



HAL
open science

Non-splitting bi-unitary perfect polynomials over F_4 with less than five prime factors

Olivier Rahavandrainy

► **To cite this version:**

Olivier Rahavandrainy. Non-splitting bi-unitary perfect polynomials over F_4 with less than five prime factors. 2024. hal-04850368

HAL Id: hal-04850368

<https://hal.univ-brest.fr/hal-04850368v1>

Preprint submitted on 20 Dec 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Non-splitting bi-unitary perfect polynomials over \mathbb{F}_4 with less than five prime factors

Olivier Rahavandrainy
Univ Brest, UMR CNRS 6205
Laboratoire de Mathématiques de Bretagne Atlantique

December 19, 2024

Mathematics Subject Classification (2010): 11T55, 11T06.

Abstract We identify all non-splitting bi-unitary perfect polynomials over the field \mathbb{F}_4 , which admit at most four irreducible divisors. There is an infinite number of such divisors.

1 Introduction

In this paper, we work over the finite field \mathbb{F}_4 of 4 elements:

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\} \text{ where } \alpha^2 + \alpha + 1 = 0.$$

As usual, \mathbb{N} (resp. \mathbb{N}^*) denotes the set of nonnegative integers (resp. of positive integers).

Throughout the paper, every polynomial is a monic one.

Let $S \in \mathbb{F}_4[x]$ be a nonzero polynomial. A divisor D of S is called unitary if $\gcd(D, S/D) = 1$. We designate by $\gcd_u(S, T)$ the greatest common unitary divisor of S and T . A divisor D of S is called bi-unitary if $\gcd_u(D, S/D) = 1$. We denote by $\sigma(S)$ (resp. $\sigma^*(S)$, $\sigma^{**}(S)$) the sum of all divisors (resp. unitary divisors, bi-unitary divisors) of S . The functions σ , σ^* and σ^{**} are all multiplicative. We say that S is *perfect* (resp. *unitary perfect*, *bi-unitary perfect*) if $\sigma(S) = S$ (resp. $\sigma^*(S) = S$, $\sigma^{**}(S) = S$).

Finally, we say that A is *indecomposable* bi-unitary perfect if A has no proper divisor which is bi-unitary perfect.

Several studies are done about perfect, unitary and bi-unitary perfect polynomials (see [1], [2], [3], [4], [7], [8], [9] and references therein).

In this paper, we are interested in non-splitting polynomials over \mathbb{F}_4 which are bi-unitary perfect (b.u.p.) and divisible by r irreducible factors, where $r \leq 4$.

The splitting case is already treated in ([11], Proposition 3.1 and Theorem 3.2). However, we better precise these results in Theorem 1.1.

We consider the two following sets:

$$\begin{aligned}\Omega_1 &:= \{P \in \mathbb{F}_4[x] : P \text{ and } P + 1 \text{ are both irreducible}\} \\ \Omega_2 &:= \{P \in \mathbb{F}_4[x] : P, P + 1, P^2 + P + 1 \text{ and } P^3 + P^2 + 1 \text{ are all irreducible}\}.\end{aligned}$$

We see that $\Omega_2 \subset \Omega_1$, Ω_2 contains the four (monic) monomials of $\mathbb{F}_4[x]$ and it is an infinite set ([6], Lemma 2). For example, for any $k \in \mathbb{N}$, $P_k := x^{2 \cdot 5^k} + x^{5^k} + \alpha \in \Omega_2$.

We get the following two results related to the fact that A splits or not.

Theorem 1.1. *Let $A = x^a(x+1)^b(x+\alpha)^c(x+\alpha+1)^d \in \mathbb{F}_4[x]$, where $a, b, c, d \in \mathbb{N}$ are not all odd. Then, A is b.u.p if and only if one of the following conditions holds:*

- i) $a = b = c = d = 2$,
- ii) $a = b = 2$ and $c = d = 2^n - 1$, for some $n \in \mathbb{N}$,
- iii) $a = b = 2^n - 1$ and $c = d = 2$, for some $n \in \mathbb{N}$,
- iv) a, b, c, d are given by Table (1).

a	4	4	4	4	4	4	4	5	5	5	5	6	6	6	6
b	3	3	4	4	4	4	3	3	4	4	6	6	6	6	
c	3	4	3	4	5	6	4	6	4	5	3	4	5	6	
d	4	3	5	4	3	6	4	6	5	4	5	4	3	6	

