

浙江省新昌中学

作者：贾子涵 张启煊 项羽铭

指导老师：吴裕东

对平面魔方群及其 Cayley 图直径的研究

中国 浙江

对平面魔方群及其 Cayley 图直径的研究

摘要

借鉴魔方的游戏规则, 本文设计了一款游戏“平面魔方”, 并运用群论、计算机等工具对其性质进行了深入的挖掘. 首先, 本文对平面魔方的规则进行了详细介绍, 其次, 运用群论的知识, 本文研究了平面魔方的各个性质, 如平面魔方置换群的阶、Cayley 图直径等, 最后将模型推广到异形并得出了一般性的结论.

关键字: 平面魔方 置换群 Cayley 图直径

Abstract

According to the rules of magic cube, the authors have designed a two-dimension magic cube in this paper. And the rules of the cube are explained integrallty. Also, by making use of group theory and the computer, the authors study the properties of the cube, such as the order of the permutation group of the cube, the diameter of Cayley Graph, etc. The authors also extend the model to irregular situations and the common results of the cube are obtained in this paper.

Keywords: two-dimension magic cube; permutation group; the diameter of Cayley Graph

目录

摘要

Abstract

1.基本介绍	1
1.1 引言	1
1.2 平面魔方规则介绍	1
1.3 问题的提出	2
2.模型建立	3
2.1 群论基本介绍	3
2.2 平面魔方群	4
三、 G_n 的阶	5
四、Cayley 图直径	6
4.1 Cayley 图的相关定义	6
4.2 n 阶平面魔方群 Cayley 图直径机解算法	7
4.3 n 阶平面魔方群 Cayley 图直径下界估计	10
五、模型推广	13
5.1 基本介绍	13
5.2 $G_{m \times n}$ 的阶	13
5.3 $G_{m \times n}$ 的 Cayley 图直径	14
5.4 $G_{m \times n}$ 的 Cayley 图直径下界估计	14
六、未解决的问题	15
七、参考文献	15
八、附录	15
8.1 平面魔方群 Cayley 图直径计算源码	15
8.2 n 阶平面魔方群 Cayley 图直径下界计算源码	17

1.基本介绍

1.1 引言

魔方是当今流行的一款益智玩具.自其于 1974 年被匈牙利建筑学家 Rublik 发明以来,受到了世界各地人民的喜爱.最初的魔方是三阶魔方(图 1),随后便衍生出了各种各样的魔方(图 2),但魔方的改变都主要是在阶数、结构的改变上.曾有魔方爱好者将魔方推广到四维并制作出了可视化的计算机游戏,但最终由于操作过于繁琐、模型不够直观且无法在现实中实现等原因,未能流行开来.

我们由此想到,既然可以将魔方推广到四维空间之中,那么是否也可以将其“压缩”到二维平面之中呢?受此启发,我们以魔方的规则为模板,设计出了一款新游戏——“平面魔方”,这将成为本文后几章中研究的重点.(注:平面魔方并非三维魔方在平面上的投影,它是一个由魔方启发而来,和魔方具有相似规则的游戏.)



图 1



图 2

1.2 平面魔方规则介绍

在本节中,我们将对平面魔方游戏规则进行介绍.

1.2.1 平面魔方结构

n 阶平面魔方由 n^2 个大小相等的正方形魔方块组成,每个魔方块上标有各不相同的数字 $0, 1, 2, \dots, n^2-1$,且各个魔方块均可安置在任意的位置,组成一个 $n \times n$ 的正方形(如图 3).

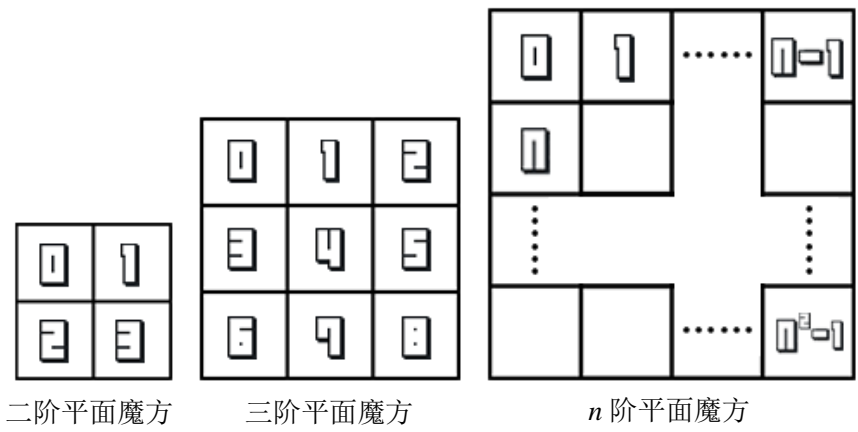


图 3

1.2.2 操作规则

定义 1.1 **移动**指将 n 阶平面魔方中任意一列/行中的所有数字上移/左移 1 格, 超出方阵范围的魔方块平移至该列/行的末尾.**操作**指将 n 阶平面魔方中任意一列/行进行任意 (不为 n 的倍数) 次移动.

如图 4 就是三阶平面魔方中的一种操作.

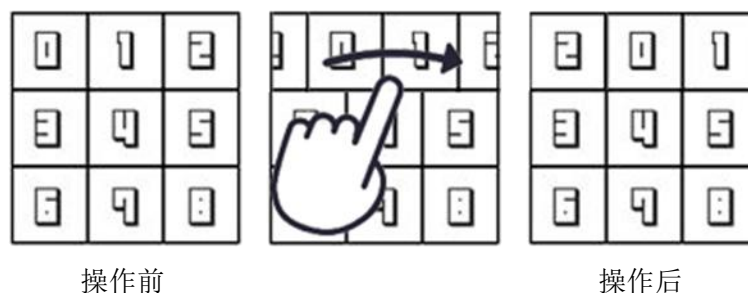


图 4

我们可以发现, 对平面魔方无论如何进行操作, 所得到的结果仍然是一个 $n \times n$ 的方阵, 且仍由数字 $0, 1, 2, \dots, n^2-1$ 不重复填充.

1.2.3 初始状态、还原与还原步数

下面我们给出初始状态、还原与还原步数的定义:

定义 1.2 一个平面魔方处于**初始状态**, 当且仅当平面魔方每个魔方块上的数字从左到右, 从上到下递增.

