PERFECT POLYNOMIALS OVER $\mathbb{F}_p$
WITH $p + 1$ IRREDUCIBLE DIVISORS

L. H. GALLARDO and O. RAHAVANDRAINY

ABSTRACT. We consider, for a fixed 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. We give necessary conditions for the existence of such polynomials, called perfect polynomials, having $p + 1$ irreducible factors. These conditions allow us to describe the set of all perfect polynomials with $p + 1$ irreducible divisors in the first unknown case, namely, the case $p = 3$.

1. Introduction

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

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

be the sum of all monic divisors of $A$ (1 and $A$ included). The restriction to monic polynomials is necessary since the sum of all divisors of $A$ that have a given degree is zero. 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). This fact is 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 that $n$ divides $\sigma(n)$. For example, 120 is a multiperfect number since 120 divides 360 = $\sigma(120)$. Indeed, since $\deg(A) = \deg(\sigma(A))$, 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). This definition is natural in the understanding that a polynomial $P \in \mathbb{F}_p[x]$, with absolute value $|P| := p^{\deg(P)}$ is even if and only if it has a divisor $d$ with absolute value $|d| = p$.

Received March 2, 2013.
2010 Mathematics Subject Classification. Primary 11T55, 11T06.
Key words and phrases. Sum of divisors; polynomials; finite fields; characteristic $p$. 

Acta Math. Univ. Comenianae
Vol. LXXXIII, 1 (2014), pp. 93–112
Throughout the paper, we assume that “a polynomial” means a monic polynomial and that the notion of polynomial irreducibility is defined over $\mathbb{F}_p$.

Important results about perfect polynomials appear in the work of Canaday [1] and Beard et al. ([2], [3]). Indeed Canaday introduced the subject, working in the case $p = 2$ in his thesis under Carlitz while Beard et al. extended these results to $\mathbb{F}_p$ with odd $p$ in the special case where the polynomials considered split completely over $\mathbb{F}_p$. Trivially, there is no odd perfect polynomial over $\mathbb{F}_2$ with $\omega(A) = 1$.

Canaday [1, Theorem 17] proved the inexistence of odd perfect polynomials over $\mathbb{F}_2$ with two irreducible factors, i.e., with $\omega(A) = 2$. We obtained recently some results about even or splitting perfect polynomials that generalize the work of Canaday and Beard et al., (see [9] and the references therein). Nevertheless, providing complete lists of perfect polynomials satisfying some properties (even polynomials, odd polynomials, splitting polynomials) remains difficult because it is difficult to know precisely the manner in which a given polynomial factorizes over $\mathbb{F}_p$, (like the difficulty of factorization of special type of integers prevents to know more about the multiperfect numbers).

Observe that for any given positive integer $w$, there is an infinity of polynomials $A \in \mathbb{F}_p[x]$ with $\omega(A) = w$, so potentially an infinity of perfect polynomials with $\omega(A) = w$ may exist. The following restriction is important.

A perfect polynomial over $\mathbb{F}_p$ must have a multiple of $p$ number of minimal irreducible divisors (see Lemma 2.2), so trivially there is no perfect polynomial over $\mathbb{F}_p$ with less than $p$ irreducible factors. We proved in [6], [8] (resp. [7]) the inexistence of odd perfect polynomials over $\mathbb{F}_2$ with $\omega(A) \in \{3, 4\}$ (resp. over $\mathbb{F}_3$ with $\omega(A) = 3$). In particular, this settles the case $p = 2$ of the present paper. We should take then $p$ as an odd prime in all the paper. We proved also [10] some general results about odd perfect polynomials over $\mathbb{F}_p$ with $p$ irreducible factors, leaving unknown the list of such polynomials. However, we got the following explicit result (see [10, Theorem 1.2]):

The unique odd perfect polynomial over $\mathbb{F}_p$, with $p$ irreducible factors of degree 2 for which all exponents do not exceed two is

$$A(x) := \prod_{a \in \mathbb{F}_p} \left((x + a)^2 - 3/8\right)^2,$$

where either $(p \equiv 11 \mod 24)$ or $(p \equiv 17 \mod 24)$.

It is natural to consider the following case. What can we say about perfect polynomials with $p + 1$ irreducible factors? Is it possible to provide the complete list $L(p)$ of such polynomials? In particular, is this list finite? We know only $L(2)$ (see [1, Theorem 9] and [6, Theorem 3.1]) that consists of the four even polynomials in $\mathbb{F}_2[x]$

$$S_1(x) = x(x + 1)^2(x^2 + x + 1), \quad S_2(x) = S_1(x + 1),$$

$$S_3(x) = x^3(x + 1)^4(x^4 + x^3 + 1), \quad S_4(x) = S_3(x + 1).$$

From some computations reported in [2], the list $L(3)$ contains the following three perfect polynomials of degree 8 in $\mathbb{F}_3[x]$ which are also even:

$$A_1(x) := x^3(x + 1)^2(x + 2)(x^2 + 1), \quad A_2(x) := A_1(x + 1), \quad A_3(x) := A_1(x + 2).$$
In this paper, in Theorem 1.1, we first establish some necessary conditions for the non-vacuity of the list \( L(p) \), for a fixed odd prime number. Secondly, we prove Theorem 1.2 by means of Theorem 1.1 that \( L(3) \) does not contain anything else.

**Theorem 1.1.** Let \( p \) be an odd prime number. Let \( A = P_1^{a_1} \cdots P_p^{a_p} Q^b \) be a perfect polynomial over \( \mathbb{F}_p \) with \( p + 1 \) irreducible factors. Then \( d := \deg(P_1) = \cdots = \deg(P_p) \) and

i) \((A \text{ is even}) \ or \ (a_j \text{ is even for at least one } j \in \{1, \ldots, p\})\),

ii) for at least one \( j \in \{1, \ldots, p\} \), \( a_j \) is of the form \( N_j p^{n_j} - 1 \) with \( N_j, n_j \in \mathbb{N}, \ N_j \geq 1, p \nmid N_j \), and \( N_j \mid (p - 1) \),

iii) either \((p \nmid b + 1) \ or \ (b \in \{p - 1, 2p - 1\} \ and \ d \mid \deg(Q)).\)

**Theorem 1.2.** The only perfect polynomials over \( \mathbb{F}_3 \) with four irreducible factors are:

\[
\begin{align*}
x^3(x + 1)^2(x + 2)(x^2 + 1), & \quad x(x + 1)^3(x + 2)^2(x^2 + 2x + 2), \\
\text{and} \quad x^2(x + 1)(x + 2)^3(x^2 + x + 2).
\end{align*}
\]

By contrast with the integer perfect numbers, observe that Sylvester [12] already proved in 1888 that every odd perfect number has at least five prime factors. Later, Dickson [4] proved that there is a finite number of odd perfect numbers with a given number \( \omega \) of prime divisors. For polynomials over finite fields, we have not yet an analogue of these important results.

## 2. Some useful facts

We denote, the set of nonnegative integers (resp. of positive integers) as usual by \( \mathbb{N} \) (resp. by \( \mathbb{N}^* \)). For a set \( A \), we denote the cardinal of \( A \) by \#\( A \).

For polynomials \( A, B \in \mathbb{F}_p[x] \), we write: \( A^n \parallel B \) if \( A^n \mid B \) but \( A^{n+1} \nmid B \).

**Definition 2.1.** We say that a polynomial \( P \) is a minimal irreducible divisor of \( A \) if \( P \) is an irreducible divisor of \( A \) such that \( \deg(P) \leq \deg(R) \) for any irreducible divisor \( R \) of \( A \).

A basic but important result is the following.

**Lemma 2.2.** (see [5, Lemma 2.5]) Let \( p \) be a prime number. Let \( A \in \mathbb{F}_p[x] \) be a perfect polynomial. Then the number of minimal irreducible divisors of \( A \) is a multiple of \( p \).

We immediately get the corollary.

**Corollary 2.3.** Any perfect polynomial \( A \) over \( \mathbb{F}_p \), with exactly \( p + 1 \) irreducible factors may be written as

\[
A = P_1^{a_1} \cdots P_p^{a_p} \cdot Q^b, \quad \text{where } a_j, b \in \mathbb{N}^* \text{ and } \deg(P_1) = \cdots = \deg(P_p) < \deg(Q).
\]

**Notation 2.4.** In the rest of the paper, we fix an odd prime number \( p \).

According to Corollary 2.3 for a perfect polynomial \( A \in \mathbb{F}_p[x] \) with \( \omega(A) = p + 1 \), we put

\[
A = P_1^{a_1} \cdots P_p^{a_p} \cdot Q^b,
\]
where \( a_1, \ldots, a_p, \) \( b \in \mathbb{N}^* \) and \( \deg(P_1) = \cdots = \deg(P_p) < \deg(Q), \) \( a_i = N_ip^{n_i} - 1, \) \( b = Mp^{n_1} - 1, \) \( N_1, n_i, M, m \in \mathbb{N}, \) \( N_1, M \geq 1, \) \( p \nmid N_1, p \nmid M. \)

Note that \( P_1, \ldots, P_p \) may be even whereas \( Q \) is always odd.

