On the Solution of Equations of Degree

Victor Zinoviev

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

On the Solution of Equations of Degree ≤ 10 Over Finite Fields $GF(2^m)$

V.A. Zinoviev

N° 2829
Janvier 1996

THÈME 2

Rapport de recherche

ON THE SOLUTION OF EQUATIONS OF DEGREE ≤ 10 OVER FINITE FIELDS GF(2^m)

SUR LA RÉSOLUTION DES ÉQUATIONS DE DEGRÉ ≤ 10 SUR LES CORPS FINIS GF(2^m)

V.A. Zinoviev*

* Institute for Problems of Information Transmission, Russian Academy of Sciences, Bol'shoi Karetnyi 19, Moscow, 101447, Russia

Invité au Projet CODES, du 1er juillet au 31 décembre 1995

ABSTRACT

Algorithms for solving polynomial equations of small degree ≤ 10 over the finite fields of characteristic 2 are considered. In many cases our algorithms are more efficient and less complex than the conventional Chien search.

RÉSUMÉ

Nous étudions les algorithmes de résolution d'équations de degré inférieur ou égal à 10 sur un corps fini de caractéristique 2. Dans de nombreux cas nous proposons des améliorations par rapport aux résultats connus de Chien.

1. INTRODUCTION

It is well known that for decoding of BCH codes or Reed-Solomon (R-S) codes we have to solve equations over Galois fields. A general method of solving such equations is the classical Chien procedure, where as solutions of the polynomial equation over F_q

$$\sigma(x) = \alpha^{t} + \alpha^{t-1}\sigma_1 + \ldots + \alpha\sigma_{t-1} + \sigma_t = 0, \qquad \sigma_i \in F_q ,$$

we try all the elements of GF(q). It is known, however, that for the case $t \leq 4$ it is possible to find all roots of $\sigma(x)$ directly by solving the equation $\sigma(x) = 0$ [1] (see also [2]). Also it is known that roots of polynomials can be found using the affine multiple polynomial of f(z). In this report we consider the complexity of a procedure described by Berlekamp, Rumsey and Solomon [3]. For degrees $d \leq 6$ the algorithm seems to be simpler than the Chien procedure even for the fields F_{2^8}. In Part 2 we follow Berlekamp [4] and Lidl and Niederreiter [5] and in Part 3 we follow Berlekamp [4].

2. LINEARIZED AND AFFINE POLYNOMIALS

Let q denote a prime power and let F_q, F_{q^m}, F_{q^s} be the Galois fields, where F_{q^m} (of order q^m) is an extension field of F_q and F_{q^s} is an extension field of F_{q^m}.

Definition 2.1: A polynomial of the form

$$L(z) = \sum_{i=0}^{n} L_i z^{q^i} \tag{2.1}$$

with coefficients in F_{q^m} is called a linearized polynomial (or a q-polynomial) over F_{q^m}.

It follows from the definition that any linear combination of roots of L(z) with coefficients in F_q is again a root. Indeed let $\alpha, \beta \in F_{q^s}$ and $c \in F_q$. Then

$$L(\alpha+\beta) = \sum L_i(\alpha+\beta)^{q^i} = \sum L_i(\alpha^{q^i} + \beta^{q^i}) =$$
$$= \sum L_i \alpha^{q^i} + \sum L_i \beta^{q^i} = L(\alpha) + L(\beta) . \tag{2.2}$$

$$L(c\alpha) = \sum L_i(c\alpha)^{q^i} = \sum L_i c\alpha^{q^i} = cL(\alpha) . \tag{2.3}$$

It follows that the roots of L(z) form a linear subspace over F_q. The special character of the set of roots of the linearized polynomial is given by the following result [5].

Statement 2.1. Let L(z) be a nonzero linearized polynomial over F_{q^m} and let the extension field F_{q^s} of F_{q^m} contain all the roots of L(z). Then each root of L(z) has the same multiplicity, which is either 1 or a power of q, and the roots form a linear subspace of F_{q^s}, where F_{q^s} is regarded as a vector space over F_q.

Proof: We prove the second statement. If L(z) has the form (2.1), then its derivate

$L'(z) = L_0$, so that L(z) has only simple roots in case $L_0 \neq 0$. Otherwise, we have $L_0 = L_1 = \ldots = L_{k-1} = 0$, but $L_k \neq 0$ for some $k \geq 1$, and then

$$L(z) = \sum_{i=k}^{n} L_i z^{q^i} = \sum_{i=k}^{n} L_i^{q^{mk}} z^{q^i} = \Big(\sum_{i=k}^{n} L_i^{q^{(m-1)k}} z^{q^{i-k}}\Big)^{q^k},$$

which is the q^kth power of a linearized polynomial having only simple roots. In this case, each root of L(z) has multiplicity q^k.

There is also a partial converse of this statement, which we give without proof (see [5]).

Statement 2.2. Let U be a linear subspace of F_{q^m}, considered as a vector space over F_q. Then for any nonnegative integer k the polynomial

$$L(z) = \prod_{\beta \in U} (z-\beta)^{q^k}$$

is a linearized polynomial over F_{q^m} .

