Gulf Journal of Mathematics
Vol 12, Issue 2 (2022) 39-48

ISSN: 2309-4966
https://doi.org/10.56947/gjom.v12i2.722

ON THE EQUATION $\prod_P \Phi_3(P) = \prod_P P^2$ OVER $\mathbb{F}_2[x]$

LUIS H. GALLARDO[1*]

Abstract. We study a polynomial variant of an arithmetic problem solved by Steuerwald in 1937. More precisely, we prove, under a mild condition, that the equation on the title, has no solutions $A := \prod_P P^2 \in \mathbb{F}_2[x]$, with irreducible P, and $\omega(A) < 16$. Unconditionally, we prove that $\deg(P) \geq 40$. This improves on known results.

1. Introduction

Steuerwald [26] proved in 1937 that there is no odd perfect number n of the form $n := p^k p_1^2 \cdots p_m^2$, where p and the p_j are distinct odd prime numbers, and $k = 1 \pmod 4$. In other words, the equation $2n = \sigma(n)$, or

$$2p^k \prod_{p_j} p_j^2 = \sigma(p^k) \prod_{p_j} \Phi_3(p_j), \tag{1.1}$$

do not hold.

Since the ring of binary polynomials $\mathbb{F}_2[x]$ appears to be the closest arithmetic ring to the ring of integers $\mathbb{Z}$, we are interested, in this paper, to study an analogue equation (the equation on the title over $\mathbb{F}_2[x]$) to the equation (1.1). Generally, an arithmetic problem over the integers, translated to polynomials, is easier to manage, since we have more tools available in $\mathbb{F}_2[x]$, for example, the formal derivation ($P \mapsto P'$), whose kernel in $\mathbb{F}_2[x]$ are the squares (a more general notion of derivation appears in [4, 18]). However, in our specific case, the polynomial problem is much more complicated, thus more interesting, and we are forced to consider it only under some mild condition.

In order to explain in more detail our work in the analogue of (1.1), we consider an irreducible (*prime*) polynomial $f(x)$ over a finite field $\mathbb{F}_q$, of characteristics p, and a rational fraction $g(x) := g_1(x)/g_2(x)$ over the same field. What properties have the composite polynomial $F(x) = g_2(x)^{deg(f(x))} f(g(x))$? (see [1, 2, 3, 5, 6, 8, 9, 19, 20, 21, 23, 24, 25]). More generally, $g(x)$ has been chosen as a power of x, as a *linearized* polynomial, e.g., $g(x) = x^{p^r} - x$, or as an appropriate quotient A/B of two other polynomials. In particular, recently Panario et al. [23] worked on the case $g(x) = 1/(cx + 1) \neq 1$, in order to obtain conditions such that

Date: Received: Oct 22, 2021; Accepted: Mar 8, 2022.

* Corresponding author.

2010 *Mathematics Subject Classification.* Primary 11T55, 11T06; Secondary 11A07.

Key words and phrases. Cyclotomic polynomials, characteristic 2, fixed points of σ, factorization.

$f(x)$ irreducible implies $F(x)$ irreducible. More generally, one finds in Lidl and Niederreiter [22], and in Swan [27], the most basic results about polynomials over finite fields, including results about the factorization of these polynomials. Work on some special quotients of $\mathbb{F}_q[x]$ when $q = 2^d$ appear in [28].

In the present paper we work on a related problem, in which $P := g(x) \in \mathbb{F}_2[x]$ (a *binary* polynomial), is a (prime) polynomial (i.e., $g_2(x) := 1$), $f(x) = \Phi_3(x) = x^2 + x + 1$, is the 3-th cyclotomic polynomial, and given a square $A \in \mathbb{F}_2[x]$, we consider an invariant property of the product of P^2, over all prime divisors P of A, in which appears naturally the product over the same primes of the composite polynomial $F(x) = \Phi_3(P)$. Namely, we are interested in possible solutions in primes $P \in \mathbb{F}_2[x]$ of the following equation (natural analogue of the equation (1.1) studied by Steuerwald):

$$\prod_P \Phi_3(P) = \prod_P P^2. \tag{1.2}$$

In order to explain a little more the motivation of our interest in the specific equation (1.2), i.e., explain why we consider this equation as a good polynomial analogue of (1.1), we give some notation that will be useful throughout the paper. A binary polynomial B is *odd* if $B(0) = B(1) = 1$, otherwise B is *even*. A *minimal* prime of an odd polynomial A is a prime divisor P of A that has minimal degree. Analogously, a *maximal* prime of an odd polynomial A is a prime divisor P of A that has maximal degree. A prime divisor of A that is neither minimal, nor maximal is a *medium* prime [11]. We let $\omega(A)$ denote the number of distinct prime factors of A over $\mathbb{F}_2$.