For \( S \in \{ Q, P_1, \ldots, P_p \} \) and for \( s \in \{ b, a_1, \ldots, a_p \}, \) we would like to understand how \( \sigma(S^s) = 1 + S + \cdots + S^s \) may be factorized into irreducible divisors of \( A \)

\[
\sigma(S^s) = P_1^{c_1} \cdots P_p^{c_p} \cdot Q^c, \quad \text{where } c, c_l \geq 0 \text{ for any } l \in \{1, \ldots, p\}.
\]

We may write \( s := Np^n - 1 \) for some \( N, n \in \mathbb{N} \) such that \( N \geq 1 \) and \( p \nmid N. \)

In that case, we put \( d := \gcd(N, p - 1) \) and we denote by \( L_N \) the splitting field of \( x^N - 1 \) over \( \mathbb{F}_p \), which is a strict subset of the algebraic closure \( \mathbb{F}_p \).

Moreover, since \( p \nmid N, \) the polynomial \( x^N - 1 \) has no multiple root (in \( L_N \)). The set \( \mathbb{U}_N := \{ \lambda \in L_N : \lambda^N = 1 \} \) of \( N \)-th roots of unity in \( L_N \) is a cyclic group of order \( N \) (see \([11, \text{Theorem 2.42}]\)).

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 extension \( L_N \) over \( \mathbb{F}_p \) is generated by \( \phi_p. \) The Galois group \( G \) 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 recall that a polynomial \( P \in L_N[x] \) lies in \( \mathbb{F}_p[x] \) if and only if \( \phi_p(P) = P. \)

In Sections 3 and 4 we will use the following facts very often.

**Lemma 2.5.** (see \([10, \text{Lemma 2.4}]\)) Let \( S \in \mathbb{F}_p[x] \) be an irreducible polynomial such that \( S - \mu \) is irreducible for any \( \mu \in \mathbb{F}_p. \) Then \( \deg(S) = 1, \) so that \( S \) is even.

**Lemma 2.6.** Let \( S \in \mathbb{F}_p[x] \) be an irreducible polynomial and \( N \in \mathbb{N}^* \) with \( p \nmid N. \) If \( \sigma(S^{N-1}) = Q_1^{c_1} \cdots Q_l^{c_l}, \) where \( Q_l \) is irreducible, \( \gcd(S, Q_l) = 1 \) and \( \deg(S) \leq \deg(Q_l) \) for any \( l, \) then \( c_l \in \{0, 1\} \) for any \( l. \)

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

\[
1 + S + \cdots + S^{N-1} = R^mC, \quad \text{where } m = c_l \text{ and } R = Q_l.
\]

We get

\[
S^N - 1 = (S - 1)R^mC.
\]

Since \( p \nmid N \) by taking derivatives on both sides of (1) one has

\[
0 \neq NS^{N-1}S' = R^{m-1}(S'R'C + (S - 1)(mR'C + RC')), \n\]

so with the observation \( \gcd(S, R) = 1, \)

\[
R^{m-1} \mid S'.
\]

Thus, we get the contradiction

\[
\deg(S) \leq (m - 1) \deg(S) = (m - 1) \deg(R) \leq \deg(S') < \deg(S). \quad \square
\]
3. The proof of Theorem 1.1

We recall (see Notation 2.4) that we are interested in perfect polynomials of the form

\[ A = P_{a_1}^{\alpha_1} \cdots P_{a_p}^{\alpha_p} \cdot Q^b, \]

where \( a_1, \ldots, a_p, b \in \mathbb{N}^* \) and \( \deg(P_1) = \cdots = \deg(P_p) < \deg(Q) \), \( \alpha_i = N_i p^{n_i} - 1 \), \( b = Mp^m - 1 \), \( N_i, n_i, M, m \in \mathbb{N} \), \( N_i, M \geq 1 \), \( p \nmid N_i \), \( p \nmid M \).

We give more precisions about \( Q \) and its exponent \( b \) below.

### 3.1. Necessary conditions on \( Q \) and on \( b \)

In this section we consider the following subsets of \( \{1, \ldots, p\} \)

\[ \Lambda := \{ i : n_i = 0 \}, \quad \Sigma_1 := \{ i : Q \nmid (P_i^{\alpha_i}) \}, \quad \Sigma_2 := \{ i : Q \nmid (P_i^{\alpha_i}) \}. \]

We see that \( \Sigma_1 \neq \emptyset \), \( \Sigma_1 \cap \Sigma_2 = \emptyset \) and \( \Sigma_1 \cup \Sigma_2 = \{1, \ldots, p\} \).

**Lemma 3.1.** If \( i \in \Lambda \setminus \Sigma_1 \), then \( a_i \leq p - 2 \).

**Proof.** One has

\[ a_i = N_i - 1, \quad p \nmid N_i, \quad \sigma(P_i^{\alpha_i}) = \prod_{j \neq i} P_j^{\alpha_j}, \]

where \( \alpha_{ji} \in \{0, 1\} \) by Lemma 2.6.

Thus

\[ a_i = \sum_{j \neq i} \alpha_{ji} \leq p - 1 \quad \text{and} \quad a_i = N_i - 1 \neq p - 1 \quad \text{since} \quad p \nmid N_i. \quad \Box \]

**Lemma 3.2.**

i) If \( i \in \Sigma_1 \), then \( Q^{\alpha_i} \parallel \sigma(P_i^{\alpha_i}) \).

ii) One has

\[ b = Mp^m - 1 = \sum_{i \in \Sigma_1} p^{n_i} = \#(\Lambda \cap \Sigma_1) + \sum_{i \in \Sigma_1 \setminus \Lambda} p^{n_i}. \quad (2) \]

**Proof.** i) One has

\[ \sigma(P_i^{\alpha_i}) = (P_i - 1)^{p^{n_i} - 1 \cdot \sigma(P_i^{N_i - 1})^{p^{n_i}}}, \]

where \( \sigma(P_i^{N_i - 1}) \) is square free by Lemma 2.6. Hence, \( Q \parallel \sigma(P_i^{N_i - 1}). \)

ii) The exponent of \( Q \) in \( A \) is \( b \). The exponent of \( Q \) in \( \sigma(A) \) is that of \( Q \) in \( \prod_{i \in \Sigma_1} \sigma(P_i^{\alpha_i}) \). We get (2) from i). \quad \Box

**Corollary 3.3.** Let \( A = P_{a_1}^{\alpha_1} \cdots P_{a_p}^{\alpha_p} \cdot Q^b \in \mathbb{F}_p[x] \) be perfect with \( b = Mp^m - 1 \), \( p \nmid M \). If \( m \geq 1 \), then \( \#(\Lambda \cap \Sigma_1) = p - 1 \) and \( \deg(P) \mid \deg(Q) \).

More precisely, we must have:

i) \( M = m = 1 \) if \( \#\Lambda = p, \#\Sigma_1 = p - 1 \) or \( \#\Lambda = \#\Sigma_1 = p - 1 \).

ii) \( M = p^{n_k - 1} + 1, \ m = 1, \ Q(\alpha) \notin \{-1, 1\} \) for any \( \alpha \in \mathbb{F}_p \) if \( \#\Lambda = p - 1 \) and \( \#\Sigma_1 = p \), where \( k \) is the unique integer not lying on \( \Lambda \) (\( n_k \geq 1 \)).
Proof. We see that
\[ \#(\Lambda \cap \Sigma_1) \leq \#\Lambda \leq p. \]
We apply Relations (2) in Lemma 3.2.
If \( m \geq 1 \), then \( \#(\Lambda \cap \Sigma_1) \equiv -1 \mod p \). So, \( \#(\Lambda \cap \Sigma_1) = p - 1 \).
We get four cases:
- If \( \#\Lambda = \#\Sigma_1 \), then \( \#\Lambda = \#\Sigma_1 = \{1, \ldots, p\} \) and \( p - 1 = \#(\Lambda \cap \Sigma_1) = p \), which is impossible.
- If \( \#\Lambda = p \) and \( \#\Sigma_1 = 1 \), then \( b = Mp^m - 1 = p - 1 \). So, \( M = m = 1 \).
- If \( \#\Lambda = p - 1 \) and \( \#\Sigma_1 = p \), let \( k \) be the unique integer such that \( k \not\in \Lambda \).

