J. Symbolic Computation (1987) **4**, 77–82

Deterministic Irreducibility Testing of Polynomials over Large Finite Fields†

ERICH KALTOFEN

Rensselaer Polytechnic Institute, Department of Computer Science,
Troy, New York 12181 *and*
Mathematical Sciences Research Institute,
1000 *Centennial Drive, Berkeley, California* 94720, *U.S.A.*

We present a sequential deterministic polynomial-time algorithm for testing dense multivariate polynomials over a large finite field for irreducibility. All previously known algorithms were of a probabilistic nature. Our deterministic solution is based on our algorithm for absolute irreducibility testing combined with Berlekamp's algorithm.

1. Introduction

Berlekamp (1970) first showed how the factoring problem for univariate polynomials over large finite fields could be solved in polynomial-time by introducing random choices. However, already Butler (1954) had established that the determination of the number of factors in polynomial-time does not require random choices. Although great effort has been spent in the last fifteen years to remove the necessity for random choices for the factoring problem (cf. Zassenhaus, 1969; Shanks, 1972; Moenck, 1977; Cantor & Zassenhaus, 1981; Camion, 1983; Schoof, 1985; Huang, 1985; von zur Gathen, 1985; Adleman & Lenstra, 1986), the problem remains in general unresolved. Only within the last five years has it been shown that for multivariate polynomials probabilistic polynomial time solutions exist as well (cf. Chistov & Grigoryev, 1982; von zur Gathen & Kaltofen, 1985; Lenstra, 1985). However, in the dense representation case these results did not quite parallel the univariate factorisation theory. The reason was that all the algorithms known needed to factor a univariate polynomial in order to determine irreducibility and therefore were not deterministic. Here we present an algorithm that tests dense multivariate polynomials over large finite fields for irreducibility in deterministic polynomial time. Contrary to most univariate deterministic factoring results, our solution is not subject to any unproven mathematical conjecture, such as the Riemann hypothesis.

We have observed (Kaltofen, 1985*a*) that absolute irreducibility of multivariate polynomials over large finite fields could be decided in polynomial time. Here we essentially modify the algorithm presented there to solve the problem of irreducibility over the field itself. It comes as a small surprise that irreducibility can be related to absolute irreducibility. Absolute irreducibility is a purely rational question, that is it can be decided by field arithmetic alone (Noether, 1922), whereas irreducibility over certain constructive fields can be shown undecidable (Fröhlich & Shepherdson, 1955). Our solution, which

† This material is based upon work supported by the National Science Foundation under Grant No. DCR-85-04391 and by an IBM Faculty Development Award. Part of this work was dône while the author was visiting the Tektronix Computer Research Laboratory in Beaverton, Oregon.

0747–7171/87/040077+06 $03.00/0

makes use of the Butler–Berlekamp Q-matrix construction seems to establish this relationship only for finite fields. It is therefore very special and does not contradict the differences of the problems known for arbitrary fields.

In this paper we restrict ourselves to bivariate polynomials. It is fairly easy to generalise our algorithms to dense multivariate polynomials, see e.g. Algorithm 2 in Kaltofen (1985*b*).

Notation: $\mathbb{F}_q$ denotes a finite field with q elements; $\deg_x(f)$ denotes the highest degree of x in $f \in \mathbb{F}_q[y, x]$ and $\deg(f)$ the total degree of f. The coefficient of the highest power of x in f, a polynomial in y, is referred to as the leading coefficient of f in x and will be denoted by $\mathrm{ldcf}_x(f)$. We call f monic in x if $\mathrm{ldcf}_x(f)$ is the one of $\mathbb{F}_q$. By $F[[z]]$ we denote the formal power series over F in z.

