Finite Fields and Their Applications 18 (2012) 458–472

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Construction of self-dual normal bases and their complexity

François Arnault [a], Erik Jarl Pickett [b,*,1], Stéphane Vinatier [a]

[a] XLIM UMR 6172 CNRS – Université de Limoges, 123 avenue Albert Thomas, 87060 Limoges cedex, France
[b] Mathématiques, École Polytechnique Fédérale de Lausanne, 1015 Lausanne, Switzerland

ARTICLE INFO

Article history:
Received 27 July 2010
Revised 5 September 2011
Accepted 24 October 2011
Available online 12 November 2011
Communicated by S. Gao

MSC:
11T30
11T71
11T23
11T24

Keywords:
Finite field extensions
Self-dual normal basis
Complexity
Orthogonal circulant group

ABSTRACT

Recent work of Pickett has given a construction of self-dual normal bases for extensions of finite fields, whenever they exist. In this article we present these results in an explicit and constructive manner and apply them, through computer search, to identify the lowest complexity of self-dual normal bases for extensions of low degree. Comparisons to similar searches amongst normal bases show that the lowest complexity is often achieved from a self-dual normal basis.

0. Introduction

Let q be a power of a prime, n an integer, and let $\mathbb{F}_q$ be the field of q elements. The Galois group G of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a cyclic group, generated by the Frobenius automorphism $\phi : x \mapsto x^q$.

A basis for $\mathbb{F}_{q^n}/\mathbb{F}_q$ consisting of the orbit $(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$ of a single element α under the action of the Frobenius is known as a normal basis. We call it the *normal basis generated by* α (note that in this paper we consider the basis generated by any other conjugate of α to be different, as its elements

* Corresponding author.
E-mail addresses: francois.arnault@unilim.fr (F. Arnault), erikjarl.pickett@epfl.ch (E.J. Pickett), stephane.vinatier@unilim.fr (S. Vinatier).

[1] Part of this work was completed when the author was visiting the University of Limoges, funded by the London Mathematical Society Cecil King Travel Scholarship.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.10.002

are in a different order). Using such a basis, both exponentiation by q and computation of traces are straightforward operations; the former being simply a cyclic shift of coordinates. The difficulty of multiplying two elements written as linear combinations of the conjugates of α is measured by the so-called *complexity* of α, defined as the number of non-zero entries in the multiplication-by-α matrix [19, §4.1]. It has been shown in [20] to be at least $2n-1$, in which case the basis is called *optimal*, but this occurs only for very special values of n [9].

The search for normal bases with low complexity has taken two complementary directions. On the theoretical side, several authors have attempted to build them either from roots of unity in larger extensions, using Gauss periods [1,6,9,15] or traces of optimal normal bases [5,6], again with some limitations on the degree; or from the extension itself, using division points of a torus [3,8] or of an elliptic curve [7]. In the latter case the authors show that fast arithmetic can be implemented using their bases, as was also shown to be the case for normal bases generated by Gauss periods in [10].

More precisely, the normal basis generated by α is said to be self-dual if $\mathrm{Tr}(\alpha^{q^i}\alpha^{q^j}) = \delta_{i,j}$ for $0 \leqslant i, j \leqslant n-1$, where Tr is the trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ and δ is the Kronecker delta. Its complexity is the number of non-zero entries in the matrix:

$$\left(\mathrm{Tr}\left(\alpha\alpha^{q^i}\alpha^{q^j}\right)\right)_{0\leqslant i,j\leqslant n-1}.$$

Self-dual normal bases are useful for arithmetic and Fourier transform, and have applications in coding theory and cryptography. Contrary to normal bases, not all extensions of finite fields admit self-dual normal bases, but the existence conditions, recalled in Theorem 1 below, are mild. The theoretical techniques used to construct normal bases with low complexity sometimes yield self-dual normal bases, see for example [8, §5.4] or [3, §5], [10, Corollary 3.5], [5, Theorem 5], [21].

On the experimental side, exhaustive searches of all normal bases of a given extension have been carried out. Mullin, Onyszchuk, Vanstone and Wilson [20] have given a first list of lowest complexities in degree less than 30 over $\mathbb{F}_2$. This list was extended up to degree 33 by Geiselmann [11, Table 5.1]. In odd characteristic, Blake, Gao and Mullin [3] computed the lowest complexities of normal bases for a handful of small degree extensions. Recently, Masuda, Moura, Panario and Thomson [18] have reached degree 39 over $\mathbb{F}_2$ and given appealing statistics and conjectures about the distribution of complexities. It is clear that the cost of the exhaustive enumeration of the elements of $\mathbb{F}_{2^n}$ used to look for normal basis generators is a severe limitation to their method when the degree grows. On the other hand, their Table 4 shows that the minimal complexity for normal bases is very often reached by so-called self-dual bases (in all degrees not divisible by 4 up to 35 apart from 7, 10, 21). Restricting to self-dual normal bases enables one to push computations further; Geiselmann [11] was indeed able to compute the lowest complexity for self-dual normal bases over $\mathbb{F}_2$ up to degree 47. Comparing his results and [18, Table 5], we see that the best found complexity for normal bases in degree over 40, obtained by theoretical constructions or random search, is also reached by a self-dual normal basis for odd degrees up to 47.

In this paper we focus on the experimental side and give the lowest complexity of self-dual normal bases in various characteristics and degrees. At present, the only known strategy to reach this goal is to compute the complexity of all the self-dual normal bases of the extension (unless it admits an optimal self-dual normal basis, which is easily predictable, see [10, §3] or [16, Theorem 2] for a compact statement). In order to do so, we first construct a self-dual normal basis for the extension, then act on it by the *orthogonal circulant* group, namely the group of change of self-dual normal basis matrices. This group has been extensively studied, with accurate descriptions being given in [4,12,17]. Its size is in $O(q^{n/2})$ (see Remark 2.5 below), roughly the square root of the number of normal bases in view of [19, Corollary 4.14]. It follows that exhaustive enumeration of self-dual normal bases is easier than that of normal bases. We shall restrict ourselves to extensions $\mathbb{F}_{q^n}/\mathbb{F}_q$ which are either *semi-simple* (the degree n prime to the characteristic p) or *ramified* (n a power of p), the description of the orthogonal circulant group in the "mixed" case being a bit more elaborate.

We now describe our work more precisely. First we recall the necessary and sufficient conditions for the existence of self-dual normal bases [14].

Theorem 1 *(Lempel–Weinberger). The extension field $\mathbb{F}_{q^n}/\mathbb{F}_q$ has a self-dual normal basis if and only if either the degree n is odd, or $n \equiv 2$ modulo 4 and q is even.*

The existence proof in [14] is constructive in the sense that, given a normal basis for the extension, it describes a procedure to transform it into a self-dual normal basis. Wang [25] proposed another transformation procedure when $q = 2$ and n is odd, involving solving a system of equations. Poli [23] extended Wang's method to deal with the general characteristic 2 case. Recently, Pickett [22] designed a construction that extends the former ones to the odd characteristic case, dealing separately with the semi-simple case and the ramified case.

The construction of a normal basis for a given extension is well known and widely implemented. Therefore, the methods described above enable one to construct a self-dual normal basis under the existence conditions of Theorem 1. To our knowledge, this has not been implemented before, except in the restrictive case in which Wang's method applies. In this paper we apply Pickett's construction to compute a self-dual normal basis of a given extension whenever it exists. Note that for this first goal, the method in [14] is simpler and faster, but most of the computations involved in Pickett's construction must be implemented if one wants to compute the action of the orthogonal circulant group as well.

The criterion used in [25] to determine which changes of basis are appropriate has been generalised to any characteristic and degree, see [11, Lemma 5.5.3], where it is expressed in terms of circulant matrices. Here we restate it in terms of the group algebra $\mathbb{F}_q[G]$ as in [22]. Conjugation $u \mapsto \overline{u}$ in $\mathbb{F}_q[G]$ is the $\mathbb{F}_q$-algebra automorphism obtained from $g \mapsto g^{-1}$ for all $g \in G$; if $u = \sum_{k=0}^{n-1} u_k \phi^k \in \mathbb{F}_q[G]$ and $\alpha \in \mathbb{F}_{q^n}$, we put $u \circ \alpha = \sum_{k=0}^{n-1} u_k \phi^k(\alpha) \in \mathbb{F}_{q^n}$.

