ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 13 (2007) 635–647

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Finite field arithmetic using quasi-normal bases

Christophe Negre

Équipe DALI, Laboratoire LP2A, Université de Perpignan, 52 avenue P. Alduy, Perpignan, France

Received 3 June 2005; revised 20 September 2006

Available online 13 November 2006

Communicated by Gary L. Mullen

Abstract

Efficient multiplication in finite fields $\mathbb{F}_{q^n}$ requires $\mathbb{F}_q$-bases of low density, i.e., such that the products of the basis elements have a sparse expression in the basis. In this paper we introduce a new family of bases: the quasi-normal bases. These bases generalize the notion of normal bases and provide simple exponentiation to the power q in $\mathbb{F}_{q^n}$. For some extension fields $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, we construct quasi-normal bases of low density.

Keywords: Finite field; Multiplication; Exponentiation; Quasi-normal basis; Density

1. Introduction

Efficient finite field arithmetic is required in various domains concerning information exchange including cryptography [5,9,12] and error correcting codes [4]. For cryptographic applications, efficient field exponentiation is needed for Diffie–Hellman protocols [5] and digital signatures [6], while efficient scalar multiplications on curve are required for efficiently implementing elliptic curve cryptography [9,12].

Field exponentiation can be done with a chain of multiplications and exponentiations to the qth power in $\mathbb{F}_{q^n}$. Similarly in special elliptic curves, such as the Koblitz curves [16], scalar multiplication can be done efficiently by a repeated application of the Frobenius automorphism and point addition. Consequently, the research done to improve the efficiency of these cryptographic protocols deal, in large part, with efficient multiplication and exponentiation to the qth power in $\mathbb{F}_{q^n}$.

E-mail address: christophe.negre@univ-perp.fr.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2006.09.008

Each extension field $\mathbb{F}_{q^n}$ has an underlying structure of $\mathbb{F}_q$-vector spaces. Given an $\mathbb{F}_q$-basis $\mathcal{B} = (B_1, \ldots, B_n)$ of $\mathbb{F}_{q^n}$, an element $U \in \mathbb{F}_{q^n}$ is represented by its coordinates $U = (u_1, \ldots, u_n)$ in $\mathcal{B}$. Following the definition of Silverman in [14,15] we define the *density* $d(\mathcal{B})$ of the basis $\mathcal{B}$ as

$$d(\mathcal{B}) = \frac{1}{n} \sum_{i,j=1,\ldots,n} \omega_{\mathcal{B}}(B_i B_j), \tag{1}$$

where $\omega_{\mathcal{B}}(B_i B_j)$ is equal to the number of non-zero $\lambda_{i,j}(B_\ell)$ of

$$B_i B_j = \sum_{\ell=1}^{n} \lambda_{i,j}(B_\ell) B_\ell. \tag{2}$$

Originally, Silverman used the term *complexity*, but here we prefer to use the term *density* to keep the notion of complexity as the quantity of field operations. When we express multiplication complexity in $\mathbb{F}_{q^n}$ in terms of operations in the field $\mathbb{F}_q$, the complexity is related to basis density: let $U, V \in \mathbb{F}_{q^n}$, the ℓth coordinates of $W = UV$ is equal to $w_\ell = {}^tU \cdot M_{B_\ell} \cdot V$, where the coefficients of the matrix

$$M_{B_\ell} = \left[\lambda_{i,j}(B_\ell)\right]_{i,j=1,\ldots,n}, \tag{3}$$

come from the products (2). Thus we can multiply two elements with at most $n(d(\mathcal{B}) + n)$ multiplications and additions in $\mathbb{F}_q$. Consequently a low density basis ensures a small complexity for finite field multiplication. This motivates the construction of bases of low density. Until now, two types of bases have been studied for finite field arithmetic:

(1) *Polynomial basis.* These bases are of the form $\mathcal{B} = (1, \alpha, \ldots, \alpha^{n-1})$ for $\alpha \in \mathbb{F}_{q^n}$ with minimal polynomial $P \in \mathbb{F}_q[X]$ of degree n. The polynomial basis $\mathcal{B}$ has a low density when the polynomial P is sparse (e.g. binomial, trinomial, etc.). When P is not a binomial, the polynomial bases generally do not give efficient exponentiation to q.

(2) *Normal basis.* These bases are of the form $\mathcal{B}(\zeta) = (\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}})$ where ζ is a normal element of $\mathbb{F}_{q^n}$ (cf. [2]). Normal bases were first introduced by Massey and Omura [11] in 1986. These bases provide a simple exponentiation to q consisting of a simple cyclic shift of the coordinates. During the past 20 years, several theoretical works were done [3,13] concerning the construction of normal bases of low density, and practically for software and hardware implementations [1,8,10,17].

As shown in [2], the density of normal bases is at least $(2n-1)$ and only the density of optimal normal bases [13] reaches this lower bound $(2n-1)$. Gaussian bases are the generalized form of optimal normal bases, they provide low density normal bases when no optimal normal bases exist. Specifically Ash et al. [3] showed the following proposition.

Proposition 1 *(Gaussian bases [3]). Let k be an integer such that $r = kn + 1$ is prime and $\gcd(r, q) = 1$, and let e be the order or q in $(\mathbb{Z}/r\mathbb{Z})^\times$. Let $\mathcal{K}$ be the unique subgroup of $(\mathbb{Z}/r\mathbb{Z})^\times$ of order k. Let $\gamma \in \mathbb{F}_{q^{kn}}$ be a primitive rth roots of the unity. Then*

$$\zeta = \sum_{a \in \mathcal{K}} \gamma^a$$

is a normal element of $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ *if and only if* $\gcd(nk/e, n) = 1$. *If* ζ *is normal, the density of the normal basis generated by* ζ *satisfies* $d(\mathcal{B}(\zeta)) \leqslant (k+1)n$.

