Portugal. Math. (N.S.)
Vol. 66, Fasc. 2, 2009, 131–145

Portugaliae Mathematica

There is no odd perfect polynomial over $\mathbb{F}_2$ with four prime factors

Luis H. Gallardo and Olivier Rahavandrainy

(Communicated by Arnaldo Garcia)

Abstract. A perfect polynomial over the binary field $\mathbb{F}_2$ is a polynomial $A \in \mathbb{F}_2[x]$ that equals the sum of all its divisors. If $\gcd(A, x^2 + x) = 1$ then we say that A is odd. It is believed that odd perfect polynomials do not exist. In this article we prove this for odd perfect polynomials A with four prime divisors, i.e., polynomials of the form $A = P^a Q^b R^c S^d$ where P, Q, R, S are distinct irreducible polynomials of degree > 1 over $\mathbb{F}_2$ and a, b, c, d are positive integers.

Mathematics Subject Classification (2000). Primary 11T55; Secondary 11T06.

Keywords. Sum of divisors, polynomials, finite fields, characteristic 2.

1. Introduction

A multiperfect number n is a positive integer $n > 1$ such that n divides the sum $\sigma(n)$ of all its positive divisors. When the quotient $\sigma(n)/n = 2$, n is called a perfect number. All known multiperfect numbers are even. It is believed that there are no odd multiperfect numbers, but this has not been proved.

We investigate in this article an analogue over the ring $\mathbb{F}_2[x]$:

For a polynomial $A \in \mathbb{F}_2[x]$, where $\mathbb{F}_2$ is the binary field $\{0, 1\}$, let

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

be the sum of divisors of A. Let $\omega(A)$ be the number of distinct prime (irreducible) polynomials that divide A. Observe that σ is multiplicative, a fact that shall be used many times without more reference in the rest of the paper. A perfect polynomial A is a polynomial that divides $\sigma(A)$, or, equivalently, is a polynomial A such that $\sigma(A) = A$.

The notion of 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. He discovered the following list of five even perfect polynomials with four irreducible factors and claimed that the list is complete, leaving open the case of the odd ones:

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

In other words Canaday's conjecture says:

There is no odd perfect polynomial in $\mathbb{F}_2[x]$.

Some work has been done on this. A simple congruence argument shows that an odd perfect polynomial in $\mathbb{F}_2[x]$ must be a perfect square. Also (trivially) there is no odd perfect polynomial over $\mathbb{F}_2$ with $\omega(A) = 1$. Canaday [2], Theorem 17, proved the inexistence of odd perfect polynomials with two prime factors, i.e., with $\omega(A) = 2$. Recently, we proved in [5] the inexistence of perfect polynomials over $\mathbb{F}_2$ with $\omega(A) = 3$.

The object of this paper is to prove that there is no odd perfect polynomial over $\mathbb{F}_2$ with $\omega(A) = 4$.

In contrast with the case of perfect numbers, observe that Sylvester [7] already proved in 1888 that every odd perfect number requires at least five prime factors. More recent results about multiperfect numbers are surveyed in [6].

2. Some facts and the general strategy of the proof

We denote, as usual, by $\mathbb{N}$ the set of non-negative integers. The first two facts (over $\mathbb{F}_2$) come from Canaday [2]:

Lemma 2.1 ([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 not constant, i.e.,* $Q \notin \mathbb{F}$ *and* $\sigma(P^{2n}) = 1 + \cdots + P^{2n} = Q^m$. *Then* $m \in \{0, 1\}$.

The following lemma is a consequence of the proof of Lemma 6 in [2].

Lemma 2.2. *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, $m > 1$ and $\sigma(P^{2n}) = 1 + \cdots + P^{2n} = Q^m C$ for some $C \in \mathbb{F}[x]$. Then*

$$\deg(P) > 2\deg(Q).$$

In other words, if $\deg(P) = \deg(Q)$ then $m = 1$.

