自由群, 群的展示与 Todd--Coxeter 算法

Free Groups, Presentations, and the Todd--Coxeter Algorithm

组合群论: 从符号构造群, 关系与陪集枚举

RongYu

抽象代数

2026.8.9

目录

1 导言 3

I 自由群 4

2 字与约化 5

3 约化形式的唯一性 6

4 字的等价与乘法相容性 7

5 自由群的构造 8

6 自由群的映射性质 9

II 群的展示 10

7 关系与正规闭包 11

8 展示的定义 12

9 展示的例子 13

10 商群的映射性质 14

11 展示到群的典范同态 15

12 不改变群地变换展示 16

13 字问题 17

III Todd–Coxeter 陪集枚举 18

14 陪集表与 Todd–Coxeter 思想 19

15 条目如何被强制 20

16 工作示例：S3 的展示 21

17 工作示例：四面体群 22

18 一个崩塌的例子 23

19 为什么 Todd–Coxeter 能证明有限展示 24

20 实用清单 25

IV 总结与练习 26

21 内容总结 27

22 概念要点 28

23 练习 29

24 练习解答 30

A 课件英文原文 31

B 课件中文翻译 44

1

导言

本讲义基于 Jiarui Fei 的课件《Free Groups, Presentations, and the Todd–Coxeter Algorithm》撰写, 对该课件的三个主题作详细的展开: 第一部分介绍自由群 (free group), 其元素是字母表及其形式逆上的约化字; 第二部分介绍群的展示 (presentation), 通过用正规子群对自由群取商来施加关系; 第三部分介绍 Todd–Coxeter 陪集枚举 (coset enumeration), 一个判定有限展示的实用算法. 正文的每一节都配有完整的证明与工作示例, 可作为笔记《抽象代数》群论章中组合群论一节的详细讲义. 课件原文与中文翻译分别收入附录 A 与附录 B, 翻译中首次出现的术语均以括号标注英文, 人名一律保留英文.

引导问题

设一个群由展示

$$G = \langle x_1, \cdots, x_n \mid r_1 = 1, \cdots, r_k = 1 \rangle$$

给出. 它的元素是什么? 它是否有限? 它是否是一个熟悉的群? 我们能否判定生成元上的两个字是否表示同一个元素?

自由群在施加关系之前回答了第一个问题; 商群编码了这些关系; 陪集枚举常常能回答有限的情形.

阅读本讲义需要群, 子群, 陪集与指数, 正规子群与商群, 群同态与群同构定理等基本概念 (见笔记群论章), 特别是 Lagrange 定理 $|G| = [G : H]|H|$ 与循环群的分类定理. 记号与笔记保持一致: $\langle S \rangle$ 表示由子集 S 生成的子群, $|g|$ 表示元素 g 的阶, $[G : H]$ 表示子群 H 在 G 中的指数, $N \triangleleft G$ 表示 N 是 G 的正规子群, 换位子定义为 $[x, y] = xyx^{-1}y^{-1}$.

Part I

自由群

Free Groups

内容概要

- 字, 约化与约化形式的唯一性.
- 字的等价与乘法相容性.
- 自由群的构造与群结构.
- 自由群的映射性质 (泛性质) 及其证明.

2 字与约化

Def. 1　字, 长度与约化

设 S 是一个符号集合. 对每个 $s \in S$ 引入一个形式逆符号 (formal inverse) s^{-1}, 令

$$S^{\pm} = S \cup S^{-1}.$$

$S^{\pm}$ 中元素的有限串 $w = x_1 x_2 \cdots x_m$ 称为一个字 (word), 其中每个 $x_i \in S^{\pm}$; 空串称为空字 (empty word), 记为 1; 正整数 m 称为 w 的长度 (length). 删除相邻符号对 ss^{-1} 或 $s^{-1}s$ 的操作称为一次约化 (cancellation); 不能进行任何约化的字称为约化字 (reduced word).

Eg. 1　约化过程

取 $S = \{a, b, c\}$, 则

$$w = abb^{-1}c^{-1}ca^{-1}b \quad \rightsquigarrow \quad aa^{-1}b \quad \rightsquigarrow \quad b.$$

约化字为 b. 相反, $aba^{-1}b^{-1}$ 已经是约化字. 它在自由群中不是单位元, 尽管在施加交换关系 (commutativity relation) $aba^{-1}b^{-1} = 1$ 之后它成为单位元.

