几何与对称

李思

清华大学

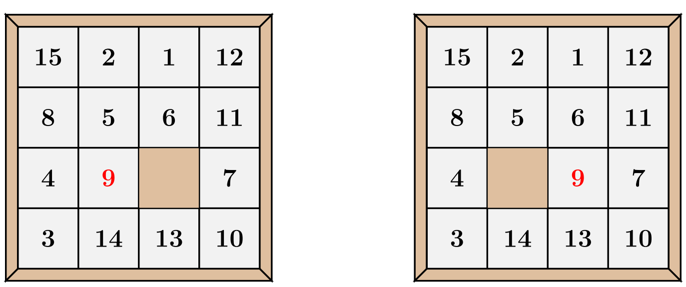
摘要

本文来源于作者 2018 年在清华大学为首届丘成桐英才班开设的教改课程《几何与对称》的部分内容 [1]，通过几何直观和棋盘游戏实例来解释"群"这个重要数学概念的一些基本思想和应用方法。

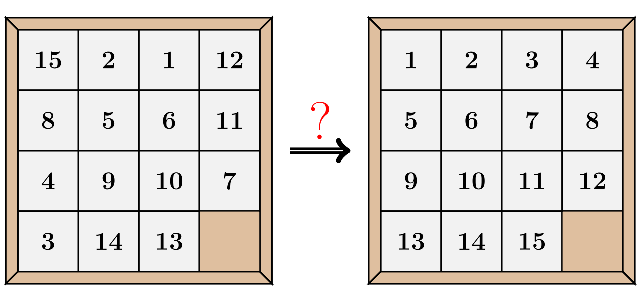
1 引言

大学数学系里通常有一门基础课称为"抽象代数"，主要内容是群、环、域等这些现代代数学中的基本概念和方法。读书的时候感觉这些概念初学起来的确很"抽象"，就像这门课的名称一样。随着不断学习和积累，逐渐发现这些概念其实非常直观，朋友们也经常笑谈到这门课应该被教为"非抽象代数"。本文通过一个具体的数字游戏来聊聊非抽象代数。

我们探讨的这个经典例子称为数字推盘问题，玩法类似于华容道。考虑一个 4×4 的方形棋盘以及标记 $1-15$ 的数字方块。游戏者每次移动一个数字方块到相邻空白格，例如



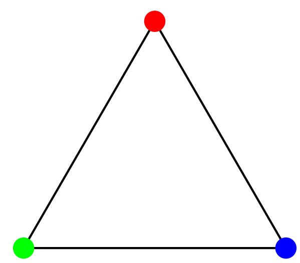
问题: 是否可以由下图左还原到下图右的原始状态?



