doi:10.16055/j.issn.1672-058X.2015.0007.005

二元域上一类正规基与 q-循环*

李　波
(重庆邮电大学 移通学院,重庆 401520)

摘　要:设 q 为素数的方幂,$n(\geq 2)$为正整数,给出了模 q^n-1 的 q-循环的一些性质,并利用这些性质讨论了 F_{2^n}到 F_2 上一类特殊正规基的存在性,最后证明了 $n=4$ 时,这类正规基可为Ⅰ型最优正规基;$n\neq 4$ 时,它一定不是最优正规基.

关键词:有限域;正规基;q-循环
中图分类号:O156.1　　**文献标识码**:A　　**文章编号**:1672-058X(2015)07-0026-04

1　基础知识

设 q 为素数 p 的方幂,$n(\geq 2)$为正整数,F_{q^n}是 q 元域 F_q 的 $n(\geq 2)$次扩张.若 $N=\{\alpha_i=\alpha^{q^i}\mid i=0,1,\cdots,n-1\}$是 F_{q^n}到 F_q 的一个正规基,则称 α 是 F_{q^n}到 F_q 的一个正规元.设

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

则$(t_{i,j})_{n\times n}$中非零元的个数称为 N 的复杂度,记为 C_N.R Mullin 等[1]证明了 $C_N\geqslant 2n-1$,当 $C_N=2n-1$ 时,称 N 为最优正规基.以最优正规基为代表的低复杂度正规基已经有许多结果[2-11].R Mullin 等给出了Ⅰ型和Ⅱ型最优正规基的构造定理之后;高绪洪[12]证明了只存在这两类最优正规基;1990 年,A Wassermann[13]把最优正规基推广为 k-型高斯正规基.

定义 1[13]　设 q 为素数 p 的方幂,k 和 n 为正整数,且满足 $kn+1$ 为素数,$(kn+1,p)=1$.假定 $\gamma\in F_{q^{kn}}$是 $kn+1$次本原单位根,s 是 q 模 $kn+1$ 的次数.若$(kn/s,n)=1$,l 是 Z_{kn+1}的一个 k 本原的单位根,则

$$\alpha=\sum_{j=0}^{k-1}\gamma^{l^j}$$

生成 F_{q^n}到 F_q 的一个正规基,称 N 为 F_{q^n}到 F_q 的一个 k-型高斯正规基.

注 1　设 N 为 F_{q^n}到 F_q 的一个 k-型高斯正规基,由Ⅰ型和Ⅱ型最优正规基的定义可知,当 $k=1$ 时,N 为Ⅰ型最优正规基;当 $k=q=2$ 时,N 为Ⅱ型最优正规基.

熟知,最优正规基(特别是低复杂度正规基)在编码理论、密码学、数字通信等领域有着广泛的应用.通过计算发现,当扩张次数 $n=4,8,16$ 时,存在 F_{2^n}到 F_2 的正规基 N,使得序列 $t_i=\mathrm{Tr}(\alpha\alpha_i)(i=0,1,\cdots,n-1)$中 $t_0=t_1=t_{n-1}=1,t_i=0(i\neq 0,1,n-1)$,其中 Tr 表示 F_{q^n}到 F_q 的迹映射.这类正规基在编码中有着很好的应用.自然的问题是:扩张次数 n 满足什么条件,才存在 F_{2^n}到 F_2 的正规基满足 $t_0=t_1=t_{n-1}=1,t_i=0(i\neq 0,1,n-1)$.

由有限域上正规基的性质可知,$t_i=t_{n-i}$.Perlis[14]给出了如下结论:设 $q=p^s$,p 为素数,$n=p^m$,$m\geqslant 1$.若 $\alpha\in F_{q^n}$,则 α 为 F_{q^n}到 F_q 的一个正规元$\Leftrightarrow\mathrm{Tr}(\alpha)\neq 0$.从而当 $n=2^t(t\geqslant 1)$时,$t_0=1$.故此时只需考虑 $i\neq 0$ 的情形.对

收稿日期:2014-09-08;**修回日期**:2014-10-20.
* **基金项目**:国家自然科学基金项目资助(10990011).
作者简介:李波(1984-),男,四川苍溪人,讲师,硕士,从事数论和有限域研究.

