A Test for Absolute Irreducibility of Polynomials with Rational Coefficients

Jean-François Ragot
Université de Limoges

October 6, 1997

[summary by Bruno Salvy]

While univariate polynomials with coefficients in a field k can always be factored as products of linear polynomials over the algebraic closure $\overline{k}$ of k, in the multivariate case irreducible polynomials over $\overline{k}$ may have arbitrary degree. A multivariate polynomial with coefficients in k which is irreducible over $\overline{k}$ is called *absolutely irreducible* and the decomposition of a multivariate polynomial as a product of absolutely irreducible polynomials is called its *absolute factorization.* Geometrically, absolutely irreducible polynomials correspond to irreducible algebraic varieties. Factorization is available in all the general computer algebra systems, but absolute factorization is much harder. There are algorithms that compute the absolute factorization of polynomials over $\mathbb{Q}$ and one of them is available in Maple. There are other algorithms that only test whether polynomials over $\mathbb{Q}$ are absolutely irreducible. Both these operations are computationally expensive. In this work, J.-F. Ragot gives a probabilistic test for absolute irreducibility.

1. Algorithms

The property on which are based the algorithms dealing with absolute irreducibility is related to *simple* solutions of polynomials.

Definition 1. Let k be a field. The polynomial $f \in k[x_1, \dots, x_r]$ is said to have a *simple solution* at a point $P \in \overline{k}^r$ when

$$f \in I(P) \setminus I(P)^2,$$

$I(P)$ being the ideal of polynomials vanishing at P:

$$I(P) := \{g \in k[x_1, \dots, x_r], g(P) = 0\}.$$

For instance, the polynomials belonging to $I(0)^p$ are those that do not have any monomial of degree less than p.

Theorem 1. *If $f \in k[x_1, \dots, x_r]$ is irreducible over the perfect field k and has a simple solution at a point $P \in k^r$, then f is absolutely irreducible.*

Proof. Examples of perfect fields are fields of characteristic 0 and the fields $\mathbb{Z}/p\mathbb{Z}$ (for prime p). The polynomial f being irreducible over k, its absolutely irreducible factors are conjugate over k. Thus if P cancels one of them it must cancel the other ones; simplicity then implies uniqueness. □

For instance, the polynomial

$$f = x^3 + 2xy + 5x - 3xy^2 - y^3$$

can be seen to be irreducible over $\mathbb{Q}$ (e.g., by attempting to factor it). Since $(0,0)$ is obviously a simple solution, f is absolutely irreducible.

One of the algorithms for absolute factorization then proceeds by constructing extension fields where the polynomials have simple solutions. Absolute factorization is thus reduced to factorization over algebraic extensions, which is possible but expensive when the degree of the extension is large.

Theorem 1 can also be used to prove absolute irreducibility when one can find simple solutions. While this is difficult in characteristic 0, it is relatively easier in characteristic p. Then, one can use the following theorem to obtain the conclusion over $\mathbb{Q}$.

Theorem 2. [3] *Let f be a polynomial in $\mathbb{Z}[x_1,\ldots,x_r]$ and p be a prime number. If* $\deg(f \bmod p) = \deg(f)$ *and* $f \bmod p$ *is absolutely irreducible (i.e., over $\overline{\mathbb{F}_p}$) then f is absolutely irreducible (i.e, over $\overline{\mathbb{Q}}$).*

For instance, the polynomial

$$g = x^3 + y^3 + 7xy + 4y + x^2 + 5$$

is irreducible mod 5 and there (0,0) is a simple solution. Therefore, g is absolutely irreducible.

Now the good news is that by a theorem of Emmy Noether, there are only finitely many p for which an absolutely irreducible f over $\mathbb{Q}$ is not absolutely irreducible mod$p$. Moreover, there are also finitely many p for which f does not have simple solutions mod p. Combining these two results it is even possible to compute an explicit upper bound $B(f)$ for the largest "bad" prime p. This gives a deterministic algorithm. However, the bound is so large that this approach is completely impractical. Instead, J.-F. Ragot's idea is to use a few prime numbers to check whether a polynomial is absolutely irreducible. This is implemented by a very simple procedure which loops over a finite set of prime numbers p until the polynomial is found to be irreducible modulo p and to have a simple root in $\mathbb{F}_p$ (success) or the set of prime numbers is exhausted (failure).

