Czechoslovak Mathematical Journal

Karol Nemoga; Štefan Schwarz

An explicit description of the set of all normal bases generators of a finite field

Czechoslovak Mathematical Journal, Vol. 49 (1999), No. 1, 81–96

Persistent URL: http://dml.cz/dmlcz/127469

Czechoslovak Mathematical Journal, 49 (124) (1999), 81–96

AN EXPLICIT DESCRIPTION OF THE SET OF ALL NORMAL BASES GENERATORS OF A FINITE FIELD

Karol Nemoga and $\boxed{\text{Štefan Schwarz}}$, Bratislava

(Received March 27, 1996)

1. Preliminaries

Let $F_q = GF(q)$ be a finite field with $\operatorname{char}(F_q) = p$, p a prime, and $F_{q^n} = GF(q^n)$ the n-dimensional extension of F_q.

By a basis of F_{q^n} with respect to F_q (shortly a basis of $F_{q^n}|F_q$) we mean a set of elements $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, $\alpha_i \in F_{q^n}$, such that any element $\gamma \in F_{q_n}$ can be written uniquely in the form $\gamma = \sum\limits_{i=1}^{n} c_i \alpha_i$, with $\alpha_i \in F_q$. Viewing F_{q^n} as a vector space of dimension n over F_q the set $\{\alpha_1, \ldots, \alpha_n\}$ is a set of n linearly independent vectors (of length n) over F_q.

A basis is called a normal basis of $F_{q^n}|F_q$ if it is of the form $A = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$, where $\alpha \in F_{q^n}$. The element α is called a generator of the basis A. It is known that a normal basis always exists. The element α is then a root of an irreducible polynomial of degree n over F_q, often called a normal polynomial (or an N-polynomial).

Let $A = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ and $B = \{\beta, \beta^q, \ldots, \beta^{q^{n-1}}\}$ be two normal bases of $F_{q^n}|F_q$. Since $\beta \in F_{q^n}$ there exist n elements $c_1, \ldots, c_n$ (all belonging to F_q) such that $\beta = c_1\alpha + c_2\alpha^q + \ldots + c_n\alpha^{q^{n-1}}$. This implies

$$\begin{aligned}
\beta^q &= c_n\alpha + c_1\alpha^q + \ldots + c_{n-1}\alpha^{q^{n-1}},\\
&\vdots\\
\beta^{q^{n-1}} &= c_2\alpha + c_3\alpha^q + \ldots + c_1\alpha^{q^{n-1}}.
\end{aligned}$$

Denote by C the circulant matrix

$$\begin{pmatrix} c_1, & c_2, & \ldots, & c_n \\ c_n, & c_1, & \ldots, & c_{n-1} \\ \vdots & & & \\ c_2, & c_3, & \ldots, & c_1 \end{pmatrix},$$

and $A^T = \begin{pmatrix} \alpha \\ \alpha^q \\ \vdots \\ \alpha^{q^{n-1}} \end{pmatrix}$, $B^T = \begin{pmatrix} \beta \\ \beta^q \\ \vdots \\ \beta^{q^{n-1}} \end{pmatrix}$. We then have $B^T = C \cdot A^T$.

Analogously, there exists a circulant matrix D such that $A^T = DB^T$. From these relations we obtain by a simple reasoning the following well known proposition:

Proposition 1.1. *If $A = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a normal basis of $F_{q^n}|F_q$, then any other normal basis of $F_{q^n}|F_q$ is of the form $C\,A^T$, where C is an invertible circulant matrix (with elements of F_q). Conversely, if C is any invertible $n \times n$ circulant matrix with elements in F_q, then $C\,A^T$ is a normal basis of $F_{q^n}|F_q$.*

Recall that the set of all $n \times n$ circulant matrices with elements in F_q forms (with respect to multiplication) a commutative semigroup, while the invertible ones form a commutative group (contained in this semigroup).

Denote by P the matrix

$$P = \begin{pmatrix} 0, & 1, & 0, & \ldots & 0 \\ 0, & 0, & 1, & \ldots & 0 \\ \vdots & & & & \\ 0, & 0, & 0, & \ldots & 1 \\ 1, & 0, & 0, & \ldots & 0 \end{pmatrix}.$$

We then have

$$C = c_1 E + c_2 P + \ldots + c_n P^{n-1}, \quad \text{and} \quad P^n = E,$$

where E is the unit matrix. In the correspondence $\omega\colon\ x^\ell \longleftrightarrow P^\ell$ $(\ell = 0, 1, \ldots, n-1)$ the set of all circulant $n \times n$ matrices is isomorphic to the ring $R = R(n,q) = F_q[x]/(x^n - 1)$. In this way we assign to the circulant matrix C the polynomial $c(x) = c_1 + c_2 x + \ldots + c_n x^{n-1}$ and the arithmetical operations with C are reduced to the calculations with polynomials over F_q modulo $(x^n - 1)$. In particular, the invertible circulant matrices correspond to the polynomials of degree at most $(n-1)$, which are relatively prime to $x^n - 1$.

Notation. In the following we shall write "NB-generator" instead of "normal basis generator". The set of all NB-generators of $F_{q^n}|F_q$ will be denoted by $\Gamma = \Gamma(n,q) \subset F_{q^n}$. The multiplicative semigroup of the ring $R = F_q(x)/(x^n-1)$ will be denoted by $\overline{R}$. The group of all elements of $\overline{R}$ relatively prime to x^n-1 will be denoted by $G(1)$.

The necessity to consider $\overline{R}$ is due to the fact that in what follows we shall deal with subsets of $\overline{R}$ which are multiplicatively closed, but not closed under addition.

The preceding arguments imply (the again well known)

Proposition 1.2. *If $c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ is a polynomial relatively prime to x^n-1 [i.e. $c(x) \in G(1)$] and α is an NB-generator of $F_{q^n}|F_q$, then $g = c_0\alpha + c_1\alpha^q + \ldots + c_{n-1}\alpha^{q^{n-1}}$ is an NB-generator. Moreover, if α is a fixed chosen NB-generator, then all NB-generators of $F_{q^n}|F_q$ are obtained in this manner by choosing suitably $c(x)$.*

In what follows we denote by Ω the mapping $\Omega\colon\, x^\ell \to \alpha^{q^\ell}$ and we shall write $\Omega x^\ell = \alpha^{q^\ell}$. This mapping is "additive" in the sense that $\Omega(ax^u + bx^v) = a\alpha^{q^u} + b\alpha^{q^v}$ for $a, b \in F_q$.

The goal of this paper is the following. Suppose that we know one NB-generator of $F_{q^n}|F_q$, say $\alpha \in F_{q^n}$. We shall give an explicit description of all NB-generators of $F_{q^n}|F_q$.

