Improvements on the Cantor-Zassenhaus
Factorization Algorithm *

Michele Elia, Torino – Davide Schipani, Zurich

October 16, 2013

Abstract

We describe a new simplified version of the Cantor-Zassenhaus polynomial factorization algo-
rithm, which entails a lower computational cost. The key point is to use linear test polynomials,
which not only reduce the computational burden, but also enable us to derive good estimates and
deterministic bounds on the number of attempts needed to factor a given polynomial.

Key words: Polynomial factorization, Cantor-Zassenhaus
Mathematics Subject Classification (2010): 12Y05, 12E30

1 Introduction

The Cantor-Zassenhaus polynomial factorization algorithm ([5]) is an efficient (polynomial-time)
probabilistic algorithm for factoring polynomials over a finite field $\mathbb{F}_{p^m}$, which are the product of
irreducible polynomials with common degree $s$ and multiplicity one. When the multiplicity is above
1, the factors can be separated by computing the greatest common divisor of the given polynomial
and its formal derivative. If the irreducible polynomials have different degrees, the factors are sepa-
rated by computing the greatest common divisors with polynomials of the form $x^{p^m r - 1} - 1$, starting
from $r = 1$, so as to obtain the product of all irreducible factors of degree $r = 1, 2, \ldots$ (see e.g. [1]).
Thus standard methods can be used to reduce the problem to the above case.

First, we will introduce the Cantor-Zassenhaus factorization algorithm, providing a non-standard
description that will be the basis for the rest of the paper. In Section 2 we will discuss a more agile
version of the algorithm, with more favorable estimates of its complexity and success rate. Further,
the new description leads us to consider a deterministic version of the algorithm, so that in Section
3 we will deal with the problem of establishing how many attempts are needed in the worst case to
obtain a factor. Lastly, in Section 4, we will consider a kind of dual problem, namely, what is the least
degree of a polynomial such that a factor is found with at most a fixed number of attempts.

1.1 Preliminaries and notations

Let $f(z)$ be a polynomial of degree $t$ over $\mathbb{F}_{p^m}$ which is a product of irreducible polynomials of degree
$s$. We take first the case $s = 1$, and suppose that the trivial factor $z$ does not divide $f(z)$. We first

*The Research was supported in part by the Swiss National Science Foundation under grants No. 126948 and 132256.
deal with the case \( p = 2 \), and following [5] we assume that \( m \) is even, otherwise we would consider a quadratic extension solely for the computations. If \( \alpha \) is a known primitive element of \( \mathbb{F}_{2^m} \), we define \( \ell_m = \frac{2^m - 1}{3} \) and \( \rho = \alpha^{\ell_m} \), which is thus a primitive cubic root of unity in the field \( \mathbb{F}_{2^m} \).

Let \( c(z) \) be a non-constant polynomial over \( \mathbb{F}_{2^m} \) of degree less than \( t \), and let
\[
a(z) = c(z)^{\ell_m} \mod f(z)
\]
which is again a polynomial of degree at most \( t - 1 \). Furthermore, we have
\[
(c(z)^{\ell_m} + 1)(c(z)^{\ell_m} + \rho)(c(z)^{\ell_m} + \rho^2) = (a(z) + 1)(a(z) + \rho)(a(z) + \rho^2) \equiv 0 \mod f(z).
\]

Now, either \( \gcd(c(z), f(z)) \) is non-trivial (and thus we already have a factor of \( f(z) \)) or else \( c(z)^{2^m - 1} - 1 = 0 \mod f(z) \). In this latter case, if we write \( c(z)^{2^m - 1} - 1 = u(z)f(z) + r(z) \) and specialize it into the roots \( \{ z_i \} \) of \( f(z) \), we see that \( r(z) \), which is a polynomial of degree \( t - 1 \), takes the value 0 for all \( t \) roots, as \( b^{2^m - 1} - 1 = 0 \) for any \( b \in \mathbb{F}_{2^m} \). This implies that \( r(z) \) is identically 0. Thus we can write
\[
(c(z)^{\ell_m} + 1)(c(z)^{\ell_m} + \rho)(c(z)^{\ell_m} + \rho^2) = (a(z) + 1)(a(z) + \rho)(a(z) + \rho^2) \equiv 0 \mod f(z).
\]

Since every factor of the product \((a(z) + 1)(a(z) + \rho)(a(z) + \rho^2)\) has degree less than \( t \), at least two of them must have a common non-trivial factor with \( f(z) \), unless \( a(z) = 1, \rho, \rho^2 \). In this latter case, the Cantor-Zassenhaus algorithm considers another random polynomial instead of \( c(z) \), and reiterates the procedure until all factors have been found.

Notice that \( a(z) \equiv 0 \) never occurs, since \( c(z) \) has degree less than \( f(z) \), so that at least one root of \( f(z) \), say \( b \), is not a root of \( c(z) \); then substituting \( b \) in the identity \( c(z)^{\ell_m} = v(z)f(z) + a(z) \), we get \( a(b) \neq 0 \), therefore \( a(z) \) is identically zero (this holds even if the roots of \( f \) were not in the field of the coefficients, as in the original description of the algorithm).

For the case \( p > 2 \), the procedure is similar: we consider \( \ell_m = \frac{p^m - 1}{2} \) and \( \rho = \alpha^{\ell_m} = -1 \), where \( \alpha \) is a primitive element of \( \mathbb{F}_{p^m} \). Here we compute \( a(z) = c(z)^{\ell_m} \mod f(z) \) and then factor as soon as \( a(z) \neq \pm 1 \).

Let us now consider the case \( s > 1 \). One option is to look at \( \mathbb{F}_p^m \), where the polynomial fully splits into linear factors: once a factor \( z - b \) is found, it can be multiplied by the factors \( z - b^{p^m} \), with \( 1 \leq i \leq s - 1 \), to obtain an irreducible factor of degree \( s \). A second option is to apply the algorithms over \( \mathbb{F}_p^m \) ([4], [5]), to directly find the irreducible factors of degree \( s \) over \( \mathbb{F}_p^m \). If \( p = 2 \), the argument follows as above: either \( \gcd(c(z), f(z)) \) is non-trivial, or \( \gcd(c(z), f(z)) = 1 \), in which case
\[
(c(z)^{\ell_{sm}} + 1)(c(z)^{\ell_{sm}} + \rho)(c(z)^{\ell_{sm}} + \rho^2) = (a(z) + 1)(a(z) + \rho)(a(z) + \rho^2) \equiv 0 \mod f(z).
\]

Since every factor of the product \((a(z) + 1)(a(z) + \rho)(a(z) + \rho^2)\) has degree less than \( t \), at least two of them must have a common non-trivial factor with \( f(z) \) in \( \mathbb{F}_{2^m} \), unless \( a(z) = 1, \rho, \rho^2 \). In this latter case, the Cantor-Zassenhaus algorithm considers another random polynomial \( c(z) \), and reiterates the procedure until all factors have been found.

For the case \( p > 2 \), the procedure is similar: we consider \( \ell_{sm} = \frac{p^m - 1}{2} \) and compute \( a(z) = c(z)^{\ell_{sm}} \mod f(z) \) and then factor as soon as \( a(z) \neq \pm 1 \).

