苏州大学

硕士学位论文

群论在魔方中的应用

姓名：朱磊

申请学位级别：硕士

专业：基础数学

指导教师：施武杰

20080401

摘 要

本文从群论的角度讨论了魔方 (Rubik's cube) 的数学性质. 首先, 本文以魔方作为工具, 展示了群论中的各种概念及其相关性质的实际应用, 如置换, 作用, 轨道, 传递性, 本原性, 共轭, 换位子, 同态; 其次, 介绍了魔方群的结构; 最后, 作为本文的核心, 将魔方群对应的 Cayley 图直径下界由 20 提升到 21.

关键词: 魔方, 置换群, 直径, 下界

作者: 朱磊

导师: 施武杰

Applications of Group Thoery in Rubik's Cube

Abstract

This paper discussed the mathematical properties of the Rubik's cube from the viewpoint of group theory. First of all, taking the Rubik's cube as a tool, this paper demonstrated the practical applications of all kinds of concepts and their relevant properties in group theory, such as permutation, action, orbit, transitivity, primitivity, conjugation, commutator and homomorphism; secondly, this paper introduced the structure of the Rubik's cube group; At last, as the core of this paper, it promoted the lower bound of the diameter of the Cayley graph with respect to the Rubik's cube group, from 20 to 21.

Keywords: Rubik's cube, permutation groups, diameter, lower bound

Written by L. Zhu

Supervised by Prof. WJ. Shi

苏州大学学位论文独创性声明及使用授权的声明

学位论文独创性声明

本人郑重声明：所提交的学位论文是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不含其他个人或集体已经发表或撰写过的研究成果，也不含为获得苏州大学或其它教育机构的学位证书而使用过的材料。对本文的研究作出重要贡献的个人和集体，均已在文中以明确方式标明。本人承担本声明的法律责任。

研究生签名：宋磊 日 期：2008年4月16日

学位论文使用授权声明

苏州大学、中国科学技术信息研究所、国家图书馆、清华大学论文合作部、中国社科院文献信息情报中心有权保留本人所送交学位论文的复印件和电子文档，可以采用影印、缩印或其他复制手段保存论文。本人电子文档的内容和纸质论文的内容相一致。除在保密期内的保密论文外，允许论文被查阅和借阅，可以公布（包括刊登）论文的全部或部分内容。论文的公布（包括刊登）授权苏州大学学位办办理。

研究生签名：宋磊 日 期：2008年4月16日

导师签名：[illegible] 日 期：2008年4月16日

第一章　群论概念在魔方中的应用

1.1　前言

魔方最初是在 1974 年由一位匈牙利的建筑学教授 Rubik 所发明，其最初的目的不过是为了使学生对立体事物增加一些实感. 令 Rubik 始料未及的是，魔方一经问世后竟然风靡全球，成了 20 世纪 80 年代初期最受欢迎的玩具.

魔方不仅是一个令千万人着迷的有趣玩具，同时也是一个能够展示许多群论概念及其相关性质的有力工具. 如置换，作用，轨道，传递性，本原性，同态等诸多概念在魔方中的体现，如共轭和换位子在复原魔方的过程中起到的化繁为简的作用.

人们在玩魔方的时候，很自然地会提出如下问题：魔方不同色彩组合的种数是多少？这个问题已经得到解决，大致思路是建立所有魔方色彩组合到魔方群的双射，计算出该群的阶，从而确定魔方不同色彩组合的种数. 更进一步地，利用群论作为工具，还可以分析出魔方的结构，这点将在后文中详细介绍.

除了上述问题，人们在玩魔方的时候，最核心的问题是：如何将一个处于混乱状态的魔方复原？这个问题已经得到解决，而且解法远远不止一种，这都归功于众多魔方爱好者. 本文不对如何复原魔方进行探讨，如果有兴趣，可以参考 [1].

上述问题是比较特殊的一种形式，与之对应的是由此衍生的问题：魔方群 Cayley 图的直径是多少？这个问题目前没有得到解决. 有人把该直径称为上帝之数 (God's number). 相应地，还原魔方的步骤被称为上帝的算法 (God's algorithm).

1982 年， Singmaster 和 Frey 在 [2] 中猜想上帝之数是 20 出头的一个数

字. 直接求解上帝之数恐非易事, 否则它也不会背上上帝之数这个称号屹立 26 年不倒了. 一种比较可行的办法是分别从上界和下界逼近, 如果最后能够达到上下界相等, 那么该相等的值也即是上帝之数.

Kunkle 和 Cooperman 在 [3] 中给出了目前关于上界的最好结果: 26(该值是在包含半周旋转的情况下所得, 如果只考虑四分之一周旋转, 该值应该更大).[4] 给出了目前关于下界的结果: 20.

本文的主要成果是将下界从 20 提升到 21, 基本思路是把魔方群的元素按照长度进行分类, 并且尽可能地排除每个分类中重复的元素, 最后将这些分类的元素个数相加, 与魔方群的阶比较大小, 最终确定下界.

