



HAL
open science

All bi-unitary perfect polynomials over \mathbb{Z} with at most four irreducible factors

Olivier Rahavandrainy

► **To cite this version:**

Olivier Rahavandrainy. All bi-unitary perfect polynomials over \mathbb{Z} with at most four irreducible factors. 2022. hal-03676944

HAL Id: hal-03676944

<https://hal.univ-brest.fr/hal-03676944>

Preprint submitted on 24 May 2022

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

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

All bi-unitary perfect polynomials over \mathbb{F}_2 with at
most four irreducible factors

Olivier Rahavandrainy
Univ Brest, UMR CNRS 6205
Laboratoire de Mathématiques de Bretagne Atlantique
e-mail : olivier.rahavandrainy@univ-brest.fr

May 23, 2022

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

Abstract

We give, in this paper, all bi-unitary perfect polynomials over the prime field \mathbb{F}_2 , with at most four irreducible factors.

1 Introduction

Let $S \in \mathbb{F}_2[x]$ be a nonzero polynomial. We say that S is odd if $\gcd(S, x(x+1)) = 1$, S is even if it is not odd. A *Mersenne (prime)* is a polynomial (irreducible) of the form $1 + x^a(x+1)^b$, with $\gcd(a, b) = 1$. A divisor D of S is called unitary if $\gcd(D, S/D) = 1$. We denote by $\gcd_u(S, T)$ the greatest common unitary divisor of S and T . A divisor D of S is called bi-unitary if $\gcd_u(D, S/D) = 1$.

We denote by $\sigma(S)$ (resp. $\sigma^*(S)$, $\sigma^{**}(S)$) the sum of all divisors (resp. unitary divisors, bi-unitary divisors) of S . The functions σ , σ^* and σ^{**} are all multiplicative. We say that a polynomial S is *perfect* (resp. *unitary perfect*, *bi-unitary perfect*) if $\sigma(S) = S$ (resp. $\sigma^*(S) = S$, $\sigma^{**}(S) = S$).

Finally, we say that S is *indecomposable bi-unitary perfect (i.b.u.p.)* if it is bi-unitary perfect but it is not a product of two coprime nonconstant bi-unitary perfect polynomials.

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

Several studies are done about perfect and unitary perfect. In particular, we gave ([3], [4], [5]) the list of all (unitary) perfect polynomials A over \mathbb{F}_2 (even or not), with $\omega(A) \leq 4$.

In this paper, we are interested in bi-unitary perfect polynomials (b.u.p. polynomials) A with $\omega(A) \leq 4$. If $A \in \mathbb{F}_2[x]$ is nonconstant b.u.p., then $x(x+1)$ divides A so that $\omega(A) \geq 2$ (see Lemma 2.5). Moreover, the only b.u.p. polynomials over \mathbb{F}_2 with exactly two prime factors are $x^2(x+1)^2$ and $x^{2^n-1}(x+1)^{2^n-1}$, for any nonnegative integer n ([1], Theorem 5). We prove (Theorems 1.1 and 1.2) that the only b.u.p. polynomials $A \in \mathbb{F}_2$, with $\omega(A) \in \{3, 4\}$, are those given in [1], plus four other ones. Note that all odd irreducible divisors of the C_j 's are Mersenne primes (there is a misprint for C_6 , in [1]).

In the rest of the paper, for $S \in \mathbb{F}_2[x]$, we denote by \bar{S} the polynomial obtained from S with x replaced by $x+1$: $\bar{S}(x) = S(x+1)$.

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

For $S, T \in \mathbb{F}_2[x]$ and $n \in \mathbb{N}^*$, we write: $S^n || T$ if $S^n | T$ but $S^{n+1} \nmid T$.

Finally, let \mathcal{M} denotes the set of all Mersenne primes.

We consider the following polynomials over \mathbb{F}_2 :

$$\begin{aligned}
M_1 &= 1 + x + x^2 = \sigma(x^2), \quad M_2 = 1 + x + x^3, \quad M_3 = \overline{M_2} = 1 + x^2 + x^3, \\
M_4 &= 1 + x + x^2 + x^3 + x^4 = \sigma(x^4), \quad M_5 = \overline{M_4} = 1 + x^3 + x^4, \\
S_1 &= 1 + x(x+1)M_1 = 1 + x + x^4, \\
C_1 &= x^3(x+1)^4M_1, \quad C_2 = x^3(x+1)^5M_1^2, \quad C_3 = x^4(x+1)^4M_1^2, \\
C_4 &= x^6(x+1)^6M_1^2, \quad C_5 = x^4(x+1)^5M_1^3, \quad C_6 = x^7(x+1)^8M_5, \\
C_7 &= x^7(x+1)^9M_5^2, \quad C_8 = x^8(x+1)^8M_4M_5, \quad C_9 = x^8(x+1)^9M_4M_5^2, \\
C_{10} &= x^7(x+1)^{10}M_1^2M_5, \quad C_{11} = x^7(x+1)^{13}M_2^2M_3^2, \\
C_{12} &= x^9(x+1)^9M_4^2M_5^2, \quad C_{13} = x^{14}(x+1)^{14}M_2^2M_3^2, \\
D_1 &= x^4(x+1)^5M_1^4S_1, \quad D_2 = x^4(x+1)^5M_1^5S_1^2.
\end{aligned}$$

The polynomials $M_1, \dots, M_5 \in \mathcal{M}$. We set $\mathcal{U} := \{M_1, \dots, M_5\}$.

Theorem 1.1. *Let $A \in \mathbb{F}_2[x]$ be b.u.p. such that $\omega(A) = 3$. Then $A, \overline{A} \in \{C_j : j \leq 7\}$.*

Theorem 1.2. *Let $A \in \mathbb{F}_2[x]$ be b.u.p. such that $\omega(A) = 4$. Then $A, \overline{A} \in \{C_j : 8 \leq j \leq 13\} \cup \{D_1, D_2\}$.*

2 Preliminaries

We need the following results. Some of them are obvious or (well) known, so we omit their proofs.

