ALL EVEN (UNITARY) PERFECT POLYNOMIALS OVER F 2 WITH ONLY MERSENNE PRIMES AS ODD DIVISORS

Luis H Gallardo, Olivier Rahavandrainy

ALL EVEN (UNITARY) PERFECT POLYNOMIALS OVER $\mathbb{F}_2$ WITH ONLY MERSENNE PRIMES AS ODD DIVISORS

LUIS H. GALLARDO[1] AND OLIVIER RAHAVANDRAINY[1]

Abstract. We address an arithmetic problem in the ring $\mathbb{F}_2[x]$. We prove that the only (unitary) perfect polynomials over $\mathbb{F}_2$ that are products of x, $x+1$ and of Mersenne primes are precisely the nine (resp. nine "classes") known ones. This follows from a new result about the factorization of $M^{2h+1}+1$, for a Mersenne prime M and for a positive integer h.

1. Introduction

Let $A \in \mathbb{F}_2[x]$ be a nonzero binary polynomial. Let $\sigma(A)$ denote the sum of all divisors of A (including 1 and A). If $\sigma(A) = A$, then one says that A is a *one-ring* ([5]) or in other words, A is *perfect* ([4]). In addition to polynomials of the form $(x^2+x)^{2^n-1}$, with some positive integer n, E. F. Canaday ([5]) discovered eleven non-splitting perfect polynomials (cf. **Notation**): $T_1, \ldots, T_9$ and C_1, C_2. The T_j's are divisible only by x, $x+1$ and by irreducible polynomials of the form $U_{a,b} := x^a(x+1)^b + 1$, for some positive integers a, b. The last two C_1 and C_2 are divisible by x^4+x+1 which is not of the form $U_{a,b}$. The parallel with the integer case is then natural to be considered. We know that all perfect numbers are of the form $2^m(2^m-1)$, where m is a prime number and 2^m-1 is a Mersenne prime number. So, we may consider the following notions. We say ([6]) that a binary polynomial is *even* if it has a linear factor. It is *odd*, otherwise. We ([10]) also define a *Mersenne prime* (polynomial) over $\mathbb{F}_2$ as an irreducible polynomial of the above form $U_{a,b}$. The name comes as an analogue of the integral Mersenne primes, taking $x^a(x+1)^b$ as an analogue of the prime power 2^{a+b}.

Note that the notion of Mersenne prime polynomial is only useful over $\mathbb{F}_2$, whereas one may consider the "parity" of a polynomial over any finite field.

Unitary perfect polynomials are defined and studied in several directions by J. T. B. Beard Jr. et al. ([1], [2], [4]). As over the integers, for $A \in \mathbb{F}_2[x]$, a divisor D of A is *unitary* if $\gcd(D, A/D) = 1$. Let $\sigma^*(A)$ denote the sum of all unitary divisors of A (including 1 and A). If $\sigma^*(A) = A$, then A is *unitary perfect*.

We say that a (unitary) perfect polynomial is *indecomposable* if it is not a product of two coprime nonconstant (unitary) perfect polynomials.

Key words and phrases. Sum of divisors, polynomials, finite fields, characteristic 2.

2010 *Mathematics Subject Classification.* Primary: 11T55. Secondary: 11T06.

DOI

Received:

Accepted:

Any unitary perfect polynomial is even (Lemma 3.4). The known ones, which are only divisible by Mersenne primes (as odd factors), belong to the equivalence classes (see Lemma 3.5) of $B_1, \ldots, B_9$ (see **Notation**). The other ones (which are divisible by non-Mersenne primes) belong to several different (perhaps, infinitely many) classes (see [2] and [12]).

Since a few moments, we would like to continue this investigation (with more or less success). In particular, we want to find all non-splitting (unitary) perfect binary polynomials which are only divisible by x, $x+1$ and by Mersenne primes. Some results are obtained ([8], Theorems 1.1 and 1.3) but they are not complete. The main obstacle is the fact that we cannot understand how $M^{2h+1}+1 = (M+1)\ \sigma(M^{2h})$ factors over $\mathbb{F}_2$, for a Mersenne prime M and a positive integer h. We have formulated ([10]) a conjecture about that (Conjecture 4.1). The further we make progress on that conjecture, the better we reach our goal. Conjecture 4.1 is already proved under some conditions on M and h ([10, Theorem 1.4]). In this paper, we continue working toward its proof with some new conditions on M and h, where the sets $\mathcal{M}$ and Δ defined below intersect. We get Proposition 1.1 which in turn, allows us to obtain Theorems 1.1 and 1.2.

The study of Mersenne primes have some interest. For example, we have established ([10, Theorem 1.3]) that if $\gcd(a,b)=1$, then $U_{a,b} = x^a(x+1)^b+1$ has exactly the same number of irreducible divisors as the trinomial $x^{a+b}+x^b+1$. In particular, they are both irreducible or both not irreducible. So, they would be useful in the domain of error-correcting codes.

It is convenient to fix some notation.

Notation

• The set of integers (resp. of nonnegative integers, of positive integers) is denoted by $\mathbb{Z}$ (resp. $\mathbb{N}$, $\mathbb{N}^*$).

• For $S, T \in \mathbb{F}_2[x]$ and for $m \in \mathbb{N}^*$, $S^m \mid T$ (resp. $S^m \| T$) means that S divides T (resp. $S^m \mid T$ but $S^{m+1} \nmid T$). We also denote by $\overline{S}$ the polynomial defined as $\overline{S}(x) = S(x+1)$ and by $val_x(S)$ (resp. $val_{x+1}(S)$) the valuation of S, at x (resp. at $x+1$).

• We put

$$M_1 = 1+x(x+1),\ M_2 = 1+x(x+1)^2,\ M_3 = 1+x(x+1)^3,$$

$$T_1 = x^2(x+1)M_1,\ T_3 = x^4(x+1)^3M_3,\ T_2 = \overline{T_1},\ T_4 = \overline{T_3},$$

$$T_5 = x^4(x+1)^4M_3\overline{M_3} = \overline{T_5},\ T_6 = x^6(x+1)^3M_2\overline{M_2},\ T_7 = \overline{T_6},$$

$$T_8 = x^4(x+1)^6M_2\overline{M_2}M_3,\ T_9 = \overline{T_8},$$

$$C_1 = x^2(x+1)M_1^2(x^4+x+1),\ C_2 = \overline{C_1}.$$

$B_1 = x^3(x+1)^3 M_1^2,\ B_2 = x^3(x+1)^2 M_1,\ B_3 = x^5(x+1)^4 M_3,$

$B_4 = x^7(x+1)^4 M_2\overline{M_2},\ B_5 = x^5(x+1)^6 M_1^2 M_3,\ B_6 = x^5(x+1)^5 M_3\overline{M_3},$

