Portugal. Math. (N.S.)
Vol. 69, Fasc. 4, 2012, 283–303
DOI 10.4171/PM/1918

**Portugaliae Mathematica**


# On perfect polynomials over $\mathbb{F}_p$ with $p$ irreducible factors

Luis H. Gallardo and Olivier Rahavandrainy

(Communicated by Miguel Ramos)

**Abstract.** We consider, for a fixed odd prime number $p$, monic polynomials in one variable over the finite field $\mathbb{F}_p$ which are equal to the sum of their monic divisors. Call them *perfect* polynomials. We prove that the exponents of each irreducible factor of any perfect polynomial having no root in $\mathbb{F}_p$ and $p$ irreducible factors are all less than $p-1$. We completely characterize those perfect polynomials for which each irreducible factor has degree two and all exponents do not exceed two.

**Mathematics Subject Classification (2010).** Primary 11T55; Secondary 11T06.

**Keywords.** Sum of divisors, polynomials, finite fields, characteristic $p$.

## 1. Introduction

Let $p$ be a prime number. For a monic polynomial $A \in \mathbb{F}_p[x]$ let

$$\sigma(A) = \sum_{d \mid A, d \text{ monic}} d$$

be the sum of all monic divisors of $A$ (1 and $A$ included). Observe that $A$ and $\sigma(A)$ have the same degree. Let us call $\omega(A)$ the number of distinct monic irreducible polynomials that divide $A$. The function *sigma* is multiplicative on co-prime polynomials while the function *omega* is additive (on co-prime polynomials), a fact that shall be used many times without more reference in the rest of the paper.

A *perfect polynomial* is a monic polynomial $A$ such that:

$$\sigma(A) = A.$$

This notion is a good function field analogue of the notion of a multiperfect natural number $n$ that satisfies: $n$ divides $\sigma(n)$. For example, 120 is a multiperfect number since 120 divides $360 = \sigma(120)$. Indeed, since $\deg(A) = \deg\big(\sigma(A)\big)$, if a monic polynomial $A \in \mathbb{F}_p[x]$ divides $\sigma(A)$, then both are forced to be equal.

We say that a polynomial $A$ is *odd* (resp. *even*) if it has no root in $\mathbb{F}_p$ (that is: $\gcd(A, x^p - x) = 1$) (resp. it is not odd). So, the even polynomials are the polynomials with at least one divisor $D$ of (the usual) absolute value equal to $p$, i.e., $|D| := p^{\deg(D)} = p$; for example, $T = x^p + x$ is even since $x$ divides $T$, with $|x| = p$.

Throughout the paper, we shall assume that "a polynomial" means a monic polynomial and that the notion of polynomial irreducibility is defined over $\mathbb{F}_p$. For some recent results about even or splitting perfect polynomials see e.g. [10] and the references therein. Important results about perfect polynomials appear in the work of Canaday ([4]) and Beard et al. ([3], [1]). However, little is known about odd perfect polynomials.

Observe that any odd perfect polynomial in $\mathbb{F}_2[x]$ must be a perfect square. Indeed, if $A$ is odd perfect, then

$$\sigma(A) = A \not\equiv 0 \mod x. \tag{1}$$

If $A$ is not a square, then there exists an irreducible polynomial $P$ and an integer $m$ such that: $A = P^{2m+1} \cdot C$, where $C \in \mathbb{F}_p[x]$, $\deg(P) \geq 2$ and $\gcd(P, C) = 1$. So, $\sigma(A) = \sigma(P^{2m+1}) \cdot \sigma(C) \equiv 0 \bmod \sigma(P^{2m+1})$. Since $P(0) = 1$, we have $\sigma(P^{2m+1}) = 1 + P + \cdots + P^{2m+1} \equiv 0 \bmod x$. Thus, $\sigma(A) \equiv 0 \bmod x$, which contradicts (1).

Also trivially, there is no odd perfect polynomial over $\mathbb{F}_2$ with $\omega(A) = 1$. Canaday [4], Theorem 17, proved the inexistence of odd perfect polynomials over $\mathbb{F}_2$ with two irreducible factors, i.e., with $\omega(A) = 2$. We proved in [7], [9] (resp. [8]) the inexistence of odd perfect polynomials over $\mathbb{F}_2$ with $\omega(A) \in \{3, 4\}$ (resp. over $\mathbb{F}_3$ with $\omega(A) = 3$).

A perfect polynomial over $\mathbb{F}_p$ must have $np$ minimal irreducible divisors (see Lemma 2.1), so trivially there is no perfect polynomial over $\mathbb{F}_p$ with less than $p$ irreducible factors. However, we prove in [5] that there exist odd perfect polynomials over $\mathbb{F}_p$ for infinitely many values of $p$. We elaborated on Link's construction (described in [12] and more detailed in [2]) of an explicit odd perfect polynomial of degree 11 over $\mathbb{F}_{11}$. More precisely, we were able to find odd perfect polynomials $A$ over $\mathbb{F}_p$ with $\omega(A) = p$ for primes $p$ congruent to 11 or 17 modulo 24.

The question that arises naturally is the following: For a given odd prime number $p$, how can we describe the odd perfect polynomials over $\mathbb{F}_p$ with exactly $p$ irreducible factors?

Motivated by Link's construction mentioned above, we will consider the smallest possible unknown case, besides some general results displayed in Theorem 1.1. Namely, we would like (see Theorem 1.2) to determine all odd perfect polynomials of the form $A = P_1^{a_1} \ldots P_p^{a_p}$, where for any $j$, $\deg(P_j) = 2$ and $a_j \in \{1, 2\}$.

Our main objective is to prove the following results:

**Theorem 1.1.** *Let $p$ be an odd prime number. Let $A = P_1^{a_1} \dots P_p^{a_p}$ be an odd perfect polynomial over $\mathbb{F}_p$, with $p$ irreducible factors. Then*

i) *$a_j$ is even for at least one $j \in \{1, \dots, p\}$,*

ii) *$a_j \leq p-2$ for any $j \in \{1, \dots, p\}$,*

iii) *$a_j + 1 \not\mid p-1$ for at least one $j \in \{1, \dots, p\}$,*

iv) *$a_j \leq p-3$ whenever $x^p - x$ does not divide $P_j - 1$.*

**Theorem 1.2.** *Let $p$ be an odd prime number. Let $A = P_1^{a_1} \dots P_p^{a_p}$ be an odd perfect polynomial over $\mathbb{F}_p$, such that for any $j$, $P_j$ is irreducible,* $\deg(P_j) = 2$ *and $a_j \in \{1, 2\}$. Then $A$ is perfect over $\mathbb{F}_p$ if and only if*

$$\begin{cases} a_j = 2 \text{ for any } j, \\ \text{either } (p \equiv 11 \bmod 24) \text{ or } (p \equiv 17 \bmod 24). \end{cases}$$

*In this case such a polynomial is unique and equals $\prod_{a \in \mathbb{F}_p} \left((x+a)^2 - 3/8\right)^2$.*

Note that if $p = 3$, then conditions i) and ii) of Theorem 1.1 imply that $a_j = 2$ and $a_j = 1$ for at least one $j \in \{1, 2, 3\}$, which is impossible. So again we get Theorem 2.10 in [8]: There exists no odd perfect polynomial over $\mathbb{F}_3$ with 3 irreducible factors.

## 2. Preliminaries

**2.1. Some useful facts.** We denote as usual by $\mathbb{N}$ (resp. by $\mathbb{N}^*$) the set of non-negative integers (resp. of positive integers). For a set $S$ we denote by $\#S$ the cardinal of $S$. For polynomials $A, B \in \mathbb{F}_p[x]$, we write $A^n \parallel B$ if $A^n \mid B$ but $A^{n+1} \not\mid B$.

