arXiv:2302.01114v1 [math.GR] 2 Feb 2023

有限群的多维舒尔环

GANG CHEN、QING REN 和 ILIA PONOMARENKO

Abstract. 对于任意有限群 G和正整数 m，我们定义并研究直积幂 G^m上的一个舒尔环，它为 G^m 的划分提供了一种代数解释，该划分由 m维魏斯费勒-莱曼算法得到。我们证明，当 $m \geq 3$时，该环能够确定群 G 至同构；随着 m 增大，它趋近于由自然作用在 G^m 上的群 Aut(G)所关联的舒尔环。结果表明，求出这一极限环的问题与群同构问题多项式时间等价。

1. Introduction

理解有限群同构问题的一种方式，是寻找能够唯一确定给定群（在同构意义下）的“自然”不变量。这类不变量的例子包括群行列式 [10], 、群环的线性不变量 [17],、凯莱图 [2], 等。然而，所有这些不变量都难以计算，因为目前已知的算法都无法在关于群的阶的多项式时间内计算它们。另一方面，有许多易于计算的不变量，它们能够在同构意义下确定的并非所有群，而只是属于某个特定类的群。例如，阿贝尔群和所有单群都由其所有元素阶构成的多重集唯一确定，参见例如 [11]。

对于有限群 G ，尝试从其直积幂 $G^m = G \times \cdots \times G$ (m 次方)，$m = 1$、2、.....中易于计算的不变量里寻找不变量，似乎很有希望；我们希望对于某个（不太大的） m，这些不变量能够确定群 G 至同构。近期两篇论文 [4, 5]引入并研究了这种方法。其思路是为 G^m的元素定义一种自然的规范着色，借助 m维 Weisfeiler-Leman 算法（m-维 WL）对着色进行细化，并研究由所得着色关联的数值参数构成的 G 不变量。这些不变量可在 $n^{O(m)}$时间内计算，其中 $n = |G|$, 并且当$m = O(d)$时，能够确定 G 至同构；此处及下文中， $d = d(G)$表示 G的生成集的最小基数。

撰写本文的最初动机，是用 S-环（舒尔环）来寻找 m-维 WL 不变量的代数解释。S-环理论由 I. Schur 于 1931年 创立，并由 H. Wielandt 发展，参见 [18, 第 IV 章]; 此后，S-环被广泛应用于群论和代数组合学。回顾一下，群环 $\mathbb{Z}G$ 的子环 $\mathfrak{A}$ 称为群 G 上的 S-环，若存在一个（唯一确定的）划分 $\mathcal{S} = \mathcal{S}(\mathfrak{A})$，将 G 划分为若干类，其中单位元素 1_G 单独构成一类，该划分在取逆元下封闭，并且满足

$$\mathfrak{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \ X \in \mathcal{S}\}, \tag{1}$$

其中，$\underline{X}$ 表示 X 中元素在 $\mathbb{Z}G$里的和；由元素 $\underline{X}$、$X \in \mathcal{S}$组成的 $\mathfrak{A}$ 的线性基称为标准线性基。在两种极端情形下，若划分 $\mathcal{S}$ 是离散划分，或至多由两类组成（$\{1_G\}$ 及其补集），则 S-环 $\mathfrak{A}$ 分别是群环 $\mathbb{Z}G$ 或平凡环 $\mathcal{T}(G)$。

一个自然的 S-环例子（由 I. Schur 提出）可由任意包含一个与 G 同构的正则子群的置换群 K 给出。在这种情况下，可将 K 作用的集合识别为 G，使得 $K \leq \mathrm{Sym}(G)$，且 G 在 K 中 1_G 的稳定子的轨道划分具有 $\mathcal{S}(\mathfrak{A})$ 的形式，其中 $\mathfrak{A}$ 是某个定义在 G 上的 S-环。以这种方式与置换群相关联的每个 S-环都称为舒尔型。舒尔型 S- 环的一个显然例子是自然的次直积 $K = G \rtimes M$ 与 $M \leq \mathrm{Aut}(G)$：此时，$\mathcal{S}(\mathfrak{A}) = \mathrm{Orb}(M)$，而 $\mathfrak{A}$ 记作 $\mathrm{Cyc}(M, G)$。并非每个定义在 G 上的 S-环 $\mathfrak{A}$ 都是舒尔型，但无论如何，都存在唯一的极大群 $K \leq \mathrm{Sym}(G)$，使得与 K 相关联的 S-环包含 $\mathfrak{A}$ 作为子环；这个 K 称为 $\mathfrak{A}$ 的自同构群，记作 $\mathrm{Aut}(\mathfrak{A})$。

设 G 是一个群，$m \geq 1$ 是一个整数。平凡 S-环 $\mathcal{T}(G)$ 的 m 次张量幂 $\mathcal{T}_m(G)$ 是群 G^m 上的一个 S-环。若 $m \neq 1$，则“对角”元素 $\mathrm{Diag}(G^m) \in \mathbb{Z}G^m$ 不属于 $\mathcal{T}_m(G)$~~。我们方~~法的关键环节是由该元素唯一确定的 $\mathcal{T}_m(G)$ 的扩张，

$$\mathfrak{A}_m(G) = \mathcal{T}_m(G)[\underline{\mathrm{Diag}(G^m)}],$$

也就是说，是 G^m 上同时包含 $\mathcal{T}_m(G)$ 和“对角”元素的最小 S-环。[1] 对于 $m = 1$，该 S-环是平凡的；在不计语言表述的情况下，它是 [12，小节 2.1 中定义的秩 5 关联方案的一个特例。5] 若 $m = 2$ 且 $|G| \geq 3$。

对于 $m \geq 3$，S-环 $\mathfrak{A}_m(G)$ 的结构相当复杂（不过，通过对 $G^m \times G^m$ 的适当着色应用二维 WL，可以轻易计算出划分 $\mathcal{S}(\mathfrak{A}_m(G))$）。另一方面，根据 [3] 的结果（另见推论 5.3），不难推得，若 $m \geq 2$，则

$$\mathrm{Aut}(\mathfrak{A}_m(G)) = \mathrm{Hol}_m(G), \tag{2}$$

其中，$\mathrm{Hol}_m(G) = G^m \rtimes \mathrm{Aut}(G)$ 是作用在 G^m 上的置换群，由 G^m 的右乘以及 $\mathrm{Aut}(G) \leq \mathrm{Sym}(G^m)$ 的逐分量作用诱导。此外，我们在第 5 节证明，对于 $m \geq 3$，群 G 由 S-环 $\mathfrak{A}_m(G)$ 唯一确定。

定理 1.1. 对于 $m \geq 3$ 以及任意两个群 G 和 G'，下列命题等价：

(1) 群 G 和 G' 同构；(2) S-环 $\mathfrak{A}_m(G)$ 与 $\mathfrak{A}_m(G')$ 组合同构；(3) 群 $\mathrm{Hol}_m(G)$ 与 $\mathrm{Hol}_m(G')$ 置换同构。

定理 1.1 中的等价关系对于 $m = 1$ 及所有阶至少为 4 的 G 并不成立。对于哪些 G，这些等价关系在 $m = 2$ 上成立，是一个值得研究的问题。

对于固定的 m，S-环 $\mathfrak{A}_m(G)$ 提供了群 G的一个易于计算的不变量，即相对于标准

[1] 在 S-环范畴中，$\mathfrak{A}_m(G)$ 所起的作用，与相干配置范畴中相干配置的 m-扩张所起的作用相同，参见 [7]。

线性基的结构常数张量。一般来说，这个张量不是一个完备不变量，因为它只能确定 S-环 $\mathfrak{A}_m(G)$ 到代数同构（而非组合同构）的意义下（确切定义见第 2 节）。然而，如果 S-环 $\mathfrak{A}_m(G)$ 对固定的 m 和所有 G 都是舒尔型的，那么这个不变量就足以高效地检验任意两个群是否同构（见下文定理 1.4）。

我们的第二个结果表明，序列 $\mathfrak{A}_1(G)$、$\mathfrak{A}_2(G)$、.....具有稳定性：当指标足够大时，这些 S-环到 G 的某个固定幂的投影都成为舒尔型。更准确地说，令 $\mathrm{Cyc}_m(G) = \mathrm{Cyc}(\mathrm{Aut}(G)\ G^m)$，并将 $\mathfrak{A}_{m+k}(G)_{G^m}$, $k \geq 0$ 记为 S-环 $\mathfrak{A}_{m+k}(G)$ 在 G^{m+k} 到前 m 个坐标的自然投影下的像（注意，该像是 G^m 上的 S-环）。

定理 1.2. 设 G 是一个群，且 m、k 是正整数。则

$$\mathfrak{A}_m(G) \leq \mathfrak{A}_{m+k}(G)_{G^m} \leq \mathrm{Cyc}_m(G). \tag{3}$$

此外，当 $k \geq \max\{2, d\}$ 时，第二个包含关系变为等式，其中 $d = d(G)$。特别地，存在一个正整数 $t \leq \max\{2, d\}$，使得

$$\mathcal{T}(G) = \overline{\mathfrak{A}}_1(G) \leq \overline{\mathfrak{A}}_2(G) \leq \cdots \leq \overline{\mathfrak{A}}_t(G) = \overline{\mathfrak{A}}_{t+1}(G) = \cdots = \mathrm{Cyc}_1(G),$$

其中，对所有 i，我们令 $\overline{\mathfrak{A}}_i(G) = \mathfrak{A}_i(G)_G$。

S-环 $\mathfrak{A}_m(G)$ 可以自然地用 G^m 的典范划分 $\mathrm{WL}_m(G)$ 来解释；该划分由针对群的 m 维 Weisfeiler-Leman 算法 WL_I 构造，见 [4]。具体而言，根据定理 6.1，$\mathrm{WL}_{3m}(G)$ 到 G^m 的投影（下文记为 $\mathrm{WL}_{3m}(G)_{G^m}$）构成 G^m 上的一个 S-环。由此，我们可以比较两个划分 $\mathrm{WL}_m(G)$ 和 $\mathcal{S}(\mathfrak{A}_m(G))$。

定理 1.3. 设 G 是一个群。那么对于任意正整数 m,

$$\mathrm{WL}_{3m}(G)_{G^m} \geq \mathcal{S}(\mathfrak{A}_m(G)) \quad and \quad \mathcal{S}(\mathfrak{A}_{m+1}(G))_{G^m} \geq \mathrm{WL}_m(G).$$

此外，存在一个整数 $s(G) \geq 3$，使得若 $m \geq s(G)$，则从 S-环 $\mathfrak{A}_m(G)$ 出发的每个代数同构都由一个同构诱导，而且

$$\dim_{\mathrm{WL}}(G) \leq 3s(G) \quad and \quad s(G) \leq \dim_{\mathrm{WL}}(G) + 1, \tag{4}$$

其中，$\dim_{\mathrm{WL}}(G)$ 是 G 的 WL 维数。

本文的主要动机之一是进一步理解群同构问题，即高效地检验给定的两个群是否同构。与图同构问题的情形一样，考虑彩色群是很自然的：假定输入群的元素带有颜色，并且同构保持颜色，见 [5]。在这一范式下，S-环 $\mathfrak{A}_m(G)$ 的定义只需作显而易见的修改。具体而言，若 X_1、.....、X_c 是 G 的着色类，则 $\mathfrak{A}_m(G)$ 的彩色版本定义为将元素 $\mathrm{Diag}(X_1^m)$.....、$\mathrm{Diag}(X_c^m) \in \mathbb{Z}G$ 加入 $\mathcal{T}_m(G)$ 所得的扩张。

以下定理（及其证明）与图的相应定理（及其证明）非常相似，参见 [14]。然而，与图的情形不同，群和着色群的同构问题是否多项式时间等价尚不明确。

定理 1.4. 着色群的同构判定与给定着色群 G 时求出 S-环 $\mathrm{Cyc}_1(G)$ 的问题是多项式时间等价的。

本文结构如下。第 2 节介绍 S-环理论所需的背景知识。第 3 节和第 4 节分别描述群的 Weisfeiler-Leman 方法，并研究 S-环 $\mathfrak{A}_m(G)$ 的基本性质。主要结果的证明见第 5–8 节。

