Sidon 空间和循环子空间码的构造

刘雪梅,张佳瑢

(中国民航大学 理学院,天津 300300)

摘 要:子空间码特别是循环子空间码在随机网络编码中具有高效的编码和译码算法,因此近年来受到了广泛关注.Sidon 空间是构造循环子空间码的重要工具,利用有限域上的本原元和不可约多项式的根,构造了不同维数的 Sidon 空间,并在此基础上得到了码字个数更多的循环子空间码.

关键词:有限域;循环子空间码;Sidon 空间;不可约多项式的根

中图分类号:O157.4 **文献标志码**:A **文章编号**:1000-2367(2025)03-0066-06

子空间码,尤其是循环子空间码具有高效的编码和译码算法,在随机网络编码[1-2]中得到了广泛的应用.近年来,文献[3-4]研究了子空间码的构造方法,因此对于给定的 n,k,q,寻找码字个数和最小距离尽可能大的循环子空间码也成为数学研究者关注的重点之一.目前,研究循环子空间码主要有两种思路:一种是通过线性化多项式构造循环子空间码,如文献[5]使用线性化多项式 $x^{q^k}+x^q+x\in F_q[x]$ 构造出码字个数为 $\frac{q^n-1}{q-1}$,最小距离为 $2k-2$ 的循环子空间码.更多的用线性化多项式构造循环子空间码的方法,可参考文献[6-8].另一种思路是用 Sidon 空间构造循环子空间码.ROTH 等[9]提出了 Sidon 空间的概念,并找到了 Sidon 空间与循环子空间码之间的关系.文献[10]利用 Sidon 空间的并集来构造具有更多码字的循环子空间码,且最小距离仍然为 $2k-2$.文献[11]给出了几个 Sidon 空间的直和仍然是 Sidon 的充分条件,为构造 Sidon 空间提供了新的思路.有关 Sidon 空间构造循环子空间码的更多方法,可参考文献[12-13].本文利用有限域上的本原元和不可约多项式的根构造了一些新的 Sidon 空间,进而得到了新的循环子空间码,并在此基础上得到了码字个数更多且最小距离仍为 $2k-2$ 的循环子空间码.

1 预备知识

首先介绍 Sidon 空间和循环子空间码的相关概念及主要结论.设 F_q 是含有 q 个元素的有限域,q 为素数方幂,F_{q^n} 是 F_q 上扩张次数为 n 的有限域,那么 F_{q^n} 可看作是 F_q 上的 n 维向量空间.令 $P_q(n)$ 表示 F_{q^n} 的所有子空间集合,对任意的 $U,V\in P_q(n)$,定义子空间距离:

$$d(U,V)=\dim U+\dim V-2\dim(U\cap V),$$

称上面具有度量的集合 $P_q(n)$ 为一个度量空间.设 $G_q(n,k)$ 表示 F_{q^n} 的所有 k 维子空间集合,若 $C\subseteq G_q(n,k)$ 是非空子集,称 C 是一个常维子空间码,则对 $U,V\in C$,码 C 中码字之间的距离为:

$$d(U,V)=2k-2\dim(U\cap V).$$

收稿日期:2024-01-16;**修回日期**:2024-11-25.

基金项目:国家自然科学基金(11701558);天津市教委科研计划重点项目(2023ZD041).

作者简介(通信作者):刘雪梅(1977-),女,黑龙江哈尔滨人,中国民航大学教授,研究方向为代数组合、编码与密码,E-mail:xm-liu771216@163.com.

引用本文:刘雪梅,张佳瑢.Sidon 空间和循环子空间码的构造[J].河南师范大学学报(自然科学版),2025,53(3):66-71.(Liu Xuemei,Zhang Jiarong.Constructions of Sidon spaces and cyclic subspace codes[J].Journal of Henan Normal University(Natural Science Edition),2025,53(3):66-71.DOI:10.16366/j.cnki.1000-2367.2024.01.16.0001.)

对于任意的子空间 $V \in G_q(n,k)$ 和 $\alpha \in F_{q^n}^*$,V 的循环移位为 $\alpha(V)=\{\alpha v \mid v \in V\}$,显然 αV 仍是子空间且维数与 V 相同,V 的轨道记为 $O(V)=\{\alpha V \mid \alpha \in F_{q^n}^*\}$,那么 $O(V)$ 是一个循环子空间码.称码字个数为 $\frac{q^n-1}{q-1}$,最小距离为 $2k-2$ 的循环子空间码为最优循环子空间码.

