GAUSS PERIODS, PRIMITIVE NORMAL BASES, AND FAST EXPONENTIATION IN FINITE FIELDS

SHUHONG GAO, JOACHIM VON ZUR GATHEN AND DANIEL PANARIO

ABSTRACT. Gauss periods can be used to implement arithmetic in finite fields efficiently and to construct primitive (self-dual) normal bases. With these methods, exponentiation of an arbitrary element in $\mathbb{F}_{q^n}$ can be done with $O(n^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_q$, and exponentiation of a Gauss period with $O(n^2)$ operations in $\mathbb{F}_q$, for a small prime power q and infinitely many integers n. Experimental results indicate that Gauss periods almost always have high multiplicative order and are frequently (more than half the time) primitive elements over $\mathbb{F}_2$. In fact, for every $n \leq 527$ not divisible by 8, we find a primitive Gauss period in $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Thus Gauss periods in finite fields generate many primitive (self-dual) normal bases.

1. INTRODUCTION

For a prime power q and an integer $n \geq 2$, let $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ be finite fields with q and q^n elements, respectively. An element $\alpha \in \mathbb{F}_{q^n}$ is *normal* over $\mathbb{F}_q$ if and only if its conjugates $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are linearly independent over $\mathbb{F}_q$. When α is normal, the basis $(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$ is the *normal basis* generated by α. If α is also primitive, i.e., has multiplicative order $q^n - 1$, then α is a *primitive normal element*, and the basis generated by it is a *primitive normal basis*.

The existence of primitive normal elements in finite fields is established by Carlitz (1952), Davenport (1968), and Lenstra & Schoof (1987). There is currently no efficient algorithm for constructing primitive normal elements in finite fields, since already the efficient construction of a primitive element is a difficult open problem. However, von zur Gathen & Giesbrecht (1990) reduce the first problem to the second one probabilistically in polynomial time; see Stepanov & Shparlinski (1990) for a different approach.

This paper discusses a method for constructing primitive normal bases in finite fields. Our method is based on Gauss periods, introduced by Gauss in 1796 to investigate when a regular polygon can be constructed by ruler and compass (Gauss 1801, articles 343–366). Gauss periods were originally defined in cyclotomic number fields. One can adapt the definition to any finite Galois extension of fields, including finite fields. Here we only give the definition for finite fields.

Let $r = nk + 1$ be a prime not dividing q, and $\mathcal{K}$ the unique subgroup of order k of the multiplicative group of $\mathbb{Z}_r$. Let $\mathcal{K}_0, \ldots, \mathcal{K}_{n-1}$ be the cosets of $\mathcal{K}$ in $\mathbb{Z}_r^\times$. Since r divides

$q^{nk}-1$, there is a primitive rth root of unity $\beta \in \mathbb{F}_{q^{nk}}$. For $0 \le i < n$, define

$$\alpha_i = \sum_{a \in \mathcal{K}_i} \beta^a.$$

Then $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ are called *Gauss periods* of type (n,k) over $\mathbb{F}_q$. It is easy to see that a Gauss period of type (n,k) over $\mathbb{F}_q$ belongs to $\mathbb{F}_{q^n}$, and the set of Gauss periods of type (n,k) does not depend on the particular choice of β as a primitive rth root of unity.

Gauss periods have been used to construct normal bases in finite fields by Mullin et al. (1989) and Ash et al. (1989). The texts by Menezes et al. (1993) and Jungnickel (1993) present detailed discussions. Wassermann (1990) gives the exact condition for a Gauss period of type (n,k) to form a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In Section 2, we give a slightly different form of the condition, and we prove that the normal basis is self-dual if and only if k is even and divisible by the characteristic of $\mathbb{F}_q$.

A fundamental question for applications is how to do arithmetic fast in finite fields, i.e., addition, multiplication, division, and exponentiation. A polynomial representation of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is of the form $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f)$, where $f \in \mathbb{F}_q[x]$ is irreducible of degree n, and every element of $\mathbb{F}_{q^n}$ is represented by a polynomial in $\mathbb{F}_q[x]$ of degree less than n. In such a representation, these three operations can be done with $O(n)$, $O(n \log n \operatorname{loglog} n)$, and $O(n^2 \log n \operatorname{loglog} n \log q)$ operations in $\mathbb{F}_q$, respectively, with fast multiplication (Schönhage & Strassen 1971, Schönhage 1977, and Cantor & Kaltofen 1991) and repeated squaring. (We may always assume an exponent to be less than q^n.) Popular belief has long held that fast multiplication is advantageous only for exceedingly large inputs. Shoup's (1993) clever implementation proved that fast multiplication is better than classical multiplication for polynomials of degree ≥ 25 over $\mathbb{F}_p$, where p has about 100 bits. However, we are unaware of any implementation comparing fast multiplication to the Karatsuba-Ofman algorithm.

When $\mathbb{F}_{q^n}$ is represented by a normal basis, the qth power of an element is just a cyclic shift of its coordinates. Agnew et al. (1988), Stinson (1990, for $q=2$) and von zur Gathen (1991) show that in any normal basis exponentiation can be computed with $O(n/\log_q n)$ multiplications in $\mathbb{F}_{q^n}$ for q small (compared to n), with a storage for $O(n/\log_q^2 n)$ elements of $\mathbb{F}_{q^n}$. The question is how to implement multiplication fast under normal bases. The recent hardware implementations of large finite fields (Massey & Omura 1986, Onyszchuk et al. 1988, Agnew et al. 1991, 1993) exploit the symmetry in the multiplication table of a normal basis. In an attempt to minimize hardware cost, Mullin et al. (1989) introduce optimal normal bases. For a normal basis $N = (\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}})$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, the number of nonzero terms in the n products $\alpha\alpha^{q^i}$ expressed in the basis N itself is at least $2n-1$. If it is equal to $2n-1$, then N is called optimal. Under an optimal normal basis, hardware cost (i.e., the number of cell connections) is minimized to $2n-1$ (for $q=2$) in the designs used by Massey & Omura (1986) and Onyszchuk et al. (1988). But the total number of operations in $\mathbb{F}_q$ required for one multiplication in $\mathbb{F}_{q^n}$ is still about n^2, and exponentiation in $\mathbb{F}_{q^n}$ needs about $n^3/\log n$ operations in $\mathbb{F}_q$. Can we reconcile fast multiplication and division with normal bases?

