On the Cassa-Alvero Conjecture

Duong Hoang Dung

1 Introduction

Let K be a field and let $K[X]$ be a ring of univariate polynomials over K. For any polynomial $P \in K[X]$ of degree d :

$$P = a_0X^d + a_1X^{d-1} + \cdots + a_d$$

and for any non-negative integer i, we denote by $P^{(i)}$ the i-th derivative of P, and by P_i the i-th Hasse derivative, which is $P^{(i)}$ devided by $i!$ in characteristic zero:

$$P_i = \binom{d}{i}a_0X^{d-i} + \cdots + \binom{i+1}{i}a_{d-i-1}X + \binom{i}{i}a_{d-i}$$

It is clear that a polynomial of the form $(X-\alpha)^d$ has a non-trivial common factor with each of its $d-1$ first derivatives. The converse has been conjectured by Casas-Alvero :

Conjecture (Casas-Alvero) : *Let P be a monic univariate polynomial of degree d over a field K. Then $gcd(P, P_i)$ is non-trivial for $i = 1, \cdots, d-1$ if and only if $P = (X-\alpha)^d$ for some $\alpha \in K$.*

We have some notices as follows:

- It is clear for the implication from right to left.
- It is neccessary to prove the conjecture for the algebraically closed field only. Since if $P = a(x-b)^d$, with $a, b \in \overline{K}$, then since $P_i \in K[X]$, then a and b must be in K as well.
- The conjecture fails for the case of characteristic p, in which P is just a $p-$power of linear factors.
- The conjecture is proved in ([2]) by using Gröbner basis computations up to the degree $d = 7$.
- There is a *simple proof* of the conjecture of Peter Ullrich in 2005 (Ref. [6]). It seems good, but it was wrong in the main proof, so the author withdrawed the paper already. However, you may still download the first version at `arxiv`.

In this talk, I will present the main result of ([1]) for the conjecture, which is stated as follows :

Theorem *Let d be of the form p^k or $2p^k$ for some prime number p. Then the Casas-Alvero conjecture holds in characteristic 0 for polynomials of degree d.*

This report is organized as follows :

- Section 2 is devoted for presenting some preparation : the first part (2.1) introduces the concept of resultant $Res(f, g)$of two polynomials f and g, and the theorem that they have a common non-zero factor if and only if $Res(f, g) = 0$. And then we state the lemma which is stated that the $Res(P, P_i)$ is a weighted homogeneous polynomial of degree $d(d - i)$ if we give weight j for each a_j. This result is proved in [5]. The concepts and some neccessary results from schemes are stated without proof in the second part (2.2), in particular, the concept of weighted projective schemes. The main result we need is that the weighted projective scheme $\mathbb{P}_{\mathbb{Z}}(1, 2, \cdots, d - 1)$ is proper thank to the lectures of Bas last week. For the reference, please take a look at [4] and [3].
- Section 3 is devoted for presenting the main result of [1], which proved the conjecture for the case the degree of polynomial is a power of a prime or twice of it, in the field of characteristic 0. Then we present the counter examples of the conjecture in positive characteristic that in each finite field $\mathbb{F}_p$, with prime p, there always exists polynomial P of degree $d > p$ with a non-zero common factor with its $d - 1$ first Hasse derivatives P_i.

2 Preliminaries

2.1 Resultants

Given two polynomials $f, g \in k[x]$ of positive degree as follows

$$f(x) = a_m x^m + ... + a_0, \quad g(x) = b_n x^n + .. + b_0, \quad a_m, b_n \neq 0$$

The resultant of f and g is defined to be the determinant of the matrix

$$Res(f,g) = det \begin{pmatrix} a_m & & & & b_n & & & \\ a_{m-1} & a_m & & & b_{n-1} & b_n & & \\ a_{m-2} & a_{m-1} & \ddots & & b_{n-2} & b_{n-1} & \ddots & \\ \vdots & a_{m-2} & \ddots & a_m & \vdots & b_{n-2} & \ddots & b_n \\ a_0 & \vdots & \ddots & a_{m-1} & b_0 & \vdots & \ddots & b_{n-1} \\ & a_0 & & a_{m-2} & & b_0 & & b_{n-2} \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_0 & & & & b_0 \end{pmatrix}$$

This is sometime called Sylvecter resultant, in honor of James Joseph Sylvecter $(1814 - 1897)$.

Remarks

1. $Res(f,g) = (-1)^{mn} Res(g,f)$. It is easy to obtain just by changing columns in computing the determinant.

