Probabilistic Construction of Normal Basis.
(Note)

Gudmund S. Frandsen

version August 10, 1998

Abstract

Let \( F_q \) be the finite field with \( q \) elements. A normal basis polynomial \( f \in F_q[x] \) of degree \( n \) is an irreducible polynomial, whose roots form a (normal) basis for the field extension \( F_{q^n} : F_q \). We show that a normal basis polynomial of degree \( n \) can be found in expected time \( O(n^{3+\epsilon} \cdot \log(q) + n^{3+\epsilon}) \), when an arithmetic operation and the generation of a random constant in the field \( F_q \) cost unit time.

Given some basis \( B = \{\alpha_1, \alpha_2, ..., \alpha_n\} \) for the field extension \( F_{q^n} : F_q \) together with an algorithm for multiplying two elements in the \( B \)-representation in time \( O(n^\beta) \), we can find a normal basis for this extension and express it in terms of \( B \) in expected time \( O(n^{1+\beta+\epsilon} \cdot \log(q) + n^{3+\epsilon}) \).

CR Categories: F.2.1.

1991 Mathematics Subject Classification: Primary 11Y16; Secondary 11T30.

Related Work.

[BDS90] give a probabilistic construction of a normal basis for \( F_{q^n} : F_q \) for restricted values of \( q \) and \( n \). They use that the ground field \( F_q \) can have at most \( n(n-1) \) elements \( a \) for which

\[
g(a) = \frac{f(a)}{(a - \alpha)f'(\alpha)} \in F_{q^n}
\]

is not a normal basis element, when \( f \) is an arbitrary but fixed irreducible polynomial of degree \( n \) over \( F_q \) and \( \alpha \) is a root of \( f \) [Art48, implicit in proof of theorem 28].

Hence, a random \( a \in F_q \) leads to a normal basis element \( g(a) \in F_{q^n} \) with probability \( \geq \frac{1}{2} \) when \( q > 2n(n-1) \). By our lemma 1 (last part) an arbitrary \( b \in F_{q^n} \) is a normal basis element with probability \( \geq \frac{1}{2} \), under the same restriction. Hence, our construction may also be used in the restricted case without loss of efficiency.

Deterministic constructions can be found in [BDS90, Len91].

---

1This research was supported by the ESPRIT II Basic Research Actions Program of the EC under contract No. 3075 (project ALCOM).
2Department of Computer Science, Aarhus University, Ny Munkegade, 8000 Aarhus C, Denmark. gsfrandsen@daimi.aau.dk
Lemma 1.

Let \( N \) denote the number of normal basis polynomials of degree \( n \) over \( \mathbb{F}_q \). Then

\[
N \geq q^n \cdot \frac{1}{n} \cdot \frac{1}{q} \cdot \frac{1}{(1 + \log_q(n))e}
\]

Under the restriction \( q \geq 2n(n - 1) \), a stronger inequality holds:

\[
N \geq q^n \cdot \frac{1}{n} \cdot \frac{1}{2}
\]

Proof.

If \( f(x) \in \mathbb{F}_q[x] \) and the complete factorisation of \( f(x) \) is \( f(x) = \prod_{i=1}^{l} f_i(x)^{e_i} \) (the irreducible factors \( f_i(x), f_j(x) \) are distinct, when \( i \neq j \)), then define \( \Phi(f(x)) = q^n \prod_{i=1}^{l} (1 - \frac{1}{q^{n_i}}) \), where \( n_i \) is the degree of \( f_i \), and \( n \) is the degree of \( f \).

The relevance of this concept comes from \( N = \frac{1}{n} \Phi(x^n - 1) \) (See [LiNi83]).