Lemma 2.1. *Let T be an irreducible polynomial over \mathbb{F}_2 and $k, l \in \mathbb{N}^*$. Then, $\gcd_u(T^k, T^l) = 1$ (resp. T^k) if $k \neq l$ (resp. $k = l$). In particular, $\gcd_u(T^k, T^{2n-k}) = 1$ for $k \neq n$, $\gcd_u(T^k, T^{2n+1-k}) = 1$ for any $0 \leq k \leq 2n+1$.*

Lemma 2.2. *Let $T \in \mathbb{F}_2[x]$ be irreducible. Then*
*i) $\sigma^{**}(T^{2n}) = (1+T)\sigma(T^n)\sigma(T^{n-1})$, $\sigma^{**}(T^{2n+1}) = \sigma(T^{2n+1})$.*
*ii) For any $c \in \mathbb{N}$, T does not divide $\sigma^{**}(T^c)$.*

Proof. i): $\sigma^{**}(T^{2n}) = 1 + T + \dots + T^{n-1} + T^{n+1} + \dots + T^{2n} = (1 + T^{n+1})\sigma(T^{n-1}) = (1+T)\sigma(T^n)\sigma(T^{n-1})$, $\sigma^{**}(T^{2n+1}) = 1 + T + \dots + T^{2n+1}$.
ii) follows from i). □

Corollary 2.3. *Let $T \in \mathbb{F}_2[x]$ be irreducible. Then*
*i) If $a \in \{4r, 4r+2\}$, where $2r-1$ or $2r+1$ is of the form $2^\alpha u - 1$, u odd, then $\sigma^{**}(T^a) = (1+T)^{2^\alpha} \cdot \sigma(T^{2r}) \cdot (\sigma(T^{u-1}))^{2^\alpha}$, $\gcd(\sigma(T^{2r}), \sigma(T^{u-1})) = 1$.*
*ii) If $a = 2^\alpha u - 1$ is odd, with u odd, then $\sigma^{**}(T^a) = (1+T)^{2^\alpha-1} \cdot (\sigma(T^{u-1}))^{2^\alpha}$.*

Corollary 2.4. *i) The polynomial $\sigma^{**}(x^a)$ splits over \mathbb{F}_2 if and only if $a = 2$ or $a = 2^\alpha - 1$, for some $\alpha \in \mathbb{N}^*$.*

*ii) Let $T \in \mathbb{F}_2[x]$ be odd and irreducible. Then $\sigma^{**}(T^c)$ splits over \mathbb{F}_2 if and only if (T is Mersenne, $c = 2$ or $c = 2^\gamma - 1$ for some $\gamma \in \mathbb{N}^*$).*

Lemma 2.5. *If A is a nonconstant b.u.p. polynomial over \mathbb{F}_2 , then $x(x+1)$ divides A so that $\omega(A) \geq 2$.*

Lemma 2.6. *If $A = A_1A_2$ is b.u.p. over \mathbb{F}_2 and if $\gcd(A_1, A_2) = 1$, then A_1 is b.u.p. if and only if A_2 is b.u.p.*

Lemma 2.7. *If A is b.u.p. over \mathbb{F}_2 , then the polynomial \overline{A} is also b.u.p. over \mathbb{F}_2 .*

Lemma 2.8 below gives some useful results from Canaday's paper ([2], Lemmas 4, 5, 6, Theorem 8 and Corollary on page 728).

Lemma 2.8. *Let $P, Q \in \mathbb{F}_2[x]$ be such that P is irreducible and let $n, m \in \mathbb{N}$.*

i) If $\sigma(P^{2n}) = Q^m$, then $m \in \{0, 1\}$.

ii) If $\sigma(P^{2n}) = Q^mT$, with $m > 1$ and $T \in \mathbb{F}_2[x]$ is nonconstant, then $\deg(P) > \deg(Q)$.

iii) If P is a Mersenne prime and if $P = P^$, then $P \in \{M_1, M_4\}$.*

iv) If $\sigma(x^{2n}) = PQ$ and $P = \sigma((x+1)^{2m})$, then $2n = 8$, $2m = 2$, $P = M_1$ and $Q = P(x^3) = 1 + x^3 + x^6$.

v) If any irreducible factor of $\sigma(x^{2n})$ is a Mersenne prime, then $2n \leq 6$.

vi) If $\sigma(x^{2n})$ is a Mersenne prime, then $2n \in \{2, 4\}$.

vii) If $\sigma(x^n) = \sigma((x+1)^n)$, then $n = 2^h - 2$, for some $h \in \mathbb{N}^$.*

Lemma 2.9. [see [6], Lemma 2.6] *Let $m \in \mathbb{N}^*$ and T be a Mersenne prime. Then, $\sigma(x^{2m})$, $\sigma((x+1)^{2m})$ and $\sigma(M^{2m})$ are all odd and squarefree.*

The following equalities (obtained from Corollary 2.3) are useful.

$$\left\{ \begin{array}{l} \sigma^{**}(T^2) = (1 + T)^2, \text{ if } T \text{ is irreducible} \\ \\ \text{For } a, b \geq 3, \\ \\ \sigma^{**}(x^a) = (1 + x)^{2^\alpha} \cdot \sigma(x^{2r}) \cdot (\sigma(x^{u-1}))^{2^\alpha}, \text{ with } \gcd(\sigma(x^{2r}), \sigma(x^{u-1})) = 1, \\ \text{if } a = 4r, 2r - 1 = 2^\alpha u - 1, \text{ (resp. } a = 4r + 2, 2r + 1 = 2^\alpha u - 1), u \text{ odd} \\ \\ \sigma^{**}((x + 1)^b) = x^{2^\beta} \cdot \sigma((x + 1)^{2s}) \cdot (\sigma((x + 1)^{v-1}))^{2^\beta}, \\ \text{if } b = 4s, 2s - 1 = 2^\beta v - 1, \text{ (resp. } b = 4s + 2, 2s + 1 = 2^\beta v - 1), v \text{ odd} \\ \\ \sigma^{**}(x^a) = (1 + x)^{2^\alpha - 1} \cdot (\sigma(x^{u-1}))^{2^\alpha}, \text{ if } a = 2^\alpha u - 1 \text{ is odd, with } u \text{ odd} \\ \sigma^{**}((x + 1)^b) = x^{2^\beta - 1} \cdot (\sigma((x + 1)^{v-1}))^{2^\beta}, \text{ if } b = 2^\beta v - 1 \text{ is odd, with } v \text{ odd} \\ \\ r, \alpha, \beta \geq 1. \end{array} \right. \quad (1)$$

Moreover, we shall also (prove and) consider the following relations:

$$c \in \{2, 2^\gamma - 1 : \gamma \geq 1\}, \sigma^{**}(P^c) = (1 + P)^c \text{ (in Section 3)}. \quad (2)$$

In Section 4.1:

$$c, d \in \{2, 2^\gamma - 1 : \gamma \geq 1\}, \sigma^{**}(P^c) = (1 + P)^c, \sigma^{**}(Q^d) = (1 + Q)^d \quad (3)$$

and in Section 4.2:

$$\left\{ \begin{array}{l} \sigma^{**}(P^c) = (1 + P)^{2^\gamma} \cdot \sigma(P^{2t}) \cdot (\sigma(P^{w-1}))^{2^\gamma}, \text{ with } \gcd(\sigma(P^{2t}), \sigma(P^{w-1})) = 1, \\ \text{if } c \in \{4t, 4t + 2\}, \text{ where } 2t - 1 \text{ or } 2t + 1 \text{ is of the form } 2^\gamma w - 1, w \text{ odd} \\ \\ \sigma^{**}(P^c) = (1 + P)^{2^\gamma - 1} \cdot (\sigma(P^{w-1}))^{2^\gamma}, \text{ if } c = 2^\gamma w - 1 \text{ is odd, with } w \text{ odd} \\ \\ d \in \{2, 2^\gamma - 1 : \gamma \geq 1\}, \sigma^{**}(Q^d) = (1 + Q)^d = x^{u_2 d} (x + 1)^{v_2 d} P^{w_2 d} \\ \\ r, \alpha, \beta, u_2, v_2, w_2 \geq 1, \varepsilon_1 = \min(1, u - 1), \varepsilon_2 = \min(1, v - 1), \varepsilon_1, \varepsilon_2 \in \{0, 1\}. \end{array} \right. \quad (4)$$

3 Proof of Theorem 1.1

We set $A = x^a (x + 1)^b P^c$, with $a, b, c \in \mathbb{N}^*$ and P odd irreducible.

