准循环码和准循环子空间

辛小龙

(西北大学 数学系,陕西 西安 710069)

摘要:引入了线性空间的准循环子空间的概念,进而研究了准循环码与准循环子空间的关系,给出了准循环码的准循环子空间表示定理。

关 键 词:准循环码;循环无关;准循环子空间。

中图分类号:O157.4 **文献标识码**:A **文章编号**:1000-274X(2002)06-0597-04

循环码是线性分组码的一个重要子类,它有很多固有的代数结构,特别是循环码可以由循环子空间来表示。利用循环码的这些代数结构,我们可以找到各种简单实用的译码方法。由于循环码具有众多的良好性质,所以它在理论和实用中都是十分重要的。准循环码是循环码的推广,因此研究准循环码的代数结构也是非常重要的。本文首先将循环子空间的概念推广到准循环子空间,进而研究了准循环码与准循环子空间的关系,给出了准循环码的准循环子空间表示定理。

1 预 备

定义1[1] 对来自信源的信息序列,首先将其分成消息组,每个消息组由 k 个接续的信息数字组成,总有 2^k 种不同的消息;其次编码器按照一定的准则把每个消息变成较长的 n 位二进制数组,称其为码字,由这 2^k 个消息所获得的 2^k 个码字的全体,便称为码组长为 n,信息位为 k 的二元分组码。

定义2 设 $GF(q)$ 表示 q 元域,$GF(q)$ 上的 n 维向量空间 V_n 的 k 维线性子空间 V_k 称为分组长为 n,信息位为 k 的 q 元分组码。

定义3 (n,k) 线性码 V_k 的基底向量

$$\begin{gathered}\boldsymbol{e}_1=(v_{11}\quad v_{12}\quad \cdots v_{1n}),\\ \boldsymbol{e}_2=(v_{21}\quad v_{22}\quad \cdots v_{2n}),\\ \vdots\\ \boldsymbol{e}_k=(v_{k1}\quad v_{k2}\quad \cdots v_{kn})\end{gathered}$$

构成的矩阵

$$\boldsymbol{G}=\begin{bmatrix}\boldsymbol{e}_1\\ \boldsymbol{e}_2\\ \vdots\\ \boldsymbol{e}_k\end{bmatrix}=\begin{bmatrix}v_{11} & v_{12} & \cdots & v_{1n}\\ v_{21} & v_{22} & \cdots & v_{2n}\\ & \vdots & & \\ v_{k1} & v_{k2} & \cdots & v_{kn}\end{bmatrix}$$

称为 (n,k) 码的生成矩阵。

定义4 V_n 的 k 维子空间 V_k 称为一个循环码,如果对于任意 $(a_0,a_1,\cdots,a_{n-1})\in Vn$,只要 $(a_0,a_1,\cdots,a_{n-1})\in V_k$,就有 $(a_{n-1},a_0,\cdots,a_{n-2})\in V_k$。

定义5 设 T 是 V_n 到 V_n 的线性变换,$a\in V_n$. 称 $Z(a)=\{f(T)(a)\parallel f(x)\in F(x)\}$ 为由元素 a 生成的 T-循环子空间,$f(T)$ 是变换 T 的任意多项式。

定义6 生成矩阵形如

$$\boldsymbol{G}=\begin{bmatrix}1 & 0 & 0 & a_{11} & \cdots & a_{1n-k}\\ 0 & 1 & 0 & a_{21} & \cdots & a_{2n-k}\\ & & \vdots & & & \\ 0 & 0 & 1 & a_{k1} & \cdots & a_{kn-k}\end{bmatrix}$$

的 (n,k) 线性码称作 (n,k) 系统码。

定理1 设 W 是 n 维向量空间 V_n 的 k 维子空间,则 W 的零化子空间 U 是 n-k 维的,并且 U 由 W 惟一确定。

定理2 对于域 F 上的 V_n 到 V_n 的任何线性变换,恒存在惟一的 F 上的首一多项式 $m(x)$ 具有下述性质:

1) $m(T)=0$;

2) 对于任意 $f(x)\in F(x)$,若 $f(T)=0$ 则 $m(x)$ 整除 $f(x)$。

收稿日期:2001-02-09

基金项目:教育部留学回国人员科研基金资助项目(教外司留[2000]367号);陕西省自然科学基金资助项目(2000SL06)

作者简介:辛小龙(1955-),男,陕西西安人,西北大学教授,主要从事代数和编码理论研究。

$m(x)$ 称为变换 T 的最小多项式。

定理 3 设 S 为域 F 上 n 维线性空 V_n 的子空间，T 为 V_n 到 V_n 的线性变换。于是 S 为 T-循环子空间，当且仅当存在 $a(\neq 0)\in S$，使得，$a,T(a),\cdots,T^{d-1}(a)$ 构成 S 基底。

对于任意一个 n 维向量 $V=(v_0,v_1,\cdots,v_{n-1})$，都可以用一个次数不超过 $n-1$ 次的多项式

$$V(x)=v_0+v_1x+\cdots+v_{n-1}x^{n-1} \quad (1)$$

惟一确定，反之亦然。当 V 是一个码字时，就称 $V(x)$ 为相应码字的多项式。显然 V 与 $V(x)$ 一一对应，我们可以把任何一个 (n,k) 线性码等价的看作一类由 2^k 个次数不超过 $n-1$ 的多项式集合，即群代数 FG. 容易看到，群代数 FG 与 V_n 同构，且 V_n 的子空间 V_k 与 FG 的子群代数同构。因此，我们可以将一个码字多项式 $V(x)$ 视作一个向量 V。作变换

$$T(V(x))=xV(x),V(x)\in V_n。\quad (2)$$

显然 T 是 V_n 到 V_n 的线性变换。

定理 4 V_k 是循环码当且仅当 V_k 是群代数 FG 中的理想。

事实上，循环码 V_k 还是群代数 FG 的主理想。若设 $g(x)$ 为该主理想的生成多项式，我们称 $g(x)$ 为循环码 V_k 的生成多项式。

定理 5 V_n 的子空间 V_k 为由 $g(x)$ 生成的循环码当且仅当 V_k 是由 a 生成的 T-循环子空间，其中 T 为线性变换(2)，a 为 $g(x)$ 所对应的码向量。

2 准循环码与准循环子空间

在线性码 V_k 中，码字 $(a_0,a_1,\cdots a_{n-1})$ 对应的多项式 $a(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ 称为码字多项式，有时我们也称 $a(x)$ 为码字。在循环码 C_x 中，每一码字，左移或右移循环一位仍是 C_x 的一个码字。也即 $C(x)\in C_x$，则 $xC(x)\in C_x(\bmod x^n-1)$，即码在循环移位一次下具有不变性。但是，对某些码而言并不具有这些性质，即循环移位一次不一定是该码的码字。对一些码而言，虽然码字循环移位一次得到的不是该码的码字，但若循环移位 $n(\geqslant 1)$ 次得到的仍是该码的一个码字。如下例：

例 1 $C_{[6,3]}$ 为一个[6,3]码，它是由以下矩阵 G 生成的

$$G=\begin{bmatrix}1&0&0&1&0&1\\0&1&1&0&0&1\\0&1&0&1&1&0\end{bmatrix}$$

可以检验，若 $C(x)\in C_{[6,3]}$ 则 $xC(x)\notin C_{[6,3]}$，但是 $x^2C(x)\in C_{[6,3]}(\bmod x^6-1)$，亦即循环移位两次所得到的仍是该码的一个码字。由此，我们有准循环码的概念。

定义 7[2] 一个$[mn,mk]$线性分组码，若它的任意码字左移或右移循环移位 n 次后，得到的仍是该码的一个码字，则称这类码为 n 阶准循环码，简称准循环码。

