环 F_2+uF_2 上长为 2^s 线性循环码的极小距离分布

李　雨[1],陈鲁生[2]
LI Yu[1],CHEN Lu-sheng[2]

1.华北电力大学(保定) 数理学院,河北 保定 071003
2.南开大学 数学科学学院,天津 300071
1.School of Mathematics and Physics,North China Electric Power University,Baoding,Hebei 071003,China
2.College of Mathematical Science,Nankai University,Tianjin 300071,China
E-mail:xeon_liyu@163.com

LI Yu,CHEN Lu-sheng.On minimum distance distribution of cyclic codes over ring F_2+uF_2 with length 2^s.Computer Engineering and Applications,2008,44(12):69-70.

Abstract: Based on the structure of the cyclic codes over the ring F_2+uF_2,an accurate formula about the minimum distance distribution of the cyclic codes over the ring F_2+uF_2 with length 2^s is given.
Key words: linear cyclic code;Hamming distance;Lee distance

摘　要: 研究了环 F_2+uF_2 上线性循环码的极小距离分布。首先给出了环 F_2+uF_2 上线性循环码的结构,利用该结构给出了长度为 2^s 线性循环码的极小距离分布的精确表示。
关键词: 线性循环码;汉明距离;Lee 距离
文章编号: 1002-8331(2008)12-0069-02　**文献标识码:** A　**中图分类号:** TN919.1

1　引言

近年来环上的编码理论得到了编码研究者的普遍重视,原因是 Hammons[1]等人的文章揭示了一种利用 Gray 映射通过环 Z_4 上的线性循环码来构造二元域 F_2 上的非线性码的全新方法。通过这种方法,Hammons 等人成功地构造出了 Kerdock、Delsarte-Goethals 等许多种广为人知的非线性码,环上编码理论的研究因此逐渐升温。继环 Z_4 之后,环 F_2+uF_2 成为了又一种备受重视的有限环,原因是它同时具有环 Z_4 和域 F_4 的部分性质,通过 Gray 映射,同样可以得到性能良好的非线性二元码。极小距离作为衡量码性能的一个重要标准,对其进行的研究具有重要的理论和实践意义。本文主要研究了环 F_2+uF_2 上长度为 2^s 的线性循环码其极小距离分布的情况。

2　基本概念

环 F_2+uF_2 是指剩余类环 $R=F_2[u]/\langle u^2\rangle$,其元素集合记为 $\{0,1,u,1+u\}$,R 是局部环,其唯一的极大理想是 $\langle u\rangle$,R 上长为 n 的线性码 C 定义为 R^n 加法子群。

任意 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\in C$ 定义映射 P:

$P:(c_0,c_1,\cdots,c_{n-1})\to c_0+c_1x+\cdots+c_{n-1}x^{n-1}+(x^n-1)$

$P(\boldsymbol{c})$ 称为 $\boldsymbol{c}$ 对应的码字多项式,记为 $c(x)$。C 中的码字与剩余类环 $R[x]/(x^n-1)$ 中的元素存在一一对应关系。

引理 1[2]　C 是 R 上一个线性循环码当且仅当 $P(C)$ 是 $R[x]/(x^n-1)$ 的一个理想。

证明　参见 MacWilliams[2]中有关循环码的部分章节,其证明过程完全类似,不再赘述。

定义 1　R 上的码字 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$ 的 Lee 重量定义为:$w_L(\boldsymbol{x})=n_1(\boldsymbol{x})+2n_2(\boldsymbol{x})$,其中 $n_1(\boldsymbol{x})$ 是 $\boldsymbol{x}$ 中 1 和 $1+u$ 的个数,而 $n_2(\boldsymbol{x})$ 是 $\boldsymbol{x}$ 中 u 的个数。

定义 2　从环 R 到 Z_2^2 的 Gray 映射 ϕ 定义如下:

