基于勒让德对问题的一个解的轨道凸包的维数

Kristopher N. Kilpatrick[a]，Dursun A. Bulutoglu[a]

[a]美国俄亥俄州赖特-帕特森空军基地空军理工学院数学与统计学系，邮编 45433

arXiv:2301.01839v1 [math.RT] 4 Jan 2023

摘要

勒让德对问题是秩一半正定描述问题的一个特例，旨在寻找一对向量 $(\mathbf{u}、\mathbf{v})$，二者的长度均为 ℓ，使得向量 $(\mathbf{u}^\top、\mathbf{v}^\top)^\top$ 满足秩一半正定描述。群 $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ 通过$((i,j),k)(\mathbf{u}、\mathbf{v}) = ((i,k)\mathbf{u}\ (j,k)\mathbf{v})$作用于满足秩一半正定描述的解，其中每个 $((i,j),k) \in (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ 均成立。对于满足秩一半正定描述的给定解 $(\mathbf{u}^\top、\mathbf{v}^\top)^\top$，运用 Bulutoglu 在 [《Discrete Optim.》45（2022）],中基于表示论的方法，以及 Ingleton 在 [《伦敦数学会杂志》s(1- 31)（1956），445-460] 和 Lam 和 Leung 在 [《代数杂志》224（2000），91-109],中的结果，我们证明，在满足 $\ell = p^n$ 或 $\ell = pq^i$ 的条件下，对于 $i = 1$、2、任意正整数 n以及任意两个奇素数 p、q，$\mathbf{u}$ 在$\mathbb{Z}_\ell$ 或 $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 作用下的轨道的凸包维数为 $\ell - 1$。我们的结果导出一个猜想：这两种情形下，该维数均为 $\ell - 1$。我们还证明，若长度为 ℓ的勒让德对问题至少有一个可行点，则其所有可行点的凸包维数为 $2\ell - 2$。

关键词：循环矩阵、凸包、拉马努金和、有理表示、单位根的消失和
2000年 MSC：90C22 68R05 20C15 05E20 20G0511L03

1. 引言

通过求解一对向量的约束系统，可以构造出一个 Hadamard矩阵。为定义该约束系统，令 $\mathbb{Z}_\ell = \{0, \ldots, \ell - 1\}$ 表示模 ℓ的整数。两个长度为 ℓ的向量 $(\mathbf{u}, \mathbf{v})$ 是一个 Legendre

电子邮箱：kristopher.n.kilpatrick@gmail.com（Kristopher N. Kilpatrick），dursun.bulutoglu@gmail.com（Dursun A. Bulutoglu）

提交至 Elsevier 的预印本　　2023年1月6日

对（LP），当

$$\begin{aligned} P_{\mathbf{u}}(j)+P_{\mathbf{v}}(j)&=-2,\ \ \forall j\in\mathbb{Z}_\ell-\{0\},\\ \mathbf{1}^\top\mathbf{u}&=\mathbf{1}^\top\mathbf{v},\ \ \mathbf{u},\mathbf{v}\in\{-1,1\}^\ell, \end{aligned} \tag{1.1}$$

其中 $P_{\mathbf{x}}(j)=\sum_{i\in\mathbb{Z}_\ell}\mathbf{x}(i)\mathbf{x}(i-j)$是向量 $\mathbf{x}\in\mathbb{C}^\ell$的周期自相关函数。求解约束系统 (1.1) 的问题称为线性规划问题。约束系统 (1.1) 可表示为以下秩 1 约束半定描述（秩 1 CSDD）。

$$\begin{aligned} \sum_{\substack{i-j=r\ (\mathrm{mod}\ \ell)\\ 1\leqslant i,j\leqslant\ell}} Y_{ij}+\sum_{\substack{i-j=r\ (\mathrm{mod}\ \ell)\\ \ell+1\leqslant i,j\leqslant 2\ell}} Y_{ij} &= -2, \quad \text{for } r=1,\ldots,\ell,\\ Y_{jj} &= 1, \qquad \text{for } j=1,\ldots,2\ell,\\ \mathbf{Y} &\geq 0,\\ \mathrm{rank}(\mathbf{Y}) &= 1,\\ \sum_{j=0}^{\ell-1} Y_{1j+1} &= \sum_{j=0}^{\ell-1} Y_{1(\ell+j+1)}, \end{aligned} \tag{1.2}$$

其中 $\mathbf{Y}\succeq 0$ 表示 Y 是半正定的。在针对线性规划的这一秩 1 CSDD 中，通过对 $j=0$、.....、$\ell-1$取 $u_j=Y_{1(j+1)}$和 $v_j=Y_{1(\ell+j+1)}$，可得到一个线性规划 $(\mathbf{u},\mathbf{v})$。关于秩 1 约束半定规划问题（即秩 1 CSDD）的可行集定义，见 [3]。

令 $\mathbb{Q}^{\mathbb{Z}_\ell}$ 为从 $\mathbb{Z}_\ell$ 到 $\mathbb{Q}$的全体函数空间。将 $\mathbf{u}\in\mathbb{Q}^{\mathbb{Z}_\ell}$循环移位 $j\in\mathbb{Z}_\ell$次，记作 $c_j\mathbf{u}$，是一种满足 $c_j\mathbf{u}(i)=\mathbf{u}(i-j), i\in\mathbb{Z}_\ell$的变换。$\mathbf{u}\in\mathbb{Q}^{\mathbb{Z}_\ell}$的循环矩阵记作 $\mathbf{C_u}$，是一个矩阵，其 $\mathbf{C_u}$ 的第 $(j+1)$行是 $(c_j\mathbf{u})^\top$。如果 $(\mathbf{u},\mathbf{v})$ 是一个线性规划，且 $\mathbf{1}^\top\mathbf{u}=\mathbf{1}^\top\mathbf{v}=-1$，那么

$$\mathbf{H}=\begin{bmatrix} 1 & 1 & \mathbf{1}^\top & \mathbf{1}^\top\\ 1 & -1 & \mathbf{1}^\top & -\mathbf{1}^\top\\ \mathbf{1} & \mathbf{1} & \mathbf{C_v} & \mathbf{C_u}\\ \mathbf{1} & -\mathbf{1} & \mathbf{C_u}^\top & -\mathbf{C_v}^\top \end{bmatrix}$$

是一个 $(2\ell+2)\times(2\ell+2)$ Hadamard矩阵，其中 1 是长度为 ℓ [2]、元素全为 1 的向量。也可以使用满足 $\mathbf{1}^\top\mathbf{u}=\mathbf{1}^\top\mathbf{v}=1$ 的线性规划来构造 Hadamard矩阵。因此，要构造某个奇数 ℓ 对应的 $(2\ell+2)\times(2\ell+2)$ Hadamard矩阵，只需找到一个长度为 ℓ 的线性规划。人们猜想，对于每个奇数 ℓ，都存在长度为 ℓ 的线性规划，而这一猜想意味着 Hadamard猜想。Arasu 等人 [2] 证明，线性规划 $(\mathbf{u},\mathbf{v})$ 必须满足

$$\mathbf{1}^\top\mathbf{u}=\mathbf{1}^\top\mathbf{v}=\pm 1.$$

本文中，我们选择所有线性规划 $(\mathbf{u}, \mathbf{v})$，使其满足

$$\mathbf{1}^\top \mathbf{u} = \mathbf{1}^\top \mathbf{v} = -1. \tag{1.3}$$

令 $N \rtimes H$ 为由两个群 N 和 H 构成的半直积，其定义见 Rotman [12]。那么，群 $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 通过 $(j$ 对 $\mathbf{u} \in \mathbb{Q}^{\mathbb{Z}_\ell}$ 作用：$k)\mathbf{u}(i) = \mathbf{u}((j,k)^{-1}i)$，其中每个 $(j,k) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times, i \in \mathbb{Z}_\ell$ 均成立，且 $(a,b)i = bi + a$ 对于 $(a,b) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times, i \in \mathbb{Z}_\ell$ 成立。群 $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ 对任意一对 $(\mathbf{u}, \mathbf{v}) \in \mathbb{Q}^{\mathbb{Z}_\ell} \oplus \mathbb{Q}^{\mathbb{Z}_\ell}$ 的作用为

$$((i,j),k)(\mathbf{u},\mathbf{v}) = ((i,k)\mathbf{u}, (j,k)\mathbf{v})$$

其中每个 $((i,j),k) \in (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ 均成立。如果长度为 ℓ 的向量对 $(\mathbf{u}, \mathbf{v})$ 和 $(\mathbf{u}', \mathbf{v}')$ 中，$(\mathbf{u}', \mathbf{v}')$ 或 $(\mathbf{v}', \mathbf{u}')$ 属于 $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ 作用下 $(\mathbf{u}, \mathbf{v})$ 的轨道，则这两对向量等价。如果 $(\mathbf{u}, \mathbf{v})$ 是一个线性规划，且 $(\mathbf{u}', \mathbf{v}')$ 与 $(\mathbf{u}, \mathbf{v})$ 等价，那么 $(\mathbf{u}', \mathbf{v}')$ 也是一个线性规划 [2]。秩约束 CSDD 的对称群是其所有解向量排列中能够将解映射为解的排列的集合。因此，线性规划的秩 1 CSDD 的对称群包含群 $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$。

全文中，对于每个 $n \in \mathbb{Z}_{\geqslant 1}$，令 $[n] = \{1、\ldots\ldots、n\}$，并且

$$\{d : d \mid \ell\} = \{d \in [\ell] : d \mid \ell\}.$$

对于标量域 $\mathbb{F}$ 上向量空间中的向量集 S，$\mathrm{Span}_{\mathbb{F}}(S)$ 表示其张成空间，$\mathrm{Aff}_{\mathbb{F}}(S)$ 表示其仿射包，而 $\dim_{\mathbb{F}}(S)$ 表示 $\mathbb{F}$ 上 S 中向量的仿射包的维数。对于矩阵 $\mathbf{M}$，$\mathrm{Col}_{\mathbb{F}}(\mathbf{M})$ 表示 $\mathbf{M}$ 在 $\mathbb{F}$ 上的列空间。若未提供 $\mathbb{F}$，则 $\mathbb{F} = \mathbb{R}$。此外，令 $\mathrm{Conv}(S)$ 表示 S 中向量的凸包。对于在线性作用于向量空间 V 上的有限群 G，$G\mathbf{v}$ 表示 $\mathbf{v}$ 在群 G 的作用下的轨道 $\in V$，而 $\mathrm{Conv}(G\mathbf{v})$ 表示经过 $\mathbf{v}$ [13] 的 G 的轨道凸体。此外，令 $\mathcal{F}_\ell$ 为满足线性规划问题的秩 1 CSDD 的所有对 $(\mathbf{u}^\top、\mathbf{v}^\top)^\top$ 组成的可行集。本文确定 $\dim(\mathrm{Conv}(\mathcal{F}_\ell))$，并研究当 $(\mathbf{u}、\mathbf{v})$ 是线性规划问题时，$\dim(\mathrm{Conv}((\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times)\,\mathbf{u}))$ 和 $\dim(\mathrm{Conv}((\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times)\,\mathbf{v}))$ 的所有可能取值。以下定理和推论是本文的主要结果。

定理 1.1。设 ℓ 为奇正整数，$\mathcal{F}_\ell$ 为所有满足该线性规划问题的秩 1 CSDD 的数对 $(\mathbf{u}^\top, \mathbf{v}^\top)^\top$ 的可行集。若 $\mathcal{F}_\ell \neq \varnothing$，则

$$\dim(\mathrm{Conv}(\mathcal{F}_\ell)) = 2\ell - 2.$$

以下推论可由定理 1.1 直接得出。

推论 1.2。设 $(\mathbf{u}^\top, \mathbf{v}^\top)^\top$ 满足线性规划问题的秩 1 CSDD。那么，由线性规划问题的秩 1 CSDD 中包含约束 (1.2) 可推出两个与 $\mathbf{1}^\top\mathbf{u} = \mathbf{1}^\top\mathbf{v}$ 线性无关的线性约束，即 $\mathbf{1}^\top\mathbf{u} = \pm 1$。此外，不能推出任何一个与约束 $\mathbf{1}^\top\mathbf{u} = \pm 1$ 和 $\mathbf{1}^\top\mathbf{u} = \mathbf{1}^\top\mathbf{v}$ 线性无关的线性约束。

