PORTUGALIAE MATHEMATICA
Vol. 64 Fasc. 1 – 2007
Nova Série

PERFECT POLYNOMIALS OVER $\mathbb{F}_4$ WITH LESS THAN FIVE PRIME FACTORS

Luis Gallardo and Olivier Rahavandrainy

Recommended by A. Garcia

Abstract: A perfect polynomial $A \in \mathbb{F}_4[x]$ is a monic polynomial that equals the sum of its monic divisors. There are no perfect polynomials $A \in \mathbb{F}_4[x]$ with exactly 3 prime divisors, i.e., of the form $A = P^a Q^b R^c$ where $P, Q, R \in \mathbb{F}_4[x]$ are irreducible and a, b, c are positive integers. We characterize the perfect polynomials A with 4 prime divisors such that one of them has degree 1. Assume that A has an arbitrary number of distinct prime divisors, we discuss some simple congruence obstructions that arise and we propose three conjectures.

1 – Introduction

As usual, we denote by $\mathbb{F}_q$ the finite field with q elements. When $q=4$, we write $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$, where $\alpha^2 = \alpha+1$.

For a monic polynomial $A \in \mathbb{F}_q[x]$, let $\sigma(A)$ denote the sum of all monic divisors of A, i.e.,

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

If $\sigma(A) = A$, then we call A a perfect polynomial (if necessary we add the words: "over $\mathbb{F}_q$"). Furthermore, we denote by $\omega(A)$ the number of distinct prime (irreducible) factors of A and by $d_1 \leq \cdots \leq d_{\omega(A)}$ the degrees of the prime factors of A.

In [6] we obtained for $q=4$, the complete list of all perfect polynomials with either $\omega(A) \leq 2$ or with $\omega(A) = 3$ and $d_1 = 1$, $d_2 = 1$, $d_3 > 1$; or with $\omega(A) = 4$

Received: November 12, 2005; *Revised*: February 8, 2006.
AMS Subject Classification: 11T55, 11T06.
Keywords: polynomials; sum of divisors; finite fields; characteristic 2.

and $d_1 = d_2 = d_3 = d_4 = 1$. We also disproved a conjecture of Beard et al. [1, p. 287] by proving [6, Corollary 3.11] that there are perfect polynomials over $\mathbb{F}_q$ without linear factors, namely $(x^4 + x + 1)^{2^n - 1}$ for any integer $n > 0$. It may be deduced easily from the proof of [11, Theorem 1.10.8] that for all integers $k \geq 0$ the polynomials $P_k = x^{3^k} + \alpha$ and $Q_k = P_k + 1$ are irreducible over $\mathbb{F}_4$ so that we have an infinity of perfect polynomials A over $\mathbb{F}_4$ with $\omega(A) = 2$, namely $A = (P_k Q_k)^{2^n - 1} = (x^{2 \cdot 3^k} + x^{3^k} + 1)^{2^n - 1}$ for $k = 1, ..., \infty$ and any positive integer $n > 0$.

Other counter-examples, one over $\mathbb{F}_{11}$ and two over $\mathbb{F}_{17}$ are in [2, Section 4].

In this paper we prove the nonexistence of perfect polynomials A with 3 prime factors, (see Theorem 3.1), generalizing our earlier work. Moreover for the next "target case", i.e., the case when A has 4 prime factors, we do here a first step in order to resolve it, by characterizing the perfect polynomials A with 4 prime factors (see Theorem 3.2) with at least one of these factors being linear.

Observe that Sylvester in 1888, [13, 5, Vol. 1, p. 27] proved the nonexistence of odd perfect numbers with 4 prime factors. Later, Dickson [4] showed that there are only finitely many odd perfect numbers with a given number of prime factors.

We also provide some general (i.e., we assume only $\omega(A) \geq 3$ instead of $\omega(A) < 5$ as in our results above) congruence results that imply the nonexistence of perfect polynomials A in the special case where all prime divisors of A are quadratic polynomials (see Theorem 4.4).

Finally, we propose some general conjectures (see Section 5).

2 – Some useful Lemmata

We denote, as usual, by $\mathbb{N}$ (resp. $\mathbb{N}^*$) the set of nonnegative (resp. positive) integers. In this section, we collect some results for the next sections.

The following three Lemmata were proved for polynomials in $\mathbb{F}_2[x]$ and $\mathbb{F}_4[x]$ in previous work. However, their proofs work over any perfect field of characteristic 2. The perfectness is required since the proofs use differentiation. More precisely, it is necessary for the derivative P' of an irreducible polynomial P to be nonzero.

Lemma 2.1 ([3, Lemma 5], [6, Lemma 2.1]). *Let $P, Q \in \mathbb{F}[x]$, where $\mathbb{F}$ is a perfect field of characteristic 2, and let $n, m \in \mathbb{N}$ such that P is irreducible and $\sigma(P^{2n}) = 1 + \cdots + P^{2n} = Q^m$. Then $m \in \{0, 1\}$.* ∎

Lemma 2.2 ([3, Lemma 6]). *Let $P, Q \in \mathbb{F}[x]$ where $\mathbb{F}$ is a perfect field of characteristic 2, and let $n, m \in \mathbb{N}$ such that P is irreducible, $m > 1$ and $\sigma(P^{2n}) = 1 + \cdots + P^{2n} = Q^m A$. Then $\deg(P) > 2\deg(Q)$.* ∎

