On the Casas-Alvero Conjecture and its proof

Soham Ghosh

University of Washington
(UW)

(05/02/25)

Birational Geometry Seminar 2025
UCLA

Conjecture (Casas-Alvero, 2001):

Let k be an alg. closed field of char 0.
If $f(X) \in k[X]$ is monic of deg n s.t
$\gcd(f, f^{(i)}) \neq 1 \;\; \forall\, 1 \leq i \leq n-1$, where
$f^{(i)}(X) :=$ i^{th} formal derivative wrt X, then
$f(X) = (X-\alpha)^n$ for some $\alpha \in k$.

$\gcd(f, f^{(i)}) \neq 1 \;\; \forall\, 1 \leq i \leq j < n-1$
$\implies f$ has a root of order $\geq (j+1)$.

E.g. $f(x) = x^2(x-1)(x-2/3)$.
$\gcd(f, f^{(1)}) \neq 1$ and $\gcd(f, f^{(2)}) \neq 1$.

Over char $p>0$: Conjecture can be formulated using Hasse-Schmidt derivatives f_i in place of $f^{(i)}$. Then known that conjecture fails in char $p>0$: counterexample is $X^{p+1} - X^p$.

§1: Existing approaches and results:

(A) von Bothmer - Labs - Schicho - de Woestijne (2007)

- $P(X) := X^n + a_1 X^{n-1} + a_2 X^{n-2} + \cdots + a_{n-1} X$
  $\in \mathbb{Z}[a_1, \ldots, a_{n-1}][X]$ be a generic degree n monic poly with one of the roots $= 0$.

  $P_i(X) :=$ i^{th} Hasse-Schmidt derivative of P.
  $(1 \le i \le n-1)$

- Assign weight j to the variable a_j.

- $\gcd(P, P_i) \neq 1 \iff \underbrace{\mathrm{Res}_X(P(X), P_i(X))}_{\substack{\text{weighted homogeneous} \\ \text{poly of deg } n(n-i) \\ \text{in } a_1, \ldots, a_{n-1}}} = 0$

- n^{th} Casas-Alvero scheme X_n is:

the weighted projective $\mathbb{Z}$- subscheme of $\mathbb{P}_{\mathbb{Z}}(1,2,\dots, n-1)$ defined by the weighted homogeneous ideal:

$$\mathcal{J}_n := \langle \mathrm{Res}_x(P, P_i) : 1 \leq i \leq n-1 \rangle$$
$$\triangle$$
$$\mathbb{Z}^{\omega}[a_1, \dots, a_{n-1}]$$

- Conjecture true $/k \iff X_n(k) = \phi$.

Since: True $/k \iff P(x)$ has $a_1 = \dots = a_{n-1} = 0$

- Structure morphism $\Phi_n : X_n \longrightarrow \mathrm{Spec}\,\mathbb{Z}$ is projective.

$$\implies \mathrm{Im}\,\Phi_n \subseteq \mathrm{Spec}\,\mathbb{Z} = \begin{cases} \text{finite} \\ \mathrm{Spec}\,\mathbb{Z} \end{cases}$$

- Conjecture true / char 0

$$\iff X_n(\overline{\mathbb{Q}}) = \emptyset$$

$$\iff X_n \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\mathbb{Q} = \emptyset$$

$$\iff \operatorname{Im}\phi_n \subseteq \operatorname{Spec}\mathbb{Z} \text{ finite.}$$

$$\Downarrow$$

- Mod p reduction strategy:

$X_n(\overline{\mathbb{F}}_p) = \emptyset \implies \operatorname{Im}\phi_n \subsetneq \operatorname{Spec}\mathbb{Z}$ finite.

- Proposition (BLSW '07): If $d = np^k$, p prime, $k > 0$ and $X_n(\overline{\mathbb{F}}_p) = \emptyset$, then $X_d(\overline{\mathbb{F}}_p) = \emptyset$.

- Corollary ('07): Conjecture true / char 0 if $d = p^k$ or $2p^k$ for primes p.

(B) Subsequent results:

- Theorem (Draisma, de Jong '11):
  Conjecture true / char 0 $\forall$ degrees $d = np^k$ where $n \in \{1, 2, 3, 4\}$ and prime $p > n$ s.t. $p \neq 5$ if $n = 3$ and $p \neq 7$ if $n = 4$.