Some questions are still open concerning normal bases. First of all the Gaussian bases are just a partial answer to the problem of constructing normal bases of low density: it can happen, for some n and q, that the smallest k satisfying the hypothesis of Proposition 1 is quite big. Moreover Gaussian bases do not always have the smallest density among all normal bases.

We approached these problems in a different way: we wondered if it was possible to construct bases which have lower density than all normal bases, and yet still provide a simple exponentiation to the qth power. In other words, by slightly relaxing the condition on the high efficiency of the exponentiation to the qth power (i.e., exponentiation could be slightly more complicated than a cyclic shift), could we construct bases with lower density than all normal bases?

Following this idea we introduce a new family of bases: the quasi-normal bases.

2. Quasi-normal bases: Definition and construction

To construct the quasi-normal bases we will use some results concerning the structure of $\mathbb{F}_q[t]$-modules of $\mathbb{F}_{q^n}$. This structure is given by the following action of $Q \in \mathbb{F}_q[t]$ on $U \in \mathbb{F}_{q^n}$

$$Q \cdot U = \left(\sum_{i=0}^{r} \mu_i t^i \right) \cdot U = \sum_{i=0}^{r} \mu_i U^{q^i}.$$

This structure of $\mathbb{F}_q[t]$-modules provides a notion of submodule of $\mathbb{F}_{q^n}$; by definition a submodule H of $\mathbb{F}_{q^n}$ satisfies $H^q = t \cdot H \subset H$. This implies that for every $\zeta \in H$, the elements $\zeta^q, \ldots, \zeta^{q^r}, \ldots$ belong to H. Thus, for $\zeta \in H$, if the system $\mathcal{B}_H(\zeta) = (\zeta, \zeta^q, \ldots, \zeta^{q^{\dim H - 1}})$ is linearly independent, we could call such basis of H a *normal basis* of H.

We consider a decomposition of $\mathbb{F}_{q^n}$ as direct sum of submodules

$$\mathbb{F}_{q^n} = \bigoplus_{i=0}^{n} H_i.$$

The quasi-normal basis associated to such decomposition is simply the union of the normal bases of each submodule H_i of the decomposition.

Definition 1. Let $\mathbb{F}_{q^n}$ be a finite field.

(1) Let H be a submodule of $\mathbb{F}_{q^n}$ and $\zeta \in H$. A basis of the form $\mathcal{B}_H(\zeta) = (\zeta, \zeta^q, \ldots, \zeta^{q^{\dim H - 1}})$ is called a normal basis of H.
(2) Let $\mathbb{F}_{q^n} = \bigoplus_{i=1}^{k} H_i$ be a submodule decomposition of $\mathbb{F}_{q^n}$ and let $\zeta_i \in H_i$ such that $\mathcal{B}_{H_i}(\zeta_i)$ is a normal basis of H_i. We define the quasi-normal basis of $\mathbb{F}_{q^n}$ associated to this submodule decomposition of $\mathbb{F}_{q^n}$ and elements ζ_i as

$$\mathcal{B} = \big(\mathcal{B}_{H_1}(\zeta_1), \ldots, \mathcal{B}_{H_k}(\zeta_k)\big).$$

The notion of quasi-normal basis generalizes the notion of normal basis. Indeed, in the particular case where the submodule $\mathbb{F}_{q^n}$ is decomposed as a sum of only one submodule, $\mathbb{F}_{q^n}$ itself, the corresponding quasi-normal basis is a normal basis of $\mathbb{F}_{q^n}$.

This ensures the existence of a quasi-normal basis for every finite field extension since it has been shown in [7] that there exists a normal basis in every field $\mathbb{F}_{q^n}$.

Now let us go through the problem of constructing the general form of a quasi-normal basis. We need to decompose $\mathbb{F}_{q^n}$ as a direct sum of submodules and then construct a normal basis for each submodule of the decomposition. We restrict $\gcd(q,n)=1$ for simplification. We will use in the sequel the following facts:

- a submodule H is irreducible if any submodule of H is equal to 0 or to H;
- the polynomial $\mathbf{Ann}(H) \in \mathbb{F}_q[t]$ of a submodule H is the generator of the ideal $\mathrm{Ann}(H) = \{P \in \mathbb{F}_q[t] \mid P \cdot H = 0\} \subset \mathbb{F}_q[t]$;
- the nullspace of a polynomial $P \in \mathbb{F}_q[t]$ is the submodule $\mathrm{Null}(P) = \{U \in \mathbb{F}_{q^n} \mid P \cdot U = 0\}$.

The following theorem (cf. [2, Lemma 4.8]) will enable us to decompose $\mathbb{F}_{q^n}$ as a sum of submodules.

Theorem 1 *(Irreducible decomposition [2]). Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be a finite field extension. Under the hypothesis* $\gcd(n,q)=1$ *and if $t^n - 1 = \Phi_1 \Phi_2 \cdots \Phi_r$ with Φ_i irreducible, we have*:

(1) *Any irreducible submodule I of $\mathbb{F}_{q^n}$ is the nullspace of an irreducible factor Φ_i of $t^n - 1$*

$$I \text{ irreducible } \Rightarrow \exists i \text{ such that } I = \mathrm{Null}(\Phi_i).$$

(2) *If H is an $\mathbb{F}_q[t]$-submodule of $\mathbb{F}_{q^n}$ and $\Theta = \mathbf{Ann}(H)$ there exists a subset $\{i_1, \ldots, i_k\} \subset \{1, \ldots, r\}$ such that*

$$\Theta = \prod_{l=1}^{k} \Phi_{i_l}, \qquad I_{i_l} = \mathrm{Null}(\Phi_{i_l}) \quad \text{and} \quad H = \bigoplus_{l=1}^{k} I_{i_l}.$$

Furthermore we have $\dim H = \deg \Theta$.