A basic but important result is

**Lemma 2.1** ([6], Lemma 2.5). *Let $p$ be a prime number. Let $A \in \mathbb{F}_p[x]$ be a perfect polynomial. Then the number of irreducible divisors of $A$, having minimal degree, is a multiple of $p$.*

We immediately get

**Corollary 2.2.** *If $A \in \mathbb{F}_p[x]$ is a perfect polynomial with exactly $p$ irreducible factors $P_1, \dots, P_p$, then* $\deg(P_1) = \dots = \deg(P_p)$.

According to Corollary 2.2, we are interested to know the factorization of $\sigma(P^a)$ into irreducible divisors of the same degree as $P$, for any polynomial $P$ and for any positive integer $a$ such that $P^a \parallel A$.

We generalize Lemma 6 in [4] (that covered the case $p = 2$):

**Lemma 2.3.** *Let $p$ be a prime number and let $P \in \mathbb{F}_p[x]$ be an irreducible polynomial. If $\sigma(P^a) = Q_1^{c_1} \dots Q_t^{c_t}$, where $Q_l$ is irreducible,* $\gcd(P, Q_l) = 1$, $\deg(P) = \deg(Q_l)$, *for any $l$, and $p \not| a + 1$, then $c_l \in \{0, 1\}$ for any $l$.*

*Proof.* If $c_l \geq 2$ for some $l$, then put

$$1 + \dots + P^a = Q^m C \qquad \text{where } m = c_l \text{ and } Q = Q_l.$$

We get

$$P^{a+1} - 1 = (P - 1)Q^m C. \tag{2}$$

Then by taking derivatives on both sides of (2), one has

$$0 \neq (a + 1)P^a P' = Q^{m-1}\big(P'QC + (P - 1)(mQ'C + QC')\big)$$

so that, with the observation that $\gcd(P, Q) = 1$,

$$Q^{m-1} \mid P'.$$

Thus, we get the contradiction

$$\deg(P) \leq (m - 1)\deg(P) = (m - 1)\deg(Q) \leq \deg(P') < \deg(P). \qquad \square$$

**2.2. Notations.** Given an odd prime number $p$, an irreducible polynomial $P \in \mathbb{F}_p[x]$ and an integer $a \in \mathbb{N}^*$, we would like to understand, as mentioned in Section 2.1, how $\sigma(P^a) = 1 + P + \dots + P^a$ may be factorized into irreducible divisors of the same degree as $P$:

$$\sigma(P^a) = Q_1^{c_1} \dots Q_t^{c_t} \qquad \text{with } \deg(P) = \deg(Q_l) \text{ for any } l.$$

We may write $a := Np^n - 1$ for some $N$, $n \in \mathbb{N}$, such that $N \geq 1$ and $p \not| N$. In that case we put $d := \gcd(N, p - 1)$ and denote by $L_N$ the splitting field of $x^N - 1$ over $\mathbb{F}_p$, which is a strict subset of the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$.

Moreover, since $p \not| N$, the polynomial $x^N - 1$ has no multiple root (in $L_N$). It is well known that the set $\Omega_N$ of $N$-th roots of *unity* in $\mathbb{F}_p$ consists exactly of $d$ elements:

$$\Omega_N := \{\mu \in \mathbb{F}_p : \mu^N = 1\}, \qquad \#\Omega_N = d = \gcd(N, p - 1).$$

Consider the Frobenius map: $\phi_p(t) = t^p$ for $t \in L_N$, acting over $L_N$. The action is extended trivially to $L_N[x]$ by sending $x$ to $x$. The Galois group $G$ of the exten-

sion $L_N$ over $\mathbb{F}_p$ is generated by $\phi_p$. The Galois group $G_e$ of the extension ring $L_N[x]$ over $\mathbb{F}_p[x]$ is isomorphic to $G$ and acts as $G$ on the coefficients of any element $A \in L_N[x]$.

We say that two elements $t, u \in L_N$ are *conjugate* if $t = \rho(u)$ for some $\rho \in G$. In the same manner, two polynomials $A, B \in L_N[x]$ are *conjugate* if $A = \rho(B)$ for some $\rho \in G_e$.

Finally, we put for $\mu \in L_N$ and for $R \in L_N[x]$:

$$\mathrm{Conj}(\mu) := \{\lambda \in L_N : \lambda \text{ and } \mu \text{ are conjugate}\},$$
$$\mathrm{Conj}(R) := \{S \in L_N[x] : S \text{ and } R \text{ are conjugate}\}.$$

Throughout Sections 2.3 and 2.4, we keep the notations

$$a = Np^n - 1, \qquad d = \gcd(N, p-1) \qquad \text{with } N, n \in \mathbb{N},\ N \geq 1 \text{ and } p \not\mid N.$$

**2.3. The case $N \mid p - 1$.** In Section 3, we will very often use the following obvious fact:

**Lemma 2.4.** *Let $P \in \mathbb{F}_p[x]$ be an odd irreducible polynomial. Then there exists $\mu \in \mathbb{F}_p \backslash \{0\}$ such that $P - \mu$ is even and hence reducible over $\mathbb{F}_p$.*

*Proof.* It suffices to remark that the monomial $x$ always divides $P - P(0)$. □

We give now some information on $\omega\big(\sigma(P^a)\big)$ for an irreducible polynomial $P \in \mathbb{F}_p[x]$ such that any irreducible divisor of $\sigma(P^a)$ has the same degree as $P$.

**Lemma 2.5.** *If $N \mid p - 1$ and if $P \in \mathbb{F}_p[x]$ is irreducible such that $\sigma(P^a) = Q_1^{c_1} \dots Q_t^{c_t}$, with $t = \omega\big(\sigma(P^a)\big)$, $\deg(P) = \deg(Q_j)$ for any $j$ and $Q_j$ irreducible, then $t \in \{N-1, N\}$ and for any $j$ there exists $\mu_j \in \Omega_N$ such that $Q_j = P - \mu_j$, $c_j = p^n - 1$ if $\mu_j = 1$, and $c_j = p^n$ if $\mu_j \neq 1$.*

*Proof.* Since $N \mid p - 1$ and $p \not\mid N$, the polynomial $x^N - 1$ splits over $\mathbb{F}_p$ and has no multiple root. Hence,

$$1 + x + \dots + x^a = \frac{x^{a+1} - 1}{x - 1} = \frac{(x^N - 1)^{p^n}}{x - 1} = \prod_{\mu \in \Omega_N} (x - \mu)^{c_\mu},$$

where $c_1 = p^n - 1$ and $c_\mu = p^n$ if $\mu \neq 1$. So,

$$\sigma(P^a) = 1 + P + \dots + P^a = \frac{(P^N - 1)^{p^n}}{P - 1} = \prod_{\mu \in \Omega_N} (P - \mu)^{c_\mu}.$$

Still by hypothesis, any irreducible divisor of $\sigma(P^a)$ is of degree $\deg(P)$, so each $P-\mu$ must be irreducible whenever $c_\mu \geq 1$. Thus, $t = N-1$ (resp. $N$) if $n=0$ (resp. $n \geq 1$). □

**2.4. The case $N \nmid p-1$.** In this section we will give detailed information on the possible irreducible factors of $S=\sigma(P^a)$ in the extension field $L_N$ and its consequences on the irreducible factors of $S$ in the ground field $\mathbb{F}_p$.