1.2 基本介绍

从外观看, 魔方是由 $3\times3\times3-1=26$ 个块 (不包含最里面的块) 组成的立方体. 它有 6 个面, 每个面有 $3\times3=9$ 个小面, 共 $6\times9=54$ 个小面. 26 个块中, 有 3 个小面是角块, 有 2 个小面是边块, 只有 1 个小面是中心块. 显然, 魔方共有 8 个角块, 12 个边块和 6 个中心块.

定义 1.1 转动是指将魔方的某个面上的所有块顺时针 (面对该面) 旋转 $\pi/2$. 类似地, 逆转动是逆时针旋转 $\pi/2$. 转动和逆转动统称为转动.

这里定义的转动都是四分之一周旋转, 不包括半周旋转. 为了简明, 若非特别提及, 本文不使用魔方中间层面的转动, 因为其可以被相邻两侧的面转动所替代.

作为惯例, 本文使用 Singmaster 记号表示 6 个面的转动及各小面和块的方位. 用大写的 U(上), D(下), F(前), B(后), L(左), R(右) 表示各面相应的转动, 用小写的 u,d,f,b,l,r 表示各面及相应的中心块. 对于角块上的小面, 用 xyz 表示其方位, 含义是: x 面 yz 方位的小面. 如 ufl 表示 u(上) 面 fl(前左) 方位的小面. 这种方法也可以用来表示相应的角块. 类似地, 对于边块

上的小面，用 xy 表示 x 面 y 方位的小面．如 db 表示 d(下) 面 b(后) 面方位的小面．同样，这种方法也可以用来表示相应的边块．这种既表示小面又表示块的方法不会造成混淆，可以通过上下文理解其含义．

一个简单的事实是：在不对魔方中间层面进行转动的情况下，无论怎样转动魔方，各个面的中心块总是固定的．据此，在涉及魔方各面的时候，总是指其中心块所代表的那个面，这样为讨论问题提供了一个固定的参考系．

1.3 魔方群

规定魔方的转动合成运算是从左向右的，即 $\forall\, M_1, M_2 \in \{U, D, F, B, L, R\}$，$M_1M_2$ 表示先转动 M_1，再转动 M_2．如 RU 表示先转动 R(右) 面，再转动 U(上) 面．用 c 表示魔方状态，即各块和小面的方位，用 $M(c)$ 表示魔方在状态 c 下经 M 转动后所生成的新状态．考虑到转动合成运算是从左到右的，有 $(M_1M_2)(c) = M_2(M_1(c))$

定理 1.2 由魔方所有转动生成的集合，以合成作为运算，构成一个群，称为魔方群．

证明： 设 $G =< U, D, F, B, L, R >$ 是魔方所有转动生成的集合．

G 中任意元素都可以表示成一系列转动的合成，则 G 中任意两个元素的合成同样是一系列转动的合成．故 G 是封闭的．

用 c 表示任意魔方状态，则 $\forall\, M_1, M_2, M_3 \in G$, 有：

$$((M_1M_2)M_3)(c) = M_3((M_1M_2)(c)) = M_3(M_2(M_1(c)))$$

$$(M_1(M_2M_3))(c) = (M_2M_3)(M_1(c)) = M_3(M_2(M_1(c)))$$

根据 c 的任意性，可得 $(M_1M_2)M_3 = M_1(M_2M_3)$．故结合律成立．

若魔方状态 c 在转动 M 的作用下不发生改变，则 M 是单位转动．故单位元存在．

若 $M = M_1M_2 \ldots M_n$ 是生成元素的乘积，$M_i \in \{U, D, F, B, L, R\}, i \in \{1, 2, \ldots, n\}$，

则 $M^{-1} = M_n^{-1} \dots M_2^{-1} M_1^{-1}$. 故逆元存在.

综上四点， $G =< U, D, F, B, L, R >$ 构成一个群，称为魔方群. □

1.4 置换

魔方群 G 的生成元可以用一系列小面的置换来表示：

$U = (ulb\ ubr\ urf\ ufl)(ub\ ur\ uf\ ul)(bul\ rub\ fur\ luf)(bu\ ru\ fu\ lu)(bru\ rfu\ flu\ lbu)$

$D = (dbl\ dlf\ dfr\ drb)(db\ dl\ df\ dr)(bld\ lfd\ frd\ rbd)(bd\ ld\ fd\ rd)(bdr\ ldb\ fdl\ rdf)$

$F = (flu\ fur\ frd\ fdl)(fu\ fr\ fd\ fl)(ufl\ rfu\ dfr\ lfd)(uf\ rf\ df\ lf)(urf\ rdf\ dlf\ luf)$

$B = (bul\ bld\ bdr\ bru)(bu\ bl\ bd\ br)(ulb\ ldb\ drb\ rub)(ub\ lb\ db\ rb)(ubr\ lbu\ dbl\ rbd)$

$L = (luf\ lfd\ ldb\ lbu)(lu\ lf\ ld\ lb)(ufl\ fdl\ dbl\ bul)(ul\ fl\ dl\ bl)(ulb\ flu\ dlf\ bld)$.

