Algorithms for exponentiation in finite fields

SHUHONG GAO[†], JOACHIM VON ZUR GATHEN[‡],
DANIEL PANARIO[§] AND VICTOR SHOUP[¶]

[†] *Department of Mathematical Sciences, Clemson University, Clemson SC 29634-1907, USA,* sgao@math.clemson.edu

[‡] *Fachbereich Mathematik-Informatik, Universität Paderborn, D-33095 Paderborn, Germany,* gathen@uni-paderborn.de

[§] *Department of Computer Science, University of Toronto, Toronto M5S 3G4, Canada,* daniel@cs.toronto.edu

[¶] *IBM Research-Zurich, Säumerstr. 4, 8803 Rüschlikon, Switzerland,* sho@zurich.ibm.com

Gauss periods yield (self-dual) normal bases in finite fields, and these normal bases can be used to implement arithmetic efficiently. It is shown that for a small prime power q and infinitely many integers n, multiplication in a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ can be computed with $O(n \log n \operatorname{loglog} n)$, division with $O(n \log^2 n \operatorname{loglog} n)$ operations in $\mathbb{F}_q$, and exponentiation of an arbitrary element in $\mathbb{F}_{q^n}$ can be done with $O(n^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_q$. We also prove that using polynomial basis exponentiation in $\mathbb{F}_{2^n}$ can be done with the same number of operations in $\mathbb{F}_2$ for all n. The previous best estimates were $O(n^2)$ for multiplication in a normal basis, and $O(n^2 \log n \log\log n)$ for exponentiation in a polynomial basis.

1. Introduction

For a prime power q and an integer $n \geq 1$, let $\mathbb{F}_{q^n}$ be a finite field with q^n elements. A fundamental question for applications is how to do arithmetic fast in finite fields, i.e., addition, multiplication, division, and exponentiation. A *polynomial basis* 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 four operations can be done with $O(n)$, $O(n \log n \operatorname{loglog} n)$, $O(n \log^2 n \operatorname{loglog} n)$, and $O(n^2 \log n \operatorname{loglog} n \log q)$ operations in $\mathbb{F}_q$, respectively, with fast multiplication (Schönhage and Strassen 1971, Schönhage 1977, Karatsuba and Ofman 1962; see also Cantor and Kaltofen 1991, Cantor 1989), and repeated squaring. We may always assume an exponent to be less than q^n. Implementation reports are in Shoup (1993) and von zur Gathen and Gerhard (1999), Section 9.7. Fast polynomial factorization software is also discussed in Montgomery (1991) and von zur Gathen and Gerhard (1996).

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 $\mathbb{F}_{q^n}$. For an arbitrary f, the preprocessing takes $O(n^2 \log n \operatorname{loglog} n)$ operations in $\mathbb{F}_q$. For $q = 2$ and for a sparse f, say with $O(\log n)$ nonzero terms, squaring in $\mathbb{F}_{q^n}$ can be done in $O(n)$ operations in $\mathbb{F}_q$, so that the preprocessing takes $O(n^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_q$. It is conjectured that sparse irreducible polynomials exist; see Gao *et al.* (1999) for experiments with this type of polynomials. Under this conjecture, the algorithm of Brickell *et al.* (1992) takes time $O(n^2 \operatorname{loglog} n)$ for exponentiation in $\mathbb{F}_2$.

Our main result of Section 2 is an exponentiation algorithm that works for an *arbitrary* polynomial basis representation of $\mathbb{F}_{2^n}$ and uses $O(n^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_2$.

Another standard way of representing the elements in $\mathbb{F}_{q^n}$ is using a *normal* basis representation. For an integer $n \geq 1$, 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.

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 efficiently under normal bases. Hardware implementations of large finite fields (Massey and Omura 1986, Onyszchuk *et al.* 1988, Calmos 1988, Rosati 1989, Agnew *et al.* 1991 and Agnew *et al.* 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 and 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 4, where fast arithmetic is implemented in $\mathbb{F}_{q^n}$ when represented by a normal basis generated by Gauss periods. 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. Thus 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. In their implementation, von zur Gathen and Nöcker (1997) found exponentiation under a suitable normal basis to be significantly faster than that under a polynomial basis.

