对数独魔方及其性质的研究

作者: 王可为 王尧勇 李颖

指导老师:陈珈颖

浙江省新昌中学

浙江·中国

学术诚信声明

本参赛团队声明所提交的论文是在指导老师指导下进行的研究工作和取得的研究成果。尽本团队所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果。若有不实之处，本人愿意承担一切相关责任。

参赛队员：王可为 王光宇 李颖

指导老师：陈加颖

2019.9.5

对数独魔方及其性质的研究

摘要

本文结合三阶魔方和数独的规则,设计了一款新的游戏“数独魔方”并且运用了群论、编程等工具研究了数独魔方的一些性质.首先,本文介绍了数独魔方的定义和规则并提出了一系列问题.其次,我们对数独魔方进行了数学建模,并研究了数独魔方群的性质和数独魔方数字分布的规律以及二者之间的关系.最后,我们讨论了数独魔方的上帝之数.

关键词:数独魔方; 群论; $Cayley$图直径;

Research into Sudoku Cube and its Nature

Abstract

This paper combines the Rubik's Cube and Sudoku to design a new game named "Sudoku Cube" and uses group theory, programming and other tools to study some properties of Sudoku Cube. First, this paper introduces the definitions and rules about Sudoku Cube and raises a series of questions. Secondly, we carried out mathematical modeling of Sudoku Cube, and studied the nature of the group of Sudoku Cube as well as the law of the distribution of numbers in a Sudoku Cube and the relationship between them. Finally, We discussed the God's number of Sudoku Cube.

Keywords: Sudoku Cube; group theory; the diameter of Cayley Graph;

目录

一. 基本介绍

1.1 引言

魔方, 最早以三阶的形式出现于1974年, 是匈牙利建筑学教授 Ernő Rubik 为帮助学生认识空间立方体结构而发明的一种益智玩具（图1.1）. 其在空间上具有高度对称性, 并逐渐由三阶向更高阶发展, 也衍生出了多种变种魔方（图1.2）.

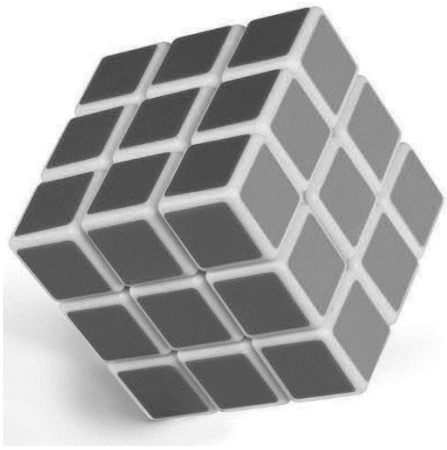

图 2.1

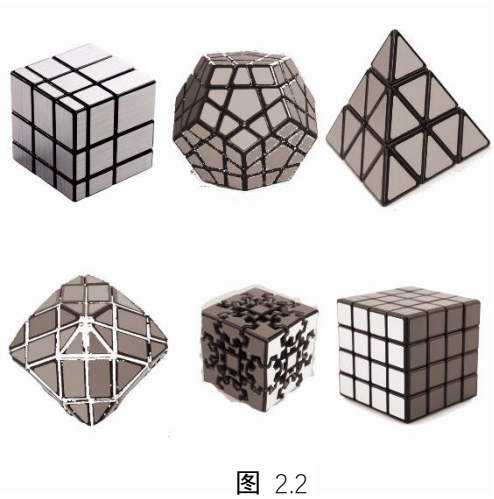

图 2.2

数独, 是一种源于18世纪瑞士的数字游戏（图1.3）. 其基本规则是根据9×9盘面上的已知数字, 推理出剩余空格的数字, 并满足每一行、每一列、每一粗线宫（3×3）内的数字均含1~9且不重复. 和魔方一样, 数独也衍生出了大量变种.

		7			9			
8			1			5		
	2			3			6	
		4						3
1			5			7		
	6			2			9	
		3			4			8
7			6			1		
	9			8			2	

图 1.3

由魔方在空间上的高度对称性, 数独在数字分布上的高度互异性, 我们想到, 将平面范围内的数独与立体的三阶魔方结合在一起, 从而产生一种新游戏——数独魔方. 这是本文研究的主要对象.

1.2 对数独魔方的基本介绍与定义

1.2.1 结构及有关定义

数独魔方（图1.4），是在普通三阶魔方的空间结构基础上，将三组1~9的数字对$3\times3\times3$个小立方体进行赋值. 与数独相类似的是，要求在一定范围内不得出现重复的数字.

