密级:_____

中国科学院大学
University of Chinese Academy of Sciences

# 硕士学位论文

## 矩阵乘法的群论方法


作者姓名：齐嘉悦

指导教师：高小山 研究员

中国科学院数学与系统科学研究院


学位类别：理学硕士

学科专业：应用数学

研究所：中国科学院数学与系统科学研究院

2017 年 5 月

# The Group-theoretical Method of Matrix Multiplication

**By**

**Jiayue Qi**

**A Dissertation Submitted to**

**The University of Chinese Academy of Sciences**

**In partial fulfillment of the requirement**

**For the degree of**

**Master of Applied Mathematics**

Academy of Mathematics and Systems Science, Chinese Academy of Sciences

**May, 2017**

# 摘　　要

矩阵乘法的算法复杂度分析是计算理论中一个重要问题。我们首先介绍了这一方面的开创性工作—Strassen 算法；接下来介绍了矩阵乘法的群论方法和其中的一些重要的概念、相关性质以及两个可以推出$\omega = 2$ 的猜想，给出了一些具体群的已有构造验证和新的构造并由新构造推导出一个$\omega$ 的非平凡上界，然后介绍了搜索极大三乘积组的蚁群算法；接下来介绍$5 \times 5$ 小矩阵乘法的群理论方法并研究了$6 \times 6$ 小矩阵乘法的群论方法；最后研究了一种特定情形下三乘积组的构造原则及其在两个群结构上的具体应用。

本论文的主要结果总结如下：一是针对已有的例子（具体群结构及其三乘积组）进行扩充构建得出一些新的同时二乘积组或三乘积组，并由扩充构建的例子推导出一个$\omega$ 的非平凡上界$\omega < 2.9262$。二是证明了群的西罗子群组的三乘积性质和二乘积性质。三是在$6 \times 6$ 小矩阵乘法群理论方法的研究中，提出了若干群的$\langle 6, 6, 6\rangle$ 三乘积性质的必要条件，从而较大地缩减了问题的搜索空间。四是针对几个具体群给出了它们的三乘积组具体结构：构造证明了4 阶偶置换群$A_4$ 的$\langle 3, 3, 2\rangle$ 三乘积性质，给出并证明了该群的三乘积容量的确切值，然后由此结论抽象构造了群$C_6 \times A_4$ 的$\langle 6, 3, 3\rangle$ 三乘积组（这里$C_6$ 是6 阶循环群），接着给出了该抽象形式的一个具体解；构造证明了群$C_3 \times A_4$ 的$\langle 6, 4, 3\rangle$ 三乘积组（这里$C_3$ 是3阶循环群）。五是从理论上探讨了抽象群$B$的三乘积性质与群$C_2 \times B$、$C_3 \times B$和$C_n \times B$ 的三乘积性质之间的联系并将理论成果应用于两个具体群的$\langle 6, 6, 6\rangle$ 三乘积性质的研究（这里$C_2$ 是2 阶循环群），得到了有关$1 \times B$ 与$2 \times B$ 在群$C_2 \times B$的$\langle 6, 6, 6\rangle$ 三乘积组中具体分布的一些结论（这里$1, 2 \in C_2$ 且1 是其中的单位元）。

**关键词：** 矩阵乘法算法计算复杂度，矩阵乘法的群论方法，小矩阵乘法的群论方法，三乘积性质

## Abstract

Complexity analysis of matrix multiplication is a vital problem in computational theory. We introduce the pioneering work in the complexity of matrix multiplication—Strassen's algorithm. Also we introduce the concept of matrix multiplication exponent. Then we introduce the group theoretical method of matrix multiplication and construct some new group examples, from one of which we get a new non-trivial upper bound for $\omega$. Next we introduce ant colony for TPP(Triple Product Property) triples to fast matrix multiplication. Besides, we introduce the group theoretical method for $5 \times 5$ matrix multiplication and consider on the group theoretical method for $6 \times 6$ matrix multiplication. In the last section we study on the principal for constructing TPP triples under a certain situation and also the application of those principals to two specific groups.

This paper mainly contains five aspects of innovative results: First, we construct some new simultaneous double product property two-tuples and TPP triples, deduce a non-trivial upper bound for $\omega$–$\omega < 2.9262$. Second we study the triple product property and double product property of the Sylow subgroups of a group in general. Third, in the study of $6 \times 6$ matrix multiplication, we prove some necessary conditions for the $\langle 6, 6, 6\rangle$ triple product property, which to a great degree reduce the search space of the problem. Fourth, we give some concrete structures of several groups: we prove the $\langle 3, 3, 2\rangle$ triple product property of the 4 order alternating group $A_4$ via a concrete construction, give and prove the specific TPP capacity of this group. Following this result, we construct abstractly the $\langle 6, 3, 3\rangle$ TPP triples of the group $C_6 \times A_4$, where $C_6$ represents the 6 order cyclic group. And then we present a concrete solution of the $\langle 6, 3, 3\rangle$ TPP triples of the group $C_6 \times A_4$. Besides, we construct and prove the $\langle 6, 4, 3\rangle$ triple product property of the group $C_3 \times A_4$ via a concrete TPP triple, where $C_6$ represents 6 order cyclic group and $C_3$ represents the 3 order cyclic group. Fifth, we investigate the relations between the triple product property of an abstract group $B$ and the group $C_n \times B$ (but mainly$C_2 \times B$), after which we apply the principles

into two specific groups and obtain some conclusions on the concrete distribution of two sets—$1 \times B$ and $2 \times B$ in the $\langle 6, 6, 6\rangle$ TPP triples of group $C_2 \times B$, where $C_2$ denotes 2 order cyclic group and W.L.O.G we assume $C_2 = \{1, 2\}$.

**Keywords:** the complexity of matrix multiplication, the group-theoretical method of matrix multiplication, the group-theoretical method of small matrix multiplication, triple product property(TPP)

# 目　　录

# 第一章　引言

## 1.1　矩阵乘法指数

矩阵乘法的一般定义如下：如果$\mathbf{A}$是$n \times m$矩阵，$\mathbf{B}$ 是$m \times p$ 矩阵，

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12}... & a_{1m} \\ a_{21} & a_{22}... & a_{2m} \\ ... & & \\ a_{n1} & a_{n2}... & a_{nm} \end{pmatrix} \tag{1.1}$$

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12}... & b_{1p} \\ b_{21} & b_{22}... & b_{2p} \\ ... & & \\ b_{m1} & b_{m2}... & b_{mp} \end{pmatrix} \tag{1.2}$$

该矩阵积$\mathbf{AB}$被定义为$n \times p$ 矩阵

$$\mathbf{AB} = \begin{pmatrix} c_{11} & c_{12}... & c_{1p} \\ c_{21} & c_{22}... & c_{2p} \\ ... & & \\ c_{n1} & c_{n2}... & c_{np} \end{pmatrix} \tag{1.3}$$

即，

$$(\mathbf{AB})_{ij} = \sum_{k=1}^{m} A_{ik} B_{kj}. \tag{1.4}$$

因为矩阵乘法在许多数值算法中处于基础地位，在矩阵乘法上的微小改进都会使得整个算法或工程效率大大提高，所以存在大量工作试图改进传统的矩阵乘法算法以降低其算法复杂度。

当我们计算域上的两个$n \times n$矩阵$A, B$的乘积时，定义$C(n)$是计算该乘积所需最小的算术操作数。下面给出矩阵乘法指数的定义：

**定义 1.1** (矩阵乘法指数$\omega$). $\omega = inf\{\alpha | C(n) \leq n^{\alpha}$对所有足够大的$n$都成立$\}$。

**注 1.** 不太正式地讲，$\omega$是满足条件“对任意$\varepsilon > 0$，两个$n \times n$矩阵乘积都可以在$O(n^{\omega+\varepsilon})$ 步算术操作内计算出来”的最小值。

为引出$\omega$在域上的一些性质，接下来给出域上$\omega$的定义。对一个给定的域$K$，$K$上的矩阵乘法指数$\omega(K)$是如下定义的：

**定义 1.2** (矩阵乘法复杂度指数$\omega$，[1]1.2节). $\omega(K) := inf\{h \in \mathbb{R}^{+} | M_K(n) = O(n^h), n \to \infty\}$，这里$M_K(n)$是$K$上的两个$n \times n$矩阵相乘所需要的非除算术操作$\{+, -, \times\}$的总数目。

**定理 1.1** ([2]第383页). *矩阵乘法指数在标量扩张下保持不变：若$k \subset K$ 是一个域扩张，那么$\omega(k) = \omega(K)$。*

**定理 1.2** ([3]). *$\omega(K)$只与域$K$的特征值有关。*

**注 2.** 也就是说若$char(K) = 0$，则$\omega(K) = \omega(\mathbb{Q})$，否则$\omega(K) = \omega(\mathbb{Z}_p)$，这里$\mathbb{Z}_p$是特征为素数$p$的有限域。

我们在用传统算法将两个$n \times n$的矩阵相乘时，要用到$n^3$步乘法和$n^3 - n^2$步加法，则可推出$M_K(n) = 2n^3 - n^2 < 2n^3 = O(n^3)$，即对常数$C' = 2$，有$M_K(n) < C'n^3$，这就推出了$\omega$ 的一个上界3([2]，p.375)。至于下界，我们注意到由于矩阵乘法的乘积是一个$n \times n$的矩阵，有$n^2$ 个元素，因此我们需要的操作数至少应为$n^2$的某个常数倍，记该常数为$C$，则当$n$充分大时，有$M_K(n) \geq C \cdot n^2$，此等式即可推出$\omega$ 的一个下界2。若能证明$\omega = 2$，则可推出对任意$n$，有$Cn^2 < M_K(n) < C'n^2$，这里$C', C > 1$ 是独立于$n$ 的常量。

**定理 1.3** ([1]定理2). *对任一个域$K$，都有：（1）$2 \leq \omega \leq 3$；（2）$\omega(K) = h \in [2, 3]$当且仅当$C \cdot n^2 \leq M_K(n) = O(n^h)$，这里$h$取到最小值。*

## 1.2 Strassen算法

在矩阵乘法算法方面的一个的开创性工作由Volker Strassen在1969年发表[4]。该算法简述如下：设$A, B$是两个环$R$上的矩阵。令$C = AB$，$A, B, C \in R^{2^n \times 2^n}$。这里如果矩阵$A, B$ 不是$2^n \times 2^n$ 的规模那么我们就用0填满那些缺少的行和列。现在把$A, B, C$分成尺寸一样的块状小矩阵：

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \tag{1.5}$$

$$B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} \tag{1.6}$$

$$C = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix} \tag{1.7}$$

这里$A_{ij}, B_{ij}, C_{ij} \in R^{2^{n-1}\times 2^{n-1}}$。那么由传统算法，有：

$$C_{11} = A_{11}B_{11} + A_{12}B_{21} \tag{1.8}$$

$$C_{12} = A_{11}B_{12} + A_{12}B_{22} \tag{1.9}$$

$$C_{21} = A_{21}B_{11} + A_{22}B_{21} \tag{1.10}$$

$$C_{22} = A_{21}B_{12} + A_{22}B_{22} \tag{1.11}$$

这样的话需要8步乘法，下面是重要的部分，我们定义7 个新的矩阵：

$$\begin{aligned} M_1 &:= (A_{11} + A_{22})(B_{11} + B_{22}) \\ M_2 &:= (A_{21} + A_{22})B_{11} \\ M_3 &:= A_{11}(B_{12} - B_{22}) \\ M_4 &:= A_{22}(B_{21} - B_{11}) \\ M_5 &:= (A_{11} + A_{12})B_{22} \\ M_6 &:= (A_{21} - A_{11})(B_{11} + B_{12}) \\ M_7 &:= (A_{12} - A_{22})(B_{21} + B_{22}) \end{aligned} \tag{1.12}$$

接下来我们可以用上述7个矩阵来表示矩阵$C$的不同小块：

$$\begin{aligned} C_{11} &= M_1 + M_4 - M_5 + M_7 \\ C_{12} &= M_3 + M_5 \\ C_{21} &= M_2 + M_4 \\ C_{22} &= M_1 - M_2 + M_3 + M_6 \end{aligned} \tag{1.13}$$

如此一来，乘法由之前的8次减少到7次。我们将这个过程重复$n$次，直到子矩阵降维至数字（即环$R$的元素），这样就完成了矩阵A与B的乘法运算。

我们如下计算Strassen算法中的加法和乘法次数：记$f(n)$ 为两个$2^n \times 2^n$矩阵乘法的运算总次数，通过递归，有

$$f(n+1) = 7f(n) + l \cdot 4^n,$$

这里$l$表示每应用这个算法一次要用到的加法次数。则有：

$$f(n) = (7 + o(1))^n,$$

那么对于规模为$N = 2^n$ 的矩阵来说，应用Strassen算法的渐进复杂度是：

$$O((7 + o(1))^n) = O(N^{\log_2 7 + o(1)}) \approx O(N^{2.8074}).$$

## 1.3 矩阵乘法计算复杂度发展

传统算法是直接应用矩阵乘法的数学定义给出的算法，该算法需要$n^3$量级的时间来乘以两个$n \times n$矩阵。在这一问题上有三个里程碑意义的新算法：一是Volker Strassen在1969 年提出的算法[4]，有结论$\omega \leq 2.8074$。二是Don Coppersmith 和Shmuel Winograd在1990年提出的张量积算法[5]，它可以在$O(n^{2.375477})$ 的时间内实现两个$n \times n$ 矩阵的乘法，一直到2010年它都是领域内具有最佳渐进复杂度的算法，在后文中有时我们简称此算法为$CW90$算法或$CW1990$ 算法。在2010年，Andrew Stothers 提出了对CW1990算法的改进[6]，它可以在$O(n^{2.374})$ 的时间内实现两个$n \times n$ 矩阵的乘法；在2011年，Virginia Williams 将Stother文章中的一个数学捷径和她自己的洞察力相结合，在计算机上进行自动优化，把结果优化到$O(n^{2.3728642})$ [7]；在2014年，Francois Le Gall简化了Williams 的算法，得到了改进的上界$O(n^{2.3728639})$[8]。三是Henry Cohn, Robert Kleinberg, Balázs Szegedy 和Chris Umans 在2003和2005年的两篇文章[9] [10]，他们提出了群理论方法来解决矩阵乘法计算复杂度问题，他们提出了两个猜想，任一个成立都可以证明$\omega = 2$（$\omega = 2$是计算理论中一个重要猜想），其中的一个已经在2016年他们的新一篇文章[11] 中被否定了。群理论的方法目前还不能给出比CW90[5] 更好的$\omega$的上界。但很多人对此持乐观态度，因为文献[12]证明了CW90[5] 这条思路的算法框架有一个瓶颈，不能通过此种方式得到$\omega < 2.3725$，因此这种算法在证明$\omega = 2$ 的路上也不能走得更远了。

在本论文中，CW1990[5]以及相关算法不作为讨论重点，本论文着重点放在群论方法以及群的三乘积性质。

## 1.4　论文框架

第一章主要介绍矩阵乘法、矩阵乘法指数的基本定义以及领域内的开创性工作—Strassen算法，最后梳理了矩阵乘法算法复杂度分析的发展历程；第二章主要介绍矩阵乘法指数的群理论框架以及搜索极大三乘积组的蚁群算法；第三章介绍了秩的概念并探究了小矩阵乘法的群论方法；第四章介绍了几种情形下三乘积组的构建原则及应用。

# 第二章　群论方法

在2003年，通过群论方法来研究矩阵乘法计算复杂性的观点由Henry Cohn和Christopher Umans 提出。本章介绍该方法以及由该方法框架延伸出的一些结果。

## 2.1　准备知识

下面是有关该理论的一些表示论基础知识：

**引理 2.1.** （*1*）一个有限群$G$的群代数$\mathbb{C}[G]$可被分解为如下矩阵代数的直积形式$\mathbb{C}[G] \cong \mathbb{C}^{d_1\times d_1} \times ... \times \mathbb{C}^{d_k\times d_k}$，这些矩阵代数的阶分别为$d_1, ..., d_k$。而这些阶$d_i$就是群$G$的特征标。这里$\mathbb{C}$是复数域。
（*2*）对于上面的等式，如果我们分别计算等号两边的维数，就得到：

$$|G| = \sum_i d_i^2.$$

（*3*）*[16]*如果群$G$有一个交换子群$A$，那么$G$的所有特征标都小于等于$[G : A]$。

**引理 2.2** ([10]引理1.1). 设$s_1, s_2, ..., s_n$是非负实数，假设对每个非负整向量$\mu = (\mu_1, ..., \mu_n)$，这里$\sum_{i=1}^n \mu_i = N$，我们都有$\binom{N}{\mu} \prod_{i=1}^n s_i^{\mu_i} \leq C^N$。那么

$$\sum_{i=1}^n s_i \leq C.$$

## 2.2　二乘积性质

**定义 2.1** (右商). 设$S$是一个群$G$的子集合，记$Q(S)$ 为$S$ 的右商集，即
$Q(S) = \{s_1 s_2^{-1} : s_1, s_2 \in S\}$。

**注 3.** 注意到若$S$是群$G$的一个子群，那么就有$Q(S) = S$。

**定义 2.2** (二乘积性质，[10]第4 节). 我们说一个群$H$的子集合$S_1, S_2$ 满足二乘积性质，若

$$q_1 q_2 = 1 \implies q_1 = q_2 = 1,$$

这里$q_i \in Q(S_i)$。

**定义 2.3** (同时二乘积性质，[10]定义4.1). 我们说一个群$H$的n组子集合$A_i, B_i (1 \leq i \leq n)$满足同时二乘积性质如果下面条件均成立：

- 对所有的i，子集组$A_i, B_i$都满足二乘积性质，并且
- 对所有i，j，k，$a_i(a'_j)^{-1}b_j(b'_k)^{-1} = 1 \Rightarrow i = k$，这里$a_i \in A_i, a'_j \in A_j, b_j \in B_j, b'_k \in B_k$。

**引理 2.3** ([10]引理4.2). *若$n$组子集合$A_i, B_i \subset H$满足同时二乘积性质，且$n'$组子集合$A'_i, B'_i \subseteq H'$满足同时二乘积性质，那么$nn'$组子集合$A_i \times A'_i, B_j \times B'_j \subseteq H \times H'$也满足同时二乘积性质。*