$R = (rfu\ rub\ rbd\ rdf)(ru\ rb\ rd\ rf)(urf\ bru\ drb\ frd)(ur\ br\ dr\ fr)(ubr\ bdr\ dfr\ fur)$

如 1.2 节介绍的那样，这里各个循环中的 xyz 和 xy 表示相应的小面. 类似地，可以用块置换表示生成元，不过块置换没有小面置换全面，因为小面的方向这个信息被遗漏了. 后文将会建立这两者之间的同态.

引理 1.3 [5](p. 37) S_n 中的不相交循环是可交换的.

引理 1.4 [5](p. 38) S_n 中的所有置换都是一系列不相交循环的乘积.

定理 1.5 S_n 中的不相交置换是可交换的.

证明： 设 f, g 是 S_n 中的不相交置换. 由引理 1.4, $f = f_1 f_2 \dots f_n$, $g = g_1 g_2 \dots g_m$. f_i 和 g_j 是不相交循环， $i \in \{1, 2, \dots, n\}$, $j \in \{1, 2, \dots, m\}$. 由引理 1.3, 这些循环是交换的， $fg = f_1 f_2 \dots f_n g_1 g_2 \dots g_m = g_1 g_2 \dots g_m f_1 f_2 \dots f_n = gf$. □

推论 1.6 魔方群的对面转动是可交换的.

证明： 在魔方群 $G =< U, D, F, B, L, R >$ 中，对面转动是不相交的. 根据定理 1.5, 对面转动是可交换的，即 $UD = DU, FB = BF, LR = RL$. □

1.5 作用，传递性，轨道和本原性

用 F_* 表示魔方的小面集合，B_* 表示魔方的块集合，E_F 表示魔方边块上的小面集合，V_F 表示魔方角块上的小面集合，E_B 表示魔方的边块集合，V_B 表示魔方的角块集合. 显然，有：

$$F_* = E_F \bigcup V_F, E_F \bigcap V_F = \emptyset$$
$$B_* = E_B \bigcup V_B, E_B \bigcap V_B = \emptyset$$

定理 1.7 魔方群 G 分别作用在 F_*, B_* 上.

证明： 只需将 1.3 节中的魔方状态 c 换成这里的 F_*, B_* 就可以了. □

推论 1.8 魔方群 G 分别作用在 E_F, V_F, E_B, V_B 上.

定理 1.9 魔方群 G 在 E_F, V_F, E_B, V_B 上的作用是传递的.

证明： 以 dfl 角块为例，考虑如下转动：$M = FFFDBBBD^{-1}$，则 dfl 角块沿着上述路径遍历所有角块，最终回到起点. 于是 V_B 中任意两个元素都可以在 G 的作用下传递，从而 G 在 V_B 上的作用是传递的. 类似地，可以证明 G 在 E_F, V_F, E_B 上的作用也是传递的. 实际上，只需找到一条遍历所有元素的路径，就证明了传递性. □

魔方群 G 在 F_*, B_* 上却不是传递的. 因为角块不能传递到边块，角块上的小面也不能传递到边块上的小面，反之亦然.

推论 1.10 魔方群 G 在 F_* 上有两个轨道：E_F 和 V_F; 在 B_* 上有两个轨道：E_B 和 V_B.

定义 1.11 群 G 在集合 Ω 上是传递的，称 Ω 的子集 Δ 是非本原块，如果 $\forall\, g \in G, \Delta \bigcap g(\Delta) = \Delta$ 或 $\emptyset$. 如果非本原块只是单点集和 Ω, 则称 G 是本原的，否则称为非本原的.

定理 1.12 魔方群 G 在 E_F, V_F 上的作用是非本原的.

证明: 设同一边块上两个小面组成的子集是 Δ, 在 $g \in G$ 的作用下, 若该边块的位置发生变化, 则 $\Delta \bigcap g(\Delta) = \emptyset$, 否则 $\Delta \bigcap g(\Delta) = \Delta$, 从而 Δ 是非本原块. 另外 $1 < |\Delta| = 2 < |E_F| = 24$, G 在 E_F 上的作用是非本原的. 类似地, 同一角块上三个小面组成的子集也是不同于单点集和全集的非本原块, G 在 V_F 上的作用也是非本原的. □

G 在 E_B, V_B 上的作用却是本原的, 因为非本原块只能是单点集或全集.

1.6 共轭和换位子

魔方复原是一个复杂的过程, 因为牵扯到大量的置换运算. 如果没有策略乱转一通, 很可能把魔方状态弄得更加混乱. 本小节讨论共轭和换位子在魔方复原中的作用.

引理 1.13 [5](p. 142)$g, h \in S_n$, $i, j \in \{1, 2, \ldots, n\}$, 若 $g(i) = j$, 则 $g^h(h(i)) = h(j)$.

共轭在魔方复原中是一种常用的手段. 引理 1.13 说明如果 g 把 i 变到 j, 则 g 的共轭 g^h 则把 $h(i)$ 变到 $h(j)$. 了解这点对于魔方复原十分有用.

定理 1.14 [5](p. 142)S_n 中两个元素有相同的循环结构, 则它们共轭.

