OPTIMAL NORMAL BASES IN GF\((p^n)\)*

R.C. MULLIN, I.M. ONYSZCHUK and S.A. VANSTONE

Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

R.M. WILSON

Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, USA

Received 24 February 1987
Revised 21 December 1987

In this paper the use of normal bases for multiplication in the finite fields GF\((p^n)\) is examined. We introduce the concept of an optimal normal basis in order to reduce the hardware complexity of multiplying field elements. Constructions for these bases in GF\((2^n)\) and extensions of the results to GF\((p^n)\) are presented. This work has applications in cryptography and coding theory since a reduction in the complexity of multiplying and exponentiating elements of GF\((2^n)\) is achieved for many values of \(n\), some prime.

1. Introduction

Recently, there has been much interest in the design of fast GF\((2^n)\) multipliers. Work in this area has resulted in several hardware [5, 9, 11, 12] and software [1, 8] designs or implementations, including a single-chip exponentiator for GF\((2^{127})\) [13]. This research is motivated by important applications of finite field arithmetic which include: cryptography (multiplication and discrete exponentiation) and error correction coding. Due to hardware complexity, GF\((2^n)\) arithmetic processors have been constrained to fields with \(n < 300\), impractical for the implementation of secure cryptosystems based on the discrete logarithm problem. This paper addresses the computational difficulty of multiplication in GF\((p^n)\) using a normal basis representation of field elements. The result is that by using an optimal normal basis in GF\((2^n)\) and new system architectures [7], a processor for \(n > 1000\) may be realized.

A normal basis in GF\((p^n)\) is a basis \(N\) of the form \(N = \{\beta, \beta p, \beta p^2, \ldots, \beta p^{n-1}\}\). It is well known that a normal basis exists in every finite field [4]. Every \(B \in \text{GF}(p^n)\) may be uniquely expressed in terms of \(N\) as

\[
B = \sum_{i=0}^{n-1} b_i \beta^{p^i}, \quad b_i \in \text{GF}(p).
\]

* This research was supported in part by NSERC Strategic Grant #G1588

Further, let

\[ A = \sum_{i=0}^{n-1} a_i \beta^p^i, \]

and let

\[ C = AB = \sum_{i=0}^{n-1} c_i \beta^p^i \]

where \( c_i \) is referred to as a product digit. Now

\[ C = \left( \sum_{i=0}^{n-1} a_i \beta^p^i \right) \left( \sum_{j=0}^{n-1} b_j \beta^p^j \right) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j \beta^p^i \beta^p^j. \]

The expressions \( \beta^p^i \beta^p^j \) are referred to as cross-product terms. Since \( N \) is a basis for the vector space, we can write

\[ \beta^p^i \beta^p^j = \sum_{k=0}^{n-1} \lambda_{ij}^{(k)} \beta^p^k, \quad \lambda_{ij}^{(k)} \in \text{GF}(p). \]  

(1)

Substitution yields

\[ c_k = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \lambda_{ij}^{(k)} a_i b_j. \]  

(2)

Define a matrix \( T_N \) as follows: index the rows of \( T_N \) by the ordered pairs \((i,j)\), \(0 \leq i, j \leq n-1\). In row \((i,j)\), column \(k\) put \( \lambda_{ij}^{(k)} \), the coefficient of \( \beta^p^k \) in the expansion of \( \beta^p^i \beta^p^j \).

For \( X \in \text{GF}(p^n) \), let \( X = (x_0, x_1, \ldots, x_{n-1}) \) denote the coordinate vector for \( X \) in the basis \( N \). Since \( N \) is normal, we have

\[ A^{p^m} = (a_{-m}, a_{-m+1}, \ldots, a_{-m-1}) \]

where the subscripts are taken modulo \( n \). Also

\[ A^{p^{m-n}} B^{p^{n-m}} = (c_0(A^{p^{m-n}}, B^{p^{n-m}}), c_1(A^{p^{m-n}}, B^{p^{n-m}}), \ldots, c_{n-1}(A^{p^{m-n}}, B^{p^{n-m}})), \]

so equating coefficients yields

\[ c_m(A, B) = c_0(A^{p^{m-n}}, B^{p^{n-m}}). \]  

(3)

Therefore viewing \( c_m \) as a bilinear form, the form \( c_m \) is obtained from \( c_0 \) by an \( m \)-fold cyclic shift of the variables involved. Let \( C_N \) denote the number of nonzero terms in the form \( c_0 \), and therefore \( c_m \), in the basis \( N \).

