5.3 Complexity of normal bases

Shuhong Gao, Clemson University
David Thomson, Carleton University

5.3.1 Optimal and low complexity normal bases

5.3.1 Definition Let $\alpha \in \mathbb{F}_{q^n}$ be normal over $\mathbb{F}_q$ and let $N = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ be the normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ generated by α, where

$$\alpha_i = \alpha^{q^i}, \quad 0 \le i \le n-1.$$

Denote by $T = (t_{ij})$ the $n \times n$ matrix given by

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, \quad 0 \le i \le n-1,$$

where $t_{ij} \in \mathbb{F}_q$. The matrix T is the *multiplication table* of the basis N. Furthermore, the number of non-zero entries of T, denoted by C_N, is the *complexity* (also called the *density*) of the basis N.

5.3.2 Remark An exhaustive search for normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for $n < 40$ is given in [2015], extending previous tables such as those found in [1631]. Using data from the search, the authors in [2015] indicate that normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ follow a normal distribution (with respect to their complexities) which is tightly compacted about a mean of roughly $n^2/2$. We define *low complexity* normal bases loosely to mean normal bases known to have sub-quadratic bounds, with respect to n, on their complexity.

5.3.3 Remark In addition, [2015] gives the minimum-known complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for many values of n using a variety of constructions that appear in this section. Further tables on normal bases are provided in Section 2.2.

5.3.4 Proposition [2199] The complexity C_N of a normal basis N of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is bounded by

$$2n - 1 \le C_N \le n^2 - n + 1.$$

5.3.5 Definition A normal basis is *optimal normal* if it achieves the lower bound in Proposition 5.3.4.

5.3.6 Theorem [139, 2199]

1. (Type I optimal normal basis) Suppose $n+1$ is a prime and q is a primitive element in $\mathbb{Z}_{n+1}$. Let α be a primitive $(n+1)$-st root of unity. Then α generates an optimal normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
2. (Type II optimal normal basis) Suppose $2n+1$ is a prime and let γ be a primitive $(2n+1)$-st root of unity. Assume that the multiplicative group of $\mathbb{Z}_{2n+1}$ is generated by 2 and -1 (that is, either 2 is a primitive element in $\mathbb{Z}_{2n+1}$, or $2n+1 \equiv 3 \pmod 4$ and 2 generates the quadratic residues in Z_{2n+1}). Then $\alpha = \gamma + \gamma^{-1}$ generates an optimal normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

5.3.7 Theorem (Optimal normal basis theorem) [1184] Every optimal normal basis is equivalent to either a Type I or a Type II optimal normal basis. More precisely, suppose $\mathbb{F}_{q^n}$ has an optimal normal basis over $\mathbb{F}_q$ generated by α and let $b = \mathrm{Tr}(\alpha) \in \mathbb{F}_q$. Then one of the following must hold:

1. $n+1$ is a prime, q is primitive modulo $n+1$ and $-\alpha/b$ is a primitive $(n+1)$-st root of unity;
2. $q = 2^v$ with $\gcd(v, n) = 1$, $2n+1$ is a prime such that 2 and -1 generate the multiplicative group of $\mathbb{Z}_{2n+1}$, and $\alpha/b = \gamma + \gamma^{-1}$ for some primitive $(2n+1)$-st root of unity γ.

5.3.8 Remark Gao and Lenstra [1184] prove a more general version of the optimal normal basis theorem. They show that if a finite Galois extension L/K, where K is an arbitrary field, has an optimal normal basis, say generated by α, then there is a prime number r, an r-th root of unity γ in some algebraic extension of L and a nonzero constant $c \in K$ so that one of the following holds:

1. $\alpha = c\gamma$ and L has degree $r-1$ over K (so the polynomial $x^{r-1} + x^{r-2} + x + 1$ is irreducible over K);
2. $\alpha = c(\gamma + \gamma^{-1})$ and L has degree $(r-1)/2$ over K (so the minimal polynomial of $\gamma + \gamma^{-1}$ over K has degree $(r-1)/2$).

5.3.9 Theorem [308] Let $F(x) = x^{q+1} + dx^q - (ax + b)$ with $a, b, d \in \mathbb{F}_q$ and $b \neq ad$. Let f be an irreducible factor of F of degree $n > 1$ and let α be a root of f. Then all the roots of f are

$$\alpha_i = \alpha^{q^i} = \varphi^i(\alpha),\ i = 0, 1, \ldots, n-1,$$

where $\varphi(x) = (ax+b)/(x+d)$. If $\tau = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$, then $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that

$$\alpha \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} = \begin{pmatrix} \tau^* & -e_{n-1} & -e_{n-2} & \cdots & -e_1 \\ e_1 & e_{n-1} & & & \\ e_2 & & e_{n-2} & & \\ \vdots & & & \ddots & \\ e_{n-1} & & & & e_1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{pmatrix} + \begin{pmatrix} b^* \\ b \\ b \\ b \\ b \end{pmatrix}, \qquad (5.3.1)$$

where $e_1 = a$, $e_{i+1} = \varphi(e_i)$ $(i \geq 1)$, $b^* = -b(n-1)$ and $\tau^* = \tau - \epsilon$ with

$$\epsilon = \sum_{i=0}^{n-1} e_i = \begin{cases} (n-1)(a-d)/2 & \text{if } p \neq 2, \\ a = d & \text{if } p = n = 2, \\ a - d & \text{if } p = 2 \text{ and } n \equiv 3 \pmod 4, \\ 0 & \text{if } p = 2 \text{ and } n \equiv 1 \pmod 4. \end{cases}$$

