FINITE FIELDS AND THEIR APPLICATIONS **2**, 1–20 (1996)
ARTICLE NO. 0001

Explicit Iterative Constructions of Normal Bases and Completely Free Elements in 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 Scott Vanstone

Received February 23, 1994; revised October 18, 1994

A characterization of normal bases and complete normal bases in $GF(q^{r^n})$ over $GF(q)$, where $q > 1$ is any prime power, r is any prime number different from the characteristic of $GF(q)$, and $n \geq 1$ is any integer, leads to a general construction scheme of series $(v_n)_{n\geq 0}$ in $GF(q^{r^\infty}) := \bigcup_{n\geq 0} GF(q^{r^n})$ having the property that the partial sums $w_n := \sum_{i=0}^{n} v_i$ are free or completely free in $GF(q^{r^n})$ over $GF(q)$, depending on the choice of v_n.

In the case where r is an odd prime divisor of $q - 1$ or where $r = 2$ and $q \equiv 1 \bmod 4$, for any integer $n \geq 1$, all free and completely free elements in $GF(q^{r^n})$ over $GF(q)$ are explicitly determined in terms of certain roots of unity.

In the case where $r = 2$ and $q \equiv 3 \bmod 4$, for any $n \geq 1$, in terms of certain roots of unity, an explicit recursive construction for free and completely free elements in $GF(q^{2^n})$ over $GF(q)$ is given.

As an example, for a particular series of completely free elements the corresponding minimal polynomials are given explicitly.

1. NORMAL BASES AND COMPLETELY FREE ELEMENTS, AN OUTLINE

Let $q > 1$ be a prime power, $m > 1$ and integer, and let $GF(q)$ and $GF(q^m)$ denote the Galois fields of order q and q^m, respectively. Let $G^{(m,q)}$ be the Galois group of the field extension $GF(q^m)$ over $GF(q)$, i.e., the group of field automorphisms of $GF(q^m)$ fixing the field $GF(q)$ elementwise.

An element v in $GF(q^m)$ is called a *normal basis generator in* $GF(q^m)$ *over* $GF(q)$ or a *free element in* $GF(q^m)$ *over* $GF(q)$, provided that $\{g(v) \mid g \in G^{(m,q)}\}$, the set of $G^{(m,q)}$-*conjugates* of v, is a $GF(q)$-basis of $GF(q^m)$. Such a basis is called a *normal basis in* $GF(q^m)$ *over* $GF(q)$.

1071-5797/96 $12.00

In [2], among other things, Blessenohl and Johnsen have proved the remarkable theorem that for any pair (q, m), there exist elements in $\mathrm{GF}(q^m)$ which simultaneously are free over *every* intermediate field of the field extension $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$, i.e., elements v whose $G^{(m/d,q^d)}$-conjugates simultaneously build a $\mathrm{GF}(q^d)$-basis in $\mathrm{GF}(q^m)$ for *every* positive divisor d of m. Such elements are called *completely free in* $\mathrm{GF}(q^m)$ *over* $\mathrm{GF}(q)$. We therefore call the corresponding normal basis a *complete normal basis in* $\mathrm{GF}(q^m)$ *over* $\mathrm{GF}(q)$. The most difficult part of the proof is to settle the existence in the case where m is a prime power, say r^n. Once this is done, the general result follows from Theorem 1.1, a detailed proof of which is given in Hachenberger [5] (Theorem 3.1 and (3.1.3)).

THEOREM 1.1. *Let $m > 1$ be an integer and let $\prod_{i:=1}^{k} p_i^{a_i}$ be the prime power factorization of m. Let $q > 1$ be any prime power. If v_i is free in $\mathrm{GF}(q^{p_i^{a_i}})$ over $\mathrm{GF}(q)$ for $1 \le i \le k$, then $w := \prod_{i:=1}^{k} v_i$ is free in $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$. Moreover, if v_i is completely free in $\mathrm{GF}(q^{p_i^{a_i}})$ over $\mathrm{GF}(q)$ for $1 \le i \le k$, then w is completely free in $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$.*

In [5] we have given a constructive and more transparent proof of the difficult part of Blessenohl and Johnsen's theorem. This was done mainly by using basic properties of cyclotomic polynomials which occur as additive orders of the field elements; i.e., by means of these qualities we have considered the various decompositions of the additive group $(\mathrm{GF}(q^{r^n}), +)$ viewed as $\mathrm{GF}(q^{r^i})G^{(r^{n-i},q^{r^i})}$-module for any i in $\{0, \ldots, n-1\}$. Furthermore, we even were able to give a recursive formula for the number of completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$.

Here, we consider the problem to construct explicitly normal and complete normal bases in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ for any integer $n \ge 0$. For this reason, in Section 2, we briefly reexamine our results obtained in [5] and give a characterization of free and completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ under the assumption that r is a prime number different from the characteristic of $\mathrm{GF}(q)$. This characterization immediately leads to a general construction scheme of series $(v_n)_{n\ge 0}$ in the field $\mathrm{GF}(q^{r^\infty}) := \bigcup_{n\ge 0} \mathrm{GF}(q^{r^n})$ having the property that the partial sums $\sum_{i:=0}^{n} v_i$ are free or completely free in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$, depending on the choice of v_n.

The case where r is equal to the characteristic of $\mathrm{GF}(q)$ is essentially different but easy to handle: Let r be the characteristic of $\mathrm{GF}(q)$. In [12, Theorem 1], Perlis has characterized the free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ as exactly the elements whose $\mathrm{GF}(q)$-trace is nonzero. By the transitivity of the trace function, we therefore obtain that any such element is already completely free in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$.

In [12, Theorem 3] and Semaev [14, Section 4], one finds explicit constructions of free elements in such field extensions of $\mathrm{GF}(q)$.

In the present paper, after giving the general construction scheme mentioned above, we restrict our attention to the case where r is a prime divisor of $q - 1$. If $r = 2$, we have to consider the cases $q \equiv 1 \bmod 4$ and $q \equiv 3 \bmod 4$ separately.

In Section 3 the case where r is odd or where $r = 2$ and $q \equiv 1 \bmod 4$ is considered. This case is particularly simple since $\mathrm{GF}(q^{r^n})$ can easily be obtained by adjoining a suitable root of unity to the given ground field $\mathrm{GF}(q)$, a root whose minimal polynomial is a binomial. Furthermore, the complete factorizations of the r^nth cyclotomic polynomials, which play an important role in the explicit construction of the series $(v_n)_{n\geq 0}$, are easy to manage over any extension field of $\mathrm{GF}(q)$. In terms of the root of unity we explicitly determine all free and completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$.

In Section 4, we consider field extensions of degree 2^n over $\mathrm{GF}(q)$, where $q \equiv 3 \bmod 4$ and where $n \geq 1$ is any integer. There, we likewise give an explicit recursive construction of free and completely free elements.

The case where r is an arbitrary prime number different from the characteristic of $\mathrm{GF}(q)$ is more involved since there is no obvious construction for the extension fields $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ $(n \geq 1)$. We will therefore consider the general situation in a forthcoming paper [6], where, after discussing how the general case can be reduced to the special one studied here, we likewise give explicit constructions of free and completely free elements.

Several other authors also have considered the construction of normal bases generators in field extensions of prime power degree over $\mathrm{GF}(q)$. We have already mentioned the papers of Perlis [12] and Semaev [14]. Later, we will also discuss some of the work of Gao [4] and Scheerhorn [13]. However, the construction of completely free elements is not considered in these papers.[1] Of course, in order to construct complete normal bases, knowledge on ordinary free elements is required. We therefore state many of our results for both types of elements.