Lemma 2.3 ([6, Lemma 2.3]). *The following properties hold for polynomials in $\mathbb{F}[x]$ where $\mathbb{F}$ is a perfect field of characteristic 2. For $h \in \mathbb{N}$, consider $\sigma(x^h) = 1 + x + \cdots + x^h$. Then:*

i) *$\sigma(x^h) = (1+x)^h$ if and only if $h = 2^n - 1$ for some $n \in \mathbb{N}$.*

ii) *$\sigma(x^h) = \sigma\big((x+1)^h\big)$ if and only if $h = 2^n - 2$ for some $n \in \mathbb{N}$.*

iii) *$\sigma(x^{2h}) = (1 + x + x^2)^h$ if and only if $h \in \{0, 1\}$.*

iv) *$\sigma(x^h) = (1 + x + x^2)\,(x+1)^{h-2}$ if and only if $h = 2$.*

v) *Assume that $\mathbb{F}$ contains $\mathbb{F}_4$. Then*

$$1 + (x + \alpha) + \cdots + (x + \alpha)^h \;=\; x\,(x+1)\,(x + \alpha + 1)^{h-2}$$

if and only if $h = 2$.

vi) *Let $P \in \mathbb{F}[x]$ be a nonconstant polynomial. Then:*
$1 + P + \cdots + P^h = (1+P)^h$ if and only if $h = 2^n - 1$ for some $n \in \mathbb{N}$. ∎

Lemma 2.4 ([6, Lemmata 2.4, 2.5], [9, Theorem 2.47]). *Let p be an odd prime number and $n \in \mathbb{N}^*$. If d is the smallest positive integer such that $(2^n)^d = 1 \pmod{p}$, and if μ is the number of irreducible distinct factors of degree d, in $\mathbb{F}_{2^n}[x]$, of $1 + \cdots + x^{p-1}$, then*

$$\mu \;=\; \frac{p-1}{d}\;.$$

It follows that for all integers $n \geq 2$, the polynomial

$$x^n + \cdots + x + 1$$

is reducible over $\mathbb{F}_4$. ∎

New lemmata follow:

First of all, we generalize a result of Beard et al.:

Lemma 2.5 ([1, Theorem 7], see also [7]). *Let q be a power of a prime p. Let $A \in \mathbb{F}_q[x]$ be a monic polynomial. Let $\{p_1, ..., p_r\}$ be the list of all monic irreducible polynomials in $\mathbb{F}_q[x]$ of minimal degree that divide A.*

If A is perfect over $\mathbb{F}_q$ then $r \equiv 0 \pmod{p}$.

Proof: By definition one has

$$A = \sigma(A) \iff \sum_{d\,|\,A,\ d\neq A,\ d\,\text{monic}} d = 0\ .$$

In particular the leading coefficient of

$$\frac{A}{p_1} + \cdots + \frac{A}{p_r}$$

equals 0, i.e., r is divisible by p, thereby finishing the proof of the lemma. ∎

Lemma 2.6.

i) *If* $1+\cdots+x^h = PQ$, *with* h *even,* $P, Q \in \mathbb{F}_4[x]$ *irreducible, then* $p = h+1$ *is prime,* $deg(P) = deg(Q)$ *and* $P(0) = Q(0) = 1$ *for* $h \geq 4$.

ii) *If* $1+\cdots+x^h = 1+\cdots+(1+x)^h = PQ$, *with* h *even and* $P, Q \in \mathbb{F}_4[x]$ *irreducible, then* $h = 6$ *and* $P = x^3+x^2+1$, $Q = x^3+x+1$.

iii) *If* $1+\cdots+x^h = \big(x^a(x+1)^b+1\big)\big(x^c(x+1)^d+1\big)$, *with* h *even and* $P = x^a(x+1)^b+1$, $Q = x^c(x+1)^d+1$ *irreducible in* $\mathbb{F}_4[x]$, *then* $h = 6$, $a = d = 2$, $b = c = 1$, $P = x^3+x^2+1$, $Q = x^3+x+1$.

Proof: **i)**: if $h+1 = ab$, with $a, b \geq 2$ then:

$$1+\cdots+x^h \;=\; \frac{1+x^{h+1}}{1+x} \;=\; \frac{(1+x^a)}{1+x}\left(1+\cdots+(x^a)^{b-1}\right)$$

has at least 3 factors since $1+\cdots+(x^a)^{b-1}$ is reducible.

Thus $p = h+1$ is prime and $\deg(P) = \deg(Q) = \dfrac{h}{2}$ by Lemma 2.4.

Assume that $h \geq 4$. Let $\overline{\mathbb{F}_4}$ be an algebraic closure of $\mathbb{F}_4$. Let g be a generator of the cyclic group $\left\{z \in \overline{\mathbb{F}_4} \mid\ z^p+1 = 0\right\}$.

We have:

$$PQ \;=\; 1+\cdots+x^h \;=\; (x+g)\,(x+g^2)\cdots(x+g^{p-1})\ .$$

So,

$$P \;=\; (x+g^{t_1})\,(x+g^{t_2})\cdots(x+g^{t_m})\ ,$$

where $m = \dfrac{p-1}{2}$, and $t_1, \ldots, t_m \in \{1, \ldots, p-1\}$.

Thus, $P(0) = g^{t_1+\cdots+t_m} \in \mathbb{F}_4-\{0\}$. So, $1 = P(0)^3 = g^{3(t_1+\cdots+t_m)}$.

We deduce that p divides $3(t_1+\cdots+t_m)$ so that it divides $t_1+\cdots+t_m$ since $p>3$. Thus, $P(0)=1$ and $Q(0)=1$.

ii): We have, by Lemma 2.3, $h=2^m-2$ for some m, and by i), $p=h+1=2^m-1$ is a prime number.

