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

Daniel Schaub, Mark Spivakovsky

A description of and an upper bound 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

November 26, 2024

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 is a power of a linear polynomial. One approach to proving the conjecture is to first prove it for polynomials of some small degree n, compile a list of bad primes for that degree (namely, those primes p for which the conjecture fails in degree n and characteristic p) and then deduce the conjecture for all degrees of the form np^ℓ, $\ell \in \mathbb{N}$, where p is a good prime for n. In this paper we give an explicit description of the set of bad primes in any given degree n. We show that if the conjecture holds in degree n then the bad primes for n are bounded above by $\binom{\frac{n^2-n}{2}}{n-2}! \prod_{i=1}^{n-1} \binom{i+n-2}{n-2}^{\binom{d-i+n-2}{n-2}}$.

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.

Let K be a field, $f \in K[x]$ a non-constant monic univariate polynomial, $n := \deg(f)$:

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

Let

$$H_i(f) = \binom{n}{i} x^{n-i} + \binom{n-1}{i} a_1 x^{n-i-1} + \cdots + \binom{i}{i} a_{n-i}$$

be the i-th Hasse derivative of f.

Definition 1.1 *The polynomial f is said to be a* **Casas–Alvero polynomial** *if for each $i \in \{1, \ldots, n-1\}$ it has a non-constant common factor with its i-th Hasse derivative $H_i(f)$.*

Conjecture 1.2 (Casas–Alvero) *Assume that char $K = 0$. If $f \in K[x]$ is a Casas-Alvero polynomial of degree n, then there exists $b \in K$ such that $f(x) = (x-b)^n$.*

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

Remark 1.3 *The following fact is known and easy to prove. If the Casas–Alvero conjecture holds for the algebraic closure $\bar{K}$ of K then it also holds for K (the converse is not established, to our knowledge). From now on we will assume that K is algebraically closed.*

We will write $\mathrm{CA}_{n,p}$ for the statement "The Casas–Alvero conjecture holds for polynomials of degree n over algebraically closed fields of characteristic p".

The following equivalences are known for each n ([4], [7]):

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

Note: The results of the present paper provide, among other things, an elementary, independent proof of this fact without using valuation theory as in [4] or the theory of projective schemes over Spec $\mathbb{Z}$ as in [7].

Definition 1.4 *A prime number p is said to be a **bad prime for** n if $CA_{n,p}$ is false. If p is not a bad prime for n, we will say that p is a **good prime for** n.*

Proposition 1.5 *([7], Propositions 2.2 and 2.6) Take a strictly positive integer n, a prime number p and a non-negative integer ℓ. Assume that $CA_{n,p}$ holds. Then so do $CA_{np^\ell,p}$ and $CA_{np^\ell,0}$.*

This result suggests the following general approach to the problem:

(1) prove the conjecture for a small number n;

(2) compile lists of good and bad primes for n;

(3) conclude that $\mathrm{CA}_{np^\ell,0}$ holds for all the primes p that are known to be good for n.

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

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

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

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

The purpose of this paper is to give an explicit description of the set of bad primes in any given degree n. In particular, we obtain an explicit upper bound on bad primes for n, assuming that $C_{n,0}$ holds. These results are based on recent work of Soham Ghosh [6].

2 A reformulation of the problem by S. Ghosh

Notation: For $j \in \{1, \ldots, n-1\}$, let the involution

$$\Phi_j : K[x_1, \ldots, x_{n-1}] \to K[x_1, \ldots, x_{n-1}], \tag{1}$$

be defined by

$$\Phi_j(x_i) = x_i - x_j \text{ for } i \neq j \text{ and } \Phi_j(x_j) = -x_j. \tag{2}$$

Let

$$\Phi_n : K[x_1, \ldots, x_{n-1}] \to K[x_1, \ldots, x_{n-1}], \tag{3}$$

denote the identity map.

Let $\sigma_i(x_1, \ldots, x_{n-1})$ denote the i-th elementary symmetric function of $x_1, \ldots, x_{n-1}$.

Let $\mathcal{T} = \{1, \ldots, n\}^{n-1}$; the set $\mathcal{T}$ is the collection of all the $(n-1)$-tuples of the form $(j_1, \ldots, j_{n-1})$, where $j_1, \ldots, j_{n-1} \in \{1, \ldots, n\}$.

