JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Luis H. GALLARDO et Olivier RAHAVANDRAINY

Odd perfect polynomials over $\mathbb{F}_2$

Tome 19, n° 1 (2007), p. 165-174.

<http://jtnb.cedram.org/item?id=JTNB_2007__19_1_165_0>

© Université Bordeaux 1, 2007, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/), implique l'accord avec les conditions générales d'utilisation (http://jtnb.cedram.org/legal/). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Journal de Théorie des Nombres
de Bordeaux **19** (2007), 165-174

Odd perfect polynomials over $\mathbb{F}_2$

par Luis H. GALLARDO et Olivier RAHAVANDRAINY

Résumé. Un polynôme $A \in \mathbb{F}_2[x]$ est dit parfait s'il est égal à la somme de tous ses diviseurs et il est dit impair s'il n'a pas de facteurs de degré 1. Il n'y a pas de polynômes parfaits impairs ayant 3 facteurs irréductibles. Il n'y a pas non plus de polynômes parfaits impairs ayant au plus 9 facteurs irréductibles dans le cas où tous les exposants sont égaux à 2.

Abstract. A perfect polynomial over $\mathbb{F}_2$ 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. In this paper we show the non-existence of odd perfect polynomials with either three prime divisors or with at most nine prime divisors provided that all exponents are equal to 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 all divisors D 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 classical fact that will be used without further reference in the rest of the paper. When $\mathbb{F}_2$ is replaced by a field $\mathbb{F}$ of characteristic $p > 0$, we just sum the "monic" divisors of A. If A divides $\sigma(A)$ or equivalently if $\sigma(A) = A$, then we call A a perfect polynomial.

The notion of perfect polynomial was introduced by Canaday [1], the first doctoral student of Leonard Carlitz. He studied mainly the case $\mathbb{F} = \mathbb{F}_2$, and $\gcd(A, x^2 + x) \neq 1$. We may think of $x^2 + x \in \mathbb{F}_2[x]$ 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 $\gcd(A, x^2+x) = 1$. It is easy to see that an odd perfect polynomial in $\mathbb{F}_2[x]$ must be a square. Canaday (among other results in [1]) classifies the even perfect polynomials with

Manuscrit reçu le 13 novembre 2005.

three irreducible factors, leaving open the classification of the odd ones. Moreover, in the special case when A is a product of squares of primes P in $\mathbb{F}_2[x]$ he proves the non-existence of odd perfect polynomials when all such P's are of the same degree [1, Theorem 18], and announces without proof [1, Theorem 21] that $P \equiv 1 \mod x^2+x+1$, and that P has even degree.

In our papers [3] and [4] we worked on polynomials with coefficients in an extension field of $\mathbb{F}_2$, while here we come back to the original problem (*i.e.*, the study of perfect polynomials over the ground field $\mathbb{F}_2$), extending some results in [1] mentioned above.

The object of this paper is to prove two results:

a) There are no odd perfect polynomials A with three prime factors, *i.e.*, of the form $A = P^a Q^b R^c$ where P, Q, R are distinct irreducible (and non-linear) polynomials in $\mathbb{F}_2[x]$ and a, b, c are positive integers.

b) If A is an odd perfect polynomial which is a product of squares of primes, then $\omega(A) \geq 10$. Moreover, every prime divisor Q of such A has even degree $d \geq 30$, and satisfies: $Q \equiv 1 \mod x^2+x+1$.

A useful lemma for both results a) and b), is a generalization of a result of Beard [2] (see section 2) about the degrees of the possible prime factors of A. Also some general lemmata required for b) (see section 4) may also have some interest in their own right.

It just remains to observe two things. First of all, with a) available, the complete list of perfect polynomials A with $\omega(A) \leq 3$ over $\mathbb{F}_2$ is (see [1]):

$$\{x^{2^n-1}(x+1)^{2^n-1},\ x^2(x+1)(x^2+x+1),\ x(x+1)^2(x^2+x+1),$$
$$x^4(x+1)^3(x^4+x^3+x^2+x+1),\ x^3(x+1)^4(x^4+x^3+1)\}$$

where $n > 0$ is a positive integer.

