & & \vdots & \vdots & \\ \vdots & & & & \vdots & \vdots & \\ \vdots & & & & \vdots & \vdots & \\ \vdots & & & & \vdots & \vdots & \\ \vdots & & & & \vdots & \vdots & \\ \cdots & 0 & \binom{d}{i} & \tilde{a}_{i,1} & \tilde{a}_{i,2} & \cdots & a_{d-i} \end{array} \end{array} \right)$$

By definition, the determinant  $D(d, i)$  of the  $(2d - i) \times (2d - i)$  matrix  $M(d, i) = (m_{\ell_j})$  is

$$\Delta = \sum_{\sigma \in \Sigma_{2d-i}} (-1)^{\epsilon(\sigma)} m_{\sigma(1),1} m_{\sigma(2),2} \cdots m_{\sigma(2d-i),2d-i}, \quad (3)$$

where  $\Sigma_{2d-i}$  is the group of permutations of  $\{1, \dots, 2d - i\}$  and

$$\begin{aligned} \epsilon(\sigma) &= 0 && \text{if } \sigma \text{ is even} \\ &= 1 && \text{if } \sigma \text{ is odd.} \end{aligned}$$

First of all, note that the last column of  $M(d, i)$  has only one non-zero entry that equals  $a_{d-i}$ . Hence  $a_{d-i} \mid D(d, i)$ . In particular no pure power of  $a_j$  can appear in  $D(d, i)$  for  $j \neq d - i$ .

**Remark 7** *The entry  $a_{d-i}$  appears only in the last  $d$  columns of  $M(d, i)$ : exactly once in each of the last  $i$  columns and exactly twice in each of the columns numbered  $d - i + 1, d - i + 2, \dots, 2d - 2i$ .*

By inspection of the matrix  $M(d, i)$ , we see that

- (1) a monomial  $\omega$  appearing in  $D(d, i)$  cannot be divisible by  $a_{d-i}^{d+1}$
- (2) if  $a_{d-i}^d \nmid \omega$ , then  $\omega$  is not a pure power of  $a_{d-i}$
- (3) if  $a_{d-i}^d \mid \omega$ , then in the notation of formula (3),  $\omega = (-1)^{\epsilon(\sigma)} m_{\sigma(1),1} \cdots m_{\sigma(2d-i),2d-i}$  with  $\sigma(j) = j$  for  $j \in \{2d - 2i + 1, \dots, 2d - 1\}$  and  $\sigma(j) \in \{j, j - d + i\}$  for  $j \in \{d - i + 1, \dots, 2d - 2i\}$ .

The term in (3) corresponding to  $\sigma = \text{Id}$  is the product of the elements on the main diagonal of  $M(d, i)$ ; this product is equal to  $a_{d-i}^d$ . There are other choices of  $\sigma \in \Sigma_d$  for which the corresponding summand in (3) is of the form  $ca_{d-i}^d$ , where  $c \in \mathbb{Z}$ . Let us group all of these terms together and calculate the total coefficient of  $a_{d-i}^d$  in (3)

Now, the coefficient of  $a_{d-i}^d$  in  $D(d, i)$  is given by the coefficient of  $a_{d-i}^{d-i}$  in the expansion of the determinant  $\tilde{D}(d, i)$  of the  $(2d - 2i) \times (2d - 2i)$ -matrix  $\tilde{M}(d, i)$  obtained by deleting the last  $i$  lines and the last  $i$  columns of  $M(d, i)$ .