As we work with iterative constructions, as a wider background, we would like to draw the attention of the reader to the book of Brawley and Schnibben [3] and the paper of Lüneburg [11]. For the general algebraic background, the reader is refered to Jacobson [8]. Our standard references for the theory of finite fields are Jungnickel [9] and Lidl and Niederreiter [10]. All number theoretic results we use can be found in Berlekamp [1] and Ireland and Rosen [7].

[1] In Blake, Gao and Mullin [15] and Scheerhorn [16] there are given examples of polynomials whose roots are completely free (see also Examples 3.8 and 3.9). The author wants to thank Dr. Scheerhorn for kindly providing him with these references.

2. Module Structures and a General Construction Scheme for Free and Completely Free Elements

We start by recalling some important facts on the structure of the additive group of the extension fields considered. Although these results hold for arbitrary finite extensions, for our purposes, we concentrate on the case where the degree of extension is a prime power, say r^n.

Let $GF(q)$ be the given ground field, let $n \geq 1$ be an integer, and let $j \in \{0, 1, \ldots, n-1\}$. In order to simplify the notation, in contrast to Section 1, let $G^{(n,j)}$ denote the Galois group of $GF(q^{r^n})$ over $GF(q^{r^j})$. By naturally extending the action of $G^{(n,j)}$, it is seen that the additive group $(GF(q^{r^n}), +)$ is turned into a module over the group algebra $GF(q^{r^j})G^{(n,j)}$. Since $G^{(n,j)}$ is cyclic and has the *Frobenius automorphism*

$$\sigma^{(n,j)}: GF(q^{r^n}) \mapsto GF(q^{r^n}), \qquad v \mapsto v^{q^{r^j}},$$

as canonical generator, it is appropriate to describe the scalar multiplication in terms of the polynomial ring in the indeterminate x over the field $GF(q^{r^j})$, i.e., by

$$GF(q^{r^j})[x] \times GF(q^{r^n}) \mapsto GF(q^{r^n}), \qquad (g, v) \to g(\sigma^{(n,j)})(v).$$

Therefore, $(GF(q^{r^n}), +)$ is considered as a vector space over $GF(q^{r^j})$ together with the $GF(q^{r^j})$-linear mapping $\sigma^{(n,j)}$. This is the familiar situation studied in linear algebra. The existence of a normal basis in $GF(q^{r^n})$ over $GF(q^{r^j})$ just means that this vector space is a cyclic module. Its generators are exactly the free elements in $GF(q^{r^n})$ over $GF(q^{r^j})$.

The minimal polynomial of $\sigma^{(n,j)}$ is equal to $x^{r^{n-j}} - 1$. For any v in $GF(q^{r^n})$, the *q^{r^j}-order* of v is the monic polynomial g of least degree with coefficients in $GF(q^{r^j})$ such that v is annihilated by g, i.e., such that $g(\sigma^{(n,j)})(v) = 0$. Of course, g is a divisor of $x^{r^{n-j}} - 1$. Furthermore, v is free in $GF(q^{r^n})$ over $GF(q^{r^j})$, if and only if its q^{r^j}-order is equal to $x^{r^{n-j}} - 1$.

From now on, throughout this entire section, we assume that r is not a divisor of the characteristic of $GF(q)$. In Theorem 2.4 below, we give the fundamental characterization of free and completely free elements in $GF(q^{r^n})$ over $GF(q)$, which will immediately lead to the iterated construction scheme mentioned in Section 1. The detailed proof is given in [5] and therefore is omitted here. We just mention that it essentially relies on the following well-known basic three facts which will be required later.

Fact 2.1 (see [10, Section 2.4] or [9, Section 1.5]). For any j in $\{0, 1, \ldots, n-1\}$, the polynomial $x^{r^{n-j}} - 1$ is squarefree and, over the prime field of

$GF(q)$, decomposes into

$$(x^{r^{n-1-j}} - 1)\Phi_{r^{n-j}},$$

where $\Phi_{r^{n-j}}$ denotes the r^{n-j}th *cyclotomic polynomial,* i.e., the polynomial whose roots are exactly the primitive r^{n-j}th roots of unity.

Fact 2.2 (see Lemma 3.3 in [5]). If v and w are elements in $GF(q^{r^n})$ with relatively prime q^{r^j}-orders f and g, respectively, then $v + w$ has q^{r^j}-order fg.

Conversely, any element u with q^{r^j}-order fg can uniquely be written as $v + w$ with v and w having q^{r^j}-order f and g, respectively, provided that f and g are relatively prime.

Fact 2.3. The intermediate fields of $GF(q^{r^n})$ over $GF(q)$ are linearly ordered by inclusion.

In Fact 2.1, a factorization of the monic generator of the annihilator ideal of $(GF(q^{r^n}), +)$ viewed as a $GF(q^{r^j})G^{(n,j)}$-module is given. Fact 2.2 actually holds in a more general setting of modules over a principal ideal domain, see e.g., [8, Section 3.9]. Its content is that knowing the complete factorization of the polynomial $x^{r^{n-j}} - 1$ over $GF(q^{r^j})$ and a generator of each irreducible $GF(q^{r^j})G^{(n,j)}$-submodule of $(GF(q^{r^n}), +)$, which correspond bijectively to the irreducible $GF(q^{r^j})$-divisors of that polynomial, we obtain a free element by building the sum of all these generators. Moreover, any free element has this form. Fact 2.3 is straightforward, but crucial for proving the existence of completely free elements and for the iterative constructions we give.

THEOREM 2.4. *Let $v \in GF(q^{r^n})$, where r is a prime number different from the characteristic of $GF(q)$ and where $n \geq 1$ is any integer. Then there exist unique elements v_1 and v_2 in $GF(q^{r^n})$ such that $v = v_1 + v_2$ and the following conditions hold:*

(2.4.1) *For any $0 \leq j \leq n - 1$, the q^{r^j}-order of v_1 is a monic divisor of $x^{r^{n-j-1}} - 1$, while the q^{r^j}-order of v_2 is a monic divisor of $\Phi_{r^{n-j}}$.*

(2.4.2) *v is free in $GF(q^{r^n})$ over $GF(q^{r^j})$ for some $j \in \{0, \ldots, n-1\}$ if and only if v_1 has q^{r^j}-order $x^{r^{n-j-1}} - 1$, i.e., is free in $GF(q^{r^{n-1}})$ over $GF(q^{r^j})$, and v_2 has q^{r^j}-order $\Phi_{r^{n-j}}$.*

(2.4.3) *v is completely free in $GF(q^{r^n})$ over $GF(q)$ if and only if v_1 is completely free in $GF(q^{r^{n-1}})$ over $GF(q)$ and the q^{r^j}-order of v_2 is equal to $\Phi_{r^{n-j}}$ for all $j \in \{0, \ldots, n-1\}$.*

This characterization immediately leads to a recursive construction

scheme for free and completely free elements in field extensions of prime power degree.

THEOREM 2.5. *Let $q > 1$ be a prime power and let r be a prime number different from the characteristic of* $\mathrm{GF}(q)$.

(2.5.1) *Let v_0 be any nonzero element of* $\mathrm{GF}(q)$. *Then $w_0 := v_0$ is free and completely free in* $\mathrm{GF}(q)$ *over* $\mathrm{GF}(q)$.

