International Electronic Journal of Algebra
Volume 9 (2011) 85-102

ON SPLITTING PERFECT POLYNOMIALS OVER $\mathbb{F}_{p^p}$

Luis H. Gallardo and Olivier Rahavandrainy

Received: 10 March 2010; Revised: 29 July 2010
Communicated by Abdullah Harmancı

Abstract. We characterize some splitting perfect polynomials in $\mathbb{F}_q[x]$, where $q = p^p$ and p is a prime number.

Mathematics Subject Classification (2000): 11T55, 11T06
Keywords: Artin-Schreier extension, finite fields, splitting polynomials, perfect polynomials

1. Introduction

Let q be a power of a prime p. For a monic polynomial $A \in \mathbb{F}_q[x]$, let $\omega(A)$ be the number of distinct irreducible monic factors of A, and let $\sigma(A)$ be the sum of all monic divisors of A (included the trivial divisors 1 and A):

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

If $\sigma(A) = A$, then we call A a perfect polynomial.
This is the appropriate analogue for polynomials of the notion of "multiperfect" numbers for two reasons: a) it is easy to see that A is perfect if and only if A divides $\sigma(A)$ and b) we are forced to consider monic polynomials only, since the sum of all divisors of a non-monic polynomial is trivially equal to 0. Canaday [2] and Beard [1] studied principally the case when $q = p$ that even now is far from being understood. Assume now that $q \neq p$. Gallardo and Rahavandrainy [4,5] investigated the case $q = 4$ mainly considering polynomials with a small number of prime factors in order to be able to get some results. So for general $q \neq p$, it is natural to consider first the study of some class of simple polynomials. A natural choice is to consider splitting polynomials that is, polynomials with all their roots in the same field where are the coefficients. Beard [1] does that for the case $q = p$. Recently, Gallardo and Rahavandrainy [7] studied splitting perfect polynomials over quadratic extensions ($q = p^2$). On the other hand the p-th extension field of $\mathbb{F}_p$, that is the Artin-Schreier extension of the prime field $\mathbb{F}_p$ has been recently [10,3,9] considered in relation to the minimal period of Bell numbers. Some arithmetic properties of the

prime number p appear there naturally. We decided then to consider the study of splitting perfect polynomials over the field $\mathbb{F}_{p^p}$. Lemmas 2.9, 2.10, 3.2 contain some simple arithmetic properties of the prime number p useful for our work. Of course, we just scratch the subject in this paper.

More precisely, let p be a prime number and let $q = p^p$. We denote by $\mathbb{F}_q$ the field with q elements. It is the splitting field of the irreducible Artin-Schreier polynomial $f(x) = x^p - x - 1 \in \mathbb{F}_p[x]$.
The splitting perfect polynomials over $\mathbb{F}_4$ are known (see [4, Theorem 3.4]) so we shall assume in the rest of the paper that p is an odd prime.

By Lemma 2.4, a splitting perfect polynomial A can be expressed as

$$A = A_0 \cdots A_r = \prod_{j \in \mathbb{F}_p} (x - a_0 - j)^{h_{0j}} \cdots \prod_{j \in \mathbb{F}_p} (x - a_r - j)^{h_{rj}},$$

where

$$\begin{aligned} & r + 1 = \frac{\omega(A)}{p} \in \mathbb{N}, \quad 0 \leq r \leq \frac{q}{p} - 1, \\ & A_i = \prod_{j \in \mathbb{F}_p} (x - a_i - j)^{h_{ij}}, \ \gcd(A_i, A_l) = 1 \text{ if } i \neq l \\ & a_i \in \mathbb{F}_q, \ a_i - a_l \notin \mathbb{F}_p \text{ for } 0 \leq i \neq l \leq r. \end{aligned}$$

By changing $A(x)$ by $A(x + a_0)$, and by Lemma 2.2, we may suppose that $a_0 = 0$. We say that A is trivially perfect if for any $0 \leq i \leq r$, the polynomial A_i is perfect. In that case, A is perfect and for any $0 \leq i \leq r$, there exist $N_i, n_i \in \mathbb{N}$ such that:

$$h_{ij} = N_i p^{n_i} \text{ for any } j \in \mathbb{F}_p, \ N_i \mid p - 1.$$

Observe (see Corollary 2.8) that there exists an infinite number of splitting trivially perfect polynomials with $\omega(A) = (r+1)p$. There exists also an infinite number of splitting non-trivially perfect polynomials with $\omega(A) = q$ (see Theorem 3 in [1]), namely those of the form $A = \prod_{b_i \in \mathbb{F}_q} (x - b_i)^{Np^m - 1}$ where $N, m \in \mathbb{N}$ and N divides $q - 1$.

We do not know if all splitting perfect polynomials are trivially perfect. However, we are able to classify some of them in our main result below:

Theorem 1.1. *Let $0 \leq r \leq \frac{q}{p} - 1$ be an integer. In the following cases, any splitting perfect polynomial, with $\omega(A) = (r+1)p$, is trivially perfect:*
i) $0 \leq r \leq p^2 - 1$ and $a_i + a_l, \ a_i + a_l - a_k \notin \mathbb{F}_p$ for $i \neq l \neq k$.
ii) $0 \leq r \leq 5$.

After some useful technical lemmas in section 2 we prove Theorem 1.1 in section 3. The proof of part ii) requires some involved computations with non-linear systems over $\mathbb{F}_q/\mathbb{F}_p$.

2. Preliminary

In this section, we recall some useful results for the next sections. Let G be the Galois group of the polynomial $f(x) = x^p - x - 1$. It is well known that G is a cyclic group of order p, generated by the Frobenius morphism:

$$\pi : \mathbb{F}_q^* \to \mathbb{F}_q^*,\ \pi(t) = t^p.$$

The orbit, under the action of G, of an element $\omega \in \mathbb{F}_q$ but outside $\mathbb{F}_p$ contains exactly p elements: $\omega, \omega^p, \dots, \omega^{p^{p-1}}$.
In the following, we put: $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$.

Lemma 2.1. *i) The polynomial $x^l - 1$ splits in $\mathbb{F}_p$ if and only if $l = Np^m$, where $N, m \in \mathbb{N}$ and N divides $p-1$.*
ii) The polynomial $x^l - 1$ splits in $\mathbb{F}_q$ if and only if $l = Np^m$, where $N, m \in \mathbb{N}$ and N divides $q-1$.
In that case, if $d = \gcd(p-1, N)$, then $N = d + rp$ for some $r \in \mathbb{N}$, and for some $j_1, \dots, j_d \in \mathbb{F}_p$, $b_1, \dots, b_r \in \mathbb{F}_q - \mathbb{F}_p$, one has:

$$x^l - 1 = (x^N - 1)^{p^m} = \Big(\prod_{\mu=1}^{d} (x - j_\mu) \ \prod_{\lambda=1}^{r} \big((x - b_\lambda)(x - {b_\lambda}^p) \cdots (x - {b_\lambda}^{p^{p-1}})\big) \ \Big)^{p^m}.$$

Lemma 2.2. *The polynomial $P(x) \in \mathbb{F}_q[x]$ is perfect if and only if for all $a \in \mathbb{F}_q$, $P(x+a)$ is perfect.*

Definition 2.3. For a monic polynomial $A \in \mathbb{F}_q[x]$, we define the integer $\omega(A)$ as the number of distinct irreducible monic factors of A.