$B_7 = x^7(x+1)^7 M_2^2\overline{M_2}^2,\ B_8 = x^7(x+1)^6 M_1^2 M_2\overline{M_2},\ B_9 = x^7(x+1)^5 M_2\overline{M_2}\ \overline{M_3}.$

- The following sets play important roles:

$\mathcal{M} = \{M_1, M_2, \overline{M_2}, M_3, \overline{M_3}\},\ \mathcal{P} = \{T_1, \ldots, T_9\},\ \mathcal{P}_u = \{B_1, \ldots, B_9\}$

$\Delta_1 = \{p \in \mathbb{N}^* : p$ is a Mersenne prime$\}$,

$\Delta_2 = \{p \in \mathbb{N}^* : p$ is prime and $ord_p(2) \equiv 0 \bmod 8\}$,
where $ord_p(2)$ denotes the order of 2 in $\mathbb{F}_p \setminus \{0\}$,

$\Delta = \Delta_1 \cup \Delta_2$.

In particular, Δ contains all Fermat primes greater than 5.

Throughout this paper, we **always** suppose that any (unitary) perfect polynomial is **indecomposable**. We have often used Maple software for computations. Our main results are the following.

Proposition 1.1. *Let $h \in \mathbb{N}^*$ and let $M \in \mathbb{F}_2[x]$ be a Mersenne prime. Then in the following cases, $\sigma(M^{2h})$ is divisible by a non-Mersenne prime:*

(i) *$(M \in \{M_1, M_3, \overline{M_3}\})$ or $(M \in \{M_2, \overline{M_2}\}$ and $h \geq 2)$.*

(ii) *$M \notin \mathcal{M}$ and $2h+1$ is divisible by a prime number p lying in $\Delta \setminus \{7\}$.*

Theorem 1.1. *Let $A = x^a(x+1)^b \prod_{i \in I} P_i^{h_i} \in \mathbb{F}_2[x]$ be such that each P_i is a Mersenne prime and $a, b, h_i \in \mathbb{N}^*$. Then A is perfect if and only if $A \in \mathcal{P}$.*

Theorem 1.2. *Let $A = x^a(x+1)^b \prod_{i \in I} P_i^{h_i} \in \mathbb{F}_2[x]$ be such that each P_i is a Mersenne prime and $a, b, h_i \in \mathbb{N}^*$. Then A is unitary perfect if and only if $A = B^{2^n}$, for some $n \in \mathbb{N}$ and $B \in \mathcal{P}_u$.*

We first prove the two theorems before the proposition.

2. Proof of Theorem 1.1

Sufficiencies are obtained by direct computations. For the necessities, we shall apply Lemma 2.3 and Proposition 2.1. We fix:

$A = x^a(x+1)^b \prod_{i \in I} P_i^{h_i} = A_1A_2$, where $a, b, h_i \in \mathbb{N}$, P_i is a Mersenne prime,

$A_1 = x^a(x+1)^b \prod_{P_i \in \mathcal{M}} P_i^{h_i}$ and $A_2 = \prod_{P_j \notin \mathcal{M}} P_j^{h_j}$.

Lemma 2.1. *If A is perfect, then $\sigma(x^a)$, $\sigma((x+1)^b)$ and each $\sigma({P_i}^{h_i})$, with $i \in I$, are only divisible by x, $x+1$ or by Mersenne primes.*

Proof. Since σ is multiplicative, $\sigma(A) = \sigma(x^a)\sigma((x+1)^b) \prod_{i \in I} \sigma({P_i}^{h_i})$. Any divisor of $\sigma(x^a)$, $\sigma((x+1)^b)$ and $\sigma({P_i}^{h_i})$ divides $\sigma(A) = A$. □

Lemma 2.2 ([4], Lemma 2)**.** *A polynomial S is perfect if and only if for any irreducible polynomial P and for any $m_1, m_2 \in \mathbb{N}^*$, we have:*

$$(P^{m_1} \| S, P^{m_2} \| \sigma(S)) \Rightarrow m_1 = m_2.$$

Example 2.1 (useful for Proposition 2.1).
The polynomial $S_1 = x^{13}(x+1)^2 M_1^3 {M_2}^2 \overline{M_2}^{\,2} M_3 \overline{M_3}$ is not perfect because $x^{13} \| S_1$ and $x^7 \| \sigma(S_1)$.

Lemma 2.3 ([8], Theorem 1.1)**.** *If $h_i = 2^{n_i} - 1$ for any $i \in I$, then $A \in \mathcal{P}$.*

We get from Theorem 8 in [5] and from Proposition 1.1.

Lemma 2.4. (i) *If $h \in \mathbb{N}^*$ and if $\sigma(x^{2h})$ is only divisible by Mersenne primes, then $2h \in \{2, 4, 6\}$ and all its divisors lie in $\mathcal{M}$. More precisely, $\sigma(x^2) = M_1 = \sigma((x+1)^2)$, $\sigma(x^4) = M_3$, $\sigma((x+1)^4) = \overline{M_3}$ and $\sigma(x^6) = M_2\overline{M_2} = \sigma((x+1)^6)$.*

(ii) *Let $M \in \mathcal{M}$ and $h \in \mathbb{N}^*$ be such that $\sigma(M^{2h})$ is only divisible by Mersenne primes, then $2h = 2$, $M \in \{M_2, \overline{M_2}\}$ and $\sigma(M^2) \in \{M_1M_3, M_1\overline{M_3}\}$.*

We dress from Lemma 2.4, the following table of all the forms of a, b, P_i and h_i which satisfy Lemma 2.1, if $P_i \in \mathcal{M}$ and if $h_i \neq 2^{n_i} - 1$.

Table 2.1.

a	$\sigma(x^a)$
$3 \cdot 2^n - 1$	$(x+1)^{2^n-1}{M_1}^{2^n}$
$5 \cdot 2^n - 1$	$(x+1)^{2^n-1}{M_3}^{2^n}$
$7 \cdot 2^n - 1$	$(x+1)^{2^n-1}{M_2}^{2^n}\ \overline{M_2}^{\,2^n}$

b	$\sigma((x+1)^b)$
$3 \cdot 2^m - 1$	$x^{2^m-1}{M_1}^{2^m}$
$5 \cdot 2^m - 1$	$x^{2^m-1}\overline{M_3}^{\,2^m}$
$7 \cdot 2^m - 1$	$x^{2^m-1}{M_2}^{2^m}\ \overline{M_2}^{\,2^m}$

