International Journal of Pure and Applied Mathematics
Volume 52 No. 2 2009, 301-314

EVEN PERFECT POLYNOMIALS OVER $\mathbb{F}_2$ WITH FOUR PRIME FACTORS

Luis H. Gallardo[1 §], Olivier Rahavandrainy[2]
[1,2]Department of Mathematics
University of Brest
U.M.R. 6205, CNRS
6, Avenue Le Gorgeu, C.S. 93837,
Brest Cedex 3, 29238, FRANCE
[1]e-mail: luisgall@univ-brest.fr
[2]e-mail: rahavand@univ-brest.fr

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 $\gcd(A, x^2 - x) \neq 1$ then we call A even. The list of all even perfect polynomials over $\mathbb{F}_2$ with at most 3 prime factors in known. The object of this paper is to give the list of all even perfect polynomials over $\mathbb{F}_2$ with four prime factors. These are all the known perfect polynomials with four prime factors over $\mathbb{F}_2$.

AMS Subject Classification: 11T55, 11T06
Key Words: sum of divisors, polynomials, finite fields, characteristic 2

1. Introduction

As usual, we denote by $\mathbb{F}_2$ the finite field with two elements $\{0, 1\}$. For a polynomial $A \in \mathbb{F}_2[x]$, let $\sigma(A) = \sum_{D|A} D$ be the sum of divisors of A. We denote also, as usual, by $\omega(A)$ the number of distinct prime (irreducible) polynomials that divide A. These two functions are multiplicative, a fact that we shall use without more reference in the rest of the paper. If $\sigma(A) = A$, then we call A a perfect polynomial.

Received: March 29, 2009

§Correspondence author

The notion of perfect polynomial (over $\mathbb{F}_2$) was introduced by Canaday [1], the first doctoral student of Leonard Carlitz. He studied mainly the case in which $\gcd(A, x^2+x) \neq 1$.

We may think $x^2+x \in \mathbb{F}_2[x]$ as being the analogue of $2 \in \mathbb{Z}$ so that the "even" polynomials are the polynomials with linear factors and the "odd" ones are such that $\gcd(A, x^2+x) = 1$. Canaday (among other results in [1]) classifies the even perfect polynomials with three irreducible factors and gives without proof [1, Theorem 11] the list of all even perfect polynomials A with $\omega(A) = 4$.

The object of this paper (see Theorem 2.10) is to prove Canaday's results in [1, Theorem 11]: The following polynomials are the only even perfect polynomials $A \in \mathbb{F}_2[x]$ with $\omega(A) = 4$ prime factors:

$$C_1(x) = x^2(x+1)(x^2+x+1)^2(x^4+x+1),\ C_2(x) = C_1(x+1),$$
$$C_3(x) = C_3(x+1) = x^4(x+1)^4(x^4+x^3+x^2+x+1)(x^4+x^3+1),$$
$$C_4(x) = x^6(x+1)^3(x^3+x^2+1)(x^3+x+1),\ C_5(x) = C_4(x+1).$$

Observe that the two latter polynomials are also perfect over $\mathbb{F}_4$ (see [4]).

The complete list of all even perfect polynomials over $\mathbb{F}_2$ with $\omega(A) \leq 4$ is then:

$$0, 1,\ \ (x^2+x)^{2^n-1},\ \ T_1(x) = x^2(x+1)(x^2+x+1),\ \ T_1(x+1),$$
$$T_2(x) = x^3(x+1)^4(x^4+x^3+1),\ \ T_2(x+1),\ \ C_1(x), \ldots, C_5(x),$$

in which $n > 0$ is a positive integer.

In fact this list is the list of all perfect polynomials over $\mathbb{F}_2$ with $\omega(A) \leq 4$. (see [6]).

There are only two more known perfect polynomials over $\mathbb{F}_2$, both even, with $\omega(A) = 5$ and with degree 20, namely:

$$S_1(x) = x^6(x+1)^4(x^3+x+1)(x^3+x^2+1)(x^4+x^3+1),\ \ S_1(x+1).$$

It may have some interest to know whether or not there are perfect polynomials over $\mathbb{F}_2$ with degree moderately bigger that 20 (so that we may compute them with a computer). These have been investigated in [5, Theorem 5.5] (no solutions up to degree 28) in the special case in which all exponents are equal to 2 and the polynomial is odd.