We answer this question affirmatively in Section 3, where fast arithmetic is implemented in $\mathbb{F}_{q^n}$ when represented by a normal basis generated by Gauss periods of type (n,k) with k constant. In this case, multiplication and division can be also done with $O(n \log n \operatorname{loglog} n)$ and $O(n \log^2 n \operatorname{loglog} n)$ operations in $\mathbb{F}_q$, respectively. Together with Agnew et al. (1988), Stinson (1990) and von zur Gathen (1991), we find that exponentiation in $\mathbb{F}_{q^n}$ can be done in $O(n^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_q$ when q is small (with a storage for $O(n/\log_q^2 n)$ elements of $\mathbb{F}_{q^n}$). This proves that normal bases offer some asymptotic computational advantage over polynomial bases. We do not have an implementation, and so it is not clear at what input sizes this method becomes more efficient in practice than other approaches.

Brickell et al. (1992) show that in a polynomial basis, exponentiation can be executed with $O(n/\log n)$ multiplications in $\mathbb{F}_{q^n}$, thus $O(n^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_q$; their algorithm seems to require a preprocessing stage of about n multiplications in $\mathbb{F}_{q^n}$ and storage for $O(n/\log n)$ elements from $\mathbb{F}_{q^n}$.

After the work presented here was done, Shoup (1994) discovered a different method of achieving exponentiation in $\mathbb{F}_{2^n}$ with $O(n^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_2$ and storage for $O(n/\log n)$ elements from $\mathbb{F}_{2^n}$. His algorithm uses polynomial bases and fast matrix multiplication, say à la Strassen (1969). Shoup (private communication, 1994) also points out that if $\mathbb{F}_{2^n}$ is presented as $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f)$ with $f = x^n + g$ irreducible and $g \in \mathbb{F}_2[x]$ of small degree, say $\deg g \leq 2 \log n$, then a similar time bound can be achieved. It seems reasonable to conjecture that such an f exists for each n. In fact, for $n \leq 1000$, one can always take $\deg g \leq 2 + \log_2 n$.

In Section 4, we consider a special exponentiation problem, and give a method for computing a power of a Gauss period of type (n,k) in $\mathbb{F}_{q^n}$ with $O(n^2 q k)$ operations in $\mathbb{F}_q$. When k and q are small, this is faster than exponentiation of an arbitrary element. No storage is required here.

In Section 5, we mention some results on the existence of k such that Gauss periods of type (n,k) over $\mathbb{F}_q$ form a normal basis, and a result on the size of smallest such k assuming the Extended Riemann Hypothesis. We also remark on the implication of these results on constructing irreducible polynomials and normal bases in finite fields.

Section 6 reports on experimental results on the multiplicative orders of Gauss periods of type (n,k) over $\mathbb{F}_q$ for $3 \leq k \leq 20$, $2 \leq n \leq 1200$, and $q = 2$. They were done with the algorithm from Section 4. The case $k = 2$ has been dealt with by Gao and Vanstone (1994). Our experiments show that a large portion of Gauss periods are primitive elements. This leads us to believe that for every n not divisible by 8 there is a suitable k such that Gauss periods of type (n,k) are primitive in $\mathbb{F}_{2^n}$. We verified this for all $n < 527$. (When $m \geq 527$, the factors of $2^m - 1$ were often not known by the time we did our computations.) When k is even, since the normal basis formed by Gauss periods of type (n,k) over $\mathbb{F}_2$ is self-dual, our experiments indicate that Gauss periods also induce a large number of self-dual primitive normal bases in finite fields over $\mathbb{F}_2$. No systematic construction of self-dual primitive normal bases seems to be in the literature, though there are explicit constructions of self-dual normal bases (Lempel & Seroussi 1991, Blake et al. 1994, Poli

1995).

Since Gauss periods have high multiplicative orders and are easy to exponentiate, they are useful in cryptosystems where one needs a fixed primitive element such that large powers of it are easy to compute. An industrial example is the Calmos (1988) cryptoprocessor, whose fundamental operation is exponentiation in $\mathbb{F}_{2^{593}}$ (see also Rosati 1989). They are also useful in generating secure random sequences, particularly exponential pseudorandom number (or bit) generators. Gauss periods (in finite fields and in number fields) are also useful in the study of the algebraic structure of field extensions (Pohst & Zassenhaus 1989, Washington 1982), and in integer factorization (Bach & Shallit 1989).

2. Normal bases generated by Gauss periods

In this section, we discuss when Gauss periods generate normal bases in finite fields and when the normal bases generated are self-dual.

Theorem 2.1. *Suppose that $r = nk + 1$ is a prime not dividing q, and e is the order of q modulo r. Let $\mathcal{K}$ be the unique subgroup of order k of the multiplicative group of $\mathbb{Z}_r$. Let β be a primitive rth root of unity in $\mathbb{F}_{q^r}$. Then the Gauss period*

$$\alpha = \sum_{a \in \mathcal{K}} \beta^a$$

is a normal element in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $\gcd(nk/e, n) = 1$.

Proof. If two subgroups of a cyclic additive group have indices i_1 and i_2, then the subgroup generated jointly by the two has index $\gcd(i_1, i_2)$. For the subgroups $\mathcal{K}$ and $<q>$ of $\mathbb{Z}_r^\times$, of indices n and nk/e, respectively, this means that

$$\gcd(nk/e, n) = 1 \quad \Longleftrightarrow \quad \mathbb{Z}_r^\times = <q, \mathcal{K}> .$$

The latter condition is equivalent to α being normal over $\mathbb{F}_q$ (see Wassermann 1990, or 1993, Theorem 3.1.3). □

We say that a pair (n, k) is *admissible* for q if $r = nk + 1$ is a prime not dividing q and $\gcd(nk/e, n) = 1$, where e is the order of q modulo r. When q is understood, we simply say that (n, k) is admissible, and also that k is admissible for n. The condition $\gcd(nk/e, n) = 1$ can be easily verified, without actually calculating e, by checking that $q^{nk/\ell} \not\equiv 1 \bmod r$ for every prime divisor ℓ of n, since

$$\gcd(nk/e, n) = 1 \Longleftrightarrow \forall \ell, \quad \ell \nmid \frac{nk}{e} \Longleftrightarrow \forall \ell, \quad e \nmid \frac{nk}{\ell} \Longleftrightarrow \forall \ell, \quad q^{nk/\ell} \not\equiv 1 \bmod r.$$

We should also remark that for $q = 2$, if either $8|n$, or $4|n$ and $2|k$, or $2|n$ and $4|k$, then (n, k) is never admissible for q, since if $8|(r-1)$ then 2 is a quadratic residue modulo r.