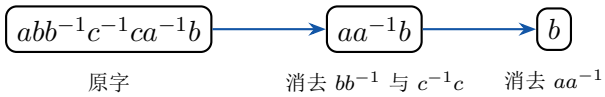


图 1: 字 $w = abb^{-1}c^{-1}ca^{-1}b$ 的约化链.

警告 1: 现阶段符号不交换

形如 $aba^{-1}b^{-1}$ 的字在代数上看似熟悉, 但符号之间并没有交换律. 在自由群中, 唯一的约化是相邻逆对的约化.

Eg. 2　两种不同的约化途径

字 $w = abb^{-1}c^{-1}cb$ 可以先约化 bb^{-1}, 也可以先约化 $c^{-1}c$. 无论哪种方式, 在所有可能的约化之后, 结果都是 ab. 这正说明了关键定理 1 的内容: 最终的约化字与约化过程中的选择无关.

3

约化形式的唯一性

Thm. 1　约化形式的唯一性

每个字都有唯一的约化形式.

Pf　存在性是直接的: 每次约化使字长减少 2, 因此任何约化序列必然终止, 终止时得到的字即为约化字, 从而至少存在一个约化形式.

唯一性: 对原字的长度 m 归纳. 若 w 已约化, 则无须证明. 否则在 w 中选取一个相邻可约对, 设

$$w = \cdots x x^{-1} \cdots .$$

设 w_0 是 w 经某个约化序列得到的任意约化字. 我们证明, 这个 w_0 可以先把所显示的 xx^{-1} 对约化掉而得到.

若在给定约化序列中, 这一对最终是作为一对被约化的, 则可以把这次约化交换到序列的最前面: 在它之前发生的约化都在这两个字母之外, 或缩短字的无关部分, 先约化 xx^{-1} 再继续, 仍得到相同的最终结果.

若这两个字母不是作为一对被约化, 则由于 w_0 是约化字, 二者中至少有一个最终必须与相邻的逆元约化. 涉及这两个字母中任意一个的第一次约化, 必然发生在下列两种三字母块之一中:

$$x^{-1}xx^{-1} \quad \text{或} \quad xx^{-1}x.$$

两种情形下, 约化相邻对与约化原来的中间对给出完全相同的中间字. 例如

$$x^{-1}xx^{-1} \longrightarrow x^{-1},$$

无论先约化前两个字母还是后两个字母. 于是约化序列可以再次被修改, 使所选的 xx^{-1} 对先被约化.

首次约化之后, 字的长度变为 $m-2$. 由归纳假设, 较短的字有唯一的约化形式, 因此 w 的所有约化形式都相同. □

4

字的等价与乘法相容性

Def. 1　字的等价

两个字 u 与 v 称为等价的 (equivalent), 记作 $u \sim v$, 若它们有相同的约化形式. 这是一个等价关系 (equivalence relation). 字 w 的等价类 (equivalence class) 记为 $[w]$.

Prop. 1　与乘法的相容性

若 $u \sim u'$ 且 $v \sim v'$, 则 $uv \sim u'v'$.

Pf　将 u 与 v 分别约化为约化字 u_0 与 v_0. 乘积 uv 先约化为 $u_0 v_0$, 之后只剩下跨越 u_0 与 v_0 边界的约化. 对 $u'v'$ 施加同样的过程, 由于 u' 与 v' 和 u 与 v 有相同的约化形式, 得到同一个中间字 $u_0 v_0$. 因此 uv 与 $u'v'$ 有相同的约化形式. □

5

自由群的构造

Def. 1　自由群

S 上的自由群 (free group), 记作 $F(S)$, 是 $S^{\pm}$ 中字的等价类构成的集合, 其乘法定义为

$$[u][v] = [uv].$$

命题 1 说明这个运算是良定义的.

Thm. 1　$F(S)$ 是群

$F(S)$ 是一个群. 其单位元是空字的等价类, 并且

$$[x_1 x_2 \cdots x_m]^{-1} = [x_m^{-1} \cdots x_2^{-1} x_1^{-1}]. \tag{5.1}$$

Pf　结合律来自字拼接的结合律:

$$([u][v])[w] = [uv][w] = [(uv)w] = [u(vw)] = [u][vw] = [u]([v][w]).$$

空字充当单位元, 因为拼接空字不改变任何字. 最后,

$$(x_1 \cdots x_m)(x_m^{-1} \cdots x_1^{-1})$$

从中间向外逐对约化, 完全约化为空字; 逆序乘积同样约化. 故(5.1) 中按逆序取逆元的字代表逆元. □

Eg. 1　单生成元的自由群

设 $S = \{a\}$. 每个约化字都是 a^n, 其中 n 是唯一的整数. 因此

$$F(a) \cong (\mathbb{Z}, +), \qquad a^n \longleftrightarrow n.$$

这是除平凡自由群之外唯一可交换的自由群.

