Discrete Applied Mathematics 25 (1989) 191–210
North-Holland

LOW COMPLEXITY NORMAL BASES*

David W. ASH, Ian F. BLAKE and Scott A. VANSTONE
University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

Received 24 February 1987
Revised 2 August 1988

A normal basis in GF(q^m) is a basis of the form $\{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{m-1}}\}$, i.e., a basis of conjugate elements in the field. In GF(2^m) squaring with respect to a normal basis representation becomes simply a cyclic shift of the vector. For hardware design this is one of the very attractive features of these bases. Multiplication with respect to a normal basis can be defined in terms of a certain bilinear form. Define the complexity of the normal basis to be the number of nonzero terms in this form. Again, for hardware design, it is important to find normal bases with low complexity. In this paper we investigate low complexity normal bases, give a construction for such bases and apply it to a number of cases of interest.

1. Introduction

Many coding, cryptographic and signal processing techniques require implementation of finite field arithmetic. The realization of arithmetic operations in these structures, in either hardware or software, can often be made more efficient by an astute choice of field representation and operational algorithm. An interesting example of this is the use of a dual basis to achieve an efficient bit serial hardware multiplier for use in Reed–Solomon encoders [2]. The problem is particularly important in the design of integrated circuit chips for multiplication in large finite fields where the simplicity of the algorithm and the minimization of the number of cell interconnections is crucial for a successful design. The particular application of interest is discrete exponentiation in fields of characteristic two for application in data encipherment and public key distribution.

Such practical constraints are often translated into interesting mathematical problems. This paper examines one such problem that arose out of the Massey–Omura multiplication scheme using normal bases [11]. The problem involves the construction of normal bases with certain properties. It is described in the remainder of this section and the known results on it are reviewed. Generalizations of these results are given in the following sections and other aspects of the problem are also considered.

Let $A = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a basis of $V_n(q)$, the vector space of GF(q^n) over GF(q). A is a polynomial basis if $\alpha_i = \alpha^i$ and a normal basis if $\alpha_i = \alpha^{q^i}$, $i = 0, 1, \ldots, n-1$, for some element $\alpha \in$ GF(q). If A is a normal basis, then $\alpha_i = \alpha^{q^i}$ will sometimes be referred to as basis element i, but only in cases where this terminology

* This work was supported by NSERC Grant G-1588.

is unambiguous with respect to which normal basis we are referring to. If B is another basis $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ and $T(\cdot)$ is the trace function of GF(q^n) over GF(q), then B is called the dual basis of A if $T(\alpha_i \beta_j) = \delta_{ij}$, the Kronecker delta function. Every basis has a unique dual basis [10]. If $T(\alpha_i \alpha_j) = \delta_{ij}$, A is called a self-dual basis which will exist [15] iff (i) q is even or (ii) both q and n are odd. A is called a trace orthogonal basis if $T(\alpha_i \alpha_j) = 0$, $i \neq j$ and $T(\alpha^2) \neq 0$ and such a basis always exists for $V_n(q)$.

Normal bases are particularly interesting and it is known that such a basis always exists for $V_n(q)$. In fact a primitive normal basis (all elements of the basis are primitive) always exists [3, 5, 9]. The dual of a normal basis is also normal and when the number of distinct normal bases is odd, such a self-dual normal basis exists. The existence of self-dual normal bases is completely determined, namely they exist over GF(q) iff n is odd or $n \equiv 2 (\mathrm{mod}\, 4)$ and q is even.

Interest in normal bases stems in part from the following multiplication algorithm of Massey and Omura [11]. Let $N = \{\beta, \beta^2, \ldots, \beta^{2^{n-1}}\}$ be a normal basis of GF(2^n) over GF(2) and let $\beta_i = \beta^{2^i}$, $i = 0, 1, \ldots, n-1$. An element $a \in \mathrm{GF}(2^n)$ with the representation

$$a = \sum_{i=0}^{n-1} a_i \beta_i$$

is identified with the vector $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ and it is noted that a^2 has the representation $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$. If

$$b = \sum_{i=0}^{n-1} b_i \beta_i$$

and $c = ab \equiv (c_0, c_1, \ldots, c_{n-1})$ with respect to the basis N, then there exist $\lambda_{ij} \in \mathrm{GF}(2)$ such that

$$c_k = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \lambda_{ij} a_{i+k} b_{j+k}, \quad k = 0, 1, \ldots, n-1,$$

where the subscripts on a and b are taken modulo n. Thus $c_0 = \boldsymbol{a} \lambda \boldsymbol{b}^{\mathrm{T}}$, $\lambda = (\lambda_{ij})$, $\boldsymbol{b}^{\mathrm{T}}$ is the transpose of $\boldsymbol{b}$, and the remaining coefficients of c can be found using the same matrix but with $\boldsymbol{a}$ and $\boldsymbol{b}$ cyclically shifted. In terms of hardware, the circuit to compute c_0 also computes c_k if the registers holding $\boldsymbol{a}$ and $\boldsymbol{b}$ are cyclically shifted k positions to the left.

Define the quantity

$$C_N = |\{(i,j) \mid \lambda_{ij} \neq 0,\ 0 \leq i, j \leq n-1\}|,$$

which will be referred to as the complexity of multiplication with respect to the basis N. For the proofs of results which follow we find it useful to define the following 0-1 matrix associated with the basis N:

$$T = [t_{ij}] \quad \text{where} \quad t_{ij} = \lambda_{(-j)(i-j)}.$$

It is easy to see that the number of ones in the matrix T is equal to C_N. Now, observe that

$$\beta \cdot \beta^{2^l} = \beta_0 \beta_l = \sum_{k=0}^{n-1} c_k \beta_k = \sum_{k=0}^{n-1} \beta_k \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \lambda_{ij} a_{i+k} b_{j+k}$$
$$= \sum_{k=0}^{n-1} \lambda_{(-k)(l-k)} \beta^{2^k} = \sum_{k=0}^{n-1} t_{lk} \beta^{2^k}.$$

Thus, we see that the number of ones in row l of the matrix T (which will henceforth be called the T-matrix) is equal to the number of nonzero terms in the basis representation of basis element l multiplied by basis element 0. This important fact will be used in the sequel whenever we wish to evaluate the complexity of a normal basis N.

Clearly $C_N \leq n^2$ and it has recently been shown that [13] $C_N \geq 2n-1$. In the design of an integrated circuit to implement the multiplication, each nonzero element of λ corresponds to a cell connection and it is important to find bases of low

Table 1. Normal basis search results.

n	# normal bases	min C_N	max C_N
2	1	3*	3
3	1	5*	5
4	2	7*	9
5	3	9*	15
6	4	11*	17
7	7	19	27
8	16	21	35
9	21	17*	45
10	48	19*	61
11	93	21*	61
12	128	23*	83
13	315	45	101
14	448	27*	135
15	675	45	137
16	2048	85	157
17	3825	81	177
18	5376	35*	243
19	13797	117	229
20	24576	63	257
21	27783	95	277
22	95232	63	363
23	182183	45*	325
24	262144	105	375
25	629145	93	383
26	1290240	51*	555
27	1835001	141	443
28	3670016	55*	≥ 515
29	9256395	57*	≥ 505
30	11059200	59*	≥ 587

complexity. Table 1 (from [13]) shows the range of values of complexity for all normal bases of $GF(2^n)$ over GF(2) for $2 \le n \le 27$ with partial results for $n = 28, 29, 30$, all results obtained by computer search. Bases that achieve the minimum complexity possible for any given value of n are referred to as minimal normal bases. If this minimum complexity is, in fact, the theoretical minimum of $2n-1$, the minimal normal basis is called an optimal normal basis. These are marked with an asterisk in the table. It is important to note that for some values of n there does not exist a normal basis that achieves complexity $2n-1$.