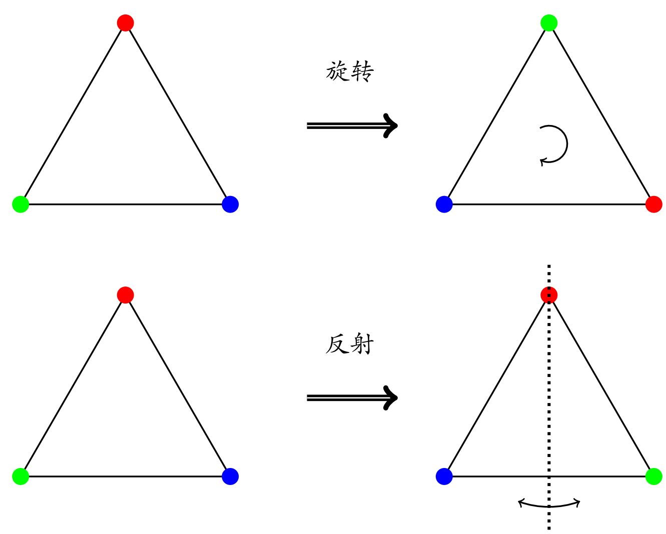
我们将围绕如何解决这个经典问题来解释"群"这个基本数学概念。

2 几何变换与对称性

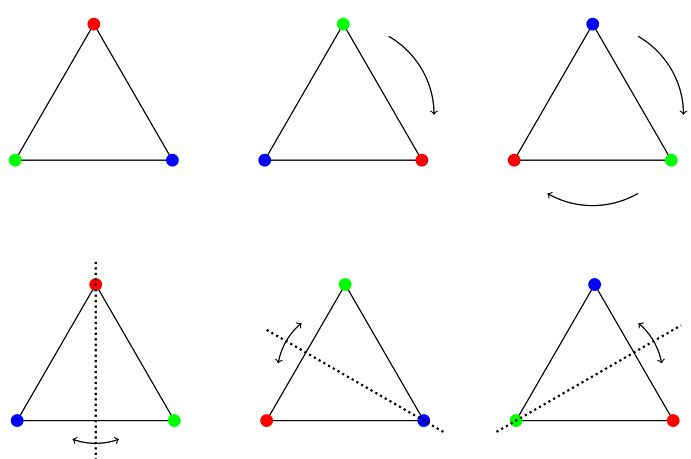
具有几何对称的物体通常都有强烈美感和丰富结构,“群”即刻画如此。考虑等边三角形



这个图形具有很强的几何对称性：我们可以通过如下的几何变换把三角形变换到它自己

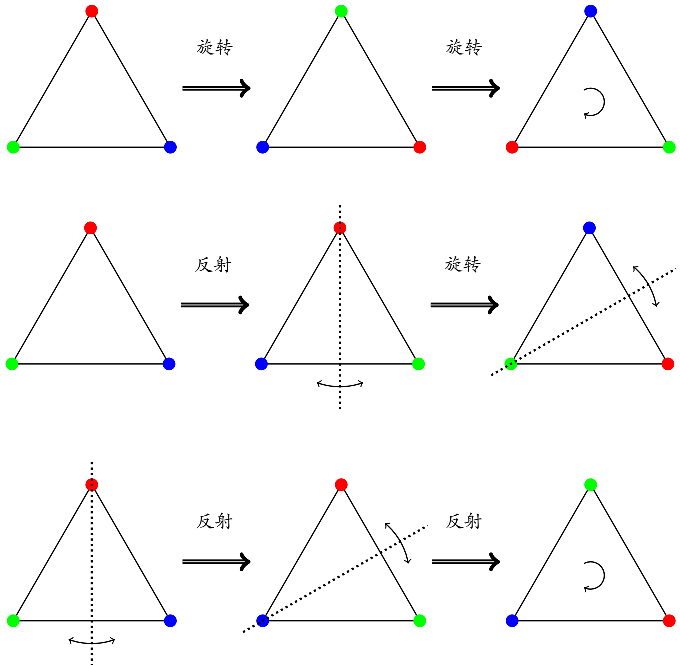


我们总共得到如下 6 个对称变换

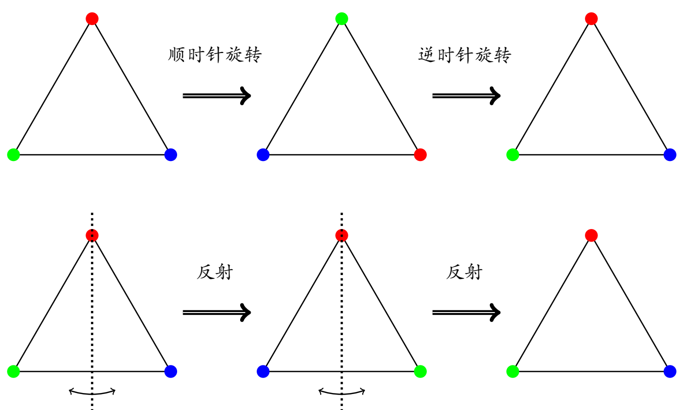


观察到这些几何变换满足如下两个重要性质：

1. 对称变换的复合还是对称变换



2. 对称变换可以由逆变换来还原



3 群的概念

几何对称变换的这些性质构成的数学对象称为“群”。

抽象定义而言，一个群由一个集合 G 和满足结合律的二元运算

$$\bullet : G \times G \to G$$

（称为群 G 中的乘积）组成，满足

- 单位元：存在单位元1_G，使得：$1_G \bullet g = g \bullet 1_G = g$
- 可逆性：对任一元素 g，存在逆元g^{-1} 使得：$g \bullet g^{-1} = g^{-1} \bullet g = 1_G$