文献[9]提出对于 $G_q(n,k)$ 中的子空间 V,V 的循环移位是最优循环子空间码的充要条件为 V 是 Sidon 空间,因此 Sidon 空间是构造循环子空间码的重要工具,下面给出 Sidon 空间的定义及性质.

定义 1[14]　设子空间 $V \in G_q(n,k)$,对任意的非零元素 $a,b,c,d \in V$,若 $ab=cd$,那么有 $\{aF_q,bF_q\}=\{cF_q,dF_q\}$. 则称子空间 V 是一个 Sidon 空间.

定理 1[9]　子空间 $V \in G_q(n,k)$,$C=\{\alpha V \mid \alpha \in F_{q^n}^*\}$ 是大小为 $\frac{q^n-1}{q-1}$、最小距离为 $2k-2$ 的循环子空间码,当且仅当 V 是一个维数为 k 的 Sidon 空间.

定理 1 表明可以通过构造 Sidon 空间,进一步构造最优循环子空间码.

定理 2[9]　对于任意不同的子空间 $U,V \in G_q(n,k)$,下面两个条件等价:

(1)对任意的 $\alpha \in F_{q^n}^*$,$\dim(U \cap \alpha V) \leq 1$;

(2)对任意非零元 $a,c \in U$ 和非零元 $b,d \in V$,若 $ab=cd$,那么有 $\{aF_q\}=\{cF_q\}$ 且 $\{bF_q\}=\{dF_q\}$.

定理 3[15-16]　对任意正整数 n,k 且 $n>2k$,存在循环子空间码 $C \subseteq G_q(n,k)$,大小为 $\frac{q^n-1}{q-1}$,最小距离为 $2k-2$.

定理 4[13]　设 l,k 是正整数且 $\gcd(l,k)=1$,u,u',v,v' 是 F_{q^k} 上的非零元素,满足 $uv=u'v'$.若 $u^{q^l}v=u'^{q^l}v'$,那么 $\frac{u}{u'}=\frac{v'}{v} \in F_q^*$.

2　Sidon 空间和循环子空间码的构造

首先给出 Sidon 空间的构造,由定理 1,可得到对应的新的循环子空间码.

引理 1　设 u,v,u',v' 是 F_{q^k} 上的非零元素使得 $uv=u'v'$,并且 $uv^q+u^qv=u'v'^q+u'^qv'$.那么 $\frac{u}{v'}=\frac{u'}{v} \in F_q^*$.

证明　令 $\frac{u}{u'}=\frac{v'}{v}=\tau \in F_{q^k}^*$,则 $u=\tau u'$,$v'=\tau v$,结合等式 $uv^q+u^qv=u'v'^qu'^qv'$,有

$$\tau u'v^q+\tau^q u'^q v=\tau^q u'v^q+\tau u'^q v,$$

于是 $(\tau-\tau^q)u'v^q=(\tau-\tau^q)u'^q v$,即 $(\frac{u'}{v})^{q-1}=1$,因此 $\frac{u'}{v} \in F_q^*$.

引理 2　设 k,l 是正整数且 $\gcd(k,l)=1$,u,u',v,v' 是 F_{q^k} 上的非零元素使得 $uv=u'v'$,并且 $uv^{q^l}+u^{q^l}v=u'v'^{q^l}+u'^{q^l}v'$.那么 $\frac{u}{v'}=\frac{u'}{v} \in F_q^*$.

证明　结合引理 1 的证明,易知.

引理 3　设 k,l 是正整数且 $\gcd(k,l)=1$,a,a',b,b' 是 F_{q^l} 上的非零元素,满足 $ab=a'b'$,u,u',v,v' 是 F_{q^k} 上的非零元素使得 $uv=u'v'$.如果 $av+bu=a'v'+b'u'$,则 $\frac{u}{v'}=\frac{u'}{v}=\frac{a'}{b}=\frac{a}{b'} \in F_q^*$.

