arXiv:2304.09124v1 [math.QA] 18 Apr 2023

一个关于4个点上的量子置换群的具体模型

NICOLAS FAROSS 和 MORITZ WEBER

ABSTRACT. 2019年，Jung-Weber 给出了一个具体魔幻酉矩阵M的例子，它定义了量子置换群 S_4^+的一个 C^*代数模型。我们借助计算机证明，不存在次数不超过50的多项式能够将 M 的各个条目与 $C(S_4^+)$的生成元区分开来。这表明，魔法酉矩阵 M 可能已经定义了S_4^+的一个忠实模型。

1. INTRODUCTION

量子置换群 S_n^+ 最早由 Wang 在 [Wan98] 中引入；按照 Woronowicz紧矩阵量子群的观点（见 [Wor87]），它可以被视为经典对称群 S_n 的一种推广。它通过如下的泛 C^*代数定义：

$$C(S_n^+) := C^*(u_{ij},\, 1 \leq i,j \leq n \mid u \text{ is a magic unitary}),$$

如果矩阵 $u =(u_{ij})$ 的各个条目满足以下关系，则称其为魔法酉矩阵：

$$u_{ij}^2 = u_{ij}^* = u_{ij}, \qquad \sum_{k=1}^{n} u_{ik} = 1, \qquad \sum_{k=1}^{n} u_{kj} = 1 \qquad (1 \leq i,j \leq n).$$

注意到，条目属于 $\mathbb{C}$ 的魔幻酉矩阵恰好就是置换矩阵，这也说明了“量子置换群”这一名称的由来。在 [JW20], Jung 与第二作者给出了一个具体魔幻酉矩阵的例子，它定义了量子置换群 S_4^+ 的一个模型。该矩阵为

$$M = \begin{pmatrix} p\otimes p\otimes p \\ +(1-p)\otimes q\otimes(1-p) & p\otimes(1-p)\otimes q \\ +(1-p)\otimes(1-q)\otimes(1-q) & p\otimes p\otimes(1-p) \\ +(1-p)\otimes q\otimes p & p\otimes(1-p)\otimes(1-q) \\ +(1-p)\otimes(1-q)\otimes q \\ \\ (1-p)\otimes p\otimes p \\ +p\otimes q\otimes(1-p) & (1-p)\otimes(1-p)\otimes q \\ +p\otimes(1-q)\otimes(1-q) & (1-p)\otimes p\otimes(1-p) \\ +p\otimes q\otimes p & (1-p)\otimes(1-p)\otimes(1-q) \\ +p\otimes(1-q)\otimes q \\ \\ q\otimes(1-p)\otimes p \\ +(1-q)\otimes(1-q)\otimes(1-p) & q\otimes p\otimes q \\ +(1-q)\otimes q\otimes(1-q) & q\otimes(1-p)\otimes(1-p) \\ +(1-q)\otimes(1-p)\otimes p & q\otimes p\otimes(1-q) \\ +(1-q)\otimes q\otimes q \\ \\ (1-q)\otimes(1-p)\otimes p \\ +q\otimes(1-q)\otimes(1-p) & (1-q)\otimes p\otimes q \\ +q\otimes q\otimes(1-q) & (1-q)\otimes(1-p)\otimes(1-p) \\ +q\otimes(1-q)\otimes p & (1-q)\otimes p\otimes(1-q) \\ +q\otimes q\otimes q \end{pmatrix},$$

日期：2023年4月19日。关键词和短语：量子置换群、魔法酉矩阵、紧量子群。

其中 p 和 q 是满足 $p^2 = p^* = p$ 和 $q^2 = q^* = q$ 的泛投影。然而，该模型是否忠实仍是一个悬而未决的问题，即 $*$-同态

$$\varphi\colon C(S_4^+) \to B,\ u_{ij} \mapsto M_{ij}$$

是单射，其中 B 表示由条目 M_{ij}生成的 C^*代数。特别是，Jung-Weber 关注是否存在一个非交换多项式P，使得 P 在 M 的条目中消失，但在 C的生成元中不消失（S_4^+）。这样的多项式将证明映射 φ 不是单射。我们的主要结果借助计算机（使用 GAP:GBNP [CK16] 和 SageMath [The20]）部分地对此问题给出了否定答案，证明不存在次数不超过 50 的此类多项式。

定理（定理 3.3）。设 $P \in \mathbb{C}\langle X\rangle$ 是一个 4×4矩阵 $X = (x_{ij})$ 的条目中的非交换多项式，且次数为 $P \leq 50$。如果 $P(M) = 0$，那么 P包含于由魔幺正关系生成的理想中

$$\begin{aligned} x_{ij}^2 &= x_{ij}, && (1 \leq i, j \leq 4) \\ \sum_{k=1}^{n} x_{ik} &= \sum_{k=1}^{n} x_{kj} = 1, && (1 \leq i, j \leq 4) \\ x_{ij}x_{ik} &= x_{ji}x_{ki} = 0. && (1 \leq i, j, k \leq 4, j \neq k) \end{aligned}$$

由于 $C(S_4^+)$ 的生成元也满足前一定理中的关系，因此，任何次数不超过 50 且在 M 的条目中为零的多项式，都必然在 $C(S_4^+)$ 的生成元中为零。因此，我们立即得到以下推论。

推论（推论 6.1）。记 $C(S_4^+)$ 的生成元为 u，并设 $P \in \mathbb{C}\langle X\rangle$ 是一个满足 $\deg P \leq 50$ 的多项式。那么，$P(M) = 0$ 当且仅当 $P(u) = 0$。

请注意，前述结果中的 50 次是一个任意界限，只要为我们的算法提供更多的时间和空间，就可以提高这一界限。此外，最大次数 50 已经相当大，这表明不存在任何在 M 的条目中为零、但在 u 的生成元中不为零的多项式。在这种情况下，具体魔幻酉矩阵 M 可能定义量子置换群 S_4^+ 的一个忠实 C^*-代数模型。

我们将在第 2 节首先定义量子置换群，并介绍一些相关事实，然后回顾上文中具体魔幻酉矩阵M 的构造。接着，我们将在第 3 节陈述主要定理，并概述其证明算法。第 4 节和第 5 节将进一步介绍细节和计算结果。在第 6 节中，我们将给出更多论据，说明 M 可能是 S_4^+ 的忠实模型，并结合量子群以及 S_n^+ [BM07], [BBS09], [BB15],[BN17]的其他模型讨论我们的结果。此外，我们还将考虑更大的 n 情形，并证明，对于具有 $n > 4$的 S_n^+类似模型，我们的结果不再成立。

Acknowledgements

第二作者得到 SFB-TRR 195（本工作是 SFB-TRR 195 的一项成果）、德国研究基金会的海森堡计划以及 OPUS-LAP“表示论中的量子群、图与对称性”的资助。本工作是第一作者学士学位论文的一部分。

2. Models of the Quantum Permutation Group

我们首先给出魔幻酉矩阵和量子置换群S_n^+的定义，然后介绍 S_n^+ 的模型以及具体魔幻酉矩阵 M的构造。这些定义以（泛） C^*-代数的语言表述，即 A 带有对合 $*$ 的复结合代数 $A \to A$，并配备满足 C^*-恒等式 $\|a\|^2 = \|a^*a\|$. 的相容范数。然而，在大多数情况下，我们不会使用这些额外结构，而仅将 C^*-代数视为结合复代数（不一定是交换的）。关于 C^*-代数的一般理论，请参阅 [Bla05]；关于泛 C^*-代数的介绍，请参阅 [LVW20]。

定义 2.1（魔法酉矩阵）。设 A 是一个含单位元的 C^*-代数，且 $M \in M_n(A)$。如果矩阵 M 的元素都是投影，并且每一行及每一列的和均为 1，即

$$M_{ij}^2 = M_{ij}^* = M_{ij}, \qquad \sum_{k=1}^{n} M_{ik} = 1, \qquad \sum_{k=1}^{n} M_{kj} = 1 \qquad (1 \le i, j \le n).$$