It is interesting to note that exponentiation of Gauss periods of type (n, k), as defined below, can be done with $O(n^2)$ operations in $\mathbb{F}_q$ for small k and q. No storage is required here. Experimental results indicate that Gauss periods are often primitive, or at least have high multiplicative order, see Gao and Vanstone (1994) and Gao *et al.* (1998). Von zur Gathen and Shparlinski (1998) show that Gauss periods of type $(n, 2)$ have order at least $2^{\sqrt{2n}-2}$.

In Section 3, we present some well-known properties of Gauss periods in a form that is convenient for us. As a by-product, we determine explicitly the dual basis of a normal basis generated by Gauss periods and give a simple necessary and sufficient condition for them to be self-dual; such results may be useful for other applications. The second main result is the combination of fast arithmetic with Gauss periods in Section 4.

A summary of the main results of this paper follows.

- Exponentiation in $\mathbb{F}_{2^n}$ can be performed with $O(n/\log n)$ multiplications in $\mathbb{F}_{2^n}$ using polynomial basis.
- Multiplication and division in $\mathbb{F}_{q^n}$ in normal basis representation given by certain Gauss periods can be performed with $O(n \log n \operatorname{loglog} n)$ and $O(n \log^2 n \operatorname{loglog} n)$ operations in $\mathbb{F}_q$, respectively.
- For a small q, exponentiation in $\mathbb{F}_{q^n}$ can be done with $O(n^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_q$, with storage for $O(n/\log_q^2 n)$ elements of $\mathbb{F}_{q^n}$.
- The dual basis of the normal basis generated by a Gauss period over $\mathbb{F}_q$ is given explicitly.

2. Fast exponentiation using polynomial bases

The main result of this section is an exponentiation algorithm that works for an *arbitrary* power basis representation of $\mathbb{F}_{2^n}$, and uses only $O(n/\log n)$ multiplications in $\mathbb{F}_{2^n}$. The proof of this result requires some lemmas.

We rely on the following result of Brickell *et al.* (1992).

FACT 2.1. *There is an algorithm with the following properties. It takes as input an element g from an arbitrary semi-group G and a positive integer m. The algorithm constructs a table of powers of g, using $O(m)$ squarings in G. After this precomputation, the algorithm will compute g^e for any $0 \le e < 2^m$ using an additional $O(m/\log m)$ multiplications in G.*

We shall also need an efficient algorithm for *modular composition*: given polynomials $f, g, h \in K[x]$, compute $g(h) \bmod f$. Here, K is a field, and the degrees of g and h are less than that of f.

Let ω be a feasible exponent of matrix multiplication, so that we can multiply two $n \times n$ matrices using $O(n^\omega)$ arithmetic operations. Moreover, let $\mathsf{M}(n)$ be a bound on the time required to multiply polynomials in $\mathbb{F}_2[x]$ of degree less than n. Using the classical polynomial multiplication algorithm, we can take $\mathsf{M}(n) = O(n^2)$. Using Karatsuba's algorithm, we can take $\mathsf{M}(n) = O(n^{\log_2 3})$. Using the asymptotically fastest algorithm currently known, due to Schönhage and Strassen (1971) and Schönhage (1977), we can take $\mathsf{M}(n) = O(n \log n \log\log n)$.

The following result is due to Brent and Kung (1978).

FACT 2.2. *For a field K and polynomials $f, g, h \in K[x]$ with $\deg f = n$ and degrees* *of g and h less than n, we can compute the modular composition $g(h) \bmod f$ using $O(\mathsf{M}(n)n^{1/2} + n^{(\omega+1)/2})$ operations in K.*

Using the classical algorithm, we can take $\omega = 3$. For the proof of our main theorem, we shall require $\omega < 3$, which can be obtained using one of several algorithms; Strassen's (1969) algorithm, giving $\omega = \log_2 7$, will suffice.

