ON THE CASAS-ALVERO CONJECTURE

JAN DRAISMA

1. The problem

Eduardo Casas-Alvero conjectured the following.

Conjecture 1.1. *Let K be a field of characteristic 0 and let $f \in K[x]$ be a monic polynomial of degree n. Suppose that $\gcd(f, f^{(k)}) \neq 1$ for all $k = 1, \ldots, n-1$. Then there exists an $\alpha \in K$ with $f = (x-\alpha)^n$.*

Example 1.2. Let $K = \mathbb{C}$. By Gauss-Lucas, the zeroes of f' lie in the convex hull of the zeroes of f—and, apart possibly from double zeroes of f, in the relative interior of that convex hull. This readily proves the conjecture for $n = (1), 2, 3, 4$. For f with only real zeroes, also $n = 5$ is easily settled this way. For higher degrees, it is not at all clear—but there might well be a "mechanical" proof for the real/complex case!

Clearly the statement of the conjecture is false for $\operatorname{char} K = p$: any polynomial in which only p-th powers appear has zero derivatives, while not necessarily being a power of a linear polynomial. Therefore, for

$$f := x^n + s_1 x^{n-1} + \ldots + s_{n-1}x + s_n$$

let

$$f_k := \binom{n}{k} x^{n-k} + \binom{n-1}{k} s_1 x^{n-k-1} + \ldots + \binom{k}{k} s_k x^0$$

be the *Hasse derivative* and let, for any field K (not necessarily of characteristic 0), $\mathrm{CA}(n, K)$ be the following statement:

> Any monic polynomial $f \in K[x]$ of degree n for which $\gcd(f, f_k) \neq 1$ for all $k = 1, \ldots, n-1$ is of the form $(x-\alpha)^n$ for some $\alpha \in \overline{K}$.

Observations:

(1) If $\operatorname{char} K = 0$, then $\mathrm{CA}(n, K)$ is equivalent to the conjecture above. Indeed, if $f = (x-\alpha)^n$, then α in K. (This is not true, e.g., for $f = x^p - t \in \mathbb{F}_p(t)$.)
(2) $\mathrm{CA}(n, \overline{K}) \Rightarrow \mathrm{CA}(n, K)$. This is trivial.
(3) If f satisfies the assumptions for $\mathrm{CA}(n, K)$, then for all $\alpha \in K$ the polynomial $f(x-\alpha)$ also satisfies the assumptions for $\mathrm{CA}(n, K)$, and for all $\beta \in K^*$ the polynomial $\beta^n f(x/\beta)$ also satisfies the assumptions.

We from now on assume that K is algebraically closed. The following examples show that $\mathrm{CA}(n, K)$ is, in general, false in characteristic p.

Example 1.3. Let K be of characteristic p and let $f = x^{p+1} - x^p$. Then f and f_k both have 0 as a zero for $k = 1, \ldots, p-1$, while $f_p = x - 1$ and f share the zero 1.

There are less obvious examples, as well.

Date: Eindhoven, 14 June 2006.

So if $\operatorname{char} K = p$, then there exist n for which $\mathrm{CA}(n, K)$ is not true. However, the followin proposition says that there also exist n for which $\mathrm{CA}(n, K)$ *is* true.

Proposition 1.4 (Hans-Christian Graf Von Bothmer, Oliver Labs, Josef Schicho, Christiaan van de Woestijne, `math.AC/0605090`)**.** *Suppose that* $\operatorname{char} K = p$*. Then* $\mathrm{CA}(p^e, K)$ *is true for all* $e \in \mathbb{N}$*.*

This needs the following lemma.

Lemma 1.5 (Kummer)**.** *Suppose that* $p^e | n$ *and* $p^e \not| k$*. Then* $\binom{n}{k} \cong 0 \mod p$*.*

Proof of the Proposition. By the lemma $\binom{p^e}{k} = 0$ in K for $k = 1, \ldots, p^e$. Now suppose that $f \in K[x]$ is of degree $n := p^e$ satisfies the assumptions for $\mathrm{CA}(n, K)$. Then in particular

$$f_{n-1} = \binom{p^e}{p^e - 1} x - s_1 = s_1.$$

If this constant polynomial is to have a zero in common with f, s_1 better be 0. But then consider

$$f_{n-2} = \binom{p^e}{p^e - 2} x^2 - s_2 = s_2.$$

Again, we find that $s_2 = 0$. Continuing this way, we find that $s_1 = \ldots = s_{n-1} = 0$, so that $f = x^n + s_2$. But this is a p^e-th power in $\overline{K}[x]$. □