We get
\[ b = Mp^m - 1 = p - 1 + p^n = p(p^n - 1) - 1, \text{ where } p \nmid (p^n - 1). \]
It follows that
\[ \sigma(Q^b) = \frac{Q^{b+1} - 1}{Q - 1} = (Q - 1)^{p - 1} \cdot (1 + Q + \cdots + Q^{p^n - 1})^p. \]
We see that \( Q - 1 \) divides \( \sigma(A) = A \) which is odd, so for any \( \alpha \in \mathbb{F}_p \), \( Q(\alpha) \neq 1 \).
Remark also that for any \( v \geq 1 \) and for any \( \alpha \in \mathbb{F}_p \), one has
\[ (1 + \cdots + Q^v)(\alpha) = \left( \frac{Q^{v+1} - 1}{Q - 1} \right)(\alpha) = \frac{(Q(\alpha))^{v+1} - 1}{Q(\alpha) - 1} = Q(\alpha) + 1. \]
Thus
\[ (\sigma(Q^b))(\alpha) = 0 \text{ whenever } Q(\alpha) = -1. \]
It is impossible since \( \sigma(Q^b) \) divides \( \sigma(A) = A \) and \( A \) is odd. \( \square \)

Corollary 3.4. Let \( A = P_{a1} \cdots P_{ap} \cdot Q^b \in \mathbb{F}_p[x] \) be perfect with \( b = Mp^m - 1 \), \( p \nmid M \). If \( m = 0 \), then
i) \( b = M - 1 = \sum_{i \in \Sigma_1} p^{n_i} = \#(\Lambda \cap \Sigma_1) + \sum_{i \in \Sigma_1 \cap \Lambda} p^{n_i} \),
ii) we have either \( \Lambda = \Sigma_1 = \{1, \ldots, p\} \) or \( \#(\Lambda \cap \Sigma_1) \leq p - 2 \).

Proof. Relations (2) in Lemma 3.2 give i) and imply that \( p \) divides \( M \) if \( \#(\Lambda \cap \Sigma_1) = p - 1 \). It is impossible. \( \square \)

Lemma 3.5. One has
\[ \sigma(x^p) = (1 + x) \cdot \prod_{i=1}^{p-1} (x^2 - u_ix + 1), \]
where \( u_i = \xi^i + \frac{1}{\xi} \) with \( \xi \) a primitive \((p + 1)\)-root of unity, \( u_i \not\in \{-2, 2\} \), and \( x^2 - u_ix + 1 \) is irreducible over \( \mathbb{F}_p \).
For any $i \in \{1, \ldots, \frac{p-1}{2}\}$, $x^2 - u_ix + 1 = (x - \xi^i)(x - \frac{1}{\xi^i})$ lies in $\mathbb{F}_p[x]$ since $u_i = \xi^i + \frac{1}{\xi^i}$ is invariant by the Frobenius morphism $\phi_p: x \mapsto x^p$.

Note that $(\xi^i)^2 \neq 1$ for any $i \in \{1, \ldots, \frac{p-1}{2}\}$ and $u_i \not\in \{-2, 2\}$. Remark also that $\phi_p(\xi^i - \frac{1}{\xi^i}) = -\xi^i + \frac{1}{\xi^i} \neq \xi^i - \frac{1}{\xi^i}$ so that $\xi^i - \frac{1}{\xi^i} \not\in \mathbb{F}_p$.

Each polynomial $x^2 - u_ix + 1$ is then irreducible over $\mathbb{F}_p$, because its discriminant $\delta_i := (\xi^i + \frac{1}{\xi^i})^2 - 4 = (\xi^i - \frac{1}{\xi^i})^2$ is not a square in $\mathbb{F}_p$. \hfill \Box

**Lemma 3.6.** Let $v \geq 2$ and let $\xi$ be a primitive $p^v + 1$-root of unity. Then, for any $i, j \in \{1, \ldots, p-1\}$ and for any $k, r \in \{0, \ldots, 2v-1\}$

$$\xi^{ip^k} \neq \xi^{jp^r}$$

whenever $(i, k) \neq (j, r)$.

**Proof.** If $\xi^{ip^k} = \xi^{jp^r}$ for some $(i, k) \neq (j, r)$, then $ip^k - jp^r \equiv 0 \mod (p^v + 1)$. We may suppose that $k \geq r$, so that $ip^{k-r} - j \equiv 0 \mod (p^r + 1)$.

If $k = r$, then $i - j \equiv 0 \mod (p^r + 1)$ and we must have $i = 0$ since $v \geq 2$. So, $k > r$. Put

$$ip^{k-r} - j = c \cdot (p^r + 1).$$

We easily see that $p \nmid c$ and we may write $c$ in base $p$ expansion

$$c = e_0p^z + e_1p^{z-1} + \cdots + e_{z-1}p + e_z,$$

where $e_l \in \{0, \ldots, p-1\}$ and $z \geq 0$. Therefore,

$$ip^{k-r} = p^v \cdot \sum_{l=0}^{z} e_l p^{z-l} + e_0p^z + e_1p^{z-1} + \cdots + e_{z-1}p + e_z + j. \quad (3)$$

Hence

$$z + v = k - r, \quad e_0 = i \neq 0.$$ 

If $z = 0$, then $v = k - r$ and $ip^v = i \cdot (p^r + 1) + j$, which is impossible. If $z \geq 1$, then $ip^v$ occurs in the right hand side of Relation (3), but not in the left. It is also impossible. \hfill \Box

**Lemma 3.7.** For any $v \geq 2$, $\sigma(x^{p^v})$ is divisible at least by $p - 1$ polynomials (irreducible or not) $R_1, \ldots, R_{p-1}$ of degree $2v$ such that $\gcd(R_i(S), R_j(S)) = 1$ if $i \neq j$ for any $S \in \mathbb{F}_p[x]$. 


Proof. As above, let $\xi$ be a primitive $p^v + 1$-root of unity. Put $N := p^v + 1$ and
\[
R_1 = (x - \xi)(x - \xi^p) \cdots (x - \xi^{p^v - 1}), \\
R_2 = (x - \xi^2)(x - \xi^{2p}) \cdots (x - \xi^{2p^{v-1}}), \\
\vdots \\
R_l = (x - \xi^l)(x - \xi^{lp}) \cdots (x - \xi^{lp^{v-1}}), \\
\vdots
\]
For $S \in \mathbb{F}_p[x]$ and for $l \in \{1, \ldots, p - 1\}$, we get
\[
R_l(S) = (S - \xi^l)(S - \xi^{lp}) \cdots (S - \xi^{lp^{v-1}}).
\]
For any $l$, let $S_{1,l}, \ldots, S_{2v,l}$ be the elementary symmetric polynomials in $(\xi^l, \xi^{lp}, \ldots, \xi^{lp^{v-1}})$. For any $l$ and for any $1 \leq k \leq 2v$, we get
\[
\phi_p(S_{k,l}) = (S_{k,l})^p = S_{k,l},
\]
so that
\[
\phi_p(R_l) = R_l \quad \text{and} \quad R_l \in \mathbb{F}_p[x].
\]
We see that $\deg(R_l) = 2v$ and if $\gcd(R_l(S), R_j(S)) = 1$ in $L_N[x]$, then $\gcd(R_l(S), R_j(S)) = 1$ in $\mathbb{F}_p[x]$.

Let us prove that $\gcd(R_l(S), R_j(S)) = 1$ in $\mathbb{F}_p[x]$ if not, let $W \in L_N[x]$ be an irreducible (over $L_N$) common divisor of $R_l(S)$ and $R_j(S)$. We must have modulo $W$
\[
\xi^{lp^k} = S \equiv \xi^{lp^r},
\]
for some $k \in \{0, \ldots, 2i - 1\}$ and for some $r \in \{0, \ldots, 2j - 1\}$. Thus
\[
\xi^{lp^k} = \xi^{lp^r},
\]
which contradicts Lemma 3.6. \qed

Lemma 3.8. If $A = P_1^{a_1} \cdots P_p^{a_p} \cdot Q^p$ is perfect (with $\deg(Q) > \deg(P_j)$) and if $Q^2 - uQ + 1$ divides $\sigma(Q^p)$ for some $u \in \mathbb{F}_p \setminus \{-2, 2\}$, then
\[
\omega(Q^2 - uQ + 1) \geq 2.
\]

Proof. If $\omega(Q^2 - uQ + 1) = 1$, then
\[
Q^2 - uQ + 1 = P^w
\]
for some $P \in \{P_1, \ldots, P_p\}$, because $Q \mid (Q^2 - uQ + 1)$ and $(Q^2 - uQ + 1) \mid \sigma(Q^p) \mid \sigma(A) = A$.

Since $\deg(Q) > \deg(P)$, we see that $w = \frac{2 \deg(Q)}{\deg(P)} \geq 3$. By taking derivatives in both sides of (4), one has
\[
Q' \cdot (2Q - u) = w P^w - 1, \quad P'.
\]
If $P$ divides $2Q - u$, then $2Q \equiv u \mod P$ and
\[
\frac{u^2}{4} + 1 = \frac{u^2}{4} - \frac{u^2}{2} + 1 \equiv Q^2 - uQ + 1 \equiv 0 \mod P.
\]
Thus $u^2 = 4 \mod P$ and $u \in \{-2, 2\}$, which is impossible. So,

$$P \nmid (2Q - u), \quad P^{w-1} | Q', \quad Q' = P^{w-1} \cdot R$$

for some $R \in \mathbb{F}_p[x]$ and

$$R \cdot (2Q - u) = wP',$$

which is impossible by considering degrees. □

Remark 3.9. The conclusion in Lemma 3.8 does not hold in a more general context. For example, take $p = 3$, $Q = x^2 + 1$ which is odd and irreducible over $\mathbb{F}_3$, $\xi$ a primitive 4-root of 1. One has $\xi \not\in \{-2, 2\}$, $u := \xi + \frac{1}{\xi} = 0$ and

$$Q^2 - uQ + 1 = Q^2 + 1 = x^4 + 2x^2 + 2$$

which is irreducible over $\mathbb{F}_3$ with $\omega(Q^2 - uQ + 1) = 1$.

