Functiones et Approximatio
55.1 (2016), 7–21
doi: 10.7169/facm/2016.55.1.1

CHARACTERIZATION OF SPORADIC PERFECT POLYNOMIALS OVER $\mathbb{F}_2$

Luis H. Gallardo, Olivier Rahavandrainy

Abstract: We complete, in this paper, the characterization of all known even perfect polynomials over the prime field $\mathbb{F}_2$. In particular, we prove that the last two of the eleven known "sporadic" perfect polynomials over $\mathbb{F}_2$ are the unique of them of the form $x^a(x+1)^b M^{2h}\sigma(M^{2h})$, where M is a Mersenne prime and $a, b, h \in \mathbb{N}^*$.

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

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 it is *odd* otherwise. We define a *Mersenne polynomial* over $\mathbb{F}_2$ as a polynomial of the form $1 + x^a(x+1)^b$, for some positive integers a, b. If such a polynomial is irreducible, we say that it is a *Mersenne prime*.

Let $\omega(A)$ denote the number of distinct irreducible (or *prime*) factors of A over $\mathbb{F}_2$ and let $\sigma(A)$ denote the sum of all divisors of A (σ is a multiplicative function). If $\sigma(A) = A$, then we say that A is a *perfect* polynomial. The notion of perfect polynomials is introduced ([3]) by E.F. Canaday in 1941 and extended by J.T.B. Beard Jr. et al. in several directions ([1], [2]). We are interested in this subject since a few years and have obtained some results ([4], [5], [6], [7], [8]).

If $A \in \mathbb{F}_2[x]$ is nonconstant and perfect, then $\omega(A) \geqslant 2$ (Lemma 2.1). Moreover ([3]), the only perfect polynomials A over $\mathbb{F}_2$ with $\omega(A) = 2$ are those of the form $(x^2+x)^{2^n-1}$, for some positive integer n. We call them "trivial" perfect. Contrary to the integer case in which any even perfect number has exactly two distinct prime factors, we do not know the value of $\omega(A)$ for a non-trivial even perfect polynomial $A \in \mathbb{F}_2[x]$. We are unable to describe a general form of such polynomials in terms of Mersenne primes. However, as discussed below, with only two exceptions, all known non-trivial even perfect polynomials have factorizations with Mersenne primes as odd divisors.

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

In the rest of the paper:

(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) We denote by α a root of the irreducible polynomial x^2+x+1 in a fixed algebraic closure of $\mathbb{F}_2$. In other words: $\mathbb{F}_4 := \mathbb{F}_2[\alpha]$, where $\mathbb{F}_4$ is the finite field with 4 elements.

Remark 1.1. In other words, for any $S \in \mathbb{F}_2[x]$, one has

$$S(\alpha) \neq 0 \iff \gcd(S(x), x^2+x+1) = 1.$$

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

We proved ([5], [6]) that any nonconstant and non-trivial perfect polynomial $A \in \mathbb{F}_2[x]$ with $\omega(A) \leqslant 4$ is even and takes one of the following forms:

$$T_1 = x^2(x+1)M_1, \qquad T_2 = \overline{T}_1, \qquad T_3 = x^4(x+1)^3M_3, \qquad T_4 = \overline{T}_3,$$
$$C_1 = x^2(x+1)(x^4+x+1){M_1}^2, \qquad C_2 = \overline{C}_1, \qquad C_3 = x^4(x+1)^4M_3\overline{M_3} = \overline{C}_3,$$
$$C_4 = x^6(x+1)^3M_2\overline{M_2}, \qquad C_5 = \overline{C}_4,$$

where $M_j = 1 + x(x+1)^j, j = 1, 2, 3$.

Moreover, there are only two more known even perfect polynomials with five prime factors: $S_1 = x^4(x+1)^6M_2\overline{M_2}M_3$ and $S_2 = \overline{S}_1$.

These eleven polynomials are the only known non-trivial perfect polynomials over $\mathbb{F}_2$. We call them "sporadic" perfect.

We immediately remark that, except for C_1 and C_2, all of them are of the form $x^a(x+1)^bP_1 \cdots P_r$ where $a, b \in \mathbb{N}^*$ and each P_j is a Mersenne prime. These two exceptions C_1, C_2 show that contrary to the case of integers, there exist even perfect polynomials over $\mathbb{F}_2$ which are divisible by a non Mersenne prime. We showed ([9], Theorem 1.1) that these nine known polynomials are the unique perfect polynomials that have factorizations involving Mersenne primes as odd prime divisors raised to powers of the form 2^n-1. We want to better understand the factorisation of the last two sporadic perfect polynomials C_1 and C_2. We obviously see that $C_1 = x^2(x+1){M_1}^2\sigma({M_1}^2)$ and $C_2 = x(x+1)^2{M_1}^2\sigma({M_1}^2)$. So, it is natural to think of perfect polynomials of the form $x^a(x+1)^bM^{2h}\sigma(M^{2h})$, where M is a Mersenne prime and $a, b, h \in \mathbb{N}^*$. Proposition 3.5 implies that, in this case, $M \in \{M_1, M_3\}$ and the polynomial $\sigma(\sigma(M^{2h}))$ must be of the form $x^u(x+1)^vM^w$, for some $u, v, w \in \mathbb{N}^*$. Theorem 1.3 shows that $M \neq M_3$.

In this paper, we characterize in Theorem 1.4 (with the help of Theorems 1.2 and 1.3) the polynomials C_1 and C_2, as the unique perfect polynomials that are of the form $x^a(x+1)^bM^{2h}\sigma(M^{2h})$, where M is a Mersenne prime.

Theorem 1.2. *If $M = 1+x+x^2$ and if $\sigma(\sigma(M^{2h})) = x^u(x+1)^vM^w$, then $u = v$ and w is odd. Moreover, if $u = v = 1$, then $w = h = 1$.*

Theorem 1.3. *If $M = 1+x+\cdots+x^4$, then for any $a, b, h \in \mathbb{N}^*$, there exists no perfect polynomial over $\mathbb{F}_2$ of the form $x^a(x+1)^bM^{2h}\sigma(M^{2h})$.*

Theorem 1.4. *Let $A = x^a(x+1)^b M^{2h}\sigma(M^{2h})$ be an even polynomial over $\mathbb{F}_2$, where M is a Mersenne prime and $h \in \mathbb{N}^*$. Then A is perfect if and only if $M = x^2+x+1$, $h = 1$ and $(a,b) \in \{(1,2),(2,1)\}$ so that $\{A, \overline{A}\} = \{C_1, C_2\}$.*

2. Preliminaries

Some of the following results are obvious or well known, so we omit their proofs.