Consider the function $\sigma\colon \mathbb{F}_2[x] \mapsto \mathbb{F}_2[x]$ defined over a polynomial $A \in \mathbb{F}_2[x]$ by $\sigma(A) = \sum_{D|A} D \in \mathbb{F}_2[x]$, i.e., by the sum of all divisors of A, including 1 and A. The function σ is *multiplicative*, i.e., for coprime binary polynomials X, Y one has, as over the integers $\mathbb{Z}$, $\sigma(XY) = \sigma(X)\sigma(Y)$. This σ function is more natural, but also more complex, than the usual sum of divisor function $\sigma_1(A) = \sum_{D|A} 2^{\deg(A)}$. We consider this function σ as the natural analogue on $\mathbb{F}_2[x]$ of the usual sum of divisors function over the integers $\mathbb{Z}$ (see [17]). For instance, some divisors D of A can sum up to 0, while a sum over D of $2^{\deg D}$ is always greater than 0. We recall that a *binary perfect* polynomial A is defined by the equality $\sigma(A) = A$, i.e., $\sigma(A)/A$ belongs to the ring $\mathbb{F}_2[x]$. We can also say that A is a *fixed* point of the σ function (see [7, 10, 11, 12, 13, 14, 15, 16]). This corresponds by our analogy between $\mathbb{F}_2[x]$ and $\mathbb{Z}$, to a multiperfect number n in the ring of integers, i.e., a positive integer n with the property that $\sigma(n)/n$ belongs to the ring $\mathbb{Z}$ (a slightly more general property than the study of the perfect numbers, i.e., the usual case when $\sigma(n)/n = 2$). Canaday [7], the first Ph.D. student of Leonard Carlitz, started the work on binary perfect polynomials in 1941. Finally, when A is odd perfect and equals the square of a square-free polynomial, we say that A is *special perfect* [11]. It is known that a perfect polynomial A must have an even number of minimal primes, [11, Lemma 2.3]. No analogue result is known for the parity of the number of medium or maximal primes dividing a perfect polynomial. No odd perfect polynomial A is known, besides the trivial perfect $A = 1$. The only general result known about odd perfect polynomials A is that

A must be a square [7] (this explains why the divisor p^k of n in (1.1) has no analogue in (1.2)).

First, solving (1.2) is a problem of factorization. Thus, a difficult issue, since we do not know many things about the primes P in $\mathbb{F}_2[x]$. Moreover, when $\deg(P) > 1$, no general results are known about the factorization of the composed cyclotomic polynomial $\Phi_n(P)$, even for our special case $n = 3$. But the main motivation of our interest in equation (1.2) comes from the simple fact that σ is multiplicative, and

$$\Phi_n(P) = \sigma(P^{n-1}) \tag{1.3}$$

for prime n and prime P. This implies that the equation (1.2), with $A := \prod_P P^2$, is exactly equivalent to the following equation, in the unknown $A \in \mathbb{F}_2[x]$:

$$\sigma(A) = A. \tag{1.4}$$

In other words, in this paper, we are interested in the existence of special perfect polynomials (fixed points of the σ function that are the product of squares of primes in $\mathbb{F}_2[x]$).

Equation (1.4) seems very difficult to resolve. The contribution of the present paper consists of proving the non-existence of solutions with a small number of distinct prime divisors, under a mild condition (see Theorem 1.2 (a)) on the number of distinct prime divisors that must have some polynomials related to the maximal prime divisors of special perfect polynomials [11]. We also, in Theorem 1.2 (b), bound below the degree of these prime divisors as well as the degree of a possible solution A.

More precisely, we first quote the most important of the known results about these special perfect polynomials [11, Theorem 5.5], (see also Lemma 2.5) as follows:

Theorem 1.1. (a) *Any special perfect polynomial A has $\omega(A) \geq 10$.*
(b) *For any prime divisor P of A we have $\deg(P) \geq 30$.*

The following theorem is our main result.

