Portugal. Math. (N.S.)
Vol. 66, Fasc. 3, 2009, 261–273

Portugaliae Mathematica

On splitting perfect polynomials over $\mathbb{F}_{p^2}$

Luis H. Gallardo and Olivier Rahavandrainy

(Communicated by Arnaldo Garcia)

Abstract. We study some properties of the exponents of the terms appearing in the splitting perfect polynomials over $\mathbb{F}_{p^2}$, where p is a prime number. This generalizes the work of Beard et al. over $\mathbb{F}_p$.

Mathematics Subject Classification (2000). Primary 11T55; Secondary 11T06.

Keywords. Sum of divisors, polynomials, finite fields, quadratic extensions, circulant matrices.

1. Introduction

Let p be a prime number and let $\mathbb{F}_q$ be a finite field of characteristic p with q elements. Let $A \in \mathbb{F}_q[x]$ be a monic polynomial. Let $\omega(A)$ denote the number of distinct monic irreducible factors of A over $\mathbb{F}_q$, and let $\sigma(A)$ denote the sum of all monic divisors of A (σ is a multiplicative function). If A divides $\sigma(A)$ (so that $\sigma(A) = A$), then we say that A is a perfect polynomial. E. F. Canaday, the first doctoral student of Leonard Carlitz, began in 1941 the study of perfect polynomials by working over the ground field $\mathbb{F}_2$ [3]. Later, in the seventies, J. T. B. Beard Jr. et al. extended this work in several directions (see, e.g., [1], [2]). Recently, we became interested in this subject [6], [7], [8], [10]. In our two first papers we considered the smallest nontrivial field extension of the ground field, namely $\mathbb{F}_4$, while in the remaining papers we continued to work on the binary case by considering "odd" and "even" perfect polynomials. We began to study the special case where the polynomial splits over $\mathbb{F}_q$. Our first results about splitting perfect polynomials are in [9], where $\mathbb{F}_q = \mathbb{F}_{p^p}$ is the Artin–Schreier extension of $\mathbb{F}_p$. See also [5] for another direction.

Beard et al. [2], Theorem 7, showed that if a perfect monic polynomial A splits over $\mathbb{F}_q$, then the integer $\omega(A)$ is a multiple of p, and A may be written as a product

$$A = A_0 \dots A_r,$$

where $A_i = \prod_{j \in \mathbb{F}_p} (x - a_i - j)^{N_{ij} p^{n_{ij}} - 1}$, $r = \frac{\omega(A)}{p} - 1$, $a_0 = 0$, $a_i \in \mathbb{F}$, $a_i - a_l \notin \mathbb{F}_p$ for $i \neq l$, $N_{ij} \mid q - 1$, $n_{ij} \geq 0$.

We say that a polynomial $A \in \mathbb{F}_q[x]$ is a *splitting perfect* polynomial if A has all its roots in $\mathbb{F}_q$ and A is a perfect polynomial. We say that A is *trivially perfect* if for any $0 \leq i \leq r$, 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

$$N_{ij} = N_i,\ n_{ij} = n_i \qquad \text{for all } j \in \mathbb{F}_p,\ N_i \mid p - 1.$$

The case when $q = p$ was considered by Beard [1] and Beard et al. [2]. They showed that a polynomial

$$A = \prod_{\gamma \in \mathbb{F}_p} (x - \gamma)^{N(\gamma) p^{n(\gamma)} - 1}$$

is perfect over $\mathbb{F}_p$ if and only if the following condition holds:

$$\text{There exist } N,\ n \in \mathbb{N} \text{ such that } N \mid p - 1,\ N(\gamma) = N,\ n(\gamma) = n \text{ for all } \gamma \in \mathbb{F}_p. \quad (*)$$

Thus, the only splitting perfect polynomials over $\mathbb{F}_p$ are of the form

$$A = (x^p - x)^{Np^n - 1},$$

where $N \mid p - 1$ and $n \in \mathbb{N}$.

Their method consists of showing, in a first step, that $n(\gamma) = n(\delta)$ for any $\gamma, \delta \in \mathbb{F}_p$ and, in a second step, that $N(\gamma) = N(\delta)$ for any $\gamma, \delta \in \mathbb{F}_p$.

