Normal Bases and Completely Free Elements in Prime Power Extensions over Finite Fields

DIRK HACHENBERGER

Institut für Mathematik der Universität Augsburg, Universitätsstrasse 14, D-86135 Augsburg, Germany
E-mail: Hachenberger@math.uni-augsburg.de

Communicated by Dieter Jungnickel

Received March 1, 1994; revised February 14, 1995

We continue the work of the previous paper (Hachenberger, *Finite Fields Appl.*, in press), and, generalizing some of the results obtained there, we give explicit constructions of free and completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$, where n is any nonnegative integer and where r is any odd prime number which does not divide the characteristic of $\mathrm{GF}(q)$ or where $r = 2$ and $q \equiv 1 \bmod 4$. Together with results on the case where $r = 2$ and $q \equiv 3 \bmod 4$ obtained in the previous paper and results on the well-known case where r is equal to the characteristic of $\mathrm{GF}(q)$, we are able to explicitly determine free and completely free elements in $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$ for every nonnegative integer m and every prime power q. © 1996 Academic Press, Inc.

1. PRIME POWER EXTENSIONS OVER A FINITE FIELD

Let $\mathrm{GF}(q)$ denote the Galois field of order q, where $q > 1$ is any prime power. Given any finite dimensional extension of $\mathrm{GF}(q)$, say of degree m, it is our aim to find elements w in $\mathrm{GF}(q^m)$ which are *free over* $\mathrm{GF}(q)$, i.e., which generate normal bases in $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$, or, which are *completely free over* $\mathrm{GF}(q)$, i.e., which simultaneously generate normal bases in $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q^d)$ for every intermediate field $\mathrm{GF}(q^d)$ of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$.

The existence of completely free elements in finite fields was first proved by Blessenohl and Johnsen in [1]. By Hilfssatz 4.4 in [1] (in the case of finite fields see also Theorem 3.1 in [3] or, in the case of ordinary free elements in finite fields, Lemma 1.1 in [9]) the existance problem is easily reduced to the case where m is a prime power:

1071-5797/95 $12.00

If m_1, $m_2 \geq 1$ are relatively prime integers and w_1, w_2 are free in $\mathrm{GF}(q^{m_1})$ over $\mathrm{GF}(q)$ and $\mathrm{GF}(q^{m_2})$ over $\mathrm{GF}(q)$, respectively, then w_1w_2 is free in $\mathrm{GF}(q^{m_1m_2})$ over $\mathrm{GF}(q)$. Moreover, if w_1 and w_2 are completely free in $\mathrm{GF}(q^{m_1})$ over $\mathrm{GF}(q)$ and $\mathrm{GF}(q^{m_2})$ over $\mathrm{GF}(q)$, respectively, then w_1w_2 is completely free in $\mathrm{GF}(q^{m_1m_2})$ over $\mathrm{GF}(q)$.

This reduction is our motivation for studying extensions of $\mathrm{GF}(q)$ of prime power degree.

In Hachenberger [3] we gave a constructive proof of the existence of completely free elements in prime power extensions over finite fields and even were able to determine the exact number of completely free elements in those extensions. In the present paper, we continue the work of Hachenberger [4], which will be our standard reference throughout. There, based on results of [3], we have studied field extensions of prime power degree over $\mathrm{GF}(q)$ with the aim of explicitly constructing normal bases and completely free elements. The term explicit is meant in the sense of Theorems 3.3, 3.5, 3.6, and 4.3 and Algorithm 3.7 in [4] and of Theorem 2.1 and Theorem 3.1 of the present paper; i.e., we describe free and completely free elements in terms of a suitable root of unity which is used to obtain a certain field extension of the ground field $\mathrm{GF}(q)$.

The construction of ordinary normal basis in extensions of prime power degree is also studied in Semaev [9]. At the end of Section 2 of the present paper we will shortly discuss some of the results of [9].

From now on, let r be a prime number. We will always assume that r is different from the characteristic of $\mathrm{GF}(q)$. The case where r is equal to the characteristic of $\mathrm{GF}(q)$ is conceptionally different but easy to handle (see Theorem 3.2 in [3], Section 1 of [4], and, for ordinary free elements, Section 4 of [9]):

If r is equal to the characteristic of $\mathrm{GF}(q)$, then $w \in \mathrm{GF}(q^{r^n})$ is completely free over $\mathrm{GF}(q)$ if and only if w is free over $\mathrm{GF}(q)$ if and only if the $\mathrm{GF}(q)$-trace of w is nonzero.

Now, let $n \geq 0$ be any integer. In Section 2 of [4] (Theorem 2.4), based on results of [3], we have given a characterization of free and completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$, which led to a general recursive construction scheme of these elements (Theorem 2.5 of [4]). In Sections 3 and 4 of [4], we have restricted our attention to the case where $q - 1$ is divisible by r and have given explicit constructions of free and completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$. In the present paper, we drop the assumption that $q - 1$ is divisible by r and generalize some results obtained in [4] (see Theorem 2.1 and Theorem 3.1 in Section 2 and Section 3 of the present paper, respectively):

Besides the case where $r = 2$ and $q \equiv 3 \bmod 4$, for every prime number r different from the characteristic of $\mathrm{GF}(q)$, we explicitly construct series $(v_n)_{n\geq 0}$ in $\mathrm{GF}(q^{r^\infty}) := \cup_{n\geq 0}\mathrm{GF}(q^{r^n})$ such that the partial sums $w_n := \Sigma_{i:=0}^{n} v_i$

are free or completely free in $GF(q^{r^n})$ over $GF(q)$, depending on the choice of the series $(v_n)_{n\geq 0}$. In this context the reader might consult the book of Brawley and Schnibben [2] for background information.

