EXISTENCE OF EVEN PERFECT POLYNOMIALS

LUIS H. GALLARDO and OLIVIER RAHAVANDRAINY

Communicated by Alexandru Zaharescu

Perfect polynomials are a natural analogue (in the ring $\mathbb{F}_p[x]$) of multiperfect numbers (in the ring of integers). The latter numbers are classical objects that are poorly understood, since only their definition is simple. We describe, by elementary methods, the most basic objects in the polynomial case of the general problem. We display, for every prime number $p \not\equiv 1 \mod 12$ (resp. $p \not\equiv 1 \mod 24$) many new even non-splitting perfect (resp. unitary perfect) polynomials over $\mathbb{F}_p$. Moreover, for any prime number $p \not\equiv 1 \mod 24$, new bi-unitary perfect polynomials are also given. These examples substantially improve our knowledge about these kinds of polynomials.

AMS 2020 Subject Classification: Primary 11T55; Secondary 11T06.

Key words: (bi-unitary) perfect polynomials, finite fields, characteristic p.

1. **INTRODUCTION**

The paper is about an analogue of perfect numbers over the integers and some variants of them, like unitary perfect or bi-unitary perfect integers. In other words, for a few years, we try to work an analogue of the study of integers n for which the classical function $\sigma_{-1}(n) := \sigma(n)/n = \sum_{d|n} 1/d$ attains the special value 2 (and variants in which the sum is restricted to some special divisors of n).

We replace the ring $\mathbb{Z}$ of integers by the ring $\mathbb{F}_p[x]$ of polynomials over the finite field $\mathbb{F}_p$ with a prime number p of elements. We define (see below) the corresponding sigma functions, so that we essentially have the analogue problem to describe the fixed points of the analogue of the σ_{-1} (and variants) function. We are forced to choose 1 as the quotient (this is why we search for fixed points), since these functions are degree preserving. A more precise discussion follows below. Since we will work with arithmetic functions, replacing the ring $\mathbb{Z}$ by the ring $F_p[x]$ does not necessarily simplify things because in an arbitrary ring, we are unable to describe the irreducible elements.

Let $\mathbb{F}_p$ be the ground field of p elements (with p prime). We say that a divisor D of a monic polynomial A is unitary if D is monic and $\gcd(D, A/D) = 1$. We also say that a divisor D of a monic polynomial A

doi: 10.59277/mrar.2023.25.75.1.47

is bi-unitary if 1 is the greatest common unitary divisor of the polynomials D and A/D. We denote by $\omega(A)$ (resp. $\sigma(A)$, $\sigma^*(A)$, $\sigma^{**}(A)$) the number of distinct monic irreducible factors (resp. the sum of all monic (unitary) divisors, resp. the sum of all monic bi-unitary divisors of A) over $\mathbb{F}_p$. Observe that A, $\sigma(A), \sigma^*(A)$ and $\sigma^{**}(A)$ all have the same degree. The functions σ, σ^* and σ^{**} are multiplicative whereas ω is additive (Lemma 2.1). These facts will be used many times without more reference.

The restriction to monic polynomials is necessary since the sum of all divisors of a non-monic polynomial is zero.

A polynomial is *even* if it has at least one root in $\mathbb{F}_p$, and *odd* if it is not even (see [14] for more details). It *splits* over $\mathbb{F}_p$ if it can be written as a product of linear factors in $\mathbb{F}_p[x]$ (see [18], Definition 1.90). We say that a monic polynomial A is a perfect (resp. unitary perfect) polynomial if $\sigma(A) = A$ (resp. $\sigma^*(A) = A$). In this case, $A = 1$ or $\omega(A) \geq p$ (see [1] and [4]).

A (unitary) perfect polynomial is *indecomposable* if it has no nontrivial factorization as a product of two relatively prime (unitary) perfect polynomials (see Definition 2.3).

Throughout the paper, we shall assume that "a polynomial" means a monic polynomial and that the notion of irreducibility is defined over the field $\mathbb{F}_p$. We shall also suppose that "(unitary) perfect polynomial" means "indecomposable (unitary) perfect polynomial".

The notions of perfectness and unitary perfectness for a polynomial are introduced by E. F. Canaday, J. T. B. Beard et al. (see [1], [2], [4], [9]). These papers essentially characterize the splitting perfect polynomials over $\mathbb{F}_p$ and for odd p, the splitting unitary perfect polynomials over $\mathbb{F}_p$. Recently, we have extended some of their results (see [11] – [16]).

Characterizations of the splitting (unitary) perfect polynomials over $\mathbb{F}_p$ are established in [1, Theorem 4], in [2] and in [4, Theorem 8]. Concerning non-splitting (unitary) perfect polynomials (abbreviated as *n.s.p* and *n.s.u.p*), only numerical examples with fixed primes p are given. More precisely, in [1], examples of n.s.p polynomials with $p \leq 5$, are displayed. Examples of n.s.u.p polynomials in [3], for $p \leq 5$, are improved to $p \leq 19$ in [17] and for $p < 97$ in [6]. Moreover, in the latter paper, the results about the existence of n.s.u.p polynomials are extended further to all primes $p \not\equiv 1 \mod 8$, while in [7] the extension is for some special types of primes $p \equiv 1 \mod 8$ called "square-separables" (see also [8]). We also proved, jointly with P. Pollack ([10]), that the perfect polynomial $\displaystyle\prod_{a \in \mathbb{F}_p} \left((x+a)^2 - \frac{3}{8}\right)^2$, where $p \equiv 11, 17 \mod 24$, discovered in [10], is the only one that is a product of p irreducible polynomials of degree

2 over $\mathbb{F}_p$.

In other words, little significant results have been obtained about the existence of non-splitting perfect (or unitary perfect) polynomials.

In the present paper, we substantially improve on the above results, by showing the existence of n.s.p (resp. n.s.u.p) polynomials over $\mathbb{F}_p$, for every prime number $p \not\equiv 1 \bmod 12$ (resp. $p \not\equiv 1 \bmod 24$).

We denote, as usual by $\mathbb{N}$ (resp. by $\mathbb{N}^*$) the set of nonnegative integers (resp. of positive integers).

