INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Testing polynomial irreducibility without GCDs

Jörg Arndt

N° 6542

May 2008

Thème SYM

Rapport de recherche

ISSN 0249-6399 ISRN INRIA/RR--6542--FR+ENG

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

INRIA

centre de recherche NANCY - GRAND EST

Testing polynomial irreducibility without GCDs

Jörg Arndt*

Thème SYM — Systèmes symboliques
Équipe-Projet CACAO

Rapport de recherche n° 6542 — May 2008 — 6 pages

Abstract: We determine classes of degrees where testing irreducibility for univariate polynomials over finite fields can be done without any GCD computation. This work was partly funded by the INRIA Associate Team "Algorithms, Numbers, Computers" (`http://www.loria.fr/~zimmerma/anc.html`).

Key-words: finite fields, irreducible polynomial, GCD

* ANU, Canberra, `arndt@jjj.de`

Centre de recherche INRIA Nancy – Grand Est
LORIA, Technopôle de Nancy-Brabois, Campus scientifique,
615, rue du Jardin Botanique, BP 101, 54602 Villers-Lès-Nancy
Téléphone : +33 3 83 59 30 00 — Télécopie : +33 3 83 27 83 19

Test d'irréductibilité de polynôme sans PGCD

Résumé : Nous identifions des familles pour lesquelles le test d'irréductibilité de polynômes univariés sur un corps fini peut être effectué sans aucun PGCD. Ce travail a été réalisé en partie dans le cadre de l'équipe associée INRIA "Algorithms, Numbers, Computers" (`http://www.loria.fr/~zimmerma/anc.html`).

Mots-clés : corps fini, polynôme irréductible, PGCD

Recall Rabin's test for the irreducibility of a polynomial over GF(p) where p is prime [1, p.7]: A polynomial $C \in \mathrm{GF}(p)[x]$ of degree d is irreducible if and only if

$$x^{p^d} \equiv x \bmod C \tag{1}$$

and, for all prime divisors l_i of d,

$$\gcd\left(x^{p^{d/l_i}} - x \bmod C,\, C\right) = 1 \tag{2}$$

The number of GCD computations equals the number of prime divisors of d.

We call a polynomial C a *pseudo irreducible* (PI) if it has no linear factor and relation (1) holds. We denote by I_d the set of all irreducible polynomials of degree d, and by PI_d the set of all pseudo irreducibles of degree d.

A composite polynomial C of degree d can be a PI only if it has no square factor: relation (1) tells us that C must divide the polynomial $x^{p^d} - x$ which has no square factors. Let the factorization of a composite polynomial C that is a PI into irreducible polynomials C_j be

$$C = \prod_{j=1}^{f} C_j \tag{3}$$

then the degrees of all factors $d_j := \deg(C_j)$ must be divisors of d (the polynomial $x^{p^d} - x$ is the product of all irreducibles whose degrees divide d).

We define

$$L := \mathrm{lcm}_{j=1\ldots f}(d_j) \tag{4}$$

For a composite C that is a PI we have $x^{p^L} = x \bmod C$. This motivates our next definition.

We call a polynomial C of degree d that is a PI and for which the relation

$$x^{p^k} \neq x \bmod C \qquad \text{for} \quad 1 \leq k \leq d-1 \tag{5}$$

holds, a *strong pseudo irreducible* (SPI). We write SPI_d for the set of all polynomials of degree d that are SPI.

A composite C that is a SPI must factor into mutually distinct irreducibles C_j where all degrees d_j must divide d (so L divides d) and $L = d$.

The following algorithm (SPI-test) determines whether a polynomial $C \in \mathrm{GF}(p)[x]$ of degree d is a SPI:

1. If C has a linear factor then return false.
2. Set $t := x$.
3. Do the following $d-1$ times: set $t := t^p \bmod C$, if $t = x$ then return false.
4. Set $t := t^p \bmod C$, if $t \neq x$ return false.
5. Return true.

The detection of linear factors is cheap if the characteristic is small. For example, a binary polynomial has no linear factor if its constant term is one and its weight is odd. The costs of the test by evaluation at the nonzero elements of GF(p) is $\sim (p-1)\,d$.

Next we will identify classes of degrees where $I_d = SPI_d$, that is, testing for strong pseudo irreducibility is sufficient to determine irreducibility. Note that the test does not involve any GCD computations.

For a composite C that is SPI we have a factorization as in relation (3) and

$$d \;=\; \sum_{j=1}^{f} d_j \tag{6}$$

That is, the degrees of the irreducible factors are a partition of d into numbers d_j that are divisors of d where $2 \le d_j \le d$ and $L = d$.

Theorem 1 *If d is a prime power then $I_d = SPI_d$.*

Proof: Let $d = r^e$ where r is prime (and $e \ge 1$). The divisors of d that can appear in the partition given in relation (6) are r, r^2, $\ldots$, r^{e-1}. We have $L \le r^{e-1} < d$ so the polynomial cannot be a SPI. □

Theorem 2 *If d is the product of two primes then $I_d = SPI_d$.*

Proof: Let $d = r\,s$ where r and s are distinct primes. The divisors of d allowed in the partition are r and s. Let the partition be $d = a\,r + b\,s$. Now $d = r\,s \equiv a\,r \bmod s$, and as r and s are coprime, a must be a multiple of s. The choices for a are the following: firstly, $a = 0$ corresponding to the partition $d = 0\,r + r\,s$ (i.e., r factors of degree s) but then we have $L = s < d$; secondly, $a = s$ corresponding to the partition $d = s\,r + 0\,s$ (i.e., s factors of degree r) but then we have $L = r < d$ again. □

Now we give classes of degrees d where $I_d = SPI_d$ for polynomials over GF(p). Here the conditions for the degree depend on the characteristic p.