Two constructions of optimal normal bases of $GF(2^n)$ over GF(2) are given in [13] and these will be briefly described here as background for the following sections. Suppose that $2n+1$ is a prime and that 2 is a primitive element of $GF(2n+1)$. Since $2n+1 \mid 2^{2n}-1$, $GF(2^{2n})$ contains a primitive $(2n+1)$st root of unity, β, and $N = \{\beta^{2^i} \mid i = 0, 1, \ldots, 2n-1\}$ is an optimal normal basis of $GF(2^{2n})$ over GF(2). Furthermore if

$$\gamma = \beta + \beta^{-1},$$

then $\gamma \in GF(2^n)$ and $N' = \{\gamma^{2^i} \mid 0 \le i \le n-1\}$ is an optimal normal basis of $GF(2^n)$ over GF(2). The idea of this projection mapping will be used effectively in later sections. The same technique also produces an optimal normal basis if $2n+1 \equiv 3 \pmod 4$ and 2 generates the quadratic residues of $GF(2n+1)$. In this case $\beta \in GF(2^n)$ and the mapping is not a projection.

2. General results

The general method of constructing normal bases of low complexity used in this paper is as follows: To find a normal basis for $GF(2^n)$, select a (relatively small) integer k such that $kn+1$ is a prime. Under certain conditions there will exist $\beta \in GF(2^{kn})$, $\beta \neq 1$ and $\beta^{kn+1} = 1$. Then by applying a trace-like operator to β, we can "project" it down into $GF(2^n)$ giving a generator of a low complexity normal basis.

Definition. If G is an abelian group, and $n \in \mathbb{Z}$, then we define G^n by

$$G^n = \{a^n \mid a \in G\}.$$

Lemma. 2.1. *Let $kn+1$ be prime and $G = GF(kn+1)^*$. If $G = \langle 2, G^n \rangle$ and γ is a primitive kth root of unity in $GF(kn+1)$, then every element β of G can be written uniquely in the form*

$$\beta = 2^i \gamma^j,$$

where $0 \le i \le n-1$, $0 \le j \le k-1$.

Proof. Existence will follow from uniqueness since there are kn choices for (i, j) and kn elements of G, and $2^i\gamma^j$ is always in G. To prove uniqueness, suppose

$$2^i\gamma^j = 2^{i'}\gamma^{j'} (\text{mod } kn+1) \quad \text{or} \quad 2^{i-i'} = \gamma^{j'-j}$$
$$\text{or} \quad 2^{k(i-i')} = 1 \quad \text{or} \quad \text{ord}(\langle 2\rangle) \mid k(i-i').$$

Let λ be a generator of G. Then suppose $2 = \lambda^a$. Then $G = \langle 2, G^n\rangle = \langle \lambda^a, \lambda^n\rangle$ so $\gcd(a, n) = 1$. Also,

$$\text{ord}(\langle 2\rangle) = \frac{nk}{\gcd(nk, a)}.$$

Hence

$$\frac{nk}{\gcd(nk, a)} \mid k(i-i') \quad \text{and} \quad n \mid \gcd(nk, a)(i-i') \quad \text{and} \quad n \mid a(i-i'),$$

which implies $n \mid (i-i')$ since $\gcd(a, n) = 1$. Thus $i = i'$ and hence $j = j'$. □

Theorem 2.2. *Let $kn+1$ be prime and $G = \text{GF}(kn+1)^*$. If $G = \langle 2, G^n\rangle$ and β is a primitive $(kn+1)$st root of unity in $\text{GF}(2^{kn})$, then α generates a normal basis of $\text{GF}(2^n)$ over $\text{GF}(2)$, where*

$$\alpha = \sum_{i=0}^{k-1} \beta^{\gamma^i}$$

and γ is a primitive kth root of unity in $\text{GF}(kn+1)$.

Proof. First we show that α lies in $\text{GF}(2^n)$. Since $\alpha^{2^n} = \sum_{i=0}^{k-1} \beta^{2^n\gamma^i}$ and $(2^n)^k \equiv 1 (\text{mod } kn+1)$ so $2^n \equiv \gamma^l$ for some l. Thus

$$\alpha^{2^n} = \sum_{i=0}^{k-1} \beta^{\gamma^{i+l}} = \alpha$$

as we have merely permuted exponents. Thus $\alpha \in \text{GF}(2^n)$. Now suppose

$$\sum_{i=0}^{n-1} a_i \sum_{j=0}^{k-1} \beta^{2^i\gamma^j} = 0,$$

where not all the a_i are zero. Reducing exponents modulo $kn+1$ we get

$$\sum_{i=0}^{n-1} a_i \sum_{j=0}^{k-1} \beta^{[2^i\gamma^j]} = 0$$

where $[z]$ is the least residue of z modulo $kn+1$. Clearly β is a root of the polynomial

$$f(x) = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{k-1} x^{[2^i\gamma^j]}.$$

Suppose ξ is a primitive $(kn+1)$st root of unity and $f(\xi) = 0$. Then

$$f(\xi^2) = f(\xi)^2 = 0$$

and also

$$f(\xi^\gamma) = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{k-1} \xi^{[2^i\gamma^j+1]} = f(\xi) = 0,$$

so ξ^2 and ξ^γ are also roots of $f(x)=0$. But we already know by Lemma 2.1 that

$$\{[2^i\gamma^j] \mid 0 \le i \le n-1,\ 0 \le j \le k-1\} = \{1, 2, \ldots, kn\}$$

so $\beta, \beta^2, \ldots, \beta^{kn}$ are all roots of $f(x)=0$. Thus

$$(1+x+x^2+\cdots+x^{kn}) \mid f(x).$$

Since all the a_i are not zero, $f(x) \not\equiv 0$. Also $\deg(f) \le kn$, so

$$f(x) = x^{kn} + \cdots + 1.$$

Since $f(x)$ has at most kn nonzero terms, this is a contradiction and completes the proof. □

One of the reviewers of this paper pointed out that the element α in this theorem is of classical origin and is referred as a period of Gauss [19]. It was also noted that there will exist a k such that $\langle 2, G^n \rangle = G$ if and only if $8 \nmid n$. The condition that $8 \nmid n$ is also a result of the nonexistence of self-dual normal bases of GF(2^{4m}) over GF(2). If $8 \mid n$ then $\langle 2, G^n \rangle$ contains only quadratic residues and hence is not G. The converse apparently depends on [17, Lemma 6 and Theorem 2].

The dual of the normal basis given by Theorem 2.2 can be easily exhibited. This is of some interest since the dual basis can be used in certain hardware multipliers for finite fields [2]. More details on the dual basis can be found in Appendix A.