In the remainder of this paper, we assume that (n, k) is admissible and $r = nk + 1$. We fix the order of Gauss periods as follows. For $i \geq 0$, we define

$$\mathcal{K}_i = \{aq^i : a \in \mathcal{K}\} \subseteq \mathbb{Z}_r^\times, \quad \alpha_i = \sum_{a \in \mathcal{K}_i} \beta^a. \tag{1}$$

Then $\mathcal{K}_0 = \mathcal{K}$ and $\alpha_0 = \alpha$. Since $\mathcal{K}_i = \mathcal{K}_{i-1}q = \mathcal{K}q^i$, we have $\alpha_i = \alpha_{i-1}^q = \alpha^{q^i}$. Then $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ is a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

To do arithmetic in $\mathbb{F}_{q^n}$, we need to know the products $\alpha_i\alpha_j$ expressed again in the basis $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$. For $0 \le j, h < n$, let t_{jh} be the number of elements $a \in \mathcal{K}_j$ such that $1 + a \in \mathcal{K}_h$, i.e.,

$$t_{jh} = |(1 + \mathcal{K}_j) \cap \mathcal{K}_h|. \tag{2}$$

In the theory of cyclotomy (Storer 1967), the t_{jh} are called cyclotomic numbers. Let $j_0 < n$ be the unique index such that $-1 \in \mathcal{K}_{j_0}$. If k is even then $j_0 = 0$, and if k is odd then $j_0 = n/2$. For $0 \le j < n$, let

$$\delta_j = \begin{cases} 0 & \text{if} \quad j \ne j_0, \\ 1 & \text{if} \quad j = j_0. \end{cases}$$

Lemma 2.2. *For $0 \le i, j < n$,*

$$\left(\sum_{a\in\mathcal{K}} x^{aq^i}\right)\left(\sum_{b\in\mathcal{K}} x^{bq^j}\right) \equiv k\delta_{j-i} + \sum_{0\le h<n} t_{j-i\,h}\left(\sum_{a\in\mathcal{K}} x^{aq^{i+h}}\right) \bmod \Phi_r, \tag{3}$$

where $\Phi_r = (x^r - 1)/(x - 1)$ is the rth cyclotomic polynomial, and the subscripts of δ and t are reduced modulo n.

Proof. Since $x^r \equiv 1 \bmod \Phi_r$, if $a \equiv b \bmod r$ then $x^a \equiv x^b \bmod \Phi_r$. Therefore

$$\left(\sum_{a\in\mathcal{K}} x^{aq^i}\right)\left(\sum_{b\in\mathcal{K}} x^{bq^j}\right) \equiv \sum_{a,b\in\mathcal{K}} x^{aq^i+bq^j} \equiv \left(\sum_{a,b\in\mathcal{K}} x^{a(1+bq^{j-i})}\right)^{q^i} \bmod \Phi_r.$$

For each $b \in \mathcal{K}$, either $1 + bq^{j-i} \equiv 0 \bmod r$, or $1 + bq^{j-i} \in \mathcal{K}_h$ for a unique h with $0 \le h < n$. If $1 + bq^{j-i} \equiv 0 \bmod r$ then

$$\sum_{a\in\mathcal{K}} x^{a(1+bq^{j-i})} \equiv k \bmod \Phi_r.$$

If $1 + bq^{j-i} \in \mathcal{K}_h$, then

$$\sum_{a\in\mathcal{K}} x^{a(1+bq^{j-i})} \equiv \sum_{a\in\mathcal{K}} x^{aq^h} \bmod \Phi_r.$$

So (3) follows from a direct counting when b runs through $\mathcal{K}$. □

Since β is a root of Φ_r, by replacing x by β in the above Lemma, the next result follows immediately.

Theorem 2.3. *For any $0 \le i, j < n$,*

$$\alpha_i\alpha_j = k\delta_{j-i} + \sum_{0\le h<n} t_{j-i\,h}\alpha_{h+i} = \sum_{0\le h<n} (t_{j-i\,h} - k\delta_{j-i})\alpha_{h+i}. \tag{4}$$

The $n \times n$-matrix (t_{jh}) is called the multiplication table of the normal basis. Since $1+\mathcal{K}_j$ has k nonzero elements if $j \neq j_0$ and $k-1$ if $j = j_0$, there are at most k nonzero t_{jh} for any j. So the n products $\alpha\alpha_j$ have at most $n(k+1)-1$ nonzero terms, including the k in $\alpha\alpha_{j_0}$. In practice, one should store the matrix (t_{jh}) sparsely when k is small.

When $k = 1$, or $k = 2$ and $q = 2$ (thus $k = 0$ in $\mathbb{F}_q$), the normal bases generated by Gauss periods are optimal (Mullin et al. 1989). For more information, see Gao & Lenstra (1992) and Menezes et al. (1993, chapter 5).

Since self-dual bases are useful in implementing finite fields (Berlekamp 1982, Geiselmann & Gollmann 1989, Jungnickel 1993, Wang 1989), we next determine when normal bases formed by Gauss periods are self-dual.

Let $(\gamma_1, \gamma_2, \ldots, \gamma_n)$ and $(\delta_1, \delta_2, \ldots, \delta_n)$ be two bases for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. They are said to be dual to each other if $Tr(\gamma_i\delta_j) = 0$ when $i \neq j$, and 1 when $i = j$, where Tr denotes the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$: $Tr(A) = A + A^q + \cdots + A^{q^{n-1}}$ for $A \in \mathbb{F}_{q^n}$. One can prove that for any basis there is a unique dual basis. If a basis is dual to itself, we say it is self-dual. We now determine the dual basis of the normal basis generated by a Gauss period.