(2.5.2) *Assume that w_n is free in* $\mathrm{GF}(q^{r^n})$ *over* $\mathrm{GF}(q)$ *and let* $v_{n+1} \in \mathrm{GF}(q^{r^{n+1}})$ *be an element of q-order $\Phi_{r^{n+1}}$. Then $w_{n+1} := w_n + v_{n+1}$ is free in* $\mathrm{GF}(q^{r^{n+1}})$ *over* $\mathrm{GF}(q)$. *Moreover, if w_n is completely free in* $\mathrm{GF}(q^{r^n})$ *over* $\mathrm{GF}(q)$, *then w_{n+1} is completely free in* $\mathrm{GF}(q^{r^{n+1}})$ *over* $\mathrm{GF}(q)$ *if and only if v_{n+1} has q^j-order $\Phi_{r^{n+1-j}}$ for all $0 \le j \le n$.*

So, we are able to iteratively find normal bases or complete normal bases in any finite subfield of $\mathrm{GF}(q^{r^\infty})$ over $\mathrm{GF}(q)$, if we can solve the following main problem.

Problem 2.6. For any integer $n \ge 1$, find elements in $\mathrm{GF}(q^{r^n})$ having q-order Φ_{r^n}, and find elements v_n in $\mathrm{GF}(q^{r^n})$ satisfying the property

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

In order to settle the existence of completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$, in [5], we had to study property $(\nabla_{n,r,q})$ of Problem 2.6. Fortunately, see Theorem 2.7 below, it turned out that in almost all cases the problem of finding an element in $\mathrm{GF}(q^{r^n})$ satisfying $(\nabla_{n,r,q})$ is the same as that of finding an element in $\mathrm{GF}(q^{r^n})$ having q^{r^t}-order $\Phi_{r^{n-t}}$ for a suitable t in $\{0, 1, \ldots, n-1\}$ depending only on r, n, and q. From our iterative point of view, this means that in most cases, the problem of finding a completely free element in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ essentially is not more difficult than finding a free element in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$.

Though the following theorem is an immediate consequence of the proof of Theorem 3.10 in [5], it is not explicitly stated there. In order to formulate it, we need some further notation:

For q, r, and n as above, let $\mathrm{ord}_{r^n}(q)$ be the *multiplicative order* of q *modulo* r^n, i.e., the least positive integer $N \ge 1$ such that $q^N - 1$ is divisible by r^n. From elementary number theory (see, e.g., Theorem 2 and Theorem 2′ in Chapter 4 of [7]), it is known that $\mathrm{ord}_{r^n}(q)$ is of the form sr^l, where s is a divisor of $r - 1$ and l is an integer satisfying $0 \le l \le n - 1$. As in [2], the case where $r = 2$, $\mathrm{ord}_{2^n}(q) = 2$, $n \ge 3$, and $q \not\equiv 5^{2^{n-3}} \bmod 2^n$ is called the *exceptional case.*

THEOREM 2.7. *Let $q > 1$ be a prime power, $n \geq 1$ an integer, and r a prime number different from the characteristic of* GF(q). Let $\mathrm{ord}_{r^n}(q) = sr^l$ *with $l \leq n - 1$ and s being a divisor of $r - 1$. Furthermore, let $v \in \mathrm{GF}(q^{r^n})$.*

(2.7.1) *Excluding the exceptional case, let $t := l/2$ if l is even and $t := (l - 1)/2$ if l is odd. Then v satisfies $(\nabla_{n,r,q})$ if and only if the q^{r^l}-order of v is equal to $\Phi_{r^{n-t}}$.*

(2.7.2) *Assuming the exceptional case, then v satisfies $(\nabla_{n,2,q})$ if and only if the q-order of v is equal to Φ_{2^n} and the q^2-order of v is equal to $\Phi_{2^{n-1}}$.*

As we have pointed out the importance of the cyclotomic polynomial Φ_{r^n} so far, it is worthwhile noting that for $n \geq 1$, with x as indeterminate,

$$\Phi_{r^n} = \Phi_r(x^{r^{n-1}}) = \sum_{j:=0}^{r-1} x^{jr^{n-1}}.$$

Thus, with σ being the Frobenius automorphism in $\mathrm{GF}(q^{r^\infty})$ over GF(q), we see that $\Phi_{r^n}(\sigma)$ restricted to $\mathrm{GF}(q^{r^n})$ is just the trace function onto $\mathrm{GF}(q^{r^{n-1}})$. If $(w_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ as in Theorem 2.5 are series which build free elements, then, since v_n lies in the kernel of $\Phi_{r^n}(\sigma)$, and w_{n-1} is an element of $\mathrm{GF}(q^{r^{n-1}})$, we obtain

$$\Phi_{r^n}(\sigma)(w_n) = r \cdot w_{n-1}.$$

Therefore, the series $(w_n/r^n)_{n\geq 0}$ naturally satisfies what is called *trace-compatible* in [13]. There, some examples of such series are given.

Before we turn to explicit constructions, we need the following result on the multiplicative order of q modulo r^n. This is essentially Theorem 6.52 in [1].

THEOREM 2.8. *Let $q > 1$ be a prime power, r a prime number which does not divide q and let $s := \mathrm{ord}_r(q)$ be the multiplicative order of q modulo r. Furthermore, let $\rho(q^s)$ be the largest positive integer $N \geq 1$ such that $q^s - 1$ is divisible by r^N. Then the following holds for the multiplicative order of q modulo r^n, where $n \geq 1$ is any integer:*

(2.8.1) *Assume that r is odd or that $r = 2$ and $q \equiv 1 \bmod 4$ (in which case $s = 1$). Then*

$$\mathrm{ord}_{r^n}(q) = \begin{cases} s, & \text{if } 1 \leq n \leq \rho(q^s), \\ sr^{n-\rho(q^s)}, & \text{if } n \geq \rho(q^s). \end{cases}$$

Furthermore, for any integer $t \geq 0$, $\rho(q^{sr^t}) = \rho(q^s) + t$.

(2.8.2) *Assume that* $r = 2$ *and that* $q \equiv 3 \bmod 4$. *Then* $s = 1$, $\rho(q) = 1$, *and*

$$\operatorname{ord}_{2^n}(q) = \begin{cases} 1, & \text{if} \quad n = 1, \\ 2, & \text{if } 2 \le n \le \rho(q^2), \\ 2^{n-\rho(q^2)+1}, & \text{if} \quad n \ge \rho(q^2). \end{cases}$$

Furthermore, for any integer $t \ge 0$, $\rho(q^{2^t}) = \rho(q^2) + t - 1$.

3. Explicit Constructions of Free and Completely Free Elements

In this section, again, for any integer $n \ge 1$, we consider the field extensions of degree r^n over a finite field $\mathrm{GF}(q)$. But we assume here that r is a prime divisor of $q - 1$. Due to Theorem 2.8, in the case where $r = 2$, we must handle the cases $q \equiv 1 \bmod 4$ and $q \equiv 3 \bmod 4$ separately. In this section, we therefore additionally assume that $q \equiv 1 \bmod 4$, if $r = 2$. The case where $q \equiv 3 \bmod 4$ is essentially different and is dealt with in Section 4.

As in Theorem 2.8, we define $\rho(q)$ to be the largest positive integer $N \ge 1$ such that $q - 1$ is divisible by r^N (observe that the parameter s is equal to 1 here).

Under these assumptions, for any $n \ge 1$, the field $\mathrm{GF}(q^{r^n})$ is easily obtained by adjoining a suitable root of unity to the ground field $\mathrm{GF}(q)$. A proof of the following lemma can be found in [9] (see Corollary 2.3.6).

