MATHEMATICAL COMMUNICATIONS
Math. Commun., Vol. **14**, No. 1, pp. 47-65 (2009)


# All perfect polynomials with up to four prime factors over $F_4$

Luis H. Gallardo[1,*] and Olivier Rahavandrainy[1]

[1] *Department of Mathematics, University of Brest 6, Avenue Victor Le Gorgeu, C.S. 93 837, 29 238 Brest Cedex 3, France*

Received July 26, 2008; accepted February 18, 2009

**Abstract.** A perfect polynomial over the field $\mathbb{F}_4$ is a monic polynomial $A \in \mathbb{F}_4[x]$ that equals the sum of all its monic divisors. If $\gcd(A, x^4 + x) = 1$, then we say that $A$ is odd over $\mathbb{F}_4$. In this paper, we characterize odd perfect polynomials over $\mathbb{F}_4$, with four prime divisors. There follows a classification of all perfect polynomials over $\mathbb{F}_4$ with up to four prime divisors.
**AMS subject classifications**: 11T55, 11T06
**Key words**: sum of divisors, polynomials, finite fields, characteristic 2

## 1. Introduction

We denote, as usual, by $\mathbb{N}$ (resp. $\mathbb{N}^*$) the set of nonnegative (resp. positive) integers. We consider the finite field $\mathbb{F}_4$ of 4 elements, which is a quadratic extension of the binary field $\mathbb{F}_2 = \{0, 1\}$. We write $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$, for some $\alpha$ in a fixed algebraic closure of $\mathbb{F}_2$. One has: $\bar{\alpha} = \alpha^2 = \alpha + 1$.

For a polynomial $A \in \mathbb{F}_4[x]$, let

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

be the sum of all monic divisors of $A$. Let us also call $\omega(A)$ the number of distinct prime (irreducible) monic polynomials that divide $A$. Observe that $\sigma$ is multiplicative, a fact that will be used many times without more reference in the rest of the paper. A perfect polynomial $A$ is a monic polynomial such that $\sigma(A) = A$.

The notion of a perfect polynomial over $\mathbb{F}_2$ was introduced by Canaday [2], the first doctoral student of Leonard Carlitz. He studied mainly the case when $\gcd(A, x^2 + x) \neq 1$. We call these polynomials even over $\mathbb{F}_2$. He claims (see [8] for a complete proof ) that there are exactly 5 even perfect polynomials over $\mathbb{F}_2$, with four irreducible factors:

$$\begin{aligned}
&C_1(x) = x^2(x+1)(x^2+x+1)^2(x^4+x+1),\ C_2(x) = C_1(x+1),\\
&C_3(x) = x^4(x+1)^4(x^4+x^3+x^2+x+1)(x^4+x^3+1),\\
&C_4(x) = x^3(x+1)^6(x^3+x^2+1)(x^3+x+1),\ C_5(x) = C_4(x+1);
\end{aligned}$$

*Corresponding author. *Email addresses:* luisgall@univ-brest.fr (L. H. Gallardo), rahavand@univ-brest.fr (O. Rahavandrainy)

 

leaving the case of the odd ones open. In other words, Canaday's claim implies that:

$$\textit{There is no odd perfect polynomial over } \mathbb{F}_2. \qquad (\diamond)$$

In his own words [2, p. 721]: "It seems plausible that none of this exist but this is not proved." Some work has been done on this. The assertion $(\diamond)$ is true if $\omega(A) = 1$ (trivial), $\omega(A) = 2$ (see [2, Theorem 17]), and $\omega(A) \in \{3, 4\}$ (see [6], [7]).

The next interesting case is to consider the problem over the finite field $\mathbb{F}_4$, with four elements:

Now, working over $\mathbb{F}_4$, we may define an *even* (resp. *odd*) polynomial as a polynomial $A$ such that $\gcd(A, x^4 + x) \neq 1$ (resp. $\gcd(A, x^4 + x) = 1$). The analogue over $\mathbb{F}_4$ of the assertion $(\diamond)$ is false: there exist odd perfect polynomials $A$ over $\mathbb{F}_4$, with $\omega(A) = 2$ (see [4]). Gallardo and Rahavandrainy [4, 5], characterize the even perfect polynomials $A$ such that $\omega(A) \in \{2, 3, 4\}$. Furthermore, Gallardo and Rahavandrainy [5] prove that there is no odd perfect polynomial with 3 prime factors. Odd perfect polynomials that we have found, including our main result below, confirm [5, Conjecture 2].

Observe that from a result [10, p. 140] of Hall, there is an infinity of pairs $P, P+1$ of irreducible polynomials over $\mathbb{F}_4$ (since $4 = \mathrm{card}(\mathbb{F}_4) > 3$), so that we have an infinity of odd perfect polynomials $A \in \mathbb{F}_4[x]$ with $\omega(A) \in \{2, 4\}$.

The object of this paper is to characterize all odd perfect polynomials over $\mathbb{F}_4$ with $\omega(A) = 4$. Our main result is:

**Theorem 1.** *Let $A = P^a Q^b R^c S^d \in \mathbb{F}_4[x]$ be an odd polynomial, where $P, Q, R, S$ are distinct irreducible polynomials, and $a, b, c, d \in \mathbb{N}^*$. Then $A$ is perfect over $\mathbb{F}_4$ if and only if, up to rearranging $P, Q, R, S$:*
*either:*

$$(i) : \begin{cases} Q = P + 1,\ R = P^3 + P^2 + 1,\ S = P^3 + P + 1, \\ a = 3,\ b = 6,\ c = d = 1, \end{cases}$$

*or*

$$(ii) : \begin{cases} Q = P + 1,\ S = R + 1, \\ a = b = 2^n - 1,\ c = d = 2^m - 1,\ \textit{for some } m, n \in \mathbb{N}^*. \end{cases}$$

So that either $A$ is a product of two coprime perfect polynomials with two prime divisors each, or $A$ belongs to a family that, at first sight, might be eventually finite.

Indeed, we learned recently by Paul Pollack that this family is actually *infinite*. Observe that this disproves our conjecture [5, Conjecture 3]. For completeness we repeat here this conjecture:

**Conjecture 1.** *Let $k = 2m > 0$ be an even integer, and assume that there exists some integer $j \in \{1, \ldots, k\}$ for which the positive integer $h_j$ is even. Then there are finitely many perfect polynomials $A$ over $\mathbb{F}_4$ of the form*

$$A = \prod_{i=1}^{k} P_i^{h_i}.$$

We give here below essentially his proof of the infinity of the family.

In order to do that, observe that Serret [13] and Dickson [3] proved a general result (see [12, Lemma 1] for this, and see all the papers for related results) from which we get as a special case:

**Lemma 1.** *Let $P \in \mathbb{F}_4[x]$ be a prime polynomial of degree $d$. Let $l$ be an odd prime. Suppose that $P$ has a root $\alpha \in \mathbb{F}_{4^d}$ which is not an $l$-th power. Then the substitution $x \longrightarrow x^{l^k}$ leaves $P$ prime for every $k = 1, 2, 3, \ldots$.*

Precisely we prove.