- Several computational/partial results towards the conjecture as well as towards potential counterexamples by Castryck, Laterveer, Ounaies, Chellali ... since 2012.

- Theorem (Schaub-Spirakorsky '23):
  Let p be a prime and $p \mid \binom{n}{i} - 1$ for some $1 \leq i \leq n-1$, then $X_n(\overline{\mathbb{F}_p}) \neq \phi$.

- Definition: A prime p is a bad prime for n if $X_n(\overline{\mathbb{F}_p}) \neq \phi$.

§2: A Geometric Approach

(based on arXiv: 2402.18717)

$k :=$ alg. closed field (arbitrary char).

(A) Broad idea:

$$\nu_n : \underset{\text{root space}}{\mathbb{P}^{n-1}_k} \xrightarrow{\text{finite map}} \underset{\text{coefficient space}}{\mathbb{P}_k(1,2,3,\ldots,n-1,n)}$$

$$\bar{x} := (x_1, \ldots, x_n) \longmapsto (-e_1(\bar{x}), e_2(\bar{x}), \ldots, (-1)^n e_n(\bar{x}))$$

$e_i(\bar{x}) :=$ deg i elementary symmetric poly in $\bar{x} := x_1, \ldots, x_n$.

Include:

$$\underset{X_n(k)}{\mathbb{P}_k(1,2,\ldots,n-1)} \hookrightarrow \mathbb{P}_k(1,2,\ldots,n-1,n)$$

as the hyperplane $V(y_n)$ (coordinates on $\mathbb{P}_k(1,\ldots,n)$ being $y_1, \ldots, y_n$)

$$\boxed{\text{Thus: Understand } X_n(k) \text{ by studying } \nu_n^{-1}(X_n(k)).}$$

- Since $X_n(k) \subseteq V(y_n) \subset \mathbb{P}_k(1,2,\dots,n-1,n)$, $\forall\, [x_1:\dots:x_n] \in \nu_n^{-1}(X_n(k))$, must have $x_i = 0$ for some $1 \le i \le n$.

Suffices to fix $x_n = 0$, i.e. study

$$\boxed{\nu_n^{-1}(X_n(k)) \cap V(x_n)}$$

(since $\nu_n : \mathbb{P}^{n-1} \to \mathbb{P}(1,2,\dots,n)$ is S_n-invariant)

- Let $q : \mathbb{A}^n_k \longrightarrow \mathbb{P}^{n-1}_k$ be the usual map.

$$\boxed{\mathfrak{X}_n(k) := q^{-1}\left(\nu_n^{-1}(X_n(k)) \cap V(x_n)\right)}$$

(B) Description of $\mathcal{X}_n(k)$:

- **Definition ①**: $\forall\ 1 \le j \le n-1$, define

$$\phi_{j,n-1}^{i} : k[x_1,\dots,x_{n-1}] \to k[x_1,\dots,x_{n-1}]$$
$$x_i \longmapsto x_i - x_j \text{ if } i \neq j$$
$$x_j \longmapsto -x_j$$

and $\phi_{n,n-1} : k[x_1,\dots,x_{n-1}] \to k[x_1,\dots,x_{n-1}]$ to be the identity.

② $\forall\ 1 \le i \le n$, let i^{th} multivariate Hasse-Schmidt derivation be

$$HD_n^i : k[x_1,\dots,x_n] \to k[x_1,\dots,x_n],$$

defined as:

$$\boxed{HD_n^i\, x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} = \sum_{j_1+\dots+j_n = i} \binom{a_1}{j_1} \cdots \binom{a_n}{j_n} x_1^{a_1-j_1} \cdots x_n^{a_n-j_n}.}$$

Proposition 1:

$$\mathcal{X}_n(k) = \bigcup_{1 \le j_1, \dots, j_{n-1} \le n} \left(\bigcap_{i=1}^{n-1} V\left(\overset{\phi_{j_i, n-1}}{\overset{\|}{\phi_{j_i}}} \left(HD^{i-1}_{n-1}\, \mathscr{X}_{n-1} \right) \right) \right)$$

$$\subseteq \mathbb{A}^{n-1}_k \cong V(x_n) \subseteq \mathbb{A}^n_k .$$

where $\mathscr{X}_{n-1} := x_1 x_2 \cdots x_{n-1} \in k[x_1, \dots, x_{n-1}]$.