证明。首先，线性规划问题的秩 1 CSDD 可行。于是，任何其他与约束 $\mathbf{1}^\top \mathbf{u} = \pm 1$ 和$\mathbf{1}^\top \mathbf{u} = \mathbf{1}^\top \mathbf{v}$ 线性无关的线性约束，都必然意味着 $\dim(\mathrm{Conv}(\mathcal{F}_\ell)) < 2\ell - 2$，这与定理 1.1 矛盾。 □

定理 1.3。设 $(\mathbf{u}, \mathbf{v})$ 是一个线性规划，且满足 $G = \mathbb{Z}_\ell$ 或 $G = \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$。那么存在 $U_1, U_2 \subseteq \{d : \ d \mid \ell\}$，使得 $U_1 \cap U_2 = \varnothing$ 并且

$$\dim(\mathrm{Conv}(G\,\mathbf{u})) = \ell - 1 - \left(\sum_{d \in U_1} \phi\left(\frac{\ell}{d}\right)\right),$$
$$\dim(\mathrm{Conv}(G\,\mathbf{v})) = \ell - 1 - \left(\sum_{d \in U_2} \phi\left(\frac{\ell}{d}\right)\right).$$

定理 1.4。设 p, q 是互不相同的奇素数，且 $n \in \mathbb{Z}_{\geqslant 1}$。设 $\ell = p^n$，或当 $i = 1$ 时 $\ell = pq^i$，2。设 $(\mathbf{u}, \mathbf{v})$ 是长度为 ℓ 的线性规划，且满足 $G = \mathbb{Z}_\ell$ 或 $G = \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$。那么

$$\dim(\mathrm{Conv}(G\,\mathbf{u})) = \dim(\mathrm{Conv}(G\,\mathbf{v})) = \ell - 1.$$

在第 2 节中，我们介绍表示论、功率谱密度、单位根的消失和以及仿射几何方面的必要背景。在第 3 节中，我们证明主要结果，并猜想定理 1.4 中对 ℓ 的限制（ℓ 为正奇数这一条件除外）可以去掉。第 4 节讨论未来的工作。

2. 背景理论

设 G 是一个有限群，V 是域 $\mathbb{F}$ 上的有限维向量空间。设 $\mathbf{GL}(V)$ 为 V 的 $\mathbb{F}$ 自同构群。G 的一个 n 维 $\mathbb{F}$ 表示是一个有序对 $(\rho、\ V)$，满足 $\rho\colon G \to \mathbf{GL}(V)$ 是同态，且 V 是域 $\mathbb{F}$ 上的 n 维向量空间。若子空间 W 满足 $\rho(g)W \subseteq W\ \forall g \in G$，则称其为 V 的一个 $\mathbb{F}$ 子表示。若 G 的表示 $(\rho、\ V)$ 的唯一子表示是 $\mathrm{Span}_{\mathbb{F}}(\mathbf{0})$ 和 V，则称该表示为不可约表示。若存在可逆线性变换 $\phi\colon W \to W' \ni \phi(\rho_1(g)w) = \rho_2(g)\phi(w)\ \forall w \in W$，且 $g \in G$，则称 G 的两个 $\mathbb{F}$ 表示 $\rho_1\colon G \to \mathbf{GL}(W)$ 和 $\rho_2\colon G \to \mathbf{GL}(W')$ 等价。对于群 G 的一个不可约表示分解 $V = m_1V_1 \oplus \cdots \oplus m_bV_b$，$m_i$ 是不可约 $\mathbb{C}$ 表示 V_i（在等价意义下）出现的次数。这个 $m_i \geqslant 1$ 称为 V_i 的重数。

本文仅考虑域 $\mathbb{F}$ $\mathbb{Q}$、$\mathbb{R}$ 和 $\mathbb{C}$，它们分别是有理数、实数和复数。若 $\mathbb{F}$-表示 $\rho\colon G \to \mathbf{GL}(V)$ 关于 V 中的内积 $\langle \cdot, \cdot \rangle$ 是酉的，则对于所有 $\mathbf{u}, \mathbf{v} \in V$，都有 $\langle \rho(g)\mathbf{v}\ \rho(g)\mathbf{u} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle$。每个表示都关于复内积 [14] 是酉的。我们采用约定 $\langle \alpha\mathbf{u} \mid \mathbf{v} \rangle = \bar{\alpha}\langle \mathbf{u} \mid \mathbf{v} \rangle$，其中 $\alpha \in \mathbb{F}$，且 $\mathbf{u}, \mathbf{v} \in V$。若群 G 的表示 (ρ, V) 满足对所有 ....., $\rho(g)$ 都置换了 V 的一组基

$g \in G$，则称 (ρ, V) 为置换 $\mathbb{F}$-表示。每个置换$\mathbb{F}$-表示都关于复点积是酉的。本文中，所有群 G 都是有限群，所有向量空间 V 都是有限维的，并且任何指定群的每个表示都是置换表示，因此关于复点积是酉的。

定理 2.1。 /Maschke/对于某个内积，有限群的每个表示都是正交不可约子表示的直和。

定理 2.1 中的分解称为无重数的，如果每个不可约表示只出现一次。群的 $\mathbb{F}$ 表示 (ρ的特征标是映射 χ_ρ: $G \to \mathbb{F}$ ，定义为 $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$，其中 Tr $(\rho(g))$ 是 $\rho(g)$ 的迹。如果该特征标属于一个不可约表示，我们称其为不可约特征标。有限群的两个 $\mathbb{F}$表示等价，当且仅当它们具有相同的特征标 [5]。如果根据上下文可以明确表示，我们也可以将特征标简单记为 χ 。下面的定理来自 Serre [14]。

定理 2.2。设 (ρV) 是群 G 的一个 $\mathbb{C}$表示。令

$$V = m_1 V_1 \oplus \ldots \oplus m_h V_h$$

设 $m_i \in \mathbb{Z}_{\geqslant 1}$ 是 V 到不可约表示 $(\rho_i、 V_i)$ 的分解，其特征标为 $\chi_i \forall i \in [h]$, 其中 $\chi_i = \chi_{\rho_i}$。则 V 到 $m_i V_i = \bigoplus_{k=1}^{m_i} V_i$ 的正交投影 $\mathbf{P}_i$ 为

$$\mathbf{P}_i = \frac{\dim_{\mathbb{C}}(V_i)}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \mathbf{M}_{\rho(g)}.$$

其中，$\mathbf{M}^{\rho(g)}$ 是 $\rho(g)$ 在 V 的某个标准正交基下的矩阵。

群 G 的指数 m 是满足 $g^m = e \ \forall g \in G$ 的最小非负整数。设 $(\rho、 V)$ 是群 G 的一个指数为 m 的 $\mathbb{C}$-表示。则 $\rho(g)^m = id \ \forall g \in G$，其中 id 是 V 上的恒等映射。因此， $\rho(g)$ 的特征值是 m 次单位根。在全文中，设 $\zeta_m = e^{2\pi i/m}$。由于 $\chi(g)$ 是 $\rho(g)$ 的迹， $\chi(g) \in \mathbb{Q}(\zeta_m)$，其中 $\mathbb{Q}(\zeta_m)$ 是通过添加 ζ_m 得到的 $\mathbb{Q}$ 的域扩张。

令 $\mathbb{Z}_m^\times = \{r \in \mathbb{Z}_m \mid (r, m) = 1\}$ 为 $\mathbb{Z}_m$的乘法群，其中 (r, m)是 r 和 m的最大公约数。 $\mathbb{Q}(\zeta_m)$ 的自同构群 $\mathrm{Aut}(\mathbb{Q}(\zeta_m))$是域扩张 $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$ 的伽罗瓦群，记作 $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$。$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ 的元素可由$\mathbb{Z}_m^\times$的元素进行索引，其中对于 $\sigma_r \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$

$$\sigma_r(\zeta_m) = \zeta_m^r, \ \sigma_r(q) = q \text{ for each } q \in \mathbb{Q}, \text{ and } r \in \mathbb{Z}_m^\times.$$

映射 $\sigma_r \to r$ 是 $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ 与 $\mathbb{Z}_m^\times$之间的同构。令 $\mathrm{Aut}(\mathbb{C})$为 $\mathbb{C}$ 的所有自同构构成的群，并且

$$\mathrm{Aut}(\mathbb{C})_{\mathbb{Q}(\zeta_m)} = \{\tau_{|\mathbb{Q}(\zeta_m)} \mid \tau \in \mathrm{Aut}(\mathbb{C})\},$$

其中 $\tau_{|\mathbb{Q}(\zeta_m)}$ 是 $\tau \in \mathrm{Aut}(\mathbb{C})$ 在 $\mathbb{Q}(\zeta_m)$上的限制。对于每个 $\tau \in \mathrm{Aut}(\mathbb{C})$, $(\tau(\zeta_m))^m = \tau((\zeta_m)^m) = \tau(1) = 1$，且对于每个 $q \in \mathbb{Q}$， $\tau(q) = q$。因此，我们有 $\mathrm{Aut}(\mathbb{C})_{\mathbb{Q}(\zeta_m)} \subseteq \mathrm{Aut}(\mathbb{Q}(\zeta_m))$。由于 $\mathbb{C}$ 的任意子域的自同构都可以延拓为 $\mathbb{C}$ [15]的自同构，因此每个 $\sigma_r \in \mathrm{Aut}(\mathbb{Q}(\zeta_m))$ 都可以延拓为一个 $\sigma'_r \in \mathrm{Aut}(\mathbb{C})$。于是 $\mathrm{Aut}(\mathbb{Q}(\zeta_m)) \subseteq \mathrm{Aut}(\mathbb{C})_{\mathbb{Q}(\zeta_m)}$，这意味着

$$\mathrm{Aut}(\mathbb{Q}(\zeta_m)) = \mathrm{Aut}(\mathbb{C})_{\mathbb{Q}(\zeta_m)}.$$

由于 $\rho(g)$的矩阵的元素属于 $\mathbb{Q}(\zeta_m)$，$\mathrm{Aut}(\mathbb{Q}(\zeta_m))$ ($\mathrm{Aut}(\mathbb{C})$) 作用于维数相同的 G 的 $\mathbb{C}$- 表示（的特征标）上。

设 $V = \mathbb{F}^G$ 为从 G 到 $\mathbb{F}$的全体函数空间。那么标准基

$$\mathbf{e}_g(h) = \begin{cases} 1 & \text{if } g = h, \\ 0 & \text{otherwise} \end{cases}$$

对于 g， $h \in G$ 张成 V。我们进一步在 V上赋予通常的内积 $\langle \cdot \mid \cdot \rangle$（复点积），使得 $\{\mathbf{e}_g\}_{g\in G}$ 构成标准正交基。于是， $\mathbb{F}$的正则 $\mathbb{F}$-表示是满足以下条件的一对 $(\rho、 V)$： ρ: $G \to \mathrm{GL}(V)$ 是由 G 在 V的基上的作用所确定的同态，其中 $\rho(h)$ $\mathbf{e}_g = \mathbf{e}_{hg}$ $\forall h$， $g \in G$。显然， G 的正则 $\mathbb{F}$-表示也是一个置换表示。

域 $\mathbb{Q}$ 上的向量空间 U的复化定义为 $U_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{Q}} U$。显然，若 U 是一个 $\mathbb{Q}$-表示，则 $U_{\mathbb{C}}$ 是通过将 U的标量域 $\mathbb{Q}$扩张到 $\mathbb{C}$而得到的 $\mathbb{C}$-表示。设 $\langle \cdot \mid \cdot \rangle$为 $\mathbb{F}$ 上的V 的内积。容易证明，可以在 $V_{\mathbb{C}}$ 上定义内积为$\langle z \otimes \mathbf{v} \mid z' \otimes \mathbf{v}' \rangle = z\overline{z'}\langle \mathbf{v} \mid \mathbf{v}' \rangle$。于是，以下引理立即得出。

引理 2.3. 设 V 是定义在 $\mathbb{Q}$ 上的内积空间，且 U、 W 是 V 的子空间。那么，当且仅当 $U_{\mathbb{C}}$ 与 $W_{\mathbb{C}}$ 正交时， U 与 W 正交。

以下定理是众所周知的。

定理 2.4. 设 $\left(R、 \mathbb{Q}^{\mathbb{Z}_\ell}\right)$ 是 $\mathbb{Z}_\ell$ 的正则 $\mathbb{Q}$-表示。那么

$$\left(\mathbb{Q}^{\mathbb{Z}_\ell}\right)_{\mathbb{C}} = \bigoplus_{i\in\mathbb{Z}_\ell} V_i$$