From Theorem 1 and from the factorization of $t^n - 1 = \prod_{i=1}^{r} \Phi_i$ we can decompose $\mathbb{F}_{q^n}$ as a sum of irreducible submodules

$$\mathbb{F}_{q^n} = I_1 \oplus I_2 \oplus \cdots \oplus I_r.$$

Each I_i is the kernel of the $\mathbb{F}_q$-linear application $U \mapsto \Phi_i \cdot U$. Thus we can explicitly compute a basis of each submodule. Next, by regrouping the submodules I_i in different packages, we obtain different decompositions of $\mathbb{F}_{q^n}$ as a direct sum of submodules that are not necessarily irreducible. In other words, with a partition of $\{1, \ldots, r\}$ given by k sets $\mathcal{S}_1, \ldots, \mathcal{S}_k$, we construct the following k submodules of $\mathbb{F}_{q^n}$

$$H_j = \bigoplus_{i \in \mathcal{S}_j} I_i \quad \text{for } j = 1, \ldots, k.$$

The corresponding decomposition of $\mathbb{F}_{q^n}$ is then

$$\mathbb{F}_{q^n} = H_1 \oplus H_2 \oplus \cdots \oplus H_k.$$

The next step in the construction of quasi-normal basis consists to find normal bases $\mathcal{B}_{H_i}$ for each $\mathbb{F}_q[t]$-submodule of H_i. By regrouping all these bases we will obtain a quasi-normal basis of $\mathbb{F}_{q^n}$

$$\mathcal{B} = (\mathcal{B}_{H_1}, \mathcal{B}_{H_2}, \ldots, \mathcal{B}_{H_k}).$$

We use the following proposition, which is Corollary 4.13 of [2].

Proposition 2. *Let $\mathbb{F}_{q^n}$ be a finite field such that* $\gcd(q, n) = 1$. *Let H be an $\mathbb{F}_q[t]$-submodule of $\mathbb{F}_{q^n}$, $H = \bigoplus_{\ell=1}^{k} I_{i_\ell}$ be the irreducible decomposition of H given in Theorem* 1 *and $\zeta = \sum_{\ell=1}^{k} \zeta_{i_\ell}$ with $\zeta_{i_\ell} \in I_{i_\ell}$. Then $H = \mathbb{F}_q[t] \cdot \zeta = \{Q \cdot \zeta \mid Q \in \mathbb{F}_q[X]\}$ if and only if $\zeta_{i_\ell} \neq 0$ for each ℓ.*

Such an element ζ of a submodule H is usually called a generator of H.

The previous proposition induces the following lemma concerning a normal basis of a submodule of $\mathbb{F}_{q^n}$.

Lemma 1. *Let $\mathbb{F}_{q^n}$ be a finite field such that* $\gcd(q, n) = 1$. *Let H be an $\mathbb{F}_q[t]$-submodule of $\mathbb{F}_{q^n}$ and $\zeta \in H$ such that $\mathbb{F}_q[t] \cdot \zeta = H$. Then the following system of vectors*

$$\mathcal{B}(H) = \left(\zeta, \zeta^q, \ldots, \zeta^{q^{\dim H - 1}}\right)$$

forms a basis of H.

Proof. Let $\zeta \in H$ such that $\mathbb{F}_q[t] \cdot \zeta = H$. We denote $\Theta = \mathbf{Ann}(H)$ and $c = \dim H$. From Theorem 1 we know that $c = \deg \Theta$.

To prove that the system of vectors $\mathcal{B}_H(\zeta) = (\zeta, \zeta^q, \ldots, \zeta^{q^{c-1}})$ is a basis of H it is sufficient to check that $\mathcal{B}_H(\zeta)$ is linearly independent: $\mathcal{B}_H(\zeta)$ is constituted by $c = \dim H$ elements, if $\mathcal{B}_H(\zeta)$ is linearly independent, it is by necessity a generator.

If the system $\mathcal{B}_H(\zeta)$ is linearly dependent, there exists a relation

$$\alpha_0 \zeta + \alpha_1 \zeta^q + \cdots + \alpha_{c-1} \zeta^{q^{c-1}} = 0. \tag{4}$$

If we define $Q = \sum_{i=0}^{c-1} \alpha_i t^i$, we have $Q \cdot \zeta = 0$. Let us show that $Q \cdot U = 0$ for every $U \in H$. By hypothesis ζ generates H, this means that for each $U \in H$ there exists $S_U \in \mathbb{F}_q[t]$ such that $U = S_U \cdot \zeta$. This implies

$$Q \cdot U = Q \cdot (S_U \cdot \zeta) = S_U \cdot (Q \cdot \zeta) = 0.$$

Finally, we have $Q \in \mathrm{Ann}(H) = (\Theta)$ with $\deg Q < c = \deg \Theta$. The polynomial Q is then nothing else than 0 and the relation (4) is trivial. The system $\mathcal{B}_H(\zeta)$ is thus an $\mathbb{F}_q$-basis of H. □

In the sequel we will call an irreducible quasi-normal basis (IQNB) a quasi-normal basis associated to the decomposition $\mathbb{F}_{q^n} = \bigoplus_{i=1}^{r} I_i$ where the I_i are all irreducible.

Example 1. Let $\mathbb{F}_{7^4} = \mathbb{F}_7[X]/(X^4 + X + 1)$ be the field extension over $\mathbb{F}_7$ of degree 4. First, we factor $t^4 - 1$,

$$t^4 - 1 = (t-1)(t+1)\big(t^2+1\big).$$

We construct the two following quasi-normal bases of $\mathbb{F}_{7^4}$.