**Corollary 3.10.** Let $A = P_1^{a_1} \ldots P_p^{a_p} \cdot Q^p \in \mathbb{F}_p[x]$ be perfect (with $\deg(Q) > \deg(P_j)$). Then

i) The polynomial $\sigma(Q^p)$ has at least $p + 1$ irreducible factors.

ii) More generally, $\sigma(Q^{p^v})$ has at least $p + 1$ irreducible factors for any $v \geq 1$.

**Proof.** i) We get

$$\sigma(Q^p) = (Q + 1) \cdot \prod_{i=1}^{p-1} (Q^2 - u_i Q + 1).$$

Remark that

- for any $i$, $u_i \not\in \{-2, 2\}$, $\gcd(Q + 1, Q^2 - u_i Q + 1) = 1$,
- for any $i, j$, $u_i \neq u_j$ and $\gcd(Q^2 - u_i Q + 1, Q^2 - u_j Q + 1) = 1$,
- for any $i$, $\omega(Q^2 - u_i Q + 1) \geq 2$ by Lemma 3.8 and $\omega(Q + 1) \geq 2$.

It follows that

$$\omega(\sigma(Q^p)) \geq 2 \cdot \frac{p-1}{2} + 2 = p + 1.$$

ii) Each polynomial $R_i(Q)$ divides $\sigma(Q^{p^v})$ and $\gcd(R_i(Q), R_j(Q)) = 1$ in $\mathbb{F}_p[x]$ if $i \neq j$. Moreover, $\omega(R_i(Q)) \geq 2$ for any $l$. So

$$\omega(\sigma(Q^{p^v})) \geq 2(p-1) \geq p + 1.$$ □

From Corollaries 3.3, 3.4 and 3.10, we get the following corollary

**Corollary 3.11.** Let $A = P_1^{a_1} \ldots P_p^{a_p} \cdot Q^p \in \mathbb{F}_p[x]$ be perfect (with $\deg(Q) > \deg(P_j)$) and $b = Mp^m - 1$, $p \nmid M$.

i) If $m = 0$, then $p \nmid b + 1$ and $\#(\Lambda \cap \Sigma_1) \leq p - 2$.

ii) If $m \geq 1$, then $m = 1$, $M \in \{1, 2\}$, so $b \in \{p - 1, 2p - 1\}$.

**Proof.** i) If $m = 0$ and if $\Lambda = \Sigma_1 = \{1, \ldots, p\}$, then $b = p$. We get

$$p \geq \omega(\sigma(Q^p)) \geq p + 1,$$

which is impossible.
ii) If \( m \geq 1 \), then \( m = 1 \). If \( M = p^{n_k} + 1 \) with \( n_k \geq 2 \), then \( \sigma(Q^{M-1}) = \sigma(Q^{p^{n_k-1}}) \) has at least \( p+1 \) irreducible factors. It is impossible as in the proof of Corollary 3.10.

\[ \square \]

3.2. The proof

By using Notation 2.4, Propositions 3.12 and 3.13 give the first and second part of our theorem. Corollary 3.11 gives the third part.

**Proposition 3.12.** There are no odd perfect polynomials over \( \mathbb{F}_p \) of the form \( P_1^{a_1} \cdots P_r^{a_r} \cdot Q^b \) with \( p+1 \) irreducible divisors where \( a_i \) is odd for any \( i \in \{1, \ldots, r\} \).

**Proof.** Since \( a_1 \) is odd, \( P_1 + 1 \) divides \( \sigma(P_1^{\alpha_1}) \). \( P_1 + 1 \) 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, \( \{P_1, \ldots, P_r\} = \{P_1, P_1 + 1, P_1 + 2, \ldots, P_1 + (p - 1)\} \) and hence \( P - \mu \) is irreducible for any \( \mu \in \mathbb{F}_p \). This contradicts Lemma 2.5.

**Proposition 3.13.** There exist no perfect polynomials over \( \mathbb{F}_p \) of the form \( P_1^{a_1} \cdots P_r^{a_r} \cdot Q^b \) with \( p+1 \) irreducible divisors where for any \( i \in \{1, \ldots, r\} \),

\[ a_i = N_i p^{n_i} - 1, \quad p \nmid N_i, \quad N_i \mid p - 1. \]

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

\[ \sigma(P_i^{\alpha_i}) = \prod_{\mu \in \Omega_{N_i}} (P_i - \mu)^{c_\mu}. \]

If \( A \) is perfect, then

\[ A = \sigma(A) = \prod_i \sigma(P_i^{\alpha_i}) \cdot \sigma(Q^b) = \prod_i \prod_{\mu \in \Omega_{N_i}} (P_i - \mu)^{c_\mu} \cdot \sigma(Q^b). \]

Therefore, we may put

\[ A = \prod_i A_i \cdot \sigma(Q^b) = \prod_i \prod_{\xi \in \mathbb{F}_p} (P_i - \xi)^{b_\xi} \cdot \sigma(Q^b), \]

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

Since \( Q \nmid \sigma(Q^b) \), we see that \( Q \) does not divide \( A \), which is impossible.

\[ \square \]

4. THE PROOF OF THEOREM 1.2

In this section, we take \( p = 3 \), so (see Notation 2.4)

\[ A = P_1^{a_1} P_2^{a_2} P_3^{a_3} \cdot Q^b, \]

where \( a_1, a_2, a_3, b \in \mathbb{N}^* \), \( \text{deg}(P_1) = \text{deg}(P_2) = \text{deg}(P_3) < \text{deg}(Q) \), \( a_i = N_i 3^{n_i} - 1 \), \( b = M \cdot 3^m - 1 \), \( N_i, n_i, M, m \in \mathbb{N} \), \( N_i, M \geq 1 \), \( 3 \nmid N_i \), \( 3 \nmid M \).

As in Section 3.1, we put

\[ \Lambda = \{i \in \{1, 2, 3\} : n_i = 0\} \text{ and } \Sigma_1 = \{i \in \{1, 2, 3\} : Q \mid \sigma(P_i^{\alpha_i})\}. \]
PERFECT POLYNOMIALS OVER $\mathbb{F}_p$ WITH $p+1$ IRREDUCIBLE DIVISORS 103

The following results are useful.

**Lemma 4.1.** Let $A = P_{a_1}^1 P_{a_2}^2 P_{a_3}^3 : Q^b \in \mathbb{F}_3[x]$ be perfect.

- If $j \in \Lambda$, then $a_j = N_j - 1 \neq 2$.
- If $j \in \Lambda \setminus \Sigma_1$, then $a_j = N_j - 1 = 1$.

**Proof.** We suppose that $j = 2$ without loss of generality. From Lemma 2.6, we get

$$\sigma(P_{a_2}^2) = P_{\beta_1}^1 P_{\beta_3}^3,$$

$$a_2 = \beta_1 + \beta_3 \leq 2.$$  

Since $3 \nmid N_2$, we must have $a_2 = 1$. $\square$

**Lemma 4.2.** Let $p$ be an odd prime number such that $p \equiv 3 \mod 4$ and let $v$ be a positive integer. Then the polynomial $1 + (x^2)^1 + \cdots + (x^2)^v$ is irreducible over $\mathbb{F}_p$ if and only if $v = 1$.

**Proof.** The sufficiency is obvious since $1 + x^2$ is irreducible over $\mathbb{F}_p$ whenever $p \equiv 3 \mod 4$. Now, we prove the necessity. One has

$$S(x) := 1 + (x^2)^1 + \cdots + (x^2)^v = \frac{(x^2)^{v+1} - 1}{x^2 - 1} = \frac{(x^v + \cdots + x + 1) \cdot (x^{v+1} + 1)}{x + 1},$$

- If $v \geq 2$ and if $v$ is odd, then

$$S(x) = \frac{x^v + \cdots + x + 1}{x + 1} \cdot (x^{v+1} + 1) = (1 + (x^2)^1 + \cdots + (x^2)^{\frac{v-1}{2}}) \cdot (x^{v+1} + 1),$$

which is reducible.

- If $v \geq 2$ and if $v$ is even, then

$$S(x) = \frac{x^{v+1} + 1}{x + 1} \cdot (x^v + \cdots + x + 1) = (x^v - x^{v-1} + \cdots - x + 1) \cdot (x^v + \cdots + x + 1),$$

which is also reducible. $\square$

Now, we are ready to prove Theorem 1.2. According to Corollaries 3.3 and 3.4, since $Q(\alpha) \in \{-1, 1\}$ for any $\alpha \in \mathbb{F}_3$, it remains to consider the following cases:

(●) $m = 0$, $\# \Lambda \cap \Sigma_1 \in \{0, 1\}$,

(●●) $M = m = 1$, $b = 2$, $\Lambda = \{1, 2, 3\}$, $\Sigma_1 = \{1\}$,

(●●●) $M = m = 1$, $b = 2$, $\Lambda = \{1, 2\} = \Sigma_1$.