2. Previous Results Needed

We now discuss several facts needed in the deterministic irreducibility test. First we observe that the input polynomial $f \in \mathbb{F}_q[y, x]$ can be assumed monic in x and $f(0, x)$ can be assumed squarefree. The preprocessing necessary to enforce these conditions is discussed, e.g. in Kaltofen (1985*b*), §4, or in Kaltofen (1985*a*), §2. Notice that the translation necessary to make $f(0, x)$ squarefree requires

$$q \geqslant 2 \deg_x(f) \deg_y(f).$$

We can also assume this because otherwise even the factorisation problem in $\mathbb{F}_q[y, x]$ can be solved in deterministic polynomial time, cf. von zur Gathen & Kaltofen (1985), §4.2. It should be also noted that the monicity requirement can be at all avoided by slightly changing the algorithm along the lines of von zur Gathen & Kaltofen (1985), Remark 2.4. An even simpler way to get monicity than the methods referred to above would be to translate the original polynomial as $f(x, y+bx)$ for a suitable $b \in \mathbb{F}_q$, see Kaltofen (1985*c*), Lemma 6.1. We could also have restricted ourselves to q being a prime since the algorithm in Trager (1976) can reduce the problem of irreducibility testing over algebraic extensions to that of irreducibility testing over the base field in deterministic polynomial time. However, this restriction does not simplify our proofs but would drastically increase the complexity of the complete algorithm.

We now outline the basic algorithm from Kaltofen (1985*b*) for testing multivariate polynomials for irreducibility. We will not prove the correctness of this algorithm here but refer the reader to Kaltofen (1985*b*), §5, for more details on the algorithm and the necessary arguments.

Algorithm 1

[Given $f(y, x) \in F[y, x]$ monic in x, $f(0, x)$ squarefree, F an arbitrary field, and given an irreducible factor $t(z)$ of $f(0, z)$ in $F[z]$, this algorithm determines irreducibility of f over F:]

```
(N) [Compute approximation of root in $G[[y]]$, where $G = F[z]/(t(z))$:]
    $n \leftarrow \deg_x(f)$; $d \leftarrow \deg_y(f)$; $k \leftarrow (2n-1)d$; $a_0 \leftarrow (z \bmod t(z)) \in G$.
    By Newton iteration, calculate $a_1, \ldots, a_k \in G$ such that
        $f(y, a_0 + a_1 y + \cdots + a_k y^k) \equiv 0 \bmod y^{k+1}$.
    FOR $i \leftarrow 0, \ldots, n-1$ DO $\alpha^{(i)} \leftarrow (a_0 + \cdots + a_k y^k)^i \bmod y^{k+1} \in G[y]$.
```

(L) [Try to find a polynomial of degree $n-1$ in $F[y, x]$ for which $\alpha^{(1)}$ is the approximation for one of its roots:]

Try to solve the equation

$$\alpha^{(n-1)}+\sum_{i=0}^{n-2} u_i(y)\alpha^{(i)} \equiv 0 \bmod y^{k+1} \tag{1}$$

for polynomials $u_i \in F[y]$ with $\deg(u_i) \leqslant d$. This equation leads to a linear system over F in $(k+1)\deg(t)$ equations and $(n-1)(d+1)$ unknown coefficients of u_i. If there exists a solution then RETURN ("reducible"). Otherwise RETURN ("irreducible"). □

The problem is that $t(z)$ cannot be found in deterministic polynomial time. It turns out that in the absolute irreducibility test we can work with $f(0, z)$ instead. The following theorem establishes the connection between working with any irreducible factor of $f(0, z)$, as we may, and working with $f(0, z)$.

THEOREM 1 (Butler, 1954). *Let $f(z) \in \mathbb{F}_q[z]$ be monic and squarefree of degree $n, f=f_1 \cdots f_r$ be its factorisation into monic irreducible polynomials. Consider the subalgebra of $\mathbb{F}_q[z]/(f(z))$,*

$$V(f(z)) := \{v(z) | \deg(v) < n, (v \bmod f_j) \in \mathbb{F}_q \text{ for all } 1 \leqslant j \leqslant r\},$$

and the matrix

$$Q(f) := [a_{i,j}]_{0 \leqslant i, j \leqslant n-1}, \quad \text{where} \quad a_{i,0}+a_{i,1}z+\cdots+a_{i,n-1}z^{n-1} :\equiv (z^{iq} \bmod f(z)).$$