2. Schur rings

2.1. S-环。设 G 是一个有限群。群环 $\mathbb{Z}G$ 的一个 $\mathbb{Z}$-子模 $\mathfrak{A}$ 称为 G 上的舒尔环（简称 S-环），如果存在 G 的一个划分 $\mathcal{S} = \mathcal{S}(\mathfrak{A})$，使得

(S1) $\{1_G\} \in \mathcal{S}$，(S2) 对所有 $X \in \mathcal{S}$，$X^{-1} \in \mathcal{S}$；(S3) 对所有 X、$Y \in \mathcal{S}$ 以及某些整数 c_X^Z，$\underline{X}\,\underline{Y} = \sum_{Z\in\mathcal{S}} c_{X,Y}^Z \underline{Z}_Y$。

$\mathcal{S}$ 的元素和数目 $\mathrm{rk}(\mathfrak{A}) = |\mathcal{S}|$ 分别称为 $\mathfrak{A}$的基本集和秩。包含 $x \in G$ 的基本集记作 $[x]$。非负整数 $c_{X,Y}^Z$ 等于对于固定的 $z \in Z$，满足 $x \in X$ 和$y \in Y$的表示 $z = xy$ 的数目。

基本集的任意并称为一个 $\mathfrak{A}$-集。所有这类集合关于取逆元、乘积以及标准集合论运算封闭。作为 G 的子群的 $\mathfrak{A}$-集称为 $\mathfrak{A}$-群。例如，若 X 是一个 $\mathfrak{A}$-集，那么由 X 生成的群 $\langle X\rangle$ 是一个 $\mathfrak{A}$-群。对于任意基本集 X 和$\mathfrak{A}$-群 H，我们定义

$$n(X,H) = \sum_Y c_{Y,X}^X, \tag{5}$$

其中 Y 遍历包含于 H中的基本集。不难证明，对于每个 $x \in X$，都有$n(X,H) = |X \cap Hx|$。

设 H 是 G的正规 $\mathfrak{A}$-子群，且 $\pi\colon G \to G/H$ 是自然满同态。那么集合 $\mathcal{S}_{G/H} = \{\pi(X)\colon X \in \mathcal{S}\}$ 构成 G/H的一个划分。此外，元素 $\pi(X)$张成 G/H 上的一个~~S-环;~~ 它记作 $\mathfrak{A}_{G/H}$，称为 $\mathfrak{A}$ 模 H的商。

对 G 上的 S-环而言，$\leq$ 偏序由包含关系诱导。因此，$\mathfrak{A} \leq \mathfrak{A}'$当且仅当 $\mathfrak{A}$ 的任一基本集都是 $\mathfrak{A}'$中若干基本集的并；此时我们称 $\mathfrak{A}'$ 是 $\mathfrak{A}$的扩张。关于 $\leq$，最小元和最大元分别是由 $\underline{1_G}$ 和 $\underline{G}$张成的平凡 S-环 $\mathcal{T}(G)$，以及群环 $\mathbb{Z}G$。对于任意 $X \subseteq G$，$\mathfrak{A}$ 经 $\underline{X}$ 扩张得到的扩张$\mathfrak{A}[\underline{X}]$ 是 G上的最小 S-环，且包含 $\mathfrak{A}$ 和 $\underline{X}$。

2.2. 同构。对于任意 $X \in \mathcal{S}$，可以定义一个凯莱图 $\mathrm{Cay}(G,X)$，其顶点集为 G，使得顶点 x 和 y 相邻，当且仅当 $xy^{-1} \in X$。该图的自同构群包含对称群 $\mathrm{Sym}(G)$ 的一个正则子群，该子群由 G的右乘诱导。

设 $\mathfrak{A}$ 是 G 上的一个 S-环，$\mathfrak{A}'$ 是 G' 上的一个 S-环。若对于每个 $X \in \mathcal{S}(\mathfrak{A})$，都存在$X' \in \mathcal{S}(\mathfrak{A}')$，使得.....，则称双射 $f\colon G \to G'$ 是从 $\mathfrak{A}$ 到 $\mathfrak{A}'$ 的（组合）同构

$$f \in \mathrm{Iso}(\mathrm{Cay}(G,X), \mathrm{Cay}(G',X')),$$

或者，等价地，对于所有 $y \in G$，$(Xy)^f = X'f(y)$。特别地，从 $\mathfrak{A}$ 到 $\mathfrak{A}'$ 的所有同构组成的集合 $\mathrm{Iso}(\mathfrak{A},\mathfrak{A}')$包含所有群同构 $f\colon G \to G'$，其中 $\mathcal{S}(\mathfrak{A})^f = \mathcal{S}(\mathfrak{A}')$。任何这样的 f都是规范化同构，即 $f(1_G) = 1_{G'}$。

注意，S-环 $\mathfrak{A}$ 与 $\mathfrak{A}'$ 同构，当且仅当存在从 $\mathfrak{A}$ 到 $\mathfrak{A}'$的规范化同构。

所有从 $\mathfrak{A}$ 到其自身的同构构成的群 $\mathrm{Iso}(\mathfrak{A}) = \mathrm{Iso}(\mathfrak{A},\mathfrak{A})$ 有一个正规子群，它等于群 $\mathrm{Aut}(\mathrm{Cay}(G,X))$、 $X \in \mathcal{S}$ 的交。该群称为 $\mathfrak{A}$ 的自同构群，记作 $\mathrm{Aut}(\mathfrak{A})$。特别地，

$$\mathrm{Aut}(\mathfrak{A}) \le \mathrm{Aut}(\mathrm{Cay}(G,X)) \tag{6}$$

对每个 X 均成立。因此，当且仅当对于所有 $X \in \mathcal{S}$ 和所有 $y \in G$，$(Xy)^f = Xy^f$， f 才是 $\mathfrak{A}$ 的自同构。注意， $f \in \mathrm{Aut}(G)$ 属于 $\mathrm{Aut}(\mathfrak{A})$，当且仅当 f 保持 $\mathfrak{A}$ 的每个基本集不变。

引理 2.1. 设 $\mathfrak{A}$ 和 $\mathfrak{A}'$ 分别是定义在 G 和 G' 上的 S-环，且令 $X \subseteq G$ 和 $X' \subseteq G'$。假设 $f \in \mathrm{Iso}(\mathfrak{A},\mathfrak{A}')$ 是一个规范化同构，使得

$$f(Xy) = X'f(y)$$

对所有 $y \in G$ 均成立。则 $f \in \mathrm{Iso}(\mathfrak{A}[\underline{X}],\mathfrak{A}'[\underline{X'}])$。特别地，若 $G = G'$、 $\mathfrak{A} = \mathfrak{A}'$ 且 $X = X'$，则 $f \in \mathrm{Aut}(\mathfrak{A}[\underline{X}])$。

证明。由 [9, 引理 2.3]可得。 □

设 $m \ge 1$ 为一个整数， $A \le \mathrm{Aut}(G)$，且 $\mathcal{S}$ 为 G^m 按 A的逐分量作用所得轨道构成的划分。那么，由公式 (1) 定义的模 $\mathfrak{A}$ 是 G^m上的一个 S-环。记作 $\mathrm{Cyc}_m(A, G)$。这是一个与 $\mathrm{Sym}(G)$ 的子群相关联的 S-环的特例，该子群包含由 G的右乘所诱导的置换。

2.3. 代数同构。在上一小节的记号下，环同构 $\varphi : \mathfrak{A} \to \mathfrak{A}'$ 称为代数同构，如果对任意 $X \in \mathcal{S}$，都存在 $X' \in \mathcal{S}'$ 使得 $\varphi(\underline{X}) = \underline{X'}$。由定义可知，映射 $X \mapsto X'$ 是从 $\mathcal{S}$ 到 $\mathcal{S}'$的双射。这个双射自然延拓为 $\mathfrak{A}$-集与 $\mathfrak{A}'$-集之间的双射，并将 $\mathfrak{A}$-群映到 $\mathfrak{A}'$-群；一个 $\mathfrak{A}$-集 X 在 $\varphi(X)$下的像 X' 也是如此。等式

$$c^Z_{X,Y} = c^{Z'}_{X',Y'} \quad \text{and} \quad n(X,H) = n(X',H')$$

对所有基本集 X, Y, Z 和所有 $\mathfrak{A}$-群 H 均成立。若 H 是 G 的正规 $\mathfrak{A}$-子群， $\pi : G \to G/H$ 为自然满同态，且 H' 是 $G' = \varphi(G)$ 的正规子群，则映射 $\pi(X) \mapsto \pi'(X')$， $X \in \mathcal{S}$ 诱导一个代数同构 $\varphi_{G/H} : \mathfrak{A}_{G/H} \to \mathfrak{A}'_{G'/H'}$，使得

$$\varphi_{G/H}(\pi(X)) = \pi'(\varphi(X)), \tag{7}$$

其中 $\pi' : G' \to G'/H'$ 是自然满同态。

引理 2.2. 设 $\varphi : \mathfrak{A} \to \mathfrak{A}'$ 是一个代数同构。则对于任意 S-环 $\tilde{\mathfrak{A}} \ge \mathfrak{A}$ 和 $\tilde{\mathfrak{A}}' \ge \mathfrak{A}'$，从 $\mathfrak{A}$ 到 $\mathfrak{A}'$ 至多存在一个延拓 φ 的代数同构。

证明. 由 [9, 引理 2.1] 得出。 □

每个规范化同构 $f : \mathfrak{A} \to \mathfrak{A}'$ 都定义了一个双射 $\varphi : \mathcal{S} \to \mathcal{S}', X \mapsto X^f$，它是一个代数同构；我们称 φ由 f诱导。例如，平凡的代数同构 $\varphi = \mathrm{id}$ 由 $\mathfrak{A}$的每个规范化自同构诱导。然而，并非每个代数同构都由一个同构诱导。

2.4. 张量积。设 $\mathfrak{A}$ 和 $\mathfrak{A}'$ 分别是群 G 和 G'上的 S-环。那么，笛卡尔积 $X \times X'$ 与 $X \in \mathcal{S}$ 和 $X' \in \mathcal{S}'$构成直积 $G \times G'$的一个划分$\mathcal{S} \times \mathcal{S}'$。此外，存在唯一确定的 S-环 $\mathfrak{A} \otimes \mathfrak{A}'$，它定义在 $G \times G'$ 上，使得

$$\mathcal{S}(\mathfrak{A} \otimes \mathfrak{A}') = \mathcal{S} \times \mathcal{S}'.$$

这称为 $\mathfrak{A}$ 和 $\mathfrak{A}'$的张量积。以下引理由 [8, 引理 2.2]证明。

引理 2.3. 设 G 和 G' 为群，且 $\pi\colon G \times G' \to G$ 和 $\pi'\colon G \times G' \to G'$为自然投影。设 $\mathfrak{A}$ 是定义在 $G \times G'$ 上的 S-环，使得 G 和 G' 是 $\mathfrak{A}$-群。那么对所有 $X \in \mathcal{S}(\mathfrak{A})$，有 $\pi(X)$ $\pi'(X) \in \mathcal{S}(\mathfrak{A})$。特别地，$\mathfrak{A} \geq \mathfrak{A}_G \otimes \mathfrak{A}_{G'}$。

m 个平凡 S-环 $\mathcal{T}_G$ 的张量积记作 $\mathcal{T}_m(G)$。该 S-环的基本集 X 与集合 $I \subseteq \{1, \ldots, m\}$一一对应；也就是说，当且仅当 $i \in I$}时，$X = \{x \in G^m\colon\ x_i = 1_G$。