As an example, consider the prime field \( \text{GF}(2^5) \) as generated by the irreducible polynomial \( f(x) = x^5 + x^2 + 1 \). If we choose \( \alpha \) to be a zero of \( f(x) \) and set \( \beta = \alpha^3 \), then \( N = \{ \beta, \beta^2, \beta^4, \beta^8, \beta^{16} \} \) is a normal basis. The matrix \( T_N \) for this basis is given in Table 1. The value of \( C_N \) in this example is 15. If \( \beta = \alpha^5 \), then \( N = \{ \beta, \beta^2, \beta^4, \beta^8, \beta^{16} \} \) is again a normal basis. Its matrix is given in Table 2, and \( C_N = 9 \) for this basis.
We define $N$ to be an optimal normal basis of $\text{GF}(p^n)$ if and only if $C_N = 2n - 1$. In Section 2, we prove that $C_N \geq 2n - 1$ for all $N$. Constructions for optimal normal bases and extensions to fields $\text{GF}(p^n)$ are presented in Section 3. We then summarize results of normal basis searches and give a conjecture on the existence of optimal normal bases in $\text{GF}(2^n)$ for all $n$. Lastly, we comment on the cryptographic significance of the results.

## 2. The minimum number of terms

We prove that $2n - 1$ is the minimum possible number of terms in (2). The proof of the following theorem is based on an examination of $n$ rows of a submatrix of $T_N$.

**Theorem 2.1.** If $N$ is a normal basis for $\text{GF}(p^n)$ with matrix $T_N$, then $C_N \geq 2n - 1$. 

<table>
<thead>
<tr>
<th>$2^k$</th>
<th>$2^l$</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>16</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>8</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Proof. Let \( N = \{\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}\} \) and, for simplicity, denote \( \beta^{p^i} \) by \( \beta_i \). Since \( N \) is a normal basis, \( \sum_{i=0}^{n-1} \beta_i = \text{trace} \beta. \)

Let \( b \) denote trace \( \beta \). Consider the \( n \times n \) submatrix \( T_0 \) of \( T_N \) consisting of the \( n \) rows of \( T_N \) corresponding to the elements \( \beta_0 \beta_i, \ 0 \leq i \leq n-1 \). Now

\[
b \beta_0 = \beta_0 \sum_{i=0}^{n-1} \beta_i = \sum_{i=0}^{n-1} \beta_0 \beta_i.
\]

Therefore, the sum of the rows of \( T_0 \) is an \( n \)-tuple with a \( b \) in position 1 and zeros elsewhere. Hence, each column of \( T_0 \) contains at least two nonzero elements with the possible exception of column 1 because each column of \( T_0 \) must contain at least one nonzero element since the rows of \( T_0 \) are linearly independent or equivalently, \( \{\beta_0 \beta_i: 0 \leq i \leq n-1\} \) is a basis for \( \text{GF}(p^n) \).

Therefore, the total number of nonzero elements in \( T_0 \) is at least \( 2n-1 \). If we

<table>
<thead>
<tr>
<th>2^i</th>
<th>2^j</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>8</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
define $T_j$ to be the matrix obtained from $T_0$ by raising each element (associated with a row) of $T_0$ to the $p^j$th power, then $\beta_0 \beta_i$ in $T_0$ becomes $\beta_{0+j \mod n} \beta_{i+j \mod n}$ in $T_j$ for $0 \leq i,j \leq n-1$.

From the definition of a normal basis, $T_j$ must also contain a total of at least $2n-1$ nonzero elements. Thus, the total number of nonzero elements in $T_N$ is at least $n(2n-1)$ and since each column has $C_N$ nonzero elements, $C_N \geq 2n-1$. □

**Corollary 2.2.** Given an optimal normal basis in $GF(p^n)$, for every $0 \leq k \leq n-1$, equation (2) will contain two occurrences of subscript $i$ for every $0 \leq i \leq n-1$, and one occurrence of subscript $k$. This is also true for the subscripts $j$.