于 k-型高斯正规基,文献[7]得到了如下结论:若 α 生成 F_{q^n} 到 F_q 的一个 k-型高斯正规基,则 $\mathrm{Tr}(\alpha)=-1$.

下面给出 q-循环的定义.

定义 2[15]　设 $a_0,a_1,\cdots,a_{l-1}$ 为 $\{0,1,\cdots,m-1\}$ 中 l 个不同的元素,q 为素数的方幂,若满足

$$a_iq\equiv a_{i+1}(\mathrm{mod}\ m),a_{l-1}q\equiv a_0(\mathrm{mod}\ m),i=0,1,\cdots,l-2$$

则称序列 $(a_0,a_1,\cdots,a_{l-1})$ 为一个模 m 的 q-循环,l 为该 q-循环的长度.

以下用 l_i 表示 i 模 q^n-1 的 q-循环的长度.由定义 2,$iq^{l_i}\equiv i(\mathrm{mod}\ q^n-1)$.

2　主要结果及证明

这里先给出一个引理.

引理 1[12]　设 k,n 是正整数,$kn+1$ 为素数,q 模 $kn+1$ 的阶是 e.如果 $(kn/e,n)=1$,T 是 Z_{kn+1} 的一个 k-次本原单位根,则 Z_{kn+1} 中任意非零元 r 都能唯一表示成如下形式:

$$r\equiv T^iq^j(\mathrm{mod}(kn+1)),0\leqslant i\leqslant k-1,0\leqslant j\leqslant n-1$$

定理 1　设 q 为素数的方幂,$n(\geqslant 2)$ 是正整数,则 $l_i\mid n$,其中 $0\leqslant i\leqslant q^n-1$.

证明　由文献[15]知若 ξ 是 F_{q^n} 的一个本原元,且存在 k 个不同的 q-循环,令 $i_1,i_2,\cdots,i_k$ 分别来自这 k 个不同的 q-循环,则 x^n-1 在 F_q 上的完全分解式为

$$x^n-1=f_{i_1}(x)f_{i_2}(x)\cdots f_{i_k}(x)$$

其中 $f_{i_m}(x)=\prod\limits_{j=0}^{l_{i_m}}(x-(\xi^{i_m})^{q^j})$,$1\leqslant m\leqslant k$.

设 $F_{q^n}^*$ 是 F_{q^n} 的乘法群,α 为 $F_{q^n}^*$ 的一个生成元.令 $x^{q^n}-x$ 在 F_q 上的完全分解式为

$$x^{q^n}-x=x(x^{q^n-1}-1)=xf_{i'_1}(x)f_{i'_2}(x)\cdots f_{i'_k}(x)$$

其中 $f_{i'_m}(x)=\prod\limits_{j=0}^{l_{i'_m}}(x-(\alpha^{i'_m})^{q^j})$,$1\leqslant i\leqslant m$.则 $f_{i'_m}(x)$ 在 F_q 上不可约,且 $\deg(f_{i'_m}(x))=l_{i'_m}$.又 $\alpha^{i'_m}\in F_{q^n}$,且 $f_{i'_m}(\alpha^{i'_m})=0$,则

$$F_{q^{l_{i'_m}}}\cong F_q[x]/f_{i'_m}(x)\cong F_q(\alpha^{i'_m})\subseteq F_{q^n}$$

即 $F_{q^{l_{i'_m}}}$ 是 F_{q^n} 的子域,于是 $l_{i'_m}\mid n$.从而对一般的 $0\leqslant i\leqslant q^n-1$,有 $l_i\mid n$.

下面给出模 q^n-1 的 q-循环的一个循环.

命题 1　设 q 为素数的方幂,序列 $(i,iq,\cdots,iq^{l_i-1})$ 为 i 模 q^n-1 的一个 q-循环,则

1) 序列 $(<q^n-1-i>,<q^n-1-i>q,\cdots,<q^n-1-i>q^{l_i-1})$ 也是模 q^n-1 的一个 q-循环;

2) $l_i=l_{q^n-1-i}$,其中 $<\cdot>$ 表示模 q^n-1 的最小非负剩余.

