doi：10.13413/j.cnki.jdxblxb.2025208

基于子空间多项式的循环子空间码的构造

张嘉璇，金 永，黄紫芯
（中国民航大学 理学院，天津 300300）

摘要：首先，针对子空间轨道长度与子空间多项式指数之间联系的结论，给出一较简洁的证明；其次，通过对子空间做 Frobenius 移位与合并循环子空间码，得到码字个数更多 $\left(rn\dfrac{q^N-1}{q-1}\right)$、极小距离为 $2k-2$ 的循环子空间码；最后，给出构造循环子空间码的实例.

关键词：循环子空间码；子空间多项式；Frobenius 移位；轨道
中图分类号：O157.4 **文献标志码**：A **文章编号**：1671-5489(2026)02-0251-07

Construction of Cyclic Subspace Codes Based on Subspace Polynomials

ZHANG Jiaxuan, JIN Yong, HUANG Zixin
(*College of Science, Civil Aviation University of China, Tianjin* 300300, *China*)

Abstract: Firstly, we gave a relatively concise proof concerning the relationship between the length of subspace orbits and the exponent of subspace polynomials. Secondly, by applying Frobenius shifts to subspaces and merging cyclic subspace codes, we obtained cyclic subspace codes with a larger size of $rn\dfrac{q^N-1}{q-1}$ and a minimum distance of $2k-2$. Finally, we gave an example of constructing a cyclic subspace code.

Keywords: cyclic subspace code; subspace polynomials; Frobenius shift; orbit

0 引 言

设 q 为素数幂，$\mathbb{F}_{q^n}$ 是 q 元有限域 $\mathbb{F}_q$ 的 n 次扩域，显然 $\mathbb{F}_{q^n}$ 可视为 $\mathbb{F}_q$ 上的 n 维向量空间. 记 $\mathscr{P}_q(n)$ 为 $\mathbb{F}_{q^n}$ 的所有 $\mathbb{F}_q$-子空间的集合，称为 $\mathbb{F}_q$ 上的 n 维射影空间[1]. $\mathscr{P}_q(n)$ 的非空子集称为 $\mathbb{F}_q$ 上的子空间码. $\mathscr{G}_q(n,k)$ 表示 $\mathbb{F}_{q^n}$ 的所有 k 维子空间的集合，称为 $\mathbb{F}_q$ 上的 Grassman 空间. $\mathscr{G}_q(n,k)$ 的一个非空子集称为 $\mathbb{F}_q$ 上的常维码，其元素个数称为该码的码字个数.

对任意的 $U,V\in\mathscr{P}_q(n)$，U 和 V 的子空间距离定义为

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

$\mathscr{P}_q(n)$ 及其上的子空间距离构成一个度量空间[2]. 码 $\mathscr{C}$ 的极小距离定义为

$$d(\mathscr{C})\triangleq\min\{d(U,V):U,V\in\mathscr{C},U\neq V\}.$$

设 $V\in\mathscr{G}_q(n,k)$，$\alpha\in\mathbb{F}_{q^n}^*=\mathbb{F}_{q^n}\backslash\{0\}$，则 $\alpha V=\{\alpha v:v\in V\}$ 称为 V 的循环移位，$V^{q^i}=\{v^{q^i}:v\in V\}$ 称为

收稿日期：2025-07-04.
第一作者简介：张嘉璇(2001—)，男，汉族，硕士研究生，从事代数编码的研究，E-mail：2990665055@qq.com. **通信作者简介**：金 永(1981—)，男，汉族，博士，讲师，从事仿射代数几何及代数编码的研究，E-mail：kingmeng@126.com.
基金项目：国家自然科学基金(批准号：12301670)和天津市教委科研项目(批准号：2023ZD041).

V 的 Frobenius 移位(其中 $i=0,1,\cdots,n-1$). 显然 αV 和 V^{q^i} 仍是 $\mathbb{F}_{q^n}$ 的 k 维子空间. 集合 $\mathrm{Orb}(V)=\{\alpha V:\alpha\in\mathbb{F}_{q^n}^*\}$ 称为 V 的轨道. 若子空间码 $\mathscr{C}$ 的码字经过循环移位后仍是 $\mathscr{C}$ 中的码字,则码 $\mathscr{C}$ 称为循环子空间码. 若循环子空间码 $\mathscr{C}=\{\alpha V:\alpha\in\mathbb{F}_{q^n}^*\}$ 的码字个数为 $\frac{q^n-1}{q-1}$,极小距离为 $2k-2$,则码 $\mathscr{C}$ 称为最优循环子空间码. Gluesing-Luerssen 等[3]提出猜想:对任意的正整数 n 和 k,若 $k<n/2$,则存在最优循环子空间码.

构造循环子空间码,目前主要有基于 Sidon 空间和基于子空间多项式的核空间两种构造方法. Roth 等[4]证明了构造 $\mathscr{G}_q(n,k)$ 中的最优循环子空间码等价于构造 $\mathscr{G}_q(n,k)$ 中的 Sidon 空间,并构造出一类 Sidon 空间. 文献[5-8]给出了利用 Sidon 空间构造多类循环子空间码的相关结果.