ϕ:0→00
　1→01
　u→11
　$1+u$→10

引理 2　从环 R^n 到 Z_2^{2n} 的 Gray 映射 ϕ 是同构映射,并且是保持距离不变的(分别指的是 Lee 距离和汉明距离)。

证明　Hammons[1]中定理 1。

R 上任意一个非零的码字 C 在置换等价的意义下都有相同的生成矩阵:

$$\boldsymbol{G}=\begin{bmatrix}\boldsymbol{I}_{k_1} & \boldsymbol{A} & \boldsymbol{B}\\ 0 & u\boldsymbol{I}_{k_2} & u\boldsymbol{D}\end{bmatrix}$$

其中 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 是 R 上的矩阵而 $\boldsymbol{D}$ 是 F_2 上的矩阵。码 C 包含所有形如 $[\boldsymbol{v}_0\ \ \boldsymbol{v}_1]\boldsymbol{G}$ 的码字,其中 $\boldsymbol{v}_0$ 是 R 上长为 k_1 的向量而 $\boldsymbol{v}_1$ 是 F_2 上长为 k_2 的向量。任何一个 R 上的码字 C 都可以分解为两个二元码[3]:剩余码(residue code)

$$C_1=\{\boldsymbol{x}\in F_2^n\mid\exists\,\boldsymbol{y}\in F_2^n|\boldsymbol{x}+u\boldsymbol{y}\in C\}$$

和扭转码(torsion code)

$$C_2=\{\boldsymbol{x}\in F_2^n|u\boldsymbol{x}\in C\}$$

作者简介: 李雨(1981-),男,研究方向为信道编码;陈鲁生,男,教授,研究方向为信息论、编码理论和密码学。
收稿日期: 2007-08-15　**修回日期:** 2007-11-16

定义 3 映射 μ 是环 R 上多项式的二元像

$$\sum_{i=0}^{r} a_i x^i \xrightarrow{\mu} \sum_{i=0}^{r} \hat{a} x^i$$

其中 $\hat{a}_i \equiv a_i \bmod u$

引理 3[4] 假设 C 是 R 上一个 n 长的循环码,存在 $F_2[x]$上唯一的单调多项式 f,g,h 使得 $C=\{fh,ufg\}$,其中 $fgh=x^n-1$,并且满足 $C=4^{\deg(g)}2^{\deg(h)}$。

注 $C=\{fh,ufg\}$表示这样一个循环码,它所对应的剩余码和扭转码,其生成多项式分别为 $C_1=\mu(fh)$和 $C_2=\mu(fg)$。

3　环 R 上长为 2^s 的线性循环码的距离分布

引理 4 环 R 上长为 $n=2^s$ 的循环码 C 对应的 $R[x]/(x^n-1)$中的理想拥有如下的形式:

$\langle (x+1)^i+u(x+1)^j \rangle, 0\leqslant i,j\leqslant n-1$

证明 根据引理 3,环 R 上的循环码可以写成 $C=\{fh,ufg\}$的形式,其中$\langle\mu(fh)\rangle$和$\langle\mu(fg)\rangle$都是 $F_2[x]/(x^n-1)$的理想,已知环 $F_2[x]/(x^n-1)$上的理想都是$<(x+1)^i>, 0\leqslant i\leqslant n-1$ 的形式,那么 C 所对应的 $R[x]/(x^n-1)$的理想必可写成$\langle (x+1)^i+u(x+1)^j\rangle, 0\leqslant i, j\leqslant n-1$ 的形式。

引理 5[5] 任意非零的单调多项式$f(x),g(x)\in F_2[x]/(x^n-1)$,必存在着唯一的单调多项式 $q(x),r(x)\in F_2[x]/(x^n-1)$,使得 $f(x)=q(x)g(x)+r(x)$,且 $\deg r(x)<\deg g(x)$。