In the next Section we will present a variant of the Cantor-Zassenhaus algorithm, according to the description given above, and then deal with probabilistic as well as deterministic considerations about its success rate.
2 Variations of the algorithm

We focus first on the case $s = 1$ and show that it is enough, and indeed convenient, to choose $c(z) = z$ as initial test polynomial, and to choose $c(z) = z + b$, for some random $b \neq 0$, as further test polynomial, and to continue by choosing random $bs$ different from the previous ones until a factor is found.

We then consider the case $s > 1$, where polynomials of degree 1 or $s$ will be involved as test polynomials in order to obtain bounds on the number of attempts to find a factor.

More deterministic aspects of the algorithm will be postponed to Sections 3 and 4.

We notice that a similar approach was already present in [4, 11], but only for the case of odd characteristic and factors of degree 1; also, the analysis was of a different type, with focus on the expected number of operations used by the algorithm.

2.1 Case $s = 1$

Suppose $f(z)$ is over $\mathbb{F}_{2^m}$ and $z^{\ell_m} = \rho^i \mod f(z)$, $i \in \{0, 1, 2\}$. Now, any element in $\mathbb{F}_{2^m}$ can be written as $\alpha^{k+3n}$, with $k \in \{0, 1, 2\}$: we define $A_0 = \{\alpha^{3i} : i = 0, \ldots, \ell_m - 1\}$, that is the subgroup of the elements of $\mathbb{F}_{2^m}$ that are cubic powers, and let $A_1 = \alpha A_0$ and $A_2 = \alpha^2 A_0$ be the two cosets that complete the coset partition of $\mathbb{F}_{2^m}$. If we substitute $\alpha^{k+3n}$ for any root $z_i$ of $f(z)$ in $z^{\ell_m} - \rho^i = Q(z)f(z)$, we obtain $\rho^k - \rho^i = 0$, which implies $k = i$. This means that if $z^{\ell_m} = \rho^i \mod f(z)$, then all the roots of $f(z)$ are of the form $\alpha^{i+3n}$, that is they belong to the same coset. When this situation occurs, we consider another test polynomial $c(z) = z + b$, which is equivalent to testing $c(z) = z$ for the polynomial $c(z)$ whose set of roots is $\{z_i + b\}$. The test succeeds as soon as we find a $b$ such that the roots $z_i + b$ do not all belong to the same coset.

The next step is to determine an upper bound to the number of attempts needed in the worst case scenario, or on average, until a factor is found.

Let us first consider the simple case $t = 2$: suppose that $z_1$ and $z_2$ belong to the same coset; then we look for a $b$ such that $z_1 + b$ and $z_2 + b$ are in different cosets. For the worst case scenario, we need to know how many pairs $(z_1 + b, z_2 + b)$ have both elements in the same coset. This is equivalent to knowing the number of ways in which $z_1 - z_2 = z_1 + b - (z_2 + b)$ can be written as the sum of two elements in the same coset. This number is actually $\frac{2^{m-1}}{3} - 1$, as can be deduced from [17, Theorem 1] specialized with $i = 0$ and $\chi$ the cubic character. So at most with $\frac{2^{m-1}}{3}$ attempts we can factor a polynomial of degree 2. Clearly, at each test we can factor with a probability of $\frac{2}{3}$, so that the expected number of attempts is 1.5.

If $f(z)$ is a polynomial over $\mathbb{F}_{p^m}$, $p > 2$, then the maximum number of attempts is $\frac{2^{m-1}}{2^m - 1}$, by similar reasoning: we again use some additive properties of residues ([9, 10, 12, 17]). At each test we can factor with a probability of $\frac{2}{2^m - 1}$, so that the expected number of attempts is 2.

The remainder of this paper will be devoted to establishing both probabilistic estimates and deterministic bounds on the number of attempts needed to successfully factor, for a generic $t$. A first deterministic, though very loose, bound is the following:

**Proposition 1.** Let $s = 1$. The maximum number of attempts needed to find a factor is upper bounded by $\ell_m$ (that is $\frac{2^{m-1}}{2^m - 1}$ or $\frac{2^{m-1}}{2}$ for $p = 2$ or $p$ odd, respectively). In particular, in the Cantor-Zassenhaus algorithm it is sufficient to consider only linear polynomials as test polynomials $c(z)$.

**Proof.** In characteristic 2, if a root $z_i$ belongs to a given known coset, we can test all the $\ell_m$ elements of that coset, until we obtain $z_i$: $z_i + z_i$ adds to 0, which does not belong to any coset. Thus we
will succeed with at most \( \ell_m \) attempts. In characteristic \( p \) greater than 2, it is sufficient to add all the elements of the coset multiplied by \( p - 1 \).

That it is enough to consider all the \( p^m \) monic linear polynomials is anyway clear, since computing \( \gcd\{z - b, f(z)\} \) for all \( b \) in \( \mathbb{F}_{p^m} \) would be enough to find all the factors.

\[ \square \]

**Remark 1** The above argument implies that, if the first attempt fails, we know which coset the roots belong to, and can restrict our choice of \( b \) to that coset.

**Remark 2** Alternatively, the upper bounds of the proposition follow from the above remarks about \( t = 2 \): clearly, if \( t \) is greater than 2, then a degree-2 polynomial is anyway a factor of the \( t \)-degree polynomial, so that the maximum number of attempts cannot exceed the number needed to factor this degree-2 polynomial.

**Remark 3** In the original version of the Cantor-Zassenhaus algorithm, \( \gcd(a(z), f(z)) \) is computed when searching for a factor of \( f(z) \), corresponding to the case when \( \gcd(c(z), f(z)) \) is non-trivial. Our version of the algorithm avoids this computation, since it is sufficient to evaluate \( f(z) \) in \( b \) with any efficient polynomial evaluation algorithm; this can be done before elevating to the power \( \ell_m \).

**Remark 4** If \( q \) is a prime factor of \( p^m - 1 \), then we may consider the exponent \( \ell_m = \frac{p^m - 1}{q} \); in this case the probability of success is \( \frac{q - 1}{q} \) and the corresponding expected number of attempts is \( \frac{q}{q-1} \cdot \ell_m \), which is close to 1 already for small primes like 5 or 7; the drawback is that, if \( q \) is large, in the worst case we must check \( q \) greatest common divisors, namely \( \gcd(a(z) + \zeta_q^j, f(z)) \), for \( 0 \leq j \leq q - 1 \), where \( \zeta_q \) is a \( q \)-th primitive root of unity.

**Remark 5** It is interesting to assess the probability of factoring with the above method. Given that the set of \( \{z_i + b\} \) for some \( b \) is made up of elements each belonging to a given coset \( A_i \), with probability 1/3 (or 1/2 in the case \( p > 2 \)), the probability that they all belong to a common coset of the three is \( 3 \cdot \frac{1}{3} \) (and \( 2 \cdot \frac{1}{2} \) in case of the two cosets in \( \mathbb{F}_{p^m}^* \), \( p > 2 \)). Therefore the expected number of attempts to obtain a factor is \( \frac{1}{1 - \frac{1}{3}} = 1 + \frac{1}{3 - 1} \) or \( 1 + \frac{1}{2 - 1 - 1} \) and so decreases exponentially with the degree of the polynomial, so that the probability of factoring with one test is close to 1 when the degree is large enough. Clearly, once a factor is found, the polynomial splits into two parts, to which we can re-apply the previous computation if we are interested in a complete factorization, until all linear factors are obtained.