2. Some Useful Facts

We denote, as usual by $\mathbb{N}$ the set of nonnegative integers. In this section we recall, and we present, some necessary results for the next sections.

First of all, we recall some definitions and lemmata.

Definitions. – We define (following Canaday's terminology) as the inverse of a polynomial $P(x)$ of degree m, the polynomial $P^*(x) = x^m P(\frac{1}{x})$.

– We say that P inverts into itself if $P = P^*$.

– A polynomial P is complete if there exists $h \in \mathbb{N}$ such that:

$$P = \sigma(x^h) = 1 + x + \cdots + x^h.$$

The following lemma essentially based on a result of Dickson (see the proof of [1, Lemma 2]) is key.

Lemma 2.1. *i) Let $P \in \mathbb{F}_2[x]$ be such that $P(0) = 1$. We have: $(P^*)^* = P$.*

ii) Any complete polynomial inverts into itself.

iii) If $1 + x + \cdots + x^m = PQ$, where P, Q are irreducible, then either $(P = P^*, Q = Q^*)$ or $(P = Q^*, Q = P^*)$.

iv) If $P = P^*$, P irreducible and if $P = x^a(x+1)^b + 1$, then:

$$P \in \{1 + x + x^2, 1 + x + \cdots + x^4\}.$$

Proof. i) and ii) are obvious.

iii) follows by ii).

iv) is the corollary of Lemma 7 in [1] (that follows from Lemma 2 of ibid.).

Lemma 2.2. *If $A(x)$ is a perfect polynomial over $\mathbb{F}_2$, then $A(x+1)$ is also perfect.*

Lemma 2.3. (see Lemma 5 in [1]) *Let $P, Q \in \mathbb{F}_2[x]$ and $n, m \in \mathbb{N}$ such that P is irreducible and $\sigma(P^{2n}) = 1 + \cdots + P^{2n} = Q^m$. Then $m \in \{0, 1\}$.*

Lemma 2.4. (see Lemma 6 in [1]) *Let $P, Q \in \mathbb{F}_2[x]$ and $n, m \in \mathbb{N}$ such that P is irreducible and $\sigma(P^{2n}) = 1 + \cdots + P^{2n} = Q^m A,\ m > 1$. If m is odd (resp. even) then $deg(P) > (m-1)deg(Q)$ (resp. $deg(P) > m\ deg(Q)$).*

Lemma 2.5. (see Lemma 4 in [1]) *If $PQ = 1 + \cdots + x^{2h}$ and $P = 1 + \cdots + (x+1)^{2k}$, then $h = 4$ and $k = 1$; that is: $P = 1 + x + x^2$, $Q = P(x^3) = 1 + x^3 + x^6$.*

The proof of the following lemma in [1] uses the properties i) to iii) in Lemma 2.1.

Lemma 2.6. (see Theorem 8 in [1]) *Let $A = 1 + \cdots + x^{2h} \in \mathbb{F}_2[x]$ such that any irreducible factor of A is of the form $x^a(x+1)^b + 1$. Then $h \in \{1, 2, 3\}$.*

The following crucial lemma follows from Lemma 2.5 in [4] that says that the number of minimal primes dividing a perfect polynomial is even.

Lemma 2.7. *Every even perfect polynomial A over $\mathbb{F}_2$ with $\omega(A) = 4$, is of the form $x^h(x+1)^k P^l Q^m$, for some odd prime polynomials P, Q and for some positive integers h, k, l, m.*

We provide proofs of the following two lemmata claimed but not proved by Canaday.

