Journal of Mathematical Research & Exposition
Sept., 2010, Vol. 30, No. 5, pp. 869–875
DOI:10.3770/j.issn:1000-341X.2010.05.014
Http://jmre.dlut.edu.cn

On Primitive Optimal Normal Elements of Finite Fields

Qun Ying LIAO
College of Mathematics and Software Sciences, Sichuan Normal University, Sichuan 610066*, P. R. China*

Abstract Let q be a prime or prime power and F_{q^n} the extension of q elements finite field F_q with degree n $(n > 1)$. Davenport, Lenstra and Schoof proved that there exists a primitive element $\alpha \in F_{q^n}$ such that α generates a normal basis of F_{q^n} over F_q. Later, Mullin, Gao and Lenstra, etc., raised the definition of optimal normal bases and constructed such bases. In this paper, we determine all primitive type I optimal normal bases and all finite fields in which there exists a pair of reciprocal elements α and α^{-1} such that both of them generate optimal normal bases of F_{q^n} over F_q. Furthermore, we obtain a sufficient condition for the existence of primitive type II optimal normal bases over finite fields and prove that all primitive optimal normal elements are conjugate to each other.

Keywords finite fields; normal bases; primitive elements; optimal normal bases.

Document code A
MR(2000) Subject Classification 12E20
Chinese Library Classification O156.1

1. Introduction and main results

Let q be a power of the prime p and F_{q^n} the extension of the finite field F_q with degree $n(n > 1)$. If $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a normal basis of F_{q^n} over F_q, then $\alpha \in F_{q^n}$ is called a normal basis generator element (or a normal element)of F_{q^n}. Set

$$\alpha \cdot \alpha^{q^i} = \sum_{j=0}^{n-1} t_{i,j}\alpha^{q^j}, \quad 0 \le i \le n-1,$$

then the complexity C_N of N is defined to be the number of non-zero elements $t_{i,j}$, where $t_{i,j} \in F_q$, $i, j, = 0, 1, \ldots, n-1$. Mullin [13] proved that $C_N \ge 2n-1$. The normal basis N is called an optimal normal basis when $C_N = 2n-1$.

There are many papers on normal bases [2–11] or optimal normal bases over finite fields [5, 7]. Mullin, etc., [13] obtained the construction theorems for both type I and type II optimal normal bases.

The construction theorem for a type I optimal normal basis *Suppose that* $n+1$ *is*

Received December 15, 2008; Accepted March 17, 2009
Supported by the National Natural Science Foundation of China (Grant No. 10990011), Special Research Found for the Doctoral Program Issues New Teachers of Higher Education (Grant No. 20095134120001) and the Found of Sichuan Province (Grant No. 09ZA087).
E-mail address: liao_qunying@yahoo.com.cn

a prime and q is primitive in Z_{n+1}, where q is a prime or prime power. Then the n nonunit $(n+1)$-th roots of unity are linearly independent and they form an optimal normal basis N of F_{q^n} over F_q. And $N = \{\alpha^{q^i} | i = 0, \ldots, n-1\} = \{\alpha^j | j = 1, \ldots, n\}$ is called a type I optimal normal basis of F_{q^n} over F_q, where α is a primitive $(n+1)$-th root of unity.

The construction theorem for a type II optimal normal basis *Let $2n+1$ be a prime and assume that either*

(a) 2 is primitive in Z_{2n+1},

or

(b) $2n+1 \equiv 3 \pmod 4$, and 2 generates the quadratic residues in Z_{2n+1}.

Then $\alpha = r + r^{-1}$ generates an optimal normal basis N of F_{2^n} over F_2, where r is a primitive $(2n+1)$-th root of unity. And $N = \{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\} = \{\alpha = r + r^{-1}, r^2 + r^{-2}, \ldots, r^n + r^{-n}\}$ is called a type II optimal normal basis of F_{2^n} over F_2.

Let N be an optimal normal basis of F_{q^n} over F_q. Then for $a \in F_q^*$, $aN = \{a\alpha \,|\, \alpha \in N\}$ is also an optimal normal basis of F_{q^n} over F_q. N and aN are called to be equivalent to each other. Gao and Lenstra [6] proved that an optimal normal basis is always equivalent to the type I or the type II optimal normal basis, therefore they are all optimal normal bases over finite fields.