First of all, recall that $\#\Omega_N = d$ and $d < N$ because $N \nmid p-1$. We may write

$$\Omega_N = \{\xi_1 = 1, \xi_2, \ldots, \xi_d\} \subset \mathbb{F}_p.$$

Now we factor $x^N-1$ over $\mathbb{F}_p$:

$$\begin{cases} x^N - 1 = \prod_{l=1}^{d}(x-\xi_l)\cdot B_1 \ldots B_r, \\ \text{where each } B_j \text{ is odd and irreducible, for } 1 \leq j \leq r = \omega(x^N-1) - d. \end{cases} \tag{3}$$

Furthermore, for any $j \in \{1,\ldots,r\}$, $B_j$ splits over $L_N$, namely,

$$\text{there exists } \mu_j \in L_N \backslash \mathbb{F}_p \text{ such that } B_j = \prod_{\lambda \in \mathrm{Conj}(\mu_j)} (x-\lambda). \tag{4}$$

It follows that, for any $j$,

$$v_j := \deg(B_j) = \#\mathrm{Conj}(\mu_j) \geq 2. \tag{5}$$

Thus, one has

$$\begin{cases} \sigma(x^a) = 1 + x + \cdots + x^a = \frac{(x^N-1)^{p^n}}{x-1} = (x-1)^{p^n-1} A_1^{p^n} A_2^{p^n}, \\ \text{where } A_1 = 1 \text{ if } d=1,\ A_1 = (x-\xi_2)\ldots(x-\xi_d), \text{ if } d \geq 2, \\ A_2 = B_1 \ldots B_r, \\ \mu_i \text{ and } \mu_j \text{ are not conjugate if } i \neq j. \\ A_2 \text{ is of degree } v_1 + \cdots + v_r = N-d. \end{cases} \tag{6}$$

We get two intermediate results:

**Lemma 2.6.** *We suppose that $N \nmid p-1$ and $d \geq 2$. Let $A \in \mathbb{F}_p[x]$ be odd and perfect with $\omega(A) = p$. If $P^a \parallel A$ for some odd irreducible polynomial $P$, then*

$$P-\xi_2, \ldots, P-\xi_d \text{ are all irreducible divisors of } A.$$

*Moreover, $P-1$ is also irreducible and divides $A$ if $n \geq 1$.*

*Proof.* By substituting $x$ by $P$ in (6), we see that $P-\xi_2,\dots,P-\xi_d$ divide $\sigma(P^a)$ and thus divide $\sigma(A)=A$. It follows by Corollary 2.2 that $P-\xi_2,\dots,P-\xi_d$ must be irreducible. If $n\geq 1$, we may add the polynomial $P-1$. □

**Lemma 2.7.** *We suppose that $N\not\equiv p-1$. Let $P\in\mathbb{F}_p[x]$ be odd irreducible such that $\sigma(P^a)=Q_1^{c_1}\dots Q_t^{c_t}$, where $t=\omega\big(\sigma(P^a)\big)$, $\deg(P)=\deg(Q_l)$ for any $l\in\{1,\dots,t\}$. Then $P-\mu_j$ is reducible over $L_N$ for any $j\in\{1,\dots,r\}$.*

*Proof.* By substituting $x$ by $P$ in (6), we have

$$\sigma(P^a)=(P-1)^{p^n-1}\big(A_1(P)\big)^{p^n}\big(A_2(P)\big)^{p^n},$$

where

$$A_2(P)=B_1(P)\dots B_r(P),\qquad B_j(P)=\prod_{\lambda\in\mathrm{Conj}(\mu_j)}(P-\lambda).$$

If $P-\mu_j$ is irreducible over $L_N$ for some $j$, then the polynomial $B_j(P)$ is irreducible over $\mathbb{F}_p$ and divides $\sigma(P^a)$, with $\deg\big(B_j(P)\big)>\deg(P)$. But this is impossible. □

According to Lemma 2.6, we may put without loss of generality:

$$Q_1:=P-1,\dots,Q_d:=P-\xi_d \text{ if } n\geq 1,$$
$$Q_1:=P-\xi_2,\dots,Q_{d-1}:=P-\xi_d \text{ if } n=0.$$

In other words, the number of irreducible divisors of $\sigma(P^a)$, of the form $P-\xi\in\mathbb{F}_p[x]$, is exactly

$$d-1+\min(1,n).$$

More precise results follow.

**Lemma 2.8.** *With the same hypothesis and notations as in Lemma 2.7, for any $k\geq d+\min(1,n)$, there exist $j\in\{1,\dots,r\}$ and $l\in\{1,\dots,w_j\}$ such that $V_{jl}$ is an irreducible divisor of $P-\mu_j$ and $Q_k=\prod_{S\in\mathrm{Conj}(V_{jl})}S$.*

*Proof.* We recall that

$$\sigma(P^a)=(P-1)^{p^n-1}\big(A_1(P)\big)^{p^n}\big(A_2(P)\big)^{p^n},$$

where

$$A_2(P)=B_1(P)\dots B_r(P),\qquad B_j(P)=\prod_{\lambda\in\mathrm{Conj}(\mu_j)}(P-\lambda).$$

Put, for any $j \in \{1, \dots, r\}$,

$$P - \mu_j = V_{j1}^{\gamma_{j1}} \dots V_{jw_j}^{\gamma_{jw_j}} \quad \text{and} \quad R_{jl} = \prod_{S \in \mathrm{Conj}(V_{jl})} S,$$

where each $V_{jl}$ is irreducible over $L_N$, $w_j$ is the number of irreducible divisors (in $L_N[x]$) of $P - \mu_j$ and $\gamma_{jl} \geq 1$ for any $l \in \{1, \dots, w_j\}$. Then each $R_{jl}$ lies on $\mathbb{F}_p[x]$ and is irreducible (over $\mathbb{F}_p$). We see that

$$B_j(P) = R_{j1}^{\gamma_{j1}} \dots R_{jw_j}^{\gamma_{jw_j}}.$$

Hence, $R_{jl}$ divides $A_2(P)$ and $\sigma(P^a)$. Thus, we may put $Q_k = R_{jl}$ which is of degree $v_j \deg(V_{jl})$. □

**Lemma 2.9.** *With the same hypothesis and notations as in* (*the proof of*) *Lemma* 2.8*, we have*

i) $\deg(R_{jl}) = v_j \deg(V_{jl})$, $\deg(V_{jl}) = \deg(V_{jk}) \geq 1$, *for any* $l, k \in \{1, \dots, w_j\}$,

ii) $(\gamma_{j1} + \dots + \gamma_{jw_j}) b_j = \deg(P) = \deg(R_{jl}) = v_j b_j$ *where* $b_j := \deg(V_{jl})$,

iii) $v_j = \gamma_{j1} + \dots + \gamma_{jw_j}$ *for any* $j \in \{1, \dots, r\}$,

iv) $c_k = \gamma_{jl} p^n$ *if* $Q_k = R_{jl}$.

*Proof.* i) For any $l, k \in \{1, \dots, w_j\}$, we have

$$\deg(R_{jl}) = \#\mathrm{Conj}(V_{jl}) \cdot \deg(V_{jl}) = \#\mathrm{Conj}(\mu_j) \cdot \deg(V_{jl}) = v_j \deg(V_{jl}),$$
$$v_j \deg(V_{jl}) = \deg(R_{jl}) = \deg(P) = \deg(R_{jk}) = v_j \deg(V_{jk}).$$

So, $\deg(V_{jl}) = \deg(V_{jk})$.

ii) Since $P - \mu_j = V_{j1}^{\gamma_{j1}} \dots V_{jw_j}^{\gamma_{jw_j}}$ and $R_{jl} = \prod_{S \in \mathrm{Conj}(V_{jl})} S$, we obtain

$$(\gamma_{j1} + \dots + \gamma_{jw_j}) b_j = \deg(P) = \deg(R_{jl}) = v_j b_j.$$

iii) follows from ii).

iv) is obtained from the fact that the exponent of $R_{jl}$ in the factorization of $\sigma(P^a)$ is exactly $\gamma_{jl} p^n$.

