hexagon:2611.00040v1

RECYCLED ROOTS UNDER REDUCTION AND DESCENT IN THE CASAS-ALVERO PROBLEM

DAVID NIEDBALA GIRAUDIN

Abstract. For a Casas-Alvero polynomial f, the type of f is one less than the minimal number of roots of f needed to meet every Hasse derivative $H_1 f, \dots, H_{d-1} f$. We show that the type does not increase under reduction modulo a prime and under the descent from degree np^e to degree n in characteristic p. Consequently, if no Casas-Alvero polynomial of degree n and type at most k exists over $\overline{\mathbb{F}}_p$, then none of degree np^e and type at most k exists in characteristic 0, for every $e \geq 0$. For $k = 2$ the hypothesis is equivalent to $p \nmid N_n$ for an explicit integer N_n, and we show by a finite computation that $N_n \neq 0$ for $3 \leq n \leq 22$ and $n = 24$. In particular there is no counterexample of type at most 2 in degree 24. This gives infinite families of degrees for which the conjecture is not known and every counterexample has type at least 3: the degrees $5 \cdot 8009^e$, the degrees $6p^e$ for 21 primes p that are bad for degree 6, the degrees $7p^e$, $8p^e$, $9p^e$ and $10p^e$ for 13, 17, 16 and 103 explicit primes p that are bad for these degrees, and the degrees $20p^e$ and $24p^e$ for all primes p outside a finite set (for $20p^e$, including $p = 2^{31} - 1$). For $k = 3$ we obtain the first degrees in which every counterexample has type at least 4: the degrees $6p^e$ for $p \in \{983, 1901, 51313000813080529\}$, the degrees $8 \cdot 397^e$, the degrees $9p^e$ for $p \in \{613, 757\}$ and the degrees $10p^e$ for 13 primes p.

1. Introduction

Let K be a field and $f \in K[x]$ monic of degree $d \geq 2$. Write $H_i f$ for the i-th Hasse derivative, so that $f(x+t) = \sum_{i \geq 0} (H_i f)(x)\, t^i$. Following [2], we call f a *CA-polynomial* if $\gcd(f, H_i f) \neq 1$ for $1 \leq i \leq d-1$ and f is not of the form $(x-\alpha)^d$ over $\overline{K}$. The Casas-Alvero conjecture asserts that there are no CA-polynomials in characteristic 0. It is known in degrees p^k and $2p^k$ [1], in degrees $3p^k, 4p^k$ for most p [4], in degrees $5p^k, 6p^k, 7p^k$ for p outside the finite sets of bad primes $B(5), B(6), B(7)$ [3, 2], where $B(n)$ is the set of primes p such that a CA-polynomial of degree n exists over $\overline{\mathbb{F}}_p$, and in degree 12 [2]. The smallest open degree is 20. A proof of the conjecture in all degrees has been announced in [5]; in this note a degree is called open when it is not covered by the results listed above, and nothing below depends on [5].

Definition 1.1. A *recycling set* of a CA-polynomial f is a set R of roots of f in $\overline{K}$ such that for every $1 \leq i \leq d-1$ some $\theta \in R$ satisfies $H_i f(\theta) = 0$. The *type* of f is $\mathrm{type}(f) = \min |R| - 1$ [2, §1.2].

If $R = \{\theta\}$ then $H_i f(\theta) = 0$ for $0 \leq i \leq d-1$ and $f = (x-\theta)^d$; hence $\mathrm{type}(f) \geq 1$ always. In characteristic 0 one has $\mathrm{type}(f) \geq 2$ [2, §2.2]; the type-one values are identified with MacMahon's descent numbers in [6]. Counterexamples of type 2 were excluded in degree 12 [2] and in degree 20 [7, Thm. 7.10] (see Remark 4.4).

Our main tool is the following transfer statement.

Theorem 1.2. *Let p be a prime, $e \geq 0$, $n \geq 2$, $d = np^e$ and $k \geq 1$. If there is no CA-polynomial of degree n and type at most k over $\overline{\mathbb{F}}_p$, then there is no CA-polynomial of degree d and type at most k over any field of characteristic 0.*

Date: 2 November 2026.

ORCID 0009-0009-1526-1178. Technical assistance: Claude (Anthropic).

For $k = 2$ we make the hypothesis effective (Proposition 4.2) and verify it (Proposition 4.3).