Theorem 1.2. *Let $A = p_1^2 \cdots p_m^2 \in \mathbb{F}_2[x]$ be a special perfect polynomial with $\omega(A) = m$, $d_k := \deg(p_k)$, for all $k = 1, \ldots, m$, and $d_1 \leq \cdots \leq d_m$. In particular, p_1 is minimal, and p_m is maximal. Let P^* be a minimal prime divisor of A. Then,*

(a) *Assume that for any maximal prime M dividing A, for which $M \mid \phi_3(p_j)$, with p_j maximal prime, we have $\omega(\phi_3(p_j)) = 2$. Then, there is no such polynomial A with $\omega(A) < 16$.*
(b) *We have, unconditionally, that $\deg(P^*) \geq 40$ and, on the condition in* (a), *that $\deg(A) \geq 1364$.*

Observe also that the computational part of the proof of the theorem concerns only part (b). Proving part (a), does not require computer computations; it required exploiting carefully a simple new idea, as is explained below.

Remark 1.3. Our main new idea for improving Theorem 1.1, is to focus on the k maximal primes that divide a possible special perfect polynomial $A := \prod_{s=1}^{r} p_s^2$. There are three different types of prime divisors of $\sigma(P^2)$, with P maximal prime: minimal, medium, or maximal. Thus, we need a condition to reduce this freedom. We choose the condition in part (a) of the theorem since this restrict the prime divisors of $\sigma(P^2)$, to the maximal ones (see Lemma 2.4), so that, we can obtain a contradiction that will bar A to be perfect, provided that m is small (i.e., $\omega(A) < 16$).

Observe that (with the notations in the Theorem) M cannot divide $\Phi_3(Q)$ with Q a minimal prime, while M does divide $\Phi_3(R)$ with medium R (see Lemma 2.3). But we have no information on the possible prime factors of $\Phi_3(S)/M$, where S is a maximal prime such that M divides $\Phi_3(S)$.

Finally, observe that there are few general theorems to study the properties of factors of binary polynomials. Thus, work done on solving (even conditionally) the equation (1.2) (i.e., (1.4)) might help to advance our understanding of these factors.

The rest of the paper is organized as follows: In section 2 we quote the more important results of [11] that are required for the proof of part (a) of the theorem. Another result of the same paper, useful for computations, is also quoted. We will also display, in the same section, some details about the computer calculations done that lead to the proof of part (b) of the theorem. The proof of Theorem 1.2 appears in section **??**.

2. Tools

The following lemma [11, Lemma 2.3] is used in the proof of parts (b) of the theorem.

Lemma 2.1. *Let q be a power of 2. Let $A \in \mathbb{F}_q[x]$ be a perfect polynomial. Let $p_1, \ldots, p_r$ be the list of all monic minimal primes of A. Then the integer r is even.*

The following two lemmas [11, Lemma 4.1 and Lemma 4.2] are important for the proof of part (a) of the theorem.

Lemma 2.2. *Let P, Q be two distinct prime divisors of the same degree d of a special perfect polynomial A. If Q divides $\Phi_3(P)$ then P does not divide $\Phi_3(Q)$.*

Parts (a),(b), and (c) of the following lemma follows from [11, Lemma 4.2]. Part (d) is [11, Corollary 4.4]. Part (e) follows from parts (a), and (b). Part (f) follows from Lemma 2.2.

Lemma 2.3. *Let $P \in \mathbb{F}_2[x]$ be a maximal prime of a special perfect polynomial $A = p_1^2 \cdots p_m^2 \in \mathbb{F}_2[x]$, with $\omega(A) = m$, $d_k := \deg(p_k)$, for all $k = 1, \ldots, m$, and $d_1 \leq \cdots \leq d_m$. In particular, p_1 is minimal, and p_m is maximal. Then, there exists a unique pair (i, j), $i, j \in \{1, \ldots, m\}$ such that:*

(a) *$p_j \neq P$, $d_1 < d_i < d_j = \deg(p_j) = \deg(P) = d_m$. In other words, p_j is maximal, while p_i is medium.*