Note that $v_j \geq 2$ for any $j \in \{1, \dots, r\}$, but $b_j$ may equal 1 for some $j$,

$$\{Q_{d+\min(1,n)}, \dots, Q_t\} = \{R_{jl} : 1 \leq j \leq r, 1 \leq l \leq w_j\},$$

$$\sum_{l=d+\min(1,n)}^{t} c_l = \sum_{j=1}^{r} \sum_{l=1}^{w_j} \gamma_{jl} p^n = p^n \sum_{j=1}^{r} (\gamma_{j1} + \dots + \gamma_{jw_j}) = p^n \sum_{j=1}^{r} v_j = (N-d) p^n,$$

$$\sum_{l=1}^{t} c_l = \sum_{l=1}^{d-1+\min(1,n)} c_l + (N-d) p^n = p^n - 1 + (d-1) p^n + (N-d) p^n = a. \quad \square$$

**Corollary 2.10.** *With the same hypothesis and notations as in (the proof of) Lemma* 2.8,

i) $\sigma(P^a)$ *has at most* $N$ *irreducible distinct divisors if* $n \geq 1$.

ii) $\sigma(P^a)$ *has exactly* $N-1$ *irreducible distinct divisors if* $n = 0$.

*Proof.* First of all, we have, for any $j$,

$$w_j \leq \gamma_{j1} + \cdots + \gamma_{jw_j} = v_j.$$

i) If $n \geq 1$, the irreducible distinct divisors of $\sigma(P^a)$ are:

$$\begin{aligned} &P-1, P-\xi_2, \ldots, P-\xi_d, \\ &R_{11}, \ldots, R_{1w_1}, \\ &\qquad \vdots \\ &R_{r1}, \ldots, R_{rw_r}. \end{aligned}$$

So there are $d + w_1 + \cdots + w_r$ such divisors with

$$d + w_1 + \cdots + w_r \leq d + v_1 + \cdots + v_r = d + (N-d) = N.$$

ii) If $n = 0$, then $P-1$ does not divide $\sigma(P^a)$, and by Lemma 2.3, $\sigma(P^a)$ is square free. Thus, $\gamma_{jl} = 1$ for any $j$, $l$.

Therefore, $w_j = \gamma_{j1} + \cdots + \gamma_{jw_j} = v_j$ for any $j$. Thus, the number of irreducible distinct divisors of $\sigma(P^a)$ is

$$d - 1 + w_1 + \cdots + w_r = d - 1 + v_1 + \cdots + v_r = d - 1 + (N-d) = N - 1. \quad \square$$

## 3. The proof of Theorem 1.1

By using notations from Section 2.2, we obtain our main results including several sufficient conditions for non perfection as stated in Corollary 3.4.

Propositions 3.1 and 3.2 give the first and second part of our theorem. Corollary 3.5 iv) gives the third part. The last part is obtained from Proposition 3.6.

**Proposition 3.1.** *There are no odd perfect polynomials* $A \in \mathbb{F}_p[x]$ *with* $p$ *irreducible divisors* $P_1, \ldots, P_p$, *of the form* $A = P_1^{a_1} \ldots P_p^{a_p}$, *where* $a_i$ *is odd for any* $i \in \{1, \ldots, p\}$.

*Proof.* Since $a_1$ is odd, $P_1 + 1$ divides $\sigma(P_1^{a_1})$. $P_1 + 1$ cannot be composite since any of its irreducible factors should have degree $< d$. So $P_1 + 1$ is an irreducible divisor of $A$. By applying the same argument to $P_1 + 1$, we see that $P_1 + 2$ is

also an irreducible divisor of $A$, and so on. Thus, $\{P_1, \dots, P_p\} = \{P_1, P_1 + 1, P_1 + 2, \dots, P_1 + (p-1)\}$ and hence $P - \mu$ is irreducible for any $\mu \in \mathbb{F}_p$. This contradicts Lemma 2.4. □

**Proposition 3.2.** *There are no odd perfect polynomials $A \in \mathbb{F}_p[x]$ with $p$ irreducible divisors $P_1, \dots, P_p$, of the form $A = P_1^{a_1} \dots P_p^{a_p}$, where for any $i \in \{1, \dots, p\}$,*

$$a_i = N_i p^{n_i} - 1, \qquad N_i, n_i \in \mathbb{N},\ N_i \geq 1,\ p \nmid N_i,\ N_i \mid p - 1.$$

*Proof.* Since $N_i \mid p - 1$, we may write

$$\sigma(P_i^{a_i}) = \prod_{\mu \in \Omega_{N_i}} (P_i - \mu)^{c_\mu}.$$

Hence,

$$A = \sigma(A) = \prod_i \sigma(P_i^{a_i}) = \prod_i \prod_{\mu \in \Omega_{N_i}} (P_i - \mu)^{c_\mu}.$$

Therefore, we may put

$$A = \prod_i A_i = \prod_i \prod_{\xi \in \mathbb{F}_p} (P_i - \xi)^{b_\xi},$$

where $b_\xi \in \mathbb{N}$ (may be equal to 0) and $P_i - P_j \notin \mathbb{F}_p$ if $i \neq j$.

It follows that, for any $i \neq j$, $\gcd(A_i, A_j) = 1 = \gcd\big(A_i, \sigma(A_j)\big)$. We see that $A$ is perfect if and only if each $A_i$ is perfect. Hence $\omega(A_i) = p$, $i = 1$ and $\#\Omega_{N_1} = p - 1$, $N_1 = p - 1$. So each $P - \mu$ is irreducible for any $\mu \in \mathbb{F}_p$. This contradicts Lemma 2.4. □

**Proposition 3.3.** *Let $A = P_1^{a_1} \dots P_p^{a_p}$ be an odd perfect polynomial with $p$ irreducible divisors, with $a_i = N_i p^{n_i} - 1$, $N_i, n_i \in \mathbb{N}$, $N_i \geq 1$, $p \nmid N_i$.*

*If $n_l = 0$ for some $l$, then $N_l - 1 \leq p - 2$ and $n_j = 0$ for any $j$ such that $P_l$ divides $\sigma(P_j^{a_j})$.*

*Proof.* If $N_l \mid p - 1$ then $N_l - 1 \leq p - 2$.

We suppose that $N_l \nmid p - 1$. If $n_l = 0$, then by Corollary 2.10, $N_l - 1 < \omega(A) = p$. So, $N_l - 1 \leq p - 1$. Since $p \nmid N_l$, we must have $N_l - 1 \leq p - 2$.

If $j \in \{1, \dots, r\}$ such that $P_l \mid \sigma(P_j^{a_j})$, then the exponent of $P_l$ in $\sigma(A)$ is at least $p^{n_j} - 1$, and the exponent of $P_l$ in $A$ is $a_l = N_l - 1 \leq p - 2$. So we must have

$$p^{n_j} - 1 \leq a_l \leq p - 2.$$

Thus, $n_j$ must be equal to 0. □

**Corollary 3.4.** *Let $A = P_1^{a_1} \dots P_p^{a_p} \in \mathbb{F}_p[x]$ be an odd polynomial, with $\omega(A) = p$ and $\deg(P_1) = \dots = \deg(P_p)$. Then $A$ is not perfect if at least one of the following conditions holds:*

i) *There exists $j$ such that $v_j$ does not divide $\deg(P_1)$.*

ii) *There exists $j$ such that $\sigma(x^{a_j})$ is irreducible over $\mathbb{F}_p$ and $N_j - 1 \not\mid \deg(P_1)$.*

iii) *There exists $j$ such that $a_j = Np^n - 1$, $\sigma(x^{a_j}) = (x-1)^{p^n-1} A_1^{p^n} A_2^{p^n}$, where $A_2$ is irreducible (over $\mathbb{F}_p$) and $N - d \not\mid \deg(P_1)$, $d = \gcd(N, p-1)$.*

iv) *$a_1 = \dots = a_p = Np^n - 1$ with $(n \geq 1)$ or $(\gcd(N, p-1) \geq 2)$.*

v) *For any $j$, $a_j = N_j p^{n_j} - 1$ with ($n_j \geq 1$ for any $j$) or ($N_j = N, \gcd(N, p-1) \geq 2$ for any $j$).*

*Proof.* Observe that ii) and iii) follow from i), and v) implies iv). It suffices to prove i) and v).

i) We will proceed by proving the contrapositive: If $A$ is perfect, then by Lemma 2.9, we must have $\deg(P_1) = v_j b_j$ for any $j$. So $v_j$ divides $\deg(P_1)$.

v) If $n_j \geq 1$ for any $j$, then after re-indexing, we have $P_2 = P_1 - 1$, $P_3 = P_2 - 1 = P_1 - 2, \dots, P_p = P_1 - (p-1)$. So $P_1 - \mu$ is irreducible for any $\mu \in \mathbb{F}_p$. This contradicts Lemma 2.4.

