arXiv:2303.00235v1 [cs.IT] 1 Mar 2023

有限域上的常二面体码

Yun Fan，Yue Leng

华中师范大学数学与统计学院，中国武汉 430079

摘要

文献（Fan、Lin，IEEE信息论汇刊，第67卷，第5016–5025页）证明，有限域 F上的自对偶（二者分别为 LCD）二面体码在 q 为偶数（奇数）时是渐近良好的。本文研究了 F上的常二面体码的代数性质和渐近性质，并证明：如果 q为偶数或 $4|(q-1)$，则自对偶常二面体码是渐近良好的；否则，LCD consta-二面体码是渐近良好的。此外，借助本文提出的一种技术，我们纠正了上述文献中的一些错误。

关键词：有限域；二面体码；常二面体码；自对偶码；LCD码。

1 引言

设 F是一个基数为 $|F|=q$的有限域，其中 q 是素数的幂。任意 $a=(a_1,\cdots,a_n)\in F^n$, $a_i\in F$称为一个字。汉明重量w(a)定义为满足 $a_i\neq 0$的指标 i 的个数。两个字 $a,a'\in F^n$之间的汉明距离定义为d(a,a') = w($a-a'$)。任意 $\emptyset\neq C\subseteq F^n$称为 F上的长度为 n的码；码中的字称为码字。最小汉明距离d(C)是 C中不同码字之间的最小距离。若 C是 F^n的线性子空间，则 C称为线性码，最小汉明重量w(C)定义为 C的非零码字的最小重量，并且已知w(C) =d(C)。分数 $\Delta(C)=\mathrm{d}(C)_n = \mathrm{w}(C)_n$ 称为 C的相对最小距离，R(C) = $\dim_n^F C$称为 C的码率。若码序列 $C_1,C_2,\cdots$的长度 n_i 趋于无穷，且R(C_i)和 $\Delta(C_i)$都有正的下界，则称该码序列为渐近良好。若一个码类中存在渐近良好的码序列，则称该码类渐近良好。字 $a=(a_1,\cdots,a_n)$和 $b=(b_1,\cdots,b_n)$的内积

Email address: yfan@mail.ccnu.edu.cn（Yun Fan）；

定义为 $\langle a,\ b\rangle = \sum_{i=1}^{n} a_i b_i$。然后，自正交码、自对偶码、LCD码等均按通常方式定义，例如参见[14]。

设 G 是一个阶为 n 的有限群。群代数 FG 是以 F 为标量域、以 G 为基的向量空间，并且其乘法由群 G 的乘法诱导得到。任意元素 $\sum_{x\in G} a_x x \in FG$ 都可表示为一个字 $(a_x)_{x\in G} \in F^n$。于是， FG 的任意左理想都称为一个 FG 码。若 G 是循环群（阿贝尔群、二面体群），则 FG 码分别称为循环码（阿贝尔码、二面体码）。$FG\times FG$ 的任意 FG-子模都称为指标 2 的拟-FG 码。若 G 是循环群（阿贝尔群），则指标 2 的拟-FG 码也分别称为指标 2 的拟循环码（拟阿贝尔码）。

若 $G=\langle x\,|\,x^n=1\rangle$ 是一个循环群，则 FG 是由 x 生成并满足关系式 $x^n=1$ 的 F 代数。对于 $0\neq\lambda\in F$，由 x 生成并满足关系式 $x^n=\lambda$ 的 F 代数称为常循环群代数，其理想称为常循环码。接下来，设 $G=\langle u、\ v\,|\,u^n=1、\ v^2=1、\ vuv^{-1}=u^{-1}\rangle$ 为一个二面体群。那么， FG 是由 u、v 生成并满足三个关系式 $u^n=1$、 $v^2=1$ 和 $vu=u^{-1}v$ 的 F 代数（非交换）。如果将关系式“$v^2=1$”替换为关系式“$v^2=-1$”，并保持另外两个关系式不变，则所得的 F 代数称为常二面体群代数，其左理想称为常二面体码（详细内容参见第3节）。

这是一个长期悬而未决的问题（参见 [20]）：有限域上的循环码是否渐近良好？然而，人们早已知道，若特征 char(F) $=2$，则 F 上的指标 2 拟循环码渐近良好，参见 [6, 7, 15]。有限二面体群与有限循环群十分相近，因为阶为 $2n$ 的二面体群有一个阶为 n的正规循环子群。Bazzi 和 Mitter [4] 证明了二进制二面体码渐近良好。随后，Mart´ınez-P´erez 和 Willems [21] 证明了指标 2 的二进制自对偶拟循环码渐近良好。Borello 和 Willems [5] 证明了这类 FG码渐近良好，其中 $|F|=p$是奇素数，且 G是由阶为 p 的循环群与有限循环群构成的半直积。

对于任意有限域 F，即对于任意素数幂 q，文献[17] 已证明， F 上的指标 2 准循环码是渐近良好的；并且，如果 q 是偶数，或 $4\,|\,(q-1)$，即 $q\not\equiv 3$（模 4），那么 F 上的指标 2 自对偶准循环码是渐近良好的。注意， F 上存在指标 2 自对偶准循环码，当且仅当 $q\not\equiv 3$（模 4），参见 [19] 或[18, 定理 IV.5]。基于 Artin本原根猜想，在对 q 作相同的¨假设下，Alahmadi、Ozdemir 和 Sol´e [1] 也证明了指标 2 自对偶准循环码的渐近良好性。Lin 和 Fan [18] 进一步指出，若 $q\not\equiv 3$ （模 4），则指标 2 自对偶准阿贝尔码（包括准循环情形）是渐近良好的。最近，Fan 和 Liu [12] 讨论了指标 2 准常循环码，并证明这类码是渐近良好的。

另一方面，Fan 和 Lin [10] 将二面体码的渐近良好性推广到了任意 q 元情形；更准确地说，他们证明了自对偶二面体码（如果 q 为偶数）和 LCD二面体码（如果 q 为奇数）是渐近良好的。因此，自对偶

（如果 q 为偶数）以及指标 2 的 LCD（如果 q 为奇数）准循环码也得到了。顺便一提，我们发现参考文献 [10], 中的两个定理的证明存在一些错误；由于这些错误， [10, 定理 IV.5(1)] 是错误的；详见下文第 6 节。幸运的是，这个问题不影响上述结果的正确性。

关于指标 2 的拟循环码与二面体码之间的关系，任何二面体（常二面体）码都以一种自然的方式成为 ¨指标 2 的拟循环码。Alahmadi、Ozdemir 和 Sol´e [1] 证明了，当 q为偶数时，自对偶双循环码（指标 2 的一类自对偶准循环码）是二面体码。Fan 和 Zhang [13] 对此进行了推广，并给出了指标 2 的自对偶准循环码成为二面体码（当 q 为偶数时）或常二面体码（当 q 为奇数时）的充要条件。

上述研究方向促使我们将重点放在常二面体码上。在本文中，我们研究常二面体码的代数性质和渐近性质，并处理参考文献 [10] 中的问题。为研究常二面体码的代数性质，我们通过矩阵计算发展出一种评估（常）二面体码正交性的技术；并构造出一类具有良好代数性质（自正交、LCD 等）的常二面体码。借助这一技术，我们处理了 [10] 上述提到的问题，并恢复了 [10] （下文定理 6.7 ）中错误定理的正确版本。为研究常二面体码的渐近性质，在我们构造的常二面体码类中，我们统计具有不良渐近性质的此类码的数量；该数量远小于该类码的总数，因此得到以下结果。

定理 1.1 （定理 5.12 见下文）。 假设 q为偶数，或 $4|(q-1)$。那么， F 上的自对偶常二面体码是渐近良好的。特别地，2阶 F 上的自对偶准循环码是渐近良好的。

定理 1.2 （定理 5.8 见下文）。 假设 q为奇数，且 $4\nmid(q-1)$。那么， F 上的 LCD 常二面体码是渐近良好的。特别地，2阶 F 上的 LCD 准循环码是渐近良好的。

第 2 节概述了一些预备知识。

第 3 节从三种方式描述常二面体群代数，展示其性质，并刻画常二面体群代数中极小理想的结构。

第 4 节基于上一节刻画的常二面体群代数结构，构造一类常二面体码，并精确刻画其代数性质（如自正交或 LCD 等）。

第5 节致力于研究常数二面体码的渐近性质。上文列出的两个定理将在本节中得到证明。

在第6节中，我们分析了上述问题的成因 [10] ，并运用本文提出的技术解决该问题，恢复了 [10, 定理 IV.5(1)]的正确版本。

最后，第 7 节给出结论。

2 预备知识

本文中，F 始终是一个有限域，其 $|F| = q$ 为素数的幂，其中 $|S|$ 表示任意集合 S的基数。并且 $n > 1$ 是一个整数。

设 G为有限群，群代数 $FG = \{\sum_{x\in G} a_x x \,|\, a_x \in F\}$是以 G 为基的 F-向量空间，其乘法由群的乘法诱导。因此，FG是一个 F-代数，称为 G 上的 F 群代数。任意 $\sum_{x\in G} a_x x \in FG$ 都可视为一个字（a_x），其为 F 上的字，坐标由 G索引。FG 的任意左理想 C 称为 G 上的 F群码。简而言之，我们也称 C为一个 FG-码。

它是群的一个反自同构：$G \to G,\ g \mapsto g^{-1}$，并由此诱导出群代数的一个反自同构：

$$FG \longrightarrow FG, \quad \sum_{g\in G} a_g g \longmapsto \sum_{g\in G} a_g g^{-1}. \tag{2.1}$$

我们记为 $\sum_{g\in G} a_g g^{-1} = \overline{\sum_{g\in G} a_g g}$，并为方便起见，将等式（2.1）称为 FG 的“横线”映射。因此，$\overline{\overline{a}} = a$，$\overline{ab} = b\overline{a}$，对于 $a,\ b \in FG$。当 FG 是 G阿贝尔群时，它是一个自同构。下面给出 FG的一个线性型：

$$\sigma:\ FG \longrightarrow F, \quad \sum_{g\in G} a_g g \longmapsto a_{1_G} \quad (1_G \text{ is the identity of } G). \tag{2.2}$$

对于 $a = \sum_{g\in G} a_g g$，$b = \sum_{g\in G} b_g g \in FG$，内积 $\langle a,\ b\rangle = \sum_{g\in G} a_g b_g$。以下只是 [10, 引理 II4]。

引理 2.1. (1) $\sigma(ab) = \sigma(ba)$，$\forall\ a, b \in FG$.
(2) $\langle a, b\rangle = \sigma(a\overline{b}) = \sigma(\overline{a}b)$，$\forall\ a, b \in FG$. (3) $\langle da,\ b\rangle = \langle a,\ \overline{d}b\rangle$，$\forall\ a, b, d \in FG$. (4) 如果 C 是一个 FG-码，那么 $C^\perp$ 也是。
(5) 对于 FG-码 C 和 D，$\langle C, D\rangle = 0$ 当且仅当 $C\overline{D} = 0$。

设 H 是一个阶为奇数 $n > 1$ 的循环群，且 $\gcd(n, q) = 1$。设 $e_0, e_1, \cdots, e_\ell$ 是 FH 的所有本原幂等元，其中 $e_0 = \frac{1}{n}\sum_{x\in H} x$。因此，$FH$ 是一个半单代数，即 FH 如下直和分解为单理想：

$$FH = FHe_0 \oplus FHe_1 \oplus \cdots \oplus FHe_\ell, \tag{2.3}$$

其中 FHe_i 为带有单位元 e_i的域。

由于 bar 映射 Eq.(2.1) 是 FH 的一个阶为 2 的自同构，它将 Eq.($e_0, e_1, \cdots, e_\ell$ 2.3) 中的本原幂等元置换（注意，$\overline{e}_0 = e_0$）。由引理 2.1(5) 可得：

$$\left\langle FHe_i, FHe_j \right\rangle = \begin{cases} 0, & \text{if } e_i \neq \overline{e}_j; \\ F, & \text{if } e_i = \overline{e}_j. \end{cases} \tag{2.4}$$

对于任意环 R（带有单位元 1_R），我们用 $R^\times$ 表示其单位群，即 R的所有单位（可逆元素）构成的乘法群。对于域 F，$F^\times = F\backslash\{0\}$。我们用 $\mathbb{Z}_n$ 表示模 n的整数剩余类环，因此 $\mathbb{Z}_n^\times$ 是由既约剩余类构成的乘法群。接着，$q \in \mathbb{Z}_n^\times$（因为 $\gcd(n,q) = 1$）。在乘法群 $\mathbb{Z}_n^\times$中，$\mathrm{ord}^{\mathbb{Z}_n^\times}(q)$ 表示 q的阶，而 $\langle q\rangle_{\mathbb{Z}_n^\times}$表示由 q生成的循环子群。以下事实众所周知。

引理 2.2。沿用上文式(2.3)中的记号。

(1) ([16, 定理 1]) $\overline{e_j} = e_j$，$\forall j \geq 0$当且仅当 $-1 \in \langle q\rangle_{\mathbb{Z}_n^\times}$。**(2)** ([2, 定理 6]) $\overline{e_j} \neq e_j$，$\forall j > 0$当且仅当 $\mathrm{ord}^{\mathbb{Z}_n^\times}(q)$ 为奇数。

设 e_0，e_1，$\cdots$，e_ℓ，其中 $e_0 = \frac{1}{n}\sum_{x\in H} x$，是$FH$ 中如式（2.3）所示的所有本原幂等元。记

$$\lambda(n) = \min\left\{\dim_F(FHe_1), \cdots, \dim_F(FHe_\ell)\right\}. \tag{2.5}$$

众所周知（参见 [18, 引理 II.2]）：

引理 2.3. $\lambda(n) = \min\left\{\mathrm{ord}^{\mathbb{Z}_p^\times}(q) \,\middle|\, p\text{遍历 } n\right\}$的所有素因子。

对于 X, Y在 F上的方程，我们需要以下结果。

引理 2.4. 设 $g \in F$和 $g \neq \pm 2$。那么，方程 $X^2 + gXY + Y^2 = -1$有解 $(s, s') \in F \times F$；并且，存在一个解 (s, s')，使得 $s' = 0$ 当且仅当 q是偶数或 $4 \mid (q-1)$。