We suppose that A is b.u.p.:

$$\sigma^{**}(x^a) \cdot \sigma^{**}((x + 1)^b) \cdot \sigma^{**}(P^c) = \sigma^{**}(A) = A = x^a (x + 1)^b P^c.$$

We show that P is a Mersenne prime. By direct (Maple) computations, we get our result from Lemma 3.4.

Lemma 3.1. *The polynomial $\sigma^{**}(x^a(x+1)^b)$ does not split, so that ($a \geq 3$ or $b \geq 3$) and ($a \neq 2^n - 1$ or $b \neq 2^m - 1$ for any $n, m \geq 1$).*

Proof. If $\sigma^{**}(x^a(x+1)^b)$ splits, then $\sigma^{**}(x^a(x+1)^b) = x^b(x+1)^a$. Thus, $a = b$ and $\sigma^{**}(P^c) = P^c$. It contradicts Lemma 2.2-ii).

If $a, b \leq 2$ or ($a = 2^n - 1, b = 2^m - 1$ for some $n, m \geq 1$), then $\sigma^{**}(x^a)$ and $\sigma^{**}((x+1)^b)$ split. \square

Corollary 3.2. *The polynomial P is a Mersenne prime, $P \in \{M_1, M_4, M_5\}$. Moreover, $c = 2$ or $c = 2^\gamma - 1$, for some $\gamma \geq 1$ and $c \leq \min(a, b)$.*

Proof. By Lemma 3.1, there exists $m \geq 1$ such that $\sigma(x^{2m})$ or $\sigma((x+1)^{2m})$ divides $\sigma^{**}(A) = A$. Moreover, P does not divide $\sigma^{**}(P^c)$. We conclude that $P \in \{\sigma(x^{2m}), \sigma((x+1)^{2m})\}$. Thus, $2m \leq 4$ by Lemma 2.8-vi). By Corollary 2.4, $\sigma^{**}(P^c)$ must split. So, c takes the expected value. Furthermore, x^c and $(x+1)^c$ both divide $\sigma^{**}(A) = A$, because they divide $(1+P)^c = \sigma^{**}(P^c)$. So, $c \leq \min(a, b)$. \square

Lemma 3.3. *If a (resp. b) is even, then $a \geq 4$ (resp. $b \geq 4$).*

Proof. Put $P = 1 + x^{u_1}(x+1)^{v_1}$. If $a = 2$, then $b \geq 3$, $\sigma^{**}(x^a) = (1+x)^2$, $x^2 \parallel A = \sigma^{**}(A)$. By comparing a with the exponent of x in $\sigma^{**}(A)$, we get $a = 2^\beta + u_1c > 2$ if b is even, $a = 2^\beta - 1 + u_1c$ if b is odd, with $b = 2^\beta v - 1$. So, b is odd, $\beta = u_1 = c = 1$. We also have: $P = \sigma((x+1)^{v-1})$ and $c = 2^\beta \geq 2$, which is impossible. \square

Lemma 3.4. *i) If a is even, then $a \in \{4, 6, 8, 10\}$ and $c \in \{1, 2, 3, 7\}$.*

ii) If a is even and b odd, then $b \in \{2^\beta v - 1 : v \in \{1, 3, 5\}, \beta \in \{1, 2, 3\}\}$.

iii) If a and b are both odd, then $a, b \in \{1, 3, 5, 7, 9\}$ and $c \in \{1, 2, 3, 7\}$.

Proof. i): Since $a \geq 4$ (Lemma 3.3), put $a = 4r$ or $a = 4r + 2$, with $r \geq 1$. Then, $\sigma(x^{2r})$ divides $\sigma^{**}(A)$. So, $2r \leq 4$ and $c \leq a \leq 10$.

ii): Write $b = 2^\beta v - 1$, where v is odd. Since $\sigma((x+1)^{v-1})$ divides $\sigma^{**}(A) = A$, $v \in \{1, 3, 5\}$ and $2^\beta - 1 \leq a \leq 10$.

iii): Write $a = 2^\alpha u - 1$ and $b = 2^\beta v - 1$, where u, v are odd. As above, $u, v \in \{1, 3, 5\}$. $\sigma^{**}(x^a(x+1)^b)$ does not split, so $u \geq 3$ or $v \geq 3$. Moreover, $\alpha = 1$ (resp. $\beta = 1$) if $u \geq 3$ (resp. $v \geq 3$). We also get: $2^\beta - 1 \leq a$, $2^\alpha - 1 \leq b$.

If $\alpha = 1 = \beta$, then $a, b \leq 9$. If $\alpha = 1$ and $v = 1$, then $b = 2^\beta - 1 \leq a \leq 9$ so that $b \leq 7$. If $u = 1$ and $\beta = 1$, then $a = 2^\alpha - 1 \leq 7$ and $b \leq 9$. \square

4 Proof of Theorem 1.2

In this section, we set $A = x^a(x+1)^b P^c Q^d$, with $a, b, c, d \in \mathbb{N}^*$, P, Q odd irreducible, and $\deg(P) \leq \deg(Q)$. We suppose that A is b.u.p.:

$$\sigma^{**}(x^a) \cdot \sigma^{**}((x+1)^b) \cdot \sigma^{**}(P^c) \cdot \sigma^{**}(Q^d) = \sigma^{**}(A) = A = x^a(x+1)^b P^c Q^d.$$

We prove that $P \in \mathcal{M}$ (Lemma 4.1). Moreover, $Q \in \mathcal{M}$ or it is of the form $1 + x^{u_2}(x+1)^{v_2} P^{w_2}$, where $u_2, v_2, w_2 \geq 1$.