If $\mathbb{F}_q$ is a nontrivial extension field of $\mathbb{F}_p$, then the condition $(*)$ remains sufficient (see again [1], [2]) but no more necessary (see [6], Theorem 3.4, in the case $p = 2$, $q = 4$).

If $A = \prod_{\gamma \in \mathbb{F}_q} (x - \gamma)^{N(\gamma) p^{n(\gamma)} - 1}$ is perfect, then two natural cases arise:

Case 1: There exists $N \in \mathbb{N}$ such that $N \mid q - 1$, $N(\gamma) = N$ for all $\gamma \in \mathbb{F}_q$.

Case 2: There exists $n \in \mathbb{N}$ such that $n(\gamma) = n$ for all $\gamma \in \mathbb{F}_q$.

We observe that case 2 does not imply case 1 (consider trivially perfect polynomials).

Let us fix an algebraic closure of $\mathbb{F}_p$. In order to get some progress in the classification of splitting perfect polynomials over a nontrivial extension field of $\mathbb{F}_p$, we would like to know if case 1 implies case 2 when we work over the smallest nontrivial extension field of $\mathbb{F}_p$, namely the quadratic extension $\mathbb{F}_{p^2}$.

In the rest of the paper, we put $q = p^2$. Our new idea is to consider suitable (block) circulant matrices (see [4], Sec. 5.6 and 5.8). The object of this paper is to prove the following result.

Theorem 1.1. *Let $N \in \mathbb{N}$ be a divisor of $q-1$, and let*

$$A = \prod_{\gamma \in \mathbb{F}_q} (x-\gamma)^{Np^{n(\gamma)}-1}$$

be a splitting perfect polynomial over $\mathbb{F}_q$.

i) *If N divides $p-1$, then A is trivially perfect so that the integers $n(\gamma)$ may differ.*

ii) *If N does not divide $p-1$, then $n(\gamma) = n(\delta) := n$, say, for any $\gamma, \delta \in \mathbb{F}_q$ so that $A = (x^q - x)^{Np^n-1}$.*

2. Proof of Theorem 1.1

We need to introduce some notation. The integers $0, 1, \ldots, p-1$ will be also considered as elements of $\mathbb{F}_p$.

We put

$$A = \prod_{\gamma \in \mathbb{F}_q} (x-\gamma)^{Np^{n(\gamma)}-1}, \qquad \text{where } N \text{ divides } q-1,$$

$$U = \{0, 1, \ldots, p-1\} \subset \mathbb{N}.$$

If $N \geq 2$, we denote by $\zeta_2, \ldots, \zeta_N \in \mathbb{F}_q$ the N-th roots of 1, distinct from 1.

Finally, we denote by $\overline{\mathbb{F}_p}$ a fixed algebraic closure of $\mathbb{F}_p$.

2.1. Preliminary. We put $\mathbb{F}_q = \mathbb{F}_{p^2} = \{j_0\alpha + j_1 : j_0, j_1 \in \mathbb{F}_p\} = \mathbb{F}_p[\alpha]$, where $\alpha \in \overline{\mathbb{F}_p}$ is a root of an irreducible polynomial of degree 2 over $\mathbb{F}_p$. Every element $i\alpha + j \in \mathbb{F}_q$ will be, if necessary, identified to the pair $(i, j) \in \mathbb{F}_p \times \mathbb{F}_p$. We define the following two order relations:

- on $\mathbb{F}_p$: $0 \leq 1 \leq 2 \leq \cdots \leq p-1$,
- on $\mathbb{F}_q$ (lexicographic order): $(j_0, j_1) \leq (l_0, l_1)$ if either $(j_0 < l_0)$ or $(j_0 = l_0, j_1 \leq l_1)$.

For $\gamma \in \mathbb{F}_q$, we put

$$\Lambda^\gamma = \{\delta \in \mathbb{F}_q : \delta \neq \gamma, (\gamma + 1 - \delta)^N = 1\} = \{\gamma + 1 - \zeta_2, \ldots, \gamma + 1 - \zeta_N\}.$$

Observe that

$$\Lambda^\gamma \neq \emptyset \text{ if } N \geq 2 \text{ and } \Lambda^\gamma \subset \{\gamma + j : j \in \mathbb{F}_p\} \text{ if } N \mid p-1.$$

For $P, Q \in \mathbb{F}_q[x]$, $P^m \parallel Q$ means that P^m divides Q and P^{m+1} does not divide Q. The following straightforward result is useful.