### 2.2 Case \( s > 1 \)

If \( s > 1 \), either we look for linear factors in \( \mathbb{F}_{p^s} \), and the analysis is the same as in the case \( s = 1 \), or we choose the direct method, as explained in the previous section. In this latter case, by a similar argument as above, the algorithm succeeds as soon as \( c(z_i) \), \( z_i \) being the roots of \( f(z) \), are not all in the same coset. This is equivalent of requiring non conjugate roots not all to be in the same coset, as

\[ c(z_i^{p^m})^{\ell_{sm}} = ((c(z_i))^{p^m})^{\ell_{sm}} = ((c(z_i))^{\ell_{sm}})^{p^m} = (c(z_i))^{\ell_{sm}} \]
by the properties of the Frobenius automorphism $\tau(z) = z^p$.

Let us examine this more precisely, describing in detail the case $p = 2$, while a similar argument applies in the case of odd primes. Let $f(z)$ be, as above, a polynomial of degree $t$ over $\mathbb{F}_{2^m}$, which is a product of $\frac{1}{2}$ irreducible polynomials $f_i(z)$ of degree $s$ over the same field $\mathbb{F}_{2^m}$, where it is not restrictive to assume even $m$. According to the Cantor-Zassenhaus algorithm, a polynomial $c(z)$ over $\mathbb{F}_{2^m}$, relatively prime with $f(z)$, separates $f(z)$ into two polynomials of smaller degree if $a(z) = c(z)^{s_m} \mod f(z)$ is different from $1, \rho, \rho^2$; at least two factors $f_i(z)$ are in two distinct greatest common divisors between $f(z)$ and $a(z) + 1, a(z) + \rho,$ and $a(z) + \rho^2$, respectively.

Lemma 1. With the above hypotheses and definitions, a polynomial $c(z)$ over $\mathbb{F}_{2^m}$ separates $f(z)$ into two polynomials, one containing the factor $f_1(z)$, and a second containing the factor $f_2(z)$, if and only if $c(z)^{s_m} \mod f_1(z) \neq c(z)^{s_m} \mod f_2(z)$. Equivalently, $f_1(z)$ and $f_2(z)$ are separated if and only if $c(z_1)$ and $c(z_2)$ belong to different cosets $A'_i$ of $\mathbb{F}_{2^m}$, where $z_1$ and $z_2$ are roots of $f_1(z)$ and $f_2(z)$, respectively.

Proof. The polynomial $f(z)$ can be written as a product of three polynomials, i.e. $f_1(z)$, $f_2(z)$, and $f_3(z)$ which collects the remaining factors, thus $a(z)$ can be decomposed, using the Chinese Remainder Theorem (CRT), as

$$a(z) = a_1(z)\psi_1(z) + a_2(z)\psi_2(z) + a_3(z)\psi_3(z) \mod f(z), \quad \psi_1(z) + \psi_2(z) + \psi_3(z) = 1,$$

where $a_1(z) = c(z)^{s_m} \mod f_1(z)$, $a_2(z) = c(z)^{s_m} \mod f_2(z)$, and $a_3(z) = c(z)^{s_m} \mod f_3(z)$.

If $a(z) = 1, \rho, \rho^2$, the uniqueness of the CRT decompositions implies that $a_1(z) = a_2(z) = a_3(z)$.

If $a(z) \neq 1, \rho, \rho^2$, then $c(z)$ separates $f(z)$ into two polynomials of smaller degree, and we distinguish two cases:

1) $a_1(z) \neq a_2(z)$: the polynomials $f_1(z)$ and $f_2(z)$ are in different factors because, if both of them were in the same factor, they would both divide the same polynomial $a(z) + \rho^i$, thus $a_i(z) = a(z) \mod f_i(z)$, $i = 1, 2$, contrary to the assumption.

2) $a_1(z) = a_2(z)$: $f_1(z)$ and $f_2(z)$ are in the same factor; if we suppose they are not, then $a_1(z) = a(z) \mod f_1(z) \neq a_2(z) = a(z) \mod f_2(z)$, yielding a contradiction.

Also, since $a(z) = c(z)^{s_m} \mod f(z)$ and $a(z) = a_i(z) = \rho^{hi} \mod f_i(z)$, we have that $c(z_i)^{s_m} = \rho^{hi}, i = 1, 2$, which means that $c(z_i) \in A'_{hi}$, hence it follows from the first part of the lemma that $c(z)$ separates $f_1(z)$ and $f_2(z)$ if and only if $c(z_1) \neq c(z_2)$.

□

Now, as in the case $s = 1$, we are interested in upper bounds for the number of attempts, and we can limit the choice of $c(z)$ according to our convenience. For example, if we know at least one primitive polynomial $m(z)$ of degree $s$, we can choose the polynomials $c(z)$ within the set of monic irreducible polynomials of degree $s$, so that we get directly $\frac{\mathbb{F}_{2^m}}{\mathbb{F}_{2^s}}$ as an upper bound. If we do not have any primitive polynomial of degree $s$, that is, we have no means of obtaining and drawing from the pool of irreducible polynomials of degree $s$, then we can choose the polynomials $c(z)$ within the larger set of monic polynomials of degree $s$, and we have the looser bound $\rho^{ms}$. Somewhat surprisingly, we show next that again it is usually actually sufficient to consider linear polynomials.

Let $\chi_3(x)$ be a non-trivial cubic character over $\mathbb{F}_{2^m}$, namely $\chi_3$ is a mapping from $\mathbb{F}_{2^m}$ into the complex numbers defined as

$$\chi_3'(a^h\theta) = c^h_3, \quad \theta \in A'_0, \quad h = 0, 1, 2,$$

5
\( \alpha \) being a primitive element of \( \mathbb{F}_{2^m} \), \( \zeta_3 \) a primitive complex cubic root of unity, and \( \mathcal{A}'_0 \) the coset of cubes in \( \mathbb{F}_{2^m} \). Moreover, we set \( \chi_3'(0) = 0 \) by definition.

If \( z_1 \) and \( z_2 \) are roots of two distinct irreducible polynomials of degree \( s \), we denote with \( N_2^{(m)}(z_1, z_2) \) the number of monic polynomials \( c(z) = z + b \) with \( b \in \mathbb{F}_{2^m} \) such that \( \chi_3'(c(z_1)) = \chi_3'(c(z_2)) \).

**Proposition 2.** Let \( s > 1 \). The maximum number \( N_A \) of attempts needed to find an irreducible factor of degree \( s \), using monic linear polynomials as test polynomials, is upper bounded by \( \frac{2^{m+1}}{3} \left( 1 + \frac{4s-2}{\sqrt{2^m}} + \frac{1}{2^m} \right) \) if \( p = 2 \), or by \( \frac{p^m}{4} \left( 1 + \frac{2s-1}{\sqrt{p^m}} \right) \) if \( p \) is odd. In particular linear polynomials are sufficient to find a factor if \( \frac{4s-2}{\sqrt{2^m}} < 2 \) or \( \frac{2s-1}{\sqrt{p^m}} < 1 \), respectively.

