Functiones et Approximatio
45.1 (2011), 67–78

UNITARY PERFECT POLYNOMIALS OVER $\mathbb{F}_4$ WITH LESS THAN FIVE PRIME FACTORS

Luis H. Gallardo, Olivier Rahavandrainy

Abstract: We determine all unitary perfect polynomials with less than five distinct prime factors over a finite field with four elements.

Keywords: Sum of divisors, polynomials, finite fields, characteristic 2.

1. Introduction

Let p be a prime number and let $\mathbb{F}_q$ be a finite field of characteristic p with q elements. Let $A \in \mathbb{F}_q[x]$ be a monic polynomial. We say that a divisor d of A is unitary if d is monic and $\gcd(d, \frac{A}{d}) = 1$. Let $\omega(A)$ denote the number of distinct monic irreducible (or *prime*) factors of A over $\mathbb{F}_q$ and let $\sigma(A)$ (resp. $\sigma^*(A)$) denote the sum of all monic divisors (resp. unitary divisors) of A (σ and σ^* are multiplicative functions). We call *even* a polynomial with some zero in $\mathbb{F}_q$, and *odd* a polynomial that is not even. If any zero of A lies in $\mathbb{F}_q$ then we say that A is a splitting polynomial (or that A splits in $\mathbb{F}_q$). We consider only nonconstant polynomials $A \notin \mathbb{F}_q$.
If $\sigma(A) = A$ (resp. $\sigma^*(A) = A$), then we say that A is a perfect (resp. unitary perfect) polynomial. This is a polynomial analogue of the notions of multiperfect (resp. unitary multiperfect) numbers, (see, e.g., [14]).

E. F. Canaday [5], the first doctoral student of Leonard Carlitz, began in 1941 the study of perfect polynomials by working on the prime field $\mathbb{F}_2$. Later, in the seventies, J. T. B. Beard Jr. et al. [3],[4] extended this work in several directions. We [6], [7], [8], [9], [10],[11] became interested in this subject, a few years ago. In particular we [6], [7],[11] determined all perfect polynomials A over $\mathbb{F}_4$ such that $\omega(A) \leqslant 4$.

J. T. B. Beard Jr et al. [1], [2] obtained the first results about unitary perfect polynomials. We [12] continued this work by considering splitting polynomials over

2010 Mathematics Subject Classification: primary: 11T55; secondary: 11T06

the quadratic extension $\mathbb{F}_{p^2}$ of the prime field $\mathbb{F}_p$. Recently, we [13] characterized all unitary perfect binary polynomials $A \in \mathbb{F}_2[x]$ such that $\omega(A) \leqslant 4$.

We determine in this paper all unitary perfect polynomials A over $\mathbb{F}_4$, such that $\omega(A) \leqslant 4$. This extends the results for $p = 2$ in [12]. The number of cases to consider is reasonable so we discuss all of them here, contrary to the case of odd perfect polynomials in [8]. However, as in the analogue cases over the integers, the computations grow exponentially when $\omega()$ grows so for the moment it seems very difficult to study perfect or unitary perfect polynomials with a moderately large number of distinct prime factors. New ideas are required to properly treat these cases.

As usual, $\mathbb{N}$ denotes the nonnegative integers and $\mathbb{N}^*$ the positive integers. We denote by $A^{'}$ the formal derivative of a polynomial A relative to x. We put:

$\mathbb{F}_4 =$ $\{0, 1, \alpha, \alpha^2\}$ where α is in a fixed algebraic closure of the prime field $\mathbb{F}_2$ and satisfies $\alpha^2 + \alpha + 1 = 0$,

$\Omega_1 =$ $\{P \in \mathbb{F}_4[x] : P$ and $P + 1$ are odd and irreducible$\}$,

$\Omega_2 =$ $\{P \in \mathbb{F}_4[x] : P,\ P + 1, P^3 + P^2 + 1,\ P^3 + P + 1$ are odd and irreducible$\}$,

$\bar{\alpha} =$ $\alpha + 1 = \alpha^2$ the conjugate of α by the Frobenius automorphism.