**Lemma 2.** *There exists an infinity of prime polynomials $P \in \mathbb{F}_4[x]$ such that $P+1$, $P^3+P+1$, and $P^3+P^2+1$ are also all prime.*

**Proof**. Let $\alpha$ be a root of $x^2+x+1$ in $\mathbb{F}_4$, and let

$$P(x) = x^{2\cdot 5^k} + x^{5^k} + \alpha.$$

Then $P(x), P(x)+1, P(x)^3+P(x)+1$, and $P(x)^3+P(x)^2+1$ are all irreducible over $\mathbb{F}_4$, for each $k \geq 0$.

To see this, let $P_0(x) := x^2+x+\alpha$. With a computer algebra system, one can check that the hypothesis of the Serret-Dickson's Lemma 2 hold with $l = 5$, for each of the polynomials $f = P_0, P_0+1, P_0^3+P_0+1$, and $P_0^3+P_0^2+1$. So replacing $x$ by $x^{5^k}$ should preserve irreducibility of each of these. This proves the result. □

Moreover, see some examples of perfect polynomials at the end of the paper.

Thus, with [4, 5] and the present work, we have completely classified all perfect polynomials $A$ over $\mathbb{F}_4$ with $\omega(A) \leq 4$. According to the fact that a polynomial $A(x)$ is perfect over $\mathbb{F}_4$ if and only if for any $a \in \mathbb{F}_4$, $A(x+a)$ is perfect, any such perfect polynomial can be obtained from the following list:

(a) $0$, $1$ and $(x^2+x)^{2^n-1}(x^2+x+1)^{2^m-1}$ for some $n, m \in \mathbb{N}$.

(b) $(x^4+x)^{2^n-1}$, $(x^4+x)^{3\cdot 2^n-1}$, for some $n \in \mathbb{N}$.

(c) $(x^2+ax)^{3\cdot 2^n-1}(x^2+ax+a+1)^{2\cdot 2^n-1}$ , for $a \in \{\alpha, \bar{\alpha}\}$, and for some $n \in \mathbb{N}$.

(d) $(P^2+P)^{2^n-1}$, where $P \in \mathbb{F}_4[x]$, $P$ and $P+1$ are both prime, and $n \in \mathbb{N}$. Observe that (e.g.) when $P = x^2+x+\alpha$, we get a perfect polynomial over $\mathbb{F}_4$ without roots in $\mathbb{F}_4$. I.e., we have more non-trivial odd perfect polynomials over $\mathbb{F}_4$. For more on this see also [9].

(e) $x^3(x+1)^6(x^3+x^2+1)(x^3+x+1)$, called a "sporadic" even perfect polynomial. This polynomial is also even perfect over $\mathbb{F}_2$.

(f) $(x^2+x+b)^{2^n-1}(Q(Q+1))^{2^m-1}$ where $b \in \mathbb{F}_2$, $n, m \in \mathbb{N}$, $Q \in \mathbb{F}_4[x]$, $Q$ and $Q+1$ are both prime of degree $> 1$.

(g) $(P(P+1))^{2^n-1}(Q(Q+1))^{2^m-1}$ where $P, Q \in \mathbb{F}_4[x]$, $P, Q, P+1, Q+1$ are all prime of degree $> 1$, $n, m \in \mathbb{N}$.

(h) $P^3(P+1)^6(P^3+P^2+1)(P^3+P+1)$, where $P$, $P+1$, $P^3+P^2+1$ and $P^3+P+1$ are all irreducible over $\mathbb{F}_4$. Note that if $P = x$, then we obtain the sporadic polynomial in (e).

It is easy to see from direct computations that our conditions are sufficient. It remains to prove that they are also necessary.

## 2. Preliminary

### 2.1. Some facts

By using the multiplicativity of $\sigma$, we obviously obtain

**Lemma 3.** *Let $A = A_1A_2 \in \mathbb{F}_4[x]$ such that $\gcd(A_1, A_2) = 1$. If $A$ and $A_1$ are both perfect, then $A_2$ is also perfect.*

Canaday [2] proved the following two results over $\mathbb{F}_2$. The generalization below was observed first in [5, Lemma 2.1, Lemma 2.2].

**Lemma 4** (see [2], Lemma 5)**.** *Let $\mathbb{F}$ be a perfect field of characteristic 2. Let $P, Q \in \mathbb{F}[x]$ and $n, m \in \mathbb{N}$ such that $P$ is irreducible and $Q$ is nonconstant.*
*If $\sigma(P^{2n}) = 1 + \cdots + P^{2n} = Q^m$, then $m \in \{0, 1\}$.*

**Lemma 5** (see [2], Lemma 6)**.** *Let $\mathbb{F}$ be a perfect field of characteristic 2. Let $P, Q \in \mathbb{F}[x]$ and $n, m \in \mathbb{N}$ such that $P$ is irreducible, $m > 1$.*
*If $\sigma(P^{2n}) = 1 + \cdots + P^{2n} = Q^m C$ for some $C \in \mathbb{F}[x]$, then:*

$$\begin{cases} \deg(P) > (m-1)\deg(Q) & \text{if } m \text{ is odd,} \\ \deg(P) > m\deg(Q) & \text{if } m \text{ is even.} \end{cases}$$

We also need the lemmas:

**Lemma 6** (see [6], Lemma 2.3 or [5], Lemma 2.5)**.** *Let $A \in \mathbb{F}_4[x]$ be a perfect polynomial. Then the number of monic prime divisors of $A$, of minimal degree, is even.*

**Lemma 7.** *For any even integer $h \geq 2$, for any nonconstant polynomial $U \in \mathbb{F}_4[x]$, the polynomials $1 + U$ and $V = 1 + U + \cdots + U^h$ are coprime.*

**Proof**. It follows by Bezout's theorem, since:

$$1 = V.\ 1 + (1 + U)(U^{h-1} + U^{h-3} + \cdots + U).$$

□

**Lemma 8.** *If $P \in \mathbb{F}_4[x]$ is nonconstant and $h = 2^e u - 1 \in \mathbb{N}$ such that $e \geq 1$ and $u$ odd, then:*

$$\sigma(P^h) = 1 + P + \cdots + P^h = (1 + P)^{2^e - 1}(1 + P + \cdots + P^{u-1})^{2^e}.$$

*In particular, $1 + P$ divides $\sigma(P^h)$.*

**Proof**. It follows from the fact: $\sigma(P^h) = \dfrac{1 + P^{h+1}}{1 + P} = \dfrac{(1 + P^u)^{2^e}}{1 + P}$. □

**Lemma 9.** *Let $A = P^aQ^bR^cS^d$ be a perfect polynomial over $\mathbb{F}_4$, such that $P, Q, R, S$ are prime and $\deg(P) = \deg(Q) \leq \deg(R) \leq \deg(S)$.*
*If $a$ is odd, then $1 + P \in \{Q, R, S\}$.*

**Proof**. In this case, $1+P$ divides $\sigma(A)=A$, since it divides $\sigma(P^a)$, by Lemma 8. So, by minimality of $\deg(1+P)=\deg(P)$, we must have: $1+P\in\{Q,R,S\}$. □

**Lemma 10** (see [5], Lemma 2.4)**.** *For any integer $h\geq 2$, for any nonconstant polynomial $U\in\mathbb{F}_4[x]$, the polynomial $1+U+\cdots+U^h$ is reducible over $\mathbb{F}_4$.*