(1) We construct an IQNB of $\mathbb{F}_{7^4}$: we fix the following generators ζ_1 of $\mathrm{Null}(t-1)$, ζ_2 of $\mathrm{Null}(t+1)$ and ζ_3 of $\mathrm{Null}(t^2+1)$

$$\zeta_1 = 1, \qquad \zeta_2 = 6X^3 + X^2 + 5X + 1, \qquad \zeta_3 = 3X^2 + X.$$

In this situation, the IQNB of $\mathbb{F}_{7^4}$ is $\mathcal{B} = (\zeta_1, \zeta_2, \zeta_3, \zeta_3^7)$.

(2) We consider the decomposition $\mathbb{F}_{7^4} = H_1 \oplus H_2$ where

$$H_1 = \mathrm{Null}(t+1),$$
$$H_2 = \mathrm{Null}(t-1) \oplus \mathrm{Null}\big(t^2+1\big).$$

We determine a generator of H_1 and H_2: for $H_1 = \mathrm{Null}(t+1)$ we can still take ζ_2. To construct ζ the generator of H_2 we use the generators of $\mathrm{Null}(t-1)$ and $\mathrm{Null}(t^2+1)$ found previously,

$$\zeta = \zeta_1 + \zeta_3.$$

From Proposition 2, ζ is a generator of H_2. Finally, the quasi-normal basis associated to ζ_1 and ζ is $\mathcal{B} = (\zeta_2, \zeta, \zeta^7, \zeta^{7^2})$.

3. Exponentiation to q in a quasi-normal basis

In this section, we study the exponentiation to q in $\mathbb{F}_{q^n}$ when the field elements are given in a quasi-normal basis representation.

Let $\mathcal{B}$ be a quasi-normal basis of $\mathbb{F}_{q^n}$ associated to the decomposition $\mathbb{F}_{q^n} = \bigoplus_{i=1}^{k} H_i$ and to the generators ζ_i of H_i. Let $U = U_1 + \cdots + U_k \in \mathbb{F}_{q^n}$ be a field element, where $U_i \in H_i$. If we exponentiate U to q we obtain

$$U^q = U_1^q + \cdots + U_k^q.$$

Since H_i is an $\mathbb{F}_q[t]$-module, we have $U_i^q \in H_i$. Hence, the computation of U^q is reduced to express the coefficients of U_i^q in $\mathcal{B}_{H_i}(\zeta_i)$ in term of the coefficients of U_i in $\mathcal{B}_{H_i}(\zeta_i)$ for $i = 1, \ldots, k$.

Let $c_i = \dim H_i$ and $\Theta_i = \sum_{j=0}^{c_i-1} \alpha_j t^j + t^{c_i} = \mathbf{Ann}(H_i)$ and let $U_i = \sum_{j=0}^{c_i-1} u_{i,j} \zeta_i^{q^j}$ be the expression of U_i in the basis $\mathcal{B}_{H_i}(\zeta_i)$.

As $\Theta_i = \mathbf{Ann}(H_i)$ and $\zeta_i \in H_i$ we have $\Theta_i \cdot \zeta_i = 0$. This implies

$$\zeta_i^{q^{c_i}} = -\sum_{j=0}^{c_i-1} \alpha_j \zeta_i^{q^j}. \tag{5}$$

We deduce that

$$U_i^q = u_{i,0}\zeta_i^q + u_{i,1}\zeta_i^{q^2} + \cdots + u_{i,c_i-2}\zeta_i^{q^{c_i-1}} - u_{i,c_i-1}\big(\alpha_0\zeta_i + \alpha_1\zeta_i^q + \cdots + \alpha_{c_i-1}\zeta_i^{q^{c_i-1}}\big). \quad (6)$$

The exponentiation to the qth power of the U_i consists of a right-shift of the coefficients of U_i and a subtraction of u_{c_i-1}-times the constant vector $(\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{c_i-1})$.

Thus the cost of the exponentiation to the qth power of U in quasi-normal bases is reduced to n multiplications and n additions in the ground field. It is slightly more complicated than an exponentiation to the qth power in normal bases, but it remains quite simple.

4. Multiplication in quasi-normal basis

In this section we will present a possible simplification of the multiplication process when we use a quasi-normal basis. Let us note $\mathrm{Coeff}(W, \zeta_i^{q^j})$ the coefficient of W corresponding to the basis element $\zeta_i^{q^j}$.

Recall that to multiply two elements $U, V \in \mathbb{F}_{q^n}$ we compute the n coefficients $\mathrm{Coeff}(W, \zeta_i^{q^j})$ of $W = UV$ as

$$\mathrm{Coeff}\big(W, \zeta_i^{q^j}\big) = U \cdot M_{\zeta_i^{q^j}} \cdot V$$

where the matrices $M_{\zeta_i^{q^j}}$ are defined in Eq. (3) of Section 1.

Lemma 2. *Let W be an element of $\mathbb{F}_{q^n}$ and $\mathcal{B}$ be a quasi-normal basis of $\mathbb{F}_{q^n}$. The following identity holds for $j < c_i - 1$*

$$\mathrm{Coeff}\big(W, \zeta_i^{q^j}\big) = \mathrm{Coeff}\big(W^{q^{c_i-1-j}}, \zeta_i^{q^{c_i-1}}\big) + \sum_{\ell=0}^{c_i-2-j} \alpha_{j+\ell+1}\,\mathrm{Coeff}\big(W^{q^\ell}, \zeta_i^{q^{c_i-1}}\big) \quad (7)$$

with α_i as defined in Eq. (5).