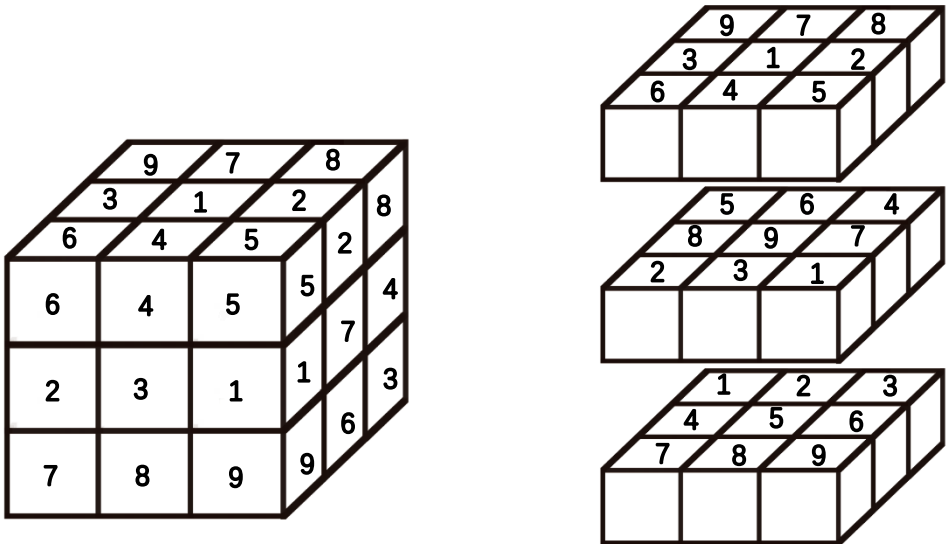

图 1.4

数独魔方的操作方法与三阶魔方一致. 但为了后文研究与表达更方便，我们对每一次操作都进行了专门定义.

定义 1. 2. 1 数独魔方的最小研究单位为**块**，即$1\times1\times1$的小立方体块（图1.5）. 每一个数独魔方有27个块.

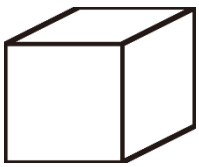

图 1.5

定义 1. 2. 2 数独魔方中每$3\times3\times1$的结构为**层**（图1.6）. 每一个数独魔方中有9个层.

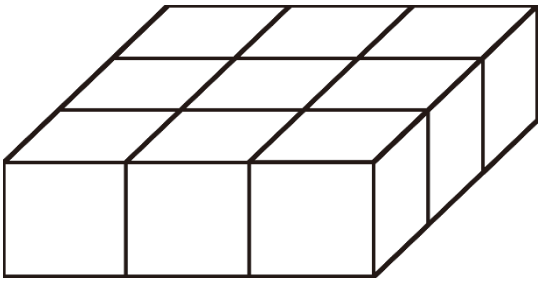

图 1.6

定义 1.2.3 将要发生位置变换的层的3×3的面正对操作者,进行一次**逆(顺)时针**旋转90°的操作,我们称之为**旋转**(**逆旋转**).可以发现,一个数独魔方中有三层夹于相邻两层之间,若对其进行一次旋转,则相当于对与该层相邻的两层分别进行一次逆旋转.为研究方便,我们将这三层的旋转,视为其相邻两层旋转的合成(会在后文中详细叙述).

1.2.2 状态及有关定义

定义 1.2.4 当一个数独魔方每一层中的数字均不重复时,我们称它处于**初始状态**(图1.4就是一种初始状态).

定义 1.2.5 在三阶魔方中,只要27个块中存在3组1~9的数字,我们就称它为**数字魔方**.如果一个数字魔方经过若干次旋转之后能处于初始状态,我们就称这个数字魔方为**数独魔方**.显然,数独魔方是一种能够被还原为初始状态的特殊的数字魔方.

定义 1.2.6 不为初始状态的数独魔方通过一系列旋转得到初始状态,则称该数独魔方被**还原**.记操作次数为**还原步数**.

1.3 问题的提出

问题 1 数独魔方可构造的初始状态总数为多少.为避免重复研究,如何判断这些初始状态是否等价.

问题 2 数独魔方在数字分布上是否具有某些性质特征.

问题 3 对于一个给定的数独魔方,共有多少种状态.

问题 4 如何判断一个数字魔方是否为数独魔方.

问题 5 2010年人们利用计算机证明了任何组合的普通三阶魔方均可以在20步以内回到原来状态,也就是其上帝之数是20.那么对于任意一个数独魔方,其上帝之数是多少.

二. 模型建立

2.1 群论简介

定义 2.1.1 设G是一个非空集合, 在G中定义一种二元运算“$\cdot$”, 如果满足:
(1) $\forall a,b\in G$, 有$c=a\cdot b\in G$, 即**封闭性**.
(2) $\forall a,b,c\in G,(a\cdot b)\cdot c=a\cdot(b\cdot c)$, 即**结合律**成立.
(3) $\exists e\in G,\forall a\in G,a\cdot e=e\cdot a=a,e$称为$G$的**单位元**.
(4) $\forall a\in G,\exists a^{-1}\in G$, 使得$a\cdot a^{-1}=a^{-1}\cdot a=e,a^{-1}$称为$a$的**逆元**.
那么, 我们称集合G以“$\cdot$”为运算构成一个**群**.

定义 2.1.2 若群G的元素有无数个, 则称G是一个**无限群**; 若G的元素是有限的, 则称G是一个**有限群**, 其元素个数称为群的**阶**, 记作$|G|$.

定义 2.1.3 设Ω是由n个文字组成的集合, $\Omega=\{\alpha_1,\alpha_2,\alpha_3,\dots,\alpha_n\},\Omega$到自身的一个一一映射称为作用于$\Omega$上的**$n$元置换**, 简称**置换**.