证明　令 $\frac{u}{u'}=\frac{v'}{v}=\tau \in F_{q^k}^*$,$\frac{a}{a'}=\frac{b'}{b}=\lambda \in F_{q^l}^*$,那么 $a=\lambda a'$,$b'=\lambda b$,$u=\tau u'$,$v'=\tau v$,则有 $\lambda a'v+\tau bu'=\tau a'v+\lambda bu'$,于是 $(\lambda-\tau)a'v=(\lambda-\tau)bu'$,则有 $\frac{a'}{b}=\frac{u'}{v}$.因为 $\gcd(k,l)=1$,所以 $\frac{a'}{b}=\frac{u'}{v} \in F_q^*$.

引理 4 设 k,l 是正整数且 $\gcd(k,l)=1$,a,a',b,b' 是 F_{q^l} 上的非零元素使得 $ab=a'b'$,u,u',v,v' 是 F_{q^k} 上的非零元素,使得 $uv=u'v'$.如果 $av=a'v'$,则 $\frac{a}{a'}=\frac{v'}{v}\in F_q^*$.

证明 结合引理 3 的证明,易知.

设 ω 是 F_{q^k} 上的本原元,$\gamma\in F_{q^n}^*$ 是 F_{q^k} 上次数为 $\frac{n}{k}(k\mid n)$ 的不可约多项式的根,记:$\gamma_{ij}=\omega^i\gamma^j$.

定理 5 设 k,n 为正整数且 $k\mid n$,$n\geq 5k$.设 s,t 为非负整数满足 $st\neq 0$,$\gcd(k,t-s)=1$.令 $\rho=\lceil\frac{n}{4k}\rceil-1$,对于给定的整数 i,j,其中 $0\leq i\leq q^k-2$,$1\leq j\leq\rho$,,令 $U_{ij}=\{u+u^{q^s}\gamma_{ij}+u^{q^t}\gamma_{ij}^2\mid u\in F_{q^k}\}$,则 U_{ij} 是一个维数为 k 的 Sidon 空间.

证明 设 $\alpha=u+u^{q^s}\gamma_{ij}+u^{q^t}\gamma_{ij}^2$,$\alpha'=u'+u'^{q^s}\gamma_{ij}+u'^{q^t}\gamma_{ij}^2$,$\beta=v+v^{q^s}\gamma_{ij}+v^{q^t}\gamma_{ij}^2$,$\beta'=v'+v'^{q^s}\gamma_{ij}+v'^{q^t}\gamma_{ij}^2$ 是 U_{ij} 中的非零元素,其中 $u,u',v,v'\in F_{q^k}$,且 $\alpha\beta=\alpha'\beta'$.根据 Sidon 空间的定义,只需证明 $\{\alpha F_q,\beta F_q\}=\{\alpha' F_q,\beta' F_q\}$. 由已知可得:

$$(u+u^{q^s}\gamma_{ij}+u^{q^t}\gamma_{ij}^2)(v+v^{q^s}\gamma_{ij}+v^{q^t}\gamma_{ij}^2)=uv+(uv^{q^s}+u^{q^s}v)\gamma_{ij}+(uv+uv^{q^t}+u^{q^t}v)\gamma_{ij}^2+(u^{q^s}v^{q^t}+u^{q^t}v^{q^s})\gamma_{ij}^3+(uv)^{q^t}\gamma_{ij}^4,$$

$$(u'+u'^{q^s}\gamma_{ij}+u'^{q^s}\gamma_{ij}^2)(v'+v'^{q^s}\gamma_{ij}+v'^{q^s}\gamma_{ij}^2)=u'v'+(u'v'^{q^s}+u'^{q^s}v')\gamma_{ij}+(u'v'+u'v'^{q^t}+u'^{q^t}v')\gamma_{ij}^2+(u'^{q^s}v'^{q^t}+u'^{q^t}v'^{q^s})\gamma_{ij}^3+(u'v')^{q^t}\gamma_{ij}^4.$$