By Lemma 2.4, $1+\cdots+x^h=PQ$ implies that 4 has order $\frac{p-1}{2}$ modulo p.

But, $4^m-1=(2^m-1)(2^m+1)=0$ modulo p and $m\leq\frac{p-1}{2}=2^{m-1}-1$. So we must have: $m=2^{m-1}-1$, i.e., $m=3$.

iii): First of all, observe that we have: $a+b=c+d=\frac{h}{2}$.

- If $a=0$ then $b=1$ by irreducibility. So x divides $1+\cdots+x^h$, which is impossible.
- Idem if $c=0$.
- If $b=0$ then $a=1$ and $x+1$ divides $1+\cdots+x^h$, which is impossible since h is even.
- Idem if $d=0$.

So, $a,b,c,d\geq 1$.

If either $(a,c\geq 2)$ or $(a=c=1)$, then $\left(x^a(x+1)^b+1\right)\left(x^c(x+1)^d+1\right)$ does not contain the monomial x. So $a=1$, $c\geq 2$ or $c=1$, $a\geq 2$.

Suppose that $a=1$ so that $d=1$ and $c=b=\frac{h}{2}-1\geq 2$.

Suppose that $h>6$. Then

$$1+\cdots+x^h \;=\; \left(x(x+1)^{\frac{h}{2}-1}+1\right)\left(x^{\frac{h}{2}-1}(x+1)+1\right)$$

implies:

$$x+\cdots+x^h \;=\; x(x+1)\left(x^{\frac{h}{2}-1}(x+1)^{\frac{h}{2}-1}+(x+1)^{\frac{h}{2}-2}+x^{\frac{h}{2}-2}\right),$$

$$x\,(x+1)\,(1+\cdots+x^{\frac{h}{2}-1})^2 \;=\; x\,(x+1)\left(x^{\frac{h}{2}-1}(x+1)^{\frac{h}{2}-1}+(x+1)^{\frac{h}{2}-2}+x^{\frac{h}{2}-2}\right),$$

$$1+x^2+x^4+\cdots+x^{h-2} \;=\; x^{\frac{h}{2}-1}(x+1)^{\frac{h}{2}-1}+(x+1)^{\frac{h}{2}-2}+x^{\frac{h}{2}-2}\;.$$

- If $\frac{h}{2}-2$ is odd, then $\frac{h}{2}-2\geq 3$, so that the right hand member of the last equality above contains the monomial x, which is impossible.
- If $\frac{h}{2}-2=2u$ is even, then $x^{\frac{h}{2}-1}(x+1)^{\frac{h}{2}-1}+(x+1)^{\frac{h}{2}-2}+x^{\frac{h}{2}-2}$ does not contain the monomial $x^{\frac{h}{2}-2}=x^{2u}$. This is impossible.

So $\frac{h}{2}-2=1$, and we are done. ∎

We characterize now some special perfects:

Lemma 2.7.

i) *For all integers* $l,t \geq 0$, *the polynomial* $x^6\,(1+x)^6\,(x^3+x^2+1)^l\,(x^3+x+1)^t$ *is not perfect over* $\mathbb{F}_4$.

ii) $x^6\,(1+x)^k\,(x^3+x^2+1)^l\,(x^3+x+1)^t$, *with* k,l,t *odd, is perfect over* $\mathbb{F}_4$ *if and only if* $k=3$, $l=t=1$.

Proof: **i)**: Suppose that $x^6\,(1+x)^6\,(x^3+x^2+1)^l\,(x^3+x+1)^t$ is perfect over $\mathbb{F}_4$ for some nonnegative integers l,t.

Putting $P = x^3+x^2+1$, $Q = x^3+x+1$, we have:

$$\begin{aligned} 1+\cdots+x^6 &= 1+\cdots+(x+1)^6 = PQ\ , \\ 1+\cdots+P^l &= x^u\,(x+1)^v\,Q^{t-2}\ , \\ 1+\cdots+Q^t &= x^{6-u}\,(x+1)^{6-v}\,P^{l-2}\ . \end{aligned}$$

- If l is even, then $u=v=0$ since $P(0)=P(1)=1$.
  Thus, $1+\cdots+P^l = Q^l$, which is impossible.
- Idem if t is even.
- If l and t are odd, then:

$$\begin{aligned} x^6\,(x+1)^6\,P^lQ^t &= (1+\cdots+x^6)\left(1+\cdots+(x+1)^6\right)(1+\cdots+P^l)\,(1+\cdots+Q^t) \\ &= PQPQ\,(1+P)\,(1+Q)\,A^2 \\ &= P^2\,Q^2\,x^3\,(x+1)^3\,A^2\ , \end{aligned}$$

which is impossible since l and t are odd.

ii): Sufficiency: It is proved by direct computations.

Necessity: Suppose that $x^6\,(1+x)^k\,(x^3+x^2+1)^l\,(x^3+x+1)^t$ is perfect for some odd natural numbers $k,l,t \in \mathbb{N}$.

Putting $P = x^3+x^2+1$, $Q = x^3+x+1$, we have:

$$\begin{aligned} 1+\cdots+x^6 &= PQ\ , \\ 1+\cdots+(x+1)^k &= x\left(1+(1+x)+\cdots+(1+x)^{\frac{k-1}{2}}\right)^2 = x\ A^2\ , \\ 1+\cdots+P^l &= x^2\,(x+1)\left(1+P+\cdots+P^{\frac{l-1}{2}}\right)^2 = x^2\,(x+1)\ B^2\ , \\ 1+\cdots+Q^t &= x\,(x+1)^2\left(1+Q+\cdots+Q^{\frac{t-1}{2}}\right)^2 = x\,(x+1)^2\ C^2\ . \end{aligned}$$

Thus,

$$x^6\,(x+1)^k\,P^l\,Q^t \;=\; PQ\;x^4\,(x+1)^3\,A^2\,B^2\,C^2$$

and $k \geq 3$.