3. The Weisfeiler-Leman method for groups

群的 Weisfeiler-Leman（WL）方法的关键在于多维 WL 算法。就本文而言，不必详细描述该算法，只需了解 [1]，中介绍的所得多维相干构形的结构，另见 [13]。

3.1. 多维相干构形。设 Ω 为有限集，m 为正整数。先固定一些记号。对于元组 $x \in \Omega^m$，记 $\rho(x)$ 为 $M = \{1, \ldots, m\}$ 上的等价关系，使得 $(i, j) \in \rho(x)$ 当且仅当 $x_i = x_j$。包含 x 的划分 $\mathfrak{X}$ 的类记为 $[x]$。对于映射$\sigma\colon M \to M$，令 $x^\sigma = (x_{1^\sigma}, \ldots, x_{m^\sigma})$。

定义 3.1. Ω 上的划分 $\mathfrak{X}$ 称为 Ω 上的 m 元彩虹，如果对所有 $X \in \mathfrak{X}$ 都满足以下条件：

(C1) $\rho(x)$ 不依赖于 $x \in X$，(C2) 对所有映射 $\sigma\colon M \to M$，$X^\sigma \in \mathfrak{X}$。

Ω 上的 m 元彩虹（就语言而言）是 [13] 中的 m 元构形：区别在于，我们不使用 Ω^m 的着色来定义这些类。条件 (C2) 意味着 Sym(m) 在 Ω^m 上的逐坐标作用在 $\mathfrak{X}$ 上诱导出一个作用；特别地，

$$[x]^\sigma \in \mathfrak{X} \quad \text{for all } x \in \Omega^m,\ \sigma \in \mathrm{Sym}(m).$$

2 元彩虹是 [6]，意义下的普通彩虹，但反过来的说法不一定成立。

设 $\mathfrak{X}'$ 是 Ω′ 上的 m 元彩虹。双射 $f\colon \Omega \to \Omega'$ 称为从 $\mathfrak{X}$ 到 $\mathfrak{X}'$ 的同构，如果其诱导的双射

$$f_m : \Omega^m \to \Omega'^m,\ (x_1, \ldots, x_m) \mapsto (x_1^f, \ldots, x_m^f),$$

将 $\mathfrak{X}$ 的类映射到 $\mathfrak{X}'$的类。显然，对于所有 $x \in \Omega^m$，$\rho(x) = \rho(x^{f_m})$，且对于所有映射 $\sigma\colon M \to M$，$X^{f_m\sigma} = X^{\sigma f_m}$。

Ω 上的 m 元彩虹按划分的偏序关系构成偏序。也就是说，$\mathfrak{X} \leq \mathfrak{Y}$ 如果 $\mathfrak{X}$ 的每个类都是 $\mathfrak{Y}$ 的若干个类的并，或者等价地，如果 $\mathfrak{X}^\cup \subseteq \mathfrak{Y}^\cup$，其中 $\mathfrak{X}^\cup$（分别为 $\mathfrak{Y}^\cup$）是所有.....的集合

..... $\mathfrak{X}$ （分别为 $\mathfrak{Y}$）的类的并。最大的 m 元彩虹是离散彩虹，其中每个类都是单元素集；最小的 m 元彩虹由对称群 Sym(Ω) 在 Ω^m 上的逐分量作用的轨道构成。给定同一集合上的 m 元彩虹 $\mathfrak{X}$ 和 $\mathfrak{Y}$，存在唯一的 m 元彩虹 $\mathfrak{X}\cap\mathfrak{Y}$，使得 $(\mathfrak{X}\cap\mathfrak{Y})^\cup = \mathfrak{X}^\cup\cap\mathfrak{Y}^\cup$；它称为 $\mathfrak{X}$ 与 $\mathfrak{Y}$ 的交。

设 $\mathfrak{X}$ 是 Ω 上的一个 m 元彩虹。对于任意 $x\in\Omega^m$ 以及任意 $X_1,\dots,X_m\in\mathfrak{X}$，用 $n(x;X_1,\dots,X_m)$ 表示所有满足对任意 $i\in M$ 均有 $x_{i\leftarrow\alpha}\in X_i$ 的 $\alpha\in\Omega$ 的个数，其中

$$x_{i\leftarrow\alpha} = (x_1,\dots,x_{i-1},\alpha,x_{i+1},\dots,x_m). \tag{8}$$

这些数定义了 Ω^m 上的一个等价关系 $\sim$，使得当且仅当对于任意 $X_1,\dots,X_m\in\mathfrak{X}$，$x\sim y$

$$[x]=[y] \quad\text{and}\quad n(x;X_1,\dots,X_m)=n(y;X_1,\dots,X_m).$$

$\sim$ 的类构成 Ω^m 的一个划分，称为 $\mathfrak{X}$ 的 WL细化，记作 $\mathrm{WL}_{m,1}(\mathfrak{X})$。不难验证，WL细化将 $\mathfrak{X}$ 转化为满足 (C1) 的划分。

对于给定的 $\mathfrak{X}$，m 维魏斯费勒-莱曼算法 WL_m 逐步构造以下划分：

$$\mathfrak{X}=\mathfrak{X}_0<\mathfrak{X}_1<\ldots<\mathfrak{X}_k=\mathfrak{X}_{k+1}=\mathrm{WL}_m(\mathfrak{X}) \tag{9}$$

对于某个 $k\le|\Omega|^m$，其中 $\mathfrak{X}_{i+1}=\mathrm{WL}_{m,1}(\mathfrak{X}_i)$，适用于 $i=0,1,\dots,k$。由此得到的划分 $\mathrm{WL}_m(\mathfrak{X})$ 是 Ω 上在下文定义意义下大于或等于 $\mathfrak{X}$ 的最小 m 元相干配置。注意，映射 $\mathfrak{X}\mapsto\mathrm{WL}_m(\mathfrak{X})$ 易于计算，并在 m 元彩虹上定义了一个闭包算子。特别地，它是单调的，即 $\mathfrak{X}\le\mathfrak{X}'$ 蕴含 $\mathrm{WL}_m(\mathfrak{X})\le\mathrm{WL}_m(\mathfrak{X}')$.

定义 3.2. 若一个 m 元相干配置是满足以下附加条件的 m 元彩虹 $\mathfrak{X}$

(C3) *for any $X_0,X_1,\dots,X_m\in\mathfrak{X}$, the number $n^{X_0}_{X_1,\dots,X_m}=n(x_0;X_1,\dots,X_m)$ does not depend on $x_0\in X_0$.*

Ω 上的一元相干配置就是 Ω 的划分，而二元相干配置则是通常的相干配置，参见例如 [6]。一个 m 元相干配置的自然例子是置换群在 Ω 上的自然作用于 Ω^m 所得的轨道集合。

根据 [15, 公式 (9)], , m元相干构形 $\mathfrak{X}$ 与 $\mathfrak{X}'$ 之间的代数同构是一个双射 $\varphi:\mathfrak{X}\to\mathfrak{X}'$，满足对所有 X、X_0、.....、$X_m\in\mathfrak{X}$以及 $\sigma:M\to M$，

$$\varphi(X^\sigma)=\varphi(X)^\sigma \quad\text{and}\quad n^{X_0}_{X_1,\dots,X_m}=n^{\varphi(X_0)}_{\varphi(X_1),\dots,\varphi(X_m)}. \tag{10}$$

每个从 $\mathfrak{X}$ 到 $\mathfrak{X}'$ 的同构 f 都会诱导一个代数同构 $\varphi:\mathfrak{X}\to\mathfrak{X}'$，使得对所有 X都有 $X^\varphi=X^{f_m}$。此外，若 $X\in\mathfrak{X}$ 且 i、$j\in M$，则$(i,j)\in\rho(X)$当且仅当 $X^\sigma=X$，其中 $\sigma:M\to M$在 $M\setminus\{j\}$上恒等，并将 j 映到 i。由此可得

$$\rho(\varphi(X))=\rho(X). \tag{11}$$

我们以自然的方式将 φ 扩展为一个双射 $\mathfrak{X}^\cup\to(\mathfrak{X}')^\cup$。于是 $X\subseteq Y$ 推出，对于所有 $X,Y\in\mathfrak{X}^\cup$，都有$\varphi(X)\subseteq\varphi(Y)$。

引理 3.3. 设 φ是从一个 m元相干配置 $\mathfrak{X}$ 到另一个 m元相干配置的代数同构。那么对每个彩虹 $\mathfrak{Y} \le \mathfrak{X}$,

$$\varphi(\mathrm{WL}_m(\mathfrak{Y})) = \mathrm{WL}_m(\varphi(\mathfrak{Y})).$$

证明。对公式 (9) 中的 $i = 0, \dots, k$ 关于 $\mathfrak{X} = \mathfrak{Y}$ 使用归纳法，只需证明 $\varphi(\mathrm{WL}_{m,1}(\mathfrak{Y}_i)) = \mathrm{WL}_{m,1}(\varphi(\mathfrak{Y}_i))$。换言之，我们需要验证：若 $Y \in \mathfrak{Y}_i$ 且 $Y' \in \mathrm{WL}_{m,1}(\mathfrak{Y}_i)$，则

$$Y' \subseteq Y \quad \Rightarrow \quad \varphi(Y') \subseteq \varphi(Y).$$

但这可直接由公式 (10) 得出：将公式应用于 $\mathfrak{X}$ 的类，这些类包含在 Y' 的类中。□

3.2. 投影。设 $K = \{i_1, \dots, i_k\}$，其中 $1 \le i_1 < i_2 < \ldots < i_k \le m$。$\Omega^m$ 关于集合 $K \subseteq M$ 的投影是如下映射

$$\mathrm{pr}_K : \Omega^m \to \Omega^k,\ (\alpha_1, \dots, \alpha_m) \mapsto (\alpha_{i_1}, \dots, \alpha_{i_k}).$$

当 $K = \{1, \dots, a\}$ 时，我们将 $\mathrm{pr}_a := \mathrm{pr}_K$ 简写为。

引理 3.4。设 $\mathfrak{X}$ 是 Ω 上的一个 m 元相干配置（分别地，彩虹），且 $K \subseteq M$。那么 $\mathrm{pr}_K(\mathfrak{X}) = \{\mathrm{pr}_K(X) : \ X \in \mathfrak{X}\}$ 是 Ω 上的一个 $|K|$ 元相干配置（分别地，彩虹）。特别地，

$$\mathrm{pr}_K^{-1}(\mathrm{pr}_K(X)) \in \mathfrak{X}^\cup \quad \textit{for all } X \in \mathfrak{X}^\cup. \tag{12}$$

此外，每个代数同构 $\varphi\colon \mathfrak{X} \to \mathfrak{X}'$ 都诱导出一个代数同构 $\varphi_K : \mathrm{pr}_K(\mathfrak{X}) \to \mathrm{pr}_K(\mathfrak{X}')$，使得

$$\varphi_K(\mathrm{pr}_K(X)) = \mathrm{pr}_K(\varphi(X)) \quad \textit{for all } X \in \mathfrak{X}^\cup. \tag{13}$$

证明。第一个结论已在 [13, 练习 2.7、2.11] 中证明（另见 [15,引理 3.3]）；第二个结论显然，第三个结论见 [15, 引理 3.3]。□

设 $\mathfrak{X}$ 是 Ω 上的一个 m 元彩虹。对于每个 $X \in \mathfrak{X}$、$K \subseteq M$ 和 $x \in X$，用 $n_K(x; X)$ 表示所有满足 $\mathrm{pr}_K(y) = \mathrm{pr}_K(x)$ 的 $y \in X$ 的个数。当 $\mathfrak{X}$ 是一个 2 元相干配置时，这个数就是 X 的价，且不依赖于 $x \in X$。下面的结论将这一性质推广到任意 m （对于某些特殊的 m 元相干配置，这已在 [7, 定理 6.1] 中证明）。

引理 3.5。设 $\mathfrak{X}$ 是一个 m 元相干配置，$X \in \mathfrak{X}$，且 $K \subseteq M$。那么数目 $n_K(X) = n_K(x; X)$ 不依赖于 $x \in X$。