下面的定理可建立群的同时二乘积性质与矩阵乘法指数之间的关系。

**定理 2.4** ([10]定理4.4). *若$H$是一个有限群，它的特征标是$\{d_k\}$，它的$n$组子集合$A_i, B_i \subseteq H$满足同时二乘积性质，那么就有：*

$$\sum_{i=1}^{n}(|A_i||B_i|)^{\omega/2} \leq (\sum_k d_k^{\omega})^{3/2}.$$

现在我们使用两个参数$\alpha$和$\beta$来形容那些满足同时二乘积性质的子集组$A_i, B_i \subseteq H$；若存在$n$组，我们选择$\alpha$和$\beta$使得$|A_i||B_i| \geq n^{\alpha}$对所有$i$和$|H| = n^{\beta}$都成立。若$H$是交换的，那么由[10]定理4.4可推出$\omega \leq \frac{3\beta-2}{\alpha}$。

**命题 2.5** ([10]命题4.5). *对每个$m \geq 2$，都存在一个$Cyc_m^{2l}$中的构造满足同时二乘积性质，且当$l \to \infty$时有$\alpha = \log_2(m-1) + o(1)$和$\beta = \log_2 m + o(1)$。*

**注 4.** 若取$m = 6$，则由此命题可推出$\omega \leq 2.48$。

目前我们所知道的对于$\alpha$和$\beta$的限制只有下面这个结论：

**命题 2.6** ([10]命题4.6). *若$n$组子集合$A_i, B_i \subseteq H$满足同时二乘积性质，且对所有$i$都有$|A_i||B_i| \geq n^{\alpha}$和$|H| = n^{\beta}$，那么$\alpha \leq \beta$，且$\alpha + 2 \leq 2\beta$.*

**注 5.** 最重要的情形是当$H$为一个交换群时，此时$\omega$的上界为$\omega \leq (3\beta - 2)/\alpha$。

命题2.6表明唯一可以实现$\omega = 2$的方法就是证明$\alpha = \beta = 2$成立。因此我们提出以下猜想：

**猜想 2.1** ([10]猜想4.7). 对于任意大的$n$，存在一个交换群$H$，且有$n$ 组满足同时二乘积性质的子集合$A_i, B_i$ 使得$|H| = n^{2+o(1)}$ 和$|A_i||B_i| \geq n^{2-o(1)}$ 均成立。

**注 6.** 上述猜想若成立，则有$\omega = 2$。但是2016 年的文章[11] 证明了不可能从指数被界定的交换群出发来得出$\omega = 2$的结论，该猜想被推翻（或需要作出修改才可能成立）。

## 2.3　三乘积性质

### 2.3.1　基本概念

**定义 2.4** (三乘积性质，[9]定义2.1). 我们说一个群$G$通过$S_1, S_2, S_3$实现了$\langle n_1, n_2, n_3\rangle$，如果存在子集合$S_1, S_2, S_3 \subseteq G$ 使得$|S_i| = n_i$，并且对$q_i \in Q(S_i)$，若$q_1q_2q_3 = 1$则$q_1 = q_2 = q_3 = 1$。我们称$S_1, S_2, S_3$ 上的这种条件为三乘积性质。此时称$S_1, S_2, S_3$为群$G$的一个三乘积组。

**定义 2.5** (基本三乘积组，[17]定义2.8). 我们称一个三乘积组$(S, T, U)$是基本三乘积组如果$1 \in S \cap T \cap U$。

**引理 2.7** ([9]引理2.1). *若群$G$实现了$\langle n_1, n_2, n_3\rangle$，那么它对$n_1, n_2, n_3$ 的每个排列也都成立。*

**引理 2.8** ([10]引理1.5). *若$S_1, S_2, S_3 \subseteq G$和$S'_1, S'_2, S'_3 \subseteq G'$ 满足三乘积性质，那么$S_1 \times S'_1, S_2 \times S'_2, S_3 \times S'_3 \subseteq G \times G'$也满足三乘积性质。*

现在来介绍一下矩阵乘法是怎样转换到$\mathbb{C}[G]$ 中元素的运算的，这里$\mathbb{C}$为复数域。设$G$ 通过$S, T, U$ 实现了$\langle n, m, p\rangle$。设$A$ 是一个$n \times p$ 矩阵，$B$ 是一个$p \times m$ 矩阵。我们用$S, T, U$来作为$A, B$ 中元素的下标。现在就有：

$$(AB)_{s,u} = \sum_{t \in T} A_{s,t}B_{t,u}.$$

在文章[9]中Cohns和Umans证明了这里的$(AB)_{s,u}$与下述乘积中$s^{-1}u$的系数是相同的，这里$s \in S$，$u \in U$。

$$\Big(\sum_{s \in S, t \in T} A_{s,t}s^{-1}t\Big)\Big(\sum_{\hat{t} \in T, u \in U} B_{\hat{t},u}\hat{t}^{-1}u\Big).$$

由此结论自然推出以下定理：

**定理 2.9** (连接矩阵乘法和群论，[9] 定理2.3). 设$F$是任一个域。若$G$实现$\langle n,m,p\rangle$，那么将两个$F$ 上$n\times m$ 和$m\times p$的矩阵相乘所需要的域操作次数最多等于将$F[G]$中两元素相乘所需要的运算次数。进一步，有$\langle n,m,p\rangle_F \le F[G]$。

**注 7.** 定理中的不等号更详细含义可参考[2]14.3 节。上述定理是本章一个重要的基础性定理，揭示了矩阵乘法与群论方法之间深刻的内在联系。

**定理 2.10** ([10]定理1.8). 假设群$G$实现了$\langle n,m,p\rangle$，它的特征标是$\{d_i\}$。那么$(nmp)^{\omega/3} \le \sum_i {d_i}^{\omega}$。

**注 8.** 假设G实现了$\langle n,m,p\rangle$且有特征标$\{d_i\}$。$\omega \le 3$，因为要排除$\omega = 3$ 的可能（希望得到$\omega$的非平凡解），则由[9] 定理1.8 可推导出$\omega$ 的一个非平凡上界当且仅当$nmp > \sum_i d_i^3$。

**注 9.** 此定理连接了三乘积性质与矩阵乘法指数，很多时候我们通过研究一个群的三乘积性质，然后结合此定理推导出$\omega$的一个上界。

**推论 2.11** ([10]推论1.9). 假设$G$实现了$\langle n,m,p\rangle$，它最大的特征标是$d$。那么有$(nmp)^{\omega/3} \le d^{\omega-2}|G|$。

**证明.** 因为$\sum_i d_i^2 = |G|$，结合定理8可直接推出本结论。 □

**注 10.** 当我们对该群的性质信息掌握较少时，可应用此推论寻找$\omega$ 的上界。

三乘积性质在群论方法与矩阵乘法复杂度的联系中有重要地位，该性质及相关引申概念和结论是后面几个章节的重点内容。

### 2.3.2 右商

这部分介绍右商的相关性质，在研究三乘积组的搜索算法中有重要作用，可作为三乘积组的必要条件大大降低搜索空间的维数。

**引理 2.12** ([17]引理2.1). $\phi \ne X \subset G$，$X$是群$G$的非空子集，那么就有：

$$1 \in Q(X)$$

以及

$$g \in Q(X) \Leftrightarrow g^{-1} \in Q(X).$$

**引理 2.13** ([17]引理2.1). *若$S,T,U$满足三乘积性质，那么对所有*

$$X \neq Y \in \{S,T,U\}$$

*都有：*

$$Q(X) \cap Q(Y) = 1.$$

**定理 2.14** ([17]定理3.1). *$G$的三个子集可以形成基本三乘积组当且仅当以下三个条件同时成立：*
*(1)* $1 \in S \cap T \cap U$；
*(2)* $Q(T) \cap Q(U) = 1$；
*(3)* $Q(S) \cap Q(T)Q(U) = 1$。

**定理 2.15** ([18]定理5). *若$(S,T,U)$是$G$中的三乘积子集组，那么*

$$|Q(S)| + |Q(T)| + |Q(U)| \leq |G| + 2$$

.

下面两个定理告诉我们在一个集合中添加新元素对该集合对应的右商集大小的影响，它们在三乘积组的提升算法中有重要应用。

**引理 2.16** ([20]引理1). *若$X$是$G$的一个子群且$c \in G \setminus X$，那么*

$$2|X| \leq |Q(X \cup \{c\})| \leq 3|X|.$$

**引理 2.17** ([20]引理2). *若$X$是$G$的一个子集使得$1 \in X$和$c \in G \setminus X$ 成立，那么*

$$|Q(X)| \leq |Q(X \cup \{c\})| \leq |Q(X)| + 2|X|.$$

### 2.3.3　三乘积组

**引理 2.18** ([17]引理2.1). *若$S,T,U$是一组三乘积子集组且$1 \in S \cap T \cap U$，那么$S \cap T = S \cap U = T \cap U = 1$.*

**推论 2.19** ([18]推论6). *若$(S,T,U)$是$G$的一个三乘积子集组，那么*

$$|S| + |T| + |U| \leq |G| + 2.$$

**引理 2.20** ([19]观察2.1). 若$(S,T,U)$是$G$的三乘积子集组，那么对所有$a,b,c,d \in G$，$(dSa, dTb, dUc)$ 也是$G$ 的三乘积子集组。

**注 11.** 那么我们就可以推出任何一个三乘积组都可以用上述方式转变为一个基本三乘积组。

**引理 2.21** ([19]观察3.1). 设$s,t,u$是$G$的三乘积性质的参数。那么就有$s(t+u-1) \leq |G|$，$t(s+u-1) \leq |G|$ 和$u(s+t-1) \leq |G|$。

**猜想 2.2** ([19]). 当$\min\{s,t,u\}$与$\max\{s,t,u\}$相差不多或者当$stu > n$时，有$s(t+u) \leq |G|$，$t(s+u) \leq |G|$ 以及$u(s+t) \leq |G|$。

**注 12.** 上述猜想尽管相比引理2.21没有太多改进，仍不失为一个有价值的猜想。若上述猜想成立，则可直接推出$\beta(G) \leq (\frac{1}{2}|G|)^{3/2}$，就给出了一个更优的$\beta$的界。

**定理 2.22** ([17]定理3.5). 设$G$是一个群。若$(S,T,U)$是$G$的三乘积子群组且$S,T,U$中至少有一个是$G$ 的正规子群，那么就有：$|S| \cdot |T| \cdot |U| \leq |G|$。

**定理 2.23** (西罗子群的三乘积性质). 设群$G$有西罗$p-$子群$P$，西罗$q-$子群$Q$，西罗$r-$子群$R$且$p,q,r$两两互素。则$G$可通过子群组$P,Q,R$实现$\langle |P|,|Q|,|R| \rangle$三乘积性质。

**证明.** 设$p \in P$为$P$中任一元素，则$\langle p \rangle$ 为$P$的子群，由拉格朗日定理有：$|\langle p \rangle|$是$|P|$ 的因子，则若不为单位元就只能是素数$p$ 的幂次，$R,Q$ 中元素的阶同理。若$p_1 p_2^{-1} q_1 q_2^{-1} r_1 r_2^{-1} = 1$，这里$p_1, p_2 \in P$，$q_1, q_2 \in Q$，$r_1, r_2 \in R$，因$p_1 p_2^{-1}$阶为$p$的幂次，$q_1 q_2^{-1}$ 阶为$q$的幂次，$r_1 r_2^{-1}$ 阶为$r$的幂次，所以要使该等式成立只能都为1，即$p_1 p_2^{-1} = q_1 q_2^{-1} = r_1 r_2^{-1} = 1$，从而有$p_1 = p_2$，$q_1 = q_2$，$r_1 = r_2$。证毕。 □

**注 13.** 由于一个群的不同西罗子群的交只有单位元，则有$|G| \geq |P| \cdot |Q| \cdot |R|$，这种情况对于求$\omega$的非平凡解帮助不大。因

$$d^{\omega-2}|G| \geq d^{\omega-2}nmp \geq nmp \geq (nmp)^{\frac{\omega}{3}}$$

（上式中最后一步不等号成立是因为$2 \leq \omega \leq 3$，倒数第二步不等号成立是因为$d \leq 1$）由此自然推出推论2.11，则不可能由推论2.11 得出$\omega$的非平凡解。

**推论 2.24** (西罗子群的二乘积性质). 设群$G$有西罗$p-$子群$P$，西罗$q-$子群$Q$，$p,q$互素。则$P,Q \subset G$满足二乘积性质。

**证明.** 证明思路同定理2.23。 □

### 2.3.4 三乘积容量

**定义 2.6** (三乘积容量，[20]). 记群$G$的三乘积容量为$\beta(G)$，$\beta(G) := max\{npm$,这里$G$通过阶分别为$n,p,m$的子集组实现了$\langle n,p,m\rangle\}$，记群$G$的三乘积子群容量为$\beta_g(G)$，$\beta_g(G) := max\{npm$,这里$G$通过阶分别为$n,p,m$的子群组实现了$\langle n,p,m\rangle\}$。

**定理 2.25** ([17]定理6.1). 对任意有限群$G$，都有$\beta(G) \geq \beta_g(G)$成立。存在满足$\beta(G) > \beta_g(G)$的群。

**证明.** 第一条陈述是显然的，因为$\beta$的搜索空间包含了$\beta_g$的搜索空间。对于第二条陈述，考虑10阶群$D_{10} = \langle d, s : d^2 = d^5 = 1, sds = d^{-1}\rangle$。由[17]表格1我们知道$\beta_g(D_{10}) = 10$。但它的子集合$S := \langle s\rangle, T := \{d, s\}$和$U := \{1, sd, d^3\}$经验证可实现$\langle 2,2,3\rangle$，结合2.21经验证可知$\beta(D_{10}) = 12$。 □

**引理 2.26** ([17]引理4.1). 若$G$是一个非交换群，且有一个非正规子群$S$，$[G : S] = 3$，那么有$\beta(G) \geq \frac{4}{3}|G|$。

**引理 2.27** ([17]引理4.2). 若$G$是一个非交换群且有一个自正规化子群$S$，$[G : S] = 4$，那么有$\beta(G) \geq \frac{2}{3}|G|$。

**引理 2.28** ([17]引理5.3). 群$G$的子集$S,T,U$满足三乘积性质当且仅当$|S^{-1}| \cdot |U| = |S^{-1}U|$和$(S^{-1}(Q(T) \setminus \{1\})U) \cap S^{-1}U = \phi$均成立。

**注 14.** 应用引理2.28，我们在检验三乘积组时，可以只计算其中一个子集的右商，而不须计算定义中出现的全部三个右商。

**命题 2.29** ([10]). 若$G \neq 1$是一个有限群，那么有：$\beta(G)^{\omega/3} \leq D_\omega(G)$。这个不等式可以推出$\omega$的非平凡上界当且仅当$\beta(G) > D_3(G)$。

**命题 2.30.** 若$G$是交换的，则有：$\beta(G) = |G| = D_2(G) \leq D_3(G)$。

## 2.4 唯一可解谜题

**定义 2.7** (唯一可解谜题，[10]3.1节). 一个宽为$k$的唯一可解谜题(USP)是一个满足下述性质的子集$U \subseteq \{1,2,3\}^k$：对于$\pi_1, \pi_2, \pi_3 \in Sym(U)$ 的所有排列，或者$\pi_1 = \pi_2 = \pi_3$，或者存在$u \in U$ 和$i \in [k]$ 使得至少$(\pi_1(u))_i = 1$，$(\pi_2(u))_i = 2$，$(\pi_3(u))_i = 3$ 中的两个等式成立。

**定义 2.8** (强唯一可解谜题，[10]3.1 节). 一个宽为$k$的强唯一可解谜题是一个满足下述性质的子集$U \subseteq \{1,2,3\}^k$：对所有的排列$\pi_1, \pi_2, \pi_3 \in Sym(U)$，或者$\pi_1 = \pi_2 = \pi_3$，或者存在$u \in U$ 和$i \in [k]$ 使得下面三个等式中恰好两个成立$(\pi_1(u))_i = 1$，$(\pi_2(u))_i = 2$，$(\pi_3(u))_i = 3$。

**命题 2.31** ([10]命题3.1). 对每个$k \geq 1$，都存在一个规模为$2^k$，宽为$2k$ 的强唯一可解谜题。

**定义 2.9** (强唯一可解谜题的容量，[10]3.1节). 我们定义强唯一可解谜题的容量为最大的常量$C$，使得对于$k$的无限多取值，都存在规模为$(C - o(1))^k$，宽为$k$的强唯一可解谜题。唯一可解谜题的容量可类似定义。

显然，对于唯一可解谜题的容量，存在一个简单的上界，当然这也是强唯一可解谜题的上界。

**引理 2.32** ([10]引理3.2). 唯一可解谜题容量最多是$(27/4)^{1/3}$。

**定理 2.33** ([5]). 唯一可解谜题容量等于$(27/4)^{1/3}$。

**猜想 2.3** ([10]猜想3.4). 强唯一可解谜题容量等于$(27/4)^{1/3}$。

**注 15.** 这个猜想会推出$\omega = 2$。

**定理 2.34** ([10]命题3.8). 对每个$k \geq 1$，都存在一个规模为$2^{k-1}(2^k + 1)$，宽为$3k$的强唯一可解谜题。

**注 16.** 上述定理可以推出强唯一可解谜题容量最小是$2^{\frac{2}{3}}$ 以及$\omega < 2.48$。

## 2.5 同时三乘积性质

**定义 2.10** ([10]定义5.1). 我们说一个群$H$ 的子集组$A_i, B_i, C_i$ ( $1 \leq i \leq n$) 满足同时三乘积性质，若

- 对每个$i$，子集合$A_i, B_i, C_i$ 都满足三乘积性质，
- 且对所有的$i, j, k$，若$a_i(a'_j)^{-1}b_j(b'_k)^{-1}c_k(c'_i)^{-1} = 1$ 则$i = j = k$，这里$a_i \in A_i, a'_j \in A_j, b_j \in B_j, b'_k \in B_k, c_k \in C_k$，$c'_i \in C_i$。

我们说这样的群$H$同时实现了$\langle|A_1|, |B_1|, |C_1|\rangle$,...,$\langle|A_n|, |B_n|, |C_n|\rangle$。

**例 2.1.** • 令$H = Cyc_n^3$，我们称$H$的三个因子为$H_1, H_2$ 和$H_3$。现在定义如下集合：

- $A_1 = H_1 \setminus \{0\}$, $B_1 = H_2 \setminus \{0\}$, $C_1 = H_3 \setminus \{0\}$
- $A_2 = H_2 \setminus \{0\}$, $B_2 = H_3 \setminus \{0\}$, $C_2 = H_1 \setminus \{0\}$