- **Remark**: $HD^{i-1}_{n-1}\, \mathscr{X}_{n-1} = e_{n-i}(x_1, \dots, x_{n-1})$

(deg $n-i$ elem. sym. poly in $x_1, \dots, x_{n-1}$).

Proof sketch: For $f(X) = \prod_{i=1}^{n} (X - \alpha_i)$, let

$$\mathcal{L}_{f, \underline{\alpha}} := \left\{ (\alpha_1 + \beta, \alpha_2 + \beta, \dots, \alpha_n + \beta) \in \mathbb{A}^n_k : \beta \in k \right\}.$$

choice of labelling of roots $\underline{\alpha} := (\alpha_1, \dots, \alpha_n)$.

Obtain:

$$\gcd(f, f_i) \ne 1 \iff \mathcal{L}_{f, \underline{\alpha}} \subseteq X^i_n(k)$$

$$\begin{tikzcd}
k[x_1, \dots, x_{n-1}] \arrow[r, "HD^{i-1}_{n-1}"] \arrow[d] & k[x_1, \dots, x_{n-1}] \arrow[d] \\
k[X] \arrow[r, "HD^i_1"] & k[X]
\end{tikzcd}$$

$$X_n^{\circ}(k) := p_n^{-1}\Big(\underbrace{\bigcup_{j=1}^{n-1} V(\phi_j(HD_{n-1}^{j-1} X_{n-1}))}_{\substack{\cap \\ V(x_n) \subseteq \mathbb{A}_k^n}}\Big)$$

where $p_n : \mathbb{A}^n_k \longrightarrow V(x_n)$ is the map

$(x_1, \dots, x_n) \mapsto (x_1 - x_n, x_2 - x_n, \dots, x_{n-1} - x_n, 0)$.

$\square$

If $f(x)$ is a counterexample.
Then so is $\frac{1}{a^n} f(aX+b)$.

Theorem 1: $|X_n(k)| < \infty$ for any field k.

Slogan: "almost finitely many" counterexamples to the Conjecture over any field k.

Immediate consequence: $\phi_n : X_n \longrightarrow \operatorname{Spec}\mathbb{Z}$ is finite. Thus, X_n is affine of dim ≤ 1.

Proof sketch of Theorem 1:

By Proposition 1, equivalent to:

- $\dim X_{j_1,\dots,j_{n-1}} \le 1$ for any $1 \le j_1, \dots, j_{n-1} \le n$

$$X_{j_1,\dots,j_{n-1}} = \operatorname{Spec} \frac{k[x_1,\dots,x_{n-1}]}{\left(\phi_{i,j_i}(HD^{i-1}_{n-1}\mathfrak{x}_{n-1}) : 1 \le i \le n-1\right)}.$$

- dim ≤ 1. dim=1 $\Longleftarrow$. dim 0

$$\begin{tikzcd}
X_{j_1\dots j_{n-1}} \arrow[r, hook] \arrow[d] & \mathfrak{X}_{j_1,\dots,j_{n-1}} \arrow[d] & \bigcap_{i=1}^{n-1} V(HD^{i-1}_{n-1}\mathfrak{x}_{n-1}). \arrow[l, hook'] \arrow[d] \\
\operatorname{Spec}\frac{k[T]}{(T-1)} \arrow[r, hook] & \mathbb{A}^1 & \operatorname{Spec}\frac{k[T]}{T} \arrow[l, hook']
\end{tikzcd}$$

- $$\mathfrak{X}_{j_1\dots j_{n-1}} = \operatorname{Spec} \frac{k[x_1,\dots,x_{n-1},T,\frac{1}{1-2T}]}{\left(H_{i,j_i}[T] : 1 \le i \le n-1\right)}$$

regular seq.

with $H_{i,j_i}[T] \bmod T = HD^{i-1}_{n-1}\mathfrak{x}_{n-1}$ $\forall 1 \le i \le n-1$.