Secondly, the congruence in b), (in which we may think of the modulus x^2+x+1 as the analogue of the number $3 \in \mathbb{Z}$) seems insufficient to bar polynomials from being perfect. This is in contrast to the case of integers. Indeed, already in 1937, Steuerwald [6] proved by a clever use of congruences modulo 3 that there are no odd perfect numbers of the form $n = p^{4k+1} p_1^2 \cdots p_r^2$ where $p \equiv 1 \mod 4$ is a prime number, $k \geq 0$ is a non-negative integer, $r > 0$ is a positive integer and $p_1 < p_2 < \cdots < p_r$ are odd prime numbers.

2. Some useful facts

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

First of all, we recall two lemmas obtained by Canaday [1] over $\mathbb{F}_2$. Their proofs work in a more general setting.

Lemma 2.1. (Lemma 5 in [1]) *Let $\mathbb{F}$ be a perfect field of characteristic* 2. *Let $P, Q \in \mathbb{F}[x]$ and $n, m \in \mathbb{N}$ be such that P is irreducible and $\sigma(P^{2n}) = 1 + \cdots + P^{2n} = Q^m$. Then $m \in \{0, 1\}$.*

The following lemma follows from the proof of Lemma 6 in [1]:

Lemma 2.2. *Let $\mathbb{F}$ be a perfect field of characteristic* 2. *Let $P, Q \in \mathbb{F}[x]$ and $n, m \in \mathbb{N}$ be 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*

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

We shall deal with three types of primes:

Definition. Let $\mathbb{F}$ be a field. Let $A \in \mathbb{F}[x]$ be a polynomial. A prime divisor P of A is called a minimal (resp. maximal) prime of A if it has minimal (resp. maximal) degree. When the prime divisor P is neither minimal nor maximal we call it a medium prime of A.

We are now ready to present the following lemma [4, Lemma 2.5] that improves a result of Beard et al., [2, Theorem 7]:

Lemma 2.3. *Let $\mathbb{F}$ be a field of characteristic $p > 0$. Let $A \in \mathbb{F}[x]$ be a perfect polynomial. Then the number of monic minimal primes of A is divisible by p.*

Proof. Let $p_1, \ldots, p_r$ be the list of all monic minimal primes of A. Since $A = \sigma(A)$, we have:

$$0 = \sum_{d\,|A,\ d\neq A} d = \sum_{i=1}^{r} \frac{A}{p_i} \ + \cdots$$

It follows that the leading coefficient of the sum $\sum_{i=1}^{r} \frac{A}{p_i}$ must be zero. This proves the lemma. □

3. Perfect polynomials in $\mathbb{F}_2[x]$ of the form: $A = P^h Q^k R^l$

By Lemma 2.3, we may suppose $\deg(P) = \deg(Q) < \deg(R)$.
So, P and Q (and h, k) play symmetric roles. If $\deg(P) = \deg(Q) = 1$, so that A is even, see Canaday's results in [1] and the Introduction. If $\deg(P) = \deg(Q) \geq 2$, so that A is odd, we have:

Theorem 3.1. *There are no perfect polynomials A in $\mathbb{F}_2[x]$ with $\omega(A) = 3$ irreducible factors P, Q, R with degrees all ≥ 2.*

Proof. If $A = P^h Q^k R^l$ is perfect then, by using the multiplicativity of σ, we have:

$$1 + \cdots + P^h = Q^a R^b,$$
$$1 + \cdots + Q^k = P^c R^d,$$
$$1 + \cdots + R^l = P^e Q^f,$$

where $c + e = h,\ a + f = k,\ b + d = l$.
Case in which one of h, k, l is odd:

Suppose that h is odd. Since $P(0) = 1$, we have: $1 + \cdots + P(0)^h = 0$. So, the monomial x divides $1 + \cdots + P^h$ and then we have either $Q = x$ or $R = x$, which is impossible. The same fact happens if k or l is odd.