Theorem 2.3. *Let N be the normal basis constructed in Theorem 2.2. Then the following bounds on the complexity of N hold:*

$$kn - (k^2 - 3k + 3) \le C_N \le kn - 1, \qquad \text{if } k \text{ even},$$

$$(k+1)n - (k^2 - k + 1) \le C_N \le (k+1)n - k, \qquad \text{if } k \text{ odd}.$$

Proof. The general basis element is $\sum_{j=0}^{k-1} \beta^{2^i\gamma^j}$, so basis element i times basis element 0 is

$$\sum_{j=0}^{k-1} \beta^{2^i\gamma^j} \cdot \sum_{j=0}^{k-1} \beta^{\gamma^j} = \sum_{0 \le j,l \le k-1} \beta^{\gamma^j + \gamma^l 2^i} = \sum_{s=0}^{k-1} \left[\sum_{j=0}^{k-1} \beta^{\gamma^j + \gamma^{j+s} 2^i} \right]. \tag{1}$$

Now consider the inner sum $\sum_{j=0}^{k-1} \beta^{\gamma^j + \gamma^{j+s} 2^i}$. We claim that if $\beta^{1+\gamma^s 2^i} \ne 1$, then there exist t and l such that $\beta^{\gamma^l + \gamma^{l+s} 2^i} = \beta^{2^t}$. (t, l) satisfies this condition iff

$$\gamma^l + \gamma^{l+s} 2^t \equiv 2^t \pmod{kn+1} \quad \text{or} \quad \gamma^{-l} 2^t \equiv 1 + \gamma^s 2^i,$$

which will, by Lemma 2.1, have a solution (t, l) if $1+\gamma^s 2^i \neq 0$, or equivalently, $\beta^{1+\gamma^s 2^i} \neq 1$. Thus if $\beta^{1+\gamma^s 2^i} \neq 1$, then

$$\sum_{j=0}^{k-1} \beta^{\gamma^j + \gamma^{j+s} 2^i} = \sum_{j=0}^{k-1} \beta^{\gamma^{l+j} + \gamma^{j+s} 2^i} \quad \text{(since } \gamma^k \equiv 1\text{)}$$

$$= \sum_{j=0}^{k-1} \beta^{2^l \gamma^j},$$

which is a basis element. Lemma 2.1 implies that there exists exactly one solution (i_0, s_0) to $1+\gamma^{s_0} 2^{i_0} \equiv 0$, so for all $i \neq i_0$, the sum (1) is the sum of k possibly non-distinct basis elements, so the associated row of the T-matrix has at most k ones. If $i = i_0$, the associated row of the T-matrix certainly contains at most n ones. If k is even, we can say further that

$$\sum_{j=0}^{k-1} \beta^{\gamma^j + \gamma^{j+s_0} 2^{i_0}} = k = 0,$$

so the sum (1) is the sum of $k-1$ possibly nondistinct basis elements, and the associated row of the T-matrix contains at most $k-1$ ones. The upper bounds follow.

Now, for $i \neq i_0$, let us write the sum (1) as

$$\sum_{s=0}^{k-1} \alpha_{f(i,s)}$$

where $\alpha_j = \alpha^{2^j}$ and f maps into the set $\{0, 1, \ldots, n-1\}$. Let P_i be the number of ordered pairs (s_1, s_2) with $s_1 \neq s_2$ and $f(i, s_1) = f(i, s_2)$, and let T_i be the number of ordered triples (s_1, s_2, s_3) with s_1, s_2, and s_3 all distinct and $f(i, s_1) = f(i, s_2) = f(i, s_3)$. Also suppose that $\sum_{s=0}^{k-1} \alpha_{f(i,s)}$ is the sum of exactly D_i distinct basis elements. Then we make two claims:

$$D_i \geq k - P_i, \tag{2}$$

$$D_i = k - P_i \quad \text{iff} \quad T_i = 0. \tag{3}$$

To verify these claims, let

$$N_{i,t} = \#\{j \mid t = \#\{s \mid f(i,s) = j\}\} \quad \text{for all } t \geq 1.$$

Then the reader can easily verify that

$$D_i = N_{i,1} + N_{i,3} + N_{i,5} + \cdots, \qquad k = N_{i,1} + 2N_{i,2} + 3N_{i,3} + \cdots,$$

$$P_i = \sum_{t \geq 2} t(t-1) N_{i,t}, \qquad T_i = \sum_{t \geq 3} t(t-1)(t-2) N_{i,t}.$$

Hence

$$D_i - k + P_i = \sum_{t \text{ odd}} (1 + t(t-1) - t)N_{i,t} + \sum_{t \text{ even}} (t(t-1) - t)N_{i,t}$$

$$= \sum_{t \text{ odd}} (t-1)^2 N_{i,t} + \sum_{t \text{ even}} t(t-2)N_{i,t} \geq 0,$$

since t even implies $t \geq 2$. Equality occurs iff $N_{i,t} = 0$ for $t \geq 3$, which is precisely the condition under which $T_i = 0$.

Now, in the $i = i_0$ case, we define P_{i_0}, T_{i_0}, and D_{i_0} in precisely the same way, except that we place the added condition on s that $s \neq s_0$. (For instance, we replace $\sum_{s=0}^{k-1} \alpha_{f(i,s)}$ by $\sum_{0 \leq s \leq k-1, s \neq s_0} \alpha_{f(i,s)}$.) When k is even the following claims are verified in the same manner as above:

$$D_{i_0} \geq k - 1 - P_{i_0}, \tag{4}$$

$$D_{i_0} = k - 1 - P_{i_0} \quad \text{iff} \quad T_{i_0} = 0. \tag{5}$$

If k is odd, remember that $\sum_{j=0}^{k-1} \beta^{\gamma^j + \gamma^{j+s_0} 2^{i_0}} = 1$, and 1 is the sum of all n basis elements, so that row i_0 actually contributes $n - D_{i_0}$ ones to the T-matrix. We make the following claims:

$$n - D_{i_0} \geq n - k + 1, \tag{6}$$

$$n - D_{i_0} = n - k + 1 \quad \text{iff} \quad P_{i_0} = 0. \tag{7}$$

These are trivial; the proof is left to the reader. Now, observe that if k is even,

$$C_N = \sum_{i=0}^{n-1} D_i \geq nk - 1 - \sum_{i=0}^{n-1} P_i$$

and if k is odd,

$$C_N = \sum_{\substack{0 \leq i \leq n-1 \\ i \neq i_0}} D_i + n - D_{i_0}$$

$$\geq k(n-1) - \sum_{\substack{0 \leq i \leq n-1 \\ i \neq i_0}} P_i + n - k + 1$$

$$\geq (k+1)n - 2k + 1 - \sum_{i=0}^{n-1} P_i.$$

Letting $P = \sum_{i=0}^{n-1} P_i$, it remains to evaluate P. That is, for how many choices of (i, s_1, s_2) do we have

$$\sum_{j=0}^{k-1} \beta^{\gamma^j + \gamma^{j+s_1} 2^i} = \sum_{j=0}^{k-1} \beta^{\gamma^j + \gamma^{j+s_2} 2^i}?$$

This holds iff for some j,

$$2^i\gamma^{s_1}+1 \equiv \gamma^j+\gamma^{j+s_2}2^i (\text{mod } kn+1) \quad \text{or} \quad 2^i\gamma^{s_2}(\gamma^{s_1-s_2}-\gamma^j) \equiv \gamma^j-1.$$

Now we cannot have both $\gamma^{s_1-s_2}-\gamma^j \equiv 0$ and $\gamma^j-1 \equiv 0$ since otherwise $s_1=s_2$. So given s_1-s_2 and j we have at most one choice for (i,s_2) by Lemma 2.1, and zero choices if $\gamma^j-1\equiv 0$ or $\gamma^{s_1-s_2}-\gamma^j \equiv 0$. Thus j may be chosen in $(k-1)$ ways $(j\neq 0)$ and s_1-s_2 in $(k-2)$ ways $(s_1-s_2\neq 0,\ s_1-s_2\neq j)$. This gives rise to a total of $(k-1)(k-2)$ choices. Hence

$$P=(k-1)(k-2).$$

The lower bounds follow. □

The following theorem and lemma will allow the construction in Theorem 2.6 of projection bases that achieve the minimum complexity allowed by Theorem 2.3.