定理 2.1.4 n元置换全体组成的集合S_n对置换的乘法构成一个群, 称为**n元对称群**, 且$|S_n|$=$n!$.
证明: $[1]P11$

定义 2.1.5 若置换σ把n个文字$\alpha_1,\alpha_2,\alpha_3,\dots,\alpha_n$中的一部分$\alpha_{i1},\alpha_{i2},\alpha_{i3},\dots,\alpha_{im}(m\leqslant n)$作如下变换:

$$\alpha_{i1}^{\sigma}=\alpha_{i2},\alpha_{i2}^{\sigma}=\alpha_{i3},\cdots,\alpha_{im-1}^{\sigma}=\alpha_{im},\alpha_{im}^{\sigma}=\alpha_{i1}$$

那么称σ为一个**m-轮换**, 简称**轮换**. m称为轮换的**长度**. 若$m=2$, 则称σ为**对换**

定义 2.1.6 对于两个轮换$\sigma=(\alpha_{i1},\alpha_{i2},\alpha_{i3},\dots,\alpha_{im})$与$\tau=(\alpha_{j1},\alpha_{j2},\alpha_{j3},\dots,\alpha_{jl})$, 若$\alpha_{i1},\alpha_{i2},\alpha_{i3},\dots,\alpha_{im}$与$\alpha_{j1},\alpha_{j2},\alpha_{j3},\dots,\alpha_{jl}$各不相同, 则称$\sigma$与$\tau$是**不相交的**. 显然, 不相交的轮换是可交换的.

定理 2.1.7 任意一个置换均可表示为若干个不相交轮换的乘积, 且表示方法唯一.
证明:$[1]P13$

定理 2.1.8 n元置换σ表示成若干个对换的乘积后, 其中对换个数的奇偶性由σ唯一确定, 且与n元排列$1^{\sigma},2^{\sigma},3^{\sigma},\cdots,n^{\sigma}$奇偶一致.
证明:$[1]P16$

定义 2.1.9 若n元置换σ可表示为奇数个对换的乘积, 则称σ为**奇置换**; 若σ可以表示为偶数个置换的乘积, 则称σ为**偶置换**. 显然偶置换与偶置换的乘积仍为偶置换.

定理 2.1.10 n元偶置换对置换的乘法构成一个群$A_n,|A_n|=\frac{n!}{2}$.

证明:[1]$P17$

定理 2.1.11 $A_n(n \geq 3)$由一切长度为3的轮换生成.
证明:[1]$P77$

定义 2.1.12 G和H是两个群, φ是G到H的一个映射, 如果对于G中任意两个元素, 都有$(ab)^{\varphi} = a^{\varphi}b^{\varphi}$, φ就称为G到H的一个**同态映射**. H称为G的一个**同态象**, 记作$\boldsymbol{G}\sim\boldsymbol{H}$. 若$\varphi$是一一映射, 则称$\varphi$是$G$到$H$的一个**同构映射**. G同构于H, 记作$\boldsymbol{G} \cong \boldsymbol{H}$.

2.2 数独魔方的表示方法

2.2.1 块的表示方法

为方便描述数独魔方的位置结构, 我们采用以下两种表示方法:

1. **坐标表示法**:类比于空间直角坐标系, 对于数独魔方的每一个块, 用(x,y,z)表示其位置在从下到上第x层, 从里到外第y行, 从左到右第z列.

定义映射φ从坐标映射到坐标对应的块上的数字: $\varphi(x,y,z) = n$.

2. **字母表示法**:以小写字母u,d,l,r,f,b分别表示数独魔方外围的六个层, 即上层, 下层, 左层, 右层, 前层, 后层. 同时字母又可表示该层的中心块. 对于边块和角块, 可以用层与层的交集来表示, 如lf表示左层与前层相交的三个块的中间块, drf表示下层、右层、前层相交的一个块. 为行文方便, 在这里规定字母书写的优先级:$u(或d) > l(或r) > f(或b)$.

设集合X表示所有的块的集合(体中心块不考虑),E表示所有边块的集合, V表示所有角块的集合.

显然, 字母表示法可以在书写上明显的区分中心块、边块和角块, 坐标表示法又可以更直观的表明块所在的层, 因此后文会根据不同需要采取不同的表示方法.

2.2.2 旋转操作的表示方法

以大写字母U,D,L,R,F,B表示各个层的旋转, 例如U表示对上层进行一次旋转操作. 同样的, 可以用$U^{-1},D^{-1},L^{-1},R^{-1},F^{-1},B^{-1}$表示逆旋转操作. 显然, 对于数独魔方的每一个操作, 均可以由其他的操作合成得到.

设G是所有操作组成的集合, $G =< U,D,L,R,F,B >$. G中的每一个元素都是一个置换, 都可以表示为若干个轮换的乘积.

$U = (ulf\ ulb\ urb\ urf)(uf\ ul\ ub\ ur)$
$D = (dlf\ drf\ drb\ dlb)(df\ dr\ db\ dl)$
$L = (\ ulf\ dlf\ dlb\ ulb)(ul\ lf\ dl\ lb)$
$R = (urf\ urb\ drb\ drf)\ (ur\ rb\ dr\ rf)$
$F = (urf\ drf\ dlf\ ulf)(uf\ rf\ df\ lf)$
$B = (urb\ ulb\ dlb\ drb)(ub\ lb\ db\ rb)$

用p表示数独魔方的状态, 所有状态组成的集合记为P. 对于$M \in G$, 用p^M表示状态p经过操作M之后的状态. 显然有$\forall M_1, M_2 \in G, p \in P, p^{(M_1 \cdot M_2)} = (p^{M_1})^{M_2}$.