To understand well we first give an example. Let α be an NB-generator of $F_{5^3}|F_5$. It will be shown (Example 3.3) that all polynomials coprime to x^3-1 are of the form

$$r_0(1+x+x^2) + r_1(4+x) + r_2(4+x^2),$$

where $r_0 \neq 0$ and $(r_1, r_2) \neq (0,0)$, $\{r_0, r_1, r_2\} \in F_5$. Hence the set $\Gamma(3,5) = \big\{r_0(\alpha + \alpha^5 + \alpha^{25}) + r_1(4\alpha + \alpha^5) + r_2(4\alpha + \alpha^{25})\big\}$ is the set of all NB-generators of $F_{125}|F_5$. Clearly the cardinality $|\Gamma| = 96$. (The element α itself is obtained for $r_0 = 2$, $r_1 = r_2 = 3$.)

Remark. If $g \in \Gamma$, then $ag \in \Gamma$ for any $a \in F_q$. Also $g^q, g^{q^2}, \ldots, g^{q^{n-1}} \in \Gamma$. If $g' \in \Gamma$, $g'' \in \Gamma$, then neither $g' + g''$ nor $g' \cdot g''$ need to belong to Γ. Also, if $g \in \Gamma$, g^{-1} need not be an element of Γ.

The first two statements are obvious. To be sure that it may happen that $g^{-1} \notin \Gamma$ it is sufficient to give an example. The element α satisfying the equation $x^3 + x^2 + 1 = 0$ over F_5 is an NB-generator of $GF(5^3)|GF(5)$. But α^{-1} which satisfies (the irreducible) equation $y^3 + y + 1 = 0$ is certainly not an NB-generator. (For any N-polynomial with root β we have necessarily trace $(\beta) \neq 0$.)

2. The description of the multiplicative semigroup $\overline{R}$

It is known that the factorization of $x^n - 1$ into the product of monic irreducible factors over F_q is of the form $x^n - 1 = \left[f_1(x) \cdot f_2(x) \dots f_r(x)\right]^t$, where

$$t = \begin{cases} 1, & \text{if } (n,p) = 1, \\ p^s, & \text{if } n = n_0 p^s, (n_0, p) = 1. \end{cases}$$

The ring $R = F_q[x]/(x^n - 1)$ admits a decomposition as a direct sum of r rings in the form

$$R \approx F_q[x]/f_1(x)^t \oplus \dots \oplus F_q[x]/f_r(x)^t.$$

This can be considered an "external" description of R, and as such it is not suitable for computations in R itself.

Our aim is to describe some properties of R (and $\overline{R}$) using only elements of R, so to say to give an "internal" description of R. To this end we describe the multiplicative semigroup $\overline{R}$ as a set-theoretical union of disjoint subsemigroups each of which has a unique idempotent. We then use this decomposition to prove Proposition 2.5 (below), which is a starting point to numerical computations.

A) We first recall some notions used in the elementary theory of semigroups. Let S be a finite commutative semigroup with a zero element 0 and an identity element 1.

We shall say that $a \in S$ belongs to the idempotent e if there is an integer $\ell = \ell(a)$ such that $a^\ell = e$. Any $a \in S$ belongs to one and only one idempotent of S. Let $K(e)$ be the set of all elements of S belonging to the idempotent e. Then $K(e)$ is a subsemigroup of S (the maximal subsemigroup of S belonging to the idempotent e). We have $S = \bigcup_{e \in E} K(e)$, where E is the set of all idempotents.

Each $K(e)$, $e \in E$, has the property that $K(e).\ e$ is a group, denoted by $G(e)$ and called the maximal group belonging to the idempotent e. Note that $G(e) \subset K(e)$.

In particular, $K(1)$ is the set of all "absolutely" invertible elements of S, i.e. the group of all elements $a \in S$ for which there is an element a' such that $aa' = 1$. Hence $K(1)$ is a group, which will be denoted by $G(1)$.

The set $K(0)$ is the set of all nilpotent elements of S and $G(0) = \{0\}$ is a one-point group.

The number of maximal subgroups contained in S is equal to the number of idempotents in S. If $G(e)$ is a maximal subgroup we may speak also about the "relative inverses" with respect to the idempotent e (i.e. inside of $G(e)$).

B) We now apply the foregoing notions and results to the semigroup $\overline{R}$. Our goal is first to prove Proposition 2.4 (concerning any idempotent $e \in \overline{R}$) and then Proposition 2.5 (in which only the primitive idempotents appear).

In accordance with section A, we denote by $G(1)$ the group of all polynomials $a = a(x) \in \overline{R}$ of degree $\leqslant n-1$ which are relatively prime to $x^n - 1$. Also we denote $\deg f_i = n_i$, so that $n = \sum_{i=1}^{r} n_i t$.

The method used in the sequel is analogous to that of [5] and [6].

Any element $h = h(x) \in \overline{R}$ can be written in the form $h = f_1^{s_1} f_2^{s_2} \dots f_r^{s_r} \cdot a$, where $a \in G(1)$. If, e.g., $s_1 > t$, then $f_1^{s_1}$ can be written in the form $f_1^{s_1} = f_1^t (f_1^{s_1-t} + f_2^t \dots f_r^t) = f_1^t a_1, a_1 \in G(1)$, so that $h = f_1^{\min(s_1,t)} \cdot f_2^{\min(s_2,t)} \dots f_r^{\min(s_r,t)} \cdot b$ with $b \in G(1)$. Hence we have

Lemma 2.1. *Any element $h \in \overline{R}$ can be written in the form $h = f_1^{\tau_1} \cdot f_2^{\tau_2} \dots f_r^{\tau_r} \cdot b$, where $0 \leqslant \tau_i \leqslant t$, $b \in G(1)$.*

Suppose that $\varepsilon = f_{i_1}^{\tau_1} \dots f_{i_v}^{\tau_v} \cdot a$ is an idempotent $\varepsilon \neq 1$, $(i_1 < i_2 < \dots < i_v)$, $\tau_i > 0$, $1 \leqslant v < r$, $a \in G(1)$. Then $\varepsilon = \varepsilon^t$ implies $\varepsilon = g_{i_1}^{t\tau_1} \dots f_{i_v}^{t\tau_v} a^t$. Here $t\tau_j \geqslant t$. If $t\tau_j > 1$, then $f_{i_j}^{t\tau_j} = f_{i_j}^t \cdot b_j$, $b_j \in G(1)$, whence $\varepsilon = f_{i_1}^t \dots f_{i_v}^t \cdot c$, $c \in G(1)$. If $v = r$, we have $\varepsilon = 0$. ($\varepsilon = 1$ is obtained for $\tau_1 = \dots = \tau_r = 0$ and $a = 1$.) This implies

Lemma 2.2. *$\overline{R}$ contains 2^r idempotents. Each of the idempotents can be written in the form*

$$e = f_1^{\tau_1} f_2^{\tau_2} \dots f_r^{\tau_r} \cdot c, \ c \in G(1), \quad \textit{and} \quad \tau_i \quad \textit{is either} \quad 0 \quad \textit{or} \quad t.$$

Write (in an obvious notation) $x^n - 1 = f_i^t \cdot F_i^t$ $(i = 1, 2, \dots, r)$, then the primitive idempotents are $e_1 = F_1^t a_1, \dots, e_r = F_r^t a_r$ $(a_i \in G(1))$. Clearly $e_i \cdot e_j = 0$ for $i \neq j$. Next, the sum $F_1^{\cdot t} a_1 + \dots + F_r^{\cdot t} a_r$ is contained in $G(1)$ [since, e.g., f_1 divides $F_2, \dots, F_r$, and does not divide F_1]. Since this sum is an idempotent we have $e_1 + \dots + e_r = 1$.