- Lemma 4.1.** *i) The polynomial P is a Mersenne prime.
ii) The integer d equals 2 or it is of the form $d = 2^\delta - 1$, with $\delta \in \mathbb{N}^*$.
iii) The polynomial Q is of the form $1 + x^{u_2}(x+1)^{v_2} P^{w_2}$, where $w_2 \in \{0, 1\}$.
iv) One has: $a, b \geq 3$ and $d \leq \min(a, b)$.
v) If $\sigma^{**}(P^c)$ does not split, then Q is its unique odd divisor.*

Proof. i): We remark that $1+P$ divides $\sigma^{**}(P^c)$. If $1+P$ does not split over \mathbb{F}_2 , then Q is an odd irreducible divisor of $1+P$ and we get the contradiction: $\deg(Q) < \deg(P) \leq \deg(Q)$.

ii): If d is even and if $d \geq 4$, then d is of the form $4r$ or $4r+2$. Thus, the odd polynomial $\sigma(Q^{2r})$ divides $\sigma^{**}(A) = A$, so we must have $P = \sigma(Q^{2r})$, which contradicts the fact: $\deg(P) \leq \deg(Q)$.

If $d = 2^\delta w - 1$ is odd (with w odd) and if $w \geq 3$, then $P = \sigma(Q^{w-1})$ and $\deg(P) > \deg(Q)$, which is impossible.

iii): From ii), $\sigma^{**}(Q^d) = (1+Q)^d$ so that $(1+Q)^d$ divides A . We may put: $1+Q = x^{u_2}(x+1)^{v_2} P^{w_2}$, for some $u_2, v_2, w_2 \in \mathbb{N}$, $u_2, v_2 \geq 1$.

iv): $a, b \geq 3$ because $1+x$ divide $\sigma^{**}(x^a)$, x divides $\sigma^{**}((x+1)^b)$ and $x(x+1)$ divides both $\sigma^{**}(P^c)$ and $\sigma^{**}(Q^d)$.

From the proof of iii), x^{du_2} and $(x+1)^{dv_2}$ both divide A . Thus, $d \leq \min(a, b)$.
v) is immediate. \square

4.1 Case where $Q \in \mathcal{M}$

We get Proposition 4.2 from Lemma 4.5, by direct computations.

Proposition 4.2. *If A is b.u.p., where $P, Q \in \mathcal{M}$, then $A, \bar{A} \in \{C_8, \dots, C_{13}\}$.*

Lemma 4.3. *The polynomials P and Q lie in $\mathcal{U} = \{M_1, M_2, M_3, M_4, M_5\}$.*

Proof. First, if $m \geq 1$ and if $\sigma(x^{2m})$ divides $\sigma^{**}(A)$, then $2m \leq 6$ and $\sigma(x^{2m}) \in \{M_1, M_4, M_2 M_3\}$.

If $P, Q \notin \mathcal{U}$, then neither P nor Q divides $\sigma^{**}(x^a)\sigma^{**}((x+1)^b)$. So, $P \mid \sigma^{**}(Q^d)$, $P = \sigma(Q^{2m})$ with $m \geq 1$. It is impossible since $\deg(P) \leq \deg(Q)$.

If $P \in \mathcal{U}$ but $Q \notin \mathcal{U}$, then Q does not divide $\sigma^{**}(x^a)\sigma^{**}((x+1)^b)$. Hence, it must divide $\sigma(P^{2^m})$, for some $m \geq 1$. Thus, $Q = \sigma(P^{2^m})$. We get the contradiction: $x^{u_2}(x+1)^{v_2} = 1 + Q = 1 + \sigma(P^{2^m})$ is divisible by P . \square

Lemma 4.4. *i) For $T \in \{P, Q\}$ and $m \geq 1$, $\sigma(T^{2^m})$ does not divide $\sigma^{**}(A)$.
ii) The exponents c and d lie in $\{2, 2^\gamma - 1 : \gamma \geq 1\}$.*

Proof. i): For example, if $T = P$ and if $\sigma(T^{2^m}) \mid \sigma^{**}(A) = A$, then we must have: $\sigma(T^{2^m}) = Q$, which is impossible (see the proof of Lemma 4.3).

ii): If c is even and $c \neq 2$, then put $c = 4r$ or $c = 4r + 2$, with $r \geq 1$. $\sigma(P^{2^r})$ divides $\sigma^{**}(A)$, which contradicts i).

If c is odd, then put $c = 2^\gamma u - 1$, with u odd and $\gamma \geq 1$. We also get a contradiction if $u \geq 3$, since $\sigma(P^{u-1})$ divides $\sigma^{**}(A)$.

The proof is similar for d . \square

Lemma 4.5. *The exponents a, b, c and d satisfy:*

$a \in \{4, 6, 8, 10, 12, 14\}$, $c, d \in \{1, 2, 3, 7\}$, if a is even

$b \in \{2^\beta v - 1 : \beta \in \{1, 2, 3\}, v \in \{1, 3, 5, 7\}\}$, if a is even and b odd

$a, b \in \{1, 3, 5, 7, 9, 11, 13\}$, $c, d \in \{1, 2, 3, 7\}$, if a and b are both odd.

Proof. We refer to Relations in (1) and in (3).

- If a is even, then $a \geq 4$, $a = 4r$ or $a = 4r + 2$ and $\sigma(x^{2^r})$ divides $\sigma^{**}(A)$. So, $2r \leq 6$ and $c, d \leq a \leq 14$.

- If a is even and b odd, then $2^\beta - 1 \leq a \leq 14$ and $v \leq 7$.

- If a and b are both odd, then $u \geq 3$ or $v \geq 3$, $u, v \leq 7$. As in the proof of Lemma 3.4, if $u, v \geq 3$, then $\alpha = 1 = \beta$, then $a, b \leq 13$. If $u \geq 3$ and $v = 1$, then $b = 2^\beta - 1 \leq a \leq 13$ so that $b \leq 7$. If $u = 1$ and $v \geq 3$, then $\beta = 1$, then $a = 2^\alpha - 1 \leq 7$ and $b \leq 13$. \square

4.2 Case where $Q \notin \mathcal{M}$

We prove Proposition 4.6.

Proposition 4.6. *If A is b.u.p., where $P \in \mathcal{M}$ but $Q \notin \mathcal{M}$, then $A, \bar{A} \in \{D_1, D_2\}$.*

4.2.1 Useful facts

As in Lemma 3.1, one has: $a \geq 3$ or $b \geq 3$. Lemma 4.1 allows to write: $P = 1 + x^{u_1}(x+1)^{v_1}$ and $Q = 1 + x^{u_2}(x+1)^{v_2}P^{w_2}$, with $u_i, v_j, w_2 \geq 1$. We obtain Corollaries 4.20, 4.25 and 4.27. Only, the last of them gives b.u.p. polynomials, namely D_1, D_2, \bar{D}_1 and \bar{D}_2 (see Section 5).

For any $g \geq 1$, PQ is not of the form $\sigma(P^{2g})$, because P does not divide $\sigma(P^{2g})$. We shall see that it suffices to consider three cases (replace A by \bar{A} , if necessary): $PQ = \sigma(x^{2m})$, $Q = \sigma(x^{2m})$, $Q = \sigma(P^{2m})$, for some $m \geq 1$.