Theorem 2.4. *Let α_i, j_0 be as in Theorem 2.3, and $\gamma = (\alpha_{j_0} - k)/r$. Then $(\gamma, \gamma^q, \ldots, \gamma^{q^{n-1}})$ is the dual basis of $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$.*

Proof. We know that Tr is a linear functional over $\mathbb{F}_q$, and $Tr(\alpha_i) = -1$ for $0 \leq i < n$. Theorem 2.3 implies that for all $0 \leq i, j < n$, $Tr(\gamma^{q^i}\alpha_j)$ is 0 if $i \neq j$, and is 1 if $i = j$. □

Corollary 2.5. *For $n > 2$, a normal basis of Gauss periods of type (n,k) over $\mathbb{F}_q$ is self-dual if and only if k is even and divisible by the characteristic of $\mathbb{F}_q$.*

Proof. We know that

$$\gamma = (\alpha_{j_0} - k)/r = \frac{1}{r}\,\alpha_{j_0} + \sum_{0 \leq l < n} \frac{k}{r}\,\alpha_l.$$

Thus $\gamma = \alpha$ if and only if $j_0 = 0$ and k is divisible by the characteristic of $\mathbb{F}_q$. Note that $j_0 = 0$, i.e., $-1 \in \mathcal{K}$, if and only if k is even. □

When $q = 2$, a different form of the above result appears in Ash et al. (1989) and Theorem 5.1.5 of Jungnickel (1993). Lempel & Weinberger (1988) show that $\mathbb{F}_{q^n}$ has a self-dual normal basis over $\mathbb{F}_q$ if and only if either n is odd or $n \equiv 2 \mod 4$ and q is even.

3. Efficient arithmetic

In this section, we show how multiplication and division can be done efficiently in finite fields represented under normal bases generated by Gauss periods.

Theorem 3.1. *Suppose that $\mathbb{F}_{q^n}$ is represented by a normal basis over $\mathbb{F}_q$ generated by a Gauss period of type (n,k). Then multiplication in $\mathbb{F}_{q^n}$ can be computed with $O(nk \log(nk) \operatorname{loglog}(nk))$, division with $O(nk \log^2(nk) \operatorname{loglog}(nk))$ and exponentiation with $O(n^2 k \log(k)$*

$\mathrm{loglog}(nk))$ *operations in* $\mathbb{F}_q$*, for exponents less than* q^n *and small* q*, say* $q^5 \le n$*. Exponentiation requires storage for* $O(n/\log_q^2 n)$ *elements of* $\mathbb{F}_{q^n}$*.*

Proof. We may assume that we have $\alpha, \beta, \alpha_i, \mathcal{K}_i$ for $0 \le i < n$ as in Section 2. Then $(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$ is the normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ generated by Gauss periods of type (n,k). Let

$$A = \sum_{0 \le i < n} a_i \alpha_i, \quad B = \sum_{0 \le i < n} b_i \alpha_i \in \mathbb{F}_{q^n},$$

with all $a_i, b_i \in \mathbb{F}_q$, be arbitrary elements of $\mathbb{F}_{q^n}$. We want to compute $C = A \cdot B = \sum_{0 \le i < n} c_i \alpha_i$, with $c_i \in \mathbb{F}_q$.

For $A = \sum_{0 \le i < n} a_i \alpha_i \in \mathbb{F}_{q^n}$, we have

$$A = \sum_{0 \le i < n} a_i \sum_{j \in \mathcal{K}_i} \beta^j = \sum_{1 \le j \le nk} a'_j \beta^j,$$

where $a'_j = a_i$ if $j \in \mathcal{K}_i$. We let $\mathcal{R} = \mathbb{F}_q[x]/(\Phi_r)$, where $\Phi_r = (x^{nk+1} - 1)/(x-1) = x^{nk} + \cdots + x + 1 \in \mathbb{F}_q[x]$ is the rth cyclotomic polynomial, and $\xi = x \bmod \Phi_r \in \mathcal{R}$. $\mathcal{R}$ has the two bases $(1, \xi, \cdots, \xi^{nk-1})$ and $(\xi, \xi^2, \cdots, \xi^{nk})$ over $\mathbb{F}_q$, and it is easy to go from one basis to another:

$$\sum_{0 \le i < nk} a_i \xi^i = (-a_0)\xi^{nk} + \sum_{1 \le i < nk} (a_i - a_0)\xi^i, \quad \sum_{1 \le i \le nk} a_i \xi^i = \sum_{0 \le i < nk} (a_i - a_{nk})\xi^i.$$

We define a map $\varphi : \mathbb{F}_{q^n} \longrightarrow \mathcal{R}$ by

$$\varphi(A) = \sum_{1 \le j \le nk} a'_j \xi^j \in \mathcal{R}.$$

Obviously φ is injective and additive. We have $\varphi(\alpha_i) = \sum_{a \in \mathcal{K}} \xi^{aq^i}$ for $0 \le i < n$, and by Theorem 2.3, $\varphi(\alpha_i \alpha_j) = k\delta_{j-i} + \sum_{0 \le h < n} t_{j-ih} \left(\sum_{a \in \mathcal{K}} \xi^{aq^{i+h}} \right)$. It follows from Lemma 2.2, replacing x by ξ, that $\varphi(\alpha_i \alpha_j) = \varphi(\alpha_i)\varphi(\alpha_j)$ for $0 \le i, j < n$. So φ is multiplicative, hence a ring homomorphism. Furthermore, $\varphi(\mathbb{F}_{q^n})$ is equal to the subring

$$\mathcal{R}' = \{c_1 \xi + \ldots + c_{nk} \xi^{nk} \in \mathcal{R} \colon c_1, \ldots, c_{nk} \in \mathbb{F}_q \text{ and } c_j = c_{j'} \text{ for } 0 \le i < n \text{ and } j, j' \in \mathcal{K}_i\}$$

of $\mathcal{R}$. Thus $\varphi(A)$ is invertible in $\mathcal{R}$ for every nonzero $A \in \mathbb{F}_{q^n}$.