例如：

1. $G = \mathbb{R} - \{0\}$，$\bullet$ 为实数的乘法 $a \bullet b := ab$

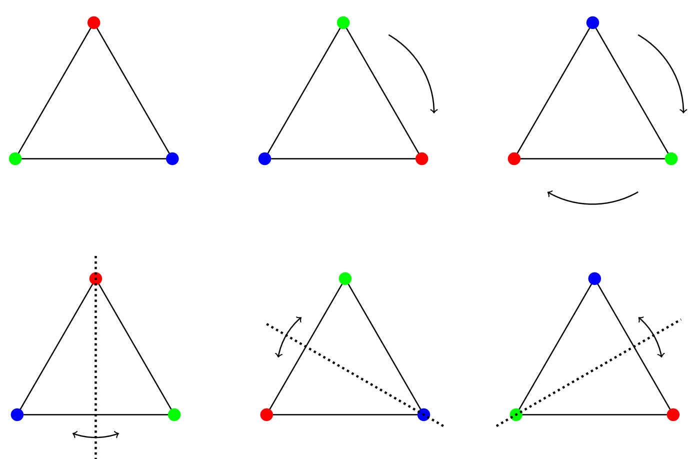
$$\text{单位元} = 1, \quad a \text{ 的逆元是 } \frac{1}{a}$$

2. $G = \mathbb{Z}$，$\bullet$ 为整数的加法 $m \bullet n := m + n$

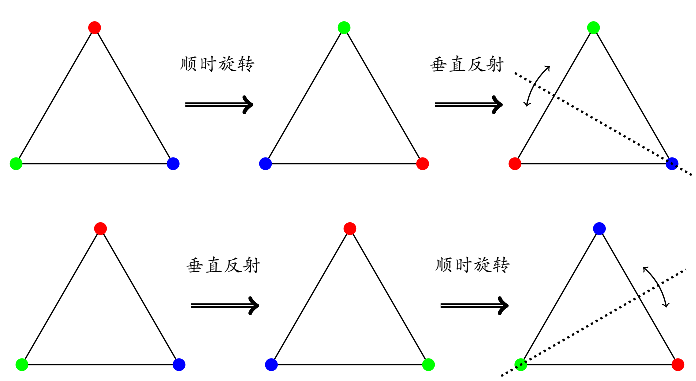
$$\text{单位元} = 0, \quad m \text{ 的逆元是 } -m$$

上述例子中 $\bullet$ 是交换的，即满足：$a \bullet b = b \bullet a$。乘积满足交换性质的群称为阿贝尔群。

例如：如下 6 个几何变换组合成一个群（称为二面体群D_3）



D_3 是非阿贝尔群：旋转和反射不交换！



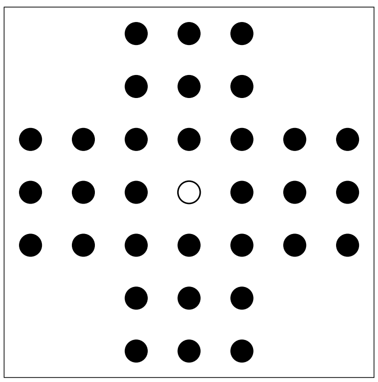
例如：Klein 四元数群是由四个元素 $K = \{1, a, b, c\}$ 组成的阿贝尔群，1 是单位元。其乘法结构为

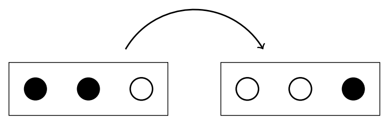
$$\begin{aligned} &a \bullet b = b \bullet a = c \qquad && b \bullet c = c \bullet b = a \qquad && c \bullet a = a \bullet c = b \\ &a^2 = 1 && b^2 = 1 && c^2 = 1 \end{aligned}$$

特别的，我们有 $a \bullet b \bullet c = 1$。

4 一个古老的游戏 (Peg Solitaire)