证明. 设 $\mathcal{Q} = \{a^2 \mid a \in F\}$是 F的一个子集。若 q是偶数，则 $\mathcal{Q} = F$，引理显然成立。假设 q是奇数。那么 $|\mathcal{Q}| = \frac{q+1}{2}$，且

$$X^2 + gXY + Y^2 = \left(X + \frac{g}{2}Y\right)^2 + \left(1 - \frac{g^2}{4}\right)Y^2 = X'^2 + bY^2,$$

其中 $X' = X + \frac{g}{2}Y$和 $b = 1 - \frac{g^2}{4} \neq 0$（作为 $g \neq \pm 2$）。那么 $|(-1 - b\mathcal{Q})| = |\mathcal{Q}|$，且 $|\mathcal{Q}| + |(-1 - b\mathcal{Q})| = q + 1 > |F|$。因此 $\mathcal{Q} \cap (-1 - b\mathcal{Q}) \neq \emptyset$，并且存在 $s', t' \in F$使得 $X' = t'$且 $Y = s'$满足 $t'^2 = -1 - bs'^2$。因此，$X = s = t' - \frac{gs'}{2}$和 $Y = s'$ 是该方程的一个解。存在一个解 (s, s')，使得 $s' = 0$ 当且仅当 -1是 F的平方，因此第二个结论显然成立。 □

我们用 $\mathrm{M}_2(F)$ 表示由所有次数为 2 的 F-矩阵构成的 F-代数。

引理 2.5. 设 $M = \mathrm{M}_2(F)$，且 $\varphi(X) = X^2 + gX + 1$是 F 上的不可约多项式。那么，存在 M 的一个子代数 E，使得 $E \cong F[X]/\langle\varphi(X)\rangle$，因此 E 是 F 上的 2 次扩张域；并且满足以下条件。

(1) 对于任意具有秩为 f 的 $f \in M = 1$，$Ef = Mf =: L$ 是 M 的单左理想，并且对于 $0 \neq c \in L$、a、$b \in E^\times$、$ac = cb$，当且仅当 $a = b \in F^\times$。

(2) M 总共有 $q+1$ 个单左理想，如下所示：

$$Mf, \qquad f=\begin{pmatrix} a & 1 \\ 0 & 0 \end{pmatrix}, \forall a \in F; \quad or \quad f=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

(3) 设 L 为 M的一个单左理想。当 β 遍历 $E^{\times}$时， $L\beta$ 遍历 M的单左理想，其中每个单左理想恰好出现 $q-1$ 次。

证明。(1)和(3)已在[10, 引理 III.6]中证明。下面证明(2)。对于秩(f)为 $=1$和 $\alpha \in M$的$f \in M$， αf的每一行都是 f各行的线性组合。因此，当 α 遍历 M 时， αf 的各行恰好构成 $F \times F$的一个一维子空间。对于(2)中列出的 $q+1$ 个向量，即 $(a, 1)$、 $a \in F$和$(1, 0)$，其中任意两个都线性无关。因此，这些 $q+1$ 个向量分别生成一个一维子空间，并且由$q+1$ 得到的任意两个一维子空间都不同。 $F \times F$中总共有 $q+1$个一维子空间。因此，(2)中列出的 $q+1$ 个单左理想正好是 M的全部单左理想。 □

3 常二面体群代数

沿用第 2 节的记号。本节将刻画常二面体群代数。从现在起直至本文结尾，除非另有明确说明，我们均假设：

$$G=\langle u, v \,|\, u^n=1=v^2, vuv^{-1}=u^{-1}\rangle, \quad n>1 \text{ is odd}, \quad \gcd(n,q)=1; \quad (3.1)$$

即， G 是阶为 $2n$的二面体群；并记

$$H=\langle u\rangle, \quad T=\langle v\rangle, \quad \text{then} \quad G=H \rtimes T.$$

我们进一步考虑群

$$\tilde{G}=\langle u, \dot{v} \,|\, u^n=1=\dot{v}^4, \dot{v}u\dot{v}^{-1}=u^{-1}\rangle = H \rtimes \tilde{T},$$

它是循环群 $H=\langle u\rangle$ （阶为 n ）与循环群 $\tilde{T}=\langle \dot{v}\rangle$ （阶为 4）的半直积，满足关系 $\dot{v}u\dot{v}^{-1}=u^{-1}$。显然， $Z=\{1, \dot{v}^2\}$ 是˜的中心子群 G，且商群 $G/Z \cong G$ 是通常的二面体˜群（阶为 $2n$）。文献中将 G 称为二循环群，例如 [3]。

定义 3.1. 令 $F*G$ 为以以下元素为基的 F-向量空间

$$\left\{u^i\dot{v}^j \,\middle|\, 0 \le i < n,\, 0 \le j < 2\right\} = \{1, u, \cdots, u^{n-1}, \dot{v},\, u\dot{v}, \cdots, u^{n-1}\dot{v}\} \qquad (3.2)$$

˜并赋予由 G 的乘法诱导的 F-线性乘法，同时认定 $\dot{v}^2=-1 \in F$，即满足以下关系：

$$u^n=1, \quad \dot{v}^2=-1, \quad \dot{v}u=u^{-1}\dot{v}. \qquad (3.3)$$

F代数 $F*G=\left\{\sum_{h\in H} a_h h + \sum_{h\in H} a_{h\dot{v}} h\dot{v} \,\middle|\, a_h, a_{h\dot{v}} \in F\right\}$，即 $F*G=\left\{\sum_{j=0}^{1}\sum_{i=0}^{n-1} a_{ij}u^i\dot{v}^j \,\middle|\, a_{ij} \in F\right\}$，称为常二面体群代数，而 $F*G$的任意左理想称为常二面体码（参见[24]）。

用另一种记法，常二面体群代数

$$F*G = F[X,Y]\big/\langle X^n-1,\, Y^2+1,\, XYX-Y\rangle,$$

其中 $F[X,Y]$ 是由 X 和 Y 生成的非交换 F-多项式代数，而$\langle X^n-1$、Y^2+1、$XYX-Y\rangle$ 是由 X^n-1、Y^2+1、$XYX-Y$ 生成的理想。˜因此，$F*G$ 可视为群代数 FG 关于由 $\dot{v}^2+1$ 生成的理想 $\langle\dot{v}^2+1\rangle$ 的商代数:

$$F*G = F\tilde{G}\big/\langle\dot{v}^2+1\rangle. \tag{3.4}$$

注记 3.2. 对于任意有限群 G，根据一般理论（[8, 第268]页），函数$\alpha: G\times G\to F^\times$称为 G 的 2-余循环，如果

$$\alpha(g_1,g_2g_3)\alpha(g_2,g_3) = \alpha(g_1g_2,g_3)\alpha(g_1,g_2),\quad \forall\, g_1,g_2,g_3\in G. \tag{3.5}$$

对于 2-余循环 α，由 α 扭化的 G 的扭群代数，记作 $F^\alpha G$，是以 G 为基的 F-向量空间，并配备 F-双线性乘积 $FG\times FG\to FG$，其定义为

$$g_1\cdot g_2 = \alpha(g_1,g_2)(g_1g_2),\qquad \forall\, g_1,g_2\in G;$$

（乘法的结合性可由等式(3.5)得出）。回到二面体群 $G=\langle u,\ v\,|\,u^n=1=v^2, uvu^{-1}=u^{-1}\rangle$。容易验证，下列 γ 是 G的一个 2-余循环:

$$\gamma(u^iv^s,u^jv^t) = \begin{cases}-1, & s=t=1;\\ 1, & \text{otherwise;}\end{cases}\quad 0\le i,j<n,\ 0\le s,t<2; \tag{3.6}$$

上文定义的常二面体群代数 $F*G$ （定义 3.1）正是由上述 2-余循环 $F^\gamma G$ 得到的扭群代数 γ。

˜注记 3.3。 由等式(2.1)，群代数 $F\tilde{G}$上有 bar映射:

$$F\tilde{G}\to F\tilde{G},\quad \sum_{g\in\tilde{G}}a_g g\mapsto \overline{\sum_{g\in\tilde{G}}a_g g} = \sum_{g\in\tilde{G}}a_g g^{-1}.$$

由于 $\overline{\dot{v}^2}=\dot{v}^2$（因为 $\dot{v}^4=1$），理想 $\langle\dot{v}^2+1\rangle$ 在 $F\tilde{G}$ 中关于 bar映射不变（即 $\overline{\langle\dot{v}^2+1\rangle}=\langle\dot{v}^2+1\rangle$），因此 $F\tilde{G}$ 上的 bar映射诱导出商代数 $F*G=F\tilde{G}/\langle\dot{v}^2+1\rangle$（见等式(3.4)）上的一个变换（仍称为“bar映射”并记作“bar映射”），如下所示：对于 $\sum_{h\in H}a_hh+\sum_{h\in H}a_{h\dot{v}}h\dot{v}\in F*G$,

$$\overline{\sum_{h\in H}a_hh+\sum_{h\in H}a_{h\dot{v}}h\dot{v}} = \sum_{h\in H}a_hh^{-1}+\sum_{h\in H}a_{h\dot{v}}(h\dot{v})^{-1}\in F*G. \tag{3.7}$$

显然，$\overline{\dot{v}}=\dot{v}^{-1}=-\dot{v}$；并且 $\dot{v}\,a=\overline{a}\,\dot{v}$，$\forall\, a\in FH$。式（3.7）可改写为 $F*G$ 在式（3.2）中的标准基的线性组合:

$$\overline{\sum_{h\in H}a_hh+\sum_{h\in H}a_{h\dot{v}}h\dot{v}} = \sum_{h\in H}a_hh^{-1}-\sum_{h\in H}a_{h\dot{v}}h\dot{v}\ \in F*G.$$

˜由于 $F*G$ 上的 bar 映射由 FG 上的 bar 映射所诱导，而后者是反自同构，因此 $F*G$ 上的 bar 映射仍然是反自同构：

$$\overline{\bar{a}} = a, \quad \overline{ab} = \bar{b}\,\bar{a}, \quad \forall\, a, b \in F*G.$$

注记 3.4。 与式（2.2）类似，利用基式（3.2）可得映射

$$\sigma:\ F*G \to F, \quad \sum_{0\le i<n,\,0\le j<2} a_{ij} u^i \dot{v}^j \mapsto a_{00},$$

它是 $F*G$ 的一个线性型。并且我们有：

- Lemma 2.1 is still valid for the consta-dihedral group algebra $F*G$.

证明与 [10, 引理 II4]类似。对于任意元素 $a,\ b \in F*G$,

$$\begin{aligned} a\bar{b} &= \sum_{0\le i<n,\,0\le j<2} a_{ij} u^i \dot{v}^j \cdot \sum_{0\le i'<n,\,0\le j'<2} b_{i'j'} \overline{u^{i'} \dot{v}^{j'}} \\ &= \sum_{0\le i,i'<n,\,0\le j,j'<2} a_{ij} b_{i'j'} u^i \dot{v}^j \dot{v}^{-j'} u^{-i'}. \end{aligned}$$

将其改写为基式（3.2）的线性组合，并取出 $u^0\dot{v}^0 = 1_{\tilde{G}}$的系数，可得

$$\sigma(a\bar{b}) = \sum_{(iji'j')} a_{ij} b_{i'j'} s_{iji'j'},$$

其中，求和遍历满足以下两个条件的指标（$iji'j'$）：

(i) $0 \le i, i' < n$ and $0 \le j, j' < 2$;

(ii) $u^i \dot{v}^j \dot{v}^{-j'} u^{-i'} = s_{iji'j'} \cdot 1_{\tilde{G}}$ for an $s_{iji'j'} \in F$.

由（i）可知，（ii）成立当且仅当 $i = i'$ 和 $j = j'$；此时 $s_{iji'j'} = 1$（注意，（i）是得出结论的必要条件；例如，$\dot{v}^3 \cdot \dot{v}^{-1} = -1 \cdot 1_{\tilde{G}}$在 $F*G$中，但 $3 \ne 1$）。因此 σ（$a\bar{b}$）$= \sum_{j=0}^{1} \sum_{i=0}^{n-1} a_{ij} b_{ij}$；也就是说，引理 2.1中的（1）对 $F*G$成立。类似地，引理 2.1中的（5）对 $F*G$成立。此外，引理 2.1 中的（2）、（3）和（4）对 $F*G$ 可直接由（1）验证。特别地，如果 C 是常二面体码，那么其正交码 $C^{\perp}$也如此。

根据定义 3.1，循环群代数 FH 是常二面体群代数 $F*G$的交换子代数；并且作为 FH-模，有

$$F*G = FH \oplus FH\dot{v} = \left\{ a + a'\dot{v} \,\middle|\, a, a' \in FH \right\}. \tag{3.8}$$

引理 3.5。 设 $FH = FHe_0 \oplus FHe_1 \oplus \cdots \oplus FHe_\ell$如等式(2.3)所示。那么幂等元 e_0 在 $F*G$中是中心的，且理想 $F*Ge_0$是一个交换 F-代数，其维数为 2，并且满足以下性质。

(1) 若 q 是奇数且 $4 \nmid (q-1)$，则 $F*Ge_0$ 是 F 上的域扩张，次数为 $|F*Ge_0 : F| = 2$。

(2) 若 q 为偶数，或 $4 \mid (q-1)$，则存在一个元素 $r \in F$，使得 $r^2 = -1$，并且 $C_0 = F*G(re_0 + e_0\dot{v})$ 是 $F*Ge_0$ 的一维理想，且 $\langle C_0,\ C_0 \rangle = 0$。

证明。由于 $\overline{e_0}=e_0$，$\dot{v}e_0=\overline{e_0}\dot{v}=e_0\dot{v}$。因此 e_0 是 $F*G$ 的中心元。已知 $F*Ge_0=FHe_0\oplus FHe_0\dot{v}$ 且 $FHe_0=\{ae_0\,|\,a\in F\}\cong F$。于是 $F*Ge_0$ 是一个交换 F-代数，其中 e_0、$e_0\dot{v}$ 构成一组基。