5.3.10 Corollary [308] The following are two special cases of the above theorem.

1. For every $a, \beta \in \mathbb{F}_q^*$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta) = 1$,

$$x^p - \frac{1}{\beta} a x^{p-1} - \frac{1}{\beta} a^p$$

is irreducible over $\mathbb{F}_q$ and its roots form a normal basis of $\mathbb{F}_{q^p}$ over $\mathbb{F}_q$ of complexity at most $3p-2$. This corresponds to the case of Theorem 5.3.9 with $n = p$, $e_1 = a$, $\varphi(x) = ax/(x+a)$, $b = b^* = 0$, and $\tau^* = a/\beta$ if $p \neq 2$ and $\tau^* = a/\beta - a$ if $p = 2$.

2. Let n be any factor of $q-1$. Let $\beta \in \mathbb{F}_q$ have multiplicative order t such that $\gcd(n, (q-1)/t) = 1$ and let $a = \beta^{(q-1)/n}$. Then

$$x^n - \beta(x - a + 1)^n$$

is irreducible over $\mathbb{F}_q$ and its roots form a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with complexity at most $3n-2$. This corresponds to the case of Theorem 5.3.9 with $e_1 = a$, $\varphi(x) = ax/(x+1)$, $b = b^* = 0$, and $\tau^* = -n(a-1)\beta/(1-\beta) - \epsilon$, with ϵ given as in Theorem 5.3.9 with $d = 1$.

5.3.11 Conjecture [3036] If there does not exist an optimal normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then the complexity of a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is at least $3n-3$.

5.3.12 Remark Explicit constructions of low complexity normal bases beyond the optimal normal bases and the constructions given in Theorem 5.3.10 are rare. In Section 5.3.2 we give a generalization of optimal normal bases arising from *Gauss periods*. Below, we illustrate how to construct new normal bases of low complexity arising from previously known normal bases.

5.3.13 Proposition [1172, 2578, 2580] Suppose $\gcd(m, n) = 1$ and α and β generate normal bases A and B for $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, respectively. By Proposition 5.2.3, $\alpha\beta$ generates a normal basis N for $\mathbb{F}_{q^{mn}}$ over $\mathbb{F}_q$. Furthermore, we have $C_N = C_A C_B$ and if α and β both generate optimal normal bases, then $C_N = 4mn - 2m - 2n + 1$.

5.3.14 Proposition [634] Let $n = mk$ and suppose $\alpha \in \mathbb{F}_{q^n}$ generates a normal basis $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ over $\mathbb{F}_q$ with multiplication table $T = (t_{ij})$ for $0 \le i, j \le n-1$. Then

$$\beta = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^m}}(\alpha) = \alpha_0 + \alpha_m + \alpha_{2m} + \cdots + \alpha_{(k-1)m}$$

generates a normal basis $(\beta_0, \beta_1, \ldots, \beta_{m-1})$ for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ with

$$\beta\beta_i = \sum_{j=0}^{m-1} s_{ij}\beta_j, \quad 0 \le i \le m-1,$$

where

$$s_{ij} = \sum_{0 \le u, v \le k-1} t_{um+i, vm+j}, \quad 0 \le i, j \le m-1.$$

5.3.15 Corollary [633, 634, 1931] Let $n = mk$. Upper-bounds on the complexity obtained from traces of optimal normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are given in Table 5.3.1.

	Type I (q odd):	Type I ($q = 2$):	Type II ($q = 2$):
m even, k odd, $p \mid k$	$km - (k+1)/2$	–	–
m even, k odd, $k \equiv 1 \pmod{p}$	$(k+1)m - (3k+1)/2$	$(k+1)m - 3k + 2^*$	$2km - 2k + 1$
m even, k odd, all other k	$(k+1)m - (3k+1)/2$	–	–
k even, $p \mid k$	$km - k/2^\dagger$	$km - k + 1$	$2km - 2k + 1$
k even, $k \equiv 2 \pmod{p}$	$(k+1)m - 3k/2 + 1^\dagger$	$km - k + 1$	$2km - 2k + 1$
k even, all other k	$(k+1)m - k$	–	–

Table 5.3.1 Upper-bounds on the complexity obtained from of traces of optimal normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $n = mk$. *Tight when $k = 3$; †tight when $k = 2, 3$.

5.3.2 Gauss periods

5.3.16 Definition [139] Let $r = nk + 1$ be a prime not dividing q and let γ be a primitive r-th root of unity in $\mathbb{F}_{q^{nk}}$. Furthermore, let K be the unique subgroup of order k in $\mathbb{Z}_r^*$ and $K_i = \{a \cdot q^i : a \in K\} \subseteq \mathbb{Z}_r^*$ be cosets of K, $0 \le i \le n-1$. The elements

$$\alpha_i = \sum_{a \in K_i} \gamma^a \in \mathbb{F}_{q^n}, \quad 0 \le i \le n-1,$$

are *Gauss periods* of type (n, k) over $\mathbb{F}_q$.