定义 2.2（量子置换群）。设 $u = (u_{ij})$ 为由生成元构成的 $n \times n$-矩阵，并定义如下泛幺 C^*-代数

$$A := C^*(u_{ij},\, 1 \le i, j \le n \mid u \text{ is a magic unitary}).$$

则称 $S_n^+ := (A, u)$ 为大小为 n [Wan98] 的量子置换群。此外，我们将该 C^*-代数记作 A，其中 $C(S_n^+)$。

关于魔幻酉矩阵的更多信息以及一些相关开放问题的概述，请参阅 [Web23] 。注意，存在一个 $*$-同态

$$\Delta\colon C(S_n^+) \to C(S_n^+) \otimes C(S_n^+),\ u_{ij} \mapsto \sum_{k=1}^{n} u_{ik} \otimes u_{kj},$$

称为余乘法，它使 S_n^+成为 Woronowicz 意义下的紧矩阵量子群 [Wor87]。例如，参见 [LES+22] ，了解计算机代数背景下量子对称性的简要介绍；参见 [Tim08], [NT13]，了解一般的紧量子群。不过，我们主要关注 $C(S_n^+)$ 的代数性质，只会在最后的第 6 节再回到量子群结构。除定义关系外，魔幻酉矩阵还满足其他关系，这些关系可由 C^*-代数结构推出。

命题 2.3。设 A 是一个含幺 C^*-代数，且 $M \in M_n(A)$ 是一个魔法酉矩阵。那么，同一行或同一列中任意两个不同元素的乘积为零，即

$$M_{ij} \cdot M_{ik} = 0, \qquad M_{ji} \cdot M_{ki} = 0 \qquad (1 \leq i, j, k \leq n,\ j \neq k).$$

证明。将关系式 $\sum_{k=1}^{n} M_{ik} = 1$ 从两侧分别乘以 M_{ij}，我们可知 $\sum_{k \neq j} M_{ij} M_{ik} M_{ij} = 0$ 是正元素之和。根据C^*-代数理论，这些加项中的每一项都必须为零，因此

$$\|M_{ik} M_{ij}\|^2 = \|(M_{ik} M_{ij})^* (M_{ik} M_{ij})\| = 0$$

根据 C^*-恒等式。 □

现在，考虑任意一个魔法酉矩阵 $M \in M_n(A)$，以及由 M 的各个元素生成的 C^*-子代数 $B \subseteq A$。于是， $C(S_n^+)$ 的泛性质蕴含了一个满射 $*$-同态 $\varphi\colon C(S_n^+) \to B$，它将生成元$u_{ij}$映射到 M_{ij}。因此，每一对魔法酉矩阵 M 及其对应的C^*-代数 B（即 (B, M)）都定义了量子置换群 S_n^+ 的一个 C^*-代数模型。然而，(B, M) 不一定是一个紧矩阵量子群，因为可能不存在余乘法 $\Delta\colon B \to B \otimes B$。

在 [JW20], Jung-Weber 构造了这类 C^* 代数模型的序列（B_i, M_i）。其构造方法是从一个初始魔法酉矩阵出发，对 [Wor87] 中的 $\circledcirc$ 算子反复迭代。对于两个矩阵 $M_1 \in M_n(A_1)$ 和 $M_2 \in M_n(A_2)$，该算子会生成一个新的矩阵 $M_1 \circledcirc M_2 \in M_n(A_1 \otimes A_2)$，其元素定义为

$$(M_1 \circledcirc M_2)_{ij} = \sum_{k=1}^{n} (M_1)_{ik} \otimes (M_2)_{kj} \qquad (1 \leq i, j \leq n).$$

可以直接验证，如果 M_1 和 M_2 都是魔幻酉矩阵，那么矩阵 $M_1 \circledcirc M_2$ 也是魔幻酉矩阵。因此，从一个初始魔法酉矩阵 $n \times n$ R 出发，可以得到一个序列

$$(B_1, R),\ (B_2, R^{\circledcirc 2}),\ (B_3, R^{\circledcirc 3}),\ \ldots$$

S_n^+ 的模型，其中每个 B_i 都是由 $R^{\circledcirc i}$ 的元素生成的 C^* 代数。此外，Jung-Weber 构造了合适的初始矩阵 R，由此可以将 S_n^+ 重构为一个逆极限。一个这样的初始魔法酉矩阵定义为

$$R := \begin{pmatrix} p & 0 & 1-p & 0 \\ 1-p & 0 & p & 0 \\ 0 & q & 0 & 1-q \\ 0 & 1-q & 0 & q \end{pmatrix} \in M_4(A),$$

其中

$$A := C^*\left(p, q \;\middle|\; p^2 = p^* = p,\ q^2 = q^* = q\right) = C^*(\mathbb{Z}_2 * \mathbb{Z}_2)$$

是由两个投影生成的泛幺元 C^*-代数。对 R 与自身反复进行 $\textcircled{+}$-积，可得到

$$R^{\textcircled{+}2} = \begin{pmatrix} p\otimes p & (1-p)\otimes q & p\otimes(1-p) & (1-p)\otimes(1-q) \\ (1-p)\otimes p & p\otimes q & (1-p)\otimes(1-p) & p\otimes(1-q) \\ q\otimes(1-p) & (1-q)\otimes(1-q) & q\otimes p & (1-q)\otimes q \\ (1-q)\otimes(1-p) & q\otimes(1-q) & (1-q)\otimes p & q\otimes q \end{pmatrix}$$

以及引言中的 $R^{\textcircled{+}3}$ 魔法酉矩阵。

定义 2.4。在本文中，令

$$M := \begin{pmatrix} \begin{matrix} p\otimes p\otimes p \\ +(1-p)\otimes q\otimes(1-p) \end{matrix} & \begin{matrix} p\otimes(1-p)\otimes q \\ +(1-p)\otimes(1-q)\otimes(1-q) \end{matrix} & \begin{matrix} p\otimes p\otimes(1-p) \\ +(1-p)\otimes q\otimes p \end{matrix} & \begin{matrix} p\otimes(1-p)\otimes(1-q) \\ +(1-p)\otimes(1-q)\otimes q \end{matrix} \\ \begin{matrix} (1-p)\otimes p\otimes p \\ +p\otimes q\otimes(1-p) \end{matrix} & \begin{matrix} (1-p)\otimes(1-p)\otimes q \\ +p\otimes(1-q)\otimes(1-q) \end{matrix} & \begin{matrix} (1-p)\otimes p\otimes(1-p) \\ +p\otimes q\otimes p \end{matrix} & \begin{matrix} (1-p)\otimes(1-p)\otimes(1-q) \\ +p\otimes(1-q)\otimes q \end{matrix} \\ \begin{matrix} q\otimes(1-p)\otimes p \\ +(1-q)\otimes(1-q)\otimes(1-p) \end{matrix} & \begin{matrix} q\otimes p\otimes q \\ +(1-q)\otimes q\otimes(1-q) \end{matrix} & \begin{matrix} q\otimes(1-p)\otimes(1-p) \\ +(1-q)\otimes(1-q)\otimes p \end{matrix} & \begin{matrix} q\otimes p\otimes(1-q) \\ +(1-q)\otimes q\otimes q \end{matrix} \\ \begin{matrix} (1-q)\otimes(1-p)\otimes p \\ +q\otimes(1-q)\otimes(1-p) \end{matrix} & \begin{matrix} (1-q)\otimes p\otimes q \\ +q\otimes q\otimes(1-q) \end{matrix} & \begin{matrix} (1-q)\otimes(1-p)\otimes(1-p) \\ +q\otimes(1-q)\otimes p \end{matrix} & \begin{matrix} (1-q)\otimes p\otimes(1-q) \\ +q\otimes q\otimes q \end{matrix} \end{pmatrix}.$$

表示我们的具体魔幻酉矩阵。它表示为 $M = R^{\textcircled{+}3}$，其元素属于 $A\otimes A\otimes A$，其中 A 是由上文定义的两个投影生成的通用 C^*代数。

注意，为了简化记号，我们在 $A\otimes A\otimes A$的第一个、第二个和第三个张量因子中，均用同一个字母表示三个生成元 p，而不写作$p_1\otimes p_2\otimes p_3$；字母 q也同样如此。在前述设定中，Jung-Weber 提出了寻找多项式 P_n的问题，以区分这些模型。

问题 2.5（[JW20]）。是否存在多项式（P_n）$_{n\in\mathbb{N}}$，使得 P_n（$R^{\textcircled{+}n}$）$=0$ 且P_n（$R^{\textcircled{+}n+1}$）$\neq 0$?