Lemma 2.4. (see Lemma 2.5 in [5]) *If A is a splitting perfect polynomial over $\mathbb{F}_q$, then $\omega(A) \equiv 0 \mod p$.*
More precisely, if $\omega(A) = (r+1)p$, then $A = \prod_{j=0}^{p-1} (x - a_0 - j)^{h_{0j}} \cdots \prod_{j=0}^{p-1} (x - a_r - j)^{h_{rj}}$, where

$$a_0, \dots, a_r \in \mathbb{F}_q,\ a_i - a_l \notin \mathbb{F}_p \text{ if } 0 \le i \ne l \le r$$
$$h_{ij} = N_{ij} p^{n_{ij}} - 1, N_{ij}, n_{ij} \in \mathbb{N} \text{ and } N_{ij} \text{ divides } q-1.$$

Remark 2.5. In the rest of paper, by Lemmata 2.4 and 2.2, a splitting perfect polynomial A such that $\omega(A) = (r+1)p$ will be always expressed as

$$A = A_0 \cdots A_r = \prod_{j=0}^{p-1} (x - a_0 - j)^{h_{0j}} \cdots \prod_{j=0}^{p-1} (x - a_r - j)^{h_{rj}},$$

where

$$\begin{array}{l} A_i = \prod_{j=0}^{p-1} (x - a_i - j)^{h_{ij}}, \ \gcd(A_i, A_l) = 1 \ \textit{if } i \neq l \\ a_0 = 0, \ a_i \in \mathbb{F}_q, \ a_i - a_l \notin \mathbb{F}_p \ \textit{for } 0 \leq i \neq l \leq r, \\ h_{ij} = N_{ij} p^{n_{ij}} - 1, N_{ij}, n_{ij} \in \mathbb{N}, \ N_{ij} \mid q - 1. \end{array}$$

Lemma 2.6. (see Theorem 5 in [1]) *The polynomial* $A_0 = \prod_{j=0}^{p-1} (x - j)^{h_{0j}}$ *is perfect over* $\mathbb{F}_p$ *if and only if for any* $i, j,$ $h_{0i} = h_{0j} = Np^m - 1,$ *where* $N, m \in \mathbb{N}$ *and* N *divides* $p - 1$.

Now, we proceed to show a crucial lemma which allows us to establish Theorem 1.1.

Lemma 2.7. *For* $r \in \mathbb{N}^*$, *let* $A = A_0 A_1 \cdots A_r = A_0 B$ *be a splitting perfect polynomial over* $\mathbb{F}_q$. *If* $N_{0j} \mid p - 1$ *for any* j, *then the polynomials* A_0 *and* B *are both perfect.*

Proof. According to Notation 2.5, we have:
$A_0 = \prod_{j=0}^{p-1} (x - j)^{h_{0j}}$ and $B = \prod_{j=0}^{p-1} \prod_{i=1}^{r} (x - a_i - j)^{h_{ij}}$.
For any j, since $N_{0j} \mid p-1$, none of the monomials $x - a_i - l$ $(l \in \mathbb{F}_p, \ i \geq 1)$, divides $\sigma((x-j)^{h_{0j}})$. So we may put:

$$\begin{array}{l} \sigma((x-j)^{h_{0j}}) = \prod_{l=0}^{p-1} (x - l)^{\alpha_l^{0j0}}, \\ \sigma((x - a_1 - j)^{h_{1j}}) = \prod_{l=0}^{p-1} (x - l)^{\alpha_l^{1j0}} (x - a_1 - l)^{\alpha_l^{1j1}} \cdots (x - a_r - l)^{\alpha_l^{1jr}}, \\ \vdots \\ \sigma((x - a_r - j)^{h_{rj}}) = \prod_{l=0}^{p-1} (x - l)^{\alpha_l^{rj0}} (x - a_1 - l)^{\alpha_l^{rj1}} \cdots (x - a_r - l)^{\alpha_l^{rjr}}. \end{array}$$

Hence, by considering degrees, we obtain, for any $j \in \{0, \ldots, p-1\}$:

$$h_{0j} = \sum_{l=0}^{p-1} \alpha_l^{0j0}, \ h_{ij} = \sum_{l=0}^{p-1} (\alpha_l^{ij0} + \cdots + \alpha_l^{ijr}) \ \text{ if } 1 \leq i \leq r.$$

Since $\sigma(A) = A$, by comparing exponent of $x - a_i - l$ in $\sigma(A)$ and in A, we get for any i, l:

$$h_{0l} = \sum_{j=0}^{p-1} (\alpha_l^{0j0} + \alpha_l^{1j0} + \cdots + \alpha_l^{rj0}),\ h_{il} = \sum_{j=0}^{p-1} (\alpha_l^{1ji} + \cdots + \alpha_l^{rji}) \text{ if } 1 \leq i \leq r.$$

We can deduce that:

$$\sum_{j=0}^{p-1}\sum_{l=0}^{p-1} \alpha_l^{0j0} = \sum_{j=0}^{p-1} h_{0j} = \sum_{l=0}^{p-1} h_{0l} = \sum_{l=0}^{p-1}\sum_{j=0}^{p-1} (\alpha_l^{0j0} + \cdots + \alpha_l^{rj0}),$$

$$\sum_{j=0}^{p-1}\sum_{l=0}^{p-1} (\alpha_l^{1j0} + \cdots + \alpha_l^{1jr}) = \sum_{j=0}^{p-1} h_{1j} = \sum_{l=0}^{p-1} h_{1l} = \sum_{l=0}^{p-1}\sum_{j=0}^{p-1} (\alpha_l^{1j1} + \cdots + \alpha_l^{rj1}),$$

$$\vdots$$

$$\sum_{j=0}^{p-1}\sum_{l=0}^{p-1} (\alpha_l^{rj0} + \cdots + \alpha_l^{rjr}) = \sum_{j=0}^{p-1} h_{rj} = \sum_{l=0}^{p-1} h_{rl} = \sum_{l=0}^{p-1}\sum_{j=0}^{p-1} (\alpha_l^{1jr} + \cdots + \alpha_l^{rjr})$$

Thus:

$$\begin{aligned} \sum_{j=0}^{p-1} (h_{1j} + \cdots + h_{rj}) &= \sum_{j=0}^{p-1}\sum_{l=0}^{p-1} \big((\alpha_l^{1j0} + \cdots + \alpha_l^{1jr}) + \cdots + (\alpha_l^{rj0} + \cdots + \alpha_l^{rjr})\big) \\ &= \sum_{j=0}^{p-1}\sum_{l=0}^{p-1} \big((\alpha_l^{1j1} + \cdots + \alpha_l^{rj1}) + \cdots + (\alpha_l^{1jr} + \cdots + \alpha_l^{rjr})\big) \end{aligned}$$

It follows that:

$$\sum_{j=0}^{p-1}\sum_{l=0}^{p-1} (\alpha_l^{1j0} + \cdots + \alpha_l^{rj0}) = 0,$$

so that:

$$\alpha_l^{1j0} = \cdots = \alpha_l^{rj0} = 0, \text{ for any } j, l.$$

Therefore, we have $\sigma(\prod_{j=0}^{p-1} (x-j)^{h_{0j}}) = \prod_{j=0}^{p-1} (x-j)^{h_{0j}}$ and we are done. □