$\square$

§3 Proof of conjecture / char 0:

(arxiv: 2501.09272)

- Conjecture in deg n $\iff$ $\{\phi_{j_i}(HD^{i-1}_{n-1} x_{n-1})\}_{i=1}^{n-1}$ being a regular seq. in $k[x_1, \ldots, x_{n-1}]$ $\forall\, 1 \leq j_1, \ldots, j_{n-1} \leq n$.

- **Proposition ②:**

Assuming in deg n

$\Updownarrow$

$\{\phi_{j_i, n-1}(HD^{i-1}_{n-1} x_{n-1})\}_{i=1}^{n-1}$ regular seq. in $k[x_1, \ldots, x_{n-1}]$ $\forall\, 1 \leq j_1, \ldots, j_{n-1} \leq n$

$$\Downarrow$$

$\{\phi_{j_i, n}(HD^{i-1}_{n} x_n)\}_{i=1}^{n-1}$ regular seq. in $k[x_1, \ldots, x_n]$ $\forall\, 1 \leq j_1, \ldots, j_{n-1} \leq n+1$.

Proof idea: Similar to that of Theorem ①, since leading coeff. of $HD^{i-1}_n x_n$ wrt x_n is $HD^{i-1}_{n-1} x_{n-1}$.

$\square$

- To complete proof by induction on deg n, need to show: (13)

$$\boxed{\phi_{j_n,n}(HD_n^{n-1}x_n) \text{ is a non-zero divisor in } \frac{k[x_1,\dots,x_{n-1},x_n]}{(\phi_{j_i,n}(HD_n^{i-1}x_n) : 1\le i\le n-1)} \text{ for all possible choices } 1\le j_1,\dots,j_n\le n+1.}$$

(*)

<u>Notation:</u> Fix a choice of indices $1\le j_1,\dots,j_n\le n+1$.

- Let $F_i := \phi_{j_i,n}(HD_n^{i-1}x_n) \in R_n := k[x_1,\dots,x_n]$

Can ensure $j_i \ne n \ \forall\, 1\le i\le n-1$.

- Let $\lambda_n : R_n = R_{n-1}[x_n] \longrightarrow R_{n-1}$ be leading coefficient function wrt x_n.

- Let $f_i := \lambda_n(F_i) = \begin{cases} \phi_{j_i,n-1}(HD_{n-1}^{i-1}x_{n-1}) & \text{if } j_i \ne n+1 \\ \phi_{n,n-1}(HD_{n-1}^{i-1}x_{n-1}) & \text{if } j_i = n+1 \end{cases}$

$(\forall\, 1\le i\le n-1)$

- $f_n := \lambda_n(F_n) = \begin{cases} 1 & \text{if } j_n \ne n. \\ -n & \text{if } j_n = n. \end{cases}$

- Truncated Koszul complex for $F_1, \dots, F_{n-1} \in R_n$

i) $\hat{K}^n(j_1, \dots, j_{n-1})_\bullet$:

$$0 \to \Lambda^2 R_n^{\oplus n-1} \xrightarrow{d_{n,2}} R_n^{\oplus n-1} \xrightarrow[(F_1, \dots, F_{n-1})]{d_{n,1}} R_n \to 0$$

filter by deg wrt x_n:
($\because F_i$ linear in x_n)

ii) $\hat{K}^n_k(j_1, \dots, j_{n-1})_\bullet$: (complex of R_{n-1}-modules)

$$0 \to \Lambda^2 R_{n-1}[x_n]^{\oplus n-1}_{k-2} \to R_{n-1}[x_n]^{\oplus n-1}_{k-1} \to \underset{\substack{\parallel \\ \deg_{x_n} \leq k.}}{R_{n-1}[x_n]_k} \to 0$$

$\forall\, k \geq 1$.

iii) $\underset{\substack{\parallel \\ \text{truncated Koszul complex of } f_1, \dots, f_{n-1}.}}{\hat{K}^{n-1}(j_1, \dots, j_{n-1})_\bullet}$: $0 \to \Lambda^2 R_{n-1}^{\oplus n-1} \xrightarrow{d_{n-1,2}} R_{n-1}^{\oplus n-1} \xrightarrow{d_{n-1,1}} R_{n-1} \to 0$

iv) $\underline{\hat{K}^n_\circ(j_1,\dots,j_{n-1})_\bullet}$:

$$0 \longrightarrow 0 \longrightarrow M \xrightarrow{d_{n,1}} R_{n-1}[x_n]_0 \longrightarrow 0,$$

where $M := \operatorname{Im}\left(\Lambda^2 R_{n-1}^{\oplus n-1} \xrightarrow[d_{n-1,2}]{} R_{n-1}^{\oplus n-1}\right)$