On the other hand, the well-known normal basis theorem and its generalization over finite fields were given as follows:

Proposition 1.1 *Let q be a power of the prime p and n a positive integer. Then there exists $\alpha \in F_{q^n}$ such that α generates a normal basis of F_{q^n} over F_q, and α is called a normal element of F_{q^n} (The proof can be seen in [3, Theorem 2.35, p57]).*

Proposition 1.2 ([1]) *Let m, n be positive integers and $m \mid n$. Then there exists $\alpha \in F_{q^n}$ such that α generates a normal basis of F_{q^n} over F_{q^m}. Such element $\alpha \in F_{q^n}$ is called a normal element of F_{q^n}.*

Furthermore, if a normal element $\alpha \in F_{q^n}$ is also a primitive element of F_{q^n}, then α is called a primitive normal element. A normal basis generated by a primitive normal element is a primitive normal basis. Davenport [4] studied primitive normal elements and proved their existence as following:

Proposition 1.3 *Let p be prime, then there exists a primitive element α of F_{p^n} which is also a normal element of F_{p^n} over F_p.*

Later, Lenstra and Schoof [9] obtained a general result:

Proposition 1.4 *There exists a primitive element α of F_{q^n} which is also a normal element of F_{q^n} over F_q, where q is a power of the prime p and n is a positive integer.*

On primitive normal elements, Tian and Qi [14] proved the following result:

Proposition 1.5 *Let q be a power of the prime and n a positive integer. If F_{q^n} is the extension of the finite field F_q with degree n $(n > 1)$, then there exists a primitive element $\alpha \in F_{q^n}$ such*

that α and α^{-1} are normal elements of F_{q^n} over F_q when $n \geq 32$.

Naturally there are two questions as follows:

(1) Does there exist a primitive element α of F_{q^n} such that α generates an optimal normal basis of F_{q^n} over F_q?

(2) Does there exist an element $\alpha \in F_{q^n}$ such that both α and α^{-1} generate optimal normal bases of F_{q^n} over F_q?

In this paper, we solve the first question partially and the second one completely. In fact we obtain the following main results.

Theorem 1.6 *Let q be a power of the prime p and F_{q^n} the extension of the finite field F_q with degree n ($n > 1$).*

(1) There exists a primitive element $\alpha \in F_{q^n}$ such that α generates a type I optimal normal basis of F_{q^n} over F_q if and only if $n = q = 2$.

(2) Let $q = 2$ and both $2n+1$ and 2^n-1 be primes. Suppose that $N = \{\alpha^{q^i} \mid i = 0, 1, \ldots, n-1\}$ is a type II optimal normal basis of F_{2^n} over F_2. Then the generator α of N is a primitive element of F_{2^n}.

Remark If $M_n = 2^n - 1$ is prime, then n is also prime. The prime with the form $2^n - 1$ is called Mersenne prime in the name of the French mathematician Marin Mersenne (1588-1648). Until now, people observe 44 distinct Mersenne primes $2^n - 1$, where

$$\begin{aligned} n =& 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, \\ & 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, \\ & 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, \\ & 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657. \end{aligned}$$

Of all the above 44 numbers, there are exactly 7 integers n such that both $2^n - 1$ ($n < 32582657$) and $2n + 1$ are primes, where

$$n = 2, 3, 5, 89, 9689, 21701, 859433$$

and

$$2n + 1 = 5, 7, 11, 179, 19379, 43403, 1718867.$$

If $n = 3$, then the prime $2n + 1 = 7$ satisfies the condition (a) of the type II optimal normal basis. And for the other cases, the corresponding primes $2n + 1$ satisfies the condition (b).

Corollary 1.7 *Let q be a power of the prime and F_{q^n} the extension of the finite field F_q with degree n ($n > 1$). If there exists a primitive element $\alpha \in F_{q^n}$ such that α generates an optimal normal basis of F_{q^n} over F_q, then $q = 2$ and there exactly exists one primitive optimal normal basis of F_{q^n} over F_q. This means there are exactly n distinct primitive optimal normal elements which are conjugate to each other.*

Theorem 1.8 *Let q be a power of the prime and F_{q^n} the extension of the finite field F_q with*

degree n ($n > 1$). If α generates an optimal normal basis of F_{q^n} over F_q, then α^{-1} generates also an optimal normal basis of F_{q^n} over F_q iff $n = q = 2$ or there exists only type I optimal normal bases of F_{q^n} over F_q.

Corollary 1.9 *Let q be a power of the prime and F_{q^n} the extension of the finite field F_q with degree n ($n > 1$). If α is a primitive optimal normal element of F_{q^n}, then α^{-1} is also a primitive optimal normal element of F_{q^n} iff $n = q = 2$.*

2. Proofs of main results

From now on, we denote $\gcd(a, b)$ to be the greatest common divisor for two integers a and b. Before proving our main results, we first give one Lemma as follows.