**Lemma 11** (see [5], Lemma 2.6)**.** *If $1+x+\cdots+x^h=UV$, with $h$ even, $U,V\in\mathbb{F}_4[x]$ irreducible, then $h+1$ is a prime number and $\deg(U)=\deg(V)$.*

**Lemma 12.** *Let $h,a,b,c\in\mathbb{N}$ and let $P$, $U$, $V$, $W$ be four prime polynomials over $\mathbb{F}_4$, such that:*

$$1+P+\cdots+P^{2h}=U^aV^bW^c,\ a\deg(U)\leq b\deg(V)\leq c\deg(W).$$

*Then; $2h+1$ is prime, $\gcd(a,b,c)=1$ and*

$$a\deg(U)+b\deg(V)=c\deg(W)\ =\ h\deg(P).$$

**Proof**. For any positive integer $n$, put: $f_n(x)=\sigma(x^{n-1})=1+x+\cdots+x^{n-1}$. If we consider cyclotomic polynomials $\Phi_l(x)$, $l\in\mathbb{N}^*$, we obtain:

$$f_n(x)=\prod_{d|n,\ d\geq 2}\Phi_d(x).$$

Then, it is easy to observe the following facts: (see also [11, p. 82])
(i)- if $m\mid n$, then $f_m(x)\mid f_n(x)$,
(ii)- if $p$ is an odd prime, then $f_p(x)$ has $2m$ irreducible factors of degree $\dfrac{p-1}{2m}$, for some divisor $m$ of $\dfrac{p-1}{2}$,
(iii)- if $p$ is an odd prime, then $\gcd\Big(\dfrac{f_{p^2}(x)}{f_p(x)},f_p(x)\Big)=1$ and $\dfrac{f_{p^2}(x)}{f_p(x)}$ has $2m$ irreducible factors of degree $\dfrac{p^2-p}{2m}$, for some divisor $m$ of $\dfrac{p^2-p}{2}$,
(iv)- if $p_1,p_2$ are odd primes, then $\gcd(f_{p_1}(x),f_{p_2}(x))=1$.

The degree assertions in (ii) and (iii) come from observing that any irreducible polynomial in $\mathbb{F}_2[x]$ of degree $2n$ splits into the product of two irreducible polynomials in $\mathbb{F}_4[x]$, each of degree $n$.

Parts (ii) and (iii) imply that $2h+1$ is square-free, because otherwise the polynomial $1+P+\cdots+P^{2h}=f_{2h+1}(P)$ would have at least four prime factors, which contradicts the hypothesis of the lemma.
Similarly, parts (ii) and (iv) imply that $2h+1$ is prime.
Thus, we may assume: $f_{2h+1}(x)=P_1P_2$, with $P_1,P_2\in\mathbb{F}_4[x]$ irreducible, each of degree $h$. It follows that:

$$1+P+\cdots+P^{2h}=f_{2h+1}(P)=P_1(P)P_2(P),\ \text{with}\ \deg(P_1(P))=\deg(P_2(P)).$$

By considering degrees, the only possibility is:

$$P_1(P)=U^aV^b,\ P_2(P)=W^c.$$

So,

$$a\deg(U)+b\deg(V)=\deg(P_1(P))=\deg(P_2(P))=c\deg(W).$$

To finish the proof, observe that Lemma 4 implies: $\gcd(a,b,c)=1$. □

**Lemma 13** (see [4], Lemma 2.3)**.** *If* $1+P+\cdots+P^h=1+(1+P)+\cdots+(1+P)^h$, *with even* $h\in\mathbb{N}^*$ *and* $P\in\mathbb{F}_4[x]$ *irreducible, then* $h=2^e-2$ *for some integer* $e\geq 2$.

**Proof**. We put: $h+2=2^ev$, where $v$ is odd. We obtain:

$$(1+P^v)^{2^e}=1+P^{h+2}=(1+P)^{h+2}=((1+P)^v)^{2^e},$$

so that: $1+P^v=(1+P)^v$.
If $v\geq 3$, then:

$$1+P^v=(1+P)^v=1+P^v+P+P^2U,$$

where $U$ has degree $v-3\geq 0$. So, $1+PU=0$. It is impossible. We conclude that $v=1$ and $h=2^e-2$. We must have $e\geq 2$ since $h\geq 1$. □

**Lemma 14** (see [4], Proposition 3.10)**.** *Let* $P_1,P_2\in\mathbb{F}_4[x]$ *be two irreducible polynomials, and let* $h,k\in\mathbb{N}$. *Then* $P_1^hP_2^k$ *is perfect over* $\mathbb{F}_4$ *if and only if:*

$$P_2=P_1+1 \text{ and } h=k=2^n-1, \text{ for some } n\in\mathbb{N}.$$

## 2.2. Strategy of the proof

Let $A=P^aQ^bR^cS^d$ be an odd perfect polynomial over $\mathbb{F}_4$ with $\omega(A)=4$. We set:

$$p=\deg(P),q=\deg(Q),r=\deg(R),s=\deg(S),\ p,q,r,s\geq 2.$$

We distinguish three main cases according to possible configurations of degrees as come from Lemma 6, namely:

Case 1: $p=q=r=s$.

Case 2: $p=q<r=s$.

Case 3: $p=q<r<s$.

Computations are simple and short enough to enable us to treat every possible case in its own section of the paper.

Each section contains several subsections whose length (always short) depends on the parity of exponents $a,b,c,d$. By using the multiplicativity of $\sigma$, we obtain some systems of four equations in four unknowns $P,Q,R,S$ to consider. The proof consists (essentially) of using repeatedly Lemma 5, of checking that the exponents of prime divisors are the same in both $A$ and $\sigma(A)$, and of checking that the degrees are the same on both sides of each equation of the system. Differentiation relative to $x$ is used when necessary. We always obtain a contradiction which is more or less (reasonably) immediate.

We may write the general system to resolve as:

$$(\star)\ \begin{cases} (E1): 1+P+\cdots+P^a = Q^{b_1}R^{c_1}S^{d_1}, \\ (E2): 1+Q+\cdots+Q^b = P^{a_2}R^{c_2}S^{d_2}, \\ (E3): 1+R+\cdots+R^c = P^{a_3}Q^{b_3}S^{d_3}, \\ (E4): 1+S+\cdots+S^d = P^{a_4}Q^{b_4}R^{c_4}, \end{cases}$$

in which $a, b, c, d > 0$ are positive numbers while the exponents on the right-hand side are non-negative numbers so that some of them may be zero.

We see below that we get part (i) of our theorem in Section Case 2.2, and part (ii) in Case 1.3 and Case 2.3.

## 3. Case 1 : $p = q = r = s$.

In this case, integers $a, b, c$ and $d$ play symmetric roles, so we have only to consider three subcases:
- Case 1.1 : $a$ is even and at least one of $b, c, d$ is even,
- Case 1.2 : $a$ is even and $b, c, d$ are all odd,
- Case 1.3 : $a, b, c, d$ are all odd.