群的结构表现为变换。在实际运用中，一个重要的思想是在一系列丰富的变换中找到不变的对象。作为一个例子，我们考虑一个古老的游戏：

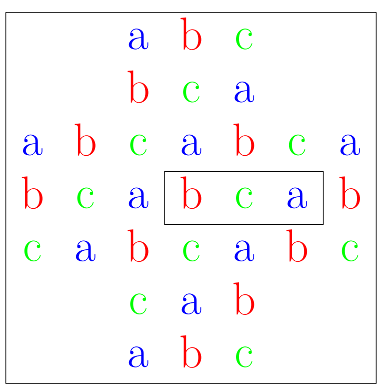




游戏规则：每次把一个黑子隔着相邻(水平或者垂直）的另一个黑子跳到空白处，同时移除被跳过的黑子。如上图。

问题：是否可以使得棋盘上最后只剩下一个黑子？如果可以，这个黑子落在哪里？

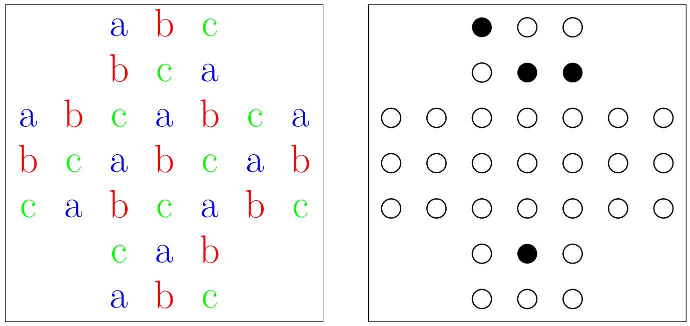
通过实践很容易发现第一问的答案是肯定的，我们用群论方法来分析第二问。把 Klein 四元数如下标记到棋盘中



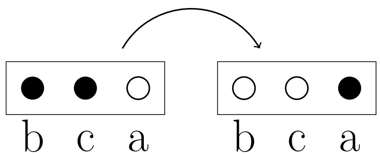
这个标记方法使得直线上任意三个相邻元素的乘积都是单位元 1。

设 C 是棋盘上的一个黑子分布。定义 C 的权为

$$[C] = \text{所有的黑子位置上的 Klein 四元数相乘}$$



上图右的权 $=acaa=b$



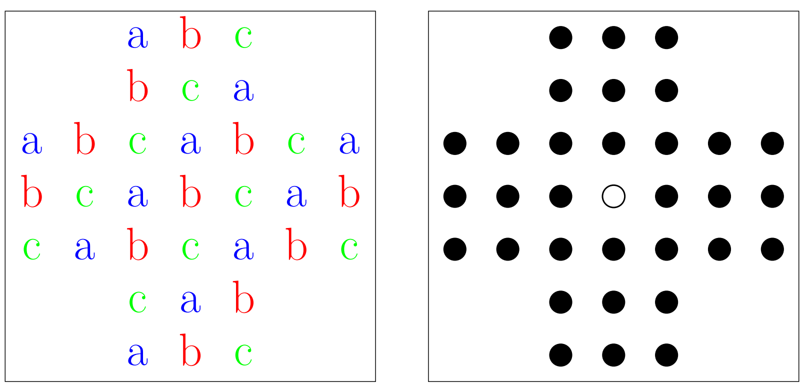
$$\mathrm{b}\cdot\mathrm{c}=\mathrm{a}$$