利用子空间多项式构造循环子空间码主要基于子空间三项式. Ben-Sasson 等[9]基于子空间三项式 $T(x)=x^{q^k}+x^q+x$ 证明了对任意的正整数 k 和 q 以及无限多个 n,$\mathscr{G}_q(n,k)$ 中存在最优循环子空间码. 进一步,文献[9]通过对子空间做 Frobenius 移位,构造出一类码字个数为 $n\frac{q^N-1}{q-1}$、极小距离为 $2k-2$ 的循环子空间码. Otal 等[10]基于 r 个三项式 $T_i(x)=x^{q^k}+\theta_i x^q+\gamma_i x\ (1\leqslant i\leqslant r)$,通过合并子空间码,构造出一类码字个数为 $r\frac{q^N-1}{q-1}$、极小距离为 $2k-2$ 的循环子空间码. Chen 等[11]将文献[9]和文献[10]中的三项式 $T(x)=x^{q^k}+x^q+x$ 和 $T_i(x)=x^{q^k}+\theta_i x^q+\gamma_i x$ 分别推广到 $T(x)=x^{q^k}+a_l x^{q^l}+a_0 x$ 和 $T_i(x)=x^{q^k}+\theta_i x^{q^l}+\gamma_i x$,分别构造出码字个数为 $\frac{q^N-1}{q-1}$ 和 $r\frac{q^N-1}{q-1}$、极小距离均为 $2k-2$ 的循环子空间码,并通过加入二项式 $T(x)=x^{q^k}+a_0 x$,构造出一类码字个数为 $r\frac{q^N-1}{q-1}+\frac{q^N-1}{q^k-1}$、极小距离为 $2k-2$ 的循环子空间码. 目前,利用四项及以上子空间多项式构造循环子空间码的研究报道较少. Zhao 等[12]考虑一般形式的子空间多项式 $T(x)=x^{q^k}+a_s x^{q^{t_s}}+\cdots+a_1 x^{q^{t_1}}+a_0 x$,给出了基于该多项式构造的循环子空间码的码字个数、极小距离与其指数之间的关系,并基于四项式 $T(x)=x^{q^k}+a_2 x^{q^2}+a_1 x^q+a_0 x$ 构造出一类最优循环子空间码. 文献[10,13-14]给出了基于子空间多项式构造混合维数或极小距离小于 $2k-2$ 的循环子空间码的相关结果.

本文针对文献[12]中给出的多项式 $T(x)=x^{q^k}+a_s x^{q^{t_s}}+\cdots+a_1 x^{q^{t_1}}+a_0 x$ 对应的子空间轨道长度与其指数之间的联系的结论,先给出一较简洁的证明,然后通过子空间的 Frobenius 移位与合并子空间码,对现有基于子空间三项式的构造方法进行推广,获得了码字个数更多、极小距离为 $2k-2$ 的循环子空间码,最后给出 $\mathbb{F}_{3^7}$ 上的实例.

1 预备知识

形如

$$f(x)=a_k x^{q^k}+a_{k-1}x^{q^{k-1}}+\cdots+a_1 x^q+a_0 x\in\mathbb{F}_{q^n}[x]$$

的多项式称为 $\mathbb{F}_{q^n}$ 上的线性化多项式(或 q-多项式)[15]. 线性化多项式 $f(x)\in\mathbb{F}_{q^n}[x]$ 的根集构成 $\mathbb{F}_{q^n}$ 的某扩域的一个子空间(作为 $\mathbb{F}_q$ 上的向量空间),并且 $f(x)$ 的根具有相同的重数[16]. 对任意的 $V\in\mathscr{G}_q(n,k)$,多项式 $f(x)=\prod_{v\in V}(x-v)$ 是 $\mathbb{F}_{q^n}$ 上的一个线性化多项式[17].

定义 1[18] 若 $\mathbb{F}_{q^n}$ 上的首一线性化多项式 $f(x)$ 满足以下等价条件,则 $f(x)$ 称为关于 $\mathbb{F}_{q^n}$ 的子空间多项式:

1) $f(x)\mid(x^{q^n}-x)$;

2) $f(x)$ 在 $\mathbb{F}_{q^n}$ 上完全分裂,并且 $f(x)$ 的所有根都是单根.

对于 $V\in\mathscr{G}_q(n,k)$,$P_V(x)=\prod_{v\in V}(x-v)$ 是唯一与 V 对应的子空间多项式,从而两个子空间相同当且仅当它们对应的子空间多项式相等.

引理 1[9]　若 $V\in\mathcal{G}_q(n,k)$，$\alpha\in\mathbb{F}_{q^n}^*$，则 $P_{\alpha V}(x)=\alpha^{q^k}P_V(\alpha^{-1}x)$. 即若 $P_V(x)=x^{q^k}+\sum_{j=0}^{i}\alpha_j x^{q^j}$，则 $P_{\alpha V}(x)=x^{q^k}+\sum_{j=0}^{i}\alpha^{q^k-q^j}\alpha_j x^{q^j}$.

引理 2[9]　若 $V\in\mathcal{G}_q(n,k)$，$P_V(x)=x^{q^k}+\sum_{j=0}^{i}\alpha_j x^{q^j}$，则对于 $s\in\{0,\cdots,n-1\}$，$P_{V^{q^s}}(x)=x^{q^k}+\sum_{j=0}^{i}\alpha_j^{q^s}x^{q^j}$.

2　子空间的轨道大小

设 $V\in\mathcal{G}_q(n,k)$，若存在 $\mathbb{F}_{q^n}$ 的子域 $\mathbb{F}_{q^d}$，使得 V 是 $\mathbb{F}_{q^d}$ 上的向量空间，则称 V 是 $\mathbb{F}_{q^n}$ 的 $\mathbb{F}_{q^d}$-子空间，此时 $d\mid n$，$d\mid k$.

引理 3　设 $V\in\mathcal{G}_q(n,k)$，$\mathbb{F}_{q^d}$ 是 $\mathbb{F}_{q^n}$ 的子域，则 V 是 $\mathbb{F}_{q^d}$-子空间当且仅当对任意的 $\alpha\in\mathbb{F}_{q^d}^*$，均有 $\alpha V=V$.

证明：由于 V 是 $\mathbb{F}_q$-子空间，因此 V 是 $\mathbb{F}_{q^d}$-子空间当且仅当 $\forall\alpha\in\mathbb{F}_{q^d}$ 及 $\forall v\in V$，有 $\alpha v\in V$，当且仅当 $\forall\alpha\in\mathbb{F}_{q^d}^*$，有 $\alpha V\subseteq V$. 又因为 αV 与 V 具有相同维数，因此 $\alpha V=V$. 证毕.