Proof. From Eq. (6) we have for each $U \in \mathbb{F}_{q^n}$

$$\mathrm{Coeff}\big(U, \zeta_i^{q^j}\big) = \mathrm{Coeff}\big(U^q, \zeta_i^{q^{j+1}}\big) + \alpha_{j+1}\,\mathrm{Coeff}\big(U, \zeta_i^{q^{c_i-1}}\big). \quad (8)$$

We construct the relations of the lemma as follows: we first begin with Eq. (8) for $U = W$

$$\mathrm{Coeff}\big(W, \zeta_i^{q^j}\big) = \mathrm{Coeff}\big(W^q, \zeta_i^{q^{j+1}}\big) + \alpha_{j+1}\,\mathrm{Coeff}\big(W, \zeta_i^{q^{c_i-1}}\big).$$

Then we use Eq. (8) for $U = W^q$ and we replace $\mathrm{Coeff}(W^q, \zeta_i^{q^{j+1}})$ by $\mathrm{Coeff}(W^{q^2}, \zeta_i^{q^{j+2}}) + \alpha_{j+2}\,\mathrm{Coeff}(W^q, \zeta_i^{q^{c_i-1}})$, we get

$$\mathrm{Coeff}\big(W, \zeta_i^{q}\big) = \mathrm{Coeff}\big(W^{q^2}, \zeta_i^{q^{j+2}}\big) + \alpha_{j+1}\,\mathrm{Coeff}\big(W, \zeta_i^{q^{c_i-1}}\big) + \alpha_{j+2}\,\mathrm{Coeff}\big(W^q, \zeta_i^{q^{c_i-1}}\big).$$

Next we replace $\mathrm{Coeff}(W^{q^2}, \zeta_i^{q^{j+2}})$ using Eq. (8) applied to $U = W^{q^2}$ and we get

$$\begin{aligned}\operatorname{Coeff}\bigl(W,\zeta_i^q\bigr) &= \operatorname{Coeff}\bigl(W^{q^3},\zeta_i^{q^{j+3}}\bigr)+\alpha_{j+3}\operatorname{Coeff}\bigl(W^{q^2},\zeta_i^{q^{c_i-1}}\bigr)\\ &\quad+\alpha_{j+2}\operatorname{Coeff}\bigl(W^{q},\zeta_i^{q^{c_i-1}}\bigr)+\alpha_{j+1}\operatorname{Coeff}\bigl(W,\zeta_i^{q^{c_i-1}}\bigr).\end{aligned}$$

We proceed in this way repetitively and we get Eq. (7). □

Let us see now how to use this result in the multiplication process. Let $W = UV$ be the product of $U, V \in \mathbb{F}_{q^n}$. For each $j = 1, \ldots, c_i - 1$ we have $W^{q^j} = U^{q^j} V^{q^j}$, thus for $j = 1, \ldots, c_i$ Eq. (7) gives us

$$\operatorname{Coeff}\bigl(W,\zeta_i^{q^j}\bigr) = {}^tU^{q^{c_i-1-j}}\cdot M_{\zeta_i^{q^{c_i-1}}}\cdot V^{q^{c_i-1-j}} + \sum_{\ell=0}^{c_i-2-j}\alpha_{j+\ell+1}\,{}^tU^{q^\ell}\cdot M_{\zeta_i^{q^{c_i-1}}}\cdot V^{q^\ell}. \quad (9)$$

In consequence, to multiply two elements

- we first compute the products $U^{q^\ell}\cdot M_{\zeta_i^{q^{c_i-1}}}\cdot V^{q^\ell}$ for $\ell = 1, \ldots, c_i - 1$,
- and then we can compute $\operatorname{Coeff}(W, \zeta_i^{q^j})$ for $j = 0, \ldots, c_i - 1$.

Using this strategy, we need only to know the k matrices $M_{\zeta_i^{q^{c_i-1}}}$ to multiply two elements $U, V \in \mathbb{F}_{q^n}$. When the coefficients $\operatorname{Coeff}(W, \zeta_i^{q^j})$ are computed sequentially, this provides a way to avoid part of data storage.

5. Upper bound on irreducible quasi-normal basis density

In this section we will establish an upper bound on the density of irreducible quasi-normal bases. We will see that, in some cases, the upper bound is low, and that the IQNB has low density.

We first need a result concerning the product of submodules.

Lemma 3. *Let H and H' be two $\mathbb{F}_q[t]$-submodules of $\mathbb{F}_{q^n}$. The following subset of $\mathbb{F}_{q^n}$*

$$HH' = \left\{ \sum_{i\in\mathcal{I}, j\in\mathcal{J}} U_i V_j \text{ such that } U_i \in H,\ V_j \in H',\ \text{and } \mathcal{I},\ \mathcal{J} \text{ are finite sets} \right\}$$

is a submodule of $\mathbb{F}_{q^n}$.

Proof. It is clear that HH' is an $\mathbb{F}_q$-sub-vector space of $\mathbb{F}_{q^n}$, thus we have only to check that it is stable under multiplication by t. In other words we have to check that $(HH')^q \subset HH'$. Let $W = \sum_{i\in\mathcal{I}, j\in\mathcal{J}} U_i V_j \in HH'$, then $W^q = \sum_{i\in\mathcal{I}, j\in\mathcal{J}} U_i^q V_j^q$, and since we have $U_i^q \in H$ and $V_j^q \in H'$, $W^q \in HH'$. □

The fact that a product of two submodules remains a submodule implies that it can be decomposed as a direct sum of irreducible submodules. We will use this fact to get the upper bound on the density of the IQNB.