Lemma 2.1 ([4, Lemma 2.3]). *If $A = P_1^{h_1} \cdots P_r^{h_r} Q_1^{k_1} \cdots Q_s^{k_s}$ is a nonconstant perfect polynomial over $\mathbb{F}_2$ such that:*

$$\begin{cases} P_1, \ldots, P_r, Q_1, \ldots, Q_s \ \text{ are distinct and irreducible,} \\ \deg(P_1) = \cdots = \deg(P_r) < \deg(Q_1) \leqslant \cdots \leqslant \deg(Q_s), \end{cases}$$

then r is even.

Lemma 2.2. *If $A = A_1A_2$ is perfect over $\mathbb{F}_2$ and if $\gcd(A_1, A_2) = 1$, then A_1 is perfect if and only if A_2 is perfect.*

Lemma 2.3. *If A is perfect over $\mathbb{F}_2$, then the polynomial $\overline{A}$ is also perfect over $\mathbb{F}_2$.*

Lemma 2.4. *If A is an odd perfect polynomial over $\mathbb{F}_2$, then A is a square.*

Lemma 2.5 ([3, Theorem 8]). *If any irreducible factor of $1 + x + \cdots + x^{2n}$ is of the form $x^a(x+1)^b + 1$, then $n \in \{1, 2, 3\}$.*

Lemma 2.6. *Let h be a positive integer and let $M \in \mathbb{F}_2[x]$ be a Mersenne prime. Then, $\sigma(x^{2h})$ and $\sigma(M^{2h})$ are both odd and squarefree.*

Proof. The facts: $\sigma(x^{2h})$ and $\sigma(M^{2h})$ are odd and $\sigma(x^{2h})$ is squarefree are immediate. Put $H = \sigma(M^{2h}) = M^{2h} + \cdots + M + 1$. By differentiating H, one has: $H' = M' \cdot (M^{h-1} + \cdots + M + 1)^2$.

We show that $\gcd(H, H') = 1$. Suppose that β is a common root of H and H' in a suitable field extension of $\mathbb{F}_2$. It is obvious that $M'(\beta) \neq 0$ since M' has at most two roots: $0, 1$ and $H(0) = H(1) = 1$.

Hence, β satisfies: $(M^{2h} + \cdots + M + 1)(\beta) = 0 = (M^{h-1} + \cdots + M + 1)(\beta)$. Thus, $0 = H(\beta) = (M^{2h} + (M^h + 1)(M^{h-1} + \cdots + M + 1))(\beta) = M^{2h}(\beta) + 0$. So $M(\beta) = 0$ and $0 = H(\beta) = 1$, which is impossible. ∎

Corollary 2.7. *Let $M \in \mathbb{F}_2[x]$ be a Mersenne prime such that $\sigma(\sigma(M^{2h})) = x^u(x+1)^v M^w$. Then, any irreducible divisor of $\sigma(M^{2h})$ is of the form $1 + x^{a_i}(x+1)^{b_i}$ or $1 + x^{c_i}(x+1)^{d_i}M^{e_i}$, for some positive integers a_i, b_i, c_i, d_i, e_i.*

Proof. Since $\sigma(M^{2h})$ is odd and squarefree, we get $\sigma(M^{2h}) = V_1 \cdots V_r$, where $r \in \mathbb{N}^*$ and each V_i is odd and irreducible. Hence, $x^u(x+1)^v M^w = \sigma(\sigma(M^{2h})) = (1+V_1)\cdots(1+V_r)$. Therefore, for any i, $1 + V_i$ is of the form $x^{a_i}(x+1)^{b_i}$ or $x^{c_i}(x+1)^{d_i}M^{e_i}$ for some $a_i, b_i, c_i, d_i, e_i \in \mathbb{N}$. The irreducibility of V_i and the fact that it is odd imply that a_i, b_i, c_i, d_i, e_i must be positive. ∎

Lemma 2.8. *[[10], Theorem 7)] Let $f \in \mathbb{F}_2[x]$ be a squarefree polynomial of degree n. Then*

i) *$f(1+x+x^2)$ is also squarefree.*
ii) *$\omega(f(1+x+x^2))$ is even if and only if $(-1)^n F(3,4) \equiv 1 \mod 8$, where $F(x,y)$ is the homogeneous lift of f to $\mathbb{Z}[x]$.*

Corollary 2.9. *If $M = x^2+x+1$, then for any $h \in \mathbb{N}^*$, the number $\omega(\sigma(M^{2h}))$ of irreducible divisors of $\sigma(M^{2h})$ is odd.*

Proof. Since the homogeneous lift of $\sigma(x^{2h})$ to $\mathbb{Z}[x]$ equals

$$F(x,y) = \frac{x^{2h+1} - y^{2h+1}}{x-y},$$

and $F(3,4) \equiv 5 \not\equiv 1 \pmod 8$ the assertion follows from Lemma 2.8-ii). ■

3. The proof of Theorem 1.4

We shall now show how our main result, Theorem 1.4, follows from Theorems 1.2 and 1.3. We start with a few technical lemmas.

3.1. Useful facts

Lemma 3.1. *Let $S \in \mathbb{F}_2[x]$ be irreducible such that $S = \overline{S}$ and $S(\alpha) \neq 0$, then $S(\alpha) = 1$ and x^2+x+1 divides $1+S$.*

Proof. Observe that from Remark 1.1 one has $\gcd(S(x), x^2+x+1) = 1$. Write $S(x) = Q(x)(x^2+x+1) + R(x)$ with $Q(x), R(x) \in \mathbb{F}_2[x]$ and $R(x) = a+bx \neq 0$. Thus, $a + b\alpha = S(\alpha) = S(\alpha+1) = a + b(\alpha+1)$. It follows that $b = 0$. Therefore $0 \neq S(\alpha) = a \in \mathbb{F}_2$. Thus, $a = 1$, thereby proving the first assertion. Since $(1+S)(\alpha) = 0$, $1+S(x)$ is divisible by the minimal polynomial of α over $\mathbb{F}_2$. In other words, x^2+x+1 divides $1+S(x)$. This completes the proof of the lemma. ■

Corollary 3.2. *Let $M = 1+x+x^2$, $h \in \mathbb{N}^*$ and $H = \sigma(M^{2h})$. Then there exists an irreducible divisor P of H such that $P = \overline{P}$ and $P(\alpha) = 1$.*

Proof. First, $H = \overline{H}$ because $M = \overline{M}$. By Lemma 2.6, $H = P_1 P_2 \cdots P_r$, where each P_j is irreducible. Since $H = \overline{H}$, one has: $P \mid H \Rightarrow \overline{P} \mid H$.