引理 4　设 $V\in\mathcal{G}_q(n,k)$，$A=\{\alpha\in\mathbb{F}_{q^n}^*:\alpha V=V\}$，则 $A\cup\{0\}$构成 $\mathbb{F}_{q^n}$ 的子域.

证明：设 $\alpha\in A$，由于 $V\in\mathcal{G}_q(n,k)$，因此 $V=-V$，又因为 $\alpha V=V$，从而

$$-\alpha V=-V=V,\qquad \alpha^{-1}V=\alpha^{-1}(\alpha V)=V,$$

即对任意的 $\alpha\in A$，有 $-\alpha,\alpha^{-1}\in A$，所以 $A\cup\{0\}$构成 $\mathbb{F}_{q^n}$ 的子域. 证毕.

推论 1　记 $\mathbb{F}_{q^d}=\{\alpha\in\mathbb{F}_{q^n}^*:\alpha V=V\}\cup\{0\}$，则 $\mathbb{F}_{q^d}$ 是使得 V 是 $\mathbb{F}_{q^d}$-子空间的 $\mathbb{F}_{q^n}$ 的最大子域.

引理 5　设 $V\in\mathcal{G}_q(n,k)$，$\mathbb{F}_{q^d}=\{\alpha\in\mathbb{F}_{q^n}^*:\alpha V=V\}\cup\{0\}$，则 $|\mathrm{Orb}(V)|=\dfrac{q^n-1}{q^d-1}$.

证明：由推论 1 可知 $\mathbb{F}_{q^d}^*$ 是 $\mathbb{F}_{q^n}^*$ 的子群，由 $\mathbb{F}_{q^d}$ 的定义可知 $\mathbb{F}_{q^d}^*$ 是 V 的稳定子群，则 V 的轨道的阶数等于用 $\mathbb{F}_{q^d}^*$ 对 $\mathbb{F}_{q^n}^*$ 做陪集分解的不同陪集个数，即 $|\mathrm{Orb}(V)|=\dfrac{q^n-1}{q^d-1}$. 证毕.

注 1　引理 5 即文献[10]中定理 1 的充分性，以上是本文给出的另一种证明方法.

引理 6[4]　设 V 是 $\mathbb{F}_{q^n}$ 的子空间(作为 $\mathbb{F}_q$ 上的向量空间)，则多项式 $f(x)=\prod_{v\in V}(x-v)$ 是 $\mathbb{F}_{q^n}$ 上的 q-多项式.

定理 1　设 $V\in\mathcal{G}_q(n,k)$，$P_V(x)=\prod_{v\in V}(x-v)$，$\mathbb{F}_{q^d}$ 是 $\mathbb{F}_{q^n}$ 的子域，则 V 是 $\mathbb{F}_{q^d}$-子空间当且仅当 $P_V(x)$各项中 x 的指数是$(q^d)^i$ 的形式，其中 i 为非负整数.

证明：充分性. 由于 V 是 $\mathbb{F}_{q^d}$-子空间，因此由引理 6 可知 $P_V(x)$是 q^d-多项式，即 $P_V(x)$各项中 x 的指数是$(q^d)^i$ 的形式.

必要性. 设 $P_V(x)$各项中 x 的指数是$(q^d)^i$ 的形式，则对任意的 $v\in V$ 和$\alpha\in\mathbb{F}_{q^d}^*$，有

$$P_V(\alpha v)=\alpha P_V(v)=0,$$

从而 $\alpha v\in V$，进而 $\alpha V\subseteq V$，所以 $\alpha V=V$. 由引理 3 可知 V 是 $\mathbb{F}_{q^d}$-子空间. 证毕.

根据上述结论，可得如下定理.

定理 2　设正整数 s 满足 $1\leqslant s<k$，正整数 $t_1,t_2,\cdots,t_s$ 满足 $1\leqslant t_1<t_2<\cdots<t_s<k$，且 $a_0,a_1,\cdots,a_s$ 是 $\mathbb{F}_{q^n}$ 中的非零元素，记 $d=\gcd(k,t_s,\cdots,t_2,t_1)$. 若 $V\in\mathcal{G}_q(n,k)$，且其对应的子空间多项式为

$$P_V(x)=x^{q^k}+a_s x^{q^{t_s}}+\cdots+a_1x^{q^{t_1}}+a_0x\in\mathbb{F}_{q^n}[x],$$

则 $|\mathrm{Orb}(V)|=\dfrac{q^n-1}{q^d-1}$.

证明：由 $\gcd(k,t_s,\cdots,t_2,t_1)=d$，得

$$P_V(x)=x^{q^k}+a_s x^{q^{t_s}}+\cdots+a_1 x^{q^{t_1}}+a_0 x=x^{(q^d)^{k/d}}+a_s x^{(q^d)^{t_s/d}}+\cdots+a_1 x^{(q^d)^{t_1/d}}+a_0 x.$$

由定理1知，V 是 $\mathbb{F}_{q^d}$-子空间，并且 $\mathbb{F}_{q^d}$ 是满足引理5条件的 $\mathbb{F}_{q^n}$ 最大子域，从而 $|\mathrm{Orb}(V)|=\dfrac{q^n-1}{q^d-1}$. 证毕.

注2 定理2是文献[12]中定理3.2的主要部分，但文献[12]中的证明很长且不易理解.

推论2 设 $V\in\mathscr{G}_q(n,k)$，$P_V(x)=x^{q^k}+a_s x^{q^{t_s}}+\cdots+a_1 x^{q^{t_1}}+a_0 x$，则 $|\mathrm{Orb}(V)|=\dfrac{q^n-1}{q^d-1}$ 当且仅当 $d=\gcd(k,t_s,\cdots,t_2,t_1)$.