证明。设 $x \in X$ 和 $A = \{y \in X : \mathrm{pr}_K(y) = \mathrm{pr}_K(x)\}$。首先，假设 $K = \{1, \dots, m-1\}$。当类 X_1、…、X_{m-1} 遍历 $\mathfrak{X}$时，非空集合

$$A(X_1, \dots, X_{m-1}) = \{y \in A : \ x_{1 \leftarrow y_m} \in X_1, \dots, x_{m-1 \leftarrow y_m} \in X_{m-1}\}$$

构成 A的一个划分。此外，$|A(X_1, \dots, X_{m-1})| = n^X_{X_1,\dots,X_{m-1},X}$。因此，数目

$$n_K(x; X) = |A| = \sum_{X_1,\dots,X_{m-1}} |A(X_1, \dots, X_{m-1})| = \sum_{X_1,\dots,X_{m-1}} n^X_{X_1,\dots,X_{m-1},X}$$

不依赖于 $x \in X$。

现在，不失一般性，我们可以假设 $K = \{1, \dots, k\}$ for some$1 \le k < m-1$。令 $K' = \{1, \dots, m-1\}$。由引理 3.4，$\mathfrak{X}' = \mathrm{pr}_{K'}(\mathfrak{X})$ 是

一个 $(m-1)$ 元相干配置。令 $A' = \mathrm{pr}_{K'}(A)$、$X' = \mathrm{pr}_{K'}(X)$ 和$x' = \mathrm{pr}_{K'}(x)$。由归纳法，我们有

$$n_K(X') = n_K(x'; X') = |A'|.$$

注意，如果 $y \in A$，那么 $y' \in A'$。此外，根据第一段中证明的结论，恰有 $n_{K'}(y) = n_{K'}(X)$ 个元素 $z \in X$，使得 $\mathrm{pr}_{K'}(z) = y'$。因此，数量

$$|A| = n_K(x; X) = |A'|\, n_{K'}(x) = n_K(X')\, n_{K'}(X)$$

不依赖于 $x \in X$。 □

若一个 m 元彩虹 $\mathfrak{X}$ 对每个 $X \in \mathfrak{X}$ 和所有 $K \subseteq M$ 都满足引理 3.5 的结论，则称其为正则的。因此，引理 3.5 指出，每个 m 元相干配置都是正则的。即使对于 $m = 2$，逆命题也不成立。

推论 3.6. 设 φ 是一个从 m 元相干配置 $\mathfrak{X}$ 出发的代数同构，则对所有 $X \in \mathfrak{X}^{\cup}$，$|X| = |\varphi(X)|$。

3.3. 直积幂的魏斯费勒-莱曼划分。设 G 是一个群，且 $m \geq 1$。记 $\mathfrak{X} = \mathfrak{X}_m(G)$为 G 上的最小 m元彩虹，使得对每个 $X \in \mathfrak{X}$ 和每个 x，$y \in X$，等价关系

$$x_i = x_j \;\Leftrightarrow\; y_i = y_j \quad \text{and} \quad x_i x_j = x_k \;\Leftrightarrow\; y_i y_j = y_k \tag{14}$$

对所有 i、j、$k \in M$均成立。第一部分恰好意味着等价关系 $\rho(x)$不依赖于 $x \in X$，而第二部分则意味着三元关系也满足同样的性质

$$\mu(x) = \{(i, j, k) \in M^3 :\ x_i x_j = x_k\}.$$

由公式 (14) 定义的 G^m 划分，在 [4] 中被用作群 G^m 的初始着色，用于版本 I 中面向群的 WL 算法。

引理 3.7. 设 G 是一个群，且 $\mathfrak{X} = \mathfrak{X}_m(G)$。那么

(1) $\{1_{G^m}\} \in \mathfrak{X}$ 和 $\mathrm{Diag}(G^m) \in \mathfrak{X}^{\cup}$，

(2) $\mathfrak{X}^{-1} = \mathfrak{X}$，(3) $\mathfrak{X} \geq \mathcal{S}(\mathcal{T}_m(G))$.

证明。命题 (1) 由 (14) 立即得出。接下来，对于每个 $x \in G^m$，都有 $\rho(x) = \rho(x^{-1})$，且 $(i, j, k) \in \mu(x)$ 当且仅当 $(j, i, k) \in \mu(x^{-1})$。这证明了命题 (2)。最后，由第 2 节末尾的说明可知，命题 (3) 成立。□

对于群 G，包含 $\mathfrak{X}_m(G)$ 的最小 m 元相干配置记作 $\mathrm{WL}_m(G)$，

$$\mathrm{WL}_m(G) = \mathrm{WL}_m(\mathfrak{X}_m(G)).$$

它与算法 WL_m^I 应用于 G for$m \geq 2$ 所得到的划分一致，见 [4]。注意，$\mathrm{WL}_1(G)$ 是一个至多包含两个类的划分。

设 $\mathfrak{X} \geq \mathrm{WL}_m(G)$ 和 $\mathfrak{X}' \geq \mathrm{WL}_m(G')$ 是 m 元相干配置。若代数同构 $\varphi\colon \mathfrak{X} \to \mathfrak{X}'$ 满足对所有 $X \in \mathfrak{X}$，则称其为真正的。

$$\mu(X) = \mu(\varphi(X)). \tag{15}$$

若存在真正的代数同构 $\varphi\colon \mathrm{WL}_m(G) \to \mathrm{WL}_m(G')$，则称群 G 和 G' 是 WL_m-等价的。这个概念对应于版本 I 中关于 m-WL 的 G 和 G' 的等价关系，该概念由 [4] 引入，适用于

$m \geq 2$。显然，任意两个同构群对于所有 m 都是 WL$_m$-等价的。群 G 的 WL 维数 $\dim_{\mathrm{WL}}(G)$ 定义为使得每个与 G WL$_m$-等价的群都与 G同构的最小 m。更多详情请参阅 [4]。

4. The S-ring $\mathfrak{A}_m(G)$

在本文余下部分中，G 是一个有限群，m 是一个正整数，$M = \{1, \dots, m\}$、$\mathfrak{X}_m = \mathfrak{X}_m(G)$、$\mathcal{T}_m = \mathcal{T}_m(G)$、$D_m = \mathrm{Diag}(G^m)$、$\mathfrak{A}_m = \mathfrak{A}_m(G)$以及$\mathcal{S}_m = \mathcal{S}(\mathfrak{A}_m)$。

4.1. 基本性质。回顾一下，S-环 $\mathfrak{A}_m$ 是由元素$\underline{D_m}$对 m次张量幂 $\mathcal{T}_m$ 进行扩张得到的。每个 $\sigma \in \mathrm{Sym}(M)$都通过置换坐标诱导出S-环 $\mathcal{T}_m$的一个规范化同构。此外，对于所有 $x \in G^m$，$(D_m x)^\sigma = D_m x^\sigma$。由引理 2.1，这意味着 σ 诱导出 $\mathfrak{A}_m$ 到其自身的一个同构。特别地，我们有以下结论。

引理 4.1. 对所有 $X \in \mathcal{S}_m$ 以及 $\sigma \in \mathrm{Sym}(M)$，$X^\sigma \in \mathcal{S}_m$。

设 $K \subseteq M$和 $K' = M \setminus K$。令

$$G_K = \{x \in G^m : \mathrm{pr}_{K'}(x) = 1_{G^{K'}}\},$$

并将 $G_i = G_{\{i\}}$ 和 $G_{i'} = G_{M\setminus\{i\}}$ 简记为 $i \in M$。容易看出，G_K是一个 $\mathcal{T}_m$-群，因此也是一个 $\mathfrak{A}_m$-群（因为 $\mathfrak{A}_m \geq \mathcal{T}_m$）。于是，$G^m$ 是 $\mathfrak{A}_m$-群 G_K 和 $G_{K'}$ 的直积。在 $\mathfrak{A}_m$模 $G_{K'}$的分解下，对角群 D_m 映到 D_k，其中 $k = |K|$。由引理 2.3，完整原像

$$D_K = D_K(G) = \{x \in G^m : K^2 \subseteq \rho(x)\}$$

群 D_k 是一个 $\mathfrak{A}_m$-群。注意，对于 $K = M$，有 $D_m = D_K$。因此，我们证明了下面的引理。

引理 4.2. 对所有 $K \subseteq M$，G_K 和 D_K 都是 $\mathfrak{A}_m$-群。

为了比较划分 $\mathcal{S}_m$ 和 WL$_m(G)$，我们定义集合

$$X_{i,j,k}(G) = \{x \in G^m : (i,j,k) \in \mu(x)\}, \qquad i,j,k \in M.$$

推论 4.3. 若 $m \geq 3$和 $i,j,k \in M$，则 $X_{i,j,k}(G)$ 是一个 $\mathfrak{A}_m$-集。

证明. 如果 $i \neq j \neq k \neq i$，那么 $X_{i,j,k}(G) = (D_{\{i,k\}} \cap G_{j'}) \cdot (D_{\{j,k\}} \cap G_{i'})$，由引理 4.2即可得证。在剩余情形下 $X_{i,j,l} = (X_{i',j',k'})^\sigma$，对于适当选取的两两不同的 i'、j'、$k' \in M$以及一个映射 $\sigma\colon M \to M$，它分别将 i、j、k映到 i'、j'、k'。□

设 $k \in M$和 $K = \{1, \dots, k\}$。群 G_K可自然地与直积幂 G^k等同，而 S-环 $\mathfrak{A}_m$ 模 $G_{K'}$ 所得的商可自然地与引言中定义的 S-环 $\mathfrak{A} = (\mathfrak{A}_m)_{G^k}$ 等同。取此商后，$\mathcal{T}_m$ 和 D_m 分别映到 $\mathcal{T}_k$ 和 D_k。由此可知，$\mathfrak{A} \geq \mathcal{T}_k$和 D_k 是一个 $\mathfrak{A}$-集。因此，$\mathfrak{A}$ 包含 $\mathcal{T}_k$ 通过 D_k的扩张，而这正是 $\mathfrak{A}_k$。于是，

$$\mathfrak{A}_m(G)_{G^k} \geq \mathfrak{A}_k(G). \tag{16}$$

以下结论使我们能够用第 3 节中的术语来解释划分 $\mathcal{S}_m$。

引理 4.4. 对于每个 $m \geq 1$，划分 $\mathcal{S}_m$ 是一个正则的 m 元彩虹。

证明。设 $X \in \mathcal{S}_m$。设 i、$j \in M$ 和 $x \in X$ 使得 $(i,j) \in \rho(x)$。于是$x \in X \cap D_{\{i,j\}}$。由引理 4.2 可知，这意味着 $X \subseteq D_{\{i,j\}}$。因此，对于所有 $x \in X$，都有 $(i,j) \in \rho(x)$。这就证明了条件 (C1)。

为验证条件 (C2)，设 $\sigma\colon\ M \to M$ 是任意映射。它可以写成 M 的一个置换与若干映射 $\sigma_{i,\ j}\colon\ M \to M$ 的复合，其中 i、$j \in M$，且对于 $k \neq j$，有 $j^{\sigma_{i,\ j}} = i$ 和 $k^{\sigma_{i,\ j}} = k$。由引理 4.1，只需证明对于所有 i、j，都有 $X^{\sigma_{i,\ j}} \in \mathcal{S}_m$。但这可由显然的等式推出

$$X^{\sigma_{i,j}} = XG_i \cap D_{\{i,j\}}.$$

因此，$\mathcal{S}_m$ 是一个 m元彩虹。还需验证，对于每个 $K \subseteq M$，数目 $n_K(x, X)$不依赖于 $x \in X$。然而，这一点成立，因为$n_K(x, X) = |X \cap G_{K'}x| = n(X, G_{K'})$，见公式 (5)。□

