PORTUGALIAE MATHEMATICA
Vol. 62 Fasc. 1 – 2005
Nova Série

ON PERFECT POLYNOMIALS OVER $\mathbb{F}_4$

Luis Gallardo and Olivier Rahavandrainy

Recommended by Arnaldo Garcia

Abstract: We characterize some perfect polynomials in $\mathbb{F}_4[x]$.

1 – Introduction

Let F be a field of characteristic 2. For a monic polynomial $A \in F[x]$, let $\sigma(A)$ be the sum of all monic divisors of A:

$$\sigma(A) = \sum_{P|A,\ P\ monic} P\ .$$

If $\sigma(A) = A$, then we call A a *perfect* polynomial (we also say that A is a perfect polynomial over F).

E.F. Canaday, the first doctoral student of L. Carlitz, began in 1941 the study of perfect polynomials by considering the case where F is the prime field $F = \mathbb{F}_2 = \{0, 1\}$ (see [1]).

Later in the seventies, T.B. Beard Jr. and collaborators continued the work of Canaday, extending it in several directions. (see e.g. [2], [3], [4]).
We are interested in their first paper, the more closely related to Canaday's work (see [2]).

Their main results were obtained by considering polynomials over the prime field $\mathbb{F}_p$, (see [1, 2]).
One of the results of Beard et al. over a non trivial extension $\mathbb{F}_q$ of the prime

Received: October 29, 2003; *Revised*: January 16, 2004.
AMS Subject Classification: 11T55, 11T06.
Keywords: Sum of divisors; polynomials; finite fields; characteristic 2.

field $\mathbb{F}_p$ is Theorem 3 in [2] in which they prove that the perfect polynomials in $\mathbb{F}_q[x]$ of the form $(x^q - x)^{Np^r-1}$ where r, N are non-negative integers, are exactly obtained when N is a divisor of $q-1$ while $r \geq 0$.

In this paper, we denote, as usual, by $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ the finite field with 4 elements $\{0, 1, \alpha, \alpha+1\}$, where $\alpha^2 = \alpha + 1$.
We want to generalize to the simplest extension of the prime field $\mathbb{F}_2$, namely the finite field with 4 elements, some of Canaday's and Beard's results. In other words, the aim of the present paper is to begin the study of the perfect polynomials over $\mathbb{F}_4$ but concentrating our attention to essentially 3 types of polynomials:

a) Polynomials that splits into linear factors.

b) Polynomials of the form $x^h(x+1)^kP^l$ with $h, k, l \geq 1$, and $P \in \mathbb{F}_4[x]$ irreducible of degree $\deg(P) > 1$.

c) Polynomials that are product of two powers of irreducible factors.

<u>Our main results are:</u>

1) Characterization of the perfect polynomials over $\mathbb{F}_4$ that split into linear factors.
(see Theorem 3.4).

2) Non existence of perfect polynomials of the form $x^h(x+1)^kP^l$ with $h, k, l \geq 1$, and $P \in \mathbb{F}_4[x]$ irreducible of degree $\deg(P) > 1$.
(see Theorem 3.9)

3) Characterization of the perfect polynomials over $\mathbb{F}_4$ that are product of two powers of irreducible factors.
(see Proposition 3.10).

Some proofs (mainly in the Preliminary section) work for more general fields of characteristic 2. We occasionally insist on this and generally restrict ourselves to $\mathbb{F}_4$ for simplicity.
We denote by the usual symbol $()'$ the derivation relative to x in $\mathbb{F}_4[x]$ and by τ the galois automorphism of $\mathbb{F}_4[x]$ over $\mathbb{F}_2[x]$ that fixes $x, 0, 1$ and moves α into $\alpha + 1$ in $\mathbb{F}_4$.

2 – Preliminary

We denote, as usual, by $\mathbb{N}$ (resp. $\mathbb{N}^*$) the set of nonnegative (resp. positive) integers. In this section, we present some results that we shall use repeatedly in the next sections.

Our first lemma below was (essentially) obtained by Canaday over $\mathbb{F}_2$ but the proof works over any perfect field of characteristic 2. (i.e. any characteristic 2 field in which every element is a square):

Lemma 2.1 (see Lemma 5 in [1]). *Let $P, Q \in \mathbb{F}[x]$ where $\mathbb{F}$ is a perfect field of characteristic 2, and let $n, m \in \mathbb{N}$; such that P, Q are non constant, i.e. $P, Q \notin \mathbb{F}$ and*

$$1 + \cdots + P^{2n} = Q^m \ . \tag{1}$$

Then $m \in \{0, 1\}$.