Theorem 1.3. *Let $3 \leq n \leq 22$ or $n = 24$. There is an explicit nonzero integer N_n such that for every prime $p \nmid N_n$ and every $e \geq 0$, every CA-polynomial of degree np^e in characteristic 0 has type at least 3. For $n \leq 20$ moreover $2^{31} - 1 \nmid N_n$. In particular, every CA-polynomial of degree 24 in characteristic 0 has type at least 3.*

Remark 1.4. For $n \leq 19$ the conjecture holds in degree n, so $B(n)$ is finite [1] and the conjecture itself holds in degree np^e for every $p \notin B(n)$. The sets $B(n)$ are known for $n \leq 7$ [1, 3, 2], and an upper bound for $B(n)$ is given in [8]; for $8 \leq n \leq 10$, [2, Table 2] gives the smallest prime $p_0(n) \nmid n$ outside $B(n)$, so that every prime $p < p_0(n)$ with $p \nmid n$ lies in $B(n)$, and for $11 \leq n \leq 19$ we are not aware of a published prime outside $B(n)$. Theorem 1.3 gives information for all $p \nmid N_n$, without determining $B(n)$; it is new where $p \in B(n)$ or where $B(n)$ is not determined, and in the cases $n = 20$ and $n = 24$, where the conjecture is open. Table 1 lists the cases in which $p \in B(n)$ is established.

2. Three lemmas

Lemma 2.1 (affine change)**.** *Let $\lambda \in K^\times$, $\mu \in K$ and $g(x) = \lambda^{-d} f(\lambda x + \mu)$. Then $H_i g(x) = \lambda^{i-d}(H_i f)(\lambda x + \mu)$. In particular g is a CA-polynomial if and only if f is, $R \mapsto (R - \mu)/\lambda$ maps recycling sets of f to recycling sets of g, and* $\operatorname{type}(g) = \operatorname{type}(f)$.

Proof. $g(x + t) = \lambda^{-d} f(\lambda x + \mu + \lambda t) = \sum_i \lambda^{i-d}(H_i f)(\lambda x + \mu)\, t^i$. □

Lemma 2.2 (triangular form)**.** *Let $f = \sum_{j=0}^{d} a_j x^{d-j}$ with $a_0 = 1$ and $f(0) = 0$, and let $\rho : \{1, \ldots, d-1\} \to R$ be a map into a set of roots of f with $H_i f(\rho(i)) = 0$. Then $a_d = 0$ and, for $1 \leq m \leq d - 1$,*

$$a_m = -\sum_{j=0}^{m-1} \binom{d-j}{m-j} a_j\, \theta^{m-j}, \qquad \theta = \rho(d-m).$$

In particular every coefficient of f lies in $\mathbb{Z}[R]$. This holds in every characteristic.

Proof. $H_{d-m} f(\theta) = \sum_{j=0}^{m} \binom{d-j}{d-m} a_j \theta^{m-j}$ and the coefficient of a_m is 1. □

Lemma 2.3 (descent)**.** *Let K be a perfect field of characteristic p, let $p^e \mid d$, and let $P \in K[x]$ be monic of degree d with* $\gcd(P, H_i P) \neq 1$ *for every i with $p^e \nmid i$. Then:*

1. *$P = Q^{p^e}$ for a unique monic $Q \in K[x]$ of degree d/p^e;*
2. *$H_{kp^e} P = (H_k Q)^{p^e}$ for all k, and $H_i P = 0$ if $p^e \nmid i$;*
3. *if P is a CA-polynomial, then Q is a CA-polynomial, every recycling set of P is a recycling set of Q, and* $\operatorname{type}(Q) \leq \operatorname{type}(P)$.

Proof. (1) This is the argument of [1, Prop. 2.6]. Write $P = \sum_j a_j x^{d-j}$ and assume $a_j = 0$ for all $j < m$ with $p^e \nmid j$, where $p^e \nmid m$. Then $H_{d-m} P = \sum_{j \leq m} \binom{d-j}{m-j} a_j x^{m-j}$. For $j < m$ with $a_j \neq 0$ we have $p^e \mid d-j$ and $p^e \nmid m-j$, so $p \mid \binom{d-j}{m-j}$ by Kummer's theorem (the lowest nonzero base-p digit of $m-j$ sits in a position below e, where $d-j$ has digit 0, so adding $m-j$ and $d-m$ produces a carry). Hence $H_{d-m} P = a_m$ is constant, and $\gcd(P, a_m) \neq 1$ forces $a_m = 0$. Thus P is a polynomial in x^{p^e}, and $P = Q^{p^e}$ since K is perfect. (2) $P(x + t) = Q(x + t)^{p^e} = \left(\sum_k H_k Q(x) t^k\right)^{p^e} = \sum_k (H_k Q(x))^{p^e} t^{kp^e}$. (3) By (2), $P(\theta) = H_{kp^e} P(\theta) = 0$ if and only if $Q(\theta) = H_k Q(\theta) = 0$. If $Q = (x - \alpha)^{d/p^e}$ then $P = (x - \alpha)^d$. □