If for any $j$, $N_j = N$ and $\gcd(N, p-1) = d \geq 2$, then after re-indexing, we have $P_2 = P_1 - \xi_2$, $P_3 = P_1 - 2\xi_2, \dots, P_p = P_1 - (p-1)\xi_2$ and $P_1$ which are both irreducible. This again contradicts Lemma 2.4. □

By part v) of Corollary 3.4, if $A$ is perfect then the set $\Lambda = \{i : n_i = 0\}$ is not empty. More precisely, we get

**Corollary 3.5.** *Let $A = P_1^{a_1} \dots P_p^{a_p}$ be an odd perfect polynomial over $\mathbb{F}_p$, with $\omega(A) = p$, and for each $i$, $a_i = N_i p^{n_i} - 1$, $N_i, n_i \in \mathbb{N}$, $N_i \geq 1$, $p \not\mid N_i$. Then*

i) *for any $i \notin \Lambda$, there exists $j \notin \Lambda$ such that $P_j = P_i - 1$.*

ii) *$\Lambda = \{1, 2, \dots, p\}$ (that is, for any $i$, $n_i = 0$),*

iii) *for any $i$, $P_i - 1$ does not divide $\sigma(P_i^{a_i})$,*

iv) *for any $i$, $a_i = N_i - 1 \leq p - 2$.*

*Proof.* Here, $N_i$ may divide $p - 1$ for some $i$.

i) If $n_i \geq 1$, then

$$\sigma(P_i^{a_i}) = \frac{(P^{N_i} - 1)^{p^{n_i}}}{P_i - 1} = (P_i - 1)^{p^{n_i} - 1} \cdot C \qquad \text{for some polynomial } C,$$

where $p^{n_i} - 1 \geq p - 1 \geq 1$. Hence, $P_i - 1$ must be irreducible. Put $P_j = P_i - 1$. If $j \in \Lambda$, then the exponent of $P_j$ in $A$ is $N_j - 1$ and $N_j - 1 \leq p - 2$ by Proposition

3.3, the exponent of $P_j$ in $\sigma(A)$ is at least $p^{n_i}-1$. So $p-2 \geq N_j - 1 \geq p^{n_i}-1 \geq p-1$, which is impossible.

ii) We prove that for any $i$, $n_i = 0$. If not, let $i$ such that $n_i \geq 1$. Then $i \notin \Lambda$. Put $P_{i_1} = P_i - 1$. We have $i_1 \notin \Lambda$. By putting $P_{i_2} = P_{i_1} - 1 = P_i - 2$, we have $i_2 \notin \Lambda$, and so on. The polynomials $P_i, P_i - 1, P_i - 2, \ldots, P_i - (p-1)$ are all irreducible. This contradicts Lemma 2.4.

iii) follows from ii).

iv) follows from ii) and from Proposition 3.3. □

**Proposition 3.6.** *Let $A = P_1^{a_1} \ldots P_p^{a_p}$ be an odd perfect polynomial over $\mathbb{F}_p$, with $\omega(A) = p$ such that $x^p - x$ does not divide $P_1 - 1$. Then $a_1 \leq p-3$.*

*Proof.* We know, by Corollary 3.5-iv), that $a_1 \leq p-2$. If $a_1 = p-2$, then

$$\sigma(P_1^{a_1}) = \frac{P_1^{a_1+1}-1}{P_1-1} = \frac{P_1^{p-1}-1}{P_1-1} = (P_1-2)\ldots\big(P_1-(p-1)\big).$$

Since $x^p - x \nmid (P_1 - 1)$, we have $P_1(\xi) \neq 1$ for some $\xi \in \mathbb{F}_p$. So $P_1(\xi) \in \{2, 3, \ldots, p-1\}$, $\big(\sigma(P_1^{a_1})\big)(\xi) = 0$, and $x - \xi$ divides $\sigma(A) = A$. This contradicts the fact that $A$ is odd. □

## 4. The proof of Theorem 1.2

We did some computational work to find some perfect polynomials satisfying the hypothesis of this theorem, but despite several attempts, we did not find any. The main difficulty appeared to be the random nature of the irreducible factors of $A$. More precisely, if we try to build an odd perfect polynomial $A$ with $p$ irreducible factors, we begin by taking an irreducible polynomial $R_1 = (x+c_1)^2 - d_1$ of degree 2 such that $R_1 \parallel A$ or $R_1^2 \parallel A$.

- If $R_1 \parallel A$, then we apply the sigma function $\sigma$, $\sigma(R_1) = 1 + R_1 = (x+c_1)^2 - (d_1 - 1) = R_2$, which must be an irreducible divisor of $\sigma(A) = A$. We do not know whether $R_2 \parallel A$ or $R_2^2 \parallel A$.
  If $R_2 \parallel A$, then as above we get $R_3 = \sigma(R_2) = 1 + R_2 = (x+c_1)^2 - (d_1 - 2)$. Again we do not know the exponents $e \in \{1, 2\}$ such that $R_3^e \parallel A$.
  If $R_2^2 \parallel A$, then $\sigma(R_2^2) = R_3 R_4$, where $R_3$ and $R_4$ are irreducible divisors of $A$. For each $j \in \{3, 4\}$, we get two cases as above.
- If $R_1^2 \parallel A$, then $\sigma(R_1^2) = R_2 R_3$, where $R_2$ and $R_3$ are irreducible divisors of $A$. We obtain similar results.

Hence, if we apply several times the sigma function $\sigma$, we see immediately that we obtain a kind of graph where each vertex is *of degree* 2 (i.e., there are two edges

incident to each vertex). This indicates that the computation time, necessary to consider all cases, may grow too fast.

Observe, that if $m$ is the greatest integer such that for any $1 \le j \le m$, $R_j \| A$ and $R_{j+1} = \sigma(R_j) = 1 + R_j$, then by repeating the procedure $m$ times from $R_1$ to $R_{m+1}$,

$$R_1 \to \sigma(R_1) = R_2 \to \cdots \to \sigma(R_m) = R_{m+1},$$

we see that the $m+1$ elements $d_1, d_1 - 1, d_1 - 2, \ldots, d_1 - m$ of $\mathbb{F}_p$ must be all non-square. The maximum value of such an $m$ is bounded above by $\sqrt{p}$ (see [11]), a nice result that, unfortunately, we were unable to apply here.