We now specify the maximal subsemigroup $K(e)$, $e \neq 1$, belonging to the idempotent $e = f_{i_1}^t f_{i_2}^t \dots f_{i_v}^t a$, $a \in G(1)$, $i_1 < i_2 < \dots < i_v$.

An element $h = f_1^{\tau_1} \dots f_r^{\tau_r} \cdot b \in \overline{R}$, $1 \leqslant \tau_i \leqslant t$, $b \in G(1)$, belongs to the idempotent e if there is an integer k such that $f_1^{k\tau_1} \dots f_r^{k\tau_r} b^k = e$.

Hence

$$f_1^{\min(k\tau_1,t)} \dots f_r^{\min(k\tau_r,t)} \cdot c \cdot b^k = f_{i_1}^t f_{i_2}^t \dots f_{i_v}^t a,$$

where $c \in G(1)$. If $k \geqslant t$ and $v < r$, we have necessarily $\tau_j = 0$ for all indices j for which $j \notin \{i_1, \dots, i_v\}$. Hence, $h(x)$ is necessarily of the form $h = f_{i_1}^{\tau_1} f_{i_2}^{\tau_2} \dots f_{i_v}^{\tau_v} \cdot b_1$, $b_1 \in G(1)$. This holds also for $v = r$, in which case $e = 0$.

Conversely, let $h = f_{i_1}^{\tau_1} \dots f_{i_v}^{\tau_v} \cdot b_2$, $1 \leqslant \tau_i \leqslant t$, and let b_2 be any element of $G(1)$. Then

$$h^t = f_{i_1}^{\tau_1 t} \dots f_{i_v}^{\tau_v t} \cdot b_2^t = f_{i_1}^t \dots f_{i_v}^t c \cdot b_2^t = f_{i_1}^t \dots f_{i_v}^t \cdot a(cb_2^t a^{-1}) = e(cb_2^t a^{-1}).$$

If ℓ is the order of the group $G(1)$, we eventually obtain $h^{t\ell} = e$. Since b_2 is any element of $G(1)$, we have $f_{i_1}^{\tau_1} \dots f_{i_v}^{\tau_v} G(1) \subset K(e)$.

We have proved

Lemma 2.3. *If $e = f_{i_1}^t \dots f_{i_v}^t a$ is an idempotent of $\overline{R}$, $1 \leqslant v \leqslant r$, $a \in G(1)$, then $K(e) = \bigcup\limits_{\tau_1,\dots,\tau_v} f_{i_1}^{\tau_1} \dots f_{i_v}^{\tau_v} \cdot G(1)$, where $1 \leqslant \tau_i \leqslant t$.*

Clearly $K(e)$ is a (set theoretical) union of t^v such "complexes", and these "complexes" are disjoint.

To specify the maximal group $G(e)$ belonging to the idempotent

$$e = f_{i_1}^t f_{i_2}^t \dots f_{i_v}^t a, \ (i_1 < i_2 \dots < i_v)$$

we use the formula $G(e) = K(e) \cdot e$.

The term $f_{i_1}^{t+\tau_1} f_{i_2}^{t+\tau_2} \dots f_{i_v}^{t+\tau_v} G(1)$ multiplied by e is equal to $f_{i_1}^{t+\tau_1} f_{i_2}^{t+\tau_2} \dots f_{i_v}^{t+\tau_v} aG(1) = f_{i_1}^t f_{i_2}^t \dots f_{i_v}^t \cdot b\, aG(1) = e \cdot b \cdot G(1) = eG(1)$, hence it is independent of $(\tau_1, \dots, \tau_v)$.

We have proved

Proposition 2.4. *If e is any idempotent of $\overline{R}$, then the maximal group $G(e)$ belonging to e is given by the formula $G(e) = G(1) \cdot e$.*

In the following $A \oplus B$ denotes the set of all elements $a + b$, where $a \in A$, $b \in B$. Consider the set $U = G(1)e_1 \oplus \dots \oplus G(1)e_r$. All elements of U are contained in $G(1)$ (since, e.g., f_1 divides all summands with the exception of $G(1)e_1$, which is not divisible by f_1). Hence $U \subset G(1)$. Next, $1 = e_1 + \dots + e_r \in U$, so that for any $b \in G(1)$ we have $b \in bG(1)e_1 \oplus \dots \oplus bG(1)e_r = G(1) \cdot e_1 \oplus \dots \oplus G(1) \cdot e_r = U$, whence $G(1) \subset U$. Therefore $U = G(1)$. Using Proposition 2.4 we have

Proposition 2.5. *If $G(e_i)$ is the maximal group belonging to the primitive idempotent e_i, then*

$$G(1) = G(e_1) \oplus G(e_2) \oplus \dots \oplus G(e_r).$$

Let us underline that $G(e_i)$ is a multiplicative group but not an additive one. Any element $\xi \in G(1)$ can be written in the form $\xi = \xi_1 + \xi_2 + \dots + \xi_r$, $\xi_i \in G(e_i)$, and $\xi_i \neq 0$ $(i = 1, \dots, r)$. This result is of essential importance for all what follows. It will turn out that the computation of the elements of the $G(e_i)$'s can be relatively easily established.

C) For computational purposes we need an explicit description of e_i. In this connection we prove

Lemma 2.6. *If $x^n - 1 = f_i^t \cdot F_i^t$, then the r primitive idempotents are given by the formula $e_i = \frac{1}{n_0}\left[x \cdot f_i' F_i\right]^t$, $i = 1, 2, \ldots, r$.*

Proof. a) Suppose first $t = 1$, i.e. $n = n_0$. We can use the well known formula that if $f(x) = x^n - 1 = f_1 f_2 \ldots f_r$, then $e_i = \frac{f_i' F_i}{f'} = \frac{f_i' F_i}{n x^{n-1}} = \frac{1}{n} x \cdot f_i' F_i$, $(i = 1, 2, \ldots, r)$.

b) Suppose next $t > 1$, hence $x^n - 1 = (x^{n_0} - 1)^t$, $t = p^s$. We have $x^{n_0} - 1 = f_1 f_2 \ldots f_r$, and $\varepsilon_i = \frac{1}{n_0} x \cdot f_i' F_i$ satisfies $\varepsilon_i^2 \equiv \varepsilon_i \left(\mathrm{mod}(x^{n_0} - 1)\right)$, i.e. $\varepsilon_i^2 - \varepsilon_i = v(x)(x^{n_0} - 1)$, where $v(x) \in R$. Taking to the power $t = p^s$ we have $\varepsilon_i^{2t} - \varepsilon_i^t = v(x)^t (x^n - 1) = 0$ (in R), whence $e_i = \frac{1}{n_0}\left[x \cdot f_i' \cdot F_i\right]^t$. $\square$

Remark. It should be remarked that the cardinality $|G(1)|$ can be calculated in advance knowing only the degrees of the irreducible factors f_i. We owe O. Ore (1934) the following result. If $\deg f_i = n_i$, so that $n = \sum_{i=1}^{r} n_i t$, we have $|G(1)| = q^n (1 - q^{-n_1}) \ldots (1 - q^{-n_r})$.