Let $d = r^e\,s$ where r and s are distinct primes. In the partitioning $d = \sum d_j$ we have $d_j = r^u\,s^v$ where u and v are nonnegative and $u + v < e + 1$.

We split the partitioning into two sets according to whether the divisors are pure powers of r: $d = R + R'$ where $R = \sum_{j:\gcd(s,d_j)=1} d_j$ and $R' = d - R = \sum_{j:\gcd(s,d_j)\ne 1} d_j$. For $L = d$ the divisors r^e must occur in the partitioning so $R \ne 0$. Also for $L = d$ some divisor d_j must have a factor s so $R' \ne 0$.

Now we determine the minimal value of R. As R is a sum of powers of r, R must be divisible by r. As R' is a sum of multiples of s, R' must be divisible by s. Thereby a partitioning with $L = d$ corresponds to a partition $d = R + R' = a\,r + b\,s$ where $a \ne 0$ and $b \ne 0$.

We have $d = a\,r + b\,s \equiv a\,r \bmod s$ and, since d has s as a factor, a must be a multiple of s: $a = u\,s$. The minimal value is $u = 1$, since $a \ne 0$, hence the minimal value of R is $R_{min} := s\,r$.

Therefore the factorization of C must contain a product of irreducible polynomials of degrees $d_j = r^{k_j}$ where $1 \le k_j \le e$ such that their product has degree

$\geq R_{min} = s\,r$. If the product of all irreducible polynomials of degrees r^k (where $1 \leq k \leq e$) has degree $< R_{min}$ then there is no partitioning of d that makes a composite polynomial C a SPI.

Write $D(n)$ for the degree of the product of all irreducible polynomials whose degrees are greater than one and divide n. The polynomial $x^{p^n} - x$ gives the product including linear irreducibles. There are p linear irreducibles, so we have $D(r^e) = p^{r^e} - p$.

For a composite C of degree $d = r^e\,s$ that is a SPI we must have $R_{min} \leq D(r^e)$, use $R_{min} = r\,s$ and divide by r to obtain $s \leq (p^{r^e} - p)/r$. Thus we have proved:

Theorem 3 *If $d = r^e\,s$ where r and s are different primes and $s > (p^{r^e} - p)/r$ we have $I_d = SPI_d$.*

For example, over GF(2) we have $I_d = SPI_d$ for the following cases where the bound is $< 10^9$:
$d = 4\,s$ and $s > (2^4 - 2)/2 = 7$,
$d = 8\,s$ and $s > (2^8 - 2)/2 = 127$,
$d = 9\,s$ and $s > (2^9 - 2)/3 = 170$,
$d = 16\,s$ and $s > (2^{16} - 2)/2 = 32,767$,
$d = 25\,s$ and $s > (2^{25} - 2)/5 = 6,710,886$, and
$d = 27\,s$ and $s > (2^{27} - 2)/3 = 44,739,242$.

The rapid growth of the bound renders the Theorem impractical for large characteristic. We give the cases where the bound is $< 10^9$ for characteristic 3:
$d = 4\,s$ and $s > 39$, $d = 8\,s$ and $s > 3,279$, $d = 9\,s$ and $s > 6,560$, and $d = 16\,s$ and $s > 21,523,359$.

For degrees d where $SPI_d \neq I_d$ the following test that delays the computation of the GCDs can be used:

1. Compute the factorization $d = \prod_{i=1}^{f} p_i^{e_i}$.
2. Set $t_0 := x$.
3. Do the following for $k = 1, 2, \ldots, d-1$: set $t_k := t_{k-1}^p \bmod C$, if $k = d/p_i$ then save $s_i := t_k$, if $t_k = x$ then return false.
4. Set $t_d := t_{d-1}^p \bmod C$, if $t_d \neq x$ return false.
5. Do the following for $i = 1, 2, \ldots, f$: set $g := \gcd(s_i, C)$, if $g \neq 1$ then return false.
6. Return true.

Depending on the ratio of the costs of powering and computing the GCD this test may be faster than Rabin's test. In the following we look at characteristic two. The speed of multiplication (and thereby powering) is very dependent on the weight of the polynomial modulus C. One of the most favorable cases for powering is when C is a trinomial. For fixed degree let S, M, and G be the time required for squaring, multiplication, and computing a GCD, respectively. For $d = 859,433$ Zimmermann [pers. comm.] gives the ratios $G/M \approx 30$ and $G/S \approx 8,800$ for a general purpose CPU (AMD Opteron 2.4GHz). When a hardware multiplier is available the ratio is much more in favor of the powering.

An average-case analysis of Rabin's algorithm is given in [2]. The fact that reducibility of a composite polynomial is almost always detected with the computation of the first GCD suggests that it may be a bad idea to postpone all GCDs. Instead one may proceed as in the test above, but compute $\gcd(s_1, C)$ as soon as s_1 is computed and postpone only the remaining GCDs. Even for degrees d where $SPI_d = I_d$ one might want to either compute the first GCD or exclude factors of small degrees by other means.

References

[1] Michael O. Rabin: **Probabilistic algorithms in finite fields**, Technical Report MIT-LCS-TR-213, Massachusetts Institute of Technology, (January-1979). Online at `http://publications.csail.mit.edu/`.

[2] Daniel Panario, Alfredo Viola: **Analysis of Rabin's polynomial irreducibility test**, Lecture Notes in Computer Science, vol.1380, pp.1-10, (1998).

Centre de recherche INRIA Nancy – Grand Est
LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399