Theorem 2. *Assume that α is a generator of a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let*

$$R = \sum_{g \in G} \mathrm{Tr}\big(\alpha\, g(\alpha)\big) g \in \mathbb{F}_q[G]. \tag{1}$$

Any $v \in \mathbb{F}_q[G]$ such that $v\overline{v} = R$ is invertible, and the map $v \mapsto v^{-1} \circ \alpha$ is a one-to-one correspondence between the set of solutions of the equation $v\overline{v} = R$ in $\mathbb{F}_q$ and the set of elements of $\mathbb{F}_{q^n}$ that generate a self-dual normal basis.

In Section 1 we first explain how this result can be deduced from the statement on circulant matrices [11, Lemma 5.5.3]. Our main interest is in implementing Pickett's method as an algorithm, and since the language he uses to describe his construction of a solution of the equation $v\overline{v} = R$ in [22, §3] is quite elaborate — his framework is wider than ours — we reformulate it in terms of the polynomial ring $\mathbb{F}_q[X]/(X^n - 1)$; the resulting algorithm to compute a self-dual normal basis is described in the last section. We remark that this construction gives an alternative proof of the sufficiency of the conditions of Theorem 1; for interest we give a proof of their necessity, mainly based on Theorem 2, and simpler than the original (see [11, Propositions 4.3.4 and 5.2.2]).

Section 2 deals with the orthogonal circulant group $O(n, q)$. Its elements are the $n \times n$ matrices P over $\mathbb{F}_q$ that are circulant ($P_{i+k \bmod n,\ j+k \bmod n} = P_{i,j}$ for $0 \leqslant i, j, k \leqslant n-1$) and orthogonal ($P^t \cdot P = I$, where P^t is the transpose matrix of P and I the identity $n \times n$ matrix). It follows from Theorem 2 that $O(n, q)$ is isomorphic to the subgroup of $\mathbb{F}_q[G]^\times$ consisting of the solutions of the equation $v\overline{v} = 1$. In both the semi-simple and the ramified case we indicate how this equation can be solved; the resulting algorithms are described in the last section. Doing so we recover the number of self-dual normal bases, as derived in [12,13] from MacWilliams' results about the orthogonal circulant group [17] (see [11, 5.3] for a summary). In the ramified (and odd characteristic) case our construction is a variation, adjusted to our situation, of MacWilliams' iterative construction; we also present a new explicit formula for the solutions.

In Section 3 we present our algorithms, experimental results and conclusions. For semi-simple extensions in odd characteristic, the lowest complexity we find is close to that obtained for normal bases from exhaustive computer search [3] or from theoretical constructions [15], as this was already

the case in even characteristic. We also observe an interesting behaviour under base field extension. When the extension is of degree p in odd characteristic p we recover the basis with very low complexity $3p-2$ described in [3].

1. Construction of a self-dual normal basis

Our algorithm to find a self-dual normal basis relies on the interpretation in terms of polynomial rings of Pickett's construction of a solution v of the equation $v\overline{v}=R$ of Theorem 2 (under the necessary conditions of Theorem 1). The majority of this section is devoted to presenting this interpretation. First, however, we deduce Theorem 2 from statements in terms of circulant matrices. At the end of the section we show how to deduce the necessity of the conditions of Theorem 1 from Theorem 2.

Proof of Theorem 2. Consider the one-to-one correspondence between $\mathbb{F}_q[G]$ and circulant $n\times n$ matrices over $\mathbb{F}_q$, given by

$$v=\sum_{j=0}^{n-1}\rho_j\phi^j\in\mathbb{F}_q[G]\mapsto C_v=(\rho_{j-i \bmod n})_{0\leqslant i,j\leqslant n-1}. \tag{2}$$

One has $C_1=I$ and, for any $v,w\in\mathbb{F}_q[G]$, $C_v\cdot C_w=C_{vw}$, so (2) yields a group isomorphism between $\mathbb{F}_q[G]^\times$ and the abelian group of invertible circulant $n\times n$ matrices over $\mathbb{F}_q$. Note that the matrix $C_R=(\mathrm{Tr}(\alpha^{q^i+q^j}))$ is invertible since α generates a normal basis, see [19, Corollary 1.3]. Hence, $R\in\mathbb{F}_q[G]^\times$ and $v\overline{v}=R$ implies v invertible as well.

Moreover one has $C_{\overline{v}}=(C_v)^t$. It follows that the equation $v\overline{v}=R$ is equivalent to

$$C_v\cdot(C_v)^t=\left(\mathrm{Tr}\left(\alpha^{q^i+q^j}\right)\right)_{0\leqslant i,j\leqslant n-1}. \tag{3}$$

For $x\in\mathbb{F}_{q^n}$, let $[x]$ denote the $n\times n$ matrix whose j-th column, $0\leqslant j\leqslant n-1$, consists of the coordinates of x^{q^j} in a fixed $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$. Then one has, for any $v\in\mathbb{F}_q[G]$, $x\in\mathbb{F}_{q^n}$:

$$[v\circ x]=[x]\cdot C_v.$$

Let P be some invertible $n\times n$ matrix over $\mathbb{F}_q$, then the columns of $B=[\alpha]P$ are the coordinates in the fixed $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ of a normal basis if and only if P is a circulant matrix, see [11, Lemma 3.1.3]. Further, for such a P, its inverse P^{-1} is also circulant and from [11, Lemma 5.5.3] we know that the columns of B form a self-dual normal basis if and only if

$$P^{-1}\cdot\left(P^{-1}\right)^t=\left(\mathrm{Tr}\left(\alpha^{q^i+q^j}\right)\right)_{0\leqslant i,j\leqslant n-1}. \tag{4}$$

If $v\overline{v}=R$, then C_v is circulant invertible and $(C_v)^{-1}=C_{v^{-1}}$ satisfies (4). Hence $B=[\alpha]C_{v^{-1}}=[v^{-1}\circ\alpha]$ is a self-dual normal basis. If β generates a self-dual normal basis, let P be such that $[\beta]=[\alpha]P$, then P is circulant and so is its inverse. By (3) the element $v\in\mathbb{F}_q[G]$ such that $P^{-1}=C_v$ satisfies $v\overline{v}=R$. These two maps are clearly mutual inverses, which completes the proof. □

1.1. Interpretation of Pickett's construction in terms of polynomial rings

The Galois group G of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is cyclic of order n and generated by the Frobenius ϕ, so we may identify the $\mathbb{F}_q$-algebras $\mathbb{F}_q[G]$ and $\mathbb{F}_q[X]/(X^n-1)$ through the isomorphism mapping ϕ to X.

Write $n=p^en_1$, where p is the characteristic of $\mathbb{F}_q$ and n_1 is prime to p. We take advantage of the following result [11, Theorems 3.3.13 and 5.1.9] to split the extension into two parts.

Lemma 1.1. *Let m, n be two co-prime integers. Suppose α (resp. β) is a generator of a self-dual normal basis of $\mathbb{F}_{q^m}$ (resp. $\mathbb{F}_{q^n}$) over $\mathbb{F}_q$, then $\alpha\beta$ is a generator of a self-dual normal basis of the compositum $\mathbb{F}_{q^{mn}}$ over $\mathbb{F}_q$. Moreover, the complexity of $\alpha\beta$ is the product of the complexities of α and of β.*

By the former result, we may deal separately with the two cases $n = p^e$ which we call the ramified case, and n co-prime to p, the so-called semi-simple case. We show how to construct a solution v of the equation $v\overline{v} = R$ of Theorem 2 in each of these two cases, under the existence conditions of a self-dual normal basis of Theorem 1. Multiplying the bases obtained this way then yields self-dual normal bases for the extensions with "mixed degree" $n = n_1 p^e$ with $n_1 \geqslant 2$ and $e \geqslant 1$.

