FEASIBILITY OF p-ADIC POLYNOMIALS

DAVI DA SILVA

ABSTRACT. The p-adic number system is pertinent to many fields, including cryptography, and many of these applications naturally rely on solving systems of polynomials over the p-adics. The question of whether, in general, such a polynomial system has a root over $\mathbb{Q}_p$ – and whether this can be verified algorithmically – is therefore of practical and theoretical importance. Some general problems in the search for p-adic polynomial roots are discussed, as are some results on the existence and computability of p-adic roots.

Definition 1. *For an integer a and a prime p, let $ord_p a$ be the highest natural number k such that p^k divides a. (For example, $ord_5 400 = 2$.) For a rational number a/b, define $|a/b|_p = p^{ord_p b - ord_p a}$. Note that $|\cdot|_p$ is independent the rational number's representation. If we define $d_p : \mathbb{Q}^2 \to \mathbb{Q}$ by $d_p(x, y) = |x - y|_p$, d defines a metric on $\mathbb{Q}$. We define $\mathbb{Q}_p$ to be the Cauchy sequence completion of $\mathbb{Q}$ with respect to d_p.*

We call $\mathbb{Q}_p$ the p-adic numbers. The usual operations $+$ and $\cdot$ on $\mathbb{Q}$ can be extended to $\mathbb{Q}_p$ in a natural way using Cauchy sequences; thus, the p-adic numbers form a field, with the rational numbers as a subfield. The definition of these operations leads naturally to the definition of polynomials over $\mathbb{Q}_p$, and the question of their solubility.

The first non-trivial way to simplify this question is to reduce a system of polynomials to a single polynomial equation with the same zero set. It is easy to see how this can be done over $\mathbb{R}$ or $\mathbb{Q}$: given a system of polynomials $\{f_i\}_{i=1}^n$, the associated polynomial $g = \Sigma_{i=1}^n f_i^2$ has a root at a point x_0 exactly when all the f_i have a root there as well. Sufficiency is true over any polynomial ring, but necessity follows from the ordering on the reals and rationals – each term in the sum defining g is a square and therefore nonnegative; and a nonnegative sum equals zero only when all the terms are zero. One of the key differences between $\mathbb{Q}_p$ and $\mathbb{R}$ or $\mathbb{Q}$ is the lack of any such ordering. (For example, as we will see later, $\mathbb{Q}_5$ contains square root of -1, which precludes the possibility of it being an ordered field.) Thus, that particular trick cannot be transferred to the p-adics – however, other techniques do exist that, while increasing the degree of the equations, reduce polynomial systems over $\mathbb{Q}_p$ to a single equation.

Another key difference between $\mathbb{R}$ and $\mathbb{Q}_p$ is the topology. Over $\mathbb{R}$, the topology of algebraic varieties can be described in terms of the number of connected components: for example, the zero set of the polynomial $x^2 + y^2 - 1$ is the unit circle, which consists of one connected component, while the zero set of the polynomial

$x^2 - y^2 - 1$ is a hyperbola with two branches and therefore has two connected components. Over the p-adics, however, the only nonempty connected sets are those consisting of a single point. Thus, the number of connected components of an algebraic variety over $\mathbb{Q}_p$ is just its cardinality, which contains less information.

How, then, can we characterize the complexity of a polynomial equation over $\mathbb{Q}_p$? Other than the degree, there are two ways: we can consider the number of terms in the polynomial, and we can consider the number of variables those terms are in. If a polynomial is in n variables and has m terms, we say it is an n-variate m-nomial, and we denote the set of such polynomials by $\mathcal{F}_{n,m}$. Some n-variate m-nomials, however, are effectively even simpler. For example, take the case $f(x, y) = 4 + 2x^{10}y^4 + x^{15}y^6$; then $f \in \mathcal{F}_{2,3}$. However, If we take $z = x^5y^2$, then f becomes $4 + 2z^2 + z^3$; to find the roots of f, we need only find the roots z_0 of the above trinomial in z; the roots of f are then given by elements of the variety $xy = z_0$. Thus, we have reduced f from a polynomial in two variables to one in one variable. In general, we can make such a reduction if the convex hull of the support of f (that is, the set of exponent vectors in $\mathbb{R}^n$) defines an n-dimensional figure; in the case of f above, the support lied on a line segment, which is one-dimensional in the two-dimensional space of exponent vectors, and therefore was dishonest. We denote the set of honest n-variate m-nomials by $\mathcal{F}^*_{n,m}$.