The properties of linearized polynomials give us the following method of finding their roots (see [4,5]). Let L(z) be a polynomial (2.1) and suppose we want to find all its roots in the field F_{q^s}. Let $\{\alpha_1,\ldots,\alpha_s\}$ be a basis of F_{q^s} over F_q, that is every $\beta \in F_{q^s}$ can be written in the form

$$\beta = \sum_{k=1}^{s} b_k \alpha_k , \quad b_k \in F_q . \tag{2.4}$$

Using (2.2) and (2.3) we obtain for $L(\beta)$

$$L(\beta) = L\Big(\sum_{k=1}^{s} b_k \alpha_k\Big) = \sum_{k=1}^{s} L(b_k \alpha_k) = \sum_{k=1}^{s} b_k L(\alpha_k) .$$

Now let expand $L(\alpha_k)$ over our basis

$$L(\alpha_k) = \sum_{j=1}^{s} l_{kj} \alpha_j , l_{kj} \in F_q .$$

If we define the matrix $M = \| l_{kj} \|$, k,j = 1, ...,s, over F_q, our equation L(z) = 0 will be equivalent to the following homogeneous system of s linear equations for $b_1 \ldots, b_s$ over F_q:

$$(b_1,\ldots,b_s)\, M = (0,\ldots,0) \tag{2.5}$$

Indeed,

$$L(\beta) = \sum_{k=1}^{s} b_k L(\alpha_k) = \sum_{k=1}^{s} b_k \sum_{j=1}^{s} l_{k,j} \alpha_j = 0 \ .$$

$$\Leftrightarrow$$

$$\sum_{j=1}^{s} \alpha_j \sum_{k=1}^{s} b_k l_{k,j} = 0$$

$$\Leftrightarrow$$

$$\sum_{k=1}^{s} b_k l_{k,j} = 0 \ \text{ for all } \ j = 1,\ldots,s \ .$$

If r is a rank of the matrix M, then system (2.5) has q^{s-r} solutions $(b_1,\ldots,b_s)$, that gives q^{s-r} roots of L(z) in F_{q^s} of the form (2.4). So to find zeroes of linearized polynomial L(z) over F_{q^s} we have to solve the homogeneous linear system of equations over F_q, where its order s does not depend from q.

Definition 2.2. A polynomial of the form

$$A(z) = L(z) - u, \tag{2.6}$$

where L(z) is a linearized polynomial over F_{q^m} and $u \in F_{q^m}$, is called an affine polynomial (or affine q-polynomial) over F_{q^m}.

An element $\beta \in F$ is a root of A(z) if and only if $L(\beta) = u$. If

$$u = \sum_{k=1}^{s} u_k \alpha_k, \qquad u_k \in F_q,$$

then in terms of the system (2.5) the equation $L(\beta) = u$ is equivalent to the following system for $b_1,\ldots,b_s$:

$$(b_1,\ldots,b_s)\, M = (u_1,\ldots,u_s) \ . \tag{2.7}$$

If $(b_1,\ldots,b_s)$ is a solution of (2.7), then the element

$$\beta = \sum_{k=1}^{s} b_k \alpha_k$$

is a root of A(z) in F .

The method of determining the roots of an affine polynomial shows that these roots form an affine subspace - that is, a translate of the linear subspace. We give the corresponding statements from [5].

Statement 2.3. Let A(z) be an affine polynomial over F_{q^m} of positive degree and let the extension field F_{q^s} of F_{q^m} contain all the roots of A(z). Then each root of A(z) has the same multiplicity, which is either 1 or a power of q, and the roots form an affine subspace of F_{q^s}, where F_q is regarded as a vector space over F_q.

Proof: The result about the multiplicities is shown in the same way as in the proof of stat.2.1. Now let A(z) = L(z)-u, where L(z) is a linearized polynomial over F_{q^m} and let β be a fixed root of A(z). Then $\gamma \in F_{q^s}$ is a root of A(z) if and only if $L(\gamma) = u = L(\beta)$ if and only if $L(\gamma-\beta) = 0$ if and only if $\gamma-\beta \in U$, where U is the linear subspace of F_{q^s} consisting of the roots of L(z). Thus the roots of A(z) form an affine subspace of F_{q^s}.

Statemrnt 2.4. [5]. Let T be an affine subspace of F_{q^m} considered as a vector space over F_q. Then for any nonnegative integer k the polynomial

$$A(z) = \prod_{\gamma \in T} (z-\gamma)^{q^k}$$

is an affine polynomial over F_{q^m}.

Proof: Let $T = \eta + U$, where U is a linear subspace of F_{q^m}. Then

$$L(z) = \prod_{\beta \in U} (z-\beta)^{q^k}$$

is a linearized polynomial over F_{q^m} according to stat.2.2. Denote $u = L(\eta)$. Then

$$A(z) = L(z) - u = L(z-\eta)$$

is an affine polynomial, and any root γ of A(z) has the form $\gamma = \eta+\beta$, where $\beta\in U$. But this means that $\gamma \in \eta + U = T$.

The fact that roots are simpler to find for affine polynomials gives the following method of finding the roots of an arbitrary polynomial f(z) over F_{q^m} is an extension field F of F_{q^m} [3]. Define a nonzero affine polynomial A(z) over F_{q^m}, which is divisible by f(z) (so called affine multiple of f(z)). Then determine all the roots of A(z) in F by the described method. Since the roots of f(z) in F must be among the roots of A(z) in F, we have to calculate $f(\alpha)$ for all roots α of A(z) in F.

The only thing that remains is to indicate how to determine an affine multiple A(z) of f(z). The following algorithm applies for arbitrary polynomials f(z).