这样的多项式对于 $n<3$ 确实存在，例如 $P_1 = x_{12}$ 和$P_2 = x_{12}x_{24}$，这可以直接验证（另见 [JW20]）。然而， $n\geq 3$的情形此前仍未解决。我们的主要结果表明，任何在 $R^{\textcircled{+}3}$中为零且满足 $\deg P\leq 50$ 的多项式 P，都属于由魔法酉矩阵的关系生成的理想。因此，它在 $R^{\textcircled{+}4}$ 的各个元素以及 C（S_4^+）的生成元中也为零。这从反面回答了上述问题：对于次数不超过 50 的多项式，不存在满足 $\deg P_3\leq 50$，且使得 P_3（$R^{\textcircled{+}3}$）$=0$、 P_3（$R^{\textcircled{+}4}$）$\neq 0$的多项式 P_3。此外，这表明根本不存在能够区分$R^{\textcircled{+}3}$ 的各个元素与 $R^{\textcircled{+}4}$的各个元素的多项式。在这种情况下， $R^{\textcircled{+}3}$ 或许已经定义了 S_4^+的一个忠实模型。关于这些模型的更多细节，我们再次参见 [JW20]。

3. Computing Separating Polynomials

下面我们引入一些记号，以便定义分离多项式并表述我们的主要定理。设 X 是一个有限集。记 $\mathbb{C}\langle X\rangle$ 为由 X 生成的自由结合含幺代数。其元素可以视为

关于变量 X 的非交换多项式。此外，我们要求每个理想 $I \subseteq \mathbb{C}\langle X\rangle$ 都是双边理想。由于我们关注的是魔幻酉矩阵，定义变量

$$X_n := \{x_{11}, x_{12}, \ldots, x_{nn}\},$$

作为一般 $n \times n$ 矩阵的元素。注意到只需考虑变量 x_{ij}，并省略 x_{ij}^*，因为魔法酉矩阵的元素是自伴的。给定某个代数 A上的矩阵 $M \in M_n(A)$，我们将 φ_M 称为代入同态

$$\varphi_M \colon \mathbb{C}\langle X_n\rangle \to A,\ x_{ij} \mapsto M_{ij}.$$

此外，我们定义由定义 2.1 和命题 2.3 中的魔幺正关系生成的理想。

定义 3.1（魔幺正理想）。设 $n \in \mathbb{N}$。则定义魔幺正理想 $I_n \subseteq \mathbb{C}\langle X_n\rangle$，其由下列多项式生成

$$\begin{aligned} &x_{ij}^2 - x_{ij}, \qquad \sum_{k=1}^{n} x_{ik} - 1, \qquad \sum_{k=1}^{n} x_{kj} - 1 && (1 \le i, j \le n),\\ &x_{ij} \cdot x_{ik}, \qquad x_{ji} \cdot x_{ki} && (1 \le i, j, k \le n,\ j \ne k). \end{aligned}$$

利用上述定义，我们现在可以引入分离多项式，并表述我们的主要结果。

定义 3.2（分离多项式）。设 A 是一个含幺 C^*-代数，并且 $M \in M_n(A)$是一个魔法酉矩阵。称非零多项式 $P \in \mathbb{C}\langle X_n\rangle$ 为分离多项式，如果 $\varphi_M(P) = 0$，但 $P \notin I_n$。

定理 3.3. 对定义 2.4 中的具体魔幻酉矩阵 M，不存在次数为 $P \le 50$ 的分离多项式 $P \in \mathbb{C}\langle X_4\rangle$。

下面我们将概述如何借助计算机 [1] 证明定理 3.3。第 4 节和第 5 节将介绍更多细节及计算结果，随后我们将在第 5.3 节给出最终证明。第 6 节将讨论我们的结果在 S_4^+ 模型中的意义，并证明定理 3.3 的推广在 $n > 4$ 情形下不成立。

为计算定义 2.4 中具体魔幻酉矩阵 M 的分离多项式，我们考虑代入同态 φ_M。由于 M 是魔法酉矩阵，因此有 $I_4 \subseteq \ker \varphi_M$，使得 φ_M可以分解为

$$\begin{array}{ccc} \mathbb{C}\langle X_4\rangle & \xrightarrow{\quad\varphi_M\quad} & A^{\otimes 3} \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\psi} & \\ & \mathbb{C}\langle X_4\rangle / I_4 & \end{array}$$

[1]我们的算法实现可在 https://github.com/nfaross/model-s4plus 找到

这里， A表示由两个投影 p 和 q生成的普适 C^*-代数。此外，记

$$V_m := \{\pi(P) \mid P \in \mathbb{C}\langle X_4\rangle, \deg P \le m\}$$

次数不超过 m 的多项式的所有剩余类所构成的子空间。于是，限制 $\psi|_{V_m}$ 的核恰好包含次数不超过 m 的分离多项式的剩余类。因此，当且仅当 $\ker \psi|_{V_m} = \{0\}$ 时，不存在次数不超过 m 的分离多项式。为证明这一结论，我们分两步进行。

(1) 在第 4 节中，我们为子空间 V_m 构造一个基 $\mathcal{B}_m$ ，它可以由魔幺正理想 I_4 的 Gr¨obner 基得到。事实证明，这样的基 $\mathcal{B}_m$ 也可以用有限自动机来描述，而有限自动机是一种特殊的标记图。借助这个有限自动机，我们便能高效枚举所有基元素，并计算 V_m 的维数。特别地，我们得到 $|\mathcal{B}_m| = \Theta(m^3)$，使得维数仅随次数 m 多项式增长。请注意，这种多项式增长至关重要，是进行后续大次数计算所必需的。

（2）在第 5 节中，我们使用基 $\mathcal{B}_m$ 构造映射 $\psi|_{V_m}$ 的变换矩阵 Ψ_m。随后，利用一种特殊形式的高斯消元，我们能够计算出 Ψ_m 的秩的下界。通过对 $m = 50$ 运行这些算法，我们在第 5.3 节中得到 $\ker\psi|_{V_{50}} = \{0\}$，从而证明了定理 3.3。此外，我们分析了这些算法，并证明矩阵构造与消元的时间和空间复杂度为 $\mathcal{O}(m^6)$。因此，通过提供更多的时间和空间，有可能提高 m 。

4. 构造商基

我们首先介绍一些关于 Gr¨obner 基和有限自动机的事实，以说明如何利用它们描述商 $\mathbb{C}\langle X\rangle/I$ 的基 $\mathcal{B}$。随后，我们将把这些结果应用于上一节中的空间 $V_m \subseteq \mathbb{C}\langle X_4\rangle/I_4$。需要注意的是，本节中的结果并非新成果，例如，Ufnarovski˘ı 曾在 [Ufn91] 中使用标记图来描述此类商的基。不过，为了方便起见，我们仍将这些结果重新陈述一遍。

4.1. 格罗布纳基。格罗布纳基将欧几里得除法推广到多变量多项式环中，例如可以用来解决理想成员问题。有关交换与非交换情形的详细介绍，请参见 [Mor94] 。下文中，用 X 表示一个有限生成元集。此外，令 $X^\star$ 为 $\mathbb{C}\langle X\rangle$ 中所有单项式（包括 1）组成的集合。在定义格罗布纳基之前，我们首先需要在 $X^\star$上定义一个良序。