Lemma 3.1. *Let* q *be a prime power,* r *a prime divisor of* $q - 1$ *and let* $\rho(q)$ *be defined as above. Assume that* $q \equiv 1 \bmod 4$ *in the case where* $r = 2$. *Furthermore, let* ζ *be a primitive* $r^{\rho(q)}$th *root of unity and let* $n \ge 0$ *be an integer.*

Then the polynomial $x^{r^n} - \zeta$ *is irreducible over* $\mathrm{GF}(q)$. *Any root* η *of this polynomial is a primitive* $r^{n+\rho(q)}$th *root of unity and* $\mathrm{GF}(q^{r^n})$ *is obtained by adjoining* η *to* $\mathrm{GF}(q)$.

Next, having Fact 2.1 and Fact 2.2 in mind, we explicitly describe the complete factorization of the r^nth cyclotomic polynomial over the field $\mathrm{GF}(q)$.

Lemma 3.2. *Let* q *be a prime power,* r *a prime divisor of* $q - 1$. *Assume that* $q \equiv 1 \bmod 4$, *if* $r = 2$. *Furthermore, let* ζ *be a primitive* $r^{\rho(q)}$th *root of unity. For a given integer* $n \ge 1$, *let* $a := \min\{n, \rho(q)\}$.

Then, over $\mathrm{GF}(q)$, *the complete factorization of the* r^nth *cyclotomic polynomial is given by*

$$\prod_{j:=1,\,\gcd(r,j)=1}^{r^a} (x^{r^{n-a}} - \zeta^{jr^{\rho(q)-a}}).$$

Proof. It is well known, see, e.g., [9, Theorem 1.5.4] or [10, Theorem 2.47], that the r^nth cyclotomic polynomial over GF(q) splits into the product of $r^{n-1}(r-1)/\mathrm{ord}_{r^n}(q) =: b$ irreducible polynomials of degree $\mathrm{ord}_{r^n}(q)$ each. As $\mathrm{ord}_{r^n}(q)$ by (2.8.1) is equal to r^{n-a} (observe that $s = 1$ by our general assumption), we obtian that $b = r^{a-1}(r-1)$. This coincides with the number of factors of the product above.

On the other hand, applying Lemma 3.1 to the case where $n \geq \rho(q)$, we know that the binomial $x^{r^{n-\rho(q)}} - \alpha$ is irreducible over GF(q), provided that α is a primitive $r^{\rho(q)}$th root of unity. Furthermore, all its roots are primitive r^nth roots of unity. Thus, this polynomial is a divisor of Φ_{r^n}. Since $\{\zeta^j | 1 \leq j \leq r^{\rho(q)}, \gcd(r, j) = 1\}$ is exactly the set of primitive $r^{\rho(q)}$th roots of unity and has cardinality $r^{\rho(q)-1}(r-1)$, we obtain that the above product is a divisor of Φ_{r^n}. Furthermore, since both polynomials are monic of the same degree, they must be equal.

If $n \leq \rho(q)$, then GF(q) contains the primitive r^nth roots of unity, whence Φ_{r^n} over GF(q) splits into linear factors. Now, since $\{\zeta^{jr^{\rho(q)-n}} | 1 \leq j \leq r^n, \gcd(r, j) = 1\}$ is exactly the set of primitive r^nth roots of unity, we similarly as above obtain the desired factorization. ∎

So far, we are able to give an explicit *polynomial presentation* (see [3]) of the field extension GF(q^{r^n}) by adjoining certain roots of unity to the field GF(q). In Corollary 3.4 we are going to describe a particular normal basis generator in GF(q^{r^n}) over GF(q) in terms of these roots while all free elements are characterized in Theorem 3.5 below. In fact, slightly weaker results may be derived from Lemma 2.1 and Theorem 2.2 in [14], where, more generally, degree-m-extensions of GF(q) are considered under the assumption that any odd prime divisor of m divides $q - 1$ and where $q \equiv 1 \bmod 4$, provided that m is even. However, in view of constructing completely free elements, in contrast to [14], we have to explicitly determine the q-order of each such root of unity. This is done in Theorem 3.3 and its proof, using the factorization of the r^nth cyclotomic polynomial given in Lemma 3.2.

THEOREM 3.3. *Let q be a prime power and let r be a prime divisor of $q - 1$. Assume that $q \equiv 1 \bmod 4$, if $r = 2$. Let $\rho(q)$ be the largest integer N such that $q - 1$ is divisible by r^N and for an integer $n \geq 1$, let $a := \min\{n, \rho(q)\}$. Furthermore, let η be a primitive $r^{n+\rho(q)}$th root of unity.*

Then the following hold:

(3.3.1) *For any integer t which is not divisible by r, the q-order of η^t is an irreducible divisor of the r^nth cyclotomic polynomial over* GF(q).

(3.3.2)

$$v_n := \sum_{j:=1,\ \gcd(j,r)=1}^{r^a} \eta^j$$

is an element in $\mathrm{GF}(q^{r^n})$ *having* q*-order* Φ_{r^n}.

Proof. As in the statement, let $a := \min\{\rho(q), n\}$, where $n \geq 1$ is some given integer. From Theorem 2.8, we know that

$$\rho(q^{r^{n-a}}) = \rho(q) + n - a = \max\{\rho(q), n\} =: A.$$

Hence, there exists an integer u which is not divisible by r and satisfying $1 + ur^A = q^{r^{n-a}} =: Q$. Now, let $\zeta := \eta^{r^n}$. Then ζ is a primitive $r^{\rho(q)}$th root of unity and thus an element of $\mathrm{GF}(q)$. If $j := u \bmod r^a$, then $1 \leq j \leq r^a$ and r does not divide j. Thus, using Theorem 3.2, we see that

$$x^{r^{n-a}} - \zeta^{jr^{\rho(q)-a}} =: f_\eta$$

is an irreducible divisor of Φ_{r^n} in $\mathrm{GF}(q)[x]$. Now, with σ being the Frobenius automorphism of $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$, we obtain

$$\begin{aligned} f_\eta(\sigma)(\eta) &= \sigma^{r^{n-a}}(\eta) - \zeta^{jr^{\rho(q)-a}}\eta = \eta^{q^{r^{n-a}}} - \zeta^{jr^{\rho(q)-a}}\eta \\ &= \eta^Q - \zeta^{jr^{\rho(q)-a}}\eta \qquad = \eta(\eta^{ur^A} - \zeta^{jr^{\rho(q)-a}}) \\ &= \eta(\zeta^{ur^{A-n}} - \zeta^{jr^{\rho(q)-a}}) = \eta(\zeta^{ur^{\rho(q)-a}} - \zeta^{jr^{\rho(q)-a}}) \\ &= 0. \end{aligned}$$

The last equation holds since the multiplicative order of $\zeta^{r^{\rho(q)-a}}$ is equal to r^a and since $j \equiv u \bmod r^a$ by definition of j.

Therefore, the q-order of η divides f_η. But since $\eta \neq 0$ and f_η is irreducible, we obtain that the q-order of η is equal to f_η.

Next, we are going to generalize the above argument. If t is any integer which is not divisible by r, then η^t likewise is a primitive $r^{\rho(q)+n}$th root of unity with the property that $\eta^{tr^n} = \zeta^t$ is a primitive $r^{\rho(q)}$th root of unity. With u as above, we define the mapping ι by $\iota(t) := ut \bmod r^a$. Doing a similar calculation as above, we obtain that the q-order of η^t is equal to

$$x^{r^{n-a}} - \zeta^{\iota(t)r^{\rho(q)-a}},$$

which by Theorem 3.2 is an irreducible divisor of Φ_{r^n} over $\mathrm{GF}(q)$. This completes the proof of (3.3.1).