**Proof.** In the case of characteristic 2, \( N_A \) is upper bounded by the maximum of \( N_2^{(m)}(z_1, z_2) + 1 \) taken over all distinct pairs of roots \( z_1 \) and \( z_2 \) of distinct irreducible polynomials of degree \( s \). Thus an upper bound for \( N_2^{(m)}(z_1, z_2) \) independent of \( z_1 \) and \( z_2 \) is also an upper bound for \( N_A - 1 \).

Consider the indicator function
\[
I_{\mathcal{A}'_h}(c(z)) = \frac{1 + \zeta_3^h \chi_3'(c(z_1)) + \zeta_3^h \chi_3'(c(z))}{3}, \quad i = 1, 2,
\]
which is 1 if the cubic character of \( c(z_1) \) is \( \zeta_3^h \), and is 0 otherwise, if we suppose \( c(z) \) relatively prime with \( f(z) \).

Therefore, for a given \( c(z) \) we have a coincidence whenever the product \( I_{\mathcal{A}'_h}(c(z_1))I_{\mathcal{A}'_h}(c(z_2)) \) is 1. Thus,
\[
\sum_{h=0}^2 I_{\mathcal{A}'_h}(c(z_1))I_{\mathcal{A}'_h}(c(z_2)) = \frac{1}{3} \left( 1 + \chi_3'(c(z_1))\chi_3'(c(z_2)) + \chi_3'(c(z_1))\chi_3'(c(z_2)) \right)
\]
is the coincidence indicator for a fixed polynomial \( c(z) \). Summing over all monic linear polynomials \( z + b \) over \( \mathbb{F}_{2^m} \), we get the total number \( N_2^{(m)}(z_1, z_2) \) of coincidences
\[
N_2^{(m)}(z_1, z_2) = \frac{1}{3} \sum_{b \in \mathbb{F}_{2^m}} (1 + \chi_3'(z_1 + b)\chi_3'(z_2 + b) + \chi_3'(z_1 + b)\chi_3'(z_2 + b)) - \frac{2}{3},
\]
where \(-\frac{2}{3}\) comes from excluding those polynomials \( z + b \) having \( z_1 \) or \( z_2 \) as root. For its computation, the summation is split into three summations: the first is simply \( 2^m \), and the second and third are complex conjugated, thus it is enough to evaluate only
\[
C = \sum_{b \in \mathbb{F}_{2^m}} \chi_3'(z_1 + b)\chi_3'(z_2 + b).
\]

This summation is hard to evaluate in closed form, thus we content ourselves with a bound. Namely, as \( \chi_3' \) can be considered as the lifted character of a nontrivial character \( \chi_3 \) over \( \mathbb{F}_{2^m} \) [7, 8], we can write
\[
C = \sum_{b \in \mathbb{F}_{2^m}} \chi_3(N_{F_{2^m}/F_{2^m}}(z_1 + b))\bar{\chi}_3(N_{F_{2^m}/F_{2^m}}(z_2 + b)),
\]
where \( N_{F_{2^m}/F_{2^m}}(x) = x \cdot x^{2^m} \cdots x^{2^m(s-1)} \) is the relative norm of \( x \).

Since \( N_{F_{2^m}/F_{2^m}}(z_i + b) \), \( i = 1, 2 \), are polynomials of degree \( s \) in \( b \), and \( \bar{\chi}_3 = \chi_3^3 \), we can then use the Weil bound ([15, Theorem 2C']; cf. also [18, Lemma 2.2]) to obtain
\[
C < (2s - 1)2^{m/2}.
\]
In conclusion, we obtain $N_A$ bounded as

$$N_A < \frac{2^m}{3} \left( 1 + \frac{4s - 2}{\sqrt{2^m}} + \frac{1}{2m} \right).$$  \hspace{1cm} (1)$$

The same argument holds similarly for $p$ odd, and making the appropriate changes the conclusion is

$$N_A < \frac{p^m}{2} \left( 1 + \frac{2s - 1}{\sqrt{p^m}} \right).$$  \hspace{1cm} (2)

\hfill \Box

3 Deterministic splitting I: fixed $t$

In the following we analyse the algorithm in greater detail from a deterministic point of view; in particular we will show that the maximum number of attempts to obtain a factor is usually very small, so that the algorithm, which is probabilistic in nature, can often be considered deterministic.

In order to simplify the subsequent analysis, we will assume from now on that $s = 1$.

If we use the proposed variant of the Cantor-Zassenhaus algorithm, the tightest upper bound to the number of attempts necessary to split a polynomial $f(z)$ of degree $t$ over $\mathbb{F}_{2^m}$ is equal to

$$M_2(t) = 1 + \max_{z_1 \neq z_2 \neq \cdots \neq z_t} N_2(t),$$

where $N_2(t)$ is the number of solutions $b$ of a system of $t$ equations in $\mathbb{F}_{2^m}$ of the form

$$\begin{cases}
\alpha_1^j w_1^3 + b = \alpha_1^k y_1^3 \\
\alpha_2^j w_2^3 + b = \alpha_2^k y_2^3 \\
\vdots \\
\alpha_t^j w_t^3 + b = \alpha_t^k y_t^3
\end{cases}$$ \hspace{1cm} (3)

where $\alpha_1^j, \alpha_2^j, \cdots, \alpha_t^j$ are given and distinct (i.e. they are the roots $z_i$ of $f(z)$), whereas the $y_i$’s must be chosen in the field to satisfy the system, and the three values $\{0, 1, 2\}$ for $k$ and $j$ are all considered. However, we may assume $j = 0$ (and $z_i = w_i$), since dividing each equation by $\alpha_i^j$, and setting $b' = b\alpha_i^{-j}$ and $k' = k - j \mod 3$, we see that the number of solutions of the system is independent of $j$. If the system is unsolvable, then the number of attempts is 1.

To evaluate $N_2(t)$, we define an indicator function of the sets $A_u$ using the cubic character, namely for every $x \neq 0$

$$I_{A_u}(x) = \frac{1 + \zeta_3^u \chi_3(x) + \zeta_3^{2u} \chi_3(x)}{3} = \begin{cases} 1 & \text{if } x \in A_u \\
0 & \text{otherwise}
\end{cases} \text{ for } u = 0, 1, 2,$$

(where the bar over $\chi$ denotes complex conjugation). Then, given a $z_i$ we can partition the elements $b \neq z_i^3$ in $\mathbb{F}_{2^m}$ into subsets depending on $k \in \{0, 1, 2\}$ such that $\chi_3(b + z_i^3) = \zeta_3^k$. Therefore, a solution of (3) for a fixed $k$ and $j = 0$ is singled out by the product

$$\prod_{i=1}^t I_{A_k}(b + z_i^3) = \frac{1}{3^t} \left[ 1 + \sum_{i=1}^t \sigma_i^{(k)} \right],$$

where $\sigma_i^{(k)}$ is the number of solutions of $\chi_3(b + z_i^3) = \zeta_3^k$.
where each $\sigma_i^{(k)}$ is a homogeneous sum of monomials which are products of $i$ characters of the form $\chi_3(b + z_i^3)$ or $\bar{\chi}_3(b + z_i^3)$. Thus

$$N_2(t) = \sum_{\substack{b \in \mathbb{F}_{p^m} \\ b \not\in \{z_i^3\}}} \left[ \prod_{i=1}^t I_{A_0}(b + z_i^3) + \prod_{i=1}^t I_{A_1}(b + z_i^3) + \prod_{i=1}^t I_{A_2}(b + z_i^3) \right]. \quad (4)$$

The roots $z_i$ in the sum need not be considered, since in any case they are not solutions ($z_i^3 + z_i^3 = 0$ cannot be in the same coset as $z_i^3 + z_i^3$ if $i \neq j$).