Our main results are the following:

Theorem 1.1. *Let A be a nonconstant polynomial over $\mathbb{F}_4$ such that $\omega(A) \leqslant 4$, then A is unitary perfect if and only if $\omega(A)$ is even and there exists $a \in \mathbb{F}_4$, such that $A(x + a)$ is of the form B^{2^k} for some $k \in \mathbb{N}$ where:*

a) $B \in \{x(x + 1)\} \cup \{P(P + 1) : P \in \Omega_1\}$, *if* $\omega(A) = 2$.

b) $B \in \{(x^2+x)^{2^r}(x^2+x+1)^{2^s} : r, s \in \mathbb{N}\} \cup \{x^4+x, (x^4+x)^3\} \cup \{x^3(x+\alpha)^3(x+1)^2(x+\bar{\alpha})^2, x^3(x+1)^3(x+\alpha)^4(x+\bar{\alpha})^6\}$, *if* $\omega(A) = 4$ *and if A splits in* $\mathbb{F}_4$.

c) $B \in \{(x^2 + x)^{2^n}(P^2 + P)^{2^m}, (P^2 + P)^{2^m}(R^2 + R)^{2^n} : m, n \in \mathbb{N}, P, R \in \Omega_1\} \cup \{P^4(P+1)^7(P^3+P^2+1)(P^3+P+1) : P \in \Omega_2\} \cup \{P^7(P+1)^7(P^3+P^2+1)^2(P^3+P+1)^2 : P \in \Omega_2\}$, *if* $\omega(A) = 4$ *and if A does not split in* $\mathbb{F}_4$.

The results above are similar [11] to those about perfect polynomials, except that there does not exist a unitary perfect polynomial over $\mathbb{F}_4$, with $\omega(A) = 3$. Furthermore, (see [13]) for $P \in \{x, x+1\}$, the polynomials $P^4(P+1)^7(P^3+P^2+1)(P^3+P+1)$ and $P^7(P+1)^7(P^3+P^2+1)^2(P^3+P+1)^2$ are both unitary perfect over $\mathbb{F}_2$. Observe also (see Lemma 2.8) that Ω_1 and Ω_2 are infinite sets. So our families of unitary perfect polynomials are non-trivially infinite.

After some preliminary results shown in section 2 we prove Theorem 1.1 in the remaining sections. The proof consists of two main parts corresponding to the cases $\omega(A) \leqslant 3$ (Propositions 3.1 and 3.4) and $\omega(A) = 4$ (Propositions 4.1 and 4.3).

2. Preliminary

We need the following results. Some of them are obvious, so we omit their proofs. Our main new result is Lemma 2.7 that may have an interest in his own since some polynomials occurring there are polynomial analogues of the Mersenne numbers. At the end of the section (see Lemma 2.8) we recall the existence of certain infinite families of irreducible polynomials. This will be useful for determining non trivial infinite families of unitary perfect polynomials. In our first lemma below we describe the primary parts with minimal degree of such a polynomial:

Lemma 2.1 ([13, Lemma 2.1]). *If $A = P_1^{h_1} \cdots P_r^{h_r} Q_1^{k_1} \cdots Q_s^{k_s}$ is a nonconstant unitary perfect polynomial over $\mathbb{F}_4$ such that:*

$$\begin{cases} P_1, \dots, P_r, Q_1, \dots, Q_s \quad \text{are monic, distinct and prime,} \\ h_1 \deg(P_1) = \cdots = h_r \deg(P_r) < k_1 \deg(Q_1) \leqslant \cdots \leqslant k_s \deg(Q_s). \end{cases}$$

Then: $r \equiv 0 \pmod{p}$.

Proof. By definition, one has

$$0 = \sigma^*(A) - A = \frac{A}{P_1^{h_1}} + \cdots + \frac{A}{P_r^{h_r}} + \cdots$$

so that the leading coefficient $r = 1 + \cdots + 1$ of $\dfrac{A}{P_1^{h_1}} + \cdots + \dfrac{A}{P_r^{h_r}}$, equals 0 in $\mathbb{F}_p$. ■

Lemma 2.2. *If $A = A_1 A_2$ is unitary perfect over $\mathbb{F}_4$ and if* $\gcd(A_1, A_2) = 1$. *Then A_1 is unitary perfect if and only if A_2 is unitary perfect.*

Unitary perfect polynomials are invariant under some transformations:

Lemma 2.3. *If $A(x)$ is unitary perfect over $\mathbb{F}_4$, then for any $a \in \mathbb{F}_4$ and for any $n \in \mathbb{N}$, the polynomials $A(x+a)$ and A^{2^n} are both unitary perfect over $\mathbb{F}_4$.*

Lemma 2.4 ([7, Lemmas 2.4 and 2.6]).