**命题 2.35** ([10]命题5.2)**.** 上面定义的两个三元组$A_1, B_1, C_1$ 和$A_2, B_2, C_2$ 满足同时三乘积性质。

**证明.** 直接由定义验证可得。 □

**定理 2.36** ([10]定理5.3)**.** 令$R$是任一个$\mathbb{C}$上的代数。如果$H$ 同时实现了$\langle n_1, m_1, p_1\rangle$，...，$\langle n_k, m_k, p_k\rangle$，那么实现$k$个规模为$n_1 \times m_1$乘$m_1 \times p_1$，...，$n_k \times m_k$乘$m_k \times p_k$的矩阵乘法所需的环操作次数最多等于将$R[H]$ 中两个元素相乘的操作数。

**引理 2.37** ([10]引理5.4)**.** 若$n$组子集三元组$A_i, B_i, C_i \subseteq H$ 满足同时三乘积性质，并且$n'$组子集三元组$A'_j, B'_j, C'_j \subseteq H'$也满足同时三乘积性质，那么$nn'$组子集三元组$A_i \times A'_j, B_i \times B'_j, C_i \times C'_j \subseteq H \times H'$ 就也满足同时三乘积性质。

下面这个定理将群的同时三乘积性质与矩阵乘法指数联系起来。

**定理 2.38** ([10]定理5.5)**.** 如果一个群$H$同时实现了$\langle a_1, b_1, c_1\rangle$,...,$\langle a_n, b_n, c_n\rangle$ 且它的特征标为$\{d_k\}$，那么就有$\sum_{i=1}^{n}(a_i b_i c_i)^{\omega/3} \leq \sum_k d_k^{\omega}$。

当$H$交换时，$\sum_k {d_k}^{\omega} = |H|$。例2.1结合定理2.38可推出$\omega < 2.93$。在文献[10]后面的内容中作者证明了任何可以用同时三乘积性质得到的$\omega$的界都可以用普通的三乘积性质推导出来，因此同时三乘积性质与三乘积性质相比并没有更多的一般性，但它仍是一个重要的概念，为我们思考三乘积性质提供了一个更为广阔的背景。

## 2.6 若干具体构造

本节内容主要基于文献[10]，是文中例子的验证以及扩展构造。在扩展构造中给出了一个$\omega$ 的非平凡上界$\omega < 2.9262$ （例2.9）。

### 2.6.1 旧例验证

这一部分内容是文献[10]中给出的例子的验证，给出了文中未列出的$\omega$的非平凡上界$\omega < 2.8156$ （例2.5）。其中提到的定理、推论、引理、命题、定义等都依循了文献[10] 中的编号。

**例 2.2** (文章[10]引理2.1中例子的验证). $H = Cyc_n^3$，$G = H^2 \rtimes Cyc_2$。$H_1, H_2, H_3$是$H = Cyc_n^3$中$Cyc_n$ 的三个因子，可以看作$H$的子群。令$H_4 = H_1$，令

$$S_i = \{(a, b)z^j : a \in H_i \setminus \{0\}, b \in H_{i+1}, j \in \{0, 1\}\}, i = 1, 2, 3$$

由文献[10]引理2.1知$S_1, S_2, s_3$满足三乘积性质，又$|S_i| = 2n(n-1)$，且因$G$的子群$H^2$交换，由本论文引理2.1(3)知群$G$的最大特征标$d \leq 2$，由文献[10] 推论1.9得到

$$(2n(n-1))^{3\cdot\frac{\omega}{3}} \leq \sum_i d_i^\omega \leq |G| \cdot d^{\omega-2} \leq |G| \cdot 2^{\omega-2},$$

而$|G| = 2n^6$，因此有$(2n(n-1))^\omega \leq 2^{\omega-2} \cdot 2n^6$。通过计算可知当$n = 17$ 时取得最佳上界$\omega < 2.9088$。

**例 2.3** (文章[10]推论3.6中结论的验证). 文中[10]推论3.6告诉我们$\omega \leq \frac{3(\log m - \log C)}{\log(m-1)}$，这里$C$ 是强$USP$ 容量。由文中[10]命题3.8可知$C \geq 2^{2/3}$。将此值代入上面的不等式，则有：

$$\omega \leq \frac{3(\log m - \log(2^{\frac{2}{3}}))}{\log(m-1)}, m \geq 3.$$

通过计算可得当$m = 6$时取到最佳上界$\omega < 2.4785$。

**例 2.4** (文中[10]命题4.5中结论的验证). 在[10]命题4.5中，我们有结论“对每个$m \geq 2$，都有一个$Cyc_m^{2l}$中的构造满足同时二乘积性质，且当$l \to \infty$时，$\alpha = \log_2(m-1) + o(1)$，$\beta = \log_2 m + o(1)$，显然$H = Cyc_m^{2l}$是交换的，因此由上述结论，若$H$ 是交换的，则[10] 定理4.4可推出$\omega \leq \frac{3\beta-2}{\alpha}$。
综上，我们得出

$$\omega \leq \frac{3(\log_2 m + o(1)) - 2}{\log_2(m-1) + o(1)},$$

当$l \to \infty$时，$m = 2$时，$\omega$的最佳上界为：

$$\omega \leq \frac{3 \cdot o(1) + 1}{o(1)} = 3 + \frac{1}{o(1)} = \infty, l \to \infty$$

是平凡解。$m \geq 3$时，当$l \to \infty$时，$o(1)$均可略去，则有

$$\omega \leq \frac{3 \cdot \log_2 m - 2}{\log_2(m-1)}$$

通过计算可得$m = 6$ 时取最佳上界$\omega < 2.4785$。

下面是文[10]中定义5.1下面的例子的验证，给出了文中未列出的$\omega$的非平凡上界$\omega < 2.8156$。

**例 2.5.** 令$H = Cyc_n^3$，$H_1, H_2, H_3$ 是$H$的三个因子。定义如下集合：
$A_1 = H_1 \setminus \{0\}$, $B_1 = H_2 \setminus \{0\}$, $C_1 = H_3 \setminus \{0\}$
$A_2 = H_2 \setminus \{0\}$, $B_2 = H_3 \setminus \{0\}$, $C_2 = H_1 \setminus \{0\}$
由[10]命题5.2可知$A_1, B_1, C_1$ 和$A_2, B_2, C_2$ 满足同时三乘积性质。由[10]定理5.5知

$$\sum_{i=1}^{2} (|A_i||B_i||C_i|)^{\omega/3} \leq \sum_k d_k^\omega,$$

因为$H$交换，则有

$$\sum_k d_k^\omega = |H| = n^3,$$

则有

$$2 \cdot (n-1)^{3 \cdot (\omega/3)} \leq n^3,$$

推出

$$2(n-1)^\omega \leq n^3,$$

推出

$$\omega \leq \frac{3 \cdot \lg n - \lg 2}{lg(n-1)}, n \geq 3$$

通过计算可以得到当$n = 16$ 时取到最佳上界$\omega < 2.8155383$。

### 2.6.2 新例构建

这部分是基于文献[10]的新例子的构建。除非特别说明，例子中提到的定理、推论、引理、命题、定义等都依循文献[10] 中的编号。

第一个是文[10]中定义4.1下面的例子的扩展：

**例 2.6.** $H = Cyc_n^k \times Cyc_n$，$A_i = \{(x,i) : x \in Cyc_n^k\}, B_i = \{(0,i)\}$，那么对$i \in Cyc_n$，$A_i, B_i \in H$就满足同时二乘积性质。由[10]定理4.4，有

$$\sum_{i=1}^{n}(|A_i||B_i|)^{\omega/2} \leq (\sum_k d_k^{\omega})^{3/2},$$

因$H$交换，有

$$(\sum_k d_k^{\omega})^{3/2} = |H|^{3/2} = (n^{k+1})^{3/2},$$

则有

$$n \cdot (n^k)^{\omega/2} \leq (n^{k+1})^{3/2},$$

推出

$$\omega \leq 3 + \frac{1}{k},$$

当$k$ 趋于无穷时，有最佳上界$\omega \leq 3$，为平凡解。

下面是一个新例子：

**例 2.7.** $H = Cyc_n \times Cyc_n^k$，$A_i = \{(x,i) : x \in Cyc_n\}, B_i = \{(0,i)\}$，那么对$i \in Cyc_n^k$，$A_i, B_i$对就满足同时二乘积性质。由文[10]中定理4.4，有

$$\sum_{i=1}^{n}(|A_i||B_i|)^{\omega/2} \leq (\sum_k d_k^{\omega})^{3/2},$$

因$H$交换，有

$$(\sum_k d_k^{\omega})^{3/2} = |H|^{3/2} = (n^{k+1})^{3/2},$$

则有

$$(n^k) \cdot n^{\omega/2} \leq (n^{k+1})^{3/2},$$

推出

$$\omega \leq 3 + \frac{3}{k},$$

当$k$ 趋于无穷时，有最佳上界$\omega \leq 3$，为平凡解。

下面是一个应用[10]定理4.3将本论文例2.6进行扩充构建得到的新例子：

**例 2.8.** $H = Cyc_n^k \times Cyc_n$，$A_i = \{(x,i) : x \in Cyc_n^k\}, B_i = \{(0,i)\}$，那么对$i \in Cyc_n$，$A_i, B_i$子集组就满足同时二乘积性质。
设$\Delta_n = \{(a,b,c) \in \mathbb{Z}^3 : a+b+c = n-1 \text{ 且} a,b,c \geq 0\}$。
对于$n$组$H$的子集$A_i, B_i$，$0 \leq i \leq n-1$，我们定义$H^3$中的子集三元组，以$v = (v_1, v_2, v_3) \in \Delta_n$ 作为指标集，如下：
$\widehat{A_v} = A_{v_1} \times \{1\} \times B_{v_3}$
$\widehat{B_v} = B_{v_1} \times A_{v_2} \times \{1\}$
$\widehat{C_v} = \{1\} \times B_{v_2} \times A_{v_3}$
令$G = (H^3)^{\Delta_n} \rtimes Sym(\Delta_n)$。
$S_1 = \{\widehat{a}\pi : \pi \in Sym(\Delta_n), \widehat{a_v} \in \widehat{A_v} \text{对所有} v\}$
$S_2 = \{\widehat{b}\pi : \pi \in Sym(\Delta_n), \widehat{b_v} \in \widehat{B_v} \text{对所有} v\}$
$S_3 = \{\widehat{c}\pi : \pi \in Sym(\Delta_n), \widehat{c_v} \in \widehat{C_v} \text{对所有} v\}$
那么由定理4.3知，$S_1, S_2, S_3 \subset G$ 满足三乘积性质。由[10]定理1.8 和推论1.9，有$(|S_1||S_2||S_3|)^{\omega/3} \leq \sum_i d_i^{\omega}$，记为(1) 式，
$|S_1| = (|\Delta_n|!)(n^k)^{|\Delta_n|} = |S_2| = |S_3|$，
$|\Delta_n| = \binom{n+1}{2} = \frac{1}{2}n(n+1)$。
$|G| = |\Delta_n|! \cdot (n^{k+1})^{3|\Delta_n|}$，代入(1) 式，因$(H^3)^{\Delta_n}$交换，由本论文中引理2.1(3) 可知$d_G \leq |\Delta_n|!$
推出

$$\omega \leq 3 + \frac{3}{k} - \frac{2 \cdot \ln((\frac{n\cdot(n+1)}{2})!)}{k \cdot n \cdot (n+1) \cdot \ln n}, n \geq 2, k \geq 1$$

因

$$\frac{2 \cdot \ln((\frac{n\cdot(n+1)}{2})!)}{n \cdot (n+1) \cdot \ln n} < \frac{\ln(\frac{1}{2}n(n+1))}{\ln n} = 1 - \frac{\ln 2}{\ln n} + \frac{\ln(n+1)}{\ln n} \leq 2, n \geq 2, k \geq 1$$

因此，当$k \to \infty, n \to \infty$时，取到最佳上界$\omega \leq 3$，是平凡解。

下面是一个应用[10]定理7.1将[10]定义5.1下面的例子进行扩充构建得到的新例子，并得到了一个$\omega$ 的非平凡解：

**例 2.9.**
- 令$H = Cyc_n^3$，$H_1, H_2, H_3$ 是$H$ 的三个因子。定义如下集合：
- $A_1 = H_1 \setminus \{0\}$, $B_1 = H_2 \setminus \{0\}$, $C_1 = H_3 \setminus \{0\}$

- $A_2 = H_2 \setminus \{0\}$, $B_2 = H_3 \setminus \{0\}$, $C_2 = H_1 \setminus \{0\}$

由[10]命题5.2可知$A_1, B_1, C_1$ 和$A_2, B_2, C_2$ 满足同时三乘积性质。令

$$G = Sym_2 \ltimes H^2,$$

构建新的$H_i'$：

$H_1' = \{h\pi : \pi \in Sym_2, h_i \in A_i$ 对每个$i\}$

$H_2' = \{h\pi : \pi \in Sym_2, h_i \in B_i$ 对每个$i\}$

$H_3' = \{h\pi : \pi \in Sym_2, h_i \in C_i$ 对每个$i\}$

由[10]定理7.1推出$H_1', H_2', H_3' \subset G$ 满足三乘积性质。因$H^2 \subset G$交换，由本论文引理2.1(3)知，$G$的最大特征标$d \leq [G : H] = |Sym_2| = 2$。由[10]定理1.8和推论1.9得到：

$$(|H_1'||H_2'||H_3'|)^{\frac{\omega}{3}} \leq \sum_i d_i^\omega \leq |G| d^{\omega-2} \leq |G|(2!)^{\omega-2},$$

而

$$|H_1'| = 2! \cdot (n-1)^2 = |H_2'| = |H_3'|, |G| = 2! \cdot n^6,$$

$$(2! \cdot (n-1)^2)^\omega \leq 2^{\omega-2} \cdot 2! \cdot n^6$$

$$2 \cdot (n-1)^{2\omega} \leq n^6$$

$$\omega \leq \frac{6 \cdot \lg n - \lg 2}{2 \cdot \lg(n-1)}, n \geq 3$$

通过计算得到：当$n = 41$时取到最佳上界$\omega \leq 2.9261305$，是一个非平凡解。

## 2.7 搜索极大三乘积组的蚁群算法

本部分内容主要基于文章[13]，介绍了一个搜索群的极大三乘积组的蚁群算法。

**蚁群算法**

蚁群算法是一种遗传算法，它是在模仿蚂蚁寻找食物资源的机制来寻找最优解。在蚁群算法中，首先有一定数目的智能蚂蚁。每只智能蚂蚁以一定几率选定一条路径，选择方式与路径中信息素的多少以及一些遗传信息有关。

具体来说，假设一直智能蚂蚁在一个图$H = (V, E)$ 中游走，它现在的位置

是顶点$i \in V$，这里$V(E)$是顶点(边)的集合，则这只蚂蚁选择边$(i,j) \in E$的概率可被如此计算：

$$P_{ij} = \frac{(\tau_{ij})^{\alpha} \cdot (\eta_{ij})^{\beta}}{\sum_{j \in N(i)} {\tau_{ij}}^{\alpha} \cdot (n_{ij})^{\beta}},$$

这里$N(i)$表示顶点$i$的相邻顶点。

在这个概率等式中，$\tau_{ij}$和$\eta_{ij}$ 分别表示边$(i,j)$上的信息素和遗传信息；$\alpha$和$\beta$ 分别表示控制信息素和遗传信息重要性的参数。边$(i,j)$ 上的遗传信息$\eta_{ij}$ 是由具体的优化问题决定的。在此暂不考虑遗传信息的影响；设定所有的$\eta_{ij} = 1$，设定$\alpha = 1$，$\beta = 1$。

每条边上的信息素量一直在动态更新，更新的基本原则是增多有可能是较优解的边上的信息素，减少其他边上的信息素。

**搜索极大三乘积组的蚁群算法**

由引理2.14，以及$S \subset Q(S)$，$T \subset Q(T)$，$U \subset Q(U)$，就有$S \cap T = \{1\}$，$S \cap U = \{1\}$，$T \cap U = \{1\}$。也就是说任一个三乘积组$(S,T,U)$ 都满足“在$G \backslash \{1\}$中，$S,T,U$ 中任意两个集合都没有共同元素”的性质。因此，对一个给定的元素$1 \neq x \in G$ 以及一个$G$ 的给定的三乘积组$(S,T,U)$，$x$要么被选进$S,T,U$ 中的一个里面，要么就不在三个子集合中的任一个里。

为了使用蚁群算法来搜索给定阶为$n+1$ 的群$G = \{1 = g_0, g_1, ..., g_n\}$ 的三乘积组$S,T,U$, 这里$n$ 是一个正数，我们构造一个有向图，如图2.1 所示，

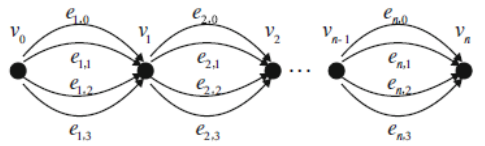


图 2.1: 搜索群的极大三乘积组的蚁群算法结构图

该图有$n+1$个结点$v_0, v_1, ..., v_n$以及$4n$ 条边，这些边与元素$g_i (i = 1, ..., n)$相联系。对$1 \leq i \leq n$，结点$v_{i-1}$ 和$v_i$之间的四条边$e_{i0}, e_{i1}, e_{i2}, e_{i3}$ 和元素$g_i \in G$相关联。这里我们不考虑单位元$g_0$，将它提前放在$S \cap T \cap U$ 中。

如果一个智能蚂蚁选了边$e_{i0}$进行游走，对应的意思是$g_i$没有被选进$S \cup T \cup U$中；若蚂蚁选了边$e_{i1}$，意味着$g_i$ 被选进$S$；若它选了$e_{i2}$，意味着$g_i$ 被选进$T$；

若它选了$e_{i3}$，对应$g_i$ 被选进$U$。在每条边上都有一定数量的信息素。

那么随着一只智能蚂蚁从$v_0$游走到$v_n$，一组$(S,T,U)$ 的解就生成了。这里一只蚂蚁选择边$e_{ij}$ 来游走的概率公式是$\frac{\tau_{ij}}{\tau_{i0}+\tau_{i1}+\tau_{i2}+\tau_{i3}},(j=0,1,2,3)$，这里$\tau_{ij}$是边$e_{ij}$上的信息素含量。

由于涉及该算法过程中未用到引理2.14的所有条件，因此该算法筛选过后选择出的结果只是可能的$G$ 的三乘积组，还需要进行一步检验，我们使用文献[17] 中的算法进行检验，该算法伪代码如下：

TPPTestMurthy(S,T,U)
Input:A triple (S,T,U)of a group
01:Begin
02: QT:=Q(T);QU:=Q(U);
03: If$|QT\cap QU|=1$ then
04: QS:=Q(S);
05: If $|QS\cap(QT\cdot QU)|=1$ then
06: Return *true*;
07: End if
08: End if
09: Return *false*
10:End