由 $n\geq 5k$,$\rho=\lceil\frac{n}{4k}\rceil-1$,$1\leq j\leq\rho$ 知 $\{1,\gamma^j,\gamma^{2j},\gamma^{3j},\gamma^{4j}\}$ 在 F_q 上是线性无关的,化简得:

$$\begin{cases}uv=u'v',\\ uv^{q^s}+u^{q^s}v=u'v'^{q^s}+u'^{q^s}v',\\ uv^{q^t}+u^{q^t}v=u'v'^{q^t}+u'^{q^t}v',\\ u^{q^s}v^{q^t}+u^{q^t}v^{q^s}=u'^{q^s}v'^{q^t}+u'^{q^t}v'^{q^s},\end{cases}\tag{1}$$

根据 $uv=u'v'$,可令 $\frac{u}{u'}=\frac{v'}{v}=\lambda\in F_{q^k}^*$,由 $u=\lambda u'$,$v'=\lambda v$,再结合式(1)中的第 4 个等式,有 $\lambda^{q^{t-s}}u'^{q^{t-s}}v+\lambda u'v^{q^{t-s}}=\lambda u'^{q^{t-s}}v+\lambda^{q^{t-s}}u'v^{q^{t-s}}$,于是 $(\lambda^{q^{t-s}}-\lambda)u'^{q^{t-s}}v=(\lambda^{q^{t-s}}-\lambda)u'v^{q^{t-s}}$,整理得 $(\frac{u'}{v})^{q^{t-s}-1}=1$,从而 $\frac{u'}{v}\in F_{q^{t-s}}$.因为 $\gcd(k,t-s)=1$,所以 $\frac{u'}{v}\in F_q$,结合 $uv=u'v'$,$\alpha\beta=\alpha'\beta'$,易得 $\frac{\alpha}{\beta'}=\frac{\alpha'}{\beta}\in F_q$.

推论 1 当 $s=0$ 时,$\gcd(k,t)=1$,对于固定的 $0\leq i\leq q^k-2$,$1\leq j\leq\rho$,$U_{ij}=\{u+u\gamma_{ij}+u^{q^t}\gamma_{ij}^2\mid u\in F_{q^k}\}$ 是维数为 k 的 Sidon 空间.

定理 6 设 k,n 为正整数且满足 $k\mid n$,$n\geq 5k$.设 $\gamma\in F_{q^n}^*$ 是 F_{q^k} 上次数为 $\frac{n}{k}$ 的不可约多项式的根,令 $\gamma_j=\gamma^j$,$\rho=\lceil\frac{n}{4k}\rceil-1$,对于给定的整数 j,其中 $1\leq j\leq\rho$.令 $U_{q^k-1,j}=\{u+u^q\gamma_j^2\mid u\in F_{q^k}\}$,那么 $U_{q^k-1,j}$ 是维数为 k 的 Sidon 空间.

证明 结合定理 5 的证明,易知.

文献[9]中提出任何 Sidon 空间的子空间也是 Sidon 空间,因此,对任意的 $1\leq t\leq k$,$G_q(n,t)$ 中也存在 Sidon 空间.下面增加 k 值,构造维数更大的 Sidon 空间,从而可对应新的循环子空间码.

定理 7 设 k,n,l 为正整数,$kl\mid n$ 且 $\gcd(k,l)=1$,设 $\gamma\in F_{q^n}^*$ 是 $F_{q^{lk}}$ 上次数为 $\frac{n}{lk}>9$ 的不可约多项式的根,令 $U=\{a+a^q\gamma+u^{q^l}\gamma^2+u\gamma^4\mid a\in F_{q^l},u\in F_{q^k}\}$,那么 U 是维数为 $k+l$ 的 Sidon 空间.

证明 设 $\alpha=a+a^q\gamma+u^{q^l}\gamma^2+u\gamma^4$,$\alpha'=a'+a'^q\gamma+u'^{q^l}\gamma^2+u'\gamma^4$,$\beta=b+b^q\gamma+v^{q^l}\gamma^2+v\gamma^4$ 和 $\beta'=$