Similarly, in characteristic greater than 2, the tightest upper bound to the number of attempts necessary to split a polynomial $f(z)$ of degree $t$ is equal to

$$M_p(t) \leq 1 + \max_{z_1 \neq z_2 \neq \cdots \neq z_t} \eta_p(t),$$

where $\eta_p(t)$ is the number of solutions $b$ of a system of $t$ equations in $\mathbb{F}_{p^m}$ of the form

$$\left\{ \begin{array}{l}
\alpha^2 w_1^2 + b = \alpha^k y_1^2 \\
\alpha^2 w_2^2 + b = \alpha^k y_2^2 \\
\vdots \\
\alpha^2 w_t^2 + b = \alpha^k y_t^2
\end{array} \right.$$

where $\alpha^2 w_1^2, \alpha^2 w_2^2, \ldots, \alpha^2 w_t^2$ are given and distinct and the two values $\{0, 1\}$ for $k$ and $j$ are considered. Again, we may assume $j = 0$ and we can define an indicator function of the sets $B_u$ using the quadratic character, where $B_0$ is the set of squares and $B_1$ the complementary set in $\mathbb{F}_{p^m}$: namely, let $\chi_2$ be a mapping from $\mathbb{F}_{p^m}$ into the complex numbers defined as

$$\chi_2(\alpha^k \theta) = (-1)^h, \quad \theta \in B_0, \quad h = 0, 1.$$

Again, we set $\chi_2(0) = 0$.

The corresponding indicator function is thus

$$I_{B_u}(x) = \frac{1 + (-1)^u \chi_2(x)}{2} = \begin{cases} 1 & \text{if } x \in B_u \\ 0 & \text{otherwise} \end{cases} \quad u = 0, 1.$$

Given a $z_i$ we partition $\mathbb{F}_{p^m} \setminus \{z_i^2\}$ into subsets depending on the value of $k$, such that $\chi_2(b + z_i^2) = (-1)^k$. Therefore, a solution of (5) for a fixed $k$ is given by the product

$$\prod_{i=1}^t I_{B_k}(b + z_i^2) = \frac{1}{2^t} [1 + \sum_{i=1}^t \sigma_i^{(k)}],$$

where each $\sigma_i^{(k)}$ is a homogeneous sum of monomials which are the products of $i$ characters of the form $\chi_2(b + z_i^2)$. Thus $N_p(t)$ is

$$N_p(t) = \sum_{\substack{b \in \mathbb{F}_{p^m} \\ b \not\in \{z_i^2\}}} \left[ \prod_{i=1}^t I_{B_0}(b + z_i^2) + \prod_{i=1}^t I_{B_1}(b + z_i^2) \right]. \quad (6)$$

The following subsections deal with computations of $N_p(t)$ for small values of $t$, then with general bounds on $N_p(t)$. 8
3.1 Computations for small $t$

In the following computations, we will use some properties of nontrivial characters that we briefly mention: $\sum_{x \in \mathbb{F}_q} \chi(x) = 0$; if $b \neq 0$, then $\sum_{x \in \mathbb{F}_q} \chi(x)(x + b) = -1$ ([13, 17]). Moreover,

$$\sum_{x \in \mathbb{F}_{2m}} \chi_3(x)\chi_3(x + 1) = G_m(1, \chi_3) = -(-2)^{m/2},$$

with $G_m(1, \chi_3)$ being the Gauss sum ([13]).

We will start with the case $p = 2$. First we compute $N_2(2)$, already found above with another technique, then analogously $N_2(3)$.

$t = 2$. Setting $x_i = b + z_i^3$, we have

$$\prod_{i=1}^{2} I_{A_k}(x_i) = \frac{1}{9} \left( 1 + \sigma_1^{(h)} + \sigma_2^{(h)} \right) \quad h = 0, 1, 2 ,$$

where

$$\sigma_1^{(h)} = \zeta_3^{2h}\chi_3(x_1) + \zeta_3^{h}\bar{\chi}_3(x_1) + \zeta_3^{2h}\chi_3(x_2) + \zeta_3^{h}\bar{\chi}_3(x_2)$$

$$\sigma_2^{(h)} = \zeta_3^{2h}\chi_3(x_1)\chi_3(x_2) + \chi_3(x_1)\bar{\chi}_3(x_2) + \bar{\chi}_3(x_1)\chi_3(x_2) + \zeta_3^{2h}\bar{\chi}_3(x_1)\bar{\chi}_3(x_2)$$

Since $\sigma_1^{(0)} + \sigma_1^{(1)} + \sigma_1^{(2)} = 0$ and $\sigma_2^{(0)} + \sigma_2^{(1)} + \sigma_2^{(2)} = 3(\chi_3(x_1)\bar{\chi}_3(x_2) + \bar{\chi}_3(x_1)\chi_3(x_2))$, the sum of the three products $\prod_{i=1}^{2} I_{A_k}(x_i)$ is $\frac{1}{9} (1 + \chi_3(x_1)\bar{\chi}_3(x_2) + \bar{\chi}_3(x_1)\chi_3(x_2))$, and thus the sum over $b$ in the whole field $\mathbb{F}_{2m}$, with the exclusion of $b = z_1^3$ and $b = z_2^3$, is

$$N_2(2) = \frac{1}{3} \left( 2^m - 2 + \sum_{b \neq z_1^3, z_2^3} \left( \chi_3(b + z_1^3)\bar{\chi}_3(b + z_2^3) + \bar{\chi}_3(b + z_1^3)\chi_3(b + z_2^3) \right) \right).$$

Let $S$ denote the above summation, then $S$ can be evaluated in closed form: by the substitution $b = z_1^3 + \eta$, since $\chi_3$ is a nontrivial cubic character, we have

$$S = \sum_{\eta \neq 0, z_1^3 + z_2^3} \left( \chi_3(\eta)\bar{\chi}_3(\eta + z_1^3 + z_2^3) + \bar{\chi}_3(\eta)\chi_3(\eta + z_1^3 + z_2^3) \right) = -2 ,$$

as the summation of each of the two parts gives $-1 (z_1^3 + z_2^3 \neq 0$ by hypothesis). In conclusion, we have

$$N_2(2) = \frac{1}{3} (2^m - 4) ,$$

so that

**Proposition 3.** $M_2(2) = \frac{1}{3} (2^m - 1)$
\( t = 3 \). In this case
\[
\prod_{i=1}^{3} I_{A_{b}}(b + z_i^3) = \frac{1}{27} \left( 1 + \sigma_1^{(h)} + \sigma_2^{(h)} + \sigma_3^{(h)} \right) \quad h = 0, 1, 2 ,
\]
where

\[
\begin{align*}
\sigma_1^{(h)} &= \zeta_3^{2h} \chi_3(x_1) + \zeta_3^{2h} \chi_3(x_2) + \zeta_3^{2h} \chi_3(x_3) \\
\sigma_2^{(h)} &= \zeta_3^{2h} \chi_3(x_1) + \chi_3(x_1) \chi_3(x_2) + \chi_3(x_1) \chi_3(x_3) + \zeta_3^{2h} \chi_3(x_2) \chi_3(x_3) \\
\sigma_3^{(h)} &= \chi_3(x_1) + \chi_3(x_1) \chi_3(x_2) + \chi_3(x_1) \chi_3(x_3) + \zeta_3^{2h} \chi_3(x_1) \chi_3(x_2) \chi_3(x_3)
\end{align*}
\]