**注 17.** 这个算法是基于引理2.14来对三乘积组进行检验的。

蚁群算法搜索极大三乘积组的基本思想和框架如上所述，文章[13]后面还有对参数的讨论和优化，以及不同蚂蚁群体量以及信息素衰减率对结果的影响的讨论和实验比较，在此不做详述。

对我们来说，与搜索检验三乘积组的精确算法相比，该算法一个显著的优点就是计算速度快，对一个阶在50 乃至80 阶以下的群，可以较快给出至少一个三乘积组的结果；不足之处在于，不能实现输入一个群输出它是否有某三乘积性质的功能；还有一点就是搜索得到的三乘积组不能确定是不是达到了容量最大值，而只有最大容量$\beta(G)$ 才对矩阵乘法指数$\omega$ 的计算有实在意义。不过与精确算法相比，此方法另辟蹊径，从机器学习算法的角度切入；或许机器学习算法会是我们研究矩阵乘法算法复杂度的一片新天地。

**机群辅助计算部分结果**

蚁群算法搜索群的极大三乘积组的机群辅助计算（作者主要使用中国科学院数学机械化实验室的机群）部分结果展示如下：

群$H_1$在GAP[14]软件中可表示为$H_1 := SmallGroup(36,11)$，它的结构为$C_3 \times A_4$，这里$C_3$是3阶循环群，$A_4$是4阶偶置换群。记群$G_1 = C_2 \times H_1$，它在GAP软件中可表示为$G_1 := SmallGroup(72,47)$。

**定理 2.39.** *群$H_1$可实现$\langle 8,3,2\rangle$以及$\langle 3,6,3\rangle$。*

**证明.** 蚁群算法针对群$H_1$进行搜索极大三乘积组的运算可得上述结果。 □

**推论 2.40.** *群$G_1$可实现$\langle 8,3,4\rangle$，$\langle 8,6,2\rangle$，$\langle 6,6,3\rangle$。*

**证明.** 群$C_2$可通过$S = \{1\}, T = \{1\}, U = \{1,2\}$实现$\langle 1,1,2\rangle$，由[10]引理1.4知$C_2$亦可实现$\langle 1,2,1\rangle$，$\langle 2,1,1\rangle$。由[10]引理1.5，因$G_1 = C_2 \times H_1$，则有：群$G_1$可实现$\langle 8,3,4\rangle$，$\langle 8,6,2\rangle$，$\langle 6,6,3\rangle$。 □

$H_2$在GAP软件中可表示为$H_2 := SmallGroup(36,3)$，它的结构为$C_2^2 \rtimes C_9$，这里$C_2$是2阶循环群，$C_9$是9阶循环群。记群$G_2 = C_2 \times H_2$，它在GAP软件中可表示为$G_2 := SmallGroup(72,16)$。

**定理 2.41.** *群$H_2$可实现$\langle 3,3,4\rangle$，$\langle 6,2,3\rangle$。*

**证明.** 蚁群算法针对群$H_2$进行搜索极大三乘积组的运算可得上述结果。 □

**推论 2.42.** *群$G_2$可实现$\langle 12,3,2\rangle$，$\langle 6,6,2\rangle$，$\langle 6,4,3\rangle$，$\langle 8,3,3\rangle$。*

**证明.** 群$C_2$可通过$S = \{1\}, T = \{1\}, U = \{1,2\}$实现$\langle 1,1,2\rangle$，由[10]引理1.4知$C_2$亦可实现$\langle 1,2,1\rangle$，$\langle 2,1,1\rangle$。由[10]引理1.5，因$G_2 = C_2 \times H_2$，则有：群$G_2$可实现$\langle 12,3,2\rangle$，$\langle 6,6,2\rangle$，$\langle 6,4,3\rangle$和$\langle 8,3,3\rangle$。 □

# 第三章　秩与小阶矩阵乘法的群理论方法

本章第一部分介绍秩的概念以及相关引申概念和性质；第二部分研究两类小阶矩阵乘法的群理论方法。第一部分有关秩的一些结论在第二部分问题的研究中可以帮助缩减问题的搜索空间。

## 3.1　秩

### 3.1.1　基本概念

**定义 3.1** ([2] 第14章定义14.7). 设$k$是一个域，$U, V, W$是有限维$k-$向量空间。设$\eta : U \times V \to W$ 是一个$k-$双线性映射。对$i \in \{1, ..., r\}$，取$f_i \in U^*$，$g_i \in V^*$(分别是$k$上$U$ 和$V$的对偶空间)和$w_i \in W$ 使得$\eta(u, v) = \sum_{i=1}^{r} f_i(u)g_i(v)w_i$ 对所有$u \in U$，$v \in V$都成立。那么$\{f_1, g_1, w_1; ...; f_r, g_r, w_r\}$ 被称作$\eta$ 的一个长度为$r$ 的$k-$ 双线性算法，当$k$ 固定时就称作一个双线性算法。$\eta$ 的所有双线性算法长度的最小值就被称作$\eta$的秩$R(\eta)$。若$A$是一个$k-$代数，那么$A$ 的秩$R(A)$ 就被定义为它的双线性映射的秩。

**定义 3.2** (双线性映射的限制，[2] 定义14.27). 令$\phi : U \times V \to W$，$\phi' : U' \times V' \to W'$ 是两个$k-$双线性映射。一个$\phi$ 到$\phi'$ 的$k-$限制，或者单说限制（当$k$ 固定时）是线性映射$\sigma : U \to U'$,$\tau : V \to V'$ 和$\zeta' : W' \to W$的一个三元组$(\sigma, \tau, \zeta')$ 使得$\phi = \zeta' \circ \phi' \circ (\sigma \times \tau)$。若存在一个$\phi'$到$\phi$ 的限制我们就记作$\phi \leq \phi'$。

**定义 3.3** (r-特征标容量，[15] 定义1.6). 设$G$是一个群，其特征标为$\{d_i\}$。我们定义$G$ 的$r$-特征标容量为$D_r(G) := \sum_i d_i^r$。

设$\langle n, m, p\rangle$表示一个$n \times m$ 和一个$m \times p$矩阵相乘得到一个$m \times p$矩阵的双线性映射。将双线性映射$\langle n, m, p\rangle$的秩记为$R(n, m, p)$，将$R(n, n, n)$ 简记为$R(n)$。若$G$ 实现了$\langle n, m, p\rangle$ 则由定理2.9可知有：$\langle n, m, p\rangle \leq \mathbb{C}[G]$ （[9] 定理2.3）；因此$R(n, m, p) \leq R(\mathbb{C}[G]) =: R(G)$。

由Wedderburn结构定理（[26] 定理2）我们有$R(G) \leq \sum_i R(d_i)$。$R(G)$ 的具体值只在少数情况下可以确切知道。因此再问题研究中我们通常使用下面这个不等式：$R(n, p, m) \leq \sum_i R(d_i)$。

### 3.1.2 代数的秩

#### 3.1.2.1 相关概念

**定义 3.4** ([23]). 设$A$是一个代数。
（1）$A$的所有幂零左理想的和就叫做$A$ 的根理想，记作$radA$;
（2）$A$的所有最大双边理想的交叫做$A$ 的贾克比森根理想，记作$J(A)$;
（3）$A$是半单的如果$radA = 0$;
（4）$A$是单的如果它不含有除$\{0\}$ 以外任何真双边理想。

**定义 3.5** (可除代数, [26]2.1 节). 一个代数$D$叫做可除代数若$D^{\times} = D \setminus \{0\}$。

### 3.1.3 Alder-Strassen 界

**命题 3.1** ([25]). 结合代数$A$的秩的一个基础下界被称作*Alder-Strassen* 界：

$$R(A) \geq 2 \dim A - t,$$

这里$t$是$A$中最大双边理想的个数。

**定义 3.6** ($L(A)$，[21]). 一个有限维结合代数$A$的复杂度$L(A)$ 是一个计算该代数中两个元素相乘的最优化算法中非标量乘法/除法的数目。

下面的两个结论是代数方面的，它们都可由Wedderburn 经典结构定理（[26] 定理2）直接推出。若$A$ 是一个代数，我们记$radA$ 为$A$ 的根理想：

**引理 3.2** ([21] 引理1). （*1*）$A$ 与$A/radA$有相同数量的最大双边理想；
（*2*）$A/radA$是半单的。

**引理 3.3** ([21] 引理2). 设$A, B$是两个代数。则有：

$$L(A \times B) \geq L((A/radA) \times B) + 2 \cdot \dim(radA).$$

**引理 3.4** ([21] 引理3). 设$A, B$是两个代数，$A$是单的。则有：

$$L(A \times B) \geq 2 \cdot \dim A - 1 + L(B).$$

**注 18.** 由引理3.3和引理3.4可推出文献[21] 的主要结论，即下面的定理3.5。

**定理 3.5** ([21]). 设$A$是任一个代数，则有：$L(A) > 2\cdot\dim A - t_A$，这里$t_A$ 是$A$的最大双边理想个数。

**证明.** 令

$$A/radA = A_1 \times ... \times A_t$$

这里$A_1, ..., A_t$ 是单代数。则有

$$L(A) \geq L(A_1 \times ... \times A_t) + 2\cdot\dim(radA)$$

（由引理3.3）

$$\geq \sum_{i=1}^{t}(2\dim A_i - 1) + 2\cdot\dim(radA)$$

（由引理3.4，应用归纳法）

$$\begin{aligned} &= 2\cdot\dim A - t \\ &= 2\cdot\dim A - t_{A/radA} \\ &= 2\cdot\dim A - t_A \end{aligned} \tag{3.1}$$

这里$t_{A/radA}$ 表示$A/radA$ 的最大双边理想个数，$t_A$ 表示$A$ 的最大双边理想个数。 □

**注 19.** 该定理给出了结合代数中著名的Alder-Strassen 界。

进一步来看，我们的证明其实可以推出以下结论：

**定理 3.6** ([21]). 若$A, B$是两个代数，则

$$L(A\times B) \geq L(B) + 2\cdot\dim A - t_A$$

这里$t_A$表示$A$ 的最大双边理想的个数。且当$B$被任一个二次映射取代时该结论也成立。

### 3.1.4　群与$\omega$

**定理 3.7** ([23] 定理3). 设$\mathcal{G} = \{G_1, G_2, ...\}$ 是一个有限群族，$|G_i| < |G_{i+1}|$。假设$k$是代数闭的且对每个$i \geq 1$，都有$char(k) = 0$或$char(k) \nmid |G_i|$。则对$G \in \mathcal{G}$，有$R(k[G]) \lessapprox (|G|)^{\omega/2}$ （这里$\omega$是$k$ 上的矩阵乘法指数），且有$\omega \geq 2\lim_{n\to\infty} sup\frac{\log R(k[G_n])}{\log|G_n|}$。

**推论 3.8** ([23] 推论1). 对于族$\{k[G_1], k[G_2], ...\}$ 中的所有群代数$k[G_n]$，若对任意但固定的$\epsilon$，都有$R(k[G_n]) = \Omega((|G_n|)^{1+\epsilon})$，那么矩阵乘法指数$\omega > 2$。

**定义 3.7** ([23] 第3节). 令$\mathcal{G} = \{G_1, G_2, ...\}$ 是一个有限群族使得$|G_t| < |G_{t+1}|$。若$char(k) = 0$ 或$char(k) = p$ 且对任意$i \geq 1$，$p \nmid |G_i|$，那么$\mathcal{G}$就叫做域$k$上的一个有限群的半单族。

**定义 3.8** (最小秩代数，[23]). 若$A$和$B$是$k$上的结合代数，$t(A)$ 是$A$的最大双边理想的个数，则有

$$R(A \times B) \geq 2 \dim A - t(A) + R(B).$$

特别地，$R(A) \geq 2 \dim A - t(A)$。此式等号成立时，代数$A$ 就称作是最小秩代数。

对一个有限群$G$，群代数$k[G]$ 是半单的当且仅当$char(k) \nmid |G|$。在这种情况下有：

$$k[G] \cong D_1^{n_1 \times n_1} \times ... \times D_t^{n_t \times n_t} \tag{3.2}$$

这里$D_\tau$是$k$ 上的可除代数。每个$D_t^{n_\tau \times n_\tau}$被称作$G$ 在$k$ 上的一个不可约表示。$n_1, ..., n_\tau$ 被称作$G$ 的特征标。现在将$G$在$k$上的维数等于$i$ 的不可约特征标的数目记作$t_i(G)$。接下来定义$T_i(G) = \sum_{j=i}^{\infty} t_j(G)$。现在可以注意到$k[G]$的最大双面理想数目就等于$T_1(G) = t$。

**定理 3.9** ([23] 定理6). 设$G$是一个有限群，$k$是一个代数闭域，$char(k) = 0$ 或$char(k) \nmid |G|$。$t$的定义如上面等式*3.2* 所述。则有：
(*1*) $T_3(G) = 0$当且仅当$k[G]$ 是最小秩代数。这种情况下$R(k[G]) = t_1(G) + 7t_2(G)$。
(*2*) 若$T_3(G) > 0$，则$R(k[G]) \geq 2|G| - t + \max\{\frac{9}{2}T_7(G), 1\}$。
(*3*) 设$\mathcal{G} = \{G_1, G_2, ...\}$ 是一个群的半单族。假设每个$G \in \mathcal{G}$ 在$k$ 上的不可约表示数目是$o(|G|)$。则对所有$G \in \mathcal{G}$，$R(k[G]) \geq \frac{5}{2}|G| - o(|G|)$。

**注 20.** （1）若$T_3(G) > 0$，则

$$R(k[G]) = 2 \dim A - (T_1(G) - T_3(G)) + R(B) \geq 2|G| - t + 1;$$

（2）对$n \geq 3$，$R(k^{n \times n}) \geq 2n^2 + n - 2$。

**注 21.** （1）对一个代数闭域$k$来说，由Strassen 的直积猜想可推出$R(k[G]) = R(k^{n_1\times n_1}) + ... + R(k^{n_t\times n_t})$。（2）若$G$不交换，至少有一个$n_\tau > 1$，由Schönhage的$\tau-$定理（[2]，(15.11)），$n_1^\omega + ... + n_t^\omega \leq R(k[G])$。

**定理 3.10** ([24]). 设$A$是一个$k-$代数，$A/radA \cong A_1 \times ... \times A_t$，这里$A_\tau = D_\tau^{n_\tau\times n_\tau}, \forall \tau$，这里$D_\tau$ 是一个$k-$可除代数。假设每个$A_\tau$ 都是非交换的，即$n_\tau \geq 2$ 或$D_\tau$是非交换的。则有

$$R(A) \geq \frac{5}{2}\dim A - 3\sum_{\tau=1}^{t} n_\tau.$$

### 3.1.5　一般代数的秩

**定义 3.9** (可分). 设$K$是一个域。一个结合$K-$代数$A$ 被称作是可分的如果对任一个域扩张$L/K$，代数$A\otimes_K L$都是半单的。

**命题 3.11** ([26]2.1 节). （*1*）任一个完全域上的代数都是可分的*;*（*2*）若一个代数是如下形式：$k^{n_1\times n_1} + ... + k^{n_t\times n_t}$，那么它就是可分的。

**引理 3.12** ([26]2.2 节). 对任一个代数$A$，都有

$$R(A) \geq R(A/radA) + 2\dim A.$$

**引理 3.13** ([26] 引理11). 若$A = B\times B'$，$B$是一个单$k-$ 代数，$B'$ 是任一个$k-$代数，则有：

$$R(A) \geq 2\dim B - 1 + R(B').$$

**引理 3.14** ([26] 引理26). 设$B_1$，$B_2$是两个代数。那么代数$B = B_1 \times B_2$ 取到最小秩（是最小秩代数）当且仅当$B_1$，$B_2$都取到最小秩（是最小秩代数）。

### 3.1.6　$\omega$ 与秩的关系

这一小节中，为忠于原参考文献[1]，用符号$\mathfrak{R}$来表示秩。$\omega$与秩的关系最早是由以下命题建立起来的：

**命题 3.15** ([2]，376-377页). 对任一个域$K$，都有

$$\omega(K) = inf\{h \in \mathbb{R}^+ | \mathfrak{R}(\langle n,n,n\rangle) = O(n^h), n \to \infty\}.$$

可以这样解释上述命题：给定域$K$，对任意小的$\varepsilon > 0$，都存在一个独立于$n$的常量$C_{K,\varepsilon} \geq 1$，使得对所有$n$，都有$\mathfrak{R}(\langle n,n,n\rangle) \leq C_{K,\varepsilon} n^{\omega(K)+\varepsilon}$ 成立。

下面我们从秩的角度来研究Strassen对$\omega$ 的第一个估计，即$\omega < 2.81$[4]。他证明了$\mathfrak{R}(\langle 2,2,2\rangle) \leq 7$ （Winograd将这个结果改进到$\mathfrak{R}(\langle 2,2,2\rangle) = 7$，[27]）从这个结论可以很容易推出$\mathfrak{R}(\langle 2^n,2^n,2^n\rangle) \leq \mathfrak{R}(\langle 2,2,2\rangle)^n \leq 7^n$，（[2] 第377 页）。因为对所有正整数$n \geq 2$，都有$n \leq 2^{\lceil \log_2 n\rceil} = n + \varepsilon_n$，这里$\varepsilon_n > 0$ 是一个取决于$n$的余数，$\lceil\cdot\rceil$ 是实数的上取整函数，则有

$$\begin{aligned}\mathfrak{R}(\langle n,n,n\rangle) &\leq \mathfrak{R}(\langle 2^{\lceil \log_2 n\rceil}, 2^{\lceil \log_2 n\rceil}, 2^{\lceil \log_2 n\rceil}\rangle)\\ &\leq \mathfrak{R}(\langle 2,2,2\rangle)^{\lceil \log_2 n\rceil}\\ &\leq 7n^{\log_2 7} \approx 7n^{2.807}\end{aligned} \tag{3.3}$$

由命题3.15 可推出$\omega < 2.81$。下面是两个进一步的研究结论。

**命题 3.16** ([1] 命题4)**.** 若$\mathfrak{R}(\langle m,p,q\rangle) \leq s$，则$(mpq)^{\frac{\omega}{3}} \leq s$。

**注 22.** 由上面的命题可知$(mpq)^{\frac{\omega}{3}} \leq \mathfrak{R}(\langle m,p,q\rangle)$，进而有$\omega \leq \frac{\log \mathfrak{R}(\langle m,p,q\rangle)}{\log(mpq)^{1/3}}$ 对任意正整数$m,p,q$ 均成立。命题3.17 是一个推广结论。