(1)

Theorem 1.2. *Let $A = P^a Q^b R^c S^d \in \mathbb{F}_4[x]$, where A does not split and a, b, c, d are not all odd. Then, A is b.u.p if and only if one of the following conditions holds:*

- i) $a = b = c = d = 2$, $P, R \in \Omega_1$, $Q = P + 1$ and $S = R + 1$,
- ii) $a = b = 2$, $c = d = 2^n - 1$, for some $n \in \mathbb{N}$, $P, R \in \Omega_1$, $Q = P + 1$ and $S = R + 1$,
- iii) $a = b = 2^n - 1$, for some $n \in \mathbb{N}$, $c = d = 2$, $P, R \in \Omega_1$, $Q = P + 1$ and $S = R + 1$,
- iv) $P \in \Omega_2$, $Q = P + 1$, $R, S \in \{P^3 + P + 1, P^3 + P^2 + 1\}$ and $(a, b, c, d) \in \{(7, 13, 2, 2), (13, 7, 2, 2), (14, 14, 2, 2)\}$.

Note that if a, b, c and d are all odd, then $\sigma^{**}(A) = \sigma(A)$. So, A is b.u.p. if and only if A is perfect. We also see that there exists no b.u.p. polynomial A with $\omega(A) = 3$.

Since Ω_1 and Ω_2 are infinite sets, we see that there are infinitely many indecomposable and odd b.u.p. polynomials over \mathbb{F}_4 , even if there are only three 4-tuples available exponents.

2 Preliminaries

Some of the following results are obvious or (well) known, so we omit their proofs. See also [10].

Lemma 2.1. *Let T be an irreducible polynomial over \mathbb{F}_4 and $k, l \in \mathbb{N}^*$. Then, $\gcd_u(T^k, T^l) = 1$ (resp. T^k) if $k \neq l$ (resp. $k = l$). In particular, $\gcd_u(T^k, T^{2n-k}) = 1$ for $k \neq n$, $\gcd_u(T^k, T^{2n+1-k}) = 1$ for any $0 \leq k \leq 2n + 1$.*

Lemma 2.2. *Let $T \in \mathbb{F}_4[x]$ be irreducible. Then*
*i) $\sigma^{**}(T^{2n}) = (1 + T)\sigma(T^n)\sigma(T^{n-1})$, $\sigma^{**}(T^{2n+1}) = \sigma(T^{2n+1})$.*
*ii) For any $c \in \mathbb{N}$, $1 + T$ divides $\sigma^{**}(T^c)$ but T does not.*

Corollary 2.3. *Let $A = P^h Q^k R^l S^t$ be such that h, k, l and t are all odd. Then, A is b.u.p. if and only if it is perfect.*

Lemma 2.4. *If $A = A_1 A_2$ is b.u.p. over \mathbb{F}_4 and if $\gcd(A_1, A_2) = 1$, then A_1 is b.u.p. if and only if A_2 is b.u.p.*

Lemma 2.5. *If A is b.u.p. over \mathbb{F}_4 , then the polynomial $A(x + \lambda)$ is also b.u.p. over \mathbb{F}_4 , for any $\lambda \in \{1, \alpha, \alpha + 1\}$.*

Lemma 2.6. *i) $\sigma^{**}(x^{2k})$ splits over \mathbb{F}_4 if and only if $2k \in \{2, 4, 6\}$.*
*ii) $\sigma^{**}(x^{2k+1})$ splits over \mathbb{F}_4 if and only if $2k + 1 = N \cdot 2^n - 1$ where $N \in \{1, 3\}$.*

Remark 2.7. We get from Lemma 2.6 and for an irreducible polynomial T :

$$\left\{ \begin{array}{ll} \sigma^{**}(T^2) = (T + 1)^2 & (i) \\ \sigma^{**}(T^4) = (T + 1)^2(T + \alpha)(T + \alpha + 1) & (ii) \\ \sigma^{**}(T^6) = (T + 1)^4(T + \alpha)(T + \alpha + 1) & (iii) \\ \sigma^{**}(T^{2^n-1}) = (T + 1)^{2^n-1} & (iv) \\ \sigma^{**}(T^{3 \cdot 2^n-1}) = (T + 1)^{2^n-1}(T + \alpha)^{2^n}(T + \alpha + 1)^{2^n} & (v) \end{array} \right. \quad (2)$$

We sometimes use the above equalities for a suitable T .