We thus have

\[
\begin{align*}
\sigma_1^0 + \sigma_1^1 + \sigma_1^2 &= 0 \\
\sigma_2^0 + \sigma_2^1 + \sigma_2^2 &= 3(\chi_3(x_1) \chi_3(x_2) + \chi_3(x_1) \chi_3(x_3) + \chi_3(x_2) \chi_3(x_3)) \\
\sigma_3^0 + \sigma_3^1 + \sigma_3^2 &= 3(\chi_3(x_1) \chi_3(x_2) + \chi_3(x_1) \chi_3(x_2) + \chi_3(x_2) \chi_3(x_3))
\end{align*}
\]

In the summation over \( b \) of the sum of the three products, the values of \( b = z_1^3, z_2^3, z_3^3 \) should be excluded. Thus we must compute

\[
N_2(3) = \frac{1}{9} \left( 2^6 - 3 + \frac{1}{3} \sum_{b \neq z_1^3, z_2^3, z_3^3} \left[ (\sigma_2^0 + \sigma_2^1 + \sigma_2^2) + (\sigma_3^0 + \sigma_3^1 + \sigma_3^2) \right] \right) .
\]

Therefore, two types of summations must be evaluated, namely

\[
S_2 = \sum_{b \neq z_1^3, z_2^3, z_3^3} \chi_3(b + z_1^3) \bar{\chi}_3(b + z_2^3) \quad \text{and} \quad S_3 = \sum_{b \neq z_1^3, z_2^3, z_3^3} \chi_3(b + z_1^3) \chi_3(b + z_2^3) ,
\]

the remaining ones being obtained by symmetry or complex conjugation. Considering \( S_2 \), and defining for short \( y_1 = z_3^2 + z_3^3, y_2 = z_1^3 + z_2^3, \) and \( y_3 = z_3^2 + z_2^3 \), we have

\[
S_2 = -\chi_3(y_3) \bar{\chi}_3(y_1) + \sum_{b \neq z_1^3} \chi_3(b + z_1^3) \bar{\chi}_3(b + z_2^3) = -\chi_3(y_2) \bar{\chi}_3(y_1) + \sum_{x \neq 0, y_3} \chi_3(x) \bar{\chi}_3(x + y_3) ,
\]

thus \( S_2 = -\chi_3(y_2) \bar{\chi}_3(y_1) - 1 \). Considering \( S_3 \) we have

\[
S_3 = \sum_{b \neq z_1^3, z_2^3, z_3^3} \chi_3(b + z_1^3) \chi_3(b + z_2^3) \chi_3(b + z_3^3) = \sum_{x \neq 0, y_3, y_2} \chi_3(x) \chi_3(x + y_3) \chi_3(x + y_2)
\]

thus, with the change of variable \( x = 1/z \), since the character is cubic we obtain

\[
S_3 = \sum_{z \neq 0, 1/y_2, 1/y_3} \chi_3(1 + z y_3) \chi_3(1 + z y_2) = \sum_{x \neq 1, 0, 1 + y_3/y_2} \chi_3(X) \chi_3(X \frac{y_3}{y_2} + 1 + \frac{y_2}{y_3})
\]

10
Let $S_3 = \chi_3(y_2)\bar{\chi}_3(y_3) + \sum_{X \neq 0, 1+y_3/y_2} \chi_3(X)\chi_3(X + 1 + \frac{y_3}{y_2})$

$= -1 + \chi_3(y_2)\bar{\chi}_3(y_3) + \sum_{X \neq 0, 1+y_3/y_2} \chi_3(X)\chi_3(X + 1 + \frac{y_3}{y_2})$

$= -1 + \bar{\chi}_3(y_2)\bar{\chi}_3(y_3)\sum_{x \in \mathbb{F}_{2^m}} \chi(x)\chi_3(x + 1)$.

In conclusion, we obtain

$N_2(3) = \frac{1}{9} \left[ 2^m - 11 - (-2)^{m/2} [\chi_3(y_1 y_2 y_3) + \bar{\chi}_3(y_1 y_2 y_3)] - (\chi_3(y_1 y_2) + \chi_3(y_1^2 y_2) + \chi_3(y_2 y_3) + \chi_3(y_2 y_3) + \chi_3(y_3 y_1^2) + \chi_3(y_3^2 y_1)] \right]$.

Note that, if $z_1 = 0$ (which corresponds to choosing $b$ in one particular coset), then $y_2$ and $y_3$ are cubes, and the number of solutions is

$N_2(3) = \frac{1}{9} \left[ 2^m - 13 - (-2)^{m/2} + 2[\chi_3(y_1) + \bar{\chi}_3(y_1)] \right]$.

Finally we focus our interest on the maximum over the $z_i$ and obtain

**Proposition 4.** $M_2(3) = \begin{cases} \frac{1}{9}(2^m + 2^{m/2} - 2) & \text{for } m/2 \text{ even} \\ \frac{1}{9}(2^m + 2^{m/2+1} + 1) & \text{for } m/2 \text{ odd} \end{cases}$

Let us now deal with the case $p > 2$:

$t = 2$. In this case, we have

$\prod_{i=1}^{2} I_{g_h}(b + z_i^2) = \frac{1}{4} \left( 1 + \sigma_1^{(h)} + \sigma_2^{(h)} \right) \quad h = 0, 1$, where $\sigma_1^{(h)} = (-1)^h \chi_2(x_1) + (-1)^h \chi_2(x_2)$, and $\sigma_2^{(h)} = \chi_2(x_1)\chi_2(x_2)$.

Since $\sigma_1^{(0)} + \sigma_1^{(1)} = 0$ and $\sigma_2^{(0)} + \sigma_2^{(1)} = 2(\chi_2(x_1)\chi_2(x_2))$, the sum over $b$ in the whole field $\mathbb{F}_{p^m}$, with the exclusion of $b = -z_1^2$ and $b = -z_2^2$, is

$N_p(2) = \frac{1}{2} \left( p^m - 2 + \sum_{b \neq -z_1^2, -z_2^2} \left( \chi_2(b + z_1^2)\chi_2(b + z_2^2) \right) \right)$.

Let $S$ denote the above summation: we evaluate it in closed form by substituting $b = \eta - z_1^2$, since $\chi_2$ is a nontrivial quadratic character, we have

$S = \sum_{\eta \neq 0, z_1^2, z_2^2} (\chi_2(\eta)\chi_2(\eta + z_1^2 - z_2^2)) = -1$, the summation being independent of the term $z_2^2 - z_1^2$, which is non-zero by hypothesis. In conclusion we have

$N_p(2) = \frac{1}{2} (p^m - 3)$, so that
Proposition 5. $M_p(2) = \frac{1}{2} (p^m - 1)$

$t = 3$. In this case

$$\prod_{i=1}^{3} I_{S_3} (b + z_i^2) = \frac{1}{8} \left( 1 + \sigma_1^{(h)} + \sigma_2^{(h)} + \sigma_3^{(h)} \right) \quad h = 0, 1,$$

where $\sigma_1^{(h)} = (-1)^h \chi_2(x_1) + (-1)^h \chi_2(x_2) + (-1)^h \chi_2(x_3)$, $\sigma_2^{(h)} = \chi_2(x_1) \chi_2(x_2) + \chi_2(x_1) \chi_2(x_3) + \chi_2(x_2) \chi_2(x_3)$, and $\sigma_3^{(h)} = (-1)^h \chi_2(x_1) \chi_2(x_2) \chi_2(x_3)$.

