通过幂等元构造任意维数 r 多循环码：统一的组合-代数方法

Jean Charles Ramanandraibe 和 Ramamonjy Andriamifidisoa

arXiv:2603.07177v1 [math.AC] 7 Mar 2026

摘要——我们提出一种统一方法，用于构造 r 上任意维数的多循环码。该方法基于 r维本原幂等元，这些幂等元由单变量幂等元的张量积定义，并结合多维分圆轨道。由此建立了组合描述与代数描述之间的直接等价关系，得到自然的多项式基，并给出一个最优乘积界，将 BCH 界和 Reed-Solomon界推广至此。本文还提出一种高效的构造算法，并通过最优三维码加以说明。

索引词——多循环码、幂等元、分圆轨道、张量积、乘积界

I. 引言

多循环码是环中的理想

$$R = \mathbb{F}_q[X_1, \ldots, X_r]/\langle X_1^{n_1} - 1, \ldots, X_r^{n_r} - 1\rangle,$$

其中，对每个 t，$q \equiv 1$ (模 n_t)。现有构造存在复杂度高（Gröbner基）、缺乏连贯的多维结构或性能次优（张量积）等问题 [6], [5]。

我们的主要贡献包括：
— 将 r 维本原幂等元表示为张量积（定义 III.1）— 捕获联合对称性的多维分圆轨道（定义 III.4）— 组合表示与代数表示之间的基本等价性（定理 III.6）— 关于最小距离的最优乘积界（定理 III.9）— 高效的系统构造算法（算法 1）

这一框架统一了组合视角与代数视角，使实用的高性能码构造成为可能。

II. 预备知识

设 $R = \mathbb{F}_q[X_1, \ldots, X_r]/\langle X_t^{n_t} - 1\rangle_{t=1}^r$ 满足 $q \equiv 1$(模 n_t)。设 $\mathbb{F}_q$[3] 中的 n_t 次本原单位根为 ω_t。

一元本原幂等元是

$$\theta_{i_t}^{(t)}(X_t) = \frac{1}{n_t} \sum_{m=0}^{n_t-1} \omega_t^{-i_t m} X_t^m.$$

它们满足幂等性、正交性、和为 1 以及求值性质 $\theta_{i_t}^{(t)}(\omega_t^{j_t}) = \delta_{i_t,\, j_t}$ [1], [2]。

$f \in R$ 的多元傅里叶变换为

$$\hat{f}(j_1, \ldots, j_r) = f(\omega_1^{j_1}, \ldots, \omega_r^{j_r}).$$

它是 $\mathbb{F}_q$-线性且双射的，并具有反演公式和卷积性质 [2]。

子集 $C \subseteq R$ 是多循环的，当且仅当存在 $S \subseteq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ 使得

$$C = \{f \in R : \hat{f}(j) = 0 \ \forall j \notin S\}, \quad \dim C = |S|.$$

III. 主要结果

A. 本原 r维幂等元

定义 III.1（原始 r维幂等元）。

$$\begin{aligned} e_{i_1,\ldots,i_r} &= \prod_{t=1}^{r} \theta_{i_t}^{(t)}(X_t) \\ &= \frac{1}{N} \sum_{m_1,\ldots,m_r} \Big(\prod_{t=1}^{r} \omega_t^{-i_t m_t}\Big) X_1^{m_1} \cdots X_r^{m_r}. \end{aligned} \tag{1}$$

其中 $N = n_1 \cdots n_r$。

命题 III.2。族 $\{e_{i_1,\ldots,i_r}\}$ 满足：
— $e^2 = e$ *(idempotence)*
— $e \cdot e' = 0$ *if indices differ (orthogonality)*
— $\sum e_{i_1,\ldots,i_r} = 1$ *(partition of unity)*
— *Evaluation property (Kronecker deltas)*