(i) *For any integer $n \geqslant 2$, the polynomial $1 + x + \cdots + x^n$ is reducible over $\mathbb{F}_4$.*

(ii) *If $1 + x + \cdots + x^{2n} = PQ$, with P, Q irreducible, then $2n+1$ is a prime number,* $\deg(P) = \deg(Q)$, *and $P(0) = Q(0) = 1$ for $n \geqslant 2$.*

(iii) *If $1 + x + \cdots + x^{2n} = 1 + (x+1) + \cdots + (x+1)^{2n} = PQ$, with P, Q irreducible, then $n = 3$ and $\{P, Q\} = \{x^3 + x^2 + 1, x^3 + x + 1\}$.*

(iv) *If $1 + x + \cdots + x^{2n} = PQ$, for irreducible polynomials P, Q such that P and Q are of the form $x^a(x+1)^b + 1$, then $n = 3$ and $\{P, Q\} = \{x^3 + x^2 + 1, x^3 + x + 1\}$.*

In the following lemmas we replace x by more general prime polynomials.

Lemma 2.5. (see [6, Lemmas 2.1 and 2.5]) *Let $P, Q \in \mathbb{F}_4[x]$ such that P is irreducible and $1 + \cdots + P^{2n} = Q^m$ for some $m, n \in \mathbb{N}$. Then $m \in \{0, 1\}$. Moreover, if Q is irreducible, then $n = m = 0$.*

Lemma 2.6. (see [5, Lemma 6] and [11, Lemmas 12, 13]) *Let $P, Q \in \mathbb{F}_4[x]$ such that P is irreducible and let $n, m \in \mathbb{N}$.*

(i) *If* $1+P+\cdots+P^{2n} = Q^m A$, *with* $m > 1$ *and* $A \in \mathbb{F}_4[x]$ *nonconstant, then* $\deg(P) > \deg(Q)$.
(ii) *If* $1+P+\cdots+P^{2n} = RS$ *then* $\deg(R) = \deg(S) = n \deg(P)$.
(iii) *If* $1+P+\cdots+P^h = 1+(P+1)+\cdots+(P+1)^h$, *then* $h = 2^n - 2$, *for some* $n \in \mathbb{N}$.

The following lemma generalizes part iv) of Lemma 2.4.

Lemma 2.7. *Assume that* $1+P+\cdots+P^{2n} = RS = \big(P^a(P+1)^b+1\big)\big(P^c(P+1)^d+1\big)$ *for some* $a,b,c,d \geqslant 1$, *with* $P, P+1$ *both irreducible. Then* $n = 3$ *and* $\{R,S\} = \{P^3+P+1, P^3+P^2+1\}$.

Proof. If either $(a,c \geqslant 2)$ or $(a = c = 1)$ then:

$$1+P+\cdots+P^{2n} = \big(P^a(P+1)^b+1\big)\big(P^c(P+1)^d+1\big) = 1+P^2C,$$

for some polynomial $C \in \mathbb{F}_4[x]$. This is impossible. We may suppose that $a = 1$ and $c \geqslant 2$. We have $a+b = c+d = n \geqslant 3$ by Lemma 2.6 ii). Thus,

$$\begin{aligned} 1+P+\cdots+P^{2n} &= \big(P(P+1)^{n-1}+1\big)\big(P^c(P+1)^{n-c}+1\big) \\ &= P^{c+1}(P+1)^{2n-c-1} + P(P+1)^{n-1} + P^c(P+1)^{n-c} + 1. \end{aligned}$$

Hence:

$$P+\cdots+P^{2n} = P(P+1)^{n-c}\big(P^c(P+1)^{n-1} + (P+1)^{c-1} + P^{c-1}\big),$$

$$P(P+1)(1+P+\cdots+P^{n-1})^2 = P(P+1)^{n-c}\big(P^c(P+1)^{n-1}+(P+1)^{c-1}+P^{c-1}\big),$$

$$(1+P+\cdots+P^{n-1})^2 = (P+1)^{n-c-1}\big(P^c(P+1)^{n-1} + (P+1)^{c-1} + P^{c-1}\big). \quad (1)$$

We claim that $n-c-1 = 0$. Assume to the contrary that $n-c-1 \geqslant 1$. Then $1+P$ divides $1+P+\cdots+P^{n-1}$, so n must be even. Since $P+1$ does not divide $P^c(P+1)^{n-1}+(P+1)^{c-1}+P^{c-1}$ both factors on the right hand side of (1) must be perfect squares so that c is odd. By differentiation of both sides of (1) one gets the contradiction (2) below:

$$0 = P^{'}P^{c-1}(P+1)^{2n-c-3}((P+1)+P) = P^{'}P^{c-1}(P+1)^{2n-c-3}. \quad (2)$$

This proves the claim. Thus, $d = 1$ and $b = c$. We have then now

$$1+P^2+P^4++\cdots+P^{2n-2} = P^{n-1}(P+1)^{n-1} + (P+1)^{n-2} + P^{n-2}. \quad (3)$$

If n is even (so that $c-1$ is also even) we get the same contradiction as in (2). If n is odd we get by differentiation of both sides of (3):

$$0 = P^{'}((P+1)^{n-3} + P^{n-3}).$$

We conclude that $n = 3$ and $b = c = 2$. This completes the proof of the lemma. ■

The following lemma describes some interesting infinite sets.

