Gauss periods as low complexity normal bases

David Thomson (Carleton)

With M. Christopoulou, T. Garefalakis (Crete)
and D. Panario (Carleton)

July 16, 2009

Outline

Introduction to normal bases

An element $\alpha \in \mathbb{F}_{q^n}$ is called normal if

$$N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\},$$

is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this case, the basis N is called a normal basis.

By convention we define $\alpha_i = \alpha^{q^i}$ for $i = 0, 1, \ldots, n-1$.

The Multiplication Table

Let $\alpha_i = \alpha^{q^i}$ for $0 \leq i \leq n-1$, and let $T = (t_{ij})$ be the $n \times n$ matrix given by

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, \quad 0 \leq i \leq n-1, \quad t_{ij} \in \mathbb{F}_q.$$

The matrix T is called the multiplication table of the basis generated by α. The number of nonzero entries in T is called the complexity of the normal basis N, denoted by c_N.

Mullin, Onyszchuk, Vanstone and Wilson (1989):
Theorem. For any normal basis N of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, $c_N \geq 2n-1$.

If $c_N = 2n-1$, then N is called an optimal normal basis.

Optimal normal bases

Theorem: Type I ONB. Suppose $n+1$ is a prime and q is a primitive element in $\mathbb{Z}_{n+1}$. Then the n non-unit $(n+1)$th roots of unity form an optimal normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Theorem: Type II ONB. Let $2n+1$ be a prime and assume either 2 is a primitive element in $\mathbb{Z}_{2n+1}$, or $2n+1 \equiv 3 \bmod 4$ and 2 generates the quadratic residues in $\mathbb{Z}_{2n+1}$. Then, $\alpha = \gamma + \gamma^{-1}$ generates an optimal normal basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, where γ is a primitive $(2n+1)$th root of unity.

Mullin et al. (1991) conjectured that every optimal normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is equivalent to a basis constructed from the above theorems. This was proven by Gao and Lenstra (1992).

Gauss periods over $\mathbb{F}_2$

Gauss periods as normal bases over $\mathbb{F}_2$ were introduced by Ash, Blake and Vanstone (1989). In particular, Gauss periods of type $(n, 1)$ define Type I optimal normal bases in all finite fields and Gauss periods of type $(n, 2)$ define Type II optimal normal bases over $\mathbb{F}_2$.

Furthermore, the authors give bounds on the complexity of normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ obtained by Gauss periods and prove the lower bound is tight for $k = p, 2p, 4p$ or k a power of 2.

$$kn - (k^2 - 3k + 3) \leq C_N \leq kn - 1 \qquad \text{if } k \text{ is even;}$$

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

Definition

Let q be a prime power and let n, k be integers such that $r = nk + 1$ is a prime not dividing q. Let κ be the subgroup of order k in $\mathbb{Z}_r^*$ and let β be a primitive rth root of unity in $\mathbb{F}_{q^r}$.

Define the elements $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ by

$$\alpha_i = \sum_{a \in \kappa_i} \beta^a$$

where $\kappa_i = \{aq^i : a \in \kappa\}$.

Then α is a Gauss period of type (n, k) and if e is the order of q modulo r then $\alpha, \alpha_1, \ldots, \alpha_{n-1}$ forms a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $\gcd(nk/e, n) = 1$.

Recent interest in Gauss periods

Gao, von zur Gathen and Panario (1995) examine using Gauss periods to construct primitive normal bases for fast exponentiation in finite fields and note experimentally that Gauss periods often have high order. A lower bound on the order of Gauss periods was given by Shparlinski and von zur Gathen (1998) and later improved by Ahmadi, Shparlinski and Voloch (2007).

Silva and Kschischang (to appear) use of normal bases due to Gauss periods in encoding/decoding procedures for Gabidulin Codes.

Fan, Han and Feng (2007) give an asymptotic result using a p-adic method to determine the existence of primitive normal polynomials with prescribed coefficients.

Computing the trace of a normal element

Let $n = km$ be integers and let α be a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then

$$\beta = \mathsf{Tr}_{q^n/q^m}(\alpha) = \sum_{i=0}^{k-1} \alpha^{q^{im}} \in \mathbb{F}_{q^m}$$

is a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Proof. Due to the linearity of the Frobenius over $\mathbb{F}_q$ and the independence of basis generated by α.

The trace of an optimal normal element

Christopoulou, Garefalakis, Panario and Thomson (2008) give upper bounds on the complexity of the trace of an optimal normal element.

	Type I (q odd):	Type I (q even):
m odd	$(k+1)m-k$	$km-k+1$
m even, k odd	$(k+2)m-3k+1$	$(k+1)m-3k+2$
m even, k even	$(k+1)m-k$	$km-k+1$

Consider Type I, $q=k=2$. The resulting basis is optimal (of Type II)!

