

**Factors of small degree of some difference
polynomials $f(x) - g(t)$ in $F[t][x]$**

By FRANÇOIS BERRONDO (Brest) and LUIS GALLARDO (Brest)

Abstract. Let $s \in F[t] \setminus F$ be a nonconstant polynomial over a perfect field F of characteristic 2. There are no factors of degree 2 of the polynomial $T = x^m + g(x)^2 + s \in F[t][x]$ where $m > 3$ is an odd integer and $g(x) \in F[x] \setminus \{0\}$ is an additive polynomial of degree $d < (m - 1)/2$ with $g(0) = 0$.

1. Introduction

It is unknown whether or not a general method to find small degree factors of polynomials $P \in k[x]$ in one variable x with coefficients in some field k of characteristic $p \geq 0$ can exist. There are several results in the literature (see [2]–[5]) concerning the special case when P is a trinomial $x^n + Ax^m + B$, in which the exponents m, n satisfy $n > m > 0$, we have $\gcd(p, mn(m - n)) = 1$ and $p > 0$, while A, B satisfy some technical conditions and lie in a finite extension of $k(y)$ where y is a variable vector; or when $p = 0$ and k is an algebraic number field. However, nothing is known in the case when the field of coefficients is a rational field of finite characteristic $p > 0$ where p divides $mn(m - n)$.

It is natural to work first in the simplest case where $k = F(t)$ for some field F and some indeterminate t . We wish to study in detail in this paper the special case in which P is a polynomial of the form $T = x^m + g(x)^2 + s$

Mathematics Subject Classification: 11T06, 11R09.

Key words and phrases: polynomials, characteristic 2, function fields.

where $m > 3$ is an odd integer and $0 \neq g(x) \in F[x]$ is a nontrivial additive polynomial of degree $d < (m-1)/2$ with $g(0) = 0$, while $s \in F[t]$ is non constant, and F is a perfect field of characteristic 2. We believe that the use of the canonical derivation over such a field k is the key to obtain useful information about the factors of T in $F[t][x]$.

Our main result is:

- 1) T has no quadratic factors in $F[t][x]$ provided $m > 3$, (see Theorems 1 and 2).

A key lemma for a neat proof of our result above was suggested by the referee (see Lemma 2). Moreover, 1) is a first step in order to generalize some results of BILU (see [1]) who classified the difference polynomials with quadratic factors in characteristic 0.

We shall use the following notations: For a field F we let $\overline{F}$ denote, as usual, a fixed algebraic closure of F . If E is an extension of the field F , then we denote by $[E : F]$ the degree of E over F , i.e. the dimension of E considered as a vector space over F . If $f(x) \in F[t][x]$ has degree $d < 4$ then we denote by K its splitting field over the rational field k . We denote by Tr the trace of K over k . We denote by N the norm of K over k , provided the degree of the extension $[K : k] \neq 6$. Observe that when $[K : k] = 6$ we denote by N the square root of the norm, instead of the norm itself. Concerning differentiation, we denote by the same classical symbol $()'$ the canonical extension to K of the derivation relative to t in k , and the derivation itself.

The derivation relative to x will be denoted by $\partial/\partial x$.

First of all we recall the definition of additive polynomials:

Definition 1. A polynomial $A \in F[z]$ where F is some field and z is an indeterminate is called additive if

$$A(x+y) = A(x) + A(y)$$

for all $x, y \in \overline{F}$.

2. We may assume that s is not a square

Lemma 1. *Let $m > 1$ be an odd integer. Assume that $s = r^2$ is a nonconstant square in $F[t] \setminus F$ where F is a perfect field of characteristic 2.*

If the difference polynomial $T = x^m + g(x)^2 + s \in F[t][x]$, where $g(x) \in F[x]$ is a polynomial of degree $< m/2$, has a factor $f(x) \in F[t][x]$ of degree d with $0 < d < 4$, then all coefficients of $f(x)$ are squares in $F[t]$ and $f(x^2)^{1/2}$ divides $(T(x^2))^{1/2} = x^m + g_1(x)^2 + s$, where the coefficients of g are the squares of the coefficients of g_1 .