Lemma 4.7. *i) Let $n \geq 1$ be such that $\sigma(x^{2n})$ (resp. $\sigma((x+1)^{2n})$, $\sigma(P^{2n})$) divides $\sigma^{**}(A)$, then $\sigma(x^{2n}) \in \{P, Q, PQ\}$ (resp. $\sigma((x+1)^{2n}) \in \{P, Q, PQ\}$, $\sigma(P^{2n}) = Q$).*

*ii) For any $n \geq 1$, $\sigma(Q^{2n})$ does not divide $\sigma^{**}(A)$.*

Proof. Recall that we suppose: $\sigma^{**}(A) = A$.

i): $\sigma(x^{2n})$, $\sigma((x+1)^{2n})$ and $\sigma(P^{2n})$ are all odd and squarefree (Lemma 2.9). Hence, they belong to $\{P, Q, PQ\}$ whenever they divide $\sigma^{**}(A)$, with $\sigma(P^{2n}) \notin \{P, PQ\}$.

ii): If $\sigma(Q^{2n}) \mid \sigma^{**}(A)$, then $P^m = \sigma(Q^{2n})$, with $m = 1$, by Lemma 2.8-i). So, we get the contradiction: $\deg(Q) \geq \deg(P) = 2n \deg(Q) > \deg(Q)$. \square

Lemma 4.8 ([2], Lemma 4, page 726).

The polynomial $1 + x(x+1)^{2^\nu - 1}$ is irreducible if and only if $\nu \in \{1, 2\}$.

Lemma 4.9. *If $\sigma(P^{2n})$ divides A for some $n \geq 1$, then $2n = 2^\gamma$, $2n - 1 \leq \min(a, b)$.*

Proof. Since $\sigma(P^{2n})$ is odd and square-free, Q must divide it. So $Q = \sigma(P^{2n})$. Put: $2n = 2^\gamma h$, with h odd.

We get: $1 + P + \dots + P^{2n-1} = \frac{1 + \sigma(P^{2n})}{P} = \frac{1 + Q}{P} = x^{u_2}(x+1)^{v_2}P^{w_2-1}$.

Thus, $w_2 = 1$ and $(1 + P)^{2^\gamma - 1}(1 + P + \dots + P^{h-1})^{2^\gamma} = 1 + P + \dots + P^{2n-1} = x^{u_2}(x+1)^{v_2}$. Hence, $h = 1$, $2n - 1 \leq (2^\gamma - 1)u_1 = u_2 \leq a$ and $2n - 1 \leq (2^\gamma - 1)v_1 = v_2 \leq b$. \square

Lemma 4.10. *i) Let $P = M_4$ and $Q = 1 + x^5(x+1)^{2^\nu - 1}P^{2^\nu - 1}$, with $\nu \geq 1$. Then, Q is irreducible if and only if $\nu = 2$.*

ii) Let $P \in \{M_1, M_4\}$ and $Q = 1 + x(x+1)^{2^\nu - 1}P^{2^\nu}$, with $\nu \leq 10$. Then, Q is irreducible if and only if $(\nu = 2, P = M_1)$ or $(\nu = 1, P = M_4)$.

iii) Let $P \in \{M_1, M_4\}$ and $Q = 1 + P(1 + P)^{2^\nu - 1}$. Then, Q is irreducible if and only if $P = M_1$ and $\nu \in \{1, 2\}$.

Proof. i): One has $Q = 1 + x^5(x+1)^{2^\nu - 1}P^{2^\nu - 1} = 1 + x^5(x^5 + 1)^{2^\nu - 1}$. The irreducibility of Q implies that $1 + x(x+1)^{2^\nu - 1}$ is irreducible. So, $\nu \in \{1, 2\}$ by Lemma 4.8.

If $\nu = 1$, then $Q = 1 + x^5 + x^{10} = (x^4 + x + 1)M_1M_5$ is reducible.

If $\nu = 2$, then $Q = 1 + x^5 + x^{10} + x^{15} + x^{20}$ which is irreducible.

ii): by direct (Maple) computations.

iii): The polynomial $U = 1 + x(x+1)^{2^\nu-1}$ must be irreducible, so $\nu \in \{1, 2\}$ by Lemma 4.8. Thus, $U \in \{M_1, M_4\}$.

If $P = U = M_1$, then $Q = 1 + x + x^4 = 1 + x(x+1)P$ is irreducible.

If $P = M_1$ and $U = M_4$, then $Q = 1 + x^3(x+1)^3P$ is irreducible.

If $P = M_4$ and $U = M_1$, then $Q = 1 + x(x+1)^3P = (x^6 + x^5 + x^4 + x^2 + 1)M_1$ is reducible.

If $P = U = M_4$, then $Q = 1 + x^3(x+1)^9P = (x^{12} + x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + x + 1)(1 + x + x^4)$ is reducible. \square

Lemma 4.11. *If $PQ = \sigma(x^{2n})$, then $(2n = 8, P = M_1, Q = 1 + x^3 + x^6)$ or $(2n = 24, P = M_4, Q = 1 + x^5(x^5 + 1)^3)$. Moreover, $Q, \overline{Q} \notin \{\sigma(x^{2g}), \sigma(P^{2g}) : g \geq 1\}$ and $PQ \notin \{\sigma(x^{2g}), \sigma((x+1)^{2g}) : g \geq 1\}$.*

Proof. Since $PQ = \sigma(x^{2n})$, we get $P = P^*$ or $P = Q^*$. But, here, $\deg(P) < \deg(Q)$. So, $P = P^*$ and $Q = Q^*$. Since P is a Mersenne prime and $P = P^*$, one has $P = M_1$ or $P = M_4$. If $P = M_1$, then by Lemma 2.8-iv), $Q = 1 + x^3(x+1)P = 1 + x^3 + x^6$. If $P = M_4$, then direct computations give $Q = 1 + x^5(x+1)^{2^\nu-1}P^{2^\nu-1}$. Since Q is irreducible, we get from Lemma 4.10-i), $\nu = 2$ and $Q = 1 + x^5(x^5 + 1)^3$. Thus, $Q \notin \{\sigma(x^6), \sigma((x+1)^6)\}$ (resp. $Q \notin \{\sigma(x^{20}), \sigma((x+1)^{20})\}$) if $P = M_1$ (resp. if $P = M_4$). We also remark that $\frac{\deg(Q)}{\deg(P)} \in \{3, 5\}$. So, $Q, \overline{Q} \notin \{\sigma(P^{2g}) : g \geq 1\}$. \square

Lemma 4.12. *If $Q = \sigma(x^{2n})$ with $n \geq 1$, then for some $\nu \geq 1$, $Q = 1 + x(x+1)^{2^\nu-1}M_1^{2^\nu}$ or $Q = 1 + x(x+1)^{2^\nu-1}M_4^{2^\nu}$. Moreover, $Q, \overline{Q} \notin \{\sigma(P^{2g}) : g \geq 1\}$ and $PQ \notin \{\sigma(x^{2g}), \sigma((x+1)^{2g}) : g \geq 1\}$.*

Proof. By direct computations, one has, for some $\nu \geq 1$: $2n = 2^\nu t$, $t \in \{3, 5\}$, $P = \sigma(x^{t-1})$ and $Q = 1 + x(x+1)^{2^\nu-1}P^{2^\nu}$. Hence, $P^{2^\nu} \parallel 1 + Q$.