1.1.1. The ramified case ($n = p^e$)

In this case, the algebra $\mathbb{F}_q[G]$ is isomorphic to $\mathbb{F}_q[X]/(X-1)^n$. Let $\epsilon : \mathbb{F}_q[G] \to \mathbb{F}_q$ be the augmentation map given by $\epsilon(\sum_{k=0}^{n-1} a_k\phi^k) = \sum_{k=0}^{n-1} a_k$. This is a homomorphism of $\mathbb{F}_q$-algebras whose kernel is a codimension 1 subspace of $\mathbb{F}_q[G]$. Further $\epsilon(\sum_{k=0}^{n-1} a_k\phi^k) = 0$ implies $\sum_{k=0}^{n-1} a_k\phi^k = \sum_{k=0}^{n-1} a_k(\phi^k - 1)$, and therefore the kernel is $(\phi-1)\mathbb{F}_q[G]$. Invertible elements in $\mathbb{F}_q[G]$ are those which have non-zero image under the map ϵ (because invertible modulo $(X-1)^n$ means invertible modulo $X-1$), hence the group $\mathbb{F}_q[G]^\times$ has order $q^{n-1}(q-1)$. In fact, it is the direct product of $\mathbb{F}_q^\times$ by $U = 1 + (\phi-1)\mathbb{F}_q[G]$, the inverse image of 1 under the map ϵ.

Under the necessary conditions of Theorem 1, we have two cases to consider.

Proposition 1.2. *Let p be the characteristic of $\mathbb{F}_q$. If $p = n = 2$, $\beta \in \mathbb{F}_{q^2}$ generates a self-dual normal basis if and only if $\mathrm{Tr}(\beta) = 1$. If p is odd and $n = p^e$, there exists $\omega \in \mathbb{F}_q[G]$ such that $\omega^2 = R$. Furthermore, $\omega = \overline{\omega}$.*

Proof. The even characteristic case is straightforward. We proceed with the odd characteristic case. Recall that $R \in \mathbb{F}_q[G]^\times$ and note that $\overline{R} = R$, which is clear from (1). One can easily see that $\epsilon(R) = \mathrm{Tr}(\alpha)^2$ (detailed in the proof of Lemma 1.6 below), so that the decomposition of R in the direct product $\mathbb{F}_q^\times \times U$ is $R = \mathrm{Tr}(\alpha)^2 \cdot (1 + (\phi-1)R')$ for some $R' \in \mathbb{F}_q[G]$. The second factor is also a square as it belongs to the group U which is of odd order, hence $R = \omega^2$ for some ω. Further $\overline{R} = R$ implies $\overline{\omega}^2 = \omega^2$, so that $\overline{\omega}/\omega$ is a square root of 1 living in the group U of odd order. Thus $\overline{\omega} = \omega$. □

1.1.2. The semi-simple case ($\gcd(n, q) = 1$)

We assume that n is odd to fit with the conditions of Theorem 1 (but q could be odd or even). The polynomial $X^n - 1$ is square free and has monic irreducible factors over $\mathbb{F}_q$:

$$X^n - 1 = \prod_{i=1}^{\sigma} f_i(X) \prod_{j=1}^{\tau} g_j(X) \cdot g_j^*(X) \tag{5}$$

where g_j^* denotes the reciprocal polynomial (up to a constant) of g_j and where the f_i are the self-reciprocal (also up to a constant) irreducible factors. We will now express the equation $R = v\overline{v}$ in this decomposition, solve it, and then lift back the solution to $\mathbb{F}_q[G]$.

Let m be the order of q modulo n. The field $\mathbb{F}_{q^m}$ contains a primitive n-th root ζ of 1. On the set $\{0, \ldots, n-1\}$ we define the *cyclotomic equivalence relation:* $s \sim s'$ if there exists k such that $s \equiv q^k s' \bmod n$. Note that 0 forms a class on its own and that the integers prime to n belong to classes with the same cardinality equal to the order of q modulo n. Namely, since n and q are co-prime, the cyclotomic equivalence relation restricts to $(\mathbb{Z}/n\mathbb{Z})^\times$ and for s, s' invertible modulo n, $s \sim s'$ if and only if s and s' belong to the same coset in $(\mathbb{Z}/n\mathbb{Z})^\times/\langle q\rangle$.

The following proposition justifies the terminology. Recall that by "self-reciprocal", we mean "self-reciprocal up to a constant factor".

Proposition 1.3.

(a) *If ζ^s is a root of an irreducible factor of X^n-1, then the other roots are the $\zeta^{s'}$ where $s'\sim s$.*
(b) *The ζ^s such that $s\sim(n-s)$ are roots of a self-reciprocal factor f_i. The ζ^s such that $s\nsim n-s$ are roots of a non-self-reciprocal factor g_j.*
(c) *The number of cyclotomic classes is equal to the number $\sigma+2\tau$ of irreducible factors of X^n-1.*
(d) *The self-reciprocal factors f_i have even degree, except $f_1=X-1$.*

Proof. (a), (b), (c) are clear. Let us prove (d). If ζ^s is a root of an f_i, then ζ^{n-s} is also a root. If we exclude the case $s=0$ corresponding to the factor $X-1$, the two roots ζ^s and ζ^{n-s} are distinct, because n is odd. Hence f_i has en even number of roots in an algebraic closure. □

From the Chinese Remainder Theorem, the algebra $\mathbb{F}_q[X]/(X^n-1)$ is isomorphic to a product of $\sigma+2\tau$ fields:

$$\frac{\mathbb{F}_q[X]}{(X^n-1)}\simeq\prod_{i=1}^{\sigma}\frac{\mathbb{F}_q[X]}{(f_i(X))}\times\prod_{j=1}^{\tau}\left(\frac{\mathbb{F}_q[X]}{(g_j(X))}\times\frac{\mathbb{F}_q[X]}{(g_j^*(X))}\right). \tag{6}$$

Each factor in the RHS of this equation is an extension of $\mathbb{F}_q$ contained in $\mathbb{F}_{q^m}$ (recall m is the order of q modulo n). The evaluation map $u(X)\in\mathbb{F}_q[X]/(f)\mapsto u(\zeta^s)\in\mathbb{F}_q(\zeta^s)$, where f is an irreducible factor of X^n-1 and $s\in\{0,\dots,n-1\}$ is such that $f(\zeta^s)=0$, is a field isomorphism. We obtain the following result:

Proposition 1.4. *Let S be a set of representatives of cyclotomic classes. The map*

$$\begin{cases}\mathbb{F}_q[X]/\big(X^n-1\big)\longrightarrow\prod_{s\in S}\mathbb{F}_q\big(\zeta^s\big),\\ u(X)\longmapsto\big(u\big(\zeta^s\big)\big)_{s\in S}\end{cases} \tag{7}$$

is an $\mathbb{F}_q$-algebra isomorphism.

For practical reasons (mainly to deal with square matrices), we also consider the map $\mathcal{F}$ (a Fourier transform)

$$\mathcal{F}:\begin{cases}\mathbb{F}_q[X]/(X^n-1)\longrightarrow(\mathbb{F}_{q^m})^n,\\ u(X)\longmapsto(u(\zeta^s))_{0\leqslant s\leqslant n-1}\end{cases} \tag{8}$$

which is a homomorphism of $\mathbb{F}_q$-algebras, with matrix $F(\zeta)=(\zeta^{ij})_{0\leqslant i,j\leqslant n-1}$. Compared with isomorphism (7), we now compute a component at every $0\leqslant s\leqslant n-1$; the components corresponding to indices in the same coset under $\sim$ are cyclically permuted when applying the Frobenius ϕ.

We note the following easy but useful relation involving the matrices $F(\zeta)$ and $F(\zeta^{-1})=(\zeta^{-ji})_{0\leqslant i,j\leqslant n-1}$.

Lemma 1.5. *We have, with the previous notation, $F(\zeta^{-1})F(\zeta)=nI$.*

As a consequence, the following linear map $\overline{\mathcal{F}}$, with matrix $F(\zeta^{-1})$, can be used to compute the inverse of $\mathcal{F}$.

$$\overline{\mathcal{F}}:\begin{cases}(\mathbb{F}_{q^m})^n\longrightarrow\mathbb{F}_{q^m}[X]/(X^n-1),\\ (r_0,\dots,r_{n-1})\longmapsto\sum_{t=0}^{n-1}u_tX^t\quad\text{where } u_t=\sum_{i=0}^{n-1}r_i\zeta^{-ti}.\end{cases} \tag{9}$$

This is because $\overline{\mathcal{F}}(\mathcal{F}(u)) = nu$ for each $u \in \mathbb{F}_q[X]/(X^n - 1)$.