We need the following lemma:

**Lemma 15.** *If the polynomial $A = P^aQ^bR^cS^d$ is perfect over $\mathbb{F}_4$, where $a$ is even, then $a = 2$ and $P + \alpha, P + \alpha + 1 \in \{Q, R, S\}$.*

**Proof**. We consider the first equation $(E1)$ of the system $(\star)$. Since $a$ is even, by Lemma 5, we have: $b_1, c_1, d_1 \in \{0, 1\}$.
Since $2p \leq ap = (b_1 + c_1 + d_1)p \leq 3p$, we must obtain: $a = b_1 + c_1 + d_1 = 2$. Thus:

$$\sigma(P^a) = 1 + P + P^2 = (P + \alpha)(P + \alpha + 1).$$

So, this complete our proof. □

### 3.1. Case 1.1

According to Lemma 15, we may assume: $Q = P + \alpha,\ R = P + \alpha + 1 = Q + 1$. So, by considering equation $(E1)$, we see that $P(0)$ must be equal to 1.
It suffices to consider the case where $b$ is even. Still by Lemma 15, we have $b = 2$. Thus, we must have: $S = Q + \alpha + 1 = P + 1$. It is impossible since $S$ is irreducible, $S \neq x$ and $P(0) = 1$.

### 3.2. Case 1.2

According to Lemma 15, we may assume: $Q = P + \alpha,\ R = P + \alpha + 1 = Q + 1$. Thus, as above we get $P(0) = 1$.
If $b, c, d$ are all odd, then by Lemma 8, $1 + Q,\ 1 + R$ and $1 + S$ divide $\sigma(Q^b),\ \sigma(R^c)$ and $\sigma(S^d)$ respectively. Thus, they belong to $\{P, Q, R, S\}$. Since $1 + Q = R$, we must have: $1 + S = P$. It follows that $S(0) = P(0) + 1 = 0$. It is impossible because $S$ is irreducible and $\deg(S) \geq 2$.

### 3.3. Case 1.3

In this case, $1+P,\ 1+Q,\ 1+R$ and $1+S$ divide $\sigma(P^a),\ \sigma(Q^b),\ \sigma(R^c)$ and $\sigma(S^d)$ respectively. Thus, they belong to $\{P,Q,R,S\}$. We may suppose:

$$P=Q+1,\ R=S+1.$$

We put:

$$a=2^hu-1,\ b=2^kv-1,\ c=2^lw-1,\ d=2^mt-1,$$
$$h,k,l,m,u,v,w,t\in\mathbb{N}^*, \text{and } u,v,w,t \text{ odd}.$$

We claim that $u=v=w=t=1$.
If one of these odd integers (say $u$) is greater than 1, then since:

$$\begin{cases}\sigma(P^a)=1+\cdots+P^a=(1+P)^{2^h-1}\ (1+\cdots+P^{u-1})^{2^h},\\ P \text{ and } Q=1+P \text{ do not divide } 1+\cdots+P^{u-1} \text{ (by Lemma 7)},\end{cases}$$

by Lemmas 5 and 10 we must have:

$$1+\cdots+P^{u-1}=RS.$$

Thus, by considering degrees, $u-1=2$ and $P+\alpha,\ P+\alpha+1\in\{R,S\}$. Therefore, $P,\ P+1,\ P+\alpha$ and $P+\alpha+1$ are all irreducible. It is impossible because $P(0)\in\{1,\alpha,\alpha+1\}$, and $p\geq 2$.
So, $u=v=w=t=1$ and $a=2^h-1,\ b=2^k-1,\ c=2^l-1,\ d=2^m-1$. It follows that:

$$P^aQ^bR^cS^d=A=\sigma(A)=\sigma(P^a)\sigma(Q^b)\sigma(R^c)\sigma(S^d)=Q^aP^bS^cR^d.$$

Hence $a=b$ and $c=d$. We obtain part (ii) of our theorem in the case: $p=q=r=s$.

## 4. Case 2: $p=q<r=s$.

The integers $a$ and $b$ (resp. $c$ and $d$) play symmetric roles. Observe that:

$$\text{either } (\gcd(1+R,S)=1) \text{ or } (S=1+R).$$

We need the following lemmas.

**Lemma 16.** *Any even $e\in\{a,b,c,d\}$ satisfies: $e\geq 4$.*

**Proof**. We may suppose that $e\in\{a,c\}$.
- If $e=a$ and if $a=2$, then $\sigma(P^a)=(P+\alpha)(P+\alpha+1)$ and equation $(E1)$ implies:

$$P+\alpha,\ P+\alpha+1\in\{Q,R,S\}.$$

It is impossible by considering degrees.
- If $e=c$ and if $c=2$, then a similar argument gives the contradiction: $R+\alpha$, $R+\alpha+1\in\{R,S\}$. □

**Lemma 17.** *If $a$ and $b$ are both even, then:*

$$\sigma(P^a) = \sigma(Q^b) = RS, \text{ and } c \text{ and } d \text{ are both odd.}$$

**Proof**. In this case, by Lemmata 5 and 12, we have:

$$c_1 = c_2 = d_1 = d_2 = 1, b_1 = a_2 = 0,$$

and thus:

$$\sigma(P^a) = RS = \sigma(Q^b).$$

If $c$ is even, then $c_4 = c - c_1 - c_2 = c - 2$ is even. Moreover, $d_3 \leq 1$ by Lemma 5. So, we obtain: $2 \leq d = d_1 + d_2 + d_3 \leq 3$.
By Lemma 16, we must have $d = 3$, and hence equation $(E4)$ implies:

$$(1+S)^3 = 1 + S + S^2 + S^3 = \sigma(S^d) = P^{a_4} Q^{b_4} R^{c_4}.$$

- If $1 + S = R$, then $c_4 = 3$, which contradicts the fact: $c_4$ is even.
- If $\gcd(1 + S, R) = 1$, then $R$ does not divide $1 + S$. So, $c - 2 = c_4 = 0$ and thus $c = 2$. It is impossible, by Lemma 16. □

**Lemma 18.** *If $e$ is an odd number satisfying $e \in \{c, d\}$ then $e = 2^l - 1$, for some $l \in \mathbb{N}^*$.*

**Proof**. We may assume that $e = c$. Put: $c = 2^l w - 1$, where $w$ is odd. Consider equation $(E3)$ of the system $(\star)$. We have, by Lemma 8:

$$1 + R + \cdots + R^c = (1+R)^{2^l - 1} \ (1 + R + \cdots + R^{w-1})^{2^l}.$$

- If $\gcd(1 + R, S) = 1$, then $S$ does not divide $1 + R$. So,

$$1 + R = P^y Q^z, \text{ for some } y, z \in \mathbb{N}.$$

If $y = 0$, then $R = Q^z + 1$. Since $R$ is irreducible, we must have $z = 1$ and thus $R = Q + 1$. It is impossible because $q < r$. So, $y \geq 1$.
Analogously, we must have $z \geq 1$.
It follows that $P$ and $Q$ are the only divisors of $1 + R$. So, by Lemma 7, we have:

$$1 + R + \cdots + R^{w-1} = S^j, \text{ for some } j \in \mathbb{N},$$

and by Lemmas 4 and 10:

$$w - 1 = j = 0, \text{ and } c = 2^l - 1.$$

- If $1 + R = S$, then:

$$1 + R + \cdots + R^c = S^{2^l - 1}(1 + R + \cdots + R^{w-1})^{2^l}.$$

If $w \geq 3$, then:

$$1 + R + \cdots + R^{w-1} = P^\beta Q^\gamma,$$

where $\beta = \gamma = 1$, by Lemmas 12 and 4. It is impossible by considering degrees. Thus, $w = 1$ and we are done. □

We have now to consider three subcases:
- Case 2.1 : $a, b$ are both even,
- Case 2.2 : $a$ is odd and $b$ is even,
- Case 2.3 : $a, b$ are both odd.