定义 1.3 若一个未处于初始状态的平面魔方经过若干次操作以后变换为了一个处于初始状态的平面魔方, 则称这个平面魔方被**还原**了, 且操作次数称为**还原步数**.

1.3 问题的提出

关于三阶魔方, 人们提出并解决了许多有趣的数学问题, 比如:

问题 1 三阶魔方共有多少种可能的组合?

解答 1 三阶魔方有 43, 252, 003, 274, 489, 856, 000 种不同的可能组合状态.

问题 2 至少需要几次操作, 就一定能够还原任意一个三阶魔方?

解答 2 任意组合的魔方均可以在 20 步之内还原.

问题 2 的解被称为魔方的上帝之数(God's number), 即三阶魔方 Cayley 图的直径. 这一问题困扰了数学家长达三十多年, 直到 2010 年 7 月, 美国加利福尼亚州科学家征用到了更加强大的资源——谷歌旧金山总部的超级主脑计算机. 随着程序的精简和设备的提升, 这量配置惊人的计算机破解了这一谜团. 研究人员利用计算机, 用枚举法验证了每一种情况, 证明任意组合的魔方均可以在 20 步之内还原, “上帝之数”正式定为 20.

需要指出的是, 群论将是解决魔方这一类变换问题的有力数学工具, 其介绍及一些基本内容将在第二章(2.1)中给出.

同样的, 关于平面魔方, 我们提出以下问题:

问题 3 三阶平面魔方共有多少种可能的组合?

问题 4 n 阶平面魔方共有多少种可能的组合?

问题 5 至少需要几次操作, 就一定能还原任意一个三阶平面魔方?

问题 6 至少需要几次操作, 就一定能还原任意一个 n 阶平面魔方?

关于问题 3、4、5 我们将在后面文章给出解答. 限于能力, 我们无法解出问题 6 的准确解, 但我们通过估计的方法给出了下界.

2. 模型建立

2.1 群论基本介绍

定义 2.1.1 设 G 是一个非空集合, 在 G 中定义了一种封闭的代数运算, 记作 " \cdot ", 即对于 G 中任意两个元素 a, b , 都存在 $c \in G$, 使得 $c = a \cdot b$. 如果 G 对这种运算还满足下面几个条件:

(1) 对 $\forall a, b, c \in G$, 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(2) $\exists e \in G$, 对 $\forall a \in G$, $e \cdot a = a \cdot e = a$.

(3) 对 $\forall a \in G$, $\exists a^{-1} \in G$, $a^{-1} \cdot a = a \cdot a^{-1} = e$.

那么 G 就称为一个群. 元素 e 称为 G 的单位元素, a^{-1} 称为 a 的逆元素.

定义 2.1.2 如果群 G 包含的元素个数有限, 则称 G 为有限群. 否则称 G 为无限群. 有限群 G 所包含的元素个数称为 G 的阶, 记作 $|G|$.

定义 2.1.3 设 Ω 是由 n 个文字组成的集合:

$$\Omega = \{\alpha_1, \alpha_2, \dots, \alpha_n\},$$

Ω 到自身的一个一一映射称为作用于 Ω 上的一个置换, 或 n 元置换, α_i^σ 表示 α_i 在置换 σ 下的象. 规定 σ 与 τ 的乘积为将 σ, τ 连续作用, 即

$$i^{\sigma\tau} = (i^\sigma)^\tau, i = 1, 2, \dots, n.$$

定义 2.1.4 由 n 元置换组成的群称为 n 元置换群, 简称置换群.

定理 2.1.5 n 元置换全体对置换的乘法构成一个群 S_n , 称为 n 元对称群, $|S_n| = n!$.

证明 [1] P13

定义 2.1.6 一般地, 如果对于 $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_m}$ 的置换 σ 把其中的 n 个字中的一部分 $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_m}$ ($m \leq n$) 作如下变换:

$$\alpha_{i_1}^\sigma = \alpha_{i_2}, \alpha_{i_2}^\sigma = \alpha_{i_3}, \dots, \alpha_{i_{m-1}}^\sigma = \alpha_{i_m}, \alpha_{i_m}^\sigma = \alpha_{i_1},$$

而其余的 $n - m$ 个文字保持不变, 则称 σ 为一个 m -轮换, 简称轮换, 记作

$$\sigma = (\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_m}).$$

若 σ 长度为 2, 则称 σ 为一个对换.

定理 2.1.7 任意 n 元置换 σ 均可以表示成若干个对换的乘积. 表示成对换乘积后, 乘积中对换个数的奇偶由 σ 唯一确定, 而且与 n 元排列 $1^\sigma, 2^\sigma, \dots, n^\sigma$ 的奇偶一致.

证明 [1] P16

定义 2.1.8 如果 n 元置换 σ 可表示为奇数个对换的乘积, 则称其为**奇置换**; 如果 n 元置换 σ 可表示为偶数个对换的乘积, 则称其为**偶置换**.

定理 2.1.9 任意两个偶置换的积是偶置换.

证明 由定义 2.1.8 可知成立.

定理 2.1.10 n 元偶置换全体对置换的乘法构成一个群 A_n , 称为 n 元**交错群**, $|A_n| = n!/2$.

证明 [1] P17

定理 2.1.11(Lagrange 定理) G 是有限群, H 为群 G 的子群, 则 $|H|$ 整除 $|G|$.

证明 [1] P29

定理 2.1.12 $A_n (n \geq 3)$ 由一切长度为 3 的轮换生成.

证明 [1] P77

定义 2.1.13 如果 G 和 H 是两个群, f 是 G 到 H 的一个映射.如果对任意的 $a, b \in G, (ab)^f = a^f b^f$, 则称 f 是 G 到 H 的一个**同态映射**;如果 f 是双射, 则 f 是 G 到 H 的一个**同构映射**, 记作 $G \cong H$.

2.2 平面魔方群

为方便文字描述及数学证明, 我们对平面魔方放置魔方块各个位置进行数字标号: 从左到右, 从上到下依次为各个位置标号 $1, 2, \dots, n^2$.为了行文方便, 我们还用坐标 (a, b) 表示第 a 行第 b 列这一位置.

记 $F_n = \{(x, y) | x, y \in \{1, 2, \dots, n\}\}$, $B_n = \{1, 2, \dots, n^2\}$, 构造一个从 F_n 到 B_n 的映射 φ :

$$\varphi(x, y) = n(x-1) + y, (x, y) \in F_n,$$

显然 φ 是双射. φ 将位置的坐标表示与数字表示一一对应.