If for any j, $P_j \neq \overline{P_j}$, then we may write without loss of generality:

$$H = P_1 \overline{P_1} P_2 \overline{P_2} \cdots P_s \overline{P_s},$$

and $\omega(H) = 2s$, which contradicts Corollary 2.9. Moreover, any irreducible divisor P of $\sigma(H)$ is distinct from M and thus satisfies: $P(\alpha) \neq 0$. We get our corollary from Lemma 3.1. ■

Corollary 3.3. *For any $h \in \mathbb{N}^*$, $M = 1+x+x^2$ divides $\sigma(\sigma(M^{2h})) = \sigma(H)$.*

Proof. By Corollary 3.2, let P be irreducible such that $P\|H$ and $P = \overline{P}$. Then, $1 + P$ divides $\sigma(H)$, and from Lemma 3.1, M divides $1 + P$. ∎

Lemma 3.4. *If $M = x^2 + x + 1$ and if $T \in \mathbb{F}_2[x]$ are such that $T = \overline{T}$. Then*

i) *there exists $S \in \mathbb{F}_2[x]$ such that $T = S(M)$.*
ii) *$\overline{\sigma(T)} = \sigma(T)$.*
iii) *If $x^u\|T$ and $(x+1)^v\|T$, then $u = v$.*

Proof. i): By induction on the degree of T, we can prove that there exists $R \in \mathbb{F}_2[x]$ such that $T = R(x(x+1))$. It suffices then to take $S(x) = R(x+1)$.

ii) is immediate.

iii): Put $T = x^u(x+1)^vU$, where U is an odd polynomial. Since $\overline{T} = T$, one has: $x^v(x+1)^u\overline{U} = \overline{T} = T = x^u(x+1)^vU$. We are done. ∎

3.2. The proof

Assume, in this section, that the polynomial $A = x^a(x+1)^bM^{2h}\sigma(M^{2h})$ is perfect over $\mathbb{F}_2$, with M a Mersenne prime, $a, b, h \in \mathbb{N}^*$ and $a \leqslant b$. We set $M_1 = 1+x+x^2$ and $M_3 = 1 + x + \cdots + x^4$.

For $r \in \mathbb{N}$, put $U_{2h} = \sigma(\sigma(M^{2h}))$ and

$$S_{r,h} = x^{2^{r+1}}(x+1)^{2^{r+1}}M^{2h-2^{r+1}}, \quad T_{r,h} = x^{2^r}(x+1)^{2^r}M^{2h-2^r} \quad \text{if } M = M_1,$$
$$S_{r,h} = x^{3\cdot 2^r}(x+1)^{2^r}M^{2h-2^r}, \quad T_{r,h} = x^{2^r}(x+1)^{3\cdot 2^r}M^{2h-2^r} \quad \text{if } M = M_3.$$

Proposition 3.5.

i) *M divides at least one of $\sigma(x^a)$ and $\sigma((x+1)^b)$.*
ii) *One has either $M = M_1$ or $M = M_3$.*
iii) *If $M = M_1$, then for some $r \in \mathbb{N}$, we have ($a = b = 3 \cdot 2^r - 1$, $U_{2h} = S_{r,h}$) or ($a = 2 \cdot 2^r - 1$, $b = 3 \cdot 2^r - 1$, $U_{2h} = T_{r,h}$).*
iv) *If $M = M_3$ then $U_{2h} \in \{S_{r,h}, T_{r,h}\}$, for some $r \in \mathbb{N}$.*

Proof. i): Put $A = x^a(x+1)^bM^{2h}\sigma(M^{2h})$, $a + 1 = 2^su$ and $b + 1 = 2^rv$, with $s, r \geqslant 0$, u, v odd. One has:

$$\sigma(x^a) = 1 + x + \cdots + x^a = (1+x)^{2^s-1}(1 + x + \cdots + x^{u-1})^{2^s},$$
$$\sigma((x+1)^b) = x^{2^r-1}(1 + (x+1) + \cdots + (x+1)^{v-1})^{2^r}.$$

We remark that the four polynomials $x, x+1, M$ and $\sigma(M^{2h})$ are pairwise coprime. Hence, $\sigma(A) = \sigma(x^a)\ \sigma((x+1)^b)\ \sigma(M^{2h})\ \sigma(\sigma(M^{2h}))$.

Since A is perfect, we get

$$x^a(x+1)^bM^{2h}\sigma(M^{2h}) = \sigma(x^a)_\sigma((x+1)^b)\ \sigma(M^{2h})\ \sigma(\sigma(M^{2h})),$$

so that $x^a(x+1)^bM^{2h} = \sigma(x^a)\ \sigma((x+1)^b)\ \sigma(\sigma(M^{2h}))$.

If $M \nmid \sigma(x^a)$ and $M \nmid \sigma((x+1)^b)$, then M^{2h} divides $\sigma(\sigma(M^{2h}))$. Thus,

$$M^{2h} = \sigma(\sigma(M^{2h})), \quad M^{2h}\ \sigma(M^{2h}) \text{ is odd and perfect,}$$

which is impossible by Lemmas 2.4 and 2.6.

ii): If $M \mid \sigma(x^a)$, then $M = 1 + x + \cdots + x^{u-1}$. Hence, by Lemma 2.5, $u = 3$ or $u = 5$.

If $M \mid \sigma((x+1)^b)$, then as above: $M \in \{M_1, M_3\}$.

iii): From i), $M = M_1$ must divide at least one of $\sigma(x^a)$ and $\sigma((x+1)^b)$.

- If $M \mid \sigma(x^a)$ and $M \mid \sigma((x+1)^b)$, then $M = 1 + x + \cdots + x^{u-1} = 1 + (x+1) + \cdots + (x+1)^{v-1}$. Hence, $u = v = 3$. Thus, $s \leqslant r$, $2^r - 1 \leqslant a = 3 \cdot 2^s - 1$ and $2^s - 1 \leqslant b = 3 \cdot 2^r - 1$. It follows that $s \leqslant r \leqslant s+1$. We get $U_{2h} = S_{r,h}$ if $s = r$. If $r = s+1$, then
$$a = 3 \cdot 2^s - 1, \quad b = 6 \cdot 2^s - 1, \quad \sigma(\sigma(M^{2h})) = x^{2^s} \cdot (x+1)^{5 \cdot 2^s} \cdot M^{2h - 3 \cdot 2^s},$$
which is impossible by Lemma 3.4.
- If $M \mid \sigma(x^a)$ but $M \nmid \sigma((x+1)^b)$, then $u = 3, v = 1$. Thus, $2^r - 1 \leqslant a = 3 \cdot 2^s - 1 \leqslant b = 2^r - 1$ and $2^s - 1 \leqslant b = 2^r - 1$. So $r \leqslant s + 1 < r$, which is impossible.
- If $M \nmid \sigma(x^a)$ but $M \mid \sigma((x+1)^b)$, then $u = 1, v = 3$. Thus, $2^r - 1 \leqslant a = 2^s - 1 \leqslant b = 3 \cdot 2^r - 1$ and $2^s - 1 \leqslant b = 3 \cdot 2^r - 1$. So $r \leqslant s \leqslant r+1$. If $s = r$, then
$$a = 2^r - 1, \quad b = 3 \cdot 2^r - 1 \quad \text{and} \quad \sigma(\sigma(M^{2h})) = (x+1)^{2^{r+1}} \cdot M^{2h - 2^r},$$
which is impossible by Lemma 3.4. We get $U_{2h} = T_{r,h}$ if $s = r+1$.

iv): Now, we suppose that $M = M_3$.