The idea here is to express R as an element of the RHS of (7), to solve the equation in each component, and to bring back the solution to $\mathbb{F}_q[X]/(X^n - 1)$. The conjugation map, induced by $X \mapsto X^{n-1}$ in $\mathbb{F}_q[X]/(X^n - 1)$ is given by $\zeta \mapsto \zeta^{-1}$ and will sometimes be denoted by J in the RHS of (7).

Let R be as in Theorem 2. The s-coordinate of $\mathcal{F}(R)$ is $R_s = \sum_{i=0}^{n-1} \mathrm{Tr}(\alpha^{1+q^i})\zeta^{si}$.

We begin with the cyclotomic class $s = 0$. Here, $\mathbb{F}_q(\zeta^s) = \mathbb{F}_q$ and the conjugation map J acts trivially. Note that $R_0 = \epsilon(R)$.

Lemma 1.6. *(See Lemma 3.5 in [22].) With $v_0 = \mathrm{Tr}(\alpha)$, we have $v_0\overline{v}_0 = R_0$.*

Proof. We have $J(\mathrm{Tr}(\alpha)) = \mathrm{Tr}(\alpha)$ and

$$\mathrm{Tr}(\alpha)^2 = \left(\sum_{i=0}^{n-1} \alpha^{q^i}\right)^2 = \sum_{i,j=0}^{n-1} \alpha^{q^i+q^j} = \sum_{i,k=0}^{n-1} \alpha^{q^i(1+q^k)} = \sum_{k=0}^{n-1} \mathrm{Tr}\big(\alpha^{1+q^k}\big) = R_0. \qquad \square$$

We now consider the cyclotomic classes s such that $s \nsim n - s$.

Lemma 1.7. *(See Lemma 3.6 in [22].) Let $s' \in S$ such that $s' \sim n - s$. We have $R_s = R_{s'}$. Putting $v_{s,s'} = (R_s, 1) \in \mathbb{F}_q(\zeta^s) \times \mathbb{F}_q(\zeta^{s'})$, we have $v_{s,s'}\overline{v}_{s,s'} = (R_s, R_s)$.*

Proof. The conjugation map J exchanges coordinates in $\mathbb{F}_q(\zeta^s) \times \mathbb{F}_q(\zeta^{s'})$: $J(u, u^*) = (u^*, u)$. As R is invariant by conjugation, we have $R_s = R_{s'}$. Therefore $v_{s,s'}J(v_{s,s'}) = (R_s, 1)(1, R_s) = (R_s, R_s)$. $\square$

We finally deal with the cyclotomic classes s such that $s \neq 0$ and $s \sim n - s$.

Lemma 1.8. *(See Lemma 3.7 in [22].) Let $s \in S$ such that $0 \neq s$ and $s \sim n - s$. Then the field $\mathbb{F}_q(\zeta^s)$ is stable under the conjugation map J, and we denote by $\mathbb{F}_q(\zeta^s)^J$ the fixed subfield. Furthermore R_s (resp. $-R_s$) has a square root u (resp. u') in $\mathbb{F}_q(\zeta^s)$. We consider three cases*:

(a) *If $u \in \mathbb{F}_q(\zeta^s)^J$, then $v_s = u$ satisfies $v_s\overline{v}_s = R_s$;*
(b) *If $u' \notin \mathbb{F}_q(\zeta^s)^J$, then $v_s = u'$ satisfies $v_s\overline{v}_s = R_s$;*
(c) *If $u \notin \mathbb{F}_q(\zeta^s)^J$ and $u' \in \mathbb{F}_q(\zeta^s)^J$, then there exists an integer n such that $-n$ is a non-zero square η^2 modulo the characteristic p of $\mathbb{F}_q$, but $-(n-1)$ is not a square modulo p, and there exists an integer ν such that $\nu^2 \equiv n - 1$ modulo p. We put $v_s = (\nu u + u')/\eta$, then $v_s\overline{v}_s = R_s$.*

Proof. From Proposition 1.3, the field $\mathbb{F}_q(\zeta^s)$ is stable under J and of even degree over $\mathbb{F}_q$. Furthermore, we have $\overline{\zeta}^s = \zeta^{-s} \neq \zeta^s$ because n is odd, hence J restricted to $\mathbb{F}_q(\zeta^s)$ is an order 2 field automorphism. By Galois theory $\mathbb{F}_q(\zeta^s)^J$ is the unique index 2 subextension of $\mathbb{F}_q(\zeta^s)/\mathbb{F}_q$. Moreover, $\mathbb{F}_q(\zeta^s)$ is the only degree 2 extension of $\mathbb{F}_q(\zeta^s)^J$ in a given algebraic closure. It follows that every element of $\mathbb{F}_q(\zeta^s)^J$ is a square in $\mathbb{F}_q(\zeta^s)$. Since R_s and $-R_s$ are both invariant under J, the existence of their square roots u and u' in $\mathbb{F}_q(\zeta^s)$ is proved.

If $\overline{u} = u$, namely in case (a), then $u\overline{u} = u^2 = R_s$. Note that the condition $u \in \mathbb{F}_q(\zeta^s)^J$ is automatically fulfilled in characteristic 2, since the Frobenius from the prime field $\mathbb{F}_2$ is an automorphism of $\mathbb{F}_q(\zeta^s)^J$ in that case. The same argument shows that q has to be odd in cases (b) and (c). If $\overline{u}' \neq u'$, namely in case (b), then $\overline{u}' = -u'$ and $u'\overline{u}' = -u'^2 = R_s$. Suppose now (case c) that $\overline{u} = -u$ and $\overline{u}' = u'$. As $-1 = -R_s/R_s$, we know that -1 is not a square in $\mathbb{F}_q(\zeta^s)^J$, nor in $\mathbb{F}_p$. Hence the first $n > 1$ such that $-n$ is a square modulo p exists and satisfies the required conditions. Also, because neither -1 nor $-(n-1)$ are squares modulo p, there exists an integer ν such that $\nu^2 \equiv (n-1)$ modulo p. Taking the residues of η and ν modulo p, we have $\overline{\eta} = \eta$ and $\overline{\nu} = \nu$ because $\mathbb{F}_p \subseteq \mathbb{F}_q(\zeta^s)^J$. With $v_s = (\nu u + u')/\eta$, we have $\overline{v}_s = (-\nu u + u')/\eta$ and it follows that $v_s\overline{v}_s = (-\nu^2 u^2 + u'^2)/\eta^2 = (-(n-1)R_s - R_s)/(-n) = R_s$. $\square$

We have solved the equation $v_s\overline{v}_s = R_s$ for every cyclotomic class s, thus by the $\mathbb{F}_q$-algebra isomorphism (7) we get a solution $v \in \mathbb{F}_q[G]$ of the equation $v\overline{v} = R$.

1.2. The necessity of the conditions of Theorem 1

If α is a generator of a self-dual normal basis of $\mathbb{F}_{q^{nm}}$ over $\mathbb{F}_q$, then $\mathrm{Tr}_{\mathbb{F}_{q^{nm}}/\mathbb{F}_{q^n}}(\alpha)$ is a generator of a self-dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, see [22, Lemma 4.3]. Therefore, to prove the necessity of the conditions in Theorem 1 we need just consider the cases $\mathbb{F}_{q^2}/\mathbb{F}_q$ for q odd and $\mathbb{F}_{q^4}/\mathbb{F}_q$ for q even.

When q is odd, $\mathrm{Tr}(\alpha\alpha^q) = 2N(\alpha)$ for any $\alpha \in \mathbb{F}_{q^2}$, where $N(\alpha)$ denotes the norm of α in the extension, hence $\mathrm{Tr}(\alpha\alpha^q) = 0$ would imply $\alpha = 0$.