PROOF. We may assume that $f(x)$ is monic and irreducible. Set $e = [K : k]$. Let $c \in F[t]$ denote the coefficient of any monomial appearing in $f(x)$. It suffices to prove that c is a square in k . Observe that every root $\alpha \in K$ of $f(x)$ is a square in K , since s is a square in $F[t]$ and

$$\alpha((\alpha^{(m-1)/2})^2) = s + g(\alpha)^2.$$

It follows from the relations between coefficients and roots of $f(x)$ that c is a square in K . Thus c is a square in $F[t]$ when $e \in \{1, 3\}$. Otherwise, let us consider first the case when $d = \deg(f) = 2$. Then $e = 2$, and assuming the separability of the extension K over k , one obtains immediately that $f(x) = x^2 + ax + b$ where b is a nonzero square in K so that $a \neq 0$.

We explain in more detail why the extension K over k cannot be inseparable, i.e. we always have $a \neq 0$.

Assume that for some $Q(x) \in F[t][x]$ we have

$$x^m + g(x)^2 + r^2 = (x^2 + b)Q(x). \quad (1)$$

We claim that $\alpha \in F[t]$. Indeed, since $\alpha^2 = b$, it follows from (1) that

$$\alpha = \frac{h(b) + r^2}{b^{(m-1)/2}} \in k$$

where the coefficients of h are the squares of the coefficients of g , proving the claim.

Since c is a square in $K = k[\alpha]$ one has

$$c = (y + z\alpha)^2 = y^2 + \alpha^2 z^2 \quad (2)$$

for some $y, z \in k$. Taking the trace Tr in (2) one has $0 = c + c = \text{Tr}(c) = z^2 a^2$, so that $z = 0$ and $c = y^2$, with $y \in F[t]$.

Now, we treat the case in which $d = \deg(f) = 3$, so that $e \in \{3, 6\}$. We may assume that $e = 6$ and that $K = k(\gamma, \beta)$ where $\beta^2 + \beta = g$, and $\gamma^3 + a\gamma + b = 0$, for some $a, b, g \in k$.

Assume that $c = z^2$ for some $z \in K$:

$$z = a_0 + a_1\gamma + a_2\gamma^2 + (b_0 + b_1\gamma + b_2\gamma^2)\beta$$

where the a_i 's and b_j 's are in k . After some computation we get

$$c = a_0^2 + gb_0^2 + u_1\gamma + u_2\gamma^2 + b_0^2\beta + u_4\beta\gamma + u_5\beta\gamma^2, \quad (3)$$

where the u_i 's are certain quadratic polynomials in the a_i 's and b_j 's with coefficients in $\{a, b, g\}$. It follows immediately from (3) that $b_0 = 0$ so that $c = a_0^2$ as claimed.

Set $T/f(x) = t_0 + t_1x + \dots + t_mx^m$ with $t_m \neq 0$ and $t_n \in F[t]$ for all $0 \leq n \leq m$. Since trivially $T = (T/f(x))f(x)$, it follows that t_0 is also a square in $F[t]$. It follows by induction on n that all these coefficients t_n of $T/f(x)$ are also squares in $F[t]$, so that $f(x^2)^{1/2}$ divides $(T(x^2))^{1/2} = x^m + g_1(x)^2 + s^{1/2}$ in $F[t][x]$, where the coefficients of g are the squares of the coefficients of g_1 .

This completes the proof of the lemma. $\square$

3. T has at most one root in $F[t]$

Theorem 1. *Let F be a perfect field of characteristic 2. Suppose $m > 3$ is odd and $0 \neq g(x) \in F[x]$ is an additive polynomial of degree $d < (m-1)/2$, with $g(0) = 0$. Let s be a nonconstant polynomial in $F[t] \setminus F$. If the difference polynomial $T = x^m + g(x)^2 + s \in F[t][x]$ has a root $r \in F[t]$, then r is the only root of T in $F[t]$.*

PROOF. This follows immediately from Theorem 2. $\square$

In the special case when $g(x) = x$, there are two other proofs of this result, a direct one, omitted for brevity, and another proof that is a corollary of the “abc” theorem for rational fields, i.e. a corollary of Mason’s theorem, (see e.g. [6]).