对于每一个平面魔方, 我们使用两种表示方法:

1. **数字表法**: 用 n^2 元有序数组 $(x_1, x_2, \dots, x_{n^2})$ 表示, 其中 x_i 表示位置 i 所对应的数字;
2. **位置表法**: 用 n^2 元有序数组 $(y_1, y_2, \dots, y_{n^2})$ 表示, 其中 y_i 表示数字 i 所在的位置标号.

记 B_n 中所有元素的所有排列组成的集合为 C_n .数字表法和位置表法都是 B_n 中所有元素的一个排列.容易证明, 任意一个 n 阶平面魔方一一对应一种数字表法, 也一一对应一种位置表法.在接下去研究平面魔方群时我们会使用位置表法, 而在研究其 Cayley 图直径时我们将会使用数字表法.

仿照魔方的标记, 我们对 n 阶平面魔方的每一操作进行标记, V_i^j 表示对第 i 列所有数字向上移动 j 次, H_i^j 表示对第 i 行所有数字向左移动 j 次(如果为负则代表向下/右移动). V_i^j 与 H_i^j 均为一次操作.记 $X = \{V_i^j | i = 1, 2, \dots, n, j \in \mathbb{Z}\} \cup \{H_i^j | i = 1, 2, \dots, n, j \in \mathbb{Z}\}$.

定义 2.2.1 B_n 上的 n^2 元置换称为**变换**, 变换应用于平面魔方, 指对该平面魔方位置表法中的每一个坐标均应用该置换.

平面魔方的操作 V_i^j, H_i^j 均为变换.如在位置表法中在 $(2, 1)$ 上的数, 经操作 V_1^1 后到了位置 $(1, 1)$, 因此变换 V_1^1 将 $(2, 1)$ 映射到了 $(1, 1)$.以此类推, 对 X 中任一元素, 我们可以用 n -轮换记

作:

$$V_i^j = (\varphi(n, i) \varphi(n-1, i) \varphi(n-2, i) \cdots \varphi(1, i))^j,$$

或

$$H_i^j = (\varphi(i, n) \varphi(i, n-1) \varphi(i, n-2) \cdots \varphi(i, 1))^j.$$

变换的合成运算即置换乘法, 方向从左到右. 任意两个变换的合成同样是变换. 需要注意的是, 我们将变换效果相同的变换视为是等价的, 如 V_1^1 与 V_1^{n+1} 为同一个变换, $V_1^1 V_2^1$ 与 $V_2^1 V_1^1$ 为同一个变换. 记 G_n 为 n 阶平面魔方所有变换组成的集合, 则 G_n 中任何一个元素都是作用于 B_n 上的一个置换.

定理 2.2.2 G_n 以合成作为运算构成一个置换群, 称为平面魔方群.

证明 G_n 中任何一个元素可以表示成 X 中若干个元素的合成. 显然 $\forall a, b \in G_n, \exists c = ab \in G_n$.

(1) 对于 $\forall M_1, M_2, M_3 \in G_n$, 均有:

$$M_1 M_2 M_3 = (M_1 M_2) M_3 = M_1 (M_2 M_3).$$

(2) 恒等置换 e 把平面魔方 c 映射到它本身. 故单位元素 e 存在.

(3) 对于 $\forall M \in G_n$ 均可表示成 X 中若干个元素的合成 $M = M_1 M_2 \cdots M_m, M_i \in X, i \in \{1, 2, \cdots, m\}$, 则

$$M^{-1} = (M_m)^{-1} \cdots (M_2)^{-1} (M_1)^{-1}$$

而对于 X 中任意元素 V_i^j 或 H_i^j ,

$$(V_i^j)^{-1} = V_i^{-j} \in X, (H_i^j)^{-1} = H_i^{-j} \in X,$$

也就说明对于 $\forall M \in G_n, \exists M' = M^{-1} \in G_n$, 故逆元素存在.

根据定义 2.1.1 可知, 由平面魔方所有变换所生成的集合, 以合成作为运算构成一个群.

3. G_n 的阶

本章中我们将证明 $|G_n| = \begin{cases} n^2!/2, n \equiv 1(mod 2), \\ n^2!, n \equiv 0(mod 2). \end{cases}$

引理 3.1 $\forall n \geq 3, n \in \mathbb{Z}, \exists M_0 \in G_n, M_0 = (1\ 2\ 3)$.

证明 容易验证, $M_0 = V_1^{-1} H_1^1 V_1^1 H_1^1 V_1^{-1} H_1^{-2} V_1^1 \in G_n$, 且 $M_0 = (1\ 2\ 3)$. 证毕.

引理 3.2 $\forall n \geq 3, n \in \mathbb{Z}, \{a, b, c\} \subseteq B_n, \exists M_0 \in G_n, M_0 = (a\ b\ c)$.

证明 (1) 若 $a = \varphi(1, y)$, 则 $\exists M_1 = H_1^{y-1}$, 否则 $a = \varphi(x, y) (x \neq 1)$, 则 $\exists M_1 = H_1^{y-1} V_1^{x-1}$, 使得 $a^{M_1} = \varphi(1, 1) = 1$.

(2) 若 $b^{M_1} = \varphi(1, y)$, 则 $\exists M_2 = V_1^{-1} H_1^{y-2} V_1^1$, 否则 $b^{M_1} = \varphi(x, y) (x \neq 1)$, 则 $\exists M_2 = H_1^{y-2} V_1^{x-1}$, 使得 $b^{M_1 M_2} = \varphi(1, 2) = 2$, 且 $a^{M_1 M_2} = 1^{M_2} = 1$.

(3) 若 $c^{M_1 M_2} = \varphi(1, y)$, 则 $\exists M_3 = V_1^{-1} H_1^{y-3} V_1^1$, 否则 $c^{M_1 M_2} = \varphi(x, y) (x \neq 1)$, 则 $\exists M_3 = H_1^{y-3} V_1^{x-1}$, 使得 $c^{M_1 M_2 M_3} = \varphi(1, 3) = 3$, 且 $a^{M_1 M_2 M_3} = 1^{M_3} = 1, b^{M_1 M_2 M_3} = 2^{M_3} = 2$.