We need a more detailed result.

Lemma 2.3. *Let $\mathbb{F}$ be a perfect field of characteristic 2. Let $a, b, c, d \in \mathbb{N}$ be non-negative integers. Let P, Q, R, S be four distinct, irreducible polynomials in $\mathbb{F}[x]$ such that $d = \deg(Q) = \deg(P)$. Assume that*

$$1 + S + S^2 = P^a Q^b R^c. \tag{1}$$

Observe that $\deg(R)$ may be unequal to d. Then the following cases occur:

(a) *If a is even, then*

$$\deg(S) > (a + b - 1)\deg(P) + (c - 1)\deg(R);$$

if a is even and $b = 0$, then

$$\deg(S) > a\deg(P) + (c - 1)\deg(R).$$

(b) *If c is even, then*

$$\deg(S) > c\deg(R) + (a + b - 2)\deg(P);$$

if c is even and $b = 0$, then

$$\deg(S) > c\deg(R) + (a - 1)\deg(P).$$

(c) *If c is odd and $b = 0$, then*

$$\deg(S) > (c - 1)\deg(R) + (a - 1)\deg(P),$$

while if c is odd, then

$$\deg(S) > (c - 1)\deg(R) + (a + b - 2)\deg(P).$$

Proof. We only prove the first assertion in (c), the other proofs are similar. By differentiation relative to x of both sides of (1) (observe that differentiation of

squares yields zero), we get

$$S' = R^c P^{a-1} Q^{b-1}(aP'Q + bQ'P). \tag{2}$$

But S is prime so that $S' \neq 0$. Thus, $\deg(aP'Q + bQ'P) \geq 0$. So by taking degrees on both sides of (2) we get $\deg(S') \geq c\deg(R) + (a+b-2)\deg(P)$. By observing that $\deg(S) > \deg(S')$ we obtain the result. □

We also need the following.

Lemma 2.4. *Let $\mathbb{F}$ be a perfect field of characteristic 2. Let $Q \in \mathbb{F}[x]$ be a non-constant polynomial, i.e., $Q \notin \mathbb{F}$. Let $n, m > 0$ be two positive integers. Let $S \in \mathbb{F}[x]$ be defined by*

$$S = 1 + \cdots + Q^n.$$

Then Q does not divide the polynomial $1 + S + \cdots + S^{2m}$.

Proof. The hypothesis implies that $S \equiv 1 \pmod{Q}$. If the conclusion is false then we obtain the contradiction $1 = 2m + 1 \equiv 1 + S + \cdots + S^{2m} \equiv 0 \pmod{Q}$. □

Canaday [2], Lemma 14, claimed but did not prove next lemma. Here we give a short proof.

Lemma 2.5. *Let $P, Q \in \mathbb{F}_2[x]$ be primes. Let m, n be two positive integers. Assume that*

$$\sigma(P^{2m}) = \sigma(Q^{2n}). \tag{3}$$

Then either $\{P, Q\} = \{x, x+1\}$ and $m = n = 1$, or $P = Q$ and $m = n$.

Proof. We may write (3) as

$$\frac{P^{2m+1} + 1}{P + 1} = \frac{Q^{2n+1} + 1}{Q + 1},$$

from which we get either $Q = P$ so that $m = n$, or $P^{2m} \equiv 1 \pmod{Q}$, $Q^{2n} \equiv 1 \pmod{P}$ so that

$$P^m \equiv 1 \pmod{Q}, \qquad Q^n \equiv 1 \pmod{P}. \tag{4}$$

If $Q \mid P + 1$ and $P \mid Q + 1$ then Q and P have the same degree. So Q and $P + 1$ have the same degree. Thus $Q = P + 1$. Moreover, P and $Q = P + 1$ are

primes, so $\{P, Q\} = \{x, x+1\}$ and $m = n = 1$. This establishes the case $\sigma(x^2) = x^2 + x + 1 = \sigma\big((x+1)^2\big)$.