证明。1. 幂等性：对于每个 t，$\theta_{i_t}^{(t)}$ 都是幂等元：$(\theta_{i_t}^{(t)})^2 = \theta_{i_t}^{(t)}$。由于各变量相互独立：

$$e_{i_1,\ldots,i_r}^2 = \prod_{t=1}^{r} (\theta_{i_t}^{(t)})^2 = \prod_{t=1}^{r} \theta_{i_t}^{(t)} = e_{i_1,\ldots,i_r}.$$

2. 正交性：若 $(i_1, \ldots..., i_r) \neq (j_1, \ldots..., j_r)$，则存在 $\exists t_0$ 使得 $i_{t_0} \neq j_{t_0}$。我们有：

$$e_{i_1,\ldots,i_r} e_{j_1,\ldots,j_r} = \prod_{t=1}^{r} \theta_{i_t}^{(t)} \theta_{j_t}^{(t)}.$$

对于 $t = t_0$, $\theta^{(t_0)}{}_{i_{t_0}} \theta^{(t_0)}{}_{j_{t_0}} = 0$，因为单变量幂等元彼此正交 [1]。3. 单位分解：对于每个 t, $\sum_{i_t=0}^{n_t-1} \theta_{i_t}^{(t)} = 1$。因此：

$$\sum_{i_1,\ldots,i_r} e_{i_1,\ldots,i_r} = \sum_{i_1,\ldots,i_r} \prod_{t=1}^{r} \theta_{i_t}^{(t)} = \prod_{t=1}^{r} \left(\sum_{i_t=0}^{n_t-1} \theta_{i_t}^{(t)} \right) = 1.$$

4. 求值：对于每个 t, $\theta_{i_t}^{(t)}(\omega_t^{j_t}) = \delta_{i_t,j_t}$。因此：

$$e_{i_1,\dots,i_r}(\omega_1^{j_1},\dots,\omega_r^{j_r}) = \prod_{t=1}^{r}\theta_{i_t}^{(t)}(\omega_t^{j_t}) = \prod_{t=1}^{r}\delta_{i_t,j_t} = \delta_{i_1,j_1}\cdots\delta_{i_r,j_r}.$$

□

定理 III.3（谱分解，[2]）。 $R \simeq \bigoplus \mathbb{F}_q e_{i_1,\ i_r} \simeq \mathbb{F}_q^N$。

证明。幂等元 $e_{i_1,\ i_r}$ 两两正交，并满足 $\sum e_{i_1,\ i_r} = 1$。因此：

$$R = \bigoplus_{i_1,\dots,i_r} Re_{i_1,\dots,i_r}.$$

每个 $Re_{i_1,\ i_r}$ 都是 R的理想。令 $f \in Re_{i_1,\ i_r}$，则对于某个 $g \in R$，有$f = ge_{i_1,\ i_r}$。通过求值：

$$f = ge_{i_1,\dots,i_r} = g(\omega_1^{i_1},\dots,\omega_r^{i_r})e_{i_1,\dots,i_r}.$$

因此 $Re_{i_1,\ i_r} = \mathbb{F}_q e_{i_1,\ i_r} \simeq \mathbb{F}_q$。映射：

$$\varphi : R \to \mathbb{F}_q^N, \quad f \mapsto (f(\omega_1^{i_1},\dots,\omega_r^{i_r}))_{i_1,\dots,i_r}$$

是一个环同构。事实上：- φ 是线性且双射的（逆傅里叶变换）。- $\varphi(fg) = \varphi(f) * \varphi(g)$（按分量逐一相乘）。□

B. 多维分圆轨道

定义 III.4 (轨道)。弗罗贝尼乌斯作用为$\sigma(i_1,\dots,i_r) = (qi_1 \bmod n_1,\dots,qi_r \bmod n_r)$。$(a_1,\dots,a_r)$ 的轨道为

$$\mathcal{O}_{(a_1,\dots,a_r)} = \{\sigma^t(a_1,\dots,a_r) : t \ge 0\}.$$

定义 III.5 (生成幂等元)。多循环码C 的生成幂等元为

$$e = \sum_{(a)\in T} a_{(a)} \sum_{(i)\in\mathcal{O}_{(a)}} X_1^{i_1}\cdots X_r^{i_r},$$