In order to prove (3.3.2), we observe that the mapping ι used in the first part of the proof induces a bijection on the set of units modulo r^a. Thus, by Theorem 3.2, *every* irreducible divisor of Φ_{r^n} over GF(q) occurs exactly once as the q-order of some η^t, where $1 \le t \le r^a$ and r is not a divisor of t. Since all these polynomials are relatively prime and since their product by Theorem 3.2 is equal to Φ_{r^n}, applying Fact 2.2, we conclude that the element v_n in (3.3.2) indeed has q-order Φ_{r^n}. This completes the proof of Theorem 3.3. ■

By the results of Section 2, we may now explicitly construct a series $(v_n)_{n\ge 0}$ of elements in $\mathrm{GF}(q^{r^\infty}) := \bigcup_{n\ge 0} \mathrm{GF}(q^{r^n})$ with the property that $\sum_{j:=0}^{n} v_j$ is free in $\mathrm{GF}(q^{r^n})$ over GF(q).

COROLLARY 3.4. *Under the assumptions of Theorem* 3.3, *for* $n \ge 1$, *let* η_n *be a primitive* $r^{\rho(q)+n}$th *root of unity. Furthermore, let* $v_0 := 1$ *and*

$$v_n := \sum_{j:=1,\gcd(r,j)=1}^{r^{\min\{\rho(q),n\}}} \eta_n^j.$$

Then

$$w_n := \sum_{i:=0}^{n} v_i$$

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

At this stage, we are able to describe explicitly *all* free elements in $\mathrm{GF}(q^{r^n})$ over GF(q) in terms of a primitive $r^{n+\rho(q)}$th root of unity η.

THEOREM 3.5. *Let* q *be a prime power and let* r *be a prime divisor of* $q - 1$. *Assume that* $q \equiv 1 \bmod 4$, *if* $r = 2$. *Let* $\rho(q)$ *be the largest integer* N *such that* $q - 1$ *is divisible by* r^N *and let* η *be a primitive* $r^{\rho(q)+n}$th *root of unity, where* $n \ge 1$ *is an integer. Then the free elements in* $\mathrm{GF}(q^{r^n})$ *over* GF(q) *are exactly the elements of the form*

$$w_0 + \sum_{i:=1}^{n} \sum_{j:=1,\gcd(r,j)=1}^{r^{\min\{\rho(q),i\}}} f_{ij}(\sigma)(\eta^{jr^{n-i}}),$$

where w_0 *is any nonzero element of* GF(q), f_{ij} *is any nonzero polynomial over* GF(q) *of degree less than* $r^{i-\min\{\rho(q),i\}}$, *and* σ *denotes the Frobenius automorphism in* $\mathrm{GF}(q^{r^n})$ *over* GF(q).

Proof. Let $1 \le i \le n$ and let $1 \le j \le r^{\min\{\rho(q),i\}}$ with $\gcd(r, j) = 1$. Then $\eta^{jr^{n-i}}$ is a primitive $r^{\rho(q)+i}$th root of unity. By Theorem 3.3, its q-order is an

irreducible divisor of the r^ith cyclotomic polynomial, say g_{ij}. The degree of g_{ij} is equal to $\mathrm{ord}_{r^i}(q) = r^{i-\min\{\rho(q),i\}}$. Now, by the irreducibility of g_{ij}, the elements of q-order g_{ij} are exactly the nonzero elements of the irreducible $\mathrm{GF}(q)\mathrm{G}^{(n,0)}$-submodule of $(\mathrm{GF}(q^{r^n}), +)$ which is annihilated by g_{ij}. Therefore, the elements having q-order g_{ij} are exactly the elements of the form $f_{ij}(\sigma)(\eta_j^{r^{n-i}})$ where f_{ij} is a nonzero polynomial with coefficients in $\mathrm{GF}(q)$ and degree less than the degree of g_{ij}.

From Fact 2.2, it follows that any element of the above form is a generator of a normal basis in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$. On the other hand, likewise by Fact 2.2, any free element actually is a sum of elements whose q-orders are exactly the irreducible divisors of $x^{r^n} - 1$. This completes the proof. ■

For the remainder of this section, we turn to the construction of completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$. We have pointed out in Section 2 (see Problem 2.6 and Theorem 2.7) that, besides the exceptional case, this is not more difficult than constructing a free element, which we already are able to do. So, we first prove that the exceptional case does not hold under our general assumptions:

Assume that $r = 2$, $n \geq 3$ and $\mathrm{ord}_{2^n}(q) = 2$. Since the elements of order 2 in the group of units modulo 2^n by Theorem 2′ in Chapter 4 of [7] are $-1 + 2^nZ$, $5^{2^{n-3}} + 2^nZ$ and $-5^{2^{n-3}} + 2^nZ$ (where Z denotes the ring of integers), we have that $q + 2^nZ$ is equal to one of them. If the exceptional case would hold, then $q \not\equiv 5^{2^{n-3}} \bmod 2^n$, leaving the possibilities $q \equiv -1 \bmod 2^n$ and $q \equiv -5^{2^{n-3}} \bmod 2^n$. But both are contradictions to our assumption that $q \equiv 1 \bmod 4$. Therefore, indeed, the exceptional case does not hold here.

Now, applying Theorem 2.7 and Theorem 3.3, we can solve problem 2.6:

THEOREM 3.6. *Let q be a prime power, r a prime divisor of $q - 1$ and let $\rho(q)$ be the largest integer N such that $q - 1$ is divisible by r^N. Assume that $\rho(q) \geq 2$, if $r = 2$. Consider the field extension $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ for some integer $n \geq 1$ and let η be a primitive $r^{\rho(q)+n}$th root of unity.*

(3.6.1) *If $n \leq \rho(q)$, then*

$$v_n := \sum_{j:=1,\gcd(r,j)=1}^{r^n} \eta^j$$

is an element in $\mathrm{GF}(q^{r^n})$ satisfying $(\nabla_{n,r,q})$.

(3.6.2) *If $n \geq \rho(q)$, define t to be the integer part of $(n - \rho(q))/2$. Then*

$$v_n := \sum_{j:=1,\gcd(r,j)=1}^{r^{\rho(q)+t}} \eta^j$$

is an element in $\mathrm{GF}(q^{r^n})$ satisfying $(\nabla_{n,r,q})$.

Proof. If $n \leq \rho(q)$, then $\mathrm{ord}_{r^n}(q) = 1$ by the definition of $\rho(q)$. Thus, the parameter l in Theorem 2.7 is equal to 1 and, since we are not in the exceptional case, applying (2.7.1), we obtain the following:

The parameter t is equal to 0, and therefore an element v satisfies $(\nabla_{n,r,q})$ if and only if its q-order is equal to Φ_{r^n}. Since v_n by (3.2.2) has q-order Φ_{r^n}, the first part is proved.

In the second part, we have $n \geq \rho(q)$. Thus, by Theorem 2.8 and our assumption, the multiplicative order of q modulo r^n is equal to $r^{n-\rho(q)}$. Furthermore, the parameters l and t in the statement of Theorem 2.7 and (2.7.1) are equal to $n - \rho(q)$ and the integer part of $(n - \rho(q))/2$, respectively. By (2.7.1), an element v satisfies $(\nabla_{n,r,q})$ if and only if its q^{r^t}-order is equal to $\Phi_{r^{n-t}}$. We therefore have to consider the field extension $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q^{r^t})$ and apply Theorem 3.3 to this situation.