### 4.1. Case 2.1

In this case, by Lemma 17:

$$1+P+\cdots+P^a = RS = 1+Q+\cdots+Q^b,$$
$c$ and $d$ are both odd.

By Lemma 18, we may put:

$$c = 2^l - 1,\ d = 2^m - 1,\ \text{where } l, m \geq 1,$$

and thus, by Lemma 8:

$$\sigma(R^c) = (1+R)^c,\ \sigma(S^d) = (1+S)^d.$$

- If $\gcd(1+R, S) = 1$, then $d_3 = 0$ and $d = 2$. It is impossible since $d$ is odd.
- If $1 + R = S$, then by considering exponents of $S$, we have:

$$2^l + 1 = 1 + 1 + (2^l - 1) = d_1 + d_2 + d_3 = d = 2^m - 1.$$

Analogously we get: $2^m + 1 = c = 2^l - 1$.

Thus, $2^l + 2 = 2^m$ and $2^m + 2 = 2^l$. It is impossible.

### 4.2. Case 2.2

We put: $a = 2^h u - 1,\ b = 2^k v$, where $u, v$ are both odd. Consider equations $(E1)$ and $(E2)$, we have by Lemmata 8 and 9:

$$\sigma(P^a) = (1+P)^{2^h-1}\ (1+P+\cdots+P^{u-1})^{2^h} = Q^{2^h-1}\ (1+P+\cdots+P^{u-1})^{2^h}.$$

The polynomials $Q$ and $P = 1 + Q$ do not divide $\sigma(Q^b)$ because $b$ is even. So:

$$\sigma(Q^b) = R^y S^z,\ \text{for some } y, z \in \mathbb{N}.$$

By Lemmas 12 and 4, $y = z = 1$, so that:

$$1 + (1+P) + \cdots + (1+P)^b = \sigma(Q^b) = RS.$$

Moreover, if $u \geq 3$, then a similar argument gives:

$$1 + P + \cdots + P^{u-1} = RS,$$

and hence: $c_1 = d_1 = 2^h,\ c_2 = d_2 = 1$.
So,

$$1+P+\cdots+P^{u-1} = RS = 1 + (1+P) + \cdots + (1+P)^b.$$

It follows by Lemma 13 that:

$$u - 1 = b = 2^e - 2,\ \text{for some } e \geq 2.$$

In fact, $e \geq 3$ since by Lemma 16 $b \geq 4$.

**4.2.1. Case $c$ odd and $\gcd(1+R,S)=1$**

In this case, $S$ does not divide $1+R$, and thus $R$ does not divide $1+S$. So,

$$d_3 = c_4 = 0.$$

By Lemma 18 we must have:

$$c = 2^l - 1,\ d = 2^m - 1 \text{ for some } l, m \in \mathbb{N}^*,$$

so that:

$$\sigma(R^c) = (1+R)^c,\ \sigma(S^d) = (1+S)^d.$$

Two subcases arise:
Subcase: $u = 1$:
The integer $b_3 + b_4$ must be odd since

$$b = b_1 + b_3 + b_4 = 2^h - 1 + b_3 + b_4$$

is even. In particular, $b_3 \neq b_4$. We are going to prove that:

$$c = d = 1,\ \min\{b_3, b_4\} = 1, \text{ and } (b_3, b_4) \in \{(1,2),(2,1)\}.$$

$c = d = 1$:
Since $a = 2^h - 1$, Lemma 8 implies: $\sigma(P^a) = (1+P)^a = Q^a$ and hence:

$$c_1 = d_1 = 0,\ b_1 = a = 2^h - 1.$$

The identity $\sigma(Q^b) = RS$ gives: $c_2 = d_2 = 1$.
Thus: $d = d_1 + d_2 + d_3 = 0 + 1 + 0 = 1$, and $c = c_1 + c_2 + c_4 = 0 + 1 + 0 = 1$.
$\min\{b_3, b_4\} = 1$:
We obtain: $1 + R = \sigma(R^c) = P^{a_3}Q^{b_3},\ 1 + S = \sigma(S^d) = P^{a_4}Q^{b_4}$.
It is easy to see that $a_3, b_3, a_4, b_4 \geq 1$, by irreducibility of $R$ and $S$ and by considering degrees.
If $\min\{b_3, b_4\} \geq 2$, then $Q^2$ divides $\gcd(1+R, 1+S)$, so it divides $(1+R)+R(1+S) = 1+RS$, while by equation $(E2)$, $Q^2$ does not divide $\sigma(Q^b)+1 = RS+1$. So, we get a contradiction.
Similarly we obtain: $\min\{a_3, a_4\} = 1$.
$(b_3, b_4) \in \{(1,2),(2,1)\}$:
Equations $(E2)$, $(E3)$ and $(E4)$ give:

$$Q^{2^k v+1} = Q^{b+1} = 1 + (1+Q)\sigma(Q^b) = 1 + PRS = 1 + P(P^{a_3}Q^{b_3} + 1)(P^{a_4}Q^{b_4} + 1).$$

By considering exponents and degrees, we have:

$$\begin{gathered}(a_3 + b_3)p = (a_4 + b_4)p = r = \frac{b}{2}\,p,\\ (2^h - 1) + b_3 + b_4 = b.\end{gathered}$$

We may suppose that $b_3 = 1$ ($b_3$ and $b_4$ are playing a symmetric role). Thus:

$$b_4 \text{ is even, } a_3 + 1 = \frac{b}{2} = 2^{k-1}v,\ b_4 + 2^h = b = 2^k v.$$

It follows that:

$$\begin{aligned} Q^{2^k v+1} &= 1 + P(P^{a_3}Q+1)(P^{a_4}Q^{b_4}+1) \\ &= 1 + P + QP^{a_3+1} + P^{a_4}Q^{b_4}(P^{a_3+1}Q+P) \\ &= Q + QP^{a_3+1} + P^{a_4+1}Q^{b_4}(P^{a_3}Q+1). \end{aligned}$$

So,

$$\begin{aligned} Q^{2^k v} &= (1+P^{2^{k-1}v}) + P^{a_4+1}Q^{b_4-1}(P^{a_3}Q+1) \\ &= (1+P)^{2^{k-1}}(1+P+\cdots+P^{v-1})^{2^{k-1}} + P^{a_4+1}Q^{b_4-1}(P^{a_3}Q+1) \\ &= Q^{2^{k-1}}(1+P+\cdots+P^{v-1})^{2^{k-1}} + P^{a_4+1}Q^{b_4-1}(P^{a_3}Q+1) \\ &= Q^{2^{k-1}}U + Q^{b_4-1}V, \end{aligned}$$

where $Q$ does not divide $UV$.
- If $b_4 - 1 > 2^{k-1}$, then $Q$ must divide $U$. It is impossible.
- If $b_4 - 1 < 2^{k-1}$, then $Q$ must divide $V$. It is impossible.
Thus: $b_4 - 1 = 2^{k-1}$, and hence

$$k = 1,\ (b_3, b_4) = (1, 2).$$

To finish the subcase $u = 1$, we have just seen that:

$$k = 1,\ a = 2^h - 1,\ 2v = b = b_1 + b_3 + b_4 = (2^h - 1) + 1 + 2 = 2^h + 2.$$