推论 1.15 魔方群 G 中的生成元 U, D, F, B, L, R 相互共轭.

证明: 证明该推论需要以后的知识, 具体证明过程参见 2.4 节. □

在群论中, 换位子是衡量元素交换性的概念, 似乎跟魔方复原没有任何关系, 但换位子在魔方复原中恰恰起到化繁为简的作用.

如 1.4 节展示的那样, 每个转动是由 5 个长度为 4 的不相交循环所合成. 当复原魔方的时候, 每转动一次, 就有 $5 \times 4 = 20$ 个小面重新分布, 使得无规律连续转动几次后的魔方状态十分混乱. 人们总是希望在保留已经

复原那部分魔方的基础上，尽可能少地改变魔方的状态，这样，换位子的重要性凸显了出来.

以下分析换位子在魔方群中的定义结构. 设 g 和 h 是魔方相邻两面的转动，$[g,h]=ghg^{-1}h^{-1}$ 表示在 gh 之后转动 $g^{-1}h^{-1}$，相当于把 g 和 h 转动过的部分小面或块复原到未转动之前的状态. 这样换位子实际上只改变了很少一部分小面或块，从而简化了魔方复原的过程.

可以验证：$[g,h]^2$ 改变 3 个边块而使角块不变；$[g,h]^3$ 改变 2 对角块而使边块不变. 如：$[U,F]^2=(uf\ ur\ fl)$; $[U,F]^3=(ufl\ fdl)(fur\ ubr)$. 除了上述比较简单的换位子，还有一些比较复杂的换位子，如包含共轭的复合换位子 $[R^{F^{-1}},L]=(urf\ ufl\ ulb)$, $[[F,D^{-1}]^B,U^2]=(urf\ ubr)(ufl\ ulb)$. 以上三个例子中置换的各元素表示的是块，而不是小面.

1.7 同态

G 是魔方群，S_V 是角块在 G 作用下的置换群，S_E 是边块在 G 作用下的置换群. $\forall\, g\in G$, 定义 $\sigma: G\longmapsto S_V$, $\sigma(g)=\sigma_g$ 是跟 g 相对应的角块置换. $\tau: G\longmapsto S_E$, $\tau(g)=\tau_g$ 是跟 g 相对应的边块置换. 可得如下定理：

定理 1.16 $\sigma: G\longmapsto S_V$ 和 $\tau: G\longmapsto S_E$ 是同态.

推论 1.17 $\psi: G\longmapsto S_V\times S_E$ 是同态.

推论 1.17 实际上是建立了从小面置换到块置换的同态，后文将会分析这个同态的具体结构.

二　魔方群的结构

2.1　扩展魔方群

定义 2.1 把魔方拆卸后再重新任意组装，这个过程实际上也是一种置换，所有这些置换构成一个比魔方群 G 大的群，称为扩展魔方群 G_*，相应的魔方状态称为扩展魔方状态 c_*.

定理 2.2 扩展魔方群和扩展魔方状态集合之间存在一一对应关系.

证明： 用 C_* 表示扩展魔方状态集合，c_0 表示复原状态. 定义映射 $\pi : G_* \longmapsto C_*, \pi(g_*) = g_*(c_0)$, 即 g_* 对应 g_* 作用复原状态后的扩展魔方状态. 显然 π 是一个满射. 若有 $g_{*1}(c_0) = g_{*2}(c_0)$, 则 $g_{*2}^{-1}g_{*1}(c_0) = (c_0), g_{*2}^{-1}g_{*1} = 1$, 于是 $g_{*1} = g_{*2}, \pi$ 是单射. 这样扩展魔方群和扩展魔方状态集合之间存在一一对应关系. □

由定理 2.2, 下文就不再对扩展魔方群和扩展魔方状态集合进行区分.

推论 2.3 魔方群的阶 $|G|$ 等于魔方不同色彩组合的种数.

定义 2.4 扩展魔方状态集合 C_* 中两个元素是等价的如果其中一个元素能够通过有限次转动作用后变成另一个元素.

定理 2.5 魔方状态集合 C 是复原状态 c_0 的等价类.

2.2　位置和方向

本节中的所有讨论对于扩展魔方群和扩展魔方状态集合同样适用.

在魔方问题中，一个值得注意的事实是：块可以在不改变位置的情况下改变方向. 如角块 urf 在 RU 作用后，其位置没有发生改变，而其方向发生了改变.

根据魔方的构造，很明显有以下结果：

定理 2.6 [5](p. 148) 魔方状态由以下四个条件共同决定：

1) 角块的位置

2) 角块的方向

3) 边块的位置

4) 边块的方向

角块的位置可以用 S_8 中的元素表示，类似地，边块的位置可以用 S_{12} 中的元素表示．而角块和边块的方向则要用另外的形式表示．

采用 Chen 的方法，参见 [6]. 从角块开始，在每个角块的一面上标记一个数字：

在 u 面上的 ufl 小面上标记 1

在 u 面上的 urf 小面上标记 2

在 u 面上的 ubr 小面上标记 3

在 u 面上的 ulb 小面上标记 4

在 d 面上的 dbl 小面上标记 5

在 d 面上的 dlf 小面上标记 6

在 d 面上的 dfr 小面上标记 7

在 d 面上的 drb 小面上标记 8

这样做有两个含义：其一，这些数字表示角块的序号；其二，所选取的小面是标准面，用以决定角块的方向．下一步，在标记有序号的这些小面上再标记 0, 然后顺时针旋转，在角块的另外两面上依次标记 1 和 2.