We will use modular composition as follows. Let $K = \mathbb{F}_2$. If $h = x^{2^m} \bmod f \in \mathbb{F}_2[x]$, then for any $g \in \mathbb{F}_2[x]$, $g^{2^m} \equiv g(h) \bmod f$. Thus, for powers of 2, we can replace exponentiation by modular composition.

We do not make any claims about the practicality of this algorithm; however, it does not seem entirely impossible that it, or some variant of it, could lead to a practical improvement.

ALGORITHM 2.3. (EXPONENTIATION VIA MODULAR COMPOSITION)
Input: $f, g \in \mathbb{F}_2[x]$ *with* $\deg f = n$ *and* $\deg g < n$*, and an exponent* e *with* $0 \le e < 2^n$
Output: $g^e \bmod f$

1. *Set* $m = \lceil n/\log_2 n \rceil$*, write* e *in base* 2^m *as* $e = \sum_{i=0}^{\ell-1} e_i 2^{mi}$*, where* $\ell = \lceil \log_2 n \rceil$.
2. *Run the precomputation stage of the algorithm in Fact 2.1 on inputs* ($g \bmod f$) *and* m.
3. *For* $0 \le i < \ell$*, compute* $g_i = g^{e_i} \bmod f$*, using the algorithm of Fact 2.1.*
4. *Compute* $h = x^{2^m} \bmod f$.
5. *Now we compute* $c = g^e \bmod f$ *using the following Horner-like scheme.*
   $c \leftarrow 1$
   for $i \leftarrow \ell - 1$ *down to* 0 *do*
   $\quad c \leftarrow c(h) \bmod f$
   $\quad c \leftarrow c \cdot g_i \bmod f$

THEOREM 2.4. *The algorithm works correctly as specified and uses $O(n/\log n)$ multiplications in $\mathbb{F}_2[x]/(f)$, plus additional time of $O(n^\lambda)$, where $\lambda < 2$ is a constant. In particular, it runs in time $O(n/\log n \cdot \mathsf{M}(n))$ for any choice of $\mathsf{M}(n) \ge n$.*

PROOF. Let f, g, and e be inputs and $n = \deg f$. Each execution of $c \leftarrow c(h) \bmod f$ has the effect of raising c to the power 2^m, from which the correctness easily follows.

Step 2 takes time $O(\mathsf{M}(n)m)$, or $O(\mathsf{M}(n)n/\log n)$. Step 3 takes time $O(\mathsf{M}(n)\ell m/\log m)$, or $O(\mathsf{M}(n)n/\log n)$. Using standard repeated squaring, step 4 takes time $O(\mathsf{M}(n)m)$, or $O(\mathsf{M}(n)(n/\log n))$. The running-time is dominated by ℓ modular compositions, which cost in total time $O((\mathsf{M}(n)n^{1/2} + n^{(\omega+1)/2})\log n)$.

The running-time of the entire algorithm is then

$$O\left(\mathsf{M}(n)n/\log n + n^{(\omega+1)/2}\log n\right).$$

Choosing any $\omega < 3$ proves the theorem for an arbitrary $\mathsf{M}(n) \ge n$. If, however, $\mathsf{M}(n) = \Omega(n^{1+\epsilon})$ for some constant $\epsilon > 0$, we can attain the running-time bound of $O(\mathsf{M}(n)n/\log n)$ with $\omega = 3$. □

We also prove the following, which is of interest when the exponent has small Hamming weight (number of nonzero digits e_i).