观察到：如果 C 走一步得到 C'，则

$$[C]=[C']$$

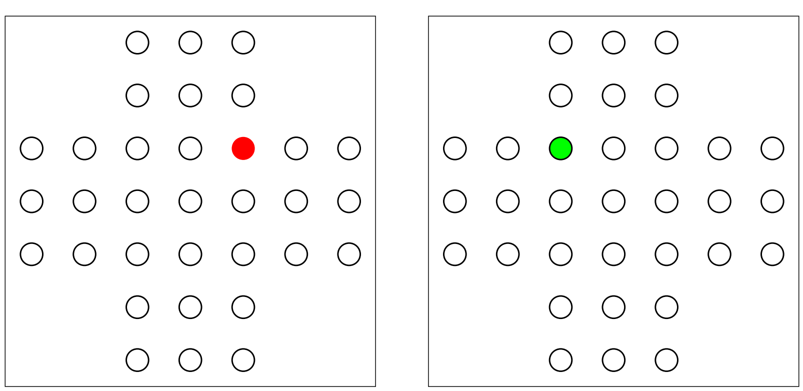
具有相同的权。因此“权”为游戏过程中的一个不变量。

容易计算初始黑子分布的权为 b

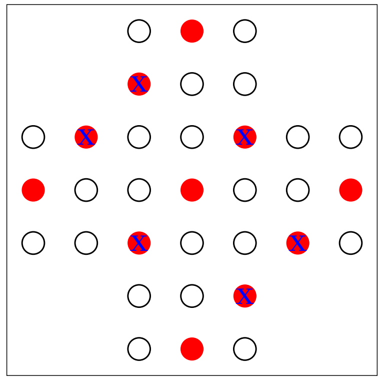


因此最后一个黑子只可能落在标记为 b 的位置。

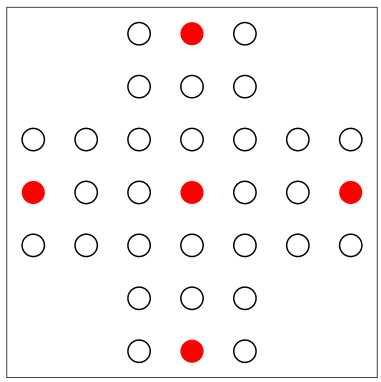
黑子最后不可能落在如下右图绿点的位置 (权为 c)。由左右对称性，可以排除最后一个黑子落在如下左图的可能性（否则可以采取左右镜像的走法使得最后落在右图绿点)。



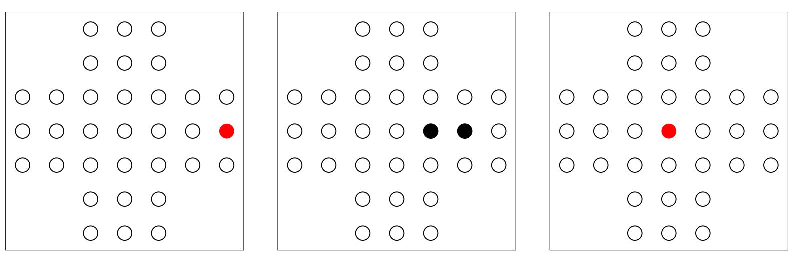
类似对称性分析，我们可以共排除如下 6 种可能



最后一个黑子只能落在如下图中的某个位置



实际上这 5 种可能性都可以达到，而且我们总可以使得最后一个黑子落在正中间。假如最后一个黑子落在如下左图的位置，则上一步如中间图。可以改变走法使得最后一个黑子落在右图的位置。这样我们就完整地解决了这个问题。



5 置换群

集合 $\{1,2,\cdots,n\}$ 到自己的一个一一映射称为一个n 元置换。例如：如下映射 σ 是一个 5 元置换

$$\sigma : 1,2,3,4,5 \to 3,1,5,2,4$$

两个置换的复合也是置换。所有 n 元置换构成一个群 (称置换群)，记为 S_n。

一个 n 元置换 σ 可以记为

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix}$$

σ 表示将 1 变成 i_1，2 变成 i_2，..., n 变成 i_n。例如

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{bmatrix}$$

表示置换 $\sigma : 1,2,3,4,5 \to 3,1,5,2,4$。乘积 $\alpha\beta$ 表示先作用 β 置换，再作用 α 置换。例如

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

如果置换 σ 把其中 k 个元素映射为

$$\sigma : i_1, i_2, i_3, \cdots, i_k \to i_2, i_3, \cdots, i_k, i_1$$

而把其他元素映射到自己，我们称 σ 是一个长度为 k 的轮换，并把 σ 简化标记为

$$\sigma = (i_1 \ i_2 \ \cdots \ i_k)$$

例如：

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{bmatrix} = (2\ 3\ 5)$$

任意一个置换总可以表示为一些轮换的乘积，例如

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 6 & 2 & 3 & 5 \end{bmatrix} = (1)(24)(365) = (24)(365)$$