3. Proof of Theorem 1.2

Let f be a CA-polynomial of degree d and type $\le k$ over a field of characteristic 0, with recycling set R, $2 \le |R| \le k+1$, and assignment ρ as in Lemma 2.2.

Step 1: algebraic coefficients. Fix two distinct elements θ_0, θ' of R. The coefficients of f, the elements of R and $(\theta_0-\theta')^{-1}$ generate a nonzero finitely generated $\mathbb{Q}$-algebra A, and the conditions $f(\theta) = 0$ ($\theta \in R$), $H_i f(\rho(i)) = 0$ are polynomial identities in A. A maximal ideal of A has residue field a number field; the induced specialization preserves these identities and $\theta_0 \neq \theta'$. We may therefore assume that f and R are defined over a number field L.

Step 2: integral model. Let $\mathfrak{p}$ be a prime of L above p, with valuation v and valuation ring $\mathcal{O}$. Choose $\theta_1 \in R \setminus \{\theta_0\}$ minimizing $v(\theta - \theta_0)$, put $\lambda = \theta_1 - \theta_0$ and $g(x) = \lambda^{-d} f(\lambda x + \theta_0)$. By Lemma 2.1, g is a CA-polynomial with recycling set $R' = (R-\theta_0)/\lambda \subset \mathcal{O}$, and $0, 1 \in R'$. By Lemma 2.2, applied to g, R' and the transported assignment, all coefficients of g lie in $\mathbb{Z}[R'] \subset \mathcal{O}$.

Step 3: reduction. Let $\bar{g} \in \overline{\mathbb{F}}_p[x]$ be the reduction. For each i, $\bar{g}$ and $H_i\bar{g} = \overline{H_i g}$ vanish at the reduction of $\rho'(i)$. Since $\bar{g}(0) = \bar{g}(1) = 0$, $\bar{g}$ is not a power of a linear polynomial. Thus $\bar{g}$ is a CA-polynomial of degree d over $\overline{\mathbb{F}}_p$ with a recycling set of at most $k+1$ elements.

Step 4: descent. By Lemma 2.3 with $p^e \mid d$, $\bar{g} = Q^{p^e}$ with Q a CA-polynomial of degree n and $\mathrm{type}(Q) \le \mathrm{type}(\bar{g}) \le k$, contrary to the hypothesis. □

4. Type at most two: the integer N_n

Fix $n \ge 3$. For $\sigma : \{1, \dots, n-1\} \to \{0,1,2\}$ with $\sigma(n-1) = 0$, let $F_\sigma = \sum_{m=0}^{n} a_m x^{n-m} \in \mathbb{Z}[y][x]$ be defined by $a_0 = 1$, $a_n = 0$ and the recursion of Lemma 2.2 with $\theta = 0, 1, y$ according as $\sigma(m) = 0, 1, 2$. Put

$$E_1^\sigma(y) = F_\sigma(1), \qquad E_2^\sigma(y) = F_\sigma(y).$$

For $\emptyset \neq S \subseteq \{1, \dots, n-2\}$ let $c_n(S) \in \mathbb{Z}$ be the value $F_\sigma(1)$ for $\sigma = \mathbf{1}_S$ (no label 2). By induction $\deg_y a_m \le m$, so $\deg E_2^\sigma \le n$.