3 循环子空间码的构造

引理7[11] 设 k 和 l 为满足 $1\leqslant l<k$ 且 $\gcd(l,k)=1$ 的正整数，并设 $T_i(x)=x^{q^k}+\theta_i x^{q^l}+\gamma_i x\in\mathbb{F}_{q^n}[x](1\leqslant i\leqslant r)$ 为 $\mathbb{F}_{q^n}$ 上的 r 个子空间多项式，其中 θ_i 和 γ_i 为 $\mathbb{F}_{q^n}$ 上的非零元素$(1\leqslant i\leqslant r)$. 假设 V_i 是子空间多项式 $T_i(x)$ 的根集，且 V_i 包含在 $\mathbb{F}_{q^N}$ 中. 若对任意的 $1\leqslant i\neq j\leqslant r$，满足

$$\left(\frac{\gamma_i}{\gamma_j}\right)^{(q^l-1)/(q-1)}\neq\left(\frac{\gamma_i}{\gamma_j}\left(\frac{\theta_i}{\theta_j}\right)^{-1}\right)^{(q^k-1)/(q-1)},$$

则 $\mathscr{C}=\bigcup_{i=1}^{r}\{\alpha V_i:\alpha\in\mathbb{F}_{q^N}^*\}$ 是一个 k 维循环子空间码，其码字个数为 $r\dfrac{q^N-1}{q-1}$，极小距离为 $2k-2$.

定理3 设 k,l 是满足 $1\leqslant l<k$ 和 $\gcd(l,k)=1$ 的正整数. 考虑 r 个多项式 $T_i(x)=x^{q^k}+\theta_i x^{q^l}+\gamma_i x\in\mathbb{F}_{q^n}[x](1\leqslant i\leqslant r)$，满足 $\theta_i\neq 0$ 和 $\gamma_i\neq 0(1\leqslant i\leqslant r)$，并且

$$\left(\frac{\gamma_i^{q^s}}{\gamma_j^{q^t}}\right)^{(q^l-1)/(q-1)}\neq\left[\frac{\gamma_i^{q^s}}{\gamma_j^{q^t}}\left(\frac{\theta_i^{q^s}}{\theta_j^{q^t}}\right)^{-1}\right]^{(q^k-1)/(q-1)},\quad 1\leqslant i,j\leqslant r,\quad 0\leqslant s,t\leqslant n-1.$$

设 V_i 是子空间多项式 $T_i(x)$ 的根集且 V_i 包含在 $\mathbb{F}_{q^N}$ 中，则由 $\mathscr{C}=\bigcup_{i=1}^{r}\bigcup_{s=0}^{n-1}\{\alpha V_i^{q^s}:\alpha\in\mathbb{F}_{q^N}^*\}$ 给出的码 $\mathscr{C}\subseteq\mathscr{G}_q(N,k)$ 是一个循环码，其码字个数为 $rn\dfrac{q^N-1}{q-1}$，极小距离为 $2k-2$.

证明：显然码 $\mathscr{C}$ 是循环的. 由引理1和引理2知，对应于 $\alpha V_i^{q^s}(1\leqslant i\leqslant r,\ 0\leqslant s\leqslant n-1)$ 的子空间多项式为

$$T_{i,\alpha}^s(x)=x^{q^k}+\alpha^{q^k-q^l}\theta_i^{q^s}x^{q^l}+\alpha^{q^k-1}\gamma_i^{q^s}x.$$

又由于 $\gcd(l,k)=1$，故由定理2知，

$$|\mathrm{Orb}(\alpha V_i^{q^s})|=\frac{q^N-1}{q-1}.$$

因此，要证明 $|\mathscr{C}|=rn\dfrac{q^N-1}{q-1}$ 及 $d(\mathscr{C})=2k-2$，只需证明对于 $1\leqslant i,j\leqslant r$，$0\leqslant s,t\leqslant n-1$，有

$$\dim(\alpha V_i^{q^s}\cap\beta V_j^{q^t})\leqslant 1.$$

当 $i=j$ 且 $s=t$ 时，由引理7可知结论成立. 当 $i\neq j$ 或 $s\neq t$ 时，由引理1和引理2知，对应于 $\alpha V_i^{q^s}$ 和 $\beta V_j^{q^t}$ 的子空间多项式分别为

$$T_{i,\alpha}^s(x)=x^{q^k}+\alpha^{q^k-q^l}\theta_i^{q^s}x^{q^l}+\alpha^{q^k-1}\gamma_i^{q^s}x,$$
$$T_{j,\beta}^t(x)=x^{q^k}+\beta^{q^k-q^l}\theta_j^{q^t}x^{q^l}+\beta^{q^k-1}\gamma_j^{q^t}x.$$

由于

$$T_{i,\alpha}^s(x)-T_{j,\beta}^t(x)=(\alpha^{q^k-q^l}\theta_i^{q^s}-\beta^{q^k-q^l}\theta_j^{q^t})x^{q^l}+(\alpha^{q^k-1}\gamma_i^{q^s}-\beta^{q^k-1}\gamma_j^{q^t})x,$$

若 $\alpha^{q^k-q^l}\theta_i^{q^s}-\beta^{q^k-q^l}\theta_j^{q^t}=0$ 且 $\alpha^{q^k-1}\gamma_i^{q^s}-\beta^{q^k-1}\gamma_j^{q^t}\neq 0$(或者 $\alpha^{q^k-q^l}\theta_i^{q^s}-\beta^{q^k-q^l}\theta_j^{q^t}\neq 0$ 且 $\alpha^{q^k-1}\gamma_i^{q^s}-\beta^{q^k-1}\gamma_j^{q^t}=0$)，则 $T_{i,\alpha}^s(x)$ 和 $T_{j,\beta}^t(x)$ 有唯一公共根0，结论成立. 若 $\alpha^{q^k-q^l}\theta_i^{q^s}-\beta^{q^k-q^l}\theta_j^{q^t}=0$，$\alpha^{q^k-1}\gamma_i^{q^s}-\beta^{q^k-1}\gamma_j^{q^t}=0$，即

$$\alpha^{q^k-q^l}\theta_i^{q^s}=\beta^{q^k-q^l}\theta_j^{q^t},\qquad\alpha^{q^k-1}\gamma_i^{q^s}=\beta^{q^k-1}\gamma_j^{q^t},$$