THEOREM 2.5. *Let $\nu(e)$ denote the number of 1-bits in e. The algorithm in Theorem 2.4 can be modified so that its running-time is*

$$O\left(n^{1.85} + \nu(e) n \log n \log\log n\right).$$

PROOF. Let us suppose that the number of 1-bits in e is $\nu(e)$. We set $m = \lceil n^{1-\alpha} \rceil$ for a constant α determined below. This takes time $O(\mathsf{M}(n)m)$. In step 1, we simply compute $g^{2^i} \bmod f$ for $0 \le i < m$. This takes time $O(\mathsf{M}(n)m)$. In step 2, we compute each g_i using the precomputed values in step 1 in the most obvious fashion. This takes in total time $O(\mathsf{M}(n)\nu(e))$. Steps 3 and 4 are as before. Altogether, the algorithm runs in time

$$O\left(\mathsf{M}(n)(n^{1-\alpha} + n^{\alpha+1/2} + \nu(e)) + n^{(\omega+1)/2+\alpha}\right).$$

The theorem then follows by plugging in $\mathsf{M}(n) = O(n \log n \log\log n)$ and $\omega < 2.376$ (Coppersmith and Winograd 1990), and optimizing the value of α (see also Kaltofen and Shoup 1998). □

3. 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.

Gauss periods were 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, see Pohst and Zassenhaus (1989). Here we consider Gauss periods over finite fields only.

Let $r = nk + 1$ be a prime not dividing q, and $\mathcal{K}$ the unique subgroup of order k of the multiplicative group $\mathbb{Z}_r^\times$ 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 $\mathbb{F}_q$. We give a form of Wasserman's condition that is somewhat easier to handle computationally.

THEOREM 3.1. *Let $r = nk + 1$ be a prime not dividing q, e the index of q in $\mathbb{Z}_r^\times$, $\mathcal{K}$ the unique subgroup of order k of $\mathbb{Z}_r^\times$, and 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 $\gcd(e, n) = 1$.

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 two subgroups $\mathcal{K}$ and $<q>$ of $\mathbb{Z}_r^\times$ of indices n and e, respectively, this means that

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

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 $\gcd(e, n) = 1$, where e is the index 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 $\gcd(e, n) = 1$ 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

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

Theorem 3.1 suggests that to construct a normal basis in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ we just need to find k such that (n, k) is admissible for q. 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 assuming the extended Riemann hypothesis, Bach and Shallit (1989) and Adleman and Lenstra (1986) prove that for all prime p and positive integer n with $p \nmid n$, there is an integer $k \leq cn^3(\log(np))^2$ such that (n, k) is admissible for p.

When n is divisible by p, there may not exist any admissible k. Wassermann (1993) proved that, for $q = p^m$ and a positive integer n, there is an admissible k for n and q if and only if

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

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

$$\mathcal{K}_i = \{aq^i : a \in \mathcal{K}\} \subseteq \mathbb{Z}_r^\times, \quad \alpha_i = \sum_{a \in \mathcal{K}_i} \beta^a. \tag{3.1}$$

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 $0 \leq j, h < n$, let t_{jh} be the number of elements $a \in \mathcal{K}_j$ such that $1 + a \in \mathcal{K}_h$, i.e.,

$$t_{jh} = |(1 + \mathcal{K}_j) \cap \mathcal{K}_h|. \tag{3.2}$$

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 $0 \leq j < n$, let

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

LEMMA 3.2. *For $0 \le i, j < n$,*

$$\left(\sum_{a\in\mathcal{K}} x^{aq^i}\right)\left(\sum_{b\in\mathcal{K}} x^{bq^j}\right) \equiv k\delta_{j-i} + \sum_{0\le h<n} t_{j-i\,h}\left(\sum_{a\in\mathcal{K}} x^{aq^{i+h}}\right) \bmod \Phi_r, \qquad (3.3)$$

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 (3.3) 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 3.3. *For any $0 \le i, j < n$,*

$$\alpha_i\alpha_j = k\delta_{j-i} + \sum_{0\le h<n} t_{j-i\,h}\alpha_{h+i} = \sum_{0\le h<n} (t_{j-i\,h} - k\delta_{j-i})\alpha_{h+i}. \qquad (3.4)$$

Since $1+\mathcal{K}_j$ has k nonzero elements if $j \ne j_0$ 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 nk nonzero terms, including the k in $\alpha\alpha_{j_0}$. In practice, one should store the matrix (t_{jh}) sparsely when k is small.

