

SOLVING QUADRATIC EQUATIONS OVER POLYNOMIAL RINGS OF CHARACTERISTIC TWO

JØRGEN CHERLY, LUIS GALLARDO,
LEONID VASERSTEIN AND ETHEL WHELAND

Abstract

We are concerned with solving polynomial equations over rings. More precisely, given a commutative domain A with 1 and a polynomial equation $a_n t^n + \cdots + a_0 = 0$ with coefficients a_i in A , our problem is to find its roots in A .

We show that when $A = B[x]$ is a polynomial ring, our problem can be reduced to solving a finite sequence of polynomial equations over B . As an application of this reduction, we obtain a finite algorithm for solving a polynomial equation over A when A is $F[x_1, \dots, x_N]$ or $F(x_1, \dots, x_N)$ for any finite field F and any number N of variables.

The case of quadratic equations in characteristic two is studied in detail.

1. Introduction

Let A be a commutative domain with 1. We consider an equation

$$(1) \quad a_n t^n + \cdots + a_0 = 0$$

for t with given a_i in A . We call such an equation a polynomial equation over A of degree $\leq n$ (or degree n if $a_n \neq 0$). Its roots t are to be found in A .

We will show that when $A = B[x]$, the polynomial ring in one variable x , then solving (1) can be reduced to solving a finite system of polynomial equations over B . Each of these equations has degree at most n , and the number of the equations can be bound in terms of degrees of a_i .

By induction on N , this gives a reduction of the problem over $A = E[x_1, \dots, x_N]$ to solving a finite sequence of equations over E . When E is a finite field or the ring of integers, there are finite algorithms

for solving polynomial equations over E . So we obtain a finite algorithm for solving (1) over $A = E[x_1, \dots, x_N]$. Solving (1) over the field R of quotients of A can be easily reduced to solving a similar equation with a monic polynomial in $A[t]$ whose roots over R belong to A . So we also obtain a finite algorithm for solving (1) over the field $A = E(x_1, \dots, x_N)$ when E is a finite field or the field of rational numbers. This can be generalized to subrings A of $E(x_1, \dots, x_N)$ when the membership in the subring can be decided in finitely many steps.

A more general problem of factorization of multivariate polynomials in any degree with coefficients in finitely generated fields has been considered before (see [2], [4]). As will be seen, we take a different approach to this problem.

Given a quadratic equation, that is, (1) with $n = 2$, $a_2 \neq 0$, a well-known formula reduces it to an equation of the form $y^2 = \Delta$ and a linear equation, provided that $2A \neq 0$. We consider in detail the case $2A = 0$ when, obviously, the above-mentioned formula doesn't apply.

2. Reduction from $A = B[x]$ to B

Given $a_i \in A = B[x]$, we want to solve (1) in A . If $a_n = 0$ or $a_0 = 0$, then (1) reduces to an equation of a smaller degree, so we will assume that $a_n a_0 \neq 0$.

First we obtain bounds for the degree $d = \deg(t)$ of a solution $t \in A = B[x]$ of (1) in terms of $d_i = \deg(a_i)$ (with the convention that $\deg(0) = -\infty$).

Proposition 1. *If (1) with $a_n a_0 \neq 0$ has a root $t \in A = B[x]$, then*

$$\deg(t) \leq \min(d_0, \max_{i=0, \dots, n-1} ((d_i - d_n)/(n - i))).$$

Proof: Since t divides a_0 , $\deg(t) \leq d_0$. If $\deg(t) > (d_i - d_n)/(n - i)$ for all i , then the term $a_n t^n$ has a higher degree in x than any other term in the left hand side of (1). ■

Remark. If we plot the points $(0, d_n), \dots, (n+1, d_0)$ in the Euclidean plane and consider the least concave function $D(i) \leq d_{n-i}$, then the maximum in the proposition is the slope of $D(i)$ at $i = 0$, which is the largest slope of D . If this slope is negative, i.e., $d_n > d_i$ for $i < n$, then (1) has no solutions in A .