However, we were able to refine our method so that it leads us to consider two main cases:

$$(a_j = 1 \text{ for at least one } j \in \{1, \ldots, p\}) \quad \text{and} \quad (a_j = 2 \text{ for any } j).$$

We need the following obvious fact (for which we omit a proof):

**Lemma 4.1.** i) *Any irreducible polynomial $P$ over $\mathbb{F}_p$ of degree 2 may be written as*

$$P = (x + a)^2 - f \qquad \textit{where } a, f \in \mathbb{F}_p \textit{ and } f \textit{ is not a square.}$$

ii) *For any odd irreducible polynomials $P$ and $Q$ over $\mathbb{F}_p$, $\sigma(P^2) = \sigma(Q^2)$ if and only if $P = Q$.*

We see that we must deal with irreducible polynomials of degree 2, which may be written (Lemma 4.1) as: $T_{a,f}(x) = (x + a)^2 - f$, where $a, f \in \mathbb{F}_p$ and $f$ is not a square. We must indicate how $\sigma(T_{a,f})$ and $\sigma\big((T_{a,f})^2\big)$ are factorized into a product of irreducible polynomials of the same kind.

We shall give some preliminary results in order to prove Theorem 1.2. Sufficiency follows from Proposition 4.12. We obtain necessity by Proposition 4.4 and Corollary 4.14.

Now we prove a crucial result:

**Lemma 4.2.** *Let $p$ be an odd prime number such that $(-3)$ is not a square in $\mathbb{F}_p$. Let $P = x^2 - f$, $P_j = (x + a_j)^2 - f_j$ and $P_k = (x + a_k)^2 - f_k$ be odd irreducible. Then $P_j P_k = \sigma(P^2)$ if and only if the following conditions are satisfied:*

$$\begin{cases} f_j = f_k,\ a_k = -a_j \neq 0 \textit{ for any } j, k, \\ 1 - f + f^2 \textit{ is a square: } 1 - f + f^2 = \alpha^2,\ \alpha \in \mathbb{F}_p, \\ 2f - 1 - 2\alpha \textit{ is not a square and } f_j + \alpha \textit{ is a square}, \\ f_j = \frac{2f - 1 - 2\alpha}{4} = a_j^2 - \alpha, \\ f_j = \frac{-3}{16a_j^2},\ f = f_j + a_j^2 + \frac{1}{2} = f_j - \frac{3}{16f_j} + \frac{1}{2}. \end{cases}$$

*Proof.* Sufficiency is obtained by direct computations.

Necessity: We have

$$\sigma(P^2) = 1 + P + P^2 = (1 - f + f^2) + (1 - 2f)x^2 + x^4,$$
$$P_j P_k = A_{jk} + B_{jk}x + C_{jk}x^2 + (2a_j + 2a_k)x^3 + x^4,$$

where $A_{jk} = (a_j^2 - f_j)(a_k^2 - f_k)$, $B_{jk} = 2a_k(a_j^2 - f_j) + 2a_j(a_k^2 - f_k)$,

$$C_{jk} = 4a_j a_k + (a_j^2 - f_j) + (a_k^2 - f_k).$$

Therefore,

$$\begin{aligned} a_j + a_k &= 0, \\ 2a_k(a_j^2 - f_j) + 2a_j(a_k^2 - f_k) &= 0, \\ 4a_j a_k + (a_j^2 - f_j) + (a_k^2 - f_k) &= 1 - 2f, \\ (a_j^2 - f_j)(a_k^2 - f_k) &= 1 - f + f^2. \end{aligned}$$

Hence, either

$$\begin{aligned} a_k = a_j &= 0, \\ f_j + f_k &= 2f - 1, \\ f_j f_k &= 1 - f + f^2. \end{aligned} \tag{7}$$

or

$$\begin{aligned} a_k &= -a_j \neq 0, \\ f_j &= f_k, \\ 2a_j^2 + 2f_j &= 2f - 1, \\ (a_j^2 - f_j)^2 &= 1 - f + f^2. \end{aligned} \tag{8}$$

In the first case $f_j$ and $f_k$ satisfy the quadratic equation

$$t^2 - (2f - 1)t + 1 - f + f^2 = 0.$$

Thus, its discriminant $\Delta = (2f - 1)^2 - 4(1 - f + f^2) = -3$ must be a square in $\mathbb{F}_p$, which contradicts our hypothesis on $p$.

Thus, the second case must hold. It follows that

$$\begin{cases} 1-f+f^2 \text{ is a square: } 1-f+f^2=\alpha^2,\ \alpha=a_j^2-f_j\in\mathbb{F}_p,\\ f_j+\alpha=a_j^2 \text{ is a square},\\ f_j=\frac{2f-1-2\alpha}{4}. \end{cases}$$

Since $f_j$ is not a square, we see that $2f-1-2\alpha$ is not a square. By (8), we get

$$f=f_j+a_j^2+\frac{1}{2}\qquad\text{and}\qquad f_j=\frac{-3}{16a_j^2}.$$ □

**Corollary 4.3.** *Let $p$ be an odd prime number such that $(-3)$ is not a square in $\mathbb{F}_p$. Let $P_i=(x+a_i)^2-f_i$, $P_j=(x+a_j)^2-f_j$ and $P_k=(x+a_k)^2-f_k$ be odd irreducible polynomials such that $P_jP_k=\sigma(P_i^2)$. Then*

$$\begin{cases} f_j=f_k,\ a_k\neq a_j,\ a_i=\frac{a_j+a_k}{2},\\ f_j=\frac{-3}{4d_{jk}^2},\ f_i=f_j+\frac{d_{jk}^2}{4}+\frac{1}{2}=f_j-\frac{3}{16f_j}+\frac{1}{2},\ \textit{where } d_{jk}=a_j-a_k. \end{cases}$$

*Proof.* Put $\overline{P_i}=P_i(x-a_i)=x^2-f_i$, $\overline{P_j}=(x+a_j-a_i)^2-f_j$, $\overline{P_k}=(x+a_k-a_i)^2-f_k$. We get

$$\overline{P_j}\,\overline{P_k}=\sigma(\overline{P_i}^2).$$

The result follows from Lemma 4.2. □

For the rest of the paper, we keep the notations:

$$A=P_1^{a_1}\dots P_p^{a_p},\qquad \text{where } \deg(P_i)=2 \text{ and } a_i\in\{1,2\} \text{ for any } i.$$

**4.1. The case $a_j=1$ for at least one $j\in\{1,\dots,p\}$.** We prove the following result:

**Proposition 4.4.** *There exists no odd perfect polynomial with $p$ irreducible factors $P_1,\dots,P_p$, of the form $A=P_1^{a_1}\dots P_p^{a_p}$, where for any $i$, $\deg(P_i)=2$, $a_i\in\{1,2\}$, and $a_k=1$ for some $k$.*

**4.1.1. The case $a_i=1$ for any $i\in\{1,\dots,p\}$.** In this case, after re-indexing, we may write:

$$P_2=\sigma(P_1)=P_1+1, P_3=P_2+1=P_1+2,\dots,P_p=P_{p-1}+1=P_1+p-1.$$

Hence, $P_1, P_1+1,\dots,P_1+p-1$ are all irreducible. This contradicts Lemma 2.4.

**4.1.2. The case: $a_j = 1$, $a_k = 2$ for some $j, k \in \{1, \ldots, p\}$.** We remark that $1 + 1 = 2$ always divides $p - 1$. If $2 + 1 = 3$ divides $p - 1$, then, by Theorem 1.1 iii), $A$ is not perfect. It remains the case $p \equiv 2 \bmod 3$.

We also adopt the following convention: we denote $P \leftrightarrow Q$ to mean that $P$ and $Q$ verify $PQ = \sigma(R^2)$ for some $R$.