有了以上标记，就可以定义角块的方向了．用 $v=(v_1,v_2,\ldots,v_8)$ 表示角块的方向，其中 v_i 表示第 i 个角块标准面上的数字，也可以认为是顺时针旋转该角块，使其标记为 0 的面与标准面重合所需要的次数． $i\in\{1,2,\ldots,8\}$. 这样， $v=(v_1,v_2,\ldots,v_8)\in C_3^8$.

类似地，可以定义边块的方向，在每个边块的一面上标记一个数字：

在 u 面上的 ub 小面上标记 1

在 u 面上的 ur 小面上标记 2

在 u 面上的 uf 小面上标记 3

在 u 面上的 ul 小面上标记 4

在 b 面上的 bl 小面上标记 5

在 b 面上的 br 小面上标记 6

在 f 面上的 fr 小面上标记 7

在 f 面上的 fl 小面上标记 8

在 d 面上的 db 小面上标记 9

在 d 面上的 dr 小面上标记 10

在 d 面上的 df 小面上标记 11

在 d 面上的 dl 小面上标记 12

在标记有序号的这些小面上再标记 0, 然后在边块的另一面上标记 1.

用 $w = (w_1, w_2, \ldots, w_{12})$ 表示边块的方向，其中 w_j 表示第 j 个边块标准面上的数字，$j \in \{1, 2, \ldots, 12\}$. 有 $w = (w_1, w_2, \ldots, w_{12}) \in C_2^{12}$.

设 $v(g)$ 和 $w(g)$ 分别表示 $g \in G$ 作用后的角块方向和边块方向. 如：$v(1) = 0, w(1) = 0$. 考虑 r(右) 面的转动，左面的角块没有发生改变，因此 $v_1 = 0, v_4 = 0, v_5 = 0, v_6 = 0$; 右边的角块发生了变化，有 $v_2 = 1, v_3 = 2, v_7 = 2, v_8 = 1$. 于是 $v(R) = (0, 1, 2, 0, 0, 0, 2, 1)$. 同样可以验证 $w(F) = (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$.

下面两个定理揭示块方向的合成法则：

定理 2.7 [5](p. 179) G 是魔方群，$\sigma_g \in S_V$ 是跟 $g \in G$ 有关的角块置换. 则 $\forall\, g_1, g_2 \in G$, 有 $v(g_1 g_2) = v(g_1) + \sigma_{g_1}^{-1}(v(g_2))$.

定理 2.8 [5](p. 180) G 是魔方群，$\tau_g \in S_E$ 是跟 $g \in G$ 有关的边块置换. 则 $\forall\, g_1, g_2 \in G$, 有 $w(g_1 g_2) = w(g_1) + \tau_{g_1}^{-1}(w(g_2))$.

2.3 (外) 半直积

定义 2.9 $\phi: H_2 \longmapsto \mathrm{Aut}(H_1)$ 是一个同态，定义集合 $H_1 \times H_2$ 上的乘积如下：

$$(x_1, x_2)(y_1, y_2) = (x_1\phi(x_2)(y_1), x_2y_2)$$

由此定义了一个群运算，称该群 $H_1 \rtimes_\phi H_2$ 是 (外) 半直积.

定义 2.10 用 C_d 表示阶为 d 的循环群， S_n 是 n 个文字的对称群， S_n 通过置换指数的方式作用在 C_d^n 上. $\forall f \in S_n$, 定义：

$f_*: C_d^n \longmapsto C_d^n$, $f_*(v) = (v_{f^{-1}(1)}, \ldots, v_{f^{-1}(n)}), v = (v_1, \ldots, v_n) \in C_d^n$.

$\forall p, q \in S_n, v, w \in C_d^n$, 定义：

$$(p, v)(q, w) = (pq, w + q_*(v))$$

称半直积 $C_d^n \rtimes S_n$ 为一般对称群.

定理 2.11 [5](p. 181) G_* 是扩展魔方群，则 $G_* \cong (C_3^8 \rtimes S_8) \times (C_2^{12} \rtimes S_{12})$.

推论 2.12 $|G_*| = 3^8 \cdot 8! \cdot 2^{12} \cdot 12!$

2.4 魔方群的结构

由定理 2.11, 扩展魔方群的元素可以用 $g_* = (v, \sigma, w, \tau) \in (C_3^8 \rtimes S_8) \times (C_2^{12} \rtimes S_{12})$ 来表示. 以下的魔方群结构定理给出了魔方群的结构：

定理 2.13 [5](p. 182) $g_* = (v, \sigma, w, \tau) \in (C_3^8 \rtimes S_8) \times (C_2^{12} \rtimes S_{12})$ 是扩展魔方群 G_* 的元素， G 是魔方群，则 $g_* \in G$ 当且仅当以下条件成立：

1) $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau)$

2) $\sum_{i=1}^{8} v_i \equiv 0 \pmod 3$

3) $\sum_{j=1}^{12} w_j \equiv 0 \pmod 2$

推论 2.14 $|G| = |G_*|/12$.