The matrix  $\tilde{M}(d, i)$  is

$$\begin{pmatrix} 1 & a_1 & a_2 & \cdots & a_{d-i-1} & a_{d-i} & \cdots & a_{d-1} & 0 \\ 0 & 1 & a_1 & \cdots & a_{d-i-2} & a_{d-i-1} & a_{d-i} & \cdots & a_{d-1} \\ \vdots & \vdots & & & \vdots & & & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & 1 & a_1 & a_2 & \cdots & a_{d-i} \\ \binom{d}{i} & \tilde{a}_{i,1} & \tilde{a}_{i,2} & \cdots & \tilde{a}_{i,d-i-1} & a_{d-i} & 0 & \cdots & 0 \\ 0 & \binom{d}{i} & \tilde{a}_{i,1} & \cdots & \tilde{a}_{i,d-i-2} & \tilde{a}_{i,d-i-1} & a_{d-i} & 0 & \cdots \\ \vdots & \vdots & & & \vdots & & & & \vdots \\ 0 & \cdots & 0 & \binom{d}{i} & \cdots & \cdots & \tilde{a}_{i,d-i-1} & a_{d-i} & 0 \\ 0 & 0 & \cdots & \cdots & \binom{d}{i} & \cdots & \cdots & \tilde{a}_{i,d-i+1} & a_{d-i} \end{pmatrix}$$

In this determinant, the first  $d - i$  columns do not contain any  $a_{d-i}$  and in the last  $d - i$  columns, each  $a_{d-i}$  appears two times, once in the first  $d - i$  rows, once in the last  $d - i$  rows.

In each of the last  $d - i$  columns we have to choose one of the two  $a_{d-i}$  and delete the rest of the line and the rest of the column to which it belongs. Fix one such choice. The corresponding monomial  $(-1)^{\epsilon(\sigma)} m_{\sigma(1),1} m_{\sigma(2),2} \cdots m_{\sigma(2d-2i),2d-2i}$ ,  $\sigma \in \Sigma_{2d-2i}$ , satisfies  $\sigma(j) \in \{j, j - d + i\}$  for all  $j \in \{d - i + 1, \dots, 2d - 2i\}$ .

Let

$$J = \{\sigma(j) \mid j \in \{d - i + 1, \dots, 2d - 2i\}\} \quad (4)$$

and  $J^c = \{1, \dots, 2d - 2i\} \setminus J$ . Write  $J = \{j_1, \dots, j_{d-i}\} \subset \{1, \dots, 2(d-i)\}$ .

$$\text{For all } q, \ell \in \{1, \dots, d-i\} \text{ we have } j_q - j_\ell \neq d-i. \quad (5)$$

The set  $J^c$  has the same property. Note that, conversely, every set

$$J = \{j_1, \dots, j_{d-i}\} \subset \{1, \dots, 2(d-i)\}$$

satisfying (5) has the form (4) for a suitable  $\sigma \in \Sigma_{2d-2i}$ .

The coefficient of the term  $a_{d-i}^{d-i}$  in the expansion of  $\tilde{D}(d, i)$  corresponding to a given choice of  $J$  is the determinant of the matrix  $N(d, i, J)$  obtained from the first  $(d-i)$  columns of  $\tilde{M}(d, i)$  by deleting the rows numbered  $j_1, \dots, j_{d-i-1}, j_{d-i}$ .

Let

$$k = \#(J^c \cap \{d-i+1, d-i+2, \dots, 2(d-i)\}). \quad (6)$$

There exists a permutation of the rows of  $N(d, i, J)$  such that the resulting matrix is an upper triangular matrix with only 1 and  $\binom{d}{i}$  on the main diagonal, where 1 appears  $(d-i-k)$  times and  $\binom{d}{i}$  appears  $k$  times. Thus the permutation  $\sigma \in \Sigma_{2d-2i}$  is uniquely determined by  $J \cap \{d-i+1, \dots, 2d-2i\}$ .

We have

$$\det N(d, i, J) = \pm \binom{d}{i}^k. \quad (7)$$

Now,  $\sigma$  is the composition of  $k$  transpositions  $(j, j-d+i)$  for  $j \in J^c \cap \{d-i+1, \dots, 2d-2i\}$ . Thus

$$\epsilon(\sigma) \equiv k \pmod{2}. \quad (8)$$

**Example** To illustrate the process, let us take

$$J = \{d-i+1, d-i+2, \dots, 2(d-i)-3, d-i-2, 2(d-i)-1, 2(d-i)\},$$

which means that we chose all the occurrences of  $a_{d-i}$  lying on the main diagonal in the last  $(d-i)$  rows of  $\tilde{M}(d, i)$  except in the column number  $2(d-i)-2$  in which case we chose the occurrence of  $a_{d-i}$  at the place  $(d-i-2, 2d-2i-2)$ . We have  $k=1$ .