We recall and complete in Section 3, the results obtained where $p \in \{2, 3\}$. For $p \geq 5$, inspired by the examples given in [3], we decided to study polynomials with (unlimited) irreducible factors of low degree. We consider polynomials of the form $(x^p - x)^a \cdot \prod_k {P_k}^{b_k}$, where each P_k is irreducible of degree 2. We choose the integers a and b_k in such a manner that $\sigma(x^a)$, $\sigma^*(x^a)$, $\sigma({P_k}^{b_k})$, $\sigma^*({P_k}^{b_k})$ do not split over $\mathbb{F}_p$ and that they are divisible by only irreducible polynomials of degree at most 2. That is why we take $a \in \{2, 3\}$, $b_k = 1$ (resp. $a \in \{2, 3, 4\}$, $b_k \in \{1, 2\}$) for the n.s.p case (resp. for the n.s.u.p case). We build the set Γ of such divisors with degree 2. We prove that the corresponding polynomial is (unitary) perfect and for a fixed integer a, it is the unique one which is indecomposable.

We expected just to find the known examples (cited in [3], [4] and in [17]) and perhaps some new ones but we surprisingly discover many others. More precisely, our main results are the following three theorems:

THEOREM 1.1. *For a prime number $p \not\equiv 1 \bmod 12$, let $m_1, m_2 \in \mathbb{N}$ such that:*

$x^2 + 1 + \ell$ is irreducible for any $\ell \leq m_1$ and $x^2 + 2 + m_1$ is reducible,

$x^2 + x + 1 + \ell$ is irreducible for any $\ell \leq m_2$ and $x^2 + x + 2 + m_2$ is reducible.

Set

$$\Gamma_1 := \{(x + j)^2 + 1 + l : 0 \leq l \leq m_1,\ j \in \mathbb{F}_p\}$$

and

$$\Gamma_2 := \{(x + j)^2 + (x + j) + 1 + l : 0 \leq l \leq m_2,\ j \in \mathbb{F}_p\}.$$

Then $A = (x^p - x)^a \prod_{P \in \Sigma} P$ is perfect over $\mathbb{F}_p$ where:

$$a = 3, \Sigma = \Gamma_1 \text{ if } p \equiv 7 \mod 12$$

and

$$a = 2,\ \Sigma = \Gamma_2 \text{ if } p \equiv 5, 11 \mod 12.$$

Theorem 1.2. *Let p be a prime number such that $p \equiv 3 \bmod 4$ or $p \equiv 17 \bmod 24$. Consider the sets Γ_1 and Γ_2 defined in Theorem 1.1. Then $A = (x^p - x)^a \prod_{P \in \Sigma} P$ is unitary perfect over $\mathbb{F}_p$ where:*

$a = 2, \Sigma = \Gamma_1$ *if* $p \equiv 3 \mod 4$

and

$a = 3,\ \Sigma = \Gamma_2$ *if* $p \equiv 17 \mod 24$.

Theorem 1.3. *Let p be a prime number such that $p \equiv 5 \bmod 8$. Put $-1 = \mu^2$, $\mu < p/2$ and $\alpha = p - 2\mu \geq 1$. Let $m_3, m_4 \in \mathbb{N}$ such that:*

$x^2 + \mu + \ell$ is irreducible for any $\ell \leq m_3$ and $x^2 + \mu + 1 + m_3$ is reducible.

$x^2 - \mu + \ell$ is irreducible for any $\ell \leq m_4$ and $x^2 - \mu + 1 + m_4$ is reducible.

Then $(x^p - x)^4 B$ is unitary perfect where:

$$B = \prod_{j=0}^{p-1} \prod_{\ell=0}^{m_3} ((x+j)^2 + \mu + \ell) \cdot \prod_{j=0}^{p-1} \prod_{\ell=0}^{m_4} ((x+j)^2 - \mu + \ell) \ \textit{if}\ m_3 < \alpha,$$

$$B = \prod_{j=0}^{p-1} \prod_{\ell=0}^{\alpha-1} ((x+j)^2 + \mu + \ell) \cdot \prod_{j=0}^{p-1} ((x+j)^2 - \mu)^2 \ \textit{if}\ m_3 \geq \alpha.$$

We would like to describe how we have proceeded. We transform the equations $\sigma(A) = A$ or $\sigma^*(A) = A$, with the above choices of A, in equations involving only different possible factorizations of polynomials of small degree with coefficients in $\mathbb{F}_p$ and no more use of neither the function σ nor σ^*. This is particularly useful when doing concrete machine computations, since our method quickly gives examples (see Section 7) of non-splitting perfect (or (bi-)unitary perfect) polynomials over $\mathbb{F}_p$ of whatever (reasonable) degree. Older calculations (see [3]) used a probabilistic algorithm which sometimes may run for indefinitely many times without giving an answer. Moreover, since irreducible polynomials of degree 2 over $\mathbb{F}_p$ are involved in the calculations, several of our results use simple arithmetic results (see Section 2) about possible "consecutive" squares or non-squares in $\mathbb{F}_p$.

In Section 7, we give other examples for $p \in \{5, 7, 11\}$ and for more general forms of A. We also give bi-unitary polynomials for $p \not\equiv 1 \mod 24$, and it happens that some of them are also (unitary) perfect polynomials.

If $p \equiv 1 \bmod 12$ (resp. $p \equiv 1 \bmod 24$), our method fails, and we are unable to show even n.s.p polynomials (resp. even n.s.u.p polynomials) over $\mathbb{F}_p$. The reason is that the polynomial $\sigma(x^k)$ (resp. $\sigma^*(x^k)$) splits for every $k \leq 4$. We should then choose $a_j \geq 5$ so that we would obtain non quadratic irreducible divisors of A for which the possible solution appears non-trivial (for us).

The proofs of the theorems are done, in a case study mode, with appropriate congruences for the prime p in each of them.

2. USEFUL FACTS

We need the following results. Some of them are obvious (or cited in [3] and [9]), so we omit their proofs.