Proof: We suppose that $m > 1$ so that $n \geq 1$.
Observe that (1) can be written:

$$(1 + \cdots + P^n)^2 + P(1 + \cdots + P^{n-1})^2 = Q^m \ . \tag{2}$$

If m is even, then (2) implies that P is a square, so that by taking enough square roots in both sides of (2) we may assume that m is odd, so that P is not a square, i.e. $P' \neq 0$.
By hypothesis,

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

so that Q is prime to $P^{n-1} + \cdots + P + 1$.

Differentiating (1) gives us: $(P^{n-1} + \cdots + P + 1)^2 P' = Q' Q^{m-1}$.
Therefore, Q^{m-1} divides P'.

If $\deg(P) = 1$, then Q^{m-1} divides 1, which is impossible.
Hence, $\deg(P) > 1$.
Thus, $m \deg(Q) = 2n \deg(P) > 2n \deg(P') \geq 2n(m-1) \deg(Q)$. I.e.

$$2n < \frac{m}{m-1} \leq 2 \ ,$$

that is impossible since $n \geq 1$. ∎

A simple, but useful, observation is:

Lemma 2.2. *For $P(x) \in \mathbb{F}_4[x]$, $P(x)$ is perfect if and only if for all $a \in \mathbb{F}_4$, $P(x+a)$ is perfect.* ∎

Necessary and sufficient conditions to have some special factorizations:

Lemma 2.3. *Let $h \in \mathbb{N}$ be a non-negative integer. We have:*

i) h even implies that $Q(x) = x^{h+1} + 1$ is square free in $\mathbb{F}_4[x]$.

ii) Let $P \in \mathbb{F}_4[x] \setminus \mathbb{F}_4$ be a nonconstant polynomial. Then:
$1 + P + \cdots + P^h = (1+P)^h$ if and only if $h = 2^n - 1$ for some $n \in \mathbb{N}$.
Observe that the equality can be written also in the form
$(1+P)^{h+1} = 1 + P^{h+1}$.

iii) $1 + x + \cdots + x^h = 1 + (x+1) + \cdots + (1+x)^h$ if and only if $h = 2^n - 2$ for some $n \in \mathbb{N}$.

iv) $1 + x + \cdots + x^{2h} = (1 + x + x^2)^h$ if and only if $h \in \{0, 1\}$.

v) $1 + x + \cdots + x^h = (1 + x + x^2)(x+1)^{h-2}$ if and only if $h = 2$.

vi) $1 + x + \cdots + (x+\alpha)^h = x(x+1)(x+\alpha+1)^{h-2}$ if and only if $h = 2$.

Proof:

i) Assume h even. Differentiating $Q(x)$ we get $Q'(x) = x^h$. This proves the result.

We prove only the necessity for each statement:

ii) If h is even, then we have: $1 + P^{h+1} = (1+P)^{h+1} = 1 + P + P^2 A$,
for some $A \in \mathbb{F}_4[t]$ i.e. $P^h = 1 + PA$ which is impossible.
If h is odd, then put $h + 1 = 2^n u$, where u is odd. We obtain:
$1 + P^{2^n u} = (1+P)^{2^n u} = (1 + P^{2^n})^u = 1 + P^{2^n} + P^{2^n+1} A$.
If $u \geq 3$, then $P^{2^n u - 1} = 1 + PA$ which is impossible.
We conclude that $u = 1$ and $h + 1 = 2^n$.

iii) follows from ii) by multiplying both sides by $x(x+1)$ to get
$x^{h+2} + 1 = (1+x)^{h+2}$.

iv), and v) with h even, follow from i) by multiplying both sides by $x+1$. When h is odd in v) we have

$$x^{h+1} + 1 = (1 + x + x^2)(x+1)^{h-1}$$

that implies the contradiction: $x^2 + x + 1$ is a square.
Finally, vi) follows from v) replacing x by $x + \alpha$, thereby finishing the proof of the lemma. ∎

The next lemma is a special case of Theorem 2.47 in [5].