定理 1 F_2 上的长为 2^s 的线性循环码 C 对应的 $F_2[x]/(x^{2^s}-1)$的理想为$<(x+1)^i>, 0\leqslant i\leqslant n-1$,那么码 C 的极小汉明重量分布是

$$w_H(C)=\begin{cases}1 & i=0\\ 2 & 1\leqslant i\leqslant 2^{s-1}\\ 2^k & \sum_{l=1}^{k-1}2^{s-l}+1<i\leqslant\sum_{l=1}^{k-1}2^{s-l}\quad 2\leqslant k\leqslant s\end{cases}\tag{1}$$

证明 $F_2[x]/(x^{2^s}-1)$的所有理想构成升链$(x+1)^{2^s}\subset(x+1)^{2^s-1}\subset\cdots\subset(x+1)^0$,并且满足 $d_H(<(x+1)^{2^s}>)\geqslant d_H(<(x+1)^{2^s-1}>)\geqslant\cdots\geqslant d_H(<(x+1)^0>)$。

当 $i=0$ 时,显然;

当 $i>2^{s-1}$ 时,若 $i=2^s-1$,$(x+1)^{2^s-1}=1+x+x^2+\cdots+x^{2^s-1}$,其中不为 0 的项有 2^s 个。由$(x+1)^{2^s-1}$所生成的循环码 C 中任意一码字 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})$对应着 $F_2[x]/(x^{2^s}-1)$中的多项式 $c(x)=f(x)(x+1)^{2^s-1}$,可以将 $f(x)$写成 $f(x)=g(x)(x+1)+r(x)$,则 $c(x)=r(x)(x+1)^{2^s-1}$,其中 $r(x)=0,1$。于是,C 中仅有一个非零码字 $1+x+x^2+\cdots+x^{2^s-1}$其 Hamming 重量为 2^s。由此猜想式(1)成立。令 $k=k_0$,k_0 是不大于 s 的正整数,由

$$\langle (x+1)^{\sum_{l=1}^{k_0-1}2^{s-l}+t}\rangle, 1\leqslant t<2^{s-k_0}$$

生成的循环码,任一个码字 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})$对应的码字多项式 $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ 可以写成

$$c(x)=\left((x+1)^{\sum_{l=1}^{k_0-1}2^{s-l}+t}\right)f(x)=\left((x+1)^{\sum_{l=1}^{k_0-1}2^{s-l}}\right)(x+1)^t f(x)$$

其中 $f(x)\in F_2[x]/(x^n-1)$。类似的,$f(x)$可以写成 $f(x)=g(x)(x+1)^{2^s-\sum_{l=1}^{k_0-1}2^{s-l}-t}+r(x)$,其中 $r(x)$是一个次数小于 $2^{s-k_0}-t$ 的多项式,则 $c(x)=r(x)(x+1)^{\sum_{l=1}^{k_0-1}2^{s-l}+t}$。一方面,观察可知$(x+1)^{\sum_{l=1}^{k_0-1}2^{s-l}}=\prod_{l=1}^{k_0-1}(x^{2^{s-l}}+1)$的展开式中非零项有 2^{k_0-1},并且任意两个非零项的次数之差不小于 2^{s-k_0};另一方面 $r(x)(x+1)^t$ 中的非零项至少有 2 个,否则假设存在多项式 $r(x)$使得$(x+1)^t r(x)=x^j$, $j<2^{s-k_0}$。因为 x^j 是多项式剩余类环 $F_2[x]/(x^{2^s}-1)$中的可逆元,因此存在 x^j 的逆元 $p(x)$使得 $x^j p(x)=1$,那么 $p(x)(x+1)^t r(x)=1$,因此 $p(x)r(x)$是$(x+1)^t$的逆元,这与$(x+1)^t$是零因子的事实产生了矛盾。因此$(x+1)^t r(x)$中的非零项至少有 2 个并且 $\deg(r(x)(x+1)^t)<2^{s-k_0}$。综上可知,$c(x)$中的非零项个数$\geqslant 2^{k_0-1}\times 2=2^{k_0}$,也即是 $w_H(\boldsymbol{c})\geqslant 2^{k_0}$;