由以上定义知，准循环码的每一个码字的码元位置号在置换：$i\to i+n(\bmod mn),i=1,2,\cdots,mn$ 下具有不变性。

显然，循环码是 $n=1$ 的准循环码，从而准循环码是循环码概念的推广。

当 $n=2$ 时，我们称准循环码为双环循环码。构造矩阵 G 为：

$$G=\begin{bmatrix}IP_0&0P_1&\cdots&0P_{m-1}\\0P_{m-1}&IP_0&\cdots&0P_{m-1}\\&\vdots&&\\0P_1&0P_2&\cdots&IP_0\end{bmatrix}\quad (3)$$

其中 I 为 $k\times k$ 阶单位阵，0 是 $k\times k$ 阶零矩阵，P_i 是 $k\times(n-k)$ 阶矩阵。容易看到以下结果：

定理 6 由(1)中定义的矩阵生成的线性码是 (mn,mk) 准循环码。

例 1 中的矩阵 G 就是具有形式(1)的矩阵，这时 $n=2,k=1,m=3$。

以下讨论准循环码的多项式表示。

设 C 是 (mn,mk) 准循环码，$V(x)$ 是 C 的一码字，在置换 $i\to i+n$ 下，$V(x)$ 被置换以后所得到的码字记为 $V^{(n)}(x)$，则它们有关系

$$V^{(n)}(x)\equiv x^nV(x)(\bmod x^{mn}-1)。$$

例 2 对于例 1 中的双环循环码，这个双环循环码的多项式表示为

$$V^{(2)}(x)\equiv x^2V(x)\bmod(x^6-1)。$$

其中的一个码多项式为 $V(x)=1+x^3+x^5$，而 $x^2V(x)=x^7+x^5+x^2$。于是

$$V^{(2)}\equiv x^2V(x)\bmod(x^6-1)。$$

另一个码多项式 $V(x)=x^5+x^2+x$ 对应的码向量(0,1,1,0,0,1)也为例 1 中双环循环码的向量。

现在，我们建立准循环子空间的概念，进而用准循环子空间的概念来描述准循环码。先给出一个循环无关的概念。

定义 8 设 V 是一个线性空间，$a_1,a_2,\cdots,a_k\in V$，其对应的多项式分别为 $g_1(x),g_2(x),\cdots,g_k(x)$. 如果 $a_1,a_2,\cdots,a_k$ 线性无关且对任意两个 $a_i\neq a_j(i\neq j)$，它们不能在有限次置换 $i\to i+n$ 下相互得到，

即对于任意正整数 I,$g_i(x) \neq x^n g_j(x)$,则称 $a_1,a_2,\cdots,a_k$ 或 $g_1(x),g_2(x),\cdots,g_k(x)$ 是 n- 循环无关的。

例　3　设 G 为式(1)所给出的准循环码的生成矩阵,取 $a_1,a_2,\cdots,a_k$ 为 G 的前 k 行构成的向量组,则 $a_1,a_2,\cdots,a_k$ 是 n- 循环无关的。

现在给出 T- 准循环子空间的概念。

设 T 是线性空间 V 上的一个线性变换,$a_1,a_2,\cdots,a_k$ 是 V 的一组线性无关向量,构造集合:$\{f_1(T)a_1+f_2(T)a_2+\cdots+f_k(T)a_k \| f_i(x)\in F(x),i=1,2,\cdots,k\}$。记这个集合为 $Z(a_1,a_2,\cdots,a_k)$,容易看到以下结果:

定理7　$Z(a_1,a_2,\cdots,a_k)$ 是线性空间 V 的一个子空间,且是线性变换 T 的不变子空间。

定义9　称 $Z(a_1,a_2,\cdots,a_k)$ 为线性空间 V 的一个由元素 $a_1,a_2,\cdots,a_k$ 生成的 T- 准循环子空间,简称为 T- 准循环子空间。

关于 T- 准循环子空间,我们有下述定理:

定理8　若 $a_1,a_2,\cdots,a_k$ 是线性空间 V 的一组 n- 循环无关向量组,则由 $a_1,a_2,\cdots,a_k$ 生成的 T- 准循环子空间是 T- 循环子空间 $Z(a_1),Z(a_2),\cdots,Z(a_k)$ 的直和,即

$$Z(a_1,a_2,\cdots,a_k)=Z(a_1)\oplus Z(a_2)\oplus\cdots\oplus Z(a_k)。$$

其中 T 定义为:$T(g(x))=x^n g(x)$,任给 $g(x)\in F[x]$。有时也记 $T(g(x))$ 为 $T(a)$,其中 a 为 $g(x)$ 对应的码向量。

证　明　由 $Z(a_1,a_2,\cdots,a_k)$ 的定义易知

$$Z(a_1,a_2,\cdots,a_k)=Z(a_1)+Z(a_2)+\cdots Z(a_k)。$$

又由 $a_1,a_2,\cdots,a_k$ 是 n- 循环无关的假设,我们可以得到:$Z(a_i)\cap Z(a_j)=\{0\}$,对 $i,j=1,2,\cdots k$;且 $i\neq j$ 成立,从而题设结论成立。

定理9　设 S 是线性空间 V_{mn} 的一个 mk 维子空间,T 是定理8中的线性变换,$a_1,a_2,\cdots,a_k$ 是 V_{mn} 中的一组 n- 循环无关的向量。则 S 是一个由 $a_1,a_2,\cdots,a_k$ 生成的 T- 准循环子空间的充要条件是

$$a_1,Ta_1,\cdots,T^{m_1-1}a_1,a_2,Ta_2,\cdots,T^{m_2-1}a_2,\cdots,a_k,Ta_k,\cdots,T^{m_k-1}a_k \tag{4}$$

构成 S 的一组基.其中 m_i 是线性变换 T 在循环子空间 $Z(a_i)$ 上的最小多项式的次数。

证　明　先证充分性。设式(4)构成 S 的一组基,对任意 $a\in S$,有

$$a=a_{10}a_1+a_{11}Ta_1+\cdots a_{1,m_1-1}T^{m_1-1}a_1+\cdots+a_{k0}a_k+a_{k1}Ta_k+\cdots+a_{k,m_k-1}T^{m_k-1}a_k=$$

$$(a_{10}+a_{11}T+\cdots+a_{1,m_1-1}T^{m_1-1})a_1+\cdots+(a_{k0}+a_{k,1}T+\cdots a_{k,m_k-1}T^{m_k-1})a_k=$$

$$f_1(T)a_1+\cdots+f_k(T)a_k\in Z(a_1,a_2,\cdots,a_k),$$

即 $a\in Z(a_1,a_2,\cdots a_k)$ 或 S 包含于 $Z(a_1,a_2,\cdots,a_k)$。另一方面,设 $a\in Z(a_1,a_2,\cdots,a_k)$,则 $a=f_1(T)a_1+f_2(T)a_2+\cdots+f_k(T)a_k$. 设 $g_i(x)$ 为变换 T 在子空间 $Z(a_i)$ 上的诱导变换的最小多项式,即设 $g_i(x)=g_0+g_1x+\cdots+g_{m_i-1}x^{m_i-1}+x^{m_i-1}$。从而

$$g_i(T)a_i=g_0a_i+g_1Ta_i+\cdots+g_{m_i-1}T^{m_i-1}a_i+T^{m_i-1}a_i=0,$$

则在 $f(T)$ 中的次数高于 m_i 的项 $T^{m_i+1}a_i(a>0)$ 可按下式

$$T^{m_i}a_i=-g_0a_i-g_1T_{a_i}-\cdots-g_{m_i-1}T^{m_i-1}a_i$$

化简。于是,可设 $f(x)$ 的次数小于 m_i,从而 a 可由基

$$a_1,T\,a_1,\cdots,T^{m_1-1}a_1,\cdots,a_k\cdots,T^{m_i-1}a_k$$

线性表示,从而 $a\in S$,即 $Z(a_1,a_2,\cdots,a_k)$ 包含于 S。综合以下两方面得 $S=Z(a_1,a_2,\cdots,a_k)$ 充分性得证。