$b'+b'^{q}\gamma+v'^{q^l}\gamma^2+v'\gamma^4$ 是 U 中非零元素,其中 $u,u',v,v'\in F_{q^k}$,$a,a',b,b'\in F_{q^l}$ 且 $\alpha\beta=\alpha'\beta'$.根据 Sidon 空间的定义,只需证明 $\{\alpha F_q,\beta F_q\}=\{\alpha' F_q,\beta' F_q\}$. 由已知得:

$$(a+a^q\gamma+u^{q^l}\gamma^2+u\gamma^4)(b+b^q\gamma+v^{q^l}\gamma^2+v\gamma^4)=ab+(ab^q+a^qb)\gamma+(a^qb^q+av^{q^l}+bu^{q^l})\gamma^2+$$
$$(a^qv^{q^l}+b^qu^{q^l})\gamma^3+(av+bu+u^{q^l}v^{q^l})\gamma^4+(a^qv+b^qu)\gamma^5+(uv^{q^l}+u^{q^l}v)\gamma^6+uv\gamma^8,$$
$$(a'+a'^{q}\gamma+u'^{q^l}\gamma^2+u'\gamma^4)(b'+b'^{q}\gamma+v'^{q^l}\gamma^2+v'\gamma^4)=a'b'+(a'b'^{q}+a'^{q}b'\gamma+(a'^{q}b'^{q}+a'v'^{q^l}+b'u'^{q^l})\gamma^2+$$
$$(a'^{q}v'^{q^l}+b'^{q}u'^{q^l})\gamma^3+(a'v'+b'u'+u'^{q^l}v'^{q^l})\gamma^4+(a'^{q}v'+b'^{q}u')\gamma^5+(u'v'^{q^l}+u'^{q^l}v')\gamma^6+u'v'\gamma^8.$$

由 $\frac{n}{lk}>9$ 可知 $\{1,\gamma,\gamma^2,\gamma^3,\gamma^4,\gamma^5,\gamma^6,\gamma^8\}$ 在 $F_{q^{lk}}$ 上是线性无关的,化简可得

$$\begin{cases} ab=a'b', \\ ab^q+a^qb=a'b'^{q}+a'^{q}b', \\ av^{q^l}+bu^{q^l}=a'v'^{q^l}+b'u'^{q^l}, \\ a^qv^{q^l}+b^qu^{q^l}=a'^{a}v'^{q^l}+b'^{q}u'^{q^l}, \\ av+bu=a'v'+b'u', \\ u^{q^l}v+uv^{q^l}=u'^{q^l}v'+u'v'^{q^l}, \\ a^qv+b^qu=a'^{q}v'+b'^{q}u', \\ uv=u'v'. \end{cases} \tag{2}$$

考虑以下几种情况.

情况 1　$ab\neq0,uv\neq0$.结合式(2)中第 1、5、8 个等式及引理 3 可得 $\frac{u'}{v}=\frac{a'}{b}\in F_q$,所以 $\frac{\alpha}{\beta'}=\frac{\alpha'}{\beta}\in F_q$.

情况 2　$ab\neq0,uv=0$.

1)u,u',v,v' 中有 1 个或 3 个元素为零显然不成立.

2)如果 u,u',v,v' 中有两个元素为零时,不妨设 $u=u'=0,v,v'\neq0$.式(2)中的第 5 个方程变为 $av=a'v'$,由引理 4 得 $\frac{a}{a'}=\frac{v'}{v}\in F_q$,所以 $\frac{\alpha}{\beta'}=\frac{\alpha'}{\beta}\in F_q$.

3) $u=u'=v=v'=0$,则 $\alpha=a+a^q\gamma,\alpha'=a'+a'^{q}\gamma,\beta=b+b^q\gamma,\beta'=b'+b'^{q}\gamma$.令 $\frac{a}{a'}=\frac{b'}{b}=\lambda=F_{ql}$.(a) 若 $\lambda\in F_q$,容易得出 $\frac{\alpha}{\beta'}=\frac{\alpha'}{\beta}\in F_q$.(b) 若 $\lambda\notin F_q$,由 $a=\lambda a',b'=\lambda b$,再结合式(2)的第 2 个等式及引理 1 可得 $\frac{a'}{b}\in F_q$,所以 $\frac{\alpha}{\beta'}=\frac{\alpha'}{\beta}\in F_q$.

情况 3　$ab=0,uv\neq0$.

1)u,u',v,v' 中有 1 个或 3 个元素为零显然不成立.