(b) *We have* $P \mid p_i^2 + p_i + 1$ *and* $P \mid p_j^2 + p_j + 1$, *so that* $P = p_i + p_j + 1$. *In particular,* P *cannot divide* $\Phi_3(Q_1)$ *and* $\Phi_3(Q_2)$ *for any two distinct maximal divisors* Q_1, Q_2 *of* A.
(c) *Set* $1 + p_i + p_i^2 = PR$ *then* $0 < \deg(R) < d_i$ *so that* $d_m < 2d_i$.
(d) *Let* m_2 *be the number of medium primes that divide* A, *and* m_3 *the number of maximal primes that divide* A. *Then*

$$m_2 \geq m_3 \geq 3.$$

(e) *We have that* $P \nmid \Phi_3(S)$ *for any minimal prime divisor* S *of* A.
(f) *Let* Q *be maximal prime dividing* A. *It is impossible to have simultaneously that* P *divides* $\Phi_3(Q)$, *and that* Q *divides* $\Phi_3(P)$.

The following lemma is important for our approach:

Lemma 2.4. *Let* P *be a maximal prime of a special perfect polynomial* A. *Let* Q *be a maximal prime divisor of* A *such that* $P \mid \Phi_3(Q)$, *as guaranteed by Lemma 2.3* (b), *and put* $S := \Phi_3(Q)/P$. *Assume that* $\omega(\Phi_3(Q)) = 2$. *Then,* S *is a maximal prime divisor of* A *such that*

$$\Phi_3(Q) = P \cdot S. \tag{2.1}$$

Proof. Let d be the common degree of the maximal prime divisors of A. Observe that $P \nmid S$, since if $P \mid S$ then $P^2 \mid \Phi_3(Q)$. Observe that both P^2 and $\Phi_3(Q)$ have degree $2d$. Thus, by comparing degrees, we get $\Phi_3(Q) = P^2$. This is impossible since this implies that the prime Q is a square: $Q = (1+Q)^2 + P^2 = (1+Q+P)^2$. Therefore, $\gcd(P, S) = 1$. It follows from $\omega(\Phi_3(Q)) = 2$ that $\omega(S) = 1$. Thus, S is a power of a prime. But S is also a divisor of the special perfect A. Hence either S is prime itself, or $S = R^2$ with R prime. We claim that the latter is impossible. Assume, contrary that we want to prove, that $S = R^2$ with prime R. By Lemma 2.3 (b), there exists a medium prime V such that $P \mid \Phi_3(V)$ and $\Phi_3(V) = P \cdot W$ with:

$$0 < \deg(W) < \deg(V). \tag{2.2}$$

Thus

$$(Q+V)(Q+V+1) = (Q+V)^2 + Q + V = \Phi_3(Q) + \Phi_3(V) = P(W + R^2). \tag{2.3}$$

But by Lemma 2.3 (b) we have $P = Q + V + 1$, thus it follows from (2.3) that

$$P + 1 = Q + V = W + R^2, \tag{2.4}$$

so that

$$P = W + (R+1)^2. \tag{2.5}$$

By derivation of (2.5) relative to x, we get then:

$$P' = W'. \tag{2.6}$$

But from derivation of $\Phi_3(V) = P \cdot W$ we get using (2.6)

$$V' = P'W + PW' = P'(W + P). \tag{2.7}$$

Observe that $\deg(W) < \deg(V) < \deg(P)$ by (2.2), and since V is a medium prime and P is a maximal prime. By taking degrees on both sides of (2.7), we obtain

$$\deg(V) > \deg(V') = \deg(P') + \deg(P) > \deg(P). \tag{2.8}$$

But, clearly, (2.8) is impossible since V is a medium prime and P is a maximal prime. This proves the result, since, by this contradiction, S must be prime. □

The following lemma [11, Lemma 5.3 and Corollary 5.4] are used for computations. It also appears, without proof, in [7, Theorem 21].

Lemma 2.5. *Let $A \in \mathbb{F}_2[x]$ be a special perfect polynomial. Let $P \in \mathbb{F}_2[x]$ be a prime divisor of A. Then*

(a) *P is congruent to 1 modulo $x^2 + x + 1$, and*
(b) *$\deg(P)$ is even.*
(c) *Assume, furthermore, that P is minimal. Then P, all prime divisors Q of $\Phi_3(P)$, all prime divisors R of $\Phi_3(Q)$, and all prime divisors of $\Phi_3(R)$ are congruent to 1 $\pmod{x^2 + x + 1}$ and have even degree.*

The following lemma follows from a computation using Lemma 2.5 and a straightforward computer program in gp-PARI. The computation lasted several days. More precisely, 21 days, 18 hours, and 45 minutes. For example, the case $\deg(P) = 30$ took 1 hour and 23 minutes; the case $\deg(P) = 34$ took 1 day, and 11 minutes, while the case $\deg(P) = 38$ took 16 days, 7 hours, and 58 minutes.