So,

$$x\,(x+1)^{\frac{k-3}{2}}\,P^{\frac{l-1}{2}}\,Q^{\frac{t-1}{2}} \;=\; ABC\;.$$

Thus, x divides ABC and x^2 does not. Then any two of the integers $\dfrac{k-1}{2}$, $\dfrac{l-1}{2}$, $\dfrac{t-1}{2}$ must be even while the third must be odd.

- If $\dfrac{k-1}{2}$ is odd and $\dfrac{k-3}{2} \geq 1$, then $x+1$ must divide BC, which is impossible since $\dfrac{l-1}{2}$, $\dfrac{t-1}{2}$ are both even.

  So, $k=3$. Thus:

  $$\begin{aligned} &A = x, \quad \text{and } x \text{ does not divide } BC\;, \\ &B \;=\; 1+P+\cdots+P^{\frac{l-1}{2}} \;=\; Q^{\frac{t-1}{2}}\;, \\ &C \;=\; 1+Q+\cdots+Q^{\frac{t-1}{2}} \;=\; P^{\frac{l-1}{2}}\;. \end{aligned}$$

  We conclude that $l=t$. But $\dfrac{l-1}{2}$ is even, so $\dfrac{l-1}{2}=0$, and $k=3$, $l=t=1$.

- If $\dfrac{k-1}{2}$ and $\dfrac{l-1}{2}$ are even, then $\dfrac{t-1}{2}$ is odd and $\gcd(B, x(x+1)) = 1$, so:

  $$B \;=\; 1+\cdots+P^{\frac{l-1}{2}} \;=\; Q^u \;=\; Q^{\frac{l-1}{2}}\;.$$

  So $l=1$, and:

  $$x\,(x+1)^{\frac{k-3}{2}}\,Q^{\frac{t-1}{2}} \;=\; AC \;=\; \left(1+x+\cdots+x^{\frac{k-1}{2}}\right)\left(1+Q+\cdots+Q^{\frac{t-1}{2}}\right)\;.$$

  So

  $$1+Q+\cdots+Q^{\frac{t-1}{2}} \;=\; x\,(x+1)^{\frac{k-3}{2}} \tag{1}$$

  since $\dfrac{k-1}{2}$ is even.

  Thus, by computing the degrees in both sides of (1), we have:

  $$3\,\frac{t-1}{2} \;=\; \frac{k-1}{2}\;,$$

  which is impossible by parity.

- Idem if $\dfrac{k-1}{2}$ and $\dfrac{t-1}{2}$ are both even. ∎

3 – Main results

3.1. Perfects of the forms: $P^h Q^k R^l$

We have the following

Theorem 3.1. *There are no perfect polynomials over $\mathbb{F}_4$ with 3 irreducible factors.*

Proof: First of all, by Lemma 2.5, we may suppose that $\deg(P) = \deg(Q) < \deg(R)$. So, P and Q (and h, k) play symmetric roles.

If $P^h Q^k R^l$ is perfect then we have:

$$\begin{aligned} 1 + \cdots + P^h &= Q^a R^b \,, \\ 1 + \cdots + Q^k &= P^c R^d \,, \\ 1 + \cdots + R^l &= P^e Q^f \,, \end{aligned}$$

where $c+e = h$, $a+f = k$, $b+d = l$.

Case h, k even:

By Lemma 2.2, we have:

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

So, $h = k$ and $l = 2$.

Thus, $1+R+R^2 = P^e Q^f$, with $e = h-1 = k-1 = f$, so, $1+R+R^2 = (PQ)^e$ which implies $e = 1$, by Lemma 2.1. Thus, P, Q and R have the same degree, a contradiction.

Case h, l even, k odd:

We have:

$$1 + \cdots + P^h = Q R \,, \qquad 1 + \cdots + Q^k = P^c R^d, \quad \text{with } d \text{ odd} \,.$$

So, $1 + Q^{k+1} = (1 + Q) P^c R^d$.

By differentiation relative to x: $(1+Q) P^u R' = A R$, for some polynomial A, where $u = \min(1, c)$. So R divides $1+Q$, a contradiction.

Case h, k odd, l even:

We have:

$$1 + P^{h+1} = (1+P)\, Q^a R^b \,, \qquad 1 + Q^{k+1} = (1+Q)\, P^c R^d \,.$$

– If b is odd, then d is odd and, by differentiation relative to x, we see that R divides $1+P$ and $1+Q$ which is impossible.

– If b is even, then d is even, a, c are odd, and e, f are even. By differentiation relative to x, Q divides $1+P$, so $Q = 1+P$. Moreover, $1+\cdots+R^l = P^e Q^f$ is a square, which is impossible by Lemma 2.1.

Case h, k, l odd:

We have:

$$P^h Q^k R^l \;=\; (1+\cdots+P^h)\,(1+\cdots+Q^k)\,(1+\cdots+R^l) \;=\; (1+P)\,(1+Q)\,(1+R)\,A^2$$

for some polynomial A.

So:

R must divide $(1+P)\,(1+Q)$, i.e., $R \in \{1+P, 1+Q\}$, a contradiction.