Notation. Given a fixed choice of $T = (j_1, \ldots j_{n-1}) \in \mathcal{T}$, for $i \in \{1, \ldots, n-1\}$ we will denote by $G_{T,i}$ the homogeneous polynomial $\Phi_{j_i}(\sigma_i(x_1, \ldots, x_{n-1}))$.

In his fundamental preprint [6], Soham Ghosh showed that the Casas–Alvero conjecture in degree n (over any field, regardless of characteristic) is equivalent to the following statement.

Conjecture 2.1 *([6], Proposition 5.2) For every choice of $T = (j_1, \ldots, j_{n-1}) \in \mathcal{T}$, the sequence of homogeneous polynomials*

$$(G_{T,1}, \ldots, G_{T,n-1}) \tag{4}$$

is a regular sequence in $K[x_1, \ldots, x_{n-1}]$.

Since the polynomial ring $K[x_1, \ldots, x_{n-1}]$ is Cohen–Macaulay, Conjecture 2.1 is equivalent to saying that $\mathrm{ht}(G_{T,1}, \ldots, G_{T,n-1}) = n-1$ and thus also to

Conjecture 2.2 *We have*

$$\sqrt{G_{T,1}, \ldots, G_{T,n-1}} = (x_1, \ldots x_{n-1}). \tag{5}$$

3 Macaulay's Theorem

We recall (a part of) Macaulay's celebrated theorem from 1916.

Let $x_1, \ldots, x_n$ be independent variables, $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$ homogeneous polynomials and let $d_i = \deg\ f_i$ denote the total degree of f_i. Let $\mathfrak{m} := (x_1, \ldots, x_n)$. Finally, put $d = \sum_{k=1}^{n} d_k - n + 1$.

Theorem 3.1 *[8] The following statements are equivalent:*

(1) $\sqrt{(f_1, \ldots, f_n)} = \mathfrak{m}$

(2) $\mathfrak{m}^d \subset (f_1, \ldots, f_n)$.

4 A description of and an upper bound on the set of bad primes

In this section we state and prove our main results.

Let $x = (x_1, \ldots, x_{n-1})$. We will use multi-index notation: x^α will stand for $\prod_{k=1}^{n-1} x_k^{\alpha_k}$ and $|\alpha|$ for $\sum_{k=1}^{n-1} \alpha_k$.

We apply Macaulay's Theorem to the polynomials $G_{T,}, \ldots, G_{T,n-1} \in K[x]$.

We have $\deg\ G_{T,i} = i$ for $i \in \{1, \ldots, n-1\}$.

Let $d = \sum_{i=1}^{n-1} \deg\ G_{T,i} - (n-2) = 1 + 2 + \cdots + (n-1) - (n-2) = \frac{n^2-3n+4}{2}$.

Let C denote the binomial coefficient $\binom{\frac{n^2-n}{2}}{n-2}$; it is the number of monomials of degree $d = \frac{n^2-3n+4}{2}$ in $n-1$ variables.

Let $S_{T,i} = \{ G_{T,i} x^\alpha \mid |\alpha| = d - i \}$, $i \in \{1, \ldots, n-1\}$ and

$$S_T := \bigcup_{i=1}^{n-1} S_{T,i}.$$

We have $|S_{T,i}| = \binom{d-i+n-2}{n-2}$.

Let $D := |S_T| = \sum_{i=1}^{n-1} |S_{T,i}| = \sum_{i=1}^{n-1} \binom{d-i+n-2}{n-2}$; we have $D \geq C$ (in fact, the inequality is strict whenever $n > 2$).

Consider the C-dimensional K-vector space V, generated by all the monomials in x of degree d; we have $S_T \subset V$.

Let M_T denote the $D \times C$ matrix formed by the row vectors $(v)_{v \in S_T}$. Let J_T be the greatest common divisor of all the $C \times C$ minors of M_T.