Theorem 2.4. *Suppose the conditions of Theorem* 2.2 *hold. In addition suppose that*

$$f(x)=(x^{t_1}-x^{j_1})(x^{j_2}-1)-(x^{t_2}-x^{j_2})(x^{j_1}-1),$$

$$g(x)=x^{j_1+t_2}-x^{t_1}-x^{j_1}+1,$$

$$h(x)=\Phi_k(x)$$

satisfy $\gcd(f,h)=1$ *in* $\mathrm{GF}(kn+1)[x]$ *for* $1\leq t_1,j_1,t_2,j_2\leq k-1$, $t_1\neq j_1$, $t_2\neq j_2$, $t_1\neq t_2$, $j_1\neq j_2$, *and when* k *is odd* $\gcd(g,h)=1$ *in* $\mathrm{GF}(kn+1)[x]$ *for* $1\leq t_1,j_1,t_2\leq k-1$, $t_1\neq t_2$. *Then the normal basis has the minimum complexity allowed by Theorem* 2.3.

(Note: Φ_k denotes the kth cyclotomic polynomial.)

Proof. We assume that the equality does not hold under the conditions of this theorem and derive a contradiction. We observed in the proof of Theorem 2.3 that the lower bound was an equality if $T_i=0$ for all i, and $P_{i_0}=0$ when k is odd. Tackling first the possibility that $T_i>0$ for some i, we see that this means there exist s_1, s_2, and s_3 all distinct with

$$\sum_{j=0}^{k-1}\beta^{\gamma^j+\gamma^{j+s_1}2^i}=\sum_{j=0}^{k-1}\beta^{\gamma^j+\gamma^{j+s_2}2^i}=\sum_{j=0}^{k-1}\beta^{\gamma^j+\gamma^{j+s_3}2^i}.$$

This holds iff for some j_1, j_2,

$$2^i\gamma^{s_3}(\gamma^{s_1-s_3}-\gamma^{j_1})\equiv\gamma^{j_1}-1,$$

$$2^i\gamma^{s_3}(\gamma^{s_2-s_3}-\gamma^{j_2})\equiv\gamma^{j_2}-1.$$

Letting $s_1 - s_3 = t_1$, $s_2 - s_3 = t_2$,

$$(\gamma^{t_1} - \gamma^{j_1})(\gamma^{j_2} - 1) \equiv (\gamma^{t_2} - \gamma^{j_2})(\gamma^{j_1} - 1)$$

$$\text{or} \quad (x^{t_1} - x^{j_1})(x^{j_2} - 1) - (x^{t_2} - x^{j_2})(x^{j_1} - 1) = 0$$

has a root x_0 in GF($kn+1$) for some x_0 which is a primitive kth root of unity. Then also $\Phi_k(x_0) = 0$. Now $t_1 \neq 0$, $t_2 \neq 0$ (since s_1, s_2, and s_3 are all distinct), $j_1 \neq 0$, $j_2 \neq 0$ (since $2^i \gamma^{s_3}$ is not a zero divisor), $t_1 \neq j_1$, $t_2 \neq j_2$ (since $j_1 \neq 0$, $j_2 \neq 0$), and $t_1 \neq t_2$ ($s_1 \neq s_2$). It is easily shown that $j_1 = j_2$ implies $t_1 = t_2$, so also $j_1 \neq j_2$.

Next suppose k is odd and $P_{i_0} > 0$. In this case there exist i, s_1, s_2, s_3, j with s_1, s_2, s_3 all distinct such that

$$2^i \gamma^{s_2}(\gamma^{s_1 - s_2} - \gamma^j) \equiv \gamma^j - 1, \qquad 2^i \gamma^{s_3} \equiv -1,$$

so

$$(\gamma^j - \gamma^{s_1 - s_2}) \equiv (\gamma^{s_3 - s_2 + j} - \gamma^{s_3 - s_2}) \quad \text{or} \quad x^{s_3 - s_2 + j} - x^{s_3 - s_2} - x^j + x^{s_1 - s_2} = 0$$

has a root x_0 in GF($kn+1$) for some x_0 which is a primitive kth root of unity. $x_0 \neq 0$, so it is also a root of

$$x^{s_3 - s_1 + j} - x^{s_3 - s_1} - x^{j - s_1 + s_2} + 1 = 0.$$

Letting $j_1 = j - s_1 + s_2$, $t_1 = s_3 - s_1$, and $t_2 = s_3 - s_2$, this becomes

$$x^{j_1 + t_2} - x^{t_1} - x^{j_1} + 1 = 0.$$

Clearly $t_1 \neq 0$, $t_2 \neq 0$ (since s_1, s_2, s_3 are distinct). If $j_1 = 0$, $t_1 = t_2$, a contradiction, so $j_1 \neq 0$. Also $t_1 \neq t_2$ (since $s_1 \neq s_2$). Thus the conditions of the theorem hold, but $\gcd(g, h) = 1$. This completes the proof. □

Lemma 2.5. *Suppose the conditions on t_1, j_1, t_2, j_2, hold from Theorem 2.4 and that k is fixed. Then*

$$(x^k - 1) \nmid f(x) \quad \textit{and} \quad (x^k - 1) \nmid g(x) \quad \textit{in } \mathbb{Q}[x]$$

and if $k = 2k'$

$$(x^{k'} + 1) \nmid f(x).$$

Proof. (First case). Let us reduce the exponents of f modulo k. This amounts to finding the remainder upon division by $x^k - 1$, and if $(x^k - 1) \mid f(x)$, this should be identically zero. Now the reduced polynomial is

$$\bar{f}(x) = x^{[t_2]} + x^{[j_1]} + x^{[t_1 + j_2]} - x^{[t_1]} - x^{[j_2]} - x^{[t_2 + j_1]}.$$

For this to be zero, $t_2 \equiv t_1, j_2$, or $t_2 + j_1 \pmod{k}$. None of these cases are allowed by Theorem 2.4. Next we reduce the exponents of $g(x)$:

$$\bar{g}(x) = x^{[j_1 + t_2]} - x^{[t_1]} - x^{[j_1]} + 1.$$

For this to be identically zero, t_1 or $j_1 \equiv 0$. This is a contradiction, so $(x^k-1) \nmid g(x)$.