Lemma 2.8.

a) *There exist infinitely many prime polynomials $P \in \mathbb{F}_4[x]$ such that $P+1, P^3+P+1$, and P^3+P^2+1 are all prime.*

b) *For all $k \in \mathbb{N}$ the polynomials P_k and P_k+1 are both prime, where*

$$P_k = x^{3^k} + \alpha, \qquad k \in \mathbb{N}.$$

Proof. For part a) see ([11, Lemma 2]). For part b) see ([7, Introduction]). ■

Remark 2.9. For Propositions *3.1*, *4.1* and *4.3*, we shall prove only necessity, since sufficiency is always obtained by direct computations.

3. Case $\omega(A) \leqslant 3$

3.1. Odd case

We prove the following result:

Proposition 3.1. *Let $A \in \mathbb{F}_4[x]$ be an odd polynomial such that $\omega(A) \leqslant 3$. Then*

a) *A is unitary perfect over $\mathbb{F}_4$ if and only if: $\omega(A) = 2$ and*

$$A = (P^2+P)^{2^n},$$

for some $n \in \mathbb{N}$, where P and $P+1$ are both odd and irreducible

b) *For any fixed nonnegative integer $n \in \mathbb{N}$ there are infinitely many unitary perfect polynomials in $\mathbb{F}_4[x]$ with two distinct prime factors.*

Assume that part a) holds. By Lemma 2.8 there are infinitely many odd irreducible polynomials $P \in \mathbb{F}_4[x]$, such that $P+1$ is also irreducible. This proves part b). Part a) is proved below. Observe that $\omega(A) \geqslant 2$ by Lemma 2.1.

Case $\omega(A) = 2$

In that case, $A = P^h Q^k$ where by Lemma 2.1, $h \deg(P) = k \deg(Q)$ and $\deg(P)$, $\deg(Q) \geqslant 2$. We obtain

$$1 + P^h = Q^k, \qquad 1 + Q^k = P^h.$$

So, Q divides $1+P$ and P divides $1+Q$. Thus $Q = 1+P$ and $h = k = 2^n$, for some $n \in \mathbb{N}$. Hence:

$$A = (P(P+1))^{2^n}, \qquad \text{where } P \text{ and } P+1 \text{ are both irreducible.}$$

By contrast (see [5]) all perfect polynomials A over $\mathbb{F}_2$ with $\omega(A) = 2$ are the $(x^2+x)^{2^n-1}$ where n goes from 1 to infinity.

Case $\omega(A) = 3$

Put: $A = P^hQ^kR^l$, $p = \deg(P)$, $q = \deg(Q)$, $r = \deg(R)$. According to Lemma 2.1, we may assume the following:

$$hp = kq \leqslant lr \qquad \text{and} \qquad p, q, r \geqslant 2.$$

Lemma 3.2. *If U, V, W are irreducible odd polynomials over $\mathbb{F}_4$ such that*

$$1 + U^h = V^aW^b,$$

then: $h = 2^n$ for some $n \in \mathbb{N}$, and h divides $\gcd(a, b)$*.*

Proof. Put: $h = 2^nu$, where u is odd and $n \in \mathbb{N}$. If $u \geqslant 3$ then since $1 + U^h = ((1 + U)(1 + U + \cdots + U^{u-1}))^{2^n}$ and since $\gcd(1 + U, 1 + U + \cdots + U^{u-1}) = 1$, we may write

$$1 + U = S^s, \qquad 1 + U + \cdots + U^{u-1} = T^t, \qquad \text{where } \{S, T\} = \{V, W\}.$$

This contradicts Lemma 2.5. We are done. ■

Corollary 3.3. *There exists no unitary odd perfect polynomial A over $\mathbb{F}_4$, with $\omega(A) = 3$.*

Proof. Assume that the contrary holds. We obtain

$$1 + P^h = Q^{b_1}R^{c_1}, \qquad 1 + Q^k = P^{a_2}R^{c_2}, \qquad 1 + S^l = P^{a_3}Q^{b_3}.$$