其中 (1) 表示的是恒等置换，可以省略不记。

6 交错群（偶置换群）

长度为 2 的轮换 $(i\ j)$ 称为一个对换。例如

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{bmatrix} = (2\ 5)$$

每个轮换均可以表示为一些对换的乘积，但是这种表达方式不唯一。例如

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3)$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$

由于每个置换总可以表示为一些轮换的乘积，因此每个置换也总可以表示成一些对换的乘积。虽然表达法不唯一，但是容易发现不同表达法里包含的对换个数的奇偶性是确定不变的，称为该置换的奇偶性。例如：长度 k 的轮换可以写成 $k-1$ 个对换相乘

$$(1\ 2\ 3\ \ \dots\ \ k) = (1\ k)(1\ k-1)\cdots(1\ 3)(1\ 2)$$

因此我们知道奇长度的轮换是偶置换，偶长度的轮换是奇置换。例如

$$\begin{aligned} \text{奇置换：}\quad & (2\ 3),\quad (1\ 3\ 4\ 7) = (1\ 7)(1\ 4)(1\ 3) \\ \text{偶置换：}\quad & (1\ 2\ 3) = (1\ 3)(1\ 2),\quad (4\ 3\ 2\ 1\ 6) \end{aligned}$$

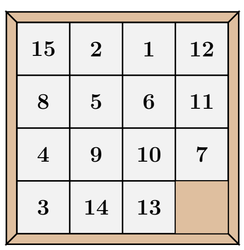
置换的复合满足

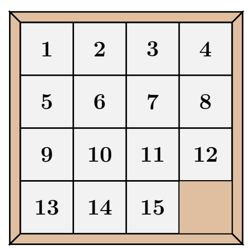
$$\begin{aligned} \text{奇置换} \times \text{奇置换} &\to \text{偶置换} \\ \text{奇置换} \times \text{偶置换} &\to \text{奇置换} \\ \text{偶置换} \times \text{偶置换} &\to \text{偶置换} \end{aligned}$$

因此 S_n 中所有偶置换构成一个群（称为交错群），记为 A_n 。

7 数字推盘问题的解-必要条件

问题: 是否可以由图左还原到图右原始位置?



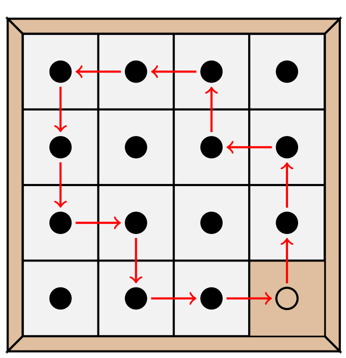


上图左对应于一个置换

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 15 & 2 & 1 & 12 & 8 & 5 & 6 & 11 & 4 & 9 & 10 & 7 & 3 & 14 & 13 & 16 \end{bmatrix}$$

这里我们把空白标记为 16。

如果棋盘的布置可以从原始的位置（上图右）移动得到，它对应的置换 σ 应该满足什么性质？移动过程可以通过记录空白位置的走动来标志



每个移动为 S_{16} 中的一个对换 (空白标志为 16)。如果要求将空白移回到出发点，则

往上走步数=往下走步数，往左走步数=往右走步数

总共要移动偶数步! 因此数字推盘问题可解的一个必要条件是

推盘对应的数字置换是偶置换

回到这节开始的问题，推盘对应的置换

$$
\begin{aligned}
\sigma &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 15 & 2 & 1 & 12 & 8 & 5 & 6 & 11 & 4 & 9 & 10 & 7 & 3 & 14 & 13 & 16 \end{bmatrix} \\
&= (1\ 15\ 13\ 3)(4\ 12\ 7\ 6\ 5\ 8\ 11\ 10\ 9)
\end{aligned}
$$

是奇置换，因此我们知道它对应的数字推盘不可能还原到原始状态。

进一步，我们可以考虑

问题：如果数字推盘对应的数字置换是偶置换，是否一定可以还原?