We may then assume that $Q \nmid P + 1$. We have $P \not\equiv 1 \pmod{Q}$. From (4) we get immediately that

$$1 + \cdots + P^{m-1} \equiv 0 \pmod{Q}. \tag{5}$$

But (3) can be also written as

$$(1 + \cdots + P^m)^2 + P(1 + \cdots + P^{m-1})^2 = (1 + \cdots + Q^n)^2 + Q(1 + \cdots + Q^{n-1})^2,$$

from which we get by differentiation relative to x:

$$P'(1 + \cdots + P^{m-1})^2 = Q'(1 + \cdots + Q^{n-1})^2. \tag{6}$$

Thus, using (5) and (6), we get that Q divides

$$1 + \cdots + Q^{n-1},$$

which is impossible. This finishes the proof of the lemma. □

For completeness we give a short proof of the simple but useful fact:

Lemma 2.6. *Let $A \in \mathbb{F}_2[x]$ be an odd perfect polynomial. Then A is a perfect square.*

Proof. Assume on the contrary that A has a primary factor of the form Q^{2m+1} so that for some polynomial $B \in \mathbb{F}_2[x]$ one has

$$A = Q^{2m+1}B, \tag{7}$$

with $\gcd(Q, B) = 1$. From the equality $A = \sigma(A)$ and the multiplicativity of σ we get

$$A = (1 + \cdots + Q^{2m+1})\sigma(B),$$

so that by evaluating both sides in 0 we obtain that

$$A(0) = \big(1 + Q(0) + \cdots + Q(0)^{2m+1}\big)\sigma(B)(0). \tag{8}$$

But from (7) we have $1 = A(0) = Q(0)^{2m+1}B(0)$, i.e., $Q(0) = 1$. So (8) gives a contradiction in $\mathbb{F}_2$:

$$1 = (2m+2)\sigma(B)(0) = 0.$$

This completes the proof of the lemma. □

The following result is [5], Lemma 4.1:

Lemma 2.7. *Let $P, Q \in \mathbb{F}_2[x]$ be two primes of the same degree d. If Q divides $\sigma(P^2)$ then P does not divide $\sigma(Q^2)$.*

The following lemma is the case $p = 2$ of [5], Lemma 2.3, or [4], Lemma 2.5. It improves a result of Beard et al. ([1], Theorem 7):

Lemma 2.8. *Let $A \in \mathbb{F}_2[x]$ be a perfect polynomial. Then the number of monic minimal primes of A, i.e., of prime divisors of minimal degree of A, is even.*

The object of the paper is to prove our main result:

Theorem 2.9. *There are no odd perfect polynomials $A \in \mathbb{F}_2[x]$ with four prime divisors, i.e., of the form $A = P^a Q^b R^c S^d$ where P, Q, R, S are distinct irreducible polynomials of degree > 1 over $\mathbb{F}_2$ and a, b, c, d are positive integers.*

The general strategy of the proof is as follows. Let A be an odd perfect polynomial with $\omega(A) = 4$. From Lemma 2.6 we see that we may assume that for some primes $P, Q, R, S \in \mathbb{F}_2[x]$ and for positive integers a, b, c, d we have

$$A = P^{2a} Q^{2b} R^{2c} S^{2d} = \sigma(A). \tag{9}$$

We shall show that this is impossible. For that purpose put $\delta_1 = \deg(P)$, $\delta_2 = \deg(Q)$, $\delta_3 = \deg(R)$, $\delta_4 = \deg(S)$. We distinguish three main cases according to the possible configurations arising from Lemma 2.8:

Case 1: $1 < \delta_1 = \delta_2 = \delta_3 = \delta_4$.

Case 2: $1 < \delta_1 = \delta_2 < \delta_3 = \delta_4$.

Case 3: $1 < \delta_1 = \delta_2 < \delta_3 < \delta_4$.