3 Proof of Theorem 1.1

This theorem is already stated in [11]. We do not rewrite its proof.

Lemma 3.1 below completes Theorem 3.4 in [4], where one family of splitting perfect polynomials over \mathbb{F}_4 was missing.

See [5] and [6] for the non-splitting case.

Lemma 3.1. *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) $h = k = l = t = N \cdot 2^n - 1$, for some $n \in \mathbb{N}$ and $N \in \{1, 3\}$,*
- iii) $h = l = 3 \cdot 2^r - 1$, $k = t = 2 \cdot 2^r - 1$, for some $r \in \mathbb{N}$,*
- iv) $h = k = 3 \cdot 2^r - 1$, $l = 6 \cdot 2^r - 1$, $t = 4 \cdot 2^r - 1$ for some $r \in \mathbb{N}$.*

Proof. Put $A = x^h(x+1)^k(x+\alpha)^l(x+\alpha+1)^t$. The sufficiency is obtained by direct computations.

For the necessity, we recall the following facts in ([4], Lemma 2.7):

Lemma 3.2. *Let $a \in \{h, k, l, t\}$. Then, $a = 3 \cdot 2^w - 1$ if $a \equiv 2 \pmod{3}$ and $a = 2^w - 1$ if $a \not\equiv 2 \pmod{3}$, with $w \in \mathbb{N}$.*

In particular, $a = 2$ if (a is even and $a \equiv 2 \pmod{3}$).

We take account of Lemmas 2.2, 2.3, 2.6 and 2.7 in [4], for the congruency modulo 3 of each exponent. We get 16 possible cases according to $a \equiv 2 \pmod{3}$ or not.

Moreover, by Lemma 2.2 in [4], the 3 maps $x \mapsto x+1$, $x \mapsto x+\alpha$ and $x \mapsto x+\alpha+1$ preserve “perfection”.

Therefore, h and k (resp. h and l , h and t) play symmetric roles. It remains 4 cases:

- i) $h, k \not\equiv 2 \pmod{3}$*
- ii) $h, l \equiv 2 \pmod{3}$ and $k, t \not\equiv 2 \pmod{3}$*
- iii) $h, k, l, t \equiv 2 \pmod{3}$*
- iv) $h, k, l \equiv 2 \pmod{3}$ and $t \not\equiv 2 \pmod{3}$.*

The first three of them are already treated in the proof of ([4], Theorem 3.4). We got the families i), ii) and iii) in Lemma 3.1.

Now, for the case iv), we may write:

$$h = 3 \cdot 2^r - 1, k = 3 \cdot 2^s - 1, l = 3 \cdot 2^u - 1 \text{ et } t = 2^v - 1, \text{ where } r, s, u, v \in \mathbb{N}.$$

Compute $\sigma(A) = \sigma(x^h) \cdot \sigma((x+1)^k) \cdot \sigma((x+\alpha)^l) \cdot \sigma((x+\alpha+1)^t)$.

$$\begin{aligned}\sigma(x^h) &= (x+1)^{2^r-1} \cdot (x+\alpha)^{2^r} \cdot (x+\alpha+1)^{2^r} \\ \sigma((x+1)^k) &= x^{2^s-1} \cdot (x+\alpha)^{2^s} \cdot (x+\alpha+1)^{2^s} \\ \sigma((x+\alpha)^l) &= (x+\alpha+1)^{2^u-1} \cdot x^{2^u} \cdot (x+1)^{2^u} \\ \sigma((x+\alpha+1)^t) &= \sigma((x+\alpha+1)^{2^v-1}) = (x+\alpha)^{2^v-1}.\end{aligned}$$

Since $\sigma(A) = A$, by comparing exponents in A and those of in $\sigma(A)$, we get:

$$\begin{aligned}2^u + 2^s - 1 &= h = 3 \cdot 2^r - 1 \\ 2^u + 2^r - 1 &= k = 3 \cdot 2^s - 1 \\ 2^r + 2^s + 2^v - 1 &= l = 3 \cdot 2^u - 1 \\ 2^u + 2^s + 2^u - 1 &= t = 2^v - 1\end{aligned}$$

It follows that $s = r$, $u = r + 1$ et $v = r + 2$. Thus, $h = k = 3 \cdot 2^r - 1$, $l = 3 \cdot 2^{r+1} - 1$ and $t = 2^{r+2} - 1$. We obtain the family iv). \square

4 Proof of Theorem 1.2

The sufficiency is obtained by direct computations. Propositions 4.1, 4.4 and 4.15 give the necessity.