(1) 由于群 $F^\times$ 是一个没有 4 阶元素的循环群，因此多项式 X^2+1 在 F 上不可约。因为 $(e_0\dot{v})^2=-e_0$，所以我们有同构 $F*Ge_0\cong F[X]/\langle X^2+1\rangle$，它是 F 上的一个 2 次域扩张。

(2) 如果 q 是偶数，那么 $-1=1$ 和 $r=1$ 满足 $r^2=-1$。如果 $4\,|\,(q-1)$，那么 $F^\times$ 有一个 4 阶元素 r，因此 $r^2=-1$。于是

$$\dot{v}(re_0+e_0\dot{v})=re_0\dot{v}+\dot{v}e_0\dot{v}=re_0\dot{v}-e_0=re_0\dot{v}+r^2e_0=r(re_0+e_0\dot{v}).$$

因此 $\dim_F(F*G(re_0+e_0\dot{v}))=1$。并且

$$\begin{aligned}&(re_0+e_0\dot{v})\overline{(re_0+e_0\dot{v})}=(re_0+e_0\dot{v})(re_0+\bar{\dot{v}}e_0)\\&=(re_0+e_0\dot{v})(re_0-e_0\dot{v})=(re_0)^2-(e_0\dot{v})^2=-e_0+e_0=0.\end{aligned}$$

根据备注 3.4 和引理 2.1(5)，$\langle C_0,\ C_0\rangle=0$。 □

引理 3.6。 沿用方程(3.8) 和方程(2.3)中的记号。设 e 是一个本原˜幂等元，属于 FH 且不同于 e_0，其中 $\overline{e}\neq e_0$。则 $F:=FHe$ 是 F 上的一个域扩张，$e+\overline{e}$ 是 $F*G$ 的一个本原中心幂等元，并且:

˜(1) 理想 $F*G(e+\overline{e})=FHe\oplus FH\bar{e}\oplus FHe\dot{v}\oplus FH\bar{e}\dot{v}\cong \mathrm{M}_2(F)$。

(2) 根据 (1) 中的同构，若 $f\in F*G(e+\overline{e})$ 对应于矩阵 $\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}\in \mathrm{M}_2(F)$，则 f 对应于矩阵 $\begin{pmatrix}a_{22}&a_{12}\\-a_{21}&a_{11}\end{pmatrix}$。 ix

证明。由于 $e\bar{e}=0$, $e+\bar{e}$ 是 $F*G$的一个幂等元。对于 $\dot{v}\in F*G$，我们有$\dot{v}(e+\bar{e})=\dot{v}e+\dot{v}\bar{e}=\bar{e}\dot{v}+e\dot{v}=(\bar{e}+e)\,\dot{v}$。因此，$e+\bar{e}$是 $F*G$的一个中心元。所以，$F*G(e+\bar{e})=FHe\oplus FHe\dot{v}\oplus FH\bar{e}\oplus FH\bar{e}\dot{v}$是 $F*G$的一个理想。我们首先˜给出一个 F-代数同构。定义一个映射:

$$\begin{array}{ccc}\mathrm{M}_2(\tilde{F})&\xrightarrow{\cong}&FHe\oplus FHe\dot{v}\oplus FH\bar{e}\oplus FH\bar{e}\dot{v},\\\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}&\longmapsto&a_{11}e-a_{12}\,e\,\dot{v}+\overline{a_{21}}\,\bar{e}\,\dot{v}+\overline{a_{22}}\,\bar{e},\end{array}\tag{3.9}$$

˜这是一个线性同构。对于 $a_{ij},b_{ij}\in F$, $1\le i,j\le 2$，注意到$\dot{v}a_{ij}=\overline{a_{ij}}\,\dot{v}$ 和 $\dot{v}\dot{v}=-1$，我们有

$$\begin{aligned}&\big(a_{11}e-a_{12}e\dot{v}+\overline{a_{21}}\,\bar{e}\dot{v}+\overline{a_{22}}\,\bar{e}\big)\big(b_{11}e-b_{12}e\dot{v}+\overline{b_{21}}\,\bar{e}\dot{v}+\overline{b_{22}}\,\bar{e}\big)\\&=\ (a_{11}b_{11}+a_{12}b_{21})e-(a_{11}b_{12}+a_{12}b_{22})e\dot{v}\\&\quad+\overline{(a_{21}b_{11}+a_{22}b_{21})}\,\bar{e}\dot{v}+\overline{(a_{21}b_{12}+a_{22}b_{22})}\,\bar{e}.\end{aligned}$$

˜因此，等式(3.9) 是一个 F-代数同构，且 (1) 成立。

接下来，我们得到 $a_{11}e - a_{12}e\dot{v} + \overline{a_{21}}\,\bar{e}\dot{v} + \overline{a_{22}}\,\bar{e}$ 的 bar映射像如下（注意 $\overline{\dot{v}} = \dot{v}^{-1} = -\dot{v}$）：

$$\begin{aligned}\overline{a_{11}e - a_{12}e\dot{v} + \overline{a_{21}}\,\bar{e}\dot{v} + \overline{a_{22}}\,\bar{e}} &= \overline{a_{11}}\,\bar{e} - \overline{\dot{v}}\,\overline{a_{12}}\,\bar{e} + \overline{\dot{v}}\,a_{21}\,e + a_{22}\,e.\\ &= a_{22}\,e + a_{12}\,e\,\dot{v} - \overline{a_{21}}\,\bar{e}\,\dot{v} + \overline{a_{11}}\,\bar{e}.\end{aligned}$$

因此，该图像对应的矩阵为：

$$\overline{a_{11}e - a_{12}e\dot{v} + \overline{a_{21}}\,\bar{e}\dot{v} + \overline{a_{22}}\,\bar{e}} \longleftrightarrow \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11}\end{pmatrix}. \tag{3.10}$$

证明完毕。 □

引理 3.7。设 e 是 FH 的一个本原幂等元，且有 $\bar{e} = e \neq e_0$。则FHe是 F 上的一个域扩张，e是 $F*G$ 的一个本原中心幂等元，$\tilde{F} = \{a \mid a \in FHe, a = \bar{a}\}$是 FHe 的一个子域，其次数为 $|FHe\colon \tilde{F}| = 2$，即 $F*Ge = FHe \oplus FHev \cong \mathrm{M}_2(\tilde{F})$，且中心 $\mathrm{Z}(F*Ge) = \tilde{F}$。

证明。由于 $\dot{v}e = \bar{e}\dot{v} = e\dot{v}$（作为 $e = \bar{e}$），e 是 $F*G$ 的一个本原中心幂等元。FHe是一个以 e 为单位元的域。由于 $n > 1$是奇数，F是 FHe 的一个子域，并且 $|FHe\colon \tilde{F}| = 2$（参见[18, 引理 II.3]）。由于 $FHe = \sum_{i=0}^{n-1} Fu^i e = \sum_{i=0}^{n-1} F(ue)^i$，$FHe = \tilde{F} \oplus \tilde{F}(ue)$ 是通过元素 ue 在 $\tilde{F}$ 上的扩张。此外，ue 在 $\tilde{F}$ 上的最小多项式为 $\varphi_{ue}(X) = X^2 + gX + 1$，其中 $\pm 2 \neq g \in F$，使得 g 与 2 不会同时在 F 中为零（因为 $\varphi_{ue}(X)$ 是不可约的）；参见 [10, 引理 III.3]。根据引理 2.4，取 s、$s' \in F$ 使得$s^2 + gss' + s'^2 = -1$，并令

$$\varepsilon = \begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}, \quad \eta = \begin{pmatrix} -g & 1 \\ -1 & 0\end{pmatrix}, \quad \nu = \begin{pmatrix} s & s' \\ sg + s' & -s\end{pmatrix}. \tag{3.11}$$

那么，η 的特征多项式为 $\varphi_\eta(X) = X^2 + gX + 1 = \varphi_{ue}(X)$，且 $\nu^2 = -\varepsilon$ 和 $\nu\eta\nu^{-1} = \eta^{-1}$。映射 $e \mapsto \varepsilon$、$ue \mapsto \eta$ 和 $\dot{v}e \mapsto \nu$，得到

$$F*Ge = FHe \oplus FH\dot{v}e = \tilde{F} \oplus \tilde{F}ue \oplus \tilde{F}\dot{v}e \oplus \tilde{F}u\dot{v}e$$

和 $\mathrm{M}_2(\tilde{F}) = F\varepsilon \oplus F\eta \oplus F\nu \oplus F\eta\nu$，以及以下内容（其中 a、b、c、$d \in F$）

$$\begin{array}{ccc} F*Ge & \longrightarrow & \mathrm{M}_2(\tilde{F}), \\ ae + bue + c\dot{v}e + du\dot{v}e & \longmapsto & a\varepsilon + b\eta + c\nu + d\eta\nu, \end{array} \tag{3.12}$$

是一个代数同构。任意 $ae \in F$ 都映射到 $a\varepsilon$；因此 $F = \mathrm{Z}(F*Ge)$。 □

定理 3.8。常二面体群代数 $F*G$ 是理想 A_t的正交直和：

$$F*G = A_0 \oplus A_1 \oplus \cdots \oplus A_m, \tag{3.13}$$

其中 $A_0 = F*Ge_0$ 如引理 *3.5* 所述；对于 $1 \leq t \leq m$，理想$A_t \cong M_2(F_t)$ 在 F_t 下是 F 上的域扩张，且 维数$_F\, F_t = k_t$，以下两种情况之一成立：

(1) 单位元 $1_{A_t}=e+\bar{e}$ 对应于 e 的本原幂等元 FH，且 $\bar{e}\neq e$，并且 $A_t=F*G(e+\bar{e})\cong \mathrm{M}_2(F_t)$ 如式（3.9）所示，其中 $F_t=FHe$。

(2) 本原幂等元 $1_{A_t}=e$ 的单位元 e 属于 FH，其中 $\bar{e}=e\neq e_0$，并且 $A_t=F*Ge\cong \mathrm{M}_2(F_t)$ 如式(3.12)所示，其中 $F_t=\{a\,|\,a\in FHe,\ a=\bar{a}\}$ 是域 FHe 的次数为 $|FHe$ 的子域： $F_t|=2$。

证明。 由引理 3.5、引理 3.6 和引理 3.7，式(3.13)中的直和立即可得；对于 $1\leq t\leq m$，(1) 或 (2) 成立。若 $0\leq s\neq t\leq m$，

$$A_s\cdot\overline{A_t}=F*G1_{A_s}\cdot\overline{F*G1_{A_t}}=F*G1_{A_s}\cdot\overline{1_{A_t}}F*G=F*G1_{A_s}1_{A_t}F*G=0.$$

由注记 3.4 和引理 2.1(5)， $\langle A_s,\ A_t\rangle=0$， $0\leq s\neq t\leq m$。也就是说，式 (3.13) 是正交分解。 □

推论 3.9。 沿用定理 3.8中的记号。设 C， D 是 $F*G$的任意左理想。则：

(1) $C=C_0\oplus C_1\oplus\cdots\oplus C_m$，其中 $C_t=C\cap A_t=1_{A_t}\cdot C$, $t=0,1,\cdots,m$。（我们称 C_t 为 C的 A_t-分量。）

(2) 设 $D=D_0\oplus D_1\oplus\cdots\oplus D_m$ 如 (1) 所述。那么对于 $c=c_0+c_1+\cdots+c_m\in C$ 和 $d=d_0+d_1+\cdots+d_m\in D$，内积 $\langle c,d\rangle=\sum_{t=0}^{m}\langle c_t,d_t\rangle$。

(3) $C^{\perp}=C_0^{\perp_{A_0}}\oplus C_1^{\perp_{A_1}}\oplus\cdots\oplus C_m^{\perp_{A_m}}$，其中 $C_t^{\perp_{A_t}}$, $0\leq t\leq m$表示 A_t中 C_t 的正交子空间。 C_t 和 $C_t^{\perp_{A_t}}$都是 A_t的左理想。

(4) C 是自正交的，当且仅当 A_t 中的每个 C_t, $0\leq t\leq m$ 都是自正交的。

(5) C 是 LCD，当且仅当 A_t 中的每个 C_t, $0\leq t\leq m$ 都是 LCD。

证明。 (1)。由公式(3.13)， $1=1_{A_0}+1_{A_1}+\cdots+1_{A_m}$。由于 $C_t\subseteq C$，我们有 $C_0\oplus C_1\oplus\cdots\oplus C_m\subseteq C$。另一方面，对于 $c\in C$，

$$c=1\cdot c=1_{A_0}\cdot c+1_{A_1}\cdot c+\cdots+1_{A_m}\cdot c\in(C\cap A_0)\ \oplus(C\cap A_1)\ \oplus\cdots\oplus(C\cap A_m);$$

因此 $C\subseteq C_0\oplus C_1\oplus\cdots\oplus C_m$。我们称 $c_t=1_{A_t}\cdot c$为 c的 A_t-分量。

(2). 根据注3.4 和引理 2.1(1)，可得

$$\begin{aligned}\langle c,d\rangle&=\sigma(c\overline{d})=\sigma(c_0\bar{d}_0+c_1\bar{d}_1\cdots+c_m\bar{d}_m)\\&=\sigma(c_0\bar{d}_0)+\sigma(c_1\bar{d}_1)+\cdots+\sigma(c_m\bar{d}_m)\\&=\langle c_0,d_0\rangle+\langle c_1,d_1\rangle+\cdots+\langle c_m,d_m\rangle.\end{aligned}$$

(3). 由 (1)， $C^{\perp}=C_0'\oplus C_1'\oplus\cdots\oplus C_m'$，其中 $C_t'=C^{\perp}\cap A_t$。由于 $C_t=C\cap A_t\subseteq C$ 且 $C^{\perp}\cap A_t\subseteq C^{\perp}$， $\langle C_t,\ C_t'\rangle\subseteq\langle C,\ C^{\perp}\rangle=0$。因此 $C_t'\subseteq C_t^{\perp_{A_t}}$。反过来，假设 $a_t\in C_t^{\perp_{A_t}}$，那么当 $j\neq t$ 时，a_t的 A_j 分量为零；对于任意 $c=c_0+c_1+\cdots+c_m\in C$，由上面的 (2)， $\langle c,\ a_t\rangle=\langle c_t,\ a_t\rangle=0$；因此 $a_t\in C^{\perp}\cap A_t=C_t'$。我们得到 $C_t^{\perp_{A_t}}\subseteq C_t'$。