2.3 数独魔方群

定理 2.3.1 G以置换的乘法为运算构成一个群,称为**数独魔方群**.

证明:(1)封闭性:

$\forall M_1, M_2 \in G, M = M_1 \cdot M_2 \in \mathrm{G}$, 故封闭性成立.

(2)结合律:

$$\forall M_{1,}, M_2, M_3 \in G, \forall p \in P,$$

$$p^{(M_1 \cdot M_2) \cdot M_3} = (p^{M_1 \cdot M_2})^{M_3} = ((p^{M_1})^{M_2})^{M_3}$$

$$p^{M_1 \cdot (M_2 \cdot M_3)} = (p^{M_1})^{(M_2 \cdot M_3)} = ((p^{M_1})^{M_2})^{M_3}$$

因此有$M_1 \cdot (M_2 \cdot M_3) = (M_1 \cdot M_2) \cdot M_3$, 故结合律成立.

(3)单位元:

不难想象,$\exists e \in G, p \in P$,使得$p^e = p$.

那么 $p^{(M \cdot e)} = (p^M)^e = p^M$

$p^{(e \cdot M)} = (p^e)^M = p^M$

所以有 $M \cdot e = e \cdot M = M$

所以e为G的单位元.

(4)逆元:

$\forall M \in G, M = M_1 \cdot M_2 \cdot \ldots \cdot M_l, l \in \mathbb{N}^*, \exists M^{-1} = M_i^{-1} \cdot M_{i-1}^{-1} \cdot \cdots \cdot M_2^{-1} \cdot M_1^{-1}$,

其中$M_i^{\pm 1} \in G, i \in \{1,2,\cdots l\}$, 使得$M \cdot M^{-1} = M^{-1} \cdot M = e$, 故$M^{-1}$为$M$的逆元.

综上,由*定义 2.1.1*得,定理 2.3.1 成立,证毕.

定理 2.3.2 G中的每一个元素都是偶置换.

证明:由 *2.2.2* 和*定义 2.1.9* 不难得出这个结论.

三. 数独魔方及数独魔方群的基本性质

3.1 换位子

从 *2.2.2* 我们可以看出,对于G的6个生成元,每次转动都由2个长度为4的角块轮换和边块轮换合成. 故每转动一次,会有8个块的位置发生改变. 所以在还原魔方时,仅进行几次操作数独魔方就会变得十分混乱. 为研究方便,我们自然希望能够尽可能少地改变块的位置以保证已还原部分的有序性.

定义 3.1.1 设$M_1, M_2 \in \{U, D, L, R, F, B\}$, M_1, M_2相交, 令$[M_1, M_2] = M_1 \cdot M_2 \cdot M_1^{-1} \cdot M_2^{-1}$. 显然, $[M_1, M_2] \in G$, 由$[M_1, M_2]$合成的置换称为**换位子**.

不难看出,换位子有仅仅改变少量块的位置而化繁为简的作用. 例如, $[M_1, M_2]^2$改变3个边块的位置而使角块不变; $[M_1, M_2]^3$改变2对角块的位置而使边块不变. 本章中的证明将大量使用换位子.

3.2 G的阶

本节我们将证明 $|G| = \frac{8! \cdot 12!}{2}$.

引理 3.2.1 G_V表示在角块之间进行的所有偶置换组成的集合, G_E表示在边块之间进行的所有偶置换组成的集合. 不难看出G_V和G_E均以置换的合成为运算构成一个群. 且有$G_V \leqslant G, G_E \leqslant G$.

证明:类比于*定理 2.3.1*,不难得出这个结论.

引理 3.2.2 $\forall a, b, c \in V, (a\ b\ c) \in G_V \subseteq G$.

证明:(1)当a, b, c在同一层时:

不失一般性,不妨设$a = ulb, b = urb, c = urf$,注意到换位子$M_1 = [U, F]^3 = (ulf\ dlf)(urf\ urb)$,换位子$M_2 = [U, L]^3 = (ulf\ dlf)(ulb\ urb), \therefore M_1 \cdot M_2 = (ulb\ dlf\ drb) = (a\ b\ c)$.

(2)当a与b位于同一条棱上, a与c位于另一个层的对角线上时:

不妨设$a = ulb, b = ulf, c = drb$. 类似于$M_1, \exists M_3 = (urf\ urb), M_4 = M_1 \cdot M_3 = (ulf\ dlf)(ulb\ dlb)$. 由(1)可知, $\exists M_5 = (dlb\ dlf\ drb), \therefore M_4 \cdot M_5 \cdot M_4 = (ulb\ ulf\ drb) = (a\ b\ c)$.

(3)当a, b, c两两连线为相邻3个层的对角线时:

不妨设$a = ulb, b = urf, c = dlf$,由(1)可知, $\exists M_6 = (ulb\ urf\ urb)$,由(2)可知$\exists M_7 = (ulb\ urb\ dlf), M_6 \cdot M_7 = (ulb\ urf\ dlf) = (a\ b\ c)$.

综上所述, $\forall a, b, c \in V, (a\ b\ c) \in G_V \subseteq G$. 证毕.

引理 3.2.3 $G_V = A_8$.

证明:由*引理3.2.2*和*定理2.1.11*,且$|V| = 8, \therefore G_V \geqslant A_8$.又$G_V \leqslant G$,由*定理2.3.2*可知, G

中的置换均为偶置换, 故G_V中的置换均为偶置换, $\therefore G_V \leqslant A_8. \therefore G_V = A_8$. 证毕.