是将 $\left(\mathbb{Q}^{\mathbb{Z}_\ell}\right)_{\mathbb{C}}$ 分解为 $\mathbb{Z}_\ell$ 的一维不可约 $\mathbb{C}$-表示，其中 $\mathbb{C}$-表示 $(\rho_k、 V_k)$、 $k \in \mathbb{Z}_\ell$ 分别由 $\rho_k(j)$ 给出：对每个 k、 $j \in \mathbb{Z}_\ell$， $V_k \to V_k$、 $\mathbf{v} \mapsto \overline{\zeta}_\ell^{jk}\,\mathbf{v}$ 和 $\chi_k(j) = \mathrm{Tr}(\rho_k(j)) = \overline{\zeta}_\ell^{jk}$。

对于每个 $k \in \mathbb{Z}_\ell$，$\mathbf{v}_k = \sum_{j\in\mathbb{Z}_\ell} \zeta_\ell^{jk}\, \mathbf{e}_j$ 是 $\mathbb{Z}_\ell$ 的一维$\mathbb{C}$-表示 V_k 的基向量。众所周知，$\{\mathbf{v}_0, \ldots\ldots, \mathbf{v}_{\ell-1}\}$ 是 $\mathbb{C}^{\mathbb{Z}_\ell}$ 的一组基。在本文中，我们将向量 $\mathbf{v}_0, \ldots\ldots, \mathbf{v}_{\ell-1}$ 称为离散傅里叶基向量。

下面的定理刻画了定理 2.4 中一维表示在 $\mathrm{Aut}(\mathbb{C})$作用下的轨道。

定理 2.5. 对于 $k \in \mathbb{Z}_\ell$，令 χ_k 为 $\mathbb{Z}_\ell$ 的 $\mathbb{C}$-表示的不可约特征标。对于 ℓ 的每个因子 d，令 $\mathcal{O}_d = \{\chi_k \,|\, (k, \ell) = d \text{ 和 } k \in \mathbb{Z}_\ell\}$。那么

(i) $|\mathcal{O}_d| = \phi(\ell/d),$，其中 ϕ 是欧拉函数。

(ii) $\mathcal{O}_d = \mathrm{Aut}(\mathbb{C})\,\chi_d = \mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))\,\chi_d.$

证明. 令 d 为 ℓ 的一个因子。根据欧拉函数的定义，(i) 立即成立。为证明 (ii),

$$\sigma_r(\chi_d(j)) = \overline{\zeta}_\ell^{jrd} = \chi_{rd}(j)$$

对于每个 $\sigma_r \in \mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d})),\ r \in \mathbb{Z}_{\ell/d}^\times$，和 $j \in \mathbb{Z}_\ell$。因此，$\sigma_r(\chi_d) = \chi_{rd}$，且 $(rd, \ell) = d$ 蕴含 $\chi_{rd} \in \mathcal{O}_d$，从而 $\mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))\,\chi_d \subseteq \mathcal{O}_d$。

令 $\chi_k \in \mathcal{O}_d$ 使得 $k = rd$ 和 $(r, \ell/d) = 1$。则 $\sigma_r \in$ 自同构群 $(\mathbb{Q}(\zeta_{\ell/d}))$，且

$$\chi_k = \chi_{rd} = \sigma_r\chi_d$$

因此，$\mathcal{O}_d \subseteq$ 自同构群 $(\mathbb{Q}(\zeta_{\ell/d}))\,\chi_d$。 □

以下定理由 Isaacs $[8,\ \text{定理 } 9.21]$，定理 2.2 以及引理 2.3 推出。

定理 2.6。设 (ρ, V) 是群 G 的一个 $\mathbb{Q}$-表示，其指数为 m。令

$$V = W_1 \oplus \cdots \oplus W_b$$

是 V 的不可约 $\mathbb{Q}$-子表示的一个分解。设 $V_\mathbb{C}$、$W_{i\mathbb{C}}$ 是从 V、W_i 中通过将 V、W_i 的标量域扩张至 $\mathbb{C}$ 而得到的 $\mathbb{C}$-表示。令

$$V_\mathbb{C} = W_{(1,1)} \oplus \cdots \oplus W_{(1,r_1)} \oplus \ldots \oplus W_{(b,1)} \oplus \cdots \oplus W_{(b,r_b)}$$

是 $V_\mathbb{C}$ 分解为具有特征标 $\chi_{\rho_{i,j}}$ 的 $\left(\rho_{i,j}, W_{(i,j)}\right)$ 个不可约 $\mathbb{C}$-子表示，其中

$$W_{i\mathbb{C}} = W_{(i,1)} \oplus \cdots \oplus W_{(i,r_i)} \ \ for\ i \in [b].$$

对于 $i \in [b]$，令 $\mathcal{O}_{\rho_{i,1}}$ 为 $\chi_{\rho_{i,1}}$ 的 $\mathrm{Aut}(\mathbb{Q}(\zeta_m))$-轨道。令 $\mathbf{M}^{\rho(g)}$ 为相对于标准基的 $\rho(g)$ $\forall g \in G$ 矩阵。若 $V_{\mathbb{C}}$ 无重数，则

$$\mathbf{P}_{W_i} = \frac{\dim_{\mathbb{C}}(W_{(i,1)})}{|G|} \sum_{g \in G} \left(\sum_{\chi \in \mathcal{O}_{\rho_{i,1}}} \overline{\chi(g)} \mathbf{M}_{\rho(g)} \right)$$

是投影到第 i 个不可约 $\mathbb{Q}$-子表示子空间 $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_{W_i})$ $\forall i \in [b]$的正交投影矩阵。

下面的定理给出了在 $\mathbb{Z}_\ell$的作用下，将 $\mathbb{Q}^{\mathbb{Z}_\ell}$ 分解为不可约 $\mathbb{Q}$-子表示的分解。

定理 2.7. 设 $\left(R, \mathbb{Q}^{\mathbb{Z}_\ell}\right)$ 是 $\mathbb{Z}_\ell$的正则 $\mathbb{Q}$-表示。设

$$\mathbf{P}_d = \frac{1}{\ell} \sum_{i \in \mathbb{Z}_\ell} \sum_{\chi \in \mathcal{O}_d} \overline{\chi(i)} \mathbf{M}_{R(i)}$$

对于 ℓ的每个因子 d ，其中 $\mathbf{M}^{R(i)}$ 是相对于标准基 $\{\mathbf{e}_i\}_{i \in \mathbb{Z}_\ell}$的 $R(i)$ 的矩阵，而 $\mathcal{O}_d$ 由定理 2.5 定义。则

$$\mathbb{Q}^{\mathbb{Z}_\ell} = \bigoplus_{d \,|\, \ell} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$$

是在 $\mathbb{Z}_\ell$的作用下将 $\mathbb{Q}^{\mathbb{Z}_\ell}$ 分解为不可约 $\mathbb{Q}$-子表示的分解。

证明。设 d 是 ℓ的一个因子。根据定理 2.5，$\mathbf{P}_d$ 中的内层求和遍历 $\mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))$作用下 χ_d 的轨道。此外，根据定理 2.4，$\left(\mathbb{Q}^{\mathbb{Z}_\ell}\right)_{\mathbb{C}}$ 是无重数的。因此，由定理 2.6，$\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ 是 $\mathbb{Q}^{\mathbb{Z}_\ell}$的一个不可约$\mathbb{Q}$-子表示。现在，根据恒等式 $\ell = \sum_{d \,|\, \ell} \phi(\ell/d),$，只需证明

$$\dim_{\mathbb{Q}} \left(\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d) \right) = \phi\left(\frac{\ell}{d}\right).$$

Since R 是 $\mathbb{Z}_\ell$的正则表示，只有 $R(0)$ 会对迹作出贡献

$\mathbf{P}_d$的。由于 $\mathbf{P}_d$ 是投影矩阵,

$$\begin{aligned}\dim_{\mathbb{Q}}\left(\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)\right) = \mathrm{rank}(\mathbf{P}_d) = \mathrm{Tr}\left(\mathbf{P}_d\right) &= \mathrm{Tr}\left(\frac{1}{\ell}\sum_{i\in\mathbb{Z}_\ell}\sum_{\chi\in\mathcal{O}_d}\overline{\chi(i)}\mathbf{M}_{R(i)}\right)\\ &= \frac{1}{\ell}\sum_{i\in\mathbb{Z}_\ell}\sum_{\chi\in\mathcal{O}_d}\overline{\chi(i)}\,\mathrm{Tr}\left(\mathbf{M}_{R(i)}\right)\\ &= \frac{1}{\ell}\sum_{\chi\in\mathcal{O}_d}\mathrm{Tr}\left(\mathbf{M}_{R(0)}\right)\\ &= \frac{1}{\ell}\sum_{\chi\in\mathcal{O}_d}\ell\\ &= \sum_{\chi\in\mathcal{O}_d}1\\ &= |\mathcal{O}_d|\\ &= \phi\left(\frac{\ell}{d}\right).\end{aligned}$$

□

群 $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 通过 $(a,b)i = bi + a\ \forall i \in \mathbb{Z}_\ell$ 和 $(a,b) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 作用于 $\mathbb{Z}_\ell$。于是，由基 $T(a,b)\mathbf{e}_i = \mathbf{e}_{bi+a}$ 上的作用给出了 $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 的一个表示 $(T, \mathbb{Q}^{\mathbb{Z}_\ell})$。下一个定理表明，在 $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 的作用下，$\mathbb{Q}^{\mathbb{Z}_\ell}$ 具有与定理 2.7 中相同的分解；也就是说，将 $\mathbb{Z}_\ell$ 扩展到 $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 不会改变定理 2.7 中的分解。

定理 2.8。分解 $\mathbb{Q}^{\mathbb{Z}_\ell} = \bigoplus_{d\,|\,\ell}\mathbf{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ 是 $\mathbb{Q}^{\mathbb{Z}_\ell}$ 在 $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 的作用下分解为不可约 $\mathbb{Q}$-子表示的分解。

证明。设 d 是 ℓ 的一个因子。我们有 $\mathbf{Col}_{\mathbb{C}}(\mathbf{P}^d) = \bigoplus_{(k,\ \ell)=d} V_k$，其中 V_k 由 $\mathbf{v}_k = \sum_{i\in\mathbb{Z}_\ell}\zeta_\ell^{ki}\mathbf{e}_i$ 张成。设 $(a,b) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$。注意到

$$T(a,b)\mathbf{v}_k = \sum_{i\in\mathbb{Z}_\ell}\zeta_\ell^{ki}\mathbf{e}_{bi+a} = \sum_{j\in\mathbb{Z}_\ell}\zeta_\ell^{k(j-a)b^{-1}}\mathbf{e}_j = \zeta_\ell^{-kab^{-1}}\mathbf{v}_{b^{-1}k}.$$

由于 $(b,\ell) = 1$, $(bk,\ell) = d$ 当且仅当 $(k,\ell) = d$。因此，$\mathbf{Col}_{\mathbb{C}}(\mathbf{P}_d)$ 是在 $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 的作用下的一个 $\mathbb{C}$-子表示。由于 $\mathbf{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ 是在 $\mathbb{Z}_\ell$ 的作用下的一个不可约 $\mathbb{Q}$-子表示，且 $\mathbb{Z}_\ell$ 是 $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 的子群，因此 $\mathbf{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ 是在 $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 的作用下的一个不可约 $\mathbb{Q}$-子表示。

□

$\mathbf{u} \in \mathbb{Q}^{\mathbb{Z}_\ell}$ 的离散傅里叶变换（DFT）为 $\mu_k(\mathbf{u}) = \langle \mathbf{u}\,|\,\mathbf{v}_k\rangle$, $k \in \mathbb{Z}_\ell$。方程 $\mu_k(\mathbf{u}) = \langle \mathbf{u}\,|\,\mathbf{v}_k\rangle$, $k \in \mathbb{Z}_\ell$ 是基变换（变量）公式，它用标准基坐标表示傅里叶坐标 $\mu_k(\mathbf{u})$

u_j。 $\mathbf{u} \in \mathbb{Q}^{\mathbb{Z}_\ell}$ 的功率谱密度（PSD）为 $|\mu_k(\mathbf{u})|^2$，其中 $k \in \mathbb{Z}_\ell$。以下定理给出了一个等价条件，用功率谱密度刻画线性规划。

定理 2.9（Fletcher 等人 [6]）。设 $\mathbf{u}, \mathbf{v} \in \{-1, 1\}^\ell$。那么 $(\mathbf{u}, \mathbf{v})$ 是线性规划，当且仅当 $\mu_0(\mathbf{u}) = \mu_0(\mathbf{v})$ 且

$$|\mu_k(\mathbf{u})|^2 + |\mu_k(\mathbf{v})|^2 = 2(\ell + 1), \quad \forall k \in \mathbb{Z}_\ell - \{0\}.$$