5.3.17 Theorem [1180, 2951] Let $\alpha_i \in \mathbb{F}_{q^n}$ be Gauss periods of type (n, k) as defined in Definition 5.3.16. The following are equivalent:

1. $N = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ is a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$;
2. $\gcd(nk/e, n) = 1$, where e is the order of q modulo r;
3. the union of $K_0, K_1, \ldots, K_{n-1}$ is $\mathbb{Z}_r^*$; equivalently, $\mathbb{Z}_r^* = \langle q, K \rangle$.

5.3.18 Remark Gauss periods of type $(n, 1)$ define Type I optimal normal bases and Gauss periods of type $(n, 2)$ define Type II optimal normal bases when $q = 2$.

5.3.19 Remark For the remainder of this section, we are concerned with Gauss periods which are *admissible* as normal bases, that is, where the properties in Theorem 5.3.17 hold. When the characteristic p does not divide n, the existence of admissible Gauss periods of type (n, k) is shown assuming the ERH in [14, 159] for any n with $k \le (cn)^3(\log(np))^2$. For any k and prime power q, assuming the GRH, there are infinitely many n such that there is an admissible Gauss period of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ [1236]. In contrast, when p divides n, [2952] contains necessary and sufficient conditions for admissible Gauss periods, thus showing the non-existence of admissible Gauss periods in certain cases.

5.3.20 Proposition [1180] There is no admissible Gauss period of type (n, k) over $\mathbb{F}_2$ if 8 divides nk.

5.3.21 Definition Let K_i be defined as in Definition 5.3.16 for $i = 0, 1, \ldots, n-1$. The *cyclotomic numbers* are given by $c_{ij} = |(1 + K_i) \cap K_j|$.

5.3.22 Proposition [259, 1180] Let $N = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ be the normal basis arising from Gauss periods of type (n, k) for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $j_0 < n$ be the unique index such that $-1 \in \kappa_{j_0}$, and let $\delta_j = 1$ if $j = j_0$ and 0 if $j \ne j_0$. Then

$$\alpha\alpha_i = \delta_i k + \sum_{j=0}^{n-1} c_{ij}\alpha_j, \quad 0 \le i \le n-1,$$

hence $C_N \le (n-1)k + n$.

5.3.23 Proposition [139, 259] Let p be the characteristic of $\mathbb{F}_q$ and let $N = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ be the normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ arising from Gauss periods of type (n, k).

1. If p divides k, then $C_N \le nk - 1$.
2. If $p = 2$, then

$$\begin{cases} kn - (k^2 - 3k + 3) \le C_N \le (n-1)k + 1 & \text{if } k \text{ even,} \\ (k+1)n - (k^2 - k + 1) \le C_N \le (n-2)k + n + 1 & \text{if } k \text{ odd.} \end{cases}$$

3. If $q = 2$ and $k = 2^v r$, where either $r = 1$ or both r is an odd prime and $v \le 2$, then the lower bounds above are tight for sufficiently large n.

5.3.24 Problem Find the complexity of Gauss periods of type (n, k) over $\mathbb{F}_2$ for all n when k is not a prime, twice an odd prime or four times an odd prime.

5.3.25 Remark [139, 634] The complexities of normal bases arising from Gauss periods of type (n, k), $2 \le k \le 6$, are given in Table 5.3.2 for all characteristics p when $n > p$.

Type $(n,1)$	Type $(n,2)$		Type $(n,3)$			Type $(n,4)$		
all p	$p=2$	$p>2$	$p=2$	$p=3$	$p>3$	$p=2$	$p=3$	$p>3$
$2n-1$	$2n-1$	$3n-2$	$4n-7$	$3n-2$	$4n-4$	$4n-7$	$5n-7$	$5n-6$

Type $(n,5)$				Type $(n,6)$			
$p=2$	$p=3$	$p=5$	$p>5$	$p=2$	$p=3$	$p=5$	$p>5$
$6n-21$	$6n-11$	$5n-7$	$6n-11$	$6n-21$	$6n-11$	$7n-15$	$7n-14$

Table 5.3.2 Complexities of normal bases from Gauss periods of Type (n, k), $2 \le k \le 6$, $n > p$.

5.3.26 Remark Let $q = 2$. Proposition 5.3.13 can be used to create normal bases of large extension degree by combining normal bases of subfields with coprime degree. By Proposition 5.3.20 Gauss periods of type (n, k) do not exist when 8 divides nk. Hence, Proposition 5.3.13 cannot be used to construct low complexity normal bases when the degree is a prime power. Thus, when n is a prime power (specifically a power of two), there are no constructions of low-complexity normal bases arising from the above propositions.

5.3.27 Problem Find explicit constructions of low-complexity normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ when n is a power of two.

5.3.28 Remark Normal bases of low complexity are useful in fast encoding and decoding of network codes, see [2665] for more details.

