A deterministic algorithm for computing a normal basis in a finite field

D. Augot *P. Camion†

Abstract

We describe a *deterministic* algorithm for computing a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The number of arithmetic $\mathbb{F}_q$-operations needed to perform the computation is $O(n^3 + n^2 \log q)$. This algorithm is better than any previously known deterministic one, and compares well with probabilistic algorithms. Our method is heavily based on linear algebra techniques.

1 Introduction

Let $\mathbb{F}_{q^n}$ denote the finite field of size q^n, and let σ be the Frobenius automorphism, $\sigma(x) = x^q$.

Definition 1 *An element $\alpha \in GF(q^n)$ is said to be* normal *if $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ form a basis of $GF(q^n)$ over $GF(q)$. A set $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ which is a basis of $GF(q^n)$ over $GF(q)$ is a* normal basis.

Normal bases can be used for implementing the arithmetic of finite fields. The significance of normal bases is mainly due to the fact that exponentiation is cheap when using a normal basis [1]. The reader is informed that *low-complexity* [2] normal bases are not sought for in this paper.

We consider the problem as a linear algebra problem. It is the problem of finding a cyclic vector for a given matrix. Let us recall a few definitions.

Definition 2 *Let $A \in M_n(\mathbf{k})$ be a linear operator over a field $\mathbf{k}$. The minimal polynomial of A relatively to a vector $v \in \mathbf{k}^n$ is the lowest degree monic polynomial $\pi_v(X)$ such that $\pi_v(A)v = 0$. Let $\pi(X)$ denote the minimal polynomial of matrix A, a vector $v \in \mathbf{k}^n$ is said to be* cyclic *if $\pi_v(X) = \pi(X)$.*

Theorem 1 ([5]) *Let $A \in M_n(\mathbf{k})$, there exists a cyclic vector for A.*

A normal element for $GF(q^n)$ is a cyclic vector for the matrix representing the Frobenius automorphism. We first consider the case where n is prime to

*INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex
†CNRS, INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex

q. The minimal polynomial of the Frobenius automorphism is $X^n - 1$ which in this case is a square-free polynomial.

The algorithm presented here computes a cyclic vector of an operator $A \in M_n(\mathbf{k})$ whose characteristic polynomial is square-free. The complexity of this algorithm is $O(n^3)$, and thus the cost of computing a normal basis is $O(n^3 + n^2 \log q)$, counting $O(n^3 + n^2 \log q)$ for computing a matrix representing the Frobenius automorphism.

We recall that Bach, Driscoll et Shallit have presented an algorithm of complexity $O((n^2 + \log q)(n \log q)^2)$ in terms of the number of bit operations, and H. W. Lenstra has presented an algorithm of the same complexity [4].

2 A useful lemma

We try to find a cyclic vector by elementary operations on the rows and the columns of the matrix A (linear combinations and permutations). The aim is to find a companion matrix similar to A. However, this is not always straightforward, and the following form of matrix may occur.

Definition 3 *A matrix $H \in M_n(\mathbf{k})$ is said to be a* Shift-Hessenberg matrix *if it has the form:*

$$H = (h_{i,j}) = \begin{bmatrix} & & \times & & & \times & & \times \\ 1 & & \times & & & \times & & \times \\ & 1 & \times & & & \times & & \times \\ & & 0 & & & \times & & \times \\ & & & 1 & & \times & & \times \\ & & & & \ddots & \times & & \\ & & & & 1 & \times & & \times \\ & & & & & 0 & & \times \\ & & & & & & 1 & \times \\ & & & & & & \ddots & \\ & & & & & & & \times \end{bmatrix}$$

i.e. $h_{i,j} = 0$ if $i > j+1$, and $(h_{i+1,i} \neq 0) \Rightarrow (h_{i+1,i} = 1$ and $\forall j \neq i+1,\ h_{j,i} = 0)$.

Proposition 1 *For every matrix $A \in M_n(\mathbf{k})$ there exists a Shift-Hessenberg matrix H and an invertible matrix P such that $H = P^{-1}AP$. Matrix H and matrix P can be obtained in $O(n^3)$ operations in $\mathbf{k}$.*

A Shift-Hessenberg matrix is a slightly modified Hessenberg matrix [6, 3], and the algorithm for computing a Shift-Hessenberg matrix similar to a given matrix is simple. A Shift-Hessenberg can be partitionned as follows.

$$H = \begin{bmatrix} H_{B_1,B_1} & H_{B_1,B_2} & \cdots & H_{B_1,B_m} \\ 0 & H_{B_2,B_2} & \cdots & H_{B_2,B_m} \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & H_{B_m,B_m} \end{bmatrix}.$$

where the matrices H_{B_i,B_i} are companion matrices. If the minimal polynomial of matrix H is square-free, then the minimal polynomials of the matrices H_{B_i,B_i} are pairwise coprime.