Lemma 2.6. *There is no minimal prime P that divides a special perfect polynomial A when $\deg(P) \in \{30, 32, 34, 36, 38\}$.*

Proof. We computed all prime polynomials of degree $d \in \{30, 32, 34, 36, 38\}$ such that conditions (a) and (b) of Lemma 2.5 hold. None of them satisfy the conclusion of Lemma 2.5 (c). This proves the result. □

2.1. **We assume that $k = 3$.** Let P, Q and R be the 3 maximal primes dividing A. By Lemma 2.3 (a) we can assume that $P \mid \Phi_3(Q)$. Since $Q \nmid \Phi_3(Q)$ and, by Lemma 2.3 (f), $Q \nmid \Phi_3(P)$, we must have by Lemma 2.3 (a) that $Q \mid \Phi_3(R)$, analogously, we get that $R \mid \Phi_3(P)$.

Write for appropriate polynomials M_1, M_2, M_3, $\Phi_3(Q) = PM_1, \Phi_3(R) = QM_2$, and $\Phi_3(P) = RM_3$. Since all maximal polynomials have the same degree, it follows, by hypothesis (a) and Lemma 2.4, that M_1, M_2 and M_3 are maximal prime divisors of A. Since $\Phi_3(Q), \Phi_3(P)$, and $\Phi_3(Q)$ are not squares in $\mathbb{F}_2[x]$, the unique possibility left is that we have $M_1 = R, M_2 = P$ and $M_3 = Q$. Thus, $P \mid \Phi_3(Q)$ and $P \mid \Phi_3(R)$. This contradicts Lemma 2.3 (b), thus $k > 3$.

2.2. **We assume that $k = 4$.** Let P_1, P_2, P_3 and P_4 be the 4 maximal primes that divide A. By Lemma 2.3 (a) we can assume that $P_1 \mid \Phi_3(P_2)$, so that $P_2 \nmid \Phi_3(P_1)$ by Lemma 2.3 (f). We can also assume that $P_2 \mid \Phi_3(P_3)$. Thus, as before, $P_3 \nmid \Phi_3(P_2)$.

We claim that $P_3 \nmid \Phi_3(P_1)$. Assume, to the contrary, that $P_3 \mid \Phi_3(P_1)$. Since P_2 and P_1 are maximal primes, hypothesis (a) and Lemma 2.4 imply that $\Phi_3(P_2)/P_1$

is also a maximal prime (distinct from P_1, since $\Phi_3(P_2)$ is not a square). Since $P_3 \nmid \Phi_3(P_2)$, and trivially $P_2 \nmid \Phi_3(P_2)$ we have

$$\Phi_3(P_2) = P_1P_4. \tag{2.9}$$

But P_1, P_2 and P_3 cannot divide $\Phi_3(P_1)/P_3$, thus the only possibility that remains is that $\Phi_3(P_1) = P_3P_4$. Hence, P_4 divides $\Phi_3(P_1)$ and, from (2.9),P_4 divides also $\Phi_3(P_2)$. But this is impossible by Lemma 2.3 (b), thereby proving the claim.

Thus, $P_3 \mid \Phi_3(P_4)$ (since trivially, $P_3 \nmid \Phi_3(P_3)$). Put $\Phi_3(P_4) := P_3M$, with M a maximal prime divisor of A, guaranteed by hypothesis (a) and Lemma 2.4. One sees that P_1 cannot divide $S_4 := \Phi_3(P_4)$, by Lemma 2.3 (b), since $P_1 \mid \Phi_3(P_2)$; trivially $P_4 \nmid S_4$; also, S_4 not being a square, we obtain that $P_3 \nmid S_4$, and, again by Lemma 2.3 (b), we have that $P_2 \nmid S_4$, since, by (2.9), we have $P_4 \mid \Phi_3(P_2)$. This is impossible. This finishes the proof that the case $k = 4$ does not happen. Therefore, $k > 4$.