引理 3.2.4 $\forall a,b,c \in E, (a\ b\ c) \in G_E \subseteq G$.

证明:由*引理 3.2.3*可知, 若在经过偶数次转动后能实现边块的置换, 则必定存在一种换位子能将角块位置复原. 故以下证明中只需考虑边块的位置变换, 而角块略去不写.

为方便描述3个边块的相对位置, 规定数独魔方的棱长为2, 边块到其相邻角块的距离为1. 不妨令$a = ul$.

(1) 当a,b,c相连的3条线段长度均为$\sqrt{2}$或$\sqrt{6}$时:

此时3个边块位于3条互不平行的棱上. 首先, $\exists M_8 = [U^{-1}, F^{-1}]^2 = (ul\ rf\ uf)$, 不妨令$b$位于与$rf$所在的棱平行的棱上, c位于与uf所在的棱平行的棱上, 而在不改变a位置的情况下, F^2, D^2, B^2的简单组合能使uf转到与其所在棱平行的棱上, 类似的, F^2, R^2, B^2的简单组合也能使rf转到与其所在棱平行的棱上. 所以$\exists M_9$, 使得b到rf, c到uf, $\therefore M_9 \cdot M_8 \cdot {M_9}^{-1} = (a\ b\ c)$.

(2) 当$b = dr$时:

若$c = dl$, 则有$(L^2D^2)^2 = (a\ b\ c)$. 若$c \neq dl$, 不妨设$c = lf$, 由(1)知,

$\exists M_{10} = (ul\ lf\ uf)$, $\exists M_{11} = (uf\ dr\ lf)$, $\therefore {M_{11} \cdot M_{10}}^2 = (a\ b\ c)$.

(3) 当a,b连线的线段长度为2时:

不妨令$b = dl$, 此时D^2把b转到dr, $\because \exists M_{12} = (a\ dr\ c), \therefore D^2 M_{12} D^2 = (a\ b\ c)$.

综上所述, $\forall a,b,c \in E, (a\ b\ c) \in G_E \subseteq G$. 证毕.

引理 3.2.5 $G_E = A_{12}$.

证明:由*引理 3.2.2*和*定理 2.1.11*, 且$|E| = 12, \therefore G_E \geqslant A_{12}$.又$G_E \leqslant G$,由*定理 2.3.2*可知, G中的置换均为偶置换, 故G_E中的置换均为偶置换, $\therefore G_E \leqslant A_{12}. \therefore G_E = A_{12}$. 证毕.

定理 3.2.6 $|G| = \frac{8! \cdot 12!}{2}$.

证明:$\forall M \in G, \exists M_1, M_2$,使得$M = M_1 \cdot M_2$, 其中$M_1$是只涉及角块的转动, M_2是只涉及边块的转动. 由于M为偶置换, 故M_1, M_2奇偶性相同.

(1) 若M_1, M_2同为偶置换, 则$M_1 \in G_V, M_2 \in G_E$, 由*引理 3.2.3*和*引理 3.2.5*可知, 这样的M共有$|G_V| \cdot |G_E| = |A_8| \cdot |A_{12}| = \frac{8! \cdot 12!}{4}$ 种.

(2) 若M_1, M_2同为奇置换, 则$\exists {M_1}' \in G_V, {M_2}' \in G_E$, 使得$F \cdot {M_1}' \cdot {M_2}'$与$M = M_1 \cdot M_2$一一对应, 由*引理 3.2.3*和*引理 3.2.5*可知, 这样的M共有$|G_V| \cdot |G_E| = |A_8| \cdot |A_{12}| = \frac{8! \cdot 12!}{4}$ 种.

综上, $|G| = \frac{8! \cdot 12!}{2}$. 证毕.

由*定理 3.2.6*的证明, 我们可以得出以下结论:

推论 3.2.7 对于置换M_1, M_2, 若M_1在角块之间进行, M_2在边块之间进行, 且$M_1 \cdot M_2$为偶置换, 则$M_1 \cdot M_2 \in G$.

3.3 数独魔方的数字分布性质及P的阶

本节我们将讨论数独魔方在数字分布上的性质, 初始状态数, 数独魔方判定定理以及证明$|P| = \frac{8! \cdot 12!}{72}$.

引理 3.3.1 数独魔方7个中心块(包括1个体中心块和6个面中心块)上的数字互异.

证明: 由于任意两个中心块共层, 所以不难得出这个结论.

定义 3.3.2 体中心块上的数字称为**中心子**, 面中心块上的数字称为**亚中心子**, 余下的两个数字称为**剩余子**.

设中心子数字为n_1, 亚中心子数字为$n_2, n_3, n_4, n_5, n_6, n_7$, 剩余子数字为$n_8, n_9$.

定理 3.3.3(P 性质) 两组剩余子均位于边块上, 亚中心子剩下的两个数字一个位于边块, 一个位于角块, 中心子剩余的两个数字均位于角块上.

证明: 假设将第一个n_8填入角块, 不妨令$\varphi(3,1,1) = n_8$, 则位于中间层的n_8只能令$\varphi(2,3,3) = n_8$, 则第三个n_8无法填入任意一个块, 矛盾. 故n_8均位于边块上. 同理可证其他数字. 证毕.