We now move to the question of how to determine the roots of an honest polynomial equation over $\mathbb{Q}_p$. We begin with a theorem.

Theorem 1 (Hensel's Lemma). *Let $f \in \mathcal{F}_{1,n}$, and suppose we have $x \in \mathbb{Q}_p$ such that:*

- $f(x) \equiv 0 \mod p$ *and*
- $f'(x) \not\equiv 0 \mod p$.

Then there exists $x_0 \in \mathbb{Q}_p$ such that:

- $f(x_0) = 0$*, and*
- $x_0 \equiv x \mod p$

For example, over $\mathbb{Q}_5$, consider the polynomial $g(x) = x^2 + 1$. $g(2) = 5 \equiv 0 \mod 5$, and $g'(2) = 4 \not\equiv 0 \mod 5$, so there exists a square root of -1 in $\mathbb{Q}_5$.

Hensel's Lemma gives a simple criterion for determining if an approximate root of a p-adic polynomial can be refined to a true root. The proof relies on a p-adic analog of Newton's method, which gives a simple algorithmic way to calculate a root given a suitable initial guess via p-adic expansions. It can also be applied to obtain more general results, among which is the following theorem.

Theorem 2 (Birch and McCann). *Given a polynomial f in any number of variables over $\mathbb{Q}_p$, there exists an integer $D(f)$ such that if for some x we have*

$$|f(x)|_p < |D(f)|_p$$

then we can refine x to a true root of f. Moreover, we can calculate $D(f)$ according to a formula.

Thus, determining whether a polynomial has a root over $\mathbb{Q}_p$ can be done in finite time; we only need check for roots over $\mathbb{Z}/p^R\mathbb{Z}$ where $p^R > |D(f)|_p^{-1}$. However, by this method, doing so is almost always impossible in practice. The effective "size" associated with calculating $L(D(f))$ is bounded by:

$$L(D(f)) < (2^n dL(f))^{(2d)^{4^n} n!}$$

where n is the number of variables and d is the degree. The size of $D(f)$ can be up to quadruply exponential in the number of variables, and thus for multivariate cases this method can be extremely inefficient. In the case of polynomials in $\mathcal{F}^*_{n,n+1}$, however, there are better methods.

Theorem 3 (Avendano, Ibrahim, Rojas, Rusek)**.** *For a fixed prime p, finding a root to a function in $\mathcal{F}_{1,3}$ is* **NP**. *Furthermore, allowing p to vary, finding roots for almost all polynomials in one variable with integer coefficients is* **NP***, as it is for $\bigcup_n \mathcal{F}^*_{n,n+1}$.*

This means that , rather than the quadruply exponential bounds in n on finding a root of a p-adic polynomial provided by Birch and McCann, the complexity is at worst exponential for honest n-variate $(n + 1)$-nomials and univariate trinomials.

References

[1] Martín Avendaño, Ashraf Ibrahim, J. Maurice Rojas, and Korben Rusek. *Faster p-adic feasibility for certain multivariate sparse polynomials.* Preprint, 2011.

[2] B.J. Birch and K McCann. *A Criterion for the p-adic Solubility of Diophantine Equations*. The Quarterly Journal of Mathematics, Oxford Series, Vol. 18. 1967.

[3] Marvin J. Greenberg. *Strictly Local Solutions of Diophantine Equations*. Pacific Journal of Mathematics, Vol. 51, No. 1. 1974.

[4] Gudmund S. Frandse. *On Reducing a System of Equations to a Single Equation*. 2004.