### 3. Constructions for optimal normal bases

By appropriately choosing $\beta$, we can generate an optimal normal basis $N=\{\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}\}$ in $GF(p^n)$, for certain values of $n$.

**Theorem 3.1.** Suppose that $K=GF(p^n)$ contains $(n+1)$st roots of unity. If the $n$ nonunit roots of unity are linearly independent, then $K$ contains an optimal normal basis.

**Proof.** Let $\beta$ denote a primitive $(n+1)$st root of unity in $k$. Then the conjugates of $\beta$ are $\beta^p, \beta^{p^2}, \ldots, \beta^{p^{n-1}}$. Since $N=\{\beta, \beta^p, \ldots, \beta^{p^{n-1}}\}$ is linearly independent, it is a normal basis for $K$. But $N$ is the set of zeros of $p(x)=(x^{n+1}-1)/(x-1)$; that is, $N$ is the set of $n$ nonunit roots of unity in $K$. Let $\beta_0=\beta$, and $\beta_i=\beta^{p^i}$, $i=1,2,\ldots,n-1$. Recall that the number of nonzero terms in the bilinear form for $c_0$ is also the number of nonzero terms in the expansion of the set $\{\beta_0 \beta_i: i=0,1,\ldots,n-1\}$ in the basis $N$. But if $\beta_i \neq \beta_0^{-1}$, then $\beta_0 \beta_i = \beta_j$ for some exponent $j$ (depending on $i$) whereas

$$\beta_0 \beta_0^{-1} = \sum_{i=0}^{n-1} \beta_i.$$

Hence there are $2n-1$ nonzero terms in the expansion, and $N$ is optimal. □

The above can be restated as below.

**Theorem 3.1'.** The field $K=GF(p^n)$ contains an optimal normal basis consisting of the nonunit $(n+1)$st roots of unity if and only if $n+1$ is a prime and $p$ is primitive in $\mathbb{Z}_{n+1}$.

**Proof.** If $n+1$ is prime, then $n+1$ divides $p^n-1$ and $K$ contains a primitive $(n+1)$st root of unity $\beta$. Since $p$ is primitive in $\mathbb{Z}_{n+1}$, the minimal polynomial of $\beta$ is $(x^{n+1}-1)/(x-1)$ and the nonunit $(n+1)$st roots are linearly independent. Con-
versely if these roots are independent in $K$ then $p$ has order $n$ modulo $n + 1$ and $n + 1$ is prime. \(\square\)

The above theorem cannot produce optimal normal bases in $\text{GF}(p^n)$ for prime $n$ unless $n = 2$. This liability can be overcome in extensions of $\text{GF}(2^n)$ in some instances by the following theorem.

**Theorem 3.2.** If

1. $2$ is primitive in $\mathbb{Z}_{2n+1}$, or
2. $2n + 1$ is a prime congruent to $3$ modulo $4$ and $2$ generates the quadratic residues in $\mathbb{Z}_{2n+1}$,

then there exists an optimal normal basis in $\text{GF}(2^n)$.

**Proof.** Since $2n + 1 | 2^{2n} - 1$, there exists a primitive $(2n + 1)$st root of unity, $\beta$ in $\text{GF}(2^{2n})$. Let 

$$y = \beta + \beta^{-1}.$$ 

Since $2^n \equiv \pm 1 \mod (2n + 1)$, either $\beta^{-1} = \beta^{2^n}$ or $\beta = \beta^{2^n}$. Now 

$$y^{2n} = (\beta + \beta^{-1})^{2n} = \beta^{2n} + \beta^{-2n} = \beta + \beta^{-1} = y.$$ 