P_i	h_i	$\sigma(P_i^{h_i})$
M_2	$3 \cdot 2^{n_i} - 1$	$(1+M_2)^{2^{n_i}-1} {M_1}^{2^{n_i}} \ \overline{M_3}^{\ 2^{n_i}}$
$\overline{M_2}$	$3 \cdot 2^{n_i} - 1$	$(1+\overline{M_2})^{2^{n_i}-1} {M_1}^{2^{n_i}} \ {M_3}^{2^{n_i}}$

Corollary 2.1. *Suppose that A_1 is perfect. Then, neither M_2 nor $\overline{M_2}$ divides $\sigma({P_i}^{h_i})$ if $P_i \in \mathcal{M}$. Moreover, $\overline{M_2}$ divides A_1 whenever M_2 divides A_1 and their exponents* (*in* A_1) *are equal.*

Proof. The first statement follows from Lemma 2.4-(ii). Now, if M_2 divides $A_1 = \sigma(A_1)$, then M_2 divides $\sigma(x^a)\ \sigma((x+1)^b) \prod_{P_i \in \mathcal{M}} \sigma(P_i^{h_i})$. Hence, M_2 divides $\sigma(x^a)\sigma((x+1)^b)$. Table 2.1 shows that a or b is of the form $7 \cdot 2^n - 1$, where $n \in \mathbb{N}$. So, $\overline{M_2}$ divides $\sigma(A_1) = A_1$. It suffices to consider two cases. If $a = 7 \cdot 2^n - 1$ and $b = 7 \cdot 2^m - 1$, then ${M_2}^{\ell} \| A_1$ and $\overline{M_2}^{\ \ell} \| A_1$, with $\ell = 2^n + 2^m$. If $a = 7 \cdot 2^n - 1$ and ($b = 3 \cdot 2^m - 1$ or $b = 5 \cdot 2^m - 1$), then ${M_2}^{\ell} \| A_1$ and $\overline{M_2}^{\ \ell} \| A_1$, with $\ell = 2^n$. □

Lemma 2.5.
If P is a Mersenne prime divisor of $\sigma(A_1)$, then $P, \overline{P} \in \{M_1, M_2, M_3\}$.

Proof. One has: $\sigma(A_1) = \sigma(x^a)\sigma((x+1)^b) \prod_{P_i \in \mathcal{M}} \sigma(P_i^{h_i})$. If P divides $\sigma(x^a)\sigma((x+1)^b)$, then $P \in \mathcal{M}$, by Lemma 2.4-(i). If P divides $\sigma(P_i^{h_i})$ with $P_i \in \mathcal{M}$, then $P_i \in \{M_2, \overline{M_2}\}$, ($h_i = 2$ or h_i is of the form $3 \cdot 2^{n_i} - 1$) and $P, \overline{P} \in \{M_1, M_3\}$ (see Table 2.1). □

Lemma 2.6. *If A is perfect, then $A = A_1$.*

Proof. We claim that $A_2 = 1$. Let $P_j \notin \mathcal{M}$ and $Q_i \in \mathcal{M}$. Then, P_j divides neither $\sigma(x^a)$, $\sigma((x+1)^b)$ nor $\sigma(Q_i^{h_i})$. Thus $\gcd(P_j^{h_j}, \sigma(A_1)) = 1$.
Observe that $P_j^{h_j}$ divides $\sigma(A_2)$ because $P_j^{h_j}$ divides $A = \sigma(A) = \sigma(A_1)\sigma(A_2)$. Hence, A_2 divides $\sigma(A_2)$. So, A_2 is perfect and it is equal to 1, A being indecomposable. □

Proposition 2.1. *If A_1 is perfect, then $h_j = 2^{n_j} - 1$ for any $P_j \in \mathcal{M}$.*

Proof. We refer to Table 2.1.
(i) Suppose that $P_j \notin \{M_2, \overline{M_2}\}$. If h_j is even, then $\sigma(P_j^{h_j})$ is divisible by a non-Mersenne prime. It contradicts Lemma 2.1. If $hj = 2^{n_j} u_j - 1$ with $u_j \geq 3$ odd, then $\sigma(P_j^{h_j}) = (1+P_j)^{2^{n_j}-1} \cdot (1+P_j+\cdots+P_j^{u_j-1})^{2^{n_j}}$. Since $1+P_j+\cdots+P_j^{u_j-1} = \sigma({P_j}^{u_j-1})$ is divisible by a non-Mersenne prime, we also get a contradiction to Lemma 2.1.
(ii) If $P_j \in \{M_2, \overline{M_2}\}$ and (h_j is even or it is of the form $2^{n_j} u_j - 1$, with $u_j \geq 3$ odd and $n_j \geq 1$), then Corollary 2.1 implies that there exists $\ell \in \mathbb{N}^*$ such that ${M_2}^{\ell} \| A_1$ and $\overline{M_2}^{\ \ell} \| A_1$. Recall that $\sigma({M_2}^2) = M_1 \overline{M_3}$ and $\sigma(\overline{M_2}^{\ 2}) = M_1 M_3$. We proceed as in the proof of Corollary 2.1. It suffices to distinguish four cases which give contradictions.

• Case 1: $a = 7 \cdot 2^n - 1$ and $b = 7 \cdot 2^m - 1$
One has $\ell = 2^n + 2^m$ and neither M_1 nor M_3 divides $\sigma(x^a)\ \sigma((x+1)^b)$.
If h_j is even, then $h_j = 2 = \ell$. So, $n = m = 0$, ${M_1}^2 \| \sigma(A_1) = A_1$. It contradicts the part (i) of our proof.
If $h_j = 2^{n_j} u_j - 1$ with $u_j \geq 3$ odd and $n_j \geq 1$, then $u_j = 3$ and ${M_1}^{2 \cdot 2^{n_j}} \| A_1$.
• Case 2: $a = 7 \cdot 2^n - 1$ and $b = 5 \cdot 2^m - 1$
One has $\ell = 2^n$ and $M_1 \nmid \sigma(x^a)\sigma((x+1)^b)$. If h_j is even, then $2^n = \ell = h_j = 2$. So, $n = 1$ and ${M_1}^2 \| A_1$. If $h_j = 2^{n_j} u_j - 1$, with $u_j \geq 3$ odd and $n_j \geq 1$, then $u_j = 3$ and $2^n = \ell = h_j = 3 \cdot 2^{n_j} - 1$. It is impossible.
• Case 3: $a = 7 \cdot 2^n - 1$, $b = 3 \cdot 2^m - 1$ and h_j is even
As above, $2^n = \ell = h_j = 2$, ${M_1}^{2^m}$ divides $\sigma((x+1)^b)$ and ${M_1}^{2^n + 2^m}$ divides $\sigma(A_1) = A_1$. So, $n = 1$ and ${M_1}^{2^m + 2} \| A_1$. Thus, the part (i) implies that $m = 0$. Hence, $A_1 = S_1 = x^{13}(x+1)^2 M_1^3 {M_2}^2 {\overline{M_2}}^{\,2} M_3 \overline{M_3}$ which is not perfect (see Example 2.1).
• Case 4: $a = 7 \cdot 2^n - 1$, $b = 3 \cdot 2^m - 1$, $h_j = 2^{n_j} u_j - 1$, $u_j \geq 3$ odd, $n_j \geq 1$
One has $u_j = 3$ and $2^n = \ell = h_j = 3 \cdot 2^{n_j} - 1$. It is impossible. □