With $Q := q^{r^t}$ and $N := n - t$, by (2.8.1), we have $\rho(Q) = \rho(q) + t$ and therefore $N + \rho(Q) = n + \rho(q)$. Furthermore, a little calculation shows that $\min\{N, \rho(Q)\} = \rho(Q)$. Therefore, with η being a primitive $r^{N+\rho(Q)}$th root of unity, applying Theorem 3.3, we obtain that

$$\sum_{j:=1,\gcd(r,j)=1}^{r^{\rho(Q)}} \eta^j$$

is an element in $\mathrm{GF}(Q^{r^N}) = \mathrm{GF}(q^{r^n})$ having Q-order $\Phi_{r^N} = \Phi_{r^{n-t}}$. Since this element is equal to v_n in the statement of (3.6.2), the proof is complete. ∎

Similar to Corollary 3.4 and Theorem 3.5, we are now able to explicitly describe *all* completely free elements in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ for any $n \geq 1$ in terms of a primitive $r^{n+\rho(q)}$th root of unity. The details should now be clear and are left to the reader. Nevertheless, we summarize this iterative construction in the form of an algorithm producing a series $(w_n)_{n\geq 0}$ in $\mathrm{GF}(q^{r^\infty})$ such that w_n is completely free in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$ for any $n \geq 0$. Here, σ denotes the Frobenius automorphism of $\mathrm{GF}(q^{r^\infty})$ over $\mathrm{GF}(q)$.

ALGORITHM 3.7. Let q be a prime power and assume that the field $\mathrm{GF}(q)$ is given. Let r be a prime divisor of $q - 1$ and assume that $q \equiv 1 \bmod 4$ if $r = 2$. Let $\rho(q)$ be the largest integer N such that $q - 1$ is divisible by r^N and let $\zeta \in \mathrm{GF}(q)$ be a primitive $r^{\rho(q)}$th root of unity. Finally, let $(x_n)_{n\geq 1}$ be a series of indeterminates over $\mathrm{GF}(q)$.

Initialization. Choose any nonzero element w_0 in $\mathrm{GF}(q)$. Construct $\mathrm{GF}(q^r)$ as $\mathrm{GF}(q)[x_1]/(x_1^r - \zeta)\mathrm{GF}(q)[x_1]$.

Induction step. Let $n \geq 1$, suppose that w_{n-1} is completely free in $\mathrm{GF}(q^{r^{n-1}})$ over $\mathrm{GF}(q)$, and let $\mathrm{GF}(q^{r^n})$ be given.

If $n \leq \rho(q)$, let

$$v_n := \sum_{j:=1,\gcd(r,j)=1}^{r^n} \lambda_j x_n^j,$$

where λ_j is any nonzero element in GF(q) for all j.

If $n \geq \rho(q)$, let t be the integer part of $(n - \rho(q))/2$ and let

$$v_n := \sum_{j:=1,\gcd(r,j)=1}^{r^{\rho(q)+t}} f_j(\sigma^r)(x_n^j),$$

where f_j is any nonzero polynomial with coefficients in GF(q^r) and degree less than $r^{n-\rho(q)-2t}$.

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

Construct GF($q^{r^{n+1}}$) as

$$\mathrm{GF}(q^{r^n})[x_{n+1}]/(x_{n+1}^r - x_n)\mathrm{GF}(q^{r^n})[x_{n+1}].$$

We close this section with two examples in order to demonstrate how Theorem 3.5 and Theorem 3.6 can be used to check that a given series of elements in GF(q^{r^∞}) is a series of free or completely free elements.

EXAMPLE 3.8. Under the assumptions of this section, using the same notation as above, let $n \geq 1$ be an integer and let η be a primitive $r^{n+\rho(q)}$th root of unity. An application of Theorem 3.4.1 in [4] (which is proved by using the results of Semaev mentioned before Theorem 3.3) shows that $(1 - \eta)^{-1}$ is free in GF(q^{r^n}) over GF(q). We are going to show that this element indeed is completely free (see also [15]).

Let $\zeta := \eta^{r^n}$. Then ζ is a primitive $r^{\rho(q)}$th root of unity lying in GF(q). Hence, $(1 - \eta)^{-1}$ is completely free, if and only if

$$(1 - \zeta)(1 - \eta)^{-1} = \sum_{j:=0}^{r^n-1} \eta^j$$

is completely free in GF(q^{r^n}) over GF(q). Now, all we must do is show that

$$\gamma_k := \sum_{j:=1,\gcd(r,j)=1}^{r^k} \eta^{jr^{n-k}}$$

is an element satisfying ($\nabla_{k,r,q}$) for all $k \in \{1, \ldots, n\}$. For simplicity, let us concentrate only on the case where $k = n$.

If $\rho(q) \geq n$, then γ_n is equal to v_n in (3.6.1) and we are ready. Assume therefore that $\rho(q) < n$. Let t be the integer part of $(n - \rho(q))/2$, let $Q := q^r$, $N := n - t$, and consider the field extension $\mathrm{GF}(Q^{r^N})$ over $\mathrm{GF}(Q)$. Since, by (2.8.1), $\rho(Q^{r^{N-\rho(Q)}}) = \rho(Q) + N - \rho(Q) = N$, there exists an integer U which is not divisible by r such that $Q^{r^{N-\rho(Q)}} = 1 + U r^N$. As in the proof of Theorem 3.3, for any integer $T \geq 0$ which is not divisible by r, the Q-order of η^T can be derived from the mapping ι which is defined by $\iota(T) := UT \bmod r^{\rho(Q)}$ and induces a bijection on the set of units modulo $r^{\rho(Q)}$.

Thus, for $1 \leq T \leq r^{\rho(Q)}$, not divisible by r, the set

$$\Gamma(T) := \{T + jr^{\rho(Q)} | 0 \leq j \leq r^{n-\rho(Q)} - 1\}$$

is exactly the subset of $\{1 \leq j \leq r^n | \gcd(r, j) = 1\}$, which under ι is mapped to $\iota(T)$. Therefore,

$$\delta_T := \sum_{j \in \Gamma(T)} \eta^j$$

is a member of the irreducible $\mathrm{GF}(Q)\mathrm{G}^{(n,t)}$-submodule of $(\mathrm{GF}(Q^N), +)$ which is annihilated by the Q-order of η^T. Since this polynomial is irreducible over $\mathrm{GF}(Q)$, we see that either δ_T has the same Q-order as η^T or $\delta_T = 0$. Now, $\delta_T = \eta^T f(\alpha)$, where $\alpha := \eta^{r^{\rho(Q)}}$ is a primitive r^{n-t}th root of unity and f denotes the polynomial $(x^{r^{n-\rho(Q)}} - 1)(x - 1)^{-1}$. Since $\rho(q) \geq 1$, we have $n - \rho(Q) = n - \rho(q) - t < n - t$. Thus, $\Phi_{r^{n-t}}$, where α is a root of, is relatively prime to f. We conclude that δ_T is not equal to 0.

As this holds for all T, we obtain that

$$\gamma_n = \sum_{T:=1, \gcd(T,r)=1}^{r^{\rho(Q)}} \delta_T$$

has Q-order Φ_{r^N} and therefore satisfies $(\nabla_{n,r,q})$.