(Second case). Again let us reduce the exponents modulo k, so

$$\bar{f}(x) = x^{[t_2]} + x^{[j_1]} + x^{[t_1+j_2]} - x^{[t_1]} - x^{[j_2]} - x^{[t_2+j_1]} \tag{8}$$

$$= (x^{k'}+1)q(x) \quad \text{(by assumption)}$$

$$= q(x)x^{k'} + q(x). \tag{9}$$

This implies that $\bar{f}(x)$ has an even number of both positive and negative terms, which means that two of the terms in (8) must cancel. It is easily shown that they must be $x^{[t_1+j_2]}$ and $x^{[t_2+j_1]}$, so

$$t_1 + j_2 \equiv t_2 + j_1.$$

It follows from (9) that

$$t_2 \equiv j_1 + k', \qquad t_1 \equiv j_2 + k'$$

so

$$2j_1 \equiv 2j_2.$$

Ruling out $j_1 \equiv j_2$, we get $j_1 \equiv j_2 + k' \equiv t_1$, a contradiction. □

Theorem 2.6. *If k is an odd prime, double an odd prime, four times an odd prime or a power of two, then for sufficiently large n, the projection basis has the minimum complexity allowed by Theorem* 2.3.

Proof. In all cases, we will show that $\Phi_k(x) \nmid f(x)$ in $\mathbb{Q}[x]$ by assuming the contrary. If $k=p$, an odd prime, then by Lemma 2.5, $(x^p-1) \nmid f(x)$. When we reduce $f(x) \pmod{x^p-1}$, we get a polynomial which is not identically zero, since $(x^p-1) \nmid f(x)$, and is divisible by $\Phi_p(x)$, and has degree at most $p-1$. Thus the reduced $f(x)$ is equal to $\Phi_p(x)$. But $\Phi_p(x)$ has an odd number (p) of terms and $f(x)$ has an even number of terms (≤ 6), which gives a contradiction. Since $(x^p-1) \nmid g(x)$, we can also show that $\Phi_k(x) \nmid g(x)$ in $\mathbb{Q}[x]$.

If $k=2p$, p an odd prime, then $\Phi_{2p}(x) = 1 - x + x^2 - \cdots + x^{p-1}$. Again, $(x^p+1) \nmid f(x)$, so if $\Phi_{2p}(x) \mid f(x)$, $f(x) \equiv \Phi_{2p}(x) \pmod{x^p+1}$, which produces a contradiction, as in the $k=p$ case.

If $k=4p$, p an odd prime, then $\Phi_{4p}(x) = 1 - x^2 + x^4 - \cdots + x^{2p-2}$. Again $(x^{2p}+1) \nmid f(x)$, so if $\Phi_{4p}(x) \mid f(x)$, then the reduced $f(x) \pmod{x^{2p}+1}$ ($\bar{f}(x)$) satisfies $\bar{f}(x) = \Phi_{4p}(x) \cdot q(x)$ where $q(x)$ is linear. If $p>3$, this implies that $\bar{f}$ has either five or at least seven terms, both contradictions. If $p=3$, let $q(x) = Ax + B$ where $|A| + |B| = 2$. Now the reduction process does not change the exponents of j modulo 2, so the form of $\bar{f}$ implies that zero, three or six of these exponents are even. Zero is impossible (t_1, j_2 odd implies $t_1 + j_2$ even). Likewise the sum of all six exponents is even, so three is impossible. Thus t_1, j_2, t_2, j_1 are all even. Hence $|A| = 0$, $|B| = 2$, and we may assume that $B = 2$, so $\bar{f}(x) = 2(x^4 - x^2 + 1)$. Now $f(x)$ reduces to the same thing mod x^6+1 as does

$$x^{t_2} + x^{j_1} + x^{t_1+j_2} + x^{t_1+6} + x^{j_2+6} + x^{t_2+j_1+6}. \tag{10}$$

Since $\bar{f}(x)=2(x^4-x^2+1)$, it can be shown that all the exponents in (10) are multiples of 4, which would imply that $4 \mid 6$, a contradiction.

If $k=2^m$, $\Phi_{2^m}(x)=x^{2^{m-1}}+1$ and so by Lemma 2.4, $\Phi_{2^m}(x) \dagger f(x)$.

Thus in all cases, $\Phi_k(x) \dagger f(x)$ in $\mathbb{Q}[x]$, and since $\Phi_k(x)$ is irreducible in $\mathbb{Q}[x]$, for all k, or $(\Phi_k(x), f(x))=1$ in $\mathbb{Q}[x]$. Thus $\exists \bar{\Phi}, \bar{f} \in \mathbb{Q}[x]$ satisfying

$$\Phi_k \bar{\Phi} + f\bar{f} = 1 \quad \text{in } \mathbb{Q}[x],$$

so there exist $\bar{\bar{f}}, \bar{\bar{\Phi}} \in \mathbb{Z}[x]$ satisfying

$$\Phi_k \bar{\bar{\Phi}} + f\bar{\bar{f}} = l \quad \text{in } \mathbb{Z}[x]$$

where $l \in \mathbb{Z}$ and $l>0$. This also holds in $\mathrm{GF}(kn+1)[x]$ so if $(kn+1) \dagger l$, $(\Phi_k, f)=1$ in $\mathrm{GF}(kn+1)[x]$. Thus as long as we pick n large enough that $(kn+1) \dagger l$ for any choice of f, we can apply Theorem 2.3. This completes the proof. □

In certain cases, the dual of the basis given in Theorem 2.2 also turns out to have low complexity, although in no known case is this complexity lower than that of the original normal basis. The interested reader is again referred to Appendix A for a specific result on the complexity of the dual basis.

We conclude this section by presenting an algorithm for actually computing the minimum value l mentioned at the end of the proof of Theorem 2.6.

Algorithm 2.7. *Given polynomials $f, g \in \mathbb{Z}[x]$, f monic, assume that* $\gcd(f,g)=1$ *in* $\mathbb{Q}[x]$. *Then there exists a least positive integer d such that*

$$ff' + gg' = d$$

for some $f', g' \in \mathbb{Z}[x]$. We show how to compute d given f and g.

Method. We already know (hybrid of Euclid's algorithm) how to find f' and g' such that

$$ff' + gg' = l > 0, \quad f', g' \in \mathbb{Z}[x].$$

It is clear that $d \mid l$ since if not we could replace d with $\gcd(d, l) < d$. Suppose $l = p^k l'$ where p is prime, $p \dagger l'$. Then the algorithm follows if we can find f'' and g'' with

$$ff'' + gg'' = p^{k-1} l'$$

or prove no such f'' and g'' exist.

Theorem 2.8. *If $f \dagger g'$ in* $\mathrm{GF}(p)$, *no such f'' and g'' exist. If $f \mid g'$ in* $\mathrm{GF}(p)$, *then let $g' = fh$ in* $\mathrm{GF}(p)$. *Pulling h out into $\mathbb{Z}[x]$, then*

$$f'' = \frac{f' + hg}{p} \quad \text{and} \quad g'' = \frac{g' - hf}{p}$$

satisfy the required conditions.