Lemma 2.4 (see Theorem 2.47 in [5])**.** *Let p be an odd prime number and let $n \in \mathbb{N}^*$. If d is the smallest positive integer such that $(2^n)^d = 1$ $(mod\ p)$, and if μ is the number of irreducible distinct factors of degree d, in $\mathbb{F}_{2^n}[x]$, of $1 + \cdots + x^{p-1}$, then $\mu = \dfrac{p-1}{d}$.* ∎

An easy corollary is:

Lemma 2.5. *For all integer $m \geq 2$, the polynomial $x^m + \cdots + x + 1$ is reducible over $\mathbb{F}_4$.*

Proof:

<u>Case $m+1$ is not a prime number:</u>

Write: $m + 1 = ab$, with $a, b \geq 2$. We have:

$x^m + \cdots + x + 1 = \dfrac{1+x^{ab}}{1+x} = \dfrac{1+(x^a)^b}{1+x} = \dfrac{1+x^a}{1+x} \cdot (1 + x^a + \cdots + (x^a)^{b-1})$,

which is reducible.

<u>Case $m+1 = p$ is a prime number:</u>

If $x^m+\cdots+x+1$ is irreducible, then, by Lemma 2.4 (with $n=2$), $\mu = \dfrac{p-1}{d} = 1$. So, $2^2 = 4$ is of order $d = p-1$ in $\mathbb{F}_p^*$. It is impossible. ∎

Lemma 2.6. *For all $a, b \in \mathbb{F}_4$ such that $a + b \in \{\alpha, \alpha + 1\}$, the monomial $x + a$ divides $P(x) = 1 + \cdots + (x + b)^n$ if and only if $n \equiv 2$ $(mod\ 3)$.*

Proof: This statement is true if and only if $P(a) = 1 + \cdots + (a + b)^n = 0$, i.e. $1 + (a + b)^{n+1} = 0$. So we are done. ∎

The next lemma describes possible factorizations of $\frac{x^{h+1}+1}{x+1}$ with only linear factors in $\mathbb{F}_4[x]$:

Lemma 2.7. *If $P(x) = 1 + x + \cdots + x^h = (x + 1)^a(x + \alpha)^b(x + \alpha + 1)^c$, then $b = c$. Furthermore:*

i) $a = 0$ if and only if h is even. In this case, $h = 2b = 2c = 2$.

ii) $b = c = 0$ if and only if $h \not\equiv 2$ $(mod\ 3)$. In this case, $h = 2^n - 1$ for some $n \in \mathbb{N}$.

iii) ($h \equiv 2$ $(mod\ 3)$ and h is odd) if and only if $h = 3.2^n - 1$, for some $n \in \mathbb{N}^*$. In this case, $a = 2^n - 1,\ b = c = 2^n$.

Proof: We consider the Galois automorphism τ such that $\tau(\alpha) = \alpha + 1$. Since $\tau(P(x)) = P(x)$, we obtain $b = c$.

i): It is clear that $a = 0$ if and only if h is even. In this case, we obtain $h = 2b = 2c$. We conclude by Lemma 2.3 part iii).

ii): $b = c = 0$ if and only if $P(\alpha)$ and $P(\alpha+1)$ do not equal 0. So we are done. Thus, in this case, we obtain $a = h$ and we conclude by Lemma 2.3 part i).

iii): We can put $h = 3s - 1$, with $s = 2^n u$, u odd.
So, we obtain:
$Q(x) = (1+x)(1+\cdots+x^h) = \big(1+(x^u)^3\big)^{2^n} = (x^u+1)^{2^n}(x^u+\alpha)^{2^n}(x^u+\alpha+1)^{2^n}$.
We can write:

$$\begin{aligned}(x^u+1)^{2^n} &= (x+1)^{a_1}(x+\alpha)^{b_1}(x+\alpha+1)^{b_1} \ ,\\ (x^u+\alpha)^{2^n} &= (x+1)^{a_2}(x+\alpha)^{b_2}(x+\alpha+1)^{c_2} \ ,\\ (x^u+\alpha+1)^{2^n} &= (x+1)^{a_3}(x+\alpha)^{b_3}(x+\alpha+1)^{c_3} \ ,\end{aligned}$$

where $a_1 + a_2 + a_3 = a + 1,\ b_1 + b_2 + b_3 = b = b_1 + c_2 + c_3$.
The integers a_2 and a_3 equal 0 since $(1+\alpha)^{2^n} \neq 0$ and $\alpha^{2^n} \neq 0$.

• If u is prime to 3, then $\alpha^u + 1 \neq 0$, so $b_1 = 0$ and $a_1 = 2^n u$.
Therefore, $1 + x^{2^n u} = (1+x^u)^{2^n} = (1+x)^{2^n u}$.
We conclude that $2^n u = 2^m$, for some $m \in \mathbb{N}$, so $u = 1,\ \ h = 3.2^n - 1,\ a_1 = b_2 = c_3 = 2^n$ and $a_2 = a_3 = b_3 = c_2 = 0$.

