THE CASAS-ALVERO CONJECTURE

LAURENT BERGER

The goal of this project is to work on the following conjecture, which looks so simple that you may be suprised to learn that it has not been proved yet! If P is a polynomial, let $P^{(i)}$ denote its i-th derivative.

Conjecture 1. *Let $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ be a monic polynomial of degree $d \geq 1$, with complex coefficients. If for all $1 \leq i \leq d-1$, there exists $x_i \in \mathbf{C}$ such that $P(x_i) = P^{(i)}(x_i) = 0$, then $P(X)$ is of the form $(X-\lambda)^d$ for some $\lambda \in \mathbf{C}$.*

This conjecture has been proposed by Eduardo Casas-Alvero around 2000, following his work [CA01] on plane curves. It is known for $d \leq 19$ as well as for any d which is a prime power or twice a prime power.

If $P(X) \in \mathbf{C}[X]$, we say that P is a *CA polynomial* if P and $P^{(i)}$ have a common root for all $1 \leq i \leq \deg(P) - 1$, so that the conjecture above says that CA polynomials have a very special shape.

Exercise 1. *Prove conjecture 1 for $d = 2, 3, 4$. If $d \geq 3$, you can assume that P is of the form $P(X) = X^2 \cdot (X-1) \cdot Q(X)$ where $\deg Q = d-3$: why? Can you do $d = 5$ as well?*

1. Roots of polynomials

Before we go on, let us explore some properties of the roots of polynomials, using a bit of real and complex analysis. The first exercise is Rolle's theorem for polynomials.

Exercise 2. *If $P(X) \in \mathbf{R}[X]$, and if $a < b$ are two real roots of $P(X)$, then $P'(X)$ has a root in the open interval $]a, b[$.*

The following asks you to prove the Gauss-Lucas theorem.

Exercise 3. *If $P(X) \in \mathbf{C}[X]$, then the roots of P' are in the convex hull of the roots of P.*

Can you use the Gauss-Lucas theorem to study the cases $d = 3, 4$? Can you say something about the minimal number of distinct roots of a CA polynomial? Unfortunately, it does not seem possible to prove conjecture 1 using these ideas if $d \geq 5$. We finish this section with a much harder exercise.

Exercise 4. *If $d \geq 2$ and $1 \leq n \leq d-1$, then there exists a monic polynomial $P(X) \in \mathbf{C}[X]$ of degree d, such that P and $P^{(i)}$ have a common root for all $1 \leq i \leq d-1$ with $i \neq n$.*

2. Resultants

Since analysis does not seem to be of much help, we turn to algebra. There is a nice algebraic way of figuring out if two polynomials have a common root. Let K be a field and let $P(X) = a_dX^d + \cdots + a_0$ and $Q(X) = b_eX^e + \cdots + b_0$ be two polynomials with coefficients in K. Let $K[X]_n$ denote the space of polynomials of degree $\leq n-1$. Let M be the matrix of the map $K[X]_e \times K[X]_d \to K[X]_{d+e}$ given by $(A,B) \mapsto AP+QB$, in the basis $\{X^{e-1}, \ldots, X, 1\}$ of $K[X]_e$, $\{X^{d-1}, \ldots, X, 1\}$ of $K[X]_d$ and $\{X^{d+e-1}, \ldots, X, 1\}$ of $K[X]_{d+e}$. We then have

$$M = \begin{pmatrix} a_d & 0 & \cdots & 0 & b_e & 0 & \cdots & 0 \\ a_{d-1} & a_d & \ddots & \vdots & \vdots & b_e & \ddots & \vdots \\ \vdots & a_{d-1} & \ddots & 0 & \vdots & & \ddots & 0 \\ \vdots & \vdots & \ddots & a_d & b_1 & & & b_e \\ a_0 & & & a_{d-1} & b_0 & \ddots & \vdots & \vdots \\ 0 & \ddots & & \vdots & 0 & \ddots & b_1 & \vdots \\ \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 & b_1 \\ 0 & \ldots & 0 & a_0 & 0 & \ldots & 0 & b_0 \end{pmatrix}.$$

The *resultant* $\mathrm{res}(P,Q)$ of P and Q is $\mathrm{res}(P,Q) = \det(M)$.

Exercise 5. *Compute* $\mathrm{res}(P,P')$ *when* $P(X) = X^2+aX+b$ *and when* $P(X) = X^3+pX+q$. *Do you recognize the results?*

Exercise 6. *Show that if* $a_d \neq 0$ *and* $b_e \neq 0$, *then* $\mathrm{res}(P,Q) = 0$ *if and only if* P *and* Q *have a common root. Show that* $\mathrm{res}(P,Q) = a_d^e \cdot \prod_{P(x)=0} Q(x) = (-1)^{de} \cdot b_e^d \cdot \prod_{Q(x)=0} P(x)$.