Using Lemmas 2.6 and 2.7, we immediately obtain:

Corollary 2.8. *For any $r \in \mathbb{N}^*$, the splitting polynomial $A = \prod_{j=0}^{p-1}\prod_{i=0}^{r} (x - a_i - j)^{N_{ij}p^{n_{ij}}-1}$ is perfect over $\mathbb{F}_q$ whenever for all $0 \leq i \leq r$, $N_{ij} = N_{il},\ n_{ij} = n_{il}$ for all $j, l \in \mathbb{F}_p$.*

Lemma 2.9. *If a prime number v divides $p^p - 1$ then either $(v \equiv 1 \mod p)$ or $(p \equiv 1 \mod v)$.*

Lemma 2.10. *For any odd integer t, the integer $1 + tp$ does not divide $p^p - 1$.*

Proof. Put $m = 1 + tp$ and $f(p) = p^p - 1$. Assume that m divides $f(p)$. Then $m = n_1 n_2$ where n_1 divides $m_1 = p - 1$ and n_2 divides $m_2 = 1 + p + \cdots + p^{p-1}$. It is well known and it is easy to prove that $\gcd(m_1, m_2) = 1$. So,

$$(1): \ e = \gcd(n_1, n_2) = 1.$$

Now, each prime factor v of n_2 divides m_2, so that $v \equiv 1 \mod p$, by Lemma 2.9. It follows that $n_2 \equiv 1 \mod p$. Moreover, clearly $m \equiv 1 \mod p$. Thus:

$$(2): \ n_1 \equiv 1 \mod p.$$

Observe that m_2 is odd and m is even, since p and t are both odd. Thus, n_2 is odd and n_1 is even since $m = n_1 n_2$.
By (2), we may write: $n_1 = 1 + sp$, with $s \geq 0$. If $s = 0$, then $n_1 = 1$. This is impossible since n_1 is even. So, $s \geq 1$ and we get:

$$n_1 = 1 + sp \geq 1 + p > p - 1 = m_1.$$

This is impossible since n_1 is a positive divisor of m_1. This proves the result. □

3. Proof of Theorem 1.1

We recall that we use Notation 2.5 for a splitting perfect polynomial.

3.1. Case (i). If N_{ij} divides $p - 1$ for all $0 \leq i \leq r$ and for all $j \in \mathbb{F}_p$, then we can apply Lemma 2.7. So, the polynomials $B = \prod_{j=0}^{p-1} \prod_{i=1}^{r} (x - a_i - j)^{h_{ij}}$ and $A_0 = \prod_{j=0}^{p-1} (x - a_0 - j)^{h_{0j}}$ are both perfect. We remark that $\omega(B) = rp$. So the result follows by induction on r.
If there exist $1 \leq i_1 \leq r$ and $j_1 \in \mathbb{F}_p$ such that $N_{i_1 j_1} = N$ does not divide $p - 1$, then there exist $i_2 \geq 1$ and $j_2 \in \mathbb{F}_p$ such that the monomial $x - a_{i_2} - j_2$ divides $x^N - 1$. So, the monomial $x - a_{i_1} - j_1 - a_{i_2} - j_2$ divides $\sigma((x - a_{i_1} - j_1)^{h_{i_1 j_1}})$ and thus divides $\sigma(A) = A$. So, either $(a_{i_1} + a_{i_2} \in \mathbb{F}_p)$ or (there exists $1 \leq u \leq r$ such that $a_{i_1} + a_{i_2} - a_u \in \mathbb{F}_p$). It is impossible by hypothesis.

3.2. Case (ii) with $w(A) \leq 2p$. - Case $w(A) = p$
It is immediate from Lemma 2.6.
- Case $w(A) = 2p$
Such polynomial may be of the form: $A = A_0 A_1 = \prod_{j=0}^{p-1} (x - j)^{h_{0j}} \prod_{j=0}^{p-1} (x - a_1 - j)^{h_{1j}}$.

We have two cases:
Case 1: If either (for all j, $N_{0j}|p-1$) or (for all j, $N_{1j}|p-1$), then by Lemma 2.7, A_0 and A_1 are both perfect, with $\omega(A_0) = \omega(A_1) = p$. The result follows from previous case.
Case 2: If there exist $j, l \in \mathbb{F}_p$ such that N_{0j} and N_{1l} do not divide $p-1$ then, we have:

$$1 + \cdots + (x-j)^{h_{0j}} = \frac{1}{x-j-1}\ ((x-j)^{N_{0j}} - 1)^{p^{n_{0j}}},$$

$$1 + \cdots + (x-a_1-l)^{N_{1l}} = \frac{1}{x-a_1-l-1}\ ((x-a_1-l)^{N_{1l}} - 1)^{p^{n_{1l}}}.$$

Put:

$$d_j = \gcd(N_{0j}, p-1),\ d_l = \gcd(N_{1l}, p-1), \gamma_0, \gamma_1 \notin \mathbb{F}_p,\ \gamma_0^{N_{0j}} = \gamma_1^{N_{1l}} = 1.$$

Then, the orbit of γ_0 contains exactly p elements and we have: $N_{0j} = d_j + p$.
It follows that: $1 \equiv p \equiv N_j \equiv 0 \mod d_j$, so $d_j = 1$ and $N_{0j} = 1 + p$.
Analogously, we obtain: $N_{1l} = 1 + p$.
But, by Lemma 2.10, $1 + p$ does not divide $q - 1$. It is impossible.

3.3. Case $w(A) \geq 3p$. We need the following lemmas.

Lemma 3.1. *Let A be a splitting perfect polynomial with $\omega(A) = (r+1)p$. If $(x-a)^{Np^m-1}$ divides A and if N does not divide $p-1$, then $N = d + \lambda p$, where $d = \gcd(N, p-1)$, $\lambda \equiv 0 \mod d$ and $1 \leq \lambda \leq r$.*

Proof. If $N = dd_1$, where d_1 divides $\dfrac{p^p - 1}{p-1}$, then, by Lemma 2.9, d_1 is congruent to 1 modulo p, so that $d_1 = 1 + \mu p$. Thus, $N = dd_1 = d + \mu dp$ has the claimed form. Put $\lambda = \mu d$. We have:

$$d + \lambda p = \omega((x-a)^{Np^m-1}) \leq \omega(A) = (r+1)p,\ \text{where } d \geq 1,$$

We conclude that: $1 \leq \lambda \leq r$. ☐

Lemma 3.2. *i) If 3 divides $p^p - 1$ then $p \equiv 1 \mod 3$.*
ii) If $d = \gcd(1+2p, p-1)$, then $d \in \{1, 3\}$.
iii) If $1+2p$ divides $p^p - 1$ then $p \equiv 2 \mod 3$ and $\gcd(1+2p, p-1) = 1$.
iv) If $1+4p$ divides $p^p - 1$ then either $(p = 3)$ or $(p \equiv 1 \mod 3)$.
v) The integers $1+2p$ and $1+4p$ do not simultaneously divide $p^p - 1$.