Then

$$v_0+v_1z+\cdots+v_{n-1}z^{n-1} \in V(f(z))$$

if and only if

$$(v_0, v_1, \ldots, v_{n-1})Q(f) = (v_0, v_1, \ldots, v_{n-1}). \ \square$$

The importance of this theorem to our irreducibility test is that membership of v in $V(f(z))$ can be enforced by linear relations on the coefficients of v. Let $v^{[1]}, \ldots, v^{[r]}$ be a basis for the left null-space of $Q(f)-I_n$, where I_n is the $n \times n$ identity matrix. Then $v \in V(f(z))$ if and only if

$$(w_1, \ldots, w_r)\begin{bmatrix} v_0^{[1]} & \cdots & v_{n-1}^{[1]} \\ \vdots & & \vdots \\ v_0^{[r]} & \cdots & v_{n-1}^{[r]} \end{bmatrix} = (v_0, \ldots, v_{n-1})$$

is solvable for w_i over $\mathbb{F}_q$.

3. Deterministic Irreducibility Testing

We now present the deterministic irreducibility test in $\mathbb{F}_q[y, x]$. The algorithm is very similar to Algorithm 1, but instead of working in G we work in $\mathbb{F}_q[z]/(f(0, z))$. This leads to an algorithm like Algorithm 2 of Kaltofen (1985*a*) except that the final linear solution is restricted further.

ALGORITHM 2

[Given $f(y, x) \in \mathbb{F}_q[y, x]$ monic in x, $f_0(x) := f(0, x)$ squarefree, this algorithm determines whether f is irreducible.]

(N) [Approximate a root of $f(y, x)$ in $R[[y]]$, where $R = \mathbb{F}_q[z]/(f_0(z))$:]
$n \leftarrow \deg_x(f)$; $d \leftarrow \deg_y(f)$; $k \leftarrow (2n-1)d$; $a_0 \leftarrow z \bmod f_0(z) \in R$.
By Newton iteration (cf. Kaltofen, 1985*a*, Algorithm 2, Steps I and N), calculate $a_1, \ldots, a_k \in R$ such that

$$f(y, a_0 + a_1 y + \cdots + a_k y^k) \equiv 0 \bmod y^{k+1}.$$

FOR $i \leftarrow 0, \ldots, n-1$ DO $\alpha^{(i)} \leftarrow (a_0 + \cdots + a_k y^k)^i \bmod y^{k+1}$.

(Q) Find a basis $\{v^{[1]}, \ldots, v^{[r]}\}$ for the left null-space of $Q(f_0) - I_n$, see Theorem 1. [More details for this step can be found in Knuth (1981), §4.6.2. Note that $z^q \bmod f_0(z)$ is computed by binary exponentiation.]

(L) [Try to find a polynomial of degree $n-1$ in $V(f_0(z))[y, x]$, $V(f_0(z))$ as defined in Theorem 1, for which $\alpha^{(1)}$ is the approximation for one of its roots:]
Examine whether the equation

$$\alpha^{(n-1)} + \sum_{i=0}^{n-2} u_i(y)\alpha^{(i)} \equiv 0 \bmod y^{k+1} \tag{2}$$

is solvable for polynomials $u_i(y) \in V(f_0(z))[y]$ such that $\deg(u_i) \leqslant d$. Let

$$u_i(y) = \sum_{\delta=0}^{d} u_{i,\delta} y^\delta$$

and let

$$\alpha^{(i)} = \sum_{\kappa=0}^{k} a_\kappa^{(i)} y^\kappa, \quad a_\kappa^{(i)} \in R.$$