Here the order is from the easiest case to more involved ones.

Case 1 reduces quickly to the case $A = P^2 Q^2 R^2 S^2$ that has already been dealt with as a special case of [5], Theorem 5.5.

In Case 2 it is easy to prove that $c = d = 1$, while in Case 3 we obtain immediately that $d = 1$.

We have then, by using the multiplicativity of σ, a system of four equations in the four unknowns P, Q, R, S to consider (see below).

For instance, the first equation of this systems is of the form $\sigma(P^{2a}) = Q^{b_1} R^{c_1} S^{d_1}$, where we discuss the possible values of the exponents. The rest of the proof consists of applying repeatedly Lemma 2.2, of checking that the exponents of the prime divisors are the same for both A and $\sigma(A)$, of checking that the degrees are the same on both sides of each equation of the system, and of using (if necessary and only in Case 3) Lemma 2.3 to get a contradiction. Sometimes the

contradiction is immediate, sometimes it is more involved. The other lemmas and some congruence arguments are also appropriately used to produce contradictions.

We may write the general system to resolve as

$$\sigma(P^{2a}) = Q^{b_1} R^{c_1} S^{d_1}, \tag{10}$$

$$\sigma(Q^{2b}) = P^{a_2} R^{c_2} S^{d_2}, \tag{11}$$

$$\sigma(R^{2c}) = P^{a_3} Q^{b_3} S^{d_3}, \tag{12}$$

$$\sigma(S^{2d}) = P^{a_4} Q^{b_4} R^{c_4}, \tag{13}$$

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

3. List of all cases to consider

Case 1: $1 < \delta_1 = \delta_2 = \delta_3 = \delta_4$.

Case 2: $1 < \delta_1 = \delta_2 < \delta_3 = \delta_4$. That includes:
Case 2A: $d_3 = 0$ and $c_4 = 0$. Subcase $b_1 = a_2 = 0$. Subcase $b_1 = a_2 = 1$.
Case 2B: $c_4 = 1$ and $d_3 = 0$. Subcase $b_1 = 1$ and $a_2 = 1$.
Case 2B: $c_4 = 1$ and $d_3 = 0$. Subcase $b_1 = 1$ and $a_2 = 1$. Sub-Case $b_1 = 1$ and $a_2 = 0$. Subcase $b_1 = 0$ and $a_2 = 1$. Subcase $b_1 = 0$ and $a_2 = 0$.

Case 3: $1 < \delta_1 = \delta_2 < \delta_3 < \delta_4$. That includes:
Case 3A: $d_3 > 0$.
Case 3A11a: $b_1 = 0$, $a_2 = 0$ and $c_2 = 0$. Case 3A11b: $b_1 = 0$, $a_2 = 0$ and $c_2 = 1$.
Case 3A12a: $b_1 = 1$, $a_2 = 1$ and $c_2 = 0$. Case 3A12b: $b_1 = 1$, $a_2 = 1$ and $c_2 = 1$.
Case 3A13a: $b_1 = 0$, $a_2 = 1$ and $c_2 = 0$: Case 1: $a > 1$ Case 2: $a = 1$. Case 3A13b: $b_1 = 0$, $a_2 = 1$ and $c_2 = 1$. Case 3A14a: $b_1 = 1$, $a_2 = 0$ and $c_2 = 0$: Case 1: $c > 1$, Case 2: $c = 1$. Case 3A14b: $b_1 = 1$, $a_2 = 0$ and $c_2 = 1$.
Case 3B: $d_3 = 0$.
Case 3B1a: $b_1 = 0,\ a_2 = 0,\ c_1 = 0,\ c_2 = 0$. Case 3B1b: $b_1 = 0,\ a_2 = 0,\ c_1 = 1,\ c_2 = 1$. Case 3B1c: $b_1 = 0,\ a_2 = 0,\ c_1 = 1,\ c_2 = 0$. Case 3B1d: $b_1 = 0,\ a_2 = 0,\ c_1 = 0,\ c_2 = 1$. Case 3B2a: $b_1 = 1,\ a_2 = 1,\ c_1 = 0,\ c_2 = 0$. Case 3B2b: $b_1 = 1,\ a_2 = 1,\ c_1 = 1,\ c_2 = 1$: Case 1: $c > 1$ Subcase 1: $c > 1$ and $a_3 = 2$, $b_3 = 3$ Subcase 2: $c > 1$ and $a_3 = 3$, $b_3 = 2$ Case 2: $c = 1$.
Case 3B2c: $b_1 = 1,\ a_2 = 1,\ c_1 = 1,\ c_2 = 0$. Case 3B2d: $b_1 = 1,\ a_2 = 1,\ c_1 = 0,\ c_1 = 1$. Case 3B3a: $b_1 = 1,\ a_2 = 0,\ c_1 = 0,\ c_2 = 0$. Case 3B3b: $b_1 = 1,\ a_2 = 0,\ c_1 = 1,\ c_2 = 1$. Case 3B3c: $b_1 = 1,\ a_2 = 0,\ c_1 = 1,\ c_2 = 0$. Case 3B3d: $b_1 = 1,\ a_2 = 0,\ c_1 = 0,\ c_2 = 1$. Case 3B4*: $b_1 = 0,\ a_2 = 1,\ c_1, c_2 \in \{0, 1\}$.