[To be historically more precise, this formula appears (in a more general setting) even in the book R. Fricke [1] in the case of the ground field F_p.]

3. The case $(n, p) = 1$

In this case $t = 1$, and we have $x^n - 1 = f_1 \ldots f_r$. Any idempotent $e \neq 1$ is of the form $e = f_{i_1} \cdot f_{i_2} \ldots f_{i_v} a$, $1 \leqslant v \leqslant r$, $a \in G(1)$. By Proposition 2.4 the maximal semigroup belonging to $e \in \overline{R}$ is $K(e) = f_{i_1} \ldots f_{i_v} G(1) = f_{i_1} \ldots f_{i_v} \cdot a \cdot G(1) = eG(1) = G(e)$. Hence $K(e) = G(e)$. This implies

Proposition 3.1. *If $(n, p) = 1$, then $\overline{R}$ is a (set theoretical) union of disjoint groups (including $G(1)$ and $\{0\}$).*

Let e_i be a primitive idempotent of $\overline{R}$, and $\varrho \in R$.

a) If $\varrho \in G(e_i)$, then $\varrho e_i = \varrho$, hence $\varrho(1 - e_i) = 0$.

b) If $\varrho \notin G(e_i)$ and $\varrho \neq 0$, then there is an idempotent $\varepsilon \neq 0$ such that $\varrho \in G(\varepsilon) \neq G(e_i)$. Next, $\varrho e_i \in G(\varepsilon) \cdot e_i = G(1) \cdot \varepsilon e_i$.

Since $\varepsilon \cdot e_i$ is either 0 or e_i, we have either $\varrho e_i = 0$ or $\varrho e_i \in G(e_i)$. In both cases we have $\varrho \neq \varrho e_i$.

We have proved

Proposition 3.2. *If $(n,p)=1$, a non-zero element $\varrho\in\overline{R}$ is contained in the group $G(e_i)$ if and only if $\varrho(1-e_i)=0$.*

This last statement enables us to describe all elements of $G(e_i)$ in the polynomial form $\varrho=r_0+r_1+\ldots+r_{n-1}x^{n-1}$. The unknowns r_i $(i=0,\ldots,r-1)$ appear as a solution of a system of linear equations.

The following two examples show how this works.

Example 3.3. We have to find all NB-generators of $F_{5^3}|F_5$ (supposing that one NB-generator α is known).

The problem reduces to finding all elements of $R=F_5[x]/(x^3-1)$ which are relatively prime to x^3-1.

In F_5 we have $x^3-1=f_1f_2=(x-1)(1+x+x^2)$ and $|G(1)|=|\Gamma(3,5)|=5^3(1-5^{-1})(1-5^{-2})=96$. The primitive idempotents are (by Lemma 2.6) $e_1=2(1+x+x^2)$, $e_2=4+3x+3x^2$.

a) We describe $G(e_1)$. The element $\varrho=r_0+r_1x+r_2x^2$, $r_i\in F_5$, $\varrho\neq 0$ is contained in $G(e_1)$ if and only if $\varrho(1-e_1)=0$, i.e. $(r_0+r_1x+r_2x^2)(4+3x+3x^2)=0$. This leads to the system of linear equations (of rank 2)

$$\begin{aligned}4r_0+3r_1+3r_2&=0,\\3r_0+4r_1+3r_2&=0,\\3r_0+3r_1+4r_2&=0,\end{aligned}$$

whence $r_0=r_1=r_2$. Finally, $G(e_1)=\big\{r_0(1+x+x^2)|r_0\neq 0\big\}$. Clearly $|G(e_1)|=4$.

b) We specify $G(e_2)$. Put $\varrho'=r_0'+r_1'x+r_2'x^2$. Then $\varrho'(1-e_2)=(r_0'+r_1'x+r_2'x^2)(2+2x+2x^2)=0$ implies a linear system of rank 1. Namely, $r_o'+r_1'+r_2'=0$. Hence $r_0'=4(r_1'+r_2')$, and $\varrho'=4(r_1'+r_2')+r_1'x+r_2'x^2$, $(r_1',r_2')\neq(0,0)$. Also $|G(e_2)|=24$.

c) Changing the notation $(r_1'\to r_1, r_2'\to r_2)$ we have

$$G(1)=\big\{r_0(1+x+x^2)\oplus\big[4(r_1+r_2)+r_1x+r_2x^2\big]\big\}.$$

Using the mapping Ω we get the following result:

If α is one NB-generator of $F_{5^3}|F_5$, then all NB-generators of $F_{5^3}|F_5$ are given by the set of 96 elements

$$\Gamma(3,5)=\big\{r_0(\alpha+\alpha^5+\alpha^{25})+r_1(4\alpha+\alpha^5)+r_2(4\alpha+\alpha^{25}\big\},$$

where the triples (r_0,r_1,r_2) are subject to the conditions $r_0\neq 0$, $(r_1,r_2)\neq(0,0)$.

Remark 1. There is of course a natural question how to decide whether an element $\alpha \in F_{q^n}$ is an NB-generator of $F_{q^n}|F_q$ or not. In this direction we refer to [7], where it is proved that α is an NB-generator of $F_q(\alpha)$ if and only if $\Omega(f_i^{t-1}F_i^t) \neq 0$ for $i = 1, \ldots, r$.

Remark 2. If we know a concrete N-polynomial of degree 3 over F_5, the formula for $\Gamma(3,5)$ can be reduced to a polynomial in α of degree 2. For instance, $x^3 + x^2 + 1$ is an N-polynomial over F_5. If α is the root of this polynomial, then $\alpha^5 = 4 + \alpha + 3\alpha^2$, $a^{25} = 3\alpha + 2\alpha^2$, and we have $\Gamma(3,5) = \{4r_0 + r_1(4 + 3\alpha^2) + r_2(2\alpha + 2\alpha^2)\}$.

Remark 3. It follows from the foregoing results: If we know a "parametric expression" for the generators $g = g(r_1, \ldots r_n)$, then $(x-g)(x-g^q)\ldots(x-g^{q^{n-1}})$ is an N-polynomial of degree n over F_q with parameters $(r_1, \ldots, r_n)$ comprising all N-polynomials of degree n over F_q. Unfortunately the "technical realization" turns out to be rather complicated. We will return to this question in Section 5.

Example 3.4. We have to find all NB-generators of $F_{7^4}|F_7$.