证明　因 $<q^n-1-i>q^j\equiv -iq^j(\mathrm{mod}(q^n-1))$,则

$$<q^n-1-i>q^{l_i}\equiv -iq^{l_i}\equiv -i\equiv <q^n-1-i>(\mathrm{mod}(q^n-1))$$

又设 $0\leqslant s,t\leqslant n-1$,当 $s\neq t$ 时,$-iq^s\neq -iq^t(\mathrm{mod}(q^n-1))$,即 $<q^n-1-i>q^s\neq <q^n-1-i>q^t(\mathrm{mod}(q^n-1))$.由定义 2 可知,命题 1 的 1)成立.进而命题 1 的 2)成立.

推论 1　设 $n=2^t$,t 为正整数,若 α 为 F_{q^n} 到 F_q 的一个正规元且 $t_i=1$,则 $l_{2i+1}=n$.

证明　(反证法)假设 $l_{2i+1}\neq n$,则由定理 1,可设 $n=2^kl_{2i+1}(k\geqslant 1)$.于是

$$t_i=\mathrm{Tr}(\alpha^{2i+1})=\sum_{j=0}^{n-1}(\alpha^{2i+1})^{2^j}=\sum_{j=0}^{n-1}\alpha^{(2i+1)2^j}=2^k\sum_{j=0}^{l_{2i+1}-1}\alpha^{(2i+1)2^j}$$

矛盾.故假设不成立.

形如 $F_e=2^{2^e}+1(e\geqslant 0)$ 的数被称为费马数.对于任意给定的两个费马数 F_{e_1},F_{e_2};若 $e_1\neq e_2$,则 $(F_{e_1},F_{e_2})=1$.下面运用这个性质给出一种特殊情形下 2^i+1 模 2^n-1 的 2-循环的长度的计算公式.

推论 2　设 $i=2^m$,$n=2^t$,则 $l_{2i+1}=\begin{cases}\dfrac{n}{2},m=t-1\\ n,m\neq t-1\end{cases}$.

证明 易知,$2^n-1=2^{2^t}-1=F_{t-1}F_{t-2}\cdots F_0$,$2^i+1=F_m$.令 $2^{l_{2^{i+1}}}-1=F_{t-1}F_{t-2}\cdots F_0$.由定理1,$l_{2^{i+1}}\mid n$,则 $t_1-1\leqslant t-1$,即 $t_1\leqslant t$.又 $2^i+1\equiv(2^i+1)2^{l_{2^{i+1}}}(\mathrm{mod}(2^n-1))$,即 $2^n-1\mid(2^i+1)(2^{l_{2^{i+1}}}-1)$.于是

$$F_{t-1}F_{t-2}\cdots F_0\mid F_mF_{t_1-1}F_{t_2-1}\cdots F_0$$

由于不同的费马数必定互素,则 $t-2\leqslant t_1-1$,即 $t-1\leqslant t_1$.从而,$t-1\leqslant t_1\leqslant t$.当 $t_1=t$ 时,$m\neq t-1$,此时 $l_{2^{i+1}}=n$;当 $t_1=t-1$ 时,$m=t-1$,此时 $l_{2^{i+1}}=\dfrac{n}{2}$.

例1 条件同推论2,

当 $i=1$ 时,$m=0$,有若 $t\geqslant 2$,则 $m<t-1$,此时 $l_3=n$;若 $t=1$,则 $m=t-1$,此时 $l_3=\dfrac{n}{2}$.

当 $i=2$ 时,$m=1$,有若 $t\neq 2$,则 $m\neq t-1$,此时 $l_5=n$;若 $t=2$,则 $m=t-1$,此时 $l_5=\dfrac{n}{2}$.

关于是否存在 F_{2^n} 到 F_2 的正规基满足 $t_0=t_1=t_{n-1}=1$,$t_i=0(i\neq 0,1,n-1)$,有

定理2 设 $N=\{\alpha_i\mid i=0,1,\cdots,n-1\}$ 是 F_{2^n} 到 F_2 上的一个 k-型高斯正规基,则

1) 若 k 为偶数,或 k 为奇数且 $n\neq 4$,则 N 不满足 $t_0=t_1=t_{n-1}=1$,$t_i=0(i\neq 0,1,n-1)$;

2) 若 k 为偶数,则 $(kn+1,\sum\limits_{i=0}^{k-1}\left(\dfrac{kn}{2}\right)^i)=1$.