(4). 若 $\langle C,$ 由于 $C_t \subseteq C$，我们有 $\langle C_t,\ C_t\rangle \subseteq \langle C,\ C\rangle = 0$；即，$C_t$ 在 A_t 中是自正交的。反过来，若对所有 $t = 0,\ 1,\ \cdots,\ m$，都有 $\langle C_t,\ C_t\rangle = 0$，那么由上面的 (2)，$\langle C,\ C\rangle = \sum_{t=0}^{m}\langle C_t,\ C_t\rangle = 0$。

(5). 由于 $(C \cap D) \cap A_t = (C \cap A_t) \cap (D \cap A_t)$，采用 (1) 中的记号可得

$$C \cap D = (C_0 \cap D_0) \oplus (C_1 \cap D_1) \oplus \cdots \oplus (C_m \cap D_m). \tag{3.14}$$

由 (3)，$C^{\perp} \cap A_t = C_t^{\perp_{A_t}}$。将式 (3.14) 应用于 $D = C^{\perp}$，得到

$$C \cap C^{\perp} = (C_0 \cap C_0^{\perp_{A_0}}) \oplus (C_1 \cap C_1^{\perp_{A_1}}) \oplus \cdots \oplus (C_m \cap C_m^{\perp_{A_m}}).$$

因此，$C \cap C^{\perp} = \{0\}$ 当且仅当 $C_t \cap C_t^{\perp_{A_t}} = \{0\}$ 对于 $t = 0, 1, \cdots, m$ 成立。 □

推论 3.10。 沿用定理 3.8中的记号。

(1) $k_1 + k_2 + \cdots + k_m = \frac{n-1}{2}$。(2) $2k_t \geq \lambda(n),\quad t = 1,\ \ldots\ldots,$ m，其中 $\lambda(n)$ 在式(2.5)中定义。

证明。 由式 (3.13)，有 $2n =$ 维数$_F$ $F*G = \sum_{t=0}^{m}$维数$_F$ A_t，其中维数$_F$ $A_0 =$ 维数$_F$ $F*Ge_0 = 2$，见引理 3.5(1)。由于 $A_t \cong M_2(F_t)$ 对于 t =1，$\cdots$，m，维数 $_F$ $A_t = 4k_t$，因此 $2(k_1 + k_2 + \cdots + k_m) = n - 1$。第二个结论显然成立。 □

4 常二面体码

常二面体代数 $F*G$ 的任意左理想称为常二面体码，其定义在 F 上，长度为 $2n$；参见定义3.1。本节构造一些常二面体码，并研究它们的代数性质。

注 4.1。沿用定理 3.8 中的记号： $F*G = A_0 \oplus A_1 \oplus \cdots \oplus A_m$，其中 $A_0 = F*Ge_0$，并且对于 $t = 1,\ \cdots,\ m$，理想 $A_t \cong \mathrm{M}_2(F_t)$ 如定理 3.8(1) 和 (2) 所述，且 dim $_F$ $F_t = k_t$。根据同构 $A_t \cong \mathrm{M}_2(F_t)$，对 $\mathrm{M}_2(F_t)$ 应用引理 2.5，可得域 $K_t \subseteq A_t$，它对应于 $\mathrm{M}_2(F_t)$ 的一个子域（引理 2.5 中记为 E），其在 F_t 上的维数为 2。因此 $\dim_F K_t = 2k_t$，因为 $\dim_F F_t = k_t$。并且有如下结论。

(1) 下列是乘法单位群 $(F*G)^{\times}$ 的一个子群：

$$K^* := \{e_0\} \times K_1^{\times} \cdots \times K_m^{\times}, \tag{4.1}$$

其中 $K_t^{\times} = K_t \backslash \{0\}$ 是域 K_t的乘法单位群。若 C是 A_t 的左理想，且 $\beta \in K_t^{\times}$，则 $C\beta$ 是 A_t 的一个左理想，且同构于 C （参见引理 2.5）。

(2) 若 $1_{A_t} = e$ 对于 e 的本原幂等元 FH 满足 $\bar{e} = e \neq e_0$，则我们选择 $K_t = FHe$，因此 $F_t = F = \{a \in K_t \mid \bar{a} = a\} = \mathrm{Z}(A_t)$ 如引理 3.7所述，其中 $\mathrm{Z}(A_t)$ 表示 A_t的中心。

引理 4.2。假设 $1_{A_t}=e+\bar{e}$ 对于 FH 的本原幂等元 e 满足 $\bar{e}\neq e$。令 $C_t=A_te$ 和 $\beta_t\in K_t^\times$。则 $C_t\beta_t$ 是 A_t 的单左理想，且 $\langle C_t\beta_t,\ C_t\beta_t\rangle=0$。

证明。设 $M:=\mathrm{M}_2(F_t)$，其中 $F_t=FHe$，见定理 3.8(1)。由式 (3.9)，$C_t=A_te$ 对应于 $M\cdot\begin{pmatrix}1&0\\0&0\end{pmatrix}$，它是 M 的一个单左理想。因此，C_t 和 $C_t\beta_t$ 是 A_t 的单左理想。若 $C_t\beta_t=C_t$，则 $C_t\beta_t\cdot\overline{C_t\beta_t}=A_te\overline{A_te}=A_te\bar{e}A_t=0$。由注记 3.4 和引理 2.1(5)，$\langle C_t\beta,C_t\beta\rangle=0$。下文中，我们假设 $C_t\beta_t\neq C_t$。由引理 3.6 和引理 2.5，单左理想 $C_t\beta_t$ 对应于 M 的单左理想 Mf，如下所示

$$C_t\beta_t\ \longleftrightarrow\ Mf,\qquad f=\begin{pmatrix}a&1\\0&0\end{pmatrix},\ \ a\in F_t.$$

令 $f'\in A_t$ 通过同构 $f\in M$ 式 (3.9) 对应。于是 $C_t\beta_t=A_tf'$。由引理 3.6(2)（参见式 (3.10)），$\overline{f'}$ 对应于矩阵 $\begin{pmatrix}0&-1\\0&a\end{pmatrix}$。因为

$$\begin{pmatrix}a&1\\0&0\end{pmatrix}\begin{pmatrix}0&-1\\0&a\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix},\ \ \text{hence}\ \ f'\cdot\overline{f'}=0.$$

因此 $C_t\beta_t\cdot\overline{C_t\beta_t}=A_tf'\cdot\overline{f'}A_t=0$，即 $\langle C_t\beta_t,C_t\beta_t\rangle=0$。 □

引理 4.3. 假设 $1_{A_t}=e$ 是 e 的一个本原幂等元，FH 满足 $\bar{e}=e\neq e_0$，并令 $C_t=A_tf$ 其中 $f=se-s'ue+\dot{v}e\in A_t$ 满足 $s,\ s'\in F_t$ 如等式(3.11)所示。则 C_t 是 A_t 的一个单左理想，且对于任意 $\beta_t\in K_t^\times$，

$$\langle C_t\beta_t,C_t\beta_t\rangle=\begin{cases}0, & \textit{if } q \textit{ is even or } 4\,\big|\,(q^{k_t}-1);\\ F, & \textit{otherwise.}\end{cases}\tag{4.2}$$

证明。注意，在这种情况下我们取 $K_t=FHe$，$F_t=\{a\,|\,a\in K_t,\overline{a}=a\}=\mathrm{Z}(A_t)$ 满足 $|K_t:\ F_t|=2$，参见定理 3.8(2) 和注 4.1(2)。由等式(3.11)及其记号，$g,\ s,\ s'\in F_t$ 满足：g 和 2 不同时为零，$g\neq\pm2$这意味着 $\det\begin{pmatrix}2&g\\g&2\end{pmatrix}\neq0$，且 $s^2+gss'+s'^2=-1$。因此矩阵

$$s\varepsilon-s'\eta+\nu=\begin{pmatrix}2s+gs'&0\\gs+2s'&0\end{pmatrix}$$

的第一列非零，因此秩$(s\varepsilon-s'\eta+\nu)\ =1$。由引理 2.5(1)，$\mathrm{M}_2(F_t)(s\varepsilon-s'\eta+\nu)$ 是 $\mathrm{M}_2(F_t)$ 的单左理想。由同构等式(3.12)，$s\varepsilon-s'\eta+\nu$ 对应于元素 $f=se-s'ue+\dot{v}e\in A_t$，且$C_t=A_tf$ 是 A_t的单左理想。对于 $\beta_t\in K_t^\times$，显然，$\overline{\beta_t\bar{\beta}_t}=\beta_t\bar{\beta}_t$；所以$\beta_t\beta_t\in F_t=\mathrm{Z}(A_t)$。于是我们得到

$$C_t\beta_t\cdot\overline{C_t\beta_t}=A_tf\beta_t\cdot\overline{A_tf\beta_t}=A_t\,f\beta_t\overline{\beta}_t\,\overline{f}\,\overline{A}_t=A_t\,f\,\overline{f}\,\beta_t\,\overline{\beta}_tA_t.$$

因此， $C_t\beta \cdot \overline{C_t\beta} = 0$ 当且仅当 $f\,\overline{f} = 0$。由于 $\overline{u} = u^{-1}$ 和 $\overline{v} = -v$，我们得到

$$\begin{aligned} f\bar{f} &= (se - s'ue + \dot{v}e)\cdot\overline{(se - s'ue + \dot{v}e)} \\ &= (se - s'ue + \dot{v}e)\cdot(se - s'u^{-1}e - \dot{v}e) \\ &= (s^2 + s'^2 + 1)e - ss'(u^{-1}e + ue) + s'(ue - u^{-1}e)\dot{v}e. \end{aligned}$$

根据式（3.12）， $u^{-1}e$ 对应于矩阵

$$\eta^{-1} = \begin{pmatrix} -g & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & -g \end{pmatrix}.$$

因此我们有如下对应关系：

$$u^{-1}e + ue \longleftrightarrow \begin{pmatrix} -g & 0 \\ 0 & -g \end{pmatrix}, \qquad ue - u^{-1}e \longleftrightarrow \begin{pmatrix} -g & 2 \\ -2 & g \end{pmatrix}.$$

因此， $ue - u^{-1}e$ 是可逆的，因为 $\det \begin{pmatrix} g & -2 \\ 2 & -g \end{pmatrix} = 4 - g^2 \neq 0$。而 $(s^2 + s'^2 + 1)\,e - ss'(u^{-1}e + ue)$ 对应于矩阵

$$(s^2 + s'^2 + 1)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - ss'\begin{pmatrix} -g & 0 \\ 0 & -g \end{pmatrix}.$$

由于 $s^2 + s'^2 + 1 + gss' = 0$，我们得到 $(s^2 + s'^2 + 1)\,e - ss'(u^{-1}e + ue) = 0$。因此

$$f\,\bar{f} = s'(ue - u^{-1}e)\dot{v}e, \qquad ue - u^{-1}e,\ \dot{v}e \in A_t^{\times}. \tag{4.3}$$

由此可知， $f\,\bar{f} = 0$ 当且仅当 $s' = 0$。由于 s， $s' \in F_t$ 且 $|F_t| = q^{k_t}$，式（4.2）由引理 2.4即可得出。 □

注 4.4. 下文中我们始终固定：

— $C_t = A_t e$ as in Lemma 4.2 if it is the case of Theorem 3.8(1);

— $C_t = A_t f$ as in Lemma 4.3 if it is the case of Theorem 3.8(2);

并考虑以下常二面体码

$$C = C_1 \oplus \cdots \oplus C_m. \tag{4.4}$$

我们有如下结论：

（1）对于 C 在式（4.4）中的码率 $\mathrm{R}(C) = \frac{1}{2} - \frac{1}{2n}$，因为

$$\dim_F C = \sum_{t=1}^{m} \dim_F C_t = 2\sum_{t=1}^{m} k_t = n - 1. \tag{4.5}$$

(2) 由 $C_t^{\perp_{A_t}}$表示 C_t 在 A_t中的正交子模（左理想）（参见推论 3.9），因此 $C_t \cap C_t^{\perp_{A_t}}$仍是 A_t的左理想。由于 C_t 是单的， $C_t \cap C_t^{\perp_{A_t}}$要么是 C_t，要么是 0。因此，

$$C_t \cap C_t^{\perp_{A_t}} = \begin{cases} C_t, & \langle C_t, C_t\rangle = 0; \\ 0, & \text{otherwise.} \end{cases} \tag{4.6}$$

引理 4.5。假设 q 是奇数，且 $4 \nmid (q-1)$。假设存在 m' 个指标 $1 \le i_1 < \cdots < i_{m'} \le m$，使得对于 $t = 1$、$\cdots$、m'、$e_{i_t} = \overline{e}_{i_t}$，$k_{i_t}$ 是奇数。令 $C' = C_{i_1} \oplus \cdots \oplus C_{i_{m'}}$ 和 $C' = A_0 \oplus C'$。那么对于任意 $\beta \in K^*$，$\prec C'\beta$ 和 $C'\beta$ 都是 LCD 常二面体码。

证明。注意到 $q^{k_{i_t}} - 1 = (q-1)(q^{k_{i_t}-1} + q^{k_{i_t}-2} + \cdots + q + 1)$。由于 k_{i_t}和 q均为奇数，且 $4 \nmid (q-1)$，故有 $4 \nmid (q^{k_{i_t}} - 1)$。令 $\beta = e_0 + \beta_1 + \cdots + \beta_m$，其中当 $t = 1, \cdots, m$时，$\beta_t \in K_t^{\times}$。则

$$C'\beta = C_{i_1}\beta_{i_1} + \cdots + C_{i_{m'}}\beta_{i_{m'}}.$$

由引理 4.3，$\langle C_{i_t}\beta_{i_t}, C_{i_t}\beta_{i_t}\rangle \neq 0$对于 $t = 1$，$\cdots$，m'。由式(4.6)，可得$C_{i_t}\beta_{i_t} \cap (C_{i_t}\beta_{i_t})^{\perp_{A_{i_t}}} = 0$。于是 $C_{i_t}\beta_{i_t}$是 A_{i_t}中的一个 LCD 常二面体码。由引理 3.9 (5)，$C'\beta$ 是一个 LCD 常二面体码。此外，由引理 3.5(1)，$\prec\langle A_0, A_0\rangle = A_0\overline{A_0} = A_0 \neq 0$；因此 $C'\beta$ 是一个 LCD 常二面体码。 □