By Lemma 3.2, we have $h = 2^n$, $k = 2^m$, $l = 2^r$ for some n, m, $r \in \mathbb{N}$, so that h, k, l respectively divide b_1 and c_1, a_2 and c_2, a_3 and b_3. Hence:

$$1 + P = Q^{\frac{b_1}{h}}R^{\frac{c_1}{h}}, \qquad 1 + Q = P^{\frac{a_2}{k}}R^{\frac{c_2}{k}}, \qquad 1 + R = P^{\frac{a_3}{l}}Q^{\frac{b_3}{l}}.$$

If $0 \in \{b_1, c_1, a_2, c_2, a_3, b_3\}$, for example if $c_1 = 0$, then $b_1 = h$ and thus $1 + P = Q$. So $1 + Q = P$ and $h = k = 2^n$. Hence P^hQ^k is unitary perfect. Thus by Lemma 2.2, $R^l = \dfrac{A}{P^hQ^k}$ is also unitary perfect. This is impossible since $l \geqslant 1$. If $0 \notin \{b_1, c_1, a_2, c_2, a_3, b_3\}$, then $Q \mid 1 + P$ and $P \mid 1 + Q$. So $1 + P = Q$ and $c_1 = 0$ which is also impossible. ■

3.2. Even non splitting case

One has

Proposition 3.4. *There exists no even non splitting unitary perfect polynomial A over $\mathbb{F}_4$ such that $\omega(A) \leqslant 3$.*

Case $\omega(A) = 2$

By Lemma 2.3 we know that A may be written as: $A = x^hP^k$, where $p = \deg(P) \geqslant 2$. Since $1 + x$ divides $1 + x^h$, P must be equal to $1 + x$, which is impossible.

Case $\omega(A) = 3$

The proof is similar to that of the case where A is odd, in Section 3.1.

4. Case $\omega(A) = 4$

4.1. Even non splitting case

We prove the following result that characterizes even non splitting unitary perfect polynomials with four distinct prime factors.

Proposition 4.1. *Let $A \in \mathbb{F}_4[x]$ be an even non splitting polynomial over $\mathbb{F}_4$ such that $\omega(A) = 4$. Then A is unitary perfect if and only if there exist $a \in \mathbb{F}_4$, $r \in \mathbb{N}$ such that $A(x+a)$ is of the form B^{2^r} where:*

i) $B = (x^2+x)^{2^n}(P^2+P)^{2^m}$ *with both P and $P+1$ odd irreducible,*
ii) $B = x^4(x+1)^7(x^3+x^2+1)(x^3+x+1)$,
iii) $B = (x^2+x)^7(x^3+x^2+1)^2(x^3+x+1)^2$.

For any fixed non negative integers $m, n \in \mathbb{N}$, there are infinitely many polynomials of the form $(x^2+x)^{2^n}(P^2+P)^{2^m}$.

The last statement follows from Lemma 2.8. Now we prove parts i), ii) and iii):

Lemma 4.2. *If A is an even non splitting unitary perfect polynomial over $\mathbb{F}_4$ such that $\omega(A) = 4$, then after a suitable translation, we may write $A = x^{h_1}(x+1)^{k_1}P^{l_1}Q^{m_1}$, with both P, Q odd and irreducible.*

Proof. Since A is even, we may suppose that x divides A. So $x+1$ which divides $1+x^{h_1}$ must divide $\sigma^*(A) = A$. Moreover, if P is also even, then $P = x+\alpha$, so $Q = x+\alpha+1$ and hence A splits. This is impossible. ■

Put now $p = \deg(P)$, $q = \deg(Q)$, $h_1 = 2^h c$, $k_1 = 2^k d$, $l_1 = 2^l r$, $m_1 = 2^m s$ with c, d, r, s odd. Since A is unitary perfect, we have four equalities:

$$\begin{aligned}
1+x^{h_1} &= (x+1)^{2^h}(1+x+\cdots+x^{c-1})^{2^h},\\
1+(x+1)^{k_1} &= x^{2^k}(1+(x+1)+\cdots+(x+1)^{d-1})^{2^k},\\
1+P^{2^l r} &= (1+P)^{2^l}(1+P+\cdots+P^{r-1})^{2^l} = (x^{a_3}(x+1)^{b_3}Q^{d_3})^{2^l},\\
1+Q^{2^m s} &= (1+Q)^{2^m}(1+Q+\cdots+Q^{r-1})^{2^m} = (x^{a_4}(x+1)^{b_4}P^{c_4})^{2^m}.
\end{aligned} \tag{4}$$

By Lemma 2.4, we have

$$\{1+x+\cdots+x^{c-1},\ 1+(x+1)+\cdots+(x+1)^{d-1}\} = \{1, PQ\}.$$

Since h_1 and k_1 play symmetric roles and since P must appear in the right hand side of (4), it suffices to consider the following three cases:

(I) $c = d = 1$,
(II) $c = 1$, $1+(x+1)+\cdots+(x+1)^{d-1} = PQ$,
(III) $1+x+\cdots+x^{c-1} = PQ = 1+(x+1)+\cdots+(x+1)^{d-1}$.