Case in which h, k, l are all even:

By Lemma 2.2, we have $0 \leq a, b, c, d \leq 1$. If $b = 0$, then $a = 1$ by Lemma 2.1 and thus $h = 1$, which is impossible, hence $b = 1$. Analogously, we have $d = 1$, so that $l = b + d = 2$.

- If $a = c = 1$, then $h = k$, $e = h - 1 = k - 1 = f$. So, $1 + R + R^2 = (PQ)^e$. Thus, by Lemma 2.1, $e = 1$ and $h = k = 2$. We have then

$$1 + P + P^2 = QR,$$
$$1 + Q + Q^2 = PR,$$
$$1 + R + R^2 = PQ.$$

Thus, P, Q and R have the same degree and $R = P + Q + 1$, a contradiction.

- If $a = 0,\ c = 1$, then

$$1 + \cdots + P^h = R,\ 1 + \cdots + Q^k = PR.$$

So, $h \deg(P) = \deg(R) = k \deg(Q) - \deg(P) = (k - 1) \deg(P)$. Thus $h = k - 1$, which is impossible since h and k are both even.

- For $a = 1,\ c = 0$ the proof is analogous.

- If $a = c = 0$, then $h = k = e = f$, $l = 2$. So $1 + R + R^2 = (PQ)^e$, with e even. This is impossible by Lemma 2.1. □

4. Odd perfect polynomials that are a product of squares of primes

Here, we present some general results about a possible odd perfect polynomial $A \in \mathbb{F}_2[x]$, which satisfies certain conditions.

Definition. An odd perfect polynomial $A \in \mathbb{F}_2[x]$ is called "special perfect" if it is a product of $\omega(A) = m$ primes $p_i \in \mathbb{F}_2[x]$ of degree d_i with exponents all equal to 2:

$$A = p_1^2 \cdots p_m^2, \text{ where } 2 \leq d_1 \leq \ldots \leq d_m.$$

First of all, we present a simple, but useful result.

Lemma 4.1. *Let $P, Q \in \mathbb{F}_2[x]$ be two distinct primes of the same degree d. If Q divides $\sigma(P^2)$ then P does not divide $\sigma(Q^2)$.*

Proof. Assume that $\sigma(P^2) = 1 + P + P^2 = QC$ and that $\sigma(Q^2) = PB$ for some polynomials $C, B \in \mathbb{F}_2[x]$. Then the first equality implies $P \not\equiv 1 \pmod{Q}$ and $P^3 \equiv 1 \pmod{Q}$. Thus, the second equality implies $B \equiv P^2 \pmod{Q}$. It follows that $B^2 + B + 1 \equiv 0 \pmod{Q}$. Therefore, Q divides $\sigma(P^2) + B^2 + B + 1 = (P + B)(P + B + 1)$. This is impossible since $\deg(P + B) < \deg(B) = \deg(P) = d$, and $\deg(P + B + 1) < d$. □

Our second lemma deals with maximal prime divisors.

Lemma 4.2. *Let $P \in \mathbb{F}_2[x]$ be a maximal prime of a special perfect polynomial $A = p_1^2 \cdots p_m^2 \in \mathbb{F}_2[x]$, with $w(A) = m$. Let $r = 2s$ be the number of minimal primes of A. Then, there exists an unique couple (i, j), $i, j \in \{1, \ldots, m\}$ such that:*

a) *$p_j \neq P$, $d_1 < d_i < d_j = \deg(p_j) = \deg(P) = d_m$. In other words, p_j is maximal while p_i is medium;*
b) *$P \mid p_i^2 + p_i + 1$ and $P \mid p_j^2 + p_j + 1$, so that $P = p_i + p_j + 1$;*
c) *if $1 + p_i + p_i^2 = PR$ then $0 < \deg(R) < d_i$ so that $d_m < 2d_i$.*