The remaining question is to evaluate the probability of success of this technique and bound the probability that a failure corresponds to an absolutely irreducible polynomial.

2. Probability Estimates

2.1. **Irreducible Polynomials.** Let $q = p^n$ for p a prime number and n a positive integer. The number of polynomials of degree at most d over $\mathbb{F}_q[X] = \mathbb{F}_q[x_1,\ldots,x_r]$ is $q^{\omega(d,r)}$ where $\omega(d,r) = \binom{r+d}{d}$. From there and the fact that $\mathbb{F}_q[X]$ is a unique factorization domain it is possible to compute an exact formula for the number of irreducible polynomials of $\mathbb{F}_q[X]$ of degree at most d [1, 2]. Then very sharp inequalities can be obtained: for $r \geq 2$ and $d \geq 3$ the probability p that a polynomial of $F_q[X]$ of degree at most d be reducible obeys

$$\frac{q^r}{q^{\omega(d,r-1)}}\left(1 - \frac{5}{q}\right) \leq p \leq \frac{q^r}{q^{\omega(d,r-1)}}\left(1 + \frac{6}{q}\right).$$

2.2. **Polynomials having simple solutions.** For any $P \in \mathbb{F}_q^r$, the set of polynomials of degree at most d in $I(P) \setminus I(P)^2$ is a subspace of the vector space $\mathbb{F}_q[X]_d$ of polynomials of degree at most d. This makes it easier to compute the probability that a polynomial of degree d has a simple solution at a fixed point P or at a point P in a given set of points, since from the dimension D of a vector space over $\mathbb{F}_q$, its cardinality is given by q^D.

The quotients $\mathbb{F}_q[X]/I(P)^q$. We first consider the point $P = 0$. There are $\omega(p-1,r)$ monomials that cannot occur in a polynomial of $I(0)^p$. In terms of dimensions, this is equivalent to

$$\dim F_q[X]/I(0)^p = \omega(p-1,r). \tag{1}$$

This enumeration applies to any point P possibly different from 0.

Chinese remainder theorem. If $P_1 \neq P_2$ are two points of $\mathbb{F}_q^r$, it follows for instance from Bézout's theorem that $\mathbb{F}_q[X] = I(P_1)^p + I(P_2)^q$ for any p, q. One can therefore apply the Chinese remainder theorem which states the ring isomorphism

$$\mathbb{F}_q[X]/\bigcap_{i=1}^{n} I(P_i)^{p_i} = \prod_{i=1}^{n} \mathbb{F}_q[X]/I(P_i)^{p_i},$$

when the points P_i, $i = 1, \ldots, n$ are distinct. This translates into a result on the dimensions of the corresponding vector spaces:

$$\dim \left(\mathbb{F}_q[X]/\bigcap_{i=1}^{n} I(P_i)^{p_i} \right) = \sum_{i=1}^{n} \dim \mathbb{F}_q[X]/I(P_i)^{p_i}.$$

It follows from (1) that the quantity D in the left-hand side is finite, and for any degree $d \geq D$,

$$\dim \left(\mathbb{F}_q[X]_d \cap \bigcap_{i=1}^{n} I(P_i)^{p_i} \right) = \omega(d,r) - D. \tag{2}$$

Inclusion-Exclusion. Let again $P_1 \neq P_2$ be two points of $\mathbb{F}_q^r$. Then the number of polynomials having a simple solution at either P_1 or P_2, or both, is the cardinality of

$$\begin{aligned}
&\left(I(P_1) \setminus I(P_1)^2\right) \cup \left(I(P_2) \setminus I(P_2)^2\right) \\
&\qquad = I(P_1) \cup I(P_2) \setminus I(P_1)^2 \setminus I(P_2)^2 \setminus \left(I(P_1) \cap I(P_2)\right) \\
&\qquad\qquad \cup \left(I(P_1)^2 \cap I(P_2)\right) \cup \left(I(P_1) \cap I(P_2)^2\right) \setminus \left(I(P_1)^2 \cap I(P_2)^2\right).
\end{aligned}$$