尚不清楚对于所有 m，$\mathcal{S}_m$ 是否总是一个 m元相干配置。对于 $m = 1$，这显然成立；而对于 $m > 1$，我们没有反例。

回顾一下，$\mathfrak{X}_m$ 是Ω上的最小 m元彩虹，且对于每个 $X \in \mathfrak{X}_m$，三元关系 $\mu(x)$ 不依赖于 $x \in X$。另一方面，根据引理 4.4，$\mathcal{S}_m$ 是Ω上的一个 m元彩虹，并且根据推论 4.3，它满足这一性质。因此，以下结论成立。

推论 4.5. 对所有 $m \geq 3$，$\mathcal{S}_m \geq \mathfrak{X}_m$。

对于 $m = 2$，推论 4.5 的结论不成立。事实上，令 $G_1 = G\times 1_G$、$G_2 = 1_G \times G$ 和 $G_3 = \mathrm{Diag}(G \times G)$。那么

$$\underline{G_i} \cdot \underline{G_j} = \underline{G \times G}, \qquad 1 \leq i \neq j \leq 3.$$

由此可知，若 $G_0 = \{1_{G^2}\}$ 且 X 是 $G_1 \cup G_2 \cup G_3$ 的补集，则元素 $\underline{G_0}$、……、$\underline{G_3}$ 和 $\underline{X}$ 张成一个秩为 5 的 S-环 $\mathfrak{A}$，其定义在 G^2 上。容易看出 $\mathcal{S}_2 = \mathcal{S}(\mathfrak{A})$，因而 $|\mathcal{S}_2| = 5$。另一方面，若 G 是一个循环 2-群，且 x 是 G 的唯一对合，则 $\{(1_G, x)\} \in \mathfrak{X}_2$。因此，若$|G| \geq 8$，则 $|\mathfrak{X}_2| > 5$。于是，$\mathcal{S}_2 \not\geq \mathfrak{X}_2$。

4.2. $\mathcal{S}_m$ 的类。令 w 为一个 m-字，即由 $2m$ 个字母 $a_1^{\pm 1}$、……、$a_m^{\pm 1}$ 组成的字。可以定义一个字映射 $G^m \to G$，它将一个 m-元组 x 映射到求值 $w(x) \in G$，其中对所有 $i \in M$，以 $x_i^{\pm 1}$ 替换 $a_i^{\pm 1}$（若 w 是空字，则对所有 x，$w(x) = 1_G$）。例如，若 $m = 2$ 且 $w = a_1a_2$，则上述映射定义了群 G 的乘法表。

定理 4.6. 设 $0 \leq k \leq m - 2$ 和 $k + 1 \leq \ell \leq m$. 那么对于每个 k-字 w和每个 $X \in \mathcal{S}_m$，等式 $x_\ell = w(x_1, \ldots, x_k)$ 对所有或不对任何 $x \in X$成立。

证明. 对字 w的长度 $|w|$ 作归纳法。设 $X \in \mathcal{S}_m$。若 $|w| = 0$，则 w为空，而等式 $x_\ell = w(x_1, \ldots, x_k)$ 对某个 $x \in X$ 成立，恰好意味着$x_\ell = 1_G$，或者等价地，$x \in G_{\ell'}$。由于 $G_{\ell'}$ 是一个 $\mathfrak{A}_m$-群，这表明$X \subseteq G_{\ell'}$，即 $x_\ell = w(x_1, \ldots, x_k)$ 对所有 $x \in X$成立。

设 $|w| \geq 1$。那么，对于某个 k-字 w' 和 $1 \leq i \leq k$，有 $w = w'a_i$ 或 $w'a_i^{-1}$。我们考虑第一种情况；第二种情况类似。不妨设 $\ell = m - 1$（引理 4.1），并且对于某个 $x \in X$，有 $x_\ell = w$（x_1，……，x_k）。令 $X' = [x']$，其中

$$x' = (x_1, \ldots, x_k, \ldots, x_{m-2}, w'(x_1, \ldots, x_k), w(x_1, \ldots, x_k)). \tag{17}$$

由于 $|w'| = |w| - 1$，归纳假设推出，对于所有 $y \in X'$，均有 $y_{m-1} = w'$（y_1，……，y_k）。此外，

$$x'_{m-1}x'_i = w'(x_1, \ldots, x_k)x'_i = w(x_1, \ldots, x_k) = x'_m.$$

由推论 4.3，我们有 $X' \subseteq X_{m-1,\ i,\ m}(G)$。因此，若 $\sigma = (m-1, m) \in \mathrm{Sym}(M)$，则集合 $Y = (X')^\sigma G_m$ 中的每个元素都具有如下形式

$$y = (y_1, \ldots, y_{m-2}, w(y_1, \ldots, y_k), y_m).$$

另一方面，根据引理 4.2，Y 是一个 $\mathfrak{A}_m$-集，并且 $x \in Y$。因此，$X \subseteq Y$，且对于所有 $x \in X$，等式 $x_{m-1} = w(x_1, \ldots, x_k)$ 都成立。□

推论 4.7。设 $m \geq 3$ 和 $0 \leq k \leq m-2$。假设 $x \in X \in \mathcal{S}_m$ 满足

$$\langle x_1, \ldots, x_m \rangle = \langle x_1, \ldots, x_k \rangle. \tag{18}$$

那么，对于给定的 $y \in X$，映射 $x_i \mapsto y_i$，$i = 1, \ldots m$ 诱导出一个从 $\langle x_1, \ldots, x_m \rangle$ 到 $\langle y_1, \ldots, y_m \rangle$ 的同构。

证明。由定理 4.6，只需验证映射 $x_i \mapsto y_i$，$i = 1, \ldots k$ 诱导出一个从 $\langle x_1, \ldots, x_k \rangle$ 到 $\langle y_1, \ldots, y_k \rangle$ 的同构。然而，当

$$w(x_1, \ldots, x_k) = w'(x_1, \ldots, x_k) \quad \Leftrightarrow \quad w(y_1, \ldots, y_k) = w'(y_1, \ldots, , y_k) \tag{19}$$

对于所有 k-词 w 和 w' 时，这成立。为验证这一等价关系，只需证明蕴含关系 $\Rightarrow$，因为由定理 4.6 可知，对所有 $y \in X$，等式 (18) 均成立。令 $X' = [x']$，其中

$$x' = (x_1, \ldots, x_{m-2}, w(x_1, \ldots, x_k), w'(x_1, \ldots, x_k)).$$

(19) 的左端意味着 $(m-1, m) \in \rho(X')$。另一方面，$\mathrm{pr}_{m-2}(y) \in \mathrm{pr}_{m-2}(X) = \mathrm{pr}_{m-2}(X')$，因此可以找到 $y' \in X'$，使得 $\mathrm{pr}_{m-2}(y') = \mathrm{pr}_{m-2}(y)$。由定理 4.6，这意味着

$$y'_{m-1} = w(y_1, \ldots, y_k), \quad y'_m = w'(y_1, \ldots, y_k).$$

由于 $(m-1, m) \in \rho(X')$，我们得出 $y'_{m-1} = y'_m$，从而推出 (19) 的右端。□

5. Isomorphisms of the S-ring $\mathfrak{A}_m(G)$

5.1. 对角群。我们对 S-环 $\mathfrak{A}_m(G)$ 的代数同构和组合同构的描述，基于文献 [3] 中关于对角群的主要结果。以下陈述是 [3, 定理 1.1(b)] 的一个特例。

引理 5.1. 设 H 是一个群，$m \geq 3$ 是一个整数。假设 H 是任意 m 个子群 H_0、H_1、……、H_m 的直积。那么存在一个群 T，使得

$$H = T^m, \quad H_0 = D_m(T), \quad H_i = T_i \text{ for all } i \in M.$$

对于 $m \geq 2$，对角图 $\Gamma_D(G, m)$ 定义为凯莱图 $\mathrm{Cay}(G^m, X_m)$，其中 $X_m = X_m(G) = G_0 \cup G_1 \cup \ldots \cup G_m$ 且 $G_0 = D_m(G)$。文献 [3, 小节 7.2] 证明了，$\Gamma_D(G, m)$ 唯一确定 G 至同构，

$$\Gamma_D(G, m) \cong \Gamma_D(G', m') \quad \Leftrightarrow \quad G \cong G' \text{ and } m = m', \tag{20}$$

并且，除四个小例外外，$\Gamma_D(G, m)$ 的自同构群等于半直积 $D(G, m) = \mathrm{Hol}_m(G) \rtimes \mathrm{Sym}(m+1)$，见 [3, 定理 1.4(b)]。以下结论可由群 $\Gamma_D(G, m)$ 的描述直接推出

[3, 备注 1.3]。下文中，我们用 $\mathrm{Aut}_m(G)$ 表示 $\mathrm{Aut}(G)$ 在 G^m 上逐分量作用所诱导的置换群。

引理 5.2. 设 G 是一个群，$m \geq 2$ 是一个整数。用 $D_0(m, G)$ 表示 $\mathrm{Aut}(\Gamma_D(G, m))$ 的子群，该子群保持顶点 1_{G^m} 以及集合$G_0, G_1, \ldots, G_m$ 分别不变。那么 $D_0(m, G) = \mathrm{Aut}_m(G)$。

推论 5.3. 对于 $m \geq 2$，我们有 $\mathrm{Aut}(\mathfrak{A}_m(G)) = \mathrm{Hol}_m(G)$。

证明. 令 $\mathfrak{A} = \mathfrak{A}_m(G)$ 且 $\overline{M} = M \cup \{0\}$。回顾一下，对于每个$i \in \overline{M}$，$G_i$ 都是一个 $\mathfrak{A}$-群。因此，稳定子 $\mathrm{Aut}(\mathfrak{A})_{1_{G^m}}$ 保持 G_i 不变（作为集合）。此外，根据 (6)，我们有 $\mathrm{Aut}(\mathfrak{A}) \leq \mathrm{Aut}(\Gamma)$，其中 $\Gamma = \Gamma_D(G, m)$。由引理 5.2可得 $\mathrm{Aut}(\mathfrak{A})_{1_{G^m}} \leq \mathrm{Aut}_m(G)$。因此，

$$\mathrm{Aut}(\mathfrak{A}) = G^m \, \mathrm{Aut}(\mathfrak{A})_{1_{G^m}} \leq G^m \, \mathrm{Aut}_m(G) = \mathrm{Hol}_m(G).$$

为证明反向包含关系，只需验证 $\mathrm{Aut}_m(G) \leq \mathrm{Aut}(\mathfrak{A})$。每个$f \in \mathrm{Aut}_m(G)$ 都是 $\mathcal{T}_m$ 的规范化自同构，使得对所有 $x \in G^m$，$(D_m x)^f = D_m x^f$。因此，根据引理 2.1 的第二部分，$f \in \mathrm{Aut}(\mathfrak{A})$。□

5.2. 代数同构。设 $\mathfrak{A} \geq \mathfrak{A}_m(G)$ 和 $\mathfrak{A}' \geq \mathfrak{A}_m(G')$。那么，对所有 $i \in \overline{M}$，G_i 和 G'_i 分别是 $\mathfrak{A}$-群和 $\mathfrak{A}'$-群。若代数同构 $\varphi : \mathfrak{A} \to \mathfrak{A}'$ 满足对所有 i，$\varphi(G_i) = G'_i$，则称其为真正的代数同构；特别地，

$$\varphi(\mathcal{T}_m(G)) = \mathcal{T}_m(G') \quad \text{and} \quad \varphi(D_m(G)) = D_m(G'). \tag{21}$$

显然，φ 通过限制诱导出一个真正的代数同构，它将 $\mathfrak{A}_m(G)$ 映到 $\mathfrak{A}_m(G')$。下述结论表明，$\mathfrak{A}_m(G)$ 的每个代数同构都是真正的代数同构。

命题 5.4. 设 $m \geq 3$, $\mathfrak{A}'$ 是群 H 上的一个 S-环，且 $\varphi : \mathfrak{A}_m(G) \to \mathfrak{A}'$ 是一个代数同构。那么，对于某个群 G'，$H = (G')^m$。此外，$\mathfrak{A}' = \mathfrak{A}_m(G')$，且 φ 是真正的代数同构。

