基于极小线性码上的秘密共享方案

宋 云[1],李志慧[1],李永明[2]
(1.陕西师范大学数学与信息科学学院,陕西西安 710062;2.陕西师范大学计算机科学学院,陕西西安 710062)

摘 要: 从理论上说,每个线性码都可用于构造秘密共享方案,但是在一般情况下,所构造的秘密共享方案的存取结构是难以确定的.本文提出了极小线性码的概念,指出基于这种码的对偶码所构造的秘密共享方案的存取结构是容易确定的.本文首先证明了极小线性码的缩短码一定是极小线性码.然后对几类不可约循环码给出它们为极小线性码的判定条件,并在理论上研究了基于几类不可约循环码的对偶码上的秘密共享方案的存取结构.最后用编程具体求出了一些实例中方案的存取结构.

关键词: 极小线性码; 存取结构; 极小码字; 秘密共享方案; 不可约循环码
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2013)02-0220-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.02.003

Secret Sharing Schemes Based on Minimal Linear Codes

SONG Yun[1], LI Zhi-hui[1], LI Yong-ming[2]
(1. *College of Mathematics and Information Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *College of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*)

Abstract: Theoretically, every linear code can be used to construct secret sharing schemes. However, determining the access structure of the schemes based on linear codes is very hard. The concept of minimal linear code is proposed, which makes the determination of the access structure of the schemes based on the duals of minimal linear codes easier. It is shown that the shortening codes of minimal linear codes are minimal as well. Then the conditions whether several types of irreducible cyclic codes are minimal or not are presented. Furthermore, the access structures of secret sharing schemes based on the duals of minimal linear codes are studied. Finally, the access structures of the schemes in specific examples are obtained through programming.

Key words: minimal linear code; access structures; minimal codeword; secret sharing scheme; irreducible cyclic codes

1 引言

为了维护秘密的安全性和有效性,A.Shamir[1]和 G.Blakley[2]于 1979 年各自独立提出了秘密共享的概念.由于秘密共享方案在信息安全中起着重要的作用,一些学者对其进行了深入的研究[3~5].对于主密钥 s,参与者集合中只有那些事先授权的子集中的参与者,利用他们所持有的秘密份额才能恢复秘密,这些子集组成的集合称为存取结构,其中的子集叫授权子集.如果一个授权子集的任意真子集均不能恢复秘密,称这个授权子集为极小授权子集.在秘密共享方案中,如果任意非授权子集都得不到秘密的任何信息,就称该方案是完善的.从信息论的角度来看,这是人们所希望的.定义信息率为主密钥长度(二进制的比特位数)与最长子密钥长度的比值,信息率越高代表方案的数据扩散程度越小,就认为此方案的效率越高.可以证明,实现一个存取结构的秘密共享方案的信息率不超过 1[6].当信息率等于 1 时,称该方案是理想的.1993 年,Massey 基于线性码提出了一种完善的理想的秘密共享方案,并且指出线性码上的秘密共享方案的极小授权子集与所用线性码的对偶码中的极小码字之间存在一一对应关系[7,8].然而,对一般的线性码来说,判定一个码字是否为极小码字是极其困难的[9,10],这也就是说,建立在一般线性码上的秘密共享方案的存取结构是很难求出的,因此也就很难在实际中应用.本文提出了极小线性码的概念,可以证明极小线性码中的极小码字比较容易求得.这就使得寻找和构造极小线性码成为问题的关键.

本文给出了极小线性码的构造方法,并研究了极小线性码的判别条件.在此基础上给出了基于一类极小线性码的对偶码所构造的秘密共享方案的极小授权子集.

收稿日期:2011-11-03;修回日期:2012-05-15
基金项目:国家自然科学基金(No.60873119)

最后用编程具体求出了一些实例中方案的存取结构.

2　极小线性码及其构造

在本文中,设 $q=p^s$,p 是一个素数,s 是一个正整数.一个$[n,k,d;q]$线性码 C 是指 F_q^n 的一个 k 维线性子空间,且它的最小 Hamming 重量为 d.

定义 1[9]　设向量 $c=(c_1,c_2,\cdots,c_n)\in F_q^n$,指标集 $\{1\leqslant i\leqslant n\mid c_i\neq 0\}$称为向量 c 的支撑.如果码字 c_2 的支撑包含码字 c_1 的支撑就称码字 c_2 覆盖码字 c_1.

定义 2[9]　如果码 C 的一个码字 c 的第一分量为 1,称这样的码字为正规码字.如果一个正规码字不覆盖码 C 的其他正规码字,称这个码字为极小码字.

定义 3[10]　如果码 C 的一个非零码字 c 只是覆盖它的倍数,不再覆盖其它的码字,称码字 c 为一个极小向量.

由以上定义可知,极小码字一定是极小向量,但是极小向量不一定为极小码字.

定义 4　如果线性码 C 的生成矩阵中不含零列,且码 C 的每个非零码字均为极小向量,则称码 C 为极小线性码.

本文以下约定所提到的线性码的生成矩阵中均不含零列.

以下给出通过缩短极小线性码中的码字的长度来构造新的极小线性码的一种方法.