Lemma 4.1. *The coefficient of y^n in E_2^σ is $c_n(\sigma^{-1}(2))$, and $E_1^\sigma(0) = c_n(\sigma^{-1}(1))$. If σ' is obtained from σ by exchanging the labels 1 and 2, then $E_1^\sigma(y) = y^n E_2^{\sigma'}(1/y)$ and $E_2^\sigma(y) = y^n E_1^{\sigma'}(1/y)$.*

Proof. Put $b_m(u) = u^m a_m(1/u) \in \mathbb{Z}[u]$. Multiplying the recursion for a_m at $y = 1/u$ by u^m gives $b_m = -\sum_{j<m} \binom{n-j}{m-j} b_j\,(u\theta)^{m-j}$ with $u\theta = 0, u, 1$ for the labels $0, 1, 2$ of σ; this is the recursion of $F_{\sigma'}$ at parameter u. Hence $E_2^\sigma(y) = \sum_m a_m(y) y^{n-m} = y^n \sum_m b_m(1/y) = y^n E_1^{\sigma'}(1/y)$ and $E_1^\sigma(y) = \sum_m a_m(y) = y^n \sum_m b_m(1/y) y^{m-n} = y^n E_2^{\sigma'}(1/y)$. At $u = 0$ the positions labelled 1 in σ are served by 0 and those labelled 2 by 1, so $[y^n]E_2^\sigma = \sum_m b_m(0) = c_n(\sigma^{-1}(2))$. Similarly $E_1^\sigma(0)$ is the value at $x = 1$ of the recursion in which label 2 is served by 0, that is $c_n(\sigma^{-1}(1))$. □

Since $c_n(S) \neq 0$ for all S ([2, §2.2], [6]), E_2^σ has degree exactly n. Let Σ_n be the set of σ using both labels 1 and 2, and define

$$N_n = \prod_{\emptyset \neq S \subseteq \{1,\dots,n-2\}} c_n(S) \cdot \prod_{\sigma \in \Sigma_n} \mathrm{Res}_y\big(E_1^\sigma, E_2^\sigma\big) \in \mathbb{Z}.$$

Proposition 4.2. *Let p be a prime. There is a CA-polynomial of degree n and type at most 2 over $\overline{\mathbb{F}}_p$ if and only if $p \mid N_n$.*

Proof. Let P be such a polynomial with a minimal recycling set R and assignment ρ. Since $P(\theta_0) = P'(\theta_0) = 0$ for $\theta_0 = \rho(1)$, choose $\theta_1 \in R \setminus \{\theta_0\}$ and apply Lemma 2.1 with $\mu = \theta_0$, $\lambda = \theta_1 - \theta_0$. Now $R = \{0,1\}$ or $R = \{0,1,z\}$ with $z \notin \{0,1\}$, and $\rho(1) = 0$. Let $\sigma(m) \in \{0,1,2\}$ be the label of $\rho(n-m)$ (with $0, 1, z$ labelled $0, 1, 2$); then $\sigma(n-1) = 0$ and, by Lemma 2.2, $P = F_\sigma \bmod p$ evaluated at $y = z$.

If p divides some $c_n(S)$, then $p \mid N_n$; assume not. If $R = \{0,1\}$, then $S = \sigma^{-1}(1) \neq \emptyset$ (otherwise $P = x^n$) and $0 = P(1) \equiv c_n(S)$, a contradiction. If $R = \{0,1,z\}$, minimality gives $\sigma \in \Sigma_n$, and z is a common root of $\bar{E}_1^\sigma, \bar{E}_2^\sigma$. Since $p \nmid c_n(\sigma^{-1}(2)) = \mathrm{lc}(E_2^\sigma)$, we have $\mathrm{Res}(E_1^\sigma, E_2^\sigma) \equiv \pm \mathrm{lc}(E_2^\sigma)^\delta \mathrm{Res}(\bar{E}_1^\sigma, \bar{E}_2^\sigma) \equiv 0 \pmod p$ for some $\delta \geq 0$ (and $\mathrm{Res}(E_1^\sigma, E_2^\sigma) \equiv 0$ directly if $\bar{E}_1^\sigma = 0$). Hence $p \mid N_n$.