证明。注意到 G^m 是任意 m 个 $\mathfrak{A}_m(G)$-子群 $G_i, i \in \overline{M}$的直积。因此，H 是任意 m 个 $\mathfrak{A}'$-子群 $H_i := \varphi(G_i)$, $i \in \overline{M}$的直积。由引理 5.1，存在一个群 G'，使得对所有 $i \in M$，$H = (G')^m$, $H_0 = D_m(G')$，且 $H_i = G'_i$。由此可得 $\mathfrak{A}' = \mathfrak{A}_m(G')$。□

我们通过归纳真正同构的一些性质来结束本小节，这些性质将在第6节中使用。

引理 5.5。设 $m \geq 1$ 和 φ 是从 $\mathfrak{A}_m$ 到另一个 S-环的真正代数同构。那么对所有 $X \in \mathcal{S}_m$、$\sigma \in \mathrm{Sym}(M)$ 和 $K \subseteq M$，有

(1) $\varphi(X^\sigma) = \varphi(X)^\sigma$, (2) $\varphi_K(\mathrm{pr}_K(X)) = \mathrm{pr}_K(\varphi(X))$, 其中 $\varphi_K = \varphi_{G^m/G_{K'}}$, (3) $n_K(X) = n_K(\varphi(X))$。

证明。记由置换 $\sigma \in \mathrm{Sym}(M)$ 诱导的 $\mathfrak{A}_m$ 的代数自同构为 ψ_σ。那么复合 $\psi' = \varphi\psi_\sigma\varphi^{-1}$ 是 $\mathfrak{A}_m(G') = \mathrm{im}(\varphi)$ 的代数自同构。由公式（21）和引理 2.2 可知，ψ' 是由 σ 诱导的 $\mathfrak{A}_m(G')$ 的代数自同构。因此，

$$\varphi(X^\sigma) = \varphi(\psi_\sigma(X)) = \psi'(\varphi(X)) = \varphi(X)^\sigma,$$

这就证明了结论 (1)。结论 (2) 由自然满同态 $\pi\colon G^m \to G^m/G_{K'}$ 的公式 (7) 得出。最后，$n_K(X) = n(X, G_{K'})$，参见引理 4.4 的证明，结论 (3) 由公式 (5) 得出。□

5.3. 同构。在本小节中，我们证明 S-环 $\mathfrak{A}_m(G)$ 将群 G 确定到同构为止。

引理 5.6. 设 $m \geq 1$。假设 $G^m = H^m$。则 $G \cong H$。此外，若 $\mathfrak{A}_m(G) = \mathfrak{A}_m(H)$，则存在 $\mathfrak{A}_m(G)$ 的一个规范化同构，它将 G_i 映到 H_i，对所有 $i \in \overline{M}$ 均成立。

证明. 设 $\{L_1, \ldots, L_k\}$ 是 G 的一组两两不同构的不可分解（关于直积）子群的完备集，因此也是 G^m 的一组完备集。由于 $H^m = G^m$，Krull-Schmidt 定理蕴含存在恰好 k 个两两不同构的不可分解子群 $M_1, \ldots, M_k$，它们属于 H^m，并且对所有 i 都有 $L_i \cong M_i$。

注意，若在将 G_1（分别为 H_1）分解为不可约直积时，n_i（分别为 n_i'）是 L_i（分别为 M_i）的重数，那么在将 G^m 分解为不可约直积时，L_i（分别为 M_i）的重数等于 mn_i（分别为 mn_i'）。因此，$mn_i = mn_i'$，从而对所有 i，$n_i = n_i'$。这表明，当 $i = 1$ 时 $G_i \cong H_i$，从而对所有 i 都成立；特别地，$G \cong H$。

同构 $G_i \to H_i$ 诱导出一个自同构 $f \in \mathrm{Aut}(G^m)$，使得对所有 $i \in \overline{M}$，$H_i = (G_i)^f$。由于 $\mathfrak{A}_m(G)$ 由 $\underline{G_i}$ 和 $\underline{H_i}$ 共同生成，因此我们有 $f \in \mathrm{Iso}(\mathfrak{A}_m(G))$。□

推论 5.7. 设 $m \geq 3$。对于任意代数同构 $\varphi\colon \mathfrak{A}_m(G) \to \mathfrak{A}_m(G')$，存在 $f \in \mathrm{Iso}(\mathfrak{A}_m(G'))$，使得复合 $\varphi\varphi_f$ 是真正的代数同构。

证明。根据命题 5.4，存在一个群 G'，使得 $\mathfrak{A}_m(G') = \mathrm{im}(\varphi) = \mathfrak{A}_m(G')^{\sim}$，且代数同构 $\varphi\colon \mathfrak{A}_m(G) \to \mathfrak{A}_m(G')$ 是真正的同构。根据引理 5.6，存在 $f \in \mathrm{Iso}(\mathfrak{A}_m(G'))$，使得对所有 $i \in \overline{M}$ 都有 $G_i' = (\widetilde{G}_i')^f$。因此，代数同构 $\varphi\varphi_f$ 是真正的同构。□

推论 5.8。设 $m \geq 3$。那么对于任意群 G 和 G'，从 $\mathfrak{A}_m(G)$ 到 $\mathfrak{A}_m(G')$ 的代数同构要么全部由同构诱导，要么一个也不是。

证明。假设代数同构 $\varphi\colon \mathfrak{A}_m(G) \to \mathfrak{A}_m(G')$ 由一个同构诱导。若 $\varphi'\colon \mathfrak{A}_m(G) \to \mathfrak{A}_m(G')$ 是另一个代数同构，则根据引理 5.6，$\varphi^{-1}\varphi'$ 由一个同构诱导。因此，φ' 也由一个同构诱导。□

定理 1.1 的证明。只需验证蕴含 (2) $\Rightarrow$ (1) 和 (3) $\Rightarrow$ (1)。假设 S-环 $\mathfrak{A}_m(G)$ 和 $\mathfrak{A}_m(G')$ 同构。由推论 5.7 和 5.8，存在一个同构 $f\colon \mathfrak{A}_m(G) \to \mathfrak{A}_m(G')$，它诱导出一个真正的代数同构。不失一般性，我们可以假设 f 已规范化。于是 $X_m(G)^f = X_m(G')$。由此可知，f 是从 $\Gamma_D(G, m)$ 到 $\Gamma_D(G', m)$ 的图同构。因此，根据公式（20），$G \cong G'$。这就证明了蕴含 (2) $\Rightarrow$ (1)。

假设群 $\mathrm{Hol}_m(G)$ 和 $\mathrm{Hol}_m(G')$ 置换同构。该置换同构也是与这两个群相关联的 S- 环 $\mathrm{Cyc}_m(G)$ 和 $\mathrm{Cyc}_m(G')$ 之间的同构。进而，此同构诱导出一个

S-环同构 f 从 $\mathfrak{A}_m(G) \le \mathrm{Cyc}_m(G)$ 到一个 S-环 $\mathfrak{A}' \le \mathrm{Cyc}_m(G')$。根据命题 5.4，对于由 f 诱导的代数同构，我们有 $\mathfrak{A}' = \mathfrak{A}_m(G)^{\sim}$，其中存在某个群 G，使得 $(G')^m = (G)^m$。根据引理 5.6，$G \cong G'$，因此$\mathfrak{A}' = \mathfrak{A}_m(G')$。由此可知，S-环 $\mathfrak{A}_m(G)$ 和 $\mathfrak{A}_m(G')$ 同构，且蕴含关系 (3) $\Rightarrow$ (1) 是蕴含关系 (2) $\Rightarrow$ (1) 的推论。□

本节的论证可用于加强 [16], 中的主要结果，该结果指出，每个群 G 都由 S-环 $\mathrm{Cyc}_3(\mathrm{Inn}(G))^{\mathrm{Sym}(3)}$ 所确定；该 S-环由 $\mathrm{Cyc}_3(\mathrm{Inn}(G))$ 中相对于由 Sym(3) 的元素诱导的同构保持不变的所有元素组成。事实上，后一个 S-环可以由一个更小的 S-环，即 $\mathfrak{A}_3(G)^{\mathrm{Sym}(3)}$，所替代。

6. Relationship between m-ary coherent configurations and S-rings

本节在 m-元相干构型 $\mathrm{WL}_m(G)$ 与 S-环 $\mathfrak{A}_m(G)$ 之间建立两种归约，这些归约将用于主要结果的证明。

定理 6.1. 设 $m \ge 1$ 和 $\mathfrak{A} = \mathfrak{A}(G)$ 是由 $\mathcal{S} = \mathrm{pr}_m(\mathrm{WL}_{3m}(G))$ 的等式 (1) 定义的线性空间。那么

(1) $\mathfrak{A}(G)$ 是 G^m 上的 S-环；(2) $\mathfrak{A}(G) \ge \mathfrak{A}_m(G)$；(3) 如果 G' 是一个群，使得 $\mathrm{WL}_{3m}(G)$ 与 $\mathrm{WL}_{3m}(G')$ 真正代数同构，那么 $\mathfrak{A}(G)$ 与 $\mathfrak{A}(G')$ 也是真正代数同构的。

证明。根据引理 3.7 的陈述 (1) 和 (2)，划分 $\mathrm{WL}_{3m}(G) \ge \mathfrak{X}_{3m}(G)$ 包含类 $\{1_{G^{3m}}\}$，并且关于取逆元封闭。由于投影 $\mathrm{pr}_m\colon G^{3m} \to G^m$ 是一个群同态，$\mathcal{S}$ 包含类 $\{1_{G^m}\}$，并且关于取逆元封闭。因此，$\mathcal{S}$ 满足条件 (S1) 和 (S2)。

为验证条件 (S3)，设 X、Y、$Z \in \mathcal{S}$。我们需要找到一个整数 $c = c^Z_{X,\,Y}$，使得每个 $z \in Z$ 都恰好有 c 个表示 $xy = z$，其中 $x \in X$ 且 $y \in Y$。为此，令 $A = X \times Y \times Z$。于是 $A \subseteq G^{3m}$，并且

$$\mathrm{pr}_{1,\dots,m}(A) = X, \qquad \mathrm{pr}_{m+1,\dots,2m}(A) = Y, \qquad \mathrm{pr}_{2m+1,\dots,3m}(A) = Z.$$

由于 $\mathfrak{X} = \mathrm{WL}_{3m}(G)$ 是一个 $3m$元相干配置，公式 (12) 表明，关于相应投影，类 X、Y和 Z 的完全原像 X'、Y'和 Z' 属于 $\mathfrak{X}^\cup$。因此，$A = X' \cap Y' \cap Z'$ 属于 $\mathfrak{X}^\cup$。此外，(14) 的右端表明，$\mathfrak{X}^\cup$ 还包含集合

$$A' = \{(x,y,z) \in G^{3m} :\ x_i y_i = z_i,\quad i = 1,\dots,m\}. \tag{22}$$

因此，$A \cap A' \in \mathfrak{X}^\cup$和 $A \cap A' = A_1 \cup \ldots \cup A_r$，其中存在某个 A_1、...、$A_r \in \mathfrak{X}$和$r \ge 0$。由于 $r = 0$ 当且仅当 $XY \cap Z = \varnothing$，我们可以假设 $r \ge 1$。

设 $z \in Z$。由于 $r \ge 1$，至少存在一对 $(x,y) \in X \times Y$such that$z = xy$。对于任意这样的一对，$(x,y,z) \in A'$，因此 $(x,y,z) \in A_i$ 恰好对一个 $i \in \{1,\dots,r\}$ 成立。由引理 3.5，所有满足 $(x,y,z) \in A_i$ 的 $(x,y) \in X \times Y$ 的数量等于满足 $K = \{2m+1,\dots,3m\}$ 的 $n_K(A_i)$ 的数量。因此，数量

$$c^Z_{X,Y} = c = |\{(x,y) \in X \times Y :\ xy = z\}| = \sum_{i=1}^{r} n_K(A_i) \tag{23}$$