Case (I)

Since $\gcd(1+P, 1+\cdots+P^{r-1}) = 1$ and since P, Q are odd, from Lemma 2.4, we obtain

$$1+P \not\in \{x^a, (x+1)^a : a \geqslant 1\} \cup \{Q^a : a \geqslant 2\},$$
$$1+P+\cdots+P^{r-1} \not\in \{x^a, (x+1)^a, Q^a : a \geqslant 1\}.$$

We necessarily have $1+P = Q$ so that $d_3 = 0$. Similarly, we obtain $c_4 = 0$. So by considering exponents and degrees, we deduce from equations (4) that:

$$2^l r = 2^m, \qquad 2^m s = 2^l.$$

Thus,

$$r = s = 1, \qquad l = m, \qquad h = k.$$

We obtain then part i) of Proposition 4.1.

Case (II)

By Lemma 2.4 ii), we have $p = q$ and $P(0) = Q(0) = 1$. So Q does not divide $1+P$. Hence, P and Q are of the form $x^a(x+1)^b + 1$. By part iv) of the same lemma, we get

$$d = 7, \qquad P = x^3 + x^2 + 1, \qquad Q = x^3 + x + 1.$$

It follows from equations (4) that:

$$2^l r = 2^m s = 2^k.$$

So

$$r = s = 1, \qquad l = m = k, \qquad h = k + 2.$$

This proves part ii) of Proposition 4.1.

Case (III)

By Lemma 2.4 iv), we have $c = d = 7$ and $P = x^3 + x^2 + 1$, $Q = x^3 + x + 1$. Thus $r = s = 1$. We get from equations (4):

$$l = m = h + 1, \qquad k = h.$$

We obtain now part iii) of Proposition 4.1.

4.2. Odd case

In this section, we prove the following result that characterizes odd unitary perfect polynomials with exactly four distinct prime divisors. We recall that:

$\Omega_1 = \{P \in \mathbb{F}_4[x] :\ P \text{ and } P+1 \text{ are odd and irreducible}\}$,

$\Omega_2 = \{P \in \mathbb{F}_4[x] :\ P,\ P+1, P^3+P^2+1,\ P^3+P+1 \text{ are odd and irreducible}\}$.

Proposition 4.3. *Let $A \in \mathbb{F}_4[x]$ be an odd polynomial over $\mathbb{F}_4$ such that $\omega(A) = 4$, then A is unitary perfect if and only if there exist $a \in \mathbb{F}_4$, $r \in \mathbb{N}$ such that $A(x+a)$ is of the form B^{2^r} where:*

i) $B = (P^2 + P)^{2^n}(R^2 + R)^{2^m}$ *with $n, m \in \mathbb{N}$ and $P, R \in \Omega_1$,*

ii) $B = P^4(P+1)^7(P^3 + P^2 + 1)(P^3 + P + 1)$ *for some $P \in \Omega_2$,*

iii) $B = (P^2 + P)^7(P^3 + P^2 + 1)^2(P^3 + P + 1)^2$ *for some $P \in \Omega_2$.*

For any fixed non-negative integers $n, m, r \in \mathbb{N}$, there are infinitely many unitary perfect polynomials in $\mathbb{F}_4[x]$ of the above forms with four distinct prime factors.

The latter statement follows from Lemma 2.8. Let us prove i), ii) and iii). For an odd unitary perfect polynomial A with $\omega(A) = 4$, say $A = P^{h_1}Q^{k_1}R^{l_1}S^{m_1}$, we suppose that:

$$p = \deg(P) \leqslant q = \deg(Q) \leqslant r = \deg(R) \leqslant s = \deg(S), \qquad p, q, r, s \geqslant 2.$$