Gao and Lenstra Jr. (1992) showed a close connection between the optimal normal bases of Mullin *et al.* (1989) and certain Gauss periods. In particular, when $k = 1$, or $k = 2$ and $q = 2$, the normal bases generated by Gauss periods are optimal. See also Menezes *et al.* (1993, Chapter 5).

Since self-dual bases are useful in implementing finite fields (Berlekamp 1982, Geiselmann and 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 $T(\gamma_i\delta_j)$ is 0 when $i \ne j$, and 1 when $i = j$, where T denotes the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, with $T(A) = A + A^q + \cdots + A^{q^{n-1}}$ for $A \in \mathbb{F}_{q^n}$. For any basis there is a unique dual basis. If a basis is dual to itself, we say that it is self-dual. We now determine the dual basis of the normal basis generated by a Gauss period.

THEOREM 3.4. *Let α_i, j_0 be as in Theorem 3.3, and $\gamma = (\alpha_{j_0} - k)/r$. Then the dual basis of $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ is $(\gamma, \gamma^q, \ldots, \gamma^{q^{n-1}})$.*

PROOF. T is a linear functional over $\mathbb{F}_q$, and $T(\alpha_i) = -1$ for $0 \leq i < n$. Theorem 3.3 implies that for all $0 \leq i, j < n$, $T(\gamma^{q^i}\alpha_j)$ is 0 if $i \neq j$, and is 1 if $i = j$. □

COROLLARY 3.5. *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

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

Since $n > 2$ and the representation is unique, it is obvious that $\gamma = \alpha$ 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 and 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 $n \equiv 2 \bmod 4$ and q is even.

4. Fast arithmetic using normal bases

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

THEOREM 4.1. *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 $O(n^2 k \log(k) \operatorname{loglog}(nk))$ operations in $\mathbb{F}_q$, for exponents less than q^n and small q, say $q^5 \leq n$. 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 $0 \leq i < n$ as in Section 3. 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

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

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

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

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

where $a'_j = a_i$ if $j \in \mathcal{K}_i$. Let $\mathcal{R} = \mathbb{F}_q[x]/(\Phi_r)$ and $\xi = x \bmod \Phi_r \in \mathcal{R}$, where $\Phi_r = (x^{nk+1} - 1)/(x - 1) = x^{nk} + \cdots + x + 1 \in \mathbb{F}_q[x]$ is the rth cyclotomic polynomial. Then

$\mathcal{R}$ has 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:

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

Thus the elements in $\mathcal{R}$ can be viewed as polynomials of degree at most $nk - 1$, or polynomials of degree at most nk with constant coefficient zero. 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 $\varphi(b) = b$ for $b \in \mathbb{F}_q$. By Theorem 3.3, $\varphi(\alpha_i \alpha_j) = k\delta_{j-i} + \sum_{0 \le h < n} t_{j-i\,h} \left(\sum_{a \in \mathcal{K}} \xi^{aq^{i+h}} \right)$. It follows from Lemma 3.2, 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

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

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, by fast multiplication algorithms of Schönhage and Strassen (1971) and Cantor and Kaltofen (1991), the two polynomials $\varphi(A), \varphi(B)$ of degree at most nk, using $O(nk \log(nk) \operatorname{loglog}(nk))$ operations in $\mathbb{F}_q$. Then we reduce all exponents of the product polynomial modulo r, in effect reducing it modulo $x^r - 1$. Finally, we reduce the result modulo Φ_r, by replacing the 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 $q^5 \le n$. (Under more specific assumptions, say $q \ge 3$ or $n \ge 626$, the constants in this estimate are calculated explicitly, and asymptotic optimality of this algorithm, in an appropriate model, is proven.) □