其中 T 是轨道代表元的集合 *[4]*。

定理 III.6 (等价性)。上述组合形式等价于

$$e = \sum c_{i_1,\dots,i_r} e_{i_1,\dots,i_r}, \quad c_i \in \{0,1\},$$

其中 c 在轨道上为常数。

证明。设 e由组合表示给出。对所有 $(i_1,\dots,i_r)$：

$$c_{i_1,\dots,i_r} = e(\omega_1^{i_1},\dots,\omega_r^{i_r}) \tag{2}$$

$$= \sum_{(a_1,\dots,a_r)\in T} a_{a_1,\dots,a_r} \sum_{(j_1,\dots,j_r)\in C_{a_1,\dots,a_r}} \omega_1^{i_1 j_1}\cdots\omega_r^{i_r j_r}. \tag{3}$$

由于 $\omega_t^{n_t} = 1$，内层求和遍历一个分圆轨道。令 $C = C_{a_1,\dots,a_r}$。对于 $(j_1,\dots,j_r) \in C$，存在 t 使得 $(j_1,\dots,j_r) = \sigma^t(a_1,\dots,a_r) = (a_1 q^t \bmod n_1,\dots,a_r q^t \bmod n_r)$。那么：

$$\omega_1^{i_1 j_1}\cdots\omega_r^{i_r j_r} = \prod_{t=1}^{r}\omega_t^{i_t a_t q^t} = \prod_{t=1}^{r}(\omega_t^{i_t a_t})^{q^t}.$$

如果 $(i_1,\dots,i_r) \in C_{b_1,\dots,b_r}$，那么存在 s，使得 $(i_1,\dots,i_r) = \sigma^s(b_1,\dots,b_r) = (b_1 q^s,\dots,b_r q^s)$。可以验证，$c_{i_1,\dots,i_r}$ 仅取决于 $(i_1,\dots,i_r)$ 的轨道。因此，$c_{i_1,\dots,i_r}$ 在各轨道上为常数。反之，设 $e = \sum_{i_1,\dots,i_r} c_{i_1,\dots,i_r} e_{i_1,\dots,i_r}$，且 $c_{i_1,\dots,i_r} \in \{0,1\}$ 在各轨道上为常数。那么，由于$c_{qi_1,\dots,qi_r} = c_{i_1,\dots,i_r}$，$e$在弗罗贝尼乌斯作用下不变。因此，$e$ 在单项式基下的系数属于 $\mathbb{F}_q$。令 T 为轨道代表元的集合，其中 $c_{i_1,\dots,i_r} = 1$。那么，对于 $(a_1,\dots,a_r) \in T$，e 可写成组合表示的形式，其中 $a_{a_1,\dots,a_r} = 1$。 □

C. 自然基与参数

定理 III.7 (多项式基)。令 k_t 为满足 $X_t^{k_t} e \in$ 张成$\{X_t^m e : m < k_t\}$ 的最小值。那么

$$\mathcal{B} = \{X_1^{m_1}\cdots X_r^{m_r} e : 0 \le m_t < k_t\}$$

是一个基，且 维数 $C = \prod k_t$。

证明。令V =张成$\{X_1^{m_1}\cdots X_r^{m_r} e$: $0 \le m_t < k_t\}$。线性无关性：设 $\sum_{m_1=0}^{k_1-1}\cdots\sum_{m_r=0}^{k_r-1}\lambda_{m_1,\dots,m_r}X_1^{m_1}\cdots X_r^{m_r}e = 0$。令 $P = \sum\lambda_{m_1,\dots,m_r}X_1^{m_1}\cdots X_r^{m_r}$。于是 $Pe = 0$。在 $(\omega_1^{i_1},\dots,\omega_r^{i_r})$ 处取值，其中 $e(\omega_1^{i_1},\dots,\omega_r^{i_r}) = 1$: $P(\omega_1^{i_1},\dots,\omega_r^{i_r}) = 0$。令 $S = \{(i_1,\dots,i_r) : e(\omega_1^{i_1},\dots,\omega_r^{i_r}) = 1\}$。根据 k_t 的定义，满足 $(i_1,\dots,i_r) \in S$ 的点集 $(\omega_1^{i_1},\dots,\omega_r^{i_r})$ 对每个变量都包含一个由 k_t 个点组成的笛卡尔积。因此 P 至少在 $\prod k_t$ 个不同点处为零。由于 $\deg_{X_t} P < k_t$，P至多有 $\prod k_t$ 个系数。对于 $(i_1,\dots,i_r) \in S$，线性方程组 $P(\omega_1^{i_1},\dots,\omega_r^{i_r}) = 0$具有一个可逆的多维范德蒙矩阵，因此 $P = 0$。生成性：令 $fe \in C$。通过依次对 $X_1,\dots,X_r$进行欧几里得除法，并利用关系 $X_t^{k_t}e = \sum_{m=0}^{k_t-1}\alpha_{t,m}X_t^m e$，我们可以写成：