令 $M = M_1 M_2 M_3$, 则 $a^M = 1, b^M = 2, c^M = 3$. 由引理 3.1 知 $\exists M' = (1\ 2\ 3)$, 则考虑 $M_0 = M M' M^{-1}$. a, b, c 三个数经过变换 M 后, $a^M = a^{M M' M^{-1}} = 1^{M' M^{-1}} = 2^{M^{-1}} = b$. 同理, $b^{M M' M^{-1}} = c, c^{M M' M^{-1}} = a$. 而对于任意 a, b, c 以外的数 p , $p^M \neq 1, 2, 3$, 故 $p^{M M'} = p^M, p^{M_0} =$

$p^{MM'M^{-1}} = p^{MM^{-1}} = p$. 因此 $M_0 = (a \ b \ c)$. 证毕.

定理 3.3 $G_n = \begin{cases} A_{n^2}, n \equiv 1(\text{mod } 2), \\ S_{n^2}, n \equiv 0(\text{mod } 2). \end{cases}$

证明 因为 G_n 是作用在 $B_n = \{1, 2, \dots, n^2\}$ 上的置换群, 故 $G_n \leq S_{n^2}$.

1. 当 $n=2$ 时, $G_2 \leq S_4, H_1^1 = (1,2), V_1^1 = (1,3), H_1^1 V_2^1 H_1^1 = (1,4), H_1^1 V_1^1 H_1^1 = (2,3), V_2^1 = (2,4), H_2^1 = (3,4)$. 由定理 2.1.7 得, 以上 6 组置换可以生成全体 4 元置换. 因此 $G_2 = S_4 = S_{2^2}$.

2. 当 $n \geq 3$ 时, 由引理 3.2 知作用于 B_n 上的任意 3-轮换均属于 G_n , 而根据定理 2.1.12, 一切 3-轮换可以生成 A_{n^2} . 因此 $G_n \geq A_{n^2}$.

(1) 当 n 为奇数时, G_n 由长度为 n 的偶置换 $H_1^1, H_2^1, \dots, H_n^1, V_1^1, V_2^1, \dots, V_n^1$ 生成, 根据定理 2.1.9 任意两个偶置换之积还是偶置换, 故平面魔方群 G_n 中不可能存在奇置换, 因此 $G_n \leq A_{n^2}$. 故 $G_n = A_{n^2}$.

(2) 当 n 为偶数时, 因为奇置换 $H_1^1 \in G_n$, 因此 $G_n \neq A_{n^2}$, 故 $G_n > A_{n^2}, |G_n| > |A_{n^2}| = n^2!/2$. 又 $G_n \leq S_{n^2}$, 由定理 2.1.11 知 $|G_n|$ 整除 $|S_{n^2}| = n^2!$, 故只能有 $|G_n| = n^2!$, 因此 $G_n = S_{n^2}$.

综上所述, 命题得证.

定理 3.4 $|G_n| = \begin{cases} n^2!/2, n \equiv 1(\text{mod } 2), \\ n^2!, n \equiv 0(\text{mod } 2). \end{cases}$

证明 结合定理 2.1.5 与定理 2.1.10 以及定理 3.3 可知结果成立.

4. Cayley 图直径

本章将对平面魔方群 Cayley 图直径问题进行研究. 本节对部分问题的处理参考了文献 [4].

4.1 Cayley 图的相关定义

定义 4.1.1 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 4.1.2 顶点 v 的度数是与 v 相连接的边数, 记作 $\deg(v)$.

定义 4.1.3 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:

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

定义 4.1.4 $v, w \in V$, 称 v 和 w 是连通的, 如果从 v 到 w 存在一条路径. 图 (V, E) 是连通的, 如果任意两点都是连通的.

定义 4.1.5 $v, w \in V$, 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 $\text{diam}((V, E)) = \max\{d(v, w) | v, w \in V\}$.

定义 4.1.6 $G = \langle g_1, g_2, \dots, g_n \rangle$ 是由集合 $X = \{g_1, g_2, \dots, g_n\}$ 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 $y = g_i x$ 或者 $x = g_i y, i = 1, 2, \dots, n$.

定理 4.1.7 $\Gamma_G = (V, E)$ 表示关于置换群 $G = \langle g_1, g_2, \dots, g_n \rangle$ 的 Cayley 图. 则 $\forall v \in V, \deg(v) = |\{g_1, g_2, \dots, g_n\} \cup \{g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}\}|$.

证明 [3]P117.

根据定理 4.1.7, 平面魔方群 $G_n = \langle X \rangle$ 的 Cayley 图中任意顶点的度数为 $|X| = 2n(n-1)$.

定理 4.1.8 设 $\Gamma_G = (V, E)$ 是平面魔方群 G_n 关于 X 的 Cayley 图, 则 $\forall v, w \in V, \exists u \in V$, 使得 $d(v, w) = d(e, u)$, 其中 e 是单位元素.

证明 不妨设 $d(v, w) = x$, 则 $vg_1g_2 \cdots g_x = w, g_i \in X, i = 1, 2, \dots, x$. 取 $u = v^{-1}w$ 即可.

推论 4.1.9 $\text{diam}(\Gamma_G) = \max\{d(e, v), v \in V\}$.

证明 根据定义 4.1.5 以及上述定理显然.

由推论 4.1.9, 平面魔方群 Cayley 图的直径等于离单位元最远的点到单位元的距离. 用 $G_n(i)$ 表示平面魔方群 G_n 中到单位元距离为 i 的元素集合, 即

$$G_n(i) = \{v \in G_n | d(e, v) = i\}.$$

根据集合理论, 定理 4.1.10, 定理 4.1.11, 定理 4.1.12 是显然成立的.

定理 4.1.10 $G_n(i) \cap G_n(j) = \emptyset, i \neq j$.

定理 4.1.11 $G_n = \bigcup_{i=0}^{\infty} G_n(i)$.

定理 4.1.12 $|G_n| = \sum_{i=0}^{\infty} |G_n(i)|$.

定理 4.1.13 $\forall M \in X, v \in G_n(i), w = vM$, 则 $w \in G_n(i-1) \cup G_n(i) \cup G_n(i+1)$.

证明 因为 $w = vM, v = wM^{-1}$, 故 $|d(e, w) - d(e, v)| \leq 1$, 即 $d(e, v) - 1 \leq d(e, w) \leq d(e, v) + 1$. 因此 $w \in G_n(i-1) \cup G_n(i) \cup G_n(i+1)$. 证毕.