Statement 2.5. (Berlekamp, Rumsey and Solomon [3]). Let f(z) be any polynomial of degree $d(d \geq 1)$ over F_{q^m}. The affine multiple A(z) of f(z) can be achieved as follows:

(a) For $j = 0,1,\ldots,d-1$ calculate the unique polynomial $r^{(j)}(z) = \sum_{i=0}^{d-1} r_i^{(j)} z^i$ of degree $\leq$ d-1 such that

$$z^{q^j} \equiv r^{(j)}(z) \pmod{(f(z))} . \qquad (2.8)$$

(b) Solve the homogeneous system of d linear equations for the d + 1 unknowns $u, L_0, L_1,\ldots,L_{d-1}$ over F_{q^m}

$$(u,L_0,L_1,\ldots,L_{d-1}) \begin{vmatrix} 0 & \cdot & \cdot & \cdot & 0 & -1 \\ r_{d-1}^{(0)} & \cdot & \cdot & \cdot & r_1^{(0)} & r_0^{(0)} \\ r_{d-1}^{(1)} & \cdot & \cdot & \cdot & r_1^{(1)} & r_0^{(1)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ r_{d-1}^{(d-1)} & \cdot & \cdot & \cdot & r_1^{(d-1)} & r_0^{(d-1)} \end{vmatrix} = (0,\ldots,0) \qquad (2.9)$$

Such a system always has a nontrivial solution. If $(u, L_0, L_1,\ldots,L_{d-1})$ is one of the solutions, then the polynomial

$$A(z) = L(z)-u = \sum_{j=0}^{d-1} L_j z^{q^j} - u$$

is an affine multiple of f(z). If at this step we have several solutions, it is clear that we may take A(z) to be a monic polynomial of least degree.

Why A(z) is a multiple of f(z)? Indeed, by (2.8)

$$\sum_{j=0}^{d-1} L_j z^{q^j} \equiv \sum_{j=0}^{d-1} L_j r^{(j)}(z) \pmod{f(z)} \quad .$$

But $r^{(j)}(z) = \sum_{i=0}^{d-1} r_i^{(j)} z^i$, that is

$$\sum_{j=0}^{d-1} L_j r^{(j)}(z) = \sum_{i=0}^{d-1} z^i \sum_{j=0}^{d-1} L_j r_i^{(j)} = u \quad ,$$

where at the last step we used (2.9). It follows, that

$$L(z) = \sum_{j=0}^{d-1} L_j z^{q^i} \equiv u \pmod{f(z)}$$

or L(z) - u = A(z) is divided by f(z) .

3. THE SOLUTION OF EQUATIONS OF DEGREE ≤ 4 in F_{2^m}

We considered in detail this problem in [2]. Here we consider the same problem using the approach developed in Part 2. All this material is directly based on [4].

3.1 The equation of degree 2

Consider the equation

$$z^2 + az + b = 0, \qquad a,b \in F_{2^m} \tag{3.1}$$

where $a \neq 0$ (we always assume that the roots are distinct). The substitution $z = ax$ gives the equation

$$x^2 + x + b/a^2 = 0 . \tag{3.2}$$

According to well known result of Berlekamp, Rumsay and Solomon [3]. has a solution in F_{2^m} if and only if $Tr(b/a^2) = 0$ (here Tr(c) means the trace function Tr: $F_{2^m} \rightarrow F_2$ given by

$$Tr(c) \triangleq c + c^2 + c^4 + \ldots + c^{2^{m-1}}) . \tag{3.3}$$

Now we consider the algorithm of solving the equation (3.2). Let

$$u = \frac{b}{a^2} = \sum_{i=0}^{m-1} u_i \alpha^i , \qquad u_i \in F_2 , \tag{3.4}$$

where α is a primitive element of F_{2^m}.. For each i, $i = 0,1,\ldots,m-1$, find x_i such that

$$x_i^2 + x_i = \begin{cases} \alpha^i & \text{if } Tr(\alpha^i) = 0 \\ \alpha^i + \alpha^k & \text{if } Tr(\alpha^i) = 1 \end{cases} , \tag{3.5}$$

where α^k is some fixed element in F_{2^m} such that $Tr(\alpha^k) = 1$. To solve the equation

$$x^2 + x = u = \sum_{i=0}^{m-1} u_i \alpha^i$$

write

$$x = \sum_{i=0}^{m-1} u_i x_i .$$

Then using (3.5) and (3.4) we get

$$x^2 + x = \sum_{i=0}^{m-1} u_i(x_i^2 + x_i) = \sum_{i=0}^{m-1} u_i \alpha^i + \sum_{i:Tr(\alpha^i)=1} u_i \alpha^k =$$

$$u + \alpha^k \sum_{i=0}^{m-1} u_i Tr(\alpha^i) =$$

$$= u + \alpha^k Tr\Big(\sum_{i=0}^{m-1} u_i \alpha^i\Big) = u + \alpha^k Tr(u) ,$$

where we have also used the fact that the trace is a linear function (indeed, the trace is the linearized polynomial; see (2.2) and (2.3)). Therefore, if $Tr(u) = 0$, then two solutions of equation (3.2) are as follows

$$x^{(1)} = \sum_{i=0}^{m-1} u_i x_i , \quad x^{(2)} = 1 + \sum_{i=0}^{m-1} u_i x_i . \tag{3.6}$$

If we have already calculated the elements x_i, $i = 0,1,\ldots,m-1$, (this can be done because the equations (3.5) do not depend from u, that is from the original equation (3.1)) then to solve (3.1) we have to do the following:

- go to (3.2) (one division and one square) ;
- expand the element u over the standard basis;
- calculate one root $x^{(1)}$ of (3.2) (m-1 additions);
- calculate one root $z^{(1)}$ of (3.1) (one multiplication)
- calculate the second root $z^{(2)}$ of (3.1) (one addition).