2.3. **About the cases when $k \in \{5, 6\}$.** Similar arguments (mainly Lemma 2.3 (b), (f)) are used for the cases $k = 5$ and $k = 6$ that follow. We will, for brevity, just give exactly each step of the proof, including the contradictions, but without explaining in detail which lemma or lemmas support(s) each step (or contradiction). In both cases hypothesis (a) and Lemma 2.4 are used extensively to guarantee that if a maximal prime M divides $\Phi_3(P)$ with P being a maximal prime, then the quotient $\Phi_3(P)/M$ is also a maximal prime divisor of A, and not merely a divisor of A with maximal degree.

2.4. **We assume that $k = 5$.** Let P_1, P_2, P_3, P_4 and P_5 be the 5 maximal primes that divide A. We can assume that $P_1 \mid \Phi_3(P_2)$, and that $P_2 \mid \Phi_3(P_3)$. If P_3 divides one of $\Phi_3(P_j)$, with $j \in \{1, 2\}$, say if $P_3 \mid \Phi_3(P_1)$, then $P_3 \nmid \Phi_3(P_2)$, so that we have two cases to consider: (a) $\Phi_3(P_2) = P_1P_4$, and (b) $\Phi_3(P_2) = P_1P_5$.

In case (a) we have two possibilities: either (a_1) holds or (a_2) holds. Assume first (a_1): $\Phi_3(P_1) = P_3P_4$. This is impossible since already $P_4 \mid \Phi_3(P_2)$. Thus, case (a_1) does not happen. The other possibility (a_2), is that we have $\Phi_3(P_1) = P_3P_5$. Consider in this case the factorization of $S_3 := \Phi_3(P_3)$. One sees that $P_1 \nmid S_3$, $P_4 \nmid S_3$, $P_3 \nmid S_3$, and $P_5 \nmid S_3$. This forces $\Phi_3(P_3) = P_2^2$. This is impossible. Thus, case (a_2) does not happen. Hence, the case (a) does not hold.

In case (b), we consider the possible prime divisors of the maximal prime $S_3 := \Phi_3(P_3)/P_2$. We have that $P_3 \nmid S_3$, $P_2 \nmid S_3$, $P_1 \nmid S_3$, and $P_5 \nmid S_3$. Thus, we must have $\Phi_3(P_3) = P_2P_4$. Consider the factorization of $S_1 := \Phi_3(P_1)$. We have that $P_1 \nmid S_1$, $P_5 \nmid S_1$, $P_2 \nmid S_1$, and $P_4 \nmid S_1$. Thus, $\Phi_3(P_1) = P_3^2$. This is impossible, thus case(b) does not happen.

Thus, P_3 does not divide $\Phi_3(P_1)\Phi_3(P_2)\Phi_3(P_3)$, therefore, P_3 must divide some $\Phi_3(P_j)$ with $j > 3$. Assume that $P_3 \mid \Phi_3(P_4)$. One sees that the only possibility is to have $\Phi_3(P_4) = P_3P_5$. Look at the factorization of $T_3 := \Phi_3(P_3)/P_2$. One sees that $P_3 \nmid T_3$, $P_2 \nmid T_3$, $P_1 \nmid T_3$, and $P_4 \nmid T_3$. Thus, $\Phi_3(P_3) = P_2^2$. This is impossible. Thus, $P_3 \mid \Phi_3(P_5)$. One sees that we must have $\Phi_3(P_5) = P_3P_4$. This, together with the fact that $P_2 \mid \Phi_3(P_3)$ forces the equality $\Phi_3(P_3) = P_2P_5$. This is impossible since $P_5 \nmid \Phi_3(P_3)$.

Therefore, the case $k = 5$ does not happen. Hence, $k > 5$.

2.5. **We assume that $k = 6$.** Let P_1, P_2, P_3, P_4, P_5 and P_6, be the 6 maximal primes that divide A. We can assume that $P_1 \mid \Phi_3(P_2)$, and that $P_2 \mid \Phi_3(P_3)$. We assume that $P_3 \mid \Phi_3(P_1)$ (the proof is analogue when $P_3 \mid \Phi_3(P_2)$). Let $S_2 := \Phi_3(P_2)/P_1$. We can assume that $S_2 = P_4$ (similar proof when $S_2 \in \{P_5, P_6\}$). Let $S_3 := \Phi_3(P_1)/P_3$. We can assume that $S_3 = P_5$ (similar proof if $S_3 = P_6$). We are then forced to have $\Phi_3(P_3) = P_2P_6$.