The case where $r = 2$ and $q \equiv 3 \bmod 4$ requires special arguments and therefore has already been considered separately in Section 4 of [4]. Since the case where $r = 2$ and $q \equiv 1 \bmod 4$ falls into the scope of Section 3 in [4], we may here restrict our attention to the case where r is odd. However, all results hold at least in the case where $r = 2$ and $q \equiv 1 \bmod 4$.

From now on we assume that the ground field $GF(q)$ is given. Let $s := \mathrm{ord}_r(q)$ denote the multiplicative order of q modulo r, i.e., the least positive integer N such that $q^N - 1$ is divisible by r. Since $q^s \equiv 1 \bmod r$, given $GF(q^s)$ and applying the results from Section 3 in [4], we can construct *all* free and *all* completely free elements in $GF(q^{sr^n})$ over $GF(q^s)$ (see Theorem 3.5 and Algorithm 3.7 in [4]). But, if $s > 1$, the questions arise of whether and how one can construct free and completely free elements in $GF(q^{r^n})$ over $GF(q)$ from those in $GF(q^{sr^n})$ over $GF(q^s)$. Given an element w in $GF(q^{sr^n})$ which is free over $GF(q^s)$, one might guess that the $(GF(q^{sr^n}), GF(q^{r^n}))$-trace of w is a free element in $GF(q^{r^n})$ over $GF(q)$. But this is not true in general. The following example illustrates that some work must be done.

EXAMPLE 1.1. Let $q := 5$, $r := 3$, and $n := 1$. Then $s := \mathrm{ord}_3(5) = 2$. Let ζ be a root of the polynomial $x^2 + x + 1$. Then ζ is a primitive third root of unity and $GF(5^2)$ is obtained by adjoining ζ to the field $GF(5)$. Let η be a root of the polynomial $x^3 - \zeta$. Since this polynomial is irreducible over $GF(5^2)$, adjoining η to that field, we obtain $GF(5^6)$.

Now, an application of Theorem 3.5 in [4] shows that

$$\gamma := 3 + \zeta + (1 + \zeta^2)\eta + \zeta\eta^2$$

is free in $GF(5^6)$ over $GF(5^2)$. However, the following calculation shows that $T(\gamma)$, the $(GF(5^6), GF(5^3))$-trace of γ, is equal to 0 and thus is not at all free in $GF(5^3)$ over $GF(5)$:

$$\begin{aligned} T(\gamma) &= \gamma + \gamma^{125} \\ &= 3 + \zeta + \eta + \zeta^2\eta + \zeta\eta^2 + 3 + \zeta^{125} + \eta^{125} + \zeta^{250}\eta^{125} + \zeta^{125}\eta^{250} \\ &= 3 + \zeta + \eta + \zeta^2\eta + \zeta\eta^2 + 3 + \zeta^2 + \zeta^2\eta^2 + \eta^2 + \zeta\eta \\ &= 1 + \zeta + \zeta^2 + (1 + \zeta + \zeta^2)\eta + (1 + \zeta + \zeta^2)\eta^2 \\ &= 0. \end{aligned}$$

What we are going to do in Section 2 of the present paper is the following:

Suppose, we are given an element v_0 which generates a normal basis in $GF(q^s)$ over $GF(q)$. We construct a series $(v_n)_{n\geq 1}$ of elements in $GF(q^{sr^\infty})$

such that the partial sums $\Sigma_{i:=0}^{n} \nu_i$ are free in $\mathrm{GF}(q^{sr^n})$ over $\mathrm{GF}(q)$. (These elements are not necessarily free over $\mathrm{GF}(q^s)$.) Now, if for $i \geq 1$, we apply the $\mathrm{GF}(q^{sr^i})$, $\mathrm{GF}(q^{r^i})$)-trace function to the element ν_i, and if we replace ν_0 by any nonzero element v_0 of $\mathrm{GF}(q)$, we obtain a series of elements $(v_n)_{n\geq 0}$ in $\mathrm{GF}(q^{r^\infty})$ such that the partial sums $\Sigma_{i:=0}^{n} v_i$ are free in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$. In particular, it turns out that for $s > 1$, the field $\mathrm{GF}(q^s)$ is needed only for theoretical purposes; i.e., in order to solve our initial problem we do not really need to have free elements in $\mathrm{GF}(q^s)$ over $\mathrm{GF}(q)$.

In Section 3, we modify the results from Section 2 and construct series $(v_n)_{n\geq 0}$ in $\mathrm{GF}(q^{r^\infty})$ such that the partial sums $w_n := \Sigma_{i:=0}^{n} v_n$ are completely free in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$.

Summarizing, together with the results in the case where $r = 2$ and $q \equiv 3 \bmod 4$ obtained in Section 4 of [4] and the results in the case where r is equal to the characteristic of $\mathrm{GF}(q)$, we are able to explicitly determine free and completely free elements in any finite dimensional extension over any finite field.