2. $Res(f, b_n) = b_n^m$.

3. If $g = qf + r$, then $Res(f,g) = a_m^{n-deg(r)} Res(f,r)$.

   Take $g_1 = g - \frac{b_n}{a_m} x^{n-m} f$. Subtract $\frac{b_n}{a_m}$ times of the first n columns of part f from columns of part g, we have

   $$Res(f,g) = a_m^{n-deg(g_1)} Res(f,g_1) =$$
   $$= a_m^{n-deg(g_1)} . a_m^{deg(g_1)-deg(g_2)} . Res(f,g_2) = ... = a_m^{n-deg(r)} Res(f,r)$$

4. $Res(f,g)$ is a polynomial in the integer polynomial in the coefficients $a_m, .., a_0, b_n, .., b_0$ of f and g, i.e.

   $$Res(f,g) \in \mathbb{Z}[a_m, ..., a_0, b_n, ..., b_0]$$

   In fact, by the definition, the determinant of matrix $A = (a_{ij})$ is defined as follow

   $$Res(f,g) = det(A) = \sum_{\sigma \in S_{n+m}} sgn(\sigma) a_{i\sigma(i)} ... a_{n+m,\sigma(m+n)}$$

   And $sgn(\sigma) = \pm 1$ which are integers.

5. If $f = a_m \prod_{i=1}^{m} (x - \alpha_i), g = b_n \prod_{j=1}^{n} (x - \beta_j)$, where α_i, β_j are roots of f and g respectively, then

   $$Res(f,g) = a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j)$$

Theorem *f and g have a nonzero common factor if and only if $Res(f,g) = 0$.*

Proof. (Ref. [**?**])

We have the following result which is needed for our setting :

Lemma *Let $P = X^d + \cdots + a_{d-1}X$ be the polynomial of degree d in $K[X]$ where K is a field. Let P_i be the $i-th$ Hasse derivative of P. If we give weight j to the variable a_j, for $1 \leq j \leq d-1$, then $Res(P, P_i)$ is homogeneous of weighted degree $d(d-i)$.*

Proof. (Ref. [5])

2.2 Schemes

Weighted projective scheme

An *affine scheme* is a locally ringed space $(X, \mathcal{O}_X)$ which is isomorphic (as a locally ringed space) to spectrum of some ring A. A *scheme* is a locally ringed space $(X, \mathcal{O}_X)$ in which every point has an open neighborhood U, such that the topological space U, together with the restricted sheaf $\mathcal{O}_X|_U$ is an affine scheme. A *morphisms* of schemes is a morphism as locally ringed spaces.

Let S be a graded ring. Let Proj(S) be the set of all homogeneous ideals of S which does not contain all of S_+. Then Proj(S) is a scheme. We call Proj(S) the *projective spectrum* of the graded ring S.

If $A = \mathbb{Z}[x_0, \cdots, x_n]$ is a ring, graded by total degree of monomials. We define the *projective n-space* over $\mathbb{Z}$ to be the scheme $\mathbb{P}^n_{\mathbb{Z}}$ =Proj(A).

If we give weight d_i for each variable x_i, $0 \leq i \leq n$, then we obtain the *weighted projective space*, denoted by $\mathbb{P}(d_0, \cdots, d_n)$. (Ref. [3]).

Fibre Product and Base Extension

Let S be a fixed scheme. A *scheme over* S is a scheme X, together with the morphism $X \to S$. If X, Y are two schemes over S, a morphism of X to Y as schemes over S is a morphism from $X \to Y$ which is compatible with the given morphisms to S.

Let S be a scheme, and let X, Y be schemes over S. We define the *fibre product* of X and Y over S, denoted by $X \times_S Y$, to be the product of X and Y in the category of schemes over S. If X and Y are scheme given without reference to any base scheme S, we take $S = Spec(\mathbb{Z})$. By the exercise II.2.5 ([4]), each scheme admits a unique morphism to $Spec(\mathbb{Z})$. Hence we can define the *product* of X and Y, denoted by $X \times Y$, to be $X \times_{Spec(\mathbb{Z})} Y$.

Theorem *For any two schemes X, Y over a scheme S, the fibred product $X \times_S Y$ exists, and is unique up to unique isomorphism.* (Ref. [4])

Let X be a scheme. For any $x \in X$, let $\mathcal{O}_m$ be the local ring at x, and $\mathfrak{m}_x$ be the unique maximal ideal in $\mathcal{O}_x$. We define the *residue field* of x on X to be the field $k(x) = \mathcal{O}_x/\mathfrak{m}_x$. By exercise II.2.7 ([4]), we have the morphism $Spec(k(x)) \to X$.