Lemma 2.6, Proposition 2.1 and Lemma 2.3 imply

Corollary 2.2. *If A is perfect, then $A = A_1 \in \mathcal{P}$.*

3. Proof of Theorem 1.2

As in Section 2, we fix:

$$A = x^a(x+1)^b \prod_{i \in I} P_i^{h_i} = A_1 A_2, \text{ where } a, b, h_i \in \mathbb{N},\ P_i \text{ is a Mersenne prime,}$$

$$A_1 = x^a(x+1)^b \prod_{P_i \in \mathcal{M}} P_i^{h_i} \text{ and } A_2 = \prod_{P_j \notin \mathcal{M}} P_j^{h_j}$$

Sufficiencies are obtained by direct computations. For the necessities, we shall apply Lemma 3.6 and Proposition 3.1.

Lemma 3.1. *If A is unitary perfect, then $\sigma^*(x^a)$, $\sigma^*((x+1)^b)$, $\sigma^*({P_i}^{h_i})$, for any $i \in I$, are only divisible by x, $x+1$ or by Mersenne primes.*

Proof. Since σ^* is multiplicative, $\sigma^*(A) = \sigma^*(x^a)\sigma^*((x+1)^b) \prod_{i \in I} \sigma^*({P_i}^{h_i})$. Any divisor of $\sigma^*(x^a)$, $\sigma^*((x+1)^b)$, $\sigma^*({P_i}^{h_i})$ divides $\sigma^*(A) = A$. □

Lemma 3.2 ([4], Lemma 2)**.** *A polynomial S is unitary perfect if and only if for any irreducible polynomial P and for any $m_1, m_2 \in \mathbb{N}^*$, we have:*

$$(P^{m_1} \| S, P^{m_2} \| \sigma^*(S)) \Rightarrow m_1 = m_2).$$

Example 3.1 (useful for Proposition 3.1).
The polynomial $S_2 = x^{14}(x+1)^7 {M_1}^2 {M_2}^3 {\overline{M_2}}^{\,3} M_3 \overline{M_3}$ is not unitary perfect since $x^{14} \| S_2$ and $x^{10} \| \sigma^*(S_2)$.

Similar arguments give Proposition 3.1 which finishes our proof.

Lemma 3.3. *Let $S \in \mathbb{F}_2[x]$ be an irreducible polynomial. Then, for any $n, u \in \mathbb{N}$ with u odd, $\sigma^*(S^{2^n u}) = (1+S)^{2^n} (\sigma(S^{u-1}))^{2^n}$.*

The following table, obtained from Lemmas 2.1, 2.4 and 3.3, are useful to prove Proposition 3.1.

Table 3.1.

a	$\sigma^*(x^a)$
$3 \cdot 2^n$	$(x+1)^{2^n} {M_1}^{2^n}$
$5 \cdot 2^n$	$(x+1)^{2^n} {M_3}^{2^n}$
$7 \cdot 2^n$	$(x+1)^{2^n} {M_2}^{2^n} \ \overline{M_2}^{\ 2^n}$

b	$\sigma^*((x+1)^b)$
$3 \cdot 2^m$	$x^{2^m} {M_1}^{2^m}$
$5 \cdot 2^m$	$x^{2^m} \overline{M_3}^{\ 2^m}$
$7 \cdot 2^m$	$x^{2^m} {M_2}^{2^m} \ \overline{M_2}^{\ 2^m}$

P_i	h_i	$\sigma^*(P_i^{h_i})$
M_2	$3 \cdot 2^{n_i}$	$(1+M_2)^{2^{n_i}} {M_1}^{2^{n_i}} \ \overline{M_3}^{\ 2^{n_i}}$
$\overline{M_2}$	$3 \cdot 2^{n_i}$	$(1+\overline{M_2})^{2^{n_i}} {M_1}^{2^{n_i}} \ {M_3}^{2^{n_i}}$

Lemma 3.4. *Let $C \in \mathbb{F}_2[x] \setminus \{0, 1\}$ be u.p. Then C is even, $\overline{C}$ and C^{2^r} are also u.p, for any $r \in \mathbb{N}$.*

Proof. If D is a divisor of C, then $\overline{D}$ divides $\overline{C}$ and D^{2^r} divides C^{2^r}. Thus, $\sigma^*(\overline{C}) = \overline{\sigma^*(C)} = \overline{C}$ and $\sigma^*(C^{2^r}) = (\sigma^*(C))^{2^r} = C^{2^r}$.
It remains to prove that C is even. Consider an irreducible divisor P of C and $k \in \mathbb{N}^*$ such that $P^k \| C$. The polynomial $1+P$ is even and divides $1+P^k = \sigma^*(P^k)$. So, $1+P$ divides $\sigma^*(C) = C$. □

Definition 3.1. We denote by $\sim$ the relation on $\mathbb{F}_2[x]$ defined as: $S \sim T$ if there exists $\ell \in \mathbb{Z}$ such that $S = T^{2^\ell}$.

Lemma 3.5. ([3], Section 2)
The relation $\sim$ is an equivalence relation on $\mathbb{F}_2[x]$. Each equivalence class contains a unique polynomial B which is not a square, with $val_x(B) \leq val_{x+1}(B)$.

Lemma 3.6 ([8], Theorem 1.3)**.** *If $h_i = 2^{n_i}$ for any $i \in I$, then A (or $\overline{A}$) is of the form B^{2^n}, where $B \in \mathcal{P}_u$.*

Proposition 3.1. *(i) If A is u.p, then $A = A_1$.*
(ii) If A_1 is u.p, then $h_j = 2^{n_j}$ for any $P_j \in \mathcal{M}$.
(iii) If A is u.p, then A or $\overline{A}$ is of the form B^{2^n}, where $B \in \mathcal{P}_u$.

Proof. The proof of (i) is analogous to that of Lemma 2.6. The statement (iii) follows from (i), (ii) and Lemma 3.6. We only sketch the proof of (ii).
Set $h_j = 2^{n_j} u_j$, where u_j is odd and $n_j \geq 0$.