2. Free Elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$

Throughout this section let $q > 1$ be a prime power and let r be an odd prime number different from the characteristic of the finite field $\mathrm{GF}(q)$; let s be the multiplicative order of q modulo r and, furthermore, let $\rho(q^s) \geq 1$ denote the largest integer N such that r^N divides $q^s - 1$.

Our general construction scheme of free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ is iterative (see Theorem 2.5 in [4]) and can be described as follows:

If $n = 0$, then every nonzero element in $\mathrm{GF}(q)$ is free over $\mathrm{GF}(q)$. If $n \geq 1$, by induction hypothesis, we assume that we have an element w_{n-1} in $\mathrm{GF}(q^{r^{n\ 1}})$ which is free over $\mathrm{GF}(q)$. We then explicitly construct a particular element v_n of the kernel of the $(\mathrm{GF}(q^{r^n}), \mathrm{GF}(q^{r^{n-1}}))$-trace function such that $w_{n-1} + v_n =: w_n$ is free in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$.

Moreover, every element in $\mathrm{GF}(q^{r^n})$ which is free over $\mathrm{GF}(q)$ can be constructed in this way (see Theorem 2.4 in [4]).

In order to state our main result, i.e., Theorem 2.1 below, we need some further notation, which will be used throughout the entire section:

Given an integer $n \geq 1$, let $a(n) := \min\{\rho(q^s), n\}$.

Since r and q are relatively prime, the multiplication with q induces a bijection on the set of units modulo $r^{a(n)}$. Furthermore, by the definition of s and $a(n)$, the order of that bijection is equal to s and all orbits of that mapping have cardinality s. Now, let I be any complete set of representatives of units modulo $r^{a(n)}$, and let $J_{n,r,q}$ be any complete set of q-orbit representatives of I. Then

$$I_{n,r,q} := \bigcup_{j:=0}^{s-1} J_{n,r,q} \cdot q^j \tag{2.1}$$

likewise is a complete set of representatives of units modulo $r^{a(n)}$.

THEOREM 2.1. *Let q, r, s, and $\rho(q^s)$ be as above. For an integer $n \geq 1$ let $a(n)$ and $J_{n,r,q}$ be as above and let η be a primitive $r^{n+\rho(q^s)}$th root of unity. Then the following holds*:

(2.1.1) *Assume that ω_{n-1} is free in $\mathrm{GF}(q^{sr^{n-1}})$ over $\mathrm{GF}(q)$. Let*

$$\nu_n := \sum_{j \in J_{n,r,q}} \eta^j.$$

Then $\omega_n := \omega_{n-1} + \nu_n$ generates a normal basis in $\mathrm{GF}(q^{sr^n})$ over $\mathrm{GF}(q)$.

(2.1.2) *Assume that w_{n-1} is free in $\mathrm{GF}(q^{r^{n-1}})$ over $\mathrm{GF}(q)$. Let T_n denote the $(\mathrm{GF}(q^{sr^n}), \mathrm{GF}(q^{r^n}))$-trace function and let*

$$v_n := \sum_{j \in J_{n,r,q}} T_n(\eta^j).$$

Then $\omega_n := \omega_{n-1} + v_n$ generates a normal basis in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$.

The proof of Theorem 2.1 proceeds in several steps. A short outline is given in the following paragraphs:

During all our considerations, we use that the additive group of $\mathrm{GF}(q^{sr^n})$ is equipped with various module structures which are induced by the Galois groups of this field over its subfields. All these structures can be studied by considering the additive group of $\mathrm{GF}(q^{sr^n})$ as vector space together with the various Frobenius automorphisms over its subfields. More details can be found in Section 1 of [3] and in Sections 1 and 2 of [4]. In this context we also refer to Lüneburg [7, 8] where the structure of finite dimensional vector spaces together with an endomorphism is studied from a constructive point of view.

Throughout this section, let η be a primitive $r^{n+\rho(q^s)}$th root of unity, and let $\zeta := \eta^{r^n}$. Then ζ is a primitive $r^{\rho(q^s)}$th root of unity. By the definition of s and $\rho(q^s)$ we know that ζ is an element of $\mathrm{GF}(q^s)$, and, from Theorem 2.8 in [4], one can deduce that $\mathrm{GF}(q^{sr^n})$ is obtained by adjoining η to $\mathrm{GF}(q^s)$.

Let σ denote the Frobenius automorphism in $\mathrm{GF}(q^{sr^n})$ over $\mathrm{GF}(q)$. Then σ^s generates the Galois group of $\mathrm{GF}(q^{sr^n})$ over $\mathrm{GF}(q^s)$. Now, since $q^s - 1$ is divisible by r and since we have assumed that r is odd, the assumptions of Section 3 in [4] are satisfied for the field extension $\mathrm{GF}(q^{sr^n})$ over $\mathrm{GF}(q^s)$:

In Theorem 3.3 of [4], we have proved that the *q^s-order* of η, i.e., the monic polynomial of least degree g over $\mathrm{GF}(q^s)$ such that $g(\sigma^s)(\eta) = 0$, is an irreducible $\mathrm{GF}(q^s)$-divisor of the r^nth cyclotomic polynomial. Since Φ_{r^n} over $\mathrm{GF}(q^s)$ splits into binomials (see Lemma 3.2 in [4]), we even were able to explicitly determine the q^s-order of η^j for every integer j which is not divisible by r (see Theorem 3.3 in [4] and its proof). This result is summarized in Proposition 2.2 below.