For $A, B \in \mathbb{F}_p[x]$ and for $n \in \mathbb{N}^*$, we write: $A^n \| B$ if $A^n \mid B$ but $A^{n+1} \nmid B$. We sometimes consider, without explicit mention, the elements of $\mathbb{F}_p$ as the integers $0, 1, \ldots, p-1$.

For $A \in \mathbb{F}_p[x]$, we denote by $\omega(A)$ (resp. $\sigma(A)$, $\sigma^*(A)$, $\sigma^{**}(A)$) the number of distinct monic irreducible factors (resp. the sum of all monic (unitary) divisors, resp. the sum of all monic bi-unitary divisors) of A over $\mathbb{F}_p$. We get

Lemma 2.1. i) *ω is an additive function: $\omega(A_1A_2) = \omega(A_1) + \omega(A_2)$ if* $\gcd(A_1, A_2) = 1$.

ii) *σ is multiplicative: $\sigma(A_1A_2) = \sigma(A_1) \cdot \sigma(A_2)$ if* $\gcd(A_1, A_2) = 1$.

iii) *σ^* and σ^{**} are also multiplicative.*

Proof. Assuming that $\gcd(A_1, A_2) = 1$, a polynomial d divides A_1A_2 if and only if ($d = d_1d_2$ with $d_1 \mid A_1$ and $d_2 \mid A_2$). We easily see that $\omega(A_1A_2) = \omega(A_1) + \omega(A_2)$. Now, for σ (similar proofs for σ^* and for σ^{**}), one has:

$$\sigma(A_1A_2) = \sum_{d_1 \mid A_1} (d_1 \cdot \sum_{d_2 \mid A_2} d_2) = \sum_{d_1 \mid A_1} (d_1 \sigma(A_2)) = \sigma(A_2) \cdot \sum_{d_1 \mid A_1} d_1 = \sigma(A_2) \cdot \sigma(A_1).$$

□

Lemma 2.2. *If $A = A_1A_2$ is (unitary) perfect over $\mathbb{F}_q$ and if* $\gcd(A_1, A_2) = 1$*. Then A_1 is (unitary) perfect if and only if A_2 is (unitary) perfect.*

Definition 2.3. Let A be a nonconstant (unitary) perfect polynomial over $\mathbb{F}_p$. We say that A is *indecomposable* if it has no nontrivial factorization as a product of two relatively prime (unitary) perfect polynomials.

Lemma 2.4. *If $A = A_1B$ is (unitary) indecomposable perfect where A_1 splits and B is odd, then $\sigma(A_1)$ (resp. $\sigma^*(A_1)$) does not split (over $\mathbb{F}_p$).*

Proof. If $\sigma(A_1)$ splits, then $\sigma(A_1) = A_1$ and thus A_1 is perfect. It is impossible by indecomposability. □

In the rest of the paper, we suppose that "(unitary) perfect polynomial" means "indecomposable (unitary) perfect polynomial".

Lemma 2.5. *The polynomial $1 + x + x^2$ (resp. $1 + x + x^2 + x^3$) splits over $\mathbb{F}_p$ if and only if $p \equiv 1 \bmod 3$ (resp. $p \equiv 1 \bmod 4$).*

Lemma 2.6. *The polynomial $x^2 + 1$ (resp. $x^3 + 1$, $x^4 + 1$) splits over $\mathbb{F}_p$ if and only if $p \equiv 1 \bmod 4$ (resp. $p \equiv 1 \bmod 6$, $p \equiv 1 \bmod 8$).*

2.1. **Case** $p \equiv 7 \bmod 12$

In this case, $p \equiv 3 \bmod 4$ and $p \equiv 1 \bmod 6$. Thus -1 is not a square so that $\sigma^*(x^2) = x^2+1$ is irreducible and $\sigma(x^3) = (x+1)(x^2+1)$ does not split. Moreover, $\sigma^*(x^3) = x^3+1 = (x+1)(x^2-x+1)$ splits over $\mathbb{F}_p$.

We denote by m_1 the integer such that $-1, -2, \ldots, -1-m_1$ are all not squares and $-2-m_1 = {\delta_1}^2$ is a square in $\mathbb{F}_p$. We put:

$$\Gamma_1 := \{(x+j)^2 + 1 + l : j \in \mathbb{F}_p,\ 0 \leq l \leq m_1\},$$

so that Γ_1 is a non-empty set of irreducible quadratic polynomials.

By direct computations with Legendre's Symbol, we get

Lemma 2.7. *If $p \equiv 3 \bmod 4$, then either* (2 *is a square*) *or* (-2 *is a square*)*.*

Lemma 2.8. i) *If $p \equiv 3 \bmod 4$ and $2 = \xi^2$, then $x^2-\xi x+1$ and $x^2+\xi x+1$ are both irreducible and $x^4+1 = (x^2-\xi x+1)(x^2+\xi x+1)$.*

ii) *If $p \equiv 3 \bmod 4$ and $-2 = \xi^2$, then $x^2-\xi x-1$ and $x^2+\xi x-1$ are both irreducible and $x^4+1 = (x^2-\xi x-1)(x^2+\xi x-1)$.*

Corollary 2.9. *Let A be unitary perfect over $\mathbb{F}_p$, with $p \equiv 3 \bmod 4$. Then:*

i) *$(x^2-\xi x+1)^2$ divides A if x^4 and $(x-\xi)^4$ both divide A provided $2 = \xi^2$.*

ii) *$(x^2+\xi x-1)^2$ divides A if x^4 and $(x+\xi)^4$ both divide A provided $-2 = \xi^2$.*

Proof. We only prove i). In this case, $x^2-\xi x+1$ divides both $\sigma^*(x^4)$ and $\sigma^*((x-\xi)^4)$. □

Remark 2.10. According to Corollary 2.9, if $p \equiv 3 \bmod 4$ and if $\deg(Q) = 2$ then $\sigma^*(Q^2) = Q^2+1$ may be irreducible. Hence, we do not take $a = 4$ for the unitary case, in order to avoid the possible fact that A would be divisible by an irreducible polynomial of degree greater than 2.