Proposition 3. *Let $\mathcal{B}$ be an IQNB of $\mathbb{F}_{q^n}$ associated to the irreducible decomposition $\mathbb{F}_{q^n} = \bigoplus_{i=1}^{r} I_i$ and to the generators $\zeta_i \in I_i$. If we denote $c_i = \dim I_i$, the density of basis $\mathcal{B}$ satisfies the following inequality*

$$d(\mathcal{B}) \leqslant \frac{1}{n} \sum_{i,j=1,\ldots,r} (c_i c_j)^2. \tag{10}$$

Proof. By definition, the density is given by the following identity (1)

$$d(\mathcal{B}) = \frac{1}{n} \sum_{i,j=1,\ldots,s} \left(\sum_{B \in \mathcal{B}_{I_i}, B' \in \mathcal{B}_{I_j}} \omega_{\mathcal{B}}(BB') \right).$$

To get (10), it is sufficient to prove that $\omega_{\mathcal{B}}(BB') \leqslant c_i c_j$ for each $B \in \mathcal{B}_{I_i}$ and each $B' \in \mathcal{B}_{I_j}$. Here, we have $BB' \in I_i I_j$. If we set $H = I_i I_j$, we know from Lemma 3 that H is a submodule of $\mathbb{F}_{q^n}$. Thus using Theorem 1 we can decompose H as a direct sum of I_{i_ℓ}

$$H = \bigoplus_{\ell=1,\ldots,k} I_{i_\ell}.$$

The non-zero coefficients of $BB' \in H$ in $\mathcal{B}$ correspond to vectors of $\mathcal{B}_{I_{i_\ell}}$ which appear in the decomposition of H. This means that BB' has at most $\dim H \leqslant c_i c_j$ non-zero coefficients, i.e., $\omega_{\mathcal{B}}(BB') \leqslant c_i c_j$. □

Remark 1. Until now, it has not been possible to obtain a similar bound in the case of general quasi-normal bases. However, from experimental results, it seems that the density of general quasi-normal bases has similar upper bounds.

Proposition 3 provides a strategy to construct quasi-normal bases of low complexity. Specifically, it suffices to find the fields $\mathbb{F}_{q^n}$ such that their irreducible submodules I_i have small dimension. The following proposition gives a type of extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with I_i of small dimension.

Proposition 4. *Let $\mathbb{F}_q$ be a finite field, let n be an integer such that $n \mid q^c - 1$ and $\mathbb{F}_{q^n}$ be an extension of degree n of $\mathbb{F}_q$. Then $t^n - 1 = \prod_{i=1}^{r} \Phi_i$, where for all i we have $\deg I_i \leqslant c$, and the irreducible $\mathbb{F}_q[t]$-submodule of $\mathbb{F}_{q^n}$ has an $\mathbb{F}_q$-dimension less than c. The density of every IQNB of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ satisfies*

$$d(\mathcal{B}) \leqslant c^4 n. \tag{11}$$

Proof. From Theorem 1 we know that the irreducible submodules are equal to $\mathrm{Null}(\Phi_i)$ for $i = 1, \ldots, r$ and that they are of dimension $\deg \Phi_i$. It suffices to show for $i = 1, \ldots, r$ that $\deg \Phi_i \leqslant c$.

The polynomial $t^n - 1$ has its roots in $\mathbb{F}_{q^c}$ because $n \mid q^c - 1$ and then $t^n - 1$ splits totally in $\mathbb{F}_{q^c}[t]$. This is also true for the Φ_i since $\Phi_i \mid t^n - 1$. The Φ_i are irreducible in $\mathbb{F}_q[t]$ and totally split in $\mathbb{F}_{q^c}$: they must satisfy $\deg \Phi_i \mid c$.

To prove the upper bound on the density (11) we use the upper bound (10) of Proposition 3

$$d(\mathcal{B}) \leqslant \frac{1}{n} \sum_{i,j=1,\ldots,r} (c_i c_j)^2.$$

Now, as $c_i \leqslant c$ for all i and since $r \leqslant n$, we have

$$d(\mathcal{B}) \leqslant \frac{1}{n}\left(c^4 r^2\right) \leqslant c^4 n. \qquad \square$$

The upper bound on the density in Proposition 3 is quite rough. In some special cases, a refined study of the decomposition of $\mathbb{F}_{q^n}$ with a less rough bound on r, yields the following upper bound

$$d(\mathcal{B}) \leqslant c^2 n.$$

It is this type of upper bound that we are going to establish for $c = 1$ and $c = 2$.

5.1. The case $n \mid q - 1$

From Proposition 4 the polynomials Φ_i all have degree 1 and thus from Theorem 1 irreducible $\mathbb{F}_q[t]$-submodules I_i of $\mathbb{F}_{q^n}$ have dimension 1. First, this implies that all the IQNB are equivalent because the possible choice of $\zeta_i \in I_i$ is reduced to one element, up to a multiplication by a coefficient of $\mathbb{F}_q \setminus \{0\}$.

Second, the upper bound on density of the IQNB given in Proposition 4 becomes

$$d(\mathcal{B}) \leqslant n.$$

In other words, these IQNB reach the minimal bound of density of general bases [14]. But, as shown by Silverman [14] a basis of this type is equivalent to a basis of the form $(1, B, B^2, \ldots, B^{n-1})$ where $B \in \mathbb{F}_{q^n}$ is a root of an irreducible binomial $X^n - \alpha \in \mathbb{F}_q[X]$.

Although this type of irreducible quasi-normal basis corresponds to already known bases, the case of $c = 1$ produces bases which have density less than the density of any normal basis.

The following example illustrates these results.

Example 2. Let $q = 7$ and $n = 3$. We represent $\mathbb{F}_{7^3}$ as $\mathbb{F}_7[X]/(X^3 + X + 1)$.