Case h even, k, l odd:

One has

$$1+\cdots+P^{h-1}+P^h \;=\; Q\,R\;. \tag{2}$$

We have also:

$$1+\cdots+Q^k \;=\; P^c R^d\;,$$
$$1+\cdots+R^l \;=\; P^e Q^f\;.$$

So, $1+Q^{k+1} = (1+Q)\,P^c R^d$, $1+R^{l+1} = (1+R)\,P^e Q^f$, and d, f, $c+e$ are even.

By differentiation relative to x, we must have: c, e odd and P divides $1+Q$ and $1+R$. So $P = 1+Q$.

Since $h-1$ is odd we get from (2) that $1+P = Q$ divides P^h which is impossible. ∎

3.2. Perfects of the forms: $S^h P^k Q^l R^t$, with $\deg(S) = 1$

Assume $S^h P^k Q^l R^t$ perfect with $1 \le \deg(S) \le \deg(P) \le \deg(Q) \le \deg(R)$. The case $\deg(R) = 1$ was already done in [6], so that by Lemma 2.5 it suffices to consider the cases where

$$1 \;=\; \deg(S) \;=\; \deg(P) \;<\; \deg(Q) \;\le\; \deg(R)\;.$$

We consider the (Frobenius) Galois automorphism τ such that $\tau(\alpha) = \alpha+1$.

Our main theorem reads:

Theorem 3.2. *Let $S, P, Q, R \in \mathbb{F}_4[x]$ be irreducible monic polynomials. The polynomial $S^h P^k Q^l R^t$, in which $1 \leq \deg(S) \leq \deg(P) \leq \deg(Q) \leq \deg(R)$ and such that $\deg(S) = 1 < \deg(R)$ is perfect if and only if $S = x + a$, for some $a \in \mathbb{F}_4$, $P(x) = S(x+1)$, and either:*

i) $h = 6,\ k = 3,\ l = t = 1,\ Q(x) = x^3 + x^2 + 1 = R(x+1)$, *or*

ii) *For some* $n \in \mathbb{N}$, $h = k = 2^n - 1$, *for some* $m \in \mathbb{N}$, $l = t = 2^m - 1$, *and* $R = Q + 1$.

Proof: Sufficiency: This follows by direct computations.

Necessity: We can assume that $S = x$. Put $P = x + a$, where $a \in \{1, \alpha, \alpha+1\}$. We already treated [6] the case where $\deg(R) = 1$. Thus, from Lemma 2.5 we get $\deg(R) \geq \deg(Q) \geq 2$.

We show now that $P = x+1$. Put $P = x + a$ and suppose that $a \in \{\alpha, \alpha+1\}$, say $a = \alpha$, we can write:

$$
\begin{aligned}
1 + \cdots + x^h &= (x+\alpha)^{a_1} Q^{b_1} R^{c_1} \ , \\
1 + \cdots + (x+\alpha)^k &= x^{d_1} Q^{b_2} R^{c_2} \ , \\
1 + \cdots + Q^l &= x^{d_2} (x+\alpha)^{a_2} R^{c_3} \ , \\
1 + \cdots + R^t &= x^{d_3} (x+\alpha)^{a_3} Q^{b_3} \ ,
\end{aligned}
$$

where:

$$d_1 + d_2 + d_3 = h \ , \quad a_1 + a_2 + a_3 = k \ , \quad b_1 + b_2 + b_3 = l \ , \quad c_1 + c_2 + c_3 = t \ .$$

If we apply the Frobenius automorphism τ to both sides of

$$1 + \cdots + x^h = (x+\alpha)^{a_1} Q^{b_1} R^{c_1} \ ,$$

then we obtain that $a_1 = 0$ and that h is even.

Analogously, by substituting x by $x + \alpha$ and by applying τ to both sides of

$$1 + \cdots + (x+\alpha)^k = x^{d_1} Q^{b_2} R^{c_2}$$

we obtain that $d_1 = 0$ and that k is even.

So, by Lemma 2.2:

$$1 + \cdots + x^h = 1 + \cdots + (x+\alpha)^k = QR$$

and thus $h = k$. Applying again τ, we obtain:

$$1 + \cdots + x^h = 1 + \cdots + (x+\alpha+1)^h = 1 + \cdots + (x+1)^h = QR \ .$$

So, $h = 6$ by Lemma 2.6, which is impossible because:

$$1 + \cdots + x^6 \neq 1 + \cdots + (x + \alpha)^6 \ .$$

So, $P = x+1,\ S = x,\ \deg(R) \geq \deg(Q) \geq 2.$

Case h, k even:

As before, by using Lemmata 2.1 and 2.2 as well as by acting with the Frobenius automorphism τ again, we get after some computation:

$$1 + \cdots + x^h \ = \ 1 + \cdots + (x+1)^k \ = \ Q\,R \ .$$

So, $h = k = 6$ by Lemma 2.6, and $Q = x^3 + x^2 + 1,\ R = x^3 + x + 1 = Q(x+1).$

But the polynomial $x^6 (1+x)^6 Q^l R^t$ is not perfect for all integers $l, t \geq 0$ (see Lemma 2.7), a contradiction.

Case h even, k odd:

As before, one has $1 + \cdots + x^h = Q R$. This implies (by Lemma 2.6):

$$p = h+1 \ \text{ is prime },\qquad \deg(Q) = \deg(R) = h/2 \qquad \text{and} \qquad Q(0) = R(0) = 1 \ .$$

So, Q and R (resp. l and t) play symmetric roles.