2)如果 a,a',b,b' 中有两个元素为零时,不妨设 $a=a'=0,b,b'\neq0$.式(2)中第 5 个等式变为 $bu=b'u'$,由引理 4 得 $\frac{b}{b'}=\frac{u'}{u}\in F_q$,所以 $\frac{\alpha}{\alpha'}=\frac{\beta'}{\beta}\in F_q$.

3) $a=a'=b=b'=0$,则 $\alpha=u^{q^l}\gamma^2+u\gamma^4,\alpha=u'^{q^l}\gamma^2+u'\gamma^4,\beta=v^{q^l}\gamma^2+v\gamma^4,\beta'=v'^{q^l}\gamma^2+v'\gamma^4$.令 $\frac{u}{u'}=\frac{v'}{v}=\tau\in F_{qk}$.(a) 若 $\tau\in F_q$,容易得出 $\frac{\alpha}{\alpha'}=\frac{\beta'}{\beta}\in F_q$.(b) 若 $\tau\notin F_q$,结合式(2)的第 6 个等式及引理 2 得 $\frac{u'}{v}\in F_q$,所以 $\frac{\alpha}{\beta'}=\frac{\alpha'}{\beta}\in F_q$.

情况 4　$ab=0,uv=0$.不妨设 $a=a'=v=v'=0,b,b',u,u'\neq0$.式(2)的第 2 个等式变为 $bu=b'u'$,由引理 4 得 $\frac{b}{b'}=\frac{u'}{u}\in F_q$,所以 $\frac{\alpha}{\alpha'}=\frac{\beta'}{\beta}\in F_q$.

综上,U 是 $k+l$ 维 Sidon 空间.

接下来利用推论 1 及定理 6 中的 Sidon 空间构造码字个数更多的循环子空间码.

定理 8 设 $U_{ij}=\{u+u\gamma_{ij}+u^{q^t}\gamma_{ij}^2 \mid u\in F_{q^k}\}$ 是推论 1 定义的 Sidon 空间,$U_{q^k-1,j}=\{u+u^q\gamma_j^2 \mid u\in F_{q^k}\}$ 是定理 6 定义的 Sidon 空间.定义 $C_{ij}=\{\alpha U_{ij} \mid \alpha\in F_{q^n}\}$,其中 $0\le i\le q^k-1,1\le j\le\rho$.令 $C=\bigcup\limits_{j=1}^{\rho}\bigcup\limits_{i=0}^{q^k-1}C_{ij}$,则 C 是码字个数为 $\dfrac{\rho q^k(q^n-1)}{q-1}$,最小距离为 $2k-2$ 的循环子空间码.

证明 由定理 1 得,对任意的 $0\le i\le q^k-1,1\le j\le\rho$,$C_{ij}$ 是码字个数为 $\dfrac{q^n-1}{q-1}$,最小距离为 $2k-2$ 的循环子空间码,从而 $|C|=\dfrac{\rho q^k(q^n-1)}{q-1}$.下面证明 C 的最小距离是 $2k-2$,由定理 2 只需证明对任意的 $\alpha\in F_{q^n}^*$,$0\le i_1,i_2\le q^k-1,1\le j_1,j_2\le\rho$ 且 $(i_1,j_1)\ne(i_2,j_2)$,$\dim(U_{i_1j_1}\cap\alpha U_{i_2j_2})\le 1$ 成立.

若 $0\le i_1,i_2\le q^k-2$,令 $\alpha=u+u\gamma_{i_1j_1}+u^{q^t}\gamma_{i_1j_1}^2$,$\alpha'=u'+u'\gamma_{i_1j_1}+u'^{q^t}\gamma_{i_1j_1}^2$ 是 $U_{i_1j_1}$ 中的非零元素,$\beta=v+v\gamma_{i_2j_2}+v^{q^t}\gamma_{i_2j_2}^2$,$\beta'=v'+v'\gamma_{i_2j_2}+v'^{q^t}\gamma_{i_2j_2}^2$ 是 U_{i_2,j_2} 中的非零元素使得 $\alpha\beta=\alpha'\beta'$,其中 $u,u',v,v'\in F_{q^k}^*$. 考虑以下情况.