We may write:

$$\begin{aligned} &Q^{2v} = Q^{2^k v} = Q^{2^{k-1}}U + Q^{b_4-1}V = Q(U+V) \\ &a_3 + 1 = a_4 + 2 = v = \frac{b}{2} = 2^{h-1} + 1 \geq 3 \text{ because } v \text{ is odd.} \end{aligned}$$

Since $Q = 1 + P$, we obtain:

$$\begin{aligned} (1+P)^{2v} &= (1+P)\Big(1 + P + \cdots + P^{v-2} + P^{2v-2}(1+P)\Big) \\ &= (1+P)(1+P+\cdots+P^{v-2}) + P^{2v-2}(1+P^2) \\ &= 1 + P^{v-1} + P^{2v-2} + P^{2v}. \end{aligned}$$

Thus: $(1+P)^v = 1 + P^{\frac{v-1}{2}} + P^{v-1} + P^v$, which implies that $v = 3$, and:

$$h = 2,\ a = 3,\ b = 6,\ c = d = 1,\ R, S \in \{P^3 + P^2 + 1, P^3 + P + 1\}.$$

We obtain part (i) of our theorem.
Subcase: $u \geq 3$:
In this case, we have seen that:

$$c_1 = d_1 = 2^h,\ c_2 = d_2 = 1 \text{ and } d_3 = c_4 = 0.$$

Hence:

$$d = d_1 + d_2 + d_3 = 2^h + 1 = c_1 + c_2 + c_4 = c,$$

and by Lemma 18,

$$2^h + 1 = d = 2^m - 1, \text{ for some } m \in \mathbb{N}^*.$$

So,

$$\begin{aligned} &h = 1,\ m = 2,\ c = d = 3,\\ &a_3 + a_4 = a = 2u - 1. \end{aligned}$$

Furthermore, since $\sigma(P^{u-1}) = RS = \sigma(Q^b)$, and $Q = 1 + P$, by Lemma 13 we obtain:

$$b = u - 1 = 2^e - 2, \text{ for some integer } e \geq 2.$$

Since $\sigma(R^c) = \sigma(R^3) = (1 + R)^3$, equation $(E3)$ implies that 3 divides $a_3$.
Analogously, equation $(E4)$ implies that 3 also divides $a_4$. So, 3 divides $a_3 + a_4 = 2u - 1$. Thus, 3 divides $u + 1 = 2^e$. It is impossible.

### 4.2.2. Case $c$ odd and $1 + R = S$

We know that $c = 2^l - 1$, and $\sigma(R^c) = (1 + R)^c = S^c$. Hence, $d = d_1 + d_2 + d_3 = 2^h + 1 + 2^l - 1$ is even. Thus, $c_4 = 0$ since $R = 1 + S$ does not divide $\sigma(S^d)$. So, $a_4 = b_4 = 1$ by Lemma 12.
Thus, by considering degrees in equation $(E4)$, we obtain:

$$2p = (a_4 + b_4)p = dr \geq 2r > 2p,$$

which is impossible.

### 4.2.3. Case $c$ and $d$ even

We recall that: $a = 2^h u - 1,\ b = 2^k v$, where $u, v$ are both odd. We need the following result:

**Lemma 19.** *If $c$ and $d$ are both even, then $c_4 = d_3 = 1$ and $u \geq 3$.*

**Proof**. Observe that:

$$c_1 \in \{0, 2^h\},\ c_2 = 1, \text{ and } c_4 \in \{0, 1\} \text{ by Lemma 5},$$

so $c_4 = 1$ because $c = c_1 + c_2 + c_4$ is even.
Analogously, we have $d_3 = 1$.
If $u = 1$, then $\sigma(P^a) = Q^a$, hence $c_1 = d_1 = 0$. It follows that:

$$c = c_1 + c_2 + c_4 = 0 + 1 + 1 = 2.$$

It is impossible by Lemma 16. □

Since by Lemma 19 $u \geq 3$ and since $Q = 1 + P$, system $(\star)$ implies:

$$\begin{aligned} &1 + P + \cdots + P^{u-1} = RS = 1 + (1 + P) + \cdots + (1 + P)^b,\\ &1 + R^{c+1} = (1 + R)SP^{a_3}Q^{b_3},\\ &1 + S^{d+1} = (1 + S)RP^{a_4}Q^{b_4}. \end{aligned}$$

So,

$$\begin{aligned}
&u-1=b=2^e-2, \text{ for some } e\geq 2, \text{ by Lemma 13,}\\
&r=\frac{b}{2}\ p=(2^{e-1}-1)p,\\
&c=c_1+c_2+c_4=2^h+1+1=2^h+2,\\
&d=d_1+d_2+d_3=2^h+1+1=2^h+2,\\
&a_3+a_4=a=2^h(2^e-1)-1 \text{ (odd)},\\
&(a_3+b_3)p=(a_4+b_4)p=(c-1)r,\\
&a_3+b_3=a_4+b_4=(2^h+1)(2^{e-1}-1) \text{ (odd)},\\
&a_3-b_4=a_4-b_3=(2^h-1)2^{e-1}.
\end{aligned}$$

If $a_3$ is even, then by differentiating $(E3)$ relative to $x$, we obtain:

$$R'R^c=((1+R)SQ^{b_3})'P^{a_3}.$$

Thus, $P^{a_3}$ must divide $R'$.
By considering degrees, we have:

$$(2^h-1)2^{e-1}p=(a_3-b_4)p\leq a_3p<r=(2^{e-1}-1)p.$$

So,

$$(2^h-1)2^{e-1}<2^{e-1}.$$

It is impossible since $h\geq 1$.
If $a_3$ is odd, then $a_4$ must be even. By differentiating $(E4)$ relative to $x$, we also obtain the same contradiction.