We factor $t^3 - 1$ and we obtain the irreducible submodules of $\mathbb{F}_{q^n}$

$$\begin{aligned} t^3 - 1 &= (t-1)(t-2)(t-4), \\ I_1 &= \mathrm{Null}(t-1) = \mathrm{Vect}_{\mathbb{F}_7}(1), \\ I_2 &= \mathrm{Null}(t-2) = \mathrm{Vect}_{\mathbb{F}_7}\left(6 + 3X + 2X^2\right), \\ I_3 &= \mathrm{Null}(t-4) = \mathrm{Vect}_{\mathbb{F}_7}\left(4 + X + 6X^2\right). \end{aligned}$$

Here the IQNB chosen is $(\zeta_0, \zeta_1, \zeta_2) = (1, 4 + X + 6X^2, 6 + 3X + 2X^2)$. We can easily show that $\zeta_1^2 = 6\zeta_2$ and that ζ_1 is a root of $X^3 - 3 = 0$. Thus the IQNB $(\zeta_0, \zeta_1, \zeta_2)$ is equivalent to $(1, \zeta_1, \zeta_1^2)$.

5.2. The case $n \mid q^2 - 1$

For simplification, we restrict ourselves to the case $\gcd(n, q-1) = 1$. In this situation, we have the following lemma, which is an improved version of Proposition 4.

Lemma 4. *Let $\mathbb{F}_q$ be a finite field with q elements and let n be an odd integer dividing $q+1$. Then we have the following factorization*

$$t^n - 1 = (t-1) \prod_{i=1}^{\frac{n-1}{2}} \Phi_i$$

where the Φ_i are irreducible of degree 2 and have a constant coefficient equal to 1. Moreover if $\mathcal{B}$ is an IQNB of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ we have

$$d(\mathcal{B}) \leqslant 4(n-1) + \frac{1}{n}.$$

Proof. The factorization form $t^n - 1$ comes from the conditions on the integer n. Indeed, $t^n - 1$ cannot have roots in $\mathbb{F}_q$ except 1 because $\gcd(n, q-1) = 1$. On the other hand, the roots of $t^n - 1$ are all in $\mathbb{F}_{q^2}$ because $n \mid (q+1)(q-1) = q^2 - 1$.

Moreover, if $\rho \in \mathbb{F}_{q^2}$ is a root of $\Phi_i \in \mathbb{F}_q[t]$, the constant coefficient of Φ_i is equal to the norm of ρ

$$N_{q^2 \mid q}(\rho) = \rho \rho^q.$$

But $\rho\rho^q$ is an nth root of unity in $\mathbb{F}_q$, and thus is equal to 1.

We shall now establish the upper bound on density. We denote $I_0, \ldots, I_{\frac{n-1}{2}}$ the irreducible submodules of $\mathbb{F}_{q^n}$, with $I_0 = \mathrm{Null}(t-1)$ and $c_i = \dim(I_i)$. We have $c_0 = 1$ and $c_i = 2$ for $i \geqslant 1$.

We use the upper bound given in Proposition 3

$$d(\mathcal{B}) \leqslant \frac{1}{n} \sum_{i,j=0,\ldots,\frac{n-1}{2}} c_i c_j.$$

We split the sum of the right side into a sum which contains the product $c_0 c_j$ and $c_i c_0$, and a second sum which contains the $c_i c_j$ with $i, j \neq 0$

$$d(\mathcal{B}) \leqslant \frac{1}{n} \left(c_0^2 + 2 \sum_{j=1,\ldots,\frac{n-1}{2}} (c_0 c_j)^2 + \sum_{i,j=1,\ldots,\frac{n-1}{2}} (c_i c_j)^2 \right).$$

We then replace c_0 and c_i with their respective values obtaining the expected upper bound

$$d(\mathcal{B}) \leqslant \frac{1}{n} \left(1 + 4(n-1) + 4(n-1)^2\right) \leqslant 4(n-1) + \frac{1}{n}. \qquad \square$$

From this result and from Proposition 1 of Section 1 if we consider field extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, with $n \mid q^2-1$, which has no Gaussian bases with a $k \leqslant 4$, the IQNB of $\mathbb{F}_{q^n}$ has a smaller density than Gaussian bases.

The following example provides an illustration of this situation.

Example 3. Let $q = 13$ and $n = 7$, and let the field $\mathbb{F}_{13^7}$ defined as $\mathbb{F}_{13}[X]/(X^7 + 10X + 1)$. In order to construct an IQNB of $\mathbb{F}_{13^7}$ over $\mathbb{F}_{13}$ we factor $t^7 - 1$ in $\mathbb{F}_{13}[t]$

$$t^7 - 1 = (t+12)\big(t^2+3t+1\big)\big(t^2+5t+1\big)\big(t^2+6t+1\big).$$

We deduce the irreducible submodules I_i and we choose a generator ζ_i for each H_i

$$\begin{aligned}
&I_0 = \mathrm{Null}(t-1) = \mathrm{Vect}_{\mathbb{F}_{13}}(1),\\
&I_1 = \mathrm{Null}\big(t^2+3t+1\big) = \mathbb{F}_{13}[t]\cdot(\zeta_1),\\
&\quad \text{where } \zeta_1 = 3X^6 + 2X^5 + 9X^4 + 9X^3 + 5X^2 + 4X + 9,\\
&I_2 = \mathrm{Null}\big(t^2+5t+1\big) = \mathbb{F}_{13}[t]\cdot(\zeta_2),\\
&\quad \text{where } \zeta_2 = 11X^6 + 7X^4 + 11X^3 + 5X^2 + 2X + 7,\\
&I_3 = \mathrm{Null}\big(t^2+6t+1\big) = \mathbb{F}_{13}[t]\cdot(\zeta_3),\\
&\quad \text{where } \zeta_3 = 6X^5 + 2X^4 + X^3 + 2X^2 + 9X.
\end{aligned}$$