As usual, $\omega(S)$ denotes the number of distinct irreducible factors of a polynomial S .

4.1 Case $\omega(A) = 2$

Put $A = P^h Q^k$ with $\deg(P) \leq \deg(Q)$.

Proposition 4.1. *If A is b.u.p., then $Q = P + 1$ and either $(h = k = 2)$ or $(h = k = 2^r - 1, \text{ for some } r \in \mathbb{N})$.*

Proof. We get:

$$\sigma^{**}(P^h)\sigma^{**}(Q^k) = \sigma^{**}(A) = A = P^h Q^k \text{ and } \omega(\sigma^{**}(P^h)) = 1 = \omega(\sigma^{**}(Q^k)).$$

If h and k are both odd, then A is perfect so that $Q = P + 1$ and $h = k = 2^r - 1$ for some $r \in \mathbb{N}$.

Now, we may suppose that h is even. If $h = 2$, then $\sigma^{**}(P^h) = (1 + P)^2$. Since P does not divide $\sigma^{**}(P^h)$, one has $Q^k = (1 + P)^2$ and thus $Q = P + 1$ and $k = 2$. If $h \geq 4$, then $\omega(\sigma^{**}(P^h)) \geq 2$, which is impossible. \square

4.2 Case $\omega(A) = 3$

Put $A = P^h Q^k R^l$ with $\deg(P) \leq \deg(Q) \leq \deg(R)$. Suppose that

$$\sigma^{**}(P^h)\sigma^{**}(Q^k)\sigma^{**}(R^l) = \sigma^{**}(A) = A = P^h Q^k R^l.$$

Lemma 4.2. *The polynomial $P + 1$ is irreducible and $Q = P + 1$.*

Proof. The polynomial $1 + P$ is divisible by Q or by R , since it divides $\sigma^{**}(P^h)$ (Lemma 2.2). We may suppose that $Q \mid (1 + P)$. So, $\deg(Q) = \deg(P)$ and $Q = P + 1$. \square

Lemma 4.3. *One has $\omega(\sigma^{**}(P^h)) \leq 2$, $\omega(\sigma^{**}(Q^k)) \leq 2$, $\omega(\sigma^{**}(R^l)) \leq 2$. Moreover, if h is even (resp. odd), then $h = 2$ (resp. $h = 2^r - 1$, $r \in \mathbb{N}^*$).*

Proof. Since P does not divide $\sigma^{**}(P^h)$, at most Q and R divide it. Hence, $\omega(\sigma^{**}(P^h)) \leq 2$. Similarly, we get $\omega(\sigma^{**}(Q^k)) \leq 2$ and $\omega(\sigma^{**}(R^l)) \leq 2$.

- If $h = 2n$ is even, then $2 \geq \omega(\sigma^{**}(P^{2n})) = \omega((1 + P)\sigma(P^n)\sigma(P^{n-1}))$. So, $n = 1$.

- If h is odd. Put $h = 2^r u - 1$, with u odd. One has:

$$2 \geq \omega(\sigma^{**}(P^{2^r u - 1})) = \omega((1 + P)^{2^r - 1} \sigma(P^{u-1})).$$

So, $u = 1$ because $\omega(\sigma(P^{u-1})) \geq 2$ if $u \geq 3$. \square

Proposition 4.4. *If h, k and l are not all odd, then A is not b.u.p.*

Proof. By Lemma 4.2, one has $Q = P + 1$ and so $A = P^h (P + 1)^k R^l$.

- If h, k are all even, then $h = k = 2$. Therefore,

$$(1 + P)^2 (1 + Q)^2 \sigma^{**}(R^l) = \sigma^{**}(A) = A = P^2 Q^2 R^l.$$

Hence, $\sigma^{**}(R^l) = R^l$. It is impossible.