如果存在 m 个 m ℓ 次单位根 $w_1, \ldots, w_m$（不一定互异）满足 $w_1 + \cdots + w_m = 0$，则称存在 m ℓ 次单位根的消失和。

定理 2.10（Lam 和 Leung [11]）。设 $\ell = p_1^{n_1} \ldots p_s^{n_s}$ 对于互异素数 $p_1, \ldots, p_s$ 和 $n_1, \ldots, n_s \in \mathbb{Z}_{\geqslant 1}$。那么，存在 $m\ell$ 次单位根的消失和，当且仅当对于某些 $a_1, \ldots, a_s \in \mathbb{Z}_{\geqslant 0}$，有 $m = a_1 p_1 + \cdots + a_s p_s$。

设 $\mathbf{u} \in \{-1, 1\}^\ell$ 满足 $\langle \mathbf{1} | \mathbf{u} \rangle = -1$。设 $J = \{j \in \mathbb{Z}_\ell | \mathbf{u}(j) = -1\}$。那么，对于 $k \neq 0$，$\mu_k(\mathbf{u})$ 有两种形式

$$\mu_k(\mathbf{u}) = -2 \sum_{j \in J} \zeta_\ell^{kj} = 2 \sum_{j \notin J} \zeta_\ell^{kj}, \tag{2.1}$$

其中 $|J| = (\ell + 1)/2$。

引理 2.11。设 $\ell = p^n$, p 为奇素数，且 $n \in \mathbb{Z}_{\geqslant 1}$。设 $\mathbf{u} \in \{-1, 1\}^\ell$ 满足$\langle \mathbf{1} | \mathbf{u} \rangle = -1$。那么 $\mu_k(\mathbf{u}) \neq 0$ $\forall k \in \mathbb{Z}_\ell$。

证明。由于 $\mu_0(\mathbf{u}) = -1$，我们只需验证 $k \in [\ell - 1]$。假设存在某个 $k \in [\ell - 1]$, 使得 $\mu_k(\mathbf{u}) = 0$，这将导致矛盾。根据方程 (2.1)，$\sum_{j \in J} \zeta_\ell^{kj} = 0$。根据定理 2.10,

$$\frac{\ell + 1}{2} = ap$$

对某个 $a \in \mathbb{Z}_{\geqslant 0}$。这意味着 $p \,|\, ((\ell + 1)/2),$，矛盾。因此，$\mu_k(\mathbf{u}) \neq 0$ $\forall k \in \mathbb{Z}_\ell$。 □

引理 2.12. 设 $\ell = pq$、 p、q 为互不相同的奇素数。设 $\mathbf{u} \in \{-1、 1\}^\ell$ 满足 $\langle \mathbf{1} | \mathbf{u} \rangle = -1$。那么 $\mu_k(\mathbf{u}) \neq 0$ $\forall k \in \mathbb{Z}_\ell$。

证明。由于 $\mu_0(\mathbf{u}) = -1$，我们只需验证 $k \in [\ell - 1]$。假设 $\mu_k(\mathbf{u}) = 0$ 对某个 $k \in [\ell - 1]$ 成立，从而导出矛盾。由方程 (2.1),

$$\sum_{j \in J} \zeta_\ell^{kj} = \sum_{j \notin J} \zeta_\ell^{kj} = 0. \tag{2.2}$$

由定理 2.10,

$$\frac{\ell+1}{2} = ap + bq \text{ and } \frac{\ell-1}{2} = cp + dq$$

对于某些 a、b、c、$d \in \mathbb{Z}_{\geqslant 0}$。这意味着

$$\ell = \frac{\ell+1}{2} + \frac{\ell-1}{2} = (a+c)p + (b+d)q.$$

若 $a+c \neq 0$ 和 $b+d \neq 0$，则 $p \mid (b+d)$ 和 $q \mid (a+c)$。因此,

$$\ell = (a+c)p + (b+d)q \geqslant pq + pq = 2\ell,$$

这就产生了矛盾。假设 $a+c=0$。那么 $a=c=0$，进而$q \mid ((\ell+1)/2),$，这就产生了矛盾。如果 $b+d=0$，也会产生类似的矛盾。因此，$\mu_k(\mathbf{u}) \neq 0 \ \forall k \in \mathbb{Z}_\ell$。□

引理 2.11 和 2.12 不能推广到任意奇数 ℓ。存在一个 $\mathbf{u} \in \{-1, 1\}^{45}$ 满足 $\langle \mathbf{1} \mid \mathbf{u} \rangle = -1$，使得对某个 $k \in \mathbb{Z}_{45} - \{0\}$，有 $\mu_k(\mathbf{u}) = 0$。

以下引理是众所周知的。

引理 2.13。设 V 是 $\mathbb{F}$上的一个向量空间。设 $S \subseteq V$。那么，$\mathbf{Aff}_{\mathbb{F}}(S)$ =张成空间 $_{\mathbb{F}}(S)$ 当且仅当 $\mathbf{0} \in \mathbf{Aff}_{\mathbb{F}}(S)$。

设 (ρ, V) 是群 G 的一个表示。设 $S \subseteq V$ 非空。那么 S 的重心是 $\beta(S) = (1/|S|) \sum_{\mathbf{v} \in S} \mathbf{v}$。$V$ 在 G 作用下的不动子空间为

$$V^G = \{\mathbf{v} \in V \mid \rho(g)\mathbf{v} = \mathbf{v} \ \forall g \in G\}.$$

显然，V^G 是 V 的一个子表示。根据定理 2.1，存在一个与 V^G 正交的子表示。

引理 2.14. 设 (ρ, V) 是群 G 的一个酉表示。设 $\mathbf{P}$ 是投影到 V^G 上的正交投影矩阵。那么对任意 $\mathbf{x} \in V$，$\mathbf{Px} = \beta(G\mathbf{x})$。

证明. 设 $\mathbf{u}_1, \ldots, \mathbf{u}_k$ 是 V^G 的一组标准正交基。那么

$$\mathbf{Py} = \sum_{i \in [k]} \langle \mathbf{u}_i \mid \mathbf{y} \rangle \mathbf{u}_i$$

对任意 $\mathbf{y} \in V$。那么，对于每个 $i \in [k]$ 和 $r \in G$，我们有

$$\langle \mathbf{u}_i \mid \rho(r)\mathbf{x} \rangle = \langle \rho(r)\mathbf{u}_i \mid \rho(r)\mathbf{x} \rangle = \langle \mathbf{u}_i \mid \mathbf{x} \rangle.$$

Then

$$\langle \mathbf{u}_i \,|\, \beta(G\,\mathbf{x})\rangle = \frac{1}{|G\,\mathbf{x}|} \sum_{\rho(r)\mathbf{x}\in G\,\mathbf{x}} \langle \mathbf{u}_i \,|\, \rho(r)\mathbf{x}\rangle = \frac{1}{|G\,\mathbf{x}|} \sum_{\rho(r)\mathbf{x}\in G\,\mathbf{x}} \langle \mathbf{u}_i \,|\, \mathbf{x}\rangle = \langle \mathbf{u}_i \,|\, \mathbf{x}\rangle.$$

由于 $\beta(G\mathbf{x}) \in V^G$,

$$\beta(G\,\mathbf{x}) = \mathbf{P}\beta(G\,\mathbf{x}) = \sum_{i\in[k]} \langle \mathbf{u}_i \,|\, \beta(G\,\mathbf{x})\rangle \mathbf{u}_i = \sum_{i\in[k]} \langle \mathbf{u}_i \,|\, \mathbf{x}\rangle \mathbf{u}_i = \mathbf{P}\mathbf{x}. \qquad \square$$

引理 2.15. 设 $\left(R, \mathbb{Q}^{\mathbb{Z}_\ell}\right)$ 是 $\mathbb{Z}_\ell$ 的正则 $\mathbb{Q}$-表示。则 $\mathbb{Q}^{\mathbb{Z}_\ell}$ 的不动子空间上的投影矩阵 $\mathbf{P}_\ell$ 为 $(1/\ell)\mathbf{J}$，其中 $\mathbf{J}$ 是 $\ell \times \ell$ 全 $\mathbf{1}$ 矩阵。

证明. 注意， V 的不动子空间是平凡表示 $\mathbb{Z}_\ell$ 的若干个副本的直和。由定理 2.2,

$$\mathbf{P}_\ell = \frac{1}{\ell} \sum_{j\in\mathbb{Z}_\ell} \overline{\chi_0(j)} \mathbf{M}_{R(j)} = \frac{1}{\ell} \sum_{j\in\mathbb{Z}_\ell} \mathbf{M}_{R(j)} = \frac{1}{\ell}\mathbf{J}. \qquad \square$$

3. 主要结果

我们首先证明主要结果中的第一个结果。

定理 1.1 的证明. 设

$$\mathcal{F}_\ell^1 = \{\mathbf{u} \in \{-1,1\}^\ell \,|\, \exists \mathbf{v} \ni (\mathbf{u}, \mathbf{v}) \text{ is an LP}\}$$

and

$$\mathcal{F}_\ell^2 = \{\mathbf{v} \in \{-1,1\}^\ell \,|\, \exists \mathbf{u} \ni (\mathbf{u}, \mathbf{v}) \text{ is an LP}\}.$$

由对称性， $\mathcal{F}_\ell^1 = \mathcal{F}_\ell^2$。由于 $\mathcal{F}_\ell \neq \varnothing$，存在 $(\mathbf{u}^\top, \mathbf{v}^\top)^\top \in \mathcal{F}_\ell$。于是 $\mathbf{u} \in \mathcal{F}_\ell^1$，且 $\mathbf{v} \in \mathcal{F}_\ell^2$。令 $\mathbf{p} = \beta(\mathbb{Z}_\ell \mathbf{u}) = -(1/\ell)\mathbf{1}$。则 $\mathbf{p} \in \mathsf{Conv}(\mathcal{F}_\ell^1) \subseteq \mathsf{Aff}(\mathcal{F}_\ell^1)$。为得出所需结论，我们注意到以下事实:

(i) Since $\mathcal{F}_\ell^1 = \mathcal{F}_\ell^2$, $\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_\ell^1 - \mathbf{p}) = \mathrm{Span}_{\mathbb{C}}(\mathcal{F}_\ell^2 - \mathbf{p})$.

(ii) 由于 $\mathsf{Span}_{\mathbb{C}}(\mathcal{F}_\ell^1 - \mathbf{p})$ 和 $\mathsf{Span}_{\mathbb{C}}(\mathcal{F}_\ell^2 - \mathbf{p})$ 都是 $\mathbb{C}$-子表示，且在 $\mathbb{Z}_\ell$ 的作用下与 $\mathbf{1}$ 正交，因此根据定理 2.1，$\mathsf{Span}_{\mathbb{C}}(\mathcal{F}_\ell^1 - \mathbf{p})$ 和 $\mathsf{Span}_{\mathbb{C}}(\mathcal{F}_\ell^2 - \mathbf{p})$ 都必须是 $(\mathbb{Q}^{\mathbb{Z}_\ell})_{\mathbb{C}}$ 的不可约 $\mathbb{C}$-子表示 $V_1, \ldots, V_{\ell-1}$ 的正交直和。

(iii) $\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_\ell^1 - \mathbf{p})$ 和 $\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_\ell^2 - \mathbf{p})$ 不可能都与某个 $k \in [\ell - 1]$ 的不可约 V_k 正交。否则，这将意味着 $\mathbf{u}$ 的 DFT 必须满足

$$\mu_k(\mathbf{u}) = \mu_k(\mathbf{u} - \mathbf{p}) = 0,$$

同样，$\mu_k(\mathbf{v}) = 0$，这与定理 2.9 矛盾。

由 (i)、(ii) 和 (iii),

$$\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_\ell^1 - \mathbf{p}) = V_1 \oplus \cdots \oplus V_{\ell-1} \text{ and } \mathrm{Span}_{\mathbb{C}}(\mathcal{F}_\ell^2 - \mathbf{p}) = V_1 \oplus \cdots \oplus V_{\ell-1}.$$