5.3.3 Normal bases from elliptic periods

5.3.29 Remark Proposition 5.2.20, Theorem 5.3.9 and its corollaries show how the multiplicative group of $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$ can be used to construct irreducible polynomials and normal bases for those degrees n whose prime factors divide $q - 1$ or $q + 1$. Also, Gauss periods use the multiplicative group of $\mathbb{F}_{q^{r-1}}$ for some prime r. Couveignes and Lercier [746] show how these methods can be generalized by using elliptic curve groups. The normal bases from their construction may not have low complexity, but these bases still allow a fast algorithm for multiplication. We outline their construction below; for more details on how to perform fast multiplication using elliptic periods, we refer the reader to [746]. For properties of elliptic curves, see Section 12.2.

5.3.30 Remark Let E be an elliptic curve over $\mathbb{F}_q$ defined by a Weierstrass equation

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6,$$

where $a_i \in \mathbb{F}_q$. The points of E over every extension of $\mathbb{F}_q$ form an additive group with the point O at infinity as the identity. The order of the group $E(\mathbb{F}_q)$ is $q+1-t$ for some integer t with $|t| \le 2\sqrt{q}$. Let $n > 1$ be an integer such that $E(\mathbb{F}_q)$ has a cyclic subgroup F of order n. The quotient $E' = E/F$ is also an elliptic curve over $\mathbb{F}_q$ and there is an isogeny

$$\phi : E \to E',$$

that has F as its kernel, and ϕ is defined by rational functions in $\mathbb{F}_q[X,Y]$. For any point $P \in E$, let $x(P)$ denote the x-coordinate of P and similarly denote $y(P)$, thus

$$P = (x(P), y(P)).$$

Vélu [2865] gives a formula for E' and ϕ. In fact, for $P \in E$,

$$\phi(P) = \left(x(P) + \sum_{T \in F \setminus \{O\}} (x(P+T) - x(T))\,,\ y(P) + \sum_{T \in F \setminus \{O\}} (y(P+T) - y(T)) \right).$$

5.3.31 Remark We describe here an explicit formula due to Kohel [1779] for E' and ϕ when E is of the form

$$E: \quad Y^2 = X^3 + aX + b.$$

We denote by D the kernel polynomial given by

$$\begin{aligned} D(X) &= \prod_{Q \in F \setminus \{O\}} (X - x(Q)) \\ &= X^n - c_1 X^{n-1} + c_2 X^{n-2} - c_3 X^{n-3} + \cdots + (-1)^n c_n \in \mathbb{F}_q[X]. \end{aligned}$$

Then, for $P = (x, y) \in E$,

$$\phi(P) = \left(\frac{N(x)}{D(x)},\ y \cdot \left(\frac{N(x)}{D(x)} \right)' \right),$$

where $N(x)$ is determined by the equation:

$$\frac{N(x)}{D(x)} = nx - c_1 - (3x^2 + a) \frac{D'(x)}{D(x)} - 2(x^3 + ax + b) \left(\frac{D'(x)}{D(x)} \right)'.$$

Furthermore, E' is defined by

$$Y^2 = X^3 + (a - 5v)X + (b - 7w),$$

where

$$v = a(n-1) + 3(c_1^2 - 2c_2), \quad w = 3ac_1 + 2b(n-1) + 5(c_1^3 - 3c_1c_2 + 3c_3).$$

5.3.32 Definition Let $T \in E(\mathbb{F}_q)$ be a point of order n and ϕ be the corresponding isogeny with its kernel generated by T. For any point $P \in E(\mathbb{F}_{q^n})$ with $\phi(P) \in E'(\mathbb{F}_q)$, let $\theta(P,T)$ denote the slope of the line passing through the two points T and $P+T$, that is

$$\theta(P,T) = \frac{y(P+T) - y(T)}{x(P+T) - x(T)} \in \mathbb{F}_{q^n}.$$

The element $\theta(P,T)$ is an *elliptic period* over $\mathbb{F}_q$.

5.3.33 Theorem [746] Let $T \in E(\mathbb{F}_q)$ be a point of order $n \geq 3$ and ϕ be the corresponding isogeny with its kernel generated by T. Suppose there is a point $P \in E(\mathbb{F}_{q^n})$ so that $n\,P \neq O$ in E and $\phi(P) \in E'(\mathbb{F}_q)$. Then either

1. the elliptic period $\theta(P,T)$ is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if the trace of $\theta(P,T)$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is nonzero, or

2. the element $1+\theta(P,T)$ is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if the trace of $\theta(P,T)$ is zero.

5.3.34 Example [746] Consider the following curve over $\mathbb{F}_7$

$$E: \quad y^2+xy-2y = x^3+3x^2+3x+2.$$

The point $T=(3,1)\in E(\mathbb{F}_7)$ has order $n=5$, so the subgroup $F=\langle T\rangle$ has order 5. By Vélu's formula, the equation for $E'=E/F$ is

$$E': \quad y^2+xy-2y = x^3+3x^2-3x-1,$$

and the corresponding isogeny is

$$\begin{aligned}\phi(x,y) \quad &= \quad \Bigg(\frac{x^5+2x^2-2x-1}{x^4+3x^2-3}, \\ &\quad \frac{\left(x^6-3x^4+3x^3-x^2+3x-3\right)y+3x^5+x^4+x^3+3x^2-3x+1}{x^6+x^4-2x^2-1}\Bigg).\end{aligned}$$