If the resulting matrix only has one block, then it is a companion matrix, and the result is found. The next lemma tells that the result can be achieved if there are only two blocks.

Lemma 1 *Let H be a block matrix of the form:*

$$\begin{bmatrix} H_{B_1,B_1} & H_{B_1,B_2} \\ 0 & H_{B_2,B_2} \end{bmatrix} \tag{1}$$

and let v_{B_1}, v_{B_2} be cyclic vectors for H_{B_1,B_1} and H_{B_2,B_2} with minimal polynomials $f_1(X)$ and $f_2(X)$ respectively. If $f_1(X)$ and $f_2(X)$ are coprime, a cyclic vector v for H can be constructed on the data of v_{B_1}, v_{B_2}, at cost $O(n^3)$.

3 A recursive construction

When the Shift-Hessenberg form of A contains more than two blocks, we use Lemma 1 recursively. The strategy is to split the matrix H into a matrix H_{split} of the form (1), such that the sizes of the matrices H_{B_1,B_1} and H_{B_2,B_2} are kept under control.

Lemma 2 (Splitting the matrix) *Let H be a Shift-Hessenberg matrix. It is possible to compute, at cost $O(n^3)$, a Shift-Hessenberg matrix H_{split} and an invertible matrix P such that $H = PH_{split}P^{-1}$, H_{split} of the form*

$$H_{split} = \begin{bmatrix} H'_{B_I,B_I} & H'_{B_I,B_J} \\ 0 & H'_{B_J,B_J} \end{bmatrix}, \tag{2}$$

where H'_{B_I,B_I} and H'_{B_J,B_J} are Shift-Hessenberg matrices, and

1. *either H'_{B_I,B_I} is a single companion block of size $\geq \frac{2}{3}n$ (thus H'_{B_J,B_J} has size $\leq \frac{1}{3}n$).*
2. *either both matrices H'_{B_I,B_I} and H'_{B_J,B_J} have size not greater than $\frac{2}{3}n$.*

For computing a cyclic vector for a matrix A, the algorithm is as follows:

Step 1*: computation of an Shift-Hessenberg form of A. This step needs to be performed only once.

Step 2: splitting the matrix. We perform the splitting showed by Lemma 2, and obtain two submatrices H_{B_I,B_I} and H_{B_J,B_J}. The algorithm is applied recursively on submatrices which are not companion matrices.

Step 3: reconstruction of a cyclic element in a new basis. We have the results returned by our algorithm for the two subcases of H_{split}. By Lemma 1, we can construct a cyclic element v_{split} for H_{split} at cost $O(n^3)$.

Step 4: reconstruction of the cyclic element in the original basis. From a cyclic vector of H_{split}, changing basis gives a cyclic vector for H from the vector v_{split}.

Step 5*: reverting to the original basis. From a cyclic vector for H, we compute a cyclic vector for A by changing basis. This is performed only once, at the end of the algorithm.

Proposition 2 *Let $A \in M_n(\mathbf{k})$ be a matrix whose characteristic polynomial is square-free. A cyclic vector for A can be computed in $O(n^3)$ elementary operations.*

Computing a matrix for the Frobenius automorphism, at cost $O(n^3+n^2 \log q)$ leads to a complexity of $O(n^3 + n^2 \log q)$ for a normal basis in $GF(q^n)$, n prime to q.

In [3], it is shown how to find a normal basis at cost $O(n^3)$ for $GF(q^{p^m})$, where p is the characteristic of $GF(q)$, by computing a Shift-Hessenberg matrix of the Frobenius automorphism. It is known how to compute a normal basis for $GF(q^{n_1 n_2})$, $\gcd(n_1, n_2) = 1$, when normal elements for $GF(q^{n_1})$ and $GF(q^{n_2})$ are known. Consequently, in the general case, a normal basis for $GF(q^n)$ can be found in $O(n^3 + n^2 \log q)$.

The algorithm has been implemented in Axiom, and is superior to the algorithm already implemented, which is a probabilistic algorithm. Computational times are given.

References

[1] G. B. Agnew, T. Beth, R.C. Mullin, and S.A. Vanstone. Arithmetic operations in $GF(2^m)$. *Journal of Cryptology*, 6:3–13, 1993.

[2] D. W. Ash and I. F. Blake and S. A. Vanstone" Low Complexity Normal Bases *Discrete Applied Mathematics* 191–210, 1989.

[3] D. Augot and P. Camion. The minimal polynomials, characteristic subspaces, normal bases and the frobenius form, 1993. *INRIA Research Report, 2006.*

[4] I.F. Blake, X.H. Gao, R.C. Mullin, S.A.Vanstone, and T. Yaghoobian. *Applications of finite fields.* Kluwer Academic Publishers, 1993.

[5] F. R. Gantmacher. *The Theory of Matrices*, volume 1. Chelsea, 1977.

[6] J. H. Wilkinson. *The Algebraic Eigenvalue Problem.* Oxford Science Publications, 1992.