Proof. Suppose $f \nmid g'$ but such f'' and g'' do exist. Then

$$f(f'-pf'')+g(g'-pg'')=0,$$

so $f \mid g(g'-pg'')$ in $\mathbb{Q}[x]$. But $\gcd(f,g)=1$ in $\mathbb{Q}[x]$, so $f \mid (g'-pg'')$ in $\mathbb{Q}[x]$.
f is monic, so

$$f \mid (g'-pg'') \text{ in } \mathbb{Z}[x]$$

$$\text{or} \quad f \mid (g'-pg'') \quad \text{in GF}(p)[x] \quad \text{or} \quad f \mid g' \quad \text{in GF}(p)[x],$$

a contradiction.

If $f \mid g'$ in GF$(p)[x]$, the above f'', g'' satisfy $ff''+gg''=p^{k-1}l$. It remains to be seen that they lie in $\mathbb{Z}[x]$. Now,

$$g'-hf=0 \quad \text{in GF}(p)[x],$$

so $p \mid (g'-hf)$ in $\mathbb{Z}[x]$ or $g'' \in \mathbb{Z}[x]$. Now

$$g'=hf+pg'', \qquad gg'=hfg+pgg''=hfg+p^k l'-p(p^{k-1}l'-gg''),$$

$$p(p^{k-1}l'-gg'')=hfg+p^k l'-gg'=hfg+ff'=f(hg+f').$$

Thus $p \mid f(hg+f')$. Since $p \nmid f$, $p \mid (hg+f')$. Therefore $f'' \in \mathbb{Z}[x]$. This completes the proof. □

3. Particular results for small k

In this section we apply the general results of Section 2 to derive explicit results for small values of k. Since the complexity of the generated basis increases, in general, as k increases, it is precisely these small values of k which interest us.

Theorem 3.1. *For sufficiently large n and $k \leq 14$, the standard projection basis from* GF(2^{kn}) *to* GF(2^n) *has the minimum complexity allowed by Theorem* 2.3.

Proof. By the proof of Theorem 2.6, the asymptotic result will follow once we have deduced that the kth cyclotomic polynomial does not divide

$$(x^{t_1}-x^{j_1})(x^{j_2}-1)-(x^{t_2}-x^{j_2})(x^{j_1}-1) \quad \text{in } \mathbb{Q}[x]$$

for any admissible choices of t_1, t_2, j_1, j_2. The proof is divided into cases.

(1) $k=1$. In this case we simply have a type I normal basis. The proof that we always generate a (minimal) normal basis with complexity $2n-1$ is given in [13]. Notice that this result also follows from Theorem 2.3.

(2) $k=2,4,8$. These are all powers of 2 and are handled by Theorem 2.6.

(3) $k=3,5,7,11,13$. These are all odd primes and are handled by Theorem 2.6.

(4) $k=6,10,14$. These are all double odd primes and are handled by Theorem 2.6.

(5) $k=9$. The proof of this case is omitted. It can be proved by assuming that

the cyclotomic polynomial $\Phi_9(x) = x^6 + x^3 + 1$ divides

$$f(x) = (x^{t_1} - x^{j_1})(x^{j_2} - 1) - (x^{t_2} - x^{j_2})(x^{j_1} - 1)$$

and

$$g(x) = (x^{j_1 + t_2} - x^{t_1} - x^{j_1} + 1)$$

and arriving at a contradiction. The details are in [1].

(6) $k = 12$. This is four times an odd prime and is handled by Theorem 2.6.

Theorem 3.2. *For $k = 3,4$, $n > 1$, the projection basis from* GF(2^{kn}) *to* GF(2^n), *in cases where it exists, has exactly $4n - 7$ complexity.*

Proof. As before, this requires that the third and fourth cyclotomic polynomials not have a common factor with

$$f(x) = (x^{t_1} - x^{j_1})(x^{j_2} - 1) - (x^{t_2} - x^{j_2})(x^{j_1} - 1) \quad \text{in } \mathbb{Q}[x].$$

For $k = 3$, t_1 and j_1 must be 1 and 2, not necessarily respectively. Similarly for t_2 and j_2. Thus up to symmetry

$$f(x) = (x^2 - x)(x^2 - 1) - (x - x^2)(x - 1) = x(x-1)(x^2 + x - 2) = x(x-1)^2(x+2).$$

For any of these primitive factors to divide $x^2 + x - 1$, we require $1 + 1 + 1 = 3 = 0$ or $4 - 2 + 1 = 0$. This cannot happen in a prime field of order $3n + 1$. Since this is a k odd case, we also have to consider the possibility that $x^2 + x + 1$ has a common factor with

$$g(x) = x^{j_1 + t_2} - x^{t_1} - x^{j_1} + 1.$$

Now, once again t_1 and t_2 are 1 and 2, not necessarily respectively so that

$$g(x) = 2 - 2x \quad \text{or} \quad g(x) = 1 - x \quad \text{or} \quad g(x) = 1 - x^2 \quad \text{or} \quad g(x) = 2 - 2x^2.$$

Once again, none of these can share a primitive factor with $x^2 + x + 1$ in a prime field of order $3n + 1$.

For $k = 4$ the cyclotomic polynomial is $x^2 + 1$. Reducing modulo $x^2 + 1$ over $\mathbb{Q}[x]$, $f(x)$ will become $Ax + B$ where $|A| + |B| \leq 6$. Also, by Lemma 2.5, A and B are not both zero. Now

$$A^2(x^2 + 1) - (Ax - B)(Ax + B) = A^2 + B^2 \leq 36.$$

Thus, by the proof of Theorem 2.6, $4n + 1$ is a prime dividing the sum of the two squares, whose sum is less than or equal to 36. In addition, $t_1 + j_1 + j_2 + t_1 + (t_1 + j_2) + (t_2 + j_1)$ is even. Since the parity of A depends on the number of elements of $\{t_1, j_1, j_2, t_2, t_1 + j_2, t_2 + j_1\}$ which are odd, we conclude that A and B are both even.

This leaves the following possible cases:

A	B	(A^2+B^2)	Prime divisors
0	2	4	2
0	4	16	2
0	6	36	2,3
2	2	8	2
2	4	20	2,5

The only prime divisor of the form $4n+1$ is 5, giving one possible exception: $n=1$. □

The complete proofs of the following two theorems are contained in [1] and are largely omitted. The techniques used to establish them are similar but more intricate than those used for the previous theorem. For Theorem 3.3, we do present the proof of the $k=6$ case because of its unusual brevity and as an example. In the case of Theorem 3.4, the full proof in [1] requires (at present) the implementation of Algorithm 2.7 on the computer.

Theorem 3.3. *If* $k=5$, $n>2$, *or* $k=6$, $n>12$, *the projection basis from* GF(2^{kn}) *to* GF(2^n), *in cases where it exists, has exactly* $6n-21$ *complexity.*

Partial Proof. For the case $k=6$, we can reduce modulo x^3+1 so that

$$(x^{t_1}-x^{j_1})(x^{j_2}-1)-(x^{t_2}-x^{j_2})(x^{j_1}-1)$$

yields

$$Ax^2+Bx+C$$

with $1\le|A|+|B|+|C|\le 6$. The cyclotomic polynomial is x^2-x+1, and

$$[(B+C)-(B+A)x](Ax^2+Bx+C)$$

$$+[(B+A)^2-A(B+C)+xA(A+B)](x^2-x+1)$$

$$=(B+A)^2+(C-A)(C+B).$$

Thus if $p>|(B+A)^2+(C-A)(C+B)|$, then we are done. Now

$$|(B+A)^2+(C-A)(C+B)|\le|(B+A)|^2+|C-A||C+B|\le 72,$$

so for $n\ge 12$, $k=6$, $kn+1=p>73>72$. This completes the proof. □

Theorem 3.4. *If* $k=7$, $n>6$, *the projection basis from* GF(2^{7n}) *to* GF(2^n), *in cases where it exists, has exactly* $8n-43$ *complexity.*

4. Specific applications of the results

Because of the difficulty of computing discrete logarithms in finite fields, discrete exponentiation has found various applications in cryptography (see for example [6, 7, 14]).