4. Complete details of the solution of some typical cases; the other are similar

4.1. Case 1: $1 < \delta_1 = \delta_2 = \delta_3 = \delta_4$. This is the simplest case. By applying Lemma 2.2 to each of the equations of the system we get immediately that all exponents

$$b_1,\ c_1,\ d_1,\ a_2,\ c_2,\ d_2,\ a_3,\ b_3,\ d_3,\ a_4,\ b_4,\ d_4,$$

are in $\{0, 1\}$. Now we take degrees on both sides of (10) to (13) and divide both sides by $\delta_1 > 0$ to get

$$2 \le 2a = b_1 + c_1 + d_1 \le 3, \qquad 2 \le 2b = a_2 + c_2 + d_2 \le 3,$$
$$2 \le 2c = a_3 + b_3 + d_3 \le 3, \qquad 2 \le 2d = a_4 + b_4 + c_4 \le 3.$$

Thus $a = b = c = d = 1$ and so $A = P^2Q^2R^2S^2$, which is impossible in view of [5], Theorem 5.5.

4.2. Case 3A12a: $b_1 = 1$, $a_2 = 1$ and $c_2 = 0$. Our system is now:

E1: $1 + \cdots + P^{2a} = QR$,

E2: $1 + \cdots + Q^{2b} = PS$,

E3: $1 + \cdots + R^{2c} = P^{a_3}Q^{b_3}S$,

E4: $1 + S + S^2 = P^{a_4}Q^{b_4}R^{c_4}$.

The exponents of P, Q, R on both sides of $\sigma(A) = A$ are the same so that $2a = 1 + a_3 + a_4$, $2b = 1 + b_3 + b_4$, $c_4 = 2c - 1$. By comparing degrees on both sides of the first three equations we obtain that $\delta_3 = (2a - 1)\delta_1$, $\delta_4 = (2b - 1)\delta_1$ and $\delta_4 = \big(4ac - 2c - (a_3 + b_3)\big)\delta_1$. Hence

$$a_3 + b_3 = 4ac - 2c - 2b + 1,$$

from which it follows that

$$a_4 + b_4 = 2a + 4b + 2c - 4ac - 3.$$

Observe in particular that $\delta_4 > \delta_3$ is equivalent to $b > a$.