We shall see that only Case (●) may happen and $A$ must be even. We retrieve (Section 4.2.1, Case $n_2 \geq 1$, $n_3 = 0$), then the three polynomials described in Theorem 1.2.
4.1. Case $A$ odd

In this section, we may write

$$A = P_1^{a_1}P_2^{a_2}P_3^{a_3} \cdot Q^b$$

with $a_2 = N_1 \cdot 3^n - 1$, $b = M \cdot 3^m - 1$, $\deg(Q) > \deg(P_i) \geq 2$.

**Lemma 4.3.** If $A = P_1^{a_1}P_2^{a_2}P_3^{a_3} \cdot Q^b \in \mathbb{F}_3[x]$ is odd and perfect, then there exists at most one $i \in \{1, 2, 3\}$ such that $n_i = 1$ (i.e. $\# \Lambda \in \{2, 3\}$).

**Proof.** Suppose to the contrary that there exist two distinct integers $j_1, j_2 \in \{1, 2, 3\}$ such that $n_{j_1}, n_{j_2} \geq 1$. Put (without loss of generality) $j_1 = 1$ and $j_2 = 2$. We see that $P_1 - 1$ and $P_2 - 1$ divide $\sigma(A) = A$. Thus

$$P_1 - 1, P_2 - 1 \in \{P_1, P_2, P_3\}.$$ 

- If $P_1 - 1 = P_2$, then $P_2 - 1 = P_3$, so $P_1, P_1 - 1$ and $P_1 - 2 = P_3$ are both irreducible, which contradicts Lemma 2.5.
- If $P_1 - 1 = P_3$, then $P_2 - 1 = P_3$, so $P_1, P_1 - 1$ and $P_1 - 2 = P_2$ are both irreducible, which is also impossible. □

4.1.1. Case (●) $m = 0$, $\# \Lambda \cap \Sigma_1 \leq 1$.

- If $\Lambda \cap \Sigma_1 = \emptyset$ since $\Sigma_1 \neq \emptyset$, from Lemma 4.3, we get $\# \Lambda = 2$. We may put $\# \Lambda = \{1, 2\}$. So $1, 2 \notin \Sigma_1$ and thus $Q \nmid \sigma(P_1^{a_1})$ and $Q \nmid \sigma(P_2^{a_2})$. Therefore, by Lemma 4.1, $a_1 = a_2 = 1$. Hence, $\sigma(P_1) = 1 + P_1 \in \{P_2, P_3\}$ and $\sigma(P_2) = 1 + P_2 \in \{P_1, P_3\}$, which contradicts Lemma 2.5.
- Now, we suppose that $\# \Lambda \cap \Sigma_1 = 1$. We may put $\Lambda \cap \Sigma_1 = \{1\}$ so that $n_1 = 0$ and $Q \nmid \sigma(P_1^{a_1})$, ($n_2 \geq 1$ or $Q \nmid \sigma(P_2^{a_2})$) and ($n_3 \geq 1$ or $Q \nmid \sigma(P_3^{a_3})$).

**Lemma 4.4.** We must have either $(n_2 \geq 1)$ or $(n_3 \geq 1)$.

**Proof.**

- First, if $n_2 \geq 1$ and $n_3 \geq 1$, then $\Lambda = \{1\}$, which contradicts Lemma 4.3.
- If $n_2 = 0 = n_3$, then $Q \nmid \sigma(P_2^{a_2})$ and $Q \nmid \sigma(P_3^{a_3})$. So, by Lemma 4.1, we must have $a_2 = a_3 = 1$.

Thus, $\sigma(P_2) = 1 + P_2 \in \{P_1, P_3\}$ and $\sigma(P_3) = 1 + P_3 \in \{P_1, P_2\}$, which contradicts Lemma 2.5 as above. □

According to Lemma 4.4, we may suppose that $n_3 \geq 1$, $n_2 = 0$ and $Q \nmid \sigma(P_3^{a_3})$.

Thus, $a_2 = 1$ by Lemma 4.1. Therefore, $P_3 - 1$ and $\sigma(P_2)$ divides $\sigma(A) = A$, $\sigma(P_2) = 1 + P_2 \in \{P_1, P_3\}$ and $P_3 - 1 \in \{P_1, P_2\}$.

If $1 + P_2 = P_3$, then $P_3 - 1 = P_2$ and $1 = a_2 \geq 3^{n_3} - 1$. It is impossible. If $1 + P_2 = P_1$, then $P_3 - 1 = P_1$. Again, this contradicts Lemma 2.5.

4.1.2. Case (●●) $M = m = 1$, $b = 2$, $A = \{1, 2, 3\}$, $\Sigma_1 = \{1, 2\}$.

By Lemma 4.1, $a_3 = 1$. So, $\sigma(P_3) = 1 + P_3 \in \{P_1, P_2\}$.

We may suppose that $1 + P_3 = P_1$ so $P_3(\xi) = 1 = -P_1(\xi)$ for any $\xi \in \mathbb{F}_3$.

Since $Q \nmid \sigma(P_i^{a_i})$ for $i \in \{1, 2\}$ and since $\sigma(A) = A$, we get

$$\sigma(P_1^{a_1}) = P_2^{a_2}P_3^{a_3}Q, \quad \sigma(P_2^{a_2}) = P_1^{a_1}P_3^{a_3}Q,$$

$$\sigma(P_3^{a_3}) = \sigma(P_3) = P_1, \quad \sigma(Q^2) = \sigma(Q^2) = (Q - 1)^2 = (P_1^{a_1}P_2^{a_2}P_3^{a_3})^2,$$
where
\[ \beta_1 + 1 + 2w_1 = a_1, \quad \alpha_2 + 2w_2 = a_2, \]
\[ \alpha_3 + \beta_3 + 2w_3 = a_3 = 1, \quad \alpha_2, \alpha_3, \beta_1, \beta_3 \in \{0, 1\}, \]
\[ a_1 - (\alpha_2 + \alpha_3) = \frac{\deg(Q)}{\deg(P)} = a_2 - (\beta_1 + \beta_3) = w_1 + w_2 + w_3. \]

It follows that \( w_3 = 0 \) and \( (\alpha_3, \beta_3) \in \{(1, 0), (0, 1)\} \).

Moreover,
- since \((\sigma(P_3^\omega))(\xi) \neq 0 \) and \( P_1(\xi) = -1 \), \( a_1 \) must be even and \((\sigma(P_3^\omega))(\xi) = 1 \),
- since \( Q - 1 = P_1^a P_2^b \), we must have \( Q(\xi) = -1 \) for any \( \xi \in \mathbb{F}_3 \).

Since \( \beta_1 + 1 + 2w_1 = a_1 \) is even, we get \( \beta_1 = 1 \) and \( a_1 = 2 + 2w_1 \).

* If \( \alpha_3 = 1, \beta_3 = 0 \), then \( a_2 = 1 + \frac{\deg(Q)}{\deg(P)} = 1 + w_1 + w_2 \).

Since \( 1 = (\sigma(P_3^\omega))(\xi) = (P_2(\xi))^{w_2} \cdot (-1) = -(P_2(\xi))^{w_2} \), we must have \( \alpha_2 = 1 \), \( P_2(\xi) = -1 \) and \( a_2 = 1 + 2w_2 \) is odd. In this case, \((\sigma(P_2^{a_2}))(\xi) = 0 \) for any \( \xi \). It is impossible, because \( A \) is odd.

* If \( \alpha_3 = 0, \beta_3 = 1 \), then \( a_2 = 1 + 1 + \frac{\deg(Q)}{\deg(P)} = 2 + w_1 + w_2 \).

As above, since \( 1 = (\sigma(P_3^\omega))(\xi) = (P_2(\xi))^{w_2} \cdot (-1) = -(P_2(\xi))^{w_2} \), we must have \( \alpha_2 = 1 \), \( P_2(\xi) = -1 \) and \( a_2 = 1 + 2w_2 \) is odd. In this case, \((\sigma(P_2^{a_2}))(\xi) = 0 \) for any \( \xi \). It is impossible, because \( A \) is odd.

4.1.3. Case (●●●) \( M = m = 1, b = 2, \Lambda = \{1, 2\} = \Sigma_1 \).

In this case, \( P_3 - 1 \) divides \( \sigma(A) = A \), so \( P_3 - 1 \in \{P_1, P_2\} \).

We may suppose that \( P_3 - 1 = P_1 \). We get
\[ \sigma(P_1^\omega) = P_2^\alpha P_3^\omega Q, \quad \sigma(P_2^\omega) = P_1^\beta P_3^\beta Q, \]
\[ \sigma(P_3^\omega) = P_1^{3\alpha - 1} P_2^{\gamma_2 \gamma_3}, \quad \sigma(Q^b) = \sigma(Q^2) = (Q - 1)^2 = (P_1^{w_1} P_2^{w_2} P_3^{w_3})^2 \]
where
\[ \beta_1 + 3^{w_1} - 1 + 2w_1 = a_1, \quad \alpha_2 + \gamma_2 \cdot 3^{w_2} + 2w_2 = a_2, \]
\[ \alpha_3 + \beta_3 + 2w_3 = a_3, \quad \alpha_2, \alpha_3, \beta_1, \beta_3, \gamma_2 \in \{0, 1\}, \]
\[ a_1 - (\alpha_2 + \alpha_3) = \frac{\deg(Q)}{\deg(P)} = a_2 - (\beta_1 + \beta_3) = w_1 + w_2 + w_3, \]
\[ N_3 \cdot 3^{w_3} - 1 = a_3 = 3^{w_3} - 1 + \gamma_2 \cdot 3^{w_2}, \text{so } N_3 = \gamma_2 + 1 \in \{1, 2\}. \]

Remark that for any \( \xi \in \mathbb{F}_3 \), \( P_3(\xi) = -1 = -P_1(\xi) \) since \( P_3 - 1 = P_1 \).