对于整数 s, t 和素数 p，$p^s \| t$ 表示 $p^s \mid t$，但 $p^{s+1} \nmid t$。

定理 4.6. 假设 q 为奇数且 $4 \nmid (q-1)$。假设 $-1 \in \langle q\rangle_{\mathbb{Z}_n^{\times}}$ 且 $2 \| \mathrm{ord}^{\mathbb{Z}_n^{\times}}(q)$。那么对任意 $\beta \in K^*$，$C\beta$ 和 $A_0 \oplus C\beta$ 都是 LCD 常二面体码。

证明. 由于 $-1 \in \langle q\rangle_{\mathbb{Z}_n^{\times}}$，由引理 2.2(1) 可得 $\overline{e}_t = e_t$，$t = 1, \cdots, m$。由引理 4.5，只需证明对于 $1 \le t \le m$，任意 k_t 都是奇数。由定理 3.8(2)，$k_t = \frac{1}{2}\dim_F FHe_t$，即 FHe_t 是 F 上次数为 $2k_t$ 的域扩张。存在一个 q-陪集 $Q \subseteq \mathbb{Z}_n$，使得 $\dim_F FHe_t = |Q|$。然而，$|Q|$ 是 $\mathrm{ord}^{\mathbb{Z}_n^{\times}}(q)$ 的一个因子。因此，根据假设 $2 \| \mathrm{ord}^{\mathbb{Z}_n^{\times}}(q)$，$k_t = \frac{1}{2}|Q|$ 是奇数。 □

定理 4.7. 假设 q为偶数，或 $4 \mid (q-1)$，假设 $r \in F$满足 $r^2 = -1$。令 $C_0 = A_0(re_0 + e_0\dot{v})$如引理 3.5(2) 中所定义，并且

$$\widehat{C} = C_0 \oplus C = C_0 \oplus C_1 \oplus \cdots \oplus C_m.$$

那么，对于任意 $\beta \in K^*$，$C\beta$ 是一个自对偶常二面体码。

证明. 由等式(4.1)，可写为 $\beta = e_0 + \beta_1 + \cdots + \beta_m$ 其中 $\beta_t \in K_t^{\times}$对于 $t = 1$，$\cdots$，m。于是

$$\widehat{C}\beta = C_0 \oplus C_1\beta_1 \oplus \cdots \oplus C_m\beta_m,$$

并由推论3.9(2)，

$$\langle \widehat{C}\beta, \widehat{C}\beta\rangle = \langle C_0, C_0\rangle + \langle C_1\beta_1, C_1\beta_1\rangle + \cdots + \langle C_m\beta_m, C_m\beta_m\rangle.$$

由引理 4.2 和引理 4.3，$\langle C_t\beta_t, C_t\beta_t\rangle = 0$、$t = 1$、$\cdots$、$m$。由引理 3.5，$\prec\langle C_0, C_0\rangle = 0$。因此，$C\beta$ 是自正交的。最后，由引理 3.5 和式 (4.5)，$\dim_F(C\beta) = \dim_F(C_0) + \dim_F(C) = n$。所以，$C\beta$ 是自对偶的。 □

注 4.8. 回顾一下，对于任意子集 $I_* = \{i_1, \cdots, i_k\} \subseteq I = \{1, 2, \cdots, n\}$($1 \le i_1 < \cdots < i_k \le n$)，存在投影 $\rho_{I_*}: F^I \to F^{I_*}$，$(a_1, a_2 \cdots, a_n) \mapsto (a_{i_1}, \cdots, a_{i_k})$。对于 $B \subseteq F^n$ 且满足 $|B| = q^k$ 的情形，如果存在 $\{1, 2, \cdots, n\}$ 的子集（允许重复） I_1、$\cdots$、I_s，使得：(1) 对于 $1 \le j \le s$，投影ρ_{I_j}：$F^n \to F^{I_j}$将 B双射到 F^{I_j}（这样的 I_j称为码 B的信息指标集）；(2) 存在一个整数 t，使得对于任意 $1 \le i \le n$，包含 i （即 $i \in I_j$）的子集 I_j 的数量等于 t；则 B 称为平衡码。一个重要结果（参见[9, 推论 3.4]）是，如果 B是平衡的，则对于 $0 \le \delta \le 1 - q^{-1}$，$|B^{\le \delta}| \le q^{kh_q(\delta)}$ 的基数为，其中

$$B^{\le \delta} = \{c \,|\, c \in B,\, \mathrm{w}(c) \le \delta n\}, \tag{4.7}$$

and

$$h_q(\delta) = \delta \log_q(q-1) - \delta \log_q(\delta) - (1-\delta)\log_q(1-\delta), \quad \delta \in [0, 1 - q^{-1}], \tag{4.8}$$

是 q-熵函数。容易看出，群码是平衡的，参见 [10,注 II.3]。并且也容易证明常循环码是平衡的，参见 [12, 引理 II.8]。

引理 4.9. 若 B是定义在 F上的常二面体码，则 B是平衡的；特别地，对于 $0 \le \delta \le 1 - q^{-1}$，基数为 $|B^{\le \delta}| \le q^{\dim_F B \cdot h_q(\delta)}$。

证明。对于任意 $a = \sum_{i=0}^{n-1} a_{i0} u^i \dot{v}^0 + \sum_{i=0}^{n-1} a_{i1} u^i \dot{v}^1 \in F*G$，作为 F^{2n}的一个字，

$$a = (a_{00}, a_{10}, \cdots, a_{n-1,0}, a_{01}, a_{11}, \cdots, a_{n-1,1}), \tag{4.9}$$

按标准基 Eq.(3.2) 编号的字 a 的坐标 $F*G$:

$$I = \{u^0\dot{v}^0, u^1\dot{v}^0, \cdots, u^{n-1}\dot{v}^0, u^0\dot{v}^1, u^1\dot{v}^1, \cdots, u^{n-1}\dot{v}^1\}.$$

令 Sym(I) 表示集合 I上的对称群。二面体群 G （如 Eq.(3.1) 所示）通过同态 I 作用在集合上 θ： $G \to \mathrm{Sym}(I)$， $g \mapsto \theta_g$如下所示： θ_u 是置换： θ_u $(u^i\dot{v}^j) = u^{i+1}\dot{v}^j$ （因为 $u \cdot u^i\dot{v}^j = u^{i+1}\dot{v}^j$），即

$$\theta_u = (u^0\dot{v}^0, u^1\dot{v}^0, \cdots, u^{n-1}\dot{v}^0)(u^0\dot{v}^1, u^1\dot{v}^1, \cdots, u^{n-1}\dot{v}^1) \tag{4.10}$$

是 I 的双循环置换；而 θ_v 是置换：

$$\theta_v(u^i\dot{v}^j) = \begin{cases} u^{n-i}\dot{v}, & j = 0; \\ u^{n-i}, & j = 1; \end{cases} \quad \left(\text{since } \dot{v}(u^i\dot{v}^j) = \begin{cases} u^{n-i}\dot{v}, & j = 0; \\ -u^{n-i}, & j = 1; \end{cases}\right) \tag{4.11}$$

即，

$$\theta_v = (u^0\dot{v}^0, u^0\dot{v}^1)(u^1\dot{v}^0, u^{n-1}\dot{v}^1)\cdots(u^{n-1}\dot{v}^0, u^1\dot{v}^1)$$

是 n 个 I对换的乘积。事实上，存在一个双射 $I \to G$ （去掉 $\dot{v}$中的点），使得如上由 θ 定义的 G 在 I 上的作用为

等价于自身上的 G 左正则作用。特别地， G 在 I上传递地作用。接下来，令 Θ_u 为置换 θ_u的置换矩阵，即

$$\Theta_u = \begin{pmatrix} Y & 0 \\ 0 & Y \end{pmatrix}_{2n\times 2n}, \quad \text{where } Y = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{pmatrix}_{n\times n}.$$

如式（4.11）所示，我们应取

$$\Theta_{\dot v} = \begin{pmatrix} 0 & -X \\ X & 0 \end{pmatrix}_{2n\times 2n}, \quad \text{where } X = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \iddots & 1 \\ & & & \\ \vdots & 0 & \iddots & \\ 0 & 1 & & \end{pmatrix}_{n\times n}.$$

根据式（4.9），任意 $a\in F*G$都对应于 F^{2n}中的一个字，即一个 $1\times 2n$矩阵；这样一来， $a\Theta_u$ 和 $a\Theta_{\dot v}$ 便有意义。根据式（4.10）和式（4.11），我们有

$$ua = a\Theta_u, \quad \dot v a = a\Theta_{\dot v}, \qquad \forall\, a\in F*G. \tag{4.12}$$

设 $J=\{u^{i_1}\dot v^0, u^{i_2}\dot v^0,\cdots,u^{i_s}\dot v^0, u^{j_1}\dot v^1, u^{j_2}\dot v^1,\cdots,u^{j_t}\dot v^1\}\subseteq I$， $s+t=k$， $0\le i_1<i_2<\cdots<i_s\le n-1$和 $0\le j_1<j_2<\cdots<j_t\le n-1$。对于 $a=\sum_{i=0}^{n-1}a_{i0}u^i\dot v^0+\sum_{i=0}^{n-1}a_{i1}u^i\dot v^1\in F*G$，由注 4.8可写为

$$\rho_J(a)=a_{i_1 0}u^{i_1}\dot v^0+\cdots+a_{i_s 0}u^{i_s}\dot v^0+a_{j_1 1}u^{j_1}\dot v^1+\cdots+a_{j_t 1}u^{j_t}\dot v^1;$$

由式(4.9)，我们可以将 $\rho_J(a)$ 视为 F^{2n} 中这样一个字：其 J 之外的坐标均为零。于是， $\rho_J(a)\Theta_u$($\rho_J(a)\Theta_{\dot v}$，分别）是有意义的，它是 F^{2n} 中的一个字，其 $\theta_u(J)$（分别是 $\theta_v(J)$）之外的坐标均为零。由式(4.12)， $\rho_J(a)\Theta_u=\rho_{\theta_u(J)}(ua)$ 和 $\rho_J(a)\Theta_{\dot v}=\rho_{\theta_v(J)}(\dot va)$。将 a 替换为 $u^{-1}a$（并将 a 替换为 $\dot v^{-1}a$），我们得到

$$\rho_{\theta_u(J)}(a)=\rho_J(u^{-1}a)\Theta_u, \quad \rho_{\theta_{\dot v}(J)}(a)=\rho_J(\dot v^{-1}a)\Theta_{\dot v}, \qquad \forall\, a\in F*G. \tag{4.13}$$

假设 $\dim_F B=k$，且 $I_*\subseteq I$ 是 B的信息指标集，即$|I_*|=k$且 $\rho_{I_*}(B)=F^{I_*}$。由于 B是 $F*G$的左理想， $u^{-1}B=B=\dot v^{-1}B$。注意， Θ_u 和 $\Theta_{\dot v}$ 均可逆。由式(4.13)，

$$\rho_{\theta_u(I_*)}(B)=\rho_{I_*}(u^{-1}B)\Theta_u=F^{\theta_u(I_*)}, \quad \rho_{\theta_v(I_*)}(B)=\rho_{I_*}(\dot v^{-1}B)\Theta_{\dot v}=F^{\theta_v(I_*)}.$$

换言之， $\theta_u(I_*)$ 和 $\theta_v(I_*)$ 都是 B 的信息指标集。对于任意$g\in G$，由于 g 可以写成若干个 u 和 v的乘积，因此 θ_g 是若干个 θ_u 和 θ_v的乘积；所以 $\theta_g(I_*)$ 也是 B 的信息指标集。

最后，固定一个信息指标集 $I_*\subseteq I$，它属于 B。那么， $2n$ 子集（允许重复）： $\theta_g(I_*)$、 $g\in G$，都是 B的信息指标集。又因为 G 作用于 I 具有传递性，根据[12, 引理 II，9], 存在一个整数 t，使得对于任意 $u^i\dot v^j\in I$，满足 $g\in G$ 的这类 $u^i\dot v^j\in\theta_g(I)$ 数量等于 t。结论是， B 是一个平衡码。 □

5 常二面体码的渐近性质

沿用第 3 节和第 4节中的记号。本节中我们始终记

$$A = A_1 \oplus \cdots \oplus A_m, \quad \text{where } A_t \cong \mathrm{M}_2(F_t),\ \dim_F A_t = 4k_t,\ t = 1, \cdots, m.$$

那么 $F*G = A_0 \oplus A$。根据推论 3.10，我们有

$$2k_t \geq \lambda(n),\ t = 1, \cdots, m; \qquad k_1 + \cdots + k_m = (n-1)/2. \tag{5.1}$$

我们进一步假设

$$\lambda(n)/2 \leq k_1 \leq k_2 \leq \cdots \leq k_m. \tag{5.2}$$

从现在起，设 δ 为满足以下条件的实数（$h_q(\delta)$ 在式（4.8）中有定义）

$$\delta \in (0, 1 - q^{-1}) \quad \text{and} \quad h_q(\delta) < 1/4. \tag{5.3}$$

在本节中，我们证明上一节构造的常二面体码是渐近良好的。

5.1 码率为 $\frac{1}{2} - \frac{1}{2n}$ 的常二面体码

在本小节中，我们考虑式（ $C = C_1 \oplus \cdots \oplus C_m$4.4中定义的常二面体码 $K^* = \{e_0\} \times K_1^\times \times \cdots \times K_m^\times$，其中每个域$K_t \subseteq A_t$ 的维数为 $\dim_F K_t = 2k_t$，见备注 4.1。对于任意 $\beta \in K^*$，$\beta = e_0 + \beta_1 + \cdots + \beta_m$，我们都有一个常二面体码 $C\beta = C_1\beta_1 \oplus \cdots \oplus C_m\beta_m$。