Lemma 2.8. (see Lemma 10 in [1]) *Let $P \neq Q$ be two odd polynomials in $\mathbb{F}_2[x]$. If $x^h(x+1)^k P^l Q^{2n-1}$ is a perfect polynomial over $\mathbb{F}_2$, and if $l \neq 2^r - 1$, then $2n - 1 = 2^s - 1$.*

Proof. If $l \neq 2^r - 1$ and $2n - 1 \neq 2^s - 1$, then put:

$$2n - 1 = 2^s u - 1, \text{ where } u \geq 3 \text{ is odd.}$$

We can write:

$$1 + \cdots + Q^{2n-1} = (Q+1)^{2^s-1}(1 + \cdots + Q^{u-1})^{2^s}.$$

Since $u - 1 \geq 2$ is even, we have by Lemma 2.3:

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

So,

$$\deg(Q) < \deg(P).$$

If l is even, then by the same argument, $\deg(Q) < \deg(P)$. It is impossible. So l is odd. We can write:

$l = 2^r v - 1,\ 1 + \cdots + P^l = (P+1)^{2^r-1}(1 + \cdots + P^{v-1})^{2^r},$ where $v \geq 3$ is odd.

Since $v - 1 \geq 2$ is even, we have by Lemma 2.3:

$$1 + \cdots + P^{v-1} = Q.$$

So,

$$\deg(P) < \deg(Q).$$

It is impossible. □

Lemma 2.9. (see Lemma 11 in [1]) *Let $P \neq Q$ be two odd polynomials in $\mathbb{F}_2[x]$. If $x^h(x+1)^k P^{2l} Q^{2n-1}$ is a perfect polynomial over $\mathbb{F}_2$, then $2l = 2^m$ and $m = n$.*

Proof. We can write:

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

So, P divides $Q + 1$ and P^2 does not. Thus,

$$Q + 1 = x^a(x+1)^b P, \text{ for some } a, b \in \mathbb{N}.$$

Since $\sigma(A) = A$, we obtain:
$(1+\cdots+x^h)(1+\cdots+(x+1)^k)(x^a(x+1)^b)^{2^n-1}P^{2^n-1}Q = x^h(x+1)^kP^{2l}Q^{2^n-1}$.

If h and k are even, then by Lemma 2.3:

$$(1+\cdots+x^h)(1+\cdots+(x+1)^k) = P^\alpha Q^\beta, \quad 0 \le \alpha, \beta \le 2.$$

Therefore, we must have:

$$\alpha = 1.$$

We are done.

If h and k are both odd, then by considering exponents of P, we see that it is impossible.

If h is even and k odd, then by considering exponents of Q, we must have:

$$1+\cdots+x^h = P.$$

Put:

$$k+1 = 2^r u, \text{ where } u \text{ is odd.}$$

We have:
$1+\cdots+(x+1)^k = x^{2^r-1}(1+\cdots+(x+1)^{u-1})^{2^r} = x^{2^r-1}(P^\gamma Q^\delta)^{2^r},\ 0 \le \gamma, \delta \le 1.$
If $\gamma = 0$, then we are done.

If $\gamma = 1$ and $\delta = 0$, then $u - 1 \ge 2$ and $n = 1$. Thus, by considering exponents of P, we get:

$$l - 1 = 2^{r-1}.$$

Furthermore, we can write:

$$Q + 1 = P + \cdots + P^{2l} = P(1+P)(1+\cdots+P^{l-1})^2.$$

So, l must be equal to 2, and then $r = 1$, $a = 3$, $h = 4$.

Thus:
$P = 1+\cdots+x^4,\ Q = 1+\cdots+P^4 = (1+x+x^4)(1+x+x^2+x^4+x^6+x^7+x^8+x^9+x^{12}.$
It is impossible since Q is irreducible.

If $\gamma = \delta = 1$, then by Lemma 2.5, $\deg(P) = 2$ and $\deg(Q) = 6$. It is impossible since $Q = 1 + \cdots + P^{2l}$.

If h is odd and k even – analogous proof. □

In the next section we prove our main result:

Theorem 2.10. *The complete list of even perfect polynomials over* $\mathbb{F}_2$ *with* 4 *prime factors consists of the five polynomials* $C_1(x), \ldots, C_5(x)$.

3. Perfects of the Forms: $A = x^h(x+1)^k P^m Q^n$

We may reduce (see Lemmata 2.8 and 2.9) our study to the following cases:

(a) $A = x^h(x+1)^k P^{2m} Q^{2n}$.

(b) $A = x^h(x+1)^k P^{2^n} Q^{2^n-1}$. (c) $A = x^{2h}(x+1)^{2k} P^{2m-1} Q^{2^n-1}$.

(d) $A = x^{2h}(x+1)^{2k-1} P^{2m-1} Q^{2^n-1}$.