证明: 由定理 2.13, 满足条件 1), 2), 3) 的元素个数分别占扩展魔方群的 1/2, 1/3, 1/2. 由定理 2.6, 这三个条件是相互独立的. 由乘法原理, $|G| = (1/2) \cdot (1/3) \cdot (1/2) \cdot |G_*| = |G_*|/12$. □

推论 2.15 设 $\psi : G \longmapsto S_V \times S_E$ 是从魔方群小面置换到块置换的同态, 则 $\ker(\psi) \cong C_3^7 \times C_2^{11}$.

证明: 实际上, 证明如下两个关系即可: $\{v \in C_3^8 | \sum_{i=1}^{8} v_i \equiv 0 \pmod 3\} \cong \mathrm{C}_3^7$, $\{w \in C_2^{12} | \sum_{j=1}^{12} w_j \equiv 0 \pmod 2\} \cong \mathrm{C}_2^{11}$. □

推论 1.15 的证明: 由定理 1.14, 生成元在扩展魔方群中是共轭的. 只需证明生成元在魔方群中同样共轭即可, 即 $\forall M_1, M_2 \in \{U, D, F, B, L, R\}$, 若 $\exists h \in G_*$, 使得 $M_1 = M_2^h$, 则 $h \in G$. 只需验证 $h \in G_*$ 满足定理 2.13 的三个条件即可. □

定理 2.16 [5](p. 184) 魔方群 G 的中心 $Z(G) = \{1, z\}$, 其中 $z = (v, \sigma, w, \tau), v = (0, \ldots, 0) \in C_3^8, w = (1, 1, \ldots, 1) \in C_2^{12}, \sigma = 1 \in S_8, \tau = 1 \in S_{12}$. 这里的 z 称作超翻转 (superflip), 表示所有边块的方向发生改变而其他不动的元素.

用 G_1 表示魔方群 G 的换位子子群.

定理 2.17 [5](p. 186) $G_1 = \{g \in G | \mathrm{sgn}(\sigma_g) = \mathrm{sgn}(\tau_g) = 1\}$. $\sigma_g \in \mathrm{S_V}$ 表示与 g 相对应的角块置换, $\tau_g \in S_E$ 表示与 g 相对应的边块置换.

推论 2.18 [5](p. 186) $|G_1| = |G|/2$.

三　魔方群 Cayley 图直径的下界

3.1　Cayley 图

定义 3.1 图是一对可数集 (V,E). 其中，V 是由可数个顶点组成的集合，称为顶点集；E 是所有无序对集合 $\{\{v_1,v_2\}|\ v_1,v_2\in V, v_1\neq v_2\}$ 的子集，称为边集.

定义 3.2 顶点 v 的度数是与 v 相连接的边数，记作 $\deg(v)$.

定义 3.3 v 和 w 是顶点，从 v 到 w 的路径是以 v 为起点，以 w 为终点的边的有限序列：

$$e_0=\{v,v_1\},e_1=\{v_1,v_2\},\ldots,e_n=\{v_n,w\}.$$

定义 3.4 $v,w\in V$, 称 v 和 w 是连通的如果从 v 到 w 有一条路径. 图 (V,E) 是连通的如果任意两点都是连通的.

定义 3.5 $v,w\in V$, 如果 v 和 w 是连通的，定义两点之间的距离 $d(v,w)$ 为 v 到 w 的最短路径的边数. 如果 v 和 w 不连通，则令 $d(v,w)=\infty$. 图的直径 $\mathrm{diam}((V,E))=\max\{d(v,w)|\ v,w\in V\}$.

定义 3.6 $G=<g_1,g_2,\ldots,g_n>$ 是由集合 $X=\{g_1,g_2,\ldots,g_n\}$ 生成的置换群，G 关于 X 的 Cayley 图是图 (V,E), 其中 V 是 G 中的元素，边由以下条件决定：如果 $x,y\in V=G$, 则 x 和 y 有边相连当且仅当 $y=g_ix$ 或者 $x=g_iy, i\in\{1,2,\ldots,n\}$.

定理 3.7 [5](p. 117) $\Gamma_G=(V,E)$ 表示关于置换群 $G=<g_1,g_2,\ldots,g_n>$ 的 Cayley 图. 则 $\forall\, v\in V$, $\deg(v)=|\{g_1,g_1^{-1},g_2,g_2^{-1},\ldots,g_n,g_n^{-1}\}|$.

根据定理 3.7, 魔方群 $G=<U,D,F,B,L,R>$ 的 Cayley 图中任意顶点的度数是 12.