The factorization of $x^4 - 1$ over F_7 is $x^4 - 1 = (x-1)(x+1)(x^2+1)$. The primitive idempotents of $F_7[x]/(x^4 - 1)$ are $e_1 = 2(1 + x + x^2 + x^3)$, $e_2 = 2(1 - x + x^2 - x^3)$, $e_3 = 4(1 - x^2)$.

a) To find $G(e_1)$ we put $\varrho(e_1 - 1) = (r_0 + r_1x + r_2x^2 + r_3x^3)(1 + 2x + 2x^2 + 2x^3) = 0$. This leads to the system of linear equations

$$\begin{pmatrix} 1 & 2 & 2 & 2 \\ 2 & 1 & 2 & 2 \\ 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 1 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{pmatrix} = 0,$$

which implies $r_0 = r_1 = r_2 = r_3$, so that $G(e_1) = \{r_0(1 + x + x^2 + x^3) | r_0 \neq 0\}$.

b) Next, in order to find $G(e_2)$ we write $\varrho'(e_2 - 1) = (r'_0 + r'_1x + r'_2x^2 + r'_3x^3)$ $(1 - 2x + 2x^2 - 2x^3) = 0$. This implies

$$\begin{pmatrix} 1 & -2 & 2 & -2 \\ -2 & 1 & -2, & 2 \\ 2 & -2 & 1 & -2 \\ -2 & 2 & -2 & 1 \end{pmatrix} \begin{pmatrix} r'_0 \\ r'_1 \\ r'_2 \\ r'_3 \end{pmatrix} = 0,$$

whence $r'_o + r'_1 = 0$, $r'_1 + r'_2 = 0$, $r'_2 + r'_3 = 0$ and $r'_1 = -r'_0$, $r'_2 = r'_0$, $r'_3 = -r'_0$, so that $G(e_2) = \{r'_0(1 - x + x^2 - x^3) | r'_0 \neq 0\}$.

c) Finally, $\varrho''(1 - e_3) = (r''_0 + r''_1x + r''_2x^2 + r''_3x^3) \cdot 4 \cdot (1 + x^2) = 0$ implies $(r''_0 + r''_2) + (r''_1 + r''_3)x + (r''_0 + r''_2)x^2 + (r''_1 + r''_3)x^3 = 0$ and $r''_2 = -r''_0$, $r''_3 = -r''_1$, so that $G(e_3) = \{r''_0(1 - x^2) + r''_1(x - x^3)\}$, where $(r''_0, r''_1) \neq (0,0)$.

We have $|G(e_1)| = |G(e_2)| = 6$, $|G(e_3)| = 48$ and $|G(1)| = 1728$.

By changing the notation, we have

$$G(1) = \Big\{ r_0(1 + x + x^2 + x^3) \oplus r_1(1 - x + x^2 - x^3) \oplus \big[r_2(1 - x^2) + r_3(x - x^3) \big] \Big\}.$$

This implies the following result.

If α is one NB-generator of $F_{7^4}|F_7$, then all NB-generators of $F_{7^4}|F_7$ are given by the set of 1728 elements

$$\begin{aligned} \Gamma(4,7) = \big\{ & r_0(\alpha + \alpha^7 + \alpha^{49} + \alpha^{343}) + r_1(\alpha - \alpha^7 + \alpha^{49} - \alpha^{343}) \\ & + r_2(\alpha - \alpha^{49}) + r_3(\alpha^7 - \alpha^{343}) \big\}. \end{aligned}$$

Hereby the quadruples (r_0, r_1, r_2, r_3) are subject to the conditions $r_0 \neq 0$, $r_1 \neq 0$ and $(r_2, r_3) \neq (0, 0)$.

Remark. The polynomial $x^4 + x^3 + 1$ is an N-polynomial over F_7. If we choose α as the root of this polynomial, we get

$$\begin{aligned} \Gamma(4,7) = \big\{ & 6r_0 + r_1(1 + 4\alpha^2 + \alpha^3) + r_2(2\alpha + 5\alpha^2 + 3\alpha^3) \\ & + r_3(3 + 5\alpha + 4\alpha^2 + 4\alpha^3) \big\}, \end{aligned}$$

where $r_0 \neq 0$, $r_1 \neq 0$ and $(r_2, r_3) \neq (0, 0)$.

4. The case $(n, p) > 1$

We now suppose $x^n - 1 = (x^{n_0} - 1)^t = (f_1 \dots f_r)^t$, $t = p^s > 1$. Our goal is to find $G(e_i)$, where e_i $(i = 1, \dots, r)$ are the primitive idempotents.

In this case the semigroup $\overline{R}$ is not a set-theoretical union of disjoint groups. So we have to follow a slightly different way.

Write $U = \overline{R}e_1 \oplus \dots \oplus \overline{R}e_r$. It is easy to see that $U = \overline{R}$ and $\overline{R}e_i \cap \overline{R}e_j = \{0\}$. The set $\overline{R}e_i$ is an ideal of the semigroup $\overline{R}$, containing exactly two idempotents, namely e_i and 0. It is known that if an ideal I of any semigroup contains an idempotent e, then I contains the whole maximal group $G(e)$.

Therefore we may write $\overline{R}e_i = G(e_i) \cup I(e_i)$, $G(e_i) \cap I(e_i) = \emptyset$, and $I(e_i)$ is the set of all nilpotent elements of $\overline{R}e_i$. The set $\overline{R}e_i$ is the set of all $\varrho \in \overline{R}$ for which $\varrho e_i = \varrho$, i.e., $\varrho(1 - e_i) = 0$.

Any $\varrho \in R$ can be written in the form $\varrho = f_{j_1}^{\tau_1} \cdot f_{j_2}^{\tau_2} \dots f_{j_v}^{\tau_v} b$, $1 \leqslant \tau_j \leqslant t$, and $e_i = F_i^t a_i$, where $b, a_i \in G(1)$. We have $\varrho \cdot e_i = f_{j_1}^{\tau_1} f_{j_2}^{\tau_2} \dots f_{j_v}^{\tau_v} \cdot F_i^t a_i \cdot b = f_i^{\tau_i} \cdot F_i^t c$, $c \in G(1)$. It is immediately seen that ϱe_i is nilpotent if and only if $\tau_i \geqslant 1$, i.e., if and only if $f_i(x)$ divides $\varrho \in Re_i$. [Also, if $\tau_i \geqslant 1$, it is clear that $\varrho^t = 0$.] We have proved

Proposition 4.1. *Let $(n, p) > 1$. An element $\varrho \in \overline{R}$ is contained in the maximal group $G(e_i)$ if and only if $\varrho(1 - e_i) = 0$, and f_i does not divide ϱ.*

Hence, to find $G(e_i)$ we have first to find all ϱ satisfying $\varrho(1 - e_i) = 0$ and then to exclude all those which are divisible by f_i.