Hence, $y$ is an element of the subfield $\text{GF}(2^n)$. We claim that $N = \{y, y^2, y^4, \ldots, y^{2^{n-1}}\}$ is an optimal normal basis of the subfield. If 

$$\sum_{i=0}^{n-1} \lambda_i y^{2^i} = 0,$$

then 

$$\sum_{i=0}^{n-1} \lambda_i (\beta^{2^i} + \beta^{-2^i}) = 0.$$ 

Now since either $2$ is a generator of the multiplicative group of $\text{GF}(2n + 1)$ or $2$ generates the quadratic residues of $\text{GF}(2n + 1)$ with $2n + 1 \equiv 3 \mod 4$ then 

$$\sum_{i=0}^{n-1} \lambda_i (\beta^{2^i} + \beta^{-2^i}) = \sum_{i=0}^{n-1} \lambda_i \beta^{2^i} + \sum_{i=0}^{n-1} \lambda_i \beta^{-2^i} = \sum_{j=1}^{2n} u_j \beta^j,$$

where each $\lambda_i$ occurs in $\{u_1, u_2, \ldots, u_{2n}\}$. Therefore $\beta$ is a zero of the polynomial 

$$f(X) = \sum_{i=0}^{2n-1} u_{i+1} X^i.$$ 

Since $f(\beta) = 0$, the minimal polynomial of $\beta$, $m_\beta(X)$, divides $f(X)$. If hypothesis (1) holds then 

$$m_\beta(X) = 1 + X + X^2 + \cdots + X^{2n}.$$
Since \( m_p(X) \mid f(X) \) we conclude that \( f(X) = 0 \) and all \( \lambda_i = 0 \). If hypothesis (2) holds \( \ell_i \), then \( m_p(X) \) has degree \( n \) as does \( m_{p-1}(X) \) and
\[
X^{2n+1} - 1 = (X-1)m_p(X)m_{p-1}(X).
\]
But \( m_p(X) \mid f(X) \) since \( f(\beta) = 0 \) and \( m_{p-1}(X) \mid f(X) \) since \( f(\beta^{-1}) = 0 \) and, hence, \( 1 + X + X^2 + \cdots + X^{2n} \mid f(X) \) implying that \( f(X) = 0 \) and that all \( \lambda_i = 0 \). Therefore, we conclude that \( N \) is a normal basis for \( GF(2^n) \). The cross-product terms are
\[
\gamma^2 \gamma^{2'} = (\beta^{2} + \beta^{-2'})^{2'} = (\beta^{(2+2')} + \beta^{-(2+2')}) + (\beta^{(2-2')} + \beta^{-(2-2')}).
\]
Now if 2 is primitive modulo \( 2n + 1 \) then each nonzero residue has the form \( 2^k \) for some integer \( k \) satisfying \( 0 \leq k \leq 2n - 1 \), whereas if 2 generates the quadratic residues modulo \( 2n + 1 \) and \( 2n + 1 \) is congruent to 3 modulo 4, then each nonzero residue has the form of either \( 2^k \) or \( -2^k \) for some integer \( k \) satisfying \( 0 \leq k \leq n - 1 \). Therefore if \( 2' \neq 2' \) mod\( (2n+1) \), then there exist integers \( k \) and \( k' \) such that
\[
2' + 2' = \pm 2^k \quad \text{and} \quad 2' - 2' = \pm 2^{k'}
\]
for at least one choice of the + or - sign in each case. In this event,
\[
\gamma^2 \gamma^{2'} = \gamma^{2k} + \gamma^{2k'}.
\]
On the other hand, if \( 2' = \pm 2' \), then one of \( 2' + 2' \) is not zero modulo \( 2n + 1 \), and so there exists a \( k \) such that at least one of the equations
\[
2' + 2' = 2^k, \quad 2' - 2' = -2^k
\]
is satisfied.

In this case, since we are in a field of characteristic 2,
\[
\gamma^2 \gamma^{2'} = \gamma^{2k}.
\]
Let \( \gamma = \gamma_2, 1, 2, \ldots, n - 1 \). Then, since \( \gamma^2 = \gamma_1 \), there are at most \( 2n - 1 \) terms in the expansion of the set \( \{\gamma_0, \gamma \} \) in terms of the basis \( N \), and therefore there are precisely \( 2n - 1 \) such terms and \( n \) is an optimal normal basis. \( \square \)

The result, of course, will hold for any field of characteristic 2.