由此我们可以将问题等价于找到 i , 使 $|G_n(i)| \neq 0$ 且 $|G_n(i+1)| = 0$, 则 i 就是 G_n 的 Cayley 图直径.

4.2 n 阶平面魔方群 Cayley 图直径机解算法

4.2.1 算法基本逻辑

构造一个映射 $f: G_n \rightarrow C_n, f(v) = v(c)$, 其中 c 表示初始状态的平面魔方的数字表法, $v(c)$ 表示 v 应用于初始状态平面魔方生成的新的平面魔方的数字表法. 显然 f 是双射且 $f(e) = c$.

记 $P_n = \{v(c) | v \in G_n\}$, 则 P_n 包含了 n 阶所有可能出现的平面魔方的数字表法. 定义 " \cdot " 为 P_n 上的一个二元运算, 满足

$$p \cdot q = (vw)(c), p, q \in P_n,$$

其中 $p = v(c), q = w(c)$. 显然 P_n 对于 " \cdot " 构成一个群.

定理 4.2.1 $P_n \cong G_n$.

证明 因为

$$f(v)f(w) = v(c)w(c) = (vw)(c) = f(vw), \forall v, w \in G_n,$$

又 f 是双射, 由定义 2.1.13 知 $P_n \cong G_n$. 证毕.

令 P_n 的生成元集合为 $\langle Y \rangle$, $Y = \{f(v) | v \in X\}$ 即 X 在映射 f 下的象. 易证明以下定理:

定理 4.2.2 P_n 与 G_n 的 Cayley 图同构.

记

$$P_n(i) = \{f(v) | v \in G_n(i)\},$$

则 $P_n(i)$ 为 $G_n(i)$ 在映射 f 下的象. 显然有 $|G_n(i)| = |P_n(i)|$.

由同构易知 $P_n(i) = \{p \in P_n | d(c, p) = i\}$, 表示 P_n 中到 c 距离为 i 的元素集合.

根据同构, 我们还可以得到以下定理:

定理 4.2.3 $P_n(i) \cap P_n(j) = \emptyset, i \neq j$.

定理 4.2.4 $P_n = \bigcup_{i=0}^{\infty} P_n(i)$.

定理 4.2.5 $|P_n| = \bigcup_{i=0}^{\infty} |P_n(i)|$.

定理 4.2.6 $\forall M \in X, v \in P_n(i), w = vM \in P_n(i-1) \cup P_n(i) \cup P_n(i+1)$.

定理 4.2.7 $G_n = \langle X \rangle$ 与 $P_n = \langle Y \rangle$ 的 Cayley 图直径相同.

我们用枚举法穷尽所有可能的排序即可得出平面魔方群 Cayley 图直径. 算法流程如下:

1. $i = 0$,
2. $P_n(0) = \{c\}$,
3. 取出 $P_n(i)$ 中一个元素 p ,
4. 对 p 右乘 Y 中所有元素, 得到 $n(n-1)$ 个新的元素 $q_1, q_2, \dots, q_{n(n-1)}$,
5. 对 $q_1, q_2, \dots, q_{n(n-1)}$ 中每一个元素 q , 如果 $q \notin P_n(i-1) \cup P_n(i) \cup P_n(i+1)$, 则将其加入 $P_n(i+1)$ 中,
6. 重复 3, 4, 5 步, 直至遍历 $P_n(i)$ 中所有元素,
7. 如果 $|P_n(i)| \neq 0, i = i+1$ 并跳到第 3 步,
8. i 就是 P_n 的 Cayley 图直径.
9. 由定理 4.2.7 知 i 就是 G_n 的 Cayley 图直径.

4.2.2 $n=3$ 时程序运行结果

由定理 3.5 知 $|G_3| = 3^2!/2 = 181440$, 在家用计算机处理能力内, 我们编写程序来对 G_3 对应的 Cayley 图直径进行求解. 采用 Python 2.7 编程, 最终可以输出如下结果(源码见附录 8.1):

```
depth: 1
the number of all states: 13
depth: 2
the number of all states: 109
depth: 3
the number of all states: 845
depth: 4
the number of all states: 6053
depth: 5
```

the number of all states: 34727

depth: 6

the number of all states: 124224

depth: 7

the number of all states: 178965

depth: 8

the number of all states: 181440

depth: 9

the number of all states: 181440

The God's number of two-dimension magic cube 3*3 is 8.

故 G_3 的 Cayley 图直径为 8.

通过程序我们还可以得到 $\sum_{k=0}^i G_3(k)$ 的值, 列表如下:

表 1 三阶平面魔方 Cayley 图直径计算结果

i	$\sum_{k=0}^i G_3(k)$	$G_3(i)$
0	1	1
1	13	12
2	109	96
3	845	736
4	6053	5208
5	34727	28674
6	124224	89497
7	178965	54741
8	181440	2475

4.3 n 阶平面魔方群 Cayley 图直径下界估计

在实际运用算法的过程中, 我们发现 4 阶及以上的平面魔方总情况数随阶数增长呈爆炸式增长, 运用一般计算机计算几乎不可能, 因此我们采用数学方法估计高阶平面魔方群 Cayley 图直径的下界.

4.3.1 理论分析

我们通过构造集合的方法来计算高阶平面魔方群 Cayley 图的下界. 构造集合 $\Omega_n(i) = \{g_1 g_2 \cdots g_i | g_k \in X, k = 1, 2, \dots\}$. 因为 $\Omega_n(i)$ 中可能存在两种不同的排列对应同一种变换, 因此有以下定理:

定理 4.3.1 $\cup_{k=0}^i \Omega_n(k) = \cup_{k=0}^i G_n(k)$.

定理 4.3.2 $|\Omega_n(k)| \geq |G_n(k)|$.

定理 4.3.3 $\sum_{k=0}^i |\Omega_n(k)| \geq \sum_{k=0}^i |G_n(k)|$.

定理 4.3.4 记 d 为 G_n 的 Cayley 图直径, 若 $\sum_{k=0}^i |\Omega_n(k)| < |G_n|$, 则 $d > i$.