To compute $C = A \cdot B \in \mathbb{F}_{q^n}$, we first multiply the two polynomials $A^*, B^* \in \mathbb{F}_q[x]$ of degree at most nk and with constant term zero, corresponding to $\varphi(A), \varphi(B)$, respectively, with $O(nk \log(nk) \mathrm{loglog}(nk))$ operations in $\mathbb{F}_q$. Then we reduce all exponents modulo r, in effect reducing A^*B^* modulo $x^r - 1$. Finally, we reduce the result modulo Φ_r, by replacing a constant coefficient c_0 by $-c_0 \sum_{1 \le i \le nk} \xi^i$, to obtain $\tilde{C} \in \mathcal{R}$. Then $\tilde{C} = \sum_{1 \le i \le nk} c'_i \xi^i = \varphi(A)\varphi(B) \in \mathcal{R}'$. For $0 \le i < n$, let $c_i = c'_j$ for $j \in \mathcal{K}_i$. Then $C = \varphi^{-1}(\tilde{C}) = \sum_{0 \le i < n} c_i \alpha_i$. This shows that $A \cdot B$ can be computed in $O(nk \log(nk) \log\log(nk))$ operations in $\mathbb{F}_q$.

We now focus on the division of $A, B \in \mathbb{F}_{q^n}$, $B \ne 0$. We can first compute B^{-1} and then compute $A \cdot B^{-1}$. To compute B^{-1}, note that $\varphi(B) \in \mathcal{R}$ is invertible, i.e., $\varphi(B)$ is relatively prime to Φ_r. Applying the fast extended Euclidean algorithm (see Aho et

al 1974, § 8.9) to Φ_r and $\varphi(B)$, we can find B_1, the inverse of $\varphi(B)$ in $\mathcal{R}'$, as above in $O(nk \log^2(nk) \log\log(nk))$ operations in $\mathbb{F}_q$. Then $\varphi^{-1}(B_1) \in \mathbb{F}_{q^n}$ is the inverse of B.

Agnew et al. (1988), Stinson (1990) (for $q = 2$) and von zur Gathen (1991) show that exponentiation in a normal basis, where qth powers are computed for free, can be done with $O(n/\log_q n)$ multiplications in $\mathbb{F}_{q^n}$, and storage for $O(n/\log_q^2 n)$ elements of $\mathbb{F}_{q^n}$. The last result assumes that $q^5 \leq n$. (Under more specific assumptions, say $q \geq 3$ or $n \geq 626$, the constants in this estimate are calculated explicitly, and asymptotic optimality of this algorithm, in an appropriate model, is proven.) □

Corollary 3.2. *Suppose that $\mathbb{F}_{q^n}$ is represented by an optimal normal basis over $\mathbb{F}_q$. Then multiplication in $\mathbb{F}_{q^n}$ can be computed with $O(n \log n \log\log n)$, division with $O(n \log^2 n \log\log n)$, and exponentiation with $O(n^2 \log\log n)$ operations in $\mathbb{F}_q$, for exponents less than q^n and small q.*

4. Fast exponentiation of Gauss periods

To compute large powers of Gauss periods, one can use the fast algorithm from the previous section. However, there is an even faster algorithm due to the special structure of Gauss periods. Let α be a Gauss period of type (n, k) over $\mathbb{F}_q$. Gao & Vanstone (1994) show that when $q = 2$ and $k = 2$, α^M can be computed in $O(n^2)$ operations in $\mathbb{F}_2$ for any $0 \leq M < 2^n$. In this section, we generalize their algorithm to arbitrary q and k, which is efficient when q and k are small.

Let M be an integer. We want to compute α^M expressed in the normal basis $(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$. We use a redundant representation of $A \in \mathbb{F}_{q^n}$, writing

$$A = \left(\sum_{0 \leq i < n} a_i \alpha_i \right) + a_n,$$

where $a_0, \cdots, a_{n-1}, a_n \in \mathbb{F}_q$. Thus A is represented by an $(n+1)$-tuple $(a_0, \cdots, a_{n-1}, a_n)$. Of course, this representation is not unique; we just want to compute any one of the representations. For example, the unit 1 can either be represented as $(0, \cdots, 0, 1)$ or $(-1, \cdots, -1, 0)$, since $-1 = \sum_{0 \leq i < n} \alpha_i$. Our algorithm benefits from this flexibility.

Thus A^q is the $(n+1)$-tuple obtained from that of A by shifting cyclically the first n coordinates to the right by one position (the last coordinate is untouched). So the cost for computing a q-th power is negligible.

For any $A \in \mathbb{F}_{q^n}$ and $0 \leq j < n$, we compute $\alpha_j A$. Assume that $A = (\sum_{0 \leq i < n} a_i \alpha_i) + a_n \in \mathbb{F}_{q^n}$, with $a_0, \cdots, a_n \in \mathbb{F}_q$. Then

$$\alpha_j A = \left(\sum_{0 \leq i < n} a_i (\alpha \alpha_{i-j})^{q^j} \right) + a_n \alpha_j.$$

By Theorem 2.3, $\alpha \alpha_i$ is a sum of at most k terms. So $\alpha_j A$ can be computed in $O(nk)$ operations in $\mathbb{F}_q$.

Now to compute α^M, we use the q-ary representation $M = \sum_{0 \le j \le \ell} m_j q^j$, with $0 \le m_j < q$ for all j. Then

$$\alpha^M = \prod_{0 \le j \le \ell} \left(\alpha^{q^j}\right)^{m_j} = \prod_{0 \le j \le \ell} \alpha_j^{m_j}.$$

This suggests that we compute α^M iteratively. Initially, set $A := 1$. For j from 0 to ℓ set $A := \alpha_j^{m_j} A$. Then, at the end, we have $A = \alpha^M$. We compute $\alpha_j^{m_j} A$ by multiplying α_j to A repeatedly m_j times. This algorithm computes α^M in

$$O\left(\left(\sum_{0 \le j < n} m_j\right) nk\right) = O(\sigma_q(M) nk)$$

operations in $\mathbb{F}_q$ where $\sigma_q(M)$ is the sum of digits of M in q-ary representation. For $0 \le M < q^n$, since $\sigma_q(M) \le (q-1)n \le qn$, α^M can be computed in $O(n^2 qk)$ operations in $\mathbb{F}_q$. When q and k are small, this is faster than the general exponentiation algorithm in Section 3.