Now if we compare this algorithm with the algorithm presented in [6] (see [2]), where the field F_{2^m} is given by normal basis, the difference is that here we have to calculate the elements x_i.

3.2 The equation of degree 3

Let us have an equation

$$z^3 + a'z^2 + b'z + c' = 0 , \qquad a', b', c' \in F_{2^m}. \tag{3.7}$$

Multiplying the left side of (3.7) on the linear multiplier $z + a'$ (that is, adding one more root $z^{(4)} = a'$) we obtain

$$z^4 + az^2 + bz + c = 0 , \tag{3.8}$$

where $a = (a')^2 + b'$, $b = a'b' + c'$, $c = a'c'$. To solve it we first find the coefficients of $L(\alpha^i)$, $i = 0,1,\ldots,m-1$, where

$$L(z) = z^4 + az^2 + bz .$$

For each $i = 0,1,\ldots,m-1$, let

$$L(\alpha^i) = \sum_{j=0}^{m-1} l_{i,j}\,\alpha^j , \qquad l_{i,j} \in F_2 \tag{3.9}$$

and let

$$c = \sum_{j=0}^{m-1} c_j \alpha^j , \qquad c_j \in F_2. \tag{3.10}$$

Then to find all roots of (3.8) we have to find all solutions of the following system of linear equations:

$$(b_0,\ldots,b_{m-1}) \begin{vmatrix} l_{0,0} & l_{0,1} & \cdots & l_{0,m-1} \\ l_{1,0} & l_{1,1} & \cdots & l_{1,m-1} \\ \cdots & \cdots & \cdots & \cdots \\ l_{m-1,0} & l_{m-1,1} & \cdots & l_{m-1,m-1} \end{vmatrix} = (c_0,\ldots,c_{m-1}) \ . \tag{3.11}$$

If (3.7) has three distinct roots in F_{2^m} (we consider the case where exactly three errors have occurred), then this system (3.11) has exactly four solutions in F_{2^m}.

Hence to solve the equation (3.7) we have to do the following:

- go to (3.8) (two multiplications, one square and two additions);
- calculate values of the polynomial $L(z)$ in m points α^i, $i = 0,1,\ldots,m-1$ (two multiplications, one square and two additions for each point; it follows from the expansion

  $$L(\alpha^i) = \alpha^i(\alpha^i(\alpha^{2i}+a)+b) \;;$$

  so we need $2(m-1)$ multiplications, $2m$ additions and $m-1$ squares) ;

- solve the linear system of equations of order m over F_2.

3.3 The equation of degree 4

Let us have an equation

$$z^4 + az^3 + bz^2 + cz + d = 0 \;, \tag{3.12}$$

where $a,b,c,d \in F_{2^m}$. The substitution $z = x+e$ reduces it to the form

$$\begin{aligned} &x^4 + ax^3 + (ae+b)x^2 + (ae^2+c)x \;+ \\ &+ e^4 + ae^3 + be^2 + ce + d = 0 \end{aligned} \tag{3.13}$$

If we choose e such that

$$ae^2 + c = 0 \tag{3.14}$$

(this is always possible in the field F_{2^m}; if $a=0$ or $c=0$ then there is nothing to do), we eliminate the linear monomial. Then transition to the inverse equation (that is, the substitution $x = 1/y$) and normalization reduces (3.12) to the equation (3.8) that we have already considered. To do it we need:

- linear substitution (one division, one square root, five multiplications and five additions);
- transition to the inverse equation (three divisions).

4. EQUATIONS OF DEGREE 5

Let us have any polynomial of degree 5

$$f(z) = z^5 + a_4 z^4 + a_3 z^3 + a_2 z^2 + a_1 z + a_0, \qquad a_0 \neq 0 \tag{4.1}$$

where $a_i \in F_{2^m}$ for all i=0,...,4. As we remember from Part 2 there is the algorithm of finding the affine multiple of f(z) of degree 2^4. We show now that it is very easy to solve the question about the existence of the affine multiple of f(z) of degree 2^3.

Statement 4.1. Let us have a polynomial f(z) of the form (4.1) over F_{2^m}. If the following equation is valid

$$a_3 a_4^3 + a_2 a_4^2 + a_1 a_4 + a_0 = 0 , \tag{4.2}$$

then the affine multiple of f(z) of degree 8 is defined by the solution of a triangular system of the linear equations in F_{2^m} that needs 12 multiplications and 9 additions in F_{2^m}.

Proof: Let us succeed in finding of the affine multiple A(z) of degree 8 for given f(z). This means that there is a polynomial y(z) of degree 3 such that

$$A(z) = f(z)y(z) . \tag{4.3}$$

Let

$$A(z) = z^8 + b_4 z^4 + b_2 z^2 + b_1 z + b_0, \qquad b_i \in F_{2^m}, \tag{4.4}$$

and

$$y(z) = z^3 + c_2 z^2 + c_1 z + c_0, \qquad c_i \in F_{2^m}, \tag{4.5}$$

where we have to find all coefficients b_i and c_i. Using (4.1), (4.4) and (4.5), the polynomial equation (4.3) gives us the following system of linear equations of order 4 for c_0, c_1, c_2:

$$\begin{cases} c_2 = a_4 \\ c_1 + a_4 c_2 = a_3 \\ c_0 + a_4 c_1 + a_3 c_2 = a_2 \\ a_3 c_0 + a_2 c_1 + a_1 c_2 = a_0 \end{cases} \tag{4.6}$$

This system is solvable if and only if the condition (4.2) is valid. In this case the coefficients of the polynomial A(z) can be written immediately

$$\begin{cases} b_0 = a_0 c_0 \\ b_1 = a_1 c_0 + a_0 c_1 \\ b_2 = a_2 c_0 + a_1 c_1 + a_0 c_2 \\ b_4 = a_4 c_0 + a_3 c_1 + a_2 c_2 + a_1 \end{cases} \tag{4.7}$$

The solution of the system (4.6) needs 3 multiplications and 3 additions and the calculation of all b_i needs 9 muliplications and 6 additions.