Now $c_4 = 2c - 1$ is odd, thus, by using Lemma 2.3(d) in E4, we get

$$\delta_4 > (2c - 2)\delta_3 + (a_4 + b_4 - 2)\delta_1.$$

Using the values of $\delta_3 = (2a - 1)\delta_1$ and $\delta_4 = (2b - 1)\delta_1$ yield

$$2b - 1 > 2(c - 1)(2a - 1) + (a_4 + b_4 - 2).$$

So, after some computation, we finally obtain that

$$0 > b - a - 1,$$

that is, $b \leq a$, which contradicts $\delta_4 > \delta_3$.

4.3. Case 3A13a: $b_1 = 0$, $a_2 = 1$ and $c_2 = 0$. The first and the third equations of our system are

E1: $1 + \cdots + P^{2a} = R$,

E3: $1 + \cdots + R^{2c} = P^{a_3} Q^{b_3} S$.

First observe that by Lemma 2.4 applied to E1 and E3 we have $a_3 = 0$.
So our system becomes:

E1: $1 + \cdots + P^{2a} = R$,

E2: $1 + \cdots + Q^{2b} = PS$,

E3: $1 + \cdots + R^{2c} = Q^{b_3} S$,

E4: $1 + S + S^2 = P^{a_4} Q^{b_4} R^{c_4}$.

The exponents of P, Q, R on both sides of $\sigma(A) = A$ are the same so that $2a = 1 + a_4$, $2b = b_3 + b_4$, $c_4 = 2c - 1$. By comparing degrees on both sides of the first three equations we get $\delta_3 = 2a\delta_1$, $\delta_4 = (2b - 1)\delta_1$ and $\delta_4 = (4ac - b_3)\delta_1$. This implies that

$$b_3 = 4ac - 2b + 1 \quad \text{and} \quad b_4 = 4b - 4ac - 1.$$

Since c_4 is odd, by applying Lemma 2.3 (c) to E4 we get

$$\delta_4 > 2(c - 1)\delta_3 + (a_4 + b_4 - 2)\delta_1$$

and so $2b - 1 > 4ac - 4a + (a_4 + b_4 - 2)$. This leads to

$$3 > 2b - 2a.$$

But $\delta_4 > \delta_3$ is equivalent here to $2b - 2a > 1$. Thus,

$$b = a + 1.$$

Hence

$$b_4 = 4a - 4ac + 3$$

is odd and so $b_4 \geq 1$. This is equivalent to

$$c \leq 1 + \frac{1}{2a} \leq \frac{3}{2}.$$

Thus $c = 1$. One has then $b_4 = 3$, $b_3 = 2a - 1$, $a_4 = 2a - 1$ and $c_4 = 1$. So our system becomes

E1: $1 + \cdots + P^{2a} = R$,

E2: $1 + \cdots + Q^{2a+2} = PS$,

E3: $1 + R + R^2 = Q^{2a-1}S$,

E4: $1 + S + S^2 = P^{2a-1}Q^3R$.

We consider two cases:

4.3.1. Case 1: $a > 1$. By differentiation of E3 we get

$$R' = Q^{2a-2}(Q'S + QS').$$

Differentiation of E1 leads to

$$R' = (1 + \cdots + P^{a-1})^2 P'.$$

Thus

$$(1 + \cdots + P^{a-1})^2 P' = Q^{2a-2}(Q'S + QS'). \tag{14}$$

Recall that $\deg(P) = \deg(Q)$ so that $\deg(Q) > \deg(P')$. Thus, $\gcd(Q, P') = 1$ and so

$$1 + \cdots + P^{a-1} = Q^{a-1}M \tag{15}$$

for some polynomial $M \in \mathbb{F}_2[x]$. If a is odd then by Lemma 2.2 we get $a \in \{1, 2\}$. But $a > 1$, hence $a = 2$, which is impossible.