证明 反证法. 假设 $d \leq i$. 因为 $|G_n| = \sum_{k=0}^d |G_n(k)|$, 故有 $\sum_{k=0}^d |G_n(k)| > \sum_{k=0}^i |\Omega_n(k)| \geq \sum_{k=0}^i |G_n(k)|$, 即 $\sum_{k=0}^d |G_n(k)| > \sum_{k=0}^i |G_n(k)|$. 这与 $d \leq i$ 矛盾. 故 $d > i$. 证毕.

定理 4.3.4 给出了一种确定下界的办法. 如果我们在 $\Omega_n(i+1)$ 中剔除在 $\cup_{k=0}^i \Omega_n(k)$ 中出现过的元素, 不难发现上述定理仍然成立.

下界的紧密程度就取决于是否能尽可能多的剔除重复元素. 从理论上来说, 如果能把所有重复的元素全部剔除, 得到的就是平面魔方群的 Cayley 图直径.

4.3.2 剔除重复

本节中操作的上标按模 n 意义下理解, V_i, H_i 分别表示 $V_i^j, H_i^j (1 \leq j < n)$. 观察以下事实:

1. $V_i^\alpha V_i^\beta = V_i^{\alpha+\beta}, H_i^\alpha H_i^\beta = H_i^{\alpha+\beta},$
2. $V_i^\alpha V_j^\beta = V_j^\beta V_i^\alpha, H_i^\alpha H_j^\beta = H_j^\beta H_i^\alpha,$

事实上这是两组 G_n 的生成元关系, 通过这两组关系我们可以剔除 $\Omega_n(k)$ 中一部分的重复. 在本节中我们用操作的排列表示某一变换. 特别地, 恒等变换记为空排列 Φ .

定义 4.3.5 称一段操作的排列是**正序**的, 如果其中任何相邻的 $V_i V_j$ 或 $H_i H_j$ 均满足 $i < j$.

定理 4.3.6 任意的操作排列均等价于一个的正序操作排列, 且这个正序操作排列的长度不超过原操作排列.

证明 如果该排列中存在相邻的 $V_i V_j$ 或 $H_i H_j$, 运用事实 1 可将其合并; 如果存在相邻的 $V_i V_j$ 或 $H_i H_j$ 满足 $i > j$, 则运用事实 2 将其交换位置即可. 经过重复操作以后, 最终可以得到一个等价的正序操作排列, 且这个正序操作排列的长度不超过原操作排列. 证毕.

由定理 4.3.6 可知, 我们可以通过筛选正序操作排列来达到剔除重复的目的. 记所有正序操作排列组成的集合为 Δ , 重新定义 $\Omega_n(i) = \{g_1 g_2 \cdots g_i \in \Delta | g_k \in X, k = 1, 2, \dots\}$. 特别地, 当 $i=0$ 时, $\Omega_n(0) = \{\Phi\}$.

为了计算正序操作排列的数量, 我们将 $\Omega_n(i) (i > 0)$ 根据最后一次操作划分为若干个集合: $v_n^k(i)$ 表示 n 阶平面魔方中长度为 i , 且最后一次操作为 $V_k (1 \leq k \leq n)$ 的正序操作排列集合; $h_n^k(i)$ 表示 n 阶平面魔方中长度为 i , 且最后一次操作为 $H_k (1 \leq k \leq n)$ 的正序操作排列集合.

定理 4.3.7 $|v_n^k(i)| = |h_n^k(i)|$.

证明 将 $v_n^k(i)$ 中每个正序操作排列的所有 V 用 H 代替, 所有 H 用 V 代替, 得到的操作排列仍然是正序操作排列, 且最后一次操作为 H_k , 故该操作属于 $h_n^k(i)$; 同理, 将 $h_n^k(i)$ 中每个正序操作排列的所有 V 用 H 代替, 所有 H 用 V 代替, 得到的操作排列仍然是正序操作排列, 且最后一次操作为 V_k , 故该操作属于 $v_n^k(i)$. 因此可以建立一个 $v_n^k(i)$ 到 $h_n^k(i)$ 的一一对应, 故 $|v_n^k(i)| = |h_n^k(i)|$. 证毕.

定理 4.3.8

$$\forall i \geq 2, |v_n^k(i)| = (n-1) \left(\sum_{j=1}^{k-1} |v_n^j(i-1)| + \sum_{j=1}^n |h_n^j(i-1)| \right).$$

证明 对于 $\forall i \geq 2, v_n^k(i)$ 中的每一个正序操作排列 M , 我们分别考虑它的最后一项操作与前 $i-1$ 项操作. 由定义知 $v_n^k(i)$ 中的正序操作排列最后一项操作为 V_k , 共 $n-1$ 种可能; 它的前 $i-1$ 项操作为长度为 $i-1$ 的正序操作排列, 若其最后一次操作为 $V_j (k \leq j < n)$, 则 M 的最后两次操作为 $V_j V_k$ 且 $k \leq j$, 这与正序操作排列的定义矛盾. 故最后一次操作只能是 $V_j (1 \leq j < k)$ 或 $H_j (1 \leq j \leq n)$, 满足这一条件的长度为 $i-1$ 的正序操作排列共 $\sum_{j=1}^{k-1} |v_n^j(i-1)| + \sum_{j=1}^n |h_n^j(i-1)|$ 组. 由乘法原理得, $|v_n^k(i)| = (n-1)(\sum_{j=1}^{k-1} |v_n^j(i-1)| + \sum_{j=1}^n |h_n^j(i-1)|)$. 证毕.

定理 4.3.9

$$\forall i \geq 2, |v_n^k(i)| = (n-1) \left(\sum_{j=1}^{k-1} |v_n^j(i-1)| + \sum_{j=1}^n |v_n^j(i-1)| \right).$$

证明 由定理 4.3.7 和定理 4.3.8 可得.

又因为 $v_n^j(i), h_n^j(i) (j = 1, 2, \dots, n)$ 是 $\Omega_n(i)$ 的划分, 因此有以下定理:

定理 4.3.10

$$|\Omega_n(i)| = \sum_{j=1}^n |v_n^j(i)| + \sum_{j=1}^n |h_n^j(i)| = 2 \sum_{j=1}^n |v_n^j(i)|.$$

结合初始值 $|v_n^1(1)| = |v_n^2(1)| = \dots = |v_n^n(1)| = n-1$ 及定理 4.3.9, 定理 4.3.10, 迭代计算即可解得 $|\Omega_n(i)|$ 的值, 从而可以通过定理 4.3.4 计算出平面魔方群 Cayley 图直径下界.