设 $\mathbf{f} = \beta\left((\mathbb{Z}_\ell \times \mathbb{Z}_\ell)\left(\mathbf{u}^\top,\ \mathbf{v}^\top\right)^\top\right) = -(1/\ell)\left(\mathbf{1}^\top, \mathbf{1}^\top\right)^\top$。则 $\mathbf{f} \in \mathsf{Conv}(\mathcal{F}_\ell) \subseteq \mathsf{Aff}(\mathcal{F}_\ell)$。显然,

$$\mathrm{Span}_{\mathbb{C}}\left(\mathcal{F}_\ell - \mathbf{f}\right) = \mathrm{Span}_{\mathbb{C}}\left(\mathcal{F}_\ell^1 - \mathbf{p}\right) \oplus \mathrm{Span}_{\mathbb{C}}\left(\mathcal{F}_\ell^2 - \mathbf{p}\right).$$

根据定理 2.7，$\mathsf{Span}_{\mathbb{Q}}(\mathcal{F}_\ell^i - \mathbf{p}) = \bigoplus_{d\,|\,\ell d \neq \ell} \mathsf{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ 对于 $i = 1$、2，且根据事实 (i),

$$\mathrm{Span}_{\mathbb{Q}}\left(\mathcal{F}_\ell - \mathbf{f}\right) = \left(\bigoplus_{\substack{d\,|\,\ell \\ d \neq \ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)\right) \oplus \left(\bigoplus_{\substack{d\,|\,\ell \\ d \neq \ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)\right).$$

因此,

维数(凸包($\mathcal{F}_\ell$)) = 维数(张成空间($\mathcal{F}_\ell - \mathbf{f}$)) = 维数$_{\mathbb{Q}}$(张成空间$_{\mathbb{Q}}$($\mathcal{F}_\ell - \mathbf{f}$)) $= 2(\ell-1) = 2\ell-2$. □

下面的定理是证明我们的下一个主要结果所需的。

定理 3.1. 设 $\mathbf{u} \in \mathbb{Q}^\ell$ 满足 $\mathsf{Span}_{\mathbb{Q}}(\mathbf{u}) \neq \mathsf{Span}_{\mathbb{Q}}(\mathbf{1})$，且 $\mathbf{y} = \mathbf{u} - (\mathbf{1}^\top\mathbf{u}/\ell)\mathbf{1}$。则存在 $T \subseteq \{d \in [\ell] :\ d \mid \ell \text{ 且 } d \neq \ell\}$，使得

$$\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell\,\mathbf{y}) = \bigoplus_{d \in T} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d), \tag{3.1}$$

其中 $\mathbf{P}_d$ 的定义见定理 2.7。此外,

$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell\,\mathbf{u})) = \dim(\mathrm{Aff}(\mathbb{Z}_\ell\,\mathbf{u})) = \dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell\,\mathbf{y})) = \mathrm{rank}(\mathbf{C}_\mathbf{y}) = \sum_{d \in T} \phi\left(\frac{\ell}{d}\right),$$

其中 $\mathbf{C}_\mathbf{y}$ 是首行为 $\mathbf{y}$ 的 $\ell \times \ell$ 循环矩阵。

证明。由于 $\mathsf{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ 是在 $\mathbb{Z}_\ell$作用下的 $\mathbb{Q}$-子表示，因此根据定理 2.1，$\mathsf{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ 是 $\mathbb{Q}^{\mathbb{Z}_\ell}$的不可约 $\mathbb{Q}$-子表示的正交直和。根据定理 2.7，$\mathbb{Q}^{\mathbb{Z}_\ell}$ 的不可约 $\mathbb{Q}$-子表示为每个 ℓ的因子 d 对应的 $\mathsf{Col}_{\mathbb{Q}}(\mathsf{P}_d)$ 。因此，存在一个由 ℓ的因子组成的集合 T，使得等式 (3.1) 成立。我们首先证明，$\mathsf{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ 仅与 $\mathsf{Col}_{\mathbb{Q}}(\mathsf{P}_\ell)$正交，其中 P_ℓ 是在 $\mathbb{Z}_\ell$作用下投影到 $\mathbb{Q}^{\mathbb{Z}_\ell}$ 的不动子空间的投影。由于 $\mathsf{Col}_{\mathbb{Q}}(\mathsf{P}_\ell) = \mathsf{Span}_{\mathbb{Q}}(\mathbf{1}), \langle \mathbf{y} \mid \mathbf{1} \rangle = 0$, 且表示 $\mathbb{Q}^{\mathbb{Z}_\ell}$是酉的，因此 $\mathsf{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ 与 $\mathsf{Col}_{\mathbb{Q}}(\mathsf{P}_\ell)$正交。

设 $\mathbf{z} = \mathbf{u} - \mathsf{P}_\ell \mathbf{u}$。于是，根据引理 2.15，$\mathbf{z} = \mathbf{y} = \mathbf{u} - (\mathbf{1}^\top \mathbf{u}/\ell)\mathbf{1}$。由于根据引理 2.14，$\mathsf{P}_\ell \mathbf{y} = \mathsf{P}_\ell \mathbf{u} - \mathsf{P}_\ell^2 \mathbf{u} = \mathbf{0}$ 且 $\beta(\mathbb{Z}_\ell \mathbf{y}) = \mathsf{P}_\ell \mathbf{y}$，$\mathbf{0} = \beta(\mathbb{Z}_\ell \mathbf{y}) \in \mathsf{Conv}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$，因为$\beta(\mathbb{Z}_\ell \mathbf{y})$ 是 $\mathbb{Z}_\ell \mathbf{y}$中点的凸组合。于是，根据引理 2.13，我们有 $\mathsf{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y}) = \mathsf{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$。注意到

$$\begin{aligned}\dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{u})) &= \dim_{\mathbb{Q}}\left(\mathrm{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{u}) - \frac{\mathbf{1}^\top \mathbf{u}}{\ell}\mathbf{1}\right) \\ &= \dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})) = \dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})).\end{aligned}$$

于是,

$$\dim(\mathrm{Aff}(\mathbb{Z}_\ell \mathbf{u})) = \dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{u})) = \dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})) = \sum_{d \in T} \phi\left(\frac{\ell}{d}\right). \quad \square$$

现在我们证明定理 1.3。

定理 1.3 的证明。

由于 $\mathbb{Z}_\ell < \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$，只需证明 $G = \mathbb{Z}_\ell$的情形。令 $X_1 = \mathbb{Z}_\ell \mathbf{u}, X_2 = \mathbb{Z}_\ell \mathbf{v}$。由于

$$\dim(\mathrm{Conv}(X_1)) = \dim(\mathrm{Aff}(X_1)) \quad \text{and} \quad \dim(\mathrm{Conv}(X_2)) = \dim(\mathrm{Aff}(X_2)),$$

根据定理 3.1，只需证明 $U_1 \cap U_2 = \varnothing$。为导出矛盾，设 $d' \in U_1 \cap U_2$ 满足 $d' \neq \ell$。这意味着对每个 $i = 1, 2$，$\mathsf{Span}_{\mathbb{C}}(X_i + (1/\ell)\mathbf{1})$ 与 $\mathsf{Col}_{\mathbb{C}}(\mathsf{P}_{d'})$正交。此外，$\mathsf{Col}_{\mathbb{C}}(\mathsf{P}_{d'}) \subset (\mathbb{Q}^{\mathbb{Z}_\ell})_{\mathbb{C}}$ 和 $\mathsf{Col}_{\mathbb{C}}(\mathsf{P}_{d'})$ 在 $\mathbb{Z}_\ell$的作用下保持不变。于是，根据定理 2.1 和 2.4，存在$U' \subset \mathbb{Z}_\ell - \{0\}$ 使得 $\mathsf{Col}_{\mathbb{C}}(\mathsf{P}_{d'}) = \bigoplus_{i \in U'} V_i$。这意味着对每个 $i = 1, 2$，$\mathsf{Span}_{\mathbb{C}}(X_i + (1/\ell)\mathbf{1})$ 与某个不可约 V_k 正交，其中 $k \in [\ell - 1]$。于是

$$\mu_k(\mathbf{u}) = \mu_k\left(\mathbf{u} + \frac{1}{\ell}\mathbf{1}\right) = 0,$$

同理，$\mu_k(\mathbf{v}) = 0$，这与定理 2.9 矛盾。 $\square$

引理 3.2。设 m、$n \in \mathbb{Z}$。若 $m - 2 \geqslant 2$、$n - 2 \geqslant 1$ 或 $m - 2 \geqslant 1$、$n - 2 \geqslant 2$，则 $n - 2 \geqslant 2(n-1)/m$.

证明。若 $m-2\geqslant 2$、$n-2\geqslant 1$ 或 $m-2\geqslant 1$、$n-2\geqslant 2$，则 $(m-2)(n-2)\geqslant 2$。在 $(m-2)(n-2)\geqslant 2$ 两边加上 $2(n-2)$，得到 $m(n-2)\geqslant 2(n-1)$。因此 $n-2\geqslant 2(n-1)/m$。 □

引理 3.3. 设 p,q 是互不相同的奇素数。那么 $2(q-1)(p-1)$ 除以 p 所得的商至少为 q。此外，对于 $2(q-1)(p-1)=sp+r$，其中 $s=2(q-1)-k$，$r=kp-2(q-1)$，且 k 是满足 $kp-2(q-1)\geqslant 0$ 的最小整数，则 s 和 r 分别是 $2(q-1)(p-1)$ 除以 p 所得的商和余数。

证明. 对于任意整数 k, $2(q-1)(p-1)=(2(q-1)-k)p+(kp-2(q-1))$，我们都可以选取满足 $kp-2(q-1)\geqslant 0$ 的最小 k。于是 $k=\lceil 2(q-1)/p\rceil$，其中 $\lceil n\rceil$ 是 n 的向上取整。设 $2(q-1)(p-1)=sp+r$，其中 $s=2(q-1)-k$ 且 $r=kp-2(q-1)$。现在，由于 p,q 是互不相同的奇素数，不失一般性，设 $p\geqslant 3$，则 $q\geqslant 5\geqslant 4$。由于 $p-2\geqslant 1$ 且 $q-2\geqslant 2$，根据引理 3.2，$q-2\geqslant 2(q-1)/p$。因此，$q-2\geqslant k$。于是 $s-q=2(q-1)-k-q=q-2-k\geqslant k-k=0$。最后，由于 $k-1<2(q-1)/p$, $r=pk-2(q-1)<p$。

□

引理 3.4. 设 $\ell=p^\alpha q^\beta$，其中 p、q 是互不相同的奇素数，且 α、$\beta\in\mathbb{Z}_{\geqslant 1}$。则 $\phi(\ell)>(\ell-1)/2$。

证明。由引理 3.3，$2(q-1)(p-1)=sp+r$，其中 $s\geqslant q$。于是

$$\begin{aligned}2\phi(\ell)&=2(q-1)(p-1)p^{\alpha-1}q^{\beta-1}\\&=(sp+r)p^{\alpha-1}q^{\beta-1}\\&\geqslant p^\alpha q^\beta+rp^{\alpha-1}q^{\beta-1}\\&>p^\alpha q^\beta-1\\&=\ell-1,\end{aligned}$$

结论由此得证。 □

引理 3.5. 设 $\mathbf{u}\in\mathbb{Q}^\ell$，则

$$||\boldsymbol{\mu}(\mathbf{u})||^2=\ell||\mathbf{u}||^2.$$

证明。设 U 为以离散傅里叶基向量 $\mathbf{v}_0$、……、$\mathbf{v}_{\ell-1}$ 为列的矩阵。于是，由于 $\boldsymbol{\mu}=\mathbf{U}^\top\mathbf{u}$,

$$||\boldsymbol{\mu}(\mathbf{u})||^2=\sum_{k\in\mathbb{Z}_\ell}|\mu_k(\mathbf{u})|^2=\boldsymbol{\mu}^*\boldsymbol{\mu}=\mathbf{u}^\top\mathbf{U}^*\mathbf{U}\mathbf{u}=\mathbf{u}^\top\ell\mathbf{I}_{\mathbb{Q}^\ell}\mathbf{u}=\ell||\mathbf{u}||^2,$$

其中我们用到了 $\mathbf{U}^*\mathbf{U}=\ell\mathbf{I}_{\mathbb{Q}^\ell}$ 这一事实。 □

推论 3.6. 设 $\mathbf{u} \in \mathbb{Q}^{\mathbb{Z}_\ell}$ 满足 $||\mathbf{u}||^2 = \ell$ 且 $\langle \mathbf{1} | \mathbf{u} \rangle = -1$。那么

$$\sum_{k=1}^{\ell-1} |\mu_k(\mathbf{u})|^2 = (\ell+1)(\ell-1).$$

证明。由引理 3.5,

$$\sum_{k=1}^{\ell-1} |\mu_k(\mathbf{u})|^2 = ||\boldsymbol{\mu}(\mathbf{u})||^2 - |\mu_0(\mathbf{u})|^2 = \ell^2 - 1 = (\ell+1)(\ell-1). \qquad \square$$