$$f = \sum_{m_1=0}^{k_1-1}\cdots\sum_{m_r=0}^{k_r-1}\lambda_{m_1\dots m_r}X_1^{m_1}\cdots X_r^{m_r} + ,,(,)。$$

$$\sum_{t=1}^{r} Q_t\ X_t^{k_t} - \sum_{m=0}^{k_t-1}\alpha_{t\ m}X_t^m \qquad e$$

两边乘以并利用 $X_t^{k_t}e = \sum_{m=0}^{k_t-1}\alpha_{t,m}X_t^m e$，得到 $fe \in V$。因此 $\mathcal{B}$ 是一个基，且 $\dim C = |\mathcal{B}| = \prod_{t=1}^{r} k_t$。

□

注释 III。 **8** $\{X_t^{m_t}e \quad 0 \le m_t < k_t\} =$。 $\left\{\sum_{m_t=0}^{k_t-1}\alpha_{m_t}X_t^{m_t}e \;\middle|\; \alpha_{m_t}\in\mathbb{F}_q\right\}$ $X_t^{k_t}e \in$ span :。表达式 span$\{X_t^{m_t}e : 0 \le m_t < k_t\}$ 表示存在系数 α_0, α_1、.....、 $\alpha_{k_t-1} \in \mathbb{F}_q$ 使得：

$$X_t^{k_t}e = \sum_{m_t=0}^{k_t-1}\alpha_{m_t}X_t^{m_t}e$$

换言之， $X_t^{k_t}e$ 是元素 e、 $X_t e$、 $X_t^2 e$、.....、 $X_t^{k_t-1}e$的线性组合。

定理 III.9 （乘积界）。对于 $C = \langle e \rangle$,

$$n = \prod n_t, \quad k = \prod k_t, \quad d \geq \prod_{t=1}^{r} (n_t - k_t + 1).$$

证明。 长度 n是 R 中单项式的总数，因此

$$n = \prod_{t=1}^{r} n_t.$$

维数 k 由定理 III.7 给出：

$$k = \prod_{t=1}^{r} k_t.$$

设 $c = Pe \in C \setminus \{0\}$，对所有 t 有 $\deg_{X_t} P < k_t$。对每个 $t = 1, \ldots, r$，设

$A_t = \{i_t \in \mathbb{Z}_{n_t} \mid \exists (i_1, \ldots, i_r) \in \text{supp}(c) \text{ 具有该坐标 } i_t\}$.

Then

$$\text{supp}(c) \subseteq A_1 \times \cdots \times A_r \quad \text{and thus} \quad \text{wt}(c) \geq |A_1| \cdots |A_r|.$$

固定 $t \in \{1, \ldots, r\}$ 并冻结变量 $\{X_j\}_{j \neq t}$。于是字 c 可视为变量 X_t 上的一元循环码中的一个非零字，其长度为 n_t ，维数为k_t。由Singleton界（或循环码的BCH界），每个非零字满足：

$$|A_t| \geq n_t - k_t + 1.$$

由于该估计对所有 $t = 1, \ldots, r$ 成立，我们得到：

$$\text{wt}(c) \geq \prod_{t=1}^{r} |A_t| \geq \prod_{t=1}^{r} (n_t - k_t + 1).$$