Eg. 2　双生成元的自由群

在 $F(a,b)$ 中, 字 ab 与 ba 不同, 因为二者均为约化字且作为字符串不相等. 因此 $F(a,b)$ 是非 Abel 群. 字

$$aba^{-1}, \qquad b^{-1}a^2b, \qquad [a,b] = aba^{-1}b^{-1}$$

都已约化, 其中没有一个自动等于 1.

6

自由群的映射性质

Thm. 1　自由群的映射性质

设 $F(S)$ 是 S 上的自由群. 对任意群 G 与任意函数 $f : S \to G$, 存在唯一的群同态

$$\varphi : F(S) \to G$$

使得对所有 $s \in S$ 成立 $\varphi(s) = f(s)$.

Pf　将 f 延拓到形式逆字母, 令

$$f(s^{-1}) = f(s)^{-1}.$$

对字 $w = x_1 \cdots x_m$, 定义

$$\Phi(w) = f(x_1) f(x_2) \cdots f(x_m) \in G.$$

若一个字因一次约化而改变, 例如删去 ss^{-1}, 则 Φ 不变, 因为 $f(s)f(s)^{-1} = 1$; 删去 $s^{-1}s$ 时同理. 因此等价字在 Φ 下有相同的像, Φ 下降到等价类上的良定义映射:

$$\varphi([w]) = \Phi(w).$$

它是同态, 因为

$$\varphi([u][v]) = \varphi([uv]) = \Phi(uv) = \Phi(u)\Phi(v) = \varphi([u])\varphi([v]).$$

按构造, 它把每个生成元 s 送到 $f(s)$.

唯一性: $F(S)$ 的每个元素都由 S 的元素及其逆组成的字表示. 一个同态被迫把

$$s_1^{\varepsilon_1} \cdots s_m^{\varepsilon_m} \quad \text{送到} \quad f(s_1)^{\varepsilon_1} \cdots f(s_m)^{\varepsilon_m},$$

其中 $\varepsilon_i = \pm 1$. 因此在 S 上取相同值的同态只能有一个. □

Eg. 1　在具体群中求值

设 $F(a, b)$ 在 a, b 上自由, $G = S_3$, 取

$$f(a) = (123), \qquad f(b) = (12).$$

泛性质给出同态 $\varphi : F(a, b) \to S_3$. 例如

$$\varphi(aba^{-1}b^{-1}) = (123)(12)(132)(12),$$

这是 (123) 与 (12) 在 S_3 中的换位子. 自由群使我们一旦给生成元赋值, 就能在任意群中求形式字的值.

Part II

群的展示

Presentations

内容概要

- 关系, 正规闭包与展示的定义.
- 商群的映射性质与展示到群的典范同态.
- 循环群, 自由 Abel 群与二面体群的展示.
- 变换展示与字问题.

7

关系与正规闭包

Def. 1　关系与正规闭包

关系 (relation) 是我们希望其成为单位元的字. 设 $R \subseteq F(S)$, 定义 R 的正规闭包 (normal closure) 为

$$\langle\langle R \rangle\rangle = \bigcap \{ N \triangleleft F(S) : R \subseteq N \}. \tag{7.1}$$

Prop. 1　正规闭包的构造

$\langle\langle R \rangle\rangle$ 是 $F(S)$ 中包含 R 的最小的正规子群; 等价地, 它由所有共轭 (conjugate) 生成:

$$\langle\langle R \rangle\rangle = \left\langle g r g^{-1} \mid g \in F(S),\ r \in R \right\rangle. \tag{7.2}$$

Pf　交集(7.1) 中的每个 N 都是 $F(S)$ 的正规子群, 且任何两个正规子群的交集仍是正规子群, 因此 $\langle\langle R \rangle\rangle$ 是包含 R 的正规子群, 并且包含于每个含 R 的正规子群, 故为最小者.