Lemma 2.1 (Lemma 2 in [2]). *The polynomial A is perfect if and only if for any irreducible polynomial $P \in \mathbb{F}_q[x]$ and for any positive integers m_1, m_2, we have*

$$\left(P^{m_1} \parallel A, P^{m_2} \parallel \sigma(A)\right) \Rightarrow (m_1 = m_2).$$

We obtain an immediate consequence:

Proposition 2.2. *If $N \geq 2$, then the polynomial A is perfect if and only if*

$$Np^{n(\gamma+1)} = p^{n(\gamma)} + \sum_{\delta \in \Lambda^{\gamma}} p^{n(\delta)} \quad \text{for all } \gamma \in \mathbb{F}_q.$$

Proof. For every $\gamma \in \mathbb{F}_q$, we may apply Lemma 2.1 to the polynomial $P = x - \gamma - 1$, where $m_1 = Np^{n(\gamma+1)} - 1 \geq 1$ since $N \geq 2$.

By considering

$$\sigma(A) = \prod_{\delta \in \mathbb{F}_q} \sigma\left((x-\delta)^{Np^{n(\delta)}-1}\right) = \prod_{\delta \in \mathbb{F}_q} \left((x-\delta-1)^{p^{n(\delta)}-1} \prod_{j=2}^{N} (x-\delta-\zeta_j)^{p^{n(\delta)}}\right),$$

we see that the exponent of P in $\sigma(A)$ is exactly the integer

$$m_2 = p^{n(\gamma)} - 1 + \sum_{\delta \in \Lambda^{\gamma}} p^{n(\delta)}.$$

Furthermore, $m_2 \geq 1$ since Λ^{γ} is not empty. $\square$

2.2. Circulant matrices. In this section we recall some results about circulant matrices and block circulant matrices (see [4], Chap. 3 and 4) that will be useful in the proof of our main result.

Definition 2.3. Let n be a positive integer. A *circulant* matrix of order n is a square matrix $C = (c_i^j)_{0 \leq i,j \leq n-1}$ such that the entries c_i^j satisfy

$$c_i^j = c_{i-1}^{j-1}, \; c_i^0 = c_{i-1}^{n-1} \quad \text{for } 1 \leq i, j \leq n-1.$$

Definition 2.4. Let n, m be positive integers. A *block circulant* matrix of type (n, m) is a square matrix $S = (S_i^j)_{0 \leq i,j \leq n-1}$ of order nm such that

$$\text{each matrix } S_i^j \text{ is a square matrix of order } m, \qquad S_i^j = S_{i-1}^{j-1}, \qquad S_i^0 = S_{i-1}^{n-1}$$

for $1 \leq i, j \leq n-1$. Furthermore, if every S_i^j is a circulant matrix, then S is called a *block circulant with circulant blocks*.

Notation. If C is a circulant matrix of order n and if we denote for $0 \le j \le n-1$

$$c_j = c_0^j,$$

then C may be written as

$$C = \mathrm{circ}(c_0, \dots, c_{n-1}) = \begin{pmatrix} c_0 & c_1 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & \cdots & c_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{pmatrix}.$$

Analogously, a block circulant matrix S may be written as

$$S = \mathrm{bcirc}(S_0, \dots, S_{n-1}) = \begin{pmatrix} S_0 & S_1 & \cdots & S_{n-1} \\ S_{n-1} & S_0 & \cdots & S_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ S_1 & S_2 & \cdots & S_0 \end{pmatrix},$$

where $S_j = S_0^j$ for $0 \le j \le n-1$.

We shall use several times the following crucial result when $n = p$.