Since $\sigma_1^0 + \sigma_1^1 = 0$, $\sigma_2^0 + \sigma_2^1 = 2(\chi_2(x_1) \chi_2(x_2) + \chi_2(x_1) \chi_2(x_3) + \chi_2(x_2) \chi_2(x_3))$, and $\sigma_3^0 + \sigma_3^1 = 0$, the summation over $b$ of the sum of the two products, where the values of $b$ equal to $-z_1^2, -z_2^2, -z_3^2$ are excluded, becomes

$$N_p(3) = \frac{1}{4} \left( p^m - 3 + \sum_{b \neq -z_1^2, -z_2^2, -z_3^2} [\chi_2(x_1) \chi_2(x_2) + \chi_2(x_1) \chi_2(x_3) + \chi_2(x_2) \chi_2(x_3)] \right).$$

We thus need to evaluate only one type of summation, namely

$$S_2 = \sum_{b \neq -z_1^2, -z_2^2, -z_3^2} \chi_2(b + z_i^2) \chi_2(b + z_j^2) = \sum_{\eta \neq 0} \chi_2(\eta) \chi_2(\eta + z_2^2 - z_3^2) = -1 - \chi_2(z_2^2 - z_3^2) \chi_2(z_2^2 - z_3^2),$$

the remainder being obtained by symmetry. In conclusion, we obtain

$$N_p(3) = \frac{1}{4} \left[ p^m - 6 - (\chi_2(z_1^2 - z_2^2) \chi_2(z_3^2 - z_2^2) + \chi_2(z_1^2 - z_2^2) \chi_2(z_2^2 - z_3^2) + \chi_2(z_1^2 - z_2^2) \chi_2(z_2^2 - z_1^2)) \right].$$

And, if we consider the maximum, we have

**Proposition 6.** $M_p(3) = \begin{cases} \frac{1}{3} (p^m - 1) & p = 4k + 1 \\ \frac{1}{3} (p^m - 1) & p = 4k + 3, \ m \ odd \\ \frac{1}{3} (p^m - 1) & p = 4k + 3, \ m \ even \end{cases}$

### 3.2 Bounds

As the number of equations in system 3 or 5 becomes larger, exact computations become less meaningful for our purpose, as it would then be necessary to consider estimates and bounds on rather cumbersome expressions. We will thus shift our interest to a general upper bound for the function $N_p(t)$; we will first deal with the case $p = 2$, then the case $p > 2$.

Consider equation (4) written as

$$N_2(t) = \frac{1}{3^t} \sum_{b \in \mathbb{Z}_m, \ b \neq (z_i^2)} [\mathcal{P}_0 + \mathcal{P}_1 + \mathcal{P}_2], \quad (7)$$

where

$$\mathcal{P}_k = 3^t \prod_{i=1}^{t} I_{A_k}(x_i) = 1 + \sigma_1^{(k)} + \sigma_2^{(k)} + \cdots + \sigma_t^{(k)} \quad k = 0, 1, 2,$$
Using the binomial sum and its derivative, we finally obtain linear functions of \( b \) and each \( \sigma_j^{(k)} \) is a sum of monomials which are products of the same number \( j \) of distinct variables (characters) \( \chi_3(x_i) \) or \( \bar{\chi}_3(x_i) \), possibly times \( \zeta_3 \) or \( \zeta_3^2 \). In particular, the number of addends in \( \sigma_j^{(k)} \) is \( 2^j \binom{t}{j} \).

Define \( \sigma_j = \sigma_j^{(0)} + \sigma_j^{(1)} + \sigma_j^{(2)} \) for every \( j = 1, \ldots, t \); then \( \sigma_j \) contains fewer addends than any \( \sigma_j^{(k)} \), since all monomials multiplied by either \( \zeta_3 \) or \( \zeta_3^2 \) are canceled out with monomials multiplied by 1, and the surviving monomials are multiplied by 3 (see also the examples above). In particular, \( \sigma_1 \) is zero; \( \sigma_2 \) is a sum of monomials of the form \( \chi_3(x_i)\bar{\chi}_3(x_i) \) \((i, l \text{ distinct})\), whose total number is \( 2 \binom{t}{2} \); \( \sigma_3 \) is a sum of monomials of the form \( \chi_3(x_i)\chi_3(x_j)\chi_3(x_m) \) \((i, l, m \text{ all distinct})\), whose total number is \( 2 \binom{t}{3} \); and \( \sigma_4 \) is a sum of monomials of the form \( \chi_3(x_i)\chi_3(x_j)\bar{\chi}_3(x_m)\bar{\chi}_3(x_s) \) \((i, l, m, s \text{ all distinct})\), whose total number is \( 6 \binom{t}{4} \). In general, the number of surviving monomials of degree \( j \) can be computed by considering that each monomial is a product of \( n_1 \) characters and \( n_2 \) complex conjugate characters; thus \( n_1 + n_2 = j \). Supposing that \( \chi_3(x_i) \) are multiplied by \( \zeta_3 \) and \( \bar{\chi}_3(x_i) \) are multiplied by \( \zeta_3^2 \), the surviving monomial satisfies the condition \( n_1 + 2n_2 = 0 \mod 3 \). Therefore, the admissible values of \( 0 \leq n_2 \leq j \) satisfy the condition \( n_2 = 2j \mod 3 \): if \( e = 2j \mod 3 \) and \( e \in \{0, 1, 2\} \), the number of surviving monomials is \( \binom{t}{j} \) \( a_j \), where \( a_j = \sum_{h=0}^{\lfloor \frac{j-1}{3} \rfloor} \binom{j}{e+3h} \), with \( \{a_j\}_{j=1}^{2} = 2, 6, 10, 22, 46, 86, 170, 342 \ldots \) matching the sequence A078008 in [16] with the first two terms disregarded. We observe now that the product of \( j \) characters, whose arguments are distinct linear functions of \( b \), can be interpreted as a single character whose argument is a polynomial \( f(b) \) with \( j \) distinct roots: by [15, Theorem 2C'], each sum of these characters is upper bounded by \( (j - 1)^{\sqrt{2m}} \), so that

\[
N_2(t) \leq \left[ \frac{1}{3^{\frac{1}{3}}} \right] \left[ 2^m - t + \sum_{j=2}^{t} a_j (j - 1) \binom{t}{j} \sqrt{2^m} \right].
\]