- If h is even, k odd and l even, then $h = l = 2$, $k = 2^r - 1$. Therefore,

$$Q^2 P^{2^r - 1} (1 + R)^2 = (1 + P)^2 (1 + Q)^{2^r - 1} (1 + R)^2 = \sigma^{**}(A) = A = P^2 Q^{2^r - 1} R^2.$$

Hence, R divides PQ . It is impossible.

- If h is even, k and l odd, then $h = 2$, $k = 2^r - 1$, $l = 2^s - 1$. One has:

$$Q^2 P^{2^r - 1} (1 + R)^{2^s - 1} = (1 + P)^2 (1 + Q)^{2^r - 1} (1 + R)^{2^s - 1} = \sigma^{**}(A) = A = P^2 Q^{2^r - 1} R^{2^s - 1}.$$

Hence, R divides PQ . It is impossible. \square

4.3 Case $\omega(A) = 4$

Put $A = P^h Q^k R^l S^t$ with $\deg(P) \leq \deg(Q) \leq \deg(R) \leq \deg(S)$.

We suppose that A is b.u.p. and indecomposable (i.e., neither $P^h Q^k$ nor $R^l S^t$ are b.u.p).

Lemma 4.5. *One has: $Q = P + 1, 1 + R = P^{u_1} Q^{v_1}, 1 + S = P^{u_2} Q^{v_2} R^z$ where $u_1, v_1 \geq 1$ and $u_2, v_2, z \geq 0$.*

Moreover, if $\deg(R) = \deg(S)$ then $u_2, v_2 \geq 1$ and $z = 0$.

Proof. The polynomial $1 + P$ divides $\sigma^{**}(A) = A$, so Q divides $1 + P$ and thus, $Q = 1 + P$ because $\deg(P) \leq \deg(Q)$.

Now, $1 + R$ divides $\sigma^{**}(A) = A$, so $1 + R = P^{u_1} Q^{v_1} S^{u_3}$ and $u_3 = 0$ because $\deg(R) \leq \deg(S)$. Since $R = P^{u_1} Q^{v_1} + 1$ is irreducible, we conclude that $u_1, v_1 \geq 1$ and $\gcd(u_1, v_1) = 1$. By the same reason, $1 + S = P^{u_2} Q^{v_2} R^z$ where $u_2, v_2, z \geq 0$ and z may be positive. \square

4.3.1 Case $\deg(P) = 1$

We may suppose that $P = x$. Lemma 4.2 implies that $Q = x + 1$. Moreover, $\deg(S) = 1$ if $\deg(R) = 1$. So, $\deg(S) \geq \deg(R) > 1$.

We write: $A = x^h (x + 1)^k R^l S^t$. The exponents h and k play symmetric roles.

Lemma 4.6 ([5], Lemma 2.6). *If $1 + x + \dots + x^{2w} = UV$, then $\deg(U) = \deg(V)$ and $U(0) = 1 = V(0)$.*

Moreover, if R and S are both of the form $x^{u_1}(x + 1)^{v_1} + 1$, then $2w = 6$ and $U, V \in \{x^3 + x + 1, x^3 + x^2 + 1\}$.

Lemma 4.7. *If h is even, then $h \in \{2, 14\}$. Moreover, $R, S \in \{x^3 + x + 1, x^3 + x^2 + 1\}$ if $h = 14$.*

Proof. • If $h \in \{4, 6\}$, then $x + \alpha$ and $x + \alpha + 1$ both divide $\sigma^{**}(x^h)$ and thus, they divide $\sigma^{**}(A) = A$. So, A splits, which is impossible.

• If $h = 2n \geq 8$, then $\sigma^{**}(x^h) = (1 + x)\sigma(x^n)\sigma(x^{n-1})$.

- If $n = 2w \geq 4$, then $\sigma(x^n) = RS$ because it divides $\sigma^{**}(A) = A$ and neither x nor $x + 1$ divide $\sigma(x^n)$. So, by Lemma 4.6, $\deg(R) = \deg(S)$ and $R(0) = 1 = S(0)$. From Lemma 4.5, we may put $1 + R = x^{u_1}(x + 1)^{v_1}$, $1 + S = x^{u_2}(x + 1)^{v_2}$, where $u_1, u_2, v_1, v_2 \geq 1$. Therefore, $2w = 6$ and $h = 12$. But, the monomials $x + 1, x + \alpha$ and $x + \alpha + 1$ all divide $\sigma^{**}(x^{12})$. It contradicts the fact that A does not split.