Remark. The condition that $f_i(x)$ divides $\varrho(x) = r_0 + r_1 x + \ldots r_{n-1} x^{n-1}$ leads to a system of n_i homogeneous linear equations for $\{r_0, \ldots, r_{n-1}\}$ from which the constrains for the $r_i{}'s$ follow. To see this let ξ be a root of the irreducible polynomial $f_i(x)$. Then $f_i(\xi) = 0$ enables us to compute ξ^k for all $k \geqslant n_i$ in the form $\xi^k = b_0^{(k)} + b_1^{(k)}\xi + \ldots b_{n_i-1}^{(k)}\xi^{n_i-1}$. We then have $\varrho(\xi) = r_0 + r_1\xi + \ldots + r_{n-1}\xi^{n-1} = c_0 + c_1\xi + \ldots + c_{n_i-1}\xi^{n_i-1}$, where the $c_i{}'s$ are linear forms of $\{r_0, r_1, \ldots, r_{n-1}\}$ (with coefficients in F_q). Now, $f_i(x)$ divides $\varrho(x)$ if and only if $c_0 = c_1 = \ldots = c_{n_i-1} = 0$.

Example 4.2. We have to find all NB-generators of $F_{3^6}|F_3$ (supposing that one NB-generator α is known).

We have $x^6 - 1 = (x-1)^3(x+1)^3$. By Proposition 2.6 the primitive idempotents of $F_3[x]/(x^6 - 1)$ are $e_1 = 2(1 + x^3)$ and $e_2 = 2(1 - x^3)$.

a) Write $\varrho = r_0 + r_1 x + \ldots + r_5 x^5$. The condition $\varrho(1 - e_1) = (r_0 + r_1 x + \ldots + r_5 x^5)(x^3 - 1) = (r_3 - r_0) + (r_4 - r_1)x + (r_5 - r_2)x^2 + (r_0 - r_3)x^3 + (r_1 - r_4)x^4 + (r_2 - r_5)x^5 = 0$ implies $r_3 = r_0$, $r_4 = r_1$, $r_5 = r_2$. Hence all polynomials $\varrho \neq 0$ satisfying $\varrho e_1 = \varrho$ are $\{r_0 + r_1 x + r_2 x^2 + r_o x^3 + r_1 x^4 + r_2 x^5\} = \big\{(1 + x^3)(r_0 x + r_1 x + r_2 x^2)\big\}$, where $(r_0, r_1, r_2) \neq (0, 0, 0)$.

Now we have to exclude those polynomials which are divisible by $f_1 = x - 1$. These are the polynomials for which $r_0 + r_1 + r_2 = 0$. Hence

$$G(e_1) = \big\{(r_o(1 + x^3) + r_1(x + x^4) + r_2(x^2 + x^5)\big\}, \quad \text{where} \quad r_0 + r_1 + r_2 \neq 0.$$

Clearly, $|G(e_1)| = 18$.

b) Next, write $\varrho' = r_0' + r_1' x + \ldots + r_5' x^5$. The condition $\varrho(1 - e_2) = (r_0' + r_1' x + \ldots + r_5' x^5)(2 + 2x^3) = 0$ implies $r_0' + r_3' = 0$, $r_1' + r_4' = 0$, $r_2' + r_5' = 0$.

Hence all elements ϱ of R satisfying $\varrho e_2 = \varrho$ are

$$\{r_0' + r_1' x + r_2' x^2 - r_0' x^3 - r_1' x^4 - r_2' x^5\}, \quad \text{where} \quad (r_0', r_1', r_2') \neq (0, 0, 0).$$

From these polynomials we have to exclude those which are divisible by $f_2 = x + 1$. These are the polynomials for which $r_0' - r_1' + r_2' = 0$. Hence

$$G(e_2) = \big\{r_0'(1 - x^3) + r_1'(x - x^4) + r_2'(x^2 - x^5)\big\}, \quad \text{where} \quad r_0' - r_1' + r_2' \neq 0.$$

Again, $|G(e_2)| = 18$.

c) Finally, $G(1) = G(e_1) \oplus G(e_2)$ implies

$$\Gamma(6,3) = \big[r_0(\alpha+\alpha^{27}) + r_1(\alpha^3+\alpha^{81}) + r_2(\alpha^9+\alpha^{243})\big]$$
$$\oplus \big[r_0'(\alpha-\alpha^{27}) + r_1'(\alpha^3-\alpha^{81}) + r_2'(\alpha^9-\alpha^{243})\big].$$

Denoting $A = \alpha + \alpha^{27}$, $B = \alpha - \alpha^{27}$, we may write this in the form

$$\Gamma(6,3) = \big\{[r_0A + r_1A^3 + r_2A^9] \oplus [r_0'B + r_1'B^3 + r_2'B^9]\big\},$$

where $r_0 + r_1 + r_2 \neq 0$ and $r_0' - r_1' + r_2' \neq 0$. Clearly, $|\Gamma(6,3)| = 324$.

Example 4.3. To see how the results look like for larger n we give here (without the necessary computations) the result concerning the set of all NB-generators of $GF(3^{12})|GF(3)$.

The factorization of $x^{12}-1$ into irreducible factors over F_3 is $x^{12}-1 = (x-1)^3(x+1)^3(x^2+1)^3 = f_1^3 f_1^3 f_3^3$. By Proposition 2.6 the primitive idempotents are $e_1 = 1 + x^3 + x^6 + x^9$, $e_2 = 1 - x^3 + x^6 - x^9$, $e_3 = x^6 - 1$.

$$G(e_1) = \big\{(r_0 + r_1x + r_2x^2)(1+x^3+x^6+x^9) | r_0 + r_1 + r_2 \neq 0\big\}, \text{ and } |G(e_1)| = 18.$$

$$G(e_2) = \big\{(r_0' + r_1x' + r_2'x^2)(1-x^3+x^6-x^9) | r_0' - r_1' + r_2' \neq 0\big\}, \text{ and } |G(e_2)| = 18.$$

$$G(e_3) = \big\{(r_0'' + r_1''x + r_2''x^2 + r_3''x^3 + r_4''x^4 + r_5''x^5)(1-x^6)\big\},$$

where $(r_0'' - r_2'' + r_4'', r_1'' - r_3'' + r_5'') \neq (0,0)$, and $|G(e_3)| = 2^3 \cdot 3^4$.

Hence $G(1) = G(e_1) \oplus G(e_2) \oplus G(e_3)$ and $|G(1)| = 2^5 \cdot 3^8 = 209952$.

Denote $A_1 = \alpha + \alpha^{3^3} + \alpha^{3^6} + \alpha^{3^9}$, $A_2 = \alpha - \alpha^{3^3} + \alpha^{3^6} - \alpha^{3^9}$, $A_3 = \alpha - \alpha^{3^6}$. Then the set of all NB-generators of $GF(3^{12})|GF(3)$ is given by the formula

$$\Gamma(12,3) = \big\{(r_0A_1 + r_1A_1^3 + r_2A_1^9) \oplus (r_0'A_2 + r_1'A_2^3 + r_2'A_2^9)$$
$$\oplus (r_0''A_3 + r_1''A_3^3 + r_2''A_3^9 + r_3''A_3^{27} + r_4''A_3^{81} + r_5''A_3^{243})\big\},$$

where the restrictions for the $r_i's$ are given above.