- Suppose that $P_j \not\in \{M_2, \overline{M_2}\}$. If $u_j \geq 3$, then $\sigma(P_j^{u_j-1})$ and thus $\sigma^*(P_j^{h_j})$ are divisible by a non-Mersenne prime. It contradicts Lemma 2.1.
- If $P_j \in \{M_2, \overline{M_2}\}$ and if $u_j \geq 3$, then $u_j = 3$ and (a or b is of the form $7 \cdot 2^n$). Recall that $\sigma^*({M_2}^3) = (1 + M_2)M_1\overline{M_3}$ and $\sigma^*(\overline{M_2}^{\,3}) = (1 + \overline{M_2})M_1 M_3$. We consider two cases. The first gives non unitary perfect polynomials whereas the second leads to a contradiction.

• Case 1: $a = 7 \cdot 2^n$ and $b = 7 \cdot 2^m$, with $n, m \geq 0$
One has ${M_2}^{\ell} \| A_1$ and $\overline{M_2}^{\,\ell} \| A_1$, with $\ell = 2^n + 2^m$. Neither M_1 nor M_3 divides $\sigma(x^a)\ \sigma((x + 1)^b)$.
Thus, $3 \cdot 2^{n_j} = h_j = \ell = 2^n + 2^m$. So, ($n = m + 1$ and $n_j = m$) or ($m = n + 1$ and $n_j = n$). Therefore, $({M_1}^2)^{2^{n_j}}$, ${M_3}^{2^{n_j}}$ and $\overline{M_3}^{\,2^{n_j}}$ divide $\sigma^*(M_2^{h_j})\sigma^*(\overline{M_2}^{\,h_j})$ and they divide $\sigma^*(A_1) = A_1$. Thus, $A_1 = {S_2}^{2^m}$ or $A_1 = \overline{S_2}^{\,2^n}$ where $S_2 = x^{14}(x + 1)^7 {M_1}^2 {M_2}^3 \overline{M_2}^{\,3} M_3 \overline{M_3}$. In both cases, A_1 is not unitary perfect because S_2 is not u.p (Example 3.1).

• Case 2: $a = 7 \cdot 2^n$ and ($b = 5 \cdot 2^m$ or $b = 3 \cdot 2^m$), with $n, m \geq 0$
One has $\ell = 2^n$. So, we get the contradiction: $3 \cdot 2^{n_j} = h_j = \ell = 2^n$. □

4. Proof of Proposition 1.1

That proposition partially solves

Conjecture 4.1. ([10], Conjecture 1.1) Let $h \in \mathbb{N}^*$ and let $M \in \mathbb{F}_2[x]$ be a Mersenne prime. Then, $\sigma(M^{2h})$ is always divisible by a non-Mersenne prime, except for $M \in \{M_2, M_3\}$ and $h = 1$.

We mainly prove it by contradiction (to Corollary 4.1). Lemma 4.1 states that $\sigma(M^{2h})$ is square-free, for any $h \in \mathbb{N}^*$.
Recall that we set $M = x^a(x + 1)^b + 1$, $U_{2h} = \sigma(\sigma(M^{2h}))$ and

$$\sigma(M^{2h}) = \prod_{j \in J} P_j,\ P_j = 1 + x^{a_j}(x + 1)^{b_j} \text{ irreducible, } P_i \neq P_j \text{ if } i \neq j. \tag{4.1}$$

By Lemma 4.3, if there exists a prime divisor p of $2h + 1$ such that $\sigma(M^{p-1})$ is divisible by a non-Mersenne prime, then $\sigma(M^{2h})$ is also divisible by a non-Mersenne. Therefore, it suffices to consider that $2h + 1 = p$ is a prime number, except for $p = 3$ with $M \in \{M_2, \overline{M_2}\}$ (see Section 4.3).

4.1. **Useful facts.** For $S \in \mathbb{F}_2[x] \backslash \{0, 1\}$, of degree s, we denote by $\alpha_l(S)$ the coefficient of x^{s-l} in S, $0 \leq l \leq s$. One has: $\alpha_0(S) = 1$.

Lemma 4.1 ([10], Lemmas 4.6 and 4.8)**.**
The polynomial $\sigma(M^{2h})$ *is square-free and* $M \neq M_1$.

Lemma 4.2 ([10], Theorem 1.4)**.** *Let $h \in \mathbb{N}^*$ be such that $p = 2h+1$ is prime and let M be a Mersenne prime such that $M \not\in \{M_2, \overline{M_2}\}$ and $\omega(\sigma(M^{2h})) = 2$. Then, $\sigma(M^{2h})$ is divisible by a non-Mersenne prime.*

The lemma below generalizes Lemma 4.10 in [10] (with an analogous proof).

Lemma 4.3. *If k is a divisor (prime or not) of $2h+1$, then $\sigma(M^{k-1})$ divides $\sigma(M^{2h})$.*

We sometimes apply Lemmas 4.4 and 4.5 without explicit mentions.

Lemma 4.4. *Let $S \in \mathbb{F}_2[x]$ be such that $s = \deg(S) \geq 1$ and $l, t, r, r_1, \ldots, r_k \in \mathbb{N}$ be such that $r_1 > \cdots > r_k$, $t \leq k, r_1 - r_t \leq l \leq r \leq s$. Then*

(i) $\alpha_l[(x^{r_1} + \cdots + x^{r_k})S] = \alpha_l(S) + \alpha_{l-(r_1-r_2)}(S) + \cdots + \alpha_{l-(r_1-r_t)}(S)$.

(ii) $\alpha_l(\sigma(S)) = \alpha_l(S)$ *if any divisor of S has degree at least $r+1$.*

Proof. The equality in (i) (resp. in (ii)) follows from the definition of α_l (resp. from the fact: $\sigma(S) = S + T$, where $\deg(T) \leq \deg(S) - r - 1$). □

Corollary 4.1. (i) *The integers $u = \sum_{j \in J} a_j$ and $v = \sum_{j \in J} b_j$ are both even.*

(ii) *The polynomial U_{2h} splits (over $\mathbb{F}_2$) and it is a square.*

(iii) *The polynomial $\sigma(M^{2h})$ is reducible.*

Proof. (i) See [10, Corollary 4.9].
For (ii), Assumption (4.1) implies that $U_{2h} = \sigma(\sigma(M^{2h})) = \sigma(\prod_{j \in J} P_j)$.
Hence, $U_{2h} = \prod_{j \in J} x^{a_j}(x+1)^{b_j} = x^u(x+1)^v$, where u and v are both even.
(iii) If $\sigma(M^{2h}) = Q$ is irreducible, then $U_{2h} = 1 + Q$ is not a square. □

Lemma 4.5. *One has $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h})$ if $l \leq a+b-1$ and $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h} + M^{2h-1})$ if $a+b \leq l \leq 2(a+b)-1$.*

