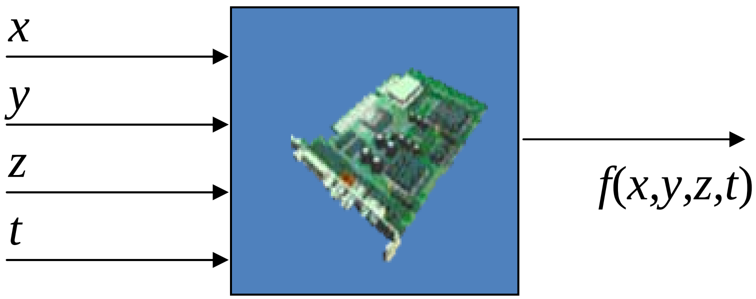
置换群的应用

陶先平，赵建华

置换群的应用

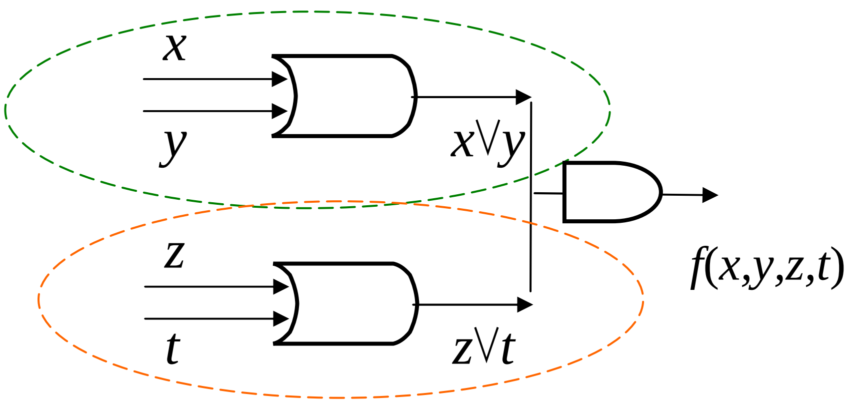
- 置换群诱导的等价关系
- 轨道
- 轨道的大小
- 轨道的个数-Burnside定理
- Burnside定理的应用