(e) $A = x^{2h-1}(x+1)^{2k-1} P^{2m-1} Q^{2^n-1}$.

Compare with [1, p. 733].

Case (a). Since x and $x+1$ do not divide $\sigma(P^{2m})$, we obtain by Lemma 2.3:

$$\sigma(P^{2m}) = 1 + \cdots + P^{2m} = Q.$$

Analogously,

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

Therefore, considering degrees, we have:

$$4mn = 1,$$

which is impossible.

Case (e). Since $\sigma(A) = A$, we obtain: $x(x+1)(P+1)(Q+1)B^2 = x^{2h-1}(x+1)^{2k-1} P^{2m-1} Q^{2^n-1}$, for some polynomial B. It follows that P (respectively Q) must divide $Q+1$ (resp. $P+1$). So $P = Q+1$, which is impossible.

Case (b). We obtain: $1 + \cdots + P^{2^n} = Q$, by Lemma 2.3, and since $x,\ x+1$ do not divide $\sigma(P^{2^n})$, $1 + \cdots + Q^{2^n-1} = (Q+1)^{2^n-1}$. Thus, P divides $Q+1$ and P^2 does not. So, Q does not divide $P+1$. We may write:

$$\begin{aligned} Q + 1 &= P(1+P)^{2^n-1}, \\ P + 1 &= x^\alpha (x+1)^\beta,\ \alpha, \beta \geq 1\,. \end{aligned}$$

Case h, k even. The two monomials x and $x+1$ do not divide $\sigma(x^h), \sigma((x+1)^k)$. So:

$$\begin{aligned} 1 + \cdots + x^h &= P^{a_0} Q^{b_0},\ a_0, b_0 \in \{0,1\}, \\ 1 + \cdots + (x+1)^k &= P^{a_1} Q^{b_1},\ a_1, b_1 \in \{0,1\}. \end{aligned}$$

Since $\sigma(A) = A$, we obtain:

$$\begin{aligned} Q(Q+1)^{2^n-1} P^l Q^r &= x^h (x+1)^k P^{2^n} Q^{2^n-1}, \\ l = a_0 + a_1,\ r &= b_0 + b_1,\ l, r \in \{0,1,2\}. \end{aligned}$$

Considering the exponents of P and Q, we have:

$$2^n - 1 + l = 2^n,\ r + 1 = 2^n - 1.$$

So,

$$l = 1,\ n \in \{1, 2\}.$$

(i) Case $n = 1$. We have:

$r = 0,\ 1 + P + P^2 = Q,\ 1 + \cdots + x^h = P = 1 + \cdots + (x + 1)^k,\ h = k.$

Since $P = x^\alpha(x + 1)^\beta + 1$, by Lemma 2.6, $P \in \{1 + x + x^2, 1 + \cdots + x^4\}$.

– If $P = 1+x+x^2$, then $h = k = 2,\ Q = 1+x+x^4$. Thus $A = x^2(x+1)^2P^2Q$ which is not perfect.

– If $P = 1+\cdots+x^4$, then $Q = 1+P+P^2 = (1+x+x^2)(1+x^2+x^4+x^5+x^6)$ is reducible. It is impossible.

(ii) Case $n = 2$. We have:

$$\begin{aligned} &r = 2,\ 1 + \cdots + P^4 = Q,\\ &1 + \cdots + x^h = PQ,\\ &1 + \cdots + (x + 1)^k = Q. \end{aligned}$$

By Lemma 2.5, we have:

$$h = 8,\ k = 2,\ Q = 1 + x + x^2,\ P = 1 + x^3 + x^6.$$

So, $Q \neq 1 + \cdots + P^4$. It is impossible.

Case h, k odd. Since $\sigma(A) = A$, we obtain:

$$x(x + 1)Q(Q + 1)^{2^n-1}B^2 = x^h(x + 1)^k P^{2^n} Q^{2^n-1}. \tag{1}$$

Since P divides $Q + 1$ and P^2 does not, by considering the exponent of P, we see that the equality (1) is impossible.

Case h odd, k even. Put $h = 2l - 1$ and $k = 2r$.