则

$$\frac{\theta_i^{q^s}}{\theta_j^{q^t}}=\left(\frac{\beta}{\alpha}\right)^{q^k-q^l},\qquad \frac{\gamma_i^{q^s}}{\gamma_j^{q^t}}=\left(\frac{\beta}{\alpha}\right)^{q^k-1},$$

从而

$$\left(\frac{\theta_i^{q^s}}{\theta_j^{q^t}}\right)\left(\frac{\gamma_i^{q^s}}{\gamma_j^{q^t}}\right)^{(q^l-q^k)/(q^k-1)}=\left(\frac{\beta}{\alpha}\right)^{q^k-q^l}\left(\frac{\beta}{\alpha}\right)^{q^l-q^k}=1,$$

即

$$\left(\frac{\theta_i^{q^s}}{\theta_j^{q^t}}\right)\left(\frac{\gamma_i^{q^s}}{\gamma_j^{q^t}}\right)^{(q^l-q^k)/(q^k-1)}=\frac{\gamma_i^{q^s}}{\gamma_j^{q^t}},$$

进而

$$\left(\frac{\gamma_i^{q^s}}{\gamma_j^{q^t}}\right)^{(q^l-1)/(q-1)}=\left[\frac{\gamma_i^{q^s}}{\gamma_j^{q^t}}\left(\frac{\theta_i^{q^s}}{\theta_j^{q^t}}\right)^{-1}\right]^{(q^k-1)/(q-1)},$$

矛盾.

因此，假设 $\alpha^{q^k-q^l}\theta_i^{q^s}-\beta^{q^k-q^l}\theta_j^{q^t}\neq 0$ 和 $\alpha^{q^k-1}\gamma_i^{q^s}-\beta^{q^k-1}\gamma_j^{q^t}\neq 0$. 设 u,v 是 $\alpha U_i^{q^s}\cap\beta U_j^{q^t}$ 中的非零元，只需证明存在 $\lambda\in\mathbb{F}_q^*$，使得 $u=\lambda v$. 由于

$$T_{i,\alpha}^s(u)=T_{i,\alpha}^s(v)=T_{j,\beta}^t(u)=T_{j,\beta}^t(v)=0,$$

因此

$$T_{i,\alpha}^s(u)-T_{j,\beta}^t(u)=(\alpha^{q^k-q^l}\theta_i^{q^s}-\beta^{q^k-q^l}\theta_j^{q^t})u^{q^l}+(\alpha^{q^k-1}\gamma_i^{q^s}-\beta^{q^k-1}\gamma_j^{q^t})u=0,$$
$$T_{i,\alpha}^s(v)-T_{j,\beta}^t(v)=(\alpha^{q^k-q^l}\theta_i^{q^s}-\beta^{q^k-q^l}\theta_j^{q^t})v^{q^l}+(\alpha^{q^k-1}\gamma_i^{q^s}-\beta^{q^k-1}\gamma_j^{q^t})v=0.$$

从而得

$$u^{q^l-1}=\frac{-(\alpha^{q^k-1}\gamma_i^{q^s}-\beta^{q^k-1}\gamma_j^{q^t})}{\alpha^{q^k-q^l}\theta_i^{q^s}-\beta^{q^k-q^l}\theta_j^{q^t}}=v^{q^l-1},$$

即 $\frac{u}{v}=\left(\frac{u}{v}\right)^{q^l}$，则 $\frac{u}{v}\in\mathbb{F}_{q^l}$.

设 $\frac{u}{v}=\lambda\in\mathbb{F}_{q^l}$，$u=\lambda v$. 由 $T_{i,\alpha}^s(u)=0$，得

$$0=T_{i,\alpha}^s(u)=u^{q^k}+\alpha^{q^k-q^l}\theta_i^{q^s}u^{q^l}+\alpha^{q^k-1}\gamma_i^{q^s}u=\lambda^{q^k}v^{q^k}+\alpha^{q^k-q^l}\theta_i^{q^s}\lambda^{q^l}v^{q^l}+\alpha^{q^k-1}\gamma_i^{q^s}\lambda v=$$
$$\lambda^{q^k}v^{q^k}+\alpha^{q^k-q^l}\theta_i^{q^s}\lambda v^{q^l}+\alpha^{q^k-1}\gamma_i^{q^s}\lambda v.$$

由于 $\lambda T_{i,\alpha}^s(v)=\lambda v^{q^k}+\alpha^{q^k-q^l}\theta_i^{q^s}\lambda v^{q^l}+\alpha^{q^k-1}\gamma_i^{q^s}\lambda v=0$，对比系数可得 $\lambda=\lambda^{q^k}$，因此 $\lambda\in\mathbb{F}_{q^k}$. 因为 $\gcd(l,k)=1$，从而得 $\lambda\in\mathbb{F}_q$，结论得证.

注 3　定理 3 通过加入子空间的 Frobenius 移位，构造出码字个数更多、极小距离不变的循环子空间码，并且能包含文献[9-11]中给出的大部分构造方法. 与文献[11]同理，可以通过添加二项式 $T(x)=x^{q^k}-a_0x$，构造码字个数为 $rn\frac{q^N-1}{q-1}+\frac{q^N-1}{q^k-1}$、极小距离为 $2k-2$ 的循环子空间码.

