On (unitary) perfect polynomials over $\mathbb{F}_2$ with only Mersenne primes as odd divisors

Gallardo Luis H. - Rahavandrainy Olivier

Université de Brest, UMR CNRS 6205

Laboratoire de Mathématiques de Bretagne Atlantique

e-mail : luisgall@univ-brest.fr - rahavand@univ-brest.fr

August 2, 2019

1

Abstract

The only (unitary) perfect polynomials over $\mathbb{F}_2$ that are products of x, $x+1$ and 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. Other consequences of such a factorization are new results about odd perfect polynomials.

1 Introduction

Let $A \in \mathbb{F}_2[x]$ be a nonzero polynomial. We say that A is *even* if it has a linear factor and that it is *odd* otherwise. We define a *Mersenne prime* (polynomial) over $\mathbb{F}_2$ as an irreducible polynomial of the form $1 + x^a(x+1)^b$, for some positive integers a, b. This comes as an analogue of the prime factors of the even perfect numbers. As over the integers, we say that a divisor d of A is *unitary* if $\gcd(d, \dfrac{A}{d}) = 1$. Let $\omega(A)$ denote the number of distinct irreducible (or *prime*) factors of A over $\mathbb{F}_2$ and let $\sigma(A)$ (resp. $\sigma^*(A)$) denote the sum of all (unitary) divisors of A (both σ and σ^* are multiplicative functions). If $\sigma(A) = A$ (resp. $\sigma^*(A) = A$), then we say that A is (unitary) *perfect*. Finally, we say that a (unitary) perfect polynomial is *indecomposable* if it is not a product of two coprime nonconstant (unitary) perfect polynomials.

The notion of (unitary) perfect polynomials is introduced in [3] (a simplified version of this Ph. D. thesis under Carlitz) by E. F. Canaday in 1941 and extended by J. T. B. Beard Jr. et al. (probably still inspired by Carlitz that advised the advisor of Beard) in several directions ([1], [2]). Later research in the subject ([4], [5], [6], [7], [8]) allows us to more precisely describe such polynomials. For the perfect case, we get:
- the "trivial" ones, of the form $(x^2 + x)^{2^n-1}$, for some positive integer n,
- nine others which are the unique even all whose odd factors are Mersenne primes raised to powers of the form $2^n - 1$ ([9], Theorem 1.1),
- and the last two which are divisible by a non Mersenne prime.
By analogy, since we can also consider perfect polynomials, $A \in \mathbb{F}_2[x]$ with $\sigma(A)/A = 1$, as an analogue of multiperfect numbers, $n \in \mathbb{N}^*$ avec $\sigma(n)/n \in \mathbb{N}^*$, it might have some interest to observe that most known multiperfect numbers (see OEIS sequence A007691) appear to be divisible by a Fermat

2

prime or by a Mersenne prime.

Obviously, all unitary perfect polynomials are even. We prove for the unitary case that essentially, the known ones belong to the nine "classes" relative to the equivalence relation : two unitary perfect polynomials are equivalent if and only if some power of 2 of one equals some power of 2 of the other (see below).

The paper consists of two major results that we describe now. The most important is Theorem 1.2 that improves significantly on these results (because, now there are no conditions on the powers of the M_j's). Its proof is obtained from new results given in Theorem 1.4 which in turn, extends recent non-trivial results in [11, Theorem 1.4].

We began to study odd perfect polynomials in [4]. They are all squares [3] and must have [5] at least five distinct prime divisors. We have also considered [4] "special perfect" polynomials which are of the form $S = P_1^2 \cdots P_m^2$, with each P_j odd and irreducible. We proved [4] that if such a polynomial S is perfect, then $\omega(S) \geq 10$, $\min_j \deg(P_j) \geq 30$ and $P_j \equiv 1 \mod x^2 + x + 1$. We get a new result for them as well as a new result about the existence of more general odd perfect polynomials, in Theorem 1.3, as a consequence of Theorem 1.4.

Observe that Theorem 1.4 is a new step on the proof of a Conjecture about Mersenne primes that is discussed in the recent paper [11].