By Lemma 2.4, we have:

$1 + \cdots + (x + 1)^k = 1 + \cdots + (x + 1)^{2r} = P^aQ^b,$ for some $a, b \in \{0, 1\}$.

Since $\sigma(A) = A$, we obtain:

$(x + 1)(1 + \cdots + x^{l-1})^2Q(Q + 1)^{2^n-1}P^aQ^b = x^{2l-1}(x + 1)^{2r}P^{2^n}Q^{2^n-1}.$

Since P divides $Q+1$ and P^2 does not, if $b = 1$ (resp. $a = 0$), then the exponent of Q (resp. of P) in the right hand side is even (resp. odd). It is impossible. So, $b = 0$ and $a = 1$. Therefore:

$$P = 1 + \cdots + (x + 1)^{2r} = x^\alpha(x + 1)^\beta + 1.$$

By Lemma 2.6, $P \in \{1 + x + x^2, 1 + x^3 + x^4\}$.

(i) Case $P = 1 + x + x^2$. We have $k = 2r = 2$, and by considering the exponent of $x + 1$ we get:

$$n = 1,\ Q = 1 + P + P^2 = 1 + x + x^4.$$

So,

$$l = 1,\ h = 1.$$

We obtain the polynomial $C_1(x)$, and by Lemma 2.2, we get the polynomial $C_1(x+1)$.

(ii) Case $P = 1 + x^3 + x^4$. We have:

$$2r = 4,\ Q + 1 = (1+P)^{2^n-1}P = x^{3(2^n-1)}(x+1)^{2^n-1}P.$$

By considering the exponent of $x+1$, we have:

$$(2^n-1)^2 + 1 \leq 4\,.$$

So,

$$n = 1,$$

and

$$Q = 1 + P + P^2 = 1 + x^3 + x^4 + x^6 + x^8 = (1 + x + x^2)(1 + x + x^4 + x^5 + x^6).$$

It is impossible.

Case (c). By Lemma 2.4, we obtain:

$$\begin{aligned} &1 + \cdots + x^{2h} = P^{a_0}Q^{b_0},\\ &1 + \cdots + (x+1)^{2k} = P^{a_1}Q^{b_1},\\ &a_0, b_0, a_1, b_1 \in \{0, 1\}. \end{aligned}$$

Since $\sigma(A) = A$, we obtain:

$$(P+1)(Q+1)^{2^n-1}P^{a_0+a_1}Q^{b_0+b_1}(1 + \cdots + P^{m-1})^2 = x^{2h}(x+1)^{2k}P^{2m-1}Q^{2^n-1}.$$

Thus:

$$\begin{aligned} &1 + P = x^{\alpha_1}(x+1)^{\beta_1}Q^{\gamma_1},\\ &1 + Q = x^{\alpha_2}(x+1)^{\beta_2}P^{\gamma_2},\\ &\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2 \in \mathbb{N}. \end{aligned}$$

We can reduce the work to three cases, since the integers h and k play symmetric roles (by Lemma 2.2).

Case $a_0 = b_0 = b_1 = 1, a_1 = 0$. We have:

$$\begin{aligned} &1 + \cdots + x^{2h} = PQ,\\ &1 + \cdots + (x+1)^{2k} = Q. \end{aligned}$$

So, by Lemma 2.5, we obtain:

$$Q = 1 + x + x^2,\ P = 1 + x^3 + x^6,\ h = 4,\ k = 1.$$

Since $\sigma(A) = A$, by considering the exponent of $x+1$, we obtain:

$$n = 1,$$

and thus:

$$x^4(x+1)^2PQ^3(1+\cdots+P^{m-1})^2 = x^8(x+1)^2P^{2m-1}Q.$$

Thus, x must divide $B = 1+\cdots+P^{m-1}$. So, $x+1$ must divide B. It is impossible.

Case $a_0 = b_0 = a_1 = 1, b_1 = 0$. We have:

$$1+\cdots+x^{2h} = PQ,$$
$$1+\cdots+(x+1)^{2k} = P.$$

So, by Lemma 2.5, we obtain:

$$P = 1+x+x^2,\ Q = 1+x^3+x^6,\ h = 4,\ k = 1.$$

We obtain the same contradiction as in the previous case.