- If $M \mid \sigma(x^a)$ and $M \mid \sigma((x+1)^b)$, then $M = 1 + x + \cdots + x^{u-1} = 1 + (x+1) + \cdots + (x+1)^{v-1}$, which is impossible.
- If $M \mid \sigma(x^a)$ but $M \nmid \sigma((x+1)^b)$, then $u = 5, v = 1$. Thus, $2^r - 1 \leqslant a = 5 \cdot 2^s - 1$ and $2^s - 1 \leqslant b = 2^r - 1$. So $s \leqslant r \leqslant s+2$.
  - If $r = s$, then
  $$x^a (x+1)^b M^{2h} = \sigma(x^a)\sigma((x+1)^b) U_{2h} = (x+1)^{2^s - 1} M^{2^s} x^{2^s - 1} U_{2h},$$
  so that $U_{2h} = x^{4 \cdot 2^s} M^{2h - 2^s}$. Hence, any irreducible divisor of $\sigma(M^{2h})$ is of the form $1 + x^c M^d$, which is impossible by Corollary 2.7.
  - If $r = s+1$, then
  $$a = 5 \cdot 2^s - 1, \quad b = 2 \cdot 2^s - 1, \quad U_{2h} = x^{3 \cdot 2^s} (x+1)^{2^s} M^{2h - 2^s} = S_{s,h}.$$
  - If $r = s+2$, then
  $$a = 5 \cdot 2^s - 1, \quad b = 4 \cdot 2^s - 1, \quad U_{2h} = x^{2^s} (x+1)^{3 \cdot 2^s} M^{2h - 2^s} = T_{s,h}.$$
- If $M \nmid \sigma(x^a)$ but $M \mid \sigma((x+1)^b)$, then $u = 1, v = 5$. As above, we get $r \leqslant s \leqslant r+2$ and $U_{2h} \in \{S_{s,h}, T_{s,h}\}$. ∎

We can now finish the proof of Theorem 1.4. If A is perfect, then the case $M = M_3$ is excluded by Theorem 1.3. From Theorem 1.2, we get: $\sigma(\sigma(M^{2h})) = x^u (x+1)^u M^w$, for some $u, w \in \mathbb{N}^*$, with w odd.
Proposition 3.5-iii) gives: $\sigma(\sigma(M^{2h})) = T_{r,h} = x^{2^r} \cdot (x+1)^{2^r} \cdot M^{2h - 2^r}$,
with $r = 0$ and $a = 2 \cdot 2^r - 1 = 1, b = 3 \cdot 2^r - 1 = 2$. Again, Theorem 1.2 implies that $h = 1$ and we get our theorem.

4. Proof of Theorem 1.2

In this section, we take $M = 1 + x + x^2$. Primo, we see that $u = v$ since $\sigma(\sigma(M^{2h})) = \overline{\sigma(\sigma(M^{2h}))}$. Secundo, Lemma 4.1 below states that $w = h = 1$ if $u = v = 1$. It remains then to show that w is odd.

Lemma 4.1. *If $\sigma(\sigma(M^{2h})) = x(x+1)M^{2h-1}$, then $h = 1$.*

Proof. We may write, by Corollary 2.7: $\sigma(M^{2h}) = V_1 \cdots V_r$, where each V_i is odd and irreducible of the form $1+x^{a_i}(x+1)^{b_i}$ or $1+x^{c_i}(x+1)^{d_i}M^{e_i}$, for some positive integers $r, a_i, b_i, c_i, d_i, e_i$. If $r \geqslant 2$, then x^2 divides $\sigma(\sigma(M^{2h}))$, which is impossible. So, $r = 1$ and $\sigma(M^{2h}) = V_1 = 1 + x(x+1)M^{2h-1}$. Hence, $M^{2h} + \cdots + M = \sigma(M^{2h}) + 1 = x(x+1)M^{2h-1}$ and $2h - 1 = 1$. ■

Notation 4.2. For a polynomial $S \in \mathbb{F}_2[x]$ of degree s, we denote by $\alpha_k(S)$ the coefficient of x^{s-k} in S, $1 \leqslant k \leqslant s$.

Lemma 4.3. *Let $S \in \mathbb{F}_2[x]$ such that $\gcd(S, x(x+1)(x^2+x+1)) = 1$, then $\alpha_1(\sigma(S)) = \alpha_1(S)$ and $\alpha_2(\sigma(S)) = \alpha_2(S)$.*

Proof. In this case, $\sigma(S) = S + T$, where $\deg(T) \leqslant \deg(S) - 3$. We are done. ■

Lemma 4.4. *If $u, v, w \in \mathbb{N}^*$, then one has modulo 2:*

$$\alpha_2(M^w) = \frac{w(w+1)}{2}, \qquad \alpha_2(\sigma(M^w)) = 1 + \alpha_2(M^w),$$
$$\alpha_2(x^u(x+1)^v M^w) = \frac{v(v-1)}{2} + \frac{w(w+1)}{2} + vw.$$

Proof. $M^w = ((x^2+x)+1)^w = (x^2+x)^w + w(x^2+x)^{w-1} + \cdots$. So

$$M^w = x^{2w} + wx^{2w-1} + \binom{w}{2}x^{2w-2} + \cdots + w(x^2+x)^{w-1} + \cdots$$

and

$$\alpha_2(M^w) = \binom{w}{2} + w = \binom{w+1}{2},$$
$$\alpha_2(\sigma(M^w)) = \alpha_2(M^w + M^{w-1} + \cdots) = \alpha_2(M^w) + 1.$$

We have $\alpha_2(x^u(x+1)^v M^w) = \alpha_2((x+1)^v M^w)$ and

$$(x+1)^v M^w = (x^v + vx^{v-1} + \binom{v}{2}x^{v-2} + \cdots)(x^{2w} + wx^{2w-1} + \binom{w+1}{2}x^{2w-2} + \cdots)$$

Hence

$$\alpha_2((x+1)^v M^w) = \frac{v(v-1)}{2} + \frac{w(w+1)}{2} + vw. \qquad ■$$

We can now finish the proof of Theorem 1.2. We suppose that $\sigma(\sigma(M^{2h})) = x^u(x+1)^u M^w$ where $w = 2\ell$ is even. By comparing degrees, we get: $u = 2d$ is even and $h = \ell + d$. We apply Lemmas 4.3 and 4.4 to $S = \sigma(M^{2h})$ and to M^{2h}. We get modulo 2: $\alpha_2(\sigma(\sigma(M^{2h}))) = \alpha_2(\sigma(M^{2h})) = 1 + \alpha_2(M^{2h}) = 1 + h$.