If the condition (4.2) is not satisfied, the substitution $z = 1/x$ and the normalization reduces the equation $f(z) = 0$ to the following form:

$$x^5 + d_4 x^4 + d_3 x^3 + d_2 x^2 + d_1 x + d_0 = 0 \ , \tag{4.8}$$

where $d_i = a_{5-i}/a_0$, $i = 1,2,3,4$ and $d_0 = 1/a_0$. Using the statement 4.1 for (4.8), we obtain the following

Statement 4.2. Let us have a polynomial f(z) of the form (4.1) over F_{2^m}. Then if the following equation

$$\left(\frac{a_1}{a_0}\right)^3 a_2 + \left(\frac{a_1}{a_0}\right)^2 a_3 + \left(\frac{a_1}{a_0}\right) a_4 + 1 = 0 \tag{4.9}$$

is satisfied, then the affine multiple of y(z) of degree 8 is defined by the solution of a triangular system of linear equations in F_{2^m} with the same complexity as in Statement 4.1.

Now consider the case when both conditions (4.2) and (4.9) are not satisfied. Of course, we can use the same approach as in proof of Statement 4.1. But it is better to use the algorithm of Berlekamp, Rumsey and Solomon, given in Statement 2.5, which we now consider in detail.

Let us have a polynomial f(z) of the form (4.1). At step (a) (see Statement 2.1) we calculate 5 polynomials

$$r^{(j)}(z) = \sum_{i=0}^{4} r_i^{(j)} z^i$$

of degree ≤ 4 such that

$$z^{2^j} \equiv r^{(j)}(z) \pmod{f(z)}, \qquad j=0,1,2,3,4 \ .$$

The polynomials $r^{(0)}(z)$, $r^{(1)}(z)$ and $r^{(2)}(z)$ can be written immediately,

$$r^{(0)}(z) = z,\ r^{(1)}(z) = z^2,\ r^{(2)}(z) = z^4 \ .$$

To find $r^{(3)}(z)$ we have to solve the congruences

$$z^8 \equiv r^{(3)}(z) \pmod{f(z)} \ . \tag{4.10}$$

The usual way is to divide z^8 by f(z), and as f(z) has 5 nonzero coefficients we have to do 5 multiplications and 5 additions for one step of division or 20 multiplications and 20 additions for all. The calculation of $r^{(4)}(z)$ needs 12 steps with 5 multiplications and 5 additions for each step, that is, all together 60 multiplications and 60 additions for finding $r^{(4)}(z)$.

Another way to find $r^{(4)}(z)$ is to use $r^{(3)}(z)$. Let $r^{(3)}(z)$ have the form

$$r^{(3)}(z) = r_4 z^4 + r_3 z^3 + r_2 z^2 + r_1 z + r_0 \ . \tag{4.11}$$

From (4.10) we have

$$z^{16} \equiv (r^{(3)}(z))^2 \pmod{f(z)}$$

or using (4.11)

$$z^{16} \equiv r_4^2 z^8 + r_3^2 z^6 + r_2^2 z^4 + r_1^2 z^2 + r_0^2 \ , \tag{4.12}$$

where we again can use (4.10) to find

$$r'(z) = r_4^2 \cdot r^{(3)}(z) \equiv r_4^2 \cdot z^8 \pmod{f(z)}$$

(for 5 multiplications) and calculate

$$r''(z) \equiv r_3^2 z^6 \pmod{f(z)}$$

by division, which needs 10 multiplications and 10 additions. Therefore to find $r^{(4)}(z)$ from $r^{(3)}(z)$ we have to do 20 multiplications and 20 additions. Then we have to solve the homogeneous system (2.9) of 5 linear equations over F_{2^m} for the 6 unknowns. As each of the first 4 rows of matrix in (2.9) has exactly one nonzero element 1 this system can be solved by performing not more than 10 multiplications and 10 additions in F_{2^m}. It is clear that this last method seems to be simpler than the approach described in the proof of Statement 4.1.

Thus, if for given f(z) of the form (4.1) the condition (4.2) is satisfied, we use Statement 4.1. for finding the affine multiple A(z) of degree 8. If not, it is better for finding of A(z) of degree 16 to use the algorithm of Statement 2.5. But then, of course, we must calculate first $r^{(3)}(z)$ and then $r^{(4)}(z)$. But this is not good, because of the extra calculations for checking of condition (4.2). Can we use this condition (4.2) in the algorithm of Berlekamp, Rumsey and Solomon directly? We give the positive answer by the following statement, which is really a refinement of Statement 2.5 for this case.