Proof. a) and b): We may assume that $P = p_m$. If p_m^2 divides some $\sigma(p_i^2)$ for some $i < m$, then $2d_m \leq 2d_i$. So, $d_m = d_i$ and $p_m^2 = p_i^2 + p_i + 1$. This implies that

$$p_i = (p_m + p_i + 1)^2$$

is a square, which is impossible. So, p_m appears in exactly two $\sigma(p_k^2)$, say for $k \in \{i, j\}$ with $i < j < m$, $d_i \leq d_j$:

$$p_m \mid p_i^2 + p_i + 1, \ \ p_m \mid p_j^2 + p_j + 1.$$

This implies that p_m divides the product $\pi = (p_i + p_j)(p_i + p_j + 1)$ since $(p_i^2 + p_i + 1) + (p_j^2 + p_j + 1) = \pi$. So, $d_m \leq d_j$, *i.e.*, $d_j = d_{j+1} = \ldots = d_m$. If $d_i = d_j$ then $p_i + p_j$ and $p_i + p_j + 1$ both have degree $< d_j$ and since p_m divides one of them, we obtain the contradiction: $d_m < d_j = d_m$. Consequently, $d_i < d_j$. Since p_m divides the product $(p_i + p_j)(p_i + p_j + 1)$ and $\deg(p_m) = d_m = d_j = \deg(p_i + p_j) = \deg(p_i + p_j + 1)$, we derive either $p_m = p_i + p_j + 1$ or $p_m = p_i + p_j$. The second possibility does not happen because $p_i + p_j$ is not irreducible.

Clearly $p_m \neq \sigma(p_j^2)$ since $d_m < 2d_m$ while if $p_m = \sigma(p_i^2)$ then we immediately have the contradiction $p_j = p_i^2$. So, p_m divides strictly $\sigma(p_i^2)$ and $\sigma(p_j^2)$.

Now we prove that $d_1 < d_i$. Suppose that the contrary holds: $d_i = d_1$. One has:

$$p_m Q = p_i^2 + p_i + 1$$

so that $\deg(Q) = 2d_1 - d_m < d_1$. This implies $Q = 1$. But this is impossible, since p_m divides $\sigma(p_i^2)$ strictly.

c): We have just seen that $\rho = \deg(R) = 2d_i - d_m > 0$ so that $d_m < 2d_i$. Moreover, trivially, $\rho = 2d_i - d_m < d_i$ since $d_i < d_m$.

The uniqueness of the couple (i, j) follows from the fact that the maximal prime P appears exactly two times in $\sigma(A) = A$. □

Corollary 4.3. *Let A be a special perfect polynomial. Then, for every maximal prime P of A, and for every minimal prime Q of A, P does not divide $\sigma(Q^2)$.*

Proof. If P is a maximal prime, then by Lemma 4.2, P divides some $\sigma(R^2)$ and some $\sigma(S^2)$, where R is maximal and S is medium. So, P cannot divide $\sigma(Q^2)$. □

Corollary 4.4. *Let A be a special perfect polynomial, let t be the number of maximal primes of A, and let u be the number of medium primes of A. Then $u \geq t \geq 3$.*

Proof. By part a) of Lemma 4.2, there are at least 2 maximal primes, *i.e.*, $t \geq 2$. Assume that $t = 2$ so that p_m and p_{m-1} are the two maximal primes of A. By our preceding argument there are two indices $k < m-1$ and $l < m-1$ such that p_m divides $\gcd(\sigma(p_{m-1}^2), \sigma(p_k^2))$ and p_{m-1} divides $\gcd(\sigma(p_m^2), \sigma(p_l^2))$. This is impossible by Lemma 4.1. In other words, we have proved that $t \geq 3$, *i.e.*, that A has at least three maximal primes. □

If, for some medium prime p_k, two maximal primes P, Q divide the same $\sigma(p_k^2)$, then PQ divides also $\sigma(p_k^2)$. This is impossible since $2d_m > 2d_k$. So, $u \geq t$, thereby finishing the proof of the corollary.