In Proposition 2.3 we determine the *q-order* of η^j, where j is not divisible by r, i.e., the monic polynomial f of least degree over $\mathrm{GF}(q)$ such that $f(\sigma)(\eta^j) = 0$. This enables us to prove that the element ν_n in statement (2.1.1) of Theorem 2.1 has q-order $\Phi^{r_n}(x^s)$, where x denotes an indeterminate (see Proposition 2.4). After that we can easily deduce that the element ω_n in (2.1.1) has q-order $x^{sr^n} - 1$, which is equivalent to the fact that it generates a normal basis in $\mathrm{GF}(q^{sr^n})$ over $\mathrm{GF}(q)$.

Finally, statement (2.1.2) in Theorem 2.1 follows from similar arguments in combination with Lemma 2.5, where the $(\mathrm{GF}(q^{sr^n}), \mathrm{GF}(q^{r^n}))$-trace function is considered.

PROPOSITION 2.2. *Under the assumptions above, let $Q := q^{sr^{n\ a(n)}}$ and let $A := \max\{n, \rho(q^s)\}$. Then $Q = 1 + ur^A$, where u is an integer which is not divisible by r. If j is any integer which is not divisible by r, then the q^s-order of η^j is equal to*

$$x^{r^{n\ a(n)}} - \zeta^{jur^{\rho(q^s)\ a(n)}}. \tag{2.2}$$

Furthermore, this polynomial is an irreducible $\mathrm{GF}(q^s)$*-divisor of the* r^nth *cyclotomic polynomial.*

Before we determine the q-order of each η^j with j not divisible by r, we consider the complete factorization of the r^nth cyclotomic polynomial over $\mathrm{GF}(q)$:

With u as in the statement of Proposition 2.2 let

$$\begin{aligned} f_{\eta^j} &:= \prod_{i:=0}^{s-1} \left(x^{r^{n\cdot a(n)}} - \sigma^i\left(\zeta^{jur^{\rho(q^s)\ a(n)}}\right)\right) \\ &= \prod_{i:=0}^{s-1} \left(x^{r^{n-a(n)}} - \zeta^{juq^i r^{\rho(q^s)-a(n)}}\right). \end{aligned} \tag{2.3}$$

Since $\zeta \in \mathrm{GF}(q^s)$ and since σ^s is the identity on $\mathrm{GF}(q^s)$, we see that f_{η^j} is a polynomial over $\mathrm{GF}(q)$. Furthermore, since uj is not divisible by r, we have that $\zeta^{ujr^{\rho(q^s)-a(n)}}$ is a primitive $r^{a(n)}$th root of unity. Moreover, by the definition of $a(n)$, the multiplicative order of q modulo $r^{a(n)}$ is equal to s, whence f_{η^j} is square-free and thus is a $\mathrm{GF}(q)$-divisor of Φ_{r^n}. Finally, as the multiplicative order of q modulo r^n by Theorem 2.8 in [4] is equal to $sr^{n-a(n)}$, which is equal to the degree of f_{η^j}, we conclude that f_{η^j} is irreducible over $\mathrm{GF}(q)$. (For the factorization pattern of cyclotomic polynomials see also Jungnickel [5, Theorem 1.5.4] or Lidl and Niederreiter [6, Theorem 2.47].)

Next, due to the fact that $J_{n,r,q}$ is a complete set of q-orbit representatives modulo $r^{a(n)}$, we obtain that

$$\Phi_{r^n} = \prod_{j \in J_{n,r,q}} f_{\eta^j} \tag{2.4}$$

is the complete factorization of Φ_{r^n} over $\mathrm{GF}(q)$. (Observe that f_{η^j} and f_{η^k} are different for different j and k in $J_{n,r,q}$ and that the degree of the product in (2.4) is equal to

$$|J_{n,r,q}| \cdot sr^{n-a(n)} = |I_{n,r,q}| \cdot r^{n-a(n)} = r^{a(n)-1}(r-1)r^{n-a(n)} = r^{n-1}(r-1),$$

where $I_{n,r,q}$ is as in (2.1). This number is equal to the degree of Φ_{r^n}.)

Proposition 2.3. *Suppose the general assumptions of this section. Let η be a primitive $r^{n+\rho(q^s)}$th root of unity, let j be any integer which is not divisible by r, and let f_{η^j} be as in (2.3).*

Then the q-order of η^j is equal to $f_{\eta^j}(x^s)$.

Proof. Since

$$f_{\eta^j}(x^s)(\sigma) = f_{\eta^j}(\sigma^s), \tag{2.5}$$

and since the q^s-order of η^j by Proposition 2.2 and the definition of f_{η^j} is a divisor of f_{η^j}, it is clear that the q-order of η^j is a divisor of $f_{\eta^j}(x^s)$. In order to show that η^j indeed has q-order $f_{\eta^j}(x^s)$, we must consider various module structures of the additive group of $\mathrm{GF}(q^{sr^n})$, which for simplicity is denoted by E.

Let

$$V := \{v \in E | f_{\eta^j}(\sigma^s)(v) = 0\}. \tag{2.6}$$

Then V is a σ-invariant $\mathrm{GF}(q)$-subspace of E which likewise is a σ^s-invariant $\mathrm{GF}(q^s)$-subspace of E. It can be characterized as the set of elements in E having q-order dividing $f_{\eta^j}(x^s)$ or, alternatively, as the set of elements having q^s-order dividing f_{η^j} (see Theorem 2.1 in [3]).