**命题 3.17.** 若$\mathfrak{R}(\oplus_i \langle m_i,p_i,q_i\rangle) \leq s$，则$\sum_i (m_i p_i q_i)^{\frac{\omega}{3}} \leq s$。

## 3.2 $5 \times 5$ 矩阵乘法的群理论方法

下面我们探讨的问题来源于文献[15]。

**问题背景：** 问题来源于小矩阵的乘法。著名的$O(n^{2.81})$ 算法（Strassen算法）是基于一个可以计算两个$2 \times 2$ 矩阵乘积的算法，只需要7步乘法就能完成。Winograd[27]证明了这种情况下需要的最少乘法步数就是7步。而将两个$n \times n$ 矩阵相乘所需最小乘法步数的确切值$R(n)$ 在$n > 2$ 的情形下都是未知的。不过[28] 表格3给出了$n \leq 30$ 情况下的$R(n)$的上界。Hedtke 和Murthy 在[17]中证明了通过群理论方法不能在$R(3)$ 和$R(4)$上得到更优的结果。因此我们要考虑$R(5)$ 能否通过群理论方法（这里特指三乘积方法）得到比该表格所列已有算法（Makarov 算法）更优的结果。

**问题陈述：** 是否存在一个群$G$可以实现$\langle 5,5,5\rangle$ 三乘积性质并且该群的秩的

下界$\underline{R}(G)$（定义如下）小于100（[28] 表格3）。

**解决方案** 由于搜索空间太大，我们的主要思想第一步是通过必要条件来缩减搜索空间。下面我们看看有哪些必要条件可以用来缩减搜索空间。

我们记$\bar{R}(G) := \sum_i R(d_i)$ 为$R(G)$ 的已知最佳上界，记$\underline{R}(G)$ 为$R(G)$的已知最佳下界。对一个有限群$G$，记它的不可约复特征值的总个数为$T(G)$，记它的最大不可约特征标为$b(G)$。

**定理 3.18** ([23]定理6). *$G$是一个群*
*（1）若$b(G) = 1$，则$R(G) = |G|$。*
*（2）若$b(G) = 2$，则$R(G) = 2|G| - T(G)$。*
*（3）若$b(G) \geq 3$，则$R(G) \geq 2|G| + b(G) - T(G) - 1$。*

**注 23.** 该定理以及定理3.6、定理3.10、定理3.9以及引理3.13等相关结论均可用来限定群$G$的秩的范围，从而帮助缩减问题搜索空间。

**定义 3.10** ([15] 定义1.5). 记$\beta(G)$为$nmp$ 的最大值，这里$G$ 实现了$\langle n, m, p\rangle$，则$\beta(G)$称作群$G$ 的三乘积容量。

**定理 3.19** ([9] 定理4.1). *若$G \neq 1$是一个有限群，那么$\beta(G)^{\omega/3} \leq D_\omega(G)$。*

**定理 3.20.** *若$G$是一个交换群且$G$实现了$\langle 5, 5, 5\rangle$，则有$R(G) \geq 125$。*

**证明.** 如果$G$是交换的且非平凡($|G| \neq 1$)，那么$b(G) = 1$ 并且由定理3.18 我们有：$R(G) = |G|$。而当$G$交换时，由三乘积性质保证映射$S \times T \times U \to G$是单射（$G$ 通过子集组$(S, T, U)$ 实现三乘积性质），则有$|G| \geq 125$，则有$R(G) \geq 125$。 □

**注 24.** 因为我们要找的是$\underline{R}(G) < 100 < 125$ 的群$G$，所以从现在起只需要考虑非交换群。

**引理 3.21** (交换群判断条件). *（1）若$|G|$ 是一个素数，那么$G$ 是交换的。*
*（2）若$|G| = pq$，这里$p$ 和$q$都是素数，$p < q$, 若$q \neq 1 (mod\ p)$，那么$G$ 就是交换的。*
*（3）若$|G| = pq^2$，$p$和$q$是两个不同的素数且$p$ 不能整除$|Aut(G)|$，那么$G$ 就是*

交换的。
(4) 若$|G| = pqr$，$p, q$ 和$r$是三个相互不同的素数且$q < r$，$r \not\equiv 1(mod\ q)$，$qr < p$，$p \not\equiv 1(mod\ r)$，$p \not\equiv 1(mod\ q)$，那么$G$就是交换的。

**定理 3.22** ([15] 引理3.3). 如果$G$是非交换的，那么$T(G) \leq \frac{5}{8}|G|$。等号成立时有$|G : Z(G)| = 4$。这里$Z(G)$为群$G$的中心。

**注 25.** 那么如果我们结合考虑定理3.18和定理3.22，就有：
$R(G) \geq 2|G| - T(G) \geq (11/8)|G|$
因为我们要下式成立：$R(G) < 100$，则有：
$(11/8)|G| < 100$
$|G| \leq 72$。

**定义 3.11** ($\langle 5,5,5\rangle$C1竞争者，[15] 定义3.2). 一个群$G$如果实现了$\langle 5,5,5\rangle$ 且满足$\underline{R}[G] < 100$，那么我们称这个群是一个$\langle 5,5,5\rangle$ *C1* 竞争者。本节后面简称之为*C1* 竞争者。

**命题 3.23** ([15] 命题3.8). 如果群$G$是一个*C1* 竞争者，那么$45 \leq |G| \leq 72$。

**证明.** 由引理2.21我们知道，$|G| \geq 5 \cdot (5 + 5 - 1) = 45$。由定理3.22 的结论，有$|G| \leq 72$。 □

**定义 3.12** ([15] 定义3.4). 令$G$是一个有三乘积子集组$(S, T, U)$ 的群，假设$H$是一个$G$的指数为2的子群。我们定义$S_0 = S \cap H, T_0 = T \cap H, U_0 = U \cap H$，$S_1 = S \setminus H$，$T_1 = T \setminus H$ 和$U_1 = U \setminus H$。

**引理 3.24** ([15] 引理3.5). 若群$G$实现了$\langle 5,5,5\rangle$。如果$G$ 有一个指数为2的子群$H$，那么$H$一定实现了$\langle 3,3,3\rangle$。

**证明.** 假设群$G$通过子集组$(S, T, U)$实现了$\langle 5,5,5\rangle$。若$|S_0| < |S_1|$，那么对任意$a \in S_1$，用$Sa^{-1}$ 取代$S$。这会使得$S_0$和$S_1$互换。因此不妨设$|S_0| \geq |S_1|$，$|T_0| \geq |T_1|$，$|U_0| \geq |U_1|$。现在$(S_0, T_0, U_0)$ 就是$H$的三乘积子集组，由于$S_0$，$T_0$，$U_0$ 都至少有三个元素，那么就有结论：$H$ 实现了$\langle 3,3,3\rangle$。 □

**引理 3.25** ([15] 引理3.6). 假设$G$有三乘积子集组$(S, T, U)$。令$H$ 是$G$ 的指数为2的一个交换子群。那么下面几个等式成立。

(1) $|S_0^{-1}T_0U_0| = |S_0||T_0||U_0|$;
(2) $|S_1^{-1}T_1U_0| \geq |S_1||T_1|$;
(3) $|S_1^{-1}U_1| = |S_1||U_1|$;
(4) $S_0^{-1}T_0U_0 \cap S_1^{-1}T_1U_0 = \emptyset$;
(5) $S_0^{-1}T_0U_0 \cap S_1^{-1}U_1T_0 = \emptyset$;
(6) $S_1^{-1}T_1U_0 \cap S_1^{-1}U_1T_0 = \emptyset$。

**引理 3.26** ([15] 定理3.7). *若群$G$实现了$\langle 5,5,5\rangle$，那么$G$ 就不可能有指数为2的交换子群。*

**证明.** 假设$G$有一个指数为2的交换子群$H$ 且$G$ 实现了通过三乘积子集组$(S,T,U)$实现了$\langle 5,5,5\rangle$。和之前同样定义$S_0,T_0,U_0,S_1,T_1,U_1$。那么，像上面证明的一样，我们可以假设$|S_0| \geq 3$，$|T_0| \geq 3$和$|U_0| \geq 3$。不影响一般性我们可以假设$|S_0| \geq |T_0|$ 和$|S_0| \geq |U_0|$。现在由于$|G| \leq 72$，就有$|H| \leq 36$。从引理3.25 可得：

$$\begin{aligned} 36 \geq |H| &\geq |S_0^{-1}T_0U_0 \cup S_1^{-1}U_1T_0 \cup S_1^{-1}T_1U_0| \\ &= |S_0||T_0||U_0| + |S_1^{-1}U_1T_0| + |S_1^{-1}T_1U_0| \\ &\geq |S_0||T_0||U_0| + |S_1||U_1| + |S_1||T_1| \end{aligned} \tag{3.4}$$

由3.4 式，若$|T_0| \geq 4$ 或$|U_0| \geq 4$，均可推出$|S_0| \geq 4$，从而有$|H| \geq 48$，矛盾！因此$|T_0| = |U_0| = 3$。若$|S_0| \geq 4$，则$|H| \geq 40$，矛盾！因此$|S_0| = |T_0| = |U_0| = 3$，从而推出$|H| \geq 27 + 4 + 4 = 35$, 因此$|H| \in \{35, 36\}$。若$Q(S_0), Q(T_0), Q(U_0)$ 中的两个是阶为4的群，那么它们会生成一个阶为16 的$H$的子群，这是不可能的。因此，在必要的时候改换$S,T,U$ 的顺序，就不妨假设$Q(T_0), Q(U_0)$ 都不是阶为4的子群。
现在考虑$S_1^{-1}U_1T_0$。记$X = S_1^{-1}U_1$, 则$|X| = 4$。若$|XT_0| = 4$, 则有$XT_0 = X$,因此$X\langle T_0\rangle = X$, 这说明$X$ 是$\langle T_0\rangle$ 陪集的并。特别地，$4 = |X|$ 可以被$\langle T_0\rangle$ 的阶整除。但$T_0$至少有3个元素，因此$\langle T_0\rangle$ 阶为$4$。通过检验可得$Q(T_0) = \langle T_0\rangle$，这与$Q(T_0)$不是一个阶为4的子群的事实相矛盾。因此我们证明了$|S_1^{-1}U_1T_0| > 4$。一个类似的推理过程可以得到$|S_1^{-1}T_1U_0| > 4$。将结果代回*3.4* 式，有$|H| \geq 27 + 5 + 5 = 37$，矛盾出现！因此，阶小于等于72的群不可能同时实现$\langle 5,5,5\rangle$，又有指数为2的交换子群。 □

**定理 3.27** ([15] 定理3.9). *阶为64的群都不是C1竞争者。*

**证明.** 首先，经过GAP辅助计算$R(G)$的下界（注23）排除$R(G) \geq 100$的群，然后排除掉那些有指数为2的交换子群的群，最终得到了一个可能是C1竞争者的64阶群的列表。如果列表中有群实现了$\langle 5,5,5\rangle$，则它的阶为32的子群就肯定实现了$\langle 3,3,3\rangle$。通过直接计算，发现列表中的这些64阶群都至少有一个32阶子群不能实现$\langle 3,3,3\rangle$。因此，阶为64的群都不是C1竞争者。 □

**定理 3.28** ([15] 定理3.10). *所有可能的C1竞争者如下列出（按照群在GAP软件中的序号）:（GAP ID）*
$[48,3],[48,28],[48,29],[48,30],[48,31],[48,32]$
$[48,33],[48,48],[48,49],[48,50],[54,10],[54,11].$

**证明.** 首先，由前述命题可知我们只需要考虑阶在45 和72 之间的群。通过一个简单的GAP辅助计算$R(G)$ 的下界（注23），排除掉$R(G)$的下界大于99的那些群。接着，排除掉那些有指数为2的交换子群的群，并且排除掉所有阶为64的群。通过以上几步排除，剩下的群就只有20个了。而且如果一个群的阶为48且是一个C1竞争者那么它的任一个24阶子群必须实现$\langle 3,3,3\rangle$；通过对24阶群是否实现$\langle 3,3,3\rangle$ 的直接计算，又排除了列表中的10个48阶群，上述所列是剩下来的可能的C1 竞争者。 □

**计算结果** 接下来我们要做的就是针对这12个可能的C1竞争者应用精确算法，看它们是否能实现$\langle 5,5,5\rangle$。计算结果显示，这12个群都不能实现$\langle 5,5,5\rangle$。因此，不存在可以在实现$\langle 5,5,5\rangle$ 三乘积性质且乘秩小于100 的群。

## 3.3 $6\times 6$ 矩阵乘法的群理论方法

**问题背景** 本部分内容主要由上一节研究的问题引申而来，接着文献[15] 结尾提出的开放问题，考虑是否存在可以实现$\langle 6,6,6\rangle$ 三乘积性质且它的秩小于161（[28] 表格3）的群，考虑$R(6)$ 能否通过群理论方法（这里特别指通过三乘积方法）得到比该表格所列已有算法（Strassen算法）更优的结果。

**问题陈述** 是否存在一个阶小于90的群可以实现$\langle 6,6,6\rangle$ 三乘积性质且该群的秩的下界小于161（[28]表格3）?

**解决方案** 由于搜索空间太大，我们的主要思想第一步是通过很多必要条件来缩减搜索空间。接下来我们研究有哪些必要条件可以缩减搜索空间。

**定理 3.29.** *若$G$是一个交换群且$G$实现了$\langle 6,6,6\rangle$，则有$R(G)\geq 216$。*

**证明.** 如果$G$是交换的且非平凡($|G|\neq 1$)，那么$b(G)=1$ 并且由定理?? 我们有：$R(G)=|G|$。而当$G$交换时，由三乘积性质保证映射$S\times T\times U\to G$是单射（$G$ 通过子集组$(S,T,U)$ 实现三乘积性质），则有$|G|\geq 216$，则有$R(G)\geq 216$。 □

**注 26.** 因为我们要找的是$\underline{R}(G)<161<216$ 的群$G$，所以从现在起只需要考虑非交换群。

**定义 3.13** ($\langle 6,6,6\rangle$C1竞争者). 一个群$G$如果实现了$\langle 6,6,6\rangle$ 且满足$\underline{R}[G]<161$，那么我们称这个群是一个$\langle 6,6,6\rangle$*C1 竞争者*。在本节中后面简称之为*C1 竞争者*。

**命题 3.30.** *如果群$G$是一个C1竞争者，那么$66\leq|G|\leq 117$。*

**证明.** 再结合考虑定理3.18和定理3.22，就有：
$R(G)\geq 2|G|-T(G)\geq(11/8)|G|$
因为我们要下式成立：$R(G)<161$，则有：
$\frac{11}{8}|G|<161$，推出
$|G|\leq 117$。且由引理2.21我们知道，$|G|\geq 6\cdot(6+6-1)=66$。证毕。 □

**定义 3.14** ([15]，定义3.4). 令$G$是一个有三乘积子集组$(S,T,U)$ 的群，假设$H$是一个$G$的指数为2的子群。我们定义$S_0=S\cap H, T_0=T\cap H, U_0=U\cap H$，$S_1=S\setminus H$，$T_1=T\setminus H$ 和$U_1=U\setminus H$。

**引理 3.31.** *若群$G$实现了$\langle 6,6,6\rangle$。如果$G$ 有一个指数为2的子群$H$，那么$H$一定实现了$\langle 3,3,3\rangle$。*

**证明.** 假设群$G$通过子集组$(S,T,U)$实现了$\langle 6,6,6\rangle$。若$|S_0|<|S_1|$，那么对任意$a\in S_1$，用$Sa^{-1}$ 取代$S$。这会使得$S_0$和$S_1$互换。因此不妨设$|S_0|\geq|S_1|$，$|T_0|\geq|T_1|$，$|U_0|\geq|U_1|$。现在$(S_0,T_0,U_0)$ 就是$H$的三乘积子集组，由于$S_0$，$T_0$，$U_0$ 都至少有三个元素，则有结论：$H$ 实现了$\langle 3,3,3\rangle$。 □

将上述证明推广以后可得下面的定理：

**定理 3.32.** *若群$G$实现了$\langle n,n,n\rangle$。当$n$为奇数时，如果$G$有一个指数为2的子群$H$，那么$H$一定实现了$\langle \frac{n+1}{2},\frac{n+1}{2},\frac{n+1}{2}\rangle$；当$n$为偶数时，如果$G$有一个指数为2的子群$H$，那么$H$一定实现了$\langle \frac{n}{2},\frac{n}{2},\frac{n}{2}\rangle$。*

**引理 3.33** ([15]，引理3.6). *假设$G$有三乘积子集组$(S,T,U)$。令$H$是$G$的指数为2的一个交换子群。那么下面几个等式成立：*

*(1)* $|S_0^{-1}T_0U_0| = |S_0||T_0||U_0|$；

*(2)* $|S_1^{-1}T_1U_0| \geq |S_1||T_1|$；

*(3)* $|S_1^{-1}U_1| = |S_1||U_1|$；

*(4)* $S_0^{-1}T_0U_0 \cap S_1^{-1}T_1U_0 = \emptyset$；

*(5)* $S_0^{-1}T_0U_0 \cap S_1^{-1}U_1T_0 = \emptyset$；

*(6)* $S_1^{-1}T_1U_0 \cap S_1^{-1}U_1T_0 = \emptyset$。

**引理 3.34.** *若群$G$实现了$\langle 6,6,6\rangle$并且$|G| < 90$，那么$G$就不可能有指数为2的交换子群。*

**证明.** 假设$G$有一个指数为2的交换子群$H$且$G$实现了通过三乘积子集组$(S,T,U)$实现了$\langle 6,6,6\rangle$。和之前同样定义$S_0,T_0,U_0,S_1,T_1,U_1$。那么，像上面证明的一样，我们可以假设$|S_0| \geq 3$，$|T_0| \geq 3$和$|U_0| \geq 3$。不影响一般性我们可以假设$|S_0| \geq |T_0|$和$|S_0| \geq |U_0|$。现在由于$|G| < 90$，就有$|H| < 45$。从引理3.33可得：

$$\begin{aligned} 45 > |H| &\geq |S_0^{-1}T_0U_0 \cup S_1^{-1}U_1T_0 \cup S_1^{-1}T_1U_0| \\ &= |S_0||T_0||U_0| + |S_1^{-1}U_1T_0| + |S_1^{-1}T_1U_0| \\ &\geq |S_0||T_0||U_0| + |S_1||U_1| + |S_1||T_1| \end{aligned} \tag{3.5}$$

若$|U_0| \geq 4$，那么由$|H| \geq 64$，矛盾出现！所以$|U_0| = 3$：

(1) $|U_0| = 3 = |T_0| = |S_0|$，则由不等式3.5有：$|H| \geq 45$，矛盾；

(2) $|U_0| = 3 = |T_0|$，$|S_0| = 4$，则由不等式3.5有：$|H| \geq 48$，矛盾；

(3) $|U_0| = 3$，$|T_0| = |S_0| = 4$，则由不等式3.5有：$|H| \geq 58$，矛盾；

(4) $|U_0| = 3 = |T_0|,|S_0| = 5$，则由不等式3.5有：$|H| \geq 51$，矛盾；

(5) $|U_0| = 3$，$|T_0| = 4,|S_0| = 5$，则由不等式3.5有：$|H| \geq 65$，矛盾；

(6) $|U_0| = 3$，$|T_0| = |S_0| = 5$，则由不等式3.5有：$|H| \geq 79$，矛盾；

（7）$|U_0|=3=|T_0|$，$|S_0|=6$，则由不等式3.5有：$|H|\geq 54$，矛盾；
（8）$|U_0|=3|T_0|=4,|S_0|=6$，则由不等式3.5 有：$|H|\geq 72$，矛盾；
（9）$|U_0|=3,|T_0|=5,|S_0|=6$，则由不等式3.5有：$|H|\geq 90$，矛盾；
（10）$|U_0|=3,|T_0|=|S_0|=6$，则由不等式3.5 有：$|H|\geq 108$，矛盾。
因此，若群$G$实现了$\langle 6,6,6\rangle$ 并且$|G|<90$，那么$G$ 就不可能有指数为2的交换子群。 □

**注 27.** 目前为止，经过上述必要条件的排筛选，以及GAP 辅助计算$R(G)$的下界（注23）排除$R(G)\geq 161$ 的群。可得所有阶小于90 的群中，可能的C1竞争者用它们的GAP ID（即它们在GAP 软件中的序号）列出如下（共56 个）：
(68,3),(72,3),(72,15),(72,16),(72,19),(72,20),(72,21),(72,22),(72,23),(72,24),(72,25),
(72,39),(72,40),(72,41),(72,42),(72,43),(72,44),(72,45),(72,46),(72,47),(75,2),(78,1),
(78,2),(80,3),(80,15),(80,18),(80,28),(80,29),(80,30),(80,31),(80,32),(80,33),(80,34),
(80,39),(80,40),(80,41),(80,42),(80,49),(80,50),(81,3),(81,4),(81,6),(81,7),(81,8),
(81,9),(81,10),(81,12),(81,13),(81,14),(84,1),(84,2),(84,7),(84,8),(84,9),(84,10),(84,11).