Remember that we have $\Phi_3(P_2) = P_1P_4$ and $\Phi_3(P_1) = P_3P_5$. Put $S_4 := \Phi_3(P_4)$. One sees that $P_4 \nmid S_4, P_1 \nmid S_4, P_2 \nmid S_4, P_3 \nmid S_4, P_5 \nmid S_4$, and $P_6 \nmid S_4$. This is impossible.

Thus, P_3 do not divide $\Phi_3(P_1)$ and do not divide $\Phi_3(P_2)$. It follows that we can assume that $P_3 \mid \Phi_3(P_4)$ (the case when P_3 divides one of $\Phi_3(P_5), \Phi_3(P_6)$ is similar). We deduce that we can take $\Phi_3(P_4) = P_3P_5$ (the other possibility: $\Phi_3(P_4) = P_3P_6$ is similar). This forces $\Phi_3(P_3) = P_2P_6$. But we must also have, $\Phi_3(P_2) = P_1P_4$.

Consequently, we obtain that each of the six maximal primes $P_1, \ldots, P_6$ cannot divide $\Phi_3(P_1)$. This is impossible. Thus, the case $k = 6$ does not happen.

We have then, by Lemma 2.1, that the number of minimal primes, say m_1, being even, satisfies $m_1 \geq 2$, the number of maximal primes is $m_3 \geq 7$ and, following Lemma 2.3 (d), the number of medium primes is $m_2 \geq m_3 \geq 7$. It follows that $\omega(A) \geq 16$. In more detail: $\omega(A) = m_1 + m_2 + m_3$. Thus,

$$\omega(A) \geq 2 \cdot m_3 + m_1 = 2 \cdot 7 + 2 = 16.$$

This finishes the proof of part (a) of the theorem.

2.6. **Proof of part (b).** One has $\deg(P^*) \geq 30$ by Theorem 1.1. The result follows then from Lemma 2.6, since $\deg(P^*)$ is even by Lemma 2.5 (b). We have then

$$\deg(P^*) \geq 40. \tag{2.10}$$

Finally, $\deg(A) \geq 2 \cdot m_1 \deg(p_1) + 2 \cdot m_2 \deg(p_d) + 2 \cdot m_3 \deg(p_m)$, where p_d is a medium prime divisor of A, such that p_{d-1} is a minimal prime. It follows from Lemma 2.5 (b) and from (2.10), that $\deg(p_1) \geq 40$. But it follows from Lemma 2.5 (b), that the degrees of all the p_k are even. Therefore, we have $\deg(p_d) \geq 42$, and $\deg(p_m) \geq 44$. Thus, with $m_1 \geq 2, m_2 \geq 7, m_3 \geq 7$, we have

$$\deg(A) \geq 2 \cdot (m_1 \cdot 40 + m_2 \cdot 42 + m_3 \cdot 44) \geq 160 + 14(42 + 44) = 1364.$$

This proves part (b) of the theorem.

Acknowledgement. We thank the referee and the editor for detailed comments and suggestions.

References

1. S. Agou, *Irréducibilité des polynômes $f(x^{p^r} - ax)$ sur un corps fini $\mathbb{F}_{p^s}$*, J. Reine Angew. Math., **292** (1977), 191–195.
2. S. Agou, *Irréducibilité des polynômes $f(x^{p^{2r}} - ax^{p^r} - bx)$ sur un corps fini $\mathbb{F}_{p^s}$*, J. Number Theory, **10** (1978), 64–69, **11** (1979), 20.
3. O. Ahmadi, M.-S. Khosro, *A note on the stability of trinomials over finite fields*, Finite Fields Appl., **63** (2020), 101649, 13 pp.