Case $a_0 = b_1 = 1, a_1 = b_0 = 0$. We have:

$$1+\cdots+x^{2h} = P,$$
$$1+\cdots+(x+1)^{2k} = Q\,.$$

Therefore, the monomials $x,\ x+1$ divide $P+1$ and $Q+1$. But x^2 (resp. $(x+1)^2$) does not divide $P+1$ (resp. $Q+1$).

Since $\sigma(A) = A$, we have:

$$PQ(P+1)(Q+1)^{2^n-1}(1+\cdots+P^{m-1})^2 = x^{2h}(x+1)^{2k}P^{2m-1}Q^{2^n-1}\,. \quad (2)$$

(i) Case $\gamma_1 = \gamma_2 = 0$. In this case, P does not divide $Q+1$ and Q does not divide $P+1$.

We obtain:

$$P+1 = x(x+1)^{\beta_1},\ Q+1 = x^{\alpha_2}(x+1).$$

Therefore, by relation (2):

$$m = 1 \text{ and } n = 1.$$

So, by Lemma 2.6:

$$P \in \{1+x+x^2, 1+\cdots+x^4\},\ Q \in \{1+x+x^2, 1+x^3+x^4\}.$$

We must have:

$$P = 1+\cdots+x^4,\ Q = 1+x^3+x^4.$$

So,

$$h = k = 2.$$

We get the polynomial $C_3(x)$, and thus the polynomial $C_3(x+1) = C_3(x)$.

(ii) Case $\gamma_1 = 0,\ \gamma_2 \geq 1$. The polynomial P divides $Q+1$, and by relation (2), the integer γ_2 must be even. So:

$$Q+1 = x^{\alpha_2}(x+1)P^{2u},\ u \geq 1.$$

In particular, P^2 divides $Q+1$.

Furthermore, Q does not divide $P+1$. So,

$$P = x(x+1)^{\beta_1} + 1.$$

So, by Lemma 2.6, $P \in \{1+x+x^2, 1+\cdots+x^4\}$.

– If $P = 1+x+x^2$, then $2h = 2,\ n = 1$ and $\alpha_2 = 1$ (consider the exponents of x in the relation (2)). We can write:

$$Q+1 = x(x+1)P^{2u}.$$

By considering the exponent of P, we have:

$$u = m-1\,,$$

and thus:

$$m \geq 2.$$

Moreover, the relation (2) becomes:

$$(1+\cdots+P^{m-1})^2 = (x+1)^{2k-2}.$$

So,

$$k = 1,\ m = 1.$$

It is impossible.

– If $P = 1+\cdots+x^4$, then $2h = 4$.

We can write:

$$Q+1 = x^{\alpha_2}(x+1)P^{2u},\ \text{where } \alpha_2 \text{ is odd and } u \geq 1.$$

By considering the exponent of x in relation (2), we have:

$$\text{either } (n=2,\ \alpha_2 = 1) \text{ or } (n = 1,\ \alpha_2 \in \{1,3\}).$$

Case $n = 2,\ \alpha_2 = 1$. By considering the exponent of P, we have:

$$m = 3u+1 \geq 4.$$

Moreover, we must have:

$$1+\cdots+P^{m-1} = (x+1)^{k-3}Q.$$

So,

$$k = 3,\ 1+\cdots+P^{m-1} = Q.$$

Thus, P^2 does not divide $Q+1$. It is impossible.

Case $n = 1$. By considering the exponent of P, we have:

$$u = m-1 \geq 1.$$

Moreover, we must have:

$$(1+\cdots+P^{m-1})^2 = x^{4-\alpha_2-1}(x+1)^{2k-4}.$$

Thus, $m-1$ is odd, $\alpha_2 = 1$.

By writing:

$$1 + \cdots + P^{m-1} = (1+P)(1+\cdots+P^{m/2-1})^2.$$

We must have: $m = 2$, $u = 1$, and $k = 5$. So,

$$Q = 1 + \cdots + (x+1)^{10} = 1 + x + x^2 + x^7 + x^8 + x^9 + x^{10},$$
$$Q + 1 = x(x+1)P^2 = x(x+1)(1+\cdots+x^4)^2 = x + \cdots + x^{10}.$$

It is impossible.