相同？不同？



4个变量，可能的输入值有2^4个；因此，可以定义$2^{16}(65,536)$个不同的函数。

但是，真的需要这么多种电路吗？

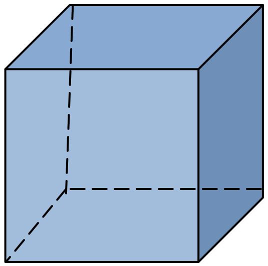


由于对称性，只要调整接入线，同样的电路可以实现不同的函数。

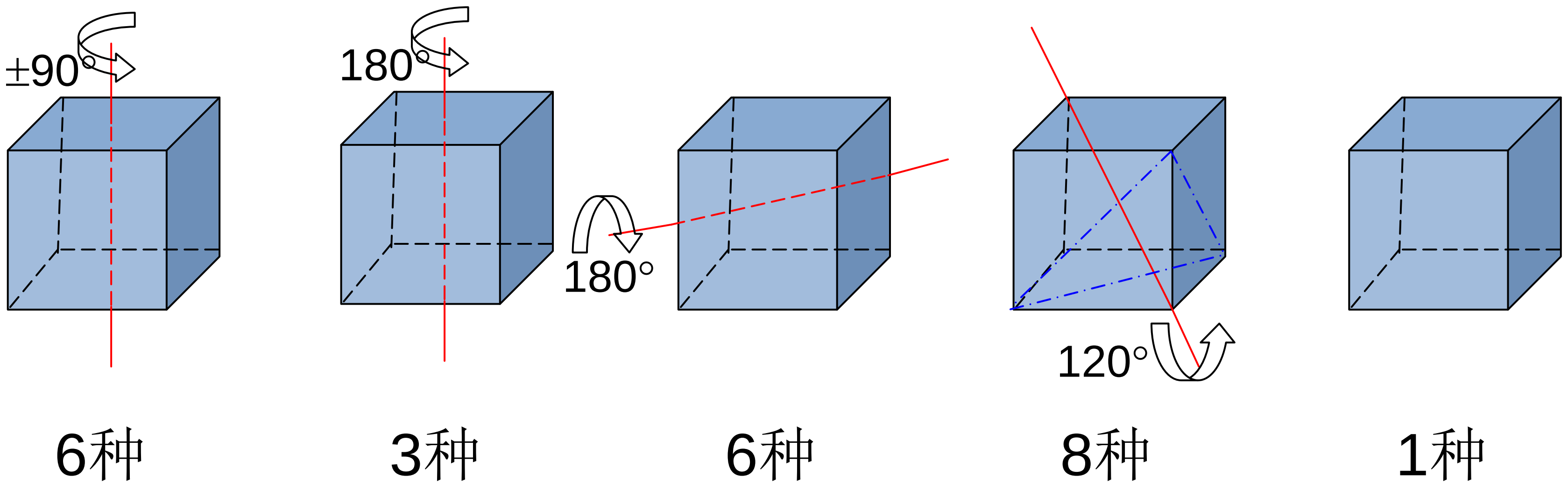
等价类计数

- 函数的集合上的关系R：函数f_1, f_2满足关系关系R iff 可以用同一个电路实现
  - 通过调整接入方式或使用外部转相器。
- 显然，上述关系R是等价关系。
  - 可以用同一电路实现的所有函数包含在同一个等价类中。
- 本质不同的不同电路总数 = 等价类的个数