**定理 3.35** ([10] 定理1.8). 假设群$G$实现了$\langle n,m,p\rangle$，它的特征标是$\{d_i\}$。那么$(nmp)^{\omega/3}\leq \sum_i {d_i}^{\omega}$。

**注 28.** 若上述C1竞争者可实现$\langle 6,6,6\rangle$，则可应用定理3.35，推出关于$\omega$ 上界的如下结论（只列出非平凡解的情况）：
$(72,3)/(72,25)\Rightarrow \omega\leq 2.69631424$,
$(72,16)/(72,47)\Rightarrow \omega\leq 2.77655751$,
$(72,20)/(72,21)/(72,46)\Rightarrow \omega\leq 2.888690173$,
$(72,22)/(72,23)/(72,24)\Rightarrow \omega\leq 2.916302468$,
$(72,42)\Rightarrow \omega\leq 2.849410311$,
$(81,3)/(81,4)/(81,6)/(81,12)/(81,13)/(81,14)\Rightarrow \omega\leq 2.84509229$,
$(84,10)\Rightarrow \omega\leq 2.965002029$.

**注 29.** 即使我们由一个群的三乘积性质推出了$\omega$ 的非平凡上界，$R(G)$仍然不容易具体求出，可见下一步工作任务依旧艰巨。

**命题 3.36** ([10]). 若$G\neq 1$是一个有限群，那么有：$\beta(G)^{\omega/3}\leq D_\omega(G)$。这个不等式可以推出$\omega$的非平凡上界当且仅当$\beta(G)>D_3(G)$。

**注 30.** 当我们应用命题3.36来推导$\omega$的非平凡解时，针对$\langle 6,6,6\rangle$ 三乘积的情况，有可能对某群$G$有：$216 \le \beta(G) \le D_3(G)$，从而得到$\omega$的平凡解，但该群的秩$\underline{R}(G) < 216$（或$\underline{R}(G) < 161$）仍成立（即秩的值非平凡）。因此我们不能通过命题3.36 来对注27 中剩下的可能的C1竞争者进行进一步排除。

**总结**

对于进一步工作，我们认为比较可行的一个方案是将文献[15] 中的精确算法并行化，然后对上述56 个群进行直接验证。不过此方法比较“笨拙”，主要难点在于并行化程序设计的技巧。同时，我们也致力于在理论上寻找更多有关群$\langle 6,6,6\rangle$三乘积性质的必要（筛选）条件。

# 第四章　三乘积组构造原则及应用

## 4.1　群$C_6 \times A_4$

这部分主要分析一个72阶群的三乘积等相关性质，在GAP 软件中，该群表示为$G := SmallGroup(72, 47)$。记该群为$G$，该群结构为$C_6 \times A_4$，即$C_2 \times C_3 \times A_4$。在GAP 软件中群$H_1 = SmallGroup(36, 11)$，$H_2 = SmallGroup(36, 3)$，$H_1$同构于$C_3 \times A_4$，$H_2$结构为$C_2^2 \rtimes C_9$。

**引理 4.1.** *群$H_1, H_2$均不能实现$\langle 4, 4, 4\rangle$。*

**证明.** 通过文献[15]中的精确搜索算法在GAP 软件中直接计算得到的结果。 □

**定理 4.2.** *$A_4$可实现$\langle 3, 3, 2\rangle$，$\beta(A_4) = 18$。*

**证明.** 搜索群的极大三乘积组的蚁群算法（在第二章有介绍）在集群上计算得到的结果显示$A_4$ 可实现$\langle 3, 3, 2\rangle$。可构造证明如下：
构造$A_4$的子集合$S, T, U$：
$S : \{(1), (13)(24)\}$;
$T : \{(1), (243), (234)\}$;
$U : \{(1), (124), (142)\}$.
根据三乘积性质的定义验证可知上述集合$S, T, U$满足该性质。
由文献[19]推论3.2有

$$\beta(A_4) \leq (\frac{1 + \sqrt{1 + 8 \cdot 12}}{4})^3$$

可得$\beta(A_4) \leq 19$，若$\beta(A_4) = 19$，因为19 是质数，因此只能是$A_4$实现$\langle 19, 1, 1\rangle$，而这说明群$A_4$ 有一个阶为19的子集合，但$|A_4| = 12 < 19$，矛盾！因此$\beta(A_4) = 18$。证毕。 □

由上述定理可尝试构造群$G$的三乘积组，有如下结果：

**命题 4.3.** *在不增添新的$A_4$中元素的情况下，可构造证明群$G$ 的$\langle 6, 3, 3\rangle$三乘积性质。*

**证明.** 设$A_4$通过子集组$S,T,U$实现$\langle 3,2,3\rangle$，
$S=\{1,s_1,s_2\}$;
$T=\{1,t_1\}$;
$U=\{1,u_1,u_2\}$.
因$G=C_6\times A_4$，这里$C_6$是6阶循环群，且其中有一个单位元，一个二阶元，两个三阶元和两个六阶元，可表示为：
$C_6=\{1,\bar{2}^{(1)},\bar{3}^{(1)},\bar{3}^{(2)},\bar{6}^{(1)},\bar{6}^{(2)}\}$。
可构造$G$ 的子集组$S_1,T_1,U_1$如下（在不增添新的$A_4$ 中元素的情况下）：
$S_1:=\{(1,1),(1,s_1),(1,s_2),(\bar{2}^{(1)},1),(\bar{2}^{(1)},s_1),(\bar{2}^{(1)},s_2)\}$;
$T_1:=\{(1,1),(1,t_1),(\bar{3}^{(1)},1),(\bar{3}^{(2)},1),(\bar{3}^{(1)},t_1),(\bar{3}^{(2)},t_1)\}$;
$U_1:=\{(1,1),(1,u_1),(1,u_2)\}$.
可以验证，上述三个$G$的子集合满足三乘积性质，但在不增添新的$A_4$中元素的情况下，如果继续向集合$U_1$ 中增添元素，则会产生矛盾！$U_1$中的$A_4$部分添入$S$或$T$中的元素显然不行，就以添入元素$(\bar{6}^{(1)},u_1)$为例，此时有：
$(1,1)(\bar{2}^{(1)},1)^{-1}(1,1)(\bar{3}^{(1)},1)^{-1}(\bar{6}^{(1)},u_1)(1,u_1)^{-1}=1$，
与$S_1,T_1,U_1$的三乘积性质矛盾！（这里6阶循环群中的乘法表不失一般性，可以含有$(\bar{2}^{(1)})\cdot(\bar{3}^{(2)})(\bar{6}^{(1)})=1$）其他情况经验证均会产生类似矛盾，因此此种方法（增添新的$A_4$ 中元素到新集合的右边一列）的极大构造结果如上所示，有$G$可实现$\langle 6,3,3\rangle$ 的结论。证毕。 □

**命题 4.4.** *$G$可通过如下集合$S_1,T_1,U_1$实现$\langle 6,6,3\rangle$：*
$S_1:=\{(1,1),(1,(13)(24)),(\bar{3}^{(1)},1),(\bar{3}^{(1)},(13)(24)),(\bar{3}^{(2)},1),(\bar{3}^{(2)},(13)(24))\}$;
$T_1:=\{(1,1),(1,(243)),(1,(234)),(\bar{2}^{(1)},1),(\bar{2}^{(1)},(243)),(\bar{2}^{(1)},(234))\}$;
$U_1:=\{(1,1),(1,(124)),(1,(142))\}$.

**证明.** 根据三乘积性质的定义可以验证上述命题成立。 □

记$H:=C_3\times A_4$，在GAP软件中，$H:=SmallGroup(36,11)$。

**定理 4.5.** *群$H$可实现$\langle 6,4,3\rangle$。*

**证明.** 构造$H$的子集$S,T,U$如下：
$S:=\{(1,1),(1,(13)(24)),(\bar{3}^{(1)},(13)(24)),(\bar{3}^{(2)},(13)(24)),(\bar{3}^{(1)},1),(\bar{3}^{(2)},1)\}$;

$T := \{(1,1),(1,(14)(23)),(1,(143)),(1,(134))\}$;
$U := \{(1,1),(1,(123)),(1,(132))\}$.
上面每个括号括起来二元组，前面一个元素$x \in C_3$，$C_3$ 是3阶循环群，（不妨设$C_3 = \{1, 3^{(1)}, 3^{(2)}\}$，这里1 是单位元，$3^{(1)}, 3^{(2)}$分别表示$C_3$中的两个三阶元）后面一个元素$y \in A_4$，$A_4$表示4 阶偶置换群。可验证上面构造出的$S, T, U$ 满足三乘积性质，则群$H$ 实现了$\langle 6,4,3\rangle$。 □

**推论 4.6.** *群$G$可实现$\langle 12,4,3\rangle$，$\langle 8,6,3\rangle$，$\langle 6,6,4\rangle$。*

**证明.** 因为$G = H \times C_2$，$C_2$为2阶循环群，显然有$C_2$ 实现$\langle 2,1,1\rangle$，结合定理4.5结论以及（[10]，引理1.5）可知$G$ 可实现$\langle 12,4,3\rangle$，$\langle 8,6,3\rangle$及$\langle 6,6,4\rangle$。 □

**命题 4.7.** *由$H$实现了$\langle 6,4,3\rangle$可得一个平凡解$\omega \leq 3.5421$。*

**证明.** 由GAP辅助计算可知$H$的特征标为9个1和3个3，由（[10]，定理1.8）有，$72^{\omega/3} \leq 9 + 3 \cdot 3^{\omega}$，解之可得：$\omega \leq 3.5421$。 □

**命题 4.8.** *由$G$实现了$\langle 12,4,3\rangle$（或$\langle 8,6,3\rangle$或$\langle 6,6,4\rangle$）可得一个平凡解$\omega \leq 3.3428$。*

**证明.** 由GAP辅助计算可知$G$的特征标为18个1和6个3，由[10]，定理1.8 有，$144^{\omega/3} \leq 18 + 6 \cdot 3^{\omega}$，解之可得：$\omega \leq 3.3428$。 □

GAP软件结算部分结果展示如下：

**定理 4.9.** *如下群（以$GAP\ ID$表示）可实现$\langle 4,4,4\rangle$：(72,47),(72,16),(68,3),(72,3),(72,19),(72,20)。*

**证明.** 算法来自文献[15]，用GAP软件在中科院数学机械化实验室的机群上直接计算，目前已出结果如上所述，更多结果还在计算中。 □

**注 31.** 上述群的结构简述如下，

在GAP软件中，$G_1 = SmallGroup(72,47)$，它的结构是$C_6 \times A_4$，这里$C_6$是6阶循环群，$A_4$是4 阶偶置换群。

在GAP软件中，$G_2 = SmallGroup(72,16)$，它的结构是$C_2 \times (C_2^2 \rtimes C_9)$，这里这里$\rtimes$表示半直积，相当于下面群结构中出现的: 符号，$C_2$ 是2阶循环群，

$C_9$是9 阶循环群。

在GAP软件中，$G_3 = SmallGroup(68, 3)$，它的结构是$C_{17} : C_4$，$C_{17}$与$C_4$的半直积，这里$C_{17}$是17 阶循环群，$C_4$ 是4 阶循环群。

在GAP软件中，$G_4 = SmallGroup(72, 3)$，它的结构是$Q_8 : C_9$，$Q_8$与$C_9$的半直积，这里$Q_8$ 是8四元群，$C_9$是9 阶循环群。

在GAP软件中，$G_5 = SmallGroup(72, 19)$，它的结构是$(C_3 \times C_3) : C_8$，$C_3 \times C_3$与$C_8$的半直积，这里$C_3$是3 阶循环群，$C_8$ 是8阶循环群。

在GAP软件中，$G_5 = SmallGroup(72, 20)$，它的结构是$(C_3 : C_4) \times S_3$，$C_3$与$C_4$ 的半直积和$S_3$ 的直积，这里$C_3$ 是3阶循环群，$C_4$ 是4阶循环群，$S_3$是3阶对称群。

## 4.2 构造三乘积组

本部分内容主要分析研讨如何从群$B$的三乘积组出发，构建群$D := C_2 \times B$的三乘积组，也有关于群$F := C_n \times B$三乘积性质的一些推广结论（这里$C_n$为$n$阶循环群）。

**引理 4.10** ([17]引理2.1). *若$S, T, U \subset G$ 满足三乘积性质，则有$Q(X) \cap Q(Y) = \{1\}$，$\forall X, Y \in \{S, T, U\}$且$X \neq Y$。*

**证明.** 不失一般性，不妨以$X = T, Y = U$为例。若$\{Q(T) \cap Q(U)\} \setminus \{1\} \neq \phi$，可设$1 \neq x \in Q(T) \cap Q(U)$。则$t_1 t_2^{-1} = u_1 u_2^{-1} = x$且$t_1 \neq t_2, u_1 \neq u_2$，这里$t_1, t_2 \in T, u_1, u_2 \in U$。那么$\forall x_1 \in S$，有$x_1 x_1^{-1} t_1 t_2^{-1} u_2 u_1^{-1} = 1$，但$t_1 \neq t_2, u_1 \neq u_2$。这与$S, T, U$的三乘积性质相矛盾！证毕。 □

从群$B$的三乘积组出发，构建群$C_n \times B$ 的三乘积组：

**引理 4.11.** *若$S, T, U$为群$B$的一个基本三乘积组，$S_1 = \{(1, s) | s \in S\}$，$T_1 = \{(1, t) | t \in T\}$，$U_1 = \{(1, u) | u \in U\}$，则$S_1, T_1, U_1$为群$C_2 \times B$的三乘积组（这里$C_2$为2阶循环群）。*

**证明.** 若$(1, s_1)(1, s_2)^{-1}(1, t_1)(1, t_2)^{-1}(1, u_1)(1, u_2)^{-1} = 1$，则有$s_1 s_2^{-1} t_1 t_2^{-1} u_1 u_2^{-1} = 1$，由$S, T, U$ 为群$B$的一个三乘积组，有$s_1 = s_2$，$t_1 = t_2$，$u_1 = u_2$，则

有$(1,s_1)=(1,s_2)$，$(1,t_1)=(1,t_2)$，$(1,u_1)=(1,u_2)$，即$S_1,T_1,U_1$为群$C_2\times B$的三乘积组。证毕。 □

**引理 4.12** (推广). *若$S,T,U$为群$B$的一个基本三乘积组，$S_1=\{(1,s)|s\in S\}$，$T_1=\{(1,t)|t\in T\}$，$U_1=\{(1,u)|u\in U\}$，则$S_1,T_1,U_1$为群$C_n\times B$的三乘积组(这里$C_n$为$n$阶循环群)。*

**证明.** 证明思路同引理4.11。 □

接下来，令$S_1\subset S_2$，$T_1\subset T_2$，$U_1\subset U_2$，下面我们讨论$S_2,T_2,U_2\subset D$的三乘积相关性质。设$S_2$ 限制在$B$上与$S_1$限制在$B$上相比新添加的元素集合为$X$，$T_2$限制在$B$ 上与$T_1$限制在$B$上相比新添加的元素集合为$Y$，$U_2$限制在$B$上与$U_1$限制在$B$上相比新添加的元素集合为$Z$。为便于理解，现将$S_2,T_2,U_2$以$\langle 6,6,6\rangle$为例示意如下：
$S_2:=\{(1,1),(1,s_1),(1,s_2),(2,x_1),(2,x_2),(2,x_3)\}$;
$T_2:=\{(1,1),(1,t_1),(1,t_2),(2,y_1),(2,y_2),(2,y_3)\}$;
$U_2:=\{(1,1),(1,u_1),(2,z_1),(2,z_2),(2,z_3),(2,z_4)\}$。
这里，$S=\{1,s_1,s_2\}$，$T=\{1,t_1,t_2\}$，$U=\{1,u_1\}$，
$X=\{x_1,x_2,x_3\}$，$Y=\{y_1,y_2,y_3\}$，$Z=\{z_1,z_2,z_3,z_4\}$，且$C_2=\{1,2\}$为2阶循环群，1表示其中的单位元，2表示其中的2阶元。