Example 4.4. Simple results are obtained if we consider the extension $F_{q^n}|F_q$, where n is a power of the characteristic, $p = \mathrm{char}(F_q)$.

Consider, e.g., the case $F_{p^p}|F_p$. The ring $F_p[x]/(x^p-1) = F_p[x]/(x-1)^p$ contains a unique non-zero idempotent (namely 1), and $G(1)$ consists of all polynomials $\varrho = r_0 + r_1x + \ldots + r_{p-1}x^{p-1}$ which are not divisible by $x-1$, i.e., such that $r_0 + r_1 + \ldots + r_{p-1} \neq 0$. Hence $G(1) = \big\{r_0 + r_1x + \ldots + r_{p-1}x^{p-1} | r_0 + r_1 + \ldots + r_{p-1} \neq 0\big\}$. If α is one NB-generator of $F_{p^p}|F_p$, then all the others are given by

$$\Gamma(p,p) = \big\{r_0\alpha + r_1\alpha^p + \ldots + r_{p-1}\alpha^{p^{p-1}} | r_0 + r_1 + \ldots + r_{p-1} \neq 0\big\}.$$

Here $|\Gamma(p,p)| = p^p - p^{p-1}$.

In the preceding sections we have shown how to describe all NB-generators of $F_{q^n}|F_q$ by one formula (containing parameters). If $g = g(\alpha, r_1, \dots, r_n)$ is this "general expression", then $h(x) = h(x, r_1, \dots, r_n) = (x-g)(x-g^q)\dots(x-g^{q^{n-1}})$ is a "general expression" for all N-polynomials of degree $n \geqslant 2$ over F_q. In other words, if we know one N-polynomial of degree $n \geqslant 2$, we are able (in principle) to describe all N-polynomials of degree n by one formula (containing parameters r_i). It is sufficient to write down $h(x)$ as a polynomial with coefficients $\in F_q$. For $n = 2$ this is rather easy. For $n = 3$ we show in Example 3.3 how the straightforward procedure looks like. For $n \geqslant 4$ the evaluation is rather cumbersome.

Example 5.1. We prove two statements concerning quadratic N-polynomials.

Statement 1. *Let $x^2 + a_1x + a_2$ be one N-polynomial over F_q, $\operatorname{char}(F_q) = p > 2$. Then the set $\{h(x)\}$ of all quadratic N-polynomials over F_q is given by the formula*

$$h(x) = x^2 + 2a_1r_0x + r_o^2a_1^2 - r_1^2(a_1^2 - 4a_2),$$

where $r_0, r_1 \in F_q$ and $r_0r_1 \neq 0$.

P r o o f. The factorization $x^2 - 1 = (x-1)(x+1)$ over F_q implies that the primitive idempotents of $F_q[x]/(x^2-1)$ are $e_1 = \frac{1}{2}(1+x)$ and $e_2 = \frac{1}{2}(1-x)$, so that $G(1) = r_0(1+x) \oplus r_1(1-x)$, where $r_0r_1 \neq 0$, and $\Gamma(2,q) = \{r_0(\alpha+\alpha^q) \oplus r_1(\alpha - \alpha^q)\}$, where α is a root of $x^2 + a_1x + a_2 = 0$.

If $g = r_0(\alpha + \alpha^q) + r_1(\alpha - \alpha^q)$, then $g^q = r_0(\alpha^q + \alpha) + r_1(\alpha^q - \alpha)$, and $g + g^q = 2r_0(\alpha+\alpha^q) = -2a_1r_0$, $gg^q = r_0^2(\alpha+\alpha^q)^2 - r_1^2(\alpha-\alpha^q)^2 = r_0^2a_1^2 - r_1^2(a_1^2 - 4a_2)$. This proves our statement. [Clearly there are $\frac{1}{2}(q-1)^2$ different quadratic N-polynomials over F_q.] $\square$

To have a numerical example let us describe (by one formula) the set of all quadratic N-polynomials over F_7, knowing that, e.g., $x^2 + x + 3$ is an N-polynomial over F_7. We then have $h(x) = x^2 + 2r_0x + r_o^2 + r_1^2$. To obtain all the 18 different ones it is sufficient to choose $r_0 \in \{1, 2, \dots, 6\}$, $r_1^2 \in \{1, 2, 4\}$.

To complete our considerations we have to consider also the case $\operatorname{char}(F_q) = 2$, $q = 2^s$, $n = 2$.

Statement 2. *Let $x^2 + b_1x + b_2$ be one N-polynomial of degree 2 over $F_q = GF(2^s)$. Then all N-polynomials of degree 2 over F_q are given by the formula*

$$h(x) = x^2 + b_1(r_0 + r_1)x + (r_0 + r_1)^2b_2 + r_0r_1b_1^2,$$

where $r_0, r_1 \in F_q$ and $r_0 \neq r_1$.

P r o o f. The ring $F_q[x]/(x-1)^2$ has a unique non-zero idempotent (namely $e = 1$). To find $G(1)$ we have (in accordance with Proposition 4.1) to exclude all those polynomials $r_0 + r_1 x$ which are divisible by $f(x) = x + 1$. These are the polynomials for which $r_0 + r_1 = 0$ (i.e. $r_0 = r_1$). We have therefore

$$G(1) = \{r_0 + r_1 x | r_0, r_1 \in F_q,\ r_0 \neq r_1\}.$$

If β is the root of $x^2 + b_1 x + b_2$ we immediately obtain the set of all NB-generators

$$\Gamma(2, q) = \Gamma(2, 2^s) = \{r_0\beta + r_1\beta^q | r_0, r_1 \in F_q,\ r_0 \neq r_1\}.$$

If $g = r_0\beta + r_1\beta^q$ is an NB-generator, we have $g + g^q = (r_0\beta + r_1\beta^q) + (r_0\beta^q + r_1\beta) = b_1(r_0 + r_1)$ and $g \cdot g^q = (r_0\beta + r_1\beta^q)(r_o\beta^q + r_1\beta) = (r_0 + r_1)^2 \cdot b_2 + r_0 r_1(\beta + \beta^q)^2 = (r_0^2 + r_1^2)b_2 + r_0 r_1 b_1^2$. Therefore $h(x) = (x - g)(x - g^q) = x^2 + b_1(r_0 + r_1)x + (r_0 + r_1)^2 b_2 + r_0 r_1 b_1^2$. This formula comprises all the $\frac{1}{2}q(q-1)$ N-polynomials of degree 2 over F_q. □

Example 5.2. We have to find all N-polynomials of degree 3 over F_5.