Conversely, if $p \mid c_n(S)$ for some S, then $F_{\mathbf{1}_S} \bmod p$ satisfies all the conditions with recycling set $\{0,1\}$ and has the roots $0 \neq 1$, so it is a CA-polynomial of type 1. If $p \mid \mathrm{Res}(E_1^\sigma, E_2^\sigma)$ and $p \mid \mathrm{lc}(E_2^\sigma) = c_n(\sigma^{-1}(2))$, the previous case applies. If $p \mid \mathrm{Res}(E_1^\sigma, E_2^\sigma)$ and $p \nmid \mathrm{lc}(E_2^\sigma)$, then $\bar{E}_1^\sigma, \bar{E}_2^\sigma$ have a common root $z \in \overline{\mathbb{F}}_p$ (or $\bar{E}_1^\sigma = 0$ and z is any root of $\bar{E}_2^\sigma$), and $F_\sigma(z) \bmod p$ is a CA-polynomial with recycling set $\{0,1,z\}$. □

Proposition 4.3. *For $3 \leq n \leq 20$, $N_n \neq 0$ and $q = 2^{31} - 1$ does not divide N_n. Moreover N_{21}, N_{22} and N_{24} are nonzero.*

Verification. For $n \leq 20$ and all S, $c_n(S)$ was computed exactly; none is 0 or divisible by q (for $n = 20$ these are $2^{18} - 1$ values). For every n one has $c_n(S) \neq 0$ [2, §2.2], [6], which is all that is used below for $n = 21, 22, 24$. For every $\sigma \in \Sigma_n$ whose first nonzero label is 1, it was checked that $\gcd(\bar{E}_1^\sigma, \bar{E}_2^\sigma) = 1$ in $\mathbb{F}_q[y]$; as $q \nmid \mathrm{lc}(E_2^\sigma) = c_n(\sigma^{-1}(2))$ (by the values above for $n \leq 20$, and checked for each such σ for $n \geq 21$), this gives $q \nmid \mathrm{Res}(E_1^\sigma, E_2^\sigma)$. Every $\sigma \in \Sigma_n$ is of this form or is τ' for such a τ. In the latter case, a common root ζ of $\bar{E}_1^\sigma, \bar{E}_2^\sigma$ would satisfy $\zeta \neq 0$, since $\bar{E}_1^\sigma(0) = c_n(\sigma^{-1}(1)) \not\equiv 0$, and then $1/\zeta$ would be a common root for τ by Lemma 4.1; so again $q \nmid \mathrm{Res}(E_1^\sigma, E_2^\sigma)$. The number of such σ is $(3^{n-2} - 2^{n-1} + 1)/2$; for $n = 20, 21, 22, 24$ it is 193 448 101, 580 606 446, 1 742 343 625 and 15 686 335 501. For $n = 21$ the gcd condition modulo q holds for all of them; for $n = 22$ and $n = 24$ it holds except for three and five maps σ respectively, listed in the ancillary files; for each of these, $\gcd(\bar{E}_1^\sigma, \bar{E}_2^\sigma) = 1$ modulo $10^9 + 7$, which does not divide $\mathrm{lc}(E_2^\sigma)$, so again $\mathrm{Res}(E_1^\sigma, E_2^\sigma) \neq 0$; for $n = 21, 22, 24$ the reflected maps are handled as above with $\mathbb{C}$ in place of $\overline{\mathbb{F}}_q$, using only $c_n(S) \neq 0$ for all S. The computation was done with two implementations of the same algorithm, in Python and in C; the ancillary file `verify_ca_type.py` repeats it for $n \leq 12$ together with all checks of Section 5, and `run_t2f.py`, which compiles and runs a C program, covers $n \leq 22$ and $n = 24$. □

Remark 4.4. For $n = 20$ and $n = 24$ the certificate covers all 3^{n-2} maps σ (half of Σ_n directly, the other half by Lemma 4.1, and the maps without label 2 through the values $c_n(S)$), including those with $\sigma(1) = 0$, i.e. those where the root of $H_{n-1}f$ (the barycentre of the roots) is the multiple root. The enumeration of [7, Thm. 7.10] is carried out with $y_{n-1} = 1$.

5. Proof of Theorem 1.3 and explicit families

Theorem 1.3 follows from Theorem 1.2 with $k = 2$, Proposition 4.2 and Proposition 4.3.

For a given prime p, deciding whether $p \mid N_n$ is a computation over $\mathbb{F}_p$: one checks $p \nmid c_n(S)$ for all S and $\gcd(\bar{E}_1^\sigma, \bar{E}_2^\sigma) = 1$ for all $\sigma \in \Sigma_n$. By Proposition 4.2 every prime divisor of N_n lies in $B(n)$; for $n = 5, 6$ the prime divisors of N_n up to $3 \cdot 10^4$ are indeed elements of the published lists, and the primes $p_0(7), p_0(8), p_0(9), p_0(10) = 127, 419, 941, 3803$ of [2, Table 2], which lie outside $B(n)$, do not divide N_n, as they must. Running the test on the known elements of $B(n)$ gives Table 1; for $n = 8, 9, 10$ these are the primes $n < p < p_0(n)$, and the witnesses of Table 2. The row $n = 7$, and the part of the row $n = 8$ beyond $p_0(8)$, contain only primes for which Table 2 gives a witness; they are not exhaustive.