Put $h_1 = 2^h u$, $k_1 = 2^k v$, $l_1 = 2^l w$, $m_1 = 2^m t$, where u, v, w, t are all odd. We may write the general system to resolve as:

$$\begin{cases} (E1): & 1 + P^{h_1} = (1+P)^{2^h}(1 + P + \cdots + P^{u-1})^{2^h} = (Q^{b_1}R^{c_1}S^{d_1})^{2^h}, \\ (E2): & 1 + Q^{k_1} = (1+Q)^{2^k}(1 + Q + \cdots + Q^{v-1})^{2^k} = (P^{a_2}R^{c_2}S^{d_2})^{2^k}, \\ (E3): & 1 + R^{l_1} = (1+R)^{2^l}(1 + R + \cdots + R^{w-1})^{2^l} = (P^{a_3}Q^{b_3}S^{d_3})^{2^l}, \\ (E4): & 1 + S^{m_1} = (1+S)^{2^m}(1 + S + \cdots + S^{t-1})^{2^m} = (P^{a_4}Q^{b_4}R^{c_4})^{2^m}. \end{cases} \tag{5}$$

where the exponents on the right hand sides are non-negative numbers so that some of them may be zero. Some consequences are the following:

Lemma 4.4. *If A is unitary perfect, then:*

i) $Q = 1 + P$,

ii) *If $u \geqslant 3$, then $u \geqslant 5$ and R and S have the same degree,*

iii) *$w = 1$ if S does not divide $1 + R$,*

iv) *$w = t = 1$ if S divides $1 + R$.*

Proof. We have

$$1 + P^{h_1} = (1+P)^{2^h}(1 + P + \cdots + P^{u-1})^{2^h}.$$

So Q must divide $1 + P$ and hence $Q = 1 + P$ by considering degrees.

ii) If $u \geqslant 3$, then the only possibility is

$$1 + P + \cdots + P^{u-1} = RS.$$

It follows by Lemma 2.6 ii) that R and S have the same degree. If $u = 3$ then $\{R, S\} = \{P + \alpha, P + \alpha + 1\}$. So the polynomials $P, P+1, P+\alpha, P+\alpha+1$ are irreducible and odd. This is impossible.

iii) If S does not divide $1+R$, then $(E3)$ implies

$$1+R = P^{a_3}Q^{b_3},\ 1+R+\cdots+R^{w-1} = S^{d_3}.$$

Thus, by Lemma 2.5, one has

$$w-1 = d_3 = 0.$$

iv) In this case, $S = 1+R$. So w and t play symmetric roles. If $w \geqslant 3$, then $(E3)$ implies

$$1+R+\cdots+R^{w-1} = P^{a_3}Q^{b_3}$$

and by Lemmas 2.6 ii) and 2.5, we get

$$a_3 = b_3 = 1.$$

By considering degrees, we obtain $(w-1)r = 2p \leqslant 2r$, and $w = 3$.

It follows that:

$$\{P, Q\} = \{R+\alpha, R+\alpha+1\}.$$

Thus P, $P+1$, $P+\alpha$, $P+\alpha+1$ are all odd and irreducible. This is impossible. ■

Since P and Q (and hence u and v) play symmetric roles, it suffices to distinguish three main cases, namely:

(I) $u = v = 1$;
(II) $u = 1,\ v \geqslant 3$;
(III) $u, v \geqslant 3$.

Case (I)

If S divides $1+R$, then $S = 1+R$ and $w = t = 1$, by Lemma 4.4. We obtain $m = l$ from $(E3)$ and $(E4)$. It follows that $R^{l_1}S^{m_1}$ is unitary perfect and consequently that $P^{h_1}R^{k_1}$ is also unitary perfect. By Proposition 3.1, we obtain part i) of Proposition 4.3.
If S does not divide $1+R$, then $w = 1$ by Lemma 4.4. Hence, by considering the degree of S in (5), we get a contradiction:

$$0 < 2^m t = d_1 \cdot 2^h + d_2 \cdot 2^k + d_3 \cdot 2^l = 0+0+0.$$

Case (II)

If S divides $1+R$, then $S = 1+R$ and $w = t = 1$, by Lemma 4.4. Thus, equations (5) lead to a contradiction:

$$2^l = 2^k + 2^m, \qquad 2^m = 2^k + 2^l.$$

If S does not divide $1+R$, then $w = 1$ by Lemma 4.4. Hence, by considering the degree of S in (5), we get now:

$$0 < 2^m t = d_1 + d_2 + d_3 = 0 + d_2 \cdot 2^k + 0 = 2^k.$$

So

$$t = 1, \qquad m = k = l < h.$$

It follows from equations $(E2)$, $(E3)$ and $(E4)$ that:

$$1 + Q + \cdots + Q^{v-1} = RS = (P^{a_3}Q^{b_3} + 1)(P^{a_4}Q^{b_4} + 1).$$

Lemma 2.7 implies that: $v = 7$ and $\{R, S\} = \{P^3 + P + 1, P^3 + P^2 + 1\}$.

We may suppose that: $R = P^3 + P + 1$, $Q = P^3 + P^2 + 1$. Hence $h = k + 2$ by (5). In other words, we obtain part ii) of Proposition 4.3.