Proof. Since $\sigma(M^{2h}) = M^{2h} + M^{2h-1} + T$, with $\deg(T) \leq (a+b)(2h-2) = 2h(a+b) - 2(a+b)$, Lemma 4.4-(ii) implies that $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h})$ if $l \leq a+b-1$ and $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h} + M^{2h-1})$ if $a+b \leq l \leq 2(a+b)-1$. □

Lemma 4.6. *Denote by $N_2(m)$ the number of irreducible polynomials over $\mathbb{F}_2$, of degree $m \geq 1$. Then*

(i) $N_2(m) \geq \dfrac{2^m - 2(2^{m/2}-1)}{m}$,

(ii) $\varphi(m) < N_2(m)$ *if $m \geq 4$, where φ is the Euler totient function,*

(iii) *For each $m \geq 4$, there exists an irreducible polynomial of degree m, which is not a Mersenne prime.*

Proof. (i) See [11], Exercise 3.27, p. 142.
(ii) If $m \in \{4,5\}$, then direct computations give $\varphi(4) = 2,\ N_2(4) = 3$ and $\varphi(5) = 4,\ N_2(5) = 6$.
Now, suppose that $m \geq 6$. Consider the function $f(x) = 2^x - 2(2^{x/2} - 1) - x^2$, for $x \geq 6$. The derivative of f is a positive function. So, $f(x) \geq f(6) > 0$ and $x < \dfrac{2^x - 2(2^{x/2}-1)}{x}$. Thus, $\varphi(m) \leq m < \dfrac{2^m - 2(2^{m/2}-1)}{m} \leq N_2(m)$.
(iii) We remark that if $1 + x^c(x+1)^d$ is a Mersenne prime, then $\gcd(c,d) = 1$. So, $\gcd(c, c+d) = 1$. Therefore, the set $\mathcal{M}_m$ of Mersenne primes of degree m is a subset of $\{x^c(x+1)^{m-c} + 1 : 1 \leq c \leq m,\ \gcd(c,m) = 1\}$. Thus,

$$\#\mathcal{M}_m \leq \#\{c : 1 \leq c \leq m,\ \gcd(c,m) = 1\} = \varphi(m).$$

Hence, there exist at least $N_2(m) - \varphi(m)$ irreducible non-Mersenne polynomials, with $N_2(m) - \varphi(m) \geq 1$, by (ii). □

Lemma 4.7. *For any $j \in J$, $ord_p(2)$ divides $a_j + b_j = \deg(P_j)$.*

Proof. Set $d = \gcd\limits_{i \in J}(a_i + b_i)$. By Lemma 4.13 in [10], p divides $2^d - 1$. Thus, $ord_p(2)$ divides d. □

Lemma 4.8. ([11], Chap. 2 and 3)
Let $q = 2^r - 1$ be a Mersenne prime number. Then, any irreducible polynomial P of degree r is primitive. In particular, each root β of P is a primitive element of the field $\mathbb{F}_{2^r}$, so that β is of order q in $\mathbb{F}_{2^r} \setminus \{0\}$.

Lemma 4.9. *Let $P_i = 1+x^{a_i}(x+1)^{b_i}$ be a prime divisor of $\sigma(M^{p-1})$, where $2^{a_i+b_i}-1 = p_i$ is a prime number. Then, $p_i = p$ and $\sigma(M^{p-1})$ is divisible by any irreducible polynomial of degree $a_i + b_i$. Furthermore, at least one of those divisors is not a Mersenne prime if $a_i + b_i \geq 4$.*

Proof. The polynomial P_i is primitive. If α is a root of P_i, then $(M^p + 1)(\alpha) = 0$ and $M(\alpha) = \alpha^r$ for some $1 \leq r \leq p_i - 1$. Thus, $1 = M(\alpha)^p = \alpha^{rp}$, with $ord(\alpha) = p_i$. So, p_i divides rp and $p_i = p$.
Any irreducible polynomial S of degree $a_i + b_i$ is primitive. Let β be a root of S. One has $ord(\beta) = p_i = p$, $S(\beta) = 0$ and $M(\beta) = \beta^s$, for some $1 \leq s \leq p_i - 1$. Thus, $M(\beta)^p = \beta^{ps} = 1$ and S divides $M^p + 1 = x^a(x+1)^b\sigma(M^{p-1})$.
The third statement follows from Lemma 4.6-(iii). □

Corollary 4.2. *For any $i \in J$, $a_i + b_i \leq 3$ or $2^{a_i+b_i} - 1$ is not prime.*

Lemma 4.10. *Let $P, Q \in \mathbb{F}_2[x]$ be such that $\deg(P) = r$, $2^r - 1$ is prime, $P \nmid Q(Q+1)$ but $P \mid Q^p + 1$. Then $2^r - 1 = p$.*

Proof. The polynomial P is primitive. If β is a root of P, then $ord(\beta) = 2^r - 1$. Moreover, $Q(\beta) \not\in \{0,1\}$ because $P \nmid Q(Q+1)$. Thus, $Q(\beta) = \beta^t$ for some $1 \leq t \leq 2^r - 2$. Hence, $1 = Q(\beta)^p = \beta^{tp}$. So, $2^r - 1$ divides tp and $2^r - 1 = p$. □

Corollary 4.3. *Let $r \in \mathbb{N}^*$ be such that $2^r - 1$ is a prime distinct from p. Then, no irreducible polynomial of degree r divides $\sigma(M^{p-1})$.*

Proof. If P is a prime divisor of $\sigma(M^{p-1})$ with $\deg(P) = r$, then P divides $M^p + 1$ and by taking $Q = M$ in the above lemma, we get a contradiction. $\square$

In the following lemma and two corollaries, we suppose that p is a Mersenne prime of the form $2^m - 1$ (with m prime).

Lemma 4.11. *Let $P, Q \in \mathbb{F}_2[x]$ be such that P is irreducible of degree m and $P \nmid Q(Q+1)$. Then, P divides $Q^p + 1$.*

Proof. The polynomial P is primitive. If β is a root of P, then $ord(\beta) = 2^m - 1 = p$, $Q(\beta) \not\in \{0, 1\}$ because $P \nmid Q(Q+1)$. Thus, $Q(\beta) = \beta^t$ for some $1 \leq t \leq p-1$. Hence, $Q(\beta)^p = \beta^{tp} = 1$. So, P divides $Q^p + 1$. $\square$

Corollary 4.4. *Any irreducible polynomial $P \neq M$ (Mersenne or not), of degree m, divides $\sigma(M^{p-1})$.*

Proof. We may apply Lemma 4.11, with $Q = M$, because P does not divide $x^a(x+1)^b M = M(M+1) = Q(Q+1)$. So, P is odd and it divides $M^p+1 = (M+1)\,\sigma(M^{p-1}) = x^a(x+1)^b\ \sigma(M^{p-1})$. $\square$

Corollary 4.5. *The polynomial M_1 (resp. M_2, $\overline{M_2}$) divides $\sigma(M^{p-1})$ if and only if ($M \neq M_1$ and $p = 3$) (resp. $M \neq M_2$ and $p = 7$, $M \neq \overline{M_2}$ and $p = 7$).*

Proof. Apply Corollary 4.4 with $m \in \{2, 3\}$. $\square$

In order to carry on the proof (of Proposition 1.1), we distinguish three cases.