不依赖于 $z \in Z$，正如所需。这就完成了陈述 (1) 的证明。此外，由推论 4.5 和引理 3.7(3)，我们有

$$\mathrm{WL}_{3m}(G) \geq \mathfrak{X}_{3m}(G) \geq \mathcal{S}(\mathcal{T}_{3m}) \quad \text{and} \quad D_{3m} \in \mathfrak{X}_{3m}(G)^{\cup} \leq \mathrm{WL}_{3m}(G)^{\cup}.$$

由此可得 $\mathcal{S} \geq \mathrm{pr}_m(\mathcal{S}(\mathcal{T}_{3m})) = \mathcal{T}_m$ 且 $D_m = \mathrm{pr}_m(D_{3m}) \in \mathcal{S}^{\cup}$。因此，S-环 $\mathfrak{A}(G)$ 包含 $\mathcal{T}_m$ 对 D_m 的扩张，即 $\mathfrak{A}_m(G)$。这证明了陈述 (2)。

为证明陈述 (3)，设 $\varphi\colon \mathrm{WL}_{3m}(G) \to \mathrm{WL}_{3m}(G')$ 是一个真正的代数同构。根据引理 3.4 的第二部分，它诱导出唯一确定的$\widetilde{}$双射 $\psi\colon \mathcal{S}(\mathfrak{A}(G)) \to \mathcal{S}(\mathfrak{A}(G'))$，使得对所有 $A \in \mathrm{WL}_{3m}(G)$，

$$\psi(\mathrm{pr}_m(\widetilde{A})) = \mathrm{pr}_m(\varphi(\widetilde{A})). \tag{24}$$

现在设 $X, Y, Z \in \mathcal{S}$ 和 $A = X \times Y \times Z$。则 $\varphi(A) = \psi(X) \times \psi(Y) \times \psi(Z)$。由于代数同构 φ 是真正的，公式 (15) 得出

$$\mu(\varphi(A')) = \mu(A') \supseteq \{(i, i+m, i+2m) : i \in M\},$$

其中 A' 由公式 (22) 定义。因此，与上文一样，$A \cap A' = A_1 \cup \ldots \cup A_r$ 并利用引理 5.5(3)，我们得到

$$c^{\psi(Z)}_{\psi(X),\psi(Y)} = \sum_{i=1}^{r} n_K(\varphi(A_i)) = \sum_{i=1}^{r} n_K(A_i) = c^{Z}_{X,Y}.$$

由此可知，ψ 诱导出从 $\mathfrak{A}(G)$ 到 $\mathfrak{A}(G')$ 的代数同构。它是真正的，因为 φ 也是如此。□

定理 6.2. 设 $m \geq 1$ 和 $\mathfrak{X}(G) = \mathrm{pr}_m(\mathcal{S}_{m+1})$。那么

(1) $\mathfrak{X}(G)$ 是一个 m 元相干配置；(2) 若 $m \geq 2$，则 $\mathfrak{X}(G) \geq \mathrm{WL}_m(G)$；(3) 若 G' 是一个群，使得 $\mathfrak{A}_{m+1}(G)$ 与 $\mathfrak{A}_{m+1}(G')$ 代数同构且为真正的，那么 $\mathfrak{X}(G)$ 与 $\mathfrak{X}(G')$ 也如此。

证明。根据引理 4.4，划分 $\mathcal{S}_{m+1}$ 是一个正则的 $(m+1)$ 元彩虹。因此，根据引理 3.4，划分 $\mathfrak{X}(G)$ 是一个 m 元彩虹。下面验证 $\mathfrak{X} = \mathfrak{X}(G)$ 满足条件 (C3)。

令 $X_0 =: X, X_1 \ldots, X_m \in \mathfrak{X}$。根据公式 (12)，关于 pr_m 的 X 的完整原像 $Y = X \times G$属于 $(\mathcal{S}_{m+1})^{\cup}$。由此可知，以下对象也属于

$$Y_i = \{y \in Y : \mathrm{pr}_m(y^{\sigma_i}) \in X_i\}, \qquad i \in M,$$

其中 $\sigma_i = (i, m+1)$ 是 $\mathrm{Sym}(m+1)$ 的一个换位。因此，集合$A = Y_1 \cap \ldots \cap Y_m$ 属于 $\mathcal{S}_{m+1}$。注意，若 $(x, g) \in Y$ 且 $\widehat{x} = (x_1, \ldots, x_m, g)$，则 $x_{i \leftarrow g} = \mathrm{pr}_m(\widehat{x}^{\sigma_i})$ 且

$$A = \{(x, g) \in Y : x_{i \leftarrow g} \in X_i,\ i \in M\}. \tag{25}$$

令 A 为 $A_1, \ldots, A_r \in \mathcal{S}_{m+1}$的不交并，其中 $r \geq 0$。由于（$m+1$）元彩虹 $\mathcal{S}_{m+1}$ 是正则的，所有满足（x, g）$\in A_i$的 $g \in G$ 的数量 $n_{\{m+1\}}(A_i)$ 不依赖于 $x \in \mathrm{pr}_m(A_i)$、$i = 1$、...、r。因此，由公式 (25)，该数量

$$n^{X}_{X_1,\ldots,X_m} = |\{g \in G : x_{j \leftarrow g} \in X_j,\ j = 1, \ldots, m\}| =$$

$$|\{g \in G : (x, g) \in A\}| = \sum_{i=1}^{r} |\{g \in G : (x, g) \in A_i\}| = \sum_{i=1}^{r} n_{m+1}(A_i)$$

也不依赖于 $x \in \mathrm{pr}_m(A_i) = X$。因此，（$m$）元彩虹 $\mathcal{S}_m$满足条件 (C3)，故为一个 m元相干配置。这就证明了陈述 (1)。

由推论 4.5，得 $\mathcal{S}_{m+1} \geq \mathfrak{X}_{m+1}(G)$。投影到 G^m 后，利用引理 3.7(3)，可得

$$\mathfrak{X}(G) = \mathrm{pr}_m(\mathcal{S}_{m+1}) \geq \mathrm{pr}_m(\mathfrak{X}_{m+1}(G)) \geq \mathfrak{X}_m(G).$$

由陈述 (1) 以及算子 WL_m 的单调性，可得

$$\mathfrak{X}(G) = \mathrm{WL}_m(\mathfrak{X}(G)) \geq \mathrm{WL}_m(\mathfrak{X}_m(G)) = \mathrm{WL}_m(G),$$

这就证明了陈述 (2)。

为证明陈述 (3)，设 $\varphi : \mathfrak{A}_{m+1}(G) \to \mathfrak{A}_{m+1}(G')$ 是一个真正的代数同构。$\mathfrak{X}(G)$ 和 $\mathfrak{X}(G')$ 的类分别是 $\mathfrak{A}_{m+1}(G)_{G^m}$和 $\mathfrak{A}_{m+1}(G')_{(G')^m}$ 的基本集。因此，同构 φ 诱导出一个双射$\psi : \mathfrak{X}(G) \to \mathfrak{X}(G')$，使得对所有 $X \in \mathfrak{X}(G)$，都有 $\varphi(X \times G) = \psi(X) \times G'$。由引理 5.5 的陈述 (1) 和 (2)，可得

$$\varphi(Y_i) = \{y \in \varphi(Y) : \ \mathrm{pr}_m(y^{\sigma_i}) \in \psi(X_i)\}, \qquad i \in M,$$

其中 Y_i 和 X_i 如上所述。由此可得 $n_{\psi\ X_1\ (),\ldots,\psi(X_m)}^{\psi(X)} = \sum_{j=1}^{r} n_{m+1}(\psi(A_j))$。根据引理 5.5 的陈述 (3)，可得

$$n_{\psi(X_1),\ldots,\psi(X_m)}^{\psi(X)} = \sum_{i=1}^{r} n_{m+1}(\psi(A_i)) = \sum_{i=1}^{r} n_{m+1}(A_i) = n_{X_1,\ldots,X_m}^{X}.$$

因此，ψ 是从 $\mathfrak{X}(G)$ 到 $\mathfrak{X}(G')$ 的代数同构；由于 φ是实际的同构，它也是真正的同构。□

7. Proof of the main results

定理 1.2 的证明。我们来证明包含关系 (3)。容易看出

$$\mathrm{pr}_m(\mathcal{T}_{m+k}) = \mathcal{T}_m \quad \text{and} \quad \mathrm{pr}_m(D_{m+k}) = D_m.$$

因此，S-环 $\mathfrak{A} = (\mathfrak{A}_{m+k})_{G^m}$ 包含由集合 $D_m \in \mathcal{S}(\mathfrak{A})$对 S-环 $\mathcal{T}_m \leq \mathfrak{A}$ 作出的扩张。于是，$\mathfrak{A} \geq \mathfrak{A}_m$，这就证明了 (3) 中的第一个包含关系。接下来，根据推论 5.3，$\mathrm{Aut}(\mathfrak{A}_{m+k}) = \mathrm{Hol}_{m+k}(G)$。因此，$\mathfrak{A}_{m+k} \leq \mathrm{Cyc}_{m+k}(G)$，从而

$$(\mathfrak{A}_{m+k})_{G^m} \leq (\mathrm{Cyc}_{m+k}(G))_{G^m} = \mathrm{Cyc}_m(G).$$

这就证明了 (3) 中的第二个包含关系。

假设 $k \geq \max\{2, d\}$。那么 $k + m \geq 3$。设 $x \in G^{m+k}$ 是满足 $\langle x_1, \ldots, x_d\rangle = G$的任意元素。根据推论 4.7，对每个 $y \in [x]$，都存在一个群同构

$$\sigma_y : \langle x_1, \ldots, x_{m+k}\rangle \to \langle y_1, \ldots, y_{m+k}\rangle,\ x_i \mapsto y_i\ (i = 1, \ldots m + k).$$

于是 $\sigma_y \in \mathrm{Aut}(G)$ 和 $y = x^{\sigma_y}$。由于 $X = [x]$ 相对于 $\mathrm{Aut}_{k+m}(G)$ 也是不变量，这意味着 X 是 $\mathrm{Aut}_{k+m}(G)$ 的一个轨道，因此 $X' = \mathrm{pr}_{k+1,\ldots,m+k}(X)$ 是 $\mathrm{Aut}_m(G)$ 的一个轨道。当元组 $\mathrm{pr}_{k+1,\ldots,m+k}(x)$ 遍历群 G^m 时，投影 X' 遍历 $\mathfrak{A}$ 的基本集。因此 $\mathcal{S}(\mathfrak{A})$ 由 $\mathrm{Aut}_m(G)$ 的轨道组成，并且 $\mathfrak{A} = \mathrm{Cyc}(\mathrm{Aut}(G)\ G^m) = \mathrm{Cyc}_m(G)$。

定理 1.3 的证明。根据定理 6.1(1)，划分 $\mathrm{pr}_m(\mathrm{WL}_{3m}(G))$ 等于划分 $\mathcal{S}(\mathfrak{A}) =: \mathcal{S}$ 与 $\mathfrak{A} = \mathfrak{A}(G)$。此外，根据定理 6.1(2)，$\mathfrak{A} \geq \mathfrak{A}_m$，特别是 $\mathcal{S} \geq \mathcal{S}(\mathfrak{A}_m)$。因此，

$$\mathrm{pr}_m(\mathrm{WL}_{3m}(G)) = \mathcal{S} \geq \mathcal{S}(\mathfrak{A}_m(G)),$$

这证明了定理 1.3 中的第一个包含关系。类似地，由定理 6.2(1)，划分 $\mathrm{pr}_m(\mathcal{S}_{m+1})$ 是一个 m 元相干配置。此外，由定理 6.2(2)，$\mathfrak{X} \geq \mathrm{WL}_m(G)$，这证明了定理 1.3 中的第二个包含关系。