– If l is even and t odd, then $1 + \cdots + Q^l = x^{d_2} (x+1)^{a_2} R^{c_3}$ with $c_3 \leq 1$ by Lemma 2.2.
  Furthermore, $d_2 = 0$ and $1 + \cdots + Q^l = (x+1)^{a_2} R^{c_3}$.
  If $c_3 = 0$, then $1 + \cdots + Q^l = (x+1)^{a_2}$. This is impossible by Lemma 2.1.
  So, $1 + \cdots + Q^l = (x+1)^{a_2} R$ and:

$$\begin{aligned} 1 + \cdots + x^h \ &= \ Q\,R \ , \\ 1 + \cdots + (x+1)^k \ &= \ x\,A^2 \ , \\ 1 + \cdots + Q^l \ &= \ (x+1)^{a_2}\,R \ , \\ 1 + \cdots + R^t \ &= \ (1+R)\,B^2 \ . \end{aligned}$$

  Thus, $x^h (x+1)^k Q^l R^t = x\,Q\,R^2\,(1+R)\,(x+1)^{a_2}\,D^2$.
  This is impossible (consider the exponent of R).
  A similar proof works when l is odd and t is even.

– If l, t are both even, then we can write:

$$\begin{aligned} 1 + \cdots + x^h \ &= \ Q\,R \ , \\ 1 + \cdots + (x+1)^k \ &= \ x\,A^2 \ , \\ 1 + \cdots + Q^l \ &= \ (x+1)^{a_2}\,R \ , \\ 1 + \cdots + R^t \ &= \ (x+1)^{a_3}\,Q \ . \end{aligned}$$

Thus, $x^h(x+1)^k Q^l R^t = x\, Q^2 R^2 (x+1)^{a_2+a_3} A^2$.
This is of course impossible (consider the exponent of x).

So, h is even and k, l, t are odd.

We can write:

$$\begin{aligned} 1+\cdots+x^h &= QR\ , \\ 1+\cdots+(x+1)^k &= x\,A^2\ , \\ 1+\cdots+Q^l &= (1+Q)\,B^2\ , \\ 1+\cdots+R^t &= (1+R)\,C^2\ , \end{aligned}$$

with $\deg(Q)=\deg(R)$, $Q(0)=R(0)=1=Q(1)\,R(1)$. We have:

$$x^h\,(x+1)^k\,Q^l R^t = QR\,x\,(1+Q)\,(1+R)\,D^2\ .$$

We deduce that:

i) x divides $1+Q$ and $1+R$ (since $Q(0)=R(0)=1$),

ii) $x+1$ divides $(1+Q)\,(1+R)$ since k is odd.

So, either $Q(1)=1$ or $R(1)=1$.
Thus $Q(1)=R(1)=1$ and $x+1$ divides $1+Q$ and $1+R$.
Observe that $\gcd(R, 1+Q)=1=\gcd(Q, 1+R)$ since $R(1)=Q(1)=1$. So, $1+Q=x^{u_1}(1+x)^{u_2}$ and $1+R=x^{v_1}(1+x)^{v_2}$.
We obtain:

$$1+\cdots+x^h = QR = \left(x^{u_1}(1+x)^{u_2}+1\right)\left(x^{v_1}(1+x)^{v_2}+1\right)\ .$$

Then $h=6$, $u_1=v_2=1$, $u_2=v_1=2$ by Lemma 2.6. This implies that $Q=x^3+x+1$ and $R=x^3+x^2+1=Q(x+1)$.
The result follows now from Lemma 2.7.

Case h, k, l, t odd:
Put:

$$h = 2h_0-1 = 2^n\varepsilon-1\ , \qquad k=2k_0-1 = 2^m\nu-1\ ,$$
$$l = 2l_0-1 = 2^r\beta-1\ , \qquad t=2t_0-1 = 2^s\gamma-1\ ,$$

where ε, ν, β and γ are odd.
If $x^h(1+x)^k Q^l R^t$ is perfect, then the polynomial

$$x^{h_0-1}(1+x)^{k_0-1}\,Q^{l_0-1}\,R^{t_0-1}$$

must be perfect and $R=Q+1$.

Indeed, if $x^h(1+x)^k Q^l R^t$ is perfect, then:

$$x^{h-1}(1+x)^{k-1} Q^l R^t = (1+Q)(1+R) A^2 ,$$

so that l, t odd implies: R divides $(1+Q)$ and Q divides $(1+R)$, i.e., $R = 1+Q$. So, after simplification,

$$x^{(h-1)/2}(1+x)^{(k-1)/2} Q^{(l-1)/2} R^{(t-1)/2}$$

is perfect.

If one of $(h-1)/2$, $(k-1)/2$, $(l-1)/2$, $(t-1)/2$, is even, then we obtain a contradiction from the previous cases.

If all the exponents are odd, then by using the same argument, we see that the only possibility that remains is that

$$x^{h_0-1}(1+x)^{k_0-1} Q^{l_0-1} R^{t_0-1}$$

must be perfect.

According to the previous cases, one of the following two conditions must hold:

a) $h_0-1=6$, $k_0-1=3$, $l_0-1=t_0-1=1$ and $Q=x^3+x^2+1=R(x+1)$

b) h_0-1, k_0-1, l_0-1, t_0-1 are simultaneously odd.

Observe that a) does not hold since $R = Q+1$ so that we get b).