Lemma 2.5 (see [4], Sec. 3.2). *Let n be a positive integer. Any circulant matrix $C = \mathrm{circ}(c_0, \dots, c_{n-1})$ is diagonalizable on $\mathbb{C}$, and admits the following eigenvalues:*

$$c_0 + c_1\omega^k + \cdots + c_{n-1}(\omega^k)^{n-1} = \sum_{l=0}^{n-1} c_l(\omega^k)^l \quad \text{for } k \in \{0, \dots, n-1\},$$

where

$$\omega = \cos(2\pi/n) + i\sin(2\pi/n) \in \mathbb{C}$$

is a n-th primitive root of unity.

Lemma 2.6 (see [4], Theorem 5.8.1). *Let n be a positive integer and let $S = \mathrm{bcirc}(S_0, \dots, S_{n-1})$ be a block circulant of type (n, n), with circulant blocks, then $S_0, \dots, S_{n-1}$ are simultaneously diagonalizable on $\mathbb{C}$.*

2.3. The proof. For $\gamma \in \mathbb{F}_q$ we put $x_\gamma = p^{n(\gamma)}$. If we identify $\gamma = i\alpha + j$ and $\delta = r\alpha + s$ with the pairs $(i, j), (r, s) \in \mathbb{F}_p^2$, we may order the unknowns x_{ij} and x_{rs} as

$$x_{ij} \le x_{rs} \Leftrightarrow (i, j) \le (r, s),$$

according to the order relation on $\mathbb{F}_q$ defined in Section 2.1. We obtain from Proposition 2.2 a linear system of q equations in q unknowns, the x_γ's:

$$Nx_{\gamma+1} = x_\gamma + \sum_{\delta \in \Lambda^\gamma} x_\delta, \qquad \gamma \in \mathbb{F}_q. \tag{1}$$

We denote by S the matrix of the linear system (1). For $i, j \in \mathbb{F}_p$, we denote by S_i^j the square matrix of order p corresponding to the coefficients of unknowns $x_{j\alpha}, x_{j\alpha+1} \dots, x_{j\alpha+p-1}$, in the p equations

$$Nx_{\gamma+1} = x_\gamma + \sum_{\delta \in \Lambda^\gamma} x_\delta, \qquad \text{where } \gamma \in \{i\alpha, i\alpha+1, \dots, i\alpha+p-1\}.$$

We have, by direct computations, the following results:

Lemma 2.7. *The matrix S can be written as a block matrix:*

$$S = (S_i^j)_{0 \le i,j \le p-1} = \begin{pmatrix} S_0^0 & \cdots & S_0^{p-1} \\ \vdots & \vdots & \vdots \\ \cdots & S_i^j & \cdots \\ \vdots & \vdots & \vdots \\ S_{p-1}^0 & \cdots & S_{p-1}^{p-1} \end{pmatrix}.$$

Lemma 2.8. *If $(e_i^j)_{mn}$ is the entry in row m and column n of S_i^j for $0 \le m, n \le p-1$, then:*

$$\begin{aligned} (e_i^j)_{mn} &= 1 \qquad \textit{if either } (j\alpha + n = i\alpha + m) \textit{ or } (j\alpha + n \in \Lambda^{i\alpha+m}), \\ (e_i^j)_{mn} &= -N \qquad \textit{if } j\alpha + n = i\alpha + m + 1, \\ (e_i^j)_{mn} &= 0 \qquad \textit{otherwise.} \end{aligned}$$

By Lemma 2.8, and from the definition of Λ^γ, for $\gamma \in \mathbb{F}_q$ we obtain:

Lemma 2.9.
$$\begin{aligned} (e_i^j)_{mn} &= 1 \qquad \textit{if } \left((i-j)\alpha + m - n + 1\right)^N = 1, \\ (e_i^j)_{mn} &= -N \qquad \textit{if } (i = j \textit{ and } n = m+1), \\ (e_i^j)_{mn} &= 0, \qquad \textit{otherwise.} \end{aligned}$$

It follows that

Lemma 2.10. $S_i^j = S_{i-1}^{j-1}$, $S_i^0 = S_{i-1}^{p-1}$ *for* $1 \le i, j \le p-1$,

$$(e_0^j)_{mn} = (e_0^j)_{m-1\,n-1},\ (e_0^j)_{m0} = (e_0^j)_{m-1\,p-1} \qquad \textit{for } 1 \le j, m, n \le p-1.$$