以四阶平面魔方为例, 由定理 4.3.9 可得递推关系

$$\begin{aligned} |v_4^1(i)| &= 3(|v_4^1(i-1)| + |v_4^2(i-1)| + |v_4^3(i-1)| + |v_4^4(i-1)|), \\ |v_4^2(i)| &= 3(2|v_4^1(i-1)| + |v_4^2(i-1)| + |v_4^3(i-1)| + |v_4^4(i-1)|), \\ |v_4^3(i)| &= 3(2|v_4^1(i-1)| + 2|v_4^2(i-1)| + |v_4^3(i-1)| + |v_4^4(i-1)|), \\ |v_4^4(i)| &= 3(2|v_4^1(i-1)| + 2|v_4^2(i-1)| + 2|v_4^3(i-1)| + |v_4^4(i-1)|), \end{aligned}$$

及初始关系

$$|v_4^1(1)| = |v_4^2(1)| = |v_4^3(1)| = |v_4^4(1)| = 3$$

可算得下表:

表 2 四阶平面魔方计算数值表

i	$v_4^1(i)$	$v_4^2(i)$	$v_4^3(i)$	$v_4^4(i)$	$ \Omega_n(i) $	$\sum_{k=0}^i \Omega_n(k) $
0	/	/	/	/	1	1
1	3	3	3	3	24	25
2	36	45	54	63	396	421
3	594	702	837	999	6264	6685
4	9396	11178	13284	15795	99306	105991
5	148959	177147	210681	250533	1574640	1680631
6	2361960	2808837	3340278	3972321	24966792	26647423
7	37450188	44536068	52962579	62983413	395864496	422511919
8	593796744	706147308	839755512	998643249	6276685626	6699197545
9	9415028439	11196418671	13314860595	15834127131	99520869672	106220067217
10	149281304508	177526389825	211115645838	251060227623	1577967135588	1684187202805
11	2366950703382	2814794616906	3347373786381	3980720723895	25019679661128	26703866863933

又 $|G_4| = 16! = 20922789888000$, 而 $\sum_{k=0}^{10} |\Omega_n(k)| < |G_4| \leq \sum_{k=0}^{11} |\Omega_n(k)|$, 由定理 4.3.4 知四阶平面魔方 Cayley 图直径至少为 11.

根据上文论述利用 *Python 2.7* 编程(源码见附录 8.2), 以 2-8 阶为例进行计算得到结果如下表:

表 3 不同阶数平面魔方估计下界与实际值对比

阶数	下界	实际
2	3	4
3	6	8
4	11	未知
5	18	未知
6	26	未知
7	36	未知
8	48	未知

5.模型推广

5.1 基本介绍

将平面魔方的形状从正方形拓展到 m 列 n 行的矩形, 并保持原有的规则, 我们可以得到 $m \times n$ 阶异形平面魔方(我们仅研究 $m > n \geq 2$ 时的情况). 记 $G_{m \times n}$ 为 $m \times n$ 阶异形平面魔方全体变换组成的集合, 同平面魔方有以下定理:

定理 5.1 $G_{m \times n}$ 以合成作为运算构成一个置换群, 称为异形平面魔方群.

5.2 $G_{m \times n}$ 的阶

本节中我们将证明 $|G_{m \times n}| = \begin{cases} (mn)^2!/2, mn \equiv 1(mod 2), \\ (mn)^2!, mn \equiv 0(mod 2). \end{cases}$

同第三章中的构造方法, 我们也有以下定理:

引理 5.2.1 $\forall m \geq 3, m \in \mathbb{Z}, \exists M_0 \in G_{m \times n}, M_0 = (1\ 2\ 3)$.

证明 同第三章.

引理 5.2.2 $\forall m \geq 3, m \in \mathbb{Z}, \{a, b, c\} \subseteq \{1, 2, \dots, mn\}, \exists M_0 \in G_{m \times n}, M_0 = (a\ b\ c)$.

证明 同第三章.

定理 5.2.3 $G_{m \times n} = \begin{cases} A_{mn}, mn \equiv 1(mod 2), \\ S_{mn}, mn \equiv 0(mod 2). \end{cases}$

证明 因为 $G_{m \times n}$ 是作用在 $\{1, 2, \dots, mn\}$ 上的置换群, 故 $G_{m \times n} \leq S_{mn}$. 由引理 3.2 知作用于 $\{1, 2, \dots, mn\}$ 上的任意 3-轮换均属于 $G_{m \times n}$, 而根据定理 2.1.12, 一切 3-轮换可以生成 A_{mn} .

因此 $G_{m \times n} \geq A_{mn}$.

(1) 当 mn 均为奇数时, G_n 由长度为 m 的偶置换 $H_1^1, H_2^1, \dots, H_n^1$ 与长度为 n 的偶置换 $V_1^1, V_2^1, \dots, V_m^1$ 生成, 根据定理 2.1.9 任意两个偶置换之积还是偶置换, 故 $G_{m \times n}$ 中不可能存在奇置换, 因此 $G_{m \times n} \leq A_{mn}$. 故 $G_{m \times n} = A_{mn}$.

(2) 当 mn 有一者为偶数时, H_1^1 与 V_1^1 中必有一者为奇置换, 因此 $G_{m \times n} \neq A_{mn}$, 故 $G_{m \times n} > A_{mn}$, $|G_{m \times n}| > |A_{mn}| = (mn)!/2$. 又 $G_{m \times n} \leq S_{mn}$, 由定理 2.1.11 知 $|G_{m \times n}|$ 整除 $|S_{mn}| = (mn)!$, 故只能有 $|G_{m \times n}| = (mn)!$, 因此 $G_{m \times n} = S_{mn}$. 证毕.

$$\text{定理 5.2.4} \quad |G_{m \times n}| = \begin{cases} (mn)^2!/2, & mn \equiv 1 \pmod{2}, \\ (mn)^2!, & mn \equiv 0 \pmod{2}. \end{cases}$$

证明 结合定理 2.1.5 与定理 2.1.10 以及定理 5.2.3 可知结果成立.