Let us reformulate $\mathrm{CA}(n, K)$ in terms of polynomials. First note that we may restrict ourselves to f's with a zero at 0, i.e., with $s_n = 0$. For such f we have to prove that the assumptions of $\mathrm{CA}(n, K)$ imply $f = x^n$, i.e., that $s_1, \ldots, s_{n-1}$ are zero. For $k = 1, \ldots, n-1$ let R_k be the resultant of f with f_k. Thus R_k is a polynomial in the s_i with coefficients in $\mathbb{Z}$ that vanishes if and only if f has a common zero with f_k. More precisely, denote by $X(K, n)$ the variety of all $(s_1, \ldots, s_{n-1}) \in K^{n-1}$ on which all of the R_k vanish. Note that if $(s_1, \ldots, s_{n-1}) \in X(K, n)$, then also $(\lambda^i s_i)_i \in X(K, n)$ for $\lambda \in K$. Now

$$\mathrm{CA}(K, n) \equiv X(K, n) = \{0\},$$

and can prove the following theorem.

Theorem 1.6 (Same authors, same paper)**.** *If* $\operatorname{char} K = 0$*, then* $\mathrm{CA}(K, p^e)$ *for all primes* p *and all exponents* $e \in \mathbb{N}$*.*

Proof. Suppose, on the contrary, that $X(K, p^e) \neq \{0\}$, and let $s = (s_1, \ldots, s_{n-1})$ be a non-zero element of $X(K, p^e)$. Recall that we can extend the p-adic valuation $v : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ to $v : K \to \mathbb{Z} \cup \{\infty\}$, let O be the subring of K where v is non-negative, and let M be the maximal ideal of O. Hence O/M is a field of characteristic p. Replacing s by $(\lambda^i s_i)$ for some $\lambda \in K^*$ ensures that the s_i all lie in O, and at least one of them does not lie in M. (Indeed, take λ such that $\min_i v(s_i) + iv(\lambda) = 0$.) But then the image of $(s_1, \ldots, s_{n-1})$ in $(O/M)^{n-1}$ is still a (non-zero) zero of all R_k, hence we obtain a counterexample to $\mathrm{CA}(O/M, p^e)$—but the Proposition rules this out. □

A similar proof can be given for the case where $n = 2p^e$, so that $\mathrm{CA}(K, n)$ is true in char. 0 for degrees 1 through 11.

But this does, of course, not settle the conjecture! I would like to end with some ideas for a solution. Let K be of char. 0, and let I be the ideal in $K[s_1, \ldots, s_{n-1}]$ generated by the R_k, so that $X(K, n)$ is the zero set of I.

Lemma 1.7. *T.F.A.E.:*

(1) $\mathrm{CA}(K,n)$,
(2) $X(K,n)=\{0\}$,
(3) *for all* $i=1,\dots,n-1$, *some power of* s_i *lies in* I,
(4) $A:=K[s_1,\dots,s_{n-1}]/I$ *is a finite-dimensional vector space (algebra), and*
(5) *some power of* s_1 *lies in* I.

Proof. The equivalence of (2) and (3) follows from the Nullstellensatz. The implication (4) $\Rightarrow$ (3) follows from the fact that I is *homogeneous* relative to the grading where s_i has degree i (as the R_k are!). The implication (5)$\Rightarrow$(2) was observed by Aart Blokhuis: (5) should be read as "whenever a polynomial lies in $X(K,n)$ and α is a zero, then the sum of the differences of all other zeros with α is 0". From this one readily concludes that all zeroes are equal. □

In particular, one would like A to be finite-dimensional. No for some small n I have computed the Hilbert function of A, which is defined as follows: if $A=\sum_d A_d$, where $A_d=K[s_1,\dots,s_{n-1}]_d/I_d$ is the homogeneous part of degree d, then $H_A(t)=\sum_{d\in\mathbb{Z}}(\dim A_d)t^d$. In particular, we want to show that this is a polynomial. For n up to 6 the Hilbert function is actually equal to that of the quotient of $K[s_1,\dots,s_{n-1}]$ by the ideal I' generated by the s_k^n for $k=1,\dots,n-1$—which is obviously polynomial!

Conjecture 1.8. $H_A(t)=H_{K[s_1,\dots,s_{n-1}]/J'}(t)$.

Note that R_k contains a term s_{n-k}^n. So this conjecture suggests that some kind of deformation of I might yield I'—not a toric deformation, though: the R_k do not seem to form a Gröbner basis with respect to any order.