The resulting matrix  $N(d, i, J)$  looks like

$$\begin{pmatrix} 1 & a_1 & a_2 & \dots & \dots & \dots & a_{d-i-1} \\ 0 & 1 & a_1 & \dots & \dots & \dots & a_{d-i-2} \\ \vdots & \vdots & \vdots & & & & \vdots \\ 0 & \dots & 0 & 1 & a_1 & a_2 & a_3 \\ 0 & \dots & \dots & 0 & 0 & 1 & a_1 \\ 0 & \dots & \dots & \dots & 0 & 0 & 1 \\ 0 & \dots & \dots & 0 & \binom{d}{i} & \tilde{a}_{i,1} & \tilde{a}_{i,2} \end{pmatrix}$$

To obtain an upper triangular matrix, we have to apply a cyclic permutation to the rows  $d-i$ ,  $d-i-1$  and  $d-i-2$  and we obtain that the desired determinant is  $\pm \binom{d}{i}$ .

Coming back to the proof of the Theorem, for each  $k \in \{0, \dots, d-i\}$ , there are  $\binom{d-i}{k}$  choices of  $J$  satisfying (6). Combining this with (7) and (8) and summing over all  $k \in \{0, \dots, d-i\}$ , we get that the coefficient of  $a_{d-i}^d$  in  $R_i$  is

$$\sum_{k=0}^{d-i} (-1)^k \binom{d-i}{k} \binom{d}{i}^k = (-1)^{d-i} \left( \binom{d}{i} - 1 \right)^{d-i} \quad (9)$$

□

**Corollary 8** Take a prime number  $p$  such that there exists  $i \in \{1, \dots, d-1\}$  for which  $p \mid \binom{d}{i} - 1$ . Then  $CA_{d,p}$  is false.

Proof. Assume that  $\text{char}(K) = p$ . By Theorem 6, no pure power of any of the  $a_i$  appears in any of the  $R_j \pmod p$ . Hence the point of  $K^{d-1}$  whose  $i$ -th coordinate is 1 and all of whose other coordinates are zero belongs to  $V(R_1, \dots, R_{d-1})$ .  $\square$

Using similar arguments, we obtain the following Proposition.

**Proposition 9** For  $i \in \{2, \dots, d-1\}$ , the monomial  $(-1)^{(d-1)(d-i)} \binom{d}{i}^{d-1} a_{d-1}^{d-i} a_{d-i}$  appears in the resultant  $R_i$ . The term  $(-1)^{(d-1)(d-i)} \binom{d}{i}^{d-1} a_{d-1}^{d-i} a_{d-i}$  is the unique monomial in (3) of degree  $d-i+1$ ; all the other monomials appearing in (3) have degree strictly greater than  $d-i+1$ .

Proof. By inspection of the matrix  $M(d, i)$ , we see that the monomial  $(-1)^{(d-1)(d-i)} \binom{d}{i}^{d-1} a_{d-1}^{d-i} a_{d-i}$  appears in the resultant  $R_i$ : it is the monomial with

$$\begin{aligned} \sigma(j) &= d-i+j && \text{for } \{1, \dots, d-i\} \\ &= j-(d-i) && \text{for } j \in \{d-i+1, \dots, 2d-i-1\} \\ &= 2d-i && \text{for } j = 2d-i. \end{aligned}$$

Moreover, it is the unique monomial  $\omega$  of  $R_i$  such that  $a_{d-1}^{d-i} \mid \omega$ .