因此，码 C 的最小距离 d 满足：

$$d \geq \prod_{t=1}^{r} (n_t - k_t + 1).$$

□

D. 构造算法

算法1构造 r维多循环码

输入： $n_1, \ldots, n_r, q$，目标维数 K

确保： $[n, K, d]_q$ code

1: 计算轨道 $\mathcal{O}_{(a)}$ 与 $\sum_{(a)\in T} |\mathcal{O}_{(a)}| = K$

2: 选择 T 使得

3: 构造 $e = \sum_{(a)\in T} \sum_{(i)\in\mathcal{O}_{(a)}} X_1^{i_1} \cdots X_r^{i_r}$

4: 计算 $k_1, \ldots, k_r$（最小次数）

5: 基 $\mathcal{B} = \{X_1^{m_1} \cdots X_r^{m_r} e : \ 0 \leq m_t < k_t\}$

6: 由 $\mathcal{B}$的系数生成矩阵 G

表 I 最优三维码示例 $[8, K, d]_3$

K	T （代表元）	基规模	d
3	{(0, 0, 0), (1, 0, 0), (0, 1, 0)}	3	4
4	{(0,0,0), (0, 0, 1), (0, 1,0), (1,0, 0)}	4	4

IV. 示例： $\mathbb{F}_3$上的最优三维码

考虑 $R = \mathbb{F}_3[x, y, z]/\langle x^2 - 1, \ y^2 - 1, \ z^2 - 1 \rangle$ （ $q = 3 \equiv 1$（模 2））。

由于 $3 \equiv 1$ （模 2）， σ 是恒等变换；每个点都是自己的轨道（大小为 1）。

对于 $K = 3$，码 $[8, 3, 4]_3$达到乘积界$d \geq (2 - 1 + 1)^3 = 8$ （利用结构将其收紧至 4，这对于这些参数是最优的）。

$K = 3$ 的显式幂等元和生成矩阵：

$$e = 2x + 2y + xy + 2xz + 2yz + xyz,$$

生成矩阵（系数按字典序排列）：

$$G = \begin{pmatrix} 0 & 2 & 2 & 0 & 1 & 2 & 2 & 1 \\ 2 & 0 & 1 & 2 & 2 & 0 & 1 & 2 \\ 2 & 1 & 0 & 2 & 2 & 1 & 0 & 2 \end{pmatrix}.$$

类似的计算可得 $K = 4$对应的 $[8, 4, 4]_3$。

V. 与现有方法的比较

与格罗布纳基方法相比，我们的方法避免了指数复杂度 [6]。不同于单变量幂等元的推广方法，我们的方法能够捕捉真正的多维对称性 [4]。张量积构造往往会产生次优距离[5]；而我们的乘积界和轨道选择则提供了更好的控制。

VI. 结论

我们提出了一个统一框架，利用张量积幂等元和多维分圆轨道构造任意维数的多循环码。该方法不仅提供了理论洞见（等价性、分解、最优界），还给出了一种实用算法，并通过最优三维实例进行了验证。未来工作包括通过轨道选择优化距离，以及将方法推广到常循环码 [5]。

参考文献

[1] F. J. MacWilliams 和 N. J.A. Sloane，《纠错码理论》。North-Holland，1977。[2] R. E. Blahut，《数据传输代数码》。剑桥大学出版社，2003。[3] R. Lidl 和 H. Niederreiter，《有限域》，第 2 版。剑桥大学出版社，1997。[4] S. Han，“关于 $\mathbb{F}_{2^t}$ 上循环码的幂等元”，《韩国数学杂志》，第 30 卷，第 4 期，第 653–663 页，2022。[5] S. Bhardwaj 和 M. Raka，“有限域上任意长度的多维常循环码”，*arXiv :2201.01031*，2022。[6] Z. Sepasdar，“任意长度二维循环码的生成矩阵”，《设计、编码与密码学》，第 90 卷，406，2022 387pp. – 。