2.2. **Case** $p \equiv 11 \bmod 12$

In this case, $p \equiv 3 \bmod 4$ and $p \equiv 5 \bmod 6$. Thus, $\sigma^*(x^2) = x^2+1$ is irreducible and $\sigma(x^3) = (x+1)(x^2+1)$ does not split. Furthermore, $\sigma(x^2) = x^2+x+1$ and x^2-x+1 are both irreducible. So,

$$\sigma^*(x^3) = x^3+1 = (x+1)(x^2-x+1)$$

does not split. We denote by m_2 the integer such that $-3, -3-4, \ldots, -3-4m_2$ are all not squares but $-7-4m_2 = 4{\delta_2}^2$ is a square in $\mathbb{F}_p$. Then, for any $l \leq m_2$,

$x^2 \pm x + 1$ is irreducible and $x^2 \pm x + 2 + m_2 = (\pm x + \dfrac{1}{2} + \delta_2)(\pm x + \dfrac{1}{2} - \delta_2)$ is reducible.

More generally, if $p \equiv 2 \bmod 3$, then the Legendre Symbol $(\frac{-3}{p})$ equals -1. Hence, $x^2 + x + 1$ and $x^2 - x + 1$ are both irreducible over $\mathbb{F}_p$. Therefore, we get the following sets of irreducible quadratic polynomials (over $\mathbb{F}_p$):

$$\Gamma_2 := \{P_{jl} = (x+j)^2 + (x+j) + 1 + l : j \in \mathbb{F}_p,\ 0 \leq l \leq m_2\},$$
$$\Gamma_3 := \{Q_{jl} = (x+j)^2 - (x+j) + 1 + l : j \in \mathbb{F}_p,\ 0 \leq l \leq m_2\}.$$

Lemma 2.11. *One has:* $\Gamma_2 = \Gamma_3$ *whenever* $p \equiv 2 \bmod 3$.

Proof. It suffices to remark that $P_{jl} = (x+j)^2 + x + j + 1 + l = (x + j + 1)^2 - (x + j + 1) + 1 + l = Q_{j+1\ l}$. □

2.3. Case $p \equiv 1 \bmod 8$

If $p \equiv 1 \mod 24$, then $\sigma(x^a)$, $\sigma^*(x^a)$ and $\sigma^*(x^4)$ all split for $a \in \{2, 3\}$. So we suppose that $p \equiv 17 \mod 24$. In this case, only, $\sigma^*(x^3) = x^3 + 1 = (x+1)(x^2 - x + 1)$ does not split. We shall consider the subset Γ_3 which equals Γ_2 (by Lemma 2.11).

3. CASE $p \in \{2, 3\}$

3.1. n.s.p polynomials

We get by direct computations or from [9], all n.s.p polynomials A over $\mathbb{F}_p$:

$$A \in \{x^2(x+1)(x^2+x+1), x(x+1)^2(x^2+x+1)\} \text{ if } p = 2,$$
$$A \in \{S(x), S(x+1), S(x+2), T(x)\} \text{ if } p = 3, \text{ where}$$
$$S(x) = x^3(x+1)^2(x+2)(x^2+1) \text{ and}$$
$$T(x) = (x^3 - x)^2(x^2+1)(x^2+x+2)(x^2+2x+2).$$

3.2. n.s.u.p polynomials

If $p = 2$, then A is of the form $x^a(x+1)^b(x^2+x+1)^c$ so that $\omega(A) \leq 3$ and thus $A \in \{x^3(x+1)^2(1+x+x^2), x^2(x+1)^3(1+x+x^2)\}$ (see [4]).

If $p = 3$, then A is of the form

$$x^a(x+1)^b(x+2)^c(x^2+1)^u(x^2+x+2)^v(x^2+2x+2)^w,$$

where $0 \leq a, b, c \leq 3$ and $0 \leq u, v, w \leq 2$, $(u, v, w) \neq (0, 0, 0)$.

By direct computations, A is unitary perfect over $\mathbb{F}_3$ if and only if

$$A = ((x^3 - x)^2(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2))^{3^n}, \text{ for some } n \in \mathbb{N}.$$

4. PROOF OF THEOREM 1.1

In this section, we suppose that $A := A_1 B$ is (indecomposable) perfect where

$$A_1 = \prod_{j=0}^{p-1} (x + j)^a = (x^p - x)^a \text{ and } B = \prod_{P \in \Sigma} P, \quad a \in \{2, 3\},$$

$\Sigma \neq \emptyset$ is a set of irreducible quadratic polynomials.

Lemma 4.1. *The prime number p satisfies: $p \equiv 2 \bmod 3$ or $p \equiv 3 \bmod 4$.*

Proof. If $p \equiv 1 \bmod 3$ and $p \equiv 1 \bmod 4$ then $\sigma(A_1)$ splits, which is impossible by Lemma 2.4. □

We distinguish three cases: $p \equiv 5$, 7 or $11 \bmod 12$. We prove only Propositions 4.2 and 4.3. The other proofs are similar.

4.1. Case $p \equiv 5 \bmod 12$

In this case, $p \equiv 1 \bmod 4$ and $p \equiv 5 \bmod 6$. Thus, -3 is not a square, $\sigma(x^2)$ is irreducible but $\sigma(x^3) = (x + 1)(x^2 + 1)$ splits. Lemma 2.4 implies that $a = 2$. We consider the subset Γ_2 defined in Section 2.2.

Proposition 4.2. *A is perfect if and only if $\Sigma = \Gamma_2$ so that*

$$A = (x^p - x)^2 \cdot \prod_{P \in \Gamma_2} P \quad \textit{with} \quad \omega(A) = (m_2 + 2)p.$$

Proof. Sufficiency is obtained by direct computations. We get:

$$\sigma(A_1) = \prod_{j \in \mathbb{F}_p} ((x + j)^2 + (x + j) + 1),$$

$$\sigma(\prod_{P \in \Gamma_2} P) = \prod_{j \in \mathbb{F}_p} \prod_{l=0}^{m_2} ((x + j)^2 + (x + j) + 2 + l).$$

Recall that $x^2 + x + 2 + m_2 = (x + \frac{1}{2} + \delta_2)(x + \frac{1}{2} - \delta_2)$ splits. Therefore,

$$\prod_{j \in \mathbb{F}_p} ((x + j)^2 + (x + j) + 2 + m_2) = (x^p - x)^2.$$

Hence,

$$\sigma(A_1 \prod_{P \in \Gamma_2} P) = (x^p - x)^2 \cdot \prod_{j \in \mathbb{F}_p} \prod_{l=0}^{m_2} ((x+j)^2 + (x+j) + 1 + l) = A_1 \prod_{P \in \Gamma_2} P.$$

Thus, $A_1 \prod_{P \in \Gamma_2} P$ is perfect.