Corollary 4.5. *Let A be a special perfect polynomial with exactly three maximal primes P, Q, R. Assume that P divides $\sigma(Q^2)$. Then Q divides $\sigma(R^2)$ and R divides $\sigma(P^2)$. Moreover, let P_1, Q_1, R_1 be medium prime divisors of A such that P divides $\sigma(Q_1^2)$, Q divides $\sigma(R_1^2)$, R divides $\sigma(P_1^2)$, and $\deg(P_1) \leq \deg(Q_1) \leq \deg(R_1)$, then*

$$1 = P_1 + Q_1 + R_1.$$

In particular,

$$\deg(P_1) < \deg(Q_1) = \deg(R_1).$$

Proof. It follows from Lemma 4.2 and Lemma 4.1 that Q divides $\sigma(R^2)$ and that R divides $\sigma(P^2)$. Thus, we get

$$P = Q + Q_1 + 1,$$

$$Q = R + R_1 + 1,$$

and

$$R = P + P_1 + 1.$$

By summing both sides of these three equalities we obtain

$$1 = P_1 + Q_1 + R_1.$$

Thus, the inequality $\deg(P_1) < \deg(Q_1) = \deg(R_1)$ holds. □

Our third lemma deals with minimal prime divisors.

Lemma 4.6. *Let $P \in \mathbb{F}_2[x]$ be a prime divisor of a special perfect polynomial A. If $S = \sigma(P^2) = 1 + P + P^2$ is prime then S is not a maximal prime. Moreover, assume that P is minimal and that S is not prime then:*

a) $\omega(S) = 2$, *more precisely $S = 1 + P + P^2 = QR$ where Q and R are two distinct minimal primes of A;*
b) *P does not divide $\sigma(Q^2)\,\sigma(R^2)$.*

Proof. Assume that S is prime. If S is maximal, then it follows from Corollary 4.3 that S divides $\sigma(P^2)$ for some medium prime P. According to Lemma 4.2 c), S must be a proper divisor of $\sigma(P^2)$, a contradiction.

We assume now that P is minimal and that S is not prime. We can write

$$1 + P + P^2 = \prod_{i=1}^{r} Q_i,$$

with Q_i prime divisor, $\deg(Q_i) \geq \deg(P)$, $r \geq 2$. So, $r = 2$ and $\deg(Q_1) = \deg(Q_2) = \deg(P)$. Moreover, $Q_1 \neq Q_2$ since P is not a square.

The result b) follows from a) and from Lemma 4.1. □

5. $\omega(A) \geq 10$ and $d_1 \geq 30$ for special perfect polynomial A

Let $A \in \mathbb{F}_2[x]$ be a special perfect polynomial. Our first result, namely $\omega(A) \geq 10$, will be proved in two steps. Firstly, the next lemma will show that $\omega(A) \geq 8$ and secondly, we will prove that $\omega(A) \neq 8$.

Lemma 5.1. *Let $A \in \mathbb{F}_2[x]$ be a special perfect polynomial. Then $\omega(A) \geq 8$.*

Proof. It follows from corollary 4.4 that A has at least 6 prime divisors, three maximal and the other three medium. Lemma 2.3 guarantees the existence of at least 2 minimal primes of A. So, $\omega(A) \geq 8$. □

The case $\omega(A) = 8$ is settled by

Lemma 5.2. *There is no special perfect polynomial $A \in \mathbb{F}_2[x]$ with $\omega(A) = 8$.*