例 1　在定理 3 中，取 $q=3$，$n=7$，$k=3$，$l=1$，多项式组

$$T_i(x)=x^{3^3}+\theta_ix^3+\gamma_ix\in\mathbb{F}_{3^7}[x],\qquad 1\leqslant i\leqslant 314,$$

$T_i(x)$对应的子空间为 V_i. 设 $\mathbb{F}_{3^N}$ 是包含全部 $T_i(x)$分裂域的域，则可以构造循环子空间码

$$\mathscr{C}=\bigcup_{i=1}^{314}\bigcup_{s=0}^{6}\{\alpha V_i^{q^s}:\alpha\in\mathbb{F}_{3^N}^*\},$$

其码字个数为 $314\times 7\times\frac{3^N-1}{2}=1\,099(3^N-1)$，极小距离为 $2k-2=4$. 利用 Magma 软件计算得到 $T_i(x)$中的系数 θ_i 和 γ_i 如下：(w^3,w^{412})，(w^{50},w^{436})，(w^{60},w^{650})，(w^{73},w^{215})，$(w^{95},w^{2\,059})$，$(w^{104},w^{1\,431})$，$(w^{108},w^{1\,508})$，$(w^{118},w^{1\,360})$，$(w^{120},w^{1\,037})$，$(w^{127},w^{2\,013})$，(w^{129},w^{393})，$(w^{134},w^{1\,401})$，$(w^{142},w^{2\,016})$，$(w^{150},w^{1\,738})$，$(w^{151},w^{2\,007})$，$(w^{153},w^{1\,559})$，(w^{173},w^{719})，(w^{176},w^{837})，$(w^{179},w^{1\,836})$，$(w^{186},w^{1\,755})$，$(w^{188},w^{1\,156})$，(w^{193},w^{33})，$(w^{198},w^{1\,236})$，(w^{199},w^{868})，$(w^{201},w^{1\,996})$，(w^{205},w^{924})，(w^{210},w^{626})，(w^{223},w^{22})，(w^{226},w^{250})，(w^{228},w^{330})，(w^{233},w^{146})，(w^{237},w^{983})，$(w^{246},w^{1\,704})$，(w^{251},w^{627})，