定义 4.1（按次数的字典序）。设 $\le$ 是 X 上的一个良序。然后，可以通过首先比较两个

单项式的次数，将其扩展为 {v3} 上的一个良序。如果次数相同，则从左到右按字典序比较单项式。这种次序称为按次数的字典序。

下文中，我们在 X 上固定一个良序，并赋予 $X^\star$ 上一定义中所述的按次数的字典序。这使我们能够定义多项式的首项。

定义 4.2（首项）。设 $P \in \mathbb{C}\langle X\rangle$ 是一个非零多项式，它可以唯一地写成 $P = \sum_{i=1}^{n} \alpha_i x_i$，其中 a_1、……、 $\alpha_n \in \mathbb{C}\setminus\{0\}$ 以及 x_1、……、 $x_n \in X^\star$。则首项 LT(P) 是在该表示中相对于按次数的字典序最大的单项式 x_i 。在这种情况下，次数 $\deg P$ 由 LT(P) 的长度给出。

有了这些定义，我们现在可以引入 Gr¨obner 基。

定义 4.3（Gr¨obner 基）。设 $I \subseteq \mathbb{C}\langle X\rangle$ 是一个理想。若非零多项式的有限集 $G \subseteq I$ 满足：I 的首项恰好是那些可被 G 中某个首项整除的单项式，即

$$\{\mathrm{LT}(P) \mid P \in I,\ P \neq 0\} = \{a\,\mathrm{LT}(g)b \mid a, b \in X^\star, g \in G\}.$$

给定一个 Gröbner 基 $G \subseteq I$，下面的引理说明， $\mathbb{C}\langle X\rangle/I$ 的基可以用一种简单的方式描述。

引理 4.4。设 $I \subseteq \mathbb{C}\langle X\rangle$ 是一个理想， $G \subseteq I$ 是一个 Gröbner 基。那么，商 $\mathbb{C}\langle X\rangle/I$ 的一组基由以下剩余类构成

$$\mathcal{B} = X^\star \setminus \{a\,\mathrm{LT}(g)b \mid a, b \in X^\star, g \in G\}.$$

此外，以下剩余类

$$\mathcal{B}_m = \{P \in \mathcal{B} \mid \deg P \leq m\}$$

构成空间 $V_m \subseteq \mathbb{C}\langle X\rangle/I$ 的一组基，该空间由次数不超过 m 的多项式的剩余类组成。

证明。注意， $\mathcal{B}$ 中的元素线性无关，因为它们对应不同的单项式。此外，我们可以写成

$$\mathbb{C}\langle X\rangle = I \oplus \langle B\rangle,$$

其中 $\langle B\rangle$ 表示 $\mathcal{B}$的线性张成。结合 Gr¨obner 基的定义，参见 [Mor94 定理 1.3] ，即可证明这一结论。对 I取商后，我们立即得到 $\mathbb{C}\langle X\rangle/I \cong \langle B\rangle$ ，且B 的剩余类构成 $\mathbb{C}\langle X\rangle/I$的一组基。对于引理的第二部分，可以验证，若$P = P_1 + P_2$ 满足 $P_1 \in I$和 $P_2 \in \langle B\rangle$，则 deg $P_2 \leq$deg P，这意味着空间 V_m 由 $\mathcal{B}_m$的剩余类张成。□

4.2. 有限自动机。接下来，我们要用有限自动机的语言重新表述引理 4.4。有限自动机是理论计算机科学中的一项基础工具，可用于描述字母表上的词集。下面，我们先回顾语言和有限自动机的定义。关于语言和自动机的详细介绍，例如可参见 [HMU06]。

定义 4.5. 设 Σ 是一个由符号组成的有限集，称为字母表。Σ 上的词是由符号 $w_1, \ldots, w_n \in \Sigma$ 组成的有限序列 $w_1 \cdots w_n$。用 $\Sigma^\star$ 表示 Σ 的克莱尼闭包，即包含空词 ε 在内的所有 Σ 上的词的集合。于是，词集 $L \subseteq \Sigma^\star$ 称为语言。

注 4.6. 考虑非交换多项式代数 $\mathbb{C}\langle X\rangle$。变量集 X 可视为字母表。按照前面的记号，所有单项式构成的集合 $X^\star$ 与克莱尼闭包 $X^\star$ 一致，只要将空词 ε 与单位元 1 等同起来。

接下来，我们介绍有限自动机，它们可用于描述一类称为正则语言的特殊语言。

定义 4.7（有限自动机）。字母表 Σ上的有限自动机是一个有向标记图 $\Gamma = (V, E, \ell, s_0, F)$，其中

（1） V 表示顶点集， E 表示有向边集 .

（2） ℓ: $E \to \Sigma$ 为 E 中的每条边分配一个来自 Σ的符号。

（3） $s_0 \in V$ 是初始状态。（4） $F \subseteq V$ 是终态集。

注意，允许存在多重边，并且集合 F 可以为空。顶点也称为状态，边也称为转移。

定义 4.8。设 Γ 是字母表 Σ上的有限自动机。如果存在一条有向路径 $e_1, \ldots, e_n \in E$ 从初始状态 s_0 出发并以终态 $s \in F$结束，使得

$$w = \ell(e_1) \cdots \ell(e_n).$$

定义 4.9（正则语言）。如果存在一个在 Σ 上的有限自动机 Γ，使得语言 $L \subseteq \Sigma^\star$ 满足以下条件，则称其为正则语言：

$$L = \{w \in \Sigma^\star \mid \Gamma \text{ accepts } w\}.$$

在这种情况下，我们将其记为 $L = L(\Gamma)$，并称其为 Γ所接受的语言。

例4.10。图1展示了一个字母表为 $\Sigma = \{x, y, z\}$的有限自动机 Γ 。其初始状态 $s_0 = 1$ 用箭头标出，终态 $F = \{3\}$ 用圆圈标出。可以验证，它所接受的语言为

$$L(\Gamma) = \{w \in \Sigma^\star \mid w \text{ contains } xz \text{ as subword}\}.$$

请注意，在状态 1 和 3 处，标记为 x、 y 和 z 的多条边被画成一条边。

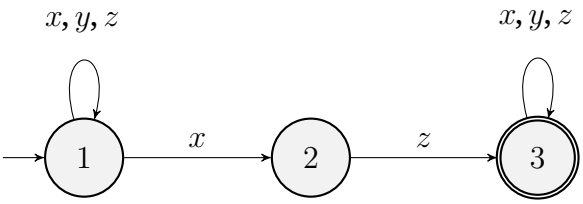


FIGURE 1. 一个具有 3 个状态的简单有限自动机。

利用前面对有限自动机和正则语言的定义，我们现在可以表述并证明以下引理。

引理 4.11. 设 Σ 为一个字母表，$S \subseteq \Sigma^\star$ 为一个有限的词集。则集合

$$\{w \in \Sigma^\star \mid w \textit{ contains no word from } S \textit{ as subword}\}$$

是一个正则语言。

证明。令 $s \in S$ 并定义集合

$$L_s = \{w \in \Sigma^\star \mid w \text{ contains } s \text{ as subword}\}.$$

由于可以仿照例4.10构造相应的有限自动机，因此这些都是正则语言。由于正则语言在并集和补集运算下封闭（参见 [HMU06，第 2]章），以下语言也仍是正则语言：

$$\Sigma^\star \setminus \bigcup_{s \in S} L_s = \{w \in \Sigma^\star \mid w \text{ contains no word from } S \text{ as subword}\}.$$

□

结合前一个引理与注 4.6，我们现在得到引理 4.4 的以下版本，它允许我们用有限自动机描述商基。

引理 4.12。设 $I \subseteq \mathbb{C}\langle X\rangle$ 是一个理想，且 G 是 I的一个 Gr ¨obner 基。那么存在一个以字母表 X 为字母表的有限自动机 Γ，使得接受语言 $L(\Gamma)$ 的剩余类构成 $\mathbb{C}\langle X\rangle/I$的一组基。

特别地，所有长度不超过 m 的被接受词的剩余类构成$V_m \subseteq \mathbb{C}\langle X\rangle/I$的一组基，其中 V_m 表示次数不超过 m的多项式的剩余类所构成的子空间。

证明。如注 4.6 所述，我们将单项式集合 $X^\star$ 视为字母表 X 上的词。定义 $S = \{\mathrm{LT}(g) \mid g \in G\}$。那么，引理 4.4 中的 $\mathcal{B}$ 可以写成

$$\mathcal{B} = \{w \in X^\star \mid w \text{ contains no word from } S \text{ as subword}\}.$$