Proof. Assume that $\omega(A) = 8$. If A has more than 2 minimal primes, then Lemma 4.2 implies that $\omega(A) > 8$. So, by Lemma 2.3, A has $r = 2$ minimal primes p_1 and p_2. From Lemma 4.6 it follows that $\sigma(p_1^2)$ and $\sigma(p_2^2)$ are also primes. Following Lemma 4.2 the only cases that remain to be studied are those of the shape $A = p_1^2 \cdots p_8^2$ where p_1 and p_2 are minimal primes, p_3, p_4, p_5, are medium primes and p_6, p_7, p_8, are maximal primes. Moreover, $\sigma(p_1^2)$ and $\sigma(p_2^2)$ must belong to $\{p_3, p_4, p_5\}$ (see Corollary 4.3). Observe that Corollary 4.5 implies that the only possibility for the degrees is the following:

$$d_1 = d_2 < d_3 < d_4 = d_5 < d_6 = d_7 = d_8.$$

One has $p_4 = \sigma(p_1^2)$, $p_5 = \sigma(p_2^2)$. We claim that $\sigma(p_3^2) = p_8 p_2$. We may assume by Lemma 4.2 that p_8 divides $\sigma(p_3^2)$. Write $p_3^2 + p_3 + 1 = p_8 M$ for some polynomial $M \in \mathbb{F}_2[x]$. Clearly, $\deg(M) = 2d_3 - d_6 < d_3$ so that only minimal primes can divide M. Take p_2 as a divisor of M and set $M = p_2 N$ for some $N \in \mathbb{F}_2[x]$. Thus, $\deg(N) = 2d_3 - d_6 - d_1 < d_3 - d_1 < d_1$ since $d_3 < d_4 = 2d_1$. So, $N = 1$. In other words, one has $p_3^2 + p_3 + 1 = p_8 p_2$, thereby proving the claim. So, the relations

$$d_1 < d_3 < d_4 = 2d_1$$

and

$$d_8 = 2d_3 - d_1 < 3d_1$$

hold. Following Lemma 4.2, set

$$p_1^4 + p_1 + 1 = \sigma(p_4^2) = p_7 A,\ p_2^4 + p_2 + 1 = \sigma(p_5^2) = p_6 B,$$

with suitable polynomials $A, B \in \mathbb{F}_2[x]$. It follows from Lemma 4.2 c) that A may have only p_2, p_3 as prime factors and that B may have only p_1, p_3 as prime factors. But

$$2d_1 = d_4 < d_7 = d_6 = d_8 < 3d_1,$$

so that p_2 does not appear as a factor in A, and p_1 does not appear as a factor in B, *i.e.*, $A = B = p_3$ and consequently

$$\sigma(p_4^2) = p_7 p_3,\ \ \sigma(p_5^2) = p_6 p_3.$$

By taking degrees in both sides of the equalities above we obtain $d_3 + d_6 = 4d_1$ which gives, together with $d_6 = 2d_3 - d_1$,

$$d_3 = \frac{5}{3} d_1,\ \ d_6 = \frac{7}{3} d_1.$$

From Lemmas 4.2 and 4.1 we obtain

$$\sigma(p_6^2) = p_8 K,\ \sigma(p_7^2) = p_6 L,\ \sigma(p_8^2) = p_7 M,$$

for some polynomials $K, L, M \in \mathbb{F}_2[x]$. It follows that

$$\deg(K) = \deg(L) = \deg(M) = \frac{7}{3}d_1.$$

Observe that the only primes available to be factors of these polynomials are p_5, p_4, p_2 once, and p_1 twice. But all these polynomials have degrees that are integral multiples of d_1, a contradiction. □

In order to prove our second result, namely, $d_1 \geq 30$, we shall provide proofs for two non proven results announced by Canaday (see [1, Theorem 21]). These results, together with a run of a Maple program, will prove the result.

Lemma 5.3. (Theorem 21 in [1]) *Let $A \in \mathbb{F}_2[x]$ be a special perfect polynomial. Let $P \in \mathbb{F}_2[x]$ be a prime divisor of A. Then*