Each polynomial $f \in \mathbb{F}_p[x]$ of Table 2 (degree $n = 7$ or 8) shares a root with $H_i f$ for $1 \leq i \leq n - 1$ and has at least four distinct roots in $\mathbb{F}_p$, so it is a CA-polynomial and $p \in B(n)$. By Proposition 4.2 and Table 1, none of these primes admits a CA-polynomial of degree n and type at most 2; the witnesses have recycling sets $\{0, 1, y, w\}$ with $y, w \in \mathbb{F}_p$.

n	primes $p \in B(n)$ with $p \nmid N_n$	source of $p \in B(n)$
5	8009	[3, 2]
6	$983, 1087, 1187, 1901, 2287, 3877, 4943, 6983, 15131, 150203, 266587,$ $547061, 685177, 885061, 17250187, 9348983563, 70016757407,$ $2610767527031, 225833117528659, 7390044713023799, 51313000813080529$	[2]
7	$53, 101, 131, 163, 191, 229, 317, 331, 359, 419, 433, 509, 569$	Table 2
8	$167, 211, 251, 281, 293, 347, 373, 397$	[2, Table 2]
	$421, 433, 439, 509, 541, 571, 587, 593, 599$	Table 2
9	$439, 463, 521, 557, 593, 613, 661, 677, 709, 739, 757,$ $769, 787, 811, 887, 919$	[2, Table 2]
10	103 primes $919 \le p \le 3761$, listed in the ancillary files	[2, Table 2]
20	all $p \nmid 20N_{20}$, e.g. $p = 2^{31} - 1$	(20 is open)
24	all $p \nmid 24N_{24}$	(24 is open)

TABLE 1. Degrees np^e ($e \ge 1$) in which every characteristic-0 CA-polynomial has type ≥ 3.

For the degrees in Table 1 the conjecture is not covered by the method of [1, 4], which needs a prime r with $d = n'r^{e'}$, $r \nmid n'$, and no CA-polynomial of degree n' over $\overline{\mathbb{F}}_r$. If $r \nmid n'$ and $n' > r$, there is such a CA-polynomial: write $n' = \sum_j n'_j r^j$ in base r, let $m = n'_h r^h$ be its leading term, so that $1 \le n' - m$ because $n'_0 \ne 0$, and put $f = x^{n'-m}(x^m - 1) = x^{n'} - x^{n'-m}$. Then $H_i f = \binom{n'}{i} x^{n'-i} - \binom{n'-m}{i} x^{n'-m-i}$ vanishes at 0 for $i \ne n'-m$, while $H_{n'-m} f = \binom{n'}{m} x^m - 1 \equiv x^m - 1$ by Lucas' theorem vanishes at the root 1 of f. In every row $p > n$: for $n \in \{20, 24\}$ this holds because a prime $p < n$ with $p \nmid n$ divides N_n by the construction just given and Proposition 4.2. If $r \nmid d$ (that is, $e' = 0$ and $n' = d$), the same construction applies when $r < d$, while a prime $r > d$ would require deciding the absence of CA-polynomials of degree d itself over $\overline{\mathbb{F}}_r$, which we are not aware of for these degrees. For $d = np^e$ ($e \ge 1$) as in the table, every prime $r \ne p$ dividing d divides $n < p$, so its cofactor n' satisfies $r \nmid n'$ and $n' \ge p^e > r$; and for $r = p$ the cofactor is n with $p \in B(n)$, or $n \in \{20, 24\}$, where the absence of CA-polynomials of degree n in characteristic p is not known.