Statement 4.3. Let f(z) be any polynomial of degree 5 over F_{2^m} of form (4.1). The affine multiple A(z) of f(z) can be achieved as follows:

(a) Calculate the polynomial $A_1(z)$ of the following form

$$A_1(z) = z^8 + b_4z^4 + b_3z^3 + b_2z^2 + b_1z + b_0 = f(z)\, y_1(z) \qquad (4.13)$$

where y(z) is a polynomial of the form (4.5). If $b_3 = 0$, then $A_1(z)$ is an affine multiple of f(z) (that needs 15 multiplications and 12 additions).

(b) Calculate the polynomial $A_2(z)$ of the following form:

$$A_2(z) = z^{16} + l_4z^4 + l_3z^3 + l_2z^2 + l_1z + l_0 = f(z)\, y_2(z)$$

(using $A_1(z)$ it takes 20 multiplications and 20 additions). If $l_3 = 0$ then $A_2(z)$ is the affine multiple of f(z).

(c) Find c such that $l_3 + cb_3 = 0$. Then the polynomial $A_2(z) + cA_1(z)$ is an affine multiple of f(z), (it takes one division, 5 multiplications and 5 additions).

To find the roots of the affine polynomial A(z) of degree 8 or 16 we use the approach of Berlekamp, Rumsey and Solomon [3], described in Part 2. Let A(z) be given by (4.4) and let $L(z) = A(z) + b_0$. For all i, $i = 0,1,\ldots,m-1$, we have to calculate $L(\alpha^i)$,

$$L(\alpha^i) = \alpha^{8i} + b_4\alpha^{4i} + b_2\alpha^{2i} + b_1\alpha^i = \sum_{j=0}^{m-1} l_{i,j}\,\alpha^j, \tag{4.14}$$

where $l_{i,j} \in F_2$. Let

$$b_0 = \sum_{j=0}^{m-1} b_{0,j}\,\alpha^j, \qquad b_{0,j} \in F_2 .$$

Then all roots of A(z) are obtained by solving of the system of equations of order m of the form (2.9).

So to find all roots of f(z) of the form (4.1) we have to perform the following steps:

- Find the affine multiple polynomial A(z) of degree 8 or 16 (see stat.4.3).
- Calculate the values $L(\alpha^i)$ in m points, $i = 0,\ldots,m-1$. For A(z) of degree 8 it takes 5 multiplications and 3 additions for one point, if we write $L(\alpha^i)$ as follows

$$L(\alpha^i) = \alpha^i(b_1+\alpha^i(b_2+\alpha^{2i}(b_4+\alpha^{4i}))) .$$

For A(z) of degree 16 it takes 7 multiplications and 4 additions for one point, if we write $L(\alpha^i)$ as follows

$$L(\alpha^i) = \alpha^i(b_1+\alpha^i(b_2+\alpha^{2i}(b_4+\alpha^{4i}(b_8+\alpha^{8i})))) .$$

- Solve the linear system of equations of order m over F_2 (about m^2 additions in F_{2^m}).
- Choose among all roots of A(z) the roots of f(z), that is, we have to calculate f(z) in 8 points of F_{2^m} for A(z) of degree 8 (4 multiplications and 4 additions in F_{2^m} for one point) and in 16 points of F_{2^m} for A(z) of degree 16.

Therefore for m=8 in the worst case when f(z) has no the affine multiple of degree 8 to find all roots of f(z) of degree 5 we need about 160 multiplications and 200 additions in F_{2^m}. The Chien procedure for the code of length n takes 5 multiplications and 5 additions for one point, that is 5n multiplications and 5n additions in F_{2^m}.

5. EQUATIONS OF DEGREE $d \le 10$

Let f(z) be any polynomial of the form

$$f(z) = z^{d} + a_{d-1}z^{d-1} + \ldots + a_{0}, \qquad a_{i} \in F_{2^m}, \tag{5.1}$$

where $d \le 5$. For given d define the natural number j_0 such that

$$2^{j_0 - 1} < 2^{j_0}. \tag{5.2}$$

Define the set of natural numbers:

$$J_1 = \{j \mid j \ne 2^{s}, 3 \le j \le d-1\}. \tag{5.3}$$

It is easy to see that the cardinality of J_1 is equal to $d-j_0-1$; let us denote $d-j_0-1=k$.

Then the algorithm for calculation of the affine multiple A(z) for the polynomial f(z) looks as follows (refinement of Statement 2.5.):

Statement 5.1. At the j-th step, $j = j_0,\ldots,d-1$, calculate the polynomial $A_j(z)$ of the form

$$A_j(z) = z^{2^j} + b_{j,d-1}z^{d-1} + b_{j,d-2}z^{d-2} + \ldots + b_{j,0} \equiv 0 \pmod{f(z)} \tag{5.4}$$

Try to solve the homogeneous system of k linear equations for $j-j_0$ unknowns $c_{j_0},\ldots,c_{j-1}$

$$(1, c_{j-1}, \ldots, c_{j_0+1}, c_{j_0}) \begin{vmatrix} b_{j,i_1} & \cdots & b_{j,i_k} \\ \cdots & \cdots & \cdots \\ b_{j_0+1,i_1} & \cdots & b_{j_0+1,i_k} \\ b_{j_0,i_1} & \cdots & b_{j_0,i_k} \end{vmatrix} = (0,0,\ldots,0) \quad ,(5.5)$$

where $\{i_1,\ldots,i_k\} = J_1$. If $c_{j_0},\ldots,c_{j-1}$ is its solution (possibly zero) then the polynomial

$$A(z) = A_j(z) + \sum_{i=j_0}^{j-1} c_i A_i(z) \tag{5.6}$$

is the affine multiple of f(z) of degree 2^j. If not, go to step j+1. The complexity of calculating of A(z) in the worst case, when A(z) has degree 2^{d-1}, can be evaluated as follows:

- the number of multiplications in $F_{2^m} \le (d-j_0+1)\frac{d^2}{2} + \frac{1}{3}(d-j_0)^3$,

- the number of additions in $F_{2^m} \le \frac{1}{2}(d-j_0+1)\, d^2 + \frac{1}{3}(d-j_0)^3$,

- the number of divisions in $F_{2^m} \le (d-j_0-1)(d-j_0-2)/2$.