- Obtain s.e.s of complexes $\forall k \geq 2$:

$$\boxed{0 \to \hat{K}^n_{k-1,\bullet} \longrightarrow \hat{K}^n_{k,\bullet} \xrightarrow{\Lambda_k} \hat{K}^{n-1}_\bullet \longrightarrow 0} \quad (A)$$

where Λ_k is induced by the maps

$$\Lambda_{n,k} : R_{n-1}[x_n]_k \longrightarrow R_{n-1}$$

mapping to coeff of x_n^k.

<u>For $k=1$:</u> Have s.e.s:

$$\boxed{0 \to \hat{K}^n_{0,\bullet} \xrightarrow{i_1} \hat{K}^n_{1,\bullet} \longrightarrow \operatorname{coker} i_{1\,\bullet} \to 0} \quad (A')$$

- Apply homology l.e.s to (A):

$$\boxed{0 \to H_0(\hat{K}^n_{k-1,\bullet}) \to H_0(\hat{K}^n_{k,\bullet}) \to H_0(\hat{K}^{n-1}_\bullet) \to 0}$$

$\forall\, k \geq 2$ (B)

($\because H_1(\hat{K}^{n-1}_\bullet) = 0$ by regularity assumption of $f_1, \dots, f_{n-1} \in R_{n-1}$.)

Apply homology l.e.s to (A'): gives (B) for $k=1$, since $H_0(\operatorname{coker} i_1) = H_0(\hat{K}^{n-1}_\bullet)$ and $H_1(\operatorname{coker} i_1) = 0$.

- Obtain filtration of R_{n-1}-modules:

$$\boxed{H_0(\hat{K}^n_{0,\bullet}) \subset H_0(\hat{K}^n_{1,\bullet}) \subset H_0(\hat{K}^n_{2,\bullet}) \subset \cdots \subset H_0(\hat{K}^n_\bullet)}$$

(C)

- Since $H_0(\hat{K}^n_\bullet) = \dfrac{R_n}{(F_1, \dots, F_{n-1})}$

(*) $\Longleftrightarrow$ $\overline{\mu}_n : H_0(\hat{K}^n_\bullet) \longrightarrow H_0(\hat{K}^n_\bullet)$ defined by multiplication by F_n being injective.

- $\overline{\mu}_n : H_0(\hat{K}^n_\bullet) \longrightarrow H_0(\hat{K}^n_\bullet)$ satisfies

$$\boxed{\begin{array}{c}\overline{\mu}_n\left(H_0(\hat{K}^n_{k-1,\bullet})\right) \subseteq H_0(\hat{K}^n_{k,\bullet}) \\ \forall\ k \geq 2.\end{array}}$$

-

$$\begin{tikzcd}
0 \arrow[r] & H_0(\hat{K}^n_{k-1,\bullet}) \arrow[r] \arrow[d, "\overline{\mu}_n|_{k-1}"] & H_0(\hat{K}^n_{k,\bullet}) \arrow[r] \arrow[d, "\overline{\mu}_n|_k"] & H_0(\hat{K}^{n-1}_\bullet) \arrow[d, "\overline{\nu}_n"] \\
0 \arrow[r] & H_0(\hat{K}^n_{k,\bullet}) \arrow[r] & H_0(\hat{K}^n_{k+1,\bullet}) \arrow[r] & H_0(\hat{K}^{n-1}_\bullet)
\end{tikzcd}$$

where $\overline{\nu}_n$ is the map induced by multiplication by $\lambda_n(F_n) = 1$ or $-n$.

In characteristic 0: $\overline{\nu_n}$ is isomorphism

Thus, by 4-lemma to above diagram

$\overline{\mu_n}|_{k-1}$ injective $\Longrightarrow$ $\overline{\mu_n}|_k$ injective.

Thus suffices to prove $H_0(\hat{K}^n_{1,\bullet}) \xrightarrow{\overline{\mu_n}|_1} H_0(\hat{K}^n_{2,\bullet})$ is injective.