(iii) Case $\gamma_1 \geq 1,\ \gamma_2 = 0$. In this case, P does not divide $Q+1$, and Q divides $P+1$.

So,

$$Q = x^{\alpha_2}(x+1) + 1.$$

So, by Lemma 2.6:

$$Q \in \{1 + x + x^2, 1 + x^3 + x^4\}.$$

Therefore, by relation (2):

$$m = 1.$$

So:

$$(P+1)(Q+1)^{2^n-1} = x^{2h}(x+1)^{2k}Q^{2^n-2}.$$

– If $Q = 1 + x + x^2$, then $k = 1$, $\gamma_1 = 2u = 2^n - 2$ is even, and β_1 is odd. We can write:

$$P + 1 = x(x+1)^{\beta_1}Q^{\gamma_1},\ \gamma_1 = 2u \geq 2.$$

Considering the exponent of $x+1$, we have:

$$2 = 2^n - 1 + \beta_1.$$

So:

$$n = \beta_1 = 1.$$

Thus:

$$\gamma_1 = 2^n - 2 = 0.$$

It is impossible.

– If $Q = 1 + x^3 + x^4$, then

$$2k = 4 = 2^n - 1 + \beta_1.$$

So:

$$\text{either } (n = 1,\ \beta_1 = 3) \text{ or } (n = 2,\ \beta_1 = 1).$$

The first case is impossible since $\gamma_1 = 2^n - 2 \geq 2$.

So,

$$n = 2,\ \beta_1 = 1, \gamma_1 = 2,\ 2h = 3.(2^n - 1) + 1 = 10.$$

Thus:
$P = 1 + \cdots + x^{10}$,
$P + 1 = x(x + 1)Q^2 = x(x + 1)(1 + x^3 + x^4)^2 = x + x^2 + x^7 + x^8 + x^9 + x^{10}$.
It is impossible.

Case (d). We obtain:

$$1 + \cdots + x^{2h} = P^{a_0}Q^{b_0},\ a_0, b_0 \in \{0, 1\} \text{ by Lemma 2.4,}$$
$$1 + \cdots + (x + 1)^{2k-1} = x(1 + \cdots + (x + 1)^{k-1})^2.$$

Since $\sigma(A) = A$, we obtain:

$$x(P + 1)(Q + 1)^{2^n-1}B^2P^{a_0}Q^{b_0} = x^{2h}(x + 1)^{2k-1}P^{2m-1}Q^{2^n-1}. \qquad (3)$$

Thus:

$$1 + P = x^{\alpha_1}(x + 1)^{\beta_1}Q^{\gamma_1},$$
$$1 + Q = x^{\alpha_2}(x + 1)^{\beta_2}P^{\gamma_2}.$$

By considering degrees, we obtain:

$$\gamma_1\gamma_2 \leq 1.$$

If $\gamma_1 = \gamma_2 = 1$, then $Q = P + 1$. It is impossible.

So, $\gamma_1\gamma_2 = 0$. We have three cases:

Case: $\gamma_1 = \gamma_2 = 0$. In this case, Q (resp. P) does not divide $P + 1$ (resp. $Q + 1$). We may write:

$$P = x^{\alpha_1}(x + 1)^{\beta_1} + 1,\ Q = x^{\alpha_2}(x + 1)^{\beta_2} + 1.$$

– If $1 + \cdots + x^{2h} = P$, then the relation (3) becomes:

$$x(P + 1)(Q + 1)^{2^n-1}B^2P = x^{2h}(x + 1)^{2k-1}P^{2m-1}Q^{2^n-1}.$$

It is impossible (consider the exponent of Q).

– If $1 + \cdots + x^{2h} = Q$, then the relation (3) becomes:

$$x(P + 1)(Q + 1)^{2^n-1}B^2Q = x^{2h}(x + 1)^{2k-1}P^{2m-1}Q^{2^n-1}.$$

It is impossible (consider the exponent of P).

– If $1 + \cdots + x^{2h} = PQ$, then by Lemma 2.6:

$$P, Q \in \{x^3 + x^2 + 1, x^3 + x + 1\},\ h = 3.$$

We get the polynomial $C_4(x)$ and thus also the polynomial $C_5(x) = C_4(x + 1)$.