We consider now the following sequences of odd integers:

$$\begin{aligned} h_\mu &= 2^{(n-\mu)}\varepsilon - 1 , && 0 \le \mu \le n-1 , && h_n = \varepsilon - 1 , \\ k_\mu &= 2^{(m-\mu)}\nu - 1 , && 0 \le \mu \le m-1 , && k_m = \nu - 1 , \\ l_\mu &= 2^{(r-\mu)}\beta - 1 , && 0 \le \mu \le r-1 , && l_r = \beta - 1 , \\ t_\mu &= 2^{(s-\mu)}\gamma - 1 , && 0 \le \mu \le s-1 , && t_s = \gamma - 1 . \end{aligned}$$

Note that

$$\frac{h_\mu - 1}{2} = h_{\mu+1} , \quad \frac{k_\mu - 1}{2} = k_{\mu+1} , \quad \frac{l_\mu - 1}{2} = l_{\mu+1} , \quad \frac{t_\mu - 1}{2} = t_{\mu+1} ,$$

and h_n, k_m, l_r, t_s are all even.

Put: $e = \min(n, m, r, s)$.

- If $e = n$, then by iterating the arguments above, we see that the polynomial $x^{h_e-1}(1+x)^{k_e-1} Q^{l_e-1} R^{t_e-1}$ must be perfect (with $R = Q+1$).

So, we must have: $k_e - 1 = h_e - 1 = h_n - 1 = \varepsilon - 1 = 0$. Thus, $n = m$, $h = k = 2^n - 1$.
So, $Q^l R^t$ must be perfect, with $R = Q + 1$. The result follows from [6, Proposition 3.10].

- We can proceed analogously if either $e = m$, $e = r$ or $e = s$. ∎

4 – Some congruence results

Let n be an odd perfect number. Write its factorization over $\mathbb{Z}$:

$$n = \prod p^e ,$$

where p is a prime number and p^e divides n while p^{e+1} does not divide n; (this is also denoted $p^e \,||\, n$ as usual).

It is well known (and it is easy to prove) that the exponent e must either satisfy $e \not\equiv 1 \pmod 2$ or $e \not\equiv 3 \pmod 4$ and that there is one and only one exponent in the latter case.

One has an analogue for polynomials:

Let us begin with the analogue for polynomials over the finite field $\mathbb{F}_q$ of characteristic p of the notion of an odd perfect number.

Definition 4.1. Let $A \in \mathbb{F}_q[x]$ be such that $\gcd(A, x^q - x) = 1$. We say that A is an odd polynomial. Moreover, if A is also perfect then we call it an odd perfect polynomial. □

First of all, we have the obvious lemma:

Lemma 4.2. *Let q be a power of a prime p. Let $P \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree $d > 1$ and let $h \in \mathbb{N}^*$ be a positive integer.*

i) *If there exists $a \in \mathbb{F}_q$ such that $P(a) = 1$ and if $h \equiv -1 \pmod p$ then for all odd $A \in \mathbb{F}_q[x]$ the polynomial $P^h A$ is not perfect.*

ii) *If there exists $a \in \mathbb{F}_q$ such that $P(a) \notin \{0, 1\}$ and if*

$$h \equiv -1 \pmod{q-1} ,$$

then for all odd $A \in \mathbb{F}_q[x]$ the polynomial $P^h A$ is not perfect.

Proof: In those cases, if $P^h A$ is perfect then the monomial $x-a$ divides $1+\cdots+P^h = \sigma(P^h)$ and thus divides $\sigma(P^h A) = P^h A$, a contradiction. ∎

Proposition 4.3. *For all $h \in \mathbb{N}^*$ such that $h \equiv 5 \mod 6$, for all irreducible monic polynomial $P \in \mathbb{F}_4[x]$ of degree $d > 1$ and for all odd perfect polynomial $A \in \mathbb{F}_4[x]$ the polynomial $P^h A$ is not perfect.*

Let $R \in \mathbb{F}_4[x]$ be a prime factor of an odd perfect polynomial $A \in \mathbb{F}_4[x]$ and let e be a positive integer such that $R^e \,||\, A$. Then the exponent e satisfies: either $e \not\equiv 1 \pmod 2$ or $e \not\equiv 2 \pmod 3$.

Proof: Clearly, h is odd and $h \equiv 2 \mod 3$. The result follows from Lemma 4.2 since $P(0) \in \{1, \alpha, \alpha+1\}$. ∎

We know, by computations, that there are exactly 6 monic irreducible polynomials of degree 2, namely:

$$\begin{array}{ll} P_1 = x^2 + x + \alpha \ , & P_2 = x^2 + x + \alpha + 1 \ , \\ P_3 = x^2 + \alpha x + 1 \ , & P_4 = x^2 + (\alpha+1)\, x + 1 \ , \\ P_5 = x^2 + \alpha x + \alpha \ , & P_6 = x^2 + (\alpha+1)\, x + \alpha + 1 \ . \end{array}$$

We see that:

$$P_3(0) = P_4(0) = P_5(1) = P_6(1) = 1 \ .$$

We are ready to present the main result of the section:

Theorem 4.4. *Let $B \in \mathbb{F}_4[x]$ be any perfect polynomial such that*

$$\gcd(B, I_2) = 1 \ ,$$

where $I_2 = x^{12} + x^9 + x^6 + x^3 + 1$. Let $r \in \{3, 4, 5, 6\}$, $k \in \{1, ..., r\}$, and let $h_1, ..., h_r \in \mathbb{N}^*$ be positive integers. Then for all irreducible monic polynomials $Q_1, ..., Q_r$ of degree 2, the polynomial $C = BA$, where $A = \prod_{k=1}^{r} Q_k^{h_k}$, is not perfect.