Necessity. Now, we suppose that A is perfect. For $j \in \mathbb{F}_p$,

$$Q_j = (x+j)^2 + x + j + 1 = \sigma((x+j)^2)$$

is an irreducible divisor of $\sigma(A) = A$. Thus, for any $0 \leq l \leq \max(0, m_2 - 1)$, $\sigma(Q_j + l) = Q_j + 1 + l$ are all irreducible and they all divide $\sigma(A) = A$. Hence, $\Gamma_2 \subset \Sigma$ and $\Sigma = \Gamma_2$ by indecomposability, since $A_1 \prod_{P \in \Gamma_2} P$ is perfect. $\square$

Examples. One has: $m_2 = 1$ if $p = 5$ and $m_2 = 2$ if $p = 17$.

4.2. **Case** $p \equiv 7 \bmod 12$

Since $p \equiv 1 \bmod 3$, Lemma 2.4 implies that $a = 3$.

Proposition 4.3. *A is perfect if and only if $\Sigma = \Gamma_1$ so that*

$$A = (x^p - x)^3 \cdot \prod_{j=0}^{p-1} \prod_{\ell=0}^{m_1} ((x+j)^2 + 1 + \ell), \ \textit{with} \ \ \omega(A) = (m_1 + 2)p.$$

Proof. We directly get sufficiency: we remark that $\sigma(x^3) = (x+1)(x^2+1)$, with $x^2+1, \cdots, x^2+1+m_1$ all irreducible and $x^2 + 2 + m_1 = (x+\delta_1)(x-\delta_1)$.

Put $B_1 := \prod_{P \in \Gamma_1} P = \prod_{j=0}^{p-1} \cdot \prod_{\ell=0}^{m_1} ((x+j)^2 + 1 + \ell)$.

We compare $\sigma(A_1 B_1) = \sigma(A_1)\sigma(B_1)$ and $A_1 B_1$:

$$\sigma(A_1) = \prod_{j=0}^{p-1} (x+j+1)((x+j)^2+1) = (x^p - x) \prod_{j=0}^{p-1} ((x+j)^2 + 1),$$

$$\begin{aligned} \sigma(B_1) &= \prod_{j=0}^{p-1} \cdot \prod_{\ell=0}^{\max(0,m_1-1)} ((x+j)^2 + 2 + \ell) \cdot \prod_{j=0}^{p-1} ((x+j)^2 + 2 + m_1), \\ &= \prod_{j=0}^{p-1} \cdot \prod_{\ell=0}^{\max(0,m_1-1)} ((x+j)^2 + 2 + \ell) \cdot \prod_{j=0}^{p-1} (x+j+\delta_1)(x+j-\delta_1), \\ &= (x^p - x)^2 \cdot \prod_{j=0}^{p-1} \cdot \prod_{\ell=0}^{\max(0,m_1-1)} ((x+j)^2 + 2 + \ell). \end{aligned}$$

We obviously see that $\sigma(A_1B_1) = \sigma(A_1)\sigma(B_1) = A_1B_1$. Thus A_1B_1 is perfect.

Necessity. As in the proof of Proposition 4.2, we see that $\Gamma_1 \subset \Sigma$ and $\Sigma = \Gamma_1$. □

Examples. One has: $m_1 = 1$ if $p = 7$ and $m_1 = 0$ if $p = 19$.

4.3. **Case** $p \equiv 11 \bmod 12$

In this case, $p \equiv 3 \bmod 4$ and $p \equiv 5 \bmod 6$. Thus, $\sigma(x^2) = x^2 + x + 1$ and $\sigma(x^3) = (x + 1)(x^2 + 1)$ do not split. Moreover, $x^2 + 1, \ldots, x^2 + 1 + m_1$, $x^2+x+1, \ldots, x^2+x+1+m_2$ are all irreducible and $x^2+2+m_1 = (x+\delta_1)(x-\delta_1)$, $x^2 + x + 2 + m_1 = (x + \frac{1}{2} + \delta_2)(x + \frac{1}{2} - \delta_2)$. Thus $a \in \{2, 3\}$ and we consider the sets Γ_1, Γ_2. As in (the proof of) Proposition 4.3, we take $\Sigma = \Gamma_2$ (resp. $\Sigma = \Gamma_1$) if $a = 2$ (resp. $a = 3$). We get:

Proposition 4.4. i) *If $a = 2$ then A is perfect if and only if*

$$A = (x^p - x)^2 \cdot \prod_{j=0}^{p-1} \prod_{\ell=0}^{m_2-1} ((x + j)^2 + (x + j) + 1 + l),$$

with $\omega(A) = (m_2 + 2)p$.

ii) *If $a = 3$ then A is perfect if and only if*

$$A = (x^p - x)^3 \cdot \prod_{j=0}^{p-1} \prod_{\ell=0}^{m_1-1} ((x + j)^2 + 1 + l),$$

with $\omega(A) = (m_1 + 2)p$.

Examples. One has: $m_1 = m_2 = 0$ if $p = 11$ and $m_1 = 3, m_2 = 0$ if $p = 23$.

5. **PROOF OF THEOREM 1.2**

We set $A := A_1B$ where $A_1 = (x^p - x)^a$, $a \in \{2, 3\}$ and $B = \displaystyle\prod_{P \in \Sigma} P$, where Σ is a subset of quadratic irreducible polynomials.

We suppose that A is unitary perfect: $\sigma^*(A_1)\sigma^*(B) = A_1B$.

Again, Lemma 2.4 implies that $p \not\equiv 1 \mod 6$ or $p \not\equiv 1 \mod 8$.