Proof. i): by Lemma 2.9, since $3 \not\equiv 1 \mod p$.
ii): the integer d must divide $1 + 2p + p - 1 = 3p$ and $d \neq p$. We get the result.
iii): If $p \equiv 1 \mod 3$, then by ii), we have: $\gcd(1+2p, p-1) = 3$. Any prime divisor

$r \neq 3$ of $1+2p$ divides $p^p - 1$, so $r \equiv 1 \mod p$, since r does not divide $p-1$. Thus, we may write:

$$1 + 2p = 3(1 + up), \text{ for some integer } u.$$

Hence: $1 \equiv 1 + 2p = 3(1 + up) \equiv 3 \mod p$. It is impossible. We are done.
If $p = 3$, we see that $7 = 1 + 2p$ does not divide $26 = p^p - 1$.
iv): If $p \equiv 2 \mod 3$, then 3 divides $1 + 4p$ and $p^p - 1$, so $p \equiv 1 \mod 3$ by i). It is impossible.
v): by iii) and iv). □

The following lemma gives the possible forms of $h_{ij} = N_{ij}p^{n_{ij}} - 1$.

Lemma 3.3. *Let A be a splitting perfect polynomial, with $w(A) = (r+1)p$, and $(x-a)^{Np^m-1}$ a monomial dividing A such that N does not divide $p-1$:*
if $r \in \{2, 3\}$, then $N = 1 + 2p$,
if $r \in \{4, 5\}$, then either $(N \in \{1 + 2p, 2 + 4p\})$ or $(N = 1 + 4p)$.

Proof. If N does not divide $p - 1$, then by Lemma 3.1, $N = d + \lambda p$, where $d = \gcd(N, p-1)$, $1 \leq \lambda \leq r$, $d \mid \lambda$.
If $r = 2$, then $1 \leq \lambda \leq 2$.
If $\lambda = 1$, then $N = 1 + p$ which does not divide $p^p - 1$ by Lemma 2.10.
If $\lambda = 2$, then $N \in \{1 + 2p, 2 + 2p\}$. If $N = 2 + 2p$, then $1 + p$ divides $p^p - 1$. It is impossible by Lemma 2.10.
If $r = 3$, then $1 \leq \lambda \leq 3$.
If $\lambda \leq 2$, then $N = 1 + 2p$.
If $\lambda = 3$, then $N \in \{1 + 3p, 3 + 3p\}$. Thus, either $1 + 3p$ or $1 + p$ divides $p^p - 1$. It is impossible by Lemma 2.10.
If $r = 4$, then $1 \leq \lambda \leq 4$.
If $\lambda \leq 3$, then $N = 1 + 2p$.
If $\lambda = 4$, then $N \in \{1 + 4p, 2 + 4p, 4 + 4p\}$. We can exclude the case $N = 4 + 4p$ since $1 + p$ does not divide $p^p - 1$. Furthermore, by Lemma 3.2, the integers $1 + 4p$ and $1 + 2p$ do not simultaneously divide $p^p - 1$.
If $r = 5$, then $1 \leq \lambda \leq 5$.
If $\lambda \leq 4$, then either $(N \in \{1 + 2p, 2 + 4p\})$ or $(N = 1 + 4p)$.
If $\lambda = 5$, then $N \in \{1 + 5p, 5 + 5p\}$. We can exclude this case since, by Lemma 2.10, $1 + 5p$ and $1 + p$ do not divide $p^p - 1$. We are done. □

3.3.1. *Case (ii) and* $\omega(A) = 3p$. Such polynomial is of the form:

$$A = A_0A_1A_2 = \prod_{j=0}^{p-1}(x-j)^{h_{0j}} \prod_{j=0}^{p-1}(x-a_1-j)^{h_{1j}} \prod_{j=0}^{p-1}(x-a_2-j)^{h_{2j}}.$$

Case 1: If there exists $i \in \{0,1,2\}$ such that for all j, $N_{ij} \mid p-1$, then, we may suppose $i = 0$. So, by Lemma 2.7, A_0 and A_1A_2 are both perfect. It follows by section 3.2, that A_0 and $B = A_1A_2$ are both trivially perfect.

Case 2: If there exist $j_0, j_1, j_2 \in \mathbb{F}_p$ such that N_{0j_0}, N_{1j_1} and N_{2j_2} do not divide $p-1$ then, by lemma 3.3, we must have: $N_{0j_0} = N_{1j_1} = N_{2j_2} = 1+2p = N$. Since the only monomials which interfere are: $x-j, x-a_1-j$ and $x-a_2-j$, for $j \in \mathbb{F}_p$, we can write:

$$x^N - 1 = (x-1)\prod_{j=0}^{p-1}(x-a_1-j)(x-a_2-j),$$

Thus, for some $l \in \mathbb{F}_p$, the monomials $x-2a_1-j-l,\ x-a_1-a_2-j-l$ must divide $\sigma(A) = A$, since they divide $\sigma((x-a_1-l)^{h_{1l}})$. Analogously, for some $s \in \mathbb{F}_p$, the monomials $x-2a_2-j-s,\ x-a_1-a_2-j-s$ must divide A. So, we must have: $2a_1-a_2, 2a_2-a_1, a_1+a_2 \in \mathbb{F}_p$. It follows that $3a_1, 3a_2 \in \mathbb{F}_p$. So, $p = 3$. But, in this case $N = 1+2p = 7$ does not divide $26 = p^p - 1$. We are done.

3.3.2. *Convention.* We consider the quotient space $\mathbb{F}_q/\mathbb{F}_p$. For $b_1, \ldots, b_m \in \mathbb{F}_q/\mathbb{F}_p$, we write: $b_1 \cdots b_m = 0$ to mean that at least one of the b_j's equals 0.
Furthermore, we denote in the same manner an element a of $\mathbb{F}_q$ and its class $\bar{a}$ modulo $\mathbb{F}_p$.

3.3.3. *Case (ii) and* $w(A) = 4p$. Such polynomial is of the form: $A = A_0A_1A_2A_3 = A_0B$.

Case 1: If there exists i (say $i = 0$) such that for all j, $N_{0j} \mid p-1$, then, by Lemma 2.7, A_0 and B are both perfect, and by Sections 3.2 and 3.3.1, they are both trivially perfect.

Case 2: If there exist $j_0, \ldots, j_3 \in \mathbb{F}_p$ such that $N_{0j_0}, \ldots, N_{3j_3}$ do not divide $p-1$. Thus, by Lemma 3.3, we must have: $N_{0j_0} = \cdots = N_{3j_3} = 1+2p = N$.
Therefore, there exist $a, b \in \{a_1, a_2, a_3\}$ and $j_a, j_b \in \mathbb{F}_p$, such that $a \neq b$ and the monomials $x-a-j_a$ and $x-b-j_b$ divide $x^N - 1$.
So, for $1 \leq i \leq 3$, the monomials $x-a_i-j_i-a-j_a$ and $x-a_i-j_i-b-j_b$ divide $\sigma((x-a_i-j_i)^{h_{ij_i}})$ and hence divide A.
Therefore, a_i+a, a_i+b, $a_i+a-a_{r_i}$, $a_i+b-a_{s_i} \in \mathbb{F}_p$, for some $r_i, s_i \in \{1,2,3\}$.