In general there are at most n distinct slopes of D , and the bound for $\deg(t)$ in the proposition can be improved as follows: $\deg(t)$ is at most the largest slope not exceeding d_0 .

Theorem 1. *Finding all roots t in $A = B[x]$ of a given degree d for (1) with $n \geq 1$ can be reduced to solving in B a finite sequence of at most $1 + n + \cdots + n^d$ polynomial equations in one variable over B , each of them of degree $\leq n$.*

Proof: Without loss of generality, we can assume that $a_n \neq 0$. We proceed by induction on d . When $d = -\infty$, i.e., $t = 0$, we do not need to solve any equations (we have to check only whether a_0 is 0).

When $d = 0$, (1) is equivalent to a system of at most $\max(\deg(a_i))$ polynomial equations over B for $t \in B$, each of them of degree $\leq n$. We solve one of them and then verify the other equations for each of at most n roots in B .

Assume now that $d \geq 1$. Let $t = t_0 + x s$ with $t_0 \in B$, $s \in A = B[x]$, $\deg(s) = d - 1$. Taking the smallest degree terms in (1), we obtain a polynomial equation for t_0 over B of positive degree $\leq n$. Solving it, we obtain at most n values for t_0 in B . Substituting each of them in (1), we obtain a polynomial equation of degree $\leq n$ for $s \in B[x]$ with $\deg(s) \leq n - 1$. Using the induction hypothesis, we reduce the problem of finding all roots of degree d for (1) to solving at most $1 + n (1 + n + \cdots + n^{d-1}) = 1 + n + \cdots + n^d$ equations over B (and verifying several equalities in B). ■

Assuming that we can solve polynomial equations over B , we can solve (1) over A in finitely many steps, using Theorem 1 together with Proposition 1. To get a good bound for the number of steps needed, one has to be able to control a possible branching.

When the left hand side of (1) is 0, every $t \in A = B[x]$ satisfies (1). Assume that $a_n \neq 0$, $n \geq 0$ in (1). When $n = 0$, (1) has no solutions.

Let now $n = 1$. When $d_1 = \deg(a_1) > d_0 = \deg(a_0)$, (1) has no roots in A . Otherwise, it has at most one root t , and $\deg(t) = d_0 - d_1 = d$. Substituting $t = \sum_{i=0}^d t_i x^i$ into the equation $a_1 t + a_0 = 0$, we obtain $d_0 + 1$ equations for t_i in B , each of them of degree ≤ 1 . As in the general case, we can find $t_0, t_1, \dots$ consecutively. There is no branching. The total number of equations in one variable over B we have to solve is $d + 1$, and we have to verify d_1 equalities.

We could also proceed from the other end, finding $t_d, t_{d-1}, \dots, t_0$ consecutively. Then the equations we have to solve are of the form $bt_i = c_i$, where $b \in B$ is the leading coefficient of $a_1 \in A = B[x]$, $c_i \in B$, and $i = d, d-1, \dots, 0$.

The rest of the paper is about the case $n = 2$. In a future paper, we will apply our methods to higher degree equations.

3. Quadratic equations in characteristic two

The well-known formula for solving the quadratic equation

$$(2) \quad a_2 t^2 + a_1 t + a_0 = 0$$

with $a_2 \neq 0$ does not work when we cannot divide by two in our ring A containing the given coefficients a_i . If we are looking for roots of (2) in a field A , then a linear change of variables reduces the equation to one of two particular forms,

$$(3) \quad y^2 + \Delta = 0$$

when $a_1 = 0$ and

$$(4) \quad y^2 + y + \Delta = 0$$

when $a_1 \neq 0$.

Junjie Tang [10], solved (2) when A is a finite field F of characteristic two. In this case, $y = \Delta^{q/2}$ is a root of (3) with $q = \text{card}(A)$, and (4) has roots in A if and only if $\text{Tr}(\Delta) = 0$, where Tr is the trace from A to $GF(2)$ (Niederreiter [8]) (see Section 6 below for more details).