Let us prove the second statement of the Proposition. Let  $M^\bullet(d, i)$  be the matrix obtained by deleting the last row and the last column of  $M(d, i)$ . Let  $D^\bullet(d, i) = \det M^\bullet(d, i)$ . We need to show that all the monomials appearing in  $D^\bullet(d, i)$  have order at least  $d-i$  and  $a_{d-1}^{d-i}$  is the only one of order exactly  $d-i$ .

**Remark 10** For  $\ell, j \in \{1, \dots, 2d-i-1\}$ , we have  $m_{\ell j} \in \mathbb{N} \setminus \{0\}$  if and only if one of the following conditions holds:

- (1)  $j \in \{d-i+1, \dots, d-1\}$  and  $\ell = j+d-i$
- (2)  $j \in \{1, \dots, d-i\}$  and  $\ell \in \{j, j+d-i\}$ .

By Remark 10, the last  $d-i$  columns of  $M^\bullet(d, i)$  do not involve any non-zero constant entries. Hence every monomial  $\omega = (-1)^{\epsilon(\sigma)} m_{\sigma(1),1} \cdots m_{\sigma(2d-i-1),2d-i-1}$  appearing in  $D^\bullet(d, i)$  has degree at least  $d-i$ . Moreover, assume that  $\deg \omega = d-i$ . Moreover, for  $j \in \{1, \dots, d-1\}$  one of the conditions (1) or (2) of Remark 10 holds with  $\ell = \sigma(j)$ . Let

$$j(\omega) = \min\{j \in \{1, \dots, d-1\} \mid \sigma(j) = j+d-i\}.$$

**Lemma 11** We have  $j(\omega) = 1$ .

Proof of Lemma. Assume that  $j(\omega) > 1$ , aiming for contradiction. By Remark 10,

$$\text{if } j \in \{d-i+1, \dots, d-1\}, \text{ then } \sigma(j) = j+d-i. \quad (10)$$

Hence  $j(\omega) \leq d-i+1$ .

Take a  $j \in \{j(\omega) + d - 2, \dots, 2d - i - 1\}$ . Then  $j > d - 1$ . From (10) we obtain  $\sigma(j) \notin \{2d - i - 1, \dots, 2d - i - 1\}$ . By inspection of the matrix  $M^\bullet(d, i)$ , it follows that

$$\sigma(j) \in \{j(\omega) - 1, \dots, d - i\}.$$

By descending induction on  $j$ , we obtain

$$\sigma(j) = j - d + 1 \text{ whenever } j \in \{j(\omega) + d - 2, \dots, 2d - i - 1\}. \quad (11)$$

By equation (11), we have  $\sigma(j(\omega) + d - 2) = j(\omega) - 1$ , so  $\sigma(j(\omega) - 1) \neq j(\omega) - 1$ . By Remark 10,  $\sigma(j(\omega) - 1) = j(\omega) - 1 + d - i$ . contradicting the definition of  $j(\omega)$ . The Lemma is proved.  $\square$

The Proposition follows from the Lemma by inspection of the matrix  $M^\bullet(d, i)$ .  $\square$

## References

- [1] Eduardo Casas–Alvero, *Higher Order Polar Germs*, Journal of Algebra, Volume 240, Issue 1, 1 June 2001, pages 326–337
- [2] W. Castryck, R. Laterveer, M. Ounaïes, *Constraints on counterexamples to the Casa-Alvero conjecture and a verification in degree 12*, arXiv:1208.5404v1, 27/08/2018.
- [3] R.M. de Frutos Marín, *Perspectivas Aritméticas para la Conjectura de Casas–Alvero*, PhD thesis, Universidad de Valladolid, 2012.
- [4] A. Salinier, M. Chellali, *La conjecture de Casas-Alvero pour les degrés  $5p^e$* , hal-00748843, 2012.
- [5] J. Draisma and J.P. de Jong, *On the Casas-Alvero conjecture*, Newsletter of the EMS 80 (June 2011) 29–33
- [6] H.-C. Graf von Bothmer, O. Labs, J. Schicho and C. Van de Woestline, *The Casas-Alvero conjecture for infinitely many degrees* Journal of Algebra, Vol. 316(1),224-230, 2007.