In Example 3.3 we have proved that any NB-generator g of $F_{5^3}|F_5$ is of the form

$$g = r_0(\alpha + \alpha^5 + \alpha^{25}) + r_1(4\alpha + \alpha^5) + r_2(4\alpha + \alpha^{25}),$$

whence

$$g^5 = r_0(\alpha + \alpha^5 + \alpha^{25}) + r_1(4\alpha^5 + \alpha^{25}) + r_2(4\alpha^5 + \alpha),$$
$$g^{25} = r_0(\alpha + \alpha^5 + \alpha^{25}) + r_1(4\alpha^{25} + \alpha) + r_2(4\alpha^{25} + \alpha^5).$$

Here α is a root of an N-polynomial $x^3 + a_1 x^2 + a_2 x + a_3 = 0$, and an admissible triple (r_0, r_1, r_2) is defined by the restrictions $r_0 \neq 0$, $(r_1, r_2) \neq (0, 0)$.

Our goal is to calculate

$$h(x) = (x - g)(x - g^5)(x - g^{25})$$

as a polynomial over F_5.

Since $r_0(\alpha + \alpha^p + \alpha^{p^2}) = -r_0 a_1$, we shall write $g + r_0 a_1 = g_1$, so that $g_1 = r_1(4\alpha + \alpha^5) + r_2(4\alpha + \alpha^{25})$, and we shall evaluate the product

$$h_1(y) = (y - g_1)(y - g_1^5)(y - g_1^{25}) = y^3 + b_1 y^2 + b_2 y + b_3.$$

Note first that $-b_1 = g_1 + g_1^5 + g_1^{25} = g + g^5 + g^{25} + 3r_0 a_1 = 3r_0(\alpha + \alpha + \alpha^{25}) + 3r_0 a_1 = -3r_0 a_1 + 3r_0 a_1 = 0$ (independently of the choice of α).

Now choose α as a root of the N-polynomial $x^3 + x^2 + 1$ (over F_5). Then $g_1 = r_1(4\alpha + \alpha^5) + r_2(4\alpha + \alpha^{25}) = r_1(4 + 3\alpha^2) + r_2(2\alpha + 2\alpha^2)$ satisfies an equation $g_1^3 + b_2 g_1 + b_3 = 0$ with unknowns b_2, b_3.

Hence

$$\big[r_1(4+3\alpha^2) + r_2(2\alpha + 2\alpha^2)\big]^3 + b_2\big[r_1(4+3\alpha^2) + r_2(2\alpha+2\alpha^2)\big] + b_3 = 0,$$

i.e.,

$$\begin{aligned}\big[r_1^3(1+3\alpha^2) + r_1^2 r_2(4+2\alpha) + r_1 r_2^2(3+2\alpha) + r_2^3(3+2\alpha+2\alpha^2)\big]&\\ + b_2\big[4r_1 + 2r_2\alpha + (3r_1+2r_2)\alpha^2\big] + b_3 = 0.&\end{aligned}$$

This leads to the following three equations:

$$\begin{aligned}&r_1^3 + 4r_1^2 r_2 + 3r_1 r_2^2 + 3r_2^2 + 4b_2 r_1 + b_3 = 0,\\ &2r_1^2 r_2 + 2r_1 r_2^2 + 2r_2^3 + 2r_2 b_2 = 0,\\ &3r_1^3 + 2r_2^3 + b_2(3r_1 + 2r_2) = 0.\end{aligned}$$

From the second (which is equivalent to the third if $r_2 \neq 0$ or $r_1 - r_2 \neq 0$) we get $b_2 = 4(r_1^2 + r_1 r_2 + r_2^2)$, and from the first $b_3 = 3r_1^3 + r_1 r_2^2 + 2r_2^3$. This holds also if $r_2 = 0$ or $r_1 - r_2 = 0$. Hence

$$h_1(y) = y^3 + 4(r_1^2 + r_1 r_2 + r_2^2)y + (3r_1^3 + r_1 r_2^2 + 2r_2^3),$$

and replacing y by $x + r_0 a_1 = x + r_0$, we finally get

$$(*)\qquad h(x) = (x+r_0)^3 + 4(r_1^2 + r_1 r_2 + r_2^2)(x + r_0) + (3r_1^3 + r_1 r_2^2 + 2r_2^3).$$

The formula $(*)$ contains formally 96 polynomials. It is of course clear that three different triples (r_0, r_1, r_2) always lead to the same N-polynomial. We show that in our case the triples (r_0, r_1, r_2), $(r_0, 4r_1 + 4r_2, r_1)$, $(r_0, r_2, 4r_1 + 4r_2)$ are giving the same polynomial $h(x)$.

To see this it is sufficient to find (r_0', r_1', r_2') such that $(r_0' + 4r_1' + 4r_2')\alpha + (r_0' + r_1')\alpha^5 + (r_0' + r_2')\alpha^{25} = g^5 = (r_0 + 4r_1 + 4r_2)\alpha^5 + (r_0 + r_1)\alpha^{25} + (r_0 + r_2)\alpha$. This implies $r_0' + 4r_1' + 4r_2' = r_0 + r_2$, $r_0' + r_1' = r_0 + 4r_1 + 4r_2$, $r_0' + r_2' = r_0 + r_1$, whence $r_0' = r_0$, $r_1' = 4r_1 + r_2$, $r_2' = r_1$. Applying once more "the shift" $(r_0, r_1, r_2) \to (r_0, 4r_1 + 4r_2, r_1)$ to the second term we obtain the third triple $(r_0, r_2, 4r_1 + 4r_2)$.

We have proved

Statement 3. *The formula $(*)$ comprises exactly all the 32 N-polynomials of degree 3 over F_5, when (r_0, r_1, r_2) runs through all admissible triples. Hereby the triples*

(r_0, r_1, r_2), $(r_0, 4r_1 + 4r_2, r_1)$ *and* $(r_0, r_2, 4r_1 + 4r_2)$ *are giving the same polynomial* $h(x)$.

Remark. It is clear from our considerations that formulas of the type $(*)$ exist for any $n \geqslant 2$ and any F_q, but the effective construction of the corresponding N-polynomials for $n \geqslant 4$ is rather complicated.

References

[1] *Fricke, R.*: Lehrbuch der Algebra, Vol 3. Branschweig, 1928.

[2] *Lidl, R.; Niedereiter, H.*: Finite Fields. Addison-Wesley Publ. Comp., 1983.

[3] *Jungnickel, D.*: Finite Fields, Structure and Arithmetics. Wissenschaftsverlag, Mannheim, 1993.

[4] *Menezes, A.; Blake, I.; Gao, S.; Mullin, R.; Vanstone, S.; Yaghoobian, T.*: Applications of Finite Fields. Kluwer, 1992.

[5] *Nemoga, K.*: Algebraic theory of pseudocyclic codes, unpublished Ph. D. thesis. Math. Inst. of the Slovak Acad. of Sciences, Bratislava (1988).

[6] *Schwarz, Š.*: The role of semigroups in the elementary theory of numbers. Math. Slovaca *31* (1981), 369–395.

[7] *Schwarz, Š.*: Irreducible polynomials over finite fields with linearly independent roots. Math. Slovaca *38* (1988), 147–158.

Authors' address: Mathematical Institute, Slovak Academy of Sciences, Štefánikova 49, 814 73 Bratislava; Slovakia.