Lemma 5.1. *The prime number p satisfies: $p \equiv 5 \bmod 6$ or $p \equiv 3 \bmod 4$ or $p \equiv 5 \bmod 8$.*

In this section, we suppose that $p \equiv 3 \mod 4$ or $p \equiv 17 \mod 24$. We consider three cases: $p \equiv 7 \mod 12$, $p \equiv 11 \mod 12$ and $p \equiv 17 \mod 24$. The proofs of Propositions 5.2 and 5.3 are similar to those of Propositions in Section 4, so they are omitted.

5.1. **Case** $p \equiv 7 \bmod 12$

In this case, $p \equiv 3 \bmod 4$ and $p \equiv 1 \bmod 6$. Lemma 2.4 implies that $a \neq 3$. From Remark 2.10, we do not take $a = 4$. Hence, we choose $a = 2$ and we consider $\Gamma_1 = \{(x+j)^2 + 1 + \ell : j \in \mathbb{F}_p, 0 \leq \ell \leq m_1\}$ defined in Section 2.1.

Proposition 5.2. *The polynomial A is unitary perfect if and only if $\Sigma = \Gamma_1$ and $\Omega = \emptyset$, so that $A = (x^p - x)^2 \cdot \prod_{P \in \Gamma_1} P$, with $\omega(A) = (m_1 + 2)p$.*

5.2. **Case** $p \equiv 11 \bmod 12$

In this case, $p \equiv 3 \bmod 4$ and $p \equiv 5 \bmod 6$. From Remark 2.10, we do not take $a = 4$ so that $a \in \{2, 3\}$. Moreover, $x^2 + 1$ and $x^3 + 1 = (x+1)(x^2 - x + 1)$ do not split. We consider Γ_1 if $a = 2$ and Γ_2 if $a = 3$.

Proposition 5.3. *The polynomial A is unitary perfect where:*

$$A = (x^p - x)^2 \cdot \prod_{j=0}^{p-1} \prod_{\ell=0}^{m_1} ((x+j)^2 + 1 + \ell), \text{ with } \omega(A) = (m_1 + 2)p,$$

$$A = (x^p - x)^3 \cdot \prod_{j=0}^{p-1} \prod_{\ell=0}^{m_2} ((x+j)^2 - (x+j) + 1 + \ell), \text{ with } \omega(A) = (m_2 + 2)p.$$

5.3. **Case** $p \equiv 17 \bmod 24$

In this case, $p \equiv 1 \bmod 8$ and $p \equiv 5 \bmod 6$. Thus, $x^2 + 1$ and $x^4 + 1$ split but $\sigma^*(x^3) = x^3 + 1 = (x+1)(x^2 - x + 1)$ does not split over $\mathbb{F}_p$. We take $a = 3$ and we consider $\Gamma_3 = \Gamma_2$ (Section 2.2, Lemma 2.11).

Proposition 5.4. *If $p \equiv 17 \bmod 24$, then $A = (x^p - x)^3 \cdot \prod_{P \in \Gamma_2} P$ is unitary perfect over $\mathbb{F}_p$, with $\omega(A) = (m_2 + 2)p$.*

Example. For $p = 41$, one has $m_2 = 4$.

6. PROOF OF THEOREM 1.3

We only sketch the proof (similar arguments as before).

6.1. Preliminaries

The polynomial $\sigma^*(x^2)$ splits because $p \equiv 1 \mod 4$; $\sigma^*(x^3)$ also splits if $p \equiv 13 \mod 24$. If $p \equiv 5 \mod 24$, then $\sigma^*(x^3) = (x+1)(x^2-x+1)$ does not split (and $(x^p - x)^3 \prod_{P \in \Gamma_2} P$ is a n.s.u.p polynomial).

Since $p \equiv 1 \mod 4$ and $p \not\equiv 1 \mod 8$, $-1 = \mu^2$ is a square but μ and $p - \mu$ are not squares (we choose $\mu < \frac{p}{2}$). Thus, $\sigma^*(x^4) = (x^2+\mu)(x^2-\mu)$ does not split without more conditions on $p \equiv 5 \mod 8$. So, we choose only polynomials of the form $(x^p - x)^4 B$, where B is odd. Moreover, 2 is not a square and thus $\alpha := p - 2\mu$ is a square. Set $\alpha = -\gamma^2$.

Let m_3 be the integer such that $-\mu, -\mu-1, \ldots, -\mu-m_3$ are all not squares and $-\mu - m_3 - 1$ is a square. Put ${\delta_3}^2 = -\mu - m_3 - 1$.

Let m_4 be the integer such that $\mu, \mu - 1, \ldots, \mu - m_4$ are all not squares, but $\mu - m_4 - 1 = {\delta_4}^2$ is a square.

We get the following sets of irreducible quadratic polynomials:

$$\Gamma_{41} := \{(x+j)^2 + \mu + l : j \in \mathbb{F}_p,\ 0 \le l \le m_3\},$$
$$\Gamma_{42} := \{(x+j)^2 - \mu + l : j \in \mathbb{F}_p,\ 0 \le l \le m_4\}, \Gamma_4 := \Gamma_{41} \cup \Gamma_{42},$$
$$\Gamma_5 := \{(x+j)^2 + \mu + l : j \in \mathbb{F}_p,\ 0 \le l \le \alpha - 1\},$$
$$\Gamma_6 := \{(x+j)^2 - \mu : j \in \mathbb{F}_p\}.$$

We set $A := A_1 B_1 B_2$ where $A_1 = (x^p - x)^4$ and $B_1 = \prod_{P \in \Sigma} P,\ B_2 = \prod_{Q \in \Omega} Q^2$, Σ and Ω are disjoint subsets of quadratic irreducible polynomials such that $\Sigma \cup \Omega \neq \emptyset$ (because A does not split). The set Ω may be non-empty by Corollary 6.6 below.

We suppose that A is unitary perfect: $\sigma^*(A_1)\sigma^*(B_1)\sigma^*(B_2) = A_1 B_1 B_2$.