引理 3.3.4 对于剩余子中两个数字n_8, n_9, 要么三对n_8, n_9均关于体中心块对称, 要么只有一对n_8, n_9关于体中心块对称. 将三对均对称的排布称为**完全对称**的, 而只有一对对称的排布称为**非完全对称**的.

证明: 假设任意一对剩余子不对称, 不妨令$\varphi(1,2,3) = \varphi(2,3,1) = \varphi(3,1,2) = n_8$, 那么标有×的$(1,3,2), (2,1,3), (3,2,1)$均不得填入$n_9$(图3.1), $(2,1,1)$和$(2,3,3)$必须有一个填入n_9. 不妨令$\varphi(2,1,1) = n_9$, 于是, 底部没有块可供n_9填入, 矛盾. 故至少有一对剩余子对称, 而当两对剩余子对称时, 最后一对剩余子也必然对称. 引理 3.3.4 成立. 证毕.

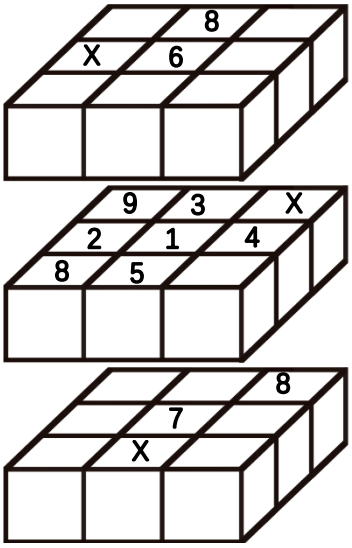

图 1.4

定理 3.3.5 在规定中心子和亚中心子的前提下, 数独魔方共有80种互异的初始状态, 记为$c_i, i \in \{1,2,\cdots,80\}$. 所有初始状态组成的集合记为$P_c$.

证明:本定理采用构造性证明.

在确定剩余子的排布后,由*定理 3.3.3* 可知,亚中心子和中心子剩下的数字的位置有很强的限制条件,结合*引理 3.3.4* 不难分类讨论得到:

(1)完全对称的剩余子排布共有$4\times2=8$种;

(2)非完全对称的剩余子排布共有$4\times2\times3=24$种;

(3)每一种完全对称的剩余子排布对应4种初始状态;

(4) 每一种非完全对称的剩余子排布对应2种初始状态;

综上,互异的初始状态共有$8\times4+24\times2=80$种. 证毕.

定理 3.3.6(数独魔方判定定理) 在规定中心子和亚中心子的前提下,一个数字魔方是数独魔方的充分必要条件是该数字魔方的数字分布满足P性质.

证明:必要性显然成立,下面证明充分性:

设v_1,v_2为角块的任意两种排布, M_1为使$v_1^{M_1}=v_2$的一个置换. 若M_1为偶置换,则已有$M_1\in G$. 若M_1为奇置换,设两个中心子n_1分别位于角块a,b上,设c为除a,b外任意一个角块,考虑到奇置换$M_2=(a\ b\ c)(b\ c)$,它实际上并没有改变角块上数字的分布. 于是有$v_1^{M_1\cdot M_2}=v_2$,而$M_1\cdot M_2\in G.\ \therefore\exists M\in G,v_1^M=v_2.$

因此,将一个数独魔方角块上的数字任意排列,所得的数字魔方仍为数独魔方. 同理可证,这对边块也同样成立. 定理 3.3.5 成立. 证毕.

根据*定理 3.3.5*,我们可以得出以下推论:

推论 3.3.7 $|P|=\frac{8!}{2!}\times\frac{12!}{3!\times3!}=\frac{8!\cdot12!}{72}.$

推论 3.3.8 $\forall c_i,c_j\in P_c,i,j\in\{1,2\cdots,80\},\exists M\in G,c_i^M=c_j$.也就是说,可以通过一系列转动,使一个数独魔方从一种初始状态转到另外任意一种初始状态.

从*推论 3.3.8*我们可以看出,数独魔方的80种初始状态是等价的,所以不妨规定c为唯一初始状态以代表P_c中的任意元素.

3.4 G和P的关系

在 *3.2* 节和 *3.3* 节的基础上,本节将讨论G和P的关系.

构造映射$\psi:G\mapsto P,\psi(M)=c^M,M\in G,c\in P$,并认为$\psi(e)=c$.

定义P上的运算"$\cdot$"满足:

$$p_1\cdot p_2=c^{M_1M_2},$$

$$\text{其中}p_1=c^{M_1},p_2=c^{M_2},\ p_1,p_2\in P,M_1,M_2\in G.$$

定理 3.4.1 P以"$\cdot$"为运算构成一个群,称为数独魔方状态群.

证明:类比于*定理 2.3.1*,不难得出此结论.

定理 3.4.2 $G\sim P$.

证明:

$$\psi(M_1M_2)=c^{M_1M_2}=c^{M_1}\cdot c^{M_2}=\psi(M_1)\psi(M_2)$$

由*定理 3.2.6*和*推论 3.3.7*可知, $|G|>|P|$,故ψ并不是一一映射,根据*定义 2.1.12*, $G\sim P$.

证毕.

定理 3.4.3 $\forall p \in P, \exists M_1 = e, M_2, \dots, M_{36} \in G$,使得$p^{M_i} = p, i \in \{1,2,3 \dots 36\}$.