5. Using the Extended Riemann Hypothesis

Suppose that we are given a prime p and a positive integer n. We want to construct a normal basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Theorem 2.1 suggests that we just need to find k such that (n,k) is admissible for p. Then Gauss periods of type (n,k) will suffice. For this algorithm to be efficient, we need to know the size of smallest such k. In general, we do not know how to get a good upper bound. But if one assumes the Extended Riemann Hypothesis (ERH), then there is a reasonable bound on k. The following result is due to Bach and Shallit (1985, 1989), formulated in the present form by Adleman and Lenstra (1986).

Theorem 5.1. *Assuming ERH, there is a constant $c > 0$ such that for all prime p and positive integer n with $p \nmid n$, there is an integer $k \le cn^3(\log(np))^2$ such that (n,k) is admissible for p.*

When n is divisible by p, there may not exist any admissible k. For example, when $p = 2$, one can prove that for an integer n there is an admissible k if and only if $8 \nmid n$, see Wassermann (1993). This means that there is an integer k such that Gauss periods of type (n,k) form a normal basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ if and only if $8 \nmid n$. In general, for $q = p^m$ and $n \in \mathbb{N}$, Wassermann (1993) proves that there is an admissible k if and only if

$$\gcd(n,m) = 1,\ 2p \nmid n \ \text{ if } \ p \equiv 1 \pmod 4, \text{ and } 4p \nmid n \ \text{ if } \ p \equiv 2,3 \pmod 4.$$

It would be nice to have a similar upper bound on k as in Theorem 5.1 when $p \mid n$.

An immediate consequence of Theorem 5.1 and Theorem 2.1 is that a normal basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ can be constructed deterministically in time polynomial in n and $\log p$ under ERH for any given positive integer n and prime p. If $p \nmid n$, we just search for the smallest integer k such that Gauss periods of type (n,k) form a normal basis. We should mention that, to construct Gauss periods of type (n,k) over $\mathbb{F}_q$, it is not necessary to compute a primitive r-th root β of unity. One just needs to compute the subgroup $\mathcal{K}$ of order

k of $\mathbb{Z}_r^\times$, and its cosets $\mathcal{K}_i = q^i\mathcal{K}$, $0 \le i < n$. Then compute the cyclotomic numbers $t_{jh} = |(1+\mathcal{K}_j) \cap \mathcal{K}_h|$, for $0 \le j, h < n$. Let $t'_{jh} = t_{jh} - k\delta_j$, where δ_j is as defined in Section 2. Then the $n \times n$ matrix $T = (t'_{jh})$ is the multiplication matrix of the normal basis. The characteristic polynomial of T is equal to the minimal polynomial of the elements in the above basis (this polynomial is called *period polynomial* in the literature). This approach is different from Gauss (1801). When $p|n$, write $n = n_1 n_2$ where $p \nmid n_1$ and n_2 is a power of p. One can construct a normal basis for $\mathbb{F}_{p^{n_1}}$ and $\mathbb{F}_{p^{n_2}}$, respectively, and then combine them to get a normal basis for $\mathbb{F}_{p^n}$. This can be done in polynomial time, see Menezes et al. (1993, chapter 4), and Blake et al. (1993).

Since the minimal polynomial of a normal element in $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is an irreducible polynomial over $\mathbb{F}_p$ of degree n, an irreducible polynomial of degree n over $\mathbb{F}_p$ can be constructed deterministically in polynomial time under the ERH. This result was first proved by Adleman and Lenstra (1986).

Finally, we make some remarks on the density of integers n such that Gauss periods of type (n,k) form a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ when q and k are fixed. When $k = 1$, we want to know how many integers n there are so that $n+1$ is a prime and q is primitive modulo $n+1$. Let $N_a(x)$ be the number of primes r less than or equal to x such that a is primitive modulo r. If $a \ne 0, 1, -1$ or a perfect square, then Artin (1965) conjectured that

$$N_a(x) \sim c(a) \cdot \frac{x}{\log x}$$

as $x \to \infty$, where $c(a)$ is a constant depending on a. Hooley (1967) proved this conjecture under the ERH. Applying this result to $a = q = p^m$ with m odd, we see that there are infinitely many integers n such that Gauss periods of type $(n,1)$ form a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. When $k = 2$, we want to know the density of integers n such that $2n+1$ is a prime and $\gcd(2n/e, n) = 1$ where e is the multiplicative order of q modulo $2n+1$. We do not know any explicit result about this in the literature, but one might expect a similar density for this "Artin conjecture in arithmetic progressions". This applies also to other values of k.

6. Experimental results

In several cryptosystems, it is desirable to construct elements in finite fields that are primitive or have high multiplicative orders and large powers of them can be computed quickly. Gao & Vanstone (1994) show that Gauss periods of type $(n,2)$ over $\mathbb{F}_2$ have exactly these properties. In section 5, we have seen that Gauss periods of type (n,k) over $\mathbb{F}_q$ can be exponentiated efficiently for all small k and q. The question is how frequently Gauss periods are primitive or have high orders. We consider only Gauss periods over $\mathbb{F}_2$. Here by "high order" of an element in $\mathbb{F}_{2^n}$, we mean that its multiplicative order is at least $(2^n - 1)/n$.

We computed the multiplicative orders of Gauss periods of type (n,k) over $\mathbb{F}_2$ for all admissible $3 \le k \le 20$ and $2 \le n < 527$. Our experiment shows that Gauss periods have

the expected multiplicative properties: they are frequently primitive and almost always have high multiplicative orders. More precisely, there are 1179 admissible pairs (n, k) in the above range, all the corresponding Gauss periods have order $\geq (2^n - 1)/n$ except for 8 pairs, and 906 of them are primitive. We also did the corresponding calculations for $527 \leq n \leq 1200$ and $2 \leq k \leq 20$. There are 1239 admissible pairs (n, k). It seems that the same properties hold in this case. Note that for many values of n in this range the complete factorization of $2^n - 1$ is not known. In such cases we used the known partial factorization. The result of our experiments can be found in the technical report (Gao et al. 1995).

Since Gauss periods over $\mathbb{F}_2$ are frequently primitive, by Theorem 2.1 and Corollary 2.5, they give many primitive normal bases, and primitive self-dual normal bases.