We finally mention (see [4]) that the minimal polynomial of $(1 - \eta)^{-1}$ up to a $\mathrm{GF}(q)$-scalar is equal to

$$\zeta x^{r^n} - (x - 1)^{r^n}.$$

EXAMPLE 3.9. This is a generalization of Example 3.8. Under the assumptions of this section, again, let η be a primitive $r^{n+\rho(q)}$th root of unity. Furthermore, let a be any nonzero element of $\mathrm{GF}(q)$. It is shown in [13] that $(\eta - a)^{-1}$ is a normal basis generator in $\mathrm{GF}(q^{r^n})$ over $\mathrm{GF}(q)$.

But, since

$$(\eta - a)^{-1} = \alpha \sum_{j:=0}^{r^n-1} \left(\frac{\eta}{a}\right)^j$$

for a suitable nonzero element α in GF(q), proceeding similarly as in Example 3.8, one can even show that this element is completely free (see also [16]). We leave the details to the reader.

We finally remark that the theory developed in Sections 2 and 3 gives a satisfactory answer to the question posed in [13, p. 116], where the author asks for the existence of trace-compatible series (other than those considered in Example 3.9) which are built up from roots of unity.

4. The Case $q \equiv 3 \bmod 4$ and $r = 2$

In this section, for any integer $n \geq 1$, we give an explicit recursive construction of free and completely free elements in GF(q^{2^n}) over GF(q) provided that $q \equiv 3 \bmod 4$ by solving Problem 2.6 for that instance.

Assume first that $n = 1$. The field GF(q^2) is obtained by adjoining a primitive 4th root of unity, say λ, to the field GF(q). Since $x^2 + 1$ is the minimal polynomial of λ and since $q \equiv 3 \bmod 4$, we obtain

$$\lambda^q + \lambda = \lambda^3 + \lambda = \lambda(\lambda^2 + 1) = 0.$$

Therefore, the q-order of λ is equal to $x + 1$. Hence, using Fact 2.2 and observing that the nonzero elements of GF(q) are exactly the elements of q-order $x - 1$, we see that the free (and completely free) elements in GF(q^2) over GF(q) are exactly the elements of the form

$$\alpha + \beta\lambda,$$

where α and β are any nonzero elements of GF(q).

From now on, we assume that $n \geq 2$. As $q \equiv 3 \bmod 4$, we have $q^2 \equiv 1$ modulo 8 and therefore, considering GF(q^{2^n}) as extension of degree 2^{n-1} over GF(q^2), we may apply the results from Section 3; i.e., we may construct all free and all completely free elements in GF(q^{2^n}) over GF(q^2) for any integer $n \geq 2$. So here it remains to study whether the normality is lost by reducing the ground field from GF(q^2) to GF(q). By doing so, we also have to consider the exceptional case, i.e., the case where $r = 2$, $\mathrm{ord}_{2^n}(q) = 2$, $n \geq 3$, and $q \not\equiv 5^{2^{n-3}} \bmod 2^n$. This case is separated from all others by the following lemma.

LEMMA 4.1. *Let $q \equiv 3 \bmod 4$ be a prime power and let $n \geq 2$ be an integer. Then exactly one of the following cases holds:*

(4.1.1) $\operatorname{ord}_{2^n}(q) = 2 \cdot \operatorname{ord}_{2^{n-1}}(q)$,

(4.1.2) *the exceptional case.*

Proof. If $n = 2$, the exceptional case does not hold, but we have

$$\operatorname{ord}_4(q) = 2 = 2 \cdot \operatorname{ord}_2(q);$$

hence (4.1.1).

From now on, we assume that $n \geq 3$. Let $\rho(q^2)$ be the largest integer N such that $q^2 - 1$ is divisible by 2^N.

If $n = \rho(q^2) + 1$, by (2.8.2) we have

$$\operatorname{ord}_{2^n}(q) = 2^{n-\rho(q^2)+1} = 4 = 2 \cdot \operatorname{ord}_{2^{n-1}}(q).$$

Therefore (4.1.1) holds, but not (4.1.2).

If $n > \rho(q^2) + 1$, by (2.8.2) we obtain

$$\operatorname{ord}_{2^n}(q) = 2^{n-\rho(q^2)+1} = 2 \cdot 2^{n-1-\rho(q^2)+1} = 2 \cdot \operatorname{ord}_{2^{n-1}}(q).$$

Again, (4.1.1) holds, but (4.1.2) does not.

If $n \leq \rho(q^2)$, then $\operatorname{ord}_{2^n}(q) = 2 = \operatorname{ord}_{2^{n-1}}(q)$, whence (4.1.1) is not satisfied. Furthermore, $q \not\equiv 1 \bmod 4$ implies $q \not\equiv 5^{2^{n-3}} \bmod 2^n$. This is the exceptional case and therefore everything is proved. ∎

In the following, we handle these two cases separately. The next theorem says that Problem 2.6 can already be solved in the field extension $\mathrm{GF}(q^{2^n})$ over $\mathrm{GF}(q^2)$, where the assumptions of Section 3 are satisfied, provided that $\operatorname{ord}_{2^n}(q) = 2 \cdot \operatorname{ord}_{2^{n-1}}(q)$.

THEOREM 4.2. *Let $q \equiv 3 \bmod 4$ be a prime power and let $n \geq 2$ be an integer. Assume that $\operatorname{ord}_{2^n}(q) = 2 \cdot \operatorname{ord}_{2^{n-1}}(q)$. Then the following hold:*

(4.2.1) *If $v \in \mathrm{GF}(q^{2^n})$ has q^2-order $\Phi_{2^{n-1}}$, then v has q-order Φ_{2^n}.*

(4.2.2) *$v \in \mathrm{GF}(q^{2^n})$ satisfies $(\nabla_{n,2,q})$ if and only if it satisfies $(\nabla_{n-1,2,q^2})$.*

Proof. The proof is a direct consequence of Theorem 3.6 in [5]. We therefore will only roughly describe how the assumption is used.

Let g be any irreducible divisor of $\Phi_{2^{n-1}}$ over $\mathrm{GF}(q)$. The assumption assures that $g(x^2)$ is an irreducible divisor of Φ_{2^n} over $\mathrm{GF}(q)$. Now, if w_g is any element of q^2-order g, then the q-order of w_g is a divisor of $g(x^2)$.

Since w_g is not equal to 0 and since $g(x^2)$ is irreducible, we obtain that w_g has q-order $g(x^2)$. Now (4.2.1) follows from Fact 2.2 since any element v in $\mathrm{GF}(q^{2^n})$ of q^2-order $\Phi_{2^{n-1}}$ can uniquely be written as $\sum w_g$, where the sum runs over all irreducible divisors g of $\Phi_{2^{n-1}}$ with coefficients in $\mathrm{GF}(q)$ and where w_g has q^2-order g for any such g.

Remembering the definition of $(\nabla_{n,2,q})$ in Problem 2.6, we see that (4.2.2) is an application of (4.2.1). ■

We finally turn to the exceptional case and solve Problem 2.6 for this instance by explicitly presenting an element v in $\mathrm{GF}(q^{2^n})$ satisfying $(\nabla_{n,2,q})$.

THEOREM 4.3. *Let $q \equiv 3 \bmod 4$ be a prime power and let $n \geq 3$ be an integer. Assume that $\mathrm{ord}_{2^n}(q) = 2$ and that $q \not\equiv 5^{2^{n-3}} \bmod 2^n$. Let $\rho(q^2)$ be the largest integer N such that $q^2 - 1$ is divisible by 2^N. Furthermore, let η be a primitive $2^{n-1+\rho(q^2)}$th root of unity. Then*

$$v := \sum_{j:=1,\gcd(2,j)=1}^{2^{n-2}} (\eta^j + \eta^{jq})$$

is an element in $\mathrm{GF}(q^{2^n})$ satisfying $(\nabla_{n,2,q})$.