5.3 $G_{m \times n}$ 的 Cayley 图直径

$G_{m \times n}$ 的 Cayley 图直径计算思路与 G_n 完全相同, 在此不再赘述. 对源码稍加改进后, 我们可以计算异形平面魔方的 Cayley 图直径(源码见附录 8.1). 计算结果见下表:

表 4 部分异形平面魔方群的 Cayley 图直径

	1 列	2 列	3 列	4 列	5 列
1 行	0	1	1	1	1
2 行	1	4	7	8	12
3 行	1	7	8	/	/
4 行	1	8	/	/	/
5 行	1	12	/	/	/

5.4 $G_{m \times n}$ 的 Cayley 图直径下界估计

我们用 $v_{m \times n}^k(i)$ 表示 $m \times n$ 阶平面魔方中长度为 i , 且最后一次操作为 V_k ($1 \leq k \leq n$) 的正序操作排列集合; $h_{m \times n}^k(i)$ 表示 $m \times n$ 阶平面魔方中长度为 i , 且最后一次操作为 H_k ($1 \leq k \leq m$) 的正序操作排列集合. 与第四章中不同的是, $|v_{m \times n}^k(i)|$ 与 $|h_{m \times n}^k(i)|$ 不再相等. 通过分别讨论, 我们可以得到以下结论:

$$\forall i \geq 2, |v_{m \times n}^k(i)| = (n-1) \left(\sum_{j=1}^{k-1} |v_{m \times n}^j(i-1)| + \sum_{j=1}^n |h_{m \times n}^j(i-1)| \right),$$

$$\forall i \geq 2, |h_{m \times n}^k(i)| = (m-1) \left(\sum_{j=1}^{k-1} |h_{m \times n}^j(i-1)| + \sum_{j=1}^m |v_{m \times n}^j(i-1)| \right),$$

$$|\Omega_{m \times n}(i)| = \sum_{j=1}^n |v_{m \times n}^j(i)| + \sum_{j=1}^m |h_{m \times n}^j(i)|,$$

$$|v_{m \times n}^1(1)| = |v_{m \times n}^2(1)| = \dots = |v_{m \times n}^m(1)| = n-1,$$

$$|h_{m \times n}^1(1)| = |h_{m \times n}^2(1)| = \dots = |h_{m \times n}^n(1)| = m-1.$$

由此即可推得结论.

对源码稍加改进后, 我们可以计算异形平面魔方的 Cayley 图直径下界(源码见附录 8.2). 部分计算结果见下表:

表 5 部分异形平面魔方群的 Cayley 图直径下界

	2 列	3 列	4 列	5 列	6 列	7 列	8 列
2 行	3	4	6	7	8	9	10
3 行	4	6	9	10	13	14	16
4 行	6	9	11	14	17	20	23
5 行	7	10	14	18	22	25	29
6 行	8	13	17	22	26	31	35
7 行	9	14	20	25	31	36	41
8 行	10	16	23	29	35	41	48

6.未解决的问题

问题 6.1 高阶平面魔方群 Cayley 图直径的确切值.

问题 6.2 异形平面魔方群 Cayley 图直径的确切值. 在异形平面魔方群的 Cayley 图直径表(表 4)中, 是否存在某种规律?

问题 6.3 如何提高平面魔方群 Cayley 图直径的下界?

问题 6.4 如何计算平面魔方群 Cayley 图直径的上界?

7.参考文献

- [1]王萼芳.有限群论基础[M].清华大学出版社, 2012.
- [2]冯克勤.近世代数引论[M].中国科学技术大学出版社, 2009.
- [3]David Joyner.Adventures in Group Theory.The Johns Hopkins University Press, 2002.
- [4]朱磊.群论在魔方中的运用[D]苏州: 苏州大学数学系, 2008.

8.附录

8.1 $m \times n$ 阶平面魔方群 Cayley 图直径计算源码

```
def rotate(lst,n):
    l=len(lst)
    n=n%l
```

```

    return lst[-n:]+lst[:n]
def move(pm,x,y,z):
    rs=list(pm[:])
    if y==0:
        temp=rotate(rs[n*(x-1):n*x:1],z)
        rs[n*(x-1):n*x:1]=temp
    else:
        temp=rotate(rs[x-1::n],z)
        rs[x-1::n]=temp
    return tuple(rs)
def god():
    global depth
    global line
    global astt
    global ct
    if len(line[depth])==0:
        depth+=1
        print "depth:"+str(depth)
        print "the number of all states:"+str(ct)
        if len(line[depth])==0:
            return False
        line.append({ })
        astt[(depth-1)%3]={ }
    j=line[depth].popitem()[0]
    y=0
    for x in range(1,m+1):
        for z in range(1,n):
            s=move(j,x,y,z)
            if ((s in astt[0]) or (s in astt[1]) or (s in astt[2]))==False:
                line[depth+1][s]=astt[(depth-1)%3][s]=0
                ct+=1
        y=1
    for x in range(1,n+1):
        for z in range(1,m):
            s=move(j,x,y,z)
            if ((s in astt[0]) or (s in astt[1]) or (s in astt[2]))==False:
                line[depth+1][s]=astt[(depth-1)%3][s]=0
                ct+=1
    return True
n=input("rows?")
m=input("columns?")
depth=0
ct=1
line=[{ },{ }]

```

```

astt=[[],[],[]]
line[0][tuple(range(0,n*m))]=[]
astt[1][tuple(range(0,n*m))]=[]
while god():
    pass
print "The God's number of two-dimension magic cube "+str(n)+"*"+str(m)+" is "+str(depth-1)+". "

```

8.2 $m \times n$ 阶平面魔方群 Cayley 图直径下界计算源码

```

def factorial(num):
    r=1
    for i in range(1,num+1):
        r*=i
    return r
m=input('rows?')
n=input('columns?')
v=[[n-1]*m]
h=[[m-1]*n]
d=1
s=m*(n-1)+n*(m-1)+1
print s
a=factorial(m*n)/(m*n%2+1)
while s<a:
    v.append([])
    h.append([])
    for i in range(0,n):
        temp=(n-1)*(sum(v[d-1][0:i])+sum(h[d-1]))
        v[d].append(temp)
        s+=temp
    for i in range(0,m):
        temp=(m-1)*(sum(h[d-1][0:i])+sum(v[d-1]))
        h[d].append(temp)
        s+=temp
    print s
    d+=1
print "The diameter of Cayley Graph of SLIDING-MATRIX "+str(m)+"*"+str(n)+" is greater than or equal to "+str(d)+". "

```