If $K = \mathbf{C}$, a polynomial P of degree d is therefore a CA polynomial if and only if

$$\mathrm{res}(P,P') = \mathrm{res}(P,P'') = \cdots = \mathrm{res}(P,P^{(d-1)}) = 0.$$

This way, we have reduced the CA conjecture to showing that certain sets of equations have no solution. We'll see how to prove this in the next section.

3. The Nullstellensatz

Let $A = \mathbf{C}[X_1, \ldots, X_n]$ be the set of polynomials in n variables, with coefficients in $\mathbf{C}$. Let I be an ideal of A, that is a subset of A such that $i+j \in I$ if $i,j \in I$ and $a \cdot i \in I$ if $a \in A$ and $i \in I$. The *Nullstellensatz* (the "zero locus theorem") is the following theorem.

Theorem 1. *If* I *is an ideal of* A *and* $I \neq A$, *then there exists* $x = (x_1, \ldots, x_n) \in \mathbf{C}^n$ *such that* $f(x) = 0$ *for all* $f \in I$.

Exercise 7. *What does theorem 1 say when* $n = 1$?

Exercise 8. *Show that theorem 1 implies the following: if $f_1, \dots, f_m \in A$, then either some A-linear combination of the f_i's is equal to 1, or there exists $x \in \mathbf{C}^n$ such that $f_i(x) = 0$ for all i.*

You should look up the Nullstellensatz; there are several different proofs, see for example §1 of Chapter IX of [Lan02], or the proof that is explained in [May03].

Exercise 9. *Show that the Casas-Alvero conjecture is equivalent to the following statement: if $P(X) = X(X-1)(X^{d-2} + a_{d-3}X^{d-3} + \cdots + a_0)$, and $A = \mathbf{C}[a_0, \dots, a_{d-3}]$, then some A-linear combination of the $\{\mathrm{res}(P, P^{(i)})\}_{1 \leq i \leq d-1}$ is equal to 1.*

Use a computer algebra system to verify the conjecture for small values of d.

This is how conjecture 1 has been proved for some values of d up to $d = 12$ (see for instance [DG06] and [CLO14]). For larger values of d, some additional theoretical input is needed as the computations become too difficult, even for a computer.

4. Polynomials in characteristic p

In this section, we consider polynomials with coefficients in a field K of characteristic p, for example $K = \mathbf{F}_p$. In this case, we can have $P'(X) = 0$ for some non constant P, for example if $P(X) = X^p$. In addition $P^{(k)}(X) = 0$ for all P as soon as $k \geq p$ (why?). Instead of working with derivatives, we work with the *Hasse derivative*. The k-th Hasse derivative of $P(X) = a_d X^d + \cdots + a_0$ is

$$H^k P(X) = \binom{d}{k} a_d X^{d-k} + \binom{d-1}{k} a_{d-1} X^{d-1-k} + \cdots + \binom{k}{k} a_k.$$

Note that $P^{(k)}(X) = k! \cdot H^k P(X)$. If $P(X) \in K[X]$, we say that P is a CA polynomial if P and $H^i P$ have a common root for all $1 \leq i \leq \deg(P) - 1$. The characteristic p version of the Casas-Alvero conjecture for polynomials of degree d is then the following.

Question 1. *If P is a monic CA polynomial, then do we necessarily have $P(X) = (X - \lambda)^d$ for some $\lambda \in K^{\mathrm{alg}}$?*

Exercise 10. *Show that if $(X - \lambda)^d \in \mathbf{F}_p[X]$, then $\lambda \in \mathbf{F}_p$. For what fields other than $\mathbf{F}_p$ does an analogous statement hold?*

Exercise 11. *Show that the answer to question 1 is* yes *for $d = 1, 2$, for $d = 3$ if $p \neq 2$, and* no *if $d = p + 1$.*

Exercise 12. *What about $P(X) = X(X-1)^4(X-8)(X-18)$ in $\mathbf{F}_{23}[X]$?*

The following is the main theorem of [BLSW].

Theorem 2. *Let K be algebraically closed. If $p \nmid n$ and question 1 has a positive answer in degree n, then it also has a positive answer in degree $d = np^e$ for all $e \geq 1$.*

In the rest of this section, we (meaning: you) prove theorem 2. If $n \geq 0$, write n in base p as $= n_k p^k + n_{k-1} p^{k-1} + \cdots + n_0$.