On the other hand, still by Lemma 4.4, we obtain:

$$\alpha_2(x^u(x+1)^u M^{2d}) \equiv \ell + d \mod 2.$$

So, we get the contradiction:

$$1 + h \equiv \alpha_2(\sigma(\sigma(M^{2h}))) = \alpha_2(x^u(x+1)^u M^{2d}) \equiv \ell + d = h \mod 2.$$

5. Proof of Theorem 1.3

In this section, we set $M = 1 + x + x^2 + x^3 + x^4$ and for $h \in \mathbb{N}^*$ and $r \in \mathbb{N}$:

$$U_{2h} = \sigma(\sigma(M^{2h})), \quad S_{r,h} = x^{3\cdot 2^r}(x+1)^{2^r} M^{2h-2^r}, \quad T_{r,h} = x^{2^r}(x+1)^{3\cdot 2^r} M^{2h-2^r}.$$

The main idea of the proof is similar (but technically more complicated) as that of Theorem 1.2: Proposition 3.5-iv) implies that $U_{2h} \in \{S_{r,h}, T_{r,h}\}$, for some $r \in \mathbb{N}$. If $r \in \{0,1\}$, we shall show directly that this is not possible. For $r \geqslant 2$, we shall see that this is also impossible by proving that $\alpha_k(U_{2h}) \neq \alpha_k(S_{r,h})$, $\alpha_l(U_{2h}) \neq \alpha_l(T_{r,h})$ for some $1 \leqslant k, l \leqslant 5$ (see Notation 4.2 and Corollaries 5.12, 5.14, 5.16 and 5.18). The rough (trivial) idea is that two polynomials are equal if and only if they have the same coefficients.

5.1. Case $r \in \{0,1\}$

We prove, directly, that if $r \in \{0,1\}$, then $U_{2h} \neq S_{r,h}, T_{r,h}$, for any $h \in \mathbb{N}^*$.

Case $r = 0$

- If $U_{2h} = S_{0,h} = x^3(x+1)M^{2h-1}$, then $\sigma(M^{2h}) = 1 + x^3(x+1)M^{2h-1}$ is irreducible. Hence $M^{2h} + \cdots + M = x^3(x+1)M^{2h-1}$, so that $2h - 1 = 1$ and $M = 1 + x^3(x+1)$. It is impossible.
- If $U_{2h} = T_{0,h} = x(x+1)^3 M^{2h-1}$, then $\sigma(M^{2h})$ is irreducible and equals $1 + x(x+1)^3 M^{2h-1}$. Hence, as above, $h = 1$ and $\sigma(M^{2h}) = (x^2+x+1)(x^6+x^5+x^4+x^2+1)$, which is not irreducible.

Case $r = 1$

Lemma 5.1. *For any $h \in \mathbb{N}^*$, $U_{2h} \neq x^6(x+1)^2 M^{2h-2} = S_{1,h}$.*

Proof. If $U_{2h} = x^6(x+1)^2 M^{2h-2}$, then by Corollary 2.7, $\sigma(M^{2h}) = (1 + x^u(x+1)M^w)((1 + x^{6-u}(x+1)M^{2h-2-w})$, where $u, w \in \mathbb{N}$, $1 \leqslant u \leqslant 5$. Hence

$$M^{2h} + \cdots + M + 1 = 1 + x^u(x+1)M^w + x^{6-u}(x+1)M^{2h-2-w} + x^6(x+1)^2 M^{2h-2}.$$

- If $w \neq 2h-2-w$, then $\min(w, 2h-2-w) = 1$ and M must divide $1+x^c(x+1)$, with $c \in \{u, 6-u\}$. This contradicts Lemma 5.3 below.
- If $w = 2h-2-w$ and $u = 3$, then $M^{2h} + \cdots + M + 1 = 1 + x^6(x+1)^2 M^{2h-2}$. Hence $2h-2 = 1$. It is impossible.
- If $w = 2h-2-w$ and $u \neq 3$, then $w = h-1$,

$$M^{2h} + \cdots + M = (x+1)M^{h-1}(x^u + x^{6-u}) + x^6(x+1)^2 M^{2h-2}.$$

So, $h - 1 = 1$, $h = 2$ and

$$U_4 = \sigma(\sigma(M^4)) = x^2(x+1)^2(x^2+x+1)(x^{10}+x^9+x^8+x^6+x^4+x^3+1) \neq S_{1,2}. \blacksquare$$

Lemma 5.2. *For any* $h \in \mathbb{N}^*$, $U_{2h} \neq x^2(x+1)^6 M^{2h-2} = T_{1,h}$.

Proof. If $U_{2h} = x^2(x+1)^6 M^{2h-2}$, then as above, $\sigma(M^{2h}) = (1+x(x+1)^u M^w)((1+x(x+1)^{6-u} M^{2h-2-w})$, where $u, w \in \mathbb{N}$, $1 \leqslant u \leqslant 5$. Hence

$$M^{2h} + \cdots + M = x(x+1)^u M^w + x(x+1)^{6-u} M^{2h-2-w} + x^2(x+1)^6 M^{2h-2}.$$

- If $w \neq 2h-2-w$, then $\delta := \min(w, 2h-2-w) = 1$ and M must divide $1 + x(x+1)^c$, with $c \in \{u, 6-u\} \subset \{1, \ldots, 5\}$. Thus, $c = 3 = u = 6-u$ and

  $$M^{2h-1} + \cdots + M + 1 = x(x+1)^3[M^{w-1} + M^{2h-3-w}] + x^2(x+1)^6 M^{2h-3}.$$

  Remark that $M^{w-1} + M^{2h-3-w} = 1 + M^{2h-4}$ if $(w = \delta)$ or $(2h-2-w = \delta)$. It follows that $M^{2h-1} + \cdots + M^2 = x(x+1)^3 M^{2h-4} + x^2(x+1)^6 M^{2h-3}$. So, $2h-4 = 2$, $h = 3$ and

  $$U_6 = x^5(x+1)^7(1+x+x^2+x^3+x^4)^2(x^4+x^3+1) \neq x^2(x+1)^6 M^4 = T_{1,3}.$$

- If $w = 2h-2-w$ and $u = 3$, then $M^{2h} + \cdots + M = x^2(x+1)^6 M^{2h-2}$. Hence $2h-2 = 1$. It is impossible.
- If $w = 2h-2-w$ and $u \neq 3$, then $w = h-1$,

  $$M^{2h} + \cdots + M = xM^{h-1}[(x+1)^u + (x+1)^{6-u}] + x^2(x+1)^6 M^{2h-2}.$$

  So, $h-1 = 1$, $h = 2$ and

  $$U_4 = \sigma(\sigma(M^4)) = x^2(x+1)^2(x^2+x+1)(x^{10}+x^9+x^8+x^6+x^4+x^3+1) \neq T_{1,2}.$$

$\blacksquare$

Lemma 5.3. *For any* $c \in \mathbb{N}$, M *does not divide* $1 + x^c(x+1)$.