证明:注意到两类置换:第一类是将一组剩余子的三个相同数字进行轮换,第二类是将两对同在角块或边块上的相同数字进行对换.两类置换均满足在一个置换的作用下,状态不变.

对于$\forall p \in P$:

(1)若只进行第一类置换,能得到$3 \times 3 - 1 = 8$种置换;

(2)若只进行第二类置换:

①若其中不包括中心子:则有$3 \times 3 = 9$种置换;

②若其中包括中心子:则有$2 \times 3 \times 3 = 18$种置换;

(3)另外考虑到恒等置换e;

综上,共有36种置换满足条件.证毕.

根据前两节,我们已经有$|G| = 36|P|$,这与*定理 3.4.3* 是相一致的.也就是说,G中每36个置换对应了P中的1种状态.同时我们不难推出如下推论:

推论 3.4.4 $\forall p \in P, \exists M_1, M_2, \dots, M_{36} \in G$,当且仅当$M = M_i, i \in \{1,2,3, \dots ,36\}$时,有$p_2 = p_1^M$.

也就是说,数独魔方任意两种状态之间的转化能且只能通过G中的36种置换实现.

四. 数独魔方的上帝之数

4.1 $Cayley$图简介

定义 4.1.1 用一对可数集(V,E)表示**图**, 其中V是**顶点集**, E是**边集**.

定义 4.1.2 若顶点v到w存在路径, 那么称v和w是**连通**的. 若$\forall v,w\in V$, v和w都是连通的, 那么称图(V,E)是**连通**的.

定义 4.1.3 用$d(v,w)$表示顶点v,w之间的最短路径边数, 若v,w不连通, 则 $d(v,w)=\infty$. 定义图(V,E)的直径$diam\big((V,E)\big)=max\{d(v,w),v,w\in V\}$.

定义 4.1.4 $G=<M_1,M_2,\cdots,M_n>$是由集合$X=\{M_1,M_2,\cdots,M_n\}$生成的置换群, G关于X的$Cayley$图是(V,E), 其中V是G中的元素, 边由以下条件决定:若$x,y\in V=G$,则当且仅当$y=M_i\cdot x$或$x=M_i\cdot y$, $i\in\{1,2,\cdots,n\}$, x和y有边相连.

定理 4.1.5 对于置换群$G=<M_1,M_2,\cdots,M_n>$的$Cayley$图, $\forall v\in V$, v的度数$deg(v)=\left|\{M_1^{\pm1},M_2^{\pm1},\cdots,M_n^{\pm1}\}\right|$.
证明: $[3]P117$.

4.2 G的$Cayley$图直径下界

定义 4.2.1 用Γ_G表示数独魔方群的$Cayley$图.
由*定理 4.1.5*可知, Γ_G中任意顶点度数为12.

定义 4.2.2 $\forall M\in G,\exists M_1,M_2,\cdots,M_k\in\{U^{\pm1},D^{\pm1},L^{\pm1},R^{\pm1},F^{\pm1},B^{\pm1}\}$, 使得$M=M_1\cdot M_2\cdot\cdots\cdot M_k$, 若$M$不能写成比$k$个元素更少的乘积形式, 那么称$M$是**不可缩减**的, 称$k$为$M$的**长度**, 并且认为单位元$e$的长度为0.

定理 4.2.3 $\Gamma_G=(V,E),\forall v,w\in V=G,\exists u\in V,d(e,u)=d(v,w)$.
证明: 令 $d(v,w)=n,v\cdot M_1\cdot M_2\cdot\cdots\cdot M_n=w,M_i\in\{U^{\pm1},D^{\pm1},L^{\pm1},R^{\pm1},F^{\pm1},B^{\pm1}\},\exists u=v^{-1}\cdot w,d(e,u)=d(v,w)$. 证毕.

推论 4.2.4 $diam(\Gamma_G)=max\{d(e,v),v\in V\}$.

也就是说, 要求数独魔方群的$Cayley$图直径, 只要求出离单位元最远的点到单位元的距离. 用$G(n)$表示G中长度为n的元素的集合.

定理 4.2.5 $G(i)\cap G(j)=\emptyset,i\neq j$.

定理 4.2.6 $G=\cup_{n=0}^{\infty}G(n)$.

推论 4.2.7 $|G|=\sum_{n=0}^{\infty}|G(n)|$

于是, 我们可以知道, 若$|G(n)| \neq 0$ 且$|G(n+1)| = 0$, 那么n即为数独魔方群$Cayley$图直径. 考虑到$|G| = \frac{8!\cdot 12!}{2} \approx 9.6 \times 10^{12}$, 若直接用计算机枚举每一个元素, 时间复杂度为$\Theta(n^2)$, 远远超过家用计算机的运算能力. 因此用另一个集合X进行近似估计.

令 $X(n) = \left\{M_1 M_2 \cdots M_n | M_i \in \{U^{\pm 1}, D^{\pm 1}, L^{\pm 1}, R^{\pm 1}, F^{\pm 1}, B^{\pm 1}\}, i \in \{1,2,\cdots,n\}\right\}$, 并且规定 $X(0) = \{e\}$.显然有$|G(n)| \leqslant |X(n)|$.于是得到:

推论 4. 2. 8 $\sum_{i=0}^{n}|X(i)| < |G| < \sum_{i=0}^{n+1}|X(i)|$,那么数独魔方群$Cayley$图直径至少是$n+1$.