4. A. Ali, A. Bano, Md. H. Rahaman, *On multiplicative generalized (α, β)-derivations in prime rings*, Gulf. J. Math., **7**, no. 1, (2019), 56–67.
5. F.-E. Brochero-Martínez, L. Reis, *Factoring polynomials of the form $f(x^n) \in \mathbb{F}_q[x]$*, Finite Fields Appl., **49** (2018), 166–179.
6. M. C. R. Butler, *The irreducible factors of $f(x^m)$ over a finite field*, J. London Math. Soc., **30** (1955), 480–482.
7. E. F. Canaday, *The sum of the divisors of a polynomial*, Duke Math. J. **8** (1941), 721–737.
8. S. D. Cohen, *On irreducible polynomials of certain types in finite fields*, Proc. Camb. Philos. Soc. **66** (1969), 335–344.
9. S. D. Cohen, *The irreducibility of compositions of linear polynomials over a finite field*, Compositio Math. **47** (1982), 149–152.
10. U. C. Cengiz, P. Pollack, E. Treviño, *Counting perfect polynomials*, Finite Fields Appl., **47** (2017), 242–255.
11. L. H. Gallardo, O. Rahavandrainy, *Odd perfect polynomials over $\mathbb{F}_2$* J. Théor. Nombres Bordx. **19**, no. 1, (2007), 165–174.
12. L. H. Gallardo, O. Rahavandrainy, *There is no odd perfect polynomial over $\mathbb{F}_2$ with four prime factors*, Port. Math., **66**, no. 2, (2009), 131–145.
13. L. H. Gallardo, O. Rahavandrainy, *On even (unitary) perfect polynomials over $\mathbb{F}_2$*, Finite Fields Appl., **18**, no. 5, (2012), 920–932.
14. L. H. Gallardo, O. Rahavandrainy, *Characterization of sporadic perfect polynomials over $\mathbb{F}_2$*, Funct. Approx. Comment. Math., **55**, no. 1, (2016), 7–21.
15. L. H. Gallardo, O. Rahavandrainy, *On Mersenne polynomials over $\mathbb{F}_2$*, Finite Fields Appl., **59** (2019), 284–296.
16. L. H. Gallardo, O. Rahavandrainy, *On (unitary) perfect polynomials over $\mathbb{F}_2$ with only Mersenne primes as odd divisors*, arXiv: 1908.00106 [math.NT].
17. R. Jakimczuk, *Sums of fractional parts and sum of restricted divisors of a number*, Gulf. J. Math. **10**, no. 1, (2021), 36–42.
18. K. H. Kim, *On alpha-semiderivations and commutativity of prime rings*, Gulf. J. Math. **8**, no. 1, (2020), 23–31.
19. M. K. Kyuregyan, *Recurrent methods for constructing irreducible polynomials over $GF(2)$*, Finite Fields Appl., **8**, no. 1, (2002), 52–68.
20. M. K. Kyuregyan, G. H. Kyuregyan, *Irreducible compositions of polynomials over finite fields*, Des. Codes Cryptogr., **61**, no. 3, (2011), 301–314.
21. A. F. Long, *Factorization of irreducible polynomials over a finite field with the substitution $x^{q^r} - x$ for x*, Acta Arith., **25** (1973), 65–80.
22. R. Lidl, H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications,* 20, Cambridge: Cambridge University Press. xiv, 755 p., 1996.
23. D. Panario, L. Reis, Q. Wang, *Construction of irreducible polynomials through rational transformations*, J. Pure Appl. Algebra, **224**, no. 5, (2020), 106241, 17 p.
24. E. L. Petterson, *Über die Irreduzibilität ganzzahliger Polynome nach einem Primzahlmodul*, J. Reine Angew. Math., **175** (1936), 209–220.
25. L. Reis, *Factorization of a class of composed polynomials*, Des. Codes Cryptogr., **87**, no. 7, (2019), 1657–1671.
26. R. Steuerwald, *Verschärfung einer notwedingen Bedingung für die Existenz einer ungeraden volkommenen Zahl*, Sitzungsber. Bayer. Akad. Wiss., Math.-Naturwiss. Abt., **2** (1937), 69–72.
27. R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math., **12** (1962), 1099–1106.
28. A. Tadmori, A. Chillali, M. Ziane, *ECC over the ring $\mathbb{F}_{2^d}[X]/(X^2)$ by using a password*, Gulf. J. Math. **6**, no. 4, (2018), 72–78.

[1] Univ. Brest, UMR CNRS 6205, Laboratoire de Mathématiques de Bretagne Atlantique, F-29238 Brest, France.

Email address: Luis.Gallardo@univ-brest.fr