• If 3 divides u, then $\alpha^u + \alpha = 1 + \alpha \neq 0$, so $b_2 = b_3 = c_2 = c_3 = 0 = a_2 = a_3$. It is impossible. ∎

3 – Main results

3.1. Perfects of the forms: $x^h(x+1)^k(x+\alpha)^l(x+\alpha+1)^t$

We characterize here below in Theorem 3.4 all perfect polynomials that have only linear irreducible factors in $\mathbb{F}_4$.

Canaday (see [1]) called "trivial" the perfect polynomials over $\mathbb{F}_2$ of the form

$$(x^2+x)^{2^n-1} \tag{3}$$

for some $n \in \mathbb{N}^*$. Beard et al. proved in Theorem 5 of [2] a result that holds for all prime numbers p and that specialized to $p = 2$ say that the only perfect polynomials over $\mathbb{F}_2$ of the form $x^k(x+1)^h$ for some non-negative integers $k, h \in \mathbb{N}$ are described in (3).

First of all we present a direct proof of the above result for $\mathbb{F}_4$:

Proposition 3.1. *The polynomials $x^h(x+1)^k$, $(x+\alpha)^h(x+\alpha+1)^k$ are perfect over $\mathbb{F}_4$ if and only if $h = k = 2^n - 1$, for some $n \in \mathbb{N}$.*

Proof:

– Sufficiency: by direct computations.

– Necessity: if $x^h(x+1)^k$ is perfect, then we have:

$$x^h = 1 + \cdots + (x+1)^k, \ (x+1)^k = 1 + \cdots + x^h .$$

So, $h = k = 2^n - 1$ for some $n \in \mathbb{N}$, by Lemma 2.3.
For $(x+\alpha)^h(x+\alpha+1)^k$: by Lemma 2.2. ∎

We can deduce the

Corollary 3.2. *If $h = k = 2^n - 1$, and $l = t = 2^m - 1$, for some $n, m \in \mathbb{N}$ then the polynomial $x^h(x+1)^k(x+\alpha)^l(x+\alpha+1)^t$ is perfect.* ∎

We require (for the sufficiency of our main result) the following result of Beard et al. (see the Introduction) obtained by the specialization $q = 4$ in ([2], Theorem 3).

Proposition 3.3 (see [2], Theorem 3)**.** *For all $n \in \mathbb{N}$, the polynomial $\Big(x(x+1)(x+\alpha)(x+\alpha+1)\Big)^{N2^n-1}$ is perfect over $\mathbb{F}_4$ if and only if $N = 1, 3$.* ∎

We present here below our first main result, i.e. the characterization of the perfect polynomials over $\mathbb{F}_4$ that split into linear factors:

Theorem 3.4. *The polynomial $x^h(x+1)^k(x+\alpha)^l(x+\alpha+1)^t$ is perfect over $\mathbb{F}_4$ if and only if one of the following conditions is satisfied:*

i) $h = k = 2^n - 1, \ l = t = 2^m - 1$ *for some* $n, m \in \mathbb{N}$.

ii) $h = k = l = t = N.2^n - 1$ *for some* $n \in \mathbb{N}$ *and for* $N \in \{1, 3\}$.

iii) $h = l = 3.2^r - 1, \ k = t = 2.2^r - 1,$ *for some* $r \in \mathbb{N}$.

Proof: We obtain the sufficiency by Corollary 3.2, by Proposition 3.3 and by direct computations.

Necessity:
We can write:

$$(4)\qquad \begin{cases} 1+\cdots+x^h = (x+1)^{a_1}(x+\alpha)^{b_1}(x+\alpha+1)^{c_1} \\ 1+\cdots+(x+1)^k = x^{d_1}(x+\alpha)^{b_2}(x+\alpha+1)^{c_2} \\ 1+\cdots+(x+\alpha)^l = x^{d_2}(x+1)^{a_2}(x+\alpha+1)^{c_3} \\ 1+\cdots+(x+\alpha+1)^t = x^{d_3}(x+1)^{a_3}(x+\alpha)^{b_3} \end{cases}$$

with $b_1 = c_1,\ b_2 = c_2,\ d_2 = a_2,\ d_3 = a_3,\ d_1 + d_2 + d_3 = h$ etc...

We observe, by Lemma 2.2, that:

– h and k (resp. l and t) play symmetric roles (substitute x by $x + 1$),

– the couples (h, k) and (l, t) play symmetric roles (substitute x by $x + \alpha$),

– l and t play symmetric roles since α and $\alpha + 1$ play symmetric roles.