Case: $\gamma_1 = 0,\ \gamma_2 \geq 1$. In this case, we may write:

$$P = x^{\alpha_1}(x + 1)^{\beta_1} + 1,\ Q = x^{\alpha_2}(x + 1)^{\beta_2}P^{\gamma_2} + 1.$$

So $\deg(P) < \deg(Q)$.

– If $1+\cdots+x^{2h}=P$, then it is impossible as in the above case (consider the exponent of Q).

– If $1+\cdots+x^{2h}=Q$, then:

$$\begin{aligned} &a_0=1,\ b_0=0,\\ &x \text{ divides } Q+1,\ x^2 \text{ does not},\\ &Q+1=x(x+1)(1+\cdots+x^{h-1})^2. \end{aligned}$$

So, $\alpha_2=1$ and γ_2 is even.

By considering the exponent of P, we see that the relation (3) does not hold. It is impossible.

– If $1+\cdots+x^{2h}=PQ$, then by Lemma 2.1, since $\deg(P)<\deg(Q)$, the polynomial P (resp. Q) inverts into itself, and $P\in\{1+x+x^2, 1+\cdots+x^4\}$.

Therefore, $\alpha_1=1$ and $\beta_1\in\{1,3\}$ is odd. Thus, by considering the equality:

$$x(P+1)(Q+1)^{2^n-1}B^2PQ=x^{2h}(x+1)^{2k-1}P^{2m-1}Q^{2^n-1},$$

we obtain that the integers α_2,β_2 and γ_2 must be even. So, $Q+1$ is a square. It is impossible by the irreducibility of Q.

Case: $\gamma_1\geq 1,\ \gamma_2=0$. In this case, we may write:

$$P=x^{\alpha_1}(x+1)^{\beta_1}P^{\gamma_1}+1,\ Q=x^{\alpha_2}(x+1)^{\beta_2}+1.$$

The proof is analogous to that of the previous case, by switching P and Q.

– If $1+\cdots+x^{2h}=Q$, then it is impossible (consider the exponent of P).

– If $1+\cdots+x^{2h}=P$, then:

$$\begin{aligned} &x \text{ divides } P+1,\ x^2 \text{ does not},\\ &P+1=x(x+1)(1+\cdots+x^{h-1})^2. \end{aligned}$$

So, $\alpha_1=1$ and γ_1 is even.

By considering the exponent of Q, we see that the following equality does not hold:

$$x(P+1)(Q+1)^{2^n-1}B^2P=x^{2h}(x+1)^{2k-1}P^{2m-1}Q^{2^n-1}.$$

It is impossible.

– If $1+\cdots+x^{2h}=PQ$, then by Lemma 2.1, since $\deg(Q)<\deg(P)$, the polynomial P (resp. Q) inverts into itself, and $Q\in\{1+x+x^2, 1+x+\cdots+x^4\}$.

Therefore, $\alpha_2=1$ and $\beta_2\in\{1,3\}$ is odd. Thus, by considering the equality:

$$x(P+1)(Q+1)^{2^n-1}B^2PQ=x^{2h}(x+1)^{2k-1}P^{2m-1}Q^{2^n-1},$$

the integers α_1,β_1 and γ_1 must be even. So, $P+1$ is a square. It is impossible by the irreducibility of P.

This finishes the proof of Theorem 2.10.

References

[1] E.F. Canaday, The sum of the divisors of a polynomial, *Duke Math. Journal*, **8** (1941), 721-737.

[2] T.B. Beard Jr., James. R. Oconnell Jr, Karen I. West, Perfect polynomials over $GF(q)$, *Rend. Accad. Lincei*, **62** (1977), 283-291.

[3] L. Gallardo, O. Rahavandrainy, On perfect polynomials over $\mathbb{F}_4$, *Portugaliae Mathematica*, **62**, No. 1 (2005), 109-122.

[4] L. Gallardo, O. Rahavandrainy, Perfect polynomials over $\mathbb{F}_4$ with less than five prime factors, *Portugaliae Mathematica*, **64**, No. 1 (2007), 21-38.

[5] L.H. Gallardo, O. Rahavandrainy, Odd perfect polynomials over $\mathbb{F}_2$, *J. Théor. Nombres Bordeaux*, **19** (2007), 167-176.

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