Thus a is even. Let us write the equation above in the form

$$1 + P^a = (1 + P)Q^{a-1}M. \tag{16}$$

By differentiation of (16) followed by division of both sides by Q^{a-2} we get

$$0 = P'QM + (1 + P)(Q'M + QM').$$

Reducing modulo Q we obtain that

$$0 \equiv (1+P)Q'M \pmod{Q}.$$

Observe that $\gcd\big(Q,(1+P)Q'\big)=1$, so that

$$Q \mid M.$$

Thus, we obtain from (15) that

$$Q^a \mid 1+\cdots+P^{a-1}.$$

So, from (14) we get

$$Q^{2a} \mid Q^{2a-2}(Q'S+QS').$$

If follows that

$$Q^2 \mid Q'S+QS'.$$

But $\gcd(Q,Q')=1$, hence

$$Q \mid S,$$

which is impossible since S and Q are primes and $\deg(S)=\delta_4>\delta_1=\deg(Q)$.

4.3.2. Case 2: $a=1$. Here our system is

E1: $1+P+P^2=R$,

E2: $1+Q+Q^2+Q^3+Q^4=PS$,

E3: $1+R+R^2=QS$,

E4: $1+S+S^2=PQ^3R$.

From E3 and E1 we have

$$QS=1+P+P^4,$$

so that

$$Q^3S^3 \equiv 1 \pmod{P}.$$

From E4 we get

$$S^3 \equiv 1 \pmod{P}.$$

Thus,

$$Q^3 \equiv 1 \pmod{P}.$$

But from E2 it follows that

$$Q^5 \equiv 1 \pmod{P}.$$

Thus,

$$Q^2 \equiv 1 \pmod{P}.$$

But this means that P divides $(1+Q)^2$. Recall that the irreducible polynomials P, Q satisfy $\deg(P) = \deg(Q) > 1$. Therefore, P divides $1+Q$. So $P = 1+Q$, which is impossible.

4.4. Case 3B2b: $b_1 = 1$, $a_2 = 1$, $c_1 = 1$, $c_2 = 1$. The system becomes

E1: $1 + \cdots + P^{2a} = QRS$,

E2: $1 + \cdots + Q^{2b} = PRS$,

E3: $1 + \cdots + R^{2c} = P^{a_3} Q^{b_3}$,

E4: $1 + S + S^2 = P^{a_4} Q^{b_4} R^{c_4}$.

The exponents of P, Q, R on both sides of $\sigma(A) = A$ are the same so that $2a = 1 + a_3 + a_4$, $2b = 1 + b_3 + b_4$, $c_4 = 2c - 2$. From E1, E2 we get immediately by taking degrees that $b = a$. By comparing degrees on both sides of the equations E1 and E3 we obtain that $\delta_4 + \delta_3 = (2a-1)\delta_1$, $2c\delta_3 = (a_3 + b_3)\delta_1$. Thus

$$a_3 + b_3 + a_4 + b_4 = 4a - 2.$$

Since c_4 is even we use Lemma 2.3(b) in E4 to get

$$\delta_4 > (2c-2)\delta_3 + (a_4 + b_4 - 2)\delta_1.$$

In other words,

$$\delta_4 > (a_3 + b_3 + a_4 + b_4 - 2)\delta_1 - 2\delta_3,$$

that is,

$$(2a-1)\delta_1 - \delta_3 > (4a-4)\delta_1 - 2\delta_3.$$

This becomes

$$\delta_3 > (2a-3)\delta_1,$$

and so

$$\delta_3 > (2a-1)\delta_1 - 2\delta_1 = \delta_3 + \delta_4 - 2\delta_1.$$

Hence

$$\delta_4 < 2\delta_1.$$

Since $\delta_4 > \delta_3$ we obtain that

$$2\delta_1 > \delta_3 > (2a-3)\delta_1.$$

Thus, $a \in \{1,2\}$. If $a=1$ we get $\delta_1 = (2a-1)\delta_1 = \delta_3 + \delta_4 > \delta_3$, which is a contradiction. Thus, $a=2$. This implies that $a_3 + a_4 = 3$, and also $b_3 + b_4 = 3$.