答案是肯定的。为了证明这个结论，我们需要引入群的生成元的概念。

8 群的生成元

群 G 的一组元素称为生成元，如果 G 中每个元素都可以通过这组元素反复相乘得到。

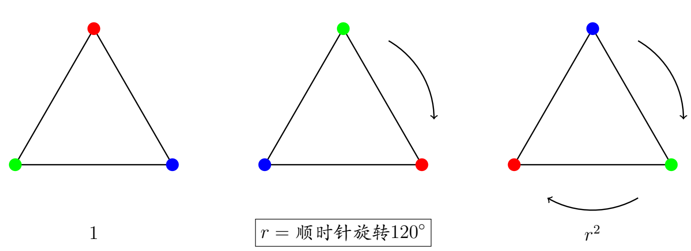
例如：Klein 群 $K = \{1, a, b, c\}$

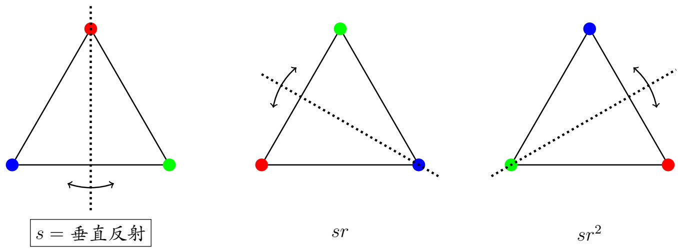
$$
\begin{aligned}
&a \bullet b = c \qquad && b \bullet c = a \qquad && c \bullet a = b \\
&a^2 = 1 && b^2 = 1 && c^2 = 1
\end{aligned}
$$

- $\{a, b\}$ 是一组生成元。比如 1 可以由 $a \bullet a$ 得到，c 可以由 $a \bullet b$ 得到。
- $\{b, c\}$ 也是一组生成元。因此生成元的选法并不唯一。

例如：二面体群 D_3 的一组生成元是 $\{r, s\}$，它们满足

$$r^3 = 1, \quad s^2 = 1, \quad sr = r^2 s$$





例如：置换群 S_n 可以由如下对换生成

$$(1\ 2),\quad (1\ 3)\quad,\quad\cdots\quad,\quad(1\ n)$$

比如任意的置换 $(i\ j)$ 可以写成

$$(i\ j)=(1\ j)(1\ i)(1\ j)$$

由此可以生成所有的置换。类似的，给定其他一个数比如 3，如下对换

$$(3\ 1),\quad (3\ 2)\quad,(3\ 4)\quad\cdots\quad,\quad(3\ n)$$

也构成 S_n 的一组生成元。

例如：交错群 A_n (即 S_n 中的偶置换) 的一组生成元是

$$(1\ 2\ 3),\quad (1\ 2\ 4)\quad,\quad\cdots\quad,\quad(1\ 2\ n)$$

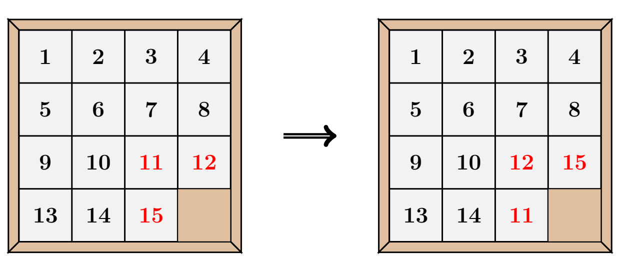
类似的，给定其他两个数比如 2, 4，如下轮换

$$(2\ 4\ 1),\quad (2\ 4\ 3)\quad,(2\ 4\ 5)\quad\cdots\quad,\quad(2\ 4\ n)$$

也构成 A_n 的一组生成元。读者可以尝试着证明这个结论。

9 数字推盘问题的解-充分条件

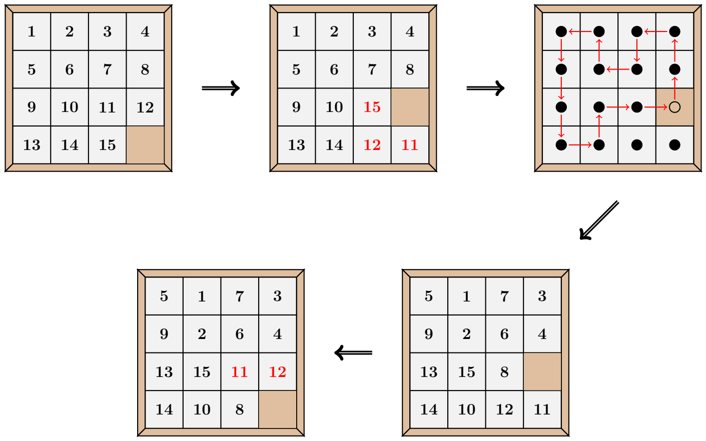
我们下面来分析求解数字推盘问题的充分条件。首先我们考虑两个特殊的移动。第一个移动为:



通过如上移动，我们知道如下置换是可以还原的

$$\tau=(11\ 12\ 15)$$

第二个移动为:



通过如上移动，我们知道如下置换是可以还原的

$$
\begin{aligned}
\rho &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 5 & 1 & 7 & 3 & 9 & 2 & 6 & 4 & 13 & 15 & 11 & 12 & 14 & 10 & 8 \end{bmatrix} \\
&= (1\ 5\ 9\ 13\ 14\ 10\ 15\ 8\ 4\ 3\ 7\ 6\ 2)
\end{aligned}
$$

观察到：如果置换 σ_1, σ_2 可以还原，那么

- $\sigma_1\sigma_2$ 可以还原：通过复合操作实现
- σ_1^{-1} 可以还原：通过逆向操作实现

换言之，所有可以还原的置换构成了一个群。

通过上述两个移动，我们知道如下两个置换是可以还原的

$$\tau = (11\ 12\ 15), \quad \rho = (1\ 5\ 9\ 13\ 14\ 10\ 15\ 8\ 4\ 3\ 7\ 6\ 2)$$

因此由它们及其逆元复合生成的置换均可还原。直接计算发现

$$\tau, \quad \rho\tau\rho^{-1}, \quad \rho^2\tau\rho^{-2}, \quad \cdots \quad , \rho^{12}\tau\rho^{-12}$$

恰好构成集合（顺序不一致）

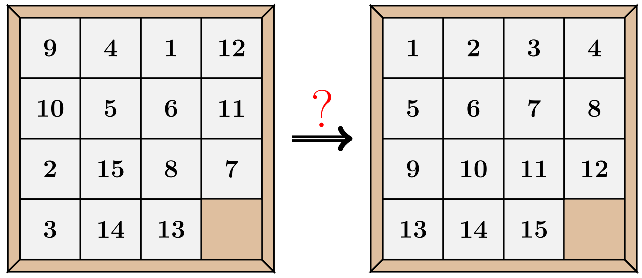
$$(11\ 12\ 1), \cdots (11\ 12\ 10), (11\ 12\ 13), (11\ 12\ 14), (11\ 12\ 15)$$

因此这些置换均可以被还原。由上述讨论，我们知道元素

$$(11\ 12\ 1), \cdots (11\ 12\ 10), (11\ 12\ 13), (11\ 12\ 14), (11\ 12\ 15)$$

生成所有的 15 元的偶置换。因此任意一个对应于偶置换的数字推盘均可以还原！总结上述讨论，我们通过置换群的结构证明了如下结论：

定理. 数字推盘可以被还原到初始状态当且仅当其对应的数字置换是偶置换。



例如对于上面这个问题，它对应的置换

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 9 & 4 & 1 & 12 & 10 & 5 & 6 & 11 & 2 & 15 & 8 & 7 & 3 & 14 & 13 \end{bmatrix}$$
$$= (1\ 9\ 2\ 4\ 12\ 7\ 6\ 5\ 10\ 15\ 13\ 3)(8\ 11)$$

是偶置换，因此我们知道它一定可以被还原。

10 后记

如果你是一名中学生，是否也渴望发表和分享新奇的想法和点子，希望当小小科学家尝试探索的乐趣？波士顿国际出版社即将发布面向中学生科研的杂志

如果你有一些好的想法，不妨来试试吧！

参考文献

[1] 李思，"几何与对称"，https://sili-math.github.io/

[2] Bogomolny, Alexander, "*Peg Solitaire and Group Theory*", Interactive Mathematics Miscellany and Puzzles, 2018

[3] Beeler, Robert A. "*The Fifteen Puzzle A Motivating Example for the Alternating Group (Supplemental Material for Intro to Modern Algebra).*"