As a result there is considerable interest in VLSI implementations of arithmetic processors in GF(2^n) for large values of n. When using a normal basis representation the problems associated with interconnecting the cells on a hardware device can be minimized by using a low complexity basis. With this in mind a Massey-Omura multiplier for GF(2^{127}) was designed by Wang [18]. The basis used had complexity over 9000 and as such was not very practical. Using the results of this paper we can construct a basis for this field having complexity 501. Because of the importance of Mersenne primes to cryptography (see [4]) Table 2 lists some Mersenne primes 2^n-1, the smallest value of k such that $kn+1$ is a prime and 2 generates the kth

Table 2. Lowest known complexities in Mersenne prime fields.

n	k	Complexity	Comments
2	2	3	Optimal
3	2	5	Optimal
5	2	9	Optimal
7	4	21	Theorem 3.2 (Table 1 gives a value of 19)
13	4	45	Minimal (Table 1)
17	6	81	Minimal (Table 1)
19	10	≤189	Theorem 2.3
31	10	≤309	Theorem 2.3
61	6	345	Theorem 3.3
89	2	177	Optimal
107	6	621	Theorem 3.3
127	4	501	Theorem 3.2
521	32	≤16671	Theorem 2.3 (unusually bad case)
607	6	3621	Theorem 3.3
1279	10	≤12789	Theorem 2.3
2203	6	13197	Theorem 3.3
2281	6	13665	Theorem 3.3
3217	16	≤51471	Theorem 2.3
4253	20	≤85059	Theorem 2.3
4423	6	26517	Theorem 3.3
9689	2	19377	Optimal
9941	12	≤119291	Theorem 2.3
11213	20	≤224259	Theorem 2.3
19937	14	≤279117	Theorem 2.3
21701	2	43401	Optimal
23209	10	≤232089	Theorem 2.3
44497	6	266961	Theorem 3.3
86243	6	517437	Theorem 3.3
132049	4	528189	Theorem 3.2

residues in GF($kn+1$) along with the lowest complexity we can determine by our results. Since n is necessarily a prime it is enough to check that $2^k \not\equiv 1 (\mathrm{mod}\ kn+1)$ in order to see if 2 generates the kth residues.

The results obtained in this paper do not always give minimal normal bases. Referring to Table 1 in Section 1 the starred entries are optimal bases found in [13]. Table 1 shows that besides the starred entries that for $n = 13,17,25,27$ our results give minimal normal bases. There are a number of entries in Table 1 which cannot be obtained by any of the currently known constructions for normal bases.

Appendix A. Results on the dual basis

Theorem A.1. *The dual of the basis given in Theorem* 2.2 *is generated by*

$$\bar{\alpha} = \left[\sum_{i=0}^{k-1} \beta^{-\gamma^i} \right] + 1,$$

if k is odd, and δ if k is even.

Proof. In the k odd case, we must evaluate the trace of products of basis elements as follows:

$$T(\alpha^{2^l}\bar{\alpha}) = \sum_{j=0}^{n-1} \alpha^{2^{l+j}}\bar{\alpha}^{2^j} = \sum_{j=0}^{n-1} \left[\sum_{i=0}^{k-1} \beta^{2^{l+j}\gamma^i} \left\{ \sum_{l=0}^{k-1} \beta^{-2^j\gamma^l} + 1 \right\} \right]$$

$$= \sum_{j=0}^{n-1} \sum_{i=0}^{k-1} \sum_{l=0}^{k-1} \beta^{2^{l+j}\gamma^i - 2^j\gamma^l} + \sum_{j=0}^{n-1} \sum_{i=0}^{k-1} \beta^{2^{l+j}\gamma^i}.$$

Now we note that $2^j\gamma^i$ takes on all primitive residues mod $kn+1$ exactly once, and $\sum_{i=1}^{kn} \beta^i = 1$. Thus

$$T(\alpha^{2^l}\bar{\alpha}) = 1 + \sum_{\lambda=0}^{k-1} \sum_{j=0}^{n-1} \sum_{i=0}^{k-1} \beta^{(2^l\gamma^\lambda - 1)2^j\gamma^i}.$$

Now, $2^l\gamma^\lambda - 1 \equiv 0 \bmod kn+1$ iff t and λ are both zero. Thus the inner pair of sums is 1 if t and λ are not both zero, and kn otherwise. But $kn+1$ is prime, so kn is even, and kn is zero. Thus

$$T(\alpha^{2^l}\bar{\alpha}) = 1 + \sum_{\lambda=0}^{k-1} (1 + \delta_{\lambda 0}\delta_{t0}) = k + 1 + \delta_{t0} = \delta_{t0}.$$

This completes the proof in the k odd case. If k is even,

$$T(\alpha^{2^l+1}) = \sum_{j=0}^{n-1} \alpha^{2^{l+j}+2^j} = \sum_{j=0}^{n-1} \left\{ \left[\sum_{i=0}^{k-1} \beta^{2^{l+j}\gamma^i} \right] \left[\sum_{i=0}^{k-1} \beta^{2^j\gamma^i} \right] \right\}$$

$$= \sum_{j=0}^{n-1} \sum_{i=0}^{k-1} \sum_{l=0}^{k-1} \beta^{2^{l+j}\gamma^i + 2^j\gamma^l} = \sum_{\lambda=0}^{k-1} \sum_{j=0}^{n-1} \sum_{i=0}^{k-1} \beta^{(2^l\gamma^\lambda + 1)2^j\gamma^i}.$$

Now, there exists one choice of (t, λ) such that $2^t\gamma^\lambda + 1 \equiv 0$. Now, we know k is even and $\gamma^k \equiv 1$. Thus $\gamma^{k/2} + 1 \equiv 0$, so $(0, \frac{1}{2}k)$ is the required choice. Thus

$$T(\alpha^{2^t+1}) = \sum_{\lambda=0}^{k-1} (1 + \delta_{t0}\delta_{\lambda,k/2}) = \delta_{t0}.$$

This completes the proof. □

Theorem A.2. *If k is an odd prime, then for sufficiently large n, the basis described in Theorem* A.1 *has $(k+2)n - (k^2+k+1)$ complexity.*