$(w^{252},w^{1\,087}),(w^{262},w^{794}),(w^{263},w^{1\,366}),(w^{277},w^{1\,281}),(w^{285},w^{922}),(w^{286},w^{1\,723}),(w^{307},w^{1\,155}),$
$(w^{317},w^{1\,480}),(w^{325},w^{1\,727}),(w^{332},w^{271}),(w^{337},w^{1\,750}),(w^{339},w^{502}),(w^{343},w^{2\,116}),(w^{349},w^{1\,339}),$
$(w^{368},w^{1\,666}),(w^{372},w^{1\,974}),(w^{403},w^{409}),(w^{440},w^{86}),(w^{441},w^{1\,653}),(w^{443},w^{339}),(w^{446},w^{1\,893}),$
$(w^{447},w^{2\,125}),(w^{450},w^{1\,714}),(w^{462},w^{812}),(w^{462},w^{1\,278}),(w^{466},w^{2\,135}),(w^{467},w^{1\,451}),(w^{475},w^{1\,289}),$
$(w^{488},w^{252}),(w^{497},w^{60}),(w^{505},w^{1\,517}),(w^{505},w^{1\,849}),(w^{511},w^{1\,566}),(w^{527},w^{1\,700}),(w^{532},w^{471}),$
$(w^{533},w^{29}),(w^{538},w^{564}),(w^{559},w^{44}),(w^{561},w^{2\,039}),(w^{565},w^{1\,736}),(w^{575},w^{825}),(w^{575},w^{1\,128}),$
$(w^{589},w^{1\,928}),(w^{592},w^{992}),(w^{600},w^{161}),(w^{600},w^{1\,383}),(w^{606},w^{1\,676})(w^{611},w^{142}),(w^{622},w^{1\,827}),$
$(w^{630},w^{2\,173}),(w^{632},w^{1\,127}),(w^{634},w^{399}),(w^{646},w^{395}),(w^{651},w^{1\,174}),(w^{654},w^{177}),(w^{655},w^{1\,194}),$
$(w^{657},w^{1\,962}),(w^{666},w^{1\,158}),(w^{667},w^{1\,672}),(w^{670},w^{320}),(w^{681},w^{1\,229}),(w^{688},w^{1\,215}),(w^{689},w^{1\,588}),$
$(w^{691},w^{1\,122}),(w^{706},w^{1\,923}),(w^{711},w^{951}),(w^{721},w^{1\,613}),(w^{727},w^{1\,778}),(w^{733},w^{1\,708}),(w^{743},w^{205}),$
$(w^{746},w^{1\,059}),(w^{748},w^{2\,027}),(w^{761},w^{991}),(w^{766},w^{172}),(w^{772},w^{2\,078}),(w^{776},w^{1\,666}),(w^{779},w^{1\,896}),$
$(w^{786},w^{1\,589}),(w^{804},w^{413}),(w^{814},w^{1\,326}),(w^{824},w^{1\,238}),(w^{839},w^{935}),(w^{840},w^{1\,047}),(w^{841},w^{2\,176}),$
$(w^{844},w^{1\,927}),(w^{845},w^{1\,725}),(w^{850},w^{410}),(w^{859},w^{1\,211}),(w^{860},1),(w^{869},w^{906}),(w^{889},w^{1\,622}),$
$(w^{898},w^{928}),(w^{902},w^{1\,969}),(w^{917},w^{1\,615}),(w^{931},w^{1\,038}),(w^{932},w^{548}),(w^{933},w^{282}),(w^{953},w^{1\,118}),$
$(w^{959},w^{1\,001}),(w^{959},w^{1\,151}),(w^{960},w^{2\,020}),(w^{980},w^{1\,958}),(w^{983},w^{2\,044}),(w^{985},w^{1\,152}),(w^{997},w^{1\,310}),$
$(w^{1\,001},w^{2\,035}),(w^{1\,012},w^{943}),(w^{1\,022},w^{553}),(w^{1\,031},w^{400}),(w^{1\,042},w^{339}),(w^{1\,044},w^{1\,130}),(w^{1\,049},w^{189}),$
$(w^{1\,049},w^{357}),(w^{1\,051},w^{1\,226}),(w^{1\,055},w^{793}),(w^{1\,063},w^{2\,032}),(w^{1\,074},w^{1\,592}),(w^{1\,077},w^{1\,600}),(w^{1\,092},w^{1\,966}),$
$(w^{1\,094},w^{1\,260}),(w^{1\,100},w^{2\,167}),(w^{1\,114},w^{1\,387}),(w^{1\,122},w^{1\,290}),(w^{1\,139},w^{1\,431}),(w^{1\,139},w^{1\,993}),$
$(w^{1\,150},w^{1\,739}),(w^{1\,156},w^{1\,743}),(w^{1\,157},w^{70}),(w^{1\,167},w^{110}),(w^{1\,169},w^{901}),(w^{1\,172},w^{316}),(w^{1\,183},w^{893}),$
$(w^{1\,189},w^{1\,239}),(w^{1\,192},w^{1\,201}),(w^{1\,204},w^{1\,489}),(w^{1\,207},w^{1\,493}),(w^{1\,213},w^{130}),(w^{1\,214},w^{1\,158}),$
$(w^{1\,227},w^{1\,109}),(w^{1\,230},w^{2\,109}),(w^{1\,235},w^{135}),(w^{1\,249},w^{1\,759}),(w^{1\,259},w^{1\,666}),(w^{1\,285},w^{1\,514}),(w^{1\,291},w^{186}),$
$(w^{1\,295},w^{1\,058}),(w^{1\,297},w^{1\,841}),(w^{1\,305},w^{1\,286}),(w^{1\,320},w^{1\,141}),(w^{1\,334},w^{1\,396}),(w^{1\,336},w^{851}),(w^{1\,345},w^{192}),$
$(w^{1\,351},w^{1\,059}),(w^{1\,356},w^{2\,150}),(w^{1\,372},w^{1\,805}),(w^{1\,373},w^{669}),(w^{1\,375},w^{673}),(w^{1\,381},w^{1\,109}),(w^{1\,389},w^{24}),$
$(w^{1\,390},w^{870}),(w^{1\,399},w^{155}),(w^{1\,401},w^{538}),(w^{1\,402},w^{1\,885}),(w^{1\,432},w^{228}),(w^{1\,433},w^{1\,666}),(w^{1\,437},w^{1\,013}),$
$(w^{1\,442},w^{1\,110}),(w^{1\,444},w^{223}),(w^{1\,445},w^{1\,005}),(w^{1\,447}w^{1\,710}),(w^{1\,450},w^{1\,067}),(w^{1\,468},w^{1\,404}),(w^{1\,469},w^{844}),$
$(w^{1\,475},w^{425}),(w^{1\,488},w^{268}),(w^{1\,490},w^{1\,486}),(w^{1\,494},w^{1\,616}),(w^{1\,516},w^{294}),(w^{1\,516},w^{1\,467}),(w^{1\,531},w^{688}),$
$(w^{1\,532},w^{973}),(w^{1\,535}w^{452}),(w^{1\,535},w^{635}),(w^{1\,541},w^{410}),(w^{1\,542},w^{2\,125}),(w^{1\,550},w^{1\,651}),(w^{1\,553},w^{1\,296}),$
$(w^{1\,568},w^{1\,921}),(w^{1\,570},w^{471}),(w^{1\,574},w^{1\,997}),(w^{1\,576},w^{2\,152}),(w^{1\,588},w^{824}),(w^{1\,588},w^{2\,109}),(w^{1\,594},w^{1\,685}),$
$(w^{1\,613},w^{2\,008}),(w^{1\,622},w^{1\,607}),(w^{1\,623},w^{1\,363}),(w^{1\,630},w^{492}),(w^{1\,630},w^{1\,401}),(w^{1\,642},w^{1\,447}),$
$(w^{1\,644},w^{1\,677}),(w^{1\,667},w^{37}),(w^{1\,669},w^{1\,240}),(w^{1\,677},w^{1\,701}),(w^{1\,680},w^{1\,842}),(w^{1\,686},w^{2\,157}),(w^{1\,710},w^{954}),$
$(w^{1\,711},w^{1\,157}),(w^{1\,714},w^{558}),(w^{1\,720},w^{1\,436}),(w^{1\,728},w^{1\,946}),(w^{1\,733},w^{1\,848}),(w^{1\,737},w^{1\,249}),(w^{1\,739},w^{452}),$
$(w^{1\,739},w^{1\,925}),(w^{1\,753},w^{716}),(w^{1\,754},w^{242}),(w^{1\,771},w^{1\,263}),(w^{1\,778},w^{739}),(w^{1\,778},w^{1\,142}),(w^{1\,785},w^{1\,772}),$
$(w^{1\,786},w^{665}),(w^{1\,813},w^{1\,406}),(w^{1\,814},w^{1\,931}),(w^{1\,821},w^{1\,891}),(w^{1\,827},w^{1\,554}),(w^{1\,839},w^{1\,738}),(w^{1\,846},w^{476}),$
$(w^{1\,851},w^{443}),(w^{1\,852},w^{2\,084}),(w^{1\,854},w^{613}),(w^{1\,860},w^{549}),(w^{1\,863},w^{807}),(w^{1\,874},w^{930}),(w^{1\,875},w^{1\,401}),$
$(w^{1\,886},w^{796}),(w^{1\,893},w^{899}),(w^{1\,905},w^{1\,939}),(w^{1\,908},w^{1\,304}),(w^{1\,916},w^{459}),(w^{1\,918},w^{1\,167}),(w^{1\,930},w^{553}),$
$(w^{1\,944},w^{2\,068}),(w^{1\,957},w^{100}),(w^{1\,976},w^{2\,155}),(w^{1\,978},w^{347}),(w^{1\,980},w^{1\,549}),(w^{1\,980},w^{1\,668}),(w^{1\,982},w^{1\,472}),$
$(w^{1\,997},w^{1\,196}),(w^{1\,999},w^{331}),(w^{2\,026},w^{769}),(w^{2\,027},w^{1\,011}),(w^{2\,028},w^{1\,404}),(w^{2\,035},w^{190}),(w^{2\,036},w^{1\,235}),$
$(w^{2\,036},w^{2\,174}),(w^{2\,044},w^{1\,034}),(w^{2\,044},w^{1\,407}),(w^{2\,048},w^{2\,073}),(w^{2\,049},w^{144}),(w^{2\,049},w^{1\,642}),(w^{2\,070},w^{434}),$
$(w^{2\,070},w^{1\,216}),(w^{2\,075},w^{1\,126}),(w^{2\,079},w^{919}),(w^{2\,086},w^{236}),(w^{2\,092},w^{29}),(w^{2\,094},w^{775}),(w^{2\,099},w^{307}),$
$(w^{2\,119},w^{764}),(w^{2\,122},w^{524}),(w^{2\,128},w^{904}),(w^{2\,129},w^{1\,760}),(w^{2\,147},w^{1\,951}),(w^{2\,156},w^{1\,466}),(w^{2\,160},w^{1\,164}),$
$(w^{2\,163},w^{736}),(w^{2\,163},w^{880}),(w^{2\,170},w^{1\,261})$, 其中 w 是 $\mathbb{F}_{3^7}$ 的本原元.