情况 1 $j_1\ne j_2$.因为 $\rho=\lceil\dfrac{n}{4k}\rceil-1,1\le j_1,j_2\le\rho$,则 $\{1,\gamma^{j_1},\gamma^{j_2},\gamma^{j_1+j_2},\gamma^{j_1+2j_2},\gamma^{2j_1+j_2},\gamma^{2j_1+2j_2}\}$ 在 F_{qk} 上线性无关,将 $\alpha\beta=\alpha'\beta'$ 展开并将其对应项的系数比较化简,得到

$$uv=u'v',uv^{q^t}=u'v'^{q^t},u^{q^t}v=u'^{q^t}v'.$$

由定理 4 得 $\dfrac{u}{u'}=\dfrac{v'}{v}\in F_q^*$,所以 $\dfrac{\alpha}{\alpha'}=\dfrac{\beta'}{\beta}\in F_q$.

情况 2 $j_1=j_2=j$.因为 $\rho=\lceil\dfrac{n}{4k}\rceil-1,1\le j_1,j_2\le\rho$,所以 $\{1,\gamma^j,\gamma^{2j},\gamma^{3j},\gamma^{4j}\}$ 在 F_{qk} 上线性无关,将 $\alpha\beta=\alpha'\beta'$ 展开并将其对应项的系数比较化简,得到 $uv=u'v',uv^{q^t}+u^{q^t}v=u'v'^{q^t}+u'^{q^t}v'$.由引理 2 得 $\dfrac{u}{u'}=\dfrac{v'}{v}\in F_q^*$,所以 $\dfrac{\alpha}{\alpha'}=\dfrac{\beta'}{\beta}\in F_q$.

若 $0\le i_i\le q^k-2,i_2=q^k-1$,令 $\alpha=u+u\gamma_{i_1j_1}+u^{q^t}\gamma_{i_1j_1}^2$,$\alpha'=u'+u'\gamma_{i_1j_1}+u'^{q^t}\gamma_{i_1j_1}^2$ 是 $U_{i_1j_1}$ 中的非零元素,$\beta=v+v^q\gamma_{j_2}^2$,$\beta'=v'+v'^q\gamma_{j_2}^2$ 是 U_{q^k-1,j_2} 中的非零元素使得 $\alpha\beta=\alpha'\beta'$,其中 $u,u',v,v'\in F_{q^k}^*$. 考虑以下情况.

情况 1 $j_1\ne j_2$.因为 $\rho=\lceil\dfrac{n}{4k}\rceil-1,1\le j_1,j_2\le\rho$,所以 $\{1,\gamma^{j_1},\gamma^{2j_1},\gamma^{2j_2},\gamma^{j_1+j_2},\gamma^{j_1+2j_2},\gamma^{2j_1+2j_2}\}$ 在 F_{qk} 上线性无关,将 $\alpha\beta=\alpha'\beta'$ 展开并将其对应项的系数比较化简,得到

$$\begin{cases}uv=u'v',\\uv^{q^t}=u'v'^{q^t},\\uv^q=u'v'^q,\\u^{q^t}v^q=u'^{q^t}v'^q.\end{cases}$$

由定理 4 得 $\dfrac{u}{u'}=\dfrac{v'}{v}\in F_q^*$,所以 $\dfrac{\alpha}{\alpha'}=\dfrac{\beta'}{\beta}\in F_q$.

情况 2 $j_1=j_2=j$.因为 $\rho=\lceil\dfrac{n}{4k}\rceil-1,1\le j_1,j_2\le\rho$,所以 $\{1,\gamma^j,\gamma^{2j},\gamma^{3j},\gamma^{4j}\}$ 在 F_{qk} 上线性无关,将 $\alpha\beta=\alpha'\beta'$ 展开并将其对应项的系数比较化简,得到

$$\begin{cases}uv=u'v',\\uv^{q^t}+u^{q^t}v=u'v'^{q^t}+u'^{q^t}v'.\end{cases}$$

由引理 2 得 $\frac{u}{u'}=\frac{v'}{v}\in F_q^*$，所以 $\frac{\alpha}{\alpha'}=\frac{\beta'}{\beta}\in F_q$.

综上，C 是码字个数为 $\frac{\rho q^k(q^n-1)}{q-1}$，最小距离为 $2k-2$ 的循环子空间码.