Case (III)

In this case we have

$$1 + P + \cdots + P^{u-1} = RS = 1 + (1 + P) + \cdots + (1 + P)^{v-1}.$$

So by Lemma 2.6 we obtain, $u = v = 2^n - 1$, $r = s$.

If S divides $1 + R$, then $S = 1 + R$ and $w = t = 1$, by Lemma 4.4. Hence:

$$a_3 = b_3 = a_4 = b_4 = 0.$$

Equations (5) give then a contradiction:

$$2^l = 2^h + 2^k + 2^m, \qquad 2^m = 2^h + 2^k + 2^l.$$

If S does not divide $1 + R$, then $w = 1$ by Lemma 4.4. Hence, by considering the degree of S in (5), we get

$$0 < 2^m t = d_1 + d_2 + d_3 = 0 + d_2 \cdot 2^k + 0 = 2^k.$$

So

$$t = 1, \qquad m = k = l < h.$$

We get from $(E2)$, $(E3)$ and $(E4)$:

$$1 + P + \cdots + P^{u-1} = 1 + Q + \cdots + Q^{v-1} = RS = (P^{a_3}Q^{b_3} + 1)(P^{a_4}Q^{b_4} + 1).$$

It follows from Lemma 2.7 that: $u = v = 7$ and $\{R, S\} = \{P^3 + P + 1, P^3 + P^2 + 1\}$. We may suppose that: $R = P^3 + P + 1$, $Q = P^3 + P^2 + 1$. Thus, by (5):

$$h = k, \qquad l = m = k + 1.$$

So we obtain part iii) of Proposition 4.3. This completes the proof of Theorem 1.1.

References

[1] J. T. B. Beard Jr, *Unitary perfect polynomials over $GF(q)$*, Rend. Accad. Lincei **62** (1977), 417–422.

[2] J. T. B. Beard Jr, A. T. Bullock and M. S. Harbin, *Infinitely many perfect and unitary perfect polynomials*, Rend. Accad. Lincei **63** (1977), 294–303.

[3] J. T. B. Beard Jr, J. R. Oconnell Jr and K. I. West, *Perfect polynomials over $GF(q)$*, Rend. Accad. Lincei **62** (1977), 283–291.

[4] J. T. B. Beard Jr , *Perfect polynomials Revisited* , Publ. Math. Debrecen **38/1–2** (1991), 5–12.

[5] E. F. Canaday, *The sum of the divisors of a polynomial*, Duke Math. J. **8** (1941), 721–737.

[6] L. Gallardo and O. Rahavandrainy, *On perfect polynomials over $\mathbb{F}_4$*, Port. Math. (N.S.) **62(1)** (2005), 109–122.

[7] L. Gallardo and O. Rahavandrainy, *Perfect polynomials over $\mathbb{F}_4$ with less than five prime factors*, Port. Math. (N.S.) **64(1)** (2007), 21–38.

[8] L. H. Gallardo and O. Rahavandrainy, *Odd perfect polynomials over $\mathbb{F}_2$*, J. Théor. Nombres Bordeaux **19** (2007), 165–174.

[9] L. H. Gallardo and O. Rahavandrainy, *Even perfect polynomials over $\mathbb{F}_2$ with four prime factors*, Intern. J. of Pure and Applied Math. **52(2)** (2009), 301–314.

[10] L. H. Gallardo and O. Rahavandrainy, *There is no odd perfect polynomial over $\mathbb{F}_2$ with four prime factors* , Port. Math. (N.S.) **66(2)** (2009), 131–145.

[11] L. H. Gallardo and O. Rahavandrainy, *All perfect polynomials with up to four prime factors over $\mathbb{F}_4$* , Math. Commun. **14(1)** (2009), 47–65.

[12] L. H. Gallardo and O. Rahavandrainy, *On unitary splitting perfect polynomials over $\mathbb{F}_{p^2}$*, Math. Commun. **15(1)** (2010), 159–176.

[13] L. H. Gallardo and O. Rahavandrainy, *All unitary perfect polynomials over $\mathbb{F}_2$ with less than five distinct prime factors*, Preprint (2009).

[14] R. K. Guy, *Unsolved problems in number theory, Problem books in Mathematics*, Springer–Verlag, New York livre, 2004.

Addresses: Luis H. Gallardo, Olivier Rahavandrainy: Department of Mathematics, University of Brest, 6 Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France.

E-mail: luisgall@univ-brest.fr, rahavand@univ-brest.fr

Received: 30 April 2010; **revised:** 17 January 2011