6. Type at least four

Theorem 1.2 holds for every k. For $k = 3$ its hypothesis in degree n and characteristic p, with $p \nmid N_n$, reduces to the absence of CA-polynomials of type exactly 3. As in Proposition 4.2, such a polynomial can be normalized to have the recycling set $\{0, 1, y, w\}$, with 0 serving H_1 and with the labels $1, 2, 3$ of the roots $1, y, w$ in order of first appearance along $m = 1, \dots, n-2$. Lemma 2.2 gives $F_\sigma \in \mathbb{Z}[y, w][x]$ for each such labelling σ, and the polynomial exists if and only if, for some σ, the three polynomials

$$A_\sigma = F_\sigma(1), \qquad B_\sigma = F_\sigma(y), \qquad C_\sigma = F_\sigma(w)$$

have a common zero in $\overline{\mathbb{F}}_p^2$; any such zero gives a CA-polynomial of type at most 3, since its roots $0, 1$ are distinct. The number of maps σ is 10, 350, 1701 and 7770 for $n = 6, 8, 9, 10$.

Proposition 6.1. *For the pairs (n, p) with $n = 6$, $p \in \{983, 1901, 51313000813080529\}$; $n = 8$, $p = 397$; $n = 9$, $p \in \{613, 757\}$; $n = 10$, $p \in \{1667, 1933, 2053, 2549, 2621, 2683, 2957, 3167, 3221, 3229, 3313, 3449, 3697\}$, there is no CA-polynomial of degree n and type at most 3 over $\overline{\mathbb{F}}_p$.*

n	p	CA-polynomial of degree n over $\mathbb{F}_p$
7	53	$x^7 + 46x^6 + 51x^4 + 15x^3 + 46x^2$
7	101	$x^7 + 94x^6 + 12x^5 + 5x^4 + 23x^3 + 67x^2$
7	131	$x^7 + 110x^5 + 43x^4 + 111x^3 + 128x^2$
7	163	$x^7 + 156x^6 + 41x^5 + 28x^4 + 72x^3 + 28x^2$
7	191	$x^7 + 184x^6 + 24x^5 + 164x^4 + 189x^3 + 11x^2$
7	229	$x^7 + 222x^6 + 153x^4 + 82x^3$
7	317	$x^7 + 310x^6 + 143x^5 + 140x^4 + 40x^2$
7	331	$x^7 + 324x^6 + 168x^5 + 169x^2$
7	359	$x^7 + 352x^6 + 75x^5 + 331x^4 + 318x^3$
7	419	$x^7 + 398x^5 + 137x^4 + 272x^3 + 30x^2$
7	433	$x^7 + 426x^6 + 226x^5 + 213x^4$
7	509	$x^7 + 502x^6 + 191x^4 + 145x^3 + 179x^2$
7	569	$x^7 + 562x^6 + 568x^5 + 135x^4 + 441x^2$
8	167	$x^8 + 159x^7 + 48x^6 + 121x^5 + 58x^3 + 114x^2$
8	211	$x^8 + 203x^7 + 112x^5 + 155x^4 + 79x^3 + 83x^2$
8	251	$x^8 + 243x^7 + 186x^6 + 181x^4 + 47x^3 + 95x^2$
8	281	$x^8 + 273x^7 + 85x^5 + 38x^4 + 151x^3 + 14x^2$
8	293	$x^8 + 285x^7 + 183x^6 + 201x^5 + 124x^4 + 211x^3 + 167x^2$
8	347	$x^8 + 339x^7 + 241x^6 + 74x^5 + 42x^4 + 344x^3$
8	373	$x^8 + 365x^7 + 46x^5 + 300x^4 + 34x^2$
8	421	$x^8 + 413x^7 + 28x^6 + 314x^5 + 403x^4 + 212x^3 + 313x^2$
8	433	$x^8 + 425x^7 + 43x^6 + 122x^5 + 44x^3 + 231x^2$
8	439	$x^8 + 431x^7 + 254x^5 + 257x^4 + 168x^3 + 206x^2$
8	509	$x^8 + 501x^7 + 237x^6 + 65x^3 + 214x^2$
8	541	$x^8 + 485x^5 + 174x^4 + 422x^2$
8	571	$x^8 + 563x^7 + 546x^5 + 373x^4 + 124x^3 + 106x^2$
8	587	$x^8 + 579x^7 + 167x^6 + 355x^5 + 74x^4 + 499x^3 + 86x^2$
8	593	$x^8 + 585x^7 + 402x^6 + 198x^4$
8	599	$x^8 + 591x^7 + 429x^6 + 440x^5 + 168x^3 + 168x^2$

TABLE 2. Witnesses for $p \in B(7)$ and $p \in B(8)$.