In this paper we are interested in solving (2) in a commutative domain A of characteristic two. This means that the given coefficients a_i belong to A , $2A = 0$, and we are looking for roots in A . We show that when $A = B[x]$ is a polynomial ring in one variable x (hence B is a commutative domain of characteristic 2), then solving a quadratic equation (2) in A can be reduced to solving several quadratic equations over B . The number of these equations is at most $\deg(a_0) + \deg(a_2) + 1$.

In particular, we get an effective algorithm for solving (2) over $A = F[x_1, \dots, x_k]$ for a finite field F .

The number of steps in our method is $O(\deg(a_0 a_2))$, at each step we solve (3) with a number $\Delta \in F$, except perhaps at one step, where we might have to solve (4) instead of (3).

When F is finite, it is easy to solve (3) and (4) with $\Delta \in F$. Namely, $y = \Delta^{q/2}$ is a root of (3) with $q = \text{card}(F)$, and solving (4) will be discussed in Section 6. In general solving (2) over $A = B[x]$ depends on solving (2) over B .

The main equation studied in the rest of the paper is (2) with $a_2 = 1$, namely

$$(5) \quad t^2 + a_1 t + a_0 = 0.$$

We can reduce (2) to an equation of the form (5) by a change of variable. More precisely, the roots $t = u/a_2$ of (2) are in 1-1 correspondence with the roots of $u^2 + a_1u + a_2a_0 = 0$ with u divisible by a_2 .

If $a_1 = 0$ in (5), i.e., we have an equation of the form (3), then it is reduced to a set of similar equations over B . Namely, (3) has a solution if and only if all the monomials in $\Delta \in B[x]$ have even degree (i.e., $\Delta' = 0$) and all the coefficients are squares. The solution, if it exists, is unique. In the case when B is a finite field with q elements, the explicit solution is $t = \sum c_{2i}^{q/2} x^i$ for $\Delta = \sum c_{2i} x^{2i}$. It can be computed in $O(\log(q) \deg(\Delta))$ multiplications in B (when $\deg(\Delta) \geq 1$).

So in the rest of the paper we assume that $a_1 \neq 0$ in (5). We will apply the method of Section 2 to (5) in the next section. In Section 5 we give a method of reducing the degree of a_1 in (5) to 0. Section 6 deals with (5) with constant a_1 . Without loss of generality, we can assume that $a_0 \neq 0$, because otherwise (5) reduces to a degree one equation.

Note that (5) has a root in a domain A if and only if the polynomial $t^2 + a_1t + a_0 \in A[t]$ is reducible. When $A = F[x]$ with a finite field F of characteristic two, there is a well-known irreducibility criterion using reduction modulo a polynomial p :

Theorem 2. *Let $F = GF(2^m)$, $a_0, a_1 \in F[x]$, $a_1 \neq 0$, and let α be one element of the algebraic closure of $GF(2)$, such that its minimal polynomial p over F is relatively prime with a_1 . Suppose that*

$$(6) \quad \text{Tr}(a_0(\alpha)/a_1(\alpha)^2) = 1.$$

Then $t^2 + a_1t + a_0$ is irreducible in the ring $F[x, t]$.

The trace Tr is always taken over the prime subfield $GF(2) = F_2$.

For example, the polynomial $t^2 + (x^2 + x)t + x^3 + x$ over $F_2[x]$ has no roots $t \in F_2[x]$, as seen by choosing the irreducible polynomial $p = x^2 + x + 1$, or, with a slightly more complicated computation, by choosing $p = x^3 + x + 1$, and it is clear that picking p of degree one gives no information here.

Besides the obstructions for existence of roots of (5) given by Theorem 2 (in the particular case when B is finite), there are degree obstructions (on degrees of a_0, a_1) given by the following proposition (for any domain B). The proof is easy and will be left to the reader.