Now, let $f : X \to Y$ be a morphism of schemes, and let $y \in Y$ be a point. Let $k(y)$ be the residue field of y, then we have a morphism $Spec(k(y)) \to Y$. We define the *fibre* of morphism f over the point y to be the scheme

$$X_y = X \times_Y Spec(k(y))$$

When X is a scheme over $Spec(\mathbb{Z})$, i.e., we have the morphism of schemes : $X \to Spec(\mathbb{Z})$. If x is the *generic* point on $Spec(\mathbb{Z})$, then the residue field of x is $\mathbb{Q}$, and then the fibre over x will be the scheme over $Spec(\mathbb{Q})$. In case x is an any closed point of $Spec(\mathbb{Z})$, corresponding to a prime number p, then the residue field of x is the finite field $\mathbb{F}_p$. Hence the fibre over x will be the scheme over $Spec(\mathbb{F}_p)$.

Now let S be a fixed scheme (*base scheme*). If S' is another base scheme over S. Then for any scheme over S, we let $X' = X \times_S S'$ be the scheme over S'. We call that X' is obtained from X by making a base extension $S' \to S$.

Proper morphisms

Let $f : X \to Y$ be a morphism of schemes. It is called to be *closed* if image of a closed set is a closed set. If, in addition, for any morphism $Y' \to Y$, where Y' is a scheme, the morphism $f' : X' \to Y'$ of base extension $X' = X \times_Y Y'$ is also closed, f is called to be *universally closed*.

The morphism f is *locally of finite type* if there exists a covering of Y by open affine subsets $V_i = Spec(B_i)$, such that for each i, $f^{-1}(V_i)$ can be covered by open affine subsets $U_{ij} = Spec(A_{ij})$, where each A_{ij} is a finitely generated B_i-algebra. The morphism f is of *finite type* if in addition each $f^{-1}(V_i)$ can be covered by a finite number of the U_{ij}.

The *diagonal morphism* is the unique morphism $\triangle : X \to X \times_Y X$ whose composition with both projection maps $p_1, p_2 : X \times_Y X \to X$ is the identity map of $X \to X$. We say that f is *separated* of the diagonal morphism $\triangle$ is a closed immersion. In that case, we also say X is separated over Y. Since any scheme X is over $Spec(\mathbb{Z})$, hence X is *separated* if it is separated over $Spec(\mathbb{Z})$.

The morphism f is called *proper* is it is separated, of finite type, and universally closed.

3 The main results

3.1 Main theorem

We may assume that P is monic, that is $a_0 = 1$. And since the common factor of P and P_{d-1} is a linear factor, P must have a root in the base field. So we can translate that root to 0, and so we can assume that $a_d = 0$. Hence, we may consider our polynomial as

$$P = X^d + a_1 X^{d-1} + \cdots + a_{d-1} X$$

which is a polynomial in $\mathbb{Z}[a_1, \cdots, a_{d-1}][X]$.

Firstly, we note that the condition of $gcd(P, P_i) \neq 1$ is equivalent to the condition $Res(P, P_i) = 0$, for $i = 1, \cdots, d-1$. And as in the section 2, if we give weight j for each a_j, then $Res(P, P_i)$ will be the weighted homogeneous polynomial of degree $d(d-i)$. So the $(a_1, \cdots, a_{d-1})$ will belong to an algebraic variety, the system $\{Res(P, P_i) : 1 \leq i \leq d-1\}$. Hence, we can consider the weighted projective scheme

$$X \subseteq \mathbb{P}_{\mathbb{Z}}(1, 2, \cdots, d-1)$$

over $\mathbb{Z}$, defined by the homogeneous ideal

$$I = \langle Res(P, P_i) : 1 \leq i \leq d-1 \rangle$$

where a_j has weight j for $1 \leq j \leq d-1$. We will consider the set $X(K)$ of $K-$rational points on X for any field K.

We know that, if the conjecture holds, so we must have $P = X^d$, hence $a_1 = a_2 = \cdots = a_{d-1} = 0$. But the point $(0, \cdots, 0)$ is not in the projective space, so $X(K)$ must be empty. Hence, the conjecture holds iff $X(K)$ is empty.