## 4.3. Case 2.3

Lemma 9 gives: $Q=P+1$, by considering degrees. Put: $a=2^hu-1,\ b=2^kv-1$, where $u,v$ are both odd. Then, by Lemmata 8, 12 and 4, equations $(E1)$ and $(E2)$ become:

$$\begin{aligned}
&1+P+\cdots+P^a=Q^{2^h-1}\ (1+P+\cdots+P^{u-1})^{2^h}=Q^{2^h-1}\ (RS)^{\varepsilon_1 2^h},\\
&1+Q+\cdots+Q^b=P^{2^k-1}\ (1+Q+\cdots+Q^{v-1})^{2^k}=P^{2^k-1}\ (RS)^{\varepsilon_2 2^k},\\
&\text{where } \varepsilon_1,\varepsilon_2\in\{0,1\}.
\end{aligned}$$

so that $c_1=d_1\in\{0,2^h\}$ and $c_2=d_2\in\{0,2^k\}$.
We also use

**Lemma 20.** *i)- If $c$ is even, then $d_3=1$ and $d=2^m-1$ for some $m\in\mathbb{N}^*$.*
*ii)- If $c$ is even and $\gcd(1+R,S)=1$, then $c_4=0$ and $u,\ v\geq 3$.*

**Proof**. i): In equation $(E3)$, by Lemma 5, $d_3\in\{0,1\}$ . If $d_3=0$, then $a_3=b_3=1$, by Lemmata 12 and 4. It is impossible by considering degrees. Thus $d_3=1$.
It follows that $d=d_1+d_2+d_3$ must be odd, and by Lemma 18:

$$d=2^m-1,\ m\in\mathbb{N}^*.$$

ii): Since $R$ does not divide $1+S$, equation $(E4)$ implies that $c_4=0$.
- If $u=1$, then $c=c_1+c_2+c_4=\varepsilon 2^k,\ d=d_1+d_2+d_3=\varepsilon 2^k+1=2^m-1$,

where $\varepsilon \in \{0,1\}$. It follows that: either $(\varepsilon = 0,\ m = 1)$ or $(\varepsilon = 1,\ k = 1,\ m = 2)$, and hence $c \in \{0,2\}$, which is impossible by Lemma 16.
- If $v = 1$, then $c = c_1 = \varepsilon 2^h,\ d = \varepsilon 2^h + 1 = 2^m - 1$. Similarly we obtain $c \in \{0,2\}$. □

**4.3.1. Case $c$ even and $\gcd(1+R,S) = 1$**

By Lemma 20, $u, v \geq 3,\ d_3 = 1,\ c_4 = 0,\ c_1 = d_1 = 2^h$ and $c_2 = d_2 = 2^k$. Thus:

$$2^m - 1 = d = d_1 + d_2 + d_3 = 2^h + 2^k + 1.$$

We conclude that:

$$(h,k) \in \{2,1),(1,2)\},\ m = 3 \text{ and } c = c_1 + c_2 + c_4 = 2^h + 2^k + 0 = 6.$$

Since:

$$1 + P + \cdots + P^{u-1} = RS = 1 + Q + \cdots + Q^{v-1}, \text{ with } Q = 1 + P,$$

by Lemma 13 we get: $2r = (u-1)p,\ u - 1 = v - 1 = 2^e - 2,$ for some $e \geq 2$.
It follows that:

$$r = (2^{e-1} - 1)p.$$

Equation $(E3)$ implies:

$$(R^3 + R^2 + 1)(R^3 + R + 1) = 1 + R + \cdots + R^6 = \sigma(R^c) = SP^{a_3}Q^{b_3}.$$

Moreover, $\gcd(R^3 + R^2 + 1, R^3 + R + 1) = 1$ by Bezout theorem, since

$$(R+1)(R^3 + R^2 + 1) + R(R^3 + R + 1) = 1.$$

So, by considering degrees, we must have one the following possibilities:

$$\begin{array}{l}
(1):\ SP^{a_3} = R^3 + R^2 + 1,\ Q^{b_3} = R^3 + R + 1,\\
(2):\ SP^{a_3} = R^3 + R + 1,\ Q^{b_3} = R^3 + R^2 + 1,\\
(3):\ SQ^{b_3} = R^3 + R^2 + 1,\ P^{a_3} = R^3 + R + 1,\\
(4):\ SQ^{b_3} = R^3 + R + 1,\ P^{a_3} = R^3 + R^2 + 1.
\end{array}$$

- Case (1) implies: $a_3 p = 2r$, so that: $a_3 = 2(2^{e-1} - 1)$ is even. Thus, by differentiating, we have:

$$S' P^{a_3} = R^2 R'.$$

It follows that $R$ must divide either $S'$ or $P$. It contradicts the fact that $\deg(R) = \deg(S) > \deg(P)$.
- Case (3) gives a similar contradiction.
- Case (2) implies: $b_3 p = 3r$, so that: $b_3 = 3(2^{e-1} - 1)$ is odd. By differentiating, we obtain:

$$Q' Q^{b_3 - 1} = R^2 R',$$

which is impossible, as above, since $\deg(R) > \deg(Q)$.
- Case (4) has not accured yet, for the same reason.

**4.3.2. Case $c$ even and $R = 1 + S$**

By Lemma 20, $d = 2^m - 1$, for some $m \in \mathbb{N}^*$. Equation $(E4)$ implies:

$$c_4 = d = 2^m - 1,\ a_4 = b_4 = 0.$$

Thus:

$$c = c_1 + c_2 + c_4 = \varepsilon_1\ 2^h + \varepsilon_2\ 2^k + 2^m - 1,\ \text{where } \varepsilon_1,\ \varepsilon_2 \in \{0, 1\}.$$

It is impossible since $c$ is even.

**4.3.3. Case $c, d$ odd**

We may put, by Lemma 18:

$$c = 2^l - 1,\ d = 2^m - 1,\ l, m \in \mathbb{N}^*,$$

so that: $\sigma(R^c) = (1 + R)^c,\ \sigma(S^d) = (1 + S)^d$.
- If $\gcd(1 + R, S) = 1$, then $d_3 = 0$ and hence:

$$d = d_1 + d_2 + d_3 = \varepsilon_1\ 2^h + \varepsilon_2\ 2^k,\ \text{where } \varepsilon_1,\ \varepsilon_2 \in \{0, 1\},$$

which is impossible since $d$ is odd.
- If $1 + R = S$, then $\sigma(R^c) = S^c$ and $\sigma(S^d) = R^d$. It follows that $c \leq d$ and $d \leq c$. Hence $c = d$, and $R^c S^d$ is perfect. Therefore, $P^a Q^b$ is also perfect by Lemma 3. By Lemma 14, we obtain part (ii) of our theorem in the case: $p = q < r = s$.
Now we treat the last case:

## 5. Case 3: $p = q < r < s$.

Integers $a$ and $b$ play symmetric roles. We need the following lemma.

**Lemma 21.** *If the polynomial $A = P^a Q^b R^c S^d$ is perfect over $\mathbb{F}_4$, then $a+b$ is even.*

**Proof**. We consider equations $(E1)$ and $(E2)$ of the system $(\star)$.
- If $a$ is even, then by Lemma 4, we have: $b_1, c_1, d_1 \in \{0, 1\}$. Since $q \neq r \neq s$ and according to Lemmata 10 and 12, we have:

$$1 + P + \cdots + P^a = QRS.$$

If $b$ is odd, then by Lemma 9 $1 + Q = P$. Therefore, $Q = 1 + P$ does not divide $1 + P + \cdots + P^a = QRS$. It is impossible. So, $b$ is even.
- If $a$ is odd, then by the same argument, $b$ must be odd ($a$ and $b$ play symmetric roles).
We are done. □

We have to consider two subcases:
- Case 3.1 : $a, b$ are both even,
- Case 3.2 : $a, b$ are both odd.