The minimal polynomial \( M_p(X) \) as defined in Theorem 3.2 can be easily determined recursively. Over \( GF(2) \), define the sequence of polynomials \( f_i(X) \), \( i = 0, 1, 2, \ldots \) as follows. Let
\[
f_0(X) = 1, \quad f_1(X) = X + 1,
\]
and
\[
f_i(X) = Xf_{i-1}(X) + f_{i-2}(X), \quad i \geq 2.
\]
If \( n \) is such that the hypotheses of Theorem 3.2 are satisfied, then \( f_n(X) \) is the minimal polynomial of \( y \). Indeed, it is easily shown by induction that

\[
f_t(Y + Y^{-1}) = 1 + \sum_{i=1}^{t} (Y^i + Y^{-i}).
\]

Therefore

\[
f_n(y) = 1 + \sum_{i=1}^{n} (\beta^i + \beta^{-i}) = 1 + \sum_{i=1}^{2n} \beta^i = 0,
\]

since \( \beta \) is a primitive \((2n + 1)\)st root of unity.

Let \( N = \{y, y^2, \ldots, y^{2^n-1}\} \) be a normal basis over \( \text{GF}(2^n) \). Let \( y^{2^i} = y_i, \ i = 0, 1, \ldots, n \).

The basis \( N \) will be said to be of type I if with the exception of one value of \( i \),
\[0 \leq i \leq n - 1,\] there exists an integer \( k \) satisfying \( 0 \leq k_i \leq n - 1 \) such that \( y_0 y_i = y_{k_i} \).

Clearly every optimal basis constructed by the method of Theorem 3.1 is a type-I basis. The basis \( N \) is said to be of type II if, for every \( i \) satisfying \( 1 \leq i \leq n - 1 \), there exists integers \( k_i \) and \( m_i \) such that

\[y_0 y_i = y_{k_i} + y_{m_i}.
\]

Clearly every optimal basis constructed by the methods of Theorem 3.2 is a type-II basis.

It is easily shown that every type-I basis can be obtained by the construction of Theorem 3.1. It will be shown that every type-II basis can be obtained by the construction of Theorem 3.2.

**Lemma 3.3.** Let \( \beta \) be any element in \( F = \text{GF}(2^n) \). Let \( \delta_0 = 1 \) and \( \delta_i = \beta^i + \beta^{-i}, \ i = 1, 2, \ldots \). Let \( \delta = \delta_1 \). Then, viewing \( F \) as a vector space over \( \text{GF}(2) \), the relation

\[\text{span}\{\delta_0, \delta_1, \delta_2, \ldots, \delta_m\} = \text{span}\{1, \delta, \delta^2, \ldots, \delta^m\}\]

holds for \( m = 1, 2, \ldots \).

**Proof.** The binomial theorem yields the equations

\[\delta^r = \sum_{s=0}^{(r-1)/2} \binom{r}{2s} \delta_{r-2s}, \ r = 0, 1, 2, \ldots \]

Since the coefficient matrix is triangular, having 1's on its main diagonal, it is invertible, and the result follows. \( \square \)

**Corollary 3.4.** The relation

\[\text{dim span}\{\delta_1, \delta_2, \ldots, \delta_m\} = \text{dim span}\{\delta, \delta^2, \ldots, \delta^m\}\]

holds for \( m = 1, 2, 3, \ldots \).

**Theorem 3.5.** Let \( N = \{y, y^2, y^4, \ldots, y^{2^n-1}\} \) be a type-II normal basis in \( \text{GF}(2^n) \).

Then there exists a primitive \((2n + 1)\)th root of unity \( \beta \) (in \( \text{GF}(2^{2n}) \), viewed as an extension of \( \text{GF}(2^n) \)) (if necessary) such that \( y = \beta + \beta^{-1} \).
Proof. Let \( \beta \) be a root of the quadratic equation \( x^2 + \gamma x + 1 = 0 \) where, if necessary, we extend \( \text{GF}(2^n) \) to \( \text{GF}(2^{2n}) \) to have the root defined. Then \( \gamma = \beta + \beta^{-1} \).

Define \( \delta_i \) by \( \delta_i = \beta^i + \beta^{-i}, i = 0, 1, 2, \ldots \). Now \( \delta_0 = 0, \delta_1 = \gamma \). Let \( S_i = \{ \delta_1, \delta_2, \ldots, \delta_i \} \).