We may suppose $a = a_1, b = a_2$, so the following conditions must be satisfied:

$$\begin{cases} (2a_1 - a_2 \in \mathbb{F}_p) \text{ or } (2a_1 - a_3 \in \mathbb{F}_p) \\ (2a_2 - a_1 \in \mathbb{F}_p) \text{ or } (2a_2 - a_3 \in \mathbb{F}_p) \\ (a_1 + a_2 \in \mathbb{F}_p) \text{ or } (a_1 + a_2 - a_3 \in \mathbb{F}_p) \\ (a_1 + a_3 \in \mathbb{F}_p) \text{ or } (a_1 + a_3 - a_2 \in \mathbb{F}_p) \\ (a_2 + a_3 \in \mathbb{F}_p) \text{ or } (a_2 + a_3 - a_1 \in \mathbb{F}_p). \end{cases}$$

By Convention 3.3.2, we obtain the following system of equations with unknowns $a_1, a_2, a_3 \in \mathbb{F}_q/\mathbb{F}_p$, $a_1 \neq a_2 \neq a_3$:

$$(\circ) : \begin{cases} (2a_1 - a_2)(2a_1 - a_3) = 0 \\ (2a_2 - a_1)(2a_2 - a_3) = 0 \\ (a_1 + a_2)(a_1 + a_2 - a_3) = 0 \\ (a_1 + a_3)(a_1 + a_3 - a_2) = 0 \\ (a_2 + a_3)(a_2 + a_3 - a_1) = 0, \end{cases}$$

which is impossible by Lemma 3.4. We are done.

Lemma 3.4. *System* $(\circ)$ *has no distinct solutions in* $\mathbb{F}_q/\mathbb{F}_p$.

Proof. : If $a_1, a_2, a_3 \in \mathbb{F}_q/\mathbb{F}_p$ satisfy this system, then any possible case leads to contradiction:

<u>Case $2a_1 - a_2 = 0$</u>

if $2a_2 - a_1 = 0$ then we have: $3(a_1 - a_2) = 0 \in \mathbb{F}_p$, so $p = 3$. Thus, $N = 1 + 2p = 7$ does not divide $26 = p^p - 1$. It is impossible.

if $2a_2 - a_3 = 0$ then $2a_1 + a_2 - a_3 = 0$. Thus $a_1 + a_2 \neq 0$, since $a_1 - a_3 \neq 0$. So we must have $a_1 + a_2 - a_3 = 0$.
Therefore, $a_1 = (2a_1 + a_2 - a_3) - (a_1 + a_2 - a_3) = 0$. It is impossible.

<u>Case $2a_1 - a_3 = 0$</u>

if $2a_2 - a_1 = 0$ then $a_1 + 2a_2 - a_3 = 0$. Thus $a_1 + a_2 \neq 0$, since $a_2 - a_3 \neq 0$. So we must have $a_1 + a_2 - a_3 = 0$.
Therefore, $a_2 = (2a_2 + a_1 - a_3) - (a_1 + a_2 - a_3) = 0$. It is impossible.

if $2a_2 - a_3 = 0$ then $2(a_1 - a_2) = 0$. It is impossible. $\square$

3.3.4. *Case (ii) and $w(A) = 5p$.* Case 1: If there exists i (say $i = 0$) such that for all j, $N_{0j} \mid p - 1$, then, by Lemma 2.7, A_0 and $B = A_1 \cdots A_4$ are both perfect and thus trivially perfect.
Case 2: If there exist $j_0, \ldots, j_4 \in \mathbb{F}_p$ such that $N_{0j_0}, \ldots, N_{4j_4}$ do not divide $p-1$. Thus, by Lemma 3.3, we must have: either $(N_{0j_0} = \cdots = N_{4j_4} = 1 + 4p)$ or $(N_{0j_0}, \ldots, N_{4j_4} \in \{1 + 2p, 2 + 4p\})$.

Case 21:
If $N_{0j_0} = \cdots = N_{4j_4} = 1 + 4p = N$, then there exist $l_1, \ldots, l_4 \in \mathbb{F}_p$ such that the four monomials $x - a_i - l_i$, $1 \leq i \leq 4$, divide $x^N - 1$.
Moreover, $p \neq 5$ since $1 + 4p$ must divide $p^p - 1$.
As in the proof in Section 3.3.3, for all $i \in \{1, \ldots, 4\}$, there exist $l_i, k_i, t_i \in \{1, \ldots, 4\}$ such that:

$$\begin{cases} (2a_i - a_{l_i} \in \mathbb{F}_p) \\ (a_i + a_{k_i} \in \mathbb{F}_p) \text{ or } (a_i + a_{k_i} - a_{t_i} \in \mathbb{F}_p). \end{cases}$$

We observe that $a_1, \ldots, a_4$ play symmetric roles, and we use Convention 3.3.2, so we can reduce to the following system of equations:

$$(*) : \begin{cases} 2a_1 - a_2 = 0 \\ (2a_2 - a_1)(2a_2 - a_3) = 0 \\ (2a_3 - a_1)(2a_3 - a_2)(2a_3 - a_4) = 0 \\ (2a_4 - a_1)(2a_4 - a_2)(2a_4 - a_3) = 0 \\ (a_1 + a_2)(a_1 + a_2 - a_3)(a_1 + a_2 - a_4) = 0 \\ (a_1 + a_3)(a_1 + a_3 - a_2)(a_1 + a_3 - a_4) = 0 \\ (a_1 + a_4)(a_1 + a_4 - a_2)(a_1 + a_4 - a_3) = 0 \\ (a_2 + a_3)(a_2 + a_3 - a_1)(a_2 + a_3 - a_4) = 0 \\ (a_2 + a_4)(a_2 + a_4 - a_1)(a_2 + a_4 - a_3) = 0 \\ (a_3 + a_4)(a_3 + a_4 - a_1)(a_3 + a_4 - a_2) = 0, \end{cases}$$

which is impossible by Lemma 3.5.

Case 22:
If $N_{0j_0}, \ldots, N_{4j_4} \in \{1+2p, 2+4p\} = \{N, 2N\}$, then there exist $a, b \in \{a_1, a_2, a_3, a_4\}$ and $j_a, j_b \in \mathbb{F}_p$, such that the monomials $x - a - j_a$ and $x - b - j_b$ divide $x^N - 1$. So, for $1 \leq i \leq 4$, the monomials $x - a_i - j_i - a - j_a$ and $x - a_i - j_i - b - j_b$ divide $\sigma((x - a_i - j_i)^{h_{ij_i}})$ and A.

As in the proof of Proposition 3.3.3, we may suppose $a = a_1, b = a_2$. Moreover, a_1 and a_2 (resp. a_3 and a_4) play symmetric roles. So, the following conditions must be satisfied:

$$(**) : \begin{cases} (2a_1 - a_2)(2a_1 - a_3) = 0 \\ (2a_2 - a_1)(2a_2 - a_3)(2a_2 - a_4) = 0 \\ (a_1 + a_2)(a_1 + a_2 - a_3)(a_1 + a_2 - a_4) = 0 \\ (a_1 + a_3)(a_1 + a_3 - a_2)(a_1 + a_3 - a_4) = 0 \\ (a_1 + a_4)(a_1 + a_4 - a_2)(a_1 + a_4 - a_3) = 0 \\ (a_2 + a_3)(a_2 + a_3 - a_1)(a_2 + a_3 - a_4) = 0 \\ (a_2 + a_4)(a_2 + a_4 - a_1)(a_2 + a_4 - a_3) = 0. \end{cases}$$

Lemma 3.6 implies that $p = 5$. Hence, we have modulo $\mathbb{F}_p$:

either $(a_2 = 2a_1,\ a_3 = -a_1,\ a_4 = -2a_1)$ or $(a_2 = -a_1,\ a_3 = 2a_1,\ a_4 = -2a_1)$.