- If $n = 2w + 1$ is odd, then $\sigma(x^{n-1}) = RS$ and as above, $n - 1 = 2w = 6$. So, $h = 14$, $\sigma^{**}(x^{14}) = (x + 1)^8 RS$ where $R, S \in \{x^3 + x + 1, x^3 + x^2 + 1\}$. \square

Lemma 4.8. *If h is odd, then $h = 2^r u - 1$ where $r \in \mathbb{N}^*$ and $u \in \{1, 7\}$.*

Proof. Put $h = 2^r u - 1$ with u odd. One has:

$$\sigma^{**}(x^h) = \sigma(x^h) = (1+x)^{2^r-1}[\sigma(x^{u-1})]^{2^r}.$$

If $u \geq 3$, then $\sigma(x^{u-1}) = RS$. So, as we have just seen above, $u-1 = 6$ and $R, S \in \{x^3 + x + 1, x^3 + x^2 + 1\}$. \square

Lemma 4.9. *If l is even (resp. odd), then $l = 2$ (resp. $l = 2^s - 1$, with $s \geq 1$).*

Proof. • If l is even and $l \geq 4$, then put $l = 2n$, $n \geq 2$. As above, $\sigma(R^n)$ and $\sigma(R^{n-1})$ divide A .

- If n is even, then we must have $\sigma(R^n) = S^z$ because P, Q divide $1 + R$, R does not divide $\sigma(R^n)$ and $\gcd(1 + R, \sigma(R^n)) = 1$. Hence $z = 1$ and $S = \sigma(R^n)$ is irreducible. It is impossible.

- If n is odd, then $\sigma(R^{n-1}) = S$ which is impossible, as above.

• If $l = 2^r u - 1$ is odd, with u odd, then $\sigma^{**}(R^l) = \sigma(R^l) = (1+R)^{2^r-1}[\sigma(R^{u-1})]^{2^r}$. If $u \geq 3$, then $\sigma(R^{u-1}) = S$, which is impossible. \square

4.3.2 Case $\deg(P) > 1$

Several proofs are similar to those in Section 4.3.1. As above, Lemma 4.2 implies that $Q = P + 1$. We write: $A = P^h(P + 1)^k R^l S^t$.

Lemma 4.10. *If $1 + P + \dots + P^{2w} = RS$, then $\deg(R) = \deg(S)$, $2w = 6$, $P \in \Omega_2$ and $R, S \in \{P^3 + P + 1, P^3 + P^2 + 1\}$.*

Proof. Suppose that $1 + P + \dots + P^{2w} = RS$. One has $1 + x + \dots + x^{2w} = UV$ where $U(P) = R$ and $V(P) = S$. By Lemma 4.6, one has: $U(0) = 1 = V(0)$, $\deg(U) = \deg(V)$. So, $\deg(R) = \deg(S)$.

Moreover, U and V must be of the form $x^u(x + 1)^v + 1$. Indeed, if $1 + U = x^{u_1}(x + 1)^{v_1}L^z$, with $z \geq 0$, then $1 + R = P^u(P + 1)^v L(P)^z$, $L(P) = S^y$, $y \geq 1$, $\deg(S) = \deg(R) = u \deg(P) + zy \deg(S)$, $zy = 0$. Thus, $z = 0$ and $1 + U = x^{u_1}(x + 1)^{v_1}$. Analogously, $1 + V = x^{u_2}(x + 1)^{v_2}$. Therefore, by Lemma 4.6, $2w = 6$ and $R, S \in \{P^3 + P + 1, P^3 + P^2 + 1\}$. \square

Lemma 4.11. *If h is even, then $h \in \{2, 14\}$.*

Proof. • If $h \in \{4, 6\}$, then $P + \alpha$ and $P + \alpha + 1$ both divide $\sigma^{**}(P^h)$ and thus, they divide $\sigma^{**}(A) = A$. So, $P, P + 1, R = P + \alpha$ and $S = P + \alpha + 1$ are all irreducible over \mathbb{F}_4 , which is impossible.