Let q be even, and assume for contradiction that there exist a normal basis generator α of $\mathbb{F}_{q^4}/\mathbb{F}_q$ and an element $v \in \mathbb{F}_q[G]$ such that $v\overline{v} = \mathrm{Tr}(\alpha^2) + \mathrm{Tr}(\alpha\alpha^q)\phi + \mathrm{Tr}(\alpha\alpha^{q^2})\phi^2 + \mathrm{Tr}(\alpha\alpha^{q^3})\phi^3$. Note that $\mathrm{Tr}(\alpha\alpha^{q^3}) = \mathrm{Tr}(\alpha\alpha^q)$ and $\mathrm{Tr}(\alpha\alpha^{q^2}) = 2\,\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(N_{\mathbb{F}_{q^4}/\mathbb{F}_{q^2}}(\alpha)) = 0$. Writing $v = a + b\phi + c\phi^2 + d\phi^3$ with $a, b, c, d \in \mathbb{F}_q$ and letting $\beta = \alpha + \alpha^{q^2}$, we easily get the equations:

$$a + b + c + d = \mathrm{Tr}(\alpha) = \beta + \beta^q, \qquad (a + c)(b + d) = \mathrm{Tr}\big(\alpha\alpha^q\big) = \beta\beta^q.$$

It follows that $\{\beta, \beta^q\} = \{a + c, b + d\}$, namely $\beta \in \mathbb{F}_q$, which is impossible since it would imply $\alpha + \alpha^{q^2} = \alpha^q + \alpha^{q^3}$, contradicting the fact that α generates a normal basis. The result now follows using Theorem 2.

2. Change of self-dual normal basis

The orthogonal circulant group $O(n, q)$ can be seen abstractly as the group of vector space automorphisms that map a self-dual normal basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$ to another one. Once a vector space basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ has been fixed, it identifies with the more concrete group of orthogonal and circulant $n \times n$ matrices with entries in $\mathbb{F}_q$. We now give a third interpretation in terms of the group algebra $\mathbb{F}_q[G]$. Our result, which is essentially a different formulation of the "key" Lemmas 2 and 3 of [13], is an immediate consequence of Theorem 2 and the observations that if α generates a self-dual normal basis, then $R = 1$, and that if $v\overline{v} = 1$, then $v^{-1} = \overline{v}$.

Corollary 2.1. *Let α generate a self-dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The map $v \mapsto \overline{v} \circ \alpha$ is an isomorphism between the group of solutions of the equation $v\overline{v} = 1$ in $\mathbb{F}_q[G]$ and the group of elements of $\mathbb{F}_{q^n}$ that generate a self-dual normal basis.*

It follows that computing all self-dual normal bases from one is equivalent to finding all the solutions $v \in \mathbb{F}_q[G]^\times$ of the equation $v\overline{v} = 1$. We devote the rest of this section to explain how this equation can be solved, first in the semi-simple case and then in the ramified case.

2.1. The semi-simple case

The decomposition (7) from Section 1 is useful to find the solutions of the equation $v\overline{v} = 1$. Let $V(X) \in \mathbb{F}_q[X]/(X^n - 1)$.

Proposition 2.2. *The polynomial $V(X)$ satisfies the equation $V(X)V(X^{n-1}) = 1$ modulo $X^n - 1$ if and only if the following conditions hold*:

$$\begin{cases} V(1) = \pm 1 & (\text{case } s = 0), \\ V\big(\zeta^s\big)V\big(\zeta^{-s}\big) = 1 & \text{for } s \nsim n - s, \\ V\big(\zeta^s\big)^{q^{r/2}+1} = 1 & \text{for } 0 \neq s \sim n - s, \text{ where } r \text{ is such that } \mathbb{F}_q(\zeta^s) = \mathbb{F}_{q^r}. \end{cases}$$

Note that r is the degree of the irreducible factor f_i of $X^n - 1$ such that $f_i(\zeta^s) = 0$.

Proof. The component at $s = 0$ is $V(1)$ and the equation we need to solve in $\mathbb{F}_q(\zeta^0) = \mathbb{F}_q$ is simply $V(1)^2 = 1$ because the action of conjugation in $\mathbb{F}_q$ is trivial.

For $s \nsim n - s$, we have to consider the product $\mathbb{F}_q(\zeta^s) \times \mathbb{F}_q(\zeta^{-s})$. We have seen in the proof of Lemma 1.7 that conjugation swaps coordinates in these two factors. The solutions are the powers of (g_s, g_s^{-1}) where g_s is any primitive element of the $\mathbb{F}_q(\zeta^s)$.

For $0 \neq s \sim n - s$, we have seen in the proof of Lemma 1.8 that the set of invariants under conjugation J is the subfield $\mathbb{F}_{q^{r/2}}$ of $\mathbb{F}_{q^r} = \mathbb{F}_q(\zeta^s)$. Conjugation J is an $\mathbb{F}_{q^{r/2}}$-automorphism of $\mathbb{F}_{q^r}$ of order 2, hence $J(x) = x^{q^{r/2}}$ for $x \in \mathbb{F}_{q^r}$. The equation we want to solve can be written $x^{q^{r/2}+1} = 1$. Note that $q^{r/2} + 1$ divides $q^r - 1$ so we find exactly $q^{r/2} + 1$ solutions, generated by any element of order $q^{r/2} + 1$ in $\mathbb{F}_q(\zeta^s)$. □

We remark that this proof provides generators for the group of solutions of $v\overline{v} = 1$, so we can easily derive the cardinality of this group, which by Corollary 2.1 is also the number of self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. As expected, this calculation agrees with the result in [13] which was obtained using the formulas given in [17] — note that the cyclic shift of a basis is considered to be the same basis in [13], but not here, so our formula differs from the one found there by a factor n.

Theorem 2.3. *Consider the decomposition* (5) *of* $X^n - 1$ *over* $\mathbb{F}_q$. *The number of self-dual normal bases of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ *is given by*

$$2^a \prod_{i=2}^{\sigma} \left(q^{c_i} + 1\right) \prod_{j=1}^{\tau} \left(q^{d_j} - 1\right) \quad \textit{with} \begin{cases} a = 0 \textit{ for even } q \textit{ and } a = 1 \textit{ for odd } q, \\ 2c_i = \deg f_i \textit{ and } d_j = \deg g_j. \end{cases}$$

Proof. The case $s = 0$ has solutions ± 1 in odd characteristic, and only 1 for even q. For the case $0 \neq s \sim n - s$, we found a generator of order $q^c + 1$ for the set of solutions in the field $\mathbb{F}_q(\zeta)$. For the case $s \nsim n - s$, let g be a primitive element in $\mathbb{F}_q[X]/(f) \simeq \mathbb{F}_q(\zeta)$, the solutions are the powers of (g, g^{-1}). □

2.2. The ramified case

We deal only with the odd characteristic case, so we let p be an odd prime number, and q and n be powers of p.

Theorem 2.4. *There are* $2q^{\frac{n-1}{2}}$ *solutions* $v \in \mathbb{F}_q[G]$ *to the equation* $v\overline{v} = 1$.

This result can easily been derived from [12, Theorem 2], which states that if $n = sp$, where s is any integer, then the following equality, about sizes of orthogonal circulant groups, holds: $|O(sp, q)| = q^{(p-1)s/2}|O(s, q)|$. The original statement is due to MacWilliams in the prime base field case [17, Theorem 2.6]. We now reinterpret MacWilliams' constructive proof in our specific case: n a power of p, so as to explain the structure of the algorithm we use to compute the orthogonal circulant group in the ramified case.