当 $1\leqslant i\leqslant 2^{s-l}$ 时,由$(x+1)^i$为生成多项式的循环码 C,其中任一个码字 $\boldsymbol{c}$ 对应的码字多项式可以写成 $c(x)=(x+1)^i f(x)$,其中 $f\in F_2[x]/x^{2^s}-1$。由上面的分析可知,$c(x)$中的非零项至少有 2 个。事实上,只需令 $f(x)=(x+1)^{2^{s-l}-i}$,则 $c(x)=(x+1)^{2^{s-l}}=x^{2^{s-l}}+1$,即 $w_H(\boldsymbol{c})\geqslant 2$。

综上可知命题得证。

定理 2 环 R 上长为 $n=2^s$ 的线性循环码 $C=\{(x+1)^i, u(x+1)^j\}, 0\leqslant i,j\leqslant n-1$ 的 Lee 距离分布是

$$d_L(C)\begin{cases}=2^{k_1} & k_1\leqslant k_2\\ >2^{k_2+1} & k_1>k_2\end{cases}$$

其中 k_1,k_2 满足 $\sum_{l=1}^{k_1-1}2^{s-l}+1\leqslant i\leqslant\sum_{l=1}^{k_1}2^{s-l}$, $\sum_{l=1}^{k_2-1}2^{s-l}+1\leqslant j\leqslant\sum_{l=1}^{k_2}2^{s-l}$,而当 $i,j\leqslant 2^{s-l}$时,$k_1,k_2=1$。

证明 环 R 上的任何一个循环码 C 都可以分解成 F_2 上的两个循环码:剩余码 C_1 和和扭转码 C_2,并且 $C=C_1+\mu C_2$,因此 $d_L(C)\geqslant\min\{d_H(C_1),2d_H(C_2)\}$,而 $d_H(C_1)$和 $d_H(C_2)$将可由定理 1 给出。因为我们讨论的循环码 C、C_1、C_2 都是线性码,$d_L(C)=w_L(C)$,$d_H(C_1)=w_H(C_1)$,$d_H(C_2)=w_H(C_2)$,为了方便起见,转而求 $w_L(C)$的极小值。C 中任意一个码字 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})$,对应的码字多项式 $c(x)$可以写成:

$$c(x)=(a(x)+ub(x))((x+1)^i+u(x+1)^j)=$$
$$a(x)(x+1)^i+u(a(x)(x+1)^j+b(x)(x+1)^i)$$

设 $\boldsymbol{c}_1$ 和 $\boldsymbol{c}_2$ 为 $\boldsymbol{c}$ 所对应的剩余码和扭转码,根据 Lee 重量的定义,容易知道:

当 $a(x)(x+1)^i=0$ 时,$w_L(\boldsymbol{c})=2w_H(\boldsymbol{c}_2)$;

当 $a(x)(x+1)^i\neq 0$ 时,$w_L(\boldsymbol{c})\geqslant w_H(\boldsymbol{c}_1)$并且等号成立当且仅当

$$a(x)(x+1)^i=a(x)(x+1)^j+b(x)(x+1)^i\tag{2}$$

或

$$a(x)(x+1)^j+b(x)(x+1)^i=0\tag{3}$$

(1)$i\leqslant j, k_1\leqslant k_2$

①若 $a(x)(x+1)^i\neq 0$

当 $i>2^{s-l}$时,令 $t=i-\sum_{l=1}^{k_1-1}2^{s-l}$,$a$ 是满足 $1\leqslant t\leqslant 2^a\leqslant 2^{s-k_1}$的正整数。$a(x)=(x+1)^{2^a-t}$,$b(x)=a(x)(1-(x+1)^{j-i})$时,即可使得(2)成立并且

$$a(x)(x+1)^i=(x+1)^{2^a-t}(x+1)^i=(x+1)^{2^a}(x+1)^{\sum_{l=1}^{k_1-1}2^{s-l}}=$$

(下转 198 页)