Since \((\sigma(P_3^\omega))(\xi) \neq 0 \) and \( P_3(\xi) = -1 \), \( a_3 \) must be even and \((\sigma(P_3^\omega))(\xi) = 1 \).

Since \( Q - 1 = P_1^{w_1} P_2^{w_2} P_3^{w_3} \), we must have \( Q(\xi) = -1 \) for any \( \xi \in \mathbb{F}_3 \). It follows that \( N_3 = 1, \gamma_2 = 0 \) and \( \alpha_3 + \beta_3 = a_3 - 2w_3 = 3^{w_3} - 1 - 2w_3 \in \{0, 2\} \). Hence, either \((\alpha_3 = \beta_3 = 0) \) or \((\alpha_3 = \beta_3 = 1) \).

Case \( \alpha_3 = \beta_3 = 0 \)
One has the following.

Lemma 4.5. For any \( \xi \in \mathbb{F}_3 \), \( P_2(\xi) = 1 \).
Proof. If $P_2(\xi) = -1$ for some $\xi \in \mathbb{F}_3$, then $(\sigma(P_2^{a_2}))(\xi) = 1$, which contradicts the fact

$$(\sigma(P_2^{a_2}))(\xi) = (P_1^\beta, Q)(\xi) = 1^\beta \cdot (-1) = -1. \quad \square$$

Lemma 4.6. Let $P \in \mathbb{F}_3[x]$ be irreducible and $a \in \mathbb{N}^*$, then $P + 1$ divides $\sigma(P^a)$ if and only if $a$ is odd.

Proof. If $a$ is odd, then we may write $a = 2s + 1$ and

$$\sigma(P^a) = 1 + P + \cdots + P^{2s} + P^{2s+1} = (1 + P)(1 + (P^2)^{1} + \cdots + (P^2)^{s}).$$

If $a$ is even, then $a - 1$ is odd and $P + 1$ divides $\sigma(P^{a-1})$. Hence $\sigma(P^a) = (P^{a-1}) + P^a$ is not divisible by $P + 1$. \quad \square

Corollary 4.7. The integers $a_1$ and $a_2$ must be even, so that $\beta_1 = \alpha_2 = 0$ and $a_1 = a_2$.

Proof. If $a_1$ is odd, then by Lemma 4.6, $P_1 + 1$ divides $\sigma(P_1^{a_1})$, so $\alpha_2 = 1$ and $P_2 = P_1 + 1 = P_3$, which is impossible. Thus, $a_1 = \beta_1 + 2w_3 + 2w_1$ is even and $\beta_1 = 0$. If $a_2$ is odd, then as above, $P_2 + 1$ divides $\sigma(P_2^{a_2})$, so $\beta_1 = 1$ and $P_1 = P_2 + 1$. Hence $P_1, P_1 - 1 = P_2, P_1 - 2 = P_3$ are both irreducible. It contradicts Lemma 2.5. So, $a_2 = \alpha_2 + 2w_2$ is even and $a_2 = 0$.

From Corollary 4.7, $\beta_1 = \alpha_2$, so $\sigma(P_1^{a_1}) = Q = \sigma(P_2^{a_2})$. Hence

$$P_1^{w_1}P_2^{w_2}P_3^{w_3} = Q - 1 = P_1(1 + P_1 + \cdots + P_1^{a_1 - 1}) = P_2(1 + P_2 + \cdots + P_2^{a_2 - 1}).$$

Thus, $w_1 = w_2 = 1$ and

$$2 = 2w_2 = a_2 = a_1 = 3^{a_3} - 1 + 2w_1 = 3^{a_3} + 1,$$

which is impossible, because $n_3 \geq 1$.

Case $a_3 = \beta_3 = 1$

We get

$$\begin{align*}
\sigma(P_1^{a_1}) &= P_2^{a_2}P_2Q, \\
\sigma(P_2^{a_2}) &= P_1^{\beta_1}P_3Q, \\
\sigma(P_3^{a_3}) &= P_1^{3^{a_3} - 1}, \\
\sigma(Q^b) &= \sigma(Q^2) = (Q - 1)^2 = (P_1^{w_1}P_2^{w_2}P_3^{w_3})^2
\end{align*}$$

where

\begin{align*}
&\beta_1 + 3^{a_3} - 1 + 2w_1 = a_1, &\alpha_2 + 2w_2 = a_2, \\
&2 + 2w_3 = a_3 = 3^{a_3} - 1, &\alpha_2, \beta_1 \in \{0, 1\}, \\
&a_1 - (a_2 + 1) = \frac{\deg(Q)}{\deg(P)} = a_2 - (\beta_1 + 1) = w_1 + w_2 + w_3.
\end{align*}

Lemma 4.8. The integer $a_1$ is odd and $a_2$ is even, so that $\beta_1 = 1$, $\alpha_2 = 0$ and $a_2 = a_1 + 1$.

Proof. The integer $a_1$ is odd by Lemma 4.6 since $P_3 = P_1 + 1$ divides $\sigma(P_1^{a_1})$. Again, if $a_2$ is odd, then $P_2 + 1$ divides $\sigma(P_2^{a_2})$. So, $P_2 + 1 = P_1$. Thus, $P_1, P_1 - 1 = P_2$ and $P_1 - 2 = P_3$ are both irreducible. This contradicts Lemma 2.5. \quad \square
Corollary 4.9.

i) For any \( \xi \in \mathbb{F}_3 \), \( P_2(\xi) = -1 \).

ii) \( w_2 + w_3, w_1 + w_2 + w_3 = \frac{\deg(Q)}{\deg(P)} \) are both even.

iii) \( a_1 = 6l + 3, a_2 = 2w_2 = a_1 + 1 = 6l + 4 \) for some \( l \in \mathbb{N} \).

Proof.

i) If \( P_2(\xi) = 1 \), then modulo 3 we get
\[
a_2 + 1 = (\sigma(P_2^{a_2}))(\xi) = (P_1 P_2 Q)(\xi) = (P_1 \cdot \sigma(P_1^{a_1}))(\xi) = 1 \cdot (a_1 + 1).
\]
Hence by Lemma 4.8, we get modulo 3
\[
a_1 = a_2 = a_1 + 1.
\]
It is impossible.

ii) We get modulo 3
\[
1 = (Q - 1)(\xi) = (P_1 w_1 P_2 w_2 P_3 w_3)(\xi) = 1 \cdot (-1)^{w_2 + w_3}.
\]
We are done.

iii) Since \( P_2(\xi) = -1 \) and \( a_2 \) is even, we get \( (\sigma(P_2^{a_2}))(\xi) = 1 \). But modulo 3
\[
(\sigma(P_2^{a_2}))(\xi) = (P_1 \cdot \sigma(P_1^{a_1}))(\xi) = 1 \cdot (a_1 + 1).
\]
We see that \( a_1 \equiv 0 \mod 3 \) and \( a_1 \equiv 3 \mod 6 \) since \( a_1 \) is odd. \( \square \)

Now, in order to end the proof for the odd case, we see that
\[
(1 + P_1)(1 + (P_2^1)^1 + \cdots + (P_2^2)^{3l+1}) = \sigma(P_1^{a_1}) = P_3 \cdot Q = (P_1 + 1) \cdot Q.
\]
So,
\[
Q = 1 + (P_2^1)^1 + \cdots + (P_2^2)^{3l+1}
\]
and \( l \) must be equal to 0 by Lemma 4.2. Hence
\[
P_1^{w_1} P_2^{w_2} P_3^{w_3} = Q - 1 = P_1^2.
\]
Thus, \( w_1 = 2 \) and \( a_1 = 1 + 3^{n_3} - 1 + 2w_1 = 3^{n_3} + 4 \). It is impossible, because \( a_1 \equiv 0 \mod 3 \).

4.2. Case \( A \) even

In this section, we put
\[
A = P_1^{a_1} P_2^{a_2} P_3^{a_3} \cdot Q^b
\]
with \( P_1 := x + 1, \ P_2 := x + 2, \ P_3 := x + 3 = x, \ a_i = N_i \cdot 3^{n_i} - 1, \ b = M \cdot 3^m - 1, \ 3 \nmid N_i, \ 3 \nmid M. \)

For \( S \in \mathbb{F}_3[x] \), we denote by \( \overline{S} \) (resp. \( \overline{\overline{S}} \)) the polynomial obtained from \( S \) by substituting \( x \) by \( x + 1 \) (resp., by \( x + 2 \)).

We need the following facts that are more precise than Lemma 4.6.