Then (2) leads to the linear system for the coefficients of y^κ

$$a_\kappa^{(n-1)} + \sum_{i=0}^{n-2} \sum_{\delta=0}^{d} a_{\kappa-\delta}^{(i)} u_{i,\delta} = 0 \tag{3}$$

for $\kappa = 0, \ldots, k$ in the variables $u_{i,\delta} \in V(f_0(z))$, $i = 0, \ldots, n-2$, $\delta = 0, \ldots, d$. Let

$$u_{i,\delta} = \sum_{j=0}^{n-1} u_{i,\delta,j} z^j, \quad a_\kappa^{(i)} = \sum_{j=0}^{n-1} a_{\kappa,j}^{(i)} z^j,$$

and let

$$z^\lambda \equiv \sum_{j=0}^{n-1} c_{\lambda,j} z^j \bmod f_0(z), \quad \lambda = n, \ldots, 2n-2, c_{\lambda,j} \in \mathbb{F}_q.$$

Then the coefficient of z^l, $0 \leqslant l \leqslant n-1$, for each equation in (3) is, setting $a_{\delta,j}^{(i)}$ and $u_{i,\delta,j}$ to 0 for $j \geqslant n$, $\delta < 0$,

$$a_{\kappa,l}^{(n-1)} + \sum_{i=0}^{n-2} \sum_{\delta=0}^{d} \left(\sum_{j=0}^{l} a_{\kappa-\delta,l-j}^{(i)} u_{i,\delta,j} + \sum_{\lambda=n}^{2n-2} \sum_{j=0}^{\lambda} c_{\lambda,l} a_{\kappa-\delta,\lambda-j}^{(i)} u_{i,\delta,j} \right), \tag{4}$$

which is a linear expression in $u_{i,\delta,j}$ and which must vanish on a solution of (3).

Furthermore, $u_{i,\delta}$ must be an element in $V(f_0(z))$. We introduce new unknowns $w_{i,\delta,\rho}$, $1 \leqslant \rho \leqslant r$, and require that

$$(w_{i,\delta,1}, \ldots, w_{i,\delta,r})[v_j^{[l]}]_{\substack{1 \leqslant l \leqslant r \\ 0 \leqslant j \leqslant n-1}} = (u_{i,\delta,0}, \ldots, u_{i,\delta,n-1}) \tag{5}$$

be solvable for all $0 \leqslant i \leqslant n-2$, $0 \leqslant \delta \leqslant d$. Equation (5) leads to the linear equations

$$u_{i,\delta,j} - \sum_{\rho=1}^{r} v_j^{[\rho]} w_{i,\delta,\rho}, \quad 0 \leqslant j \leqslant n-1. \tag{6}$$

Equations (4) and (6) determine a linear system over $\mathbb{F}_q$ in

$$n(k+1)+(n-1)n(d+1)$$

equations and

$$(n+r)(n-1)(d+1)$$

unknowns. If this system has a solution, we return "f is reducible in $\mathbb{F}_q$", otherwise, we return "f is irreducible". □

We will not fully analyse this algorithm because its running time is inferior to that of Algorithm 1 in conjunction with finding $t(z)$ probabilistically. The algorithm is clearly polynomial in $\log(q)$ and does not require random choices. However, its correctness needs explanation. First let us formulate our main result in a theorem.

THEOREM 2. *Algorithm* 2 *correctly decides irreducibility of f in $\mathbb{F}_q[y, x]$ in* $(\log(q)\deg(f))^{O(1)}$ *sequential deterministic steps.*

PROOF. Solving the linear system determined by (4) and (6) is by theorem 1 equivalent to solving (2) for $u_i(y) \in V(f_0(z))[y]$. If (2) has a solution, then for an irreducible factor $t(z)$ of $f_0(z)$, $u_i(y) \bmod t(z) \in \mathbb{F}_q[y]$. Thus by applying Algorithm 1 to f and t, f must be composite. On the other hand, if f is composite, Algorithm 1 will find a solution to (1) for *all* irreducible factors $t_\rho(z)$ of $f_0(z)$. By the Chinese remainder, Theorem (2) now becomes solvable for $u_i(y) \in V(f_0(z))[y]$. Therefore the algorithm will correctly determine the compositeness of f. □

We remark that Algorithm 3 of Kaltofen (1985*a*) applies to the solution of (4) and (6) as well. Depending on f that algorithm may split $f_0(z)$.