This latter proof is sketched below:

By Lemma 1, we do assume that s is not a square in $F[t]$. Suppose that v is another root of T in $F[t]$. Set $d = \gcd(r, v)$ and let r_1, v_1 in

$F[t]$ be defined by $r = dr_1$, $v = dv_1$, so that $\gcd(r_1, v_1) = 1$. After some computation we get

$$(r_1^m + v_1^m)r_1^m v_1^m = r_1^m v_1^m \left(\frac{(r_1 + v_1)(r_1 + v_1)}{d^{m-2}} \right), \quad (4)$$

then (since $r' \neq 0$ and $v' \neq 0$), the “abc” theorem applied to $A = r_1^m$, $B = v_1^m$, $C = A + B$ in (4) implies:

$$\begin{aligned} m \deg(r_1) &< n(r_1) + n(v_1) + 2n(r_1 + v_1) \\ &\leq \deg(r_1) + \deg(r_1) + 2\deg(r_1) = 4\deg(r_1) \end{aligned}$$

where $n(P)$ means the number of distinct roots of $P \in F[t]$ in $\overline{k}$; i.e. we get the contradiction $m < 4$.

4. T has no quadratic factors in $F[t][x]$ provided $m > 3$

The following lemma, discovered by the referee, is the key to obtain a neat proof of the main result of the section.

Lemma 2. *Let $f, g \in F[x]$, where F is a field of characteristic 2, $m = \deg(f)$ is odd and $n = \deg(g)$ is positive. If $f(x) - g(t)$ has in $F[t, x]$ a factor $x^2 + a(t)x + b(t)$, then $ab \neq 0$ and*

$$\deg(b) = 2\deg(a).$$

PROOF. Since m is odd, the equation $f(x) - g(t) = 0$ has in the algebraic closure of $F(t)$, m distinct zeros x_j , with the expansions at ∞ given by $\zeta_m^j \gamma^{1/m} t^{n/m} + T_j$, where ζ_m is a primitive root of unity of order m in $\overline{F}$, γ is the leading coefficient of g , and T_j is the sum of terms of lower degree than n/m . Since by the assumption

$$x^2 + a(t)x + b(t) \mid f(x) - g(t),$$

we have for some $i \neq j$

$$x^2 + a(t)x + b(t) = (x + x_i)(x + x_j) = x^2 + (x_i + x_j)x + x_i x_j,$$

thus at $t = \infty$

$$a(t) = (\zeta_m^i + \zeta_m^j)\gamma^{1/m}t^{n/m} + T_i + T_j, \quad b(t) = \zeta_m^{i+j}\gamma^{2/m}t^{2n/m} + U$$

where U is the sum of terms of degree lower than $2n/m$.

However, $\zeta_m^i + \zeta_m^j \neq 0$ since $\zeta_m^i \neq \zeta_m^j$ and also $\zeta_m^{i+j} \neq 0$. This gives $ab \neq 0$ and $\deg(b) = 2\deg(a)$, thereby completing the proof of the lemma. $\square$

The following lemma presents some necessary conditions that a possible quadratic factor $f(x) \in F[t][x]$ of T must satisfy.

Lemma 3. *Let F be a perfect field of characteristic 2. Let $m > 1$ be an odd integer. Let $s \in F[t] \setminus F$ be a polynomial that is not a square in $F[t]$. Let T be the polynomial $T = x^m + g(x)^2 + s \in F[t][x]$ where $m > 3$ is an odd integer and $g(x) \in F[x]$ is a nonzero additive polynomial of degree $d < m/2$ with $g(0) = 0$. Assume that $f(x) = x^2 + ax + b \in F[t][x]$ having roots $\alpha, \beta \in K$, is a factor of T . We have*

- a) $b^m = (s + g(\alpha)g(\beta))^2 + (g(\alpha) + g(\beta))^2s$.
- b) $ab' \neq 0$.
- c) $b^{m-1}(b')^2a^2 = (g(\alpha) + g(\beta))^4((b')^2 + b'a'a + (a')^2b)$.
- d) $a \in F[t]$ is not constant, i.e. $a \notin F$.

PROOF. From

$$\alpha^m = s + g(\alpha)^2, \quad \beta^m = s + g(\beta)^2,$$

we get

$$b^m = (s + g(\alpha)g(\beta))^2 + (g(\alpha) + g(\beta))^2s$$

which proves a).