设 C 是一个$[n,k;q]$极小线性码,约定它的信息位在前 k 位,且设其生成矩阵为

$$\boldsymbol{G}=\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1,n-1} & g_{1,n} \\ g_{21} & g_{22} & \cdots & g_{2,n-1} & g_{2,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g_{k1} & g_{k2} & \cdots & g_{k,n-1} & g_{k,n} \end{pmatrix}.$$

引理 1　设 C 是$[n,k;q]$线性码,且设其生成矩阵 $\boldsymbol{G}$ 的任意两列不成比例,令 $C(n)=\{c=(c_1,c_2,\cdots,c_{n-1},0)\mid c\in C\}$则

(a) $C(n)$是一个$[n,k-1;q]$线性码,

(b) $C(n)$的生成矩阵的前 $n-1$ 列中不含零列.

证明　(a)由于 C 的生成矩阵 $\boldsymbol{G}$ 的任意两列不成比例,所以 $\boldsymbol{G}$ 中肯定不含零向量,因此,$\boldsymbol{G}$ 的第 n 列不是零向量.不妨设 $g_{1,n}\neq 0$,则给 $\boldsymbol{G}$ 的第一行依次乘 $-g_{1,n}^{-1}g_{2,n},\cdots,-g_{1,n}^{-1}g_{k,n}$后分别加到第 2 行至第 k 行,可将 $\boldsymbol{G}$ 化为如下形式 $\boldsymbol{G}_1$:

$$\boldsymbol{G}_1=\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1,n-1} & g_{1,n} \\ g'_{21} & g'_{22} & \cdots & g'_{2,n-1} & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g'_{k1} & g'_{k2} & \cdots & g'_{k,n-1} & 0 \end{pmatrix},$$

令 $\boldsymbol{G}(n)=\begin{pmatrix} g'_{21} & g'_{22} & \cdots & g'_{2,n-1} & 0 \\ \cdots & \cdots & & \cdots & \cdots \\ g'_{k1} & g'_{k2} & \cdots & g'_{k,n-1} & 0 \end{pmatrix}$,

显然,以 $\boldsymbol{G}(n)$为生成矩阵生成的码是一个$[n,k-1;q]$码,且包含于 $C(n)$中,故 $\dim(C(n))\geqslant k-1$,这里符号 $\dim(C(n))$表示码 $C(n)$的维数.另一方面,C 的码字$(g_{11},g_{12},\cdots,g_{1n})$显然不在 $C(n)$中,故 $C(n)$为 C 的真子空间,从而 $\dim(C(n))\leqslant k-1$.综上所述,码 $C(n)$是一个$[n,k-1;q]$码,且其生成矩阵为 $G(n)$.

(b)下证 $C(n)$的生成矩阵的前 $n-1$ 列中不含零列.假设 $\boldsymbol{G}(n)$第 i 列为零向量$(1\leqslant i\leqslant n-1)$. 即

$$\begin{pmatrix} g'_{2i} \\ \vdots \\ g'_{ki} \end{pmatrix}=\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

由 $\boldsymbol{G}(n)$的构造过程就有下式成立:

$$\begin{pmatrix} g_{2,i}-g_{1,n}^{-1}g_{2,n}g_{1,i} \\ \vdots \\ g_{k,i}-g_{1,n}^{-1}g_{k,n}g_{1,i} \end{pmatrix}=\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

则当且仅当 $\begin{pmatrix} g_{2,i} \\ \vdots \\ g_{k,i} \end{pmatrix}=g_{1,n}^{-1}g_{1,i}\begin{pmatrix} g_{2,n} \\ \vdots \\ g_{k,n} \end{pmatrix}$

当且仅当 $\begin{pmatrix} g_{1,i} \\ g_{2,i} \\ \vdots \\ g_{k,i} \end{pmatrix}=g_{1,n}^{-1}g_{1,i}\begin{pmatrix} g_{1,n} \\ g_{2,n} \\ \vdots \\ g_{k,n} \end{pmatrix}$

即 $\boldsymbol{G}$ 的第 i 列与第 n 列成比例,矛盾.　　证毕

注:在引理 1 中,也可引入符号 $C(i)=\{c=(c_1,\cdots,c_{i-1},0,c_{i+1},\cdots,c_n)\mid c\in C\}$,可证明 $C(i)$具有与 $C(n)$同样的性质.

引理 2　设 C 是一个$[n,k;q]$线性码,令 $C(n)[n-1]=\{c=(c_1,c_2,\cdots,c_{n-1})\mid(c_1,c_2,\cdots,c_{n-1},0)\in C(n)\}$,则有

(a) $C(n)[n-1]$的生成矩阵为

$$\boldsymbol{G}(n)[n-1]=\begin{pmatrix} g'_{21} & g'_{22} & \cdots & g'_{2,n-1} \\ \vdots & \vdots & & \vdots \\ g'_{k1} & g'_{k2} & \cdots & g'_{k,n-1} \end{pmatrix}$$

其中 $G(n)[n-1]$为 $G(n)$的前 $n-1$ 列构成的矩阵,

(b) $C(n)[n-1]$是一个$[n-1,k-1;q]$线性码.

证明　由于码 $C(n)$与码 $C(n)[n-1]$同构,故由引理 1 的证明过程可知,码 $C(n)[n-1]$的生成矩阵显然为 $\boldsymbol{G}(n)[n-1]$.所以 $C(n)[n-1]$是一个$[n-1,k-1;q]$线性码.　　证毕

定理 1　如果 C 是一个$[n,k;q]$极小线性码,则 $C(n)[n-1]$是一个$[n-1,k-1;q]$极小线性码.