Lemma 6.1. *One has:*

$$x^2 + \mu + m_3 + 1 = (x + \delta_3)(x - \delta_3),\ x^2 - \mu + m_4 + 1 = (x + \delta_4)(x - \delta_4),$$
$$(x^2 - \mu)^2 + 1 = x^2(x^2 + \alpha) = x^2(x + \gamma)(x - \gamma).$$

Lemma 6.2. $\alpha = 1$ *if and only if* $p = 5$.

Proof. One has in $\mathbb{F}_p$:

$$\alpha = 1 \iff \mu + 1 = -\mu \iff \mu^2 = -1 = 2\mu \iff \mu = 2 \iff p = 5.$$

□

Remark 6.3. We may have $\mu + a = p - \mu + b$, for some $0 \leq a \leq m_3$ and for some $0 \leq b \leq m_4$.

Lemma 6.4. *If $m_3 < \alpha$, then $\Gamma_{41} \cap \Gamma_{42} = \emptyset$.*

Proof. For any $l \leq m_3$ and $t \leq m_4$, one has: $\mu + l \leq \mu + m_3 < \mu + \alpha = p - \mu \leq \mu + t$. Therefore, $\mu + l \not\equiv p - \mu + t \mod p$. □

Lemma 6.5. *If $m_3 \geq \alpha$, then for any $l < \alpha$, $x^2 + \mu + l$ is irreducible, $\Gamma_5 \subset \Gamma_{41}$, $\Gamma_5 \cap \Gamma_6 = \emptyset$ and $\Gamma_{41} \cap \Gamma_6 \neq \emptyset$.*

Proof. If $l < \alpha$, then $l < m_3$ and thus $x^2 + \mu + l$ is irreducible. Therefore, $\Gamma_5 \subset \Gamma_{41}$.

Moreover, $\mu + l < \mu + \alpha = p - \mu$. So, $\mu + l \not\equiv p - \mu \mod p$ and $\Gamma_5 \cap \Gamma_6 = \emptyset$. Finally, $x^2 + \mu + \alpha = x^2 - \mu \in \Gamma_{41} \cap \Gamma_6$. □

Corollary 6.6. *If $m_3 \geq \alpha$, then $((x+j)^2 - \mu)^2$ divides A for any $j \in \mathbb{F}_p$.*

Proof. One has: $S = x^2 - \mu = x^2 + \mu + \alpha = \sigma^*(x^2 + \mu + \alpha - 1)$. So, S divides $\sigma^*(A) = A$. S also divides $\sigma^*(x^4)$ and thus it divides $\sigma^*(A) = A$. □

6.2. **Case** $m_3 < \alpha$

Here, by Lemma 6.4, we only need Γ_4 (but neither Γ_5 nor Γ_6). So, $\Gamma_4 \subset \Sigma$ and $\Omega = \emptyset$. By direct computations, we get $\sigma^*(A_1 \prod_{P \in \Gamma_4} P) = A_1 \prod_{P \in \Gamma_4} P$. Thus $A_1 \prod_{P \in \Gamma_4} P$ is unitary perfect and $\Sigma = \Gamma_4$ by indecomposability.

Note that $\omega(A) = (m_3 + m_4 + 3)p$.

Example. For $p = 37$, one has: $\mu = 6,\ m_3 = 0 < \alpha = 25,\ m_4 = 1$.

6.3. **Case** $m_3 \geq \alpha$

By Lemma 6.5 and by Corollary 6.6, one has: $\Gamma_5 \subset \Sigma$ and $\Gamma_6 \subset \Omega$. $A = A_1 \cdot \prod_{P \in \Gamma_5} P \cdot \prod_{Q \in \Gamma_6} Q^2$ is unitary perfect, with $\omega(A) = (\alpha + 2)p$. We get then $\Gamma_5 = \Sigma$ and $\Gamma_6 = \Omega$, still by indecomposability.

Example. For $p = 13$, one has: $\mu = 5,\ m_3 = \alpha = 3$.

7. SOME COMPUTATIONS

7.1. Other n.s.p polynomials for $p = 11$

We set $A = \prod_{j=0}^{10} (x+j)^{a_j} B$, where $a_j \in \{1, 2, 3\}$ and $B = \prod_{P \in \Sigma} P$ is a product of irreducible quadratic polynomials, $\Sigma \subset \Gamma_1 \cup \Gamma_2$.

By direct computations (that lasted only about 28 minutes) in which we consider all possible cases on the a_j's, there exist such n.s.p polynomials if and only if either ($a_j = 2$ for any j and $\Sigma = \Gamma_2$) or ($a_j = 3$ for any j and $\Sigma = \Gamma_1$).

7.2. Other n.s.u.p polynomials for $p \in \{5, 7, 11\}$

We set $A = \prod_{j=0}^{p-1} (x+j)^{a_j} \cdot \prod_{P \in \Sigma} P \cdot \prod_{Q \in \Omega} Q^2$, $2 \leq a_j \leq 4$, $\Sigma \subset \bigcup_{j=1}^{5} \Gamma_j$ and $\Omega \subset \Gamma_6$.

Put, for $1 \leq k \leq 3$, $\Lambda_k := \{j \in \mathbb{F}_p : a_j = k+1\}$. Our computations consist of checking equalities $\sigma^*(A_1A_2A_3B) = A_1A_2A_3B$ for $p = 5, 7, 11$ and for all pairwise disjoint subsets Λ_1, Λ_2, Λ_3 of $\mathbb{F}_p$ such that $\Lambda_1 \cup \Lambda_2 \cup \Lambda_3 = \mathbb{F}_p$.

- For $p = 5$, one has $m_3 = \alpha = 1$ and we get unitary perfect polynomials if ($\Lambda_1 = \{0\}$, $\Lambda_3 = \mathbb{F}_5 \backslash \{0\}$), ($\Lambda_1 = \{0, 1\}$, $\Lambda_3 = \mathbb{F}_5 \backslash \{0, 1\}$), ($\Lambda_1 = \{0, 1, 2\}$, $\Lambda_3 = \{3, 4\}$), ($\Lambda_1 = \mathbb{F}_5 \setminus \{4\}$, $\Lambda_3 = \{4\}$, already cited in [4]).

- For $p = 5$, no unitary perfect polynomials exist if ($\Lambda_3 = \emptyset$, $\Lambda_1 \neq \emptyset$ and $\Lambda_2 \neq \emptyset$).