4.2. **Case I:** $M \in \{M_1, M_3, \overline{M_3}\}$**.** Lemma 4.1 implies that $M \neq M_1$. It suffices to suppose that $M = M_3$. We refer to Section 5.2 in [9]. Put $D = M_1 M_2 \overline{M_2}$. By [9, Lemma 5.4], we have to consider four situations:

(i) $\gcd(\sigma(M^{2h}), D) = 1$,

(ii) $\sigma(M^{2h}) = M_1 B$, with $\gcd(B, D) = 1$,

(iii) $\sigma(M^{2h}) = M_2 \overline{M_2} B$, with $\gcd(B, D) = 1$,

(iv) $\sigma(M^{2h}) = DB$, with $\gcd(B, D) = 1$, where any irreducible divisor of B has degree exceeding 5.

The following lemma contradicts the fact that U_{2h} is a square.

Lemma 4.12. *One has $\alpha_3(U_{2h}) = 1$ or $\alpha_5(U_{2h}) = 1$.*

Proof. For (i), (iii) and (iv), use [9], Lemmas 5.9, 5.10, 5.15 and 5.17.
(ii) Since $\sigma(M^{2h}) = (x^2 + x + 1)B$ and $U_{2h} = (x^2 + x)\sigma(B)$, we obtain (by Lemmas 4.4 and 4.5):

$$\begin{cases} 0 = \alpha_1(M^{2h}) = \alpha_1(\sigma(M^{2h})) = \alpha_1(B) + 1, \\ \alpha_3(U_{2h}) = \alpha_3(\sigma(B)) + \alpha_2(\sigma(B)) = \alpha_3(B) + \alpha_2(B), \\ 0 = \alpha_3(M^{2h}) = \alpha_3(\sigma(M^{2h})) = \alpha_3(B) + \alpha_2(B) + \alpha_1(B). \end{cases}$$

Thus, $\alpha_3(U_{2h}) = \alpha_3(B) + \alpha_2(B) = \alpha_1(B) = 1$. $\square$

4.3. **Case II:** $M \in \{M_2, \overline{M_2}\}$ **and** $h \geq 2$**.** It suffices to consider that $M = M_2$.

Lemma 4.13. (i) *If* $h \geq 4$*, then* M_1 *divides* $\sigma(M^{2h})$ *if and only if* 3 *divides* $2h+1$*.*

(ii) *If* $h \geq 4$*, then* M_2 *divides* $\sigma(M^{2h})$ *if and only if* 7 *divides* $2h+1$*.*

(iii) *If* $h \geq 4$ *and if* $2h+1$ *is divisible by a prime* $p \not\in \{3, 7\}$*, then any irreducible divisor of* $\sigma(M^{2h})$ *is of degree at least* 4*.*

Proof. The assertion (iii) follows from (i) and (ii) which in turn, are obtained from Corollaries 4.3 and 4.4. □

We consider three possibilities since $\sigma(M^{p-1}) = \sigma({M_2}^2) = M_1\overline{M_3}$ (product of two Mersenne primes), if $p = 3$.

4.3.1. *II-1:* $2h+1$ *is (divisible by) a prime* $p \in \{5, 7\}$*.*

Lemma 4.14. *For* $p \in \{5, 7\}$*, some non-Mersenne prime divides* $\sigma(M^{p-1})$*.*

Proof. Here, $h \in \{2, 3\}$. By direct computations, $U_4 = x^3(x+1)^6(x^3+x+1)$ and $U_6 = x^8(x+1)^4(x^3+x+1)^2$ which do not split (despite that U_6 is a square). □

4.3.2. *II-2:* $2h+1 = 3^w$*, for some* $w \geq 2$*.* In this case, 9 divides $2h+1$ and $\sigma(M^8)$ divides $\sigma(M^{2h})$ (by Lemma 4.3). But, $\sigma(M^8) = (x^2+x+1)(x^4+x^3+1)(x^6+x+1)(x^{12}+x^8+x^7+x^4+1)$, where $x^6+x+1 = 1+x(x+1)M_3$ is not a Mersenne prime.

4.3.3. *II-3:* $2h+1$ *is (divisible by) a prime* $p \not\in \{3, 5, 7\}$*.* We may write $p = 2h+1$ with $h \geq 4$.

Lemma 4.15. (i) *If* $l \in \{1, 2, 3\}$*, then* $\alpha_l(U_{2h}) = \alpha_l(\sigma(M^{2h}))$*.*

(ii) *If* $l \in \{1, 2\}$*, then* $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h})$*.*

(iii) *The coefficients* $\alpha_3(\sigma(M^{2h}))$ *and* $\alpha_3(M^{2h} + M^{2h-1})$ *are equal.*

Proof. (i) It follows from Lemma 4.13.
For $l \leq 2$, $6h - l = \deg(\sigma(M^{2h})) - l = \deg((M^{2h}) - l > 3(2h-1) = \deg(M^{2h-1})$ and for $3 \leq l \leq 5$, $6h - l > 3(2h-2) = \deg(M^{2h-2})$. Hence, we get (ii) and (iii). □

Corollary 4.6. *The coefficient* $\alpha_3(U_{2h})$ *equals* 1*.*

Proof. The previous lemma implies that $\alpha_3(U_{2h}) = \alpha_3(M^{2h} + M^{2h-1}) = \alpha_3[(x^3+x)M^{2h-1}] = \alpha_3(M^{2h-1}) + \alpha_1(M^{2h-1})$.
But, $M^{2h-1} = (x^3+x+1)^{2h-1} = (x^3+x)^{2h-1} + (x^3+x)^{2h-2} + \cdots$
The coefficient of x^{6h-6} (resp. of x^{6h-4}) in M^{2h-1} is exactly $\alpha_3(M^{2h-1})$ (resp. $\alpha_1(M^{2h-1})$).
So, $\alpha_3(M^{2h-1}) = 1$ and $\alpha_1(M^{2h-1}) = 0$. □

4.4. **Case III:** $M \not\in \mathcal{M}$**.** Here, we have two possibilities.

4.4.1. *III-1: the prime p is such that $ord_p(2) \equiv 0 \mod 8$.* Lemmas 4.16 and 4.7 imply Corollary 4.7.