a) *P is congruent to 1 modulo $x^2 + x + 1$;*
b) *$\deg(P)$ is even.*

Proof. First of all, by Lemma 2.3, $Q = x^2 + x + 1$ cannot divide A since it is the only prime polynomial of degree 2 in $\mathbb{F}_2[x]$. Let $\overline{\mathbb{F}_2}$ be an algebraic closure of $\mathbb{F}_2$, and let $\alpha \in \overline{\mathbb{F}_2}$ be such that $\alpha^2 + \alpha + 1 = 0$. We have $P(\alpha)P(\alpha^2) \neq 0$, since $P(\alpha) = 0$ implies that $Q = (x - \alpha)(x - \alpha^2)$ divides P so that $P = Q$, a contradiction. Assume now that $P(\alpha) \in \{\alpha, \alpha^2\}$. This implies $(1 + P + P^2)(\alpha) = 0$ and so, Q divides $\sigma(A) = A$, a contradiction. It follows that $P(\alpha) = 1 = P(\alpha^2)$ so that

$$P \equiv 1 \pmod{x^2 + x + 1}.$$

Set $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$. If P remains prime in $\mathbb{F}_4[x]$ then from the equality $A = \sigma(A)$ we deduce that P divides some $\sigma(R^2) = 1 + R + R^2 = (R + \alpha)(R + \alpha^2)$. We may assume that P divides $R + \alpha$ in $\mathbb{F}_4[x]$. Thus, $P(A + B\alpha) = R + \alpha$ for some $A, B \in \mathbb{F}_2[x]$. In particular, we get the contradiction $PB = 1$. Hence, P splits in $\mathbb{F}_4[x]$, *i.e.*, it has the form $P = (C + D\alpha)(C + D\alpha^2) = C^2 + CD + D^2$, for some $C, D \in \mathbb{F}_2[x]$, so that $\deg(P)$ is even. This finishes the proof of the lemma. □

The following corollary is used for computations:

Corollary 5.4. *Let $A \in \mathbb{F}_2[x]$ be a special perfect polynomial. Let $P \in \mathbb{F}_2[x]$ be a minimal prime divisor of A. Then P, all prime divisors Q of $\sigma(P^2)$, all prime divisors R of $\sigma(Q^2)$ and all prime divisors of $\sigma(R^2)$ are congruent to 1 $(\mathrm{mod}\ x^2 + x + 1)$ and have even degrees.*

Our main results are summarized in the next theorem:

Theorem 5.5. *Let $A \in \mathbb{F}_2[x]$ be a special perfect polynomial. Let $P \in \mathbb{F}_2[x]$ be a minimal prime divisor of A. Then:*

a) $\omega(A) \geq 10$;
b) $d_1 = \deg(P) \geq 30$.

Proof. By corollary 4.4, A has at least 6 prime divisors, hence from Lemma 2.3 (the number of monic minimal primes is even) and Lemma 5.2 one gets $\omega(A) \geq 6 + 4 = 10$ proving a). Now b) is obtained by running a Maple program that uses Corollary 5.4. All possible P's with degree up to 28 were tested, and the conclusion of the corollary was always violated. The computation used 126 hours of idle time on a sun4u sparc SUNW, Ultra Enterprise machine, running the command line version of Maple 6. □

References

[1] E. F. Canaday, *The sum of the divisors of a polynomial*. Duke Math. J. **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 - Fasc. 1** (2005), 109–122.
[4] L. Gallardo, O. Rahavandrainy, *Perfect polynomials over $\mathbb{F}_4$ with less than five prime factors*. Portugaliae Mathematica **64 - Fasc. 1** (2007), 21–38.
[5] Rudolf Lidl, Harald Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its applications*. Cambridge University Press, 1983, (Reprinted 1987).
[6] Rudolf Steuerwald, *Verschärfung einer notwendigen Bedingung für die Existenz einer ungeraden vollkommenen Zahl*. S. B. math.-nat. Abt. Bayer. Akad. Wiss München (1937), 69–72.

Luis H. Gallardo
Université de Brest
6, Avenue Le Gorgeu, C.S. 93837
29238 Brest cedex 3, France
E-mail: Luis.Gallardo@univ-brest.fr

Olivier Rahavandrainy
Université de Brest
6, Avenue Le Gorgeu, C.S. 93837
29238 Brest cedex 3, France
E-mail: Olivier.Rahavandrainy@univ-brest.fr