Now, let g be the q-order of η^j and let U be the σ-invariant $\mathrm{GF}(q)$-subspace of E which is generated by η^j. Then

$$U = \{v \in E | g(\sigma)(v) = 0\}, \tag{2.7}$$

and, since g divides $f_{\eta^j}(x^s)$, we have that U is contained in V. Moreover, U is equal to V if and only if g is equal to $f_{\eta^j}(x^s)$. It therefore remains to show that V is contained in U. This is done in what follows.

For $i \geq 0$, let V_i be the σ^s-invariant GF(q^s)-subspace of E which is generated by $\sigma^i(\eta^j) = \eta^{jq^i}$. From Proposition 2.2 we know that the q^s-order of $\sigma^i(\eta^j)$ is equal to $x^{r^{n-a(n)}} - \gamma_{j,i}$, where $\gamma_{j,i} := \eta^{ujq^i r^{n-a(n)-\rho(g^s)}}$ (with $a(n) = \min\{\rho(q^s), n\}$ and u being the cofactor of the maximal r-power dividing $q^{sr^{n\,a(n)}} - 1$). Therefore, V_i can be characterized as the GF(q^s)-eigenspace of the GF(q^s)-linear mapping $\sigma^{sr^{n\cdot a(n)}}$ belonging to the eigenvalue $\gamma_{j,i}$, i.e.,

$$V_i = \{v \in E | \sigma^{sr^{n\,a(n)}}(v) = \gamma_{j,i}v\}. \tag{2.8}$$

As f_{η^j} is square-free and $\prod_{i:=0}^{s-1} (x^{r^{n\,a(n)}} - \gamma_{j,i})$ is its complete factorization over GF(q^s), we know that $\bigoplus_{i:=0}^{s-1} V_i$ is the complete decomposition of V into σ^s-invariant GF(q^s)-subspaces. In order to complete the proof, it therefore remains to show that V_i is contained in U for every i.

Since x^i for any integer $i \geq 0$ is relatively prime to g, we have that

$$\eta^{jq^i} = \sigma^i(\eta^j) = (x^i(\sigma))(\eta^j)$$

likewise has q-order g. Thus $\sigma^i(\eta^j)$ is contained in U for all i. If we know that U is invariant under the multiplication with scalars from GF(q^s), we can conclude that V_i is contained in U for all $i \geq 0$. As we did not succeed to show this directly, we use an argument which also is very interesting in itself:

We define a scalar-multiplication $\circ$ on E by

$$\circ\colon \mathrm{GF}(q)[x] \times E \mapsto E, \qquad (h, v) \mapsto h(\sigma^s)(v) \tag{2.9}$$

(where GF$(q)[x]$ denotes the polynomial ring in the indeterminate x over GF(q)). For v in E, let the *$\circ$-order* of v be the monic polynomial h of least degree in GF$(q)[x]$ such that $h(\sigma^s)(v) = 0$. Of course, V is a $\circ$-submodule of E. Furthermore by the definition of V, the $\circ$-order of every nonzero w in V is a GF(q)-divisor of f_{η^j} of degree at least one. Since f_{η^j} is irreducible over GF(q), we see that every nonzero element of V indeed has $\circ$-order f_{η^j}. Thus, we have shown that $\circ$ induces an F-vector space structure on V, where F is isomorphic to the field GF$(q)[x]/f_{\eta^j}$GF$(q)[x]$ of residues modulo f_{η^j}. Since f_{η^j} has degree $sr^{n-a(n)}$, we obtain that F is isomorphic to

$\mathrm{GF}(q^{sr^n\ a(n)})$. Furthermore, it is clear that U and V_i for all i are $\circ$-invariant subspaces of V and therefore are F-subspaces of V.

Of course, there is a subfield of F which is isomorphic to $\mathrm{GF}(q^s)$, whence U likewise carries the structure of a $\mathrm{GF}(q^s)$-vector space. But the proof is not yet finished, since the $\circ$-multiplication and the ordinary multiplication with $\mathrm{GF}(q^s)$-scalars are different operations. So, we proceed by counting the F-dimension of the spaces involved:

The $\mathrm{GF}(q)$-degree of V is equal to the degree of $f_{\eta^j}(x^s)$. Since the $\mathrm{GF}(q)$-degree of F is equal to the degree of f_{η^j}, we obtain that the F-dimension of V is equal to s.

Now, since $V = \oplus_{i:=0}^{s-1} V_i$ and V_i is an F-subspace of V for all i, we conclude that V_i is a one-dimensional F-subspace of V. Therefore, this decomposition is a complete decomposition of V as F-vector space. Furthermore, we know that $\sigma^i(\eta^j)$ is a nonzero element of V_i, whence $V_i = F\sigma^i(\eta^j)$ for all $i \geq 0$. Now, as U likewise is an F-subspace of V and as $\sigma^i(\eta^j)$ is contained in U for all i, we finally obtain that

$$\sum_{i:=0}^{s-1} F\sigma^i(\eta^j) = \sum_{i:=0}^{s-1} V_i = V$$

is contained in U. This completes the proof of Proposition 2.3. ■

Using Proposition 2.3 and the $\mathrm{GF}(q)$-factorization of Φ_{r^n} in combination with Fact 2.2 or Lemma 3.3 from [4], which state that the q-order of $u + v$ is equal to fg provided f and g are relatively prime and u and v have q-orders f and g, respectively, we are now able to construct an element in $\mathrm{GF}(q^{sr^n})$ having q-order $\Phi_{r^n}(x^s)$.