**定理 4.13.** *当$S_2,T_2,U_2\subset D$满足三乘积性质时，若$S\cap X\neq\phi$，则有$Y\cap T=\phi$以及$Z\cap U=\phi$。*

**证明.** 分两种情况：
(1) $S_2$限制在$B$上重复的元素中有单位元。不妨设$x_1=s_1$，由$T,U$的广义对称性，不妨设$y_1=t_1$ （$y_1=1$时也同理可证)。则有：

$$(1,s_1)(2,x_1)^{-1}(1,t_1)(2,y_1)^{-1}(1,1)(1,1)^{-1}=1,$$

但显然$(1,s_1)\neq(2,x_1)$，与$S_2,T_2,U_2\subset D$满足三乘积性质矛盾!
(2) $S_2$限制在$B$上中重复的元素无单位元。不妨设$x_1=1$，由$T,U$的广义对称，不妨设
$y_1=t_1$ （$y_1=1$时也同理可证)。则有：

$$(1,1)(2,x_1)^{-1}(1,t_1)(2,y_1)^{-1}(1,1)(1,1)^{-1}=1,$$

但显然$(1,1) \neq (2,x_1)$。与$S_2,T_2,U_2 \subset D$ 满足三乘积性质矛盾!
证毕。 □

当我们考虑$Q = C_3 \times B$的三乘积组$S_3,T_3,U_3$时，不妨设$C_3 = \{1,\bar{3}^{(1)},\bar{3}^{(2)}\}$，以$C_3$ 中元素将$S_3,T_3,U_3$ 划分：$S_3|_B = S \cup X_1 \cup X_2$，$T_3|_B = T \cup Y_1 \cup Y_2$，$U_3|_B = U \cup Z_1 \cup Z_2$，这里$X_1,Y_1,Z_1$分别是$S_3,T_3,U_3$ 中$C_3$中元素为$\bar{3}^{(1)}$时对应的$B$中元素集合，$X_2,Y_2,Z_2$分别是$S_3,T_3,U_3$ 中$C_3$中元素为$\bar{3}^{(2)}$时对应的$B$中元素集合。记$X = X_1 \cup X_2$，$Y = Y_1 \cup Y_2$，$Z = Z_1 \cup Z_2$。

**定理 4.14** (推广). *当$S_3,T_3,U_3 \subset Q$满足三乘积性质时，若$S \cap X \neq \phi$，则有$Y \cap T = \phi$ 以及$Z \cap U = \phi$。*

**证明.** 不妨设集合$S_3,T_3$限制在$B$上后对应的元素各有一个重复，则可分以下三种情况：
（1）$s_1 \in X_1 \cap S \neq \phi$且$t_1 \in Y_1 \cap T \neq \phi$。此时，有

$$(1,s_1)(\bar{3}^{(1)},s_1)^{-1}(\bar{3}^{(1)},t_1)(1,t_1)^{-1}(1,u_1)(1,u_1)^{-1} = 1,$$

由$S_3,T_3,U_3 \subset Q$满足三乘积性质有：$(1,s_1) = (\bar{3}^{(1)},s_1)$，显然矛盾!
（2）$s_1 \in X_2 \cap S \neq \phi$且$t_1 \in Y_2 \cap T \neq \phi$。此时，有

$$(1,s_1)(\bar{3}^{(2)},s_1)^{-1}(\bar{3}^{(2)},t_1)(1,t_1)^{-1}(1,u_1)(1,u_1)^{-1} = 1,$$

由$S_3,T_3,U_3 \subset Q$满足三乘积性质有：$(1,s_1) = (\bar{3}^{(2)},s_1)$，显然矛盾!
（3）$s_1 \in X_1 \cap S \neq \phi$且$t_1 \in Y_2 \cap T \neq \phi$。此时，有

$$(1,s_1)(\bar{3}^{(1)},s_1)^{-1}(1,t_1)(\bar{3}^{(2)},t_1)^{-1}(1,u_1)(1,u_1)^{-1} = 1,$$

由$S_3,T_3,U_3 \subset Q$满足三乘积性质有：$(1,s_1) = (\bar{3}^{(1)},s_1)$，显然矛盾!
证毕。 □

**命题 4.15.** *当$S_2,T_2,U_2 \subset D$满足三乘积性质时，群$B$的子集组$(S,Y,U)$，$(S,Y,Z)$，$(S,T,Z)$，$(X,T,U)$，$(X,T,Z)$，$(X,Y,U)$，$(X,Y,Z)$均满足三乘积性质。*

**证明.** 因为在每个集合中取两个元素时，$C_2$中的两个2 阶元素相乘又变成了单位元，因此在$B$中取的元素须满足该性质。以$S,Y,U$ 为例来证明，若$S,Y,U$不

满足三乘积性质，则存在$s_1 s_2^{-1} y_1 y_2^{-1} u_1 u_2^{-1} = 1$，记为(1) 式，且$s_1 \neq s_2$，$y_1 \neq y_2$，$u_1 \neq u_2$ 三个不等式中至少一个成立，由(1) 式有

$$(1, s_1)(1, s_2)^{-1}(2, y_1)(2, y_2)^{-1}(1, u_1)(1, u_2)^{-1} = 1,$$

由$S_2, T_2, U_2 \subset D$满足三乘积性质，可得：$s_1 = s_2$ 且$y_1 = y_2$且$u_1 = u_2$成立，矛盾出现！证毕。其他情况同理。 □

**注 32.** 因此，在新集合的构造中，从$B$中取的元素要想重复出现，则只能在一个子集（如$S_2$）中重复。

记群$F = C_n \times B$，这里$C_n$是$n$阶循环群。

**命题 4.16** (推广). *对群$F$的三乘积组$S', T', U'$，以$C_n$中不同元素的对应为标准将$S', T', U'$限制在群$B$ 上的元素集合进行划分（即进行分块，这里有重复元素时不进行合并操作）：$S'|_B = \cup_i \bar{S}^{(i)}$，$T'|_B = \cup_i \bar{T}^{(i)}$，$U'|_B = \cup_i \bar{U}^{(i)}$，则群$B$的子集组$(\bar{S}^{(i)}, \bar{T}^{(j)}, \bar{U}^{(k)})$ （从划分后的$S, T, U$中各任取一块组成的三元组）均满足三乘积性质。*

**注 33.** 这里的划分为抽象概念，只在讨论群$F = C_n \times B$的三乘积组时才会出现，且都以此形式出现，与本节中的$S_1$($T_1$,$U_1$)，$S_2$($T_2$,$U_2$)，$S_3$($T_3$,$U_3$)并无关联。

**证明.** 证明思路同命题4.15。 □

下面根据集合$S_2$限制在$B$上对应的元素的重复情况，进一步具体讨论群$B$中的三乘积性质：

**推论 4.17.** *当$S_2, T_2, U_2 \subset D$满足三乘积性质时，若$S_2|_B$中的元素没有重复出现的情况，那么$B$可实现$\langle a, b, c\rangle$，这里$a = \max\{|S|, |X|\}$，$b = \max\{|T|, |Y|\}$，$c = \max\{|U|, |Z|\}$。*

**推论 4.18** (推广). *当$S', T', U' \subset F$满足三乘积性质时，若$S'$中$B$的元素没有重复出现的情况，那么$B$可实现$\langle a, b, c\rangle$，这里$a = \max\{|\bar{S}^{(i)}|\}$，$b = \max\{|\bar{T}^{(i)}|\}$，$c = \max\{|\bar{U}^{(i)}|\}$。*

**注 34.** 这里的$\bar{S}^{(i)}, \bar{T}^{(i)}, \bar{U}^{(i)}$ 为命题4.16中对$S'|_B$，$T'|_B$，$U'|_B$元素的划分。

**证明.** 此推论可以由命题4.16直接得出。 □

**定理 4.19.** 当$S_2, T_2, U_2 \subset D$满足三乘积性质时。若$S_2$限制在$B$上对应的元素有重复出现的情况，此时$B$ 可实现$\langle a, b, c\rangle$，这里$a = r + 1$ （$r$是$S_2$限制在$B$上对应的有重复的元素个数），$b = |T_2|$，$c = |U_2|$。

**证明.** 首先因$S_2, T_2, U_2 \subset D$满足三乘积性质，则由定理4.13可知$T_2$限制在$B$上无重复元素，$U_2$限制在$B$ 上无重复元素。

记$A = \{p, r_{S_2}\}$（$r_{S_2}$表示所有$S_2$ 限制在$B$上对应的重复出现的$B$中元素），$p \in S_2|_B$ 中的$B$ 中元素$\backslash S_2|_B$ 中重复出现的$B$ 中元素，$E = T_2$ 限制在$B$ 上的元素集合，$C = U_2$ 限制在$B$ 上的元素集合。则$A, E, C \subset B$ 满足三乘积性质。在下面的叙述中，$A$中元素用$a_i$表示，$E$中元素用$e_i$ 表示，$C$ 中元素用$c_i$表示。分如下两种情况证明：

（*1*）$a_1, a_2 \in S$，$e_1, e_2 \in T$，$c_1, c_2 \in U$，此时由$S, T, U$的三乘积性质自然得出“若$a_1 a_2^{-1} e_1 e_2^{-1} c_1 c_2^{-1} = 1$，则$a_1 = a_2, e_1 = e_2, c_1 = c_2$”的结论。且根据前述命题，此种情形可推广至只要$A$ 中两个元素都从$S$中取，$E$ 中两个元素都从$T$或都从$Y$中取，$C$中两个元素都从$U$ 或都从$Z$ 中取，均有上述性质成立。

（*2*）若不是上一种情形，则只需讨论$C_2$中所取*6* 个元素在三乘积性质中的乘积不为*1*的情况，因为若他们在三乘积性质的等式中乘积为*1*，此时若$B$中所取*6*个元素在三乘积性质的乘积式中乘积为*1*，则说明$S_2, T_2, U_2$中所取元素乘积为*1*，由它们的三乘积性质可直接得$B$中所取元素符合三乘积性质要求；当$C_2$ 中所取*6*个元素在三乘积性质中的乘积结果不为*1* 时，则有两种情形：*(I)*$(1, s_1)(2, s_2)^{-1}(1, t_1)(2, y_1)^{-1}(1, u_1)(2, z_1)^{-1}$ 中从$B$中取的元素乘积为*1*，即$s_1 s_2^{-1} t_1 y_1^{-1} u_1 z_1^{-1} = 1$，因为$s_1, s_2 \in X \cap S$，则有

$$(1, s_1)(1, s_2)^{-1}(1, t_1)(2, y_1)^{-1}(1, u_1)(2, z_1)^{-1} = 1,$$

由$(S_2, T_2, U_2)$的三乘积性质可知必有$(1, t_1) = (2, y_1)$，显然矛盾!

*(II)*$(1, s_1)(1, s_2)^{-1}(1, t_1)(1, t_2)^{-1}(1, u_1)(2, z_1)^{-1}$ 中从$B$中取的元素乘积为*1*，即

$$s_1 s_2^{-1} t_1 t_2^{-1} u_1 z_1^{-1} = 1,$$

因为$s_1, s_2 \in X \cap S$，则有

$$(1, s_1)(2, s_2)^{-1}(1, t_1)(1, t_2)^{-1}(1, u_1)(2, z_1)^{-1} = 1$$

由$(S_2,T_2,U_2)$的三乘积性质可知必有$(1,s_1)=(2,s_2)$，显然矛盾!
因$|A|=r+1$，$|E|=|T_2|$，$|C|=|U_2|$，定理得证。 □

**定理 4.20** (推广). 当$S',T',U'\subset F$满足三乘积性质时。若$\bar{S}^{(i)}$限制在$B$上的元素有重复出现的情况，此时$B$ 可实现$\langle a,b,c\rangle$，这里$a=max\{r+1,|\bar{S}^{(i)}|\}$ （$r$是$\bar{S}^{(i)}$限制在$B$上有重复的元素个数），$b=\max\{|\bar{T}^{(i)}|\}$，$c=\max\{|\bar{U}^{(i)}|\}$。这里的$\bar{S}^{(i)},\bar{T}^{(i)},\bar{U}^{(i)}$ 为命题*4.16* 中对$S'|_B$，$T'|_B$，$U'|_B$元素的划分。

**证明.** 记$A=\{p,r_{S'}\}$（$r_{S'}$表示所有$S'|_B$ 中重复出现的元素，这里不对重复元素进行任何合并操作），$p\in S'|_B$ 中元素$\backslash S'|_B$ 中重复出现的元素，$E=\bar{T}^{(j)}$ 限制在$B$ 上的元素集合，$C=\bar{U}^{(k)}$ 限制在$B$ 上的元素集合。则$A,E,C\subset B$ 满足三乘积性质。若从$A,E,C$中取的*6*个元素在$C_n$中对应的元素乘积不为*1*，因为造成它不为*1*的原因都在于集合$A$（因$E,C$ 中所取两元素在$F$中对应元素的$C_n$部分相同，在"$aa^{-1}$"乘积中抵消为*1*），可将$A$中元素左边都变为*1* （只有重复元素会使乘积不为*1*，而重复元素都有在$C_n$ 中取*1* 的对应元素），从而通过变化将为证三乘积性质所取*6* 个元素的在$C_n$ 中乘积变为*1*，之后若这*6* 个元素在$B$ 中乘积还是*1*，则由$S',T',U'\subset F$ 满足三乘积性质可推出矛盾! 因此$B$ 可实现$\langle r+1,\max\{|\bar{T}^{(i)}|\},\max\{|\bar{U}^{(i)}|\}\rangle$，结合推论*4.18*可知$B$ 可实现$\langle\max\{r+1,|\bar{S}^{(i)}|\},\max\{|\bar{T}^{(i)}|\},\max\{|\bar{U}^{(i)}|\}\rangle$。 □

## 4.3　应用

记群$G_1=C_2\times C_3\times A_4$，在GAP中可表示为$G_1=SmallGroup(72,47)$。
记$G_1=C_2\times H_1$，则$H_1$同构于$C_3\times A_4$，在GAP中可表示为$H_1=SmallGroup(36,11)$。
记群为$G_2=C_2\times(C_2^2\rtimes C_9)$，在GAP 中可表示为$G_2=SmallGroup(72,16)$。
记$G_2=C_2\times H_2$，则$H_1$的结构为$C_2^2\rtimes C_9$，在GAP中可表示为$H_2=SmallGroup(36,3)$。
本部分主要内容为群$G_1$和群$G_2$及基本三乘积性质的进一步分析，是对前述结论的综合应用。

下面具体研究$G_1$或$G_2$若能实现$\langle 6,6,6\rangle$基本三乘积性质则对应的三乘积组限制在$H_1$或$H_2$上时$C_2$ 中元素$1,2^{(1)}$ 的分布情况：（不妨设2阶循环群$C_2=\{1,2^{(1)}\}$）

**定理 4.21.** 群$G$（$G_1$或$G_2$）的$\langle 6,6,6\rangle$基本三乘积组中$2^{(1)}$ 后对应的$H_1$（或$H_2$）中元素集合与1后对应的$H_1$（或$H_2$）中元素集合交集为空集。

**证明.** 由定理4.17可直接得到若上述两集合的交不为空，则$H_1$（或$H_2$）须实现$\langle 6,6,a\rangle$，这里$a\geq 2$且为整数。而由定理2.21，$6\times(6+a-1)\geq 6\times(6+2-1)=42>|H|=36$，矛盾！证毕。 □

$G_1=C_2\times H_1$，$G_2=C_2\times H_2$，2阶循环群$C_2=\{1,2^{(1)}\}$，这里$2^{(1)}$是其中的2阶元，1是其中的单位元。

**定理 4.22.** *若群$G_1$（或$G_2$）实现$\langle 6,6,6\rangle$基本三乘积性质，则在群$G_1$（或$G_2$）的$\langle 6,6,6\rangle$基本三乘积组中$C_2$中元素取$2^{(1)}$的元素在群$G_1$（或$G_2$）的$\langle 6,6,6\rangle$基本三乘积组的18个位置中的分布情况只有这17种可能（不考虑三个三乘积子集相互之间的顺序）：*

$553,643,633,543,533,443,532,433,531,432,333,431,332,322,331,321,311$。

**证明.** 因为我们讨论的是基本三乘积性质，所以$C_2$ 中取$2^{(1)}$ 的元素在$\langle 6,6,6\rangle$三乘积组的18 个位置中最多只能占有15个位置，最少占一个位置，下面我们以$C_2$中取$2^{(1)}$的元素在$\langle 6,6,6\rangle$ 三乘积组中所占位置数开始分类讨论：（用$H$表示$H_1$ 或$H_2$）

(1)占1个位置：

此时1后的$H$中元素要满足$\langle 6,6,5\rangle$，但由定理2.21以及

$$6\times(6+5-1)=60>|H|=36$$

得出矛盾!

(2)占2个位置：

此时1后的$H$中元素要满足$\langle 6,5,5\rangle$或$\langle 6,6,4\rangle$，但由定理2.21以及

$$6\times(6+4-1)=6\times(5+5-1)=54>|H|=36$$

得出矛盾!

(3)占3个位置：

此时1后的$H$中元素要满足$\langle 5,5,5\rangle$或$\langle 6,5,4\rangle$ 或$\langle 6,6,3\rangle$，但由定理2.21 以及

$$6\times(6+3-1)=6\times(5+4-1)=48>|H|=36,$$

由引理4.1知$H$不可能实现$\langle 5,5,5\rangle$，矛盾!

(4)占4个位置：

此时1后的$H$中元素要满足$\langle 5,5,4\rangle$或$\langle 6,5,3\rangle$ 或$\langle 6,6,2\rangle$或$\langle 6,4,4\rangle$，但由定理2.21以及

$$6\times(5+3-1)=6\times(6+2-1)=42>|H|=36,$$

由引理4.1知$H$不可能实现$\langle 5,5,4\rangle$，矛盾!