If $N = 1 + 2p = 11$, then:

$$x^N - 1 = (x-1) \prod_{j=0}^{p-1} (x - a_1 - j)(x - a_2 - j), \text{ where } a_2 = 2a_1 \text{ or } a_2 = -a_1.$$

Put: $\Lambda_1 = \{b \in \mathbb{F}_q/\mathbb{F}_p\ :\ (x+b) \text{ divides } x^{11} - 1\}$.
For all $b, c \in \Lambda_1$, we see that either $(b + 2c \in \mathbb{F}_p)$ or $(b + c \in \mathbb{F}_p)$.
By computations, if $\alpha \in \mathbb{F}_q$ such that $\alpha^p - \alpha - 1 = 0$, then $b_1 = \alpha^4 + 3\alpha^3 + \alpha^2 + 2\alpha + 4$ and $c_1 = 3\alpha^4 + 4\alpha^3 + 3\alpha^2 + 3\alpha + 2$ belong to Λ_1, but $b_1 + 2c_1, b_1 + c_1 \notin \mathbb{F}_p$. It is impossible.

If $N = 2 + 4p = 22$, then:

$$x^N - 1 = (x-1)(x+1) \prod_{j=0}^{p-1} (x - a_1 - j)(x + a_1 - j)(x - 2a_1 - j)(x + 2a_1 - j).$$

Put: $\Lambda_2 = \{b \in \mathbb{F}_q/\mathbb{F}_p\ :\ (x+b) \text{ divides } x^{22} - 1\}$.
We see that, for all $b, c \in \Lambda_2$, one of the following conditions must hold: $b + c \in \mathbb{F}_p$, $b + 2c \in \mathbb{F}_p$, $b - 2c \in \mathbb{F}_p$.
But the elements b_1 and c_1 defined above do not satisfy that condition.
We are done.

Lemma 3.5. *The system of equations* $(*)$ *has no distinct solutions in* $\mathbb{F}_q/\mathbb{F}_p$.

Proof. First of all, recall that in this lemma, $p \neq 5$. We may consider only the following cases:
(i): $2a_1 - a_2 = 0,\ 2a_2 - a_1 = 0,$

(ii): $2a_1 - a_2 = 0,\ 2a_2 - a_3 = 0.$

Case (i):
In that case, we have: $3(a_1 - a_2) = 0$, so $p = 3$. Moreover, $a_1 + a_2 = 0$.
Thus, $a_1 + a_3, a_1 + a_4, a_2 + a_3, a_2 + a_4 \neq 0$.
We have: $a_1 + a_3 - a_2 \neq 0$, since $(a_1 + a_3 - a_2) + (a_1 + a_2) = 2a_1 + a_3 = a_3 - a_1 \neq 0$.
So, $a_1 + a_3 - a_4 = 0$.
Therefore:
- if $a_1 + a_4 - a_2 = 0$, then $2a_1 + 2a_2 + a_3 = 0$, so $a_3 = 0$. It is impossible.
- if $a_1 + a_4 - a_3 = 0$, then $2a_1 = 0$. It is impossible.

Case (ii):
We have: $a_1 + a_2 - 3a_1 = 0$.
If $p = 3$, then $a_1 + a_2 = 0$, and $a_2 + a_3 = 0$. It is impossible since $a_1 - a_3 \neq 0$.
Thus, $p \neq 3$, and $a_1 + a_2,\ a_2 + a_3 \neq 0$.
Since, $a_1 + a_2 - a_3 = a_1 - a_2 \neq 0$, we have: $a_1 + a_2 - a_4 = 0$. So $a_4 - 3a_1 = 0$ and $a_2 + a_4 = 5a_1 \neq 0$. Therefore, we have either $(a_2 + a_4 - a_1 = 0)$ or $(a_2 + a_4 - a_3 = 0)$. It follows that: $a_1 = 0$, which is impossible. □

Lemma 3.6. *If $p \neq 5$, then the system of equations $(**)$ has no distinct solutions in $\mathbb{F}_q/\mathbb{F}_p$.*

Proof. We may consider only the following cases:
(i): $2a_1 - a_2 = 0,\ 2a_2 - a_1 = 0,$
(ii): $2a_1 - a_2 = 0,\ 2a_2 - a_3 = 0,$
(iii): $2a_1 - a_3 = 0,\ 2a_2 - a_1 = 0,$
(iv): $2a_1 - a_3 = 0,\ 2a_2 - a_3 = 0,$
(v): $2a_1 - a_3 = 0,\ 2a_2 - a_4 = 0.$

Case (i):
In that case, we have: $3(a_1 - a_2) = 0$, so $p = 3$. Thus, $N = 1 + 2p = 7$ does not divide $26 = p^p - 1$. It contradicts the fact: N divides $q - 1 = p^p - 1$.

Case (ii):
According to the proof of Lemma 3.4, we must have: $a_1 + a_2 - a_4 = 0$, in particular,

$a_1 + a_2 \neq 0$. We obtain the following equalities:

$$\begin{aligned}
&2a_1 - a_2 = 0, 2a_2 - a_3 = 0, a_1 + a_2 - a_4 = 0, a_1 + a_4 - a_3 = 0,\\
&a_2 + a_3 - a_1 = 0, a_2 + a_4 = 0, a_1 + a_3 = 0.
\end{aligned}$$

Thus, $a_3 = 2a_2 = 4a_1$, $a_3 = a_1 - a_2 = -a_1$. So, $5a_1 = 0$. It is impossible since $p \neq 5$.

Case (iii): It is similar to the previous case (ii), since a_1 and a_2 play symmetric roles.

Case (iv): We have: $2(a_1 - a_2) = 0$. It is impossible.