Take $A=(4,2)\in E'(\mathbb{F}_7)$. We note that the polynomial

$$f(X)=(X^5+2X^2-2X-1)+3(X^4+3X^2-3)=X^5+3X^4-3X^2-2X-3$$

is irreducible over $\mathbb{F}_7$. Hence $\mathbb{F}_{7^5}=\mathbb{F}_7[\alpha]$, where α is a root of f. Compute β so that $\phi(\alpha,\beta)=(4,2)$. We find that

$$\beta=\alpha^{4756}=-\alpha^3-\alpha^2+3\alpha+2,$$

and $P=(\alpha,\beta)\in E(\mathbb{F}_{7^5})$. We check that $5\,P\neq O$ in E and we note that

$$P+T=(-3\alpha^4+3\alpha^2+2\alpha-1,-\alpha^4+\alpha^3+\alpha^2+1).$$

Hence

$$\theta(P,T)=\frac{Y(P+T)-Y(T)}{X(P+T)-X(T)}=-\alpha^4+\alpha^3+3\alpha^2-3\alpha-3$$

is a normal element in $\mathbb{F}_{7^5}$ over $\mathbb{F}_7$.

5.3.4 Complexities of dual and self-dual normal bases

5.3.35 Remark For the definition of dual and self-dual bases, see Definition 2.1.100. Self-dual normal bases have been well studied due to their efficiency in implementation, see Section 16.7. A complete treatment of dual bases over finite fields can be found in [1631, Chapter 4], see also Sections 5.1 and 5.2.

5.3.36 Remark It is computationally easier to restrict an exhaustive search to self-dual normal bases. Geiselmann in [1263, 1631] computes the minimum complexity for a self-dual normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for all $n\le 47$. These computations are repeated for odd degrees $n\le 45$ in [130] and the authors also give tables of minimum complexity self-dual normal bases over finite fields of odd characteristic and for extensions of $\mathbb{F}_{2^\ell}, \ell>1$. Some additional searches for self-dual normal bases can be found in [2015].

5.3.37 Proposition [1632] Let N be a normal basis with multiplication table T. Then N is self-dual if and only if T is symmetric.

5.3.38 Proposition [1632] Let $\gcd(m,n)=1$. Suppose α and β generate normal bases A and B for $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, respectively. Then $\gamma=\alpha\beta$ generates a self-dual normal basis N for $\mathbb{F}_{q^{mn}}$ over $\mathbb{F}_q$ if and only if both A and B are self-dual, as in Proposition 5.2.3. The complexity of the basis N is $C_N=C_AC_B$, as in Proposition 5.3.13.

5.3.39 Proposition [1632, 2422] Let n be even, $\alpha\in\mathbb{F}_{2^n}$ and $\gamma=1+\alpha$. Then,

1. the element α generates a self-dual normal basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ if and only if γ does;
2. if α and $\gamma=1+\alpha$ generate self-dual normal bases B and $\bar{B}$, respectively, for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, then the complexities of B and $\bar{B}$ are related by

$$C_{\bar{B}}=n^2-3n+8-C_B.$$

5.3.40 Corollary Suppose $n\equiv 2 \pmod 4$, then the following hold

1. the average complexity of a self-dual normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is $\frac{1}{2}(n^2-3n+8)$;
2. if B is a self-dual normal basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, we have

$$2n-1\le C_B\le n^2-5n+9,$$

and one of the equalities holds if and only if either B or its complement $\bar{B}$ is optimal.

5.3.41 Proposition [308] Let q be a power of a prime p. For any $\beta\in\mathbb{F}_q^*$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\beta)=1$,

$$x^p-x^{p-1}-\beta^{p-1}$$

is irreducible over $\mathbb{F}_q$ and its roots form a self-dual normal basis of $\mathbb{F}_{q^p}$ over $\mathbb{F}_q$ with complexity at most $3p-2$. The multiplication table is as in Theorem 5.3.10 with $e_1=\beta$, $e_{i+1}=\varphi(e_i)$ for $i\ge 1$, $\varphi(x)=\beta x/(x+\beta)$, $\tau^*=1$ if $p\ne 2$ and $\tau^*=1-\beta$ if $p=2$.

5.3.42 Proposition [308] Let n be an odd factor of $q-1$ and let $\xi\in\mathbb{F}_q$ have multiplicative order n. Then there exists $u\in\mathbb{F}_q$ such that $(u^2)^{(q-1)/n}=\xi$. Let $x_0=(1+u)/n$ and $x_1=(1+u)/(nu)$. Then the monic polynomial

$$\frac{1}{1+u^2}\big((x-x_0)^n-u^2(x-x_1)^n\big)$$

is irreducible over $\mathbb{F}_q$ and its roots form a self-dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The multiplication table is as in Theorem 5.3.9 with $a=(x_0-\xi x_1)/(1-\xi)$, $b=-x_0x_1$, $d=a-(x_0-x_1)$ and $\tau=1$.