记 $H = \langle g r g^{-1} \mid g \in F(S),\ r \in R \rangle$. 一方面, 若 $N \triangleleft F(S)$ 且 $R \subseteq N$, 则由正规性 $g r g^{-1} \in N$ 对一切 g, r 成立, 故 $H \subseteq N$, 于是 $H \subseteq \langle\langle R \rangle\rangle$. 另一方面, 对固定的 $r \in R$ 与 $g \in F(S)$, 由正规性 $g r g^{-1} \in \langle\langle R \rangle\rangle$, 故 $\langle\langle R \rangle\rangle$ 包含所有生成元, 从而 $\langle\langle R \rangle\rangle \supseteq H$. 两方向合起来给出(7.2). □

Rmk　正规性是本质的: 若商群中 $r = 1$, 则每个共轭 $g r g^{-1}$ 也必须是 1, 因为商映射是同态. 因此关系 $r = 1$ 一旦施加, 其全部共轭自动成为真, 这正是必须取正规闭包而非通常生成子群的原因.

8

展示的定义

Def. 1　群的展示

设 $S=\{x_1,\cdots,x_n\}$, $R=\{r_1,\cdots,r_k\}\subseteq F(S)$. 由生成元 S 与关系 $r_1=1,\cdots,r_k=1$ 生成的群定义为

$$\langle x_1,\cdots,x_n \mid r_1,\cdots,r_k\rangle = F(S)/\langle\langle r_1,\cdots,r_k\rangle\rangle. \tag{8.1}$$

一个字代表这个展示群中的单位元, 当且仅当它位于关系子的正规闭包中. 右侧的 r_i 称为关系子 (relator), 左侧的 x_i 称为生成元 (generator).

9 展示的例子

Eg. 1 循环群

$$C_n \cong \langle a \mid a^n \rangle .$$

Pf 由例 1, $F(a) \cong (\mathbb{Z}, +)$, 其中 $a^k \leftrightarrow k$. 由 a^n 生成的正规闭包对应子群 $n\mathbb{Z}$, 商掉之后指数模 n 相等, 故

$$\langle a \mid a^n \rangle \cong \mathbb{Z}/n\mathbb{Z},$$

每个元素形如 a^i 且 $0 \le i < n$. 由笔记中循环群的分类定理, 这就是 n 阶循环群 C_n. □

Eg. 2 无限循环群

$$\langle a \mid \rangle \cong \mathbb{Z}.$$

Pf 没有关系子, 正规闭包平凡, 群就是 $F(a) \cong (\mathbb{Z}, +)$. □

Eg. 3 秩二自由 Abel 群

$$\left\langle a, b \mid aba^{-1}b^{-1} \right\rangle \cong \mathbb{Z}^2.$$

Pf 关系 $aba^{-1}b^{-1} = 1$ 等价于 $ab = ba$. 一旦 a 与 b 交换, 每个字都可以重排为 $a^m b^n$. 定义

$$\theta : \langle a, b \mid [a, b] \rangle \to \mathbb{Z}^2, \qquad \theta(a) = (1, 0), \quad \theta(b) = (0, 1).$$

该映射满. 逆映射 $(m, n) \mapsto a^m b^n$ 良定义, 因为施加关系后群是 Abel 群. 因此两群同构. □

Eg. 4 二面体群

正 n 边形的对称群有展示

$$D_n \cong \left\langle r, s \mid r^n, s^2, srsr \right\rangle .$$

Pf 关系 $srsr = 1$ 等价于 $srs = r^{-1}$, 或 $sr = r^{-1}s$. 因此每个字都可以重写, 使所有 s 都移到右边:

$$r^i \quad \text{或} \quad r^i s, \qquad 0 \le i < n.$$

所以展示群至多有 $2n$ 个元素. 另一方面, 正 n 边形的实际旋转与反射满足这三个关系, 并构成一个 $2n$ 阶群. 由命题 1, 典范同态满射到该 $2n$ 阶群, 而定义域至多 $2n$ 个元素, 故该同态是同构, 展示完备. □

10

商群的映射性质

Thm. 1　商群的映射性质

设 $\pi : G' \to G'/N$ 是商映射, 其中 $N \triangleleft G'$. 若 $\varphi : G' \to G$ 是同态且 $N \subseteq \operatorname{Ker}\varphi$, 则存在唯一的同态

$$\bar{\varphi} : G'/N \to G$$

使得 $\bar{\varphi} \circ \pi = \varphi$.