Lemma 2.1 ([8, Ex 1.5.4, p47]) *Let q be a power of the prime p, and F_{q^n} the extension of the finite field F_q with degree n ($n > 1$). Suppose that α is a primitive element of F_{q^n}, then all primitive elements of F_{q^n} are in the form α^k, where $1 \le k \le q^n - 1$ and $\gcd(k, q^n - 1) = 1$.*

The Proof for Theorem 1.6 (1) Suppose that $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a type I optimal normal basis of F_{q^n} over F_q and the generator α of N is a primitive element of F_{q^n}. Then the order of α in the multiply group $F_{q^n}^*$ is $q^n - 1$. From the construction Theorem of the type I optimal normal basis, we know that α is also a primitive $(n+1)$-th root of unity, i.e., $\alpha^{n+1} = 1$. Thus $q^n - 1 \mid n + 1$. But N is a type I optimal normal basis, and then $n + 1$ is prime. Therefore $q^n - 1 = n + 1$ and the equality is true if and only if $n = q = 2$.

Conversely, if $n = q = 2$ and $N = \{\alpha, \alpha^2\}$ is a type I optimal normal basis of F_4 over F_2. Then α is a root of the irreducible polynomial $x^2 + x + 1 \in F_2$. Thus the order of α in the multiply group $F_{2^2}^*$ is 3, which means that the generator α of N is a primitive element of F_4.

(2) Suppose that N is a type II optimal normal basis of F_{2^n} over F_2. From the construction Theorem of the type II optimal normal basis we know that $2n + 1$ is prime and 2 is a primitive root $(\mathrm{mod}\, 2n + 1)$ or $2n + 1 \equiv 3 \pmod 4$ and the order of 2 $(\mathrm{mod}\, 2n + 1)$ is n. In any cases we have $2^{2n} \equiv 1 \pmod{2n + 1}$, therefore $(2^n - 1)(2^n + 1) \equiv 0 \pmod{2n + 1}$. Since $2n + 1$ is prime, we can get $2n + 1 \mid 2^n - 1$ or $2n + 1 \mid 2^n + 1$.

Case 1 If $2n + 1 \mid 2^n - 1$, then from the assumption $2n + 1$ and $2^n - 1$ are primes we know that $2^n - 1 = 2n + 1$. This equality is true if and only if $n = 3$. In this case, the order of 2 $(\mathrm{mod}\, 2n + 1 = 7)$ is 3, thus we obtain a type II optimal normal basis $N = \{\alpha, \alpha^2, \alpha^4\}$ of F_8 over F_2. Noticing that the set $F_8^* - \{1\}$ contains only 6 nonzero elements and each of them is the primitive element of F_8^*. Therefore the generator α of N is also a primitive element of F_8, which means that N is a primitive type II optimal normal basis of $F_{q^n}^*$ over F_q.

Case 2 If $2n+1 \mid 2^n+1$, i.e., $2^n \equiv -1 \pmod{2n+1}$. Since $2n+1$ is prime, thus 2 is a primitive root modulo $2n + 1$. Now since $2^n - 1$ is prime we know that all $2^n - 2$ nonzero elements in the set $F_{2^n}^* - \{1\}$ are primitive elements of $F_{2^n}^*$. Therefore, the generator α of the type II optimal normal basis N of $F_{2^n}^*$ over F_2 is also a primitive element of F_{2^n}, which means that N is a

primitive type II optimal normal basis of $F_{2^n}^*$ over F_2.

Thus we complete the proof of Theorem 1.6. □

The Proof for Corollary 1.7 Suppose that there exists a primitive element $\alpha \in F_{q^n}$ such that α generates an optimal normal basis N of F_{q^n} over F_q.

Case 1 If N is equivalent to a type I optimal normal basis N of F_{q^n} over F_q, then there exists a primitive type I optimal normal basis of F_{q^n} over F_q. From (1) of Theorem 1.6 we know that $n = q = 2$. Thus there exists exactly one primitive optimal normal bases of F_{q^n} over F_q.

Case 2 If N is equivalent to a type II optimal normal basis $B = \{\beta_i = \beta^{q^i} \mid i = 0, 1, \ldots, n-1\}$ of F_{q^n} over F_q, which means that there exists a primitive type II optimal normal basis of F_{q^n} over F_q. From the construction Theorem of a type II optimal normal basis we know that $q = 2$. Thus $B = N$ and so $\beta = \alpha^{q^k}$ for some $k, 0 \le k \le n-1$, i.e., β is a conjugate element of α. Therefore there exists exactly one primitive optimal normal basis.