PROPOSITION 2.4. *Suppose the general assumptions of this section. Let v_n be as in the first statement of Theorem* 2.1. *Then the q-order of v_n is equal to* Φ_{r^n} (x^s).

Proof. By Proposition 2.3, in particular for every j in $J_{n,r,q}$, the q-order of η^j is equal to $f_{\eta^j}(x^s)$, where f_{η^j} as in (2.3) is an irreducible $\mathrm{GF}(q)$-divisor of the r^nth cyclotomic polynomial Φ_{r^n}. As (2.4) is the complete factorization of Φ_{r^n} over $\mathrm{GF}(q)$, we obtain that

$$\Phi_{r^n}(x^s) = \prod_{j\in J_{n,r,q}} f_{\eta^j}(x^s). \tag{2.10}$$

Since the polynomials $f_{\eta^i}(x^s)$ and $f_{\eta^j}(x^s)$ are relatively prime for different i and j in $J_{n,r,q}$, an application of Fact 2.2 from [4] or Lemma 3.3 from [3] shows that

$$\nu_n := \sum_{j \in J_{n,r,q}} \eta^j$$

has q-order $\Phi_{r^n}(x^s)$. ■

We are now able to complete the proof of the first part of Theorem 2.1: If ω_{n-1} generates a normal basis in GF($q^{sr^{n-1}}$) over GF(q), then its q-order is equal to $x^{sr^{n-1}} - 1$. Applying once more Fact 2.2 of [4], we see that $\omega_n := \omega_{n-1} + \nu_n$ has q-order

$$(x^{sr^{n-1}} - 1)\Phi_{r^n}(x^s) = x^{sr^n} - 1, \tag{2.11}$$

which is equivalent to being free in GF(q^{sr^n}) over GF(q). ■

Now the following lemma enables us to find an element in GF(q^{r^n}) having q-order Φ_{r^n}.

Lemma 2.5. *Let q, r, and s be as above. Assume that $n \geq 1$ and let $\nu \in$ GF(q^{sr^n}) be an element having q-order $\Phi_{r^n}(x^s)$.*

Then the GF(q^{sr^n}), GF(q^{r^n}))*-trace of ν has q-order Φ_{r^n}.*

Proof. Let

$$T := \frac{x^{sr^n} - 1}{x^{r^n} - 1} = \sum_{i:=0}^{s-1} x^{ir^n}, \tag{2.12}$$

and let σ be the Frobenius automorphism in GF(q^{sr^n}) over GF(q). Then $T(\sigma)$ is the (GF(q^{sr^n}), GF(q^{r^n}))-trace function.

Comparing (2.11) and (2.12), we see that $\Phi_{r^n}(x^s)$ can be written as $\Phi_{r^n}S$, where S is the greatest common divisor of T and $\Phi_{r^n}(x^s)$. It can furthermore be shown that the cofactor R of S in T is relatively prime to Φ_{r^n}. Consequently, if ν has q-order $\Phi_{r^n}(x^s)$, then $S(\sigma)(\nu)$ has q-order Φ_{r^n}. Moreover, as R is relatively prime to Φ_{r^n}, the element $T(\sigma)(\nu) = R(S(\sigma)(\nu))$ likewise has q-order Φ_{r^n}. This completes the proof of the lemma. ■

We are now able to complete the proof of Theorem 2.1:

The element v_n in the statement (2.1.2) of Theorem 2.1 is equal to $T(\sigma)(\nu_n)$, where $\nu_n = \sum_{j \in J_{n,r,q}} \eta^j$. Since ν_n by Proposition 2.3 has q-order $\Phi_{r^n}(x^s)$, we see that v_n has q-order Φ_{r^n}. Furthermore (see Theorem 2.5 in [4]), if w_{n-1} has q-order $x^{r^{n-1}} - 1$, i.e., generates a normal basis in GF($q^{r^{n-1}}$) over GF(q), then $w_n := w_{n-1} + v_n$ is free in GF(q^{r^n}) over GF(q). ■

We close this section with some further remarks and an example.

Theorem 2.1 is also correct if $r = 2$ and $q \equiv 1 \bmod 4$. The only case not covered here is $r = 2$ and $q \equiv 3 \bmod 4$. However, this case is already handled in Section 4 of [4] for free and completely free elements.

If $s = 1$, the content of Theorem 2.1 is essentially the same as the second part of Theorem 3.3 in [4], where we have chosen $J_{n,r,q} = \{1 \leq k \leq r^{a(n)} | k$ not divisible by $r\}$.