It is convenient to fix some notations:

(a) For $S \in \mathbb{F}_2[x]$, we denote by $\overline{S}$ the polynomial obtained from S with x replaced by $x + 1$: $\overline{S}(x) = S(x + 1)$.

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

(c) To avoid trivialities, we suppose that any (unitary) perfect polynomial is indecomposable.

Notations 1.1.
Set $M_j := 1 + x(x + 1)^j, j \in \{1, 2, 3\}$, $\mathcal{M} := \{M_1, M_2, \overline{M_2}, M_3, \overline{M_3}\}$,

$\mathcal{P} := \{T_1, \ldots, T_9\}$ *and* $\mathcal{P}_u := \{U_1, \ldots, U_9\}$ *where:*

$T_1 = x^2(x+1)M_1, T_2 = \overline{T_1},$
$T_3 = x^4(x+1)^3 M_3, T_4 = \overline{T_3}, \; T_5 = x^4(x+1)^4 M_3 \overline{M_3} = \overline{T_5},$
$T_6 = x^6(x+1)^3 M_2 \overline{M_2}, T_7 = \overline{T_6},$
$T_8 = x^4(x+1)^6 M_2 \overline{M_2} M_3 \; and \; T_9 = \overline{T_8},$
$U_1 = x^3(x+1)^3 M_1^2, \; U_2 = x^3(x+1)^2 M_1, \; U_3 = x^5(x+1)^4 M_3,$
$U_4 = x^7(x+1)^4 M_2 \overline{M_2}, \; U_5 = x^5(x+1)^6 M_1^2 M_3, \; U_6 = x^5(x+1)^5 M_3 \overline{M_3},$
$U_7 = x^7(x+1)^7 M_2^2 \overline{M_2}^2, \; U_8 = x^7(x+1)^6 M_1^2 M_2 \overline{M_2}, \; U_9 = x^7(x+1)^5 M_2 \overline{M_2} \, \overline{M_3}.$

The nine nontrivial perfect polynomials cited above are: $T_1, \ldots, T_9$ *and the two others are:* $T_{10} = x^2(x+1)(x^4+x+1)M_1{}^2, \; T_{11} = \overline{T_{10}}.$
The known unitary perfects are all of the form B^{2^n}, *where* $n \in \mathbb{N}$ *and* $B \in \{U_1, \ldots, U_9\}$.

Our results are:

Theorem 1.2. *Let* $A = x^a(x+1)^b \prod_i P_i^{h_i} \in \mathbb{F}_2[x]$ *with each* P_i *Mersenne prime and* $h_i \in \mathbb{N}^*$. *Then* A *is even (unitary) perfect if and only if* $A \in \mathcal{P}$ *(resp.* $A = B^{2^n}$ *with* $n \in \mathbb{N}$ *and* $B \in \mathcal{P}_u$*).*

Theorem 1.3. *i) There exists no special perfect polynomial divisible only by Mersenne primes.*
ii) If $A = P_1^{2h_1} \cdots P_m^{2h_m}$, *where each* P_j *is a Mersenne prime and if for some* j, $2h_j + 1$ *is divisible by a Mersenne prime* $\neq 7$ *or by a Fermat prime* $\neq 5$, *then* A *is not perfect.*

Theorem 1.4. *Let* h *be a positive integer and* $M \in \mathbb{F}_2[x]$ *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, *where* $(p \neq 7$ *is a Mersenne number) or (the order of* 2 *modulo* p *is divisible by* 8 *(in particular, when* p *is a Fermat prime greater than* 5*)).*

2   Proofs of Theorems 1.2 and 1.3

Sufficiency in Theorem 1.2 is obtained by direct computations. For the necessity, we shall apply Lemmas 2.3 and 2.9, Propositions 2.7 and 2.10. We use Theorem 1.4 to prove these two propositions. A similar method gives

Theorem 1.3. We recall below [11, Theorem 1.4] which partially solves [9, Conjecture 5.2] about the factorization of $\sigma(M^{2h})$:

Conjecture 2.1 (Conjecture 5.2 in [9]). *Let $h \in \mathbb{N}^*$ and M be a Mersenne prime over $\mathbb{F}_2$ such that $M \notin \{M_2, \overline{M_2}\}$. Then, the polynomial $\sigma(M^{2h})$ is divisible by a non Mersenne prime.*

Lemma 2.2 (Theorem 1.4 in [11]). *Let $h \in \mathbb{N}^*$ such that $p = 2h+1$ is prime, M a Mersenne prime such that $M \notin \{M_2, \overline{M_2}\}$ and $\omega(\sigma(M^{2h})) = 2$. Then, $\sigma(M^{2h})$ is divisible by a non Mersenne prime.*

2.1 Proof of Theorem 1.2

We set $A := x^a (x+1)^b \prod_{i \in I} P_i^{h_i} = A_1 A_2 \in \mathbb{F}_2[x]$, 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 $A_2 = \prod_{P_j \notin \mathcal{M}} P_j^{h_j}$.

We suppose that A is indecomposable (unitary) perfect.

2.1.1 Case of perfect polynomials

Lemma 2.3 (Theorem 1.1 in [9]). *If $h_i = 2^{n_i} - 1$ for any $i \in I$, then $A \in \mathcal{P}$.*

We get from Theorem 8 in [3] and from Theorem 1.4:

Lemma 2.4. *i) If $\sigma(x^a)$ is divisible only by Mersenne primes, then $a \in \{2, 4, 6\}$ and all its divisors lie in $\mathcal{M}$.*
ii) Let $M \in \mathcal{M}$ such that $\sigma(M^a)$ is divisible only by Mersenne primes, then $a = 2$ and $M \in \{M_2, \overline{M_2}\}$.

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. We apply Lemma 2.4. If P divides $\sigma(x^a) \cdot \sigma((x+1)^b)$, then $P \in \mathcal{M}$. If P divides $\sigma(P_i^{h_i})$ with $P_i \in \mathcal{M}$, then $P_i \in \{M_2, \overline{M_2}\}$ and $P, \overline{P} \in \{M_1, M_3\}$. $\qquad\square$

Lemma 2.6. *i) For any $P_j \notin \mathcal{M}$, one has: $\gcd(P_j^{h_j}, \sigma(A_1)) = 1$ and $h_j = 0$.*
ii) $A = A_1$.

Proof. i): 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 from the indecomposibility of A.

ii) follows from i). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Proposition 2.7. *If A_1 is perfect, then $h_j = 2^{n_j} - 1$ for any $P_j \in \mathcal{M}$.*

Proof. 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 Q. So, we get the contradiction: $Q \mid A$. If $hj = 2^{n_j}u_j - 1$ with $u_j \geq 3$ odd, then $\sigma(P_j^{h_j}) = (1+P_j)^{2^{n_j}-1} \cdot (1+P_j+\cdots+P_j^{u_j-1})^{2^{n_j}}$ is also divisible by a non Mersenne prime, which is impossible.

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), then $a, b \in \{7 \cdot 2^n - 1 : n \geq 0\}$. Thus, for some $\nu \in \mathbb{N}^*$, $M_1^{2^\nu}$ divides $\sigma(A) = A$. It is impossible by the part i) of our proof. $\qquad\qquad\square$

Lemma 2.6, Proposition 2.7 and Lemma 2.3 imply

Corollary 2.8. *One has: $A = A_1 \in \mathcal{P}$.*

2.1.2 Case of unitary perfect polynomials

Similar proofs give Proposition 2.10 and thus, our result.

Lemma 2.9 (Theorem 1.3 in [9]). *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 2.10. *i) If A_1 is unitary perfect then $h_j = 2^{n_j}$ for any $P_j \in \mathcal{M}$. ii) $A = A_1$.*

Remark 2.11. Contrary to our proofs in the present paper, the proofs of [9, Corollaries 5.3 and 5.4] are not complete, since the special case where $\gcd(M_2\overline{M_2}, A) \neq 1$ was not considered.

2.2 Proof of Theorem 1.3

We also use in this proof Lemma 2.2 and Theorem 1.4.