If PQ is of the form $\sigma(x^{2g})$, then $P \parallel 1 + Q$ or $P^3 \parallel 1 + Q$ (Lemma 4.11), which is impossible.

Since $Q = \sigma(x^{2m})$, Lemma 4.14-i) implies that $Q \notin \{\sigma(P^{2m}), \sigma(\overline{P}^{2m})\}$. \square

Lemma 4.13. *If $Q = \sigma(P^{2n})$, then $2n \leq 4$, $P = M_1$, so that $Q \in \{1 + x(x+1)M_1, 1 + x^3(x+1)^3M_1\}$. Moreover, $Q, PQ \notin \{\sigma(x^{2g}), \sigma((x+1)^{2g}) : g \geq 1\}$.*

Proof. By direct computations, one has: $2n = 2^\nu$, $Q = 1 + P(1+P)^{2^\nu-1}$, for some $\nu \geq 1$. Since Q is irreducible, we get $\nu \in \{1, 2\}$ and $P = M_1$. Again, by direct computations, $Q, PQ \notin \{\sigma(x^{2g}), \sigma((x+1)^{2g}) : g \geq 1\}$. \square

Lemma 4.14. *i) For any $m, n \in \mathbb{N}^*$, $\sigma(P^{2m}) \neq \sigma(x^{2n})$, $\sigma((x+1)^{2n})$.*

ii) If $\sigma(x^{2n}) = \sigma((x+1)^{2n})$, then $\sigma(x^{2n}) \notin \{Q, PQ\}$.

Proof. i): Put $2n - 1 = 2^\alpha u - 1$ and $2m - 1 = 2^\beta v - 1$, with $\alpha, \beta \geq 1$.
If $\sigma(P^{2m}) = \sigma(x^{2n})$, then $P(1 + P + \dots + P^{2m-1}) = x(1 + x + \dots + x^{2n-1})$.
Thus, $P(P+1)^{2^\beta-1}(1+P+\dots+P^{v-1})^{2^\beta} = x(x+1)^{2^\alpha-1}(1+x+\dots+x^{u-1})^{2^\alpha}$.
Hence, $u \geq 3$ and $2^\alpha = 1$, which is impossible.
ii): One has $2n = 2^h - 2$, for some $h \geq 1$ (Lemma 2.8-vii)). If $Q = \sigma(x^{2n})$,
then by Lemma 4.12, $2^h - 2 = 2n = 2^\nu t$, with $t \in \{3, 5\}$. Therefore, $\nu = 1$,
 $t = 2^{h-1} - 1$, $h = 3 = t$, $2n = 6$ and $Q = M_2 M_3$ is reducible.
If $PQ = \sigma(x^{2n})$, then by Lemma 4.11, one has: ($2n = 8$, $P = M_1$ and
 $Q = 1 + x^3 + x^6$) or ($2n = 5 \cdot 2^\nu + 4$, $P = M_4$ and $Q = 1 + x^5(x+1)^{2^\nu-1}P^{2^\nu-1}$).
Thus, $2^h - 2 = 2n = 5 \cdot 2^\nu + 4$, $\nu = 1$, $h = 4$ and $Q = 1 + x^5(x+1)P =$
 $(x^4 + x + 1)M_1 M_5$ is reducible. \square

Without loss of generality, by Lemmas 4.11, 4.12 and 4.13, it suffices to consider the following three cases:

$$PQ = \sigma(x^{2m}), \quad Q = \sigma(x^{2m}), \quad Q = \sigma(P^{2m}), \text{ for some } m \geq 1.$$

In each case, we distinguish: (a, b both even), (a even, b odd), (a, b both odd).
We shall compare a, b, c or d with all possible values of the exponents of x ,
 $x + 1$, of P or of Q , in $\sigma^{**}(A)$.

According to Corollary 2.3 and Lemma 4.1, we get Lemma 4.15 from Relations in (1) and in (4).

Lemma 4.15.

- i) The polynomial P does not divide $\sigma^{**}(P^c)$, but it may divide $\sigma^{**}(Q^d)$.
- ii) One has: $u_2 d \leq a$, $v_2 d \leq b$, $w_2 d \leq c$, so that $d \leq \min(a, b, c)$.

4.2.2 Case where $PQ = \sigma(x^{2m})$, for some $m \geq 1$

We get, from Lemma 4.11, $Q, \bar{Q} \notin \{\sigma(x^{2g}), \sigma(P^{2g}) : g \geq 1\}$, ($2m = 8, P =$
 M_1 and $Q = 1 + x^3 + x^6 = 1 + x^3(x+1)P$) or ($2m = 24, P = M_4$ and
 $Q = 1 + x^5(x^5 + 1)^3 = 1 + x^5(x+1)^3 P^3$).

We refer to Relations in (1) and in (4).

Lemma 4.16. *On has: $c = 2$ or $c = 2^\gamma - 1$, $c \leq \min(a, b)$ and $d = 1$.*

Proof. Since $Q \neq \sigma(P^{2g})$ for any g , $\sigma^{**}(P^c)$ must split, so $c = 2$ or $c = 2^\gamma - 1$.
In this case, $\sigma^{**}(P^c) = (1 + P)^c$, where P is a Mersenne prime. So, x^c and
 $(x + 1)^c$ both divide $\sigma^{**}(A) = A$. Hence, $c \leq \min(a, b)$. Finally, $Q \parallel \sigma^{**}(A)$
because $Q, \bar{Q} \notin \{\sigma(x^{2g}), \sigma(P^{2g}) : g \geq 1\}$. Thus, $d = 1$. \square

Lemma 4.17. *At least, one of a and b is even.*

Proof. If a and b are both odd, then $PQ = \sigma(x^{u-1})$, $\sigma((x+1)^{v-1}) \in \{1, P\}$, $d = 2^\alpha$, $c = w_2d + 2^\alpha + \varepsilon_2 2^\beta$. It follows that c is even and $c \geq 4$, which contradicts Lemma 4.16. \square

Lemma 4.18. *If a and b are both even, then $a = 16$, $b \in \{4, 6\}$, $c \leq 3$, $P = M_1$ and $Q = 1 + x^3(x^3 + 1)$.*