Case (v): We have: $a_1 + a_2 - a_3$, $a_1 + a_2 - a_4 \neq 0$, since $a_1 - a_2 \neq 0$. So, $a_1 + a_2 = 0$.
Therefore, $a_3 + a_4 = 2(a_1 + a_2) = 0$, and $a_1 + a_3, a_1 + a_4, a_2 + a_3, a_2 + a_4 \neq 0$.
There are two possibilities:
- $a_1 + a_3 - a_2 = 0$. It implies: $2a_1 + a_3 = a_1 + a_2 + a_1 + a_3 - a_2 = 0$ and thus $4a_1 = 2a_1 - a_3 + 2a_1 + a_3 = 0$. It is impossible.
- $a_1 + a_3 - a_4 = 0$. It implies: $a_1 + 2a_3 = (a_1 + a_3 - a_4) + (a_3 + a_4) = 0$ and thus $5a_1 = 2(2a_1 - a_3) + a_1 + 2a_3 = 0$. It is possible only if $p = 5$. □

3.3.5. *Case (ii) and* $w(A) = 6p$. Case 1: If there exists i such that for all j, $N_{ij} \mid p - 1$, then, as in the proof in Section 3.3.4, we conclude that A is trivially perfect.
Case 2: If there exist $j_0, \ldots, j_5 \in \mathbb{F}_p$ such that $N_{0j_0}, \ldots, N_{5j_5}$ do not divide $p - 1$. Thus, by Lemma 3.3, we must have: either $(N_{0j_0} = \cdots = N_{5j_5} = 1 + 4p)$ or $(N_{0j_0}, \ldots, N_{5j_5} \in \{1 + 2p, 2 + 4p\})$.
Case 21: $N_{0j_0} = \cdots = N_{5j_5} = 1 + 4p = N$:
In this case, $p \neq 5$ and there exist $l_1, \ldots, l_5 \in \mathbb{F}_p$ such that the five monomials $x - a_i - l_i$, $1 \leq i \leq 5$, divide $x^N - 1$. So, as in the proof in Section 3.3.3, for all $i \in \{1, \ldots, 5\}$, there exist $l_i, k_i, t_i \in \{1, \ldots, 5\}$ such that:

$$\begin{cases} (2a_i - a_{l_i} \in \mathbb{F}_p) \\ (a_i + a_{k_i} \in \mathbb{F}_p) \text{ or } (a_i + a_{k_i} - a_{t_i} \in \mathbb{F}_p). \end{cases}$$

Since $a_1, \ldots, a_5$ play symmetric roles, we can reduce, as in the proof in Section 3.3.4, to the following system of equations:

$$(\overline{*}) : \begin{cases} 2a_1 - a_2 = 0 \\ (2a_2 - a_1)(2a_2 - a_3) = 0 \\ (2a_3 - a_1)(2a_3 - a_2)(2a_3 - a_4)(2a_3 - a_5) = 0 \\ (2a_4 - a_1)(2a_4 - a_2)(2a_4 - a_3)(2a_4 - a_5) = 0 \\ (2a_5 - a_1)(2a_5 - a_2)(2a_5 - a_3)(2a_5 - a_4) = 0 \\ (a_1 + a_2)(a_1 + a_2 - a_3)(a_1 + a_2 - a_4)(a_1 + a_2 - a_5) = 0 \\ (a_1 + a_3)(a_1 + a_3 - a_2)(a_1 + a_3 - a_4)(a_1 + a_3 - a_5) = 0 \\ (a_1 + a_4)(a_1 + a_4 - a_2)(a_1 + a_4 - a_3)(a_1 + a_4 - a_5) = 0 \\ (a_1 + a_5)(a_1 + a_5 - a_2)(a_1 + a_5 - a_3)(a_1 + a_5 - a_4) = 0 \\ (a_2 + a_3)(a_2 + a_3 - a_1)(a_2 + a_3 - a_4)(a_2 + a_3 - a_5) = 0 \\ (a_2 + a_4)(a_2 + a_4 - a_1)(a_2 + a_4 - a_3)(a_2 + a_4 - a_5) = 0 \\ (a_2 + a_5)(a_2 + a_5 - a_1)(a_2 + a_5 - a_3)(a_2 + a_5 - a_4) = 0 \\ (a_3 + a_4)(a_3 + a_4 - a_1)(a_3 + a_4 - a_2)(a_3 + a_4 - a_5) = 0 \\ (a_3 + a_5)(a_3 + a_5 - a_1)(a_3 + a_5 - a_2)(a_3 + a_5 - a_4) = 0 \\ (a_4 + a_5)(a_4 + a_5 - a_1)(a_4 + a_5 - a_2)(a_4 + a_5 - a_3) = 0, \end{cases}$$

which is impossible by Lemma 3.7.

Case 22:
If $N_{0j_0}, \ldots, N_{5j_5} \in \{1 + 2p, 2 + 4p\} = \{N, 2N\}$, then there exist $a, b \in \{a_1, \ldots, a_5\}$ and $j_a, j_b \in \mathbb{F}_p$, such that the monomials $x - a - j_a$ and $x - b - j_b$ divide $x^N - 1$. So, for $1 \le i \le 4$, the monomials $x - a_i - j_i - a - j_a$ and $x - a_i - j_i - b - j_b$ divide $\sigma((x - a_i - j_i)^{h_{ij_i}})$ and A.
As in the proof in Section 3.3.4, we may suppose $a = a_1, b = a_2$. Moreover, a_1 and a_2 (resp. a_3, a_4 and a_5) play symmetric roles. So the following conditions must be satisfied:

$$(\overline{**}) : \begin{cases} (2a_1 - a_2)(2a_1 - a_3) = 0 \\ (2a_2 - a_1)(2a_2 - a_3)(2a_2 - a_4) = 0 \\ (a_1 + a_2)(a_1 + a_2 - a_3)(a_1 + a_2 - a_4)(a_1 + a_2 - a_5) = 0 \\ (a_1 + a_3)(a_1 + a_3 - a_2)(a_1 + a_3 - a_4)(a_1 + a_3 - a_5) = 0 \\ (a_1 + a_4)(a_1 + a_4 - a_2)(a_1 + a_4 - a_3)(a_1 + a_4 - a_5) = 0 \\ (a_1 + a_5)(a_1 + a_5 - a_2)(a_1 + a_5 - a_3)(a_1 + a_5 - a_4) = 0 \\ (a_2 + a_3)(a_2 + a_3 - a_1)(a_2 + a_3 - a_4)(a_2 + a_3 - a_5) = 0 \\ (a_2 + a_4)(a_2 + a_4 - a_1)(a_2 + a_4 - a_3)(a_2 + a_4 - a_5) = 0 \\ (a_2 + a_5)(a_2 + a_5 - a_1)(a_2 + a_5 - a_3)(a_2 + a_5 - a_4) = 0. \end{cases}$$

Lemma 3.8 implies that $p = 5$. We get:

$$\text{either } (a_2 = 2a_1,\ a_3 = -a_1,\ a_4 = -2a_1) \text{ or } (a_2 = -a_1,\ a_3 = 2a_1,\ a_4 = -2a_1).$$

So the line 6 of $(\overline{**})$ is impossible. We are done.

Lemma 3.7. *System* $(\overline{*})$ *has no distinct solutions in* $\mathbb{F}_q/\mathbb{F}_p$.

Proof. As in the proof of Lemma 3.5, we must have: $p \neq 5$, and we may only consider the following cases:
(i): $2a_1 - a_2 = 0,\ 2a_2 - a_1 = 0$,
(ii): $2a_1 - a_2 = 0,\ 2a_2 - a_3 = 0$.