利用引理 4.11 和正则语言的定义，我们得到一个有限自动机 Γ，使得 $L(\Gamma) = \mathcal{B}$ 的剩余类构成 $\mathbb{C}\langle X\rangle/I$ 的一组基。由于次数 $\deg w$ 对应于一个词 $w \in X^\star$ 的长度，我们进一步得到，引理 4.4 中的集合 $\mathcal{B}_m$ 由所有长度不超过 m 的接受词构成。□

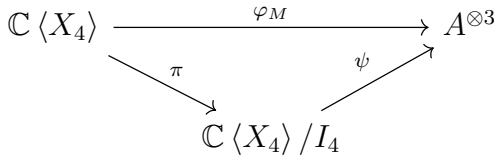
4.3. 计算结果。下面，我们介绍将引理 4.12 应用于魔幺正理想 I_4 所得到的结果。为了计算魔幺正理想 I_4 的 Gr¨obner 基 G，我们使用计算机代数系统 GAP [GAP20] 和软件包 GBNP [CK16] 。随后使用 SageMath [The20] 构造相应的有限自动机。具体方法如引理 4.11 的证明所述，通过计算较简单的有限自动机的并集与补集来完成[1]。此外，还可以简化所得有限自动机，并将其状态数降至最少。附录 A 中给出了 I_4 的最终有限自动机图。该自动机共有 17 个状态，且每个状态都是终态。此外，SageMath 还可以计算出，该自动机恰好包含 $(2m+1)^2$ 条长度为 m 的接受路径，这意味着有

$$\sum_{k=0}^{m}(2k+1)^2=\frac{1}{6}(2m+1)(2m+2)(2m+3)=\binom{2m+3}{3}$$

长度不超过 m 的接受路径。因此，我们得到 $\dim V_m=\Theta(m^3)$ 仅以关于 m 的多项式速度增长。除了理想 I_4 之外，我们还能够计算 Gr¨obner 基，并为魔幺正理想 I_5 和 I_6 构造有限自动机。所得有限自动机分别有 26 个和 37 个状态，并且包含长度为 m 的 $\Theta(6.854\ldots^m)$ 和 $\Theta(13.928\ldots^m)$ 条接受路径。因此，在这些情况下，V_m 的维数呈指数增长。

5. Matrix Construction and Elimination

下一节的目标是为第 3 节中的映射 $\psi|_{V_m}$ 构造变换矩阵 Ψ_m，并计算其秩的一个下界，以证明定理 3.3。回顾一下，映射 ψ 是通过将定义 2.4 中具体魔幻酉矩阵 M 的代入同态 φ_M 分解而得到的，如下所示。



在这里，A 是由两个投影生成的通用含单位 C^*-代数，I_4 是魔幺正理想，$V_m\subseteq\mathbb{C}\langle X_4\rangle/I_4$ 是次数不超过 m的多项式剩余类子空间。

5.1. 构造算法。为了构造映射 $\psi|_{V_m}$ 的变换矩阵，我们首先必须为其定义域和像选择一个基。在第 4 节中，我们构造了一个有限自动机，用来描述其定义域 $\psi|_{V_m}$ 的一个基 $\mathcal{B}_m$，

[1]我们的算法实现见 https://github.com/nfaross/model-s4plus

有关构造的详细信息，请参见引理 4.12；所得的自动机见附录 A。对于像的一个基，请考虑以下集合

$$\begin{aligned}\mathcal{A} &:= \{1, p, q, pq, qp, pqp, \ldots\} \subseteq A,\\ \mathcal{A}_m &:= \{a \in \mathcal{A} \mid a \text{ has at most } m \text{ factors}\} \subseteq A,\\ \mathcal{A}_m^{\otimes k} &:= \{a_1 \otimes \cdots \otimes a_k \mid a_1, \ldots, a_n \in \mathcal{A}_m\} \subseteq A^{\otimes k}.\end{aligned}$$

下一个引理表明，$\psi|_{V_m}$ 的像包含于$\mathcal{A}_m^{\otimes 3}$的线性张成中，因此可将后者选作一组基。

引理 5.1. 沿用前文的记号，$\mathcal{A}_m^{\otimes k}$中的元素线性无关，且 $\psi(V_m) \subseteq \langle \mathcal{A}_m^{\otimes 3} \rangle$。特别地，$\dim \psi(V_m) \leq (2m+1)^3$。

证明。由于 p 和 q 是泛投影，$\mathcal{A}$ 中的元素线性无关，这也意味着集合 $\mathcal{A}_m$ 和 $\mathcal{A}_m^{\otimes k}$线性无关。此外，若 $a \in \mathcal{A}_m^{\otimes k}$ 且 $b \in \mathcal{A}_n^{\otimes k}$，则$ab \in \mathcal{A}_{m+n}^{\otimes k}$。因此，若 $P \in \mathbb{C}\langle X_4 \rangle$ 是次数为 m的多项式，则 $P(M) \in \langle A_m^{\otimes 3} \rangle$，因为魔法酉矩阵$M$的各个元素都包含于 $\langle \mathcal{A}_1^{\otimes 3} \rangle$中。因此，$\psi(V_m) \subseteq \langle \mathcal{A}_m^{\otimes 3} \rangle$。此外，我们有 $|\mathcal{A}_m| = 2m+1$，这意味着 $\dim \psi(V_m) \leq |A_m^{\otimes 3}| = (2m+1)^3$。□

现在，可以使用算法 1 构造映射 $\psi|_{V_m}$ 关于基 $\mathcal{B}_m$ 的变换矩阵 Ψ_m。基 $\mathcal{B}_m$ 由附录 A 中的有限自动机Γ 描述，另一个基为上一段中的基 $\mathcal{A}_m^{\otimes 3}$。正确性的证明见下一个引理。

算法 1 矩阵构造

输入：次数 m
输出：矩阵 Ψ_m

初始化空矩阵 Ψ_m
初始化队列 Q，其中包含 $(s_0, 1 \otimes 1 \otimes 1, 0)$
当 Q 不为空时执行
    从 Q 中移除 (s, P, k)
    将对应于 P 的列插入 Ψ_m
    如果 $k < m$，则
        对 Γ 中所有标签为 x_{ij} 的转移 $s \to s'$ 执行
            $P' \leftarrow P \cdot (M)_{ij}$
            将 $(s'、\ P'、\ k+1)$ 插入 Q

引理 5.2。在前述记号下，算法 1 构造了映射 $\psi|_{V_m}$ 相对于基 $\mathcal{B}_m$ 和 $\mathcal{A}_m^{\otimes 3}$ 的变换矩阵 Ψ_m。

Proof. 为了构造变换矩阵 Ψ_m，我们必须计算 te

$$\psi(\pi(x)) = \varphi_M(x) = \prod_{\ell=1}^{k} \varphi_M(x_{i_\ell j_\ell}) = \prod_{\ell=1}^{k} M_{i_\ell j_\ell}$$

基 $\mathcal{B}_m$中的每个单项式 $x = x_{i_1j_1}x_{i_1j_1}\cdots x_{i_kj_k}$。每个乘积在相对于 $\mathcal{A}_m^{\otimes 3}$表示时，都对应于 Ψ_m 中的一列。为此，我们遍历附录 A 中有限自动机 Γ 中长度不超过 m 的所有路径，以生成所有基元素 $x \in \mathcal{B}_m$。由于 Γ 中的每个状态都是终态，因此每条路径恰好对应一个元素 $x \in \mathcal{B}_m$。此外，我们在生成路径时直接将相应的 M_{ij} 相乘，从而在同一步中得到 Ψ_m的各列。