Lemma 4.10. Let \( a \in \mathbb{N}^* \) and \( P \in \{ P_1, P_2, P_3 \} \). Then

i) \( \overline{P} \) divides \( \sigma(P^{a}) \) if and only if \( a \) is odd,

ii) \( \overline{P} \) divides \( \sigma(P^{a}) \) if and only if \( 3 \) divides \( a + 1 \).
Proof. We may suppose that $P = P_1$.
i) follows from the facts

$$P_3(1) = 0, \quad P_1(1) = 2 = -1,$$

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

ii) follows from the facts

$$P_3(0) = 0, \quad P_1(0) = 1, \quad (\sigma(P_1^{a_1}))(0) = a_1 + 1. \qed$$

Lemma 4.11.

i) If $a_1$ is odd, $n_1 = 0$ and $\sigma(P_1^{a_1}) = P_2^{n_2}P_3^{n_3}Q$, then

$$a_1 = 3, \quad a_2 = 1, \quad a_3 = 0 \quad \text{and} \quad Q = 1 + P_1^2 = 1 + (x + 1)^2.$$ 

ii) If $a_1$ is odd, $n_1 \geq 1$ and $\sigma(P_1^{a_1}) = P_2^{n_2}P_3^{n_3}Q^\alpha$, then

either $(N_1 = 2, \quad a_2 = 3^{n_1} = a_3 + 1, \quad \alpha = 0)$

or $(N_1 = 4, \quad a_2 = 3^{n_1} = a_3 + 1, \quad \alpha = 3^{n_1}, \quad Q = 1 + P_1^2 = 1 + (x + 1)^2$.

Proof.
i) if $a_1$ is odd then $P_2 = 1 + P_1$ divides $\sigma(P_1^{a_1})$ and $a_2 = 1$ since $a_2 \not\in \{0, 1\}$. 

If $a_3 \neq 0$, then $a_3 = 1$ and $P_3$ divides $\sigma(P_1^{a_1})$. Thus, we get in $\mathbb{F}_3$

$$N_1 = a_1 + 1 = (\sigma(P_1^{a_1}))(0) = (P_2P_3Q)(0) = 0,$$

which is impossible since $3 \nmid N_1$. Therefore, $a_3 = 0$ and

$$(1 + P_1)(1 + (P_1^2)^1 + \cdots + (P_1^2)^{\frac{a_1-1}{2}}) = \sigma(P_1^{a_1}) = P_2 \cdot Q.$$ 

Hence $1 + (P_1^2)^1 + \cdots + (P_1^2)^{\frac{a_1-1}{2}} = Q$ is irreducible.

So, we must have $a_1 = 3$ by Lemma 4.2.

ii) Since $a_1$ is odd, we may put $a_1 = (2c_1) \cdot 3^{n_1} - 1$ where $c_1 \in \mathbb{N}^*$.

Hence

$$\sigma(P_1^{a_1}) = P_1^{3^{n_1}-1} \cdot (1 + P_1 + \cdots + P_1^{c_1-1})^{3^{n_1}} \cdot (P_1^{c_1} + 1)^{3^{n_1}}.$$ 

If $c_1 = 1$, then $N_1 = 2$ and $\alpha = 0$.

If $c_1 = 2$, then $N_1 = 4, Q = 1 + P_1^2, a_2 = 1$ and $\alpha = 3^{n_1}$.

If $c_1 \geq 3$, then $P_1^{c_1} + 1$ is reducible over $\mathbb{F}_3$ and thus $3 \geq \omega(\sigma(P_1^{a_1})) \geq 4$. It is impossible. \qed

Lemma 4.12.

i) If $a_1$ is even, $n_1 = 0$ and $\sigma(P_1^{a_1}) = P_2^{n_2}P_3^{n_3}Q$, then

$a_1 + 1$ is a prime number, $a_2 = a_3 = 0$ and $Q = \sigma(P_1^{a_1})$.

ii) If $a_1$ is even, $n_1 \geq 1$ and $\sigma(P_1^{a_1}) = P_2^{n_2}P_3^{n_3}Q^\alpha$, then

either $(N_1 = 1, \quad a_2 = 0, \quad a_3 = 3^{n_1} - 1, \quad \alpha = 0)$
or \( N_1 \) is an odd prime number, \( \alpha_2 = 0, \ \alpha_3 = 3^{n_1} - 1, \ \alpha = 3^{n_1}, \)

\[ Q = \sigma(P_1^{N_1-1}). \]

Proof.
i) \( a_1 \) even implies \( \alpha_2 = 0 \). As above, \( \alpha_3 \neq 0 \) implies \( 3 \mid a_1 + 1 = N_1 \), which is impossible. So, \( Q = \sigma(P_1^a) \) is irreducible and \( a_1 + 1 \) must be an odd prime number.

ii) \( a_1 \) even implies \( N_1 \) odd and \( \alpha_2 = 0 \), and \( n_1 \geq 1 \) implies \( 3^{n_1} - 1 \).

If \( N_1 = 1 \), then \( \alpha = 0 \).

If \( N_1 \geq 3 \), then

\[ P_3^{3^{n_1}-1} \cdot (1 + P_1 + \cdots + P_1^{N_1-1})^{3^{n_1}} = \sigma(P_1^a) = P_3^{3^{n_1}-1} \cdot Q^{3^{n_1}}. \]

Thus \( Q = \sigma(P_1^{N_1-1}) \) is irreducible and \( N_1 \) must be an odd prime number. \( \square \)

Lemma 4.13. Let \( p \) be an odd prime number. If \( \sigma(x^a) \) is irreducible over \( \mathbb{F}_p \) and if \( \sigma(x^a) = \sigma((x + \mu)^a) \) for some \( \mu \in \mathbb{F}_p \), then \( \mu = 0 \).

Proof. Let \( \xi \) be a primitive \((a + 1)\)-root of unity. By hypothesis,

\[ S(x) := \sigma(x^a) = \prod_{i=1}^{a} (x - \xi^i) \]

is the minimal polynomial of \( \xi \).

If \( S(x) = S(x + \mu) \) with \( \mu \neq 0 \), then \( x - \xi = x + \mu - \xi^k \) for some \( 2 \leq k \leq a \).

Thus, the polynomial \( R(x) := x^k - x - \mu \in \mathbb{F}_p[x] \) satisfies

\[ R(\xi) = 0. \]

Hence, \( S \) divides \( R \) and \( S = R \), which is impossible since \( p \neq 2 \). \( \square \)

Corollary 4.14. If \( A = P_1^{a_1} P_2^{a_2} P_3^{a_3} Q^b \in \mathbb{F}_3[x] \) is even and perfect, then there exists a unique \( j \in \{1, 2, 3\} \) such that \( Q \mid \sigma(P_j^a) \), so \( \#\Sigma_1 = 1 \).

Proof. We know that \( \Sigma_1 \neq \emptyset \). If \( \#\Sigma_1 \geq 2 \), then we may suppose that \( 1, 2 \in \Sigma_1 \).

According to Lemmata 4.11 and 4.12, we get

\[ Q \notin \{1+P_1^2, \sigma(P_1^{a_1}), \sigma(P_1^{N_1-1})\} \cap \{1+P_2^2, \sigma(P_2^{a_2}), \sigma(P_2^{N_2-1})\} \]

by Lemma 4.13. \( \square \)

According to Corollary 4.14, it remains to consider only the case (●)

\[ m = 0, \quad \#\Lambda \cap \Sigma_1 \in \{0, 1\}. \]

4.2.1. Case \( m = 0, \ \#\Lambda \cap \Sigma_1 = 1 \).

We may put \( \Lambda \cap \Sigma_1 = \{1\} \), so \( n_1 = 0 \), \( Q \mid \sigma(P_1^{a_1}) \), \( Q \nmid \sigma(P_2^{a_2}) \), \( Q \nmid \sigma(P_3^{a_3}) \)

and thus \( b = 1 \).
Case $n_2 = 0 = n_3$

One has $a_2 = 1 = a_3$ by Lemma 4.1. Thus, we get

\[ \sigma(P_1^{a_1}) = P_2^{a_2} P_3^{a_3}, \quad \sigma(P_2^{a_2}) = 1 + P_2 = P_3, \]
\[ \sigma(P_3^{a_3}) = 1 + P_3 = P_1, \quad \sigma(Q^b) = 1 + Q = P_1^{w_1} P_2^{w_2} P_3^{w_3} \]

where

\[ 1 + w_1 = a_1 = \alpha_2 + \deg(Q), \quad \alpha_2 + w_2 = a_2 = 1, \quad \alpha_2 \in \{0, 1\}. \]

- If $a_1$ is odd, then $\alpha_2 = 1$ and $w_2 = 0$. So, $Q = P_1^{w_1} - 1$ is odd and irreducible. It is impossible.
- If $a_1$ is even, then $\alpha_2 = 0$ and $1 + P_1 + \cdots + P_1^{a_1} = \sigma(P_1^{a_1}) = Q$. Thus, $P_1$ does not divide $2 + P_1 + \cdots + P_1^{a_1} = 1 + Q = \sigma(Q)$. Hence $w_1 = 0$ and $a_1 = 1$, which is impossible.