Now if we let $\overline{K}$ be the algebraic closure of K, then $X(\overline{K})$ is empty if and only if the base extension $X \times Spec(K)$ is empty.

For the first step, we will prove the result that if the conjecture holds in $\overline{\mathbb{F}}_q$for a prime q, then it must hold for all degree d in characteristic 0 and in characteristic p for all but finite many primes p.
In face, since $P(1, 2, \cdots, d-1)$ is proper, then the image of X via $\phi : X \to Spec(\mathbb{Z})$ is closed. Let U be the complement of the image $\phi(X)$. Then U is the set of primes in $Spec(\mathbb{Z})$ where the fiber under ϕ is empty. But by assumption, there is prime q in U, so U is dense in $Spec(\mathbb{Z})$. Hence U contains the generic point and all but finite primes. The fiber of generic point is $X \times Spec(\mathbb{Q})$, and the fiber of prime p is $X \times Spec(\mathbb{F}_p)$.

So now, we are going to prove the first case of the conjecture that

Proposition 1 *If d is a power of some prime p, then $X(\overline{\mathbb{F}_p})$ is empty.*

Proof. Since d is a power of prime p then $\binom{d}{i} = 0$ in $\mathbb{F}_p$ for all $i = 1, \cdots, p-1$. In particular $\binom{d}{d-1} = 0$, then $P_{d-1} = a_1$. The existence of a common factor with P implies that $a_1 = 0$. But then $P_{d-2} = a_2$, hence $a_2 = 0$, and so on. Hence $a_1 = \cdots = a_{d-1} = 0$, so $X(\overline{\mathbb{F}_p})$ is empty.■

Proposition 2 *If $d = np^k$ for some prime p, then if $X_n(\overline{\mathbb{F}_p})$ is empty, then $X(\overline{\mathbb{F}_p})$ is empty.*

Proof. For the previous proposition, we have $a_1 = \cdots = a_{p^k-1} = 0$. Now we

have $P_{d-p^k} = \binom{d}{d-p^k} X^{p^k} + a_{p^k}$. Continuing, we see that in P_{d-p^k-1}, the leading coefficient vanishes, as well as the coefficient of a_{p^k}, and we get $a_{p^k+1} = 0$. So by this process, we get $a_i = 0$ unless $p^k | i$. We obtain

$$P = X^d + a_{p^k} X^{d-p^k} + \cdots + a_{d-p^k} X^{p^k}$$

But it is a p^k-power of a polynomial Q of degree in $\overline{\mathbb{F}_p}$. This Q must have a common factor with all its Hasse derivatives up to the order $n-1$, which is impossible.■

So now, since the conjecture holds for the case $d = 2$, even in the characteristic p, so $X_2(\overline{\mathbb{F}_p})$ is empty, so by the proposition 2, $X_d(\overline{\mathbb{F}_p})$ is empty, for $d = 2p^k$. Hence the theorem is proved.

3.2 Counter-examples in positive characteristic

Now the following polynomial

$$P = X^p(X-1) \in \mathbb{F}_p[X]$$

does give a counter-example for the conjecture in positive characteristic.

4 Comments

As we've seen, the conjecture is still an open question. We have known alot of cases that are true. However, there is no better result known at this moment.

- It may be potiential to use the method of [2] to do for the higher degree (> 7) in characteristic 0, but it may be very expensive in computation.
- In the last step, we showed that there is no non-trivial quadratic examples in characteristic p. Hence, I am wondering if we can do for higher level (> 2) as well ? And how ?

References

[1] Hans-Christian Graf von Bothmer, Oliver Labs, Josef Schicho, Christiaan van de Woestijne, *The Cassa-Alvero conjecture for infinitely many degrees*, Journal of Algebra 316 (2007), pp. **224-230**.

[2] Gema Diaz-Toca, Laureano Gonzalex-Vega, *On a conjecture about univariate polynomials and their roots*, in : A. Dolzmann, A. Seidl, T. Sturm (Eds), *Algorithmic Algebra and Logic 2005*, Norderstedt, Germany, 2005, pp. **83-90**.

[3] Bas' talk on *Weighted Projective Spaces*.

[4] R. Hartshorne, *Algebraic Geometry*, Springer 1977.

[5] David A. Cox, John B. Little, Donal O'Shea, *Using Algebraic Geometry*, Second Edition, Springer 2004.

[6] Peter Ullrich, *A simple proof of a conjecture on univariate polynomials and their roots*, Preprint 2005, available from `http://arxiv.org/abs/math/0504591v2`.