4.4.1. Case 1: $c > 1$. Since $c \geq 2$ and $\delta_3 > \delta_1$, we have

$$4\delta_1 \leq 2c\delta_1 < 2c\delta_3 = (a_3 + b_3)\delta_1$$

and also $b_3 \leq 3$, so that

$$4 < a_3 + b_3 \leq a_3 + 3.$$

Thus, $a_3 \in \{2,3\}$. Observe that $a_3 = 2$ implies $b_3 = 3$ and that $a_3 = 3$ implies $b_3 > 1$. Moreover, note also that

$$2 \leq c < \frac{a_3 + b_3}{2} \leq 3,$$

so we get $c = 2$.

Now $\delta_4 > \delta_3$ is equivalent to $3\delta_1 - \delta_3 > \delta_3$, so

$$6\delta_1 > 4\delta_3 = (a_3 + b_3)\delta_1.$$

It follows that

$$4 < a_3 + b_3 < 6,$$

and hence

$$a_3 + b_3 = 5.$$

It remains to consider two subcases:

4.4.2. Subcase 1: $c > 1$ and $a_3 = 2$, $b_3 = 3$. One has $c = 2$, we have also $b = a = 2$ and $a_4 = 1$, $b_4 = 0$. Thus our system becomes

E1: $1 + \cdots + P^4 = QRS$,

E2: $1 + \cdots + Q^4 = PRS$,

E3: $1 + \cdots + R^4 = P^2Q^3$,

E4: $1 + S + S^2 = PR^2$.

One has:

$$\delta_3 + \delta_4 = (2a - 1)\delta_1 = 3\delta_1,$$

and from E4 we get

$$\delta_3 - \delta_4 = -\frac{1}{2}\delta_1.$$

Thus

$$\delta_3 = \frac{5}{4}\delta_1, \qquad \delta_4 = \frac{7}{4}\delta_1.$$

By applying Lemma 2.3(b) in E4 (or Lemma 2.2) we get

$$\delta_4 > 2\delta_3.$$

Thus we arrive at the contradiction

$$7 > 10.$$

4.4.3. Subcase 2: $c > 1$ and $a_3 = 3$, $b_3 = 2$. This is the same as Case 1, by permuting P and Q.

4.4.4. Case 2: $c = 1$. Observe that $\delta_4 > \delta_3$ is equivalent to $3\delta_1 - \delta_3 > \delta_3$. Thus

$$3\delta_1 > 2\delta_3 = (a_3 + b_3)\delta_1.$$

Thus,

$$a_3 + b_3 < 3.$$

But we have also

$$2\delta_3 = (a_3 + b_3)\delta_1 > 2\delta_1.$$

Therefore we get the contradiction

$$2 < a_3 + b_3 < 3.$$

This finishes the proof of the theorem.

References

[1] 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

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

[3] L. Gallardo and O. Rahavandrainy, On perfect polynomials over $\mathbb{F}_4$. *Port. Math.* (*N.S.*) **62** (2005), 109–122. Zbl 1131.11079 MR 2126875

[4] 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 05225688 MR 2298110

[5] 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

[6] R. K. Guy, *Unsolved problems in number theory*. 3rd ed., Problem Books in Mathematics, Springer-Verlag, New York 2004. Zbl 1058.11001 MR 2076335

[7] J. J. Sylvester, Sur l'impossibilité de l'existence d'un nombre parfait impair qui ne contient pas au moins 5 diviseurs premiers distincts. *C. R. Acad. Sci. Paris* **106** (1888), 522–526. JFM 20.0173.04

Received March 4, 2008; revised May 4, 2008

L. H. Gallardo, Department of Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest, France

E-mail: Luis.Gallardo@univ-brest.fr

O. Rahavandrainy, Department of Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest, France

E-mail: Olivier.Rahavandrainy@univ-brest.fr