证明 1) 由定义1,设 $\alpha=\sum\limits_{j=0}^{k-1}\gamma^{l^j}$ 生成 F_{q^n} 到 F_q 上的 k-型高斯正规基,文献[16]中定理1的证明过程中对 $\alpha\alpha_i$ 的结构有如下描述:

$$\alpha\alpha_i=\begin{cases}k+\sum\limits_{s=0,s\neq i_0}^{k-1}\alpha_{j_1(s)}, & i=i_0\\ \sum\limits_{s=0}^{k-1}\alpha_{j_2(s)}, & i\neq i_0\end{cases}$$

其中 $1+l^{v_0}q^{i_0}\equiv 0(\mathrm{mod}(kn+1))$;$1+l^sq^{i_0}\equiv l^{\varpi_1(s)}q^{i_0}(\mathrm{mod}(kn+1))(s\neq v_0)$;$1+l^{v_0}q^{i_0}\equiv 0(\mathrm{mod}(kn+1))(i\neq i_0)$;$0\leqslant v_0,s,\varpi_1(s),\varpi_2(s)\leqslant k-1$;$0\leqslant j_1(s),j_2(s)\leqslant n-1$;且当 k 为偶数时,$i_0=0$;当 k 为奇数时,$i_0=\dfrac{n}{2}$.

因 $\mathrm{Tr}(\alpha)=-1$,故 $t_{i_0}=\mathrm{Tr}\left(k+\sum\limits_{s=0,s\neq i_0}^{k-1}\alpha_{j_1(s)}\right)=kn-(k-1)=k(n-1)+1$;$t_i=\mathrm{Tr}\left(\sum\limits_{s=0}^{k-1}\alpha_{j_2(s)}\right)=-k(i\neq i_0)$.又 $(kn+1,q)=1$,则 $k(n-1)+1\neq k$.于是,$t_i=k(n-1)+1\Leftrightarrow i=i_0$.现取 $q=2$,则

(i) 当 k 为偶数时,$t_0=1$,$t_i=0(i\neq 0)$;

(ii) 当 k 为奇数且 $n\neq 4$ 时,$t_{n/2}=0$,$t_j=1\left(j\neq\dfrac{n}{2}\right)$.

均不满足 $t_0=t_1=t_{n-1}=1$,$t_i=0(i\neq 0,1,n-1)$.故不存在 F_{2^n} 到 F_2 上的一个 k-型高斯正规基满足条件.

2) 当 k 为偶数时,$(kn+1,kn-2)=(kn+1,3)=1$,则 $2\left(kn+1,\dfrac{kn}{2}-1\right)=(2(kn+1),kn-2)=2$,即 $\left(kn+1,\dfrac{kn}{2}-1\right)=1$.假设 $kn+1\mid\sum\limits_{i=0}^{k-1}\left(\dfrac{kn}{2}\right)^i$,而 l 为 Z_{kn+1} 中一个 k 次本原单位根(由定义1),于是 $kn+1\mid\sum\limits_{i=0}^{k-1}\left(\dfrac{kn}{2}\right)^i\Leftrightarrow kn+1\mid\left(\dfrac{kn}{2}-1\right)\sum\limits_{i=0}^{k-1}\left(\dfrac{kn}{2}\right)^i=\left(\dfrac{kn}{2}\right)^k-1\Leftrightarrow\dfrac{kn}{2}$ 为 Z_{kn+1} 中一个 k 次单位根 $\Leftrightarrow$ 存在一正整数 ϖ,使得 $\dfrac{kn}{2}\equiv l^{\varpi}(\mathrm{mod}(kn+1))$.即 $kn\equiv l^{\varpi}\cdot 2(\mathrm{mod}(kn+1))$(由引理1)$\Leftrightarrow 1+l^{\varpi}\cdot 2\equiv 0(\mathrm{mod}(kn+1))$,即 $i_0=1$.这与 k 为偶数时,$i_0=0$ 矛盾.又 $kn+1$ 为素数,故 $\left(kn+1,\sum\limits_{i=0}^{k-1}\left(\dfrac{kn}{2}\right)^i\right)=1$.