The summation above is evaluated as follows, using the expression \( a_j = \frac{1}{3} \sum_{h=0}^{t} \zeta_3^{-he} (1 + \zeta_3^{h})^j \) for the sequence \( a_j \) as can be found in [2, 6]:

\[
\sum_{j=2}^{t} a_j (j - 1) \binom{t}{j} = \frac{1}{3} \sum_{j=2}^{t} \sum_{h=0}^{2} \zeta_3^{-he} (1 + \zeta_3^{h})^j (j - 1) \binom{t}{j} = \frac{1}{3} \sum_{h=0}^{t} \sum_{j=2}^{t} \zeta_3^{-he} (1 + \zeta_3^{h})^j (j - 1) \binom{t}{j}.
\]

Now, observing that \( e = -j \mod 3 \) and \( \zeta_3 \) is a cubic root of unity, we may substitute \( \zeta_3^{h} \) for \( \zeta_3^{-he} \) and write \( \zeta_3^{h} + \zeta_3^{2h} \) \( \zeta_3^{h} \zeta_3^{2h} \) in the last expression, which we then write as

\[
\frac{1}{3} \sum_{h=0}^{t} \sum_{j=0}^{t} \zeta_3^{h} + \zeta_3^{2h} \binom{t}{j} (j - 1) + 1 = \frac{1}{3} \sum_{h=0}^{t} \sum_{j=0}^{t} \zeta_3^{h} + \zeta_3^{2h} \binom{t}{j} - \sum_{j=0}^{t} \zeta_3^{h} + \zeta_3^{2h} \binom{t}{j}.
\]

Using the binomial sum and its derivative, we finally obtain

\[
\sum_{j=2}^{t} a_j (j - 1) \binom{t}{j} = 1 + \frac{1}{3} \sum_{h=0}^{t} \left( \zeta_3^{h} + \zeta_3^{2h} \right) (1 + \zeta_3^{h} + \zeta_3^{2h})^{t-1} - (1 + \zeta_3^{h} + \zeta_3^{2h})^{t}.
\]
that is
\[ \sum_{j=2}^{t} a_j(j-1) \binom{t}{j} = 1 + \frac{1}{3} [2t \cdot 3^t - 3^t] , \]

because \((1 + \zeta_3^h + \zeta_3^{2h})\) is 3 when \(h = 0\) and is 0 otherwise. In conclusion
\[ N_2(t) \leq \frac{1}{2t} \left[ 2^m + \sqrt{2^m} - t + 3^{t-2}(2t - 3)\sqrt{2^m} \right] , \]

where we see that, when \(3^{t-2}(2t - 3)\sqrt{2^m} - t + \sqrt{2^m} << 2^m\), roughly \(t << m/2\), then \(N_2(t) \simeq \frac{2^m}{3^{2t-1}}\).

In conclusion
\[ N_2(t) \leq 1 + \frac{1}{3} [2t \cdot 3^t - 3^t] , \]

which, after some manipulation, can be written as
\[ N_2(t) \leq 1 + \frac{1}{3} [2^t - 1 + 2t \cdot 3^t - 2^{t-1} + 1] \sqrt{2^m} \]

and we see that, when \(2^{t-1}(t - 2) + 1] \sqrt{2^m} - t << p^m\), roughly \(t << \frac{m}{2} \log_2 p\), then \(N_2(t) \simeq \frac{p^m}{2t-1} \).

4 Deterministic splitting II: fixed \(N\)

This section examines the smallest \(t\) such that the algorithm succeeds, in at most 1 or 2 attempts: we will call these \(t_1\) and \(t_2\), respectively.

Clearly, \(t_1 = \ell_m + 1\), since there are exactly \(\ell_m\) elements belonging to a given coset; then, if \(t > \ell_m\), the algorithm succeeds at the first attempt.

To evaluate \(t_2\), we must examine the number of representations of a \(b \neq 0\) in the field as the sum of an element in a given coset and an element in another (possibly the same) given coset (see also
We then consider the maximum $M$ of such numbers, over $b \neq 0$ in the field and over all possible pairs of cosets, so that $t_2$ is $1 + M$. This follows from considering equation (3): the worst-case scenario occurs when all roots are in the same coset, and when, by adding a $b$ to all of them, one gets elements again belonging to a common coset.

For the case of the cubic character, $M$ can be calculated as follows:

$$M = \max_{i,j,b} \sum_{z \neq 0, b} \frac{1 + \zeta_3^i \chi_3(z) + \zeta_3^j \bar{\chi}_3(b + z)}{3} \quad \frac{1 + \zeta_3^2 \chi_3(b + z) + \zeta_3^i \bar{\chi}_3(b + z)}{3}$$

which is the maximum over $i, j, b$ of the following expression:

$$\frac{1}{9} \left[ 2^m - 2 - \chi_3(b)\left(\zeta_3^{2i} + \zeta_3^{2j}\right) - \bar{\chi}_3(b)\left(\zeta_3^{i} + \zeta_3^{j}\right) - \zeta_3^{2i+j} - \zeta_3^{i+2j} - (-2)^{m/2}(\zeta_3^{2i+2j}\bar{\chi}_3(b) + \zeta_3^{i+j}\chi_3(b)) \right],$$

where we have again exploited the relations $\sum_{x \in \mathbb{F}_{2^m}} \chi_3(x) = 0$, $\sum_{x \in \mathbb{F}_{2^m}} \chi_3(x)\bar{\chi}_3(x + b) = -1$ and $\sum_{x \in \mathbb{F}_{2^m}} \chi_3(x)\chi_3(x + 1) = G_m(1, \chi_3) = (-2)^{m/2}$ ([3, 13, 17]). Then we have

**Proposition 7.** For the cubic character

$$M = \begin{cases} \frac{1}{9}(2^m + 2^{m/2} - 2) & \text{for } m/2 \text{ even} \\ \frac{1}{9}(2^m + 2^{m/2+1} + 1) & \text{for } m/2 \text{ odd} \end{cases}$$

For the case of the quadratic character, we consider similarly

$$M = \max_{i,j,b} \sum_{z \neq 0, b} \frac{1 + (-1)^i \chi_2(z)}{2} \quad \frac{1 + (-1)^i \chi_2(b - z)}{2}$$

$$= \max_{i,j,b} \left\{ \frac{1}{4} \left( p^m - 2 - \chi_2(b)(-1)^i - \chi_2(b)(-1)^j - (-1)^{i+j}\chi_2(-1) \right) \right\},$$

therefore

**Proposition 8.** For the quadratic character

$$M = \begin{cases} \frac{1}{4}(p^m - 1) & p = 4k + 1 \\ \frac{1}{4}(p^m + 1) & p = 4k + 3, \ m \ odd \\ \frac{1}{4}(p^m - 1) & p = 4k + 3, \ m \ even \end{cases}$$

**Remark 6** It is interesting to notice that $M$, which is the maximum $t$ such that it is still possible to fail to split a polynomial of degree $t$ with two attempts, is equal to the maximum number of attempts needed to split a polynomial of degree 3. Similarly, $\ell_m$ is at the same time the maximum $t$ such that it is possible to fail to split a polynomial of degree $t$ at the first attempt and the maximum number of attempts needed to split a polynomial of degree 2 (cf. also [14]).
References


Michele Elia  
Dipartimento di Elettronica  
Politecnico di Torino  
Corso Duca degli Abruzzi 24  
10129 Torino - Italy  
e-mail: michele.elia7@gmail.com

Davide Schipani  
University of Zurich  
Institute of Mathematics  
Winterthurerstrasse 190  
8057 Zurich - Switzerland  
e-mail: davide.schipani@math.uzh.ch