证明 由引理 2 可知,$C(n)[n-1]$是一个$[n-1, k-1; q]$线性码.下证 $C(n)[n-1]$是一个极小线性码.假设 $C(n)[n-1]$不是一个极小线性码,则由定义 4 可知,存在非零码字 $\boldsymbol{c}'=(c_1, c_2, \cdots, c_{n-1})\in C(n)[n-1]$不是极小向量,从而存在 $\boldsymbol{c}_0'=(c_{0,1}, c_{0,2}, \cdots, c_{0,n-1})\in C(n)[n-1]$使得 $\boldsymbol{c}'$能覆盖 $k\boldsymbol{c}'$之外的码字 $\boldsymbol{c}_0'$,其中 $k\in F_q$.令 $\boldsymbol{c}=(c_1, c_2, \cdots, c_{n-1}, 0)$, $\boldsymbol{c}_0=(c_{0,1}, c_{0,2}, \cdots, c_{0,n-1}, 0)$,显然 c 和 c_0 均在码 C 中,从而在线性码 C 中码字 $\boldsymbol{c}$ 能覆盖 $k\boldsymbol{c}$ 之外的码字 $\boldsymbol{c}_0$,故码字 $\boldsymbol{c}$ 不是一个极小向量.因此线性码 C 不是极小线性码,矛盾. 证毕

以下引入符号:

$$C(n, n-1, \cdots, n-i)$$
$$=\{\boldsymbol{c}=(c_1, c_2, \cdots, c_{n-i-1}, 0, \cdots, 0) \mid \boldsymbol{c}\in C\}\ (0\leqslant i\leqslant n-k-2).$$
$$C(n, n-1, \cdots, n-i)[n-i-1]$$
$$=\{\boldsymbol{c}=(c_1, c_2, \cdots, c_{n-i-1}) \mid (c_1, c_2, \cdots c_{n-i-1}, 0, \cdots, 0)\in C\}$$

则易证 $C(n, n-1, \cdots, n-i)$和 $C(n, n-1, \cdots, n-i)[n-i-1]$分别为$[n, k-i-1; q]$和$[n-i-1, k-i-1; q]$线性码.且有

$$C(n, n-1, \cdots, k+2)\leqslant \cdots \leqslant C(n, n-1, \cdots, n-i)\leqslant \cdots \leqslant C(n)\leqslant C$$

其中符号 $C(n)\leqslant C$ 表示前者为后者的子码.

定理 2 设 C 是一个$[n, k; q]$极小线性码,且设 $C^{\perp}$的极小距离 >2.则

(a) $C(n, n-1, \cdots, n-i)[n-i-1]$的生成矩阵中不含零列;

(b) $C(n, n-1, \cdots, n-i)[n-i-1]$是一个$[n-i-1, k-i-1; q]$极小线性码.

证明 (a)首先比较码 $C(n, n-1, \cdots, n-i)[n-i-1]$和 $C(n, n-1, \cdots, n-i-1)[n-i-2]$的对偶码之间的关系.

设$(x_1, x_2, \cdots, x_{n-i-2})\in C(n, n-1, \cdots, n-i-1)[n-i-2]^{\perp}$,则 $x_1c_1+x_2c_2+\cdots+x_{n-i-2}c_{n-i-2}=0$,

$\forall (c_1, c_2, \cdots, c_{n-i-2})\in C(n, n-1, \cdots, n-i-1)[n-i-2]$,从而 $x_1c_1+x_2c_2+\cdots+x_{n-i-2}c_{n-i-2}+0c_{n-i-1}=0$,

$\forall (c_1, c_2, \cdots c_{n-i-2}, c_{n-i-1})\in C(n, n-1, \cdots, n-i)[n-i-1]$,故$(x_1, x_2, \cdots, x_{n-i-2}, 0)\in C(n, n-1, \cdots, n-i)[n-i-1]^{\perp}(0\leqslant i\leqslant n-k-2)$.

由上述讨论可知,因为 $C^{\perp}$的极小距离 >2,则 $C(n, n-1, \cdots, n-i)[n-i-1]^{\perp}$的极小距离必 >2.故 $C(n, n-1, \cdots, n-i)[n-i-1]$的生成矩阵中任意两列一定线性无关$(0\leqslant i\leqslant n-k-2)$,从而不含零列.

(b)由于 $C(n, n-1, \cdots, n-i)[n-i-1]$是一个$[n-i-1, k-i-1; q]$线性码,由$(a)$知 $C(n, n-1, \cdots, n-i)[n-i-1]$的生成阵不含零列.由 $C(n, n-1, \cdots, n-i)[n-i-1]$的构造过程可知,若 C 是一个$[n, k; q]$极小线性码,则$C(n, n-1, \cdots, n-i)[n-i-1]$中的码字均为极小向量,故 $C(n, n-1, \cdots, n-i)[n-i-1]$是一个$[n-i-1, k-i-1; q]$极小线性码 $(0\leqslant i\leqslant n-k-2)$. 证毕

由定理 1 和定理 2 可知,通过缩短已有的极小线性码中的码字长度这一方法可构造新的极小线性码.

3 极小线性码的判定

利用极小线性码的定义,首先可将文[9]中的定理 3 叙述如下.

定理 3 在一个$[n, k; q]$线性码 C 中,设 $W_{\min}$和 $W_{\max}$分别表示码 C 的极小重量和极大重量.如果$\frac{W_{\min}}{W_{\max}}>\frac{q-1}{q}$,且码 C 的生成矩阵没有零列,则码 C 是一个极小线性码.

由极小线性码的定义易知一重量的线性码一定是极小线性码.

以下主要针对一类不可约循环码给出它们为极小线性码的判定方法.