定义 3.8 群 $G =< g_1, g_2, \ldots, g_n >$ 中的任意元素可以表示成生成元及其逆的乘积：$g = g_{i1}g_{i2}\ldots g_{ik}$. 如果 g 不能写成比 k 个元素更少的乘积形式，称 g 是不可缩减的，这时称 k 为该元素 g 的长度. 特别规定单位元的长度为 0.

3.2 基本性质

定理 3.9 设 $\Gamma_G = (V, E)$ 是魔方群 G 关于 $\{U, D, F, B, L, R\}$ 的 Cayley 图，则 $\forall\, v, w \in V, \exists\, u \in V$, 使得 $d(v, w) = d(1, u)$.

证明： 不妨设 $d(v,w)=n$, 则 $vg_1g_2\ldots g_n = w$, $g_i \in \{U^{\pm1}, D^{\pm1}, F^{\pm1}, B^{\pm1}, L^{\pm1}, R^{\pm1}\}$, $i \in \{1, 2, \ldots, n\}$. 取 $u = v^{-1}w$ 即可. □

推论 3.10 $\mathrm{diam}(\Gamma_G)=\max\{d(1,v), v \in V\}$.

由推论 3.10, 魔方群 Cayley 图的直径等于离单位元最远的点到单位元的距离. 用 $G(n)$ 表示魔方群 G 中长度为 n 的元素集合.

定理 3.11 $G(i) \bigcap G(j) = \emptyset, i \neq j$.

定理 3.12 $G = \bigcup_{n=0}^{\infty} G(n)$.

推论 3.13 $|G| = \sum_{n=0}^{\infty} |G(n)|$.

确定魔方群 Cayley 图的直径实际上等同于找到 n, 使得 $|G(n)| \neq 0$ 且 $|G(n+1)| = 0$. 但是直接计算 $|G(n)|$ 十分困难，尤其是当 n 十分大的时候. 考虑一个相对容易确定的集合近似估计 $|G(n)|$. 定义如下集合：

$X(n) = \{g_1g_2\ldots g_n |\ g_i \in \{U^{\pm1}, D^{\pm1}, F^{\pm1}, B^{\pm1}, L^{\pm1}, R^{\pm1}\}, i \in \{1, 2, \ldots, n\}\}$,

特别地，令 $X(0) = \{1\}$.

定理 3.14 $|G(n)| \leq |X(n)|$.

推论 3.15 若 $\sum_{i=0}^{n} |X(i)| < |G| < \sum_{i=0}^{n+1} |X(i)|$, 则魔方群 Cayley 图的直径至少是 n + 1.

3.3 魔方群 Cayley 图直径的下界

[4] 中给出了一种确定下界的方法：剔除 $X(n)$ 中可缩减的元素，然后对 $X(n)$ 的元素个数求和，再与 $|G|$ 比较大小，从而确定下界．本文在此基础上做了改进，得到下界是 21 的结果．

定义 3.16 在 $X(n)$ 中，设 $M, M_1, M_2 \in \{U^{\pm 1}, D^{\pm 1}, F^{\pm 1}, B^{\pm 1}, L^{\pm 1}, R^{\pm 1}\}$．满足条件 $MM^{-1} = 1$ 的叫做单位重复；满足条件 $M^2 = M^{-2}$ 的叫做对合重复；满足条件 $M_1^{\pm 1} M_2^{\pm 1} = M_2^{\pm 1} M_1^{\pm 1}$，其中 M_1 和 M_2 是对面转动的叫做交换重复；满足条件 $M^3 = M^{-1}$ 的叫做逆元重复．

定理 3.17 魔方群 Cayley 图直径的下界是 21．

证明： 当 n=0 时，显然 $|X(0)| = 1$．

当 n=1 时，由定理 3.7，从单位元出发，有 12 个点与单位元相连接，从而 $|X(1)| = 12$．

当 n=2 时，剔除单位重复，由 $X(1)$ 向外扩散的新元素是 $11 \times |X(1)|$ 个．对合重复共有 6 个；交换重复共 3 对，每对有 $2 \times 2 = 4$ 个重复，共 $3 \times 4 = 12$ 个重复．这样，$|X(2)| = 11 \times |X(1)| - 6 - 12 = 114$．

当 n=3 时，剔除单位重复，由 $X(2)$ 向外扩散的新元素是 $11 \times |X(2)|$ 个．对合重复只有 5 种情况，设 $X(1)$ 中某元素的末转动是 M，则 $MM^{-1}M^{-1} = MMM$ 这种情况不可能出现，因为其包含在了单位重复中，于是对合重复的总个数是 $5 \times |X(1)|$．另外，交换重复有 10 种情况，设 $X(1)$ 中某元素的末转动是 M_1，对面转动是 M_2，则 $M_1 M_1^{-1} M_2^{\pm 1} = M_1 M_2^{\pm 1} M_1^{-1}$ 这种情况不可能出现，因为其同样包含在了单位重复中，于是交换重复的总个数是 $10 \times |X(1)|$．最后，逆元重复有 12 个．这样，$|X(3)| = 11 \times |X(2)| - 5 \times |X(1)| - 10 \times |X(1)| - 12 = 1062$．

当 n=4 时，单位重复，对合重复，交换重复与 n=3 时类似．逆元重复有 10 种情况，设 $X(1)$ 中某元素的末转动是 M，则 $MM^3 = MM^{-1}$ 和 $MM^{-3} = MM$

这两种情况不可能出现，因为其包含在单位重复中，于是逆元重复的总个数是 $10 \times |X(1)|$. $|X(4)| = 11 \times |X(3)| - 5 \times |X(2)| - 10 \times |X(2)| - 10 \times |X(1)| = 9852$.