Proof. Let α be a root of M. Then, one has $\alpha^5 = 1$ so that $\alpha^c \in \{1, \alpha, \ldots, \alpha^4\}$. Thus, $\alpha^c(\alpha+1) \neq 1$ for any $c \in \mathbb{N}$. We are done. $\blacksquare$

5.2. Case $r \geqslant 2$

Some precisions about divisors of $\sigma(M^{2h})$

The polynomial U defined below and its divisors will be useful:

$$U := (x^2+x+1)(x^3+x+1)(x^3+x^2+1) = x^8+x^6+x^5+x^4+x^3+x^2+1.$$

Moreover, it follows from Lemma 5.4 below, that we have to distinguish the following four cases:

i) $\gcd(\sigma(M^{2h}), U) = 1$,
ii) $\sigma(M^{2h}) = (x^2+x+1)B$, with $\gcd(B, U) = 1$,
iii) $\sigma(M^{2h}) = (x^3+x+1)(x^3+x^2+1)B$, with $\gcd(B, U) = 1$,
iv) $\sigma(M^{2h}) = UB$, with $\gcd(B, U) = 1$.

Lemma 5.4.

i) *The polynomial x^3+x+1 divides $\sigma(M^{2h})$ if and only if x^3+x^2+1 divides $\sigma(M^{2h})$.*
ii) *If x^4+x^3+1 divides $\sigma(M^{2h})$ then x^4+x+1 must divide $\sigma(M^{2h})$. The converse is false.*
iii) *No irreducible polynomial of degree 4 divides $\sigma(M^{2h})$.*
iv) *No irreducible polynomial of degree 5 divides $\sigma(M^{2h})$.*

Proof. i): Suppose that x^3+x+1 divides $\sigma(M^{2h})$ and let μ be a root of x^3+x+1. Then, one has $M(\mu)^{2h+1} = 1$. But, $M(\mu) = \mu^4+\mu^2 = \mu^2(\mu+1)^2 = \mu^2\mu^6 = \mu^8 = \mu$ because $\mu \in \mathbb{F}_8$. So, $\mu^{2h+1} = 1$ and 7 divides $2h+1$.

Now, let β be a root of x^3+x^2+1. Then, $M(\beta) = \beta^4+\beta = \beta^3 \not\in \{0,1\}$ because β is of order 7. Hence $M(\beta)^7 = 1$ so that $M(\beta)^{2h+1} = 1$ and $(x^3+x^2+1) \mid \sigma(M^{2h})$.

We similarly see that $(x^3+x+1) \mid \sigma(M^{2h})$ if $(x^3+x^2+1) \mid \sigma(M^{2h})$.

ii): Suppose that x^4+x^3+1 divides $\sigma(M^{2h})$ and let γ be a root of x^4+x^3+1. Then, one has $M(\gamma)^{2h+1} = 1$. But, $M(\gamma) = \gamma(\gamma+1) = \dfrac{\gamma}{\gamma^3}$. So, $(\gamma^{-2})^{2h+1} = 1$, $\gamma^{2h+1} = 1$. Since $\gamma^{15} = 1$, γ belonging to $\mathbb{F}_{16} \setminus \{0,1\}$, $\gamma^3 \neq 1$ and $\gamma^5 \neq 1$, we see that γ is of order 15. Thus, 15 divides $2h+1$.

Now, let ζ be a root of x^4+x+1. Then, $M(\zeta) = \zeta^3+\zeta^2 = \zeta^2\zeta^4 = \zeta^6 \not\in \{0,1\}$. Hence $M(\zeta)^{15} = 1$ so that $M(\zeta)^{2h+1} = 1$ and $(x^4+x+1) \mid \sigma(M^{2h})$. By taking $h = 2$, we see that $\sigma(M^{2h}) = (x^4+x+1)(x^{12}+x^9+x^8+x^7+x^6+x^4+x^2+x+1)$, so that the converse is not true.

iii) follows from ii) and from the fact that any irreducible divisor of $\sigma(M^{2h})$ must be of the form $1+x^{a_i}(x+1)^{b_i}M^{c_i}$ (Corollary 2.7), x^4+x+1 being not of this form.

iv) follows by an analogous proof, since any element of $\mathbb{F}_{32} \setminus \{0,1\}$ is of order 31 (a prime number), we see that if an irreducible polynomial of degree 5 divides $\sigma(M^{2h})$, then all irreducible polynomials of degree 5 divide it. But, $1+x+x^2+x^4+x^5 = 1+x(x+1)^2(x^2+x+1)$ is irreducible of degree 5 and is not of the form $1+x^{a_i}(x+1)^{b_i}M^{c_i}$. This contradicts Corollary 2.7. ∎

$\alpha_l(M^w), \alpha_l(\sigma(M^{2h}))$ and $\alpha_l(U_{2h})$, for $l, w, h \in \mathbb{N}^*$, $l \leqslant 5$

In order to compute $\alpha_l(M^w), \alpha_l(\sigma(M^{2h}))$ and $\alpha_l(U_{2h})$, for $l, w, h \in \mathbb{N}^*$, we sometimes apply the following binomial coefficient properties obtained from the well-known Lucas'Theorem (see [11]), without explicit mention. Some of our results are obtained by direct computations, so we omit their proofs.

Lemma 5.5. *Let n, k be two positive integers. Then, one has modulo 2:*

i) $\binom{n}{k} \equiv 0$ *if n is even and k odd.*

ii) $\binom{n}{k} \equiv \binom{[\frac{n}{2}]}{[\frac{k}{2}]}$, *otherwise.*

iii) $\binom{2n}{n} \equiv 0.$

Lemma 5.6. *If $w \in \mathbb{N}^*$, then one has modulo 2:*

$$\alpha_1(M^w) = w, \qquad \alpha_2(M^w) = w + \binom{w}{2}, \qquad \alpha_3(M^w) = w + \binom{w}{3}$$

$$\alpha_4(M^w) = \binom{w}{4} + w\binom{w-1}{2} + w + \binom{w}{2},$$

$$\alpha_5(M^w) = \binom{w}{5} + w\binom{w-1}{3} + w\binom{w-1}{2} + (w-2)\binom{w}{2}.$$

In particular, for any $l \in \mathbb{N}^*$,

$$\alpha_1(M^{2l}) = \alpha_3(M^{2l}) = 0, \quad \alpha_2(M^{2l}) = l, \quad \alpha_4(M^{2l}) = \binom{l}{2} + l, \quad \alpha_5(M^{2l}) = 0.$$