Case $n_2 \geq 1$, $n_3 \geq 1$

We get

\[ \sigma(P_1^{a_1}) = P_2^{a_2} P_3^{a_3} Q, \quad \sigma(P_2^{a_2}) = P_1^{3^{a_2} - 1} P_3^{\beta_2 - 3^{a_2}}, \]
\[ \sigma(P_3^{a_3}) = P_2^{3^{a_3} - 1} P_1^{\gamma_1 - 3^{a_3}}, \quad \sigma(Q^b) = 1 + Q = P_1^{w_1} P_2^{w_2} P_3^{w_3} \]

where

\[ 3^{a_2} - 1 + \gamma_1 \cdot 3^{a_3} + w_1 = a_1 = \alpha_2 + \alpha_3 + \deg(Q), \quad \alpha_2, \alpha_3, \beta_2, \gamma_1 \in \{0, 1\}. \]

- If $a_1$ is odd, then by Lemma 4.11, $a_1 = 3$, $\alpha_2 = 1$, $\alpha_3 = 0$ and $Q = 1 + (x + 1)^2$. Hence $\sigma(Q^b) = 1 + Q = x^2 + 2x = P_2 P_3$, $w_1 = 0$, $w_2 = w_3 = 1$ and $a_1 = 3^{a_2} - 1 + \gamma_1 \cdot 3^{a_3}$. It is impossible since $3 \nmid (a_1 + 1)$.
- If $a_1$ is even, then $\sigma(P_1^{a_1}) = Q$ and $a_1 + 1$ is an odd prime number. Therefore, $P_1$ does not divide $2 + P_1 + \cdots + P_1^{a_1} = \sigma(Q)$, $w_1 = 0$ and $a_1 = 3^{a_2} - 1 + \gamma_1 \cdot 3^{a_3}$, which is impossible.

Case $n_2 = 0$, $n_3 \geq 1$

In this case, $a_2 = 1$ by Lemma 4.1. We get

\[ \sigma(P_3^{a_3}) = P_2^{3^{a_3} - 1} P_1^{\gamma_1 - 3^{a_3}} \]

and the contradiction $1 = a_2 \geq 3^{a_3} - 1 \geq 2$.

Case $n_2 \geq 1$, $n_3 = 0$

In this case, $a_3 = 1$ by Lemma 4.1.

\* If $a_1$ is odd, then by Lemma 4.11, $a_1 = 3$ and $\sigma(P_1^{a_1}) = P_2 \cdot (1 + P_1^2) = P_2 \cdot Q$. Since $Q$ does not divide $\sigma(P_2^{a_2})$, one has

\[ \sigma(Q) = 1 + Q = P_2 \cdot P_3 \quad \text{and} \quad a_2 = 2 = 3^1 - 1. \]

We get the three even perfect polynomials of Theorem 1.2

\[ A = x(x + 1)^3(x + 2)^2(1 + (x + 1)^2), \quad \overline{A} \quad \text{and} \quad \overline{\overline{A}}. \]

\* If $a_1$ is even, then $\sigma(P_1^{a_1}) = Q$ and $a_1 + 1$ is an odd prime number. We get

\[ \sigma(P_1^{a_1}) = Q, \quad \sigma(P_2^{a_2}) = P_1^{3^{a_2} - 1} P_3^{\beta_3 - 3^{a_2}}, \]
\[ \sigma(P_3^{a_3}) = 1 + P_3 = P_1, \quad \sigma(Q^b) = 1 + Q = P_1^{w_1} P_2^{w_2} P_3^{w_3}, \]
PERFECT POLYNOMIALS OVER $\mathbb{F}_p$ WITH $p + 1$ IRREDUCIBLE DIVISORS

$\beta_3 = 0$ since $n_2 \geq 1$ and $1 = a_3 \geq \beta_3 \cdot 3^{n_2}$. So, $a_2$ is even. Hence, $w_3 = a_3 = 1$, $a_2 = w_2 = 3^{n_2} - 1$ and $w_1 = 0$. Thus,

$$2 + P_1 + \cdots + P_1^{a_1} = \sigma(Q) = P_2^{a_2}P_3.$$

So, $a_1 = a_2 + 1$. It is impossible, because $a_1$ and $a_2$ are both even.

**4.2.2. Case $m = 0$, $\Lambda \cap \Sigma_1 = \emptyset$.**

We need the following general result.

**Lemma 4.15.** For any $T \in \mathbb{F}_3[x]$, one has

$$\gcd(1 + T, 1 + (T^2)^1 + \cdots + (T^2)^{\frac{3^{n_1} - 1}{2}}) = 1.$$

**Proof.** If $S$ is a common irreducible divisor of $1 + T$ and of $1 + (T^2)^1 + \cdots + (T^2)^{\frac{3^{n_1} - 1}{2}}$, then

$$T \equiv -1 \mod S \quad \text{and} \quad T^2 \equiv 1 \mod S.$$

Thus

$$\frac{3^{n_1} + 1}{2} \equiv 1 + (T^2)^1 + \cdots + (T^2)^{\frac{3^{n_1} - 1}{2}} \equiv 0 \mod S.$$

It is impossible since $3$ does not divide $3^{n_1} + 1$. \hfill $\square$

Since $\Sigma_1 \neq \emptyset$, one has $\#\Lambda \leq 2$. By Corollary 4.14, we may consider only two cases:

(I) $\Sigma_1 = \{1\}$ and $\Lambda = \{2, 3\}$,

(II) $\Sigma_1 = \{1\}$ and $\Lambda = \emptyset$.

**Case (I)**

Since $Q \nmid \sigma(P_2^{a_2})$ and $Q \nmid \sigma(P_3^{a_3})$, from Lemma 4.1, we get $a_2 = a_3 = 1$. Moreover, $n_1 \geq 1$, so $P_3^{3^{n_1} - 1}$ divides $\sigma(P_1^{a_1})$. Hence $1 = a_3 \geq 3^{n_1} - 1 \geq 2$, which is impossible.

**Case (II)**

$n_1 \geq 1$, $n_2 \geq 1$ and $n_3 \geq 1$. From Corollary 4.14, We get

$$\sigma(P_1^{a_1}) = P_3^{3^{n_1} - 1}(P_2^{a_2}Q)^{3^{n_1}} \quad \text{and} \quad \sigma(P_2^{a_2}) = P_3^{3^{n_2} - 1}P_3^{3^{n_2}} \quad \sigma(P_3^{a_3}) = P_2^{3^{n_3} - 1}P_1^{3^{n_3}} \quad \sigma(Q^b) = P_1^{w_1}P_2^{w_2}P_3^{w_3},$$

so $b = 3^{n_1}$.

* If $a_1$ is odd, then by Lemma 4.11, $a_2 = 1$, $a_3 = 4 \cdot 3^{n_1} - 1$ and

$$\sigma(P_1^{a_1}) = P_3^{3^{n_1} - 1}(P_2 \cdot Q)^{3^{n_1}}, \quad \text{where} \quad Q = 1 + P_1^2.$$

So, $1 + Q = P_2P_3$ and $P_2P_3 \cdot (1 + (Q^2)^1 + \cdots + (Q^2)^{\frac{3^{n_1} - 1}{2}}) = \sigma(Q^b) = P_1^{w_1}P_2^{w_2}P_3^{w_3}$. Thus, by Lemma 4.15, $w_2 = w_3 = 1$ and

$$1 + (Q^2)^1 + \cdots + (Q^2)^{\frac{3^{n_1} - 1}{2}} = P_1^{w_1}.$$

Thus

$$w_1 = \deg(P_1^{w_1}) = (3^{n_1} - 1) \deg(Q) \geq 4.$$
We get
\[ Q \equiv 1 \mod P \quad \text{and} \quad \frac{3^{n_1} + 1}{2} \equiv 1 + (Q^2)^1 + \cdots (Q^2)^{\frac{n_1-1}{2}} \equiv 0 \mod P. \]
It is impossible since 3 does not divide \( 3^{n_1} + 1 \).

* If \( \alpha_1 \) is even, then by Lemma 4.12, \( \alpha_2 = 0 \) and \( Q = 1 + P_1 + \cdots + P_1^{N_1-1} \), where \( N_1 \) is an odd prime number. Hence,
\[ (1 + Q) \cdot (1 + (Q^2)^1 + \cdots (Q^2)^{\frac{n_1-1}{2}}) = \sigma(Q^k) = P_1^k P_2^{w_2} P_3^{w_3}. \]
Since \( P_1 \) does not divide \( 2 + P_1 + \cdots + P_1^{N_1-1} = 1 + Q \), we have
\[ 1 + (Q^2)^1 + \cdots (Q^2)^{\frac{n_1-1}{2}} \equiv 0 \mod P_1. \]
But \( Q \equiv 1 \mod P_1 \), so we get
\[ \frac{3^{n_1} + 1}{2} \equiv 1 + (Q^2)^1 + \cdots (Q^2)^{\frac{n_1-1}{2}} \equiv 0 \mod P_1. \]
It is impossible as above.

**References**


L. H. Gallardo, Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France, e-mail: luisgall@univ-brest.fr

O. Rahavandrainy, Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France, e-mail: rahavand@univ-brest.fr