Thus, it suffices to consider the following cases:

- $h, k \not\equiv 2\ (mod\ 3)$
- $h, l \equiv 2\ (mod\ 3)$ and $k, t \not\equiv 2\ (mod\ 3)$
- $h, k, l, t \equiv 2\ (mod\ 3)$.

Case $h, k \not\equiv 2\ (mod\ 3)$:
By Lemma 2.6, the monomials $x + \alpha$ and $x + \alpha + 1$ do not divide the two polynomials $1+\cdots+x^h$ and $1+\cdots+(x+1)^k$. Thus, we have: $(x+\alpha)^l(x+\alpha+1)^t = (1 + \cdots + (x + \alpha)^l)(1 + \cdots + (x + \alpha + 1)^t)$,
i.e. the polynomial $(x + \alpha)^l(x + \alpha + 1)^t$ is perfect. So, by Proposition 3.1, $l = t = 2^m - 1$, for some $m \in \mathbb{N}$.
Therefore, the polynomial $x^h(x + 1)^k$ is perfect too and $h = k = 2^n - 1$, for some $n \in \mathbb{N}$.

Case $h, l \equiv 2\ (mod\ 3)$ and $k, t \not\equiv 2\ (mod\ 3)$:
We have: $b_2 = c_2 = 0,\ d_3 = a_3 = 0$.
So, $1 + \cdots + (x + 1)^k = x^{d_1}$ and by Lemma 2.3, $d_1 = k = 2^n - 1$ for some $n \in \mathbb{N}$.
Analogously, $1 + \cdots + (x + \alpha + 1)^t = (x + \alpha)^{b_3}$ and substituting x by $x + \alpha$, we obtain $b_3 = t = 2^m - 1$ for some $m \in \mathbb{N}$.

- If h is even, then $h = 2$ by Lemma 2.7. Thus $k = 1$.

Using the fact that $x^2(x + 1)(x + \alpha)^l(x + \alpha + 1)^t$ is perfect, we obtain:
$x(x + 1)(x + \alpha)^{l-1-t}(x + \alpha + 1)^{t-1} = 1 + \cdots + (x + \alpha)^l$,
So, $l = t + 1$ and $l = 2$ by Lemma 2.3.

• If l is even, then $l = 2$ by Lemma 2.7. Substitute x by $x + \alpha$ lead us to the previous case (h even).

• If h and l are odd, then by Lemma 2.7, we can write:
$1 + \cdots + x^h = (x + 1)^{a_1}(x^2 + x + 1)^{b_1}$, with $h = 3.2^r - 1,\ a_1 = 2^r - 1,\ b_1 = 2^r$,
$1+\cdots+(x+\alpha)^l = (x+\alpha+1)^{c_3}(x^2+x)^{a_2}$, with $l = 3.2^s - 1,\ c_3 = 2^s - 1,\ a_2 = 2^s$.
Thus:

$$\begin{aligned}
1 + \cdots + x^h &= (x + 1)^{2^r-1}(x + \alpha)^{2^r}(x + \alpha + 1)^{2^r}\\
1 + \cdots + (x + 1)^k &= x^{2^n-1}\\
1 + \cdots + (x + \alpha)^l &= x^{2^s}(x + 1)^{2^s}(x + \alpha + 1)^{2^s-1}\\
1 + \cdots + (x + \alpha + 1)^t &= (x + \alpha)^{2^m-1}\ .
\end{aligned}$$

Since $x^h(x + 1)^k(x + \alpha)^l(x + \alpha + 1)^t$ is perfect, we obtain:

$$\begin{aligned}
h &= 3.2^r - 1 = 2^n - 1 + 2^s\\
k &= 2^n - 1 = 2^r - 1 + 2^s\\
l &= 3.2^s - 1 = 2^m - 1 + 2^r\\
t &= 2^m - 1 = 2^s - 1 + 2^r\ .
\end{aligned}$$

Therefore, $r = s$ and $n = m = r + 1 = s + 1$.
So $h = l = 3.2^r - 1$, and $k = t = 2.2^r - 1$.

<u>Case $h, k, l, t \equiv 2\ (mod\ 3)$</u>:

• <u>Case $h,\ k$ even</u>

In this case, we have $h = k = 2$ (see Lemma 2.7). Thus, the polynomial $x^2(x + 1)^2(x + \alpha)^l(x + \alpha + 1)^t$ is perfect if and only if

$$\begin{aligned}
1 + \cdots + (x + \alpha)^l &= x(x + 1)(x + \alpha + 1)^{t-2}\\
1 + \cdots + (x + \alpha + 1)^t &= x(x + 1)(x + \alpha)^{l-2}\ .
\end{aligned}$$

So, $l = t = 2$ by Lemma 2.3.