With η, j, and f_{η^j} as above and with T_n being the $(\mathrm{GF}(q^{sr^n}), \mathrm{GF}(q^{r^n}))$-trace function, a similar argument as used in the proof of Lemma 2.5 shows that the q-order of $T_n(\eta^j)$ is an irreducible $\mathrm{GF}(q)$-divisor of Φ_{r^n}. Furthermore, by the choice of $J_{n,r,q}$, every irreducible $\mathrm{GF}(q)$-divisor of Φ_{r^n} occurs exactly once as q-order of some $T_n(\eta^j)$ with $j \in J_{n,r,q}$. Consequently with induction on n, for every irreducible $\mathrm{GF}(q)$-divisor of $x^{r^n} - 1$ one can find a generator of the corresponding irreducible σ-invariant $\mathrm{GF}(q)$-subspace of the additive group of $\mathrm{GF}(q^{r^n})$. As a consequence, similarly as in Theorem 3.5 in [4], *all* free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ can be described in terms of a primitive $r^{n+\rho(q^s)}$th root of unity η.

We have already mentioned Semaev's paper [9]. There, in order to construct free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$, likewise the decompositions of the additive group of $\mathrm{GF}(q^{sr^n})$ as σ-invariant $\mathrm{GF}(q)$-space and as σ^s-invariant $\mathrm{GF}(q^s)$-space are studied in connection with the $\mathrm{GF}(q^{sr^n})$, $\mathrm{GF}(q^{r^n})$)-trace function (σ again denotes the Frobenius automorphism in $\mathrm{GF}(q^{sr^n})$ over $\mathrm{GF}(q)$). (See Lemma 2.3, Theorem 2.4, and the discussion after Theorem 2.4). Here, in contrast to [9], we have used an induction argument which led to the iterative construction scheme outlined in Section 2 of [4] and could therefore direct our interest towards the structure of the subspaces of $\mathrm{GF}(q^{sr^n})$ and $\mathrm{GF}(q^{r^n})$ which are annihilated by the polynomials $\Phi_{r^n}(x^s)$ and Φ_{r^n}, respectively. As described in Section 2 of [4], this approach is absolutely necessary in order to understand and construct completely free elements. The latter topic is not considered in [9]. We should also mention that we have explicitly described the q^s-orders and the q-orders of the roots of unity η^j. This likewise is not done in [9], but is crucial in our approach, since this enabled us to prove the first part of Theorem 2.1, according to which we are able to explicitly give a free element in $\mathrm{GF}(q^{sr^n})$ over $\mathrm{GF}(q)$, provided we are given a free element in $\mathrm{GF}(q^s)$ over $\mathrm{GF}(q)$. Together with the property of the trace-function proved in Lemma 2.5, the second part of Theorem 2.1 is obtained as a corollary from its first part.

We finally consider an example.

EXAMPLE 2.6. Let r be an odd prime number which does not divide q. Assume that the multiplicative order of q modulo r is equal to $r - 1$ and that $\rho(q^{r-1})$, the largest integer N such that r^N divides $q^{r-1} - 1$, is equal to 1. Then (see, e.g., Theorem 2.8 in [4]) for every $n \geq 1$, the multiplicative order of q modulo r^n is equal to $r^{n-1}(r - 1)$.

Now, for $n \geq 0$, let η_n be a primitive r^{n+1}th root of unity.

By Theorem 3.3.2 of [5], the element η_0 generates a normal basis in $\mathrm{GF}(q^{r-1})$ over $\mathrm{GF}(q)$. Therefore, an application of the first part of Theorem 2.1 shows that $\sum_{j:=0}^{n} \eta_j$ generates a normal basis in $\mathrm{GF}(q^{(r-1)r^n})$ over $\mathrm{GF}(q)$.

Furthermore, the second part of Theorem 2.1 gives that $\alpha + \sum_{j:=1}^{n} T_j(\eta_j)$ generates a normal basis in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$, where α is any nonzero element in $\mathrm{GF}(q)$ and where T_j denotes the $\mathrm{GF}(q^{(r-1)r^j})$, $\mathrm{GF}(q^{r^j})$)-trace function.

3. Completely Free Elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$

In this section we modify the results obtained in Section 2 and construct completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$. Again, we assume that r is an odd prime number which does not divide q. As in Section 2, our construction is iterative and based on results from Section 2 of [4]. It can be summarized as follows:

If $n = 0$, then every nonzero element in $\mathrm{GF}(q)$ is completely free over $\mathrm{GF}(q)$. If $n \geq 1$, by induction hypothesis, we assume that we have an element w_{n-1} in $\mathrm{GF}(q^{r^{n-1}})$ which is completely free over $\mathrm{GF}(q)$. We then explicitly construct an element v_n in $\mathrm{GF}(q^{r^n})$ satisfying the property

$(\nabla_{n,r,q})$ the q^{r^j}-order of v_n is equal to $\Phi_{r^{n-j}}$ for every $j \in \{0, 1, \ldots, n-1\}$

(see Problem 2.6 in [4]). An application of Theorem 2.5 in [4] then gives that $w_n := w_{n-1} + v_n$ is completely free in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$.

Moreover, every element in $\mathrm{GF}(q^{r^n})$ which is completely free over $\mathrm{GF}(q)$ can be constructed in this way (see Theorem 2.4 in [4]).

The explict construction of an element v_n satisfying $(\nabla_{n,r,q})$ is an application of Theorem 2.7 in [4] in combination with the results obtained in Section 2 of the present paper:

First, let s again denote the multiplicative order of q modulo r and let $\rho(q^s)$ be the largest integer N such that r^N divides $q^s - 1$. Furthermore, for an integer $n \geq 1$, let again $a(n) := \min\{\rho(q^s), n\}$. By Theorem 2.8 in [4], the multiplicative order of q modulo r^n is equal to $sr^{n-a(n)}$.