Proof. Lemma 4.1-iv) implies that $a, b \geq 4$. Moreover, $PQ \in \{\sigma(x^{2r}), \sigma(x^{u-1})\}$. If $PQ = \sigma(x^{2r})$, then $P = \sigma((x+1)^{2s})$, $u = v = 1$ because $\gcd(\sigma(x^{2r}), \sigma(x^{u-1})) = 1 = \gcd(\sigma((x+1)^{2s}), \sigma((x+1)^{v-1}))$. Therefore, $2r = 8$, $a \neq 4r + 2$, $2s = 2$, $a = 16$, $b \in \{4, 6\}$. Furthermore, $c \leq b \leq 6$, so that $c \in \{1, 2, 3\}$. If $PQ = \sigma(x^{u-1})$, then $\sigma(x^{2r}) = P$ (by Lemma 4.7), which is impossible since $\gcd(\sigma(x^{2r}), \sigma(x^{u-1})) = 1$. \square

Lemma 4.19. *If a is even and b odd, then $a = 16$, $b \in \{1, 3, 7\}$, $c = 2$, $P = M_1$ and $Q = 1 + x^3(x^3 + 1)$.*

Proof. As above, a even implies that $a = 4r = 16$ and $P = M_1$. One has: $\sigma((x+1)^{v-1}) \in \{1, P\}$. So, $v \in \{1, 3\}$, $c = 1 + w_2d + \varepsilon_2 2^\beta$, where $w_2 = 1 = d$. Thus, $c = 2$, $v = 1$, $2^\beta - 1 + 3 + 2 \leq a = 16$, $\beta \leq 3$ and $b \in \{1, 3, 7\}$. \square

Corollary 4.20. *If A is b.u.p., with PQ of the form $\sigma(x^{2m})$, then $P = M_1$, $Q = 1 + x^3(x^3 + 1)$, $a, b \in \{1, 3, 4, 6, 7, 16\}$, $c \leq 3$ and $d = 1$.*

4.2.3 Case where $Q = \sigma(x^{2m})$, for some $m \geq 1$

One has (Lemma 4.12): $Q, \bar{Q} \notin \{\sigma(P^{2g}) : g \geq 1\}$, $PQ \notin \{\sigma(x^{2g}), \sigma((x+1)^{2g}) : g \geq 1\}$, $2m \geq 10$, $P \in \{M_1, M_4\}$ and $Q = 1 + x(x+1)^{2^\nu-1}P^{2^\nu}$, for some $\nu \in \mathbb{N}^*$. So, $u_1 = u_2 = 1$, $v_1 \in \{1, 3\}$, $v_2 = 2^\nu - 1$ and $w_2 = 2^\nu$. Moreover, $Q \neq \sigma((x+1)^{2m})$ (Lemma 4.14).

We consider Relations in (1) and in (4).

Lemma 4.21. *One has: ($c = 2$ or $c = 2^\gamma - 1$) and $d \leq 3$.*

Proof. If $\sigma^{**}(P^c)$ does not split, then Q is the unique odd irreducible divisor of $\sigma^{**}(P^c)$. It contradicts the fact that Q is not of the form $\sigma(P^{2g})$. So, $\sigma^{**}(P^c)$ splits and ($c = 2$ or $c = 2^\gamma - 1$). The exponent of Q in $\sigma^{**}(A)$ lies in $\{1, 2, 2^\alpha, 2^\beta, 1 + 2^\alpha, 1 + 2^\beta, 2^\alpha + 2^\beta\}$. So, by Lemma 4.1-ii), $d \leq 3$. \square

Lemma 4.22. *At least, one of a and b is even.*

Proof. If a and b are both odd, then $Q = \sigma(x^{u-1})$, $Q \neq \sigma((x+1)^{v-1})$ (by Lemma 4.14-ii)) and $\sigma((x+1)^{v-1}) \in \{1, P\}$. Thus, $v \in \{1, 3, 5\}$, $2^\alpha = d \leq 3$, $\alpha = 1$, $d = 2$, $c = 2 \cdot 2^\nu + \varepsilon_2 2^\beta$. So, c is even and $c \geq 4$. It contradicts Lemma 4.21. \square

Lemma 4.23. *If a and b are even, then $\nu \leq 2$, $20 \leq a \leq 26$, $b \leq 10$, $d = 1$, $c \in \{1, 2, 3, 7\}$, and $(P, Q) \in \{(M_1, 1 + x(x+1)^3 P^4), (M_4, 1 + x(x+1)P^2)\}$.*

Proof. One has: $Q \in \{\sigma(x^{2r}), \sigma(x^{u-1})\}$.

- If $Q = \sigma(x^{2r})$, then $Q \neq \sigma((x+1)^{2s})$ (by Lemma 4.14-ii)), Q does not divide $\sigma(x^{u-1})$ since $\gcd(\sigma(x^{2r}), \sigma(x^{u-1})) = 1$. So, $Q \parallel_{\sigma^{**}}(A)$. Therefore, $d = 1$, $P = \sigma((x+1)^{2s})$, $\sigma(x^{u-1}) \in \{1, P\}$, $u \in \{1, 3, 5\}$, $v = 1$, $2s \leq 4$, $b \leq 10$, $c = 2^\nu + \varepsilon_1 2^\alpha + 1 \geq 3$. Since $2^\alpha + c \leq b \leq 10$, we get: $c \in \{1, 2, 3, 7\}$, $\alpha \leq 2$, $\nu \leq 2$.

Here, $Q = 1 + x(x+1)^{2^\nu-1} P^{2^\nu}$, with $P \in \{M_1, M_4\}$ and $\nu \leq 2$. By Lemma 4.10-ii), one has: ($P = M_1$, $\nu = 2$ and $2r = 12$) or ($P = M_4$, $\nu = 1$ and $2r = 10$). So, $20 \leq a \leq 26$.

- If $Q = \sigma(x^{u-1})$, then $2^\alpha = d \leq 3$ and $P = \sigma(x^{2r}) = \sigma((x+1)^{2s})$. Thus, $d = 2$, $2r = 2s = 2$, $a, b \in \{4, 6\}$, $c = 2 + w_2 d = 2 + 2w_2 \geq 4$. It contradicts Lemma 4.21. \square

Lemma 4.24. *The case where a is even and b odd does not happen.*

Proof. If a is even and b odd, then $Q \in \{\sigma(x^{2r}), \sigma(x^{u-1})\}$.

- If $Q = \sigma(x^{2r})$, then $d = 1$, $\sigma(x^{u-1}), \sigma((x+1)^{v-1}) \in \{1, P\}$, $u, v \in \{1, 3, 5\}$, $w_2 d = 2^\nu$, $c = 2^\nu + \varepsilon_1 2^\alpha + \varepsilon_2 2^\beta$ is even.

Therefore, $c = 2$, $\nu = 1$, $\varepsilon_1 = \varepsilon_2 = 0$ and $u = v = 1$.