对于每个 ℓ、$n \in \mathbb{Z}_{\geqslant 1}$，拉马努金和 [1] 定义为 $c_\ell(n) = \sum_{\substack{0<k\leqslant \ell \\ (k,\ell)=1}} e^{2\pi i k n/\ell}$。

众所周知，$\forall \ell$、$n \in \mathbb{Z}_{\geqslant 1}$

$$c_\ell(n) = \mu\left(\frac{\ell}{(\ell,n)}\right) \frac{\phi(\ell)}{\phi\left(\frac{\ell}{(\ell,n)}\right)} \in \mathbb{Z},$$

其中

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 \dots p_r \text{ for distinct primes } p_1, \dots, p_r, \\ 0 & \text{if } n \text{ is divisible by some prime square} \end{cases}$$

是莫比乌斯函数。

引理 3.7。设 $\ell > 1$ 和 $\mathbf{u} \in \mathbb{Q}^\ell$。若 d 是 ℓ的因子，则

$$\sum_{\substack{0<k\leqslant \ell \\ (k,\ell)=d}} |\mu_k(\mathbf{u})|^2 = \sum_{s \in \mathbb{Z}_\ell} c_{\frac{\ell}{d}}(s) P_{\mathbf{u}}(s).$$

证明。首先,

$$\sum_{\substack{0<k\leqslant \ell \\ (k,\ell)=d}} e^{\frac{2\pi i k(h-j)}{\ell}} = \sum_{\substack{0<r\leqslant \frac{\ell}{d} \\ (r,\frac{\ell}{d})=1}} e^{\frac{2\pi i r(h-j)}{\frac{\ell}{d}}} = c_{\frac{\ell}{d}}(h-j).$$

设 $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{\ell-1}$ 为离散傅里叶基向量。注意，$\mathbf{v}_k \mathbf{v}_k^* = [a_{hj}^k]$，其中 $a_{hj}^k = e^{2\pi i k(h-j)/\ell}$。那么

$$\sum_{\substack{0<k\leqslant \ell \\ (k,\ell)=d}} \mathbf{v}_k \mathbf{v}_k^* = [b_{hj}^d],$$

其中 $b_{hj}^d = c_{\ell/d}(h-j)$。由于 $\mu_k(\mathbf{u}) = \mathbf{u}^\top \mathbf{v}_k$,

$$|\mu_k(\mathbf{u})|^2 = \mu_k(\mathbf{u})\overline{\mu_k(\mathbf{u})} = (\mathbf{u}^\top \mathbf{v}_k)(\mathbf{v}_k^* \mathbf{u}) = \mathbf{u}^\top (\mathbf{v}_k \mathbf{v}_k^*) \mathbf{u}.$$

Then

$$\begin{aligned}\sum_{\substack{0<k\leqslant\ell\\(k,\ell)=d}}|\mu_k(\mathbf{u})|^2 &= \mathbf{u}^\top\left(\sum_{\substack{0<k\leqslant\ell\\(k,\ell)=d}}\mathbf{v}_k\mathbf{v}_k^*\right)\mathbf{u}\\ &= \sum_{h,j\in\mathbb{Z}_\ell} b_{hj}^d u_h u_j\\ &= \sum_{h,j\in\mathbb{Z}_\ell} c_{\frac{\ell}{d}}(h-j)u_h u_j\\ &= \sum_{s,j\in\mathbb{Z}_\ell} c_{\frac{\ell}{d}}(s)u_j u_{j+s}\\ &= \sum_{s\in\mathbb{Z}_\ell} c_{\frac{\ell}{d}}(s)\sum_{j\in\mathbb{Z}_\ell} u_j u_{j+s}\\ &= \sum_{s\in\mathbb{Z}_\ell} c_{\frac{\ell}{d}}(s)P_{\mathbf{u}}(s).\end{aligned}$$

□

对于向量 $\mathbf{u}\in\mathbb{Q}^\ell$ 和 ℓ 的因子 d，令

$$\mathbf{u}^{\frac{\ell}{d}}(j)=\sum_{i\in\mathbb{Z}_d}\mathbf{u}\left(\frac{\ell}{d}i+j\right),\quad \forall j\in\mathbb{Z}_{\frac{\ell}{d}}.$$

那么，$\mathbf{u}^{\ell/d}\in\mathbb{Q}^{\ell/d}$ 称为 $\mathbf{u}$ 的 d-压缩。下面的引理用于证明我们的一个主要结果。

引理 3.8. 设 $\ell>1$ 和 $\mathbf{u}\in\mathbb{Q}^\ell$。如果 d 是 ℓ 的因子，那么

$$\sum_{\substack{0<k\leqslant\ell\\(k,\ell)=d}}|\mu_k(\mathbf{u})|^2=\sum_{\substack{0<k\leqslant\frac{\ell}{d}\\(k,\frac{\ell}{d})=1}}|\mu_k(\mathbf{u}^{\frac{\ell}{d}})|^2.$$

证明. 由引理 3.7,

$$\begin{aligned}\sum_{\substack{0<k\leqslant \ell\\(k,\ell)=d}} |\mu_k(\mathbf{u})|^2 &= \sum_{s\in\mathbb{Z}_\ell} c_{\frac{\ell}{d}}(s) P_{\mathbf{u}}(s)\\ &= \sum_{j\in\mathbb{Z}_{\frac{\ell}{d}}} \sum_{i\in\mathbb{Z}_d} c_{\frac{\ell}{d}}\left(\frac{\ell}{d}i+j\right) P_{\mathbf{u}}\left(\frac{\ell}{d}i+j\right)\\ &= \sum_{j\in\mathbb{Z}_{\frac{\ell}{d}}} c_{\frac{\ell}{d}}\left(\frac{\ell}{d}+j\right) \sum_{i\in\mathbb{Z}_d} P_{\mathbf{u}}\left(\frac{\ell}{d}i+j\right)\\ &= \sum_{s\in\mathbb{Z}_{\frac{\ell}{d}}} c_{\frac{\ell}{d}}(s) P_{\mathbf{u}^{\frac{\ell}{d}}}(s)\\ &= \sum_{\substack{0<k\leqslant \frac{\ell}{d}\\(k,\frac{\ell}{d})=1}} |\mu_k(\mathbf{u}^{\frac{\ell}{d}})|^2. \end{aligned}$$

□

下面的定理由 [4] 中的定理 3 推出。

定理 3.9. 设 $(\mathbf{u},\mathbf{v})$ 是长度为 $\ell = dm$ 的线性规划。那么，相应的 $m = \ell/d$-压缩序列 $(\mathbf{u}^d,\mathbf{v}^d)$ 满足

$$\begin{aligned}P_{\mathbf{u}^d}(0) + P_{\mathbf{v}^d}(0) &= 2\ell - 2\left(\frac{\ell}{d}-1\right) = 2\ell + 2 - \frac{2\ell}{d},\\ P_{\mathbf{u}^d}(j) + P_{\mathbf{v}^d}(j) &= -\frac{2\ell}{d}, \quad \forall j \in \mathbb{Z}_d - \{0\}.\end{aligned}$$

现在我们证明另一个主要结果。

定理 3.10. 设 $(\mathbf{u},\mathbf{v})$ 是长度为 ℓ 的线性规划，且对于某个 ℓ 的因子 d，有 $||\mathbf{u}^d||^2 = ||\mathbf{v}^d||^2$，并且 $2\phi(d) \geqslant d-1$。那么，$|\mu_k(\mathbf{v})|^2 > 0$ 且 $|\mu_k(\mathbf{u})|^2 > 0 \forall k \ni (k,\ell) = \ell/d$。

证明. 由对称性，只需证明关于 $\mathbf{v}$ 的结果。反设 $|\mu_{k'}(\mathbf{v})|^2 = 0$ 对某个 $k' \ni (k'$ 成立，且 $\ell) = \ell/d$ 对 ℓ 的某个因子 d 成立。那么 $|\mu_k(\mathbf{v})|^2 = 0\ \forall k \ni (k,\ell) = \ell/d$。由定理 2.9，$|\mu_k(\mathbf{u})|^2 = 2\ell+2\ \forall k \ni (k,\ell) = \ell/d$。因此,

$$\sum_{\substack{0<k\leqslant \ell\\(k,\ell)=\frac{\ell}{d}}} |\mu_k(\mathbf{u})|^2 = (2\ell+2)\phi(d). \tag{3.2}$$

于是，由引理 3.8,

$$\sum_{\substack{0<k\leqslant \ell\\(k,\ell)=\frac{\ell}{d}}} |\mu_k(\mathbf{u})|^2 = \sum_{\substack{0<k\leqslant d\\(k,d)=1}} |\mu_k(\mathbf{u}^d)|^2 = (2\ell+2)\phi(d). \tag{3.3}$$

由定理 3.9,

$$||\mathbf{u}^d||^2 = ||\mathbf{v}^d||^2 = \ell + 1 - \frac{\ell}{d}.$$

于是，由引理 3.5,

$$\sum_{k=1}^{d} |\mu_k(\mathbf{u}^d)|^2 = d||\mathbf{u}^d||^2 - |\mu_0(\mathbf{u}^d)|^2 = d||\mathbf{u}^d||^2 - 1. \tag{3.4}$$

因此，由方程 (3.2)、(3.3) 和 (3.4)

$$\sum_{\substack{0<k\leqslant d\\(k,d)=1}} |\mu_k(\mathbf{u}^d)|^2 = (2\ell+2)\phi(d) < \sum_{k=1}^{d} |\mu_k(\mathbf{u}^d)|^2 = (\ell+1)(d-1)$$

这意味着

$$2\phi(d) < (d-1),$$

矛盾。 □

以下推论由引理 3.4 和定理 3.10 得出。

推论 3.11. 设 $(\mathbf{u}, \mathbf{v})$ 是一个长度为 $\ell = p^\alpha q^\beta$ 的线性规划，其中 p, q 是互不相同的奇素数，且 $\alpha, \beta \in \mathbb{Z}_{\geqslant 1}$。令

$$T = \left\{ d \in [\ell] : d \neq 1, d \mid \ell, and\ ||\mathbf{u}^d||^2 \neq ||\mathbf{v}^d||^2 \right\}.$$

Then

$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})) = \ell - 1 - \sum_{d\in T_1} \phi(d),$$
$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{v})) = \ell - 1 - \sum_{d\in T_2} \phi(d)$$

对于某些 $T_1 \subseteq T$ 和 $T_2 \subseteq T$。等价地

$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})) \geqslant \sum_{d\in T'} \phi(d),$$
$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{v})) \geqslant \sum_{d\in T'} \phi(d),$$

其中

$$T' = \left\{ d \in [\ell] : d \neq 1, d \mid \ell,\ and\ ||\mathbf{u}^d||^2 = ||\mathbf{v}^d||^2 \right\}. \tag{3.5}$$

证明。由对称性，只需证明关于 $\mathbf{u}$ 的结论。令 $\mathbf{y} = \mathbf{u} + (1/\ell)\mathbf{1}$。首先，我们证明

$$\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_{\frac{\ell}{d'}}) \subseteq \mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell\, \mathbf{y})\ \forall d' \in T'.$$

子空间 $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ 是 $\mathbb{Q}$ 的一个子表示，因此要么

$$\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell\, \mathbf{y}) \perp \mathrm{Col}_{\mathbb{Q}}\left(\mathbf{P}_{\frac{\ell}{d'}}\right)$$

or

$$\mathrm{Col}_{\mathbb{Q}}\left(\mathbf{P}_{\frac{\ell}{d'}}\right) \subseteq \mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell\, \mathbf{y}).$$

若 $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell\, \mathbf{y}) \perp \mathrm{Col}_{\mathbb{Q}}\left(\mathbf{P}_{\ell/d'}\right),$，则 $\mathrm{Span}_{\mathbb{C}}(\mathbb{Z}_\ell\, \mathbf{y}) \perp \mathrm{Col}_{\mathbb{C}}\left(\mathbf{P}_{\ell/d'}\right),$，因此$\mu_k(\mathbf{u}) = \mu_k(\mathbf{y}) = 0$，其中某些 $k \ni (k, \ell) = \ell/d'$。由引理 3.4，这与定理 3.10 矛盾。因此，$\mathrm{Col}_{\mathbb{Q}}\left(\mathbf{P}_{\ell/d'}\right) \subseteq \mathrm{Span}_{\mathbb{Q}}\left(\mathbb{Z}_\ell\, \mathbf{y}\right)$，结论现在由定理 3.1 得出。 □