我们来证明：若 $m \geq \dim_{\mathrm{WL}}(G) + 1$，则从 S-环 $\mathfrak{A}_m(G)$ 出发的每个代数同构都由一个同构诱导；这证明了 $s(G)$ 的存在性以及式 (4) 中的第二个不等式。

设 $m = \dim_{\mathrm{WL}}(G)$，$m \geq 3$，并设 G' 是一个群，使得 S-环 $\mathfrak{A}_{m+1}(G)$ 与 $\mathfrak{A}_{m+1}(G')$ 代数同构。由推论 5.7，不妨假设它们真正代数同构。由定理 6.2 的陈述 (2) 和 (3)，这意味着 m 元相干配置 $\mathfrak{X}(G) \geq \mathrm{WL}_m(G)$ 与 $\mathfrak{X}(G') \geq \mathrm{WL}_m(G')$ 真正代数同构。由引理 3.3，对于 $\mathfrak{X} = \mathfrak{X}(G)$ 和 $\mathfrak{Y} = \mathrm{WL}_m(G)$，$m$ 元相干配置 $\mathrm{WL}_m(G)$ 与 $\mathrm{WL}_m(G')$ 也如此。由于 $m = \dim_{\mathrm{WL}}(G)$，我们得出 $G \cong G'$，并且由定理 1.1，S-环$\mathfrak{A}_{m+1}(G)$ 与 $\mathfrak{A}_{m+1}(G')$ 同构。特别地，它们之间真正的代数同构由一个同构诱导。由推论 5.8，这表明从 S-环 $\mathfrak{A}_{m+1}(G)$ 出发的每个代数同构都由一个同构诱导。这证明了数 $s(G)$ 的存在性以及式 (4) 中的第二个不等式。

令 $m = s(G)$、$m \geq 3$，并令 G' 为与 G WL_{3m}-等价的一个群。这意味着，m 元相干配置 $\mathrm{WL}_{3m}(G)$ 和 $\mathrm{WL}_{3m}(G')$ 在代数意义上确实同构。由定理 6.1 的陈述 (2) 和 (3) 可知，S- 环 $\mathfrak{A}(G) \geq \mathfrak{A}_m(G)$ 与 $\mathfrak{A}(G') \geq \mathfrak{A}_m(G')$ 也同样如此。因此，S-环 $\mathfrak{A}_m(G)$ 和 $\mathfrak{A}_m(G')$ 在代数意义上同构。由于 $m = s(G)$，它们是同构的，故由定理 1.1 可得 $G \cong G'$。因此，$\dim_{\mathrm{WL}}(G) \leq 3s(G)$。

8. 定理 1.4 的证明

定理 1.4 的陈述是下面一个更一般引理的直接推论。在证明中，所谓对着色群 G 中的元素 $x \in G$ 进行个体化 G_x，是指对 G 进行着色，使得元素 $\neq x$ 的颜色与之前相同，而 x 的颜色则不同于其他元素的颜色。

引理 8.1. 对于着色群 G 和 G'，以下问题在多项式时间内等价：

(a) 判断 $\mathrm{Iso}(G, G') \neq \varnothing$ 是否成立；若成立，则找出 $\mathrm{Iso}(G, G')$ 中的一个元素；(b) 找出集合 $\mathrm{Iso}(G, G')$；(c) 找出群 $\mathrm{Aut}(G)$；(d) 找出 S-环 $\mathrm{Cyc}_1(G)$。

证明。(a) 显然可归约为 (b)。为说明从 (b) 到 (c) 的归约，分别用 c_G 和 $c_{G'}$ 表示 G 和 G' 的着色。我们定义 c 的一个着色，

直积 $G \times G'$，使得对于任意的 $g \in G$ 和 $g' \in G'$，

$$c(g,g') = \begin{cases} c_G(g) & \text{if } g \neq 1 \text{ and } g' = 1, \\ c_{G'}(g') & \text{if } g = 1 \text{ and } g' \neq 1, \\ \varepsilon & \text{otherwise,} \end{cases} \tag{26}$$

其中，ε 是任意一个不属于 $\mathsf{im}(c_G) \cup \mathsf{im}(c_{G'})$ 的符号。容易看出，着色群 $G \times G'$ 的自同构群 $\mathsf{Aut}(G \times G')$ 保持集合 $G \cup G'$ 不变；将同时保持 G 和 G'（作为集合）不变的 $\mathsf{Aut}(G \times G')$ 的子群记为 $\mathsf{Aut}_0(G \times G')$。最后注意到，$G \cong G'$ 当且仅当

$$[\mathrm{Aut}(G \times G') : \mathrm{Aut}_0(G \times G')] = 2,$$

若是如此，则 $\mathsf{Iso}(G, G') = Kf$，其中 K 是 $\mathsf{Aut}_0(G \times G')$ 在 G 和 f 上的限制：$G \to G'$ 是由 $\mathsf{Aut}(G \times G')$ 中属于 $\mathsf{Aut}_0(G \times G')$ 的非平凡陪集的一个（任意选取的）置换所诱导的双射。

下面描述将 (c) 归约为 (a) 的方法。假设我们有一个能够求解 (a) 的算法。那么，对于着色群 G 的每个元素 x，都可以高效地找到集合

$$S_x(G) = \{f_{x,y} \in \mathrm{Iso}(G_x, G_y) : \ y \in G, \ G_x \cong G_y\},$$

其中，对每个 y，同构 $f_{x,\,y}$ 均任意选取。现在，如果 G 的着色是离散的，那么显然 $\mathsf{Aut}(G)$ 是平凡群。接下来，如果对于至少一个 $x \in G$，$\{x\}$ 不是 G 的颜色类，那么 $\mathsf{Aut}(G) = \langle S_x(G), \mathsf{Aut}(G_x)\rangle$。因此，求 $\mathsf{Aut}(G)$ 可高效地归约为求群 $\mathsf{Aut}(G_x)$。此外，G_x 的单元素颜色类数量至多为 $|G|$。因此，群 G 至多可通过 $|G|$ 次归约构造出来。

(d) 可平凡地归约为 (c)。下面描述将 (a) 归约为 (d) 的方法。我们需要一个辅助命题。

命题。设 G 和 G' 是着色群。那么，给定 $x \in G$ 和 $x' \in G'$，可以利用 (d) 作为预言机，高效地检验 $\mathsf{Iso}(G_x, G'_{x'}) \neq \varnothing$ 是否成立。

证明。用公式 (26) 为 $K = G_x \times G'_{x'}$ 着色（注意，点对 $(x, 1)$ 和 $(1, x')$ 被着成相同的颜色）。那么，$\mathsf{Iso}(G_x, G'_{x'}) \neq \varnothing$ 当且仅当 x 和 x' 位于 $\mathsf{Aut}(K)$ 的同一轨道中；当且仅当 $(x, 1)$ 和 $(1, x')$ 位于划分 $\mathcal{S}(\mathfrak{A})$ 的同一类中，其中 $\mathfrak{A} = \mathsf{Cyc}(\mathsf{Aut}(K))$。□

现在设 G 和 G' 是着色群。如果 G 的着色是离散的，那么显然可以解决 (a)。否则，设 $x \in G$。根据该断言，可以高效地检验是否存在至少一个 x'，使得 $\mathsf{Iso}(G_x, G'_{x'}) \neq \varnothing$。如果不存在，那么当然有 $\mathsf{Iso}(G, G') = \varnothing$。否则，问题 (a) 中针对 G 和 G' 的情形可以高效地归约为针对 G_x 和 $G'_{x'}$ 的情形。此外，G_x 的单元素颜色类数严格少于 G 的单元素颜色类数。因此，经过至多 $|G|$ 次归约后，我们便得到问题 (a)，其中一个输入群具有离散着色。□

Acknowledgment

第一作者的工作得到中国国家自然科学基金（编号：11971189、12161035）的资助

References

[1] L. Babai, *Group, Graphs, Algorithms: the Graph Isomorphism Problem*, 国际数学家大会论文集（ICM 2018），第3卷，WORLD SCIENTIFIC（2019），另见 L. Babai, *Graph Isomorphism in Quasipolynomial Time* 2016 1512 03547 2 ( ), arXiv: . v [ ] 3319 3336 cs.DS），第 – 页。[2] C. Bagi´nski 和 P. Grzeszczuk, *On the generic family of Cayley graphs of a finite group*, J. Combin. Theory. Ser. A, 184, 105495 （2021）。[3] R. A. Bailey, P. J. Cameron, C. Praeger 和 C. Schneider, *The geometry of diagonal groups*, Trans. Amer. Math. Soc., 375, no. 8, 5259–5311（2022）。[4] J. Brachter 和 P. Schweitzer, *On the Weisfeiler-Leman Dimension of Finite Groups*, 第35届 ACM/IEEE计算机科学逻辑研讨会论文集（美国纽约州纽约），第1期，ACM，2020年，第287–300页。[5] J. Brachter 和 P. Schweitzer, *A Systematic Study of Isomorphism Invariants of Finite Groups via the Weisfeiler-Leman Dimension* *30th Annual European Symposium on Al-* ，载于: ，文章 *gorithms (ESA 2022)* 27 2022 27 1 27 14 编号（），第: –: 页。[6] G. Chen 和 I. Ponomarenko, *Coherent configurations*, 华中师范大学出版社（2019），更新版本见 http://www.pdmi.ras.ru/~inp/ccNOTES.pdf. [7] S. Evdokimov 和 I. Ponomarenko, *On highly closed cellular algebras and highly closed iso- morphisms* **6**, 18 1999 , Electronic J. Combin., #R（）。[8] S. Evdokimov 和 I. Ponomarenko, *Schur rings over a product of Galois rings*, Beitr. Algebra Geom., 55, no. 1, 105–138（2014）。[9] S. Evdokimov 和 I. Ponomarenko, *On the separability problem for circulant S-rings*, St. Petersburg Math. J., 28, no. 1, 21–35（2017）。[10] E. Formanek 和 D. Sibley, *The Group Determinant Determines the Group*, Proc. AMS, 112, no. 3, 649–656（1991）。[11] M. Grechkoseeva, V. D. Mazurov, W. Shi, A. Vasil'ev 和 N. Yang, *Finite groups isospectral to simple groups* 2022 10 1007 40304 022 00288 5 , Commun. Math. Stat.（），doi: . /s - - -。[12] A. Heinze 和 M. Klin, *Loops, Latin Squares and Strongly Regular Graphs: An Algorith-mic Approach via Algebraic Combinatorics*, 载于《算法代数组合学与 Gr¨obner 基》，Springer Berlin Heidelberg，德国柏林，海德堡（2009），第3–65页。[13] H. Helfgott, J. Bajpai 和 D. Dona, *Graph isomorphisms in quasi-polynomial time*, arXiv:1710.04574 1 67 2017 , – （）。[14] R. Mathon, *A note on the graph isomorphism counting problem* **8**, , 131 132 1979 Inform. Process. Lett. – （）。[15] I. Ponomarenko, *On the WL-dimension of circulant graphs of prime power order*, arXiv:2206.15028 1 23 2022 , – （）。[16] E. L. Rode, *On a generalized centralizer ring of a finite group which determines the group*, Algebra Colloq., 26, no. 1, 31–50（2019）。[17] M. Roitman, *A complete set of invariants for finite groups and other results*, Advances Math. 41, no. 3, 301–311（1981）。[18] H. Wielandt, *Finite permutation groups*, Academic Press，纽约和伦敦（1964）。

School of Mathematics and Statistics, Central China Normal University, Wuhan430079, China*Email address*: chengangmath@mail.ccnu.edu.cn

School of Mathematics and Statistics, Central China Normal University, Wuhan 430079, China*Email address*: renqing@mails.ccnu.edu.cn

Steklov Institute of Mathematics at St. Petersburg, Russia

Email address: inp@pdmi.ras.ru