5.3.43 Proposition [308] Let n be an odd factor of $q+1$ and let $\xi\in\mathbb{F}_{q^2}$ be a root of $x^{q+1}-1$ with multiplicative order n. Then there is a root u of $x^{q+1}-1$ such that $(u^2)^{q+1}/n=\xi$. Let $x_0=(1+u)/n$ and $x_1=(1+u)/(nu)$. Then

$$\frac{1}{1-u^2}\big((x-x_0)^n-u^2(x-x_1)^n\big)$$

is irreducible over $\mathbb{F}_q$ and its roots form a self-dual normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The multiplication table is as in Theorem 5.3.9 with $a=(x_1-\xi x_0)/(1-\xi)$, $b=-x_0x_1$, $d=a-(x_0+x_1)$ and $\tau=1$.

5.3.4.1 Duals of Gauss periods

5.3.44 Proposition [1180, 1930] Let α be a type (n,k) Gauss period generating a normal basis N and let $j_0 = 0$ if k is even and $j_0 = n/2$ if k is odd. Then the element

$$\gamma = \frac{\alpha^{q^{j_0}} - k}{nk+1}$$

is dual to α, and hence γ generates the dual basis $\tilde{N}$ of N. Furthermore, the complexity of the dual basis $\tilde{N}$ is

$$C_{\tilde{N}} \leq \begin{cases} (k+1)n - k & \text{if } p \nmid k, \\ kn - 1 & \text{if } p \mid k. \end{cases}$$

5.3.45 Corollary [1180] For $n > 2$, a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ arising from Gauss periods of type (n,k) is self-dual if and only if k is even and divisible by the characteristic of $\mathbb{F}_q$. In particular, Type II optimal normal bases are self-dual.

5.3.46 Proposition [2924] The complexity of the dual of a Type I optimal normal basis is $3n-2$ if q is odd and $3n-3$ if q is even.

5.3.47 Remark [633] Upper bounds on the complexities of the dual basis of the $\mathbb{F}_{q^m}$-trace of optimal normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $n = mk$, are given in Table 5.3.3.

	Type I (q odd)	Type I (q even)	Type II (q even)
m odd	$(k+2)m-2$	$(k+2)(m-1)+1$	$2k(m-1)+1$
m even	$(k+3)m-k-4$	$(k+3)m-2k-3$	$2k(m-1)+1$

Table 5.3.3 Upper bounds on complexities of the dual bases of the trace of optimal normal bases.

5.3.5 Fast arithmetic using normal bases

5.3.48 Remark In practical applications it is important to know how to do fast arithmetic in finite fields, for example addition, multiplication and division; and for cryptographic applications it is also desirable to have elements of high orders and a fast algorithm for exponentiation. Details for the basic operations discussed in this section can be found in Section 11.1, see also [1227]. In hardware implementations, normal bases are often preferred, see Section 16.7 for details on hardware implementations. This subsection presents some theoretical results related to fast multiplication and exponentiation under normal bases generated by Gauss periods.

5.3.49 Remark Gao and Vanstone [1188] first observed that a Type II optimal normal basis generator has high order, which was proved later by von zur Gathen and Shparlinski [1240]; for more details see Section 4.4. Computer experiments by Gao, von zur Gathen and Panario [1179] indicate that Gauss periods of type (n,k) with $k > 2$ also have high orders; however, it is still open whether one can prove a subexponential lower bound on their orders.

5.3.50 Problem Give tight bounds on the orders of Gauss periods of type (n,k), $k > 2$.

5.3.51 Proposition [1179, 1188] Suppose $\alpha \in \mathbb{F}_{q^n}$ is a Gauss period of type (n,k) over $\mathbb{F}_q$. Then for any integer $1 \leq t < q^n - 1$, α^t can be computed using at most n^2k operations in $\mathbb{F}_q$.

5.3.52 Theorem [1180] Suppose γ is an element of order r (not necessarily a prime) and

$$\alpha = \sum_{i \in K} \gamma^i$$

generates a normal basis N for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where K is a subgroup of $\mathbb{Z}_r^\times$. With $\mathbb{F}_{q^n}$ represented under the normal basis N, we have

1. addition and subtraction can be computed in $O(n)$ operations in $\mathbb{F}_q$;
2. multiplication can be computed in $O(r \log r \log\log r)$ operations in $\mathbb{F}_q$;
3. division can be computed in $O(r \log^2 r \log\log r)$ operations in $\mathbb{F}_q$;
4. exponentiation of an arbitrary element in $\mathbb{F}_{q^n}$ can be computed in $O(nr \log r \log\log r)$ operations in $\mathbb{F}_q$.

5.3.53 **Remark** Theorem 1.5 in [1174] tells us when and how to find such a subgroup K in the above theorem. The element α can be a Gauss period or a generalized Gauss period, see Example 5.3.54 for more information. We outline the algorithm from [1180] for fast multiplication and division. The basic idea is to convert the normal basis representation to a polynomial basis in the ring $R = \mathbb{F}_q[x]/(x^r - 1)$, do fast multiplication of polynomials in the ring, then convert the result back to the normal basis. More precisely, let γ and α be as in Theorem 5.3.52. The condition of the theorem implies that that $K, qK, \ldots, q^{n-1}K$ are disjoint subsets of $\mathbb{Z}_r$ and $q^nK = K$. For $0 \le j \le n-1$, let $K_j = q^jK \subseteq \mathbb{Z}_r$, and