If $S = P_1^2 \cdots P_m^2$ is perfect, where each P_j is Mersenne, then $\sigma(P_1^2) \cdots \sigma(P_m^2) = \sigma(S) = S = P_1^2 \cdots P_m^2$. We must have: $\sigma(P_1^2) = \prod_k Q_k$. Thus, $P_1 \in \{M_2, \overline{M_2}\}$

and any $Q_k \in \{M_1, M_3, \overline{M_3}\}$. But, for any $T \in \{M_1, M_3, \overline{M_3}\}$, $\sigma(T^2)$ and thus S is divisible by a non Mersenne prime, which is impossible.

We get in the same manner the part ii) of the theorem.

3 Proof of Theorem 1.4

We mainly prove Theorem 1.4 by contradiction (to Corollary 3.5). Lemma 3.2 states that $\sigma(M^{2h})$ is square-free for any $h \in \mathbb{N}^*$. We suppose that:

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

We set $U_{2h} := \sigma(\sigma(M^{2h}))$ and $M := x^a(x+1)^b + 1$, with M irreducible (so that $\gcd(a,b) = 1$, a or b is odd). We may assume that a is odd, without loss of generality.

3.1 Useful facts

Some of the following results are obvious or cited in [11], so we omit their proofs. By Lemma 3.7, $\sigma(M^{2h})$ is divisible by a non Mersenne prime whenever $\sigma(M^{p-1})$ is too, for some prime divisor p of $2h+1$.

Lemma 3.1. *For $m \in \mathbb{N}^*$, denote, as usual, by $N_2(m)$ the number of irreducible polynomials of degree m, over $\mathbb{F}_2$. Then*
i) $N_2(m) \geq [2^m - 2(2^{m/2} - 1)]/m$.
ii) $\varphi(m) < N_2(m)$ if $m \geq 4$, where φ is the Euler totient function.
iii) There exists at least one irreducible polynomial of degree m which is not a Mersenne prime, if $m \geq 4$.

Proof. i): See Exercise 3.27, p. 142 in [12].
ii): We get by direct computations, $m < (2^m - 2(2^{m/2} - 1))/m$ for $4 \leq m \leq 5$ and by studying the function $f(x) = 2^x - 2(2^{x/2} - 1) - x^2$, for $x \geq 6$. So, $\varphi(m) \leq m < N_2(m)$.
iii): First, $1 + x^c(x+1)^d$ Mersenne prime implies that $\gcd(c, c+d) = \gcd(c, d) = 1$. Moreover, the set $\mathcal{M}_m$ of Mersenne primes of degree m is a subset of $\Sigma_m := \{x^c(x+1)^{m-c} + 1 : 1 \leq c \leq m, \ \gcd(c, m) = 1\}$, Thus,

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

Therefore, there exist at most $\varphi(m)$ Mersenne primes of degree m. So, we get iii). $\square$

Lemma 3.2. *i) $\sigma(M^{2h})$ is square-free and reducible.*
ii) $a \geq 2$ or $b \geq 2$ so that $M \neq M_1$.

Notation 3.3. For a nonconstant polynomial S of degree s, we denote by $\alpha_l(S)$ the coefficient of x^{s-l} in S, $0 \leq l \leq s$. One has: $\alpha_0(S) = 1$.

We sometimes apply Lemmas 3.4 and 3.6 without explicit mentions.

Lemma 3.4. *Let $S \in \mathbb{F}_2[x]$ of degree $s \geq 1$ and $l, t, r, r_1, \ldots, r_k \in \mathbb{N}$ 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 no irreducible polynomial of degree at most r divides S.

Proof. i): Obvious, by definition of α_l.
ii) Follows from the fact: $\sigma(S) = S + T$, where $\deg(T) \leq \deg(S) - r - 1$. $\square$

Corollary 3.5. *i) The integers $u = \sum_{j \in J} a_j$ and $v = \sum_{j \in J} b_j$ are both even.*

ii) U_{2h} splits (over $\mathbb{F}_2$).
iii) U_{2h} is a square so that $\alpha_k(U_{2h}) = 0$ for any odd positive integer k.