By putting $S_0^j = S_j$, we deduce from Lemma 2.10 the following two lemmas:

Lemma 2.11. *The matrix S is a block circulant matrix:*

$$S = \mathrm{bcirc}(S_0, \dots, S_{p-1}).$$

Lemma 2.12. *Every matrix S_j, $j \in U$, is a circulant matrix of order p:*

$$S_j = \mathrm{circ}\big((e_0^j)_{00}, \dots, (e_0^j)_{0p-1}\big).$$

In the following, for $i, j \in \{0, \dots, p-1\}$, we put

$$a_{j,i} = (e_0^j)_{0i} \qquad \text{(the entry in row 0 and column } i \text{ of } S_j).$$

Thus, the matrix S_j becomes

$$S_j = \mathrm{circ}(a_{j,0}, \dots, a_{j,p-1}).$$

We immediately obtain:

Lemma 2.13. i) $a_{0,0} = 1$, $a_{0,1} = -N$, $a_{j,i} \in \{0,1\}$ *if* $(j,i) \notin \{(0,0),(0,1)\}$.
ii) $\sum_{(i,j)\in U^2} a_{j,i} = 0$.
iii) *N divides $p-1$ if and only if $S_j = 0$ for any $j \in U\backslash\{0\}$.*
iv) *If $N = q-1$, then $a_{j,i} = 1$ for any $(j,i) \neq (0,1)$.*

Proof. We consider the equation corresponding to $\gamma = 0 = (0,0)$, in the linear system (1).

Part i) follows from direct computations.

ii) We obtain

$$\sum_{(i,j)\in U^2} a_{j,i} = a_{0,0} + a_{0,1} + \sum_{\delta\in\Lambda^0} 1 = 1 - N + \mathrm{card}(\Lambda^0) = 0,$$

since Λ^γ contains exactly $N-1$ elements, for any $\gamma \in \mathbb{F}_q$.

iii) If N divides $p-1$ and if $j \neq 0$, then, for any $i \in \mathbb{F}_p$:

$$a_{j,i} \neq -N, \text{ and } a_{j,i} \neq 1 \qquad \text{since } \big((0-j)\alpha + 0 - i + 1\big)^N \neq 1.$$

Thus, $S_j = 0$.

Conversely, if $a_{j,i} = 0$ for any $i, j \in \mathbb{F}_p$ such that $j \neq 0$, then $a_{j,i} \neq 1$ for any such i, j. By the same arguments, we see also that N must divide $p-1$.

iv) This follows from the fact that $\Lambda^0 = \mathbb{F}_q \backslash \{0, 1\}$ if $N = q - 1$. $\square$

Lemma 2.14. *If N divides $p-1$, then S is the block diagonal matrix:*

$$S = \operatorname{diag}(S_0, \ldots, S_0) = \begin{pmatrix} S_0 & 0 & \cdots & 0 \\ 0 & S_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & S_0 \end{pmatrix}.$$

Proof. By Lemma 2.13 iii), $S_j = 0$ for all $j \in U \backslash \{0\}$, so that $S = \operatorname{diag}(S_0, \ldots, S_0)$. $\square$

We put

$$\begin{aligned}
\omega &= \cos(2\pi/p) + i \sin(2\pi/p) \in \mathbb{C}, \\
\lambda_{j,k} &= \sum_{l=0}^{p-1} a_{j,l} (\omega^k)^l \quad \text{ for } j, k \in U, \\
\Delta_j &= \operatorname{diag}(\lambda_{j,0}, \ldots, \lambda_{j,p-1}) \quad \text{ for } j \in U, \\
\Delta &= \operatorname{bcirc}(\Delta_0, \ldots, \Delta_{p-1}).
\end{aligned}$$

We obtain the

Proposition 2.15. *The matrices S and Δ have the same rank.*

Proof. By Lemma 2.5, for each $j \in U$, the matrix S_j is diagonalizable and $\lambda_{j,0}, \ldots, \lambda_{j,p-1}$ are its eigenvalues. Furthermore, by Lemma 2.6, the matrices S_j, $j \in U$, are simultaneously diagonalizable. So, the matrices S and Δ are similar. We are done. $\square$

Now if we put together the rows

$$L_l, L_{p+l}, L_{2p+l}, \ldots, L_{(p-1)p+l}$$

of the matrix Δ, for each integer $l \in \{0, \ldots, p-1\}$, we obtain a matrix Δ', with the same rank.