所以只要计算出$\sum|X(n)|$, 即可估计数独魔方群$Cayley$图直径的下界. 这里参考[4]中剔除重复的方法. 根据[2]中的结论, 我们得到了关于$|X(n)|$的递推式.

定理 4. 2. 9 $|X(1)| = 12, |X(2)| = 114, |X(3)| = 1062, |X(n)| = 11 \times |X(n-1)| - 15 \times |X(n-2)| - 10 \times |X(n-3)|, n \geqslant 4$.

证明: $[2]P15$.

通过计算机编程计算递推式, 我们得到了$\sum|X(n)|$的计算结果如表4.1:

n	$\|X(n)\|$	$\sum\|X(n)\|$
0	1	1
1	12	13
2	114	127
3	1062	1189
4	9852	11041
5	91302	102343
6	845922	948265
7	7837092	8785357
8	72606162	81391519
9	672652182	754043701
10	6231710652	6985754353
11	57732972822	64718727175
12	534860519442	599579246617
13	4955154015012	5554733261629
14	45906456645282	51461189906911

表格 4.1

$|G| = \frac{8!\times 12!}{2} = 9.65667226 \times 10^{12}$, $\sum_{i=0}^{13}|X(i)| < |G| < \sum_{i=0}^{14}|X(i)|$, 所以有:

定理 4. 2. 10 数独魔方群G的$Cayley$图直径的下界为14.

由*定理 3. 4. 3* 我们已经知道, $|G| = 36|P|$, 并且G中每36个置换对应P中1种状态. 由于这36个置换的分布并无规律性, 因此可近似认为它们在$G(n)$中均匀分布. 因此若$\sum|X(n)| > |P|$,

那么n即为数独魔方状态群P的$Cayley$图直径的下界. $|P| = \frac{8!\times 12!}{72} = 2.68240896 \times 10^{11}$, 由表 4.1 我们得到:

定理 4.2.11 数独魔方状态群P的$Cayley$图直径的下界为12.

4.3 数独魔方的最小还原步数

到上一节为止, 我们只是初步得到了数独魔方群的$Cayley$图直径的下界, 并且考虑到数独魔方群G和数独魔方状态群P之间的对应关系, 需要进一步更加细致地分析其中36个置换的分布, 才能使下界更精确. 另外, 考虑到数独魔方存在80种初始状态, 那么还原到任意一种初始状态都可以视为还原成功, 则其下界又有进一步精确的空间, 但这种情况十分复杂, 需要更加全面的分析.

准确计算数独魔方的上帝之数, 目前看来主要有以下两种方法:

其一是在不断精确下界的同时, 求出$Cayley$图直径的上界, 计算上界的算法在[5]中有详细的叙述. 最后使上界和下界不断逼近, 当上界等于下界时, 也就得到了数独魔方的上帝之数.

其二是通过计算机编程, 从初始状态开始, 不断用生成元去生成新的状态, 并判断这些状态与之前产生的状态是否重复, 直至再也无法生成新的不重复的状态, 那么也就确定了上帝之数. 这种算法的空间复杂度和时间复杂度都是惊人的, 个人计算机无法完成计算.

当然, 以上两种方法都可以优化. 例如, 用第一种方法, 我们可以得到一个上帝之数的范围区间, 在此基础上, 再通过编程逐一验证. 另外, 对数独魔方群进行陪集分解亦可以降低复杂度.

五.总结

未解决的问题

问题 6 数独魔方群G和数独魔方状态群P之间对应的36个置换有什么性质,分布有什么规律.

问题 7 如何得到准确的数独魔方的上帝之数.

问题 8 是否存在性质相似的高阶数独魔方,若有,其性质有那些差异,如何计算其上帝之数.

总结

本文结合了魔方和数独的游戏规则,创造了新的游戏——数独魔方.我们对数独魔方进行了数学建模并对它的一些性质做了深入的研究,得到了几个一般的结论.在此过程中,群论和编程是必不可少的工具,帮助我们更严谨、更定量的了解数独魔方的性质.

在写作本文的过程中,我们深刻地体会到了数学的对称之美.全文最棘手的问题的核心就是对称与不对称之间的矛盾.魔方的结构是高度对称的,群论本身也是研究对称性的理论,而数独所要求的互异性则打破了对称性,使模型变得更加复杂.另外,由于引入了重复数字,又造成了一定程度上的对称性,也正是根据这些特性,我们找到了数独魔方群G和数独魔方状态群P之间的关系,并再次用群论将其统一.

由于自身水平和精力的限制,关于数独魔方的一些重要性质,我们目前尚未能得到更为精确的结果.不过在上一章最后一节,我们给出了可能的研究方向,希望日后能有人对数独魔方进行更加深入的研究.当然,我们更希望,随着自身学术水平的提高,有朝一日能够自己将这些问题解决.

鸣谢

感谢指导老师在写作本文期间不遗余力的支持.感谢贾子涵、张启煊、项羽铭学长的参赛经验传授.最后,感谢丘成桐中学科学奖主办方,给了我们一次机会,深刻地体验了学术研究的乐趣和数学之美.

参考文献

[1]王萼芳.有限群论基础[M].清华大学出版社, 2012.

[2]朱磊.群论在魔方中的应用[D].苏州:苏州大学数学系, 2008.

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

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