Case (i):
In that case, we have: $3(a_1 - a_2) = 0$, so $p = 3$. Moreover, $a_1 + a_2 = 0$.
Thus, $a_1 + a_3, a_1 + a_4, a_2 + a_3, a_2 + a_4, a_1 + a_5, a_2 + a_5 \neq 0$.
According to the proof of Lemma 3.5, case (i), we have either $(a_1 + a_3 - a_4 = 0)$ or $(a_1 + a_3 - a_5 = 0)$. Since a_4 and a_5 play symmetric roles, we may only consider the first case: $a_1 + a_3 - a_4 = 0$.
Still by the proof of Lemma 3.5, it remains this possibility: $a_1 + a_4 - a_5 = 0$. So, $a_2 + a_3 - a_5 = 0$, and $a_3 + a_4 + a_5 = (a_1 + a_4 - a_5) + (a_2 + a_3 - a_5) = 0$. Thus, $a_3 + a_5 \neq 0$.
Furthermore:
$a_3 + a_5 - a_1 \neq 0$ since $(a_3 + a_4 + a_5) - (a_3 + a_5 - a_1) = a_1 + a_4 \neq 0$,
$a_3 + a_5 - a_2 \neq 0$ since $a_2 + a_4 \neq 0$,
$a_3 + a_5 - a_4 \neq 0$ since $2a_4 = (a_3 + a_5 + a_4) - (a_3 + a_5 - a_4) \neq 0$.
We see that the line 14 of $(\overline{*})$ is not satisfied.

Case (ii):
According to the proof of Lemma 3.5, case (ii), we have: $p \neq 3$, $a_1 + a_2 \neq 0$ and $a_2 + a_3 \neq 0$.
Since $a_1+a_2-a_3 = a_1-a_2 \neq 0$, we have either$(a_1+a_2-a_4 = 0)$ or $(a_1+a_2-a_5 = 0)$.
It suffices to consider the first case: $a_1 + a_2 - a_4 = 0$.
So $a_4 - 3a_1 = 0$ and $a_2 + a_4 \neq 0$. Therefore (see proof of Lemma 3.5, case (ii)), we have either $(a_2+a_4-a_1 = 0)$ or $(a_2+a_4-a_3 = 0)$ or $(a_2+a_4-a_5 = 0)$. The condition: $(a_2 + a_4 - a_1 = 0)$ or $(a_2 + a_4 - a_3 = 0)$ does not hold since it implies $a_1 = 0$, which is impossible. So $a_2 + a_4 - a_5 = 0$. Thus: $a_2 = 2a_1,\ a_3 = 4a_1,\ a_4 = 3a_1,\ a_5 = 5a_1$.
It follows that the line 4 of $(\overline{*})$ is not satisfied. It is impossible. $\square$

Lemma 3.8. *If* $p \neq 5$, *then System* $(\overline{**})$ *has no distinct solutions in* $\mathbb{F}_q/\mathbb{F}_p$.

Proof. We may only consider (see proof of Lemma 3.6) the following cases:
(i): $2a_1 - a_2 = 0,\ 2a_2 - a_3 = 0$,

(ii): $2a_1 - a_3 = 0,\ 2a_2 - a_4 = 0.$

Case (i):
According to the proof of Lemma 3.6, case (ii), we must have: $p \neq 3$, $a_1 + a_2 \neq 0$ and $a_1 + a_2 - a_5 = 0$. So $a_5 = a_1 + a_2 = 3a_1$. We obtain: $a_3 = 2a_2 = 4a_1$. So $a_4 + a_1 = 0$ since $a_4 + a_1 - a_2 = a_4 - a_1 \neq 0$ and $a_4 + a_1 - a_3 = a_4 - a_5 \neq 0$.
Thus the line 4 of $(\overline{**})$ is not satisfied. It is impossible.

Case (ii): We have: $a_1 + a_2 - a_3,\ a_1 + a_2 - a_4 \neq 0$, since $a_1 - a_2 \neq 0$. So, either $(a_1 + a_2 = 0)$ or $(a_1 + a_2 = a_5)$.

- If $a_1 + a_2 = 0$, then according to the proof of Lemma 3.6, it just remains the case: $a_1 + a_3 = a_5$. So we obtain: $a_2 = -a_1, a_3 = 2a_1$, $a_4 = 2a_2 = -2a_1, a_5 = 3a_1$.
Thus the line 6 of $(\overline{**})$ is not satisfied. It is impossible.

- If $a_1 + a_2 = a_5$, then $a_3 + a_4 = 2(a_1 + a_2) = 2a_5 \neq 0$. Since $p \neq 3$, we have: $a_1 + a_3 = 3a_1 \neq 0$ and $a_1 + a_3 - a_5 = a_3 - a_2 \neq 0$. It remains two cases:
- if $a_1 + a_3 - a_2 = 3a_1 - a_2 = 0$, then:

$$\begin{cases} a_1 + a_4 - a_5 = a_4 - a_2 \neq 0, \\ a_1 + a_4 - a_2 = a_4 - a_3 \neq 0, \\ a_1 + a_4 - a_3 = a_4 - a_1 \neq 0. \end{cases}$$

Thus, $0 = a_1 + a_4 = a_1 + 2a_2 = 7a_1$. So $p = 7$, it is impossible because $15 = 1 + 2p$ does not divide $p^p - 1 = 7^7 - 1$.
Thus the line 5 of $(\overline{**})$ is not satisfied. It is impossible.
- if $a_1 + a_3 - a_4 = 3a_1 - a_4 = 0$, then:

$$\begin{cases} a_1 + a_4 = 4a_1 \neq 0, \\ 2(a_1 + a_4 - a_2) = 5a_1 \neq 0, \text{ since } p \neq 5, \\ a_1 + a_4 - a_3 = 2a_1 \neq 0, \\ 2(a_1 + a_4 - a_5) = 3a_1 \neq 0, \text{ since } p \neq 3. \end{cases}$$

Thus the line 5 of $(\overline{**})$ is not satisfied. It is impossible. $\square$

Acknowledgment. The authors would like to thank the referee for suggestions and for careful reading of the paper.

References

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

[2] E. F. Canaday, *The sum of the divisors of a polynomial*, Duke Math. Journal,7 (1941), 721–737.

[3] M. Car, L. H. Gallardo, O. Rahavandrainy and L. N. Vaserstein, *About the period of Bell numbers modulo a prime*, Bull. Korean Math. Soc., 45(1)(2008), 143–155.

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

[5] L. Gallardo and O. Rahavandrainy, *Perfect polynomials over $\mathbb{F}_4$ with less than five prime factors*, Port. Math. (N.S.), 64(1) (2007), 21–38.

[6] L. H. Gallardo and O. Rahavandrainy, *Odd perfect polynomials over $\mathbb{F}_2$*, J. Théor. Nombres Bordeaux, 19 (2007), 165–174.

[7] L. H. Gallardo and O. Rahavandrainy, *On splitting perfect polynomials over $\mathbb{F}_{p^2}$*, Port. Math. (N.S.), 66(3) (2009), 261–273.

[8] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1983, (Reprinted 1987).

[9] P. L. Montgomery, S. Nahm and S. S. Wagstaff, Jr., *The period of the Bell numbers modulo a prime*, Math. Comp., 79(271) (2010), 1793–1800.

[10] S. S. Wagstaff, Jr., *Aurifeuillian factorizations and the period of the Bell numbers modulo a prime*, Math. Comp., 65 (1996), 383–391.

Luis H. Gallardo
Department of Mathematics
University of Brest
6, Av. Le Gorgeu, C.S. 93837,
29238 Brest Cedex 3, France
e-mail: Luis.Gallardo@univ-brest.fr

Olivier Rahavandrainy
Department of Mathematics
University of Brest
6, Av. Le Gorgeu, C.S. 93837,
29238 Brest Cedex 3, France
e-mail: Olivier.Rahavandrainy@univ-brest.fr