Thus we complete the proof of Corollary 1.7. □

The Proof for Theorem 1.8 Suppose that N is the optimal normal basis generated by α.

If N is the type I optimal normal basis, from the construction Theorem of type I optimal normal bases we know that $\alpha^{-1} = \alpha^n$ also generates N.

Now we suppose that N is a type II optimal normal basis (and so $q = 2$) and α^{-1} also generates an optimal normal basis B of F_{q^n} over F_q.

Case 1 If B is equivalent to a type II optimal normal, then $B = N$. From the construction Theorem of type II optimal normal bases we know that $\alpha^{-1} = \alpha^s + \alpha^{-s}$ for some $s, 1 \le s \le n$. Note that $1 = \alpha\alpha^{-1}$ and $\alpha = r + r^{-1}$, where r is a primitive $(2n+1)$-th root of unity. Therefore

$$r^{2n+1} = 1 \Longrightarrow r^n = r^{-(n+1)} \Longrightarrow r^{t+n} = r^{-(n+1)} r^t = r^{-(n+1-t)}, \quad 0 \le t \le n,$$

and

$$1 = (r + r^{-1})(r^s + r^{-s}) = (r^{s+1} + r^{-(s+1)}) + (r^{s-1} + r^{-(s-1)}).$$

If $s = 1$, then $\alpha^2 = 1$, this is a contradiction since $n \le 2$. If $s \ge 3$, from $1 \le s \le n$ we know that $2 \le (s+1) + (s-1) \le 2n < 2n+1$, which means that $r^{s+1} + r^{-(s+1)} \ne r^{s-1} + r^{-(s-1)}$. But N is the type II optimal normal basis generated by α, i.e., $N = \{r^i + r^{-i} \mid i = 1, \ldots, n\}$ is basis and $q = 2$. Now we have $r^{s+1} + r^{-(s+1)}, r^{s-1} + r^{-(s-1)} \in N$, this is contradiction. Therefore, we must have $s = 2$. From $s = 2$ and

$$\begin{aligned} r + r^{-1} &= (r + r^{-1})((r^{s+1} + r^{-(s+1)}) + (r^{s-1} + r^{-(s-1)})) \\ &= (r^{s+2} + r^{-(s+2)}) + (r^{s-2} + r^{-(s-2)}). \end{aligned}$$

we can get $\alpha = \alpha^4$, i.e., $\alpha^3 = 1$, thus $\alpha^{-1} = \alpha^2$, and so $n = 2 = q$.

Case 2 If B is equivalent to a type I optimal normal, from the construction Theorem of type I optimal normal bases we know that α generates B too, which means that $N = B$ since $q = 2$. Thus $n+1$ is prime and $\alpha = r + r^{-1}$ has order $n+1$ in the multiply group $F_{2^n}^*$, where r is a

primitive $(2n+1)$-th root of unity. Note that $q=2$, we know that $\alpha^{2^k}=r^{2^k}+r^{-2^k}$ for any integer k.

Now we conclude that $n=2$. Otherwise, from $n>2$ and $n+1$ is prime we know that n is even. Thus we can set $n=2^k+s$, where $k\geq 1$, $0\leq s\leq 2^k-1$ and $s\equiv 0 \pmod 2$. Since α generates the type I optimal normal basis of F_{2^n} over F_2, thus $\alpha^{n+1}=1$.

If $s=0$, then

$$\begin{aligned}1=\alpha^{n+1}&=(r+r^{-1})(r+r^{-1})^n\\&=(r+r^{-1})(r+r^{-1})^{2^k}=(r+r^{-1})(r^{2^k}+r^{-2^k})\\&=(r^{2^k+1}+r^{-(2^k+1)})+(r^{2^k-1}+r^{-(2^k-1)})\\&=(r^{n+1}+r^{-(n+1)})+(r^{n-1}+r^{-(n-1)}).\end{aligned}$$

But r is a primitive $(2n+1)$-th root of unity, i.e., $r^{2n+1}=1$. Thus we have $r^{n+1}=r^{-n}$, therefore

$$1=\alpha^{n+1}=(r^n+r^{-n})+(r^{n-1}+r^{-(n-1)}),$$

which is contradiction to the assumption that $N=\{r^i+r^{-i}\,|\,i=1,\ldots,n\}$ is a basis of F_{2^n} over F_2 with extension degree $n>2$.