$$\alpha_j = \sum_{i \in K_j} \beta^i.$$

Then $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ is the normal basis generated by α, with the following property:

$$\alpha_0 + \alpha_1 + \cdots + \alpha_{n-1} = -1.$$

For each element $A = a_0\alpha_0 + a_1\alpha_1 + \cdots + a_{n-1}\alpha_{n-1} \in \mathbb{F}_{q^n}$, where $a_i \in \mathbb{F}_q$, we associate a polynomial

$$A(x) = \sum_{i=0}^{r-1} u_i x^i,$$

where $u_i = a_j$ if $i \in K_j$ for some j, and $u_i = 0$ if i is not in any K_j. This can be viewed as a map from $\mathbb{F}_{q^n}$ to $R = \mathbb{F}_q[x]/(x^r - 1)$. The map is in fact a ring homomorphism.

Suppose we have two arbitrary elements $A, B \in \mathbb{F}_{q^n}$. To compute AB, we first write them as polynomials $A(x), B(x) \in \mathbb{F}_q[x]$ of degree at most $r-1$ as above. Then we use a fast algorithm to compute the product polynomial $C_1(x) = A(x)B(x)$ of degree at most $2r-2$. This step needs $O(r \log r \log\log r)$ operations in $\mathbb{F}_q$, see [1227]. Next, we reduce C_1 modulo $x^r - 1$ (just reduce the exponents of x modulo r) to get a polynomial

$$C_2(x) = c_0 + c_1x + \cdots + c_{r-1}x^{r-1}.$$

The coefficients satisfy the property that $c_i = c_j$ whenever $i, j \in K_\ell$ for some $0 \le \ell \le n-1$. Since $\sum_{j=0}^{n-1} \alpha_j = -1$, we conclude that

$$AB = d_0\alpha_0 + d_1\alpha_1 + \cdots + d_{n-1}\alpha_{n-1}, \qquad \text{where } d_i = c_j - c_0 \text{ for any } j \in K_i.$$

To compute A^{-1} (assuming $A \ne 0$), we apply a fast gcd algorithm to the two polynomials $A(x)$ and $x^r - 1$ to get a polynomial $U(x)$ of degree at most $r-1$ so that $A(x)U(x) \equiv 1 \pmod{x^r - 1}$. The element in $\mathbb{F}_{q^n}$ corresponding to the polynomial $U(x)$ is the desired inverse of A. The fast gcd step needs $O(r \log^2 r \log\log r)$ operations in $\mathbb{F}_q$, see [1227].

5.3.54 **Example** (Generalized Gauss Periods [1047, 1174]) For any normal basis from Gauss periods of type (n, k), we can apply Theorem 5.3.52 to perform fast arithmetic in $\mathbb{F}_{q^n}$. To obtain an admissible Gauss period of type (n, k), $r = nk + 1$ must be a prime. Here we give an example of generalized Gauss periods where r is not prime. Suppose we want to perform fast arithmetic in $\mathbb{F}_{2^{954}}$. Let $n = 954$ and note that the smallest k so that there is an admissible Gauss period of type (n, k) over $\mathbb{F}_2$ is $k = 49$. The corresponding $r = nk + 1 = 46747$ is a little big in this case. We observe that $954 = 106 \cdot 9$ and that there is an admissible Gauss period α_1 of type $(106, 1)$ over $\mathbb{F}_2$, and an admissible Gauss period α_2 of type $(9, 2)$. Then $\alpha = \alpha_1\alpha_2$ is a normal element of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. We construct this α as follows. Let

$$r = (106 \cdot 1 + 1)(9 \cdot 2 + 1) = 2033, \quad K = \{1, 322\}.$$

Then K is a subgroup of $\mathbb{Z}_r^\times$ satisfying the condition in Theorem 5.3.52. Let γ be any primitive r-th root of unity in an extension field of $\mathbb{F}_2$. Then

$$\alpha = \gamma + \gamma^{322}$$

is a generalized Gauss period that is normal for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Now we can apply Theorem 5.3.52 to perform fast arithmetic in $\mathbb{F}_{q^n}$ with a much smaller r. In [1174], it is shown how to find generalized Gauss periods with minimum r and the related subgroups K; see [1174, Tables 2-4] for many more examples for which generalized Gauss periods are better than Gauss periods.

5.3.55 Example (Fast arithmetic under type II optimal normal bases) For type II optimal normal bases over $\mathbb{F}_2$, we describe below a slightly faster algorithm from [248, 1238]. Suppose $2n+1$ is a prime and the multiplicative group of $\mathbb{Z}_{2n+1}$ is generated by -1 and 2. Let $\gamma \in \mathbb{F}_{2^{2n}}$ be an element of order $2n + 1$. For any $i \geq 0$, define

$$\gamma_i = \gamma^i + \gamma^{-i}.$$

Then $N = (\gamma_1, \gamma_2, \ldots, \gamma_n)$ is a permutation of the normal basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ generated by

$$\alpha = \gamma_1 = \gamma + \gamma^{-1}.$$

We note that $\gamma_0 = 2$ and

$$\gamma_1 + \gamma_2 + \cdots + \gamma_n = 1.$$

To do fast multiplication and division in $\mathbb{F}_{2^n}$, we first perform a basis transition from N to the polynomial basis $P = (\alpha, \alpha^2, \ldots, \alpha^n)$, then perform a fast multiplication of polynomials and finally transform the result back to the basis N. To do the basis transitions, we need the following properties:

$$\gamma_{i+j} = \gamma_i\gamma_j + \gamma_{j-i}, \quad \text{for all } i, j.$$

To see how to go from the basis N to the basis P, suppose we have an expression

$$A = a_1\gamma_1 + a_2\gamma_2 + \cdots + a_\ell\gamma_\ell,$$

where $a_i \in \mathbb{F}_2$ and $\ell \geq 1$ is arbitrary. We want to express A as a combination of $\alpha, \alpha^2, \ldots, \alpha^\ell$ over $\mathbb{F}_2$. Let m be a power of 2 so that $\ell/2 \leq m < \ell$. Then

$$\gamma_m = \alpha^m.$$

We observe that

$$\begin{aligned}
& a_1\gamma_1 + a_2\gamma_2 + \cdots + a_\ell\gamma_\ell \\
= \;& a_1\gamma_1 + \cdots + a_m\gamma_m + a_{m+1}(\gamma_m\gamma_1 + \gamma_{m-1}) + \cdots + a_\ell(\gamma_m\gamma_{\ell-m} + \gamma_{m-(\ell-m)}), \\
= \;& (a_1\gamma_1 + \cdots + a_m\gamma_m + a_{m+1}\gamma_{m-1} + \cdots + a_\ell\gamma_{m-(\ell-m)}) \\
& \quad + \alpha^m (a_{m+1}\gamma_1 + a_{m+2}\gamma_2 + \cdots + a_\ell\gamma_{\ell-m}).
\end{aligned}$$

We note that the first part is of the form $U = u_1\gamma_1 + \cdots + u_m\gamma_m$, where $u_i \in \mathbb{F}_2$, which can be computed using m bit operations. Let $V = a_{m+1}\gamma_1 + a_{m+2}\gamma_2 + \cdots + a_\ell\gamma_{\ell-m}$, where $\ell - m \leq m$. Apply the method recursively to convert U and V into the power basis, say

$$U = b_1\alpha + \cdots + b_m\alpha^m, \quad V = b_{m+1}\alpha + \cdots + b_\ell\alpha^{\ell-m},$$

where $b_i \in \mathbb{F}_2$. Then

$$A = U + \alpha^m V = b_1\alpha + \cdots + b_m\alpha^m + b_{m+1}\alpha^{m+1} + \cdots + b_\ell\alpha^\ell.$$

This gives an algorithm for going from N to P using at most $\frac{1}{2}n\log_2(n)$ operations in $\mathbb{F}_2$, where $\log_2(n)$ is the logarithm of n in base 2. By reversing the above procedure, we get an algorithm for going from P to N using at most $\frac{1}{2}n\log_2(n)$ operations in $\mathbb{F}_2$.

This shows that multiplication in $\mathbb{F}_{2^n}$ under N can be computed by (a) two transformations from N to P, (b) one multiplication of polynomials of degree at most n in $\mathbb{F}_2[x]$, and (c) one transformation from $(\alpha, \alpha^2, \ldots, \alpha^{2n})$ to $(\gamma_1, \gamma_2, \ldots, \gamma_{2n})$ which is easily converted to N, as $\gamma_{n+1+i} = \gamma_{n-i}$. The number of bit operations used is the cost for one multiplication of polynomials of degree at most n, plus $2n\log_2 n$ bit operations for the basis transformations. Finally, for division in $\mathbb{F}_{2^n}$, we need to precompute the minimal polynomial of α and apply a fast gcd algorithm for polynomials of degree at most n in $\mathbb{F}_2[x]$.

See Also

§2.2	For standards requiring normal basis arithmetic.
§5.2	For general results on normal bases.
§11.1	For basic operations over finite fields.
§16.7	For hardware implementarions of finite fields arithmetic.
[1179, 1188, 1240]	For orders and cryptographic applications of Gauss Periods.

References cited: [14, 130, 139, 159, 248, 259, 308, 633, 634, 746, 1047, 1172, 1174, 1179, 1180, 1184, 1188, 1227, 1236, 1238, 1240, 1263, 1631, 1632, 1779, 1930, 1931, 2015, 2199, 2422, 2578, 2580, 2665, 2865, 2924, 2951, 2952, 3036].

5.4 Completely normal bases

Dirk Hachenberger, *University of Augsburg*

We present some theoretical results concerning algebraic extensions of finite fields. The starting point is the Complete Normal Basis Theorem, which is a strengthening of the classical Normal Basis Theorem. The search for completely normal elements leads to an interesting structure theory for finite fields comprising a generalization of the class of finite Galois field extensions to the class of cyclotomic modules.

5.4.1 The complete normal basis theorem

5.4.1 Remark Let $\overline{\mathbb{F}}_q$ denote an algebraic closure of the finite field $\mathbb{F}_q$. The Frobenius automorphism of $\overline{\mathbb{F}}_q/\mathbb{F}_q$ (throughout denoted by σ) is the field automorphism mapping each $\theta \in \overline{\mathbb{F}}_q$