• <u>Case h even and k odd</u>

In this case, l and t are not both even (if they were, h and k should be even by the previous case). Suppose that l is even and t is odd. We obtain, by Lemma 2.7, $h = l = 2$ and $k = 3.2^n - 1,\ t = 3.2^m - 1$.
Thus, the polynomial $x^2(x + 1)^k(x + \alpha)^2(x + \alpha + 1)^t$ is perfect if and only if $\left(1 + \cdots + (x + 1)^k\right)\left(1 + \cdots + (x + \alpha + 1)^t\right) = x(x + 1)^{k-1}(x + \alpha)(x + \alpha + 1)^{t-1}$.
It is impossible since x divides $1 + \cdots + (x + 1)^k$ and $1 + \cdots + (x + \alpha + 1)^t$.

- Case $h,\ k$ odd

This implies that l and t are odd too. So, by Lemma 2.7, we have in equations (4):

$$\begin{aligned}
&h = 3.2^n - 1,\ a_1 = 2^n - 1,\ b_1 = c_1 = 2^n\ ,\\
&k = 3.2^m - 1,\ d_1 = 2^m - 1,\ b_2 = c_2 = 2^m\ ,\\
&l = 3.2^r - 1,\ c_3 = 2^r - 1,\ d_2 = a_2 = 2^r\ ,\\
&t = 3.2^s - 1,\ b_3 = 2^s - 1,\ d_3 = a_3 = 2^s\ ,
\end{aligned}$$

for some $n, m, r, s \in \mathbb{N}^*$.
Using the fact that the polynomial is perfect, and putting $x_1 = 2^n$, $x_2 = 2^m$, $x_3 = 2^r$, $x_4 = 2^s$, we obtain:

$$\begin{cases} 3x_1 - x_2 - x_3 - x_4 = 0 \\ x_1 - 3x_2 + x_3 + x_4 = 0 \\ x_1 + x_2 - 3x_3 + x_4 = 0 \\ x_1 + x_2 + x_3 - 3x_4 = 0 \end{cases}$$

which gives us: $x_1 = x_2 = x_3 = x_4$. Thereby finishing the proof of the theorem. ∎

3.2. Perfects of the form: $x^h(x+1)^k P^l$, P irreducible and $\deg(P) > 1$

Working over $\mathbb{F}_2$, Canaday (see Theorem 9 in [1]) proves that the only perfect polynomials over $\mathbb{F}_2$, of the form $x^h(x+1)^k P^l$ with P irreducible, $\deg(P) > 1$ and $h, k, l \geq 1$ are

$$A_1(x) = x^2(x+1)(x^2+x+1) \text{ and } A_2(x) = x^4(x+1)^3(x^4+x^3+x^2+x+1)$$
$$\text{together with } A_i(x+1) \text{ for } i = 1, 2\ .$$

We prove in this section that there are no perfect polynomials of this form over $\mathbb{F}_4$.

Case 1. The irreducible polynomial P satisfy $P(0) = P(1) = 1$.

Proposition 3.5. *There are no perfect polynomials over $\mathbb{F}_4$ of the form $x^h(x+1)^k P^l$, where $P \in \mathbb{F}_4[x]$ is irreducible of degree $d \geq 2$, $P(0) = P(1) = 1$ and $h, k, l \geq 1$.*

Proof: We use here the idea of the proof of Theorem 9 in [1].
We consider four cases.

Case $l = 2n$ even:
We denote $A = x^h(x+1)^k P^{2n}$. If A is perfect, then:

$$x^h(x+1)^k P^{2n} = (x^h + \cdots + 1)\big((x+1)^k + \cdots + 1\big)(P^{2n} + \cdots + 1) \ .$$

This implies $x^h(x+1)^k = (x^h + \cdots + 1)\big((x+1)^k + \cdots + 1\big)$ since x and $x+1$ do not divide $P^{2n} + \cdots + 1$.
Therefore, $P^{2n} = P^{2n} + \cdots + 1$ which is impossible.

Case $h,\ k$ even and l odd:
Put $h = 2m$, $k = 2r$, $l = 2n-1$. If A is perfect, then:

$$x^{2m}(x+1)^{2r} P^{2n-1} = (x^{2m} + \cdots + 1)\big((x+1)^{2r} + \cdots + 1\big)(1 + P + \cdots + P^{2n-1}) \quad (\star)$$

Thus, we must have $(x^{2m} + \cdots + 1)\big(((x+1)^{2r} + \cdots + 1\big) = P^{2n-1}$. This implies, by Lemma 2.1:

$$P = x^{2m} + \cdots + 1 = (x+1)^{2r} + \cdots + 1 \ .$$

It is impossible by Lemma 2.5.