对称在计数中的作用



用6种不同颜色给正方体的六个面着色，每个面有6种选择，假如给定每个面的编号，不同的着色序列有6！(=720)个，但哪些是“**真正**”不同的？



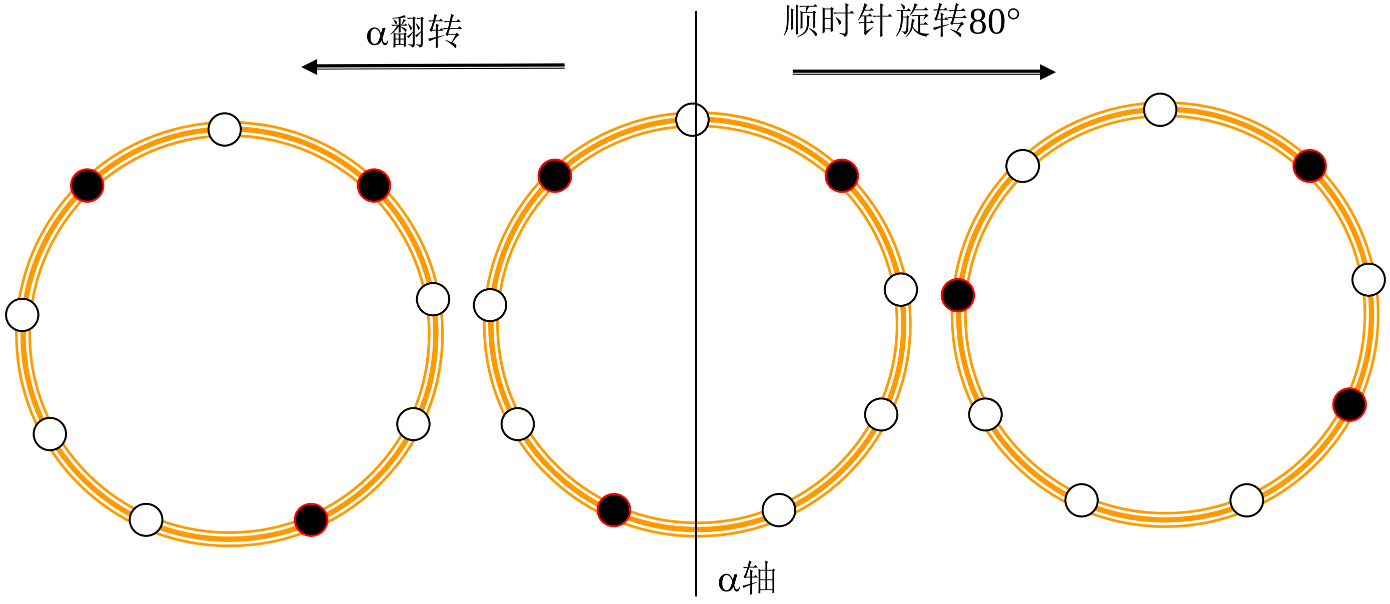
因此：不同的着色有6！/ (6+3+6+8+1) =30种

更一般的情况

- 如果不是每个面的着色都不同，比如有两个面是红的，如何判断两种着色是"**真正**"不同？
- 设着色对象的集合是S，允许使用的颜色的集合是C(我们只考虑有限集)。一种着色方案就是一个函数f:$S\rightarrow C$。f与f_2被认为"**实际上**"是一样的，当且仅当在所允许的变换(即前面例子中的对称旋转)下，f_1能转变为f_2或相反。
- 而对称旋转即置换群的元素。我们称"(置换)群作用于S，也作用于C。"

比立方体简单一点的例子

- 3个黑珍珠和6个白珍珠能做出多少样式不同的项链？



置换群诱导的等价关系

- 假设G是集合X上的置换群。定义X上的关系“~”如下：

  $\forall x,y\in X,\ x\sim y \Leftrightarrow \exists g\in G$, 使得$g(x)=y$

- “~”是等
- 将关系系

同一个轨道中的不同元素实际上是同一个东西

$$Gx=\{y \mid y\in X,\ 且\exists g\in G,\ 使得g(x)=y\}$$

这样的等价类称为X上G的***轨道***

例子

- G={(1),(1,2,3),(1,3,2)}是{1,2,3,4,5,6}上的置换群
  - G1=?   G2=?   G3=? G4=? G5=? G6=?
- 集合{1,2,3,4,5,6}在G上的轨道有几个？分别是？

保持X不变的置换构成子群

- G中所有“将x变为y”的置换构成的集合

$$\mathbf{G(x\to y)} = \{g|g\in G, \text{且} g(x)=y\}$$

  - G(1->2) ={(1,2,3)},G(1->3)={(1,3,2)}

- G中所有“保持x不变”的置换的集合

$$\mathbf{G_x}=\{g|g\in G, \text{且} g(x)=x\}$$

  - G_1={(1)};G2={(1)};G3={(1)};
  - G4=G5=G6=G;
  - 注意：G_x构成子群(why？)。

性质

- 如果$G(x\rightarrow y)$非空，那么$G(x\rightarrow y)$是G_x的右陪集

$\forall h\in G(x\rightarrow y),\ G(x\rightarrow y)=G_x h$

回顾：子群与相应的陪集等势

1、G_x是子群，

2、若$y\notin Gx$，那么$|G(x\rightarrow y)|=0$。

3、若$y\in Gx$，$\exists g(g(x)=y)$，因此$G(x\rightarrow y)\neq\varnothing$，因此$|G(x\rightarrow y)|=|G_x|$。

轨道的大小

- 性质：对任意x∈X，x所在的轨道的大小乘以保持x不变的置换的个数等于|G|
  - 给定 … ∈Gx
  - 对于 … 换恰有|G(x …

  $$|Gx|\times|G_x|=|G|$$

  - 遍历Gx中所有y，总共有|Gx|*|Gx|个转换。
  - 对于不在Gx中的y，不存在转换g使得g(x)=y。

$$\Sigma_{y\in Gx}|G_y|$$

- 对任意的$y\in X$，若$y\in Gx$，则$|G_x|=|G_y|$，即保持x不变的置换和保持y不变的置换数量相等。
  - 实际上，$G(x\rightarrow y)$是G_y的左陪集
  - 所以，对每个轨道Gx