Proof: One of the distinctions with the algorithm of Berlekamp, Rumsey and Solomon [3] (see the stat.2.5.) is that our system (5.5) of equations has half the order for small degree $d \le 10$ and binary case p=2. The other thing is that we try to solve it at each step j to get the affine multiple of less degree. Consider now how to calculate the polynomial $A_j(z)$ using the preceeding polynomial $A_{j-1}(z)$. For given d define

$$J_2 = \begin{cases} \{2i \mid d < 2i \le 2d-2\} \cup \{d+1\} & \text{for even } d \\ \{2i \mid d < 2i \le 2d-2\} & \text{for odd } d \end{cases} \tag{5.7}$$

It is easy to see that $|J_2| = [d/2]$.

For given f(z) find and keep in memory the polynomials $B_s(z)$, $s \in J_2$, of the following form:

$$B_s(z) = z^s + r_s(z) \equiv 0 \pmod{f(z)} , \tag{5.8}$$

where $\deg r_s(z) \le d-1$. Now we want to evaluate the complexity of calculation of $B_s(z)$ under the condition that we know $B_{s-2}(z)$. Let

$$B_{s-2}(z) = z^{s-2} + r_{s-2}(z) \equiv 0 \pmod{f(z)} , \tag{5.9}$$

where

$$r_{s-2}(z) = r_{s-2,\,d-1} z^{d-1} + \ldots + r_{s-2,0} .$$

Multiply both sides of (5.9) with z^2:

$$z^{s} + z^2 r_{s-2}(z) \equiv 0 \ (\mathrm{mod}\ f(z)) \ . \tag{5.10}$$

We use

$$z^{2} \cdot r_{s-2,d-1} \cdot z^{d-1} = r_{s-2,d-1}(B_{d+1}(z) + r_{d+1}(z)) \ ,$$

($d+1 \in J_2$ for any d)

$$z^{2} \cdot r_{s-2,d-2} \cdot z^{d-2} = r_{s-2,d-2}(f(z) + \sum_{i=0}^{d-1} a_i z^{i}) \ .$$

This gives for $B_s(z)$

$$B_s = z^{s} + r_s(z) = z^{s} + r_{s-2,d-1}\, r_{d+1}(z) + r_{s-2,d-2} \sum_{i=0}^{d-1} a_i z^{i}$$

(that takes 2d multiplications and 2d additions in F_{2^m}).

Therefore to calculate all polynomials $B_s(z)$ we need $2d|J_2|$ multiplications and $2d|J_2|$ additions in F_{2^m}.

Now we are ready to consider the recurrent calculation of $A_j(z)$. Let

$$A_{j-1}(z) = z^{2^{j-1}} + b_{j-1}(z) \equiv 0 (\mathrm{mod}\ f(z)) \ , \tag{5.11}$$

where

$$b_{j-1}(z) = \sum_{s=0}^{d-1} b_{j-1,s}\, z^{s} \ . \tag{5.12}$$

Squaring of (5.11) we obtain

$$z^{2} + b_{j-1}(z)^{2} \equiv 0 \ (\mathrm{mod}\ f(z)) \ .$$

But

$$b_{j-1}(z)^2 = \sum_{s=0}^{d-1} b^2_{j-1,s} z^{2s} \equiv \sum_{s=[(d+1)/2]}^{d-1} b^2_{j-1,s} r_{2s}(z) +$$

$$+ \sum_{s=0}^{[(d-1)/2]} b^2_{j-1,s} z^{2s} \pmod{f(z)} ,$$

so

$$A_j(z) = z^{2^j} + b_j(z) \equiv 0 \pmod{f(z)}$$

where

$$b_j(z) = \sum_{s=0}^{[(d-1)/2]} b^2_{j-1,s} z^{2s} + \sum_{s=[(d+1)/2]}^{d-1} b^2_{j-1,s} r_{2s}(z) .$$

Therefore using $A_{j-1}(z)$ and the polynomials $B_s(z)$, we obtain $A_j(z)$ by $d([d/2]+1)$ multiplications and $d[d/2]$ additions in F_{2^m}. The polynomial $A_{j_0}(z)$ is either $f(z)$ (when $d=2^{j_0}$) or one of $B_s(z)$ (when $d < 2^{j_0}$). So the complexity of calculation of $d-j_0-1$ polynomials $A_{j_0+1}, \ldots, A_{d-1}(z)$ is equal to $(d-j_0-1)d([d/2]+1)$ multiplications and $(d-j_0-1)\, d\, [d/2]$ additions in F_{2^m}.