Gao & Vanstone (1994) observe that if n and $2n + 1$ are both primes then Gauss periods of type $(n, 2)$ are primitive elements in $\mathbb{F}_{2^n}$. Our experimental data show that their observation still holds. We formulate this as follows.

Conjecture 1. *If n and $nk + 1$ are both primes and $k \leq \log_2 n + 1$, then Gauss periods of type (n, k) form a primitive normal basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.*

We note that normality is not a problem here. Since the order e of 2 modulo $nk + 1$ is at least $\log_2(nk + 1) > \log_2(2n) = \log_2 n + 1 \geq k$, we have $n|e$ and thus $\gcd(nk/e, n) = 1$.

Our computations lead us to believe that for every n not divisible by 8 there is an admissible small k such that Gauss periods of type (n, k) are primitive in $\mathbb{F}_{2^n}$. As an experiment, we verified this for all $n < 527$. If there is no primitive Gauss period for $k \leq 20$, then we compute the smallest admissible k whose Gauss period is primitive in $\mathbb{F}_{2^n}$. The largest such k occurs in (490, 69).

Conjecture 2. *For any positive integer n not divisible by 8, there exists an integer $k \geq 1$ such that the Gauss period of type (n, k) generates a primitive normal basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.*

Finally, we show how to construct primitive elements from elements of high orders. The constructed primitive elements will still be essentially as easy to exponentiate as Gauss periods. Suppose that $\alpha \in \mathbb{F}_{2^n}$ has order $e \geq (2^n - 1)/n$. Let $d = (2^n - 1)/e$ be the index of α. Then $d \leq n$. Write $d = d_1 d_2$, where $\gcd(d_2, e) = 1$ and every prime divisor of d_1 divides e. Let $\beta_1 \in \mathbb{F}_{q^n}$ satisfy

$$\beta^{d_1} = \alpha,$$

and let β_2 be a primitive d_2-th root of unity in $\mathbb{F}_{2^n}$. Then β_1 has order ed_1 and $\beta_1\beta_2$ has order $ed_1d_2 = 2^n - 1$, as $\gcd(ed_1, d_2) = 1$. This means that $\beta_1\beta_2$ is primitive in $\mathbb{F}_{2^n}$. For $d \leq n$ and $\alpha \in \mathbb{F}_{2^n}$, the polynomial $x^d - \alpha$ can be factored deterministically in polynomial time, and β_1 and β_2 as above can be constructed in polynomial time. In the special case $d = 2^k - 1$, the equation $x^d - \alpha$ can be written as $x^{2^k} = \alpha x$, which corresponds to a system of linear equations over $\mathbb{F}_2$. Our experimental data shows that many Gauss periods have index $3, 7, 15$, etc, if they are not primitive, and then the construction of a primitive element is particularly easy.

Based on the above discussion, we propose a new method for constructing primitive elements in $\mathbb{F}_{2^n}$ for $8 \nmid n$. For a given n, we search for the smallest admissible k. Then we test if Gauss periods of type (n,k) have high order, at least $(2^n-1)/n$. If yes, we construct a primitive element from it and stop. If not, we find the next smallest admissible k, and proceed similarly until we find a suitable k.

To support the above algorithm, we searched for Gauss periods of high order (or, equivalently, of small index). For $n < 527$ and $8 \nmid n$, we can always find Gauss periods of high order for reasonable small k, and thus construct a primitive element in $\mathbb{F}_{2^n}$ efficiently.

Acknowledgement. Many thanks go to S.S. Wagstaff for providing the factorization tables of the Cunningham project (Brillhart et al. 1988). We used MAPLE in our computations.

An Extended Abstract of this paper appeared in Proc. Latin'95, Valparaíso, Chile, Springer Lecture Notes in Computer Science **911** (1995), 311-322.

References

L.M. ADLEMAN AND H.W. LENSTRA, JR., "Finding irreducible polynomials over finite fields", *Proc. 18th Annual ACM Symp. on Theory of Computing* (1986), 350-355.

G.B. AGNEW, R.C. MULLIN, I.M. ONYSZCHUK AND S.A. VANSTONE, "An implementation for a fast public key cryptosystem", *J. of Cryptology* **3** (1991), 63-79.

G.B. AGNEW, R.C. MULLIN AND S.A. VANSTONE, "Fast exponentiation in GF(2^n)", *Advances in Cryptology-Eurocrypt '88* (LNCS 330), 251-255, 1988.

G.B. AGNEW, R.C. MULLIN AND S.A. VANSTONE, "An implementation of elliptic curve cryptosystems over $F_{2^{155}}$", *IEEE J. on Selected Areas in Communications* **11** (1993), 804–813.

A.V. AHO, J.E. HOPCROFT AND J.D. ULLMAN, "The Design and Analysis of Computer Algorithms", Addison-Wesley, 1974.

E. ARTIN, *Collected Papers*, Addison-Wesley, 1965.

D.W. ASH, I.F. BLAKE AND S.A. VANSTONE, "Low complexity normal bases", *Discrete Applied Math.* **25** (1989), 191-210.

E. BACH AND J. SHALLIT, "Factoring with cyclotomic polynomials", *Proc. 26th Annual ACM Symp. on Foundations of Computer Science* (1985), 443-450.

E. BACH AND J. SHALLIT, "Factoring with cyclotomic polynomials", *Math. Comp.* **52** (1989), 201-219.

E.R. BERLEKAMP, "Bit-serial Reed-Solomon encoders", *IEEE Trans. Info. Th.* **28** (1982), 869-874.

I.F. Blake, S. Gao and R.C. Mullin, "Specific irreducible polynomials with linearly independent roots over finite fields", submitted to *Linear Algebra and Its Applications*, 1993.

I.F. Blake, S. Gao and R.C. Mullin, "Normal and self-dual normal bases from factorization of $cx^{q+1} + dx^q - ax - b$", *SIAM J. Discrete Mathematics*, *7* (1994), 499–512.

E.F. Brickell, D.M. Gordon, K.S. McCurley and D.B. Wilson, "Fast exponentiation with precomputation", in *Proc. Eurocrypt'92*, Balatonfűred, Hungary, 1992.