By Corollary 3.4, the relation

\[
\dim \text{span } S_n = \dim \text{span} \{ \gamma, \gamma^2, \ldots, \gamma^n \}
\]

holds. Since \( N \) consists of \( \gamma \) and its algebraic conjugates, its minimal polynomial has degree \( n \), so \( \{ \gamma, \gamma^2, \ldots, \gamma^n \} \) is a linearly independent set. Therefore \( \delta_1, \delta_2, \ldots, \delta_n \) are all distinct.

The next step is to show that \( S_n = N \). We proceed by induction to show that \( S_i \subseteq N \), for \( i = 1, 2, \ldots, 2^n \). As noted \( S_1 = \{ \gamma \} \subseteq N \). Let \( k \) be the least value greater than one such that \( S_k \subseteq N \), and assume that \( k \leq 2n \).

Suppose first that \( k \) is even, that is, \( k = 2s \) for some integers \( s < k \). So \( \delta_k \in N \). But

\[
\delta_{2s} = (\beta^{2s} + \beta^{-2s}) = (\beta^s + \beta^{-s})^2 \in N.
\]

This implies that

\[
S_k = S_{k-1} \cup \{ \delta_{2s} \} \subseteq N,
\]

so the only possibility is that \( k \) is an odd number, say \( k = 2s + 1 \), where again \( s < n \).

As a notational convenience, let \( \gamma_i = \gamma^{2^i}, i = 0, 1, \ldots, n - 1 \).

Since \( \delta_i = \beta^i + \beta^{-i} \), for \( i \geq j \geq 0 \), the identity

\[
\delta_i \delta_j = \delta_{i+j} + \delta_{i-j}
\]

is valid. Applying this yields

\[
\delta_{2s+1} = \delta_2 \delta_{s+1} + \delta_1.
\]

Since \( s + 1 < 2s + 1 = k \), we have \( \{ \delta_2, \delta_{s+1} \} \subseteq N \). Further since \( k \leq 2n \) and \( k \) is odd, we have \( k \leq 2n - 1 \), so \( s + 1 \leq n \) and therefore \( \delta_s \neq \delta_{s+1} \). Therefore there exist distinct integers \( r \) and \( u \) satisfying \( 0 \leq r, u \leq n - 1 \) such that

\[
\delta_s \delta_{s+1} = \gamma_r + \gamma_u,
\]

since \( N \) is of type II. Therefore

\[
\delta_{2s+1} = \gamma_r + \gamma_u + \gamma_0.
\]

On the other hand

\[
\delta_1 \delta_{2s+1} = \delta_{2s+2} + \delta_{2s} = (\delta_{s+1})^2 + (\delta_s)^2 = \gamma_t + \gamma_v
\]

for some integers \( t \) and \( v \) satisfying \( 0 \leq t, v \leq n - 1 \). Since \( \delta_1 \delta_{2s+1} \neq 0 \), this quantity is written uniquely in the basis \( N \) as a sum of exactly two nonzero terms. However

\[
\delta_1 \delta_{2s+1} = \gamma_r \gamma_r + \gamma_r \gamma_u + \gamma_0 \gamma_v,
\]

which has an odd number of terms unless one of \( r \) or \( u \), is zero. Therefore

\[
\delta_{2s+1} = \gamma_r + \gamma_0 + \gamma_0 = \gamma_r \in N.
\]
This again implies that $\delta_k \in N$, which contradicts the definition of \( k \). This contradiction arises from the assumption that \( k \leq 2n \). Therefore \( S_k \subseteq N \) for \( k \leq 2n \), and \( S_k \subseteq N \). Since both \( S_n \) and \( N \) contain \( n \) distinct elements, it follows that \( S_n = N \). It remains to show that \( \beta^{2n+1} = 1 \), and that \( \beta^t \neq 1 \) for \( 1 \leq t \leq 2n \).