Proof. i): See [11, Corollary 4.9].
ii) and iii): Assumption (1) implies that

$$U_{2h} = \sigma(\sigma(M^{2h})) = \sigma(\prod_{j \in J} P_j) = \prod_{j \in J} x^{a_j}(x+1)^{b_j} = x^u(x+1)^v,$$

with u and v both even. $\square$

Lemma 3.6. *One has modulo 2: $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h})$ if $1 \leq l \leq a+b-1$, $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h} + M^{2h-1})$ 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 3.4-ii) implies that $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h})$ if $1 \leq l \leq a+b-1$ and $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h} + M^{2h-1})$ if $a+b \leq l \leq 2(a+b) - 1$. $\square$

Lemma below (with analogous proof) is a generalization of Lemma 4.10 in [11].

Lemma 3.7. *If k divides $2h+1$ (with k prime or not), then $\sigma(M^{k-1})$ divides $\sigma(M^{2h})$.*

We fix a prime factor p of $2h + 1$. We denote by $ord_p(2)$ the order of 2 in $\mathbb{F}_p \setminus \{0\}$.

Lemma 3.8. *For any $j \in J$, $ord_p(2)$ divides $a_j + b_j = \deg(P_j)$.*

Proof. Let $d = \gcd_i(a_i + b_i)$. By Lemma 4.13 in [11], p divides $2^d - 1$. Thus, $ord_p(2)$ divides d. $\qquad\square$

Lemma 3.9. *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*
i) any irreducible polynomial (Mersenne or not) of degree $a_i + b_i$ divides $\sigma(M^{p-1})$.
ii) $\sigma(M^{p-1})$ is divisible by a non Mersenne prime if $a_i + b_i \geq 4$.

Proof. First, P_i is a primitive polynomial. Let α be a root of P_i. One has $M(\alpha)^p = 1$, $M(\alpha) = \alpha^r$ 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 $p_i = p$.
i): If P is an irreducible polynomial of degree $a_i + b_i$, then P is primitive. Let β be a root of P. One has $ord(\beta) = p_i = p$, $P(\beta) = 0$ and $M(\beta) = \beta^s$, for some $1 \leq s \leq p_i - 1$. Thus, $M(\beta)^p = \beta^{ps} = 1$.
ii) follows from i) and from Lemma 3.1-iii). $\qquad\square$

Corollary 3.10. *For any $i \in J$, $a_i + b_i \leq 3$ or $2^{a_i+b_i} - 1$ is not prime.*

Lemma 3.11. *Let $P, Q \in \mathbb{F}_2[x]$ 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. Let β be a root of P. β is primitive, $ord(\beta) = 2^r - 1$, $Q(\beta) \notin \{0, 1\}$ 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 $2^r - 1 = p$. $\qquad\square$

Corollary 3.12. *Let $r \in \mathbb{N}^*$ 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 divides $\sigma(M^{p-1})$ with $\deg(P) = r$, then P divides $M^p + 1$ and by taking $Q = M$ in the above lemma, we get a contradiction. $\qquad\square$

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

Lemma 3.13. *Let $P, Q \in \mathbb{F}_2[x]$ such that P is irreducible of degree m and $P \nmid Q(Q+1)$. Then, P divides $Q^p + 1$.*

Proof. Let β be a root of P. P and β are primitive, $ord(\beta) = 2^m - 1 = p$, $Q(\beta) \notin \{0, 1\}$. Thus, $Q(\beta) = \beta^t$ for some $1 \le t \le p - 1$. Hence, $Q(\beta)^p = \beta^{tp} = 1$. So, P divides $Q^p + 1$. $\square$

Corollary 3.14. *Any irreducible polynomial $P \ne M$ (Mersenne or not), of degree m, divides $\sigma(M^{p-1})$.*

Proof. P does not divide $x^a(x + 1)^b M = M(M + 1) = Q(Q + 1)$. So, we apply Lemma 3.13 to $Q = M$. $\square$

Corollary 3.15. *The polynomial $1 + x + x^2$ divides $\sigma(M^{p-1})$ if and only if $(M \ne 1 + x + x^2$ and $p = 3)$,*
$1 + x^2 + x^3$ divides $\sigma(M^{p-1})$ if and only if $M \ne 1 + x^2 + x^3$ and $p = 7$,
$1 + x + x^3$ divides $\sigma(M^{p-1})$ if and only if $M \ne 1 + x + x^3$ and $p = 7$.