- For $k=0,1$, define $C^n_{k,\bullet}$:

$$0 \to \Lambda^2 R_{n-1}[x_n]_k^{\oplus n-1} \xrightarrow{\delta_k} R_{n-1}[x_n]_k \to 0$$

where,

$$\begin{tikzcd} \Lambda^2 R_{n-1}[x_n]_k^{\oplus n-1} \arrow[r, "d_{n-1,2}"'] \arrow[rr, bend left, "\delta_k"] & R_{n-1}[x_n]_k^{\oplus n-1} \arrow[r, "d_{n,1}"'] & R_{n-1}[x_n]_{k+1} \end{tikzcd}$$

since $\operatorname{Im} \delta_k \subseteq R_{n-1}[x_n]_k \subseteq R_{n-1}[x_n]_{k+1}$.

- $$\begin{tikzcd} C^n_{0,\bullet} \arrow[d, "\mu_{n,\bullet}"] \\ C^n_{1,\bullet} \arrow[u, bend left, "\tilde{\lambda}"] \end{tikzcd}$$

Section to $\mu_{n,\bullet}$ induced by the map:

map induced by multiplication by F_n.

$\dfrac{\Lambda_{n,1}}{\lambda_n(F_n)} : R_{n-1}[x_n]_1 \to R_{n-1}$

dividing by $\lambda_n(F_n) = 1$ or $-n$.

$$\Downarrow$$

multiplication by F_n.

$$H_0(C^n_{0,\bullet}) \xrightarrow{\overline{\mu_n}} H_0(C^n_{1,\bullet})$$

is injective.

- $\exists$ a subcomplex $D^n_{1,\bullet} \xhookrightarrow{j_\bullet} \hat{K}^n_{2\bullet}$ s.t the following diagram commutes:

$$\begin{tikzcd}
C^n_{0\bullet} \arrow[r, "p_{0,\bullet}"] \arrow[d, "\mu_{n\bullet}"'] & \hat{K}^n_{0,\bullet} \arrow[r, hook, "i_{1\bullet}"] \arrow[d, "\mu_{n,\bullet}"] & \hat{K}^n_{1,\bullet} \arrow[r] \arrow[d, "\mu_{n,\bullet}"] & \operatorname{coker} i_{1,\bullet} \arrow[d] \\
C^n_{1,\bullet} \arrow[r, "p_{1,\bullet}"] & D^n_{1,\bullet} \arrow[r, hook, "j_\bullet"] & \hat{K}^n_{2,\bullet} \arrow[r] & \operatorname{coker} j_\bullet
\end{tikzcd}$$

$$\Downarrow H_0(-)$$

$$\begin{tikzcd}
H_0(C^n_{0,\bullet}) \arrow[r, "\sim"] \arrow[d, "\bar{\mu}_n"'] & H_0(\hat{K}^n_{0,\bullet}) \arrow[r] \arrow[d, "\bar{\mu}_n"'] & H_0(\hat{K}^n_{1,\bullet}) \arrow[r] \arrow[d, "\bar{\mu}_n"'] & H_0(\hat{K}^{n-1}_\bullet) \arrow[d, "\bar{\nu}_n"'] \\
H_0(C^n_{1,\bullet}) \arrow[r, "\sim"] & H_0(D^n_{1,\bullet}) \arrow[r] & H_0(\hat{K}^n_{2,\bullet}) \arrow[r] & H_0(\hat{K}^{n-1}_\bullet)
\end{tikzcd}$$

injective $\Longrightarrow$ injective

injective by 4-lemma

isomorphism in char 0.

$\square$

$$X^n + \underline{a_1} X^{n-1} + \underline{a_2} X^{n-1} + \cdots + a_{n-1} X + \underline{a_0} = 0$$

$$(\underbrace{X^n, X^{n-1}, X^{n-1}}, \ldots, X, 1)$$

$$\mathbb{A}^1 \longrightarrow \mathbb{A}^n \qquad [1 : \underbrace{a_1 : a_2 : \ldots : a_0}]$$

$$a_1 = \binom{n}{1}\alpha \qquad a_2 = \binom{n}{2}\alpha^2$$

$$, \quad ,$$