- If $h = 2n \geq 8$, then $\sigma^{**}(P^h) = (1 + P)\sigma(P^n)\sigma(P^{n-1})$.
- If $n = 2w \geq 4$ is even, then $\sigma(P^n) = RS$, $\deg(R) = \deg(S)$. We obtain $2w = 6$ and $h = 12$.
But $P+1, P+\alpha$ and $P+\alpha+1$ all divide $\sigma^{**}(P^{12})$. As above, it is impossible.
- If $n = 2w + 1$ is odd, then $\sigma(P^{n-1}) = RS$ and $n - 1 = 2w = 6$. So, $h = 14$ and $R, S \in \{P^3 + P + 1, P^3 + P^2 + 1\}$. \square

Lemma 4.12. *If h is odd, then $h = 2^r u - 1$ where $r \in \mathbb{N}^*$ and $u \in \{1, 7\}$.*

Proof. Put $h = 2^r u - 1$ with u odd. One has:

$$\sigma^{**}(P^h) = \sigma(P^h) = (1 + P)^{2^r - 1} [\sigma(P^{u-1})]^{2^r}.$$

If $u \geq 3$, then $\sigma(P^{u-1}) = RS$ and as we have just seen above, $u - 1 = 6$ and $R, S \in \{P^3 + P + 1, P^3 + P^2 + 1\}$. \square

We also get the analogues of Lemma 4.9.

Lemma 4.13. *If l is even (resp. odd), then $l = 2$ (resp. $l = 2^s - 1$, with $s \geq 1$).*

4.3.3 End of the proof

We recapitulate below, for $P \in \Omega_2$, $Q = P + 1$, $R = P^3 + P + 1$ and $S = P^3 + P^2 + 1$, the expressions of $\sigma^{**}(T^z)$, for $T^z \in \{P^h, Q^k, R^l, S^t\}$.

Keep in mind that h, k, l and t are not all odd.

h	$\sigma^{**}(P^h)$	k	$\sigma^{**}(Q^k)$
2	Q^2	2	P^2
14	$Q^8 RS$	14	$Q^8 RS$
$2^r - 1$	$Q^{2^r - 1}$	$2^s - 1$	$P^{2^s - 1}$
$7 \cdot 2^r - 1$	$Q^{2^r - 1} R^{2^r} S^{2^r}$	$7 \cdot 2^s - 1$	$P^{2^s - 1} R^{2^s} S^{2^s}$

(3)

l	$\sigma^{**}(R^l)$	t	$\sigma^{**}(S^t)$
2	$P^2 Q^4$	2	$P^4 Q^2$
$2^e - 1$	$P^{2^e - 1} \cdot Q^{2 \cdot (2^e - 1)}$	$2^f - 1$	$P^{2 \cdot (2^f - 1)} \cdot Q^{2^f - 1}$

(4)

We compare from Tables (3) and (4), the exponents of P, Q, R, S in $\sigma^{**}(A)$ and in A . Instead of considering several possible cases, we give an upper bound to each exponent $a \in \{h, k, l, t\}$. We use `Maple` computations to determine those which satisfy $\sigma^{**}(A) = A$. We obtain the following results.

Lemma 4.14. - If h and k are both even, then $h, k \in \{2, 14\}$ and $e, f \leq 3$. So, $l, t \in \{1, 2, 3, 7\}$.

- If h is even and k odd, then $h \in \{2, 14\}$ and $s, e, f \leq 3$. So, $k \in \{1, 3, 7, 13, 27, 55\}$ and $l, t \in \{1, 2, 3, 7\}$.

- If h and k are both odd, then $(h, k, l, t) \in \{(3, 7, 2, 2), (7, 3, 2, 2)\}$.

Proof. - If h is even, then $h \leq 14$. Each exponent of P in the tables equals at most 14. So, $s, e, f \leq 3$.

- If $h = 2^r - 1$ and $k = 2^s - 1$, then $\sigma^{**}(P^h Q^k) = P^k Q^h$, $h = k$ and $P^h Q^k$ is b.u.p. Hence, $R^l S^t$ is also b.u.p. and $l = t = 2$.

- If $h = 2^r - 1$ and $k = 7 \cdot 2^s - 1$, then only R^{2^s} and S^{2^s} divide $\sigma^{**}(A) = A$. So, $s = 1$, $l = t = 2$, $k = 13$. Thus, $\sigma^{**}(R^l S^t) = P^6 Q^6$. By comparing the exponents of Q in the tables, we get $6 + 2^r - 1 = k = 13$. So, $r = 3$ and $h = 7$.