COROLLARY 4.2. *Suppose that k and q are bounded and that $\mathbb{F}_{q^n}$ is represented by the normal basis generated by Gauss periods of type (n, k) over $\mathbb{F}_q$. Then multiplication in $\mathbb{F}_{q^n}$ can be computed with $O(n \log n \operatorname{loglog} n)$, division with $O(n \log^2 n \operatorname{loglog} n)$, and exponentiation with $O(n^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_q$, for exponents less than q^n and small q.*

For any k and q, von zur Gathen and Pappalardi (1995) prove that there are infinitely many n such that $\mathbb{F}_{q^n}$ have normal bases generated by Gauss periods of type (n, k) over $\mathbb{F}_q$.

Remark. A preliminary version of part of this paper appeared in Proc. Latin'95, Valparaíso, Chile, Springer Lecture Notes in Computer Science **911** (1995), 311-322.

References

Adleman, L., Lenstra, H. (1986). Finding irreducible polynomials over finite fields. In *Proc. 18th ACM Symp. Theory of Computing*, pages 350–355, Berkeley CA.

Agnew, G., Mullin, R., Onyszchuk, I., Vanstone, S. (1991). An implementation for a fast public key cryptosystem. *J. of Cryptology*, **3**:63–79.

Agnew, G., Mullin, R., Vanstone, S. (1988). Fast exponentiation in $\mathbb{F}_{2^n}$. In Günther, C. G., editor, *Advances in Cryptology—EUROCRYPT '88*, volume 330 of *Lecture Notes in Computer Science*, pages 251–255. Springer, Berlin.

Agnew, G., Mullin, R., Vanstone, S. (1993). An implementation of elliptic curve cryptosystem over $\mathbb{F}_{2^{155}}$. *IEEE J. Selected Areas Commun.*, **11**:804–813.

Aho, A., Hopcroft, J., Ullman, J. (1974). *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading MA.

Ash, D., Blake, I., Vanstone, S. (1989). Low complexity normal bases. *Discrete Applied Math.*, **25**:191–210.

Bach, E., Shallit, J. (1989). Factoring with cyclotomic polynomials. *Math. Comp.*, **52**:201–219.

Berlekamp, E. (1982). Bit-serial Reed-Solomon encoders. *IEEE Trans. Inform. Theory.*, **28**:869–874.

Brent, R., Kung, H. (1978). Fast algorithms for manipulating formal power series. *J. Assoc. Comput. Mach.*, **25**:581–595.

Brickell, E., Gordon, D., McCurley, K., Wilson, D. (1992). Fast exponentiation with precomputation. In *Proc. Eurocrypt'92*, Balatonfüred, Hungary.

Calmos (1988). Ca34c168 data encryption processor, Document 01-34168-500. Calmos Semiconductor Inc., Kanata, Ontario, Canada.

Cantor, D. (1989). On arithmetical algorithms over finite fields. *J. Combin. Theory Ser. A*, **50**:285–300.

Cantor, D., Kaltofen, E. (1991). On fast multiplication of polynomials over arbitrary algebras. *Acta. Inform.*, **28**:693–701.

Coppersmith, D., Winograd, S. (1990). Matrix multiplication via arithmetic progressions. *J. Symb. Comp.*, **9**:251–280.

Gao, S., von zur Gathen, J., Panario, D. (1998). Gauss periods: orders and cryptographical applications. *Math. Comp.*, **67**:343–352.

Gao, S., Howell, J., Panario, D. (1999). Irreducible polynomials of given forms. In Mullin, R., Mullen, G., editors, *Finite fields: theory, applications and algorithms*, volume 225, pages 43–54. Contemporary Mathematics, Amer. Math. Soc.

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

Gao, S., Vanstone, S. (1994). On orders of optimal normal basis generators. *Math. Comp.*, **64**:1227–1233.