Proof. By (2.7.2) we know that v satisfies $(\nabla_{n,2,q})$ if and only if v has q-order Φ_{2^n} and q^2-order $\Phi_{2^{n-1}}$. Having Fact 2.2 in mind, we therefore consider the decompositions of $\Phi_{2^{n-1}}$ over $\mathrm{GF}(q^2)$ and Φ_{2^n} over $\mathrm{GF}(q)$.

Let ζ be a primitive 2^{n-1}th root of unity. Then $\mathrm{GF}(q^2) = \mathrm{GF}(q)(\zeta)$ and therefore $\Phi_{2^{n-1}}$ over $\mathrm{GF}(q^2)$ splits into linear factors while all irreducible $\mathrm{GF}(q)$-factors of $\Phi_{2^{n-1}}$ have degree 2. Now

$$(x - \zeta)(x - \zeta^q) = x^2 - (\zeta + \zeta^{-1})x + 1 =: f_\zeta$$

is an irreducible divisor of $\Phi_{2^{n-1}}$ over $\mathrm{GF}(q)$ (observe that under our assumption, $q + 1$ is divisible by 2^{n-1}). Furthermore, $f_\zeta(x^2)$ is a $\mathrm{GF}(q)$-divisor of Φ_{2^n} which over $\mathrm{GF}(q)$ decomposes into two irreducible factors. Thus, it can easily be deduced that

$$\Phi_{2^{n-1}} = \sum_{j:=1,\gcd(2,j)=1}^{2^{n-2}} (x - \zeta^i)(x - \zeta^{-i}),$$

while

$$\Phi_{2^n} = \sum_{j:=1,\gcd(2,j)=1}^{2^{n-2}} f_{\zeta^i}(x^2).$$

Now, let η be a primitive $2^{n-1+\rho(q^2)}$th root of unity. Then $\mathrm{GF}(q^2)(\eta) = \mathrm{GF}(q^{2^n})$ and furthermore, by Theorem 3.3, the q^2-order of η is equal to an irreducible divisor of $\Phi_{2^{n-1}}$ over $\mathrm{GF}(q^2)$. Without loss of generality, we assume that η has q^2-order $x - \zeta$, whence for any odd integer t the q^2-order of η^t is equal to $x - \zeta^t$. Since $x - \zeta$ is a divisor of f_ζ, it follows that the q-order of η is a divisor of $f_\zeta(x^2)$. In the proof of Theorem 3.9 in [5], without using the explicit factorization of $f_\zeta(x^2)$ over $\mathrm{GF}(q)$, we have shown that the q-order of η indeed is equal to $f_\zeta(x^2)$.

Now, consider the element $\eta + \eta^q$. With σ being the Frobenius automorphism in $\mathrm{GF}(q^{2^n})$ over $\mathrm{GF}(q)$, we have $\eta + \eta^q = ((x+1)(\sigma))(\eta)$. As $n \geq 3$, the polynomial $x + 1$ is relatively prime to $f_\zeta(x^2)$ and therefore, the q-order of $\eta + \eta^q$ likewise is equal to $f_\zeta(x^2)$. Furthermore, by Fact 2.2, the q^2-order of $\eta + \eta^q$ is equal to $(x - \zeta)(x - \zeta^{-1}) = f_\zeta$, as η^q has q^2-order $x - \zeta^q = x - \zeta^{-1}$.

If we repeat this argument for all divisors in the above factorizations of $\Phi_{2^{n-1}}$ and Φ_{2^n}, using once more Fact 2.2, we see that the element v in the statement has q-order Φ_{2^n} and q^2-order $\Phi_{2^{n-1}}$ and therefore satisfies $(\nabla_{n,2,q})$. This completes the proof of the theorem. ■

Using Theorem 2.5 and Theorem 2.7, we have reached our goal to recursively construct completely free elements and therefore, in particular, free elements in $\mathrm{GF}(q^{2^n})$ over $\mathrm{GF}(q)$, where n is any integer and $q \equiv 3 \bmod 4$. Due to the nature of the exceptional case, up until now we have not described all completely free elements. This would require a deeper analysis of the factorization of the 2^nth cyclotomic polynomial over $\mathrm{GF}(q)$.

However, in the context of the description of the corresponding modules, the complete $\mathrm{GF}(q)$-factorization of $x^{2^n} - 1$ is given in [14, Lemma 3.1] (see also [4, Section 3.3.3]). Indeed, using the results from [14, Section 3], it is possible to describe all completely free elements in $\mathrm{GF}(q^{2^n})$ over $\mathrm{GF}(q)$ in terms of a primitive $2^{n-1+\rho(q^2)}$th root of unity. But this should be worked out in a separate paper.

ACKNOWLEDGMENT

The author thanks Professor Dr. Dieter Jungnickel for his helpful comments and the careful reading of the manuscript.

REFERENCES

1. E. R. Berlekamp, "Algebraic Coding Theory," revised edition, Aegean Park Press, Laguna Hills, CA, 1984.

2. D. Blessenohl and K. Johnsen, Eine Verschärfung des Satzes von der Normalbasis, *J. Algebra* **103** (1986), 141–159.
3. J. V. Brawley and G. E. Schnibben, "Infinite Algebraic Extensions of Finite Fields," Contemporary Mathematics, Vol. 95, Am. Math. Soc., Providence, RI, 1989.
4. S. Gao, "Normal Bases over Finite Fields," Ph.D. thesis, Department of Combinatorics and Optimization, University of Waterloo, Ontario, Canada, 1993.
5. D. Hachenberger, On completely free elements in a finite field, *Designs, Codes and Cryptography* **4** (1994), 129–144.
6. D. Hachenberger, Normal bases and completely free elements in prime power extensions over finite fields, *Finite Fields Appl.* **2** (1996), 21–34.
7. K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," Springer, New York, 1982.
8. N. Jacobson, "Basic Algebra, I," 2nd ed., Freeman, New York, 1985.
9. D. Jungnickel, "Finite Fields: Structure and Arithmetic," BI Wissenschaftsverlag, Mannheim, 1993.
10. R. Lidl and H. Niederreiter, "Finite Fields," Addison–Wesley, Reading, MA, 1983.
11. H. Lüneburg, Effektive Konstruktion der algebraischen Erweiterungen von GF(p) sowie der vollständigen Kreisteilungskörper, preprint 65 (1983), Universität Kaiserslautern, Fachbereich Mathematik.
12. S. Perlis, Normal bases of cyclic fields of prime power degree, *Duke Math. J.* **9** (1942), 507–517.
13. A. Scheerhorn, "Darstellungen des algebraischen Abschlusses endlicher Körper und spurkompatible Polynomfolgen," Dissertation, Technische Fakultät der Universität Erlangen-Nürnberg, Erlangen, 1992.
14. I. A. Semaev, Construction of polynomials irreducible over a finite field with linearly independent roots, *Math. USSR Sb.* **63** (1989), 507–519.
15. I. F. Blake, S. Gao, and R. C. Mullin, Specific irreducible polynomials with linearly independent roots over finite fields, *Linear Algebra Appl.*, submitted.
16. A. Scheerhorn, "Dickson polynomials and completely normal elements over finite fields," *IMA Conference Proceedings Series, Oxford Univ. Press,* London, in press.