To get a lower bound for \( \Phi(f(x)) \), we observe that for a fixed \( n \) the minimal value occurs, when \( f(x) \) is the product of all distinct irreducible factors of degree 1, 2, 3, ..., \( k \) (and some of degree \( k + 1 \)). Noticing, that \( xq^n - x \) factors into distinct irreducible factors, each of which have degree at most \( k \), it follows that \( k \leq \log_q(n) \). Since every irreducible polynomial of degree \( n_i \) divides \( x^{q^{n_i}} - x \), there are at most \( \frac{q^{n_i} - 1}{n_i} \) distinct factors of degree \( n_i \) in \( f(x) \) (except for the \( q \) distinct degree 1 polynomials). Using that

\[
(1 - \frac{1}{q^{n_i}}) \frac{q^{n_i} - 1}{n_i} \geq \left( \frac{1}{e} \right)^{\frac{1}{n_i}}
\]

we find the lower bound

\[
\Phi(f(x)) \geq q^n(1 - \frac{1}{q})\left( \frac{1}{e} \right)^{1 + \log(k+1)} = q^n(1 - \frac{1}{q})\frac{1}{(k+1)e} \geq q^n(1 - \frac{1}{q})\frac{1}{(1 + \log_q(n))e}
\]

which imply the first part of the lemma.

In the remaining part of the proof, we assume that \( q \geq 2n(n - 1) \). For \( n = 1 \), we find that

\[
\Phi(f(x)) \geq q^n(1 - \frac{1}{q}) \geq q^n \frac{1}{2}
\]

which implies the lemma.
For $n = 2$, we know that $q \geq 4$ and we get the bound
\[
\Phi(f(x)) \geq q^n \cdot \left(1 - \frac{1}{q}\right)^2 \geq q^n \left(\frac{3}{4}\right)^2 \geq q^n \frac{1}{2}
\]
For $n \geq 3$, we have that $n \leq (q - 1)/2$ and we get
\[
\Phi(f(x)) \geq q^n \cdot \left(1 - \frac{1}{q}\right)^{n+1} \geq q^n \frac{1}{\sqrt{e}} \geq q^n \frac{1}{2}
\]

Theorem 2.

Given some basis $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ for the field extension $F_{q^n} : F_q$ together with an algorithm for multiplying two elements in the $B$ representation in time $O(n^\beta)$, we can find a normal basis for this extension and express it in terms of $B$ in expected time $O(n^{1+\beta+\epsilon} \cdot \log(q) + n^{3+\epsilon})$.

Proof.

By lemma 1, a fraction $\Omega(\frac{1}{1+\log(n)})$ of the elements in $F_{q^n}$ generate normal bases. Hence, we expect to have to check $O(\log(n))$ random elements in the span of $B$ before finding one that generates a normal basis.

Assume $\alpha = \sum_{i=1}^{n} c_i \alpha_i$, $c_i \in F_q$, then we may compute the representation of $\alpha^q$ in terms of $B$ for all $i$ in time $O(n^{1+\beta} \log(q))$, and hence compute $\alpha^q j$ for all $j$ in time $O(n^3)$. We know that $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$ are linearly independent if and only if $\det(d_{ij}) \neq 0$, where $d_{ij} \in F_q$ is defined by $\alpha^{q^j} = \sum_{i=1}^{n} d_{ij} \alpha_i$.

Hence, we can check an arbitrary $\alpha \in \text{span}(B)$ for the normal basis property in time $O(n^{1+\beta} \log(q) + n^3)$ from which the theorem follows.

Theorem 3.

A normal basis polynomial of degree $n$ over $F_q$ can be found in expected time $O(n^{2+\epsilon} \cdot \log(q) + n^{3+\epsilon})$.

Proof.

There are $\Theta(\frac{q^n}{n})$ irreducible polynomials of degree $n$ over $F_q$. Hence, by lemma 1, we expect to have to check $O(\log(n))$ irreducible polynomials before finding a normal basis polynomial. A random irreducible polynomial $f(x)$ can be found in expected time $O(n^{2+\epsilon} \cdot \log(q))$ (see [Ben81]).
If $\alpha$ is a root of $f(x)$, then $B = \{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is a polynomial basis for $F_{q^n} : F_q$, and we can multiply any two elements in the $B$-representation in time $O(n^{1+\epsilon})$. Using the proof of theorem 2, we can check that $\{\alpha, \alpha^q, ..., \alpha^{q^{n-1}}\}$ form a normal basis in time $O(n^{2+\epsilon} \log(q) + n^3)$ from which the theorem follows.

\[\square\]

References