Proof. Write

$$M^w = \sum_{l=0}^{2} \binom{w}{l} (x^4 + x^3)^{w-l} (x^2 + x + 1)^l + T, \qquad \text{where } \deg(T_1) \leqslant 4w - 6,$$

and consider all the coefficients of monomials of degree greater than $4w - 6$ in $(x^4 + x^3)^w$, $w(x^4 + x^3)^{w-1}(x^2 + x + 1)$ and in $\binom{w}{l}(x^4 + x^3)^{w-2}(x^2 + x + 1)^2$. ∎

Lemma 5.7. *Let $u, v, w \in \mathbb{N}^*$ and $R_{v,w} = (x+1)^v M^w$. Then $\alpha_k(x^u(x+1)^v M^w) = \alpha_k(R_{v,w})$ and*

$$\alpha_1(R_{v,w}) = v + \alpha_1(M^w) = v + w, \qquad \alpha_2(R_{v,w}) = \binom{v}{2} + v\alpha_1(M^w) + \alpha_2(M^w),$$

$$\alpha_3(R_{v,w}) = \binom{v}{3} + \binom{v}{2}\alpha_1(M^w) + v\alpha_2(M^w) + \alpha_3(M^w),$$

$$\alpha_4(R_{v,w}) = \binom{v}{4} + \binom{v}{3}\alpha_1(M^w) + \binom{v}{2}\alpha_2(M^w) + v\alpha_3(M^w) + \alpha_4(M^w),$$

$$\alpha_5(R_{v,w}) = \binom{v}{5} + \binom{v}{4}w + \binom{v}{3}\alpha_2(M^w) + \binom{v}{2}\alpha_3(M^w) + v\alpha_4(M^w) + \alpha_5(M^w).$$

Proof. We easily see that $\alpha_k(x^u(x+1)^v M^w) = \alpha_k((x+1)^v M^w)$. We write $M^w = x^{4w} + \sum_{l=1}^5 \alpha_l(M^w)x^{4w-l} + T_2$ and $(x+1)^v = \sum_{l=0}^5 \binom{v}{l} x^{v-l} + T_3$, where $\deg(T_2) \leqslant 4w-6$ and $\deg(T_3) \leqslant v-6$. As above, it suffices to consider the coefficients of all monomials of degree greater than $4w-6$ in

$$\left(x^{4w} + \sum_{l=1}^{5} \alpha_l(M^w)x^{4w-l}\right)\left(\sum_{l=0}^{5}\binom{v}{l}x^{v-l}\right). \qquad \blacksquare$$

From Lemma 5.7 and from the fact that $S_{r,h}$ and $T_{r,h}$ are squares, we get

Corollary 5.8. *If $r, h \in \mathbb{N}^*$, with $r \geqslant 2$, then one has modulo 2:*

$$\alpha_l(S_{r,h}) = \alpha_l(T_{r,h}) = 0 \qquad \text{if } l \text{ is odd},$$

$$\alpha_2(S_{r,h}) = \alpha_2(T_{r,h}) = h, \qquad \alpha_4(S_{r,h}) = \alpha_4(T_{r,h}) = 2^{r-2} + \binom{h-2^{r-1}}{2} + h.$$

Lemma 5.9. *For $h \in \mathbb{N}^*$, one has modulo 2: $\alpha_1(\sigma(M^{2h})) = \alpha_3(\sigma(M^{2h})) = 0$, $\alpha_2(\sigma(M^{2h})) = h$, $\alpha_4(\sigma(M^{2h})) = \binom{h-1}{2}$ and $\alpha_5(\sigma(M^{2h})) = 1$.*

Proof. Since $\sigma(M^{2h}) = M^{2h} + M^{2h-1} + T$, with $\deg(T) \leqslant 4(2h-2) = 8h-8$, one has $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h})$ if $1 \leqslant l \leqslant 3$, and $\alpha_l(\sigma(M^{2h})) = \alpha_l(M^{2h} + M^{2h-1}) = \alpha_l(x(x+1)^3 M^{2h-1}) = \alpha_l(R_{3,2h-1})$ if $4 \leqslant l \leqslant 5$.

From Lemmas 5.7 and 5.6, one has modulo 2:

$$\begin{aligned}
\alpha_4(R_{3,2h-1}) &= \alpha_1(M^{2h-1}) + \alpha_2(M^{2h-1}) + \alpha_3(M^{2h-1}) + \alpha_4(M^{2h-1}) \\
&= \binom{2h-1}{3} + \binom{2h-1}{4} + \binom{2h-1}{2} \\
&= \binom{h-1}{1} + \binom{h-1}{2} + \binom{h-1}{1}. \\
\alpha_5(R_{3,2h-1}) &= \alpha_2(M^{2h-1}) + \alpha_3(M^{2h-1}) + \alpha_4(M^{2h-1}) + \alpha_5(M^{2h-1}) \\
&= 1 + \alpha_4(R_{3,2h-1}) + \binom{2h-1}{5} + \binom{2h-2}{3} + \binom{2h-2}{2} \\
&= 1 + \binom{h-1}{2} + \binom{h-1}{2} + \binom{h-1}{1} + \binom{h-1}{1}.
\end{aligned}$$

So, $\alpha_4(\sigma(M^{2h})) = \binom{h-1}{2}$ and $\alpha_5(\sigma(M^{2h})) = 1$. $\blacksquare$

Lemma 5.10. *Let $S \in \mathbb{F}_2[x]$ be such that no irreducible polynomial of degree at most 5 divides S. Then $\alpha_l(\sigma(S)) = \alpha_l(S)$, for any $1 \leqslant l \leqslant 5$.*

Proof. One has: $\sigma(S) = S + T$, where $\deg(T) \leqslant \deg(S) - 6$. We are done. $\blacksquare$

Corollary 5.11. *Let $h \in \mathbb{N}^*$ be such that $\gcd(\sigma(M^{2h}), U) = 1$. Then*

$$\alpha_1(U_{2h}) = 0, \qquad \alpha_2(U_{2h}) = h, \qquad \alpha_3(U_{2h}) = 0, \qquad \alpha_4(U_{2h}) = \binom{h-1}{2}.$$

Proof. Apply Lemma 5.10 to $S = \sigma(M^{2h})$ by taking account of Corollary 2.7 and of Lemma 5.9. ■

Corollary 5.12. *If* $r, h \in \mathbb{N}^*$ *with* $\gcd(\sigma(M^{2h}), U) = 1$ *and* $r \geqslant 2$, *then*

$$\alpha_4(U_{2h}) \neq \alpha_4(S_{r,h}), \qquad \alpha_4(U_{2h}) \neq \alpha_4(T_{r,h}).$$

Lemma 5.13. *Let* $h \in \mathbb{N}^*$ *be such that* $\sigma(M^{2h}) = (x^2 + x + 1)B$, *where* $\gcd(B, U) = 1$. *Then* $\alpha_1(U_{2h}) = 0$ *and* $\alpha_2(U_{2h}) = h + 1$.