Now, the first part of Theorem 2.7 in [4] says that v satisfies $(\nabla_{n,r,q})$ if and only if its q^{r^t}-order is equal to $\Phi_{r^{n-t}}$, where t is the integer part of $(n - a(n))/2$. We therefore only have to turn from $\mathrm{GF}(q)$ to $\mathrm{GF}(q^{r^t})$ as ground field and apply the results from Section 2 to the field extension $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q^{r^t})$. This is done in what follows.

Let $Q := q^{r^t}$ and let $N := n - t$. As r is relatively prime to s, the multiplicative order of Q modulo r is likewise equal to s. Furthermore, an application of Theorem 2.8 in [4] shows that

$$\rho(Q^s) = \rho(q^{sr^t}) = \rho(q^s) + t, \tag{3.1}$$

whence

$$\rho(Q^s) + N = \rho(q^s) + t + n - t = \rho(q^s) + n. \tag{3.2}$$

Therefore, let η again be a primitive $r^{n+\rho(q^s)}$th root of unity.

The main ingredient required to obtain completely free elements instead of ordinary free elements is that we now have to consider a complete set $J_{N,r,Q}$ of Q-orbit representatives of any complete set I of representatives of units modulo $r^{A(N)}$, where $A(N) := \min\{\rho(Q^s), N\}$. Then

$$\nu_n := \sum_{j \in J_{N,r,Q}} \eta^j$$

has Q-order $\Phi_{r^N}(x^s)$, i.e., q^{r^t}-order $\Phi_{r^{n-t}}(x^s)$. Furthermore, an application of Lemma 2.5 shows that the $(\mathrm{GF}(Q^{sr^N}), \mathrm{GF}(Q^{r^N}))$-trace of ν_n, i.e., the $(\mathrm{GF}(q^{sr^n}), \mathrm{GF}(q^{r^n}))$-trace of ν, has Q-order Φ_{r^N}, i.e., q^{r^t}-order $\Phi_{r^{n-t}}$ and thus satisfies $(\nabla_{n,r,q})$.

We finally mention that by the definition of t, an easy calculation shows that $A(n) = a(n) + t$. We therefore have proved the following result on completely free elements:

THEOREM 3.1. *Let q be a prime power and let r be an odd integer different from the characteristic of* $\mathrm{GF}(q)$. *Let s be the multiplicative order of q modulo r and let $\rho(q^s)$ be the largest integer N such that $q^s - 1$ is divisible by r^N. For an integer $n \geq 1$ let $a(n) := \min\{\rho(q^s), n\}$ and let T_n denote the $(\mathrm{GF}(q^{sr^n}), \mathrm{GF}(q^{r^n}))$-trace function. Let η be a primitive $r^{n+\rho(q^s)}$th root of unity, let t be the integer part of $(n - a(n))/2$, and let J be a complete set of representatives of q^{r^t}-orbits of units modulo $r^{a(n)+t}$.*

Then

$$v_n := \sum_{j \in J} T_n(\eta^j)$$

has q^{r^j}-order $\Phi_{r^{n-j}}$ for every $j \in \{0, 1, \ldots, n-1\}$.

Moreover, if w_{n-1} is any completely free element in $\mathrm{GF}(q^{r^{n-1}})$ *over* $\mathrm{GF}(q)$, *then*

$$w_n := w_{n-1} + v_n$$

is completely free in $\mathrm{GF}(q^{r^n})$ *over* $\mathrm{GF}(q)$.

We finally remark that similar to the discussion at the end of Section 2, any irreducible divisor of Φ_{r^N} occurs exactly once as Q-order for some $T_n(\eta^j)$ with $j \in J_{N,r,Q}$ (where N and Q are as above). Therefore, using induction on n, similarly as in Algorithm 3.7 in [4], one can explicitly describe *all* completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ in terms of a primitive $r^{n+\rho(q^s)}$th root of unity η.

References

1. D. Blessenohl and K. Johnson, Eine Verschärfung des Satzes von der Normalbasis, *J. Algebra* **103** (1986), 141–159.
2. J. V. Brawley and G. E. Schnibben, "Infinte Algebraic Extensions of Finite Fields," Contemporary Mathematics, Vol. 95, Am. Math. Soc., Providence, RI, 1989.
3. D. Hachenberger, On completely free elements in a finite field, *Designs, Codes and Cryptography* **4** (1994), 129–144.
4. D. Hachenberger, Explicit iterative constructions of normal bases and completely free elements, *Finite Fields Appl.* **2** (1996), 1–20.
5. D. Jungnickel, "Finite Fields. Structure and Arithmetic," Bibliographisches Institut, Mannheim, 1993.
6. R. Lidl and H. Niederreiter, "Finite Fields," Addison–Wesley, Reading, MA, 1983.
7. H. Lüneburg, "On the Rational Normal Form of Endomorphisms: A Primer to Constructive Algebra," Bibliographisches Institut, Mannheim, 1987.
8. H. Lüneburg, "Vorlesungen über Lineare Algebra," Bibliographisches Institut, Mannheim, 1993.
9. I. A. Semaev, Construction of polynomials irreducible over a finite field with linearly independent roots, *Math. USSR Sb.* **63** (1989), 507–519.