Proof. First note that the solutions of the equation $v\overline{v} = 1$ all lie in $\mathbb{F}_q[G]^\times$, and recall from Section 1.1.1 that $\mathbb{F}_q[G]^\times$ is the (internal) direct product $\mathbb{F}_q^\times \times (1 + (\phi - 1)\mathbb{F}_q[G])$, the first component being simply the image by the augmentation map ϵ. For $v \in \mathbb{F}_q[G]^\times$, let $w \in (\phi - 1)\mathbb{F}_q[G]$ be such that $v = \epsilon(v)(1 + w)$, then $v\overline{v} = 1$ if and only if $\epsilon(v) = \pm 1$ and $w + \overline{w} + w\overline{w} = 0$. Setting $r = w + \frac{w\overline{w}}{2}$, the second condition becomes $r = -\bar{r}$, namely

$$r = \sum_{i=1}^{\frac{n-1}{2}} r_i \left(\phi^i - \phi^{n-i}\right) \tag{10}$$

for some $r_i \in \mathbb{F}_q$, hence r can take $q^{\frac{n-1}{2}}$ values in $\mathbb{F}_q[G]$. We now show that w is uniquely defined by r, and how it can be computed, see [17, Appendix A]. One has $w = -r + \frac{w\overline{w}}{2}$, hence $\overline{w} = r + \frac{w\overline{w}}{2}$ and $w\overline{w} = -r^2 + \frac{(w\overline{w})^2}{4}$, so that:

$$w = -r - \frac{r^2}{2} + \frac{(w\overline{w})^2}{8}.$$

Replacing iteratively $w\overline{w}$ by $-r^2 + \frac{(w\overline{w})^2}{4}$ in the above formula increases the (even) power to which $w\overline{w}$ appears; this process terminates since, as an element of $(\phi - 1)\mathbb{F}_q[G]$, $w = (\phi - 1)y$ for some $y \in \mathbb{F}_q[G]$, so $w^n = (\phi^n - 1)y^n = 0$. □

Remark 2.5. In the odd characteristic case, the formula in Theorem 2.3 reads:

$$2\prod_{i=2}^{\sigma}\left(q^{c_i} + 1\right)\prod_{j=1}^{\tau}\left(q^{d_j} - 1\right) \approx 2q^{\sum_i c_i + \sum_j d_j} = 2q^{(n-1)/2}.$$

In both semi-simple and ramified cases, the size of the trace-orthogonal group is close to $2\sqrt{q^{n-1}}$, which means that an exhaustive search quickly becomes lengthy when q or n increases.

We now show that one can also get an explicit formula for the solutions of the equation.

Theorem 2.6. *The solutions $v \in \mathbb{F}_q[G]$ to the equation $v\overline{v} = 1$ are exactly the sums $v = \sum_{i=0}^{n-1} v_i(\phi - 1)^i$ with $v_0 = \pm 1$ and, for $1 \leqslant i \leqslant \frac{n-1}{2}$, v_{2i-1} is any element of $\mathbb{F}_q$ and $v_{2i} \in \mathbb{F}_q$ is such that*:

$$\sum_{j=1}^{2i}\sum_{k=0}^{j}(-1)^k\binom{n-k}{2i-j}v_k v_{j-k} = 0. \tag{11}$$

Note that (11) gives a formula for v_{2i} in terms of the v_k with $0 \leqslant k \leqslant 2i-1$, for instance $-2v_0v_2 = -v_1^2 + v_0v_1$ and $-2v_0v_4 = v_0v_2 - v_1v_2 - 2v_1v_3 + v_2^2 + 3v_0v_3$.

Our proof begins as a specialisation to the case $s = 1$ of that of [2, Satz 3.3] − note that [12] points out a mistake in the end of the proof of this statement; dealing with this simpler case enables us to deduce a constructive formula.

Before starting the proof, let us recall the isomorphism

$$\mathbb{F}_q[G] \cong \mathbb{F}_q[X]/(X-1)^n \tag{12}$$

mapping ϕ to X. The family $((X-1)^i)_{0\leqslant i\leqslant n-1}$ is a basis of the $\mathbb{F}_q$-vector space $\mathbb{F}_q[X]/(X-1)^n$. As an auxiliary result we compute the conjugates $\overline{(X-1)^i} = (\overline{X} - 1)^i$ of our basis elements.

Lemma 2.7. *For $0 \leqslant i \leqslant n-1$, $(X-1)^i$ divides $(\overline{X} - 1)^i$ and, more precisely*:

$$(\overline{X} - 1)^i = (-1)^i\sum_{k=0}^{n-i-1}\binom{n-i}{k}(X-1)^{k+i} \equiv (-1)^i(X-1)^i \mod (X-1)^{i+1}.$$

Proof. Let $0 \leqslant i \leqslant n-1$, then

$$(\overline{X} - 1)^i = \left(X^{n-1} - 1\right)^i = \left((1-X)X^{n-1}\right)^i = (-1)^i(X-1)^iX^{n-i},$$

hence the equality, using Newton's formula for $X^{n-i} = (X - 1 + 1)^{n-i}$. □

Proof of Theorem 2.6. We wish to solve the equation $v\overline{v} = 1$ in $\mathbb{F}_q[G]$. We shall proceed by successive approximation, solving $v\overline{v} \equiv 1$ modulo $(X-1)^i$ for $1 \leqslant i \leqslant n$, where we identify v and its image under (12), that we write $v = \sum_{k=0}^{n-1} v_k (X-1)^k$ with $v_k \in \mathbb{F}_q$.

The first step is obvious: $\mathbb{F}_q[X]/(X-1) \cong \mathbb{F}_q$ is conjugation invariant, hence the equation reads $v^2 \equiv 1$ modulo $(X-1)$, namely $v \equiv \pm 1$ modulo $(X-1)$, in other words $v_0 = \pm 1$.

The second step is about the coefficients of v of odd index.

Lemma 2.8. *Let* $1 \leqslant i \leqslant \frac{n-1}{2}$ *and assume* $v\overline{v} \equiv 1 \bmod (X-1)^{2i-1}$, *then*

$$v\overline{v} \equiv 1 \mod (X-1)^{2i}.$$

Proof. Write $v\overline{v} \equiv 1 + u(X-1)^{2i-1} \bmod (X-1)^{2i}$ for some $u \in \mathbb{F}_q$. Applying conjugation we get that $(\overline{X}-1)^{2i}$ divides $v\overline{v} - 1 - u(\overline{X}-1)^{2i-1}$, therefore

$$v\overline{v} \equiv 1 + u(\overline{X}-1)^{2i-1} \mod (X-1)^{2i},$$

thanks to Lemma 2.7. We get:

$$0 \equiv u\big((X-1)^{2i-1} - (\overline{X}-1)^{2i-1}\big) \equiv 2u(X-1)^{2i-1} \mod (X-1)^{2i},$$

hence $u = 0$. □

In particular we get that, if $v_0 = \pm 1$, then $v\overline{v} \equiv 1 \bmod (X-1)^2$ for any value of $v_1 \in \mathbb{F}_q$. The third step is a formula for the coefficients of v of even positive index.

Lemma 2.9. *Suppose* $v\overline{v} \equiv 1 \bmod (X-1)^{2i}$ *for some integer* $1 \leqslant i \leqslant \frac{n-1}{2}$, *then* $v\overline{v} \equiv 1 \bmod (X-1)^{2i+1}$ *if and only if* v_{2i} *satisfies* (11).

Proof. Without any hypothesis on $v\overline{v}$, one checks using Lemma 2.7 that:

$$v\overline{v} = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{i} \sum_{k=0}^{j} (-1)^k \binom{n-k}{i-j} v_k v_{j-k} \right) (X-1)^i.$$

With our assumption on $v\overline{v}$, we get:

$$v\overline{v} \equiv 1 + \sum_{j=0}^{2i} \sum_{k=0}^{j} (-1)^k \binom{n-k}{2i-j} v_k v_{j-k} \mod (X-1)^{2i+1},$$

hence the result, noticing that $\binom{n}{2i} \equiv 0 \bmod p$. □

This ends the proof of Theorem 2.6. □

3. Experiments

3.1. Algorithms

Using MAGMA, we have implemented two algorithms based on the results of this paper. The first finds a self-dual normal basis for a given extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ satisfying the existence conditions of Theorem 1 and such that the degree n is either prime to the characteristic or a power of it. The

second (when run after the first) computes the orthogonal circulant group and uses it to construct all self-dual normal bases of the extension from the former one, then selects those which have the lowest complexity. Both of these algorithms have a semi-simple and a ramified version.