Therefore s is even and $s\neq 0$. Thus we can get

$$(r+r^{-1})^s=\sum_{i=1}^{t}(r^{l_i}+r^{-l_i}),\ t\leq\frac{s}{2},\ 1\leq l_i\leq n.$$

Note that $\alpha^{n+1}=1$ and $n=2^k+s$, thus

$$\begin{aligned}\alpha^n=(r+r^{-1})^n&=(r+r^{-1})^{2^k}(r+r^{-1})^s=(r^{2^k}+r^{-2^k})(r+r^{-1})^s\\&=(r^{2^k}+r^{-2^k})\sum_{i=1}^{t}(r^{l_i}+r^{-l_i})=\sum_{i=1}^{t}\left((r^{2^k+l_i}+r^{-(2^k+l_i)})+(r^{2^k-l_i}+r^{-(2^k-l_i)})\right),\end{aligned}$$

i.e.,

$$\alpha^n+\sum_{i=1}^{t}\left((r^{2^k+l_i}+r^{-(2^k+l_i)})+(r^{2^k-l_i}+r^{-(2^k-l_i)})\right)=0.$$

Note that there are at most $2t+1$ terms on the left side of the above equation. But $t\leq\frac{s}{2}<\frac{n}{2}$ from $n=2^k+s$ is even and $k\geq 1$, which means that $2t+1<n$. Thus we get a contradiction to the assumption N is a basis of F_{2^n} over F_2 with the extension degree $n>2$.

Therefore, we must have $n=2$ and so $n=2=q$.

Thus we complete the proof of Theorem 1.8. □

The Proof for Corollary 1.9 Suppose that α is a primitive optimal normal element of F_{q^n} over F_q, from Theorem 1.8 we know that α^{-1} is also a primitive optimal normal element of F_{q^n} over F_q iff $n=q=2$ or both α and α^{-1} generate type I optimal normal bases of F_{q^n} over F_q. Therefore it is enough to show that α^{-1} is also a primitive type I optimal normal element iff $n=q=2$. From (1) of Theorem 1.6 we know that this is true.

Thus we complete the proof of Corollary 1.9. □

Acknowledgement The author would like to thank professor Sun Qi for some helpful suggestions.

References

[1] BLESSENOHL D, JOHNSON K. *Eine Verschärfung des satzes von der normalbasis* [J]. J. Algebra, 1986, **103**(1): 141–159. (in German)
[2] BLAKE I F, GAO Shuhong, MULLIN R C. et al. *Applications of Finite Fields* [M]. Kluwer Academic Publishers, 1993.
[3] CAO Wei, SUN Qi. *A new characterization of dual bases in finite fields and its applications* [J]. Discrete Appl. Math., 2007, **155**(17): 2236–2241.
[4] DAVENPORT H. *Bases for Finite Fields* [J]. J. London Math. Soc., 1986, **43**: 21–39.
[5] FEISEL S, GATHEN J V Z, SHOKRO LLAHI M A. *Normal Bases via General Gauss Periods* [J]. Mathematics of Computation, 1999, **68**(225): 271–290.
[6] GAO Shuhong, LENSTRA H W JR. *Optimal normal bases* [J]. Des. Codes Cryptogr., 1992, **2**(4): 315–323.
[7] GAO Shuhong. *Abelian groups, Gauss periods, and normal bases* [J]. Finite Fields Appl., 2001, **7**(1): 149–164.
[8] JACBSON N. *Basic Algebra I* [M]. W.H. Freeman and Company, San Francisco, 1984.
[9] LENSTRA H W JR, SCHOOF R J. *Primitive normal bases for finite fields* [J]. Math. Comp., 1987, **48**(177): 217–231.
[10] LIDL R, NIEDERREITER H. *Finite Fields* [M]. Cambrige University Press, 1987.
[11] LIAO Qunying, SUN Qi. *Multiplication tables of optimal normal bases over finite fields* [J]. Acta Math. Sinica (Chin. Ser.), 2005, **48**(5): 947–954. (in Chinese)
[12] LIAO Qunying, SUN Qi. *Normal bases and their dual-bases over finite fields* [J]. Acta Math. Sin. (Engl. Ser.), 2006, **22**(3): 845–848.
[13] MULLIN R C, ONYSZCHUK I M, VANSTONE S A. et al. *Optimal normal bases in* GF(p^n) [J]. Discrete Appl. Math., 1988/89, **22**(2): 149–161.
[14] TIAN Tian, QI Wenfeng. *Primitive normal element and its inverse in finite fields* [J]. Acta Math. Sinica (Chin. Ser.), 2006, **49**(3): 657–668. (in Chinese)