当 $n \geq 4$ 时，一般的递推公式是：

$$|X(n)| = 11 \times |X(n-1)| - 5 \times |X(n-2)| - 10 \times |X(n-2)| - 10 \times |X(n-3)|.$$

其中，等式右边的第一项表示在剔除单位重复的情况下扩散的新元素个数，第二项表示剔除对合重复，第三项表示剔除交换重复，第四项表示剔除逆元重复. 经过计算，有：

$$\sum_{n=0}^{20} |X(n)| \approx 3.3 \times 10^{19} < |G| \approx 4.3 \times 10^{19} < \sum_{n=0}^{21} |X(n)| \approx 2.4 \times 10^{20},$$

根据推论 3.15, 魔方群 Cayley 图的直径至少是 21. □

评注：上述方法只是把最简单的重复情况考虑了，实际上还有很多比较复杂的重复情况存在. 设 M_1, M_2 是对面转动，$M_1^2 M_2 M_1^2 = M_2$ 这种重复情况就没有出现在上述考虑中. 另外 $M_1^2 M_2 = M_1 M_2 M_1 = M_2 M_1^2$ 也是上述方法没有考虑到的重复情况. 理论上说，如果把所有的重复情况都剔除了，则 $G(n) = X(n)$. 如果尽可能地剔除重复的元素，估计下界还有进一步上升的空间，只是要考虑的情况非常复杂，需要细致全面的分析.

四 未解决的问题

Joyner 在其著作 [5] 的末章列举了一些关于魔方的未解决的问题，现转述于此：

问题 4.1 (上帝的算法， Singmaster) 确定魔方群 Cayley 图的直径.

这是关于魔方的最著名问题，自 Singmaster 在 1982 年提出后 26 年来没有得到解决. 由于近 10 年科技的迅猛发展，一些人开始用高速计算机求解该问题，获得了不错的结果.

定义 4.2 Γ 是一个图， Γ 上的 Hamilton 巡回是指恰好经过每个点一次的路径. 如果 Hamilton 巡回存在，则称 Γ 是 Hamilton 图.

问题 4.3 (Schwenk) 魔方群 Cayley 图是否为 Hamilton 图？

问题 4.4 (Singmaster) 确定魔方群每个阶的元素个数.

问题 4.3 实际上即是确定魔方群的阶方程. 所谓阶方程就是把群的元素按照阶进行分类的表达式.

定义 4.5 G 是置换群，元素 $g \in G$ 的长度记作 $l(g)$, 定义 G 的 Poincaré 多项式为： $P_G(t) = \sum_{g \in G} t^{l(g)}$.

问题 4.6 计算魔方群的 Poincaré 多项式.

定义 4.7 G 的共轭类集合记作 G_*,$g \in G$ 的阶记作 $o(g)$, 定义 G 上的生成多项式为： $P_{G_*}(t) = \sum_{g \in G_*} t^{o(g)}$.

问题 4.8 计算魔方群的生成多项式.

参 考 文 献

[1] [美] 詹. 诺尔斯. 魔方解法. 世界知识出版社, 1982.

[2] Alexander H. Frey, Jr. and David Singmaster. Handbook of Cubik Math. Enslow Publisher, 1982.

[3] Daniel Kunkle, Gene Cooperman. Twenty-Six Moves Suffice for Rubik's Cube. ISSAC'07, Waterloo, Ontario, Canada, July 29-August 1, 2007.

[4] The Group Theory Behind Rubik's Cube. http://users.ox.ac.uk/~ quee1871/rubik. PDF

[5] David Joyner. Adventures in Group Theory. The Johns Hopkins University Press, 2002.

[6] Janet Chen, Group Theory and the Rubik's Cube, http://www.math.harvard.edu/~ jjchen/docs/Group%20Theory%20and%20the%20Rubik's%20Cube.pdf, 2004.

致谢

本文是在导师施武杰教授的悉心指导下完成的. 感谢他这几年在学业上给我的指导. 感谢 Don Taylor 教授, 从澳洲给我寄来了 30 年前关于魔方的手稿复印件. 感谢我的家人对我学业的督促, 尤其是我的兄长廖莹毅. 感谢苏州大学数学科学学院的所有领导和老师, 让我顺利完成了学业！感谢苏州大学研究生处对研究生论文的资助！最后, 我要特别感谢金晶同学, 感谢她在论文写作过程中给我的鼓励和支持, 感谢她和我讨论相关细节, 尤其是在论文排版等问题上给我的帮助.