Proof. A generator of the basis in Theorem A.1 is

$$1 + \sum_{j=0}^{k-1} \beta^{\gamma^j}.$$

We can drop the factor of -1 in the exponent since by Lemma 2.1 there exists a solution (i, s) to $2^i\gamma^s \equiv -1 (\text{mod } kn+1)$. Thus a typical product is

$$\left(1 + \sum_{j=0}^{k-1} \beta^{\gamma^j}\right)\left(1 + \sum_{j=0}^{k-1} \beta^{2^i\gamma^j}\right) \quad (\text{for } i = 0, 1, \ldots, n-1)$$

$$= 1 + \sum_{j=0}^{k-1} \beta^{\gamma^j} + \sum_{j=0}^{k-1} \beta^{2^i\gamma^j} + \sum_{l=0}^{k-1}\sum_{j=0}^{k-1} \beta^{\gamma^j(2^i\gamma^l+1)}$$

$$= \left(1 + \sum_{j=0}^{k-1} \beta^{\gamma^j}\right) + \left(1 + \sum_{j=0}^{k-1} \beta^{2^i\gamma^j}\right) + \sum_{l=0}^{k-1}\left[1 + \sum_{j=0}^{k-1} \beta^{\gamma^j(2^i\gamma^l+1)}\right].$$

Thus, each row in the matrix will contain $k+2$ ones, except in the following cases:

Case 1. $\gamma^j \equiv 0$ *or* $2^i\gamma^j \equiv 0$ *or* $\gamma^j(2^i\gamma^l + 1) \equiv 0$. The former two cases are impossible, and in the latter case there will be one choice of (i, l) which produces $2^i\gamma^l + 1 \equiv 0$. Since the 1 cancels out with the standard 1 which is a part of each term, the total complexity is reduced by 1. This is different from the nondual case where there is no 1 to cancel off a degenerate 1.

Case 2. *Some pair of terms are equal for some i.* There are four cases:

(i) $\gamma^{j_1}(2^{i_1}\gamma^{l_1} + 1) \equiv \gamma^{j_2}(2^{i_2}\gamma^{l_2} + 1)$. As in the nondual case, there are exactly $(k-1)(k-2)$ pairs (i_1, l_1) for which this equation has a solution.

(ii) $\gamma^{j_1} \equiv \gamma^{j_2}(2^{i_2}\gamma^{l_2} + 1)$. For each choice of $(j_1 - j_2)$ except $j_1 - j_2 \equiv 0$ we will have a nontrivial solution (i_2, l_2). This gives us $(k-1)$ pairs.

(iii) $\gamma^{j_1}2^i \equiv \gamma^{j_2}(2^i\gamma^{l_2} + 1)$ or $2^i\gamma^{j_1 - j_2}(1 - \gamma^{l_2 - j_1 + j_2}) \equiv 1$. For each choice of $(l_2 - j_1 + j_2)$ except $l_2 - j_1 + j_2 \equiv 0$ we will have a nontrivial solution $(i, j_1 - j_2)$. This gives us $(k-1)$ pairs.

(iv) $1 \equiv 2^i$. This happens for $i = 0$. This gives us one pair. We note that for sufficiently large n we need not worry about the possibility that three basis elements are

equal. Consider the following three cases:

(1) $\gamma^{j_1} \equiv 2^i \gamma^{j_2} \equiv \gamma^{j_3}(2^i \gamma^{l_3} + 1)$, so $i = 0$, $j_1 = j_2$, and we get

$$\gamma^{j_2 - j_3} = \gamma^{l_3} + 1,$$

so that $x^{j_2 - j_3} - x^{l_3} - 1 = 0$ shares a common factor with $\Phi_p(x)$.

(2) $\gamma^{j_1} \equiv \gamma^{j_2}(2^i \gamma^{l_2} + 1) \equiv \gamma^{j_3}(2^i \gamma^{l_3} + 1)$, so

$$(\gamma^{j_1 - j_2} - 1)\gamma^{l_3} \equiv (\gamma^{j_1 - j_3} - 1)\gamma^{l_2}.$$

Thus $(x^{j_1 - j_2} - 1)x^{l_3} - (x^{j_1 - j_3} - 1)x^{l_2}$ shares a common factor with $\Phi_p(x)$.

(3) $2^i \gamma^{j_1} \equiv \gamma^{j_2}(2^i \gamma^{l_2} + 1) \equiv \gamma^{j_3}(2^i \gamma^{l_3} + 1)$. This case is similar to (2) above.

Since in all cases we have a polynomial dependent only on p which shares a common factor with $\Phi_p(x)$, we can apply the methods of Theorem 2.6 to show that this cannot happen for sufficiently large n.

The total number of ones is thus

$$(k+2)n - 1 - 2 - (k-1)(k-2) - 4(k-1) = (k+2)n - (k^2 + k + 1).$$

Acknowledgment

The authors wish to acknowledge the important suggestions made by Professors Cam Stewart, Department of Pure Mathematics, University of Waterloo, and Rick Wilson, Department of Mathematics, California Institute of Technology, with regard to Algorithm 2.7 and Theorem 2.2 respectively. They would also like to thank the reviewers for their careful reading of the manuscript and helpful comments.

References

[1] D.W. Ash, I.F. Blake and S.A. Vanstone, On the construction of low complexity normal bases, Research Rept. CORR 86-21, University of Waterloo, Waterloo, Ont. (1986).

[2] E.R. Berlekamp, Bit serial Reed-Solomon encoders, IEEE Trans. Inform. Theory 28 (1982) 869–874.

[3] L. Carlitz, Primitive roots in a finite field, Trans. Amer. Math. Soc. 73 (1952) 373–382.

[4] B. Chor and R.L. Rivest, A knapsack type public key cryptosystem, in: Proceedings Crypto '84, Advances in Cryptology, Lecture Notes in Computer Science 196 (Springer, Berlin, 1984) 54–65.

[5] H. Davenport, Bases for finite fields, J. Lond. Math. Soc. 43 (1968) 21–39.

[6] W. Diffie and M.E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (6) (1976) 644–654.

[7] T. El Gamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory 31 (4) (1985) 469–472.

[8] K. Imamura, On self-complementary bases of $GF(q^n)$ over $GF(q)$, Trans. IECE Japan 12 (1983) 717–721.

[9] H.W. Lenstra Jr. and R.J. Schoof, Primitive normal bases for finite fields, Preprint (1985).

[10] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes (North-Holland, Amsterdam, 1977).
[11] J.L. Massey and J.K. Omura, Computational method and apparatus for finite field arithmetic, patent application (to appear).
[12] M. Morii and K. Imamura, A theorem that $GF(2^{4m})$ has no self-complementary normal bases over $GF(2)$ for odd m, Trans. IECE Japan 67 (1984) 655-656.
[13] R.C. Mullin, I.M. Onyszchuk and S.A. Vanstone, Optimal normal bases in $GF(p^n)$ (to appear).
[14] S.C. Pohlig and M.E. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, IEEE Trans. Inform. Theory 24 (1) (1978) 106–110.
[15] G. Seroussi and A. Lempel, Factorizations of symmetric matrices and trace orthogonal bases in finite fields, SIAM J. Comput. 9 (1980) 758–767.
[16] G. Seroussi and A. Lempel, On symmetric representations of finite fields, SIAM J. Algebraic Discrete Methods 4 (1983) 14-21.
[17] E. Bach and J. Shallit, Factoring with cyclotomic polynomials, in: Proceedings 26th Symposium on Foundations of Computer Science (1985) 443-450.
[18] C.C. Wang, Exponentiation in finite fields, Ph.D. Thesis, University of California (1985).
[19] L.C. Washington, Cyclotomic Fields (Springer, New York, 1980).