	Type II (q even):
all m	$2km-2k+1$

The trace of *any* normal element

We generalize the previous result to give the complexity of the trace of *any* normal element.

Let $n = km$ and let α generate a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Furthermore, let $\beta = \mathrm{Tr}_{q^n/q^m}(\alpha)$ generate a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

If T_α and T_β are the multiplication tables of the bases generated by α, β respectively, then explicit expressions for the jth row of T_β depends therefore on the number of non-zero elements in the rows of T_α defined by the m-cosets of j modulo n. That is, on the number of non-zero entries in row $j, j+m, \ldots, j+(k-1)m$.

The trace of *any* normal element

We compute the jth row of T_β as follows,

$$\begin{aligned}
\beta\beta_j &= \left(\sum_{w=0}^{k-1} \alpha^{q^{mw}}\right)\left(\sum_{u=0}^{k-1} \alpha^{q^{mu+j}}\right) \\
&= \sum_w \sum_u \left(\alpha^{q^{mw}}\right)\left(\alpha^{q^{mu+j}}\right) \\
&= \sum_w \left(\alpha\alpha^{q^j}\right)^{q^{mw}} + \sum_w \left(\alpha\alpha^{q^{j+m}}\right)^{q^{mw}} \\
&\quad + \cdots + \sum_w \left(\alpha\alpha^{q^{j+(k-1)m}}\right)^{q^{mw}}.
\end{aligned}$$

The trace of *any* normal element

Denote the number of non-zero entries in row i of T_α as r_i, then for any $l = 0, 1, \ldots, k-1$ we find

$$\sum_w (\alpha\alpha_{j+lm})^{q^{mw}} = \sum_w \left(\sum_{s=0}^{r_{j+lm}-1} a_s \alpha_{\tau_s} \right)^{q^{mw}}.$$

Since $\beta = \sum_w \alpha^{q^{mw}}$ we find

$$\sum_w (\alpha\alpha_{j+lm})^{q^{mw}} = \sum_{s=0}^{r_{j+lm}-1} a_s \beta_{\tau_s}.$$

Gauss periods of type $(n, 3)$

We generate the multiplication tables of Gauss periods over $\mathbb{F}_p$ for small n, k using Maple. For $k = 3$ we prove the following:

Proposition. Let $p > 3$ and let $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ be a normal basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ generated by a type $(n, 3)$ Gauss period. Then the complexity of N is $4n - 4$.

Furthermore, the first row of T_α contains exactly 2 nonzero terms, the $n/2$ row has n nonzero terms and each remaining row has exactly 3 nonzero terms.

Gauss periods of type $(n, 3)$ cont'd

Remark. When the characteristic $p \leq 3$ there is a reduction in the complexity due to additional cancelations.

Ash, Blake and Vanstone proved that, for $p = 2$, the complexity of the basis is precisely $4n - 7$. We additionally give the multiplication table: the first row has one nonzero term, the $n/2$ row has $n - 2$ nonzero terms and all other rows have 3 nonzero terms.

For $p = 3$ we conclude that the complexity of the basis is $3n - 2$. The first row and the $n/2$ row have 2 nonzero terms each, and every remaining row has 3 nonzero terms.

The trace of a type $(n, 3)$ Gauss period

Suppose α is a type $(n, 3)$ Gauss period generating a normal basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, $p \geq 3$. Furthermore, suppose $n = lm$ and let

$$\beta = \mathsf{Tr}_{p^n/p^m}(\alpha).$$

Then, if m is odd, an upper-bound for the complexity of the basis generated by β is $(3l + 1)m - 3l$. If m is even this becomes $(3l + 2)m - 6l$.

Further questions

Gauss periods of type (n, t), t prime. We conjecture that our method, based on examining cyclotomic numbers $(\mathrm{mod}\ p)$, is valid for Gauss periods of type (n, t), t prime.

The dual basis of the trace of a Gauss period. Additionally, we can find the complexity of the dual basis of a normal basis. The technique was first noted by Ash, Blake and Vanstone (1989) and has been used in our previous work (2008), Wan and Zhou (2007) and others.

Further questions

Suppose $q = 2$. Masuda, Moura, Panario and Thomson (2008) give a table of best known complexities for degree $n \leq 512$ using known constructions and exhaustive search data. When $n = 2^\ell$, $n > 32$, the authors needed to perform a random search yielding HIGH complexity.

Ash, Blake and Vanstone note that there is no normal basis generated by a Gauss period if 8 divides n. Thus Gauss periods are not the solution. We need a new construction...