Lemma 4.16. *There exists no Mersenne prime of degree multiple of* 8.

Proof. If $Q = 1 + x^{c_1}(x+1)^{c_2}$ with $c_1 + c_2 = 8k$, then $\omega(Q)$ is even by [10, Corollary 3.3]. So, Q is reducible. □

Corollary 4.7. *If $ord_p(2) \equiv 0 \mod 8$, then $\sigma(M^{2h})$ is divisible by a non-Mersenne prime.*

Proof. Suppose that $\sigma(M^{2h}) = \prod_{j \in J} P_j$, where each P_j is a Mersenne prime. Then, Lemma 4.7 implies that $ord_p(2)$ divides $\deg(P_j)$, for any $j \in J$. So, 8 divides $\deg(P_j)$. It contradicts Lemma 4.16. □

4.4.2. *III-2: p is a Mersenne prime number with $p \neq 7$.* Set $p = 2^m - 1$, with m and p are both prime. Note that there are (at present) 51 known Mersenne prime numbers (OEIS Sequences A000043 and A000668). The first five of them are: $3, 7, 31, 127$ and 8191.

Lemma 4.17. *If $p \geq 31$ is a Mersenne prime number, then $\sigma(M^{p-1})$ is divisible by a non-Mersenne prime.*

Proof. Here, $a + b = \deg(M) \geq 5$ since $M \notin \mathcal{M}$. We get our result from Corollary 4.4 and Lemma 4.6-(iii). □

It remains then the case $p = 3$ (since $p \neq 7$, in this section). Lemma 4.2 has already treated the case where $\omega(\sigma(M^2)) = 2$. So, we suppose that $\omega(\sigma(M^2)) \geq 3$. Put $\sigma(M^2) = M_1 \cdots M_r,\ r \geq 3$ and $U_2 = \sigma(\sigma(M^2))$.
We shall prove that $\alpha_3(U_2) = 1$ (Corollary 4.9), a contradiction to the fact that U_2 is a square. Corollary 4.5 gives

Lemma 4.18. *(i) The trinomial $1 + x + x^2$ divides $\sigma(M^2)$.*
(ii) No irreducible polynomial of degree $r \geq 3$ such that $2^r - 1$ is prime, divides $\sigma(M^2)$.

Corollary 4.8. *The polynomial $\sigma(M^2)$ is of the form $(1 + x + x^2)B$, where $\gcd(1 + x + x^2, B) = 1$ and any prime divisor of B has degree at least* 4.

Lemma 4.19. *If $\sigma(M^2) = (1 + x + x^2)B$ with $\gcd(1 + x + x^2, B) = 1$, then*

(i) $\alpha_1(\sigma(M^2)) = \alpha_1(B) + 1,\ \alpha_2(\sigma(M^2)) = \alpha_2(B) + \alpha_1(B) + 1,$

(ii) $\alpha_3(\sigma(M^2)) = \alpha_3(B) + \alpha_2(B) + \alpha_1(B),$

(iii) $\alpha_3(\sigma(M^2)) = 0.$

Proof. We directly get (i) and (ii). For (iii), $\sigma(M^2) = 1 + M + M^2 = x^{2a}(x+1)^{2b} + x^a(x+1)^b + 1$. Moreover, $2a + 2b - 3 > a + b$ because $a + b \geq 4$ and $x^{2a}(x+1)^{2b}$ is a square. So, $\alpha_3(\sigma(M^2)) = \alpha_3(x^{2a}(x+1)^{2b}) = 0$. □

Lemma 4.20. *Some coefficients of U_2 and B satisfy:*

$$\alpha_1(U_2) = \alpha_1(B) + 1,\ \alpha_2(U_2) = \alpha_2(B) + \alpha_1(B),\ \alpha_3(U_2) = \alpha_3(B) + \alpha_2(B).$$

Proof. Corollary 4.8 implies that $U_2 = \sigma(\sigma(M^2)) = \sigma((1+x+x^2)B) = \sigma(1+x+x^2)\sigma(B) = (x^2+x)\sigma(B)$. Any irreducible divisor of B has degree more than 3. Hence, $\alpha_l(\sigma(B)) = \alpha_l(B)$, for $1 \leq l \leq 3$.

One gets: $\begin{cases} \alpha_1(U_2) = \alpha_1(\sigma(B)) + 1 = \alpha_1(B) + 1, \\ \alpha_2(U_2) = \alpha_2(\sigma(B)) + \alpha_1(\sigma(B)) = \alpha_2(B) + \alpha_1(B), \\ \alpha_3(U_2) = \alpha_3(\sigma(B)) + \alpha_2(\sigma(B)) = \alpha_3(B) + \alpha_2(B). \end{cases}$ □

Corollary 4.9. *The coefficient $\alpha_3(U_2)$ equals* 1.

Proof. The polynomial U_2 is a square, so $0 = \alpha_1(U_2) = \alpha_1(B) + 1$ and thus $\alpha_1(B) = 1$. Lemma 4.19-(iii) implies that $0 = \alpha_3(\sigma(M^2)) = \alpha_3(B) + \alpha_2(B) + \alpha_1(B)$. Therefore, $\alpha_3(U_2) = \alpha_3(B) + \alpha_2(B) = \alpha_1(B) = 1$. □

Remark 4.1. Our method fails for $p = 7$. Indeed, for many M, one has $\alpha_3(U_6) = \alpha_5(U_6) = 0$. So, we do not reach a contradiction. We should find a large enough odd integer l such that, $\alpha_l(U_6) = 0$. But, this does not appear always possible.

References

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

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

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] L. H. Gallardo and O. Rahavandrainy, *On even (unitary) perfect polynomials over $\mathbb{F}_2$*, Finite Fields Appl. **18** (2012), 920–932.

[9] L. H. Gallardo and O. Rahavandrainy, *Characterization of Sporadic perfect polynomials over $\mathbb{F}_2$*, Functiones et Approx. **55**(1) (2016), 7–21.

[10] L. H. Gallardo and O. Rahavandrainy, *On Mersenne polynomials over $\mathbb{F}_2$*, Finite Fields Appl. **59** (2019), 284–296.

[11] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its applications*, Cambridge University Press, 1983 (Reprinted 1987).

[12] O. Rahavandrainy, *Familles de polynômes unitairement parfaits sur $\mathbb{F}_2$*, C. R. Math. Acad. Sci. Paris **359,2** (2021), 123–130.

[1]Univ. Brest
Laboratoire de Mathématiques de Bretagne Atlantique,
UMR CNRS 6205,
6, Av. Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France.
Email address: luis.gallardo@univ-brest.fr
Email address: olivier.rahavandrainy@univ-brest.fr