4 结 论

本文首先对子空间轨道长度与子空间多项式指数之间联系的结论给出了一个较简洁的证明;

其次，在合并循环子空间码的基础上加入了 Frobenius 移位，对任意给定的素数幂 q、正整数 n，k ($k<n$)及无穷多个 N，构造出码字个数为 $rn\frac{q^N-1}{q-1}$、极小距离为 $2k-2$ 的循环子空间码，并给出了构造实例. 结果表明，该方法构造的码字个数大于已有基于子空间多项式构造的码字个数，如文献[9,11]中构造的码字个数分别为 $n\frac{q^N-1}{q-1}$和 $r\frac{q^N-1}{q-1}$. 对于四项及以上多项式，本文方法难以推广，主要障碍在于难以构建类似定理 3 的约束条件，进而无法确保循环移位及 Frobenius 移位后不同子空间交的维数不超过 1.

参 考 文 献

[1] ETZION T, VARDY A. Error-Correcting Codes in Projective Space [J]. IEEE Transactions on Information Theory, 2011, 57(2): 1165-1173.

[2] KÖETTER R, KSCHISCHANG F R. Coding for Errors and Erasures in Random Network Coding [J]. IEEE Transactions on Information Theory, 2008, 54(8): 3579-3591.

[3] GLUESING-LUERSSEN H, MORRISON K, TROHA C. Cyclic Orbit Codes and Stabilizer Subfields [J]. Advances in Mathematics of Communications, 2015, 9(2): 177-197.

[4] 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.

[5] NIU Y F, YUE Q, WU Y S. Several Kinds of Large Cyclic Subspace Codes via Sidon Spaces [J]. Discrete Mathematics, 2020, 343(5): 111788-1-111788-11.

[6] FENG T, WANG Y. New Constructions of Large Cyclic Subspace Codes and Sidon Spaces [J]. Discrete Mathematics, 2021, 344(4): 112273-1-112273-7.

[7] LI Y, LIU H W. Cyclic Constant Dimension Subspace Codes via the Sum of Sidon Spaces [J]. Designs, Codes and Cryptography, 2023, 91(4): 1193-1207.

[8] ZHANG H, TANG C M. Constructions of Large Cyclic Constant Dimension Codes via Sidon Spaces [J]. Designs, Codes and Cryptography, 2023, 91(1): 29-44.

[9] BEN-SASSON E, ETZION T, GABIZON A, et al. Subspace Polynomials and Cyclic Subspace Codes [J]. IEEE Transactions on Information Theory, 2016, 62(3): 1157-1165.

[10] OTAL K, ÖZBUDAK F. Cyclic Subspace Codes via Subspace Polynomials [J]. Designs, Codes and Cryptography, 2017, 85(2): 191-204.

[11] CHEN B C, LIU H W. Constructions of Cyclic Constant Dimension Codes [J]. Designs, Codes and Cryptography, 2018, 86(6): 1267-1279.

[12] ZHAO W, TANG X L. A Characterization of Cyclic Subspace Codes via Subspace Polynomials [J]. Finite Fields and Their Applications, 2019, 57: 1-12.

[13] 李云. 几类子空间码的构造 [D]. 武汉：华中师范大学，2020.（LI Y. Constructions of Several Classes of Subspace Codes [D]. Wuhan: Central China Normal University, 2020.）

[14] 杜媛媛. 轨道子空间码的构造 [D]. 武汉：湖北大学，2018.（DU Y Y. The Constructions of Orbital Subspace Codes [D]. Wuhan: Hubei University, 2018.）

[15] ORE O. On a Special Class of Polynomials [J]. Transactions of the American Mathematical Society, 1933, 35(3): 559-584.

[16] LIDL R, NIEDERREITER H. Finite Fields [M]. Cambridge: Cambridge University Press, 1997: 110.

[17] MacWILLIAMS F J, SLOANE N J A. The Theory of Error-Correcting Codes: Part 2, Vol. 16 [M]. New York: Elsevier, 1977: 1-762.

[18] 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.

（责任编辑：赵立芹）