Verification. Type at most 2 is excluded by $p \nmid N_n$ (Section 5). For every σ,

$$\gcd\big(\mathrm{Res}_w(A_\sigma, C_\sigma), \mathrm{Res}_w(B_\sigma, C_\sigma)\big) = 1 \text{ in } \mathbb{F}_p[y] \quad \text{or}$$
$$\gcd\big(\mathrm{Res}_y(A_\sigma, B_\sigma), \mathrm{Res}_y(C_\sigma, B_\sigma)\big) = 1 \text{ in } \mathbb{F}_p[w];$$

since a common zero (y_0, w_0) makes y_0 a common root of the first two resultants and w_0 of the last two, no σ admits a common zero. Independently, for $n \leq 9$ and for $n = 10$ with $p \in \{1667, 3697\}$, a Gröbner basis of $(A_\sigma, B_\sigma, C_\sigma)$ over $\mathbb{F}_p$ was computed for every σ and found to be $\{1\}$. For the other primes of the row $n = 10$ only the resultant certificate was computed; the same program, run on the 90 other primes of that row, found the common zeros confirmed by Gröbner bases. For $n = 6$ and $n = 8$ the resultant certificate is repeated by the ancillary file `verify_type4.py`, and for $n = 9, 10$ by `type3_check.py`, which requires `sympy`. □

Corollary 6.2. *For the pairs (n, p) of Proposition 6.1 and every $e \geq 0$, every CA-polynomial of degree np^e in characteristic 0 has type at least 4, that is, at least five recycled roots.*

All these primes lie in $B(n)$ ([2, Table 1] for $n = 6$, [2, Table 2] for $n = 8, 9, 10$), so CA-polynomials of type at least 4 exist in these characteristics. For $n = 6$ this is confirmed directly: a CA-polynomial of degree 6 and type 4 has a double root and four simple roots, each serving

exactly one of $H_2, \ldots, H_5$, and Table 3 gives one for each of the three primes, with five distinct recycled roots in $\mathbb{F}_p$.

p	CA-polynomial of degree 6 and type 4 over $\mathbb{F}_p$ (recycled roots)
983	$x^6 + 977x^5 + 804x^4 + 241x^3 + 926x^2$ $\quad (0, 1, 13, 549, 426)$
1901	$x^6 + 1895x^5 + 1782x^4 + 1698x^3 + 327x^2$ $\quad (0, 1, 564, 428, 914)$
51313000813080529	$x^6 + 51313000813080523x^5 + 48712599420079589x^4$ $+35570669974212077x^3 + 18342732231869397x^2$ $(0,\ 1,\ 14982068566704741,\ 28063784095573572,\ 8267148150802221)$

TABLE 3. CA-polynomials of type 4 in degree 6.

For the 18 other primes of the row $n = 6$ of Table 1 (by Gröbner bases) and for the other primes of the rows $n = 7, 8$ (Table 2), CA-polynomials of type 3 exist over $\overline{\mathbb{F}}_p$. For the other 14 primes of the row $n = 9$ the resultant certificate fails; we have not decided whether CA-polynomials of type 3 exist there. For the other 90 primes of the row $n = 10$ a common zero exists for some σ, so CA-polynomials of type 3 exist.

REFERENCES

[1] H.-C. Graf von Bothmer, O. Labs, J. Schicho, C. van de Woestijne, *The Casas-Alvero conjecture for infinitely many degrees*, J. Algebra 316 (2007), 224–230.

[2] W. Castryck, R. Laterveer, M. Ounaïes, *Constraints on counterexamples to the Casas-Alvero conjecture and a verification in degree 12*, Math. Comp. 83 (2014), 3017–3037.

[3] M. Chellali, A. Salinier, *La conjecture de Casas Alvero pour les degrés* $5p^e$, An. Univ. Dunărea de Jos Galaţi Fasc. II 4(35) (2012), 54–62.

[4] J. Draisma, J. P. de Jong, *On the Casas-Alvero conjecture*, Eur. Math. Soc. Newsl. 80 (2011), 29–33.

[5] S. Ghosh, *Proof of the Casas-Alvero conjecture*, arXiv:2501.09272v2.

[6] M. F. Marashdeh, *A descent-set obstruction for the Casas-Alvero conjecture*, arXiv:2608.14726.

[7] C. Massri, *The Casas-Alvero conjecture for three recycled roots in degree 20*, arXiv:1806.09561.

[8] D. Schaub, M. Spivakovsky, *A description of and an upper bound on the set of bad primes in the study of the Casas-Alvero conjecture*, arXiv:2411.13967.