By putting together, for each integer $l \in \{0, \ldots, p-1\}$, the columns

$$C_l, C_{p+l}, C_{2p+l}, \ldots, C_{(p-1)p+l}$$

of the matrix Δ', we obtain a matrix $\tilde{\Delta}$, which has also the same rank as Δ. The matrix $\tilde{\Delta}$ is a block diagonal matrix:

$$\tilde{\Delta} = \operatorname{diag}(\tilde{\Delta}_0, \dots, \tilde{\Delta}_{p-1}),$$

where

$$\tilde{\Delta}_k = \operatorname{circ}(\lambda_{0,k}, \dots, \lambda_{p-1,k})$$

is a circulant matrix, for any $k \in U$. Thus, we obtain

Proposition 2.16. *The matrices S and $\tilde{\Delta}$ have the same rank.*

To finish the proof of Theorem 1.1, we need the following results.

Lemma 2.17. *Let $j \in U \setminus \{0\}$ and $u_0, \dots, u_{p-1} \in \mathbb{Q}$ such that $\sum_{r \in U} u_r(\omega^j)^r = 0$. Then*

$$\textit{either } (u_r = 0 \textit{ for all } r \in U) \textit{ or } (u_r = 1 \textit{ for all } r \in U).$$

Proof. Since $\{1, \omega^j, \dots, (\omega^j)^{p-1}\} = \{1, \omega, \dots, \omega^{p-1}\}$, we may assume that $j = 1$. It suffices to observe that the cyclotomic polynomial $\Phi_p(x) = 1 + \cdots + x^{p-1}$, which is irreducible, is the minimal polynomial of ω. $\square$

Lemma 2.18. *The matrix S_0 has rank $p - 1$.*

Proof. By Lemma 2.5, the eigenvalues of the matrix S_0 are

$$v_0 = a_{0,0} + \cdots + a_{0,p-1} = \sum_{(j,i) \in U^2} a_{j,i} = 0,$$

$$v_l = \sum_{r \in U} a_{0,r}(\omega^l)^r \qquad \text{for } l \in U \setminus \{0\}.$$

If $v_l = 0$ for some $l \in U \setminus \{0\}$, then by Lemma 2.17 we have

$$\text{either } (a_{0,r} = 0 \text{ for all } r \in U) \text{ or } (a_{0,r} = 1 \text{ for all } r \in U).$$

These two cases are impossible since $a_{0,0} = 1$ and $a_{0,1} = -N$. Thus, S_0 has exactly $p - 1$ nonzero eigenvalues. We are done. $\square$

If N does not divide $p - 1$, the following two lemmas give the rank of $\tilde{\Delta}_k$ for $k \in U$.

Lemma 2.19. *If N does not divide $p - 1$, then the matrix $\tilde{\Delta}_0$ has rank $p - 1$.*

Proof. We know, by Lemma 2.5, that $\tilde{\Delta}_0$ has the following eigenvalues:

$$\mu_0 = \lambda_{0,0} + \cdots + \lambda_{p-1,0} = \sum_{(j,i)\in U^2} a_{j,i} = 0,$$

$$\mu_l = \sum_{r\in U} \lambda_{r,0}(\omega^l)^r \qquad \text{for } l \in U\backslash\{0\}.$$

If $\mu_l = 0$ for some $l \in U\backslash\{0\}$, then by Lemma 2.17, we have

$$\text{either } (\lambda_{r,0} = 0 \text{ for all } r \in U) \text{ or } (\lambda_{r,0} = 1 \text{ for all } r \in U).$$

In the first case, we obtain that

$$\sum_{r\in U} a_{0,r} = \lambda_{0,0} = 0 = \sum_{(i,j)\in U^2} a_{j,i} = \sum_{r\in U} a_{0,r} + \sum_{(j,r)\in U^2, j\neq 0} a_{j,r}.$$

It follows that $a_{j,r} = 0$ for any $j, r \in U$ such that $j \geq 1$. It is impossible since the matrix S_j is not the zero matrix by Lemma 2.13 ii).