Proposition 2. *Suppose that (5) with $a_0a_1 \neq 0$ has a root t in $B[x]$, where B is a domain. Set $r = \infty$ when $a_1 \in B$, and $r = \deg(a_0)/\deg(a_1^2)$ otherwise.*

- (a) $2r \geq 1$.
- (b) *If $r \leq 1$, then one of the roots t of (5), is such that $\deg(t) = \deg(a_0) - \deg(a_1)$.*
- (c) *If $r = 1$, then both roots have the same degree, equal to $\deg(a_1)$, and $B \neq F_2$.*
- (d) *If $r > 1$, then the two roots t and $-t - a_1$ of (5) have the same degree, $\deg(a_0)$ is even and $\deg(t) = \deg(a_0)/2 = \deg(t + a_1)$.*

4. Solving (5) by the method of Section 2

We consider (5) with $a_0a_1 \neq 0$ over $B[x]$ with a domain B of characteristic 2. Set $d_i = \deg(a_i)$. We will show that finding a root of (5) can be reduced to solving $1 + \max(d_0/2, d_0 - d_1)$ equations over B of degree 1 or 2. More precisely, we have $\max(d_0/2 - d_1, 0)$ equations of type (4), at most one quadratic equation over B with a nonzero linear term, and $1 + \max(d_0 - d_1, d_1)$ linear equations over B .

Let r be as in Proposition 2. We will show that solving (5) with $r \geq 1$ can be reduced to solving a similar equation with $r < 1$ by solving a few quadratic equations over B , and that solving (5) with $r < 1$ can be reduced to solving a few linear equations over B . Let $t = \sum_{i=0}^d t_i x^i$ be an unknown root of (5) with $d \neq 0$.

When $r < 1$, we can assume that $d = d_0 - d_1$ by Proposition 2. We have a linear equation $t_d b = c_d$ for t_d , where b is the leading coefficient of a_1 and c_d is the leading coefficient of a_0 . If this equation has a root $t_d \in B$, we have a linear equation $t_{d-1} b = c_{d-1}$ with the same b and some $c_{d-1} \in B$. So consecutively solving $d + 1$ linear equations of the form $t_i b = c_i$ over B for $i = d, d - 1, \dots$, we solve (5) for t .

When $r = 1$ (this case is impossible when $B = F_2$), $d = d_1 = d_0/2$ by Proposition 2. We obtain a quadratic equation $t_d^2 + b t_d + c = 0$, where b is the leading coefficient of a_1 and c is the leading coefficient of a_0 . Having chosen a root t_d (if it exists), we obtain an equation for the rest of t of the form (5) with $r < 1$. This equation can be reduced as above to d linear equations over B .

When $r > 1$, $d = \deg(a_0)/2$ by Proposition 2. To find the leading coefficient t_d of t , we utilize the equation $t_d^2 = c_d$, where c_d is the leading coefficient of a_0 . This equation over B has at most one root. Once

t_d is found, we have a similar equation for t_{d-1} , and so on. Thus, we consecutively obtain equations $t_i^2 = c_i$ for $i = d, \dots, d_1 + 1$. For the rest of t , we solve, as above, one quadratic and $d_1 - 1$ linear equations over B .

In all three cases, there are $2d + 1$ equations over B (some of which do not contain unknown coefficients t_i of t). We find these $d + 1$ coefficients (if they exist) from $d + 1$ of the equations. Then we can check whether the other d equations hold.

Remark. Assume that B is a field, and consider the fraction $a_0/a_1^2 = u/v$ reduced to lowest terms in $B[x]$, i.e., such that $\gcd(u, v) = 1$, with monic v . When (5) has a root, it is easy to see that v is the square of a polynomial. The Eisenstein criterion follows from this observation.

5. Induction on d_1

As above, B is a domain of characteristic 2.

The idea is to write any polynomial $p \in B[x]$ as $p = f + xg$, where $f = (xp)'$ is the sum of even degree terms in p and $xg = xp'$ is the sum of odd degree terms in p .