J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman and S.S. Wagstaff, "Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ Up to High Powers", Vol. **22** of *Contemporary Mathematics*, AMS, 1988, 2nd edition.

Calmos, "CA34C168 data encryption processor, Document 01-34168-500", Calmos Semiconductor Inc., Kanata, Ontario, Canada, 1988.

D.G. Cantor and E. Kaltofen, "On fast multiplication of polynomials over arbitrary algebras", *Acta Inform.* **28** (1991), 693-701.

L. Carlitz, "Primitive roots in finite fields", *J. London Math. Soc.* **43** (1952), 373-382.

H. Davenport, "Bases for finite fields", *J. London Math. Soc.* **43** (1968), 21-39.

S. Gao, J. von zur Gathen and D. Panario, "Gauss periods, primitive normal bases, and fast exponentiation in finite fields", Technical Report 296/95, Department of Computer Science, University of Toronto, 1995.

S. Gao and H.W. Lenstra, Jr., "Optimal normal bases", *Designs, Codes and Cryptography* **2** (1992), 315-323.

S. Gao and S.A. Vanstone, "On orders of optimal normal basis generators", 1994, to appear in *Mathematics of Computation.*

J. von zur Gathen, "Efficient and optimal exponentiation in finite fields", *computational complexity* **1** (1991), 360–394.

J. von zur Gathen and M. Giesbrecht, "Constructing normal bases in finite fields", *J. Symb. Comp.* **10** (1990), 547–570.

C.F. Gauss, *Disquisitiones Arithmeticae*, Braunschweig, 1801. English Edition, Springer-Verlag, 1986.

W. Geiselmann and D. Gollmann, "Symmetry and duality in normal basis multiplication", *AAECC-6*, Lecture Notes in Computer Science **357** (1989), Springer-Verlag, 230-238.

K. Hensel "Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor", *J. Reine Angew. Math.* **103** (1888), 230-237.

C. Hooley, "On Artin's conjecture", *J. reine angew. Math.* **226** (1967), 209–220.

D. JUNGNICKEL, *Finite Fields: Structure and Arithmetics*, Bibliographisches Institut, Mannheim, 1993.

A. LEMPEL AND G. SEROUSSI, "Explicit formulas for self-complementary normal bases in certain finite fields", *IEEE Trans. Info. Th.* **37** (1991), 1220-1222.

A. LEMPEL AND M.J. WEINBERGER, "Self-complementary normal bases in finite fields", *SIAM J. Disc. Math.* **1** (1988), 193-198.

H.W. LENSTRA, JR. AND R.J. SCHOOF, "Primitive normal bases for finite fields", *Math. Comp.* **48** (1987), 217-231.

J.L. MASSEY AND J.K. OMURA, "Computational Method and Apparatus for Finite Fields Arithmetic", U. S. Patent #4,587,627, May 1986.

A.J. MENEZES, I.F. BLAKE, X. GAO, R.C. MULLIN, S.A. VANSTONE AND T. YAGHOOBIAN, *Applications of Finite Fields*, Kluwer Academic Publishers, Boston - Dordrecht - Lancaster, 1993.

R.C. MULLIN, I.M. ONYSZCHUK, S.A. VANSTONE AND R.M. WILSON, "Optimal normal bases in $GF(p^n)$", *Discrete Applied Math.* **22** (1988/1989), 149-161.

I.M. ONYSZCHUK, R.C. MULLIN AND S.A. VANSTONE, "Computational method and apparatus for finite field multiplication", U.S. patent #4,745,568, May 1988.

M. POHST AND H. ZASSENHAUS, *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989.

A. POLI, "Constructing SCN Bases in Characteristic 2", IEEE Trans. Inform. Theory, **41** (1995), 790-794.

T. ROSATI, "A high speed data encryption processor for public key cryptography", *Proc. of IEEE Custom Integrated Circuits Conference*, San Diego, 1989, 12.3.1 – 12.3.5.

A. SCHÖNHAGE, "Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2", *Acta Inf.* **7** (1977), 395-398.

A. SCHÖNHAGE AND V. STRASSEN, "Schnelle Multiplikation großer Zahlen", *Computing* **7** (1971), 281-292.

V. SHOUP, "Factoring polynomials over finite fields: asymptotic complexity vs. reality", *Proc. Int. IMACS Symp. on Symbolic Computation, New Trends and Developments*, Lille, France, 124-129, 1993.

V. SHOUP, "Exponentiation in $GF(2^n)$ using fewer polynomial multiplications", preprint, 1994.

S.A. STEPANOV AND I.E. SHPARLINSKI, "On construction of primitive elements and primitive normal bases in a finite field", in *Computational Number Theory*, ed. A. Pethő, M.E. Pohst, H.C. Williams and H.G. Zimmer, 1991. (Proc. Colloq. Comp. Number Theory,

Hungary, 1990).

D.H. STINSON, "Some observations on parallel algorithms for fast exponentiation in $GF(2^n)$", *SIAM J. Computing* **19** (1990), 711-717.

T. STORER, *Cyclotomy and Difference Sets*, Markham, Chicago, 1967.

V. STRASSEN, "Gaussian elimination is not optimal", *Numer. Mathematik* **13** (1969), 354-356.

C.C. WANG, "An algorithm to design finite field multipliers using a self-dual normal basis", *IEEE Trans. Comput.* **38** (1989), 1457-1460.

L.C. WASHINGTON, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.

A. WASSERMANN, "Konstruktion von Normalbasen", *Bayreuther Mathematische Schriften* **31** (1990), 155-164.

A. WASSERMANN, "Zur Arithmetik in endlichen Körpern", *Bayreuther Mathematische Schriften* **44** (1993), 147-251.

First author's current address: SHUHONG GAO, Department of Mathematical Sciences, Clemson University, Clemson SC 29634, USA. sgao@math.clemson.edu

Second author's current address: JOACHIM VON ZUR GATHEN, Fachbereich Math-ematik-Informatik, Universität-GH Paderborn, D-33098 Paderborn, Germany. gathen@uni-paderborn.de

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF TORONTO, TORONTO, ONTARIO M5S 1A4, CANADA, {SGAO,GATHEN,DANIEL}@CS.TORONTO.EDU