In the second case we obtain

$$\sum_{(r,s)\in U^2} a_{r,s} = \sum_{r\in U} a_{r,0} + \cdots + \sum_{r\in U} a_{r,p-1} = \sum_{r\in U} \lambda_{r,0} = p \neq 0,$$

which is also impossible. $\square$

Lemma 2.20. *If N does not divide $p-1$, then for any $j \in U\backslash\{0\}$, the matrix $\tilde{\Delta}_j$ has rank p.*

Proof. By Lemma 2.5, the matrix $\tilde{\Delta}_j$ has the following eigenvalues:

$$\mu_{jl} = \sum_{s\in U} \lambda_{s,j}(\omega^l)^s = \sum_{(r,s)\in U^2} a_{s,r}\omega^{rj+sl}, \qquad l \in U.$$

For $t \in U$ we put $U_t = \{(r,s) \in U^2 : sj + rl \equiv t \bmod p\}$. The set U^2 is the disjoint union $U_0 \sqcup \cdots \sqcup U_{p-1}$. So we can write

$$\mu_{jl} = \sum_{(r,s)\in U^2} a_{r,s}\omega^{sj+rl} = \sum_{t\in U}\Big(\sum_{(r,s)\in U_t} a_{r,s}\Big)\omega^t.$$

If $\mu_{jl} = 0$, then by Lemma 2.17, we have

$$\text{either } \Big(\sum_{(r,s)\in U_t} a_{r,s} = 0 \text{ for all } t \in U\Big) \text{ or } \Big(\sum_{(r,s)\in U_t} a_{r,s} = 1 \text{ for all } t \in U\Big).$$

In the first case we obtain that

$$\sum_{(r,s)\in U_0} a_{r,s} = 0.$$

Moreover, $a_{r,s} \geq 0$ for any $(r,s) \in U_0$ since $(0,1) \notin U_0$. Thus

$$0 = \sum_{(r,s)\in U_0} a_{r,s} \geq a_{0,0} = 1,$$

which is impossible.

The second case is also impossible since that would imply that

$$0 = \sum_{(r,s)\in U^2} a_{r,s} = \sum_{t\in U} \sum_{(r,s)\in U_t} a_{r,s} = p. \qquad \square$$

We obtain our main results:

Corollary 2.21. *If N divides $p-1$, then $n(\gamma) = n(\gamma + j)$ for any $\gamma \in \mathbb{F}_q$, $j \in \mathbb{F}_p$.*

Proof. By Lemma 2.14, the matrix S is exactly the diagonal matrix $\operatorname{diag}(S_0, \ldots, S_0)$, so the linear system (1) splits into p linear systems (each of which is of matrix S_0) in p unknowns, $x_\gamma, x_{\gamma+1}, \ldots, x_{\gamma+p-1}$:

$$Nx_{\gamma+j+1} = x_{\gamma+j} + \sum_{\delta\in\Lambda^{\gamma+j}} x_\delta \qquad \text{for } \gamma = i\alpha,\ i, j \in \mathbb{F}_p. \tag{2}$$

Moreover, by Lemma 2.18, S_0 has rank $p-1$. It remains to observe that $(1, \ldots, 1)$ belongs to the kernel of S_0, since

$$a_{0,0} + \cdots + a_{0,p-1} = \sum_{(i,j)\in U^2} a_{j,i} = 0$$

by Lemma 2.13 ii). $\square$

Corollary 2.22. *If N does not divide $p-1$, then $n(\gamma) = n(\delta)$ for any $\gamma, \delta \in \mathbb{F}_q$.*

Proof. In that case, the matrix $\tilde{\Delta}$ (and thus the matrix S) has rank

$$p - 1 + (p-1)p = p^2 - 1 = q - 1.$$

Moreover, $(1, \ldots, 1)$ belongs to the kernel of S, since

$$\sum_{(i,j) \in U^2} a_{j,i} = 0$$

by Lemma 2.13 ii). So we are done. $\square$

Final remarks. 1) If $q = p^m$ for $m \geq 3$, then our method fails since we cannot apply Lemma 2.6.

2) If $p = 2$, then the splitting perfect polynomials over $\mathbb{F}_4$ are known (see [6], Theorem 3.4).