Proof: Since $I_2 = P_1 \cdots P_6$, it suffices to prove that A cannot be perfect: If $A = \prod_{k=1}^{r} Q_k^{h_k}$ is perfect, then there exist $k \in \{3, ..., r\}$ and $j \in \{3, 4, 5, 6\}$ such that $Q_k = P_j$. So, there exists $a \in \mathbb{F}_4$ such that $Q_k(a) = 1$. So, h_k must be even by Lemma 4.2. Thus, by Lemma 2.2, $1 + \cdots + Q_k^{h_k} = Q_{l_1}^{b_1} \cdots Q_{l_{r-1}}^{b_{r-1}}$ where $b_1, ..., b_{r-1} \leq 1$. It follows that: $h_k \leq r - 1 \leq 5$. So $h_k \in \{2, 4\}$.

By computations, we can see that for $j \in \{3,4,5,6\}$, the polynomials $1+P_j+P_j^2$ and $1+\cdots+P_j^4$ have irreducible divisors of degree different from 2. So that we are done. ∎

We risk some Conjectures:

5 – Conjectures over $\mathbb{F}_4$

As observed in the introduction there are finitely many odd perfect numbers with k prime factors [12, 8, 10], namely there are at most 2^{4^k} such perfect numbers. An analogue for polynomials in $\mathbb{F}_4[x]$ may be:

Definition 5.1. Let $A \in \mathbb{F}_4[x]$ be a monic polynomial. We say that A is *minimally perfect if it is perfect and has no proper monic perfect divisors d coprime to A/d.* □

Assume that A is a minimally perfect polynomial in our 3 conjectures below.

Moreover, observe that if A is odd (see Proposition 4.3) then, in order to be perfect, the only exponents e allowed in primary divisors $p^e || A$ are either even numbers or odd numbers congruent to 0 or 1 modulo 3.

Conjecture 1. Let $k>0$ be a positive integer. If k is odd then there are finitely many, say $f(k)$, perfect polynomials A over $\mathbb{F}_4$ with k irreducible factors. Perhaps, $f(k)=0$. □

Conjecture 2. Let $r>0$ be a positive integer, let $k=2m>0$ be an even integer. For $j=1,\ldots,r$, let P_j be an irreducible polynomial in $\mathbb{F}_4[x]$ such that

$$\{x,\, x+1,\, x+\alpha,\, x+\alpha+1\} \not\subseteq \{P_1,\ldots,P_r\}\ .$$

If the positive integers $h_1,h_2,\ldots,h_{2m-1},h_{2m}$ are all odd, then the polynomial $A=\prod_{j=1}^{k} P_j^{h_j}$ is perfect if and only if:

- **(a)** For $i \in \{1,\ldots,k\}$ there exists some $j \in \{1,\ldots,k\}$ such that $P_i = P_j+1$ and
- **(b)** $h_j = 2^{m_j}-1$ for some positive integer $m_j>0$. □

Conjecture 3. Let $k = 2m > 0$ be an even integer, and assume that there exists some integer $j \in \{1, ..., k\}$ for which the positive integer h_j is odd. Then there are finitely many perfect polynomials A over $\mathbb{F}_4$ of the form $A = \prod_{i=1}^{k} P_i^{h_i}$. □

ACKNOWLEDGEMENTS – We thank the referee for suggesting that some of our results hold in a more general setting. This resulted in an improved paper.

REFERENCES

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

[**2**] Beard Jr, J.T.B. and Link, M. Leanne – Iterated sums of polynomial divisors, *Libertas Math.,* 17 (1997), 111-124.

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

[**4**] Dickson, L.E. – Finiteness of odd perfect and primitive abundant numbers with n distinct prime factors, *Amer. J. Math.,* 35 (1913), 413–426.

[**5**] Dickson, L.E. – *History of the Theory of Numbers*, Carnegie Institute of Washington, Reprints: Chelsea Publishing Company, New York, 1952, 1966, 1992.

[**6**] Gallardo, L. and Rahavandrainy, O. – On perfect polynomials over $\mathbb{F}_4$, *Portugaliae Mathematica,* 62(1) (2005), 109–122.

[**7**] Gallardo, L. and Rahavandrainy, O. – *Odd perfect polynomials over* $\mathbb{F}_2$, Preprint (2005).

[**8**] Heath-Brown, D.R. – Odd perfect numbers, *Math. Proc. Camb. Philos. Soc.,* 115(2) (1994), 191–196.

[**9**] Lidl, Rudolf and Niederreiter, Harald – *Finite Fields, Encyclopedia of Mathematics and its Applications*, Cambridge University Press, 1983 (Reprinted 1987).

[**10**] Nielsen, Pace P. – An upper bound for odd perfect numbers, *Integers,* electronic only, Paper A14, 3 (2003), 9 p.

[**11**] Pollack, Paul – *Not Always Buried Deep, Selections from Analytic and Combinatorial Number Theory*, 2003 Summer Course Notes, Ross Summer Mathematics Program, 2003 (Reprinted May 9, 2004, available at: http://www.princeton.edu/~pollack/notes/notes.pdf).

[**12**] Pomerance, C. – Multiply perfect numbers. Mersenne primes and effective computability, *Math. Ann.,* 226 (1977), 195–206.

[**13**] Sylvester, J.J. – Sur l'impossibilité de l'existence d'un nombre parfait impair qui ne contient pas au moins 5 diviseurs premiers distincts, *Comptes Rendus Paris,* 106 (1888), 522–526.

Luis Gallardo,
Mathematics, University of Brest,
6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3 – FRANCE
E-mail: luisgall@univ-brest.fr

and

Olivier Rahavandrainy,
Mathematics, University of Brest,
6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3 – FRANCE
E-mail: rahavand@univ-brest.fr