We immediately obtain from Corollary 4.3:

**Corollary 4.5.** *If $P \leftrightarrow Q$ and if $P = (x + a)^2 - f$, $Q = (x + b)^2 - g$, where $f$, $g$ are not square in $\mathbb{F}_p$, then $f = g$.*

**Lemma 4.6.** *The polynomial $A$ may be written as*

$$A = A_1 \ldots A_r,$$

*where $A_j = R_j(R_j + 1) \ldots (R_j + m_j)(R_j + m_j + 1)^2 C_{j1}^2 \ldots C_{jn_j}^2$ for any $j \in \{1, \ldots, r\}$, and either $R_j - 1$ is of exponent 2 or $R_j - 1$ does not divide $A$.*

*Proof.* We may write

$$A = P_1 \ldots P_s P_{s+1}^2 \ldots P_p^2.$$

By putting $R_1 = P_1$, we see that $R_1 + 1 = \sigma(R_1)$ divides $\sigma(A) = A$. If $R_1 + 1$ is of exponent 1, then we continue the process. After a finite number (say $m_1 + 1$) of steps, the exponent of $R_1 + m_1 + 1$ equals 2. Observe that $1 \leq m_1 + 1 \leq s < p$. We may suppose that

$$P_1 = R_1,\ P_2 = R_1 + 1, \ldots, P_{m_1+1} = R_1 + m_1.$$

Now we may apply the process to $R_2 = P_{m_1+2}$. After $m_2 + 1$ steps we get

$$P_{m_1+2} = R_2, \ldots, P_{m_1+2+m_2} = R_2 + m_2$$

and so on. Altogether, we obtain

$$1 \leq (m_1 + 1) + (m_2 + 1) + \cdots + (m_r + 1) = s < p. \qquad \square$$

**Lemma 4.7.** *If $A$ is perfect, if $C^2$ divides $A$, and if $C \neq R_j + m_j + 1$ for any $j \leq r$, then there exist $C_1$, $C_2$ such that $C_1 \leftrightarrow C \leftrightarrow C_2$.*

*Proof.* It follows from the fact that $C$ must appear two times in $\sigma(A) = A$. The case $C = R_j + m_j + 1$ is excluded since $C \mid \sigma(R_j + m_j)$. $\square$

**Corollary 4.8.** *With the same hypothesis and notations as in Lemma* 4.6*, for any* $j \leq r$*, one has the following graph:*

$$R_j + m_j + 1 \leftrightarrow C_{j1} \leftrightarrow \cdots \leftrightarrow C_{jt_j} \leftrightarrow S_j,$$

*where* $S_j$ *is of exponent* 1 *and each* $C_{kl}$ *is of exponent* 2*.*

**Corollary 4.9.** *With the same hypothesis and notations as in Lemma* 4.6*, there exists* $v \leq r$ *such that, after re-indexing, one has the following graphs:*

$$\begin{gathered} R_1 + m_1 + 1 \leftrightarrow C_{11} \leftrightarrow \cdots \leftrightarrow C_{1t_1} \leftrightarrow S_1, \\ R_2 + m_2 + 1 \leftrightarrow C_{21} \leftrightarrow \cdots \leftrightarrow C_{2t_2} \leftrightarrow S_2, \\ \vdots \\ R_v + m_v + 1 \leftrightarrow C_{v1} \leftrightarrow \cdots \leftrightarrow C_{vt_v} \leftrightarrow S_v = R_1, \end{gathered}$$

*where* $S_1 = R_2 + l_1$, $S_2 = R_3 + l_2, \ldots, S_{v-1} = R_v + l_{v-1}$, $0 \leq l_t \leq m_t$.

**Corollary 4.10.** *There exists no odd perfect polynomial with* $p$ *irreducible factors* $P_1, \ldots, P_p$ *of the form* $A = P_1^{a_1} \ldots P_p^{a_p}$*, where for any* $j$*,* $\deg(P_j) = 2$*, and* $a_k = 1$*,* $a_l = 2$ *for some* $k, l$*.*

*Proof.* Put $R_1 + m_1 + 1 = x^2 - g$, $R_j + m_j + 1 = (x - d_j)^2 - g_j$ and $S_j = (x - s_j)^2 - h_j$, where $g$, $g_j$, $h_j$ are not square in $\mathbb{F}_p$. We obtain from Corollary 4.5

$$g_1 = g = h_1, \qquad h_j = g_j, \qquad h_v = g_v = g + m_1 + 1.$$

Moreover, for $2 \leq j \leq v$, $h_{j-1} = g_j + m_j + 1 - l_{j-1}$ since $S_{j-1} = R_j + l_{j-1}$. Therefore,

$$g = h_1 = g_2 + m_2 + 1 - l_1 = h_2 + m_2 + 1 - l_1 = g_3 + m_3 + 1 - l_2 + m_2 + 1 - l_1$$

and so on. We get

$$\begin{aligned} g &= g_v + (m_2 + 1) + \cdots + (m_v + 1) - (l_1 + \cdots + l_{v-1}) \\ &= g + (m_1 + 1) + (m_2 + 1) + \cdots + (m_v + 1) - (l_1 + \cdots + l_{v-1}). \end{aligned}$$

But this is impossible since

$$1 \leq (m_1 + 1) + \cdots + (m_v + 1) - (l_1 + \cdots + l_{v-1}) < p. \qquad \square$$

In the next section we prove that there exists *at most* one odd perfect polynomial having exactly $p$ irreducible divisors, each factor being of degree 2 with

exponent 2. We give the exact conditions on $p$ that guarantee the existence of such polynomials. These polynomials were first constructed in [5].

**4.2. The case $a_j = 2$ for any $j \in \{1, \dots, p\}$.** Our proof is inspired by the proof of Theorem 2 in [5], which in turn is obtained by generalizing Link's construction in [12] and [2]. We recall this theorem here together with the main ideas to get it. But first, we need the following elementary fact.

**Lemma 4.11.** *Let $p$ be an odd prime number. Then $(-2)$ is a square in $\mathbb{F}_p$ and $(-3)$ is not if and only if*

$$p \equiv 11 \text{ or } 17 \mod 24.$$

*Proof.* We consider the Legendre symbol $\left(\frac{-}{p}\right)$. We have, by using Gauss's law of quadratic reciprocity:

$$\begin{aligned} 1 &= \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) \\ &= (-1)^{(p-1)/2}(-1)^{(p^2-1)/8} \iff (p \equiv 1 \mod 8) \text{ or } (p \equiv 3 \mod 8), \\ -1 &= \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\ &= (-1)^{(p-1)/2}(-1)^{((3-1)/2)((p-1)/2)}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) \iff (p \equiv 2 \mod 3). \end{aligned}$$

Thus,

$$\begin{aligned} \left(\frac{-2}{p}\right) = 1 \text{ and } \left(\frac{-3}{p}\right) = -1 &\iff (p \equiv 1 \text{ or } 3 \mod 8) \text{ and } (p \equiv 2 \mod 3) \\ &\iff p \equiv 11 \text{ or } 17 \mod 24. \end{aligned}$$

□

**Proposition 4.12** ([5], Theorem 2). *Let $p$ be prime number such that $p \equiv 11$ or $17 \bmod 24$. Then the polynomial $A = \prod_{a \in \mathbb{F}_p}\left((x+a)^2 - 3/8\right)^2$ is odd and perfect over $\mathbb{F}_p$.*

*Proof.* By Lemma 4.11, we may write $-2 = \alpha^2$ for some $\alpha \in \mathbb{F}_p$, whereas $3/8 = (-3)/\alpha^6$ is not a square. So, for any $a \in \mathbb{F}_p$, the polynomial $T_a = (x+a)^2 - 3/8$ is irreducible (over $\mathbb{F}_p$). We remark that

$$\sigma(T_0^2) = 1 + (x^2 - 3/8) + (x^2 - 3/8)^2 = T_{\alpha/2} \cdot T_{-\alpha/2},$$

and

$$\sigma(A) = \prod_{a\in\mathbb{F}_p} \sigma(T_a^2) = \prod_{a\in\mathbb{F}_p} (T_{a+\alpha/2}\cdot T_{a-\alpha/2}) = \prod_{b\in\mathbb{F}_p} T_b \cdot \prod_{c\in\mathbb{F}_p} T_c = A. \qquad \square$$

To finish the proof of Theorem 1.2, it remains to prove two things (which are given by Corollary 4.14):

the polynomial $\prod_{a\in\mathbb{F}_p}\left((x+a)^2 - 3/8\right)^2$ is the only one that is odd and perfect over $\mathbb{F}_p$, with all degrees and exponents equal to 2 if $p \equiv 11$ or $17 \bmod 24$,

if $p$ does not satisfy $p \equiv 11$ or $17 \bmod 24$, then there exists no such odd perfect polynomial over $\mathbb{F}_p$.