Theorem 3. *Suppose that (5) has a root $t \in B[x]$. Then $a_1^2 \mid (a_0')^2 + a_1'(a_1 a_0)'$.*

Proof: Differentiating (5) we obtain

$$(7) \quad a_1' t = a_1 t' + a_0'.$$

Squaring (7) and applying (5) we obtain $(a_1')^2(a_1 t + a_0) + a_1^2(t')^2 = (a_0')^2$. Using (7) to eliminate $a_1' t$, we get

$$(8) \quad a_1^2((t')^2 + a_1' t') + (a_0')^2 + a_1'(a_1 a_0)' = 0$$

which proves the conclusion of the theorem. ■

Remark. Suppose that $Aa_1 + Aa_1' = A = B[x]$ and that the leading coefficient of a_1 is invertible in B (when B is a field, this means that a_1 is square-free). Then the conclusion of the theorem is equivalent to $a_1 \mid (a_1')^2 a_0 + (a_0')^2$. If, furthermore, $d_0/2 \leq d_1 < d_0$, then a root t of (5) in A can be found as the polynomial t such that $a_1' t \equiv a_0'$ modulo a_1 and $\deg(t) < \deg(a_1) = d_1$.

Now we write down the reduction step. We will show that when (5) has a root, say $t = (xt)' + xt'$, then t' satisfies a ‘smaller’ quadratic equation of type (5). To obtain such an equation

$$(t')^2 + a'_1 t' + ((a'_0)^2 + a'_1(a_1 a_0)')/a_1^2 = 0$$

we divide (8) by a_1^2 ; if the constant term is not divisible by a_1^2 then (5) has no roots by Theorem 3.

Note that all coefficients in this equation are polynomials in x^2 , and the unknown root t' is also a polynomial in x^2 : $t'(x) = f(x^2)$. So we obtain a quadratic equation for f of the form $f^2 + a_3 f + a_2 = 0$ with $\deg(a_3) \leq (\deg(a_1) - 1)/2$.

Once we find f and hence t' , we can find t from (7) when $a'_1 \neq 0$. When $a'_1 = 0$, we can use the linear equation (7) to find t' , rather than the quadratic equation (8). Then, to reconstruct the even part $(xt)'$ of t we can use the even part of (5), i.e.,

$$(9) \quad (xt)'^2 + (xa_1)'(xt)' + (xt')^2 + (xa_0)' + x^2 a'_1 t' = 0.$$

This is a quadratic equation for $(xt)'$ of type (5) with linear coefficient $(xa_1)' = a_1$. Moreover, writing the coefficients and $(xt)'$ as polynomials in x^2 , we obtain a similar equation with the linear coefficient having degree equal to half the degree of a_1 .

Repeating this process at most $\lceil \log_2(\deg(a_1)) \rceil$ times, we either obtain (5) with a constant linear term, or at some step we are in violation of the conclusion of Theorem 3 (in which case the original equation (5) has no roots).

6. Solving (5) with constant a_1

The case when $a_1 = 0$ was dealt with in Section 3. So we assume now that $a_0 a_1 \neq 0$. As usual, we will reduce solving (5) over $A = B[x]$ to solving equations over B . We set $b = a_1 \in B$ and write $a_0 = \sum_{i=0}^{2d} c_i x^i$ with $c_i \in B$, $c_{2d} \neq 0$ (if $\deg(a_0)$ is odd, there are no roots). Let $t = \sum_{i=0}^d t_i x^i$.

Collecting constant terms in (5), we obtain $t_0^2 + b t_0 + c_0 = 0$. This equation over B is needed to find the constant term $t_0 = t(0)$ of t . A method of solving it in the case of finite B is considered at the end of this section.

To find the other coefficients t_i of t we can proceed as in Section 2. In degree $2i > 0$, we have $t_i^2 = c_{2i}$ when $d/2 < i \leq d$. When $d/4 < i \leq d/2$, we have $t_i^2 = c_{2i} + bt_{2i}$, and so on. Thus, to find $t_d, t_{d-1}, \dots, t_1$ we have to solve d quadratic equations over B of the form (3).