Pf　定义

$$\bar{\varphi}(gN) = \varphi(g).$$

这是良定义的:若 $gN = hN$, 则 $h^{-1}g \in N \subseteq \operatorname{Ker}\varphi$, 从而 $\varphi(h^{-1}g) = 1$, 故 $\varphi(g) = \varphi(h)$. 它是同态, 因为

$$\bar{\varphi}(gN \cdot hN) = \bar{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = \bar{\varphi}(gN)\bar{\varphi}(hN).$$

唯一性: 每个陪集都有形式 $\pi(g) = gN$, 条件 $\bar{\varphi} \circ \pi = \varphi$ 迫使 $\bar{\varphi}(gN) = \varphi(g)$. □

11 展示到群的典范同态

Prop. 1　展示的典范同态

设 G 是群, 含有元素 $x_1, \cdots, x_n$, 并假设字 $r_1, \cdots, r_k$ 在这些元素处求值时为 1. 则存在典范同态

$$\psi : \langle x_1, \cdots, x_n \mid r_1, \cdots, r_k \rangle \longrightarrow G$$

把抽象生成元 x_i 送到具体元素 $x_i \in G$. 当且仅当这些具体元素生成 G 时, ψ 是满射.

Pf　由自由群的映射性质 (定理 1), 把抽象生成元赋给具体元素的对应延拓为同态 $F(x_1, \cdots, x_n) \to G$. 每个关系子映到 1, 故关系子的正规闭包位于核中. 由商群的映射性质 (定理 1), 得到从展示群出发的所需同态. 其像恰为具体元素生成的子群, 因此满射当且仅当具体元素生成 G. □

Def. 1　完备关系组

若命题 1 中的 ψ 还是单射, 则称所列关系为完备关系组 (complete set of relations). 等价地, G 的所选元素之间的每个关系都可以由所列关系子推出.

Eg. 1　四面体的设置

正四面体的旋转对称群 T 由旋转 x, y, z 生成, 满足

$$x^3 = 1, \quad y^3 = 1, \quad z^2 = 1, \quad xyz = 1.$$

因此展示 $\langle x, y, z \mid x^3, y^3, z^2, xyz \rangle$ 满射到 T. 要证明它恰好是 T, 必须证明没有隐藏的额外关系. Todd–Coxeter 枚举提供了这个证明 (见第 17 节).

12

不改变群地变换展示

展示的某些变换是安全的.对计算最有用的是消去一个由其他生成元明确决定的生成元.

Eg. 1　在四面体展示中消去 z

从

$$\langle x, y, z \mid x^3, y^3, z^2, xyz \rangle$$

出发. 关系 $xyz = 1$ 蕴含 $z = (xy)^{-1} = y^{-1}x^{-1}$. 由于 $z^2 = 1$, 本例中也可利用 $z^{-1} = z$ 与 $xyz = 1$ 写 $z = xy$. 把 $z = xy$ 代入 $z^2 = 1$, 得到

$$(xy)^2 = xyxy = 1.$$

于是四面体展示等价于双生成元展示

$$\langle x, y \mid x^3, y^3, xyxy \rangle.$$

这个展示在陪集枚举中远为方便.

Eg. 2　S_3 的展示

设 $x = (123)$, $y = (12) \in S_3$. 则

$$x^3 = 1, \quad y^2 = 1, \quad yxy = x^{-1}.$$

第三个关系等价于 $yxyx = 1$. 因此

$$S_3 \cong \langle x, y \mid x^3, y^2, yxyx \rangle.$$

Pf　关系蕴含 $yx = x^{-1}y = x^2y$, 故每个字约化为

$$1,\ x,\ x^2,\ y,\ xy,\ x^2y$$

之一. 所以展示群至多有六个元素. 另一方面, 具体的置换 $x = (123)$, $y = (12)$ 满足这些关系并生成 S_3, 后者有六个元素. 由命题 1, 典范同态满射到 S_3, 定义域至多六个元素, 故是同构, 展示完备. □

13

字问题

Def. 1　字问题

对展示 $G = \langle S \mid R \rangle$, 字问题 (word problem) 询问: 给定字 $w \in F(S)$, w 是否表示 G 中的单位元, 即是否

$$w \in \langle\langle R \rangle\rangle.$$

Rmk　若字问题可解, 则任意两字的相等性可判定, 因为

$$w_1 = w_2 \text{ in } G \iff w_1 w_2^{-1} = 1 \text{ in } G.$$

对小的有限展示, Todd–Coxeter 枚举是最有用的实用工具之一.

Part III

Todd--Coxeter 陪集枚举

Coset Enumeration

内容概要

- 陪集表, 逆一致性与关系子的闭合路径.
- 条目如何被强制, 以及重合 (coincidence).
- 完备陪集表给出置换表示.
- 工作示例: S_3, 四面体群与崩塌例子.
- 为什么 Todd–Coxeter 能证明有限展示, 实用清单.