Proof. Apply Corollary 3.14 with $m \in \{2, 3\}$. $\square$

3.2 Case $M \in \{M_1, M_3, \overline{M_3}\}$

Lemma 3.2 implies that $M \ne M_1$. It suffices to suppose that $M = M_3$.

We refer to Section 5.2 in [10]. Put $U := M_1 M_2 \overline{M_2}$. By [10, Lemma 5.4], we have to consider four cases:
i) $\gcd(\sigma(M^{2h}), U) = 1$,
ii) $\sigma(M^{2h}) = M_1 B$, with $\gcd(B, U) = 1$,
iii) $\sigma(M^{2h}) = M_2 \overline{M_2} B$, with $\gcd(B, U) = 1$,
iv) $\sigma(M^{2h}) = UB$, with $\gcd(B, U) = 1$,
where any irreducible divisor of B has degree exceeding 5.
We get Lemma below which contradicts the fact that U_{2h} is a square.

Lemma 3.16. $\alpha_3(U_{2h}) = 1$ *or* $\alpha_5(U_{2h}) = 1$.

Proof. For i), iii) and iv) : use Lemmas 5.9, 5.10, 5.15, 5.17 (still in [10]). For ii): since $\sigma(M^{2h}) = (x^2 + x + 1)B$ and $U_{2h} = (x^2 + x)\sigma(B)$, we obtain (by Lemmas 3.4 and 3.6):

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

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

3.3 Case where $M \in \{M_2, \overline{M_2}\}$ and $h \geq 2$

It suffices to consider $M = M_2 = 1 + x + x^3$. Recall that $U_{2h} = \sigma(\sigma(M^{2h}))$ splits and it is a square. Note also that if $h = 1$, then $\sigma(M_2^{2h}) = \sigma(M_2^2) = M_1 M_3$.

For $h \in \{2, 3\}$, we get 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 (even if U_6 is a square).

So, $h \geq 4$.

Lemma 3.17. *i)* $1 + x + x^2$ *divides* $\sigma(M^{2h})$ *if and only if* 3 *divides* $2h + 1$.
ii) $1 + x^2 + x^3$ *divides* $\sigma(M^{2h})$ *if and only if* 7 *divides* $2h + 1$.
iii) Any irreducible divisor of $\sigma(M^{2h})$ *is of degree at least* 4, *if* $2h + 1$ *is divisible by a prime* $p \notin \{3, 7\}$.

Proof. i) and ii): from Corollaries 3.12 and 3.14.
iii) follows from i) and ii). $\qquad\square$

3.3.1 Case where $2h + 1$ is divisible by a prime $p \notin \{3, 7\}$

By Lemma 3.7, $\sigma(M^{p-1})$ divides $\sigma(M^{2h})$. So, we may suppose that $2h+1 = p$ so that $2h = p - 1$. It suffices then to prove (directly or by a contradiction) that $\sigma(M^{2h})$ is divisible by a non Mersenne prime.

Lemma 3.18. *i)* $\alpha_l(U_{2h}) = \alpha_l(\sigma(M^{2h}))$ *for* $l \in \{1, 2, 3\}$.
ii) $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h})$ *for* $l \in \{1, 2\}$, $\alpha_3(\sigma(M^{2h})) = \alpha_3(M^{2h} + M^{2h-1})$.

Proof. i) follows from Lemma 3.17.
ii): for $l \leq 2$, one has: $6h - l = \deg(\sigma(M^{2h})) - l = \deg((M^{2h}) - l > 3(2h-1) = \deg(M^{2h-1})$ and for $3 \leq l \leq 5$, $6h - l > 3(2h - 2) = \deg(M^{2h-2})$. Hence, we get ii). $\qquad\square$

Corollary 3.19. $\alpha_3(U_{2h}) = 1$ *if* $h \geq 4$.