3.1.1. Computation of a self-dual normal basis

Our first algorithm permits us to find a self-dual normal basis for somewhat large extensions. For example, one can find a self-dual normal basis (of complexity 44 431) for $q = 1009$ and $n = 211$. Here is the structure of this algorithm in the semi-simple case $\gcd(n, q) = 1$:

Step 1. Compute the q-cyclotomic classes of the set $\{0, \ldots, n-1\}$.
Step 2. Let m be the size of the largest class (the class which contains 1) and choose ζ of order n in $\mathbb{F}_{q^m}$.
Step 3. Build the matrices $F(\zeta) = (\zeta^{ij})_{1 \leqslant i \leqslant j}$ and $F(\zeta^{-1})$.
Step 4. Find a normal element α in $\mathbb{F}_{q^n}$. (*This was already implemented in MAGMA, and uses methods which can be found in the book* [19].)
Step 5. Compute $R \in \mathbb{F}_q[G]$ defined in Theorem 2. Using the matrix $F(\zeta)$, map R to $R' = \mathcal{F}(R) \in (\mathbb{F}_{q^m})^n$.
Step 6. Use Lemmas 1.6, 1.7 and 1.8 to find a solution $v' \in \operatorname{Im} \mathcal{F} \subseteq (\mathbb{F}_q^m)^n$ of $v'\overline{v}' = R'$. Bring back v' to $\mathbb{F}_q[G]$ using matrix $F(\zeta^{-1})$ to obtain v such that $v\overline{v} = R$. Compute $w = v^{-1}$.
Step 7. Compute and output $\gamma = w \circ \alpha$.

In the odd characteristic, ramified case, we pick a normal element α in $\mathbb{F}_{q^n}$ and compute $R \in \mathbb{F}_q[G]$; by Proposition 1.2, solving the equation $v\overline{v} = R$ reduces to computing a square root of R in $\mathbb{F}_q[G] \simeq \mathbb{F}_q[X]/(X-1)^n$, which can be achieved by computing a square root of R modulo $X - 1$ and then using Hensel lifting.

3.1.2. Computation of all self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$

The second algorithm can be used whenever the orthogonal circulant group is not too large for an exhaustive enumeration, see Remark 2.5 and the tables in the next subsection. It uses the data computed by the previous algorithm which must be run first. Its structure in the semi-simple case $\gcd(n, q) = 1$ follows.

Step 1. Use Proposition 2.2 to find generators (and their orders) of the group U of solutions of $u\overline{u} = 1$ in $\mathbb{F}_q[G]$ (this is actually done in the right-hand side with generators of $\mathbb{F}_{q^{m_k}}$ where m_k is the size of the cyclotomic class).
Step 2. For each u in U (elements of U are enumerated using the generators found above), compute: the generator $\gamma = (uw) \circ \alpha$ of a self-dual normal basis, the multiplication-by-γ matrix $(\operatorname{Tr}(\gamma^{1+q^i+q^j}))_{i,j}$, and the complexity of γ. Update statistics accordingly (the best complexity found up to now, the list of best self-dual normal bases).
Step 3. Finally, output the statistics (mainly the best complexity, and the number of times this complexity was achieved).

In the ramified case, we list all the elements of $r \in \mathbb{F}_q[G]$ satisfying (10), compute the associated w as the proof of Theorem 2.4 (*i.e.*, iteratively); the group of solutions of $v\overline{v} = 1$ consists of the elements $1 + w$ obtained in this way together with their opposites $-1 - w$. We let each of these elements act on the self-dual normal basis constructed above and we determine the complexity of the resulting self-dual normal basis.

3.2. Tables

The following tables show the complexity of the best self-dual normal basis obtained with the above algorithms, for some extensions. We give separate tables for extensions in characteristic 2 and for extensions of small prime fields of odd characteristic. Blank entries have not been computed since the cost of exhaustive enumeration grows rapidly.

3.2.1. Even characteristic

The lowest complexity for self-dual normal bases of extensions over $\mathbb{F}_2$ has been computed by Geiselmann [11, Table 5.1] for odd degree up to 47. With our method we were able to verify these values up to $n = 45$ (the computation for degree 45 took approximately 25 hours on a 64-bit Xeon quad core running at 2.33 GHz). We include our table for completeness.

n	3	5	7	9	11	13	15	17	19	21	23
min	5	9	21	17	21	45	45	81	117	105	45
n	25	27	29	31	33	35	37	39	41	43	45
min	93	141	57	237	65	69	141	77	81	165	153

Note that [18, Table 4] gives a minimal complexity of 171 for normal bases in degree 37, where we find a self-dual normal basis of complexity 141, agreeing with Geiselmann. Since only one digit differs between these two results, we suspected that there could be a typo in [18], and this was confirmed by the authors of that paper.

Using Lemma 1.1, one gets an upper bound for the best self-dual normal complexities in even degree up to $n = 90$, using the fact that any element of $\mathbb{F}_4/\mathbb{F}_2$ of trace 1 generates an optimal self-dual normal basis (of complexity 3). Comparing to the results in [18, Table 4] for n up to 34, we see that this construction yields the best possible complexity in degrees 10, 22 and 34, and a reasonably good one in degrees 6, 14, 18, 26 and 30.

We get optimal self-dual normal bases in degrees $n = 3$, 5, 9, 11, 23, 29, 33, 35, 39 and 41. We know by [20, Corollary 3.6] that $2n+1$ has to be prime and 2 of order n or $2n$ modulo $2n+1$ for this to happen, therefore we do not get optimal self-dual bases in degrees 15 and 21, since 2 is of order 5 modulo 31 and of order 14 modulo 43.

We give also a table for other small even $q = 2^r$. Note that α^{q^i} for $0 \leqslant i \leqslant n-1$ generates the same normal basis as α, so the number of times the lowest complexity is obtained is a multiple of n. When we found more than n bases with the lowest complexity, we indicate the multiplier between parentheses. For example, we found 27 bases with complexity 45 for $q = 8$ and $n = 9$.

$q\backslash n$	3	5	7	9	11	13	15	17	19	21	23	25
2	5	9	21	17	21	45	45	81	117(2)	105	45	93
4	5	9	21	17	21	45	45	81	117(2)	105	45	93
8	9(3)	9	21	45(3)	21	45	81(3)	81				
16	5	9	21	17	21	45						
32	5	19(15)	21	17	21							
64	9(21)	9	21	45(3)								
128	5	9	37(98)									
256	5	9										

When $\gcd(n, r) = 1$ we always found the same best complexity for the extension $\mathbb{F}_{2^{rn}}$ over $\mathbb{F}_{2^r}$ as for the extension $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. This observation is partially explained by the following fact, which is also valid for odd q (see [19, Lemma 4.2] for a partial proof).

Lemma 3.1. *If α generates a self-dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $\gcd(n, r) = 1$, then α generates a self-dual normal basis of $\mathbb{F}_{q^{rn}}$ over $\mathbb{F}_{q^r}$, with the same complexity.*

One easily checks that if an extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ admits both a self-dual normal basis and an optimal normal basis of type I (see [9]), then q and n have to be even, say $q = 2^r$ and $n = 2m$, with m odd and $2m+1$ prime. If this is the case, the extension is the compositum of the fields $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^m}$, each of which may admit an optimal self-dual normal basis or not. Specifically, one can show that $\mathbb{F}_{q^2}/\mathbb{F}_q$ admits one if and only if r is odd, and that $\mathbb{F}_{q^m}/\mathbb{F}_q$ admits one if 2 is of order m or $2m$ modulo $2m+1$

and m is co-prime to r. If all these conditions are satisfied, the self-dual normal basis of $\mathbb{F}_{q^n}$ obtained by multiplying these two bases is, by Lemma 1.1, of complexity $3(2m-1) = 3n-3$, which is also the complexity of the dual basis of the optimal normal basis of $\mathbb{F}_{q^n}$, see [11, Theorem 5.4.10] ([24] even shows that the dual of any basis which is equivalent to the optimal one has complexity $3n-3$). This holds for instance for the extensions of $\mathbb{F}_2$ of degrees $6, 10, 18, 22, 46, \ldots$, and those of $\mathbb{F}_8$ of degrees $10, 22, 46, \ldots$.

3.2.2. Odd characteristic

Now we give the table showing some experiments for odd q. Here, the number of bases with least complexity is a multiple of $2n$ because $\pm\alpha^{q^i}$ for $0 \leqslant i \leqslant n-1$ generates a normal basis with same complexity as the one generated by α. When this multiple is greater than $2n$, we indicate the multiplier between parentheses. For example, we found $4 \times 2n = 8n$ bases with complexity 51 for $q = 13$ and $n = 9$.

