Probabilistic Properties of p-adic Polynomials

Antoine Poulin (Université Laval)

October 5th 2019

Separability over fields and rings

- Let K be a field and R a ring.
- A polynomial $f \in K[x]$ is separable if all its roots are distinct in an algebraic closure of K.
- This is equivalent to stating that f and its derivative have no common factor, i.e $(f, f') = K[x]$.
- Over a ring, a polynomial $f \in R[x]$ is separable if $R[x]/(f)$ is a separable R-algebra.
- For monic polynomials, this is also equivalent to $(f, f') = R[x]$.
- Two monic polynomials $f, g \in R[X]$ will be coprime if there is no polynomial of positive degree which divides both f and g.

The idea

- Using the inverse limit construction of $\mathbb{Z}_p$, link (f, g) with $(\overline{f}_k, \overline{g}_k)$, where $\overline{f}_k$ is the canonical projection from $\mathbb{Z}_p[x]$ to $\left(\mathbb{Z}/p^k\mathbb{Z}\right)[x]$.

Theorem (Polak, 2018)

The proportion of monic polynomials of degree $d \geq 2$ that are separable in $(\mathbb{Z}/p^k\mathbb{Z})[x]$ is $1 - p^{-1}$.

Theorem (Hagedorn, Hatley, 2010)

The probability that two randomly chosen monic polynomials of degrees m and 2 in $(\mathbb{Z}/p^k\mathbb{Z})[x]$ are relatively prime is given by

$$P_{\mathbb{Z}/p^k\mathbb{Z}}(m, 2) = 1 - \frac{f_k(p)}{p^{3k}},$$

where $f_k(x) \in \frac{1}{2}\mathbb{Z}[x]$ is an explicit monic polynomial of degree $2k$.

Our result

Theorem (Lei, P., 2018)

Let $f, g \in \mathbb{Z}_p[x]$ be two monic polynomials of degree at least 1. Then the $\mathbb{Z}_p[x]$-ideal generated by f and g equals $\mathbb{Z}_p[x]$ if and only if the $(\mathbb{Z}/p\mathbb{Z})[x]$-ideal generated by $\overline{f}_k$ and $\overline{g}_k$ equals $(\mathbb{Z}/p^k\mathbb{Z})[x]$.

- One side of implication is easy through projection.
- Lift a linear combination from $\mathbb{Z}/p^k\mathbb{Z}$ to $\mathbb{Z}/p^{2k}\mathbb{Z}$ and inductively create a sequence of linear coefficients.
- Use compacity to find a limit in $\mathbb{Z}_p$.

Discussion

Corollary (From Polak's result)

The proportion of monic polynomials of degree $d \geq 2$ that are separable in $\mathbb{Z}_p[x]$ is $1 - p^{-1}$.

- This gives an alternative proof of a result of Weiss (2014).

Corollary (From Hagedorn and Hatley's result)

The probability that two randomly chosen monic polynomials of degrees m and 2 in $\mathbb{Z}_p[x]$ are relatively prime is 1.

The proof

- Given monic polynomials $f, g \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)[x]$ and arbitrary monic lifts $f^*, g^* \in \mathbb{Z}_p[x]$such that there exists $\alpha_0, \beta_0 \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)[x]$ such that

$$\alpha_0 f + \beta_0 g = 1.$$

  We wish to lift α_0, β_0 to $\alpha_\infty, \beta_\infty \in \mathbb{Z}_p[x]$ such that

$$\alpha_\infty f^* + \beta_\infty g^* = 1.$$

- By looking at two arbitrary lifts $\alpha_0^*, \beta_0^* \in \mathbb{Z}_p[x]$, we find

$$\alpha_0^* f^* + \beta_0^* g^* = 1 + Q,$$

  where $Q \in p^k\mathbb{Z}_p[x]$.

The proof

- Multiplying both sides by $1 - Q$, the equation becomes

$$(\alpha_0^*(1-Q)))\, f^* + (\beta_0^*(1-Q)))\, g^* = 1 - Q^2,$$

with $Q^2 \in p^{2k}\mathbb{Z}_p[x]$.

- We can then project the equation on $\mathbb{Z}/p^{2k}\mathbb{Z}$,

$$\overline{(\alpha_0^*(1-Q)))}_{2k} \cdot \overline{f^*}_{2k} + \overline{(\beta_0^*(1-Q)))}_{2k} \cdot \overline{g^*}_{2k} = 1$$

- We can then define in $\mathbb{Z}/p^{2k}\mathbb{Z}$

$$\alpha_1 := \overline{\alpha_0^*(1-Q)}_{2k};$$
$$\beta_1 := \overline{\beta_0^*(1-Q)}_{2k}.$$

The proof

- Using euclidean division, we can assume that $\deg(\alpha_1) < \deg(g), \deg(\beta_1) < \deg(f)$.
- Inductively, we create the sequence $(\alpha_i, \beta_i)_{i\in\mathbb{N}}$. By looking at this sequence as one in $\mathbb{Z}_p^{\deg(f)+\deg(g)}$, we can guarantee, by compacity, that there is a subsequence with a limit $(\alpha_\infty, \beta_\infty)$.
- It can then be verified with projections that this gives the required result, that is

$$\alpha_\infty f^* + \beta_\infty g^* = 1.$$

Bibliography

- Hagedorn, T. R., Hatley, J. (2010). The probability of relatively prime polynomials in $\mathbb{Z}_{p^k}[x]$. *Involve*. 3(2) : 223–232.
- Polak, J. K. C. (2018). Counting separable polynomials in $\mathbb{Z}/n[x]$. *Canad. Math. Bull.* 61(2) : 346–352.
- Weiss, B. L. (2013). Probabilistic Galois theory over p-adic fields. *J. Number Theory*. 133(5) : 1537–1563.

Thank you !