更具体地说，算法 1 维护一个路径队列，并以广度优先搜索的方式遍历有限自动机。在队列中，每条路径用三元组 (s, P, k) 表示，其中 s 是路径的最后一个节点，$P \in \langle \mathcal{A}^{\otimes 3} \rangle$ 是沿路径计算得到的多项式，k 是路径的长度。算法从三元组 $(s_0, 1 \otimes 1 \otimes 1, 0)$ 开始，并在每一步中从队列中取出下一条路径，将相应的列插入 Ψ_m。然后考虑从s 到 s'、标签为 x_{ij}的所有出边转移，并将新的路径 $(s', P', k+1)$ 加入队列。这些新路径沿转移 $s \to s'$ 扩展当前路径，并包含相应的多项式 $P' = P \cdot (M)_{ij}$。这样，所有长度不超过 m 的路径都会生成，相应的列也会被插入。□

5.2. 消元算法。我们的下一个目标是计算 Ψ_m 的秩，以证明定理 3.3。不过，为了高效地完成这一计算，我们必须将矩阵 Ψ_m 存储为一对映射 $\Psi_m = (rows, columns)$，其中行和列是映射，满足

(1) rows$(i) = \{j_1, \ldots, j_{n_i}\}$是第 i 行中的非零列 $j_1, \ldots, j_{n_i}$ 的集合；(2) columns$(j) = \{i_1, \ldots, i_{m_j}\}$是第 j 列中的非零行 $i_1, \ldots, i_{m_j}$ 的集合。

采用这种矩阵格式后，算法 2 现在可以计算 Ψ_m 的秩的下界。其正确性将在下面的引理中证明。

引理 5.3。算法 2 计算矩阵 Ψ_m 的秩的下界。

证明。算法 2 执行一种特殊形式的高斯消元，并通过初等行变换对 Ψ_m 进行变换。它搜索只在某一列 j 中含有一个非零项的行 i。接着，消去其他行 $k \neq i$ 中位于第 j 列的所有项。如果这样的行 k 此时只剩下一个非零项，就将其推入栈中，以便接下来处理。每个只有一个非零项的行都与其他所有行线性无关。因此，这类行的总数是矩阵 Ψ_m 的秩的下界。注意，被推入栈中的行可能在处理之前就已被消去。在这种情况下，该行可以表示为其他行的线性组合，因此不会对矩阵的秩作出贡献。□

5.3. 定理 3.3 的证明。利用算法 2，我们终于可以证明定理 3.3：对于定义 2.4 中的具体魔幻酉矩阵 M，不存在次数不超过 50 的分离多项式。

算法 2 矩阵消元

输入：稀疏 $n_r \times n_c$ 矩阵 $\Psi_m =$ （行，列）
输出： Ψ_m的秩的下界

```
秩 ← 0
初始化空栈 S
对于 i = 1, ····· , n_r do
    如果 |行(i)| = 1 则
        将 i 推入 S
当 S 不为空时执行
    从 S中移除 i
    如果 |行(i)| = 1 则
        {j} ← 行(i)
        对于 k ∈列(j) 执行
            如果 k ≠ i 则
                从行(k)中删除 j
                如果 |行(k)| = 1 则
                    将 k 推送到 S
        列（j） ← {i}
        秩 ← 秩 + 1
```

定理 3.3 的证明。运行算法 [1], 后，我们得到 Ψ_{50} 的秩下界为 176851，该数也等于列数（参见第 4.3 节）。由于列数就是像的维数，因此 Ψ_{50} 的核为零维。由第 3 节中的论证可知，该具体魔幻酉矩阵不存在分离多项式。□

5.4. 复杂度。在下文中，我们分析算法 1 和算法 2，并证明二者的复杂度均为 $\mathcal{O}(m^6)$。注意，我们固定有限自动机Γ ，仅改变次数 m。此外，我们假设映射支持在 $\mathcal{O}(1)$ 时间内进行插入和删除；使用哈希映射实现时，通常近似满足这一条件。

在介绍算法之前，我们首先需要考虑 $\langle A_m^{\otimes 3} \rangle$ 中的算术运算。注意，元素 $a \in \mathcal{A}_m$ 由其长度和奇偶性唯一确定。因此，元素 $a \in A_m^{\otimes 3}$ 可以用常数空间存储，两个元素 a、$b \in A_m^{\otimes 3}$ 可以在常数时间内相乘。对于元素 $a \in \langle A_m^{\otimes 3} \rangle$ ，用 $|a|$ 表示其相对于基 $A_m^{\otimes 3}$ 表示时的非零系数个数。于是，可以使用一个映射为 a 分配 $\mathcal{O}(|a|)$ 的空间，该映射为每个基元素存储相应的系数。此外，通过两两相乘所有基元素，我们可以在 $\mathcal{O}(|a| \cdot |b|)$ 时间内计算两个元素 a、$b \in \langle A_m^{\otimes 3} \rangle$ 的 ab。考虑到这些因素，现在我们可以分析主要算法了。

[1]我们算法的实现可在 https://github.com/nfaross/model-s4plus 找到

引理 5.4. 算法 1 和算法 2 的复杂度为 $\mathcal{O}(m^6)$。

证明。首先，考虑算法 1。由于队列支持所有操作均在常数时间内完成，其运行时间由多项式乘法和向 Ψ_m 中插入行所需的总时间决定。由于 M_3 的各项均为常数，我们可以在 $\mathcal{O}(|P|)$ 时间内计算 $P' = P\cdot(M_3)_{ij}$。此外，利用前面描述的矩阵格式，可以在 $\mathcal{O}(|P|)$ 时间内将多项式 P 插入 Ψ_m。因此，算法 1 需要 $\mathcal{O}(N)$ 的时间和空间，其中

$$N = \sum_{P \text{ computed}} |P| = \sum_{x\in\mathcal{B}_m} |\varphi_M(x)|$$

表示矩阵 Ψ_m 中非零项的数量。现在考虑算法 2。由于栈支持所有操作均在 $\mathcal{O}(1)$ 时间内完成，并且 Ψ_m 的每个 $\mathcal{O}(N)$ 非零项至多被删除一次，且删除操作耗时为常数，因此算法 2 需要 $\mathcal{O}(N)$ 时间。因此，接下来只需给出 Ψ_m 中非零项数量 N 的上界。根据引理 5.1，我们知道 Ψ_m 至多有 $|\mathcal{A}_m^{\otimes 3}| = (2m+1)^3$ 行。另一方面，列数由 $|\mathcal{B}_m|$ 给出，其已在第 4.3 节中计算。因此，Ψ_m 至多有

$$N \le (2m+1)^3 \cdot \binom{2m+3}{3} = \mathcal{O}(m^6)$$

非零项。 □

6. Concluding remarks

下面，我们将主要结果置于量子置换群的 C^*-代数模型背景下，并讨论为什么定义 2.4 中的具体魔幻酉矩阵 M 可能定义 S_4^+的忠实模型。在本节中，仍记 A 为由两个投影生成的普适含幺 C^*-代数，记B 为由具体魔幻酉矩阵 M的各项生成的 C^*-代数。

6.1. 关于 M 是忠实模型的提示。我们从定理 3.3 的一个直接推论开始。

推论 6.1. 设 u 为包含 $C(S_4^+)$ 的生成元的矩阵，设$P \in \mathbb{C}\langle X_4\rangle$ 为满足 deg $P \le 50$的多项式。那么，$P(M) = 0$ 当且仅当$P(u) = 0$。

证明。设 $P \in \mathbb{C}\langle X_4\rangle$ 为满足 deg $P \le 50$的多项式。由于 $C(S_4^+)$ 是由 4×4 魔法酉矩阵的各项生成的普适 C^*-代数，因此存在一个 $*$-同态 $\Phi\colon C(S_4^+) \to B, u_{ij} \mapsto M_{ij}$。因此，如果 $P(u) = 0$，则

$$P(M) = P(\Phi(u)) = \Phi(P(u)) = \Phi(0) = 0.$$

另一方面，如果 $P(M) = 0$，那么根据定理 3.3，$P \in I_4$。然而，根据 $C(S_4^+)$ 的定义和命题 2.3，我们有：对于每个 $P \in I_4$，$P(u) = 0$。□