Case $h,\ k$ and l odd:
Put $h = 2m-1$, $k = 2r-1$, $l = 2n-1$. If A is perfect, then:

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

Since the greatest power of P dividing the right member is even, this equation is impossible.

Case h even and $k,\ l$ odd:
Put $h = 2m$, $k = 2r-1$, $l = 2n-1$. If A is perfect, then:

$$x^{2m}(x+1)^{2r-1} P^{2n-1} = (x^{2m} + \cdots + 1)x\big((x+1)^{r-1} + \cdots + 1\big)^2 (P+1)(P^{n-1} + \cdots + 1)^2.$$

The two monomials x and $x+1$ do not divide $x^{2m} + \cdots + 1$. This requires $P = x^{2m} + \cdots + 1$, by Lemma 2.1. It is impossible by Lemma 2.5. ∎

Proposition 3.5 and Lemma 2.2 give us the

Corollary 3.6. *There are no perfect polynomial over $\mathbb{F}_4$ of the form $(x+\alpha)^h(x+\alpha+1)^k P^l$, where $P \in \mathbb{F}_4[x]$ is irreducible of degree $d \geq 2$, $P(\alpha) = P(\alpha+1) = 1$ and $h, k, l \geq 1$.* ∎

Case 2. The irreducible polynomial P satisfies: either $P(0)$ or $P(1) \in \{\alpha, \alpha+1\}$.

Proposition 3.7. *There are no perfect polynomial over* $\mathbb{F}_4$ *of the form* $x^h(x+1)^k P^l$, *where* $P \in \mathbb{F}_4[x]$ *is irreducible of degree* $d \geq 2$, *either* $P(0)$ *or* $P(1)$ *belongs to* $\{\alpha, \alpha+1\}$ *and* $h, k, l \geq 1$.

Proof: It suffices to consider the case $P(0) = \alpha$.
If $x^h(x+1)^k P^l$ is perfect, then we have:

$$x^h + \cdots + 1 = (x+1)^{b_1} P^{c_1}$$
$$(x+1)^k + \cdots + 1 = x^{a_1} P^{c_2}$$
$$P^l + \cdots + 1 = x^{a_2} (x+1)^{b_2}$$

with either $c_1 \geq 1$ or $c_2 \geq 1$, and $c_1 + c_2 = l$.
We observe that $\tau(P^{c_1}) = P^{c_1}$ and $\tau(P^{c_2}) = P^{c_2}$. So, $P^{c_1},\ P^{c_2} \in \mathbb{F}_2[x]$ and $P(0)^{c_1} = P(0)^{c_2} = 1$.
If $c_1 \geq 1$, then $\alpha^{c_1} = P(0)^{c_1} = 1$ and 3 divides c_1.
It is the same for c_2.
Furthermore, the integers h and k must be odd. If they were not, then $a_1 = b_1 = 0$, and by Lemma 2.1, $c_1 = c_2 = 1$. It is impossible by Lemma 2.5.
We consider two cases.

Case $l \equiv 2 \ (mod\ 3)$:
If $c_1,\ c_2 \geq 1$, then 3 divides c_1, c_2 and $c_1 + c_2 = l$. It is impossible.
If $c_1 = 0$ then 3 divides $c_2 = l$. It is impossible.
If $c_2 = 0$ then 3 divides $c_1 = l$. It is impossible.

Case $l \not\equiv 2 \ (mod\ 3)$:
In this case, since $P(0) = \alpha$, x does not divide $P^l + \cdots + 1$. So, $a_2 = 0$, $P(1) = 1$ and l is odd.