对于任意 $0 \neq d \in A$，存在唯一的子集 $\omega_d = \{t_1, \cdots, t_r\} \subseteq \{1, 2, \cdots, m\}$，使得 $d = d_{t_1} + \cdots + d_{t_r}$，其中对于 $i = 1$、$\cdots$、r，有 $d_{t_i} \in A_{t_i} \backslash \{0\}$；我们记作 $\ell_d = k_{t_1} + \cdots + k_{t_r}$，由等式（5.1）和等式（5.2），$k_1 \leq \ell_d \leq (n-1)/2$. (5.4)

引理 5.1。设 $0 \neq d \in A$。令 $\mathcal{K}(C)_d = \{\beta \in K^* \mid d \in C\beta\}$。则

$$|\mathcal{K}(C)_d| \leq |K^*|/q^{\ell_d}.$$

证明。假设 $\omega_d = \{t_1, \cdots, t_r\} \subseteq \{1, 2, \cdots, m\}$，且 $d = d_{t_1} + \cdots + d_{t_r}$对于 $d_{t_i} \in A_{t_i} \backslash \{0\}$。则 $d \in C\beta$当且仅当 $d_{t_i} \in C_{t_i}\beta_{t_i}$，$i = 1$，$\cdots$，$r$。该$C_{t_i}\beta_{t_i}$是 A_{t_i}的单左理想。在 A_{t_i}中，任意两个不同单左理想的交集均为 0；因此至多存在一个包含 C'_{t_i} 的 d_{t_i}。由引理 2.5(3)，恰有 $q^{k_{t_i}} - 1$ 个元素 β_{t_i} 属于 $K_{t_i}^\times$，使得$C_{t_i}\beta_{t_i} = C'_{t_i}$。因此

$$\left|\{\beta_{t_i} \in K_{t_i}^\times \mid d_{t_i} \in C_{t_i}\beta_{t_i}\}\right| \leq q^{k_{t_i}} - 1.$$

由于 $\dim_F K_{t_i} = 2k_{t_i}$，参见注释4.1，我们得到 $q^{k_{t_i}} - 1 = \frac{|K_{t_i}^\times|}{(q^{k_{t_i}}+1)}$。设 $\omega'_d = \{1, 2, \cdots, m\} \backslash \omega_d$。于是

$$|\mathcal{K}(C)_d| \leq \prod_{t' \in \omega'_d} |K_{t'}^\times| \cdot \prod_{t \in \omega_d} \frac{|K_t^\times|}{q^{k_t}+1} = \prod_{t=1}^{m} |K_t^\times| \Big/ \prod_{t \in \omega} (q^{k_t}+1) \leq |K^*| \Big/ \prod_{t \in \omega} q^{k_t},$$

即，$|\mathcal{K}(C)_d| \leq |K^*|/q^{k_{t_1}+\cdots+k_{t_r}} = |K^*|/q^{\ell_d}$。 □

记作

$$\Omega = \{A_{t_1} \oplus \cdots \oplus A_{t_r} \mid \{t_1, \cdots, t_r\} \subseteq \{1, \cdots, m\}\}, \tag{5.5}$$

其为 A 的所有理想构成的集合。

引理 5.2。设 $\mathcal{K}(C)^{\leq\delta} = \{\beta \in K^* \mid \Delta(C\beta) \leq \delta\}$。若 $\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{\lambda(n)}() > 0$，则

$$\left|\mathcal{K}(C)^{\leq\delta}\right| \leq |K^*| \cdot q^{-2\lambda(n)\left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{\lambda(n)}\right)}. \tag{5.6}$$

证明。对于任意子集 $\omega \subseteq \{1, \cdots, m\}$，记作 $A_\omega = \bigoplus_{t\in\omega} A_t$，因此 $A_\omega \in \Omega$。对于 $k_1 \leq \ell \leq \frac{n-1}{2}$，令

$$\begin{aligned} \mathcal{A}_\ell &= \left\{ A_\omega \in \Omega \;\middle|\; \dim_F A_\omega = 4\ell \right\}; \\ \mathcal{D}_\ell &= \left\{ d \in A \;\middle|\; 0 < \mathrm{w}(d)/2n \leq \delta,\, \ell_d = \ell \right\}. \end{aligned} \tag{5.7}$$

对于 $A_\omega \in \mathcal{A}_\ell$，$\dim_F A_\omega = 4\sum_{t\in\omega} k_t = 4\ell$ 以及 $k_t \geq k_1$，根据假设 Eq.(5.2)，有 $|\omega| \leq \ell/k_1$。因此，

$$|\mathcal{A}_\ell| \leq m^{\ell/k_1} \leq n^{\ell/k_1}. \tag{5.8}$$

显然（其中 $A_\omega{}^{\leq\delta}$ 在 Eq.(4.7) 中定义）

$$\mathcal{D}_\ell \subseteq \bigcup_{A_\omega\in\mathcal{A}_\ell} A_\omega{}^{\leq\delta} \qquad \text{and} \qquad \mathcal{K}(C)^{\leq\delta} = \bigcup_{\ell=k_1}^{(n-1)/2} \bigcup_{d\in\mathcal{D}_\ell} \mathcal{K}(C)_d. \tag{5.9}$$

根据引理 4.9，对于 $A_\omega \in \mathcal{A}_\ell$，有 $|A_\omega{}^{\leq\delta}| \leq q^{4\ell h_q(\delta)}$，因为 $\dim_F A_\omega = 4\ell$。由 Eq.(5.9)，得到

$$|\mathcal{D}_\ell| \leq \sum_{A_\omega\in\mathcal{A}_\ell} |A_\omega{}^{\leq\delta}| \leq |\mathcal{A}_\ell| \cdot q^{4\ell h_q(\delta)} \leq n^{\frac{\ell}{k_1}} q^{4\ell h_q(\delta)} = q^{4\ell h_q(\delta) + \frac{\ell \log_q n}{k_1}}.$$

根据引理 5.1，$|\mathcal{K}(C)_d| \leq |K^*|/q^\ell$。由式（5.9）可得

$$\begin{aligned} |\mathcal{K}(C)^{\leq\delta}| &\leq \sum_{\ell=k_1}^{(n-1)/2} \sum_{d\in\mathcal{D}_\ell} |\mathcal{K}(C)_d| \leq \sum_{\ell=k_1}^{(n-1)/2} \sum_{d\in\mathcal{D}_\ell} |K^*|/q^\ell = \sum_{\ell=k_1}^{(n-1)/2} |\mathcal{D}_\ell| \cdot |K^*|/q^\ell \\ &\leq \sum_{\ell=k_1}^{(n-1)/2} |K^*| \cdot q^{4\ell h_q(\delta) + \frac{\ell \log_q n}{k_1}}/q^\ell = \sum_{\ell=k_1}^{(n-1)/2} |K^*| \cdot q^{-4\ell\left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{4k_1}\right)}. \end{aligned}$$

因为 $\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{4k_1} > 0$ 和 $\ell \geq k_1$，我们进一步得到

$$\left|\mathcal{K}(C)^{\leq\delta}\right| \leq \sum_{\ell=k_1}^{(n-1)/2} q^{-4k_1\left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{4k_1}\right)} |K^*| \leq q^{-4k_1\left(\frac{1}{4} - h_q(\delta)\right) + 2\log_q n} |K^*|.$$

最后一个不等式成立是因为 $\frac{n-1}{2}-k_1+1 \le n = q^{\log_q n}$。此外，$\frac{1}{4}-h_q(\delta) > 0$和 $2k_1 \ge \lambda(n)$。因此

$$\left|\mathcal{K}(C)^{\le\delta}\right| \le |K^*|\cdot q^{-4k_1\left(\frac{1}{4}-h_q(\delta)\right)+2\log_q n} \le |K^*|\cdot q^{-2\lambda(n)\left(\frac{1}{4}-h_q(\delta)\right)+2\log_q n}.$$

即，$\left|\mathcal{K}(C)^{\le\delta}\right| \le |K^*|\cdot q^{-2\lambda(n)\left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{\lambda(n)}\right)}$。□

注 5.3. 设 $\mathcal{P}$ 为所有素数的集合，$\mathcal{P}_t$ 为小于或等于 t 的素数集合。记 $\mathcal{G}_t = \{p \in \mathcal{P} \mid q < p \le t, \mathrm{ord}_p^{\mathbb{Z}^\times}(q) \ge (\log_q t)^2\}$，并记 $\mathcal{G} = \bigcup_{t=1}^{\infty} \mathcal{G}_t$。那么 $\mathcal{G}$ 的密度为 $\lim\limits_{t\to\infty} |\mathcal{G}_t|/|\mathcal{P}_t| = 1$，见 [10, 引理 II.6]。因此，根据引理 2.3，存在正奇整数 n_1、n_2、$\cdots$，使得每个 n_i 都与 q 和 $n_i \to \infty$ 互素，从而

$$\lim_{i\to\infty} \frac{\log_q n_i}{\lambda(n_i)} = 0. \tag{5.10}$$

定理 5.4。设 δ如公式（5.3）所示，且 n_1、n_2、$\cdots$如公式（5.10）所示。则存在长度为 $C^{(i)}$的常二面体码 $2n_i$，对于 $i = 1$、2、$\cdots$，使得

(1) $C^{(i)}$ 的长度 $2n_i$ 趋于无穷大；

(2) $\mathrm{R}(C^{(i)}) = \frac{1}{2} - \frac{1}{2n_i}$ 对于 $i = 1$、2、$\cdots$；

(3) 相对最小距离 $\Delta(C^{(i)}) > \delta$ 对于 $i = 1$、2、$\cdots$；

因此，码序列 $C^{(1)}$、$C^{(2)}$、$\cdots$是渐近良好的。

证明。由于 $\frac{1}{4} - h_q(\delta) > 0$，通过舍去有限项（如有必要），我们可以进一步假设序列 $n_1, n_2, \cdots$满足式(5.10)，并且$\frac{1}{4} - h_q(\delta) - \log_{q^{n_i}}\lambda(n_i) > 0$，对于 $i = 1, 2, \cdots$。在引理 5.2中，取 $n = n_i$，得到

$$\lim_{i\to\infty} \frac{\left|\mathcal{K}(C)^{\le\delta}\right|}{|K^*|} \le \lim_{i\to\infty} q^{-2\lambda(n_i)\left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n_i}{\lambda(n_i)}\right)} = 0.$$

因此，对于 $i = 1, 2, \cdots$，我们可以取 $\beta^{(i)} \in K^*\backslash\mathcal{K}(C)^{\le\delta}$。令 $C^{(i)} = C\beta^{(i)}$。则 $C^{(i)}$ 是一个长度为 $2n_i$ 的常二面体码，且所得码序列

$$C^{(1)}, C^{(2)}, \cdots \tag{5.11}$$

满足陈述 (1)、(2) 和 (3)。□

备注 $\mathcal{G}$ 中素数集合的密度 5.3 等于 1，因此我们可以从 $\mathcal{G}$ 中取一些满足更多条件的子集。

引理 5.5 ([10, 推论 II。8])。存在正奇整数 n_1，n_2，$\cdots$使得每个 n_i 都与 q 互素，且 $n_i \to \infty$ 满足

$$\lim_{i\to\infty} \frac{\log_q n_i}{\lambda(n_i)} = 0; \qquad \mathrm{ord}_{\mathbb{Z}_{n_i}^\times}(q) \text{ is odd}, \quad \forall i = 1, 2, \cdots. \tag{5.12}$$

定理 5.6. 任意有限域 F上的自正交常二面体码都是渐近良好的。

证明。 取 n_1, n_2, $\cdots$如式（5.12）所示。根据引理 2.2（2），对于阶为 H 的循环群 n_i，除 e 之外的 FH 任一本原幂等元 e_0 均满足 $\overline{e} \neq e$。根据引理 4.2 和推论 3.9（4），式（ $C^{(i)}$5.11）中的长度为 $2n_i$ 的常二面体码是自正交的。 □

引理 5.7。假设 q 是奇数且 $4 \nmid (q-1)$。那么存在正奇整数 n_1、n_2、$\cdots$，其中每个 n_i 都与 q 和 $n_i \to \infty$ 互素，使得

$$\lim_{i\to\infty} \frac{\log_q n_i}{\lambda(n_i)} = 0; \quad -1 \in \langle q \rangle_{\mathbb{Z}_{n_i}^\times} \ and \ 2 \,\|\, \mathrm{ord}_{\mathbb{Z}_{n_i}^\times}(q), \ for \ i = 1, 2, \cdots, \tag{5.13}$$

其中“$2 \,\|\, t$”表示 $2 \,|\, t$，但 $2^2 \nmid t$。

证明。 令 $\mathcal{O} = \{ p \in \mathcal{P} \,|\, \text{阶}_{\mathbb{Z}_p^\times}(q) \text{ 为奇数} \}$ 且 $\overline{\mathcal{O}} = \mathcal{P} \backslash \mathcal{O}$。根据假设，我们可以写成 $q = r^s$，其中 r 是奇素数，s 是奇正整数。根据 [22,定理 1]，$\mathcal{P}$ 中 $\mathcal{O}$ 的密度等于 1 3，因此 $\overline{\mathcal{O}}$ 的密度等于 2 3。另一方面，我们考虑

$$\mathcal{T} = \left\{ p \in \mathcal{P} \,\middle|\, 2 \,\|\, (p-1) \right\} = \left\{ p \in \mathcal{P} \,\middle|\, p \equiv 3 \pmod 4 \right\}.$$