再证必要性。设 S 是由 $a_1,a_2,\cdots,a_k$ 生成的 T- 准循环子空间,即 $S=Z(a_1,a_2,\cdots,a_k)$。由定理8,有 $Z(a_1,a_2,\cdots,a_k)=z(a_1)\oplus Z(a_2)\oplus\cdots\oplus Z(a_k)$。

我们先证式(4)是线性无关的。否则,若在 F 中含不全为零的数

$$a_{10},a_{11},\cdots,a_{1,m_1-1},\cdots,a_{k0},\cdots,a_{k,m_k-1},$$

使得

$$a_{10}a_1+a_{11}T\,a_1+\cdots+a_{1,m_1-1}T^{m_1-1}a_1+\cdots+a_{k0}a_k+a_{k1}Ta_k+\cdots+a_{k,m_k-1}T^{m_k-1}a_k=0。$$

整理可得

$$\varphi_1(T)a_1+\varphi_2(T)a_2+\cdots+\varphi_k(T)a_k=0。$$

由于 $\varphi_1(T)a_1+\varphi_2(T)a_2+\cdots+\varphi_k(T)a_k=0\in S$,且 S 是 $Z(a_1),Z(a_2),\cdots,Z(a_k)$ 的直和,故 $\varphi_i(T)a_i=0$,对 $i=1,2,\cdots,k$ 成立。注意对任意 $a\in Z(a_i)$,$a=f_i(T)a_i$。从而 $\varphi_i(T)(a)=\varphi_i(T)(f_i(T)a_i)=f_i(T)(\varphi_i(T)a_i)=f_i(T)0=0$,即 $\varphi_i(T)(a)=0,\forall\, a\in Z(a_i)$。但是,这矛盾于线性变换 T 在 $Z(a_i)$ 上的最小多项式的次数为 m_i 的假设,从而式(4)是线性无关的。

再证对任意 $a\in S$,可以由向式(4)线性表示。设 $a\in S$,则

$$a=f_1(T)a_1+f_2(T)a_2+\cdots f_k(T)a_k。$$

设 $g_i(x)=g_0+g_1x+\cdots+g_{m_i-1}x^{m_i-1}+x^{m_i}$ 是 T 在 $Z(a_i)$ 上的最小多项式,则 $g_i(T)a_i=0$. 从而

$a_i^{m_i} = -(g_0 a_i + g_1 T a_i + \cdots + g_{m_i - 1} T^{m_i - 1} a_i)$。可设 $f_i(x)$ 的次数不超过 $m_i - 1, i = 1,2,\cdots k$. 这就表明 a 可由式(4)线性表示,即式(4)形成 S 的一组基。

现在,我们来讨论 T- 准循环子空间与准循环码之间的关系。

定理 10 设 $\boldsymbol{G}$ 是式(1)定义的矩阵,S 是由 $\boldsymbol{G}$ 生成的 (mn, mk) 循环码,则 S 是由 $a_1, a_2, \cdots, a_k$ 生成的 T- 准循环子空间,即 $S = Z(a_1, a_2, \cdots, a_k)$,其中 a_1, $a_2, \cdots, a_k$ 分别为 $\boldsymbol{G}$ 的第一行,第二行,…,第 K 行构成的向量,T 是定理 8 中的线性变换。

证 明 由 $\boldsymbol{G}$ 的构造知,$a_1, a_2, \cdots, a_k$ 是 n- 循环无关的向量组,且 $a_1, Ta_1, \cdots, T^{m-1}a_1, a_2, Ta_2, \cdots, T^{m-1}a_2, \cdots, a_k, Ta_k, \cdots, T^{m-1}a_k$ 形成 S 的一组基,由定理 9 知,$S = Z(a_1, a_2, \cdots, a_k)$。