The cardinalities are evaluated from the right-hand side by (1) and (2), which gives for $d \geq \omega(1,r) = 2r+2$

$$\begin{aligned}
&2q^{\omega(d,r)-\omega(0,r)} - 2q^{\omega(d,r)-\omega(1,r)} - q^{\omega(d,r)-2\omega(0,r)} + 2q^{\omega(d,r)-\omega(0,r)-\omega(1,r)} - q^{\omega(d,r)-2\omega(1,r)} \\
&\qquad = q^{\omega(d,r)} \left(1 - \left(1 - q^{\omega(0,r)} + q^{\omega(1,r)}\right)^2\right).
\end{aligned}$$

This extends to the case of n distinct points $P_1, \ldots, P_n$ to give that for $d > (r+1)n$, the proportion of polynomials in $\mathbb{F}_q[X]_d$ having at least one simple solution at one of the P_i's is

$$1 - \left(1 - \frac{1}{q} + \frac{1}{q^{r+1}}\right)^n. \tag{3}$$

Now it is sufficient to take $n = q^r$ the cardinality of $\mathbb{F}_q^r$ in the previous expression to obtain the probability that a random polynomial of degree $d \geq n$ has a simple solution at a point of $\mathbb{F}_q^r$.

Refining the Bound. The bound $d \geq q^r$ that we have just derived can be made much more precise by having a better look at the quotient on the left-hand side of (2) in the case $n = q^r$. The system of polynomials

$$\{(x_1^q - x_1)^2, \ldots, (x_r^q - x_r)^2\}$$

generates the ideal of polynomials having multiplicity at least 2 at every point of $\mathbb{F}_q^r$. This ideal is responsible for the largest value of D in (2), whence the bound q^r. It is easy to see that the system above is a *Gröbner basis* of this ideal for the lexicographic order. This means that one can take a basis of the quotient (as a vector space) where the polynomials of largest degree have degree $2q-1$. This way, one gets the following.

Proposition 1. [3] *For $d \geq r(2q-1)$, the proportion of polynomials of $\mathbb{F}_q[X]_d$ having a simple solution in $\mathbb{F}_q^r$ is*

$$1 - \left(1 - \frac{1}{q} + \frac{1}{q^{r+1}}\right)^{q^r}.$$

2.3. **Conclusion.** We are interested in polynomials that are irreducible *and* have a simple solution. Using both previous results yields a bound on the complementary event: the probability that a polynomial of degree $d > r(2p-1)$ is reducible or does not have a simple solution is upper bounded by

$$\frac{p^r}{p^{\omega(d,r-1)}}\left(1+\frac{6}{p}\right) + \left(1 - \frac{1}{p} + \frac{1}{p^{r+1}}\right)^{p^r},$$

where the first term is neglectible compared to the second one, the sum being of order

$$\exp(1/p)\exp(-p^{r-1}).$$

By taking several prime numbers p, we get a product of similar quantities which can be made as small as desired. Polynomials whose degree decreases when reduced mod p have to be taken into account, but their quantity does not change the final result much. Thus we get a bound on the probability that an absolutely irreducible polynomial hold the probabilistic algorithm in check.

Bibliography

[1] Carlitz (L.). – The distribution of irreducible polynomials in several indeterminates. *Illinois Journal of Mathematics*, vol. 7, 1963, pp. 371–375.

[2] Carlitz (L.). – The distribution of irreducible polynomials in several indeterminates. II. *Canadian Journal of Mathematics*, vol. 17, 1965, pp. 261–266.

[3] Ragot (Jean-François). – *Sur la factorisation absolue des polynômes.* – PhD Thesis, Université de Limoges, 1997.