Proof. By Corollary 2.7, since B divides $\sigma(M^{2h})$, we may apply Lemma 5.10 to $S = B$. One has, for any $1 \leqslant l \leqslant 5$, $\alpha_l(\sigma(B)) = \alpha_l(B)$.

We may write: $B = x^b + \alpha_1(B)x^{b-1} + \alpha_2(B)x^{b-2} + \cdots$ and $\sigma(M^{2h}) = (x^2+x+1)B = x^{b+2} + (\alpha_1(B)+1)x^{b+1} + (\alpha_2(B)+1)x^b + \cdots$ So, $\alpha_1(\sigma(M^{2h})) = \alpha_1(B) + 1$, $\alpha_2(\sigma(M^{2h})) = \alpha_2(B) + \alpha_1(B) + 1$.

On the other hand,

$$U_{2h} = (x^2+x)\sigma(B) = x^{b+2} + (\alpha_1(\sigma(B))+1)x^{b+1} + (\alpha_2(\sigma(B)) + \alpha_1(\sigma(B)))x^b + \cdots$$

Thus, $\alpha_1(U_{2h}) = \alpha_1(\sigma(B)) + 1 = \alpha_1(B) + 1 = \alpha_1(\sigma(M^{2h}))$ and

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

We get then our results from Lemma 5.9. ■

Corollary 5.14. *If* $r, h \in \mathbb{N}^*$ *are such that* $\sigma(M^{2h}) = (x^2 + x + 1)B$, *where* $\gcd(B, U) = 1$ *and* $r \geqslant 2$, *then* $\alpha_2(U_{2h}) = h + 1 \neq h = \alpha_2(S_{r,h}) = \alpha_2(T_{r,h})$.

Lemma 5.15. *Let* $h \in \mathbb{N}^*$ *be such that* $\sigma(M^{2h}) = (x^3 + x + 1)(x^3 + x^2 + 1)B$, *where* $\gcd(B, U) = 1$. *Then*

$$\alpha_1(U_{2h}) = 0, \qquad \alpha_2(U_{2h}) = h, \qquad \alpha_3(U_{2h}) = 0,$$
$$\alpha_4(U_{2h}) = 1 + \binom{h-1}{2}, \qquad \alpha_5(U_{2h}) = 1.$$

Proof. We proceed as in the proof of Lemma 5.13. We give relations between the $\alpha_l(\sigma(M^{2h}))$'s and the $\alpha_l(U_{2h})$'s and apply Lemma 5.9.
By writing:

$$\sigma(M^{2h}) = (x^6 + \cdots + x + 1)B, \qquad \text{with } B = x^b + \sum_{k=1}^{5} \alpha_k(B)x^{b-k} + \cdots,$$

we get:

$$\alpha_1(\sigma(M^{2h})) = \alpha_1(B) + 1, \alpha_2(\sigma(M^{2h})) = \alpha_2(B) + \alpha_1(B) + 1,$$
$$\alpha_3(\sigma(M^{2h})) = \alpha_3(B) + \alpha_2(B) + \alpha_1(B) + 1 = \alpha_3(B) + \alpha_2(\sigma(M^{2h})),$$
$$\alpha_4(\sigma(M^{2h})) = \alpha_4(B) + \alpha_3(\sigma(M^{2h})),$$
$$\alpha_5(\sigma(M^{2h})) = \sum_{k=1}^{5} \alpha_k(B) + 1 = \sum_{k=2}^{5} \alpha_k(B) + \alpha_1(\sigma(M^{2h})).$$

Since $U_{2h} = (x^3+x)(x^3+x^2)\sigma(B) = (x^6+x^5+x^4+x^3)\sigma(B)$, we obtain

$$\alpha_1(U_{2h}) = \alpha_1(\sigma(B)) + 1 = \alpha_1(B) + 1 = \alpha_1(\sigma(M^{2h})),$$
$$\alpha_2(U_{2h}) = \alpha_2(\sigma(B)) + \alpha_1(\sigma(B)) + 1 = \alpha_2(\sigma(M^{2h})),$$
$$\alpha_3(U_{2h}) = \alpha_3(\sigma(B)) + \alpha_2(\sigma(B)) + \alpha_1(\sigma(B)) + 1 = \alpha_3(\sigma(M^{2h})),$$
$$\alpha_4(U_{2h}) = \sum_{k=1}^{4} \alpha_k(\sigma(B)) = \alpha_4(\sigma(M^{2h})) + 1,$$
$$\alpha_5(U_{2h}) = \sum_{k=2}^{5} \alpha_k(\sigma(B)) = \sum_{k=2}^{5} \alpha_k(B) = \alpha_5(\sigma(M^{2h})) + \alpha_1(\sigma(M^{2h})). \qquad \blacksquare$$

Corollary 5.16. *If $r, h \in \mathbb{N}^*$ are such that $\sigma(M^{2h}) = (x^3+x+1)(x^3+x^2+1)B$, where $\gcd(B,U) = 1$ and $r \geqslant 2$, then $\alpha_5(U_{2h}) = 1 \neq 0 = \alpha_5(S_{r,h}) = \alpha_5(T_{r,h})$.*

Lemma 5.17. *Let $h \in \mathbb{N}^*$ be such that $\sigma(M^{2h}) = U \cdot B$, where $\gcd(B,U) = 1$. Then $\alpha_1(U_{2h}) = 0,\ \alpha_2(U_{2h}) = h+1$ and $\alpha_3(U_{2h}) = 1$.*

Proof. As above, we write:

$$\sigma(M^{2h}) = UB = (x^8 + x^6 + \cdots + x^2 + 1)B \quad \text{with} \quad B = x^b + \sum_{k=1}^{3} \alpha_k(B) x^{b-k} + \cdots$$

We get: $\alpha_1(\sigma(M^{2h})) = \alpha_1(B), \alpha_2(\sigma(M^{2h})) = \alpha_2(B) + 1$ and
$\alpha_3(\sigma(M^{2h})) = \alpha_3(B) + \alpha_1(B) + 1$.
Here, $U_{2h} = (x^2+x)(x^3+x)(x^3+x^2)\sigma(B) = (x^8+x^4)\sigma(B)$. So, one has:

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

Corollary 5.18. *If $r, h \in \mathbb{N}^*$ are such that $\sigma(M^{2h}) = U \cdot B$, where $\gcd(B,U) = 1$ and $r \geqslant 2$, then $\alpha_3(U_{2h}) = 1 \neq 0 = \alpha_3(S_{r,h}) = \alpha_3(T_{r,h})$.*

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] R. Kim, W. Koepf, *Parity of the number of irreducible factors for composite polynomials*, Finite Fields Appl. **16** (2010), 137–143.

[11] E. Lucas, *Théorie des Fonctions Numériques Simplement Périodiques*, Am. J. Math. **1**(3) (1878), 197–240.

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

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

Received: 6 May 2015; **revised:** 1 February 2016