Exercise 13. *If $m, n \geq 1$, then*

$$\binom{n}{m} \equiv \binom{n_k}{m_k} \cdots \binom{n_1}{m_1} \cdot \binom{n_0}{m_0} \mod p$$

Exercise 14. *Let the notation be as in theorem 2. Prove that if P is a CA polynomial of degree d, then there is a CA polynomial Q of degree n such that $P = Q^{p^e}$. Prove theorem 2.*

5. Reduction modulo p

It is possible to use the results of the previous section to prove conjecture 1 when the degree of P is a power of a prime number or twice a power of a prime number. In order to do this, you need to know a little bit of valuation theory, see for instance §4 of Chapter XII of [Lan02] (but beware that what Lang calls a valuation is what we'd call an *absolute value*; how do you relate the two definitions?). For us, a *valuation* on a field K is a function $v : K^\times \to \mathbf{R}$ such that $v(xy) = v(x) + v(y)$ and $v(x + y) \geq \min(v(x), v(y))$. It is customary to extend v to K by setting $v(0) = +\infty$. The trivial valuation is given by $v(x) = 0$ for all $x \in K^\times$. Let p be a prime number. The *p-adic valuation* on $\mathbf{Q}$ is the function $\mathrm{val}_p : \mathbf{Q}^\times \to \mathbf{Z}$ defined as follows. If $x \in \mathbf{Q}^\times$, we can write it as $x = p^n \cdot a/b$ where p divides neither a nor b and then we let $\mathrm{val}_p(x) = n$.

Exercise 15. *Check that val_p is a valuation on $\mathbf{Q}$. Conversely, show that if v is a non-trivial valuation on $\mathbf{Q}$, then there exists a prime number p such that v is a multiple of val_p.*

We use the following fact (see §4 of Chapter XII of [Lan02]).

Theorem 3. *If v is a valuation on K, and L/K is a field extension, then v extends to L.*

Exercise 16. *By (possibly infinite) induction, it is enough to prove theorem 3 for extensions of the form $L = K(x)$. How do you extend a valuation v on K to $K(x)$? Treat separately the cases where x is algebraic over K and where x is transcendental over K.*

The p-adic valuation val_p can therefore be extended (in many different ways) from $\mathbf{Q}$ to $\mathbf{C}$. We choose one such extension. Let R denote the set of elements of $\mathbf{C}$ of valuation ≥ 0 and let $\mathfrak{m}_R$ denote the set of elements of $\mathbf{C}$ of valuation > 0.

Exercise 17. *Show that R is a ring, that $\mathfrak{m}_R$ is a maximal ideal of R, and that the quotient field $R/\mathfrak{m}_R$ is a field of characteristic p.*

Exercise 18. *Prove the Casas-Alvero conjecture for polynomials $P(X) \in \mathbf{C}[X]$ whose degree is a power of a prime or twice a power of a prime.*

The same idea can be used to prove the conjecture for polynomials of degree $3p^e$, $4p^e$ or $5p^e$ for primes p, but you have to start excluding some primes (see [DdJ11] and [CS12]).

6. Going further

Now your work really begins. Look up the literature on the subject, for example the references below. There are also various papers on the arxiv that claim to give a complete proof: can you make sense of them? What is the smallest degree d for which the conjecture is currently open? Can you prove the conjecture using some totally different ideas?

References

[CA01] E. Casas-Alvero – "Higher order polar germs", *J. Algebra* **240** (2001), no. 1, p. 326–337.

[Cas13] W. Castryck – "La conjecture de Casas-Alvero", 2013, `http://images.math.cnrs.fr/La-conjecture-de-Casas-Alvero.html`.

[CLO14] W. Castryck, R. Laterveer & M. Ounaïes – "Constraints on counterexamples to the Casas-Alvero conjecture, and a verification in degree 12", Math. Comp., to appear, 2014.

[CS12] M. Chellali & A. Salinier – "La conjecture de Casas Alvero pour les degrés $5p^e$", *An. Univ. Dunărea de Jos Galaţi Fasc. II Mat. Fiz. Mec. Teor.* **4(35)** (2012), no. 1-2, p. 54–62.

[DdJ11] J. Draisma & J. P. de Jong – "On the Casas-Alvero conjecture", *Eur. Math. Soc. Newsl.* (2011), no. 80, p. 29–33. Erratum: `http://www.win.tue.nl/~jdraisma/publications/erratumcasasalvero.pdf`.

[DG06] G. M. Diaz-Toca & L. Gonzalez-Vega – "On analyzing a conjecture about univariate polynomials and their roots by using Maple.", in *Maple conference 2006. Proceedings of the conference, Waterloo, Ontario, Canada, July 23–26, 2006.*, Waterloo: Maplesoft, 2006, p. 81–98.

[BLSW] 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), no. 1, p. 224–230.

[Lan02] S. Lang – *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[May03] J. P. May – "Munshi's proof of the Nullstellensatz", *Amer. Math. Monthly* **110** (2003), no. 2, p. 133–140.

UMPA de l'ENS de Lyon, UMR 5669 du CNRS, IUF
E-mail address: `laurent.berger@ens-lyon.fr`
URL: `perso.ens-lyon.fr/laurent.berger/`