Alternatively, we can look for the unknown coefficients of t starting from lower degrees. For each odd k , we have $bt_k = c_k$ (in other words, $t'b = a'_0$, so we have a linear equation for t'). Next $bt_{2k} = c_{2k} + t_k^2$ is a linear equation for t_{2k} once we have found t_k , and so on. Thus, we can find all t_i , $i = 1, 2, \dots, d$, by solving linear equations, all of them with linear coefficient b .

In this way, necessary conditions for existence of the root t are that certain elements of B given as polynomials in given c_i are divisible by b , while in the first approach, certain elements should be squares. To make it more explicit, note that our system of equations for t_i , $i \geq 1$ splits into subsystems corresponding to odd numbers $k \leq 2d$. For each such k , we have the system $c_{k2^j} = bt_{k2^j} + t_{k2^{j-1}}^2$ for all $j \geq 0$ with $t_{k/2} = 0$. This is a system of linear equations for $t_{k2^j}^{1/2^j}$. Thus, for each k , we obtain a necessary condition for existence of t in the next theorem. This condition is sufficient (i.e., it implies that certain elements of B are divisible by b or are squares) provided that the ring B has the following property:

$$(10) \quad \text{if } y \in B \text{ and } y^2 \in b^2B, \text{ then } y \in bB.$$

The condition holds, e.g., when $bB = B$, or B is a unique factorization domain, or B is integrally closed in its field of fractions.

Theorem 4. *For the equation $t^2 + bt + a_0 = 0$ with given nonzero $b \in B$, $a_0 = \sum_{i=0}^{2d} c_i x^i \in B[x]$ to have a root $t \in B[x]$, the following two conditions must be satisfied:*

- (a) $t_0^2 + bt_0 + c_0 = 0$ has a root $t_0 \in B$,
- (b) for every integer $m \geq 0$ and every odd number k such that $d/2^m < k \leq d/2^{m-1}$,

$$(11) \quad \sum_{j=0}^m c_{k2^{m-j}}^{2^j} b^{2^{m+1}-2^{j+1}} = 0.$$

When the conditions hold and B satisfies (10), the two roots $t = \sum_{i=0}^d t_i x^i$ are given as follows: t_0 is one of two roots in B of the quadratic equation in (a) while t_k with $k \geq 1$ is given as follows:

$$t_{k2^m} = \sum_{j=0}^m c_{2^{m-j}k}^{2^j} / b^{2^j},$$

where k is odd and $m \geq 0$.

Now we consider the equation $y^2 + by + c_0 = 0$ over B in the case when B is finite (so B is a finite field). Recall that when $b = 0$, $y = c_0^{q/2}$ is the only root, where $q = 2^m = \text{card}(B)$. Otherwise b is invertible, so we can replace it by 1 by a change of variable. So we are concerned with solving the equation

$$y^2 + y + \delta = 0$$

with a given $\delta \in B = F = GF(q)$. When $\text{Tr}(\delta) = 0$, we have roots $y \in F$ by the additive analogue of Hilbert's Theorem 90, but here we need to be a little more explicit. So we use the formula of Kugurakov inspired by Berlekamp's paper [1].

Lemma 1. *Let $\delta \in B = F = GF(2^m)$, and $\text{Tr}(\delta) = 0$. Then the equation $y^2 + y = \delta$ has the explicit root $y = 1 + \sum_{j=1}^{m-1} \delta^{2^j} (\sum_{k=0}^{j-1} u^{2^k})$ where $u \in F$ and $\text{Tr}(u) = 1$. The other root is of course $y + 1$.*

Proof: We have

$$\begin{aligned} y + y^2 &= \delta^2 u + \delta^4 u + \cdots + \delta^{2^{m-1}} u + \delta^{2^m} (u^2 + \cdots + u^{2^{m-1}}) \\ &= (\text{Tr}(\delta) + \delta)u + \delta^{2^m} (\text{Tr}(u) + u). \end{aligned}$$