3　结　论

文章利用有限域上的本原元和不可约多项式的根构造了维数为 k 和 $k+1$ 的 Sidon 空间，进而可得到对应的循环子空间码.在此基础上，利用所构造 Sidon 空间得到了码字个数为 $\frac{\rho q^k(q^n-1)}{q-1}$，最小距离仍为 $2k-2$ 的循环子空间码，在最小距离不变的前提下，增加了循环子空间码的码字个数.

参　考　文　献

[1] AHLSWEDE R，CAI N，LI SYR.Network information flow[J].IEEE Transactions on Information Theory，2000，46(4)：1204-1216.

[2] 董赞强，沈苏彬.网络编码研究综述[J].南京邮电大学学报(自然科学版)，2012，32(3)：66-75.
DONG Z Q，SHEN S B.The survey on network coding research[J].Journal of Nanjing University of Posts and Telecommunications(Natural Science)，2012，32(3)：66-75.

[3] 郭军，李凤高.基于辛空间中全迷向子空间的纠错码(英文)[J].数学进展，2017，46(6)：919-931.
GUO J，LI F G.Error-correcting codes based on totally isotropic subspaces in symplectic spaces[J].Advances in Mathematics(China)，2017，46(6)：919-931.

[4] 李超，冯克勤，胡卫群.一类性能好的线性码的构造[J].电子学报，2003，31(1)：51-53.
LI C，FENG K Q，HU W Q.Construction of A class of linear codes with good parameters[J].Acta Electronica Sinica，2003，31(1)：51-53.

[5] BEN-SASSON E，KOPPARTY S，RADHAKRISHNAN J.Subspace polynomials and limits to list decoding of reed-Solomon codes[J].IEEE Transactions on Information Theory，2010，56(1)：113-120.

[6] CHEN B C，LIU H W.Constructions of cyclic constant dimension codes[J].Designs，Codes and Cryptography，2018，86(6)：1267-1279.

[7] OTAL K，ÖZBUDAK F.Cyclic subspace codes via subspace polynomials[J].Designs，Codes and Cryptography，2017，85(2)：191-204.

[8] ZHAO W，TANG X L.A characterization of cyclic subspace codes via subspace polynomials[J].Finite Fields and Their Applications，2019，57：1-12.

[9] ROTH R M，RAVIV N，TAMO I.Construction of Sidon spaces with applications to coding[J].IEEE Transactions on Information Theory，2018，64(6)：4412-4422.

[10] NIU Y F，YUE Q，WU Y S.Several kinds of large cyclic subspace codes v_1a Sidon spaces[J].Discrete Mathematics，2020，343(5)：111788.

[11] LI Y，LIU H W.Cyclic subspace codes via the sum of Sidon spaces[EB/OL].[2024-01-03].https://arxiv.org/abs/2105.12520v1.

[12] ZHANG H，CAO X W.Constructions of Sidon spaces and cyclic subspace codes[J].Frontiers of Mathematics in China，2022，17：275-288.

[13] FENG T，WANG Y.New constructions of large cyclic subspace codes and Sidon spaces[J].Discrete Math，2021，344(4)：112273.

[14] BACHOC C，SERRA O，ZEMOR G.An analogue of Vosper's theorem for extension fields[C].Mathematical Proceedings of the Cambridge Philosophical Society，2017，163(3)：423-452.

[15] GLUESING-LUERSSEN H，MORRISON K，TROHA C.Cyclic orbit codes and stabilizer subfields[J].Advances in Mathematics of Communications，2015，9(2)：177-197.

[16] FENG T，WANG Y.New constructions of large cyclic subspace codes and Sidon spaces[J].Discrete Math，2021，344(4)：112273.

Constructions of Sidon spaces and cyclic subspace codes

Liu Xuemei，Zhang Jiarong

(College of Science，Civil Aviation University of China，Tianjin 300300，China)

Abstract：Subspace codes，especially cyclic subspace codes，have attracted much attention in recent years due to their efficient coding and decoding algorithms in random network coding. Sidon space is an important tool for constructing cyclic subspace codes. In this paper，by using primitive elements and the root of irreducible polynomial over finite fields，we give a new construction of Sidon spaces with different dimensions，obtaining a new cyclic subspace code based on them.

Keywords：finite fields；cyclic subspace code；Sidon space；the root of irreducible polynomial

[责任编校　陈留院　杨浦]