The quasi-normal basis is equal to $\mathcal{B} = (1, \zeta_1, \zeta_1^{13}, \zeta_2, \zeta_2^{13}, \zeta_3, \zeta_3^{13})$. Now to get the density of this basis we express each product $\zeta_i^{q^{i'}}\zeta_j^{q^{j'}}$ in the basis $\mathcal{B}$. We can construct the matrices of multiplication $M_{\zeta_\ell^{q^i}}$ defined in (3) in the introduction. Here we only give M_{ζ_1} and $M_{\zeta_1^{13}}$.

$$M_{\zeta_1} = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 0 & 0 & 8 & 12\\
0 & 0 & 0 & 0 & 0 & 0 & 2\\
0 & 0 & 0 & 2 & 10 & 10 & 2\\
0 & 0 & 0 & 10 & 0 & 4 & 0\\
0 & 8 & 0 & 10 & 4 & 0 & 0\\
0 & 12 & 2 & 2 & 0 & 0 & 0
\end{bmatrix}, \qquad
M_{\zeta_1^{13}} = \begin{bmatrix}
0 & 0 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 11 & 12\\
1 & 0 & 0 & 0 & 0 & 5 & 1\\
0 & 0 & 0 & 0 & 10 & 0 & 4\\
0 & 0 & 0 & 10 & 2 & 2 & 10\\
0 & 11 & 5 & 0 & 2 & 0 & 0\\
0 & 12 & 1 & 4 & 10 & 0 & 0
\end{bmatrix}.$$

Table 1
Density of QNB types

Type of decomposition	Minimal density
4 submodules (IQNB)	$\frac{118}{7} \cong 16.9$
3 submodules	$\frac{190}{7} \cong 27.14$
2 submodules	$\frac{134}{7} \cong 19.14$
1 submodules (NB)	$\frac{175}{7} \cong 25$

The density of this basis $\mathcal{B}$ is equal to $\frac{118}{7}$. To complete this example in Table 1 we give the minimal density of quasi-normal bases depending on the associated decomposition of the module $\mathbb{F}_{q^n}$ as a sum of submodules.

This illustrates the fact that we can construct IQNB of densities smaller than the densities of every normal basis of $\mathbb{F}_{13^7}$.

6. Conclusion

In this article, we introduced quasi-normal bases. They are a new family of $\mathbb{F}_q$-bases of finite field $\mathbb{F}_{q^n}$ which generalizes the notion of normal bases. These bases provide an exponentiation to the qth power in $\mathbb{F}_{q^n}$ in a simple way, although not as simple as in normal bases. We also stated an upper bound on the density on a special family of quasi-normal bases: the irreducible quasi-normal bases. In particular, for field extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of odd degree n dividing $(q+1)$, we established the following inequality

$$d(\mathcal{B}) \leqslant 4n.$$

In conclusion, with regard to density, quasi-normal bases could provide a good alternative to normal bases for fields $\mathbb{F}_{q^n}$ which have no normal bases of low complexity. But the results of this paper remain theoretical. A work concerning implementation of quasi-normal bases should be done in the future to make this quasi-normal basis approach efficient in practice.

References

[1] G. Agnew, R. Mullin, S. Vanstone, An implementation for a fast public key cryptosystem, IEEE J. Cryptology 3 (1991) 63–79.
[2] A.J. Menezes, I.F. Blake, S. Gao, R.C. Mullin, S.A. Vanstone, T. Yaghoobian, Applications of Finite Fields, Kluwer Internat. Ser. Engrg. Comput. Sci., vol. 199, Kluwer Acad. Publ., 1993.
[3] D.W. Ash, I.F. Blake, S.A. Vanstone, Low complexity normal bases, Discrete Appl. Math. 25 (1989).
[4] E.R. Berlekamp, Bit-serial Reed–Solomon encoder, IEEE Trans. Inform. Theory IT-28 (1982).
[5] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 24 (1976) 644–654.
[6] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory 32 (1985) 469–472.
[7] S. Gao, D. Panario, Density of normal elements, Finite Fields Appl. 3 (1997) 141–150.
[8] M.A. Hasan, M.Z. Wang, V.K. Bhargava, A modified Massey–Omura parallel multiplier for a class of finite fields, IEEE Trans. Comput. 42 (10) (1993) 1278–1280.
[9] N. Koblitz, Elliptic curve cryptosystems, Math. Comp. 48 (1987) 203–209.
[10] C.K. Koc, B. Sunar, An efficient optimal normal basis type II multiplier, IEEE Trans. Comput. 50 (1) (2001).
[11] J.L. Massey, J.K. Omura, Computational method and apparatus for finite field arithmetic, May 1986. US Patent, Nos. 4, 587, 627.
[12] V. Miller, Use of elliptic curves in cryptography, in: Advances in Cryptology, Proceedings of CRYPTO'85, in: Lecture Notes in Comput. Sci., vol. 218, Springer, 1986, pp. 417–426.
[13] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, R.M. Wilson, Optimal normal bases in GF(p^n), Discrete Appl. Math. 22 (2) (1989) 149–161.
[14] J.H. Silverman, Low complexity multiplication in rings, Technical report, Brown University, April 1999.
[15] J.H. Silverman, Fast multiplication in finite fields gf($2n$), in: CHES '99: Proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems, Springer, London, UK, 1999, pp. 122–134.
[16] N.P. Smart, Elliptic curves over small fields of odd characteristic, J. Cryptology 12 (2) (1999) 141–151.
[17] Y.L. Yin, P. Ning, Efficient software implementation for finite field multiplication in normal basis, in: Proceedings of the 3rd International Conference on Information and Communication Security (ICICS-01), November 2001, pp. 177–188.