4. Conclusion

We have resolved one problem left open during the polynomial-time polynomial factorisation tempest of 1982, namely that random choices are not needed to test multivariate polynomials over large finite fields for irreducibility. In order to completely parallel the univariate results it would be necessary to also compute the number and the degrees of all irreducible factors without probabilistic choices. Unfortunately, it is not clear to us how our algorithm could accomplish that and we must leave this question for future research.

References

Adleman, L. M., Lenstra, H. W. (1986). Finding irreducible polynomials over finite fields. *Proc. 18th ACM Symp. Theory Comp.*, pp. 350–355.

Berlekamp, E. R. (1970). Factoring polynomials over large finite fields. *Math. Comp.* **24**, 713–735.

Butler, M. C. R. (1954). On the reducibility of polynomials over a finite field. *Quart. J. Math., Oxford Ser. (2)*, **5**, 102–107.

Camion, P. (1983). A deterministic algorithm for factorizing polynomials of $F_p[x]$. *Ann. Discrete Math.* **17**, 149–157.

Cantor, D. G., Zassenhaus, H. (1981). A new algorithm for factoring polynomials over finite fields. *Math. Comp.* **36**, 587–592.

Chistov, A. L., Grigoryev, D. Yu. (1982). Polynomial-time factoring of multivariable polynomials over a global field. *LOMI preprint E-5-82*, Steklov Institute, Leningrad.

Fröhlich, A., Shepherdson, J. C. (1955/56). Effective procedures in field theory. *Phil. Trans. Roy. Soc., Ser. A*, **248**, 407–432.

von zur Gathen, J. (1985). Factoring polynomials and primitive elements for special primes. Manuscript.

von zur Gathen, J., Kaltofen, E. (1985). Factoring multivariate polynomials over finite fields. *Math. Comp.* **45**, 251–261.

Huang, M.-D. A. (1985). Riemann hypothesis and finding roots over finite fields. *Proc. 17th ACM Symp. Theory Comp.*, pp. 121–130.

Kaltofen, E. (1985*a*). Fast parallel absolute irreducibility testing. *J. Symbolic Computation* **1**, 57–67.

Kaltofen, E. (1985*b*). Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM J. Comp.* **14**, 469–489.

Kaltofen, E. (1985*c*). Greatest common divisors of polynomials given by straight-line programs. Math. Sci. Research Inst. Preprint, vol. 01918-86, Berkeley, CA, 1986. Expanded version in *J. ACM* to appear. Preliminary version under the title "Computing with polynomials given by straight-line programs I: Greatest common divisors" in *Proc. 17th ACM Symp. Theory Comp.*, pp. 131–142.

Knuth, D. E. (1981). *The Art of Programming, vol. 2, Semi-numerical Algorithms, ed. 2.* Reading, MA: Addison-Wesley.

Lenstra, A. K. (1985). Factoring multivariate polynomials over finite fields. *J. Comput. System Sci.* **30**, 235–248.

Moenck, R. (1977). On the efficiency of algorithms for polynomial factoring. *Math. Comp.* **31**, 235–250.

Noether, E. (1922). Ein algebraisches Kriterium für absolute Irreduzibilität. *Math. Ann.* **85**, 26–33.

Schoof, R. J. (1985). Elliptic curves over finite fields and the computation of square roots mod *p*. *Math. Comp.* **44**, 483–494.

Shanks, D. (1972). Five number-theoretical algorithms. *Proc. 2nd Manitoba Conf. Numerical Math.*, pp. 51–70.

Trager, B. M. (1976). Algebraic factoring and rational function integration. *Proc. 1976 ACM Symp. Symbolic Algebraic Comp.*, pp. 219–228.

Zassenhaus, H. (1969). On Hensel factorization I. *J. Number Theory* **1**, 291–311.