首先回顾一下,$q=p^s$, p 是一个素数, s 是正整数.以下令 $r=q^m$, m 是正整数.

定义 5[9] 设 $N>1$ 是 $r-1$ 的一个因子,令 $n=q^m-1/N$, α 是有限域 F_{q^m}的一个本原元,且 $\theta=\alpha^N$.则称

$$C(q, m, N)=\{(Tr_{r/q}(\beta), Tr_{r/q}(\beta\theta), \cdots, Tr_{r/q}(\beta\theta^{n-1})) \mid \beta\in F_r\} \quad (1)$$

是有限域 F_q 上的不可约循环码,其中 $Tr_{r/q}$是从 F_r 到 F_q 的迹函数.

由于文献[11]已对一些不可约循环码的重量分布做了研究,以下将利用已得到的重量分布结果,对 N 的不同取值给出不可约循环码 $C(q, m, N)$是极小线性码所满足的条件

定理 4 设 $N=2$.

(a)当 m 是偶数时,若 $2q-q^{m/2}-1<0$,则 $C(q, m, 2)$是极小线性码.

(b)当 m 是奇数时, $C(q, m, 2)$是极小线性码.

证明 (a)由文[11]知,当 $N=2$ 且 m 是偶数时,码 $C(q, m, 2)$的重量分布是

$$1+\frac{q^m-1}{2}x^{\frac{(q-1)(q^m-q^{m/2})}{2q}}+\frac{q^m-1}{2}x^{\frac{(q-1)(q^m+q^{m/2})}{2q}}$$

根据定理 3,则有

$$\frac{W_{\min}}{W_{\max}}=\frac{q^m-q^{m/2}}{q^m+q^{m/2}}>\frac{q-1}{q},$$

进而有 $$\frac{q^{(m/2)+1}-q}{q^{(m/2)+1}-q-q^{(m/2)}+2q-1}>1,$$

故可得 $2q-q^{m/2}-1<0$.

(*b*)当 $N=2$ 且 m 是奇数时,这时码 $C(q,m,2)$是一重量码,由于一重量线性码一定是极小线性码,故 $C(q,m,2)$是极小线性码.　　证毕

定理 5　设 $N=3$,令 $q\equiv 2(\bmod 3)$,

(*a*)当 $m\equiv 0(\bmod 4)$时,若 $3q-q^{m/2}-2<0$,则 $C(q,m,3)$是极小线性码.

(*b*)当 $m\equiv 2(\bmod 4)$时,若 $3q-q^{m/2}-1<0$,则 $C(q,m,3)$是极小线性码.

令 $q\equiv 1(\bmod 3)$,当 $3\mid/m$ 时,则 $C(q,m,3)$是极小线性码.

定理 6　设 $N=4$,令 $q\equiv 3(\bmod 4)$,

(*a*)当 $m\equiv 0(\bmod 4)$时,若 $4q-q^{m/2}-3<0$,则 $C(q,m,4)$是极小线性码.

(*b*)当 $m\equiv 2(\bmod 4)$时,若 $4q-q^{m/2}-1<0$,则 $C(q,m,4)$是极小线性码.

定理 7　设 $N=4$,令 $q\equiv 1(\bmod 4)$,$p\equiv 3(\bmod 4)$且 s 是偶数.

(*a*)当 $m\equiv 0(\bmod 4)$时,若 $4q-q^{m/2}-3<0$,则 $C(q,m,4)$是极小线性码.

(*b*)当 $m\equiv 2(\bmod 4)$时,若 $2q-q^{m/2}-1<0$,则 $C(q,m,4)$是极小线性码.

定理 5,定理 6 以及定理 7 的证明过程与定理 4 类似.

当不可约循环码是极小线性码时,基于此码可利用以下定理来构造新的极小线性码.

设 l 是使得 $\theta^l\in F_q$ 的最小的非零整数,且令 $\theta^l=e$,根据定义 5 及文献[12],则易证 $l\mid n$,且 $C(q,m,N)$可表示为

$$C(q,m,N)=\{c_\beta=(|\overline{c_\beta}|e\overline{c_\beta}|\cdots|e^j\overline{c_\beta}|\cdots|e^{t-1}\overline{c_\beta}|)|\ \beta\in F_r\}\tag{2}$$

其中 $n=lt$,且 $\overline{c_\beta}=(Tr_{r/q}(\beta),Tr_{r/q}(\beta\theta),\cdots,Tr_{r/q}(\beta\theta^{l-1}))$.

定理 8　令 $\bar{C}=\{\overline{c_\beta}=(Tr_{r/q}(\beta),Tr_{r/q}(\beta\theta),\cdots,Tr_{r/q}(\beta\theta^{l-1}))|\beta\in F_r\}$　(3)

则 $C(q,m,N)$是极小线性码当且仅当 $\bar{C}$ 是极小线性码.

证明　因为式(2)中的 e^j 是 F_q 中的非零元,所以 $wt(e^j\overline{c_\beta})=wt(\overline{c_\beta})$,即 $wt(c_\beta)=twt(\overline{c_\beta})$,

则 $\dfrac{W_{\bar{C}_{\min}}}{W_{\bar{C}_{\max}}}=\dfrac{W_{C(q,m,N)_{\min}}}{W_{C(q,m,N)_{\max}}}$,由定理 3 可得结论.　　证毕

4　基于极小线性码的对偶码上的秘密共享方案

首先回顾基于线性码来构造秘密共享方案的方法,然后研究基于极小线性码的对偶码上的秘密共享方案的存取结构.