Note that \( \beta^t = 1 \) implies that \( \delta_t = 0 \). Since \( S_t \subseteq N \) for \( t \leq 2n \), and \( 0 \notin N \), then \( \beta^t \neq 1 \) for \( 1 \leq t \leq 2n \). Moreover since \( S_{n+1} \) contains only \( n \) distinct elements, we have \( \delta_{n+1} = \delta_s \) for some \( s \) satisfying \( 1 \leq s \leq n \). If \( \delta_{n+1} = \delta_s \), then

\[
\beta^{n+1} + \beta^s = \beta^{-n-1} + \beta^{-s} = (\beta^{n+1} + \beta^s)/\beta^{n+1+s}.
\]

Thus \( \beta^{n+1} = \beta^s \) or \( \beta^{n+1+s} = 1 \). Therefore either \( \beta^{n+1-s} = 1 \), which is impossible by the above, or \( \beta^{n+1+s} = 1 \), which implies \( s = n \), and \( \beta^{2n+1} = 1 \). \( \Box \)

Corollary 3.6. Suppose there exists a type-II normal basis \( N \) in \( GF(2^n) \). Then \( 2n+1 \) is a prime \( p \) and either

1. \( 2 \) generates the nonzero elements of \( \mathbb{Z}_{2n+1} \), or
2. \( p \equiv 3 \mod 4 \) and \( 2 \) generates the quadratic residues in \( \mathbb{Z}_{2n+1} \).

Proof. (A sketch is given here. We use the notation developed in the proof of Theorem 3.5.) Note that for each \( \gamma \in N \), there exists a pair of distinct primitive \((2n+1)\)st roots of unity, \( \beta \) and \( \beta^{-1} \). Thus there are \( 2n \) primitive \((2n+1)\)st roots of unity, the number \( 2n+1 \) is a prime. Now suppose neither (1) nor (2) holds. Then

\[
\text{trace}(\beta + \beta^{-1}) = \sum_{i=1}^{n-1} \beta^{2i} + \sum_{i=0}^{n-1} \beta^{-2i} = \sum (\beta^{2i} + \beta^{-2i})
\]

(where \( j \) can be taken to run through a proper subset of \( \{0, 1, 2, \ldots, n-1\} \))

\[
= \sum \gamma^{2j}.
\]

Since \( \text{trace}(\beta + \beta^{-1}) \in GF(2) \) we have either a proper subset of \( N \) summing to zero, which is impossible since \( N \) is a linearly independent set over \( GF(2) \), or a proper subset of \( N \) sums to one, which is again impossible, since 1 has the unique representation in the basis \( N \) given by the sum of all elements of \( N \). Therefore either (1) or (2) must hold. \( \Box \)

Consideration of the above shows that all type-II normal bases are obtainable by the methods of Theorem 3.2.

If \( A = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\} \) and \( B = \{\beta_0, \beta_1, \ldots, \beta_{n-1}\} \) are two bases of an extension field \( F' \) over a finite field \( F \), the \( A \) and \( B \) are called dual bases or complementary bases if \( \text{trace}(\alpha_i \beta_j) = \delta_{ij} \) where \( \delta_{ij} \) is, as usual, the Kronecker \( \delta \). It is clear that any type-II optimal normal basis is selfdual. Lempel and Weinberger [2] have shown that \( GF(q^n) \) admits a selfdual normal basis over \( GF(q) \) for even \( q \) if and only if \( n \) is not divisible by 4. Therefore, in light of Theorem 3.2, 2 cannot be primitive
modulo $p$ where $p$ is a prime congruent to 1 modulo 8, which is also true since 2 is a quadratic residue modulo $p$ in this case (by the law of quadratic reciprocity).

It is also known (see [3, p.68]) that

(a) 2 is primitive in $\mathbb{Z}_p$ for a prime $p$ if $p = 4q + 1$ and $q$ is an odd prime,
(b) 2 is primitive in $\mathbb{Z}_p$ for a prime $p$ if $p = 2q + 1$ where $q$ is a prime congruent to 1 modulo 4, and
(c) $-2$ is primitive in $\mathbb{Z}_p$ for a prime $p$ if $p = 4q + 1$ where $q$ is a prime congruent to 3 modulo 4. (In this case, then, 2 is a generator of the quadratic residues in $\mathbb{Z}_p$.)

In view of these results, the testing of the hypotheses in Theorems 3.1 and 3.2 becomes easier in certain cases.