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

von zur Gathen, J., Gerhard, J. (1996). Arithmetic and factorization of polynomials over $\mathbb{F}_2$. In Y.N., L., editor, *Proc. ISSAC'96, Zürich, Switzerland*, pages 1–9. ACM press.

von zur Gathen, J., Gerhard, J. (1999). *Modern Computer Algebra*. Cambridge University Press, Cambridge, UK.

von zur Gathen, J., Nöcker, M. (1997). Exponentiation in finite fields: theory and practice. In *Proc. AAECC 12*, volume 1255 of *Springer Lecture Notes in Computer Science*, pages 88–113.

von zur Gathen, J., Pappalardi, F. (1995). On the reverse artin problem for primitive roots. Preprint.

von zur Gathen, Shparlinski, I. E. (1998). Order of gauss periods in finite fields. *Appl. Algebra Eng. Comm. Comput.*, **9**:15–24.

Gauss, C. (1801). *Disquisitiones Arithmeticae*. Braunschweig.

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

Jungnickel, D. (1993). *Finite Fields: Structure and Arithmetics*. Wissenschaftsverlag, Mannhein-Leipzig-Wien-Zurich.

Kaltofen, E., Shoup, V. (1998). Subquadratic-time factoring of polynomials over finite fields. *Math. Comp.*, **67**:1179–1197.

Karatsuba, A., Ofman, Y. (1962). Умножение многозначных чисел на абто-матах. *Dokl. Akad. Nauk USSR*, **145**:293–294. English translation: Multiplication of multidigit numbers on automata, Soviet Physics–Doklady **7** (1963), 595-596.

Lempel, A., Weinberger, M. (1988). Self-complementary normal bases in finite fields. *SIAM J. of Discrete Math.*, **1**:193–198.

Massey, J., Omura, J. (May 1986). Computational method and apparatus for finite fields arithmetic. U. S. Patent #4,587,627.

Menezes, A., Blake, I., Gao, X., Mullin, R., Vanstone, S., Yaghoobian, T. (1993). *Applications of Finite Fields*. Kluwer Academic Publishers, Boston, Dordrecht, Lancaster.

Montgomery, P. (1991). Factorization of $X^{216091}+X+1$ mod 2 – a problem of Herb Doughty. Preprint.

Mullin, R., Onyszchuk, I., Vanstone, S., Wilson, R. (1989). Optimal normal bases in $\mathbb{F}_{p^n}$. *Discrete Applied Math.*, **22**:149–161.

Onyszchuk, I., Mullin, R., Vanstone, S. (1988). Computational method and apparatus for finite field multiplication. *United States Patent*, **4,745,568**.

Pohst, M., Zassenhaus, H. (1989). *Algorithmic Algebraic Number Theory*. Cambridge University Press.

Rosati, T. (1989). A high speed data encryption processor for public key cryptography. In *Proc. of IEEE Custom Integrated Circuits Conference*, pages 12.3.1 – 12.3.5.

Schönhage, A. (1977). Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Inf.*, **7**:395–398.

Schönhage, A., Strassen, V. (1971). Schnelle Multiplikation großer Zahlen. *Computing*, **7**:281–292.

Shoup, V. (1993). Factoring polynomials over finite fields: asymptotic complexity vs. reality. In *Proc. Int. IMACS Symp. on Symbolic Computation, New Trends and Developments*, pages 124–129, Lille, France. Software is available in http://www.shoup.net.

Stinson, D. (1990). Some observations on parallel algorithms for fast exponentiation in $\mathbb{F}_{2^n}$. *SIAM J. Comput.*, **19**:711–717.

Storer, T. (1967). *Cyclotomy and Difference Sets*. Markham, Chicago.

Strassen, V. (1969). Gaussian elimination is not optimal. *Numer. Mathematik*, **13**:354–356.

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

Wassermann, A. (1990). Konstruktion von Normalbasen. *Bayreuther Mathematische Schriften*, **31**:155–164.

Wassermann, A. (1993). Zur Arithmetik in endlichen Körpern. *Bayreuther Mathematische Schriften*, **44**:147–251.