Now consider the complexity of solving of linear system (5.5) at the last step. As this value we can take the number of operations which we need to transform the last $d-j_0-1 = k$ rows of the matrix $||b_{j,i_s}||$ in (5.5) to the upper triangular form. At the last step this matrix has order $(k+1) \times k$. Using the linear transformations over columns takes not more than k(k+1)(k+2)13 multiplications, k(k+1)(k+2)13 additions and k(k-1)12 divisions in F_{2^m}. Of course, it is not necessary to do this transformation at each step independently. We can use here the recurrent procedure. Using memory we can keep the order of columns of the matrix $||b_{j,i_s}||$ and the coefficients of the linear transformation, which we used for getting the matrix of the triangular form at the previous step.

If we have found the solution $(c_{j_0}, \ldots, c_{d-2})$ of (5.5) at the last (d-1)th step, then, to obtain the affine multiple A(z), we need (according to (5.6)) not more than $(d-j_0)d$ additions and $(d-j_0-1)d$ multiplications in F_{2^m}.. This gives the complexity of calculation of A(z) in

Statement 5.1. Now let us consider the complexity of finding of the roots of the polynomial f(z) of degree d, $5 \le d \le 10$, over F_{2^m}.. Let this polynomial have the affine multiple A(z) of degree 2^{d-1} over F_{2^m},

$$A(z) = z^{2^{d-1}} + b_{d-2} z^{2^{d-2}} + \ldots + b_0 z + u = L(z) + u \qquad (5.13)$$

We are going to find the roots of A(z) in the field F_{2^m}. Let $\{1, \alpha, \ldots, \alpha^{m-1}\}$ be a basis of F_{2^m} over F_2. Calculation of the value

$$L(\alpha^i) = (\ldots((\alpha^{i 2^{d-2}} + b_{d-2})\alpha^{i \cdot 2^{d-3}} + b_{d-3})\, \alpha^{i \cdot 2^{d-4}} + \ldots + b_0)\alpha^i$$

for any $i = 0, \ldots, m-1$ takes $2(d-2)+1$ multiplications and d-1 additions in F_{2^m}, or $(2(d-2)+1)m$ multiplications and $(d-1)m$ additions in F_{2^m} for all values $L(1), L(\alpha), \ldots, L(\alpha^{m-1})$.

If

$$L(\alpha^i) = \sum_{j=0}^{m-1} l_{i,j}\, \alpha^j \qquad (5.14)$$

and

$$u = \sum_{j=0}^{m-1} u_j \alpha^j \ , \qquad (5.15)$$

then at the next step we have to solve the linear system of equations over F_2:

$$(c_0, c_1, \ldots, c_{m-1}) \left| \begin{array}{ccc} l_{0,0} & \cdots & l_{0,m-1} \\ l_{1,0} & \cdots & l_{1,m-1} \\ \cdots & \cdots & \cdots \\ l_{m-1,0} & \cdots & l_{m-1,m-1} \end{array} \right| = (u_0, u_1, \ldots, u_{m-1}) \ ,(5.16)$$

The complexity of solving of this system is equal to m(m+1)(m+2)13 additions in F_{2^m} (the complexity of reducing of the matrix $\| l_{i,j} \|$ to the triangular form), or (m+1)(m+2)13 additions in F_{2^m}.

Let the system (5.16) have 2^{d-1} solutions (this is the worst case for us). Now we have to try all these solutions as the roots of our polynomial f(z). For one root it takes d-1 multiplications and d additions in F_{2^m} or for all roots it takes $(d-1)2^{d-1}$ multiplications and $d2^{d-1}$ additions in F_{2^m}. Here we must take into attention also m(d-1) multiplications and md additions in F_{2^m} which we need for generating all roots of (5.16).

Now we have calculated the number of operations which we need to find all roots of f(z).

Statement 5.2. Let f(z) be any polynomial of the form (5.1) of degree d, $5 \le d \le 10$, over F_{2^m}.. Let j_0 be defined by (5.2). Then to find all roots of f(z) in F_{2^m} we need $(d-1)2^{d-1} + (d-j_0+1)\frac{d^2}{2} + \frac{1}{3}(d-j_0)^3 + (3d-4)m$ multiplications, $d2^{d-1} + (d-j_0+1)\frac{d^2}{2} + \frac{1}{3}(d-j_0)^3 + (m+1)(m+2)13 + m(2d-1)$ additions, and $d-j_0-1)(d-j_0-2)12$, divisions in F_{2^m}.

REFERENCES

[1] Chen, C.L., "Formulas for the Solutions of Quadratic Equations over GF(2^m)", IEEE Trans. on Inform. Theory, Vol. 28, No. 5, pp. 792-794, 1982.

[2] Dodunekov, St.M., Zinoviev, V., "On Fast Decoding of Reed-Solomon codes over GF(2^m) Correcting $t \leq 4$ Errors", Linköping University, Dept. of EE, LiTH-ISY-I-0750, August, 1985.

[3] Berlekamp, E.R., Rumsey, H., Solomon G., "On the Solution of Algebraic Equations over Finite Fields", Information and Control, Vol. 10, pp. 553-564, 1967.

[4] Berlekamp, E.R., "Algebraic Coding Theory", McGraw-Hill, New York, 1968.

[5] Lidl, R., Niederreiter, H., "Finite Fields", Cambridge University Press, 1984.

[6] MacWilliams F.J., Sloane N.J.A., "The Theory of Error-Correcting Codes", North-Holland, Amsterdam, 1977.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Lorraine - Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)
Unité de recherche INRIA Rennes - IRISA, Campus universitaire de Beaulieu 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes 46, avenue Félix Viallet - 38031 Grenoble Cedex 1 (France)
Unité de recherche INRIA Sophia Antipolis - 2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

ISSN 0249 - 6399

* RR - 2829 *