$q\backslash n$	3	5	7	9	11	13	15	17	19	21	23	25
3	**7**	13	25	**37**	55(2)	67	−−	91	172	−−	127	135
5	6	**13**	25	46	64	85	−−	157	153	150		
7	6	16	**19**	41	61	96	87			−−		
11	6	13	25	52	**31**	100	78					
13	6	13	25	51(4)	64	**37**						
17	8	13	25	51(5)	64	100		−−				
19	8	13	31	51	67				−−			

Bold-faced entries correspond to the best complexity in the case when the degree n is a power of the characteristic. In this case, whenever n is prime, the best complexity is $3n-2$, and is obtained with the basis exhibited in [3, Theorem 5.3]. This basis is rather explicit since it is generated by the root of a trinomial, yielding a very interesting family of self-dual normal bases of complexity fairly close to the optimal one.

We have made no computation for "mixed degree" $n = n_1 p^e$ with $\gcd(n_1, p) = 1$, $n_1 > 1$ and $e > 0$, but one gets an upper bound for the lowest complexity in that case by multiplying the lowest complexity in degree n_1 by that in degree p^e, thanks to Lemma 1.1. For instance, the best complexity for $q = 5$ and $n = 15$ is at most $6 \cdot 13 = 78$. Note that when $n = \ell\ell'$ for prime numbers $\ell \neq \ell'$, both different from p, the best complexity for the compositum is not necessarily the product of those for degrees ℓ and ℓ' extensions ($n = 15$, $q = 7$); however it can be so ($n = 15$, $q = 11$; $n = 21$, $q = 5$).

In the semi-simple case, we also computed the best complexity for some odd non-prime values $q = p^r$, which do not appear in this table. When $\gcd(n, r) = 1$ we always found the same best complexity for the extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ as for the extension $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, as well as the same multiplier for the number of bases with the best complexity (as in the even characteristic case).

In odd characteristic, the only exhaustive search for lowest complexities among normal bases we are aware of is in [3], over prime base fields. The lowest complexity for self-dual normal bases is the same as the one they obtain for normal bases when $n = 3$ and $q = 7$ or 13; slightly larger when $n = 3$ and $q = 19$ (8 instead of 6) and when $n = 5$ and $q = 11$ (13 instead of 12). Note that in this last case, Liao and Feng give in [15, Example 2] a construction of a normal basis with minimal complexity 12, using Gauss periods, whose dual basis has complexity 13. Their construction remains valid when replacing the base field $\mathbb{F}_{11}$ by an extension of degree prime to 5.

3.3. Conclusion

Our algorithms enable us to compute the minimal complexity for self-dual normal bases in various extensions of finite fields, including some for which the exhaustive enumeration of normal bases would not be reasonable. In odd characteristic, the lowest complexities we obtain are either the same as or close to that obtained in former computations on normal bases using theoretical constructions

or exhaustive search, analogously to what could already be observed in even characteristic. However the cost of the exhaustive search of all self-dual normal bases (once one has been constructed) is still a limitation of this method. In order to make self-dual normal bases practical, it would thus be desirable to find a direct construction of those with low complexity.

A striking fact when looking at the tables above is the repetition of values along columns, albeit with some exceptions. We have a partial explanation for this phenomenon, that may also help in achieving the former goal, in terms of global considerations of cyclotomic extensions of the rationals generated by n^2-th roots of unity, where n is a prime. A known construction yields a global self-dual normal basis generator α_n such that, for any prime $p \neq n$ which does not split in the considered extension, the residue modulo p of α_n is a candidate for a best complexity basis for $\mathbb{F}_{p^n}/\mathbb{F}_p$. We hope to give full details about this construction in a future paper.

Acknowledgments

The authors would like to thank the anonymous referees for their valuable and insightful remarks and advice.

References

[1] D.W. Ash, I.F. Blake, S.A. Vanstone, Low complexity normal bases, Discrete Appl. Math. 25 (3) (1989) 191–210.
[2] T. Beth, W. Geiselmann, Selbstduale Normalbasen über GF(q), Arch. Math. (Basel) 55 (1) (1990) 44–48.
[3] I.F. Blake, S. Gao, R.C. Mullin, Normal and self-dual normal bases from factorization of $cx^{q+1} + dx^q - ax - b$, SIAM J. Discrete Math. 7 (3) (1994) 499–512.
[4] K.A. Byrd, T.P. Vaughan, Counting and constructing orthogonal circulants, J. Combin. Theory Ser. A 24 (1) (1978) 34–49.
[5] M. Christopoulou, T. Garefalakis, D. Panario, D. Thomson, The trace of an optimal normal element and low complexity normal bases, Des. Codes Cryptogr. 49 (1–3) (2008) 199–215.
[6] M. Christopoulou, T. Garefalakis, D. Panario, D. Thomson, Gauss periods as constructions of low complexity normal bases, Des. Codes Cryptogr., doi:10.1007/s10623-011-9490-4, in press.
[7] J.-M. Couveignes, R. Lercier, Elliptic periods for finite fields, Finite Fields Appl. 15 (1) (2009) 1–22.
[8] S. Gao, Normal bases over finite fields, PhD in Combinatorics and Optimisation, University of Waterloo, Waterloo, Ontario, Canada, 1993.
[9] S. Gao, H.W. Lenstra Jr., Optimal normal bases, Des. Codes Cryptogr. 2 (4) (1992) 315–323.
[10] S. Gao, J. von zur Gathen, D. Panario, V. Shoup, Algorithms for exponentiation in finite fields, J. Symbolic Comput. 29 (6) (2000) 879–889.
[11] D. Jungnickel, Finite Fields, Bibliographisches Institut, Mannheim, 1993, Structure and Arithmetics.
[12] D. Jungnickel, T. Beth, W. Geiselmann, A note on orthogonal circulant matrices over finite fields, Arch. Math. (Basel) 62 (2) (1994) 126–133.
[13] D. Jungnickel, A.J. Menezes, S.A. Vanstone, On the number of self-dual bases of GF(q^m) over GF(q), Proc. Amer. Math. Soc. 109 (1) (1990) 23–29.
[14] A. Lempel, M.J. Weinberger, Self-complementary normal bases in finite fields, SIAM J. Discrete Math. 1 (2) (1988) 193–198.
[15] Q. Liao, K. Feng, On the complexity of the normal bases via prime Gauss period over finite fields, J. Syst. Sci. Complex. 22 (3) (2009) 395–406.
[16] Q. Liao, Q. Sun, Normal bases and their dual-bases over finite fields, Acta Math. Sin. (Engl. Ser.) 22 (3) (2006) 845–848.
[17] F.J. MacWilliams, Orthogonal circulant matrices over finite fields, and how to find them, J. Combin. Theory Ser. A 10 (1971) 1–17.
[18] A.M. Masuda, L. Moura, D. Panario, D. Thomson, Low complexity normal elements over finite fields of characteristic two, IEEE Trans. Comput. 57 (7) (2008) 990–1001.
[19] A.J. Menezes, I.F. Blake, S. Gao, R.C. Mullin, S.A. Vanstone, T. Yaghoobian (Eds.), Applications of Finite Fields, Kluwer Academic Publishers, 1993.
[20] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, R.M. Wilson, Optimal normal bases in GF(p^n), Discrete Appl. Math. 22 (2) (1988/89) 149–161.
[21] Y. Nogami, H. Nasu, Y. Morikawa, S. Uehara, A method for constructing a self-dual normal basis in odd characteristic extension fields, Finite Fields Appl. 14 (2008) 867–876.
[22] E.J. Pickett, Construction of self-dual integral normal bases in abelian extensions of finite and local fields, Int. J. Number Theory 6 (7) (2010) 1565–1588.
[23] A. Poli, Constructing SCN bases in characteristic 2, IEEE Trans. Inform. Theory 41 (3) (1995) 790–794.
[24] Z.-X. Wan, K. Zhou, On the complexity of the dual basis of a type I optimal normal basis, Finite Fields Appl. 13 (2) (2007) 411–417.
[25] C.C. Wang, An algorithm to design finite field multipliers using a self-dual normal basis, IEEE Trans. Comput. 38 (10) (1989) 1457–1460.