**Lemma 4.13.** *Let $A = P_1^2 \dots P_p^2$ be an odd perfect polynomial with $p$ irreducible divisors $P_1, \dots, P_p$ such that, for any $j$, $P_j = (x+a_j)^2 - f_j$. Then for any $i$, there exists a unique* 4*-tuple $(j,k,l,m)$ such that*

$$j \neq i, \quad k \notin \{i,j\}, \quad l \notin \{i,j\}, \quad m \notin \{i,k\}, \quad P_iP_j = \sigma(P_l^2), \quad P_iP_k = \sigma(P_m^2).$$

*Proof.* Existence and uniqueness follow from the fact that each $P_i$ appears exactly two times in $A = \sigma(A)$. $\square$

**Corollary 4.14.** *Let $A = P_1^2 \dots P_p^2$ be an odd polynomial with $p$ irreducible divisors $P_1, \dots, P_p$, such that, for any $j$, $P_j = (x+a_j)^2 - f_j$, with $a_j, f_j \in \mathbb{F}_p$, $f_j$ not a square. Then $A$ is perfect if and only if*

$$\begin{cases} \textit{either } (p \equiv 11 \mod 24) \textit{ or } (p \equiv 17 \mod 24), \\ f_j = f_k = f = 3/8 \textit{ for any } j,k. \end{cases}$$

*Proof.* Sufficiency is obtained from Proposition 4.12.

Necessity: We remark, from Theorem 1.1 iii), that $p$ must satisfy $p \equiv 2 \bmod 3$ so that $(-3)$ is not a square in $\mathbb{F}_p$. By Corollary 4.3 and Lemma 4.13, for any $i$, there exists a unique pair $(j,k)$ such that

$$j \neq i, \quad k \neq i, \quad j \neq k, \quad f_j = f_i = f_k.$$

We then obtain a graph of the form $j \leftrightarrow i \leftrightarrow k$. Hence, by Corollary 4.5, we have $f_j = f_i = f_k$. After re-indexing, we get, for any $l \in \left\{1, \dots, \frac{p-3}{2}\right\}$,

$$3 \leftrightarrow 1 \leftrightarrow 2, \quad 2l \leftrightarrow 2l+2 \leftrightarrow 2l+4,$$
$$2l+3 \leftrightarrow 2l+1 \leftrightarrow 2l-1, \quad p-1 \leftrightarrow p \leftrightarrow p-2.$$

Thus, for any $l \in \left\{1, \dots, \frac{p-3}{2}\right\}$, we have

$$f_{2l+2} = f_2 = f_1 = f_3 = f_{2l+1} = f_p = f_{p-1}.$$

It follows that $f_j = f_k$ for any $j,k \in \{1,\dots,p\}$. By putting $f_j = f_k = f$, Lemma 4.2 gives

$$\begin{cases} f_j = f_k = f \text{ for any } j,k, \\ 1 - f + f^2 \text{ is a square: } 1 - f + f^2 = \alpha^2,\ \alpha \in \mathbb{F}_p, \\ 2f - 1 - 2\alpha \text{ is not a square and } f + \alpha \text{ is a square}, \\ f = -\frac{2\alpha+1}{2}. \end{cases}$$

We may write $A = \prod_{c\in\mathbb{F}_p}\big((x+c)^2 - f\big)^2$. Since $A$ is perfect, we can write

$$\sigma\big((x^2-f)^2\big) = \big((x+a)^2 - f\big)\big((x+b)^2 - f\big),$$

and we obtain by comparing coefficients (see (8) with $a_j = a$, $f_j = f$)

$$b = -a, \qquad -2a^2 - 1 = 0, \qquad (a^2 - f)^2 = 1 - f + f^2.$$

Therefore,

$$a^2 = -1/2, \qquad -3/4 + 2f = 0,$$

and thus

$$(-2) = (1/a)^2 \text{ is a square in } \mathbb{F}_p,\ f = 3/8,\ \alpha = -7/8 \text{ since } f = -\frac{2\alpha+1}{2}.$$

Now, since $f = 3/8 = (-3)\big(1/(-2)\big)^3$, with $(-2)$ a square and $f$ not a square, we see that $(-3)$ is not a square in $\mathbb{F}_p$. By Lemma 4.11 we obtain

$$p \equiv 11 \text{ or } 17 \mod 24. \qquad \square$$

**Acknowledgments.** We are indebted to the referees for their careful reading and interesting suggestions. The result is an improved paper.

## References

[1] J. T. B. Beard, Jr., Perfect polynomials revisited. *Publ. Math. Debrecen* **38** (1991), 5–12. Zbl 0743.11068 MR 1100900

[2] J. T. B. Beard, Jr. and M. L. Link, Iterated sums of polynomial divisors. *Libertas Math.* **17** (1997), 111–124. Zbl 0890.11033 MR 1485670

[3] J. T. B. Beard, Jr., J. R. O'Connell, Jr., and K. I. West, Perfect polynomials over GF($q$). *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (8) **62** (1977), 283–291. Zbl 0404.12014 MR 497649

[4] E. F. Canaday, The sum of the divisors of a polynomial. *Duke Math. J.* **8** (1941), 721–737. Zbl 0061.06605 MR 0005509

[5] L. Gallardo, P. Pollack, and O. Rahavandrainy, On a conjecture of Beard, O'Connell and West concerning perfect polynomials. *Finite Fields Appl.* **14** (2008), 242–249. Zbl 1130.11070 MR 2381490

[6] L. Gallardo and O. Rahavandrainy, Perfect polynomials over $\mathbb{F}_4$ with less than five prime factors. *Port. Math.* (*N.S.*) **64** (2007), 21–38. Zbl 1196.11160 MR 2298110

[7] L. H. Gallardo and O. Rahavandrainy, Odd perfect polynomials over $\mathbb{F}_2$. *J. Théor. Nombres Bordeaux* **19** (2007), 165–174. Zbl 1145.11081 MR 2332059

[8] L. H. Gallardo and O. Rahavandrainy, Perfect polynomials over $\mathbb{F}_3$. *Int. J. Algebra* **2** (2008), 477–492. Zbl 1209.11104 MR 2443823 (2010a:11235)

[9] L. H. Gallardo and O. Rahavandrainy, There is no odd perfect polynomial over $\mathbb{F}_2$ with four prime factors. *Port. Math.* (*N.S.*) **66** (2009), 131–145. Zbl 1193.11116 MR 2522765

[10] L. H. Gallardo and O. Rahavandrainy, On even (unitary) perfect polynomials over $\mathbb{F}_2$. *Finite Fields Appl.* **18** (2012), 920–932. Zbl 06092701 MR 2964733

[11] P. Hummel, On consecutive quadratic non-residues: a conjecture of Issai Schur. *J. Number Theory* **103** (2003), 257–266. Zbl 1049.11006 MR 2020271

[12] M. L. Link, Iterated sums of polynomial divisors over GF($p$). Master's thesis, Tennessee Technological University, Cookeville, TN, 1995.

Received May 19, 2012

L. H. Gallardo, Department of Mathematics, University of Brest, CNRS UMR 6205, 6 Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France

E-mail: luisgall@univ-brest.fr

O. Rahavandrainy, Department of Mathematics, University of Brest, CNRS UMR 6205, 6 Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France

E-mail: rahavand@univ-brest.fr