Put $h = 2m - 1$, $k = 2r - 1$ and $l = 2s - 1$.
If $x^h(x+1)^k P^l$ is perfect, then:

$$x^h(x+1)^k P^l = (x+1)\big(x^{m-1}+\cdots+1\big)^2 x\big((x+1)^{r-1}+\cdots+1\big)^2 (P+1)\big(P^{s-1}+\cdots+1\big).$$

Since the greatest power of P dividing the right member is even, this equation is impossible. ∎

Proposition 3.7 and Lemma 2.2 give us the

Corollary 3.8. *There are no perfect polynomials over $\mathbb{F}_4$ of the form $(x+\alpha)^h(x+\alpha+1)^kP^l$, where $P \in \mathbb{F}_4[x]$ is irreducible of degree $d \geq 2$, either $P(\alpha)$ or $P(\alpha+1)$ belongs to $\{\alpha, \alpha+1\}$ and $h, k, l \geq 1$.* ∎

Now, we summarize our main result of the section:

Theorem 3.9. *There are no perfect polynomials over $\mathbb{F}_4$ of the form $x^h(x+1)^kP^l$, where $P \in \mathbb{F}_4[x]$ is irreducible of degree $d \geq 2$ and the integers h, k, l satisfy $h, k, l \geq 1$.*

Proof: Follows from Propositions 3.5 and 3.7. ∎

3.3. Perfects of the form P^hQ^k, where P, Q are irreducible

Canaday proves (see Theorem 17 in [1]) that there no perfect polynomials over $\mathbb{F}_2$, that are squares, and that are divisible by 2 irreducible polynomials in $\mathbb{F}_2[x]$. We characterize here below the perfect polynomials over $\mathbb{F}_4$, not necessarily squares, satisfying the same condition over $\mathbb{F}_4$.

Proposition 3.10. *Let $P, Q \in \mathbb{F}_4[x]$ be two distinct irreducible polynomials. Then P^hQ^k is perfect over $\mathbb{F}_4$ if and only if $Q = P+1$ and $h = k = 2^n - 1$, for some $n \in \mathbb{N}$.*

Proof:

– The sufficiency is obtained by direct computations.

– Necessity:

If $\overline{P^hQ^k}$ is perfect, then we have: $Q^k = 1 + \cdots + P^h$ and $P^h = 1 + \cdots + Q^k$.
If h is even, then $k = 1$ by Lemma 2.1. Therefore $1 + P^{h+1} = (1+P)Q$ and $P^h = 1 + Q$.
So, $1 + P(1+Q) = 1 + P^{h+1} = (1+P)Q$. Hence $Q = P+1$ and $h = 1$. It is impossible.
Analogous proof if k is even.
If $h = 2m-1$ and $k = 2r-1$, then:

$$1 + \cdots + P^h = (1+P)(1+\cdots+P^{m-1})^2, \; 1 + \cdots + Q^k = (1+Q)(1+\cdots+Q^{r-1})^2$$

Thus, $P^hQ^k = (P+1)(Q+1)A^2$, where $A = (1+\cdots+P^{m-1})(1+\cdots+Q^{r-1})$.
We conclude that P divides $Q+1$ and Q divides $P+1$. So, $Q = P+1$ and $h = k$.

Thus $1+P^{h+1}=(1+P)(1+\cdots+P^h) = QQ^h = Q^{h+1} = (1+P)^{h+1}$. Lemma 2.3 give us: $h = 2^n - 1$, for some $n \in \mathbb{N}$. ∎

In the special case where the two irreducible polynomials are both of degree 2, a more precise result holds:

First of all observe that there are exactly 6 irreducible polynomials of degree 2 in $\mathbb{F}_4[x]$:

$$\begin{array}{ll} x^2+x+\alpha\,, & x^2+x+\alpha+1\ , \\ x^2+\alpha x+1\,, & x^2+(\alpha+1)x+1\ , \\ x^2+\alpha x+\alpha\,, & x^2+(\alpha+1)x+\alpha+1\ . \end{array}$$

Secondly, we have:

Corollary 3.11. *The only perfect polynomials over $\mathbb{F}_4$ of the form P^hQ^k, where $P, Q \in \mathbb{F}_4[x]$ are irreducible of degree 2, are: $(x^2+x+\alpha)^h(x^2+x+\alpha+1)^k$, with $h = k = 2^n - 1$, for some $n \in \mathbb{N}$.*

Proof: Follows from Proposition 3.10 and from the above list of irreducibles, since we have $Q = P + 1$. ∎

REFERENCES

[1] Canaday, E.F. – The sum of the divisors of a polynomial, *Duke Math. Journal,* 7 (1941), 721–737.

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

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

[4] Beard Jr., T.B.; Bullock, Alice T. and Mickie Sue Harbin, Karen I. – Infinitely many perfect and unitary perfect polynomials, *Rend. Accad. Lincei,* 63 (1977), 294–303.

[5] Lidl, Rudolf and Niederreiter, Harald – *Finite Fields*, in “Encyclopedia of Mathematics and its Applications”, Vol. 20, Cambridge University Press, 1983 (Reprinted 1987).

Luis Gallardo and Olivier Rahavandrainy,
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`