First of all observe that $g(\alpha) + g(\beta)$ and $g(\alpha)g(\beta)$ are polynomials in a, b so that they are elements of $F[t]$. To prove that $b' \neq 0$, assume that b is a square in $F[t]$. If $g(a) = g(\alpha) + g(\beta) \neq 0$ then from a) it follows that s is also a square, which is impossible. If $g(a) = 0$ then either $a = 0$ which is impossible by Lemma 2, or a is a nonzero constant in F . By Lemma 2 this implies that b is also a nonzero constant in F . Observing that

$$T = x^m + g(x)^2 + s = (x^2 + ax + b)A(t, x)$$

for some polynomial $A \in F[t][x]$, we get on differentiating relative to t above:

$$s' = (x^2 + ax + b) \frac{\partial A(t, x)}{\partial(t)} \quad (5)$$

which implies, by putting $x = \alpha$ in both sides of (5),

$$s' = 0.$$

But this is impossible. Result b) follows.

In order to prove c) we set $h = g(\alpha) + g(\beta)$ and we differentiate $\alpha^2 = a\alpha + b$ relative to t to obtain

$$\alpha' a = a' \alpha + b'. \quad (6)$$

On the other hand, since $\alpha^m = g(\alpha)^2 + s$ and $\beta^m = g(\beta)^2 + s$ one has

$$\delta = \alpha^{m+1} + \beta^{m+1} = (\alpha + \beta)\beta^m + (\alpha^m + \beta^m)\alpha = (a\beta)\beta^{m-1} + h^2\alpha \quad (7)$$

so that (recalling that $m+1$ and $m-1$ are even), we get by differentiating (7) relative to t :

$$\delta' = 0 = \beta^{m-1}(\beta a)' + \alpha' a^2.$$

But $\beta a = \beta\alpha + \beta^2$, so that $(\beta a)' = (\beta\alpha)' = b'$ and we obtain

$$\beta^{m-1}b' = \alpha'h^2, \quad \alpha^{m-1}b' = \beta'h^2. \quad (8)$$

This together with (6) gives

$$\beta^{m-1}b'a = h^2(a'\alpha + b'), \quad \alpha^{m-1}b'a = h^2(a'\beta + b'). \quad (9)$$

On multiplying the corresponding sides of the equations in (9), one obtains c) since $\alpha\beta = b$, while $g(\alpha) + g(\beta) = h$ and $\alpha + \beta = a$.

To prove d), assume that $a \neq 0$ is constant so that $a' = 0$. From c) it follows that

$$b^{m-1}a^2 = g(a)^4,$$

since $b' \neq 0$ by b). But this means that b is constant, contrary to b). This proves d). $\square$

Now we are ready to present our main result.

Theorem 2. *Let s be a nonconstant polynomial in $F[t] \setminus F$ where F is a perfect field of characteristic 2. Let $m > 3$ be an odd integer and $g(x) \in F[x]$ an additive polynomial of degree $d < (m-1)/2$ with $g(0) = 0$. Then the polynomial $T = x^m + g(x)^2 + s \in F[t][x]$ has no factors of degree 2.*

PROOF. First of all, using Lemma 1, we may assume that s is not a square. Assume, contrary to the conclusion, that T has some factor of degree 2 in $F[t][x]$.

More precisely, assume that $q = x^2 + ax + b \in F[t][x]$ divides T . Set $h = g(a)$. We distinguish two cases:

Case 1. $a' = 0$, so that by Lemma 3 c) and by Lemma 3 b), we get $b^{m-1}a^2 = h^4$. So

$$(m-1)\deg(b) + 2\deg(a) = 4\deg(h) \leq 4d\deg(a).$$

This implies by Lemma 3 d) and by Lemma 2 the contradiction $m \leq 2d$.