Analogously, if $h = 7 \cdot 2^r - 1$ and $k = 2^s - 1$, then $h = 13, k = 7, l = t = 2$.

- If $h = 7 \cdot 2^r - 1$ and $k = 2^s - 1$, then only $R^{2^r+2^s}$ and $S^{2^r+2^s}$ divide $\sigma^{**}(A) = A$. So, $l = t = 2$ and we get the contradiction: $2^r + 2^s = 2$ with $r, s \geq 1$. \square

We also remark that the values of the exponents h, k, l and t do not depend on the choice of $P \in \Omega_2$. Therefore, for the computations with Maple, we took two values of P : $P = x$ and $P = x^2 + x + \alpha$.

Proposition 4.15. If $A = P^h Q^k R^l S^t$ is b.u.p and indecomposable, where h, k, l and t are not all odd, then

$$P \in \Omega_2, Q = P + 1. R, S \in \{P^3 + P + 1, P^3 + P^2 + 1\},$$

and $(h, k, l, t) \in \{(7, 13, 2, 2), (13, 7, 2, 2), (14, 14, 2, 2)\}$.

4.3.4 Maple Computations

We search all $A = P^h Q^k R^l S^t$ such that h, k, l, t are not all odd, $\omega(A) \geq 3$ and $\sigma^{**}(A) = A$, by means of Lemmas 4.8, 4.9 and 4.14. We get the results stated in Proposition 4.15.

The function σ^{} is defined as Sigm2star**

```
> Sigm2star1:=proc(S,a) if a=0 then 1;else if a mod 2 = 0
then n:=a/2:sig1:=sum(S^l,l=0..n):sig2:=sum(S^l,l=0..n-1):
Factor((1+S)*sig1*sig2) mod 2:
else Factor(sum(S^l,l=0..a) mod 2:fi:fi:end:
```

```

> Sigm2star:=proc(S) P:=1:L:=Factors(S) mod 2:k:=nops(L[2]):
for j to k do S1:=L[2][j][1]:h1:=L[2][j][2]:
P:=P*Sigm2star1(S1,h1):od:P:end:

```

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, *Bi-Unitary Perfect polynomials over $GF(q)$* , Annali di Mat. Pura ed Appl. **149(1)** (1987), 61–68.
- [3] E. F. CANADAY, *The sum of the divisors of a polynomial*, Duke Math. J. **8** (1941), 721–737.
- [4] L. H. GALLARDO, O. RAHAVANDRAINY, *On perfect polynomials over \mathbb{F}_4* , Port. Math. (N.S.) **62(1)** (2005), 109–122.
- [5] L. GALLARDO, O. RAHAVANDRAINY, *Perfect polynomials over \mathbb{F}_4 with less than five prime factors*, Port. Math. (N.S.) **64(1)** (2007), 21–38.
- [6] L. H. GALLARDO, O. RAHAVANDRAINY, *All perfect polynomials with up to four prime factors over \mathbb{F}_4* , Math. Commun. **14(1)** (2009), 47–65.
- [7] L. H. GALLARDO, O. RAHAVANDRAINY, *On unitary splitting perfect polynomials over \mathbb{F}_{p^2}* , Math. Commun. **15(1)** (2010), 159–176.
- [8] L. H. GALLARDO, O. RAHAVANDRAINY, *On splitting perfect polynomials over \mathbb{F}_{p^p}* , Int. Electron. J. Algebra **9** (2011), 85–102.
- [9] L. H. GALLARDO, O. RAHAVANDRAINY, *Unitary perfect polynomials over \mathbb{F}_4 with less than five prime factors*, Funct. et Approx. **45(1)** (2011), 67–78.
- [10] L. H. GALLARDO, O. RAHAVANDRAINY, *All bi-unitary perfect polynomials over \mathbb{F}_2 only divisible by x , $x + 1$ and by Mersenne primes*, arXiv Math: 2204.13337 (2022).
- [11] L. H. GALLARDO, O. RAHAVANDRAINY, *On splitting bi-unitary perfect polynomials over \mathbb{F}_{p^2}* , arXiv Math: 2310.05540v3 (2023).