Proof. $\alpha_3(U_{2h}) = \alpha_3(M^{2h} + M^{2h-1}) = \alpha_3[(x^3 + x)M^{2h-1}] = \alpha_3(M^{2h-1}) + \alpha_1(M^{2h-1})$. But, $M^{2h-1} = (x^3+x+1)^{2h-1} = (x^3+x)^{2h-1} + (x^3+x)^{2h-2} + \cdots$ So, $\alpha_3(M^{2h-1})$ (resp. $\alpha_1(M^{2h-1})$) which is the coefficient of x^{6h-6} (resp. of x^{6h-4}) in M^{2h-1}, equals 1 (resp. 0). $\qquad\square$

3.3.2 Case where 7 divides $2h + 1$

In this case, by Lemma 3.7, $\sigma(M^6)$ divides $\sigma(M^{2h})$, where $\sigma(M^6) = (x^3 + x^2 + 1)(x^6 + x^5 + 1)(x^9 + x^7 + x^5 + x + 1)$ is divisible by the non Mersenne prime $x^9 + x^7 + x^5 + x + 1 = 1 + x(x+1)^2(x^3 + x + 1)^2$.

3.3.3 Case where 3 is the unique prime factor of $2h + 1$

In this case, $2h + 1 = 3^w$, with $w \geq 2$ because $2h + 1 \geq 9$. So, 9 divides $2h + 1$ and thus $\sigma(M^8)$ divides $\sigma(M^{2h})$ (by Lemma 3.7). We are done because $\sigma(M^8) = (x^2 + x + 1)(x^4 + x^3 + 1)(x^6 + x + 1)(x^{12} + x^8 + x^7 + x^4 + 1)$, where $x^6 + x + 1 = 1 + x(x + 1)M_3$ is not a Mersenne prime.

3.4 Case where $M \notin \mathcal{M}$ and $2h + 1$ is divisible by a Mersenne prime number $p \neq 7$

Set $p := 2^m - 1$, where m and p are both prime. We shall prove that $\sigma(M^{p-1})$ is divisible by a non Mersenne prime. Note that there are (at present) "only" 51 known Mersenne prime numbers (OEIS Sequences A000043 and A000668). The first five of them are: $3, 7, 31, 127$ and 8191.

Here, $a + b = \deg(M) \geq 5$ since $M \notin \mathcal{M}$. Corollary 3.14 and Lemma 3.1-iii) imply that for $p \geq 31$, we get our result. It remains then the case $p = 3$ because $p \neq 7$.

Lemma 2.2 has already treated the case where $\omega(\sigma(M^2)) = 2$. So, we suppose that $\omega(\sigma(M^2)) \geq 3$. Put:

$$\sigma(M^2) = M_1 \cdots M_r, \ r \geq 3 \text{ and } W := U_4 = \sigma(\sigma(M^2)).$$

We get by Corollary 3.15:

Lemma 3.20. *i)* $1 + x + x^2$ *divides* $\sigma(M^2)$.
ii) No irreducible polynomial of degree $r \geq 3$ *such that* $2^r - 1$ *is prime divides* $\sigma(M^2)$.

Lemma 3.21. *Write* $\sigma(M^2) = M_1 B$ *where* $M_1 = 1 + x + x^2$, $\gcd(M_1, B) = 1$. *One has:*

$\quad$ *i)* $\alpha_1(\sigma(M^2)) = \alpha_1(B) + 1, \ \alpha_2(\sigma(M^2)) = \alpha_2(B) + \alpha_1(B) + 1,$
$\quad$ *ii)* $\alpha_3(\sigma(M^2)) = \alpha_3(B) + \alpha_2(B) + \alpha_1(B),$
$\quad$ *iii)* $\alpha_3(\sigma(M^2)) = 0.$

Proof. $\sigma(M^2) = M_1 B = (x^2 + x + 1)B$. So we directly get i) and ii).

iii): $\sigma(M^2) = 1 + M + M^2 = x^{2a}(x+1)^{2b} + x^a(x+1)^b + 1$.