(5)占5个位置：

此时1后的$H$中元素要满足$\langle 5,5,3\rangle$或$\langle 5,4,4\rangle$ 或$\langle 6,5,2\rangle$或$\langle 6,6,1\rangle$或$\langle 6,4,3\rangle$，由引理4.1 可排除$\langle 5,4,4\rangle$ 的情况，由推论4.17 推出$H$ 须分别实现$\langle 6,5,4\rangle$ 和$\langle 6,6,5\rangle$，由定理2.21可得矛盾。因此这种情况对于$2^{(1)}$ 所占位置分布有$\langle 5,5,3\rangle$ 和$\langle 6,4,3\rangle$ 有可能成立。

(6)占6个位置：

此时1后的$H$中元素要满足$\langle 6,5,1\rangle$或$\langle 6,4,2\rangle$ 或$\langle 6,3,3\rangle$或$\langle 5,4,3\rangle$或$\langle 5,5,2\rangle$ 或$\langle 4,4,4\rangle$，由引理4.1 可排除$\langle 4,4,4\rangle$ 的情况，由推论4.17 推出$H$ 须分别实现$\langle 6,5,5\rangle$，$\langle 6,4,4\rangle$ 和$\langle 5,5,4\rangle$，由定理2.21 可得矛盾。因此这种情况对于$2^{(1)}$ 所占位置分布有$\langle 6,3,3\rangle$和$\langle 5,4,3\rangle$有可能成立。

(7)占7个位置：

此时1后的$H$中元素要满足$\langle 6,3,2\rangle$或$\langle 6,4,1\rangle$ 或$\langle 5,3,3\rangle$或$\langle 5,4,2\rangle$或$\langle 5,5,1\rangle$ 或$\langle 4,4,3\rangle$，由推论4.17 推出$H$ 须分别实现$\langle 6,3,4\rangle$和$\langle 6,4,5\rangle$ 和$\langle 5,4,4\rangle$和$\langle 5,5,5\rangle$，由定理2.21及引理4.1 可得矛盾。因此这种情况对于$2^{(1)}$ 所占位置分布有$\langle 5,3,3\rangle$ 和$\langle 4,4,3\rangle$有可能成立。

(8)占8个位置：

此时1后的$H$中元素要满足$\langle 6,2,2\rangle$或$\langle 6,3,1\rangle$ 或$\langle 5,3,2\rangle$或$\langle 5,4,1\rangle$或$\langle 4,4,2\rangle$ 或$\langle 4,3,3\rangle$，由推论4.17 推出$H$ 须分别实现$\langle 6,4,4\rangle$和$\langle 6,3,5\rangle$ 和$\langle 5,4,5\rangle$和$\langle 4,4,4\rangle$，由定理2.21及引理4.1 可得矛盾。因此这种情况对于$2^{(1)}$ 所占位置分布有$\langle 5,3,2\rangle$ 和$\langle 4,3,3\rangle$有可能成立。

(9)占9个位置：

此时1后的$H$中元素要满足$\langle 6,2,1\rangle$或$\langle 5,3,1\rangle$ 或$\langle 5,2,2\rangle$或$\langle 4,3,2\rangle$或$\langle 4,4,1\rangle$ 或$\langle 3,3,3\rangle$，由推论4.17 推出$H$ 须分别实现$\langle 6,2,5\rangle$和$\langle 5,4,4\rangle$，由定理2.21及引理4.1 可得矛盾。因此这种情况对于$2^{(1)}$ 所占位置分布有$\langle 5,3,1\rangle$，$\langle 4,3,2\rangle$和$\langle 3,3,3\rangle$ 有可能成立。

(10)占10个位置：

此时1后的$H$中元素要满足$\langle 6,1,1\rangle$或$\langle 5,1,2\rangle$ 或$\langle 4,2,2\rangle$或$\langle 4,3,1\rangle$或$\langle 3,3,2\rangle$，由推

论4.17 推出$H$ 须分别实现$\langle 6,5,5\rangle$ 和$\langle 5,5,4\rangle$和$\langle 4,4,4\rangle$，由定理2.21 及引理4.1 可得矛盾。因此这种情况对于$2^{(1)}$ 所占位置分布有$\langle 4,3,1\rangle$，$\langle 3,3,2\rangle$有可能成立。

(11)占11个位置：

此时1后的$H$中元素要满足$\langle 5,1,1\rangle$或$\langle 4,1,2\rangle$ 或$\langle 3,2,2\rangle$或$\langle 3,3,1\rangle$或$\langle 2,2,3\rangle$，由推论4.17 推出$H$ 须分别实现$\langle 5,5,5\rangle$ 和$\langle 4,5,4\rangle$，由定理2.21 及引理4.1 可得矛盾。因此这种情况对于$2^{(1)}$ 所占位置分布有$\langle 3,2,2\rangle$，$\langle 3,3,1\rangle$有可能成立。

(12)占12个位置：

此时1后的$H$中元素要满足$\langle 4,1,1\rangle$或$\langle 3,1,2\rangle$ 或$\langle 2,2,2\rangle$，由推论4.17 推出$H$ 须分别实现$\langle 4,5,5\rangle$ 和$\langle 3,5,4\rangle$ 和$\langle 4,4,4\rangle$，由定理2.21 及引理4.1 可得矛盾。因此这种情况对于$2^{(1)}$ 所占位置分布有$\langle 3,1,2\rangle$有可能成立。

(13)占13个位置：

此时1后的$H$中元素要满足$\langle 3,1,1\rangle$，由推论4.17 推出$H$ 须实现$\langle 3,5,5\rangle$。因此这种情况对于$2^{(1)}$ 所占位置分布有$\langle 3,1,1\rangle$有可能成立。

(14)占14个位置：

此时$2^{(1)}$后的$H$中元素要满足$\langle 5,5,4\rangle$，由定理4.1推出矛盾。因此这种情况不成立。

(15)占15个位置：

此时$2^{(1)}$后的$H$中元素要满足$\langle 5,5,5\rangle$，由定理4.1推出矛盾。因此这种情况不成立。

□

**总结**

若要进一步探讨群$G_1$（或$G_2$）能否实现$\langle 6,6,6\rangle$三乘积性质还需寻找更多理论上的必要条件，同时应考虑精确算法（如文献[15]中的算法）的并行化实现，因为现在精确算法直接计算的一个主要困难就是计算规模巨大导致计算所需时间过长（至少一年左右）。

# 第五章　结论

本论文主要有五个方面的结果。一是针对文献[10]中若干例子进行扩充构建，得出一些新的同时二乘积组和三乘积组，并由例2.9基于[10] 定理7.1进行扩充构建的例子推导出一个文献中未有的$\omega$ 的非平凡上界$\omega < 2.9262$。二是证明了群的西罗子群组的三乘积性质及二乘积性质。三是在$6 \times 6$小矩阵乘法群理论方法的研究中，提出了若干群的$\langle 6,6,6\rangle$ 三乘积性质的必要条件，从而较大地缩减了问题的搜索空间；这些结果在$6 \times 6$矩阵乘法的群理论研究中有一定价值，其中的一些推广结论对其他矩阵乘法的群论方法研究亦具有一定参考价值。四是针对几个具体群给出了它们的三乘积组具体结构：构造证明了4 阶偶置换群$A_4$ 的$\langle 3,3,2\rangle$ 三乘积性质，给出并证明了该群的三乘积容量的确切值，然后由此结论抽象构造了群$C_6 \times A_4$ 的$\langle 6,3,3\rangle$ 三乘积组（这里$C_6$是6阶循环群），接着给出了该抽象形式的一个具体解；构造证明了群$C_3 \times A_4$的$\langle 6,4,3\rangle$ 三乘积组（这里$C_3$ 是3阶循环群）。五是从理论上探讨了群$C_2 \times B$、$C_3 \times B$以及$C_n \times B$ 的三乘积性质与群$B$ 的三乘积性质之间的联系并将理论成果应用于两个具体群的$\langle 6,6,6\rangle$ 三乘积性质的研究（这里$C_2$ 是2 阶循环群，不妨设$C_2 = \{1,2\}$，其中1代表单位元，2表示2 阶元），得到了有关$1 \times B$ 与$2 \times B$在$\langle 6,6,6\rangle$ 三乘积组中具体分布的一些结论。这些理论在由群$B$ 的三乘积组出发，构建群$A \times B$的三乘积组（这里$A$ 是某一类给定的群）这类问题中具有一定的参考价值。

研究中尚难解决的问题有以下几个方面：一是在$6 \times 6$小矩阵乘法的90阶以下群理论方法研究中，最后还有56个$C_1$竞争者尚未判断其是否可实现$\langle 6,6,6\rangle$三乘积性质。二是没有新构建出更多可以推出$\omega$ 的非平凡上界的具体群。

针对上面提出的第一个难点有两个进一步研究建议：（1）考虑精确算法（如文献[15] 中算法）的并行化实现；（2）在理论上继续寻找$\langle 6,6,6\rangle$ 三乘积性质的必要条件从而进一步缩减问题的搜索空间；（3）尝试从不同角度构建新的群，进而导出$\omega$的非平凡上界。另外一个接下来的研究工作设想是从第五方面研究成果出发，继续考虑群$A \times B$的三乘积性质与群$B$的三乘积性质之间的联系（这里$A$是某一类给定的群）从而弱化并推广已有的结论。

# 参考文献


[1] Murthy S. The Simultaneous Triple Product Property and Group-theoretic Results for the Exponent of Matrix Multiplication[J]. arXiv preprint cs/0703145, 2007.

[2] Bürgisser P, Clausen M, Shokrollahi A. Algebraic Complexity Theory[M]. Springer Science&Business Media, 1996.

[3] Pan V. How can we speed up matrix multiplication?[J]. SIAM review, 1984, 26(3): 393-415.

[4] Strassen V. Gaussian elimination is not optimal[J]. Numerische mathematik, 1969, 13(4): 354-356.

[5] Coppersmith D, Winograd S. Matrix multiplication via arithmetic progressions[J]. Journal of symbolic computation, 1990, 9(3): 251-280.

[6] Davie A M, Stothers A J. Improved bound for complexity of matrix multiplication[J]. Proceedings of the Royal Society of Edinburgh: Section A Mathematics, 2013, 143(02): 351-369.

[7] Williams V V. Multiplying matrices faster than Coppersmith-Winograd[C]//Proceedings of the forty-fourth annual ACM symposium on Theory of computing. ACM, 2012: 887-898.

[8] Le Gall F. Powers of tensors and fast matrix multiplication[C]//Proceedings of the 39th international symposium on symbolic and algebraic computation. ACM, 2014: 296-303.

[9] Cohn H, Umans C. A group-theoretic approach to fast matrix multiplication[C]//Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on. IEEE, 2003: 438-449.

[10] Cohn H, Kleinberg R, Szegedy B, et al. Group-theoretic algorithms for matrix multiplication[C]//Foundations of Computer Science, 2005. FOCS 2005. 46th Annual IEEE Symposium on. IEEE, 2005: 379-388.

[11] Blasiak J, Church T, Cohn H, et al. On cap sets and the group-theoretic approach to matrix multiplication[J]. arXiv preprint arXiv:1605.06702, 2016.

[12] Ambainis A, Filmus Y, Le Gall F. Fast matrix multiplication: limitations of the coppersmith-winograd method[C]//Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing. ACM, 2015: 585-593.

[13] Lai X, Zhou Y, Xiang Y. Ant colony optimization for triple product property triples to fast matrix multiplication[J]. Soft Computing, 2016: 1-13.

[14] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.7.5, 2014.

[15] Hart S, Hedtke I, Müller-Hannemann M, et al. A fast search algorithm for$\langle m, m, m\rangle$ Triple Product Property triples and an application for $5\times5$ matrix multiplication[J]. Groups Complexity Cryptology, 2015, 7(1): 31-46.

[16] Huppert B. Character theory of finite groups[M]. Walter de Gruyter, 1998.

[17] Hedtke I, Murthy S. Search and test algorithms for triple product property triples[J]. Groups-Complexity-Cryptology, 2012, 4(1): 111-133.

[18] Hedtke I. A note on the group-theoretic approach to fast matrix multiplication[J]. arXiv preprint arXiv:1101.5598, 2011.

[19] Neumann P M. A note on the triple product property for subsets of finite groups[J]. LMS Journal of Computation and Mathematics, 2011, 14: 232-237.

[20] Hedtke I. Upgrading Subgroup Triple-Product-Property Triples[J]. Journal of Experimental Algorithmics (JEA), 2015, 20: 1.1.

[21] Alder A, Strassen V. The algorithmic complexity of linear algebras[C]//Algorithms in Modern Mathematics and Computer Science. Springer Berlin/Heidelberg, 1981: 343-354.

[22] Fiduccia C M, Zalcstein Y. Algebras having linear multiplicative complexities[J]. Journal of the ACM (JACM), 1977, 24(2): 311-331.

[23] Pospelov A. Group-theoretic lower bounds for the complexity of matrix multiplication[C]//International Conference on Theory and Applications of Models of Computation. Springer Berlin Heidelberg, 2011: 2-13.

[24] Bläser M. Lower bounds for the bilinear complexity of associative algebras[J]. computational complexity, 2000, 9(2): 73-112.

[25] Alder A, Strassen V. On the algorithmic complexity of associative algebras[J]. Theoretical Computer Science, 1981, 15(2): 201-211.

[26] Bläser M. A complete characterization of the algebras of minimal bilinear complexity[J]. SIAM Journal on Computing, 2005, 34(2): 277-298.

[27] Winograd S. On multiplication of 2×2 matrices[J]. Linear algebra and its applications, 1971, 4(4): 381-388.

[28] Drevet C é, Islam M N, Schost é. Optimization techniques for small matrix multiplication[J]. Theoretical Computer Science, 2011, 412(22): 2219-2236.

# 致　　谢

特别感谢我的导师高小山研究员，在他的悉心指导和鼓励下，我一步步走上了科研的道路。首先感谢老师为我选择了十分重要的领域（计算复杂性以及矩阵乘法的计算复杂性分析）作为研究方向，在学习过程中，我从只知皮毛，到通览领域发展历程，再到发现自己的兴趣问题，然后针对问题展开研究，每天都有新的困难、失败和新的问题，晚上心情绝望而头脑清醒地躺在床上看着天花板想问题想着想着睡着了，第二天早上又会因发现新的思路而雀跃万分，实在感受到了做学问的乐趣，对于做研究有了一些管窥蠡测；也因此希望自己更加坚定而长久地走在这条道路上。教诲如春风，师恩似海深。希望今后我可以全面严格要求自己，在学问上踏实精进，长路漫漫上下求索，不辜负老师的教导和付出。高老师高瞻远瞩，对问题有着敏锐的洞察力，而我是个反应慢的孩子，很多时候老师提出的建议和指导我一开始不理解，总要自己碰了一鼻子灰才会恍然大悟，明白老师所提所讲的精妙之处，进而感到获益匪浅。在科研中遇到困难的时候，老师总是会给予我们充分的信任和无私的帮助。高老师品格高尚，对科研精益求精，思维敏捷，治学严谨，忘我工作，令人感动和敬仰！老师对论文中很多细节都仔细推敲、认真修改，言传身教，这些都微妙而深刻地改变着我对科研的认识和我的治学态度。高山仰止、景行行止，导师的影响是潜移默化的。拜谢师恩！

还要深深感谢很多老师和同学在我学习矩阵乘法算法计算复杂度的过程中对我的帮助：

感谢加州理工学院的郭泽宇同学在我学习矩阵乘法的群论方法和CW1990算法的过程中给予的无私帮助！因为身边没有人研究我的这个问题，如果不是您的帮助和鼓励，我很可能很早之前就难以在这个领域里继续探索了。谢谢郭泽宇同学！

感谢Ivo Hedtke 博士在我学习及研究小矩阵乘法的群论方法过程中给予的耐心指导和帮助！当我对于他们文章提出细节上的疑问时，他总是耐心而细致

地解答；在我研究他们文章中提出的公开问题时，他又不吝赐教，给出很有价值的建议与指导。我在$6 \times 6$小矩阵乘法研究中得到的成果离不开Hedtke博士的帮助，感谢Ivo Hedtke博士!

感谢Peter Neumann教授在我学习及研究群的三乘积组过程中给予的无私帮助和耐心指导！感谢您百忙之中抽出时间详细地解答我的问题，还细心纠正我信件中latex的使用规范，让我感受到老一辈研究者的敬业、谦和还有对学问的赤子之心！谢谢您!

感谢冯如勇师兄在我探究几个具体群的三乘积组的过程中给予的帮助!

感谢唐国平老师的抽象代数课，一整学期在玉泉路的学习让我获益良多，我十分享受学习的过程，也充分感受到抽象代数的美与神奇！这门课程是群论的基础，对我的研究很有帮助。

感谢机械化中心王定康研究员在我申请使用机械化实验室机群过程中给予的无私帮助!

感谢计算机网络信息中心钱莹老师在我申请使用数学院机群以及使用机群进行实例计算过程中给予的无私帮助!

感谢中山大学周育人教授和华南理工大学赖鑫生老师在我学习研究搜索群的极大三乘积组的蚁群算法过程中提供的帮助!

感谢罗东山同学在论文的格式、模版等方面对我的帮助!

感谢思源楼217自习室和我一起自习的同学们！还要从心底里感谢217自习室，我很喜欢这儿的环境，在这里我可以舒心地工作、学习。[合掌]

衷心感谢机械化实验室，中心对我们的强大支持与无私帮助让我感受到家一样的温暖！衷心感谢李子明研究员、袁春明师兄、李伟师姐、黄章师兄、王

杰师兄、吴冬生同学、徐敬可同学、陈俣翱同学在我研究和学习中遇到困难时给予帮助和建议！珍重同门情谊，感谢荆瑞娟师姐、黄巧龙师兄，还有胡又壬同学！感谢周代珍老师、李佳老师的辛苦付出！

一直认为“致谢”是神圣的一章，迟迟无法动笔。现在快要完成，感谢自己！还有很多我想要表达衷心谢意的人和事，因为与本论文无直接学术关系，在此不做详述，不过都在心底。

好些年前，我告诉自己有两个人，我人生中要是有机会能见过一次就“朝闻道，夕死可矣”了，其中一位就是吴先生。现如今这将是我人生中永远的遗憾。唉！刚刚看到一段采访，不清楚记者问的原话是什么，吴先生回答“最幸福的事就是数学机械化中心的成立，这个是很重大的，因为可以后继有人了，这是非常重要的”，不由得热泪盈眶。吴中心凝聚了先生后半生的心血，吾辈当砥砺奋进，承先生遗志。

深深感谢、深切缅怀吴先生。

# 简　　历

## 基本情况

齐嘉悦，陕西省西安市人，1992年出生。中国科学院数学与系统科学研究院在读硕士研究生。

## 教育状况

2014.9-2017.5 中国科学院数学与系统科学研究院 硕士研究生

应用数学专业　导师：高小山 研究员

2010.9-2014.6 北京航空航天大学数学与系统科学学院 华罗庚班 本科

信息与计算机数学专业　导师：郭雷 研究员

## 联系方式

通讯地址：北京市海淀区中关村东路55号基础科学园区，思源楼

邮编：100190

E-mail: qijiayue14@mails.ucas.ac.cn