由于对于 $\mathbf{u},\mathbf{v} \in \{-1, 1\}^\ell$，有 $||\mathbf{u}^\ell||^2 = ||\mathbf{v}^\ell||^2 = \ell$，以下推论可由推论 3.11 的证明得出。

推论 3.12。设 $(\mathbf{u}, \mathbf{v})$ 是长度为 $\ell = p^\alpha q^\beta$ 的线性规划，其中 p, q 是互不相同的奇素数，且 $\alpha, \beta \in \mathbb{Z}_{\geqslant 1}$。则

(i) $\mathrm{Col}_{\mathbb{Q}}\left(\mathbf{P}_1\right) \subseteq \mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell\, \mathbf{y})$ *for* $\mathbf{y} = \mathbf{u} + (1/\ell)\mathbf{1}$ *and* $\mathbf{y} = \mathbf{v} + (1/\ell)\mathbf{1}$,

(ii) $\dim(\mathrm{Conv}(\mathbb{Z}_\ell\, \mathbf{u})) \geqslant \phi\left(\ell\right)$ 和 $\dim(\mathrm{Conv}(\mathbb{Z}_\ell\, \mathbf{v})) \geqslant \phi\left(\ell\right)$。

方程 (3.5) 中更大的 $|T'|$（见推论 3.11）会为 $\dim(\mathrm{Conv}(\mathbb{Z}_\ell\, \mathbf{u}))$ 和 $\dim(\mathrm{Conv}(\mathbb{Z}_\ell\, \mathbf{v}))$带来更大的下界。有证据表明，一般而言 $T' \neq \varnothing$。事实上，基于已知的线性规划，最近有人在 [10] 中提出猜想：对于每个可被 5 整除的正 ℓ

$$5 \in \left\{d \in [\ell] : d \neq 1,\ d \mid \ell,\ ||\mathbf{u}^d||^2 = ||\mathbf{v}^d||^2, \text{ and } (\mathbf{u}, \mathbf{v}) \text{ is an LP of length } \ell\right\}.$$

另一方面，存在满足 $||\mathbf{u}^d||^2 \neq ||\mathbf{v}^d||^2$ 的线性规划 $(\mathbf{u}, \mathbf{v})$，其中某个因子 d 属于 ℓ，见 [9, 10]。下面的定理给出了 $\dim(\mathrm{Conv}(\mathbb{Z}_\ell\, \mathbf{u}))$ 的一般下界，其中 $\mathbf{u} \in \{-1, 1\}^\ell$ 满足 $\langle \mathbf{1} \mid \mathbf{u} \rangle = -1$。

定理 3.13. 设 $\ell = p_1^{n_1} \ldots p_s^{n_s}$，其中 $p_1, \ldots, p_s$ 是互不相同的奇素数，且 $n_1, \ldots, n_s \in \mathbb{Z}_{\geqslant 1}$。设 $\mathbf{u} \in \{-1, 1\}^\ell$ 满足 $\langle \mathbf{1} \mid \mathbf{u} \rangle = -1$，则

$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell\, \mathbf{u})) \geqslant \sum_{j \in [s]} \sum_{i \in [n_j]} \phi(p_j^i).$$

证明. 设 $\mathbf{y} = \mathbf{u} + (1/\ell)\mathbf{1}$。我们先证明，对于每个 $d_{j,i} = p_1^{n_1} \cdots p_j^i \cdots p_s^{n_s}$, $j = 1, \ldots, s$, $i = 0, \ldots, n_j - 1$，都有 $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}^{d_{j,i}}) \subseteq$ 张成空间 $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$。反之，设 $\mu_k(\mathbf{y}) = 0$，其中某个 $k \ni (k,\ell) = d_{j,i}$。则 $\mu_k(\mathbf{u}) = \mu_k(\mathbf{y}) = 0$，由等式 (2.1) 和定理 2.10, $p_j \mid (\ell + 1)/2,$，矛盾。因此，$\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}^{d_{j,i}}) \subseteq$ 张成空间 $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$，由定理 3.1,

$$\begin{aligned}\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})) &= \dim(\mathrm{Aff}(\mathbb{Z}_\ell \mathbf{u})) = \dim(\mathrm{Span}(\mathbb{Z}_\ell \mathbf{y})) \\ &= \dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})) \geqslant \sum_{j\in[s]} \sum_{i\in[n_j]} \phi(p_j^i).\end{aligned}$$

□

结合推论 3.12 与定理 3.13 的证明即可得到以下推论。

推论 3.14. 设 $(\mathbf{u}, \mathbf{v})$ 是长度为 $\ell = p^\alpha q^\beta$ 的线性规划，其中 p, q 是互不相同的奇素数，且 $\alpha, \beta \in \mathbb{Z}_{\geqslant 1}$。那么

$$\begin{aligned}\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})) &\geqslant \sum_{j\in[\alpha]} \phi(p^j) + \sum_{i\in[\beta]} \phi(q^i) + \phi(\ell), \\ \dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{v})) &\geqslant \sum_{j\in[\alpha]} \phi(p^j) + \sum_{i\in[\beta]} \phi(q^i) + \phi(\ell).\end{aligned}$$

利用 Ingleton [7] 中的结果，可以得到关于 $\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u}))$ 的另一组下界。接下来，当 $\ell = pq^\beta$ 对某些互不相同的奇素数 p, q 及正整数 β 成立时，我们推导这类下界。不过，首先需要介绍非递归矩阵的概念。

设 $\mathbf{C}_\mathbf{u}$ 是 $\mathbf{u} \in \mathbb{R}^\ell$ 的循环矩阵。那么，当 ℓ 是满足以下条件的 ℓ 的唯一因子时，$\mathbf{C}_\mathbf{u}$ 是非递归的：只要 $i \equiv j$ (，就有 $u_i = u_j \mod d$)。以下引理表明，如果存在某个 $\mathbf{v}$，使得 $(\mathbf{u}, \mathbf{v})$ 是一个线性规划，那么 $\mathbf{C}_\mathbf{u}$ 是非递归的。

引理 3.15. 设 $\mathbf{u} \in \{-1, 1\}^\ell$ 且 $\langle \mathbf{1} | \mathbf{u} \rangle = \mp 1$。那么 $\mathbf{C}_\mathbf{u}$ 是非递归的 .

证明。首先注意到约束 $\langle \mathbf{1} | \mathbf{u} \rangle = \mp 1$ 意味着存在 $(\ell \pm 1)/2$ 个 -1 和 $(\ell \mp 1)/2$ 1 个。反设 $\mathbf{C}_\mathbf{u}$ 是 s-递归的。那么，当 $i \equiv j$ (模 s) 时，$s \mid \ell$ 且 $u_i = u_j$。由于 u_0、.....、u_{s-1} 各出现 $d = \ell/s$ 次，而 d 既不整除 $(\ell \pm 1)/2$ 也不整除 $(\ell \mp 1)/2,$，因此得到矛盾。

□

下面的引理及其后续推论用于根据 [7] 中关于循环矩阵 $\mathbf{C}_\mathbf{u}$（其中 $\mathbf{u} \in \{0、1\}^\ell$）的秩下界，推导循环矩阵 $\mathbf{C}_\mathbf{u}$（其中 $\mathbf{u} \in \{-1、 1\}^\ell$）的秩下界。

引理 3.16。设 $\mathbf{C}_\mathbf{u}$ 是 $\mathbf{u} \in \mathbb{R}^\ell$ 的循环矩阵，$\mathbf{J}$ 是 $\ell \times \ell$ 全 1 矩阵，且 $\lambda \in \mathbb{R}$。则

(i) 离散傅里叶基 $\{\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{\ell-1}\}$ 是 $\mathbf{C_u}$ 和 $\mathbf{C_u} + \lambda\mathbf{J}$ 的特征基,

(ii) 若对应于特征向量 $\mathbf{v}_i$ 的 $\mathbf{C_u}$ 的特征值在 $i = 0, \ldots, \ell-1$ 中为 μ_i，则对应于特征向量 $\mathbf{v}_0$ 和 $\mathbf{v}_i$ 的 $\mathbf{C_u} + \lambda\mathbf{J}$ 的特征值在 $i = 1, \ldots, \ell-1$ 中分别为 $\mu_0 + \ell\lambda$ 和 μ_i，其中 $\mu_0 = \sum_{i=0}^{\ell-1} u_i$。

证明。直接验证引理中的结论即可。 □

下面的推论由引理 3.16 得出。

推论 3.17。设 $\mathbf{u}$、$\mathbf{C_u}$、$\mathbf{J}$ λ 和 μ_0 如引理 3.16 中所述。则

(i)

$$\operatorname{rank}(\mathbf{C_u} + \lambda\mathbf{J}) = \begin{cases} \operatorname{rank}(\mathbf{C_u}) & if \quad (\mu_0 + \ell\lambda)\mu_0 \neq 0, \\ \operatorname{rank}(\mathbf{C_u}) + 1 & if \quad \mu_0 = 0 \ and \ \lambda \neq 0, \\ \operatorname{rank}(\mathbf{C_u}) - 1 & if \quad \mu_0 + \ell\lambda = 0 \ and \ \lambda \neq 0, \end{cases}$$

(ii) 对于奇数 ℓ 和 $\mathbf{u} \in \{0,1\}^\ell$,

$$\operatorname{rank}(\mathbf{C_{2u-1}}) = \operatorname{rank}(\mathbf{C_u}).$$

证明。由引理 3.16 可立即得到 (i)。由于 $\mathbf{C_{2u-1}} = 2\mathbf{C_u} - \mathbf{J}$，且对于奇数 ℓ,

$$\operatorname{rank}(2\mathbf{C_u} - \mathbf{J}) = \operatorname{rank}(2\mathbf{C_u}) = \operatorname{rank}(\mathbf{C_u}),$$

(ii) 得证。 □

对于 $\ell = p^\alpha p_1^{\alpha_1} \ldots p_{m-1}^{\alpha_{m-1}}$，其中 p、p_1、……、p_{m-1} 是互异素数，且 α、α_1、……、$\alpha_{m-1} \in \mathbb{Z}_{\geqslant 1}$，令

$$\tau(\ell, p) = 1 + \epsilon(m)\epsilon(\alpha)\phi(p) + \phi(p^\alpha) + \sum_{i \in [m-1]} \phi(pp_i^{\alpha_i}),$$

其中，对于 $k \in \mathbb{Z}_{\geqslant 1}$，$\epsilon(1) = 0$ 和 $\epsilon(k) = 1$。现在，下面的引理由关于循环 $\ell \times \ell$ 非递归循环矩阵的相应结果以及 Ingleton [7] 和推论 3.17 得出，该矩阵的元素来自 {0、1}。

引理 3.18。设 $\ell = pq^\beta$，其中 p、q 是互不相同的奇素数，且 $\beta \in \mathbb{Z}_{\geqslant 1}$。令 $\mathbf{u} \in \{-1、1\}^\ell$ 满足 $\langle \mathbf{1} \,|\, \mathbf{u} \rangle = -1$。则 $\operatorname{rank}(\mathbf{C_u}) \geqslant \min\{\tau(\ell、p)、\tau(\ell、q)\}$。

若 $\beta \geqslant 2$，则以下引理表明秩至少为 $\tau(\ell, q)$。

引理 3.19. 设 $\ell = pq^\beta$，其中 p, q 为互不相同的奇素数，且 $\beta \in \mathbb{Z}_{\geqslant 2}$。则 $\tau(\ell, q) < \tau(\ell, p)$。

证明。现在

$$\tau(\ell, q) = 1 + \epsilon(2)\epsilon(\beta)\phi(q) + \phi(q^\beta) + \phi(pq) = 1 + \phi(q) + \phi(q^\beta) + \phi(pq),$$

and

$$\tau(\ell, p) = 1 + \phi(p) + \phi(pq^\beta).$$

Then

$$\begin{aligned}\tau(\ell, p) - \tau(\ell, q) &= \phi(q)(q^{\beta-1}(\phi(p) - 1) - (\phi(p) + 1)) + \phi(p) \\ &= \phi(q)(q^{\beta-1}(p-2) - p) + \phi(p).\end{aligned}$$