由定义1知,当 $n=4$ 时,不存在 F_{2^n} 到 F_2 上的Ⅱ型最优正规基.

注2 通过定义可以验证,当 $n=4$ 时,F_{2^n} 到 F_2 上的Ⅰ型最优正规基满足 $t_0=t_1=t_{n-1}=1$,$t_i=0(i\neq 0,1,n-1)$.

由定理2和注1,注2,有

推论3 设 $N=\{\alpha_i\mid i=0,1,\cdots,n-1\}$ 是 F_{2^n} 到 F_2 上的一个正规基,且满足 $t_0=t_1=t_{n-1}=1$,$t_i=0(i\neq 0,1,$

$n-1$),则

1) 当 $n=4$ 时,N 可为 Ⅰ 型最优正规基;

2) 当 $n\neq4$ 时,N 一定不是最优正规基.

参考文献:

[1] MNLLIN R,ONYSZCHUK I,VANSTONE S,et al.Optimal Normal Bases Over F_{p^n}[J].Discrete Applied Math,1999(22):149-161

[2] LIAO Q Y,SUN Q.Normal Bases and Their Dual-bases Over Finite Fields[J].Acta Mathematics Sinica,2006,22 (3): 845-848

[3] LIAO Q Y.On the Distribution of Normal Bases Over Finite Fields[J].Advances in Mathmatics,2010,39(2): 207-211

[4] 廖群英,孙琦.有限域上最优正规基的乘法表[J].数学学报,2005,48(5): 947-954

[5] WAN Z X,ZHOU K.On the Complexity of the Dual Bases of a Type I Optimal Normal Bases[J].Finite Fields and Their Applications,2007,13(4):411-417

[6] GAO S H.Abelian Groups,Gauss Periods,and Normal Bases[J].Finite Fields and Their Applications,2001,7(1):149-161

[7] 廖群英,苏丹丹,付萍.有限域上的 2 型高斯正规基及其对偶基[J].四川大学学报:自然科学版,2010,47(6):1221-1224

[8] ASH D,BLAKE I F,VANSTONE S.Low Complexity Normal Bases[J].Discrete Applied Math,1999(25):191-210

[9] NOGAMI Y,NASU H,MORIKAWA Y,et al.A Method of Constructing a Self-dual Normal Bases in Odd Characteristic Extention Fields[J].Finite Fields and Their Applications,2008,14(2):867-876

[10] 李俊,黄琴,李波,等.有限域上的 k-型高斯正规基及其对偶基[J].四川师范大学学报:自然科学版,2011,34(3),289-295

[11] YOUNG B,PANARIO D.Low Complexity Normal Bases[J].Finite Fields and Their Applications,2004,10(1):53-64

[12] GAO S H.Normal Bases Over Finite Fields[D].Waterloo: Waterloo University,1993

[13] WASSERMANN A.Konstruktion Von Normalbasen[J].Bayreuther Mathmatische Schriften,1990(31): 155-164

[14] PERLIS S.Normal Bases of Cyclic Fields of Prime Power Degree[J].Duke Math,1942(9):507-519

[15] WAN Z X.Lectures on Finite Fields and Galois Rings[M].Singapore:World Science Publishers,2003

[16] 李波,廖群英.有限域上 k-型高斯正规基的对偶基及其乘法表[J].四川师范大学学报:自然科学版,2013,36(6):824-829

A Class of Normal Bases on Binary Field and q-Cycle

LI Bo

(College of Mobile Telecommunications,Chongqing University of Posts and Telecommunications,Chongqing 401520,China)

Abstract: Let q be the power of a prime p,$n(\geq2)$ be an integer.Some properties of q-cycle modular q^n-1are given.With these properties this paper discusses the existence of a kind of special normal bases from F_{2^n} to F_2.Finally,it is proved that this kind of special normal bases can be optimal normal bases of type Ⅰ,if $n=4$;Otherwise,it can't be optimal normal bases.

Key words: finite fields,normal bases,q-cycle