Case 2. $a' \neq 0$. Observe that $b' \neq 0$ by Lemma 3 b). We shall denote by $d_1 = \deg(a)$, $d_2 = \deg(b)$, and by $d_3 = \deg(a')$, $d_4 = \deg(b')$ the degrees of the derivatives of a, b relative to t . Taking degrees relative to t in Lemma 3 c) we get

$$(m-1)d_2 + 2d_4 + 2d_1 \leq 4dd_1 + \max(2d_4, d_4 + d_3 + d_1, 2d_3 + d_2). \quad (10)$$

Observe that we have

- a) $2 \leq 2d_1 = d_2$ by Lemma 3 b) and Lemma 2,
- b) $2 \leq d_4 < d_2$ since by Lemma 3 b) $b' \neq 0$ so that it has even degree,
- c) $4 \leq 2d_3 < 2d_1 = d_2$ since $a' \neq 0$ and by Lemma 3 b) and Lemma 2,
- d) $0 \leq 2d_4 < 2d_2$, $d_4 + d_3 + d_1 < 2d_2$, $2d_3 + 2d_1 < 2d_2$, from a), b), c) above and Lemma 2. $\square$

Thus (10) implies

$$(m-1)d_2 + 2d_4 + 2d_1 \leq 4dd_1 + 2d_2,$$

so that, using Lemma 2, we get

$$(m-1)d_2 < 4 + (m-1)d_2 \leq (2d-1)(2d_1) + 2d_2 \leq (2d+1)d_2,$$

i.e. we obtain the contradiction $m-1 < 2d+1 < m$.

5. Conjecturally, T has no cubic factors in $F[t][x]$

The key to obtain the proof that our difference polynomial $T = x^m + g(x)^2 + s \in F[t][x]$ has no quadratic factors in $F[t][x]$, (see Theorem 2), resides in the use of Lemma 2; i.e. it relies on the fact that we can prove that for a possible irreducible quadratic factor $q = x^2 + ax + b \in F[t][x]$ of T we have

$$\deg(b) = 2 \deg(a).$$

In other words, we can say that a kind of “homogeneity” must occur in q . Moreover, we may say that only this new property “earned by q ” implies the nonexistence of such q .

We were unable to prove the natural analogous property for possible cubic factors in $F[t][x]$ of T :

Conjecture 1. *Let $m > 3$ be an odd integer and let F be a perfect field of characteristic 2. Assume that $q(x) = x^3 + ax^2 + bx + c \in F[t][x]$ is an irreducible factor of the difference polynomial $T = x^m + g(x)^2 + s \in F[t][x]$ where $m > 3$ is an odd integer, s is an element of $F[t]$ that is not a square, and $g(x) \in F[x] \setminus \{0\}$ is an additive polynomial of degree $d < (m - 1)/2$ with $g(0) = 0$.*

We have $abc \neq 0$ and

- a) $\deg(c) = 3 \deg(a)$;
- b) $\deg(b) = 2 \deg(a)$.

Assuming Conjecture 1, it may be proved that $d < (m - 4)/2$ implies that T has no cubic factors in $F[t][x]$. This will be included in a future paper.

ACKNOWLEDGMENTS. We thank the organizers of the fourth European Congress of Mathematics (4ecm) at Stockholm for accepting poster 2.28 in which a short version of this paper was presented to colleagues. We also thank JEAN-MARC DESHOUILERS who invited the second named author to show an early version of the paper at Luminy. Warm thanks to the referee for great suggestions and helpful comments.

References

- [1] Y. BILU, Quadratic factors of $f(x) - g(y)$, *Acta Arith.* **90** (1999), 341–355.
- [2] A. SCHINZEL, On reducible trinomials, *Dissert. Math.* **329** (1993).
- [3] A. SCHINZEL, Errata to [2], *Acta Arith.* **73** (1995), 399–400.
- [4] A. SCHINZEL, On reducible trinomials II, *Publ. Math. Debrecen* **56**, no. 3–4 (2000), 575–608.
- [5] A. SCHINZEL, On reducible trinomials, III, *Period. Math. Hung.* **43**, no. 1–2 (2001), 43–69.
- [6] L. N. VASERSTEIN, Quantum (abc) -theorems, *J. Number Theory* **81**, no. 2 (2000), 351–358.

FRANÇOIS BERRONDO
MATHEMATICS, UNIVERSITY OF BREST
6, AVENUE LE GORGEU
C.S. 93837, 29238 BREST CEDEX 3
FRANCE

LUIS GALLARDO
MATHEMATICS, UNIVERSITY OF BREST
6, AVENUE LE GORGEU
C.S. 93837, 29238 BREST CEDEX 3
FRANCE

E-mail: Luis.Gallardo@univ-brest.fr

(Received October 28, 2003; revised October 18, 2004)