我们考虑两种情况： $p = 3$ 和 $p \geqslant 5$。如果 $p = 3$，那么

$$\tau(\ell, p) - \tau(\ell, q) = \phi(q)(q^{\beta-1} - 3) + \phi(3) \geqslant \phi(q)(5^{\beta-1} - 3) + \phi(3) > 0.$$

假设 $p \geqslant 5$。那么，由于 $q^{\beta-1} - 1 \geqslant 1$ 和 $p - 3 \geqslant 1$， $(q^{\beta-1} - 1)(p - 3) \geqslant 1$。于是 $q^{\beta-1}(p-2) - p \geqslant q^{\beta-1} - 2 \geqslant 3^{\beta-1} - 2 > 0.$，这意味着

$$\tau(\ell, p) - \tau(\ell, q) = \phi(q)(q^{\beta-1}(p-2) - p)) + \phi(p) > 0. \qquad \square$$

现在，以下推论由定理 3.13、推论 3.17 以及引理 3.18 和 3.19 得出。

推论 3.20。设 $\ell = pq^\beta$，其中 p、 q为互不相同的奇素数，且 $\beta \in \mathbb{Z}_{\geqslant 2}$。设 $\mathbf{C_u}$，其中 $\mathbf{u} \in \{-1、 1\}^\ell$，为 $\mathbf{u}$ 的循环矩阵，且 $\mathbf{C_u}$ 是非递归的。那么

$$\operatorname{rank}(\mathbf{C_u}) \geqslant L(pq^\beta) = \max\left\{\phi(pq) + \phi(q) + \phi(q^\beta) + 1,\ \phi(p) + \sum_{i\in[\beta]} \phi(q^i) + 1\right\}.$$

若 $\phi(pq) + \phi(q) + \phi(q^\beta) > \phi(p) + \sum_{i\in[\beta]} \phi(q^i)$，我们可以改进推论 3.20 中的下界。我们有如下定理。

定理 3.21. 设 $\ell = pq^\beta$，其中 p、 q 是互不相同的奇素数，且 $\beta \in \mathbb{Z}_{\geqslant 2}$。设 $\mathbf{C_u}$ 是 $\mathbf{u} \in \{-1、 1\}^\ell$ 的循环矩阵，使得 $\mathbf{C_u}$ 是非递归的。则

(i) 秩($\mathbf{C_u}$) 至少为

$$\begin{aligned}&\phi(p) + \phi(pq) + \sum_{i\in[\beta]} \phi(q^i) + 1 \quad \textit{if } \phi(pq) + \phi(q) + \phi(q^\beta) > \phi(p) + \sum_{i\in[\beta]} \phi(q^i), \\ &\phi(p) + \sum_{i\in[\beta]} \phi(q^i) + 1 \quad \textit{otherwise},\end{aligned}$$

(ii) $\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u}))$ 至少为

$$\begin{aligned}\phi(p)+\phi(pq)+\sum_{i\in[\beta]}\phi(q^i) \quad & \text{if } \phi(pq)+\phi(q)+\phi(q^\beta)>\phi(p)+\sum_{i\in[\beta]}\phi(q^i),\\ \phi(p)+\sum_{i\in[\beta]}\phi(q^i) \quad & \text{otherwise.}\end{aligned}$$

证明。我们先证明 (ii) 可由 (i) 推出。令 $\mathbf{y} = \mathbf{u} - (\mathbf{1}^\top \mathbf{u}/\ell)\mathbf{1}$。由定理 3.1,

$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})) = \dim(\mathrm{Aff}(\mathbb{Z}_\ell \mathbf{u})) = \dim(\mathrm{Span}(\mathbb{Z}_\ell \mathbf{y})) = \mathrm{rank}(\mathbf{C_y}).$$

由于 $C_y = C_u - ((\mathbf{1}^\top u)/\ell)J$，由推论 3.17 的 (i) 部分,

$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})) = \mathrm{rank}(\mathbf{C_y}) = \mathrm{rank}(\mathbf{C_u}) - 1.$$

为证明 (i)，假设$\phi(pq)+\phi(q)+\phi(q^\beta) > \phi(p)+\sum_{i\in[\beta]}\phi(q^i)$。由推论 3.17和定理 3.1,

$$\mathrm{rank}(\mathbf{C_u}) = \mathrm{rank}(\mathbf{C_y}) + 1 = 1 + \phi(p) + \sum_{i\in[\beta]}\phi(q^i) + \sum_{i\in[\beta]} a_i \phi(pq^i),$$

其中 $a_i \in \{0、1\}$、$i \in [\beta]$。若 $a_i = 0\ \forall i \in [\beta]$，则

$$\mathrm{rank}(\mathbf{C_u}) = 1 + \phi(p) + \sum_{i\in[\beta]}\phi(q^i) < 1 + \phi(pq) + \phi(q) + \phi(q^\beta),$$

这与推论 3.20 矛盾。因此，至少有一个 a_i 必须等于 1。由于 $\phi(pq^{i_1}) > \phi(pq^{i_2})$ 当且仅当 $i_1 > i_2$，$a_1 = 1$，$a_i = 0$ 对于 $i = 2$、.....、β 会得到 $\mathrm{rank}(C_u)$ 的最小值，因此我们无法排除这种情况。 □

以下推论可由定理 3.1 和定理 3.21 立即推出。

推论 3.22. 设 $\ell = pq^2$，其中 p, q 是互不相同的奇素数。令 C_u，其中 $\mathbf{u} \in \{-1, 1\}^\ell$，为 u 的循环矩阵，且 C_u 是非递归的。那么 $\mathrm{rank}(C_u)$ 至少为

$$\phi(p) + \phi(pq) + \phi(q) + \phi(q^2) + 1 = \ell - \phi(\ell).$$

因此，要么

$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})) = \ell - 1 - \phi(\ell),$$

or

$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})) = \ell - 1.$$

以下推论由引理 2.11、2.12 和 2.3 以及定理 3.1 推出。

推论 3.23. 设 p, q 是互不相同的奇素数，且 $n \in \mathbb{Z}_{\geqslant 1}$。假设 $\ell = p^n$ 或 $\ell = pq$。令 $\mathbf{u} \in \{-1, 1\}^\ell$ 满足 $\langle \mathbf{1} \,|\mathbf{u}\rangle = -1$，并令 $\mathbf{y} = \mathbf{u} + (1/\ell)\mathbf{1}$。则

$$\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y}) = \bigoplus_{\substack{d \,|\, \ell \\ d \neq \ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d),$$

其中 $\mathbf{P}_d$ 在定理 2.7 中定义。此外，

$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})) = \dim(\mathrm{Aff}(\mathbb{Z}_\ell \mathbf{u})) = \sum_{\substack{d \,|\, \ell \\ d \neq \ell}} \dim_{\mathbb{Q}}(\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)) = \ell - 1. \tag{3.6}$$

证明. 令 $d \neq \ell$。由于 $(\mathbf{Col}_{\mathbb{Q}}(\mathbf{P}_d))_{\mathbb{C}} = \mathbf{Col}_{\mathbb{C}}(\mathbf{P}_d)$ 由离散傅里叶基向量 $\mathbf{v}_k$（其中 $k \in \mathbb{Z}_\ell \ni (k, \ell) = d$）张成，且 $\mu_k(\mathbf{y}) = \mu_k(\mathbf{u})$。由引理 2.11 和 2.12，$\mu_k(\mathbf{y}) \neq 0$。由于这对 $\forall k \ni (k, \ell) = d$ 均成立，根据引理 2.3，$\mathbf{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ 与 $\mathbf{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ 不正交。由于这对 $d \neq \ell$ 的每个因子 ℓ 均成立，根据定理 3.1，我们必有

$$\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y}) = \bigoplus_{\substack{d \,|\, \ell \\ d \neq \ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d).$$

由定理 3.1 可得方程 (3.6)。 □

由推论 3.14 和 3.22 可得以下引理。

引理 3.24。设 $\ell = pq^2$，且 $(\mathbf{u}, \mathbf{v})$ 是长度为 ℓ 的线性规划，则

$$\dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})) = \dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{v})) = \ell - 1.$$

现在证明定理 1.4。

定理 1.4 的证明。由于 $\mathbb{Z}_\ell < (\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times)$，只需证明结果对 $G = \mathbb{Z}_\ell$ 成立。由推论 3.23 和引理 3.24，

$$\begin{aligned} \ell - 1 &= \dim_{\mathbb{Q}}\left(\mathrm{Aff}_{\mathbb{Q}}\left(\mathbb{Z}_\ell \mathbf{u}\right)\right) = \dim(\mathrm{Aff}(\mathbb{Z}_\ell \mathbf{u})) \\ &= \dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u})). \end{aligned}$$

由定理 1.3 可得结果，因为 $U = \varnothing$ 是唯一的可能性。 □

基于我们已有的部分结果，本文最后提出以下猜想 .

猜想 3.25. 设 $(\mathbf{u}, \mathbf{v})$ 是一个长度为 ℓ 的线性规划。那么

$$\dim(\mathrm{Conv}(G\,\mathbf{u})) = \dim(\mathrm{Conv}(G\,\mathbf{v})) = \ell - 1$$

对于 $G = \mathbb{Z}_\ell$ 和 $G = \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 。

只需针对 $G = \mathbb{Z}_\ell$ 或 $G = \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 中的一个证明猜想 3.25。这是因为根据定理 2.8，在 $G = \mathbb{Z}_\ell$ 或 $G = \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 下，$\mathbb{Q}^{\mathbb{Z}_\ell}$ 分解为不可约 $\mathbb{Q}$-子表示的方式相同。

4. 讨论

本文在证明如下猜想方面取得了进展：对于长度为 ℓ的 LP(u,v) ，

$$\dim(\mathrm{Conv}(G\,\mathbf{u})) = \dim(\mathrm{Conv}(G\,\mathbf{v})) = \ell - 1$$

对于 $G = \mathbb{Z}_\ell$和 $G = \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ 。这一猜想的直接推论是：对于线性规划问题，不能通过对 u 或 v 施加额外的线性无关线性等式约束来缩小线性规划的搜索空间，否则会导致该问题的秩 1 CSDD 不可行，或使其对称群排除 $\mathbb{Z}_\ell$的某个非空子集；前提是该秩 1 CSDD 原本可行。未来的研究将致力于在有或没有额外假设的情况下证明猜想 3.25。

致谢

本文所表达的观点仅代表作者本人，并不反映美国空军、国防部或美国政府的官方政策或立场。

参考文献

[1] T.M. Apostol。《解析数论导论》。施普林格科学与商业媒体，1998年。

[2] K.T. Arasu、D.A Bulutoglu 和 J.R. Hollon。勒让德 G-数组对及若干 G-数组族的理论统一。《组合设计杂志》，28(11):814–841，2020年。

[3] J. Dattorro。《凸优化与欧几里得距离几何》。Meboo Publishing, 2019年。[4] D.Z. Djokovic 和 I.S. Kotsireas。周期互补序列的压缩及其应用。《设计、编码与密码学》，74:365–377，2015年。[5] A. F¨assler 和 E. Stiefel。《群论方法及其应用》。Birkh¨auser，波士顿，美国，1992年。[6] R.J. Fletcher、M. Gysin 和 J. Seberry。将离散傅里叶变换应用于广义勒让德对与 Hadamard 矩阵的搜索。《澳大拉西亚组合学杂志》，23:75–86，2001年。[7] A.W. Ingleton。循环矩阵的秩。《伦敦数学学会杂志》，1(4):445–460, 1956年。[8] I.M. Isaacs。《有限群的特征标理论》。Academic Press 1976年版的修订重印本。Dover，纽约，美国，1994年。[9] I.S. Kotsireas 和 C. Koutschan。长度为 $\ell \equiv 0 \pmod 3$ 的勒让德对。《组合设计杂志》，29(12):870–887，2021年。[10] I.S. Kotsireas、C. Koutschan、D.A. Bulutoglu 和 J.S. Turner。长度为 $\ell \equiv 0 \pmod 5$ and $\ell = 85, \ell = 87$ case 的勒让德对。arXiv，2021年。[11] T.Y. Lam 和 K.H. Leung。关于单位根的消失和。《代数杂志》，224(1):91–109，2000年。[12] J.J. Rotman。《高等现代代数》，第114卷。美国数学会，2010年。[13] R. Sanyal、F. Sottile 和 B. Strumfels。轨道体。《Mathematika》，57(2):275–314，2011年。[14] J.P. Serre。《有限群的线性表示》，第42卷。施普林格，1977年。[15] P.B. Yale。复数域的自同构。《数学杂志》，39(3):135–141，1966年。