$$\Sigma_{y\in Gx}|G_y|=|Gx|\times|G_x|=|G|,$$

- $\Sigma_{y\in Gx}|G_y|$即保持轨道Gx中某个元素不变的置换的总数
  - 如果一个置换保持轨道中n个元素不变，则被统计n次

轨道的个数

- 令轨道数为t，对每个轨道，保持其中某元素不变的置换的总数均为$|G|$

$$\sum_{x\in X}|G_x| = t\bullet|G|$$

- 每个g被统计了多少次？
  - $F(g)$表示在置换g之下保持不变的元素个数，则g被统计F(g)次。

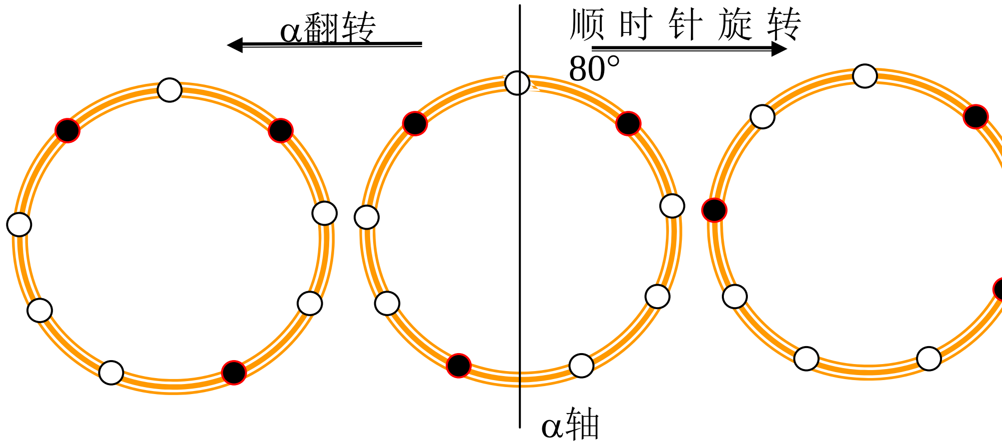
$$\sum_{g\in G}|F(g)| = \sum_{x\in X}|G_x| = t\times|G|$$

Burnside定理

$$t = \frac{1}{|G|}\sum_{g \in G} |F(g)|$$

项链问题的解

- 3个黑珍珠和6个白珍珠能做出多少样式不同的项链？
  - $|X|=84$, 即C_9^3 (*Why?*)
  - $|G|=18$
    - 9个旋转
    - 9个翻转
  - 每个翻转g, $|F(g)|=4$
  - 旋转0°的$|F(g)|=|X|=84$;
  - 旋转120°和240°的$|F(g)|$ 各为3,
  - 其它均为0。



- 结果：$(4\bullet 9+84+3\bullet 2)/18$

没有几何结构的例子

- 3个输入的逻辑电路有多少种”真正”不同的?
- 可能的输入共有8个(相当与珠子).
- 可能的输出共有2个(相当于颜色).
- 由于没有几何对称的限制，我们考虑S_3上所有的置换(共6个).
- 对于对换(1 2)，保持不变的元素由$f(0, 1, x) = f(1, 0, x)$确定，有2^6个. 而这样的对换共有3个.
- 对于置换(1 2 3)，(000，111)总是不变，因此函数值可以任意设定；(001，100，010)与(011，101，110)分别构成环，其函数值相等的函数将分别保持它们不变，因此,共有2^4个，而这样的置换有2个.
- 恒等置换保持所有的256个函数不变.
- 因此，不同的电路数：$(256+3\times2^6+2\times2^4)/6=80$

作业

- Z_5是“模5剩余加群”，$\pi(x)=2x \pmod 5$ 是Z_5上的一个置换。 G是以π为生成元的循环置换群，写出G中的元素，并求出G的轨道。
- 解13个白珍珠和3个黑珍珠的项链问题。
- 考虑一个能够解决此类问题的算法
  - 假设是对M个变量赋值，每个变量可以赋予N个值；
  - 假设有置换群G。
  - 主要问题：对于G中的每个置换g，如何计算F(g)？