<table>
<thead>
<tr>
<th>$n$</th>
<th>Number of normal bases</th>
<th>$\min C_N$</th>
<th>$\max C_N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>3*</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>5*</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>7*</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>9*</td>
<td>15</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>11*</td>
<td>17</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>19</td>
<td>27</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>21</td>
<td>35</td>
</tr>
<tr>
<td>9</td>
<td>21</td>
<td>17*</td>
<td>45</td>
</tr>
<tr>
<td>10</td>
<td>48</td>
<td>19*</td>
<td>61</td>
</tr>
<tr>
<td>11</td>
<td>93</td>
<td>21*</td>
<td>71</td>
</tr>
<tr>
<td>12</td>
<td>128</td>
<td>23*</td>
<td>83</td>
</tr>
<tr>
<td>13</td>
<td>315</td>
<td>45</td>
<td>101</td>
</tr>
<tr>
<td>14</td>
<td>448</td>
<td>27*</td>
<td>135</td>
</tr>
<tr>
<td>15</td>
<td>675</td>
<td>45</td>
<td>137</td>
</tr>
<tr>
<td>16</td>
<td>2048</td>
<td>85</td>
<td>157</td>
</tr>
<tr>
<td>17</td>
<td>3825</td>
<td>81</td>
<td>177</td>
</tr>
<tr>
<td>18</td>
<td>5376</td>
<td>35*</td>
<td>243</td>
</tr>
<tr>
<td>19</td>
<td>13797</td>
<td>117</td>
<td>229</td>
</tr>
<tr>
<td>20</td>
<td>24576</td>
<td>63</td>
<td>257</td>
</tr>
<tr>
<td>21</td>
<td>27783</td>
<td>95</td>
<td>277</td>
</tr>
<tr>
<td>22</td>
<td>95232</td>
<td>63</td>
<td>363</td>
</tr>
<tr>
<td>23</td>
<td>182183</td>
<td>45*</td>
<td>325</td>
</tr>
<tr>
<td>24</td>
<td>262144</td>
<td>105</td>
<td>375</td>
</tr>
<tr>
<td>25</td>
<td>629145</td>
<td>93</td>
<td>383</td>
</tr>
<tr>
<td>26</td>
<td>1290240</td>
<td>51*</td>
<td>555</td>
</tr>
<tr>
<td>27</td>
<td>1835001</td>
<td>141</td>
<td>443</td>
</tr>
<tr>
<td>28</td>
<td>3670016</td>
<td>55*</td>
<td>$\geq 515$</td>
</tr>
<tr>
<td>29</td>
<td>9256395</td>
<td>57*</td>
<td>$\geq 505$</td>
</tr>
<tr>
<td>30</td>
<td>11059200</td>
<td>59*</td>
<td>$\geq 587$</td>
</tr>
</tbody>
</table>
4. Existence of optimal normal bases

Complete computer searches for optimal normal bases in GF(2^n), 2 ≤ n ≤ 30 were performed (Table 3). Of course, for those values of n that satisfy the criteria of either Theorem 3.1 or Theorem 3.2, an optimal normal basis N in GF(2^n) was found (indicated by a * in Table 3). No other optimal normal bases were found for n ≤ 30.

We observed that the upper bound on the number of terms in (2), tabulated in the rightmost column of Table 3, appears to increase quadratically with n. In fact, we performed thousands of runs for n = 127 and n = 1279 by randomly generating normal bases N, only to find that C_N was approximately 4,000 and 800,000 respectively. These results illustrate the necessity of using optimal normal bases in the implementations of GF(2^n) normal basis multipliers for n > 100.

A complete list of n < 1200 for which we can construct an optimal normal basis in GF(2^n) (Table 4) has 23% of all possible values of n. The results of this section lead to the following:

**Conjecture.** If n does not satisfy the criteria for Theorem 3.1 or Theorem 3.2, then GF(2^n) does not contain an optimal normal basis.
5. Conclusions

The complexity of multiplication in \( \text{GF}(p^n) \) using a normal basis representation of the field elements is critically dependent upon the particular basis chosen. The results presented in this paper, along with new architectures [6] for custom integrated circuits implementing \( \text{GF}(2^n) \) arithmetic [7], indicate that the construction of an arithmetic processor for \( n \sim 1000 \) is feasible.

References