### 5.1. Case 3.1

We consider the system $(\star)$. In this case, as in the proof of Lemma 21, we must have:

$$(E1) : 1 + P + \cdots + P^a = QRS,$$
$$(E2) : 1 + Q + \cdots + Q^b = PRS.$$

So, $a = b$ and:

$$1 + P^{a+1} = (1 + P)QRS,\ 1 + Q^{a+1} = (1 + Q)PRS.$$

Thus,

$$(P + Q)(P^a + P^{a-1}Q + \cdots + PQ^{a-1} + Q^a) = P^{a+1} + Q^{a+1} = (P + Q)RS.$$

Therefore,

$$P^a + P^{a-1}Q + \cdots + PQ^{a-1} + Q^a = RS.$$

By considering degrees, we obtain: $ap = r + s$, while by equation $(E1)$, $(a - 1)p = r + s$. We get a contradiction.

### 5.2. Case 3.2

In this case we put: $a = 2^h u - 1,\ b = 2^k v - 1,\ h, k, u, v \in \mathbb{N}^*,\ u, v$ odd.
By Lemma 9 we must have: $Q = P + 1$.
If $u \geq 3$, then by Lemmas 5 and 10: $1 + P + \cdots + P^{u-1} = RS$.
It follows by Lemma 12 that $r = s$. It contradicts the fact: $r < s$.
We conclude that $u = 1$. Analogously, we get $v = 1$.
Therefore, $\sigma(P^a) = Q^a,\ \sigma(Q^b) = P^b$, and hence $a \leq b \leq a$. It follows that $P^a Q^b$ is perfect. Thus, $R^c S^d$ is also perfect by Lemma 3. It is impossible by Lemma 14, since $S \neq R + 1$.

## 6. Examples

We give here some perfect polynomials of the form $P^a Q^b R^c S^d$ such that: $a, b, c, d \in \mathbb{N}$ and $p, q, r, s \in \{2, 4, 6\}$.
According to part (ii) of Theorem 1, we need to know all irreducible polynomials $P$ over $\mathbb{F}_4$, such that $P + 1$ is also irreducible and $\deg(P) \in \{2, 4\}$.
There exist two (resp. twelve) such polynomials of degrees 2 (resp. 4). Observe also that there is no such polynomial of degree 3. We recall that $\bar{\alpha} = \alpha + 1$.
Degree 2: $P_1 = x^2 + x + \alpha,\ P_2 = P_1 + 1$.
Degree 4:

$$R_1 = x^4 + x^3 + x + \alpha \qquad R_3 = x^4 + x^3 + x^2 + \alpha$$
$$R_5 = x^4 + x^3 + \alpha x^2 + \alpha x + \alpha \qquad R_7 = x^4 + x^3 + \bar{\alpha} x^2 + \bar{\alpha} x + \bar{\alpha}$$
$$R_9 = x^4 + \alpha x^2 + \alpha x + \alpha \qquad R_{11} = x^4 + \bar{\alpha} x^2 + \bar{\alpha} x + \bar{\alpha},$$

and:

$$R_{2i} = R_{2i-1} + 1, \text{ for } 1 \leq i \leq 6.$$

### 6.1. Case: $p = q = r = s$

There exist exactly 15 families of odd perfect polynomials over $\mathbb{F}_4$ of the form: $P^aQ^bR^cS^d$ where $a, b, c, d \in \mathbb{N}$ and $p = q = r = s = 4$:

$$A_{ij} = \Big(R_i(R_i+1)\Big)^{2^{n_i}-1} \Big(R_j(R_j+1)\Big)^{2^{n_j}-1},$$
$$i, j \in \{1, 3, 5, 7, 9, 11\},\ i < j,\ n_i, n_j \in \mathbb{N}.$$

### 6.2. Case: $p = q < r = s$

- There exist exactly 6 families of odd perfect polynomials over $\mathbb{F}_4$ of the form: $P^aQ^bR^cS^d$ where $a, b, c, d \in \mathbb{N}$ and $p = q = 2,\ r = s = 4$:

$$B_i = \Big(P_1(P_1+1)\Big)^{2^n-1} \Big(R_i(R_i+1)\Big)^{2^{n_i}-1},\ i \in \{1, 3, 5, 7, 9, 11\},\ n, n_i \in \mathbb{N}.$$

- As examples for part (i) of Theorem 1 we have:

$$A_1 = P_1^3P_2^6S_1S_2,\ A_2 = P_2^3P_1^6S_1S_2,$$

where:

$$S_1 = x^6 + x^5 + \bar{\alpha}x^4 + x^3 + \alpha x + \alpha,$$
$$S_2 = x^6 + x^5 + \alpha x^4 + x^3 + \bar{\alpha}x + \bar{\alpha}.$$

## Acknowledgements

We gratefully acknowledge the referee for several comments, great suggestions and improvements of our initial results, namely that of crucial Lemma 12. As a consequence of his work on the paper our main result is now greatly improved with a new family of odd perfect polynomials in part (i). The referee's observation that some results in this paper may remain true over a finite extension of $\mathbb{F}_4$, encourages us to consider a forthcoming work on the subject.
We also warmly thank Paul Pollack for his nice proof of the infinity of the family above.

## References

[1] T. B. BEARD JR, J. R. OCONNELL JR, K. I. WEST, *Perfect polynomials over $GF(q)$*, Rend. Accad. Lincei **62**(1977), 283-291.
[2] E. F. CANADAY, *The sum of the divisors of a polynomial*, Duke Math. Journal **8**(1941), 721- 737.
[3] L. E. DICKSON, *Higher irreducible congruences*, Bull. Amer. Math. Soc. **3**(1897), 381-389.
[4] L. GALLARDO, O. RAHAVANDRAINY, *On perfect polynomials over $\mathbb{F}_4$*, Portugaliae Mathematica **62**(2005), 109-122.
[5] L. GALLARDO, O. RAHAVANDRAINY, *Perfect polynomials over $\mathbb{F}_4$ with less than five prime factors*, Portugaliae Mathematica **64**(2007), 21-38.
[6] L. H. GALLARDO, O. RAHAVANDRAINY, *Odd perfect polynomials over $\mathbb{F}_2$*, J. Théor. Nombres Bordeaux **19**(2007), 167-176.

[7] L. H. Gallardo, O. Rahavandrainy, *There is no odd perfect polynomial over $\mathbb{F}_2$ with four prime factors*, Portugaliae Mathematica, to appear.

[8] L. H. Gallardo, O. Rahavandrainy, *Even perfect polynomials over $\mathbb{F}_2$ with four prime factors*, International Journal of Pure and Applied Mathematics, to appear.

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

[10] C. J. Hall, *L-functions of twisted Legendre curves*, J. Number Theory **119**(2006), 128-147.

[11] R. Lidl, H. Niederreiter, *Finite fields*, in: *Encyclopedia of Mathematics and its Applications*, (G.- C. Rota, Ed.), Addison-Wesley, 1983.

[12] P. Pollack, *An explicit approach to hypothesis H for polynomials over a finite field*, in: *CRM Proceedings and Lecture Notes, Anatomy of Integers*, (J.- M. De Koninck, A. Granville, F. Luca, Eds.), AMS, 2008, 259-274.

[13] J.-A. Serret *Mémoire sur la théorie des congruences suivant un module premier et suivant une fonction modulaire irréductible*, Mémoires de l'Acadèmie des Sciences de l'Institut Impérial de France **35**(1866), 617-688.