By Lemma 4.10-ii), since $\nu = 1$, one has: $P = M_4$ and thus $v_1 = 3, v_2 = 1, w_2 = 2$, $2r = \deg(Q) = 2^\nu(1 + \deg(P)) = 2^\nu \cdot 5 = 10$. We get the contradiction: $a \in \{20, 22\}$ and $a = 2^\beta - 1 + 2u_1 + u_2 = 2^\beta - 1 + 2 + 1 = 2^\beta + 2$.

- If $Q = \sigma(x^{u-1})$, then $a > u - 1 = 2m \geq 10$, $P = \sigma(x^{2r})$, $2^\alpha = d \leq 3$. Hence, $d = 2$, $2r \leq 4$, $a \in \{4, 6, 8, 10\}$. We get the contradiction: $a > 10 \geq a$. \square

Corollary 4.25. *If A is b.u.p., with Q of the form $\sigma(x^{2m})$, then*

$(P, Q) = (M_1, 1 + x(x+1)^3 M_1^4)$ or $(P, Q) = (M_4, 1 + x(x+1)M_4^2)$,

$a, b \in \{4, 6, 8, 10, 20, 22, 24, 26\}$, $c \in \{1, 2, 3, 7\}$, $d = 1$.

4.2.4 Case where $Q = \sigma(P^{2m})$, for some $m \geq 1$

Lemma 4.13 implies that $Q, PQ \notin \{\sigma(x^{2g}), \sigma((x+1)^{2g}) : g \geq 1\}$. $P = M_1$ and ($Q = \sigma(P^2) = 1 + x(x+1)P$ or $Q = \sigma(P^4) = 1 + x^3(x+1)^3 P$). Thus, $u_1 = v_1 = 1$, $u_2 = v_2 \in \{1, 3\}$, $w_2 = 1$.

Lemma 4.26. *The integer $a + b$ is odd, $a, b \leq 11$, $c \leq 8$ and $d \leq 3$.*

Proof. We refer to Relations in (1) and in (4). Lemma 4.7 is also useful.
If c is even, then $2m = 2t \geq 2$, $\sigma(P^{2t}) = Q$. So, $w = 1, d = 1$. If c is odd, then $Q = \sigma(P^{w-1}), w \in \{3, 5\}, d = 2^\gamma$.
- If a and b are even, then $a, b \geq 4$ (by Lemma 4.1-iv)), $P = \sigma(x^{2r}) = \sigma((x+1)^{2s})$. Hence, $u = v = 1, 2r = 2s = 2, a, b \leq 6$ and $c = 2 + d$ (by considering the exponents of P). We get a contradiction on the value of c .
- If a and b are odd, then $\sigma(x^{u-1}), \sigma((x+1)^{v-1}) \in \{1, P\}$, so that $u, v \leq 3$. Moreover, if c is even, then $\sigma(P^{2t}) = Q, w = 1, d = 1$ and $c \in \{1, 1 + 2^\alpha, 1 + 2^\beta, 1 + 2^\alpha + 2^\beta\}$. It contradicts the parity of c . If c is odd, then $Q = \sigma(P^{w-1}), w \in \{3, 5\}, d = 2^\gamma$, so that $d = 2$ and $c \in \{2, 2 + 2^\alpha, 2 + 2^\beta, 2 + 2^\alpha + 2^\beta\}$. We also get a contradiction on the value of c .
- If a is even and b odd, then $a \geq 4$ (Lemma 4.1), $\sigma(x^{2r}) = P = M_1, u = 1, 2r = 2, a \leq 6$. Moreover, $\sigma((x+1)^{v-1}) \in \{1, P\}$, so $v \leq 3$. We get $\beta \leq 2, b \leq 11, d \leq 3$ and $c \leq 8$ because $2^\beta - 1 \leq a \leq 6, d \leq a \leq 6$ and $c \in \{1 + d, 1 + 2^\beta + d\}$.
The proof is similar if a is odd and b even. □

Corollary 4.27. *If A is b.u.p., with Q of the form $\sigma(P^{2m})$, then $P = M_1, Q \in \{1 + x(x+1)P, 1 + x^3(x+1)^3P\}$, $a + b$ is odd, $a, b \leq 11, c \leq 8, d \leq 3$.*

5 Maple Computations

The function σ^{**} is defined as Sigm2star, for the Maple code.

```
> Sigm2star1:=proc(S,a) if a=0 then 1;else if a mod 2 = 0
then n:=a/2:sig1:=sum(S^l,l=0..n):sig2:=sum(S^l,l=0..n-1):
Factor((1+S)*sig1*sig2) mod 2:
else Factor(sum(S^l,l=0..a) mod 2:fi:fi:end:
> Sigm2star:=proc(S) P:=1:L:=Factors(S) mod 2:k:=nops(L[2]):
for j to k do S1:=L[2][j][1]:h1:=L[2][j][2]:
P:=P*Sigm2star1(S1,h1):od:P:end:
```

We search all $S = x^a(x+1)^b P^c$ or $S = x^a(x+1)^b P^c Q^d$ such that $\sigma^{**}(S) = S$.

5.1 Case where $\omega(A) = 3$

We have proved that $P \in \{M_1, M_4, M_5\}$. By means of Lemma 3.4. We obtain C_1, \dots, C_7 .

5.2 Case where $\omega(A) = 4$ with $P, Q \in \mathcal{M}$

We have shown that $P, Q \in \{M_1, M_2, M_3, M_4, M_5\}$. From Lemma 4.5, we obtain C_8, \dots, C_{13} .

5.3 Case where $\omega(A) = 4$ with $P \in \mathcal{M}, Q \notin \mathcal{M}$

We apply Corollaries 4.20, 4.25 and 4.27.

- 1) If Q or PQ is of the form $\sigma(x^{2^m})$, then we obtain no b.u.p. polynomials.
- 2) If Q is of the form $\sigma(P^{2^m})$, then we get D_1, D_2, \overline{D}_1 and \overline{D}_2 .

References

- [1] J. T. B. BEARD JR, *Bi-Unitary Perfect polynomials over $GF(q)$* , *Annali di Mat. Pura ed Appl.* **149(1)** (1987), 61–68.
- [2] E. F. CANADAY, *The sum of the divisors of a polynomial*, *Duke Math. J.* **8** (1941), 721–737.
- [3] 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.
- [4] 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.
- [5] L. H. GALLARDO, O. RAHAVANDRAINY, *All unitary perfect polynomials over \mathbb{F}_2 with at most four distinct irreducible factors*, *Journ. of Symb. Comput.* **47(4)** (2012), 492–502.
- [6] L. H. GALLARDO, O. RAHAVANDRAINY, *Characterization of Sporadic perfect polynomials over \mathbb{F}_2* , *Functiones et Approx.* **55(1)** (2016), 7–21.