4.1　线性码上的秘密共享方案

在一个以 $\boldsymbol{G}=(g_0,g_1,\cdots,g_{n-1})_{k\times n}$为生成矩阵的 $[n,k;q]$线性码 C 上的秘密共享方案中,秘密是 F_q 中的一个元素,并包含 $n-1$ 个参与者 $P_1,P_2,\cdots,P_{n-1}$及一个秘密分发者.为了得到与秘密 s 有关的每个参与者的份额,分发者随即选取一个向量 $\boldsymbol{u}=(u_0,\cdots,u_{k-1})\in F_q^k$,使得 $s=ug_0$,易证存在 q^{k-1}个这样的向量 $\boldsymbol{u}\in F_q^k$.分发者将 u 作为一个信息向量,计算对应的码字 $t=(t_0,t_1,\cdots,t_{n-1})=uG$,他将 t_i 依次分发给 P_i 作为他们的秘密份额$(1\leqslant i\leqslant n-1)$.

注意到 $t_0=ug_0=s$,容易看出份额集$\{t_{i_1},t_{i_2},\cdots t_{i_m}\}$可计算出秘密 s 当且仅当 g_0 是 $g_{i_1},g_{i_2}\cdots,g_{i_m}$的一个线性组合.

这个结论的等价命题是如下引理.

定理 9[7]　设 G 是$[n,k;q]$线性码 C 的一个生成矩阵.在基于码 C 的秘密共享方案中,如果码 C 的对偶码 $C^\perp$中存在一个码字

$$(1,0,\cdots,c_{i_1},0,\cdots,0,c_{i_m},0,\cdots,0)\tag{4}$$

其中对至少某个 j 有 $c_{i_j}\neq 0(1\leqslant i_1<\cdots,<i_m\leqslant n-1,1\leqslant m\leqslant n-1)$,则份额$\{t_{i_1},t_{i_2},\cdots t_{i_m}\}$可计算秘密.

由定理 9 知,如果在 $C^\perp$中有(4)这样的码字,则 g_0 是 $g_{i_1},g_{i_2}\cdots,g_{i_m}$的一个线性组合,即 $g_0=\sum_{j=1}^{m}x_jg_{i_j}$,则秘密 s 通过计算 $s=\sum_{j=1}^{m}x_jt_{i_j}$可恢复,其中 $x_j\in F_q(1\leqslant j\leqslant m)$.

从定理 9 以及第一节中极小码字和极小线性码的讨论中,可以清楚地看出在所有的极小授权子集所组成的集合与线性码 C 的对偶码 $C^\perp$中的极小码字所组成的集合间有一一对应关系.所以,为了得到基于码 C 的秘密共享方案的存取结构,只需找到码 C 的对偶码中的极小码字.

4.2　基于极小线性码的对偶码上的秘密共享方案的存取结构

首先可将文献[9]中的定理 2 叙述如下:

定理 10　设 C 是一个$[n,k;q]$极小线性码,且设 $G=(g_0,g_1,\cdots,g_{n-1})_{k\times n}$是它的生成矩阵.则在基于 $C^\perp$的秘密共享方案中,存在 q^{k-1}个极小授权子集,且有如下结论

(*a*)如果 g_i 是 g_0 的倍数,$1\leqslant i\leqslant n-1$,则参与者 P_i 一定在每一个极小授权子集中.这样的参与者称作独裁参与者.

(*b*)如果 g_i 不是 g_0 的倍数,$1\leqslant i\leqslant n-1$,则参与者

P_i 一定出现在 q^{k-1} 个极小授权子集中的 $(q-1)q^{k-2}$ 个中.

由于对于不同的 N,不可约循环码 $C(q,m,N)$ 为极小线性码的条件已经讨论过,根据定理 10,可以得出:

定理 11 设码 C 是一个 $[n,k;2]$ 不可约循环码,并且是极小线性码.则基于 $C^{\perp}$ 上的秘密共享方案中,共有 2^{k-1} 个极小授权子集,且所有 $n-1$ 个参与者中的每一位都出现在 2^{k-1} 个极小授权子集中的 2^{k-2} 个中.也就是说该秘密共享方案没有独裁者.

证明 只需证明基于 $C^{\perp}$ 上的秘密共享方案无独裁者.即证码 $C^{\perp}$ 的极小距离至少为 3.假设码 $C^{\perp}$ 中有一个重量为 2 的码字,则存在两个不同的整数 $0\leqslant i\leqslant n-1, 0\leqslant j\leqslant n-1$ 使得 $Tr_{r/q}(\beta\theta^i)=Tr_{r/q}(\beta\theta^j)$ 对所有 $\beta\in F_r$ 均成立.从而 $\theta^i=\theta^j$,由码 C 的定义,则有 $i=j$,这与假设矛盾. 证毕

例 1 设 $N=3$,根据定理 5,$C(2,6,3)$ 是一个 $[21,6;2]$ 极小线性码.则基于 $C(2,6,3)^{\perp}$ 上的秘密共享方案中共有 32 个极小授权子集,如下:

{1,3,4,5,6,11,13,14,15,17,19}, {1,2,5,6,7,8,9,10,12,13,17}, {1,3,6,7,10,13,15},
{2,3,4,5,10,12,13,14,16,18,20}, {1,4,5,6,7,8,9,11,12,16,20}, {1,2,4,6,8,9,11,12,13,14,19},
{3,4,5,6,7,8,10,11,15,19,20}, {1,2,3,8,10,11,12,14,16,18,19}, {3,4,7,10,12,18,19},
{1,2,7,9,10,11,13,15,17,18,20}, {1,6,8,9,10,12,14,16,17,19,20}, {1,2,3,4,5,7,8,12,16,17,18},
{5,7,8,9,11,13,15,16,18,19,20}, {1,2,3,4,6,7,11,15,16,17,20}, {1,4,7,9,15,16,18},
{1,2,3,5,6,10,14,15,16,19,20}, {1,2,4,5,9,13,14,15,18,19,20}, {3,6,8,14,15,17,20},
{1,3,4,8,12,13,14,17,18,19,20}, {2,3,4,6,8,10,11,13,14,15,16}, {2,8,9,11,14,15,18},
{1,5,9,10,11,14,15,16,17,18,19}, {4,8,9,10,13,14,15,16,17,18,20}, {2,5,6,9,12,14,20},
{2,3,7,11,12,13,16,17,18,19,20}, {1,3,5,7,8,10,11,12,13,18,20}, {3,5,11,12,14,17,18},
{2,4,6,7,9,10,11,12,17,19,20}, {2,4,5,7,8,9,10,15,17,18,19}, {6,7,9,12,13,16,19},
{4,5,6,9,10,11,12,13,14,16,17}, {2,3,5,6,7,8,13,15,16,17,19}.

其中 {1,3,6,7,10,13,15} 表示的极小授权子集是 $\{P_1,P_3,P_6,P_7,P_{10},P_{13},P_{15}\}$.结合定理 11,每个参与者都在 32 个极小授权子集中的 16 个集合里,没有独裁者.

根据定理 1 和定理 2,例 1 中的极小线性码 $C(21)$ 的缩短码 $C(21,\cdots,21-i)[21-i-1](0\leqslant i\leqslant 3)$ 也是极小线性码.在此不妨令 $i=0$,可以通过编程得到码 $C(21)[20]$ 中的所有的极小码字,如下:

{1,1,0,1,1,1,1,0,0,0,0,1,0,1,1,1,0,1,0,1}, {1,1,1,0,0,1,1,1,1,1,1,0,1,1,0,0,0,1,0,0},
{1,1,0,1,0,0,1,1,0,0,1,0,0,1,0,1,0,0,0,0}, {1,1,1,1,0,0,0,0,1,0,1,1,1,0,1,0,1,0,1,1},
{1,0,0,1,1,0,0,1,0,0,1,0,1,0,0,0,0,0,1,1}, {1,1,1,1,1,1,0,1,1,0,0,0,1,0,0,0,1,1,1,0},
{1,1,0,0,1,0,0,1,0,1,0,0,0,0,0,1,1,0,1,0}, {1,0,0,1,0,1,0,0,0,0,0,1,1,0,1,0,0,1,1,0},
{1,0,1,1,1,0,1,0,1,0,1,1,0,1,1,1,1,0,0,0}, {1,1,0,0,0,1,0,0,0,1,1,1,0,0,1,1,1,1,1,1},
{1,1,1,0,1,0,1,0,1,1,0,1,1,1,1,0,0,0,0,1}, {1,0,1,0,0,0,0,0,1,1,0,1,0,0,1,1,0,0,1,0},
{1,0,0,0,0,0,1,1,0,1,0,0,1,1,0,0,1,0,0,1}, {1,0,1,1,0,1,1,1,1,0,0,0,0,1,0,1,1,1,1,1},
{1,0,0,0,1,1,1,0,0,1,1,1,1,1,1,0,1,1,0,0}, {1,0,1,1,0,1,1,1,1,0,0,0,0,1,0,1,1,1,0,1}.

故可得基于 $C(21)[20]^{\perp}$ 上的参与者人数为 19 的秘密共享方案的所有 16 个极小授权子集,且无独裁者.

定理 12 设码 C 是一个长度为 n,维数为 k 的 $C(3,m,2)$ 不可约循环码,并且是极小线性码.则基于 $C^{\perp}$ 上的秘密共享方案中,共有 3^{k-1} 个极小授权子集.如果 $2\nmid n$,则所有 $n-1$ 个参与者中的每一位都出现在 $2\cdot 3^{k-2}$ 个极小授权子集中;如果 $2\mid n$,则其中 $n-2$ 个参与者中的每一位都出现在 $2\cdot 3^{k-2}$ 个极小授权子集中,且存在一个独裁者 $P_{n/2}$.

证明 因为 g_i 是 g_0 的倍数当且仅当 $\theta^i\in F_3(0<i<n)$,且 $\theta=\alpha^2$,α 是 F_{3^m} 的一个本原元.即 $\mathrm{ord}(\alpha^{2i})\mid 2$,由于 $\mathrm{ord}(\alpha^{2i})=\dfrac{3^m-1}{(3^m-1,2i)}$ $3^m-1=(3^m-1,2i)$.如果 $3^m-1=(3^m-1,2i)$,矛盾.如果 $3^m-1=2(3^m-1,2i)$,且若 $2\mid n$,则 $i=\dfrac{n}{2}$.即参与者中的独裁者是 $P_{n/2}$. 证毕

例 2 设 $N=2$,根据定理 4,$C(3,4,2)$ 是一个 $[40,4;3]$ 极小线性码.则基于 $C(3,4,2)^{\perp}$ 上的秘密共享方案中共有 27 个极小授权子集,如下:

{1,2,3,4,5,6,7,8,9,12,14,15,16,18,20,21,22,23,24,25,26,27,28,29,32,34,35,36,38},
{2,3,4,5,6,7,8,9,10,11,14,16,17,18,20,22,23,24,25,26,27,28,29,30,31,34,36,37,38},

{2,4,5,6,7,8,9,10,11,12,13,16,18,19,20,22,24,25,26,27,28,29,30,31,32,33,36,38,39},
{1,4,5,6,7,9,10,12,16,17,19,20,21,24,25,26,27,29,30,32,36,37,39},
{1,2,4,6,7,8,9,10,11,12,13,14,15,18,20,21,22,24,26,27,28,29,30,31,32,33,34,35,38},
{1,2,5,6,7,8,10,11,13,17,18,20,21,22,25,26,27,28,30,31,33,37,38},
{1,3,4,5,8,9,10,11,13,14,16,20,21,23,24,25,28,29,30,31,33,34,36},
{3,5,6,7,9,11,12,13,14,15,16,17,18,19,20,23,25,26,27,29,31,32,33,34,35,36,37,38,39},
{1,4,6,7,8,10,12,13,14,15,16,17,18,19,20,21,24,26,27,28,30,32,33,34,35,36,37,38,39},
{1,2,3,6,8,9,10,12,14,15,16,17,18,19,20,21,22,23,26,28,29,30,32,34,35,36,37,38,39},
{2,6,7,9,10,11,14,15,16,17,19,20,22,26,27,29,30,31,34,35,36,37,39},
{1,3,7,8,10,11,12,15,16,17,18,20,21,23,27,28,30,31,32,35,36,37,38},
{1,2,3,4,5,6,9,11,12,13,15,17,18,19,20,21,22,23,24,25,26,29,31,32,33,35,37,38,39},
{1,2,3,4,5,6,7,10,12,13,14,16,18,19,20,21,22,23,24,25,26,27,30,32,33,34,36,38,39},
{2,3,5,9,10,12,13,14,17,18,19,20,22,23,25,29,30,32,33,34,37,38,39},
{1,2,3,4,5,6,7,8,11,13,14,15,17,19,20,21,22,23,24,25,26,27,28,31,33,34,35,37,39},
{1,3,4,6,10,11,13,14,15,18,19,20,21,23,24,26,30,31,33,34,35,38,39},
{1,2,4,5,7,11,12,14,15,16,19,20,21,22,24,25,27,31,32,34,35,36,39},
{1,2,3,5,6,8,12,13,15,16,17,20,21,22,23,25,26,28,32,33,35,36,37},
{3,4,5,6,8,9,11,15,16,18,19,20,23,24,25,26,28,29,31,35,36,38,39},
{1,3,5,6,7,8,9,10,11,12,13,14,17,19,20,21,23,25,26,27,28,29,30,31,32,33,34,37,39},
{2,3,4,6,8,9,10,11,12,13,14,15,16,17,20,22,23,24,26,28,29,30,31,32,33,34,35,36,37},
{2,3,4,7,8,9,10,12,13,15,19,20,22,23,24,27,28,29,30,32,33,35,39},
{1,2,5,7,8,9,11,13,14,15,16,17,18,19,20,21,22,25,27,28,29,31,33,34,35,36,37,38,39},
{4,5,7,8,9,12,13,14,15,17,18,20,24,25,27,28,29,32,33,34,35,37,38},
{1,2,3,4,7,9,10,11,13,15,16,17,18,19,20,21,22,23,24,27,29,30,31,33,35,36,37,38,39},
{1,2,3,4,5,8,10,11,12,14,16,17,18,19,20,21,22,23,24,25,28,30,31,32,34,36,37,38,39}.

结合定理 12,其中有 38 个参与者中的每一位都在 27 个极小授权子集中的 18 个集合里,有一个独裁者是 P_{20}.

根据定理 8,极小线性码 $C(3,4,2)$可构造极小线性码 $\bar{C}$.令式(3)中的 $l=20$,则 $\theta^{20}\in F_3$ 且 $\bar{C}=\{\overline{c_\beta}=(Tr_{3^4/3}(\beta),Tr_{3^4/3}(\beta\theta),\cdots,Tr_{3^4/3}(\beta\theta^{19}))\mid\beta\in F_{3^4}\}$是[20,4;3]极小线性码.可以通过编程得到 $\bar{C}$ 中所有的极小码字,如下:

{1,1,2,1,2,2,0,0,1,0,2,1,2,0,2,0,2,1,1,1},
{1,0,0,0,2,1,0,2,2,1,0,0,1,1,1,1,0,1,1,0},
{1,0,2,2,1,0,0,1,1,1,1,0,1,1,0,2,0,0,0,1},
{1,2,0,2,0,2,1,1,1,2,2,1,2,1,1,0,0,2,0,1},
{1,1,1,1,0,1,1,0,2,0,0,0,1,2,0,1,1,2,0,0},
{1,1,0,1,1,0,2,0,0,0,1,2,0,1,1,2,0,0,2,2},
{1,0,1,1,0,2,0,0,0,1,2,0,1,1,2,0,0,2,2,2},
{1,2,2,1,2,1,1,0,0,2,0,1,2,1,0,1,0,1,2,2},
{1,0,2,0,0,0,1,2,0,1,1,2,0,0,2,2,2,2,0,2},
{1,1,0,0,2,0,1,2,1,0,1,0,1,2,2,2,1,1,2,1},
{1,2,0,1,1,2,0,0,2,2,2,2,0,2,2,0,1,0,0,0},
{1,2,1,0,1,0,1,2,2,2,1,1,2,1,2,2,0,0,1,0},
{1,0,1,0,1,2,2,2,1,1,2,1,2,2,0,0,1,0,2,1},
{1,2,2,2,1,1,2,1,2,2,0,0,1,0,2,1,2,0,2,0},
{1,2,1,2,2,0,0,1,0,2,1,2,0,2,0,2,1,1,1,2 },
{1,2,2,0,0,1,0,2,1,2,0,2,0,2,1,1,1,2,2,1},
{1,0,2,1,2,0,2,0,2,1,1,1,2,2,1,2,1,1,0,0},
{1,0,0,1,1,1,1,0,1,1,0,2,0,0,0,1,2,0,1,1},
{1,1,1,0,1,1,0,2,0,0,0,1,2,0,1,1,2,0,0,2},
{1,1,1,2,2,1,2,1,1,0,0,2,0,1,2,1,0,1,0,1},
{1,1,2,2,1,2,1,1,0,0,2,0,1,2,1,0,1,0,1,2},
{1,1,0,2,0,0,0,1,2,0,1,1,2,0,0,2,2,2,2,0},
{1,2,1,1,0,0,2,0,1,2,1,0,1,0,1,2,2,2,1,1},
{1,0,0,2,0,1,2,1,0,1,0,1,2,2,2,1,1,2,1,2},
{1,1,2,0,0,2,2,2,2,0,2,2,0,1,0,0,0,2,1,0},
{1,2,0,0,2,2,2,2,0,2,2,0,1,0,0,0,2,1,0,2},
{1,0,1,2,2,2,1,1,2,1,2,2,0,0,1,0,2,1,2,0},

由例 1 和例 2 可以看出,基于极小线性码的对偶码上的秘密共享方案中的极小授权子集人数不再像(t,

故可得基于 $\bar{C}^{\perp}$上的参与者人数为 19 人的秘密共享方案的所有 27 个极小授权子集,且无独裁者.

n)门限那样单一.如例 1 中的极小授权子集所含人数在有些情况下为 11,而有些情况下为 7.

5 结论

本文提出了极小线性码这一概念,并研究了一类不可约循环码是极小线性码的判定条件.进一步,讨论了基于极小线性码的对偶码上的秘密共享方案及其存取结构.可以看出,建立在极小线性码上的秘密共享方案不仅是完善的,理想的,而且该方案的存取结构依码的重量分布的多样性而变得更加丰富,所对应秘密共享方案中的参与者更具民主性和权力性,也使得方案更具实用性.同时,由于利用极小线性码所构造方案的极小授权子集中含有的成员数目与极小码字的重量有关,所以研究三重量或三重量以上的极小线性码也是今后需要解决的问题.

参考文献

[1] Shamir A. How to share a secret. Communications of the ACM [J]. 1979, 24(11): 612 – 613.

[2] Blakley G R. Safeguarding cryptographickeys[A]. Proceedings of National Computer Conference[C]. Montvale, NJ: AFIPS Press, New York: 1979. 48: 313 – 317.

[3] 李大伟,杨庚,朱莉.一种基于身份加密的可验证秘密共享方案[J].电子学报,2010,38(9):2059 – 2065.
Li D W, Yang G. Zhu L. An ID based verifiable secret sharing scheme[J]. Acta Electronica Sinica, 2010, 38(9): 2059 – 2065. (in Chinese)

[4] Jin Y, Ding C S. Secret sharing schemes from three classes of linear codes[J]. IEEE Trans. Inform. Theory, 2006, 52(1): 206 – 212.

[5] 温晓军,田原,牛夏牧.一种基于秘密共享的量子强盲签名协议[J].电子学报,2010,38(3):720 – 724.
Wen X J, Tian Y, Niu X M. A strong blind quantum signature protocol based on secret sharing[J]. Acta Electronica Sinica, 2010, 38(3): 720 – 724. (in Chinese)

[6] Stinson D R. Cryptography Theory and Practice[M]. 3rd ed, UnitedStates: 2009.

[7] Massey J L. Minimal codewords and secret sharing[A]. The 6th Joint Swedish-Russian Workshop on Information Theory [C]. Netherlands: Veldhoven, 1993. 276 – 279.

[8] Massey J L. Some Applications of Coding Theory in Cryptography [M]. Cryptography and Coding IV, England: Formara Ltd, 1995: 33 – 47.

[9] Ding C S, Jin Y. Covering and secret sharing with linear codes [A]. Discrete Mathematics and Theoretical Computer Science: Lecture Notes in Computer Science[C]. Berlin: Springer Verlag, 2003. 2731: 11 – 25.

[10] Li Z H, Xue T, Lai H. Secret sharing schemes from binary linear codes[J]. Information Science, 2011, 180(22): 4412 – 4419.

[11] Ding C S. The weight distribution of some irreducible cyclic codes[J]. IEEE Trans Inform Theory, 2009, 55(3): 955 – 960.

[12] Vega G, Wolfmann J. New classes of 2-weight cyclic codes [J]. Designs, Codes and Cryptography, 2007, 42(3): 327 – 334.

作者简介

宋 云 女,1987 年生于陕西西安,陕西师范大学数学与信息科学学院博士研究生.研究方向为有限域、密码学.
E-mail: songyun19871109@yahoo.com.cn

李志慧(通讯作者) 女,1966 年生于陕西眉县,陕西师范大学数学与信息科学学院教授.目前研究方向为有限域,代数编码以及密码学方面等.
E-mail: snnulzh@yahoo.com.cn