$2a + 2b - 3 > a + b$ because $a + b \geq 4$ and $x^{2a}(x+1)^{2b}$ is a square. So, $\alpha_3(\sigma(M^2)) = \alpha_3(x^{2a}(x+1)^{2b}) = 0$. $\qquad\square$

Lemma 3.22. *One has:*

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

Proof. $W = \sigma(\sigma(M^2)) = \sigma(M_1 B) = \sigma(M_1)\sigma(B) = (x^2 + x)\sigma(B)$.

Moreover, 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:

$$\alpha_1(W) = \alpha_1(\sigma(B)) + 1 = \alpha_1(B) + 1,$$
$$\alpha_2(W) = \alpha_2(\sigma(B)) + \alpha_1(\sigma(B)) = \alpha_2(B) + \alpha_1(B),$$

and $\alpha_3(W) = \alpha_3(\sigma(B)) + \alpha_2(\sigma(B)) = \alpha_3(B) + \alpha_2(B)$. $\qquad\square$

Corollary below contradicts the fact that W is a square and finishes the proof for $p = 3$.

Corollary 3.23. $\alpha_3(W) = 1$.

Proof. W is a square, so $0 = \alpha_1(W) = \alpha_1(B) + 1$ and thus $\alpha_1(B) = 1$.

Lemma 3.21-iii) implies that $0 = \alpha_3(\sigma(M^2)) = \alpha_3(B) + \alpha_2(B) + \alpha_1(B)$.

Therefore, we get: $\alpha_3(W) = \alpha_3(B) + \alpha_2(B) = \alpha_1(B) = 1$. $\qquad\square$

Remark 3.24. Our method fails for $p = 7$. Indeed, for many M's, one has $\alpha_3(W) = \alpha_5(W) = 0$ so that we do not reach a contradiction. We should find a large enough odd integer l such that $\alpha_l(W) = 0$. But, this does not appear always possible.

3.5 Case where $M \notin \mathcal{M}$ and $2h + 1$ is divisible by a prime p with $ord_p(2) \equiv 0 \mod 8$

Lemmas 3.25 and 3.8 imply Corollary 3.26.

Lemma 3.25. *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 [11, Corollary 3.3]. $\qquad\square$

Corollary 3.26. *If $2h+1$ is divisible by a prime p such that 8 divides $ord_p(2)$ (in particular, when $p > 5$ is a Fermat prime), then $\sigma(M^{2h})$ is divisible by a non Mersenne prime.*

Proof. If not, Lemma 3.8 implies that $ord_p(2)$ divides $\deg(P_j)$, for any $j \in J$. So, we get a contradiction to Lemma 3.25: 8 divides $\deg(P_j)$.
In particular, if $p = 2^{2^w} + 1$, with $w \geq 2$, then $ord_p(2) = 2^{w+1}$ which is divisible by 8. $\qquad\square$

Remarks 3.27. i) If p is a Fermat prime, then $ord_p(2) \equiv 0 \mod 8$. The converse is false. Examples: $p \in \{97, 673\}$ with $ord_p(2) = 48$.
ii) It remains the following (large) case to complete the proof of Conjecture 2.1: $M \notin \mathcal{M}$ and $2h+1$ is divisible by $p \in \{5, 7\}$ or by $p > 7$ which is neither Mersenne prime nor Fermat prime.
Moreover, assuming Conjecture 2.1, similar proofs as in Section 2.1.1 would state that there exists no odd perfect polynomial over $\mathbb{F}_2$ which is only divisible by Mersenne primes.

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, J. R. OCONNELL JR, K. I. WEST, *Perfect polynomials over $GF(q)$*, Rend. Accad. Lincei **62** (1977), 283–291.

[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, *Odd perfect polynomials over $\mathbb{F}_2$*, J. Théor. Nombres Bordeaux **19** (2007), 165–174.

[5] L. H. GALLARDO, 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.

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

[10] L. H. GALLARDO, O. RAHAVANDRAINY, *Characterization of Sporadic perfect polynomials over* $\mathbb{F}_2$, Functiones et Approx. **55.1** (2016), 7–21.

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

[12] R. LIDL, H. NIEDERREITER, *Finite Fields, Encyclopedia of Mathematics and its applications*, Cambridge University Press, 1983 (Reprinted 1987).