根据狄利克雷密度定理（参见 [23, 第 6 章第 4 节定理 2]），$\mathcal{P}$中 $\mathcal{T}$的密度等于 1 2。因此，$\overline{\mathcal{O}} \cap \mathcal{T}$ 的密度至少为 $\frac{2}{3} + \frac{1}{2} - 1 = \frac{1}{6}$。因此，$\overline{\mathcal{O}} \cap \mathcal{T} \cap \mathcal{G}$ 的密度至少为 1 6，其中 $\mathcal{G}$的定义见注 5.3。对于任意$p \in \overline{\mathcal{O}_t} \cap \mathcal{T} \cap \mathcal{G}$，我们有 $-1 \in \langle q \rangle_{\mathbb{Z}_p^\times}$（，因为：$\mathrm{ord}_{\mathbb{Z}_p^\times}(q)$ 是偶数，且 -1 是 $\mathbb{Z}_p^\times$)中阶为 2 的唯一元素；并且 $2 \,\|\, \mathrm{ord}_{\mathbb{Z}_p^\times}(q)$（，因为：$\mathrm{ord}_{\mathbb{Z}_p^\times}(q) \,|\, (p-1)$，但 $4 \nmid (p-1)$)。因此，存在正奇整数 n_1、n_2、$\cdots$，使得每个 n_i都与 q 互素，并且 $n_i \to \infty$，从而等式 (5.13) 成立。 □

定理 5.8. 假设 q是奇数且 $4 \nmid (q-1)$（即 $q \equiv 3$ (模 4)）。那么，F 上的 LCD 常二面体码渐近良好。特别地，F 上的指标 2 LCD 准循环码渐近良好。

证明。 取 n_1, n_2, $\cdots$如方程（5.13）所示。由定理 4.6，方程（ $C^{(i)}$）中长度为 $2n_i$ 的5.11）是 LCD 常二面体码。因此，方程（5.11）中的 LCD 常二面体码序列渐近良好。由方程（3.8），任何常循环码都是指标 2 的拟循环码。因此，“特别地”部分得证。 □

5.2 自对偶常二面体码

在本小节中，我们始终假设 q为偶数，或者 $4 \,|\, (q-1)$，即 $q \not\equiv 3$ (模 4)。沿用定理 4.7中的记号：

- $\widehat{C} = C_0 \oplus C = C_0 \oplus C_1 \oplus \cdots \oplus C_m$ where $C_0 = A_0(re_0 + e_0\dot{v})$ is defined in Lemma 3.5(2);

• 对于任意 $\beta = e_0 + \beta_1 + \cdots + \beta_m \in K^*$，常二面体码

$$\widehat{C}\beta = C_0 \oplus C_1\beta_1 \oplus \cdots \oplus C_m\beta_m$$

是自对偶的；特别地，码率 R($\widehat{C}\beta$) $= \frac{1}{2}$。

^我们将找出满足相对最小距离 $\Delta(C\beta) > \delta$的 β。

^注意 $F{*}G = A_0 \oplus A$。对于任意满足 $d_0 \in A_0$ 且 ^ ^$d \in A$ 的 $d = d_0 + d \in F{*}G$，若 $d_0 \notin C_0$，则对于任意 $\beta \in K^*$，都有 $d \notin C\beta$。

^引理 5.9。假设 $0 \neq d = d_0 + d \in C_0 \oplus A$ 满足 $d_0 \in C_0$ 且 $d \in A$。

^ ^ ^令 $\mathcal{K}(C)_{\widehat{d}} = \{\beta \in K^* \mid d \in C\beta\}$。则

$$\left|\mathcal{K}(\widehat{C})_{\widehat{d}}\right| \leq |K^*|/q^{\ell_d}.$$

其中 ℓ_d 定义见公式(5.4)。

^ ^证明。显然，$d \in C\beta$ 当且仅当 $d \in C\beta$。因此，该引理可由引理5.1立即得出。 □

引理 5.10. 设 $\mathcal{K}(\widehat{C})^{\leq\delta} = \{\beta \in K^* \mid \Delta(\widehat{C}\beta) \leq \delta\}$。若 $\frac{1}{4} - h_q(\delta) - \log_{\lambda}\frac{q^n}{n}() > 0$，则

$$\left|\mathcal{K}(\widehat{C})^{\leq\delta}\right| \leq |K^*| \cdot q^{-2\lambda(n)\left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{\lambda(n)}\right) + h_q(\delta)}. \tag{5.14}$$

证明。对于 $k_1 \leq \ell \leq \frac{n-1}{2}$，我们扩展式（$\mathcal{D}_\ell$ 中的记号5.7），并设

$$\widehat{\mathcal{D}}_\ell = \left\{\widehat{d} = d_0 + d \;\middle|\; d_0 \in C_0,\, d \in A,\, 0 < \mathrm{w}(\widehat{d})/2n \leq \delta,\, \ell_d = \ell\right\}.$$

由 $\mathcal{A}_\ell$ 在式（5.7）中的定义，可得

$$\widehat{\mathcal{D}}_\ell \subseteq \bigcup_{A_\omega \in \mathcal{A}_\ell} (C_0 \oplus A_\omega)^{\leq\delta} \quad \text{and} \quad \mathcal{K}(\widehat{C})^{\leq\delta} = \bigcup_{\ell=k_1}^{(n-1)/2} \bigcup_{\widehat{d} \in \widehat{\mathcal{D}}_\ell} \mathcal{K}(\widehat{C})_{\widehat{d}}. \tag{5.15}$$

对于 $A_\omega \in \mathcal{A}_\ell$，有 $|(C_0 \oplus \mathcal{A}_\omega)^{\leq\delta}| \leq q^{(4\ell+1)h_q(\delta)}$，因为 $\dim_F(C_0 \oplus A_\omega) = 4\ell + 1$；见引理 4.9。由式（5.15）和式（5.8），可得

$$|\widehat{\mathcal{D}}_\ell| \leq \sum_{A_\omega \in \mathcal{A}_\ell} |(C_0 \oplus \mathcal{A}_\omega)^{\leq\delta}| \leq n^{\frac{\ell}{k_1}} q^{(4\ell+1)h_q(\delta)} = q^{4\ell h_q(\delta) + \frac{\ell \log_q n}{k_1} + h_q(\delta)}.$$

^ ^对于 $d = d_0 + d \in D_\ell$，我们有 $\ell_d = \ell$。由等式(5.15)和引理 5.9，

$$\begin{aligned}\left|\mathcal{K}(\widehat{C})^{\leq\delta}\right| &\leq \sum_{\ell=k_1}^{(n-1)/2} \sum_{\widehat{d} \in \widehat{\mathcal{D}}_\ell} \left|\mathcal{K}(\widehat{C})_{\widehat{d}}\right| \leq \sum_{\ell=k_1}^{(n-1)/2} \sum_{\widehat{d} \in \widehat{\mathcal{D}}_\ell} |K^*|/q^\ell \\ &= \sum_{\ell=k_1}^{(n-1)/2} |\widehat{D}_\ell| \cdot |K^*|/q^\ell \leq \sum_{\ell=k_1}^{(n-1)/2} |K^*| \cdot q^{4\ell h_q(\delta) + \frac{\ell \log_q n}{k_1} + h_q(\delta)}/q^\ell.\end{aligned}$$

因此，

$$\begin{aligned}\left|\mathcal{K}(\widehat{C})^{\leq\delta}\right| &= \sum_{\ell=k_1}^{(n-1)/2} |K^*|\cdot q^{-4\ell\left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{4k_1}\right)+h_q(\delta)} \\ &\leq \sum_{\ell=k_1}^{(n-1)/2} |K^*|\cdot q^{-4k_1\left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{4k_1}\right)+h_q(\delta)}.\end{aligned}$$

根据引理 5.2的相同论证，我们可以得到

$$\sum_{\ell=k_1}^{(n-1)/2} q^{-4k_1\left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{4k_1}\right)+h_q(\delta)} \leq q^{-2\lambda(n)\left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{\lambda(n)}\right)+h_q(\delta)}.$$

证明完毕。 □

定理 5.11。假设 q为偶数或 $4\,|(q-1)$。令 δ如式 (5.3) 所示，令 n_1、n_2、$\cdots$如式 (5.10) 所示。则存在长度为 $2n_i$的自对偶常二面体码 $\widehat{C}^{(i)}$，使得对于所有 $i=1$、2、$\cdots$，$\Delta(\widehat{C}^{(i)})>\delta$；因此，码序列 $\widehat{C}^{(1)}$、$\widehat{C}^{(2)}$、$\cdots$是渐近良好的。

证明。 在引理 5.10中，令 $n=n_i$，于是

$$\lim_{i\to\infty}\frac{\left|\mathcal{K}(\widehat{C})^{\leq\delta}\right|}{|K^*|} \leq \lim_{i\to\infty} q^{-2\lambda(n_i)\left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n_i}{\lambda(n_i)}\right)+h_q(\delta)} = 0.$$

对于 $i=1$、2、$\cdots$，我们可以取 $\beta^{(i)}\in K^*\backslash\mathcal{K}(\widehat{C})^{\leq\delta}$。令 $\widehat{C}^{(i)}=\widehat{C}\beta^{(i)}$。则 $\widehat{C}^{(i)}$是一个长度为 $2n_i$ 的自对偶常二面体码，并且码序列

$$\widehat{C}^{(1)},\widehat{C}^{(2)},\cdots \tag{5.16}$$

满足 $\Delta(\widehat{C}^{(i)})>\delta$对于 $i=1,2,\cdots$。 □

我们立即得到以下结论（参见定理 5.8的证明）。

定理 5.12. 假设 q是偶数或 $4\,|(q-1)$（即 $q\not\equiv 3$(模 4)）。那么， F上的自对偶常二面体码是渐近良好的。特别地， F 上的指标 2 自对偶准循环码是渐近良好的。

已知，若 q 为奇数，则码率为 $1\ 2$ 的 LCD二面体码是渐近良好的，见 [10, 定理 1。2]。由此可得以下推论。

推论 5.13. 若 $q\equiv 1\pmod 4$，则 F 上指标 2 的自对偶准循环码以及 F 上码率为 $1\ 2$ 的指标 2 LCD 准循环码均为渐近良好码。

6 二面体码的注记

本节旨在纠正 [10] 中的一些错误。我们先从一条微妙的说明开始。

注记 6.1。 引理 2.1(5)（即 [10, 引理 II.4(5)]）提供了一种有效评估群码正交性的技术，即对于 FG-码 C， D，

$$\langle C, D\rangle = 0 \quad \Longleftrightarrow \quad C\overline{D} = 0. \tag{6.1}$$

然而，有一点需要注意：以下说法并不正确：

$$\langle C, D\rangle = 0 \quad \Longrightarrow \quad \overline{D}C = 0. \tag{6.2}$$

下面给出一个关于式（6.2）的反例。

例。设 $|F| = 7$, $n = 3$, $G = \langle u, v \,|\, u^3 = 1 = v^2, vuv^{-1} = u^{-1}\rangle = H \rtimes \langle v\rangle$ 为阶为 6 的二面体群，其中 $H = \{1, u, u^2\}$ 是阶为 3 的循环群。则1_3 在 F 中等于 5，而 2、4 是 3 次本原单位根。 $e_0, e, \bar{e}$ 都是 FH的本原幂等元，其中

$$e_0 = 5(1 + u + u^2), \quad e = 5(1 + 2u + 4u^2), \qquad \bar{e} = 5(1 + 4u + 2u^2).$$

记 $FG = A_0 \oplus A_1$，其中

$$A_0 = FGe_0, \quad A_1 = FG(e + \bar{e}) = FHe \oplus FH\bar{e} \oplus FHev \oplus FH\bar{e}v,$$

是 FG 的极小理想。取 $C = D = A_1e = FHe \oplus FH\bar{e}v$。则

$$C\overline{D} = A_1e \cdot \overline{A_1e} = A_1e\bar{e}\overline{A}_1 = A_10\,\overline{A}_1 = 0.$$

根据方程(6.1)， $\langle C,\ D\rangle = 0$。然而， $\overline{D}C = \bar{e}\overline{A}_1 \cdot A_1e = \bar{e}A_1e \neq 0$，因为我们可以选取一个元素 $\bar{e}(\bar{e}v)e \in \bar{e}A_1e$ 以及 $\bar{e}(\bar{e}v)e = \bar{e}ve = \bar{e}\bar{e}v = \bar{e}v \neq 0$。

备注 6.2。 现在来看 [10] 中的错误。 [10] 中的主要问题是

(I) 在 [10, 定理 IV.3] 和 [10, 定理IV.5], 的证明中，有些地方引用了 [10, 引理 II.4(5)] (即方程 (6.1))，但实际上误用了错误版本的方程 (6.2)。

我们首先展示这一问题造成的影响，然后说明如何解决它。

[10, 定理 IV.3] 讨论 char(F) $= 2$的情形。尽管其证明中误用了错误的公式 (6.2)， [10, 定理 IV.3] 本身是正确的。因为：若 char(F) $= 2$，则 $-1 = 1$，常二面体群代数可视为二面体群代数，即 $F*G = FG$，参见公式 (3.3)；因此，本文的所有结果均适用于 FG 以及二面体码，前提是 char(F) 为偶数。因此，[10, 定理 IV.3] 是本文定理 4.7 （取偶数 q）的推论。

[10, 定理 IV.5] 讨论 char(F) 为奇数的情形，分为两部分：(1) $\mathrm{ord}_n^{\mathbb{Z}_n^\times}(q)$ 为奇数的情形；(2) $-1 \in \langle q \rangle_{\mathbb{Z}_n^\times}$ 的情形。对于 [10, 定理 IV.5(2)], , 尽管其证明存在漏洞，但结论仍然正确，并已在 [11, 引理 8.6(2)]中得到证明。对于 [10, 定理 IV.5(1)] （char(F) 为奇数且 $\mathrm{ord}_n^{\mathbb{Z}_n^\times}(q)$ 为奇数的情形），然而，错误地使用公式 (6.2) 导致了错误的结论，实属遗憾。

备注 6.3。 备注6.2 中所描述的问题意味着，在某些情况下，公式（6.1）不足以判断群码的正交性。本文发展了一种通过矩阵计算判断群码正交性的技术，例如，参见引理 4.2 和引理 4.3的证明。这是本文的贡献之一。为了通过该技术寻找 [10, 定理 IV.5(1)], 的正确表述，我们从引理 3.6的二面体群代数版本开始。

保留公式（3.1）和公式（2.3）中的假设。

˜引理 6.4。设 e 是 FH 的一个本原幂等元，且满足 $\overline{e} \neq e$。则 $F := FHe$ 是 F 上的一个域扩张， $e + \overline{e}$ 是 FG的一个本原中心幂等元，并且:

(1) *The ideal* $FG(e+\overline{e}) = FHe \oplus FH\bar{e} \oplus FHev \oplus FH\bar{e}v \cong \mathrm{M}_2(\tilde{F})$.