3) By using a computer program, we obtain a complete list of perfect polynomial over $\mathbb{F}_9$ of the form

$$\prod_{\gamma \in \mathbb{F}_9} (x - \gamma)^{N(\gamma) - 1}, \qquad \text{where } N(\gamma) \mid 8, \text{ and } n(\gamma) = 0 \text{ for all } \gamma \in \mathbb{F}_9.$$

Except for trivially perfect polynomials and for perfect polynomials of the form

$$(x^9 - x)^{N-1}, \qquad \text{where } N \in \{1, 2, 4, 8\},$$

we obtain two other families: $A_1(x - a)$ and $A_2(x - a)$, $a \in \mathbb{F}_9$, where $\alpha \in \mathbb{F}_9$ satisfy $\alpha^2 = -1$ and, for $A_1(x)$,

$$N(0) = N(\alpha) = N(2\alpha) = 4,$$
$$N(j) = N(\alpha + j) = N(2\alpha + j) = 2, \qquad j \in \{1, 2\},$$

and, for $A_2(x)$,

$$N(1) = N(\alpha + 1) = N(2\alpha + 1) = 2,$$
$$N(j) = N(\alpha + j) = N(2\alpha + j) = 4, \qquad j \in \{0, 2\}.$$

Then we can deduce (see [1]), for a fixed positive integer m, the list of all perfect polynomials of the form $\prod_{\gamma \in \mathbb{F}_9} (x - \gamma)^{N(\gamma) p^m - 1}$.

The computer took some substantial time to do the job. So we may think that the determination of all splitting perfect polynomials over a finite field is a non-trivial problem.

References

[1] J. T. B. Beard, Jr., Perfect polynomials revisited. *Publ. Math. Debrecen* **38** (1991), 5–12. Zbl 0743.11068 MR 1100900

[2] 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.* (8) **62** (1977), 283–291. Zbl 0404.12014 MR 497649

[3] E. F. Canaday, The sum of the divisors of a polynomial. *Duke Math. J.* **8** (1941), 721–737. Zbl 0061.06605 MR 0005509

[4] P. J. Davis, *Circulant matrices.* John Wiley & Sons, New York 1979. Zbl 0418.15017 MR 0543191

[5] L. 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. Zbl 1130.11070 MR 2381490

[6] L. Gallardo and O. Rahavandrainy, On perfect polynomials over $\mathbb{F}_4$. *Port. Math.* (*N.S.*) **62** (2005), 109–122. Zbl 1131.11079 MR 2126875

[7] L. Gallardo and O. Rahavandrainy, Perfect polynomials over $\mathbb{F}_4$ with less than five prime factors. *Port. Math.* (*N.S.*) **64** (2007), 21–38. Zbl 05225688 MR 2298110

[8] L. H. Gallardo and O. Rahavandrainy, Odd perfect polynomials over $\mathbb{F}_2$. *J. Théor. Nombres Bordeaux* **19** (2007), 165–174. Zbl 1145.11081 MR 2332059

[9] L. H. Gallardo and O. Rahavandrainy, On splitting perfect polynomials over $\mathbb{F}_{p^p}$. Preprint 2007.

[10] L. H. Gallardo and O. Rahavandrainy, Even perfect polynomials over $\mathbb{F}_2$ with four prime factors. *Int. J. Pure Appl. Math.*, to appear.

[11] R. Lidl and H. Niederreiter, *Finite fields*. Encyclopedia Math. Appl. 20, Addison-Wesley Publishing Company, Reading, MA, 1983. Zbl 0554.12010 MR 0746963

Received March 4, 2008; revised December 12, 2008

L. H. Gallardo, Department of Mathematics, University of Brest, CNRS UMR 6205, 6, Avenue Le Gorgeu, C. S. 93837, 29238 Brest Cedex 3, France.

E-mail: Luis.Gallardo@univ-brest.fr

O. Rahavandrainy, Department of Mathematics, University of Brest, CNRS UMR 6205, 6, Avenue Le Gorgeu, C. S. 93837, 29238 Brest Cedex 3, France.

E-mail: Olivier.Rahavandrainy@univ-brest.fr