Now using that $\text{Tr}(\delta) = 0$, $\text{Tr}(u) = 1$, and $\delta^{2^m} = \delta$, we obtain that $y^2 + y = \delta$, completing the proof. ■

But how can we find a $u \in F$, verifying $\text{Tr}(u) = 1$? If m is odd $u = 1$ is a root, if $m/2$ is odd $u = \rho$ with $\rho \neq 1$, a 3-root of unity is a root, but if $m/2$ is even there are no obvious roots. As observed in Berlekamp's paper, exactly one half of the elements of F have trace equal to one. So random trial is a good computational method. For small values of m , we refer to the tables of primitive polynomials in Niederreiter's book [8] or, in the recent papers of Zivkovic [11] and Morgan and Mullen [7].

But a simpler solution exists.

Lemma 2. Set $F = F_2[\theta]$, and let $P(x)$ be the minimal polynomial of θ over F_2 . Then $\text{Tr}(u) = 1$ for $u = \rho_0/P'(\theta) \in F$ with $\rho_0 \in F$ being the constant term of the polynomial $P(x)/(x - \theta)$.

Proof: Write $n = \deg(P(x))$, and

$$P(x) = (x - \theta)(\rho_0 + \rho_1 x + \cdots + \rho_{n-1} x^{n-1})$$

with the ρ_j in F . By Proposition 5.5 on page 322 of Lang's book [5], the dual basis of $1, \theta, \dots, \theta^{n-1}$ relative to the bilinear form $(x, y) \rightarrow \text{Tr}(xy)$ is

$$u, \rho_1/P'(\theta), \dots, \rho_{n-1}/P'(\theta)$$

finishing the proof. ■

Remark. A more general result concerning primitive polynomials with given trace was obtained by Cohen in [3].

References

1. E. R. BERLEKAMP, H. RAMSEY AND G. SOLOMON, On the solution of algebraic equations over finite fields, *Inform. and Control* **10** (1967), 553–564.
2. A. L. CHISTOV, Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time, *J. Soviet Math.* **34(4)** (1986), 1838–1882.
3. S. D. COHEN, Primitive elements and polynomials with arbitrary trace, *Discrete Math.* **83** (1990), 1–7.
4. D. YU. GRIGOR'EV, Factorization of polynomials over a finite field and the solution of systems of algebraic equations, *J. Soviet Math.* **34(4)** (1986), 1762–1803.
5. S. LANG, “*Algebra*,” Second Edition, Addison-Wesley Publishing Company Inc., 1984.
6. S. LANG, “*Algebra*,” Third Edition, Addison-Wesley Publishing Company Inc., 1993.
7. I. H. MORGAN AND G. L. MULLEN, Primitive normal polynomials over finite fields, *Math. Comp.* **63(208)** (1994), 759–765.
8. R. LIDL AND H. NIEDERREITER, “*Finite Fields*,” Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, 1987.

9. I. E. SHPARLINSKI, “*Computational and Algorithmic Problems in Finite Fields*,” Kluwer Academic Publishers, Dordrecht, 1992.
10. J. TANG, The root criterion of quadratic equations in the finite field $GF(2^m)$, (in Chinese), *Math. Practice Theory* **2** (1986), 57–59. Reviewed in Zentr. Math. **633** #12010.
11. M. ZIVCOVIC, A table of primitive binary polynomials, *Math. Comp.* **62(205)** (1994), 385–386.

Jørgen Cherly and
Luis Gallardo:
Department of Mathematics
University of Brest
Brest 29200
FRANCE

Leonid Vaserstein:
Department of Mathematics
Penn State University
University Park, PA 16802
U.S.A.

Ethel Wheland:
Department of Mathematical Sciences
University of Akron
Akron, OH 44325
U.S.A.

Primera versió rebuda el 21 de gener de 1997,
darrera versió rebuda el 17 d'abril de 1997