Theorem 4.1 *A prime number p is a bad prime for n if and only if $p \mid J_T$ for some $T \in \mathcal{T}$ (equivalently, if and only if $p \mid \operatorname{lcm}(J_T)_{T \in \mathcal{T}}$).*

Proof. Fix a $T \in \mathcal{T}$. By Theorem 3.1, equality (5) of Conjecture 2.2 is equivalent to

$$(x)^d \subset (G_{T1}, \ldots, G_{T,n-1}).$$

This is true if and only if $V \subset (G_{T1}, \ldots, G_{T,n-1})$. This inclusion is true if and only if the rank of the matrix M_T is maximal, that is, $\operatorname{rk} M_T = C$ or, in other words, if and only if M_T has a non-degenerate $C \times C$ minor.

Therefore Conjectures 2.1 and 2.2 fail in degree n and characteristic p if and only if $p \mid J_T$ for some $T \in \mathcal{T}$. By [6], Proposition 5.2, the failure of Conjecture 2.1 in degree n and characteristic p is equivalent to p being a bad prime for n. □

Corollary 4.2 *If $C_{n,0}$ holds but p is a bad prime for n then*

$$p < C! \prod_{i=1}^{n-1} \binom{i+n-2}{n-2}^{\binom{d-i+n-2}{n-2}}. \tag{6}$$

Proof. The corollary follows from Theorem 4.1 and the following lemma.

Lemma 4.3 *Fix a $T \in \mathcal{T}$ and let A be a $C \times C$ minor of M_T. Then*

$$|A| \leq C! \prod_{i=1}^{n-1} \binom{i+n-2}{n-2}^{\binom{d-i+n-2}{n-2}}.$$

Proof of the lemma. Write $G_{T,i}$ as a sum of (possibly repeated) monomials, each with coefficient ± 1. The monomial $x_{j_i}^i$ is repeated $\binom{i+n-2}{n-2}$ times, more than any other monomial. Therefore, once we group the like terms together, the greatest possible absolute value of a coefficient of a monomial in $G_{T,i}$ is $\binom{i+n-2}{n-2}$.

When we write the minor A as a sum of $C!$ terms, each term divides an integer of the form $\prod_{i=1}^{n-1} \prod_{j=1}^{\binom{i+n-2}{n-2}} a_{ij}$, where for all the pairs (i,j) we have $|a_{ij}| \leq \binom{i+n-2}{n-2}$. This proves the lemma and, with it, the corollary. □

Remark 4.4 *The upper bound* (6) *can be vastly improved as follows. Let the notation be as above. The product* $\prod_{i=1}^{n-1} \binom{i+n-2}{n-2}^{\binom{d-i+n-2}{n-2}}$ *has a total of* D *(not necessarily distinct) terms of the form* $\binom{i+n-2}{n-2}$*. We have* $\binom{i+n-2}{n-2} < \binom{i'+n-2}{n-2}$ *whenever* $i < i'$*. Write* $\prod_{i=1}^{n-1} \binom{i+n-2}{n-2}^{\binom{d-i+n-2}{n-2}} = \prod_{k=1}^{D} b_k$ *with the sequence* b_k *non-strictly increasing. Then*

$$p < C! \prod_{D-C+1}^{D} b_k \tag{7}$$

The proof is the same as in the corollary. The reason we did not state the corollary in this form in the first place is that we could not find an explicit, closed form for the integers b_k *appearing in* (7)*. For example, what is the value of* i *such that* $b_{D-C+1} = \binom{i+n-2}{n-2}$ *?*

Remark 4.5 *We acknowledge the fact that our bound on bad primes is not optimal/realistic: it involves double factorials and is too large to be computable even for small* n*. However, we hope that having even a theoretical bound is of some interest and that the bound can be improved in the future in order to have practical value.*

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 Casas-Alvero conjecture and a verification in degree 12*, arXiv:1208.5404v1, 27/08/2018.

[3] M. Chellali, A. Salinier, *La conjecture de Casas-Alvero pour les degrés* $5p^e$, hal-00748843, 2012.

[4] J. Draisma and J. P. de Jong, *On the Casas–Alvero conjecture,* Newsletter of the EMS 80 (June 2011), pages 29–33.

[5] R. M. de Frutos Marín, *Perspectivas Aritméticas para la Conjectura de Casas–Alvero*, PhD thesis, Universidad de Valladolid, 2012.

[6] S. Ghosh, *A finiteness result towards the Casas-Alvero Conjecture*, arXiv:2402.18717 [math.AG].

[7] 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.

[8] F. S. Macaulay, *The algebraic theory of modular systems*, Cambridge University Press, 1916.