- For $p = 7$, one has $m_1 = 1$. No unitary perfect polynomials exist if ($\Lambda_3 = \emptyset$, $\Lambda_1 \neq \emptyset$ and $\Lambda_2 \neq \emptyset$).

- For $p = 11$, one has $m_1 = m_2 = 0$, no unitary perfect polynomials exist if ($\Lambda_3 = \emptyset$ and $\Lambda_1 \neq \emptyset$ and $\Lambda_2 \neq \emptyset$).

7.3. Examples of bi-unitary perfect (b.u.p) polynomials

We refer to [5] for basic notions of bi-unitary perfect polynomials. In particular, we get for an irreducible polynomial $P \in \mathbb{F}_p[x]$:
$\sigma^{**}(P^2) = 1 + P^2 = \sigma^*(P^2)$, $\sigma^{**}(P^3) = (P+1)(P^2+1)$,
$\sigma^{**}(P^4) = (P+1)(P^3+1)$, $\sigma^{**}(P^6) = (P^4+1)(P^2+P+1)$.

7.3.1. **Case** $p \in \{2, 3\}$

If $p = 2$, then A is of the form $x^a(x+1)^b(x^2+x+1)$ so that $\omega(A) = 3$ and thus $A \in \{x^3(x+1)^4(1+x+x^2), x^4(x+1)^3(1+x+x^2)\}$ (see [19]).

If $p = 3$, then A is of the form

$$x^a(x+1)^b(x+2)^c(x^2+1)^u(x^2+x+2)^v(x^2+2x+2)^w,$$

where $0 \leq a, b, c \leq 7$ and $0 \leq u, v, w \leq 1$, $(u, v, w) \neq (0, 0, 0)$.

By direct computations, A is b.u.p over $\mathbb{F}_3$ if and only if $A(x)$, $A(x+1)$ or $A(x+2)$ takes the above form with $(a, b, c, u, v, w) \in J$ where

$$J = \{(3,4,5,1,0,0), (1,4,6,1,0,1), (2,2,2,1,1,1), (3,3,3,1,1,1), (5,5,7,1,1,1)\}.$$

7.3.2. **Case** $p \not\equiv 1 \mod 24$ **and** $p \geq 5$

Perfect polynomials in Theorem 1.1 are b.u.p if $p \equiv 7 \mod 12$.

Unitary perfect polynomials in Theorem 1.2 are b.u.p if $p \equiv 7 \mod 12$.

S is b.u.p where:

$$S = (x^p - x)^4 \prod_{P \in \Gamma_2} P \text{ if } p \equiv 5 \mod 12,$$

$$S = (x^p - x)^6 \prod_{P \in \Gamma_2} P \text{ if } p \equiv 17 \mod 24.$$

S is neither perfect nor unitary perfect.

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. **62** (1977), 283–291.

[2] J.T.B. Beard Jr., *Perfect polynomials revisited.* Publ. Math. Debrecen **38** (1991), 5–12.

[3] J.T.B. Beard Jr., A.T. Bullock Jr., and M.S. Harbin, *Infinitely many perfect and unitary perfect polynomials.* Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **63** (1977), 294–303.

[4] J.T.B. Beard Jr., *Unitary perfect polynomials over $GF(q)$*. Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **62** (1977), 417–422.

[5] J.T.B. Beard Jr., *Bi-Unitary perfect polynomials over $GF(q)$*. Ann. Mat. Pura Appl. **149** (1987), 61–68.

[6] J.T.B. Beard Jr. and M.S. Harbin, *Non splitting unitary perfect polynomials over $GF(q)$*. Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **66** (1979), 179–185.

[7] J.T.B. Beard Jr., K.J. Doyle, and K.I. Mandelberg, *Non splitting unitary perfect polynomials over $GF(q)$*. Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **68** (1980), 397–401.

[8] J.T.B. Beard Jr., *Are all primes $32k + 17$ $(k > 0)$ square separable?* Amer. Math. Monthly **87** (1980), 744–745.

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

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

[11] L.H. Gallardo and O. Rahavandrainy, *Even perfect polynomials over* $\mathbb{F}_2$ *with four prime factors.* Int. J. Pure Appl. Math. **52** (2009), 301–314.

[12] L.H. Gallardo and O. Rahavandrainy, *On perfect polynomials over* $\mathbb{F}_p$ *with* p *irreducible factors.* Port. Math. **69** (2012), 283–303.

[13] L.H. Gallardo and O. Rahavandrainy, *On even (unitary) perfect polynomials over* $\mathbb{F}_2$*.* Finite Fields Appl. **18** (2012), 920–932.

[14] L.H. Gallardo and O. Rahavandrainy, *Perfect polynomials over* $\mathbb{F}_p$ *with* $p+1$ *irreducible divisors.* Acta Math. Univ. Comenian. (N.S.) **83** (2014), 93–112.

[15] L.H. Gallardo and O. Rahavandrainy, *Characterization of Sporadic perfect polynomials over* $\mathbb{F}_2$*.* Funct. Approx. Comment. Math. **55** (2016), 7–21.

[16] L.H. Gallardo and O. Rahavandrainy, *There are finitely many even perfect polynomials over* $\mathbb{F}_p$ *with* $p+1$ *irreducible divisors.* Acta Math. Univ. Comenian. (N.S.) **85** (2016), 261–275.

[17] M.S. Harbin, *Non-splitting unitary perfect polynomials over* $GF(p)$*,* $7 \leq p \leq 19$. Notices Amer. Math. Soc **25** (1978), 351.

[18] R. Lidl and H. Niederreiter, *Finite Fields.* Encyclopedia Math. Appl. **20**, Cambridge Univ. Press, 1983.

[19] O. Rahavandrainy, *On Bi-unitary perfect polynomials over* $\mathbb{F}_2$*.* ArXiv: 1810.09697, 2018.

Received April 12, 2019

Univ. Brest UMR CNRS 6205
Laboratoire de Mathématiques de Bretagne Atlantique
F-29238 Brest, France
Luis.Gallardo@univ-brest.fr,
Olivier.Rahavandrainy@univ-brest.fr