(2) 根据 (1) 中的同构，若 $f \in FG(e+\overline{e})$ 对应于矩阵 $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{M}_2(\tilde{F})$, 则 $\overline{f}$ 对应于矩阵 $\begin{pmatrix} a_{22} & a_{12} \\ a_{21} & a_{11} \end{pmatrix}$。

˜证明。 与引理 3.6的证明类似 $F := FHe$ 是 F 上的域扩张，并且 $e + \overline{e}$是 FG的本原中心幂等元。因此 $FG(e+\bar{e}) = FHe \oplus FHev \oplus FH\bar{e} \oplus FH\bar{e}v$是 FG的理想。定义映射:

$$\begin{array}{ccc} \mathrm{M}_2(\tilde{F}) & \xrightarrow{\cong} & FHe \oplus FHev \oplus FH\bar{e} \oplus FH\bar{e}v, \\ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} & \longmapsto & a_{11}e + a_{12}\, e\, v + \overline{a_{21}}\, \bar{e}\, v + \overline{a_{22}}\, \bar{e}, \end{array} \tag{6.3}$$

˜显然是一个线性同构。对于 a_{ij}、 $b_{ij} \in F$、 $1 \leq i$、 $j \leq 2$，注意到 $va_{ij} = \overline{a_{ij}}\, v$ 和 $v^2 = 1$，我们有

$$\begin{aligned} &\left(a_{11}e + a_{12}\, e\, v + \overline{a_{21}}\, \bar{e}v + \overline{a_{22}}\, \overline{e}\right)\left(b_{11}e + b_{12}e\, v + \overline{b_{21}}\, \bar{e}v + \overline{b_{22}}\, \overline{e}\right) \\ &\quad = (a_{11}b_{11} + a_{12}b_{21})e + (a_{11}b_{12} + a_{12}b_{22})e\, v + \\ &\quad\quad \overline{(a_{21}b_{11} + a_{22}b_{21})}\, \overline{e}\, v + \overline{(a_{21}b_{12} + a_{22}b_{22})}\, \overline{e}. \end{aligned}$$

˜因此，等式（6.3）是一个 F-代数同构。

对于 $a_{11}e + a_{12}\, e\, v + \overline{a_{21}}\, \bar{e}v + \overline{a_{22}}\, \overline{e} \in FHe \oplus FHev \oplus FH\bar{e} \oplus FH\bar{e}v$, 我们有（注意 $\overline{v} = v$）：

$$\begin{aligned} \overline{a_{11}e + a_{12}e\, v + \overline{a_{21}}\, \bar{e}\, v + \overline{a_{22}}\, \bar{e}} &= \overline{a_{11}}\, \bar{e} + \overline{v}\, \overline{a_{12}}\, \bar{e} + \overline{v}\, a_{21}\, e + a_{22}\, e. \\ &= a_{22}\, e + \ a_{12}\, e\, v + \overline{a_{21}}\, \bar{e}\, v + \overline{a_{11}}\, \bar{e}. \end{aligned}$$

因此， $a_{11}e+a_{12}\,e\,v+\overline{a_{21}}\,\bar{e}v+\overline{a_{22}}\,\bar{e}$ 的横杠像对应于矩阵：

$$\overline{a_{11}e+a_{12}e\,v+\overline{a_{21}}\,\bar{e}\,v+\overline{a_{22}}\,\bar{e}}\quad\longleftrightarrow\quad\begin{pmatrix}a_{22}&a_{12}\\a_{21}&a_{11}\end{pmatrix}. \tag{6.4}$$

我们完成了。 □

˜回顾引理 2.5(2)，总共有 $|F|+1$ 个 $\tilde{\mathrm{M}}_2(F)$ 的单左理想，其生成元为：

$$\begin{pmatrix}a&1\\0&0\end{pmatrix},\quad a\in\tilde{F};\qquad\text{or}\quad\begin{pmatrix}1&0\\0&0\end{pmatrix}. \tag{6.5}$$

引理 6.5。 沿用引理 6.4中的记号。简记 $A=FG(e+\bar{e})$为。设 $f_{ab}\in A$ 是对应于 $\begin{pmatrix}a&b\\0&0\end{pmatrix}\in\mathrm{M}_2(\tilde{F})$的元素。则

˜(1) 若 char$(F)=2$，则 $\langle Af_{ab}、\ Af_{ab}\rangle=0$，其中 $a、\ b\in F$。

(2) 若 char(F) 为奇数，则 $\langle Af_{ab}、\ Af_{ab}\rangle=0$ 当且仅当 $ab=0$；特别地， A 恰有两个单左理想在 A 中是自对偶的， A 的另外 $|F|-1$ 个单左理想在 A 中是 LCD。

证明。 根据引理 2.1(5)， $\langle Af_{ab},\ Af_{ab}\rangle=0$ 当且仅当 $f_{ab}\overline{f_{ab}}=0$。根据引理 6.4 (式(6.3)和式(6.4))， $f_{ab}f_{ab}=0$ 当且仅当

$$\begin{pmatrix}a&b\\0&0\end{pmatrix}\begin{pmatrix}0&b\\0&a\end{pmatrix}=\begin{pmatrix}0&2ab\\0&0\end{pmatrix}=0.$$

若 char$(F)=2$，则 $2ab=0$总是成立，因此（1）成立。接下来，假设 char$(F)\neq2$。那么 $2ab=0$ 当且仅当 $ab=0$。在式(6.5)中，恰有两种情形使得 $ab=0$，即 $\begin{pmatrix}0&1\\0&0\end{pmatrix}$ 和 $\begin{pmatrix}1&0\\0&0\end{pmatrix}$。因此（2）得证。 □

注 6.6。 假设 q 为奇数且 ord$_{\mathbb{Z}_n^\times}(q)$ 为奇数。对于所有本原幂等元 $e_0=\frac{1}{n}\sum_{i=0}^{n-1}u^i$， e_1， $\cdots$， e_ℓ属于 FH的本原幂等元，除了 e_0之外，其余本原幂等元两两分组（见引理 2.2(2)）：

$$e_1,\ \overline{e_1},\ \cdots,\ e_m,\ \overline{e_m}.$$

(1) 令 $A_0=FGe_0$且 $A_t=FG(e_t+\overline{e_t})$ 对于 $t=1,\ \cdots,\ m$。根据引理 6.4，

$$FG=A_0\oplus A_1\oplus\cdots\oplus A_m;\qquad A_t\cong\mathrm{M}_2(F_t),\ \ t=1,\cdots,m.$$

其中 $F_t=FHe_t$是 F上的域扩张，记 $k_t=|F_t:\ F|$。由式（6.1），$\langle A_i,\ A_j\rangle=0$对于 $0\leq i\neq j\leq m$；因此推论 3.9 对于 $FG=A_0\oplus A_1\oplus\cdots\oplus A_m$仍然成立。

ˆ(2) 令 $\widehat{e}_0=e_0+e_0v\in A_0$，则 $\langle A_0\widehat{e}_0、\ A_0\widehat{e}_0\rangle=A_0\widehat{e}_0\overline{\widehat{e}_0}A_0\neq0$ 由于 $\widehat{e}_0\overline{\widehat{e}_0}=2\widehat{e}_0\neq0$，因此 $A_0\widehat{e}_0$ 是 A_0中的 LCD。

因此，以下是 [10, 定理 IV.5(1)]的正确表述。

定理 6.7。 沿用备注*6.6*中的记号。我们考虑以下二面体码：

$$C_{ab}=A_0\widehat{e}_0\oplus A_1f_{a_1b_1}\oplus\cdots\oplus A_mf_{a_mb_m},\quad 0\neq(a_t,b_t)\in F_t^2,\ t=1,\cdots,m. \tag{6.6}$$

则 $\dim_F(C_{ab})=n$，并且

(1) 式(6.6) 中的二面体码数量等于 $\prod_{t=1}^{m}(q^{k_t}+1)$。**(2)** 式(6.6) 中为 LCD 的二面体码数量等于$\prod_{t=1}^{m}(q^{k_t}-1)$。

证明。 根据 [10, 引理 III.2(3)]， $A_0\widehat{e}_0$ 是 A_0的一个一维理想，因此 $\dim_F(C_{ab})=1+\dim_F A_1f_{a_1b_1}+\cdots+\dim_F A_mf_{a_mb_m}=n$，其中 $\dim_F A_tf_{a_tb_t}=2k_t$， $t=1,\ \cdots,\ m$。由式(6.5)和引理 6.5(2)，立即得到(1)和(2)。 □

7 结论

我们研究了常二面体码，并针对参考文献 [10] 中关于二面体码的研究提出了一个问题。

为了研究常二面体码的代数性质，文献 [10]，中的现有方法不足以识别群码的正交性；因此，我们开发了一种通过矩阵计算评估群码正交性的技术。我们刻画了常二面体群代数的代数结构。利用这一代数结构和刚才提到的技术，我们构造了一类具有良好代数性质（自正交或 LCD）的常二面体码。

接下来，我们证明了所构造的这类常二面体码存在渐近优良序列。我们没有采用概率方法，而是直接统计了该类中渐近性质不佳的常二面体码的数量。这个数量远少于该类码的总数。由此我们得到（回顾一下， F 是一个有限域，且 $|F|=q$）：

— 如果 q 为偶数，或 $4\mid(q-1)$，那么 F 上的自对偶常二面体码渐近良好。

— 如果 q 为奇数且 $4\nmid(q-1)$，那么 F 上的 LCD 常二面体码渐近良好。

最后，借助本文所发展的技术，我们解决了[10] 中的问题，并得到了错误定理 [10, 定理 IV.5(1)]的正确版本。

致谢

参考文献

.[1] A. Alahmadi、F. Ozdemir、P. Sol´e, 《自对偶双循环码》, 《设计、码与密码学》, 第86卷, 第1257–1265页, 2018年。 [2, 3][2] S. A. Aly、A. Klappenecker、P. K. Sarvepalli, 《二元群代数码》, 2004年国际信息论研讨会, 2096–2100页, 2007年。 [5][3] J. Bali、B. S. Rajan, 《二面体群和二循环群上二层群码的旋转不变性》, Sddhangl, 第23卷, 第1部分, 第45–56页, 1998年。[6][4] L. M. J. Bazzi、S. K. Mitter, 《由群作用构造的一些随机码》, IEEE信息论汇刊, 第52卷, 第3210–3219页, 2006年。[2][5] M. Borello、W. Willems, 《域上的群码是渐近良好的》, 《有限域及其应用》, 第68卷（12月）, 2020年, 101738。 [2][6] C. L. Chen、W. W. Peterson、E. J. Weldon, 《关于准循环码的一些结果》, 《信息与控制》, 第15卷, 第407–423页, 1969年。 [2][7] V. Chepyzhov, 《线性准循环码和近线性准循环码最小距离的新下界》, 《信息传输问题》, 第28卷, 第33–44页, 1992年。 [2][8] C.W. Curtis、I. Reiner, 《表示理论方法》, 约翰·威立父子公司, 1981年。 [7][9] Yun Fan、Liren Lin, 《随机准阿贝尔码的阈值》, IEEE信息论汇刊, 第61卷, 第1期, 第82–90页, 2015年。 [16][10] Yun Fan、Liren Lin, 《有限域上的二面体群码》, IEEE信息论汇刊, 第67卷, 第8期, 第5016–5025页, 2021年。 [2, 3, 4, 6, 8, 10, 16,20, 23, 24, 25, 27][11]Yun Fan、Liren Lin, 《准群码的渐近性质》, arXiv:2203.00958, 2022年。 [25][12] Yun Fan、Hualu Liu, 《两个有限交换链环上的双常循环码》, IEEE信息论汇刊, 第69卷, 第3期, 第1521–1530页, 2023年。 [2, 16, 17][13]Yun Fan、Yuchang Zhang, 《自对偶二准循环码与二面体码》, 《有限域及其应用》, 第85卷（1月）, 2023年, 102127。[3]

[14] W. C. Huffman、V. Pless，《纠错码基础》，剑桥大学出版社，2003年。[2][15] T. Kasami，《针对码率为1/2的准循环码的Gilbert-Varshamov界》，IEEE信息论汇刊，第20卷，第679页，1974年。[2][16] L. Kathuria、M. Raka，《循环自正交码的存在性：关于Vera Pless一项结果的注记》，《先进数学通讯》，第6卷，第499–503页，2012年。[5][17] Liren Lin，《随机准阿贝尔码与自正交负循环码（中文）》，博士论文，华中师范大学，中国武汉，2014年。[2][18] Liren Lin、Yun Fan，《自对偶2-准阿贝尔码》，IEEE信息论汇刊，第68卷，第6417–6425页，2022年。[2, 5, 10][19] S. Ling、P. Sol´e，《关于准循环码的代数结构II：链环》，《设计、码与密码学》，第30卷，第1期，第113–130页，2003年。[2][20] C. Mart´ınez-P´erez、W. Willems，《循环码这一类是否渐近良好？》，IEEE信息论汇刊，第52卷，第2期，第696–700页，2006年。[2][21] C. Mart´ınez-P´erez、W. Willems，《自对偶双偶二准循环传递码是渐近良好的》，IEEE信息论汇刊，第53卷，第4302–4308页，2007年。[2][22] R.W.K. Odoni，《Krishnamurthy关于十进制周期的猜想及若干相关问题》，《数论杂志》，第13卷，第303–319页，1981年。[21][23] J.-P. Seere，《算术教程》，施普林格出版社，纽约，1973年。[21][24] V. Shashidhar、B. S. Rajan，《常二面体码及其变换域刻画》，2004年国际信息论研讨会，第256页。IEEE出版社，2004年。[6]