定理 11 设 S 是线性空间 V_{mn} 的一个子空间,T 是定理 9 中的线性变换。则 S 是 n 阶准循环码的充要条件是存在 V_{mn} 中一组 n- 循环无关向量 $a_1, a_2, \cdots, a_k$ 生成的 T- 准循环子空间。

证 明 先证充分性。设 S 是由 n- 循环无关的向量 $a_1, a_2, \cdots, a_k$ 生成的 T- 准循环子空间,即 $S = Z(a_1, a_2, \cdots, a_k)$。由定理 9,$S$ 有一组形式为式(2)的一组基底 $a_1, Ta_1, \cdots, T^{m_1-1}a_1, a_2, Ta_2, \cdots, T^{m_2-1}a_2, \cdots, a_k, Ta_k, \cdots, T^{m_k-1}a_k$。对上述基底中每一个向量 $V(x)$,由 $T(V(x)) = x^n V(x) \equiv V^{(n)}(x) \bmod (x^{mn} - 1)$,有 $V(x)$ 在置换 $i \to i + n$ 下具有不变性,从而上述基底的每个向量具有相同的不变性,即 S 是一个 n 阶准循环码。

再证必要性。设 S 是一个 n 阶准循环码,首先取 $a_1 \in S$. 若 $S = Z(a_1)$,则命题得证。不妨设 $S \neq Z(a_1)$,则取 $a_2 \in S$ 但 a_2 不属于 $Z(a_1)$。若 $S = Z(a_1, a_2)$,则同样命题成立。故不妨设 $S \neq Z(a_i, a_2)$。从而依此类推可取出 n- 循环无关的向量 $a_1, a_2, \cdots, a_k$,使得 $Z(a_i) \subset S$ 中,$(i = 1, 2, \cdots k)$。从而 $Z(a_1) + Z(a_2) + \cdots + Z(a_k) \subset S$。因为 S 是一个子空间,但 S 是有限集合,总可选得 n- 循环无关向量 $a_1, a_2, \cdots, a_k$ 使 $Z(a_1) + Z(a_2) + \cdots + Z(a_k) = S$。由定理 8,$Z(a_1) + Z(a_2) + \cdots + Z(a_k)$ 是直和且有 $Z(a_1, a_2, \cdots a_k) = Z(a_1) \oplus Z(a_2) \oplus \cdots \oplus Z(a_k)$,从而 $S = Z(a_1, a_2, \cdots, a_k)$,必要性得证。

例 4 设线性码 S 的生成矩阵为例 1 中的矩阵 $\boldsymbol{G}$,S 是一个双环循环码。取 $a_1 = (1,0,0,1,0,1)$ 对应 $g_1(x) = 1 + x^3 + x^5$,$Ta_1 = (0,1,1,0,0,1)$ 对应 $Tg_1(x) = x + x^3 + x^5$,$T^2 a_1 = (0,1,0,1,1,0)$ 对应 $T^2 g_1(x) = x + x^3 + x^4$。

从而构成 S 的基底,S 是由 a_1 生成的 T- 准循环子空间。

参考文献:

[1] 肖国镇,卿斯汉. 编码理论[M]. 北京:国防工业出版社,1993.
[2] 王新梅,肖国镇. 纠错码——原理与方法[M]. 西安:西安电子科技大学出版社,1991.

(编 辑 曹大刚)

Quasi-cyclic codes and quasi-cyclic subspaces

XIN Xiao-long
(Department of Mathematics, Northwest University, Xi'an 710069, China)

Abstract: The concept of quasi-cyclic subspaces in linear spaces was introduced and the relation of quasi-cyclics subspaces and quasi-cyclic codes was studied. The representations of quasi-cyclic codes was given by quasi-cyclics subspaces.

Key words: quasi-cyclic code; cyclic independent; quasi-cyclics subspace