由于 50 对于非交换多项式的次数而言是一个相当大的界，我们猜想前面的推论对于任意次数的多项式都成立。特别是，界 50 源于有限的计算能力，没有直接的理由表明定理 3.3 的情形会在 $m > 50$ 时发生改变。还要回顾一下，对于最初的问题 2.5，我们确实有一个次数为 1 的多项式 p_1 和一个次数为 2 的多项式 p_2。因此，一个多项式 p_3 需要大于 50 的次数似乎是不合理的。此外，前面的推论还表明了更强的结论，即定义 2.4 中的具体魔幻酉矩阵 M 定义了一个关于 S_n^+ 的忠实模型，也就是说，通过 $u_{ij} \mapsto M_{ij}$，$C(S_n^+) \cong B$。在这种情况下，可以将 $C(S_n)$ 作为 B 的商得到，因为 $C(S_4)$ 是 $C(S_4^+)$ 的阿贝尔化。下面的命题表明，这一必要条件确实成立。

命题 6.2。在前述记号下，$\operatorname{Spec} B \cong S_4$。特别地，$C(S_4)$ 是 B 的商。

证明。设 $\varphi \in \operatorname{Spec} B$ 是一个特征。于是，φ 由魔法酉矩阵 $\varphi(M) \in M_4(\mathbb{C})$ 唯一确定，而该矩阵是一个置换矩阵。因此，只需证明通过一个特征可以得到每个置换矩阵。令 $p_1, q_1, \ldots, p_3, q_3 \in \{0, 1\}$。由于 A 是由两个投影生成的泛 C^*-代数，存在一个 $*$-同态 $\varphi\colon A^{\otimes 3} \to \mathbb{C}$，它将第 i 个张量因子中的 p 映射到 p_i，并将第 i 个张量因子中的 q 映射到 q_i。将 φ 限制到 $B \subseteq A^{\otimes 3}$，我们得到一个特征$\varphi|_B \in \operatorname{Spec} B$。附录 B 随后说明，如何通过适当选择 $p_1, q_1, \ldots, p_3, q_3$ 来得到每个置换矩阵。因此，$\operatorname{Spec} B \cong S_4$，由 Gelfand-Naimark 定理，我们得到一个满射 $*$-同态 $\Phi\colon B \to C(S_4)$。于是，$C(S_4) \cong B/\ker \Phi$，这就证明了该陈述的第二部分。□

请注意，附录 B 表明，在命题 6.2 的证明中，可以通过将 p_0 置为零来构造每个置换矩阵。因此，可以在定义 2.4 中的具体魔幻酉矩阵 M 的各项中，将 $p = 0$ 设在第一个张量因子上，从而得到 S_4^+ 的一个稍简单且具有全谱的模型。

6.2. 关于 S_n^+ 的进一步结果。首先，回顾一下，如果存在一个单射的 $*$-同态，则称 $*$-代数 A 是剩余有限维的

$$\pi\colon A \to \prod_{i \in I} M_{n_i}(\mathbb{C})$$

嵌入矩阵代数的乘积中，其中 I 是任意的（可能是无限的）指标集。在 [BCF 20], Brannan、Chirvasitu 和 Freslon 证明了，与 S_n^+ 对应的 $*$-代数 A 是剩余有限维的。因此，对于生成元 $C(S_n^+)$ 中的每个 $*$-多项式$P \neq 0$，都存在一个 $*$-同态 $\pi_i\colon A \to M_{n_i}(\mathbb{C})$，使得 $\pi_i(P) \neq 0$，其中 π_i 是通过投影到某个取决于 p 的 i 个而得到的。对于 S_4^+ 的可能模型，这在一定程度上提供了一些信息。

其次，要证明定义 2.4 中的具体魔幻酉矩阵 M 给出了 S_4^+ 的忠实模型，一种可能的方法是证明 M 是某个紧量子群 G 的余表示矩阵，且具有 $B \subseteq C(G)$。在这种情况下， $C(G)$ 的余乘法限制在 B 上成为一个余乘法，从而将 B 变成一个具有 $S_4 \subseteq H \subseteq S_4^+$ 的紧矩阵量子群 H。由于包含 $S_4 \subseteq S_4^+$ 是极大的（见 [BB09]），且 B 是非交换的，因此可以推出 $H = S_4^+$。

注意，C^*-代数 A 对应于紧量子群 $\mathbb{Z}_2 * \mathbb{Z}_2$，其余乘法 $\Delta\colon A \to A \otimes A$ 定义为

$$\Delta(p) = p \otimes p + (1-p) \otimes (1-p),$$
$$\Delta(q) = q \otimes q + (1-q) \otimes (1-q).$$

因此，张量积 $A^{\otimes 3}$ 已经带有直接积量子群结构。然而，似乎必须找到一种不同的积结构，才能将 M 变成余表示矩阵，但作者未能实现这一点。

第三，还有其他关于 S_n^+的模型，例如在 [BM07], [BBS09], [BB15] 和 [BN17] 中进行了研究。然而，这些模型属于不同类型，由泡利矩阵、傅里叶矩阵或某些相关构造建立。在 [BM07], 的情况下， $n = 4$ 的相应模型结果是忠实的（见[BC 08]）。

6.3. 不推广至 S_n^+与 $n > 4$。最后，我们考察量子置换群 S_n^+与 $n > 4$ 的类似模型，并证明在这一背景下，我们主要结果的推广不再成立。下文中，仍记 A 为由两个投影 p 和 q生成的泛单位 C^*-代数。此外，回顾第 5 节中集合 $\mathcal{A}_m^{\otimes k} \subseteq A^{\otimes k}$ 的定义，这些集合由 p和 q 的交替乘积的张量积组成，且长度至多为 m。在此记号下，我们得到如下结果。

命题 6.3。设 $n \in \{5, 6\}$ 和 k、$\ell \in \mathbb{N}$。若 $M \in M_n(A^{\otimes k})$ 是一个条目为 $M_{ij} \in \left\langle \mathcal{A}_\ell^{\otimes k} \right\rangle$的魔法酉矩阵，则存在一个关于 M的分离多项式。

证明。与主要定理的证明一样，我们将代入同态 φ_M 分解为

$$\begin{array}{ccc} \mathbb{C}\langle X_n \rangle & \xrightarrow{\quad\varphi_M\quad} & A^{\otimes k} \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\psi} & \\ & \mathbb{C}\langle X_n \rangle / I_n & \end{array}$$

并考虑 $\psi|_{V_m}$对次数不超过 m的多项式剩余类 $V_m \subseteq \mathbb{C}\langle X_n \rangle / I_n$空间的限制。根据第 4.3 节中的计算结果，我们有，对于 $n \in \{5, 6\}$， V_m 的维数在 m中呈指数增长。然而，可以证明

类似于引理 5.1，dim $\psi(V_m) \leq (2m+1)^{kl}$。因此，当 m较大时，dim $V_m > \dim \psi(V_m)$，这意味着 dim ker $\psi > 0$。于是，我们在 ker ψ 中找到一个非平凡分离多项式的剩余类。□

请注意，我们只能计算具有 $n \leq 6$ 的魔法酉矩阵理想I_n 的 Gr¨obner 基，这使我们能够证明在这些情况下 dim V_m 呈指数增长。然而，对于更大的 n，dim V_m 应增长得更快，因此我们预计前一个命题对所有 $n > 4$ 都成立。此外，前面的维数论证表明，量子置换群 S_4^+ 比具有 $n > 4$ 的更大量子置换群 S_n^+ 更简单。将此与 [Ban98], 进行比较，后者表明 S_4^+ 的对偶群是可和的，但对于具有 $n > 4$ 的 S_n^+而言则不是可和的，这也说明 S_4^+ 相对更简单。

References

[Ban98] T. Banica。《一般余作用的对称性》。《数学年刊》，314:763–780，1998。[BB09] T. Banica 和 J. Bichon。《作用于4个点上的量子群》。《纯粹与应用数学杂志》，626:75–114，2009。[BB15] T. Banica 和 J. Bichon。《线性量子群的随机游走问题》。《国际数学研究通知》，2015(24):13406–13436，2015。[BBS09] T. Banica、J. Bichon 和 J. Schlenker。《量子置换代数的表示》。《泛函分析杂志》，257(9):2864–2910，2009。[BC08] T. Banica 和 B. Collins。《泡利量子群上的积分》。《几何与物理学杂志》，58(8):942–961，2008。[BCF20] M. Brannan、A. Chirvasitu 和 A. Freslon。《量子反射群的拓扑生成与矩阵模型》。《数学进展》，363:106982，2020。[Bla05] B. Blackadar。《算子代数：C*-代数与冯·诺伊曼代数理论》。《Springer》，2005。[BM07] T. Banica 和 S. Moroianu。《量子置换群的结构》。《美国数学学会会刊》，135(1):21–29，2007。[BN17] T. Banica 和 I. Nechita。《量子置换群的平坦矩阵模型》。《应用数学进展》，83:24–46，2017。[CK16] A. Cohen 和 J. Knopper。《GBNP：非交换多项式的 Gröbner 基计算》，1.0.3版。
https://www.gap-system.org/Packages/gbnp.html，2016。[GAP20] GAP小组。《GAP——群、算法与程序》，4.11.0版，2020。https://www.gap-system.org。[HMU06] J. E. Hopcroft、R. Motwani 和 J. D. Ullman。《自动机理论、语言与计算导论》（第3版）。Addison-Wesley Longman Publishing Co., Inc.，2006。[JW20] S. Jung 和 M. Weber。《量子置换模型》。《泛函分析杂志》，279(2):108516，2020。[LES+22] V. Levandovskyy、C. Eder、A. Steenpass、S. Schmidt、J. Schanz 和 M. Weber。《最多含七个顶点的图的量子对称性存在性：一种基于计算机的方法》。《ISSAC '22：2022年符号与代数计算国际研讨会论文集》，311–318页，2022。[LVW20] X. Li、C. Voigt 和 M. Weber。《ISem24：C*-代数与动力学，讲义》。
https://www.math.uni-sb.de/ag/speicher/weber/ISem24/ISem24LectureNotes.pdf，2020。

[Mor94] T. Mora。《交换与非交换 Gröbner 基简介》。《理论计算机科学》，134(1):131–173，1994。[NT13] S. Neshveyev 和 L. Tuset。《紧量子群及其表示范畴》。《专门课程》。法国数学学会，2013。[The20] Sage 开发团队。《SageMath，即 Sage 数学软件系统》（9.1版），2020。https://www.sagemath.org。[Tim08] T. Timmermann。《量子群与对偶性导论：从 Hopf 代数到乘法酉元及其他》。《数学教材》。欧洲数学学会，2008。[Ufn91] V. Ufnarovskiı。《利用图计算结合代数的基、增长与希尔伯特级数》。《〈苏联数学汇刊〉》，68(2):417–428，1991。[Wan98] S. Wang。《有限空间的量子对称群》。《数学物理通讯》，195:195–211，1998。[Web23]M. Weber。《量子置换矩阵》。《复分析与算子理论》，17:37，2023。[Wor87]S. Woronowicz。《紧矩阵伪群》。《数学物理通讯》，111:613–665，1987。

AppendixA. Finite automaton

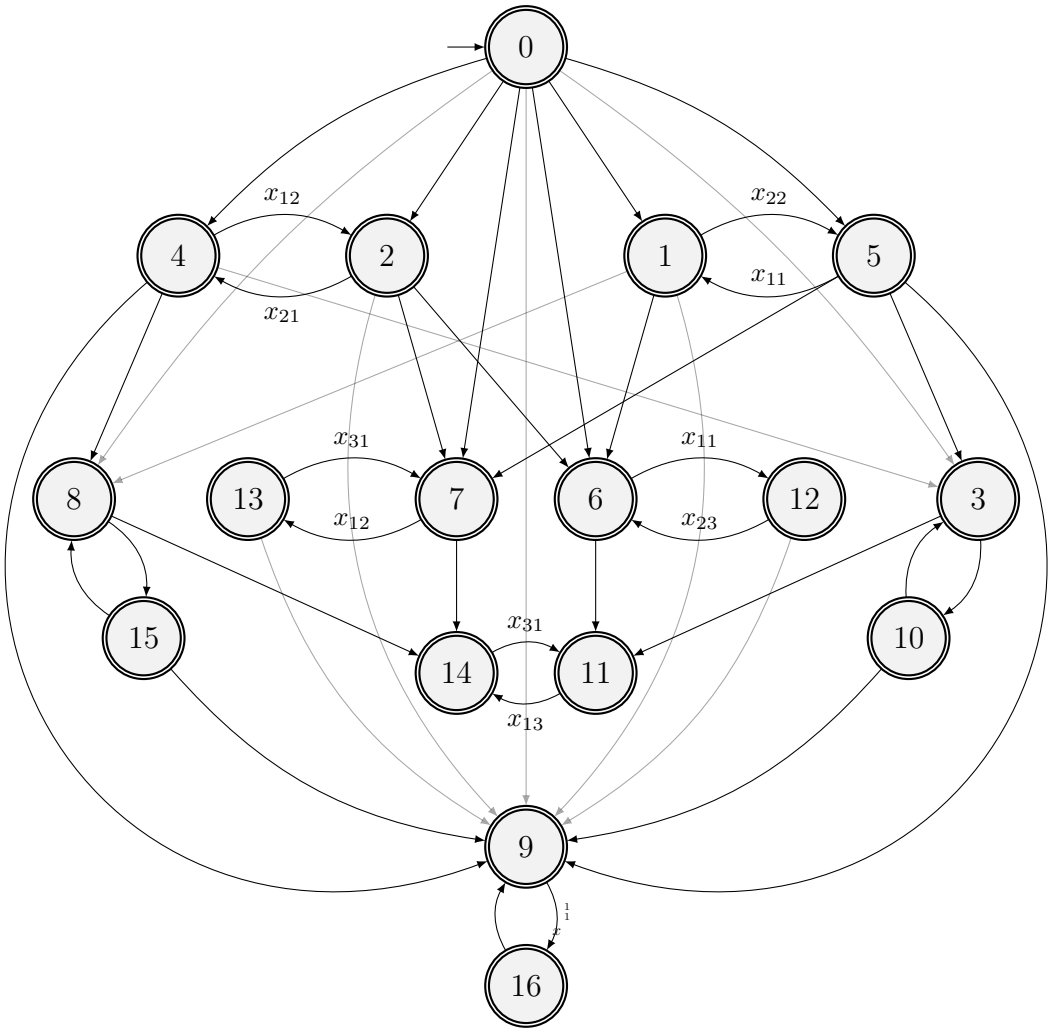


Figure 2. 第 4 节中为魔幺正理想 I_4 构造的有限自动机。它有 17 个状态，其中状态 0 是初始状态，且每个状态都是终态。灰色边仅以不同颜色标示，以便更清楚地展示。

AppendixB. Characters from Proposition 6.2

S_4	p_1	q_1	p_2	q_2	p_3	q_3
$()$	0	1	0	1	0	1
(13)(24)	0	1	0	1	1	0
(14)(23)	0	1	1	0	0	1
(12)(34)	0	1	1	0	1	0
(234)	0	0	1	1	0	1
(132)	0	0	1	1	1	0
(143)	0	0	0	0	0	1
(124)	0	1	0	0	0	0
(243)	0	0	0	1	0	0
(134)	0	0	0	1	1	1
(142)	0	0	1	0	1	1
(123)	0	0	1	0	0	0
(34)	0	0	0	1	0	1
(1324)	0	0	0	1	1	0
(1423)	0	0	1	0	0	1
(12)	0	0	1	0	1	0
(23)	0	0	1	1	0	0
(1342)	0	0	1	1	1	1
(14)	0	1	0	0	0	1
(1243)	0	0	0	0	0	0
(24)	0	1	0	1	0	0
(13)	0	1	0	1	1	1
(1432)	0	1	1	0	1	1
(1234)	0	1	1	0	0	0

Nicolas Faross and Moritz Weber, Saarland University, Fachbereich Mathe-matik, Postfach 151150, 66041 Saarbrücken, Germany电子邮箱地址：faross@math.uni-sb.de, weber@math.uni-sb.de