14

陪集表与 Todd--Coxeter 思想

设

$$G = \langle x_1, \cdots, x_n \mid r_1, \cdots, r_k \rangle$$

且 $H \leqslant G$ 由某些字生成. Todd–Coxeter 算法试图枚举 H 的右陪集

$$H,\ Hg_2,\ Hg_3,\ \ldots$$

给它们编号 $1, 2, 3, \ldots$. 一张表记录右乘生成元的作用:

$$\text{表项}(i, x) = j \iff (Hg_i)x = Hg_j.$$

Def. 1　陪集表

设 $G = \langle x_1, \cdots, x_n \mid r_1, \cdots, r_k \rangle$, $H \leqslant G$ 由某些字生成. 给右陪集 $H, Hg_2, Hg_3, \cdots$ 依次编号 $1, 2, 3, \cdots$, 并记录右乘生成元的作用, 得到陪集表 (coset table): 表项 $(i, x) = j$ 表示 $(Hg_i)x = Hg_j$.

当表包含逆列时, 必须满足逆一致性 (inverse consistency):

$$i^x = j \iff j^{x^{-1}} = i.$$

每个关系子必须从每一行追踪一条闭合路径: 若 $r = x_{i_1} \cdots x_{i_m}$, 则

$$i^r = i \quad \text{对每一行} i \text{ 成立.}$$

若 h 是 H 的子群生成元, 则第 1 行必须满足

$$1^h = 1,$$

因为 $Hh = H$.

15

条目如何被强制

Eg. 1　从关系两端工作

假设正在从第 i 行读取关系 $r = xyxy = 1$. 若表已知

$$i^x = a, \quad a^y = b, \quad i^{(xyxy)} = i,$$

则剩余字母以与回到 i 相容的方式强制 b^x 与 $(b^x)^y$ 的值. 实践中从关系的两端同时工作: 例如若

$$i^x = a, \quad j^{y^{-1}} = i,$$

则部分路径可能强制某个未知的中间条目等于 j.

Def. 1　重合

若两个不同的推导强制同一个陪集标号等于两个标号, 则合并这两个标号. 这样的合并称为重合 (coincidence).

警告 2: 主要的计算危险

一个错误的条目可能使整张表错误地崩塌. 手算时, 每个被强制的条目都应检查逆列, 且每个关系子都应从每一行读取.

Prop. 1　完备表给出什么

一张完备的陪集表给出陪集标号集合上的置换 (permutation), 每个生成元对应一个. 若每个关系子都作为恒等置换作用, 且每个子群生成元都固定第 1 行, 则这张表定义了展示群的一个置换表示 (permutation representation).

Pf　完备表对每个生成元 x 给定了标号集合 $\{1, \dots, N\}$ 上的一个映射 $i \mapsto i^x$. 由逆一致性, 逆列给出反向映射, 故每个 $i \mapsto i^x$ 是双射, 即一个置换. 把每个字 w 送到相应置换的复合, 得到 $F(S)$ 到对称群 S_N 的同态: 复合的分配性保证它是同态. 每个关系子作用为恒等置换, 故正规闭包 $\langle\langle r_1, \cdots, r_k \rangle\rangle$ 位于核中; 每个子群生成元固定第 1 行, 保证行为与右陪集作用相容. 由商群的映射性质 (定理 1), 该同态下降为展示群 G 到 S_N 的同态, 即一个置换表示. □

16

工作示例: S3 的展示

考虑

$$G = \langle x, y \mid x^3, y^2, yxyx \rangle$$

并取 $H = \langle y \rangle$. 由于 $y^2 = 1$, 子群 H 的阶至多为 2. 我们枚举 H 的右陪集. 第 1 行代表 H 本身, 故 $1^y = 1$. 关系 $x^3 = 1$ 提示在 x 下应有轮换. 完备的陪集表为:

Table 1: S_3 展示的陪集表

陪集	x	y
1	2	1
2	3	3
3	1	2

相应的置换为

$$x = (123), \qquad y = (23).$$

检验关系:

$$x^3 = 1, \qquad y^2 = 1, \qquad yxyx = (23)(123)(23)(123) = 1.$$

故表与展示相容. 因为 y 在陪集上非平凡地作用, G 中 $y \neq 1$, 所以 H 的阶为 2. 表有三个陪集, 故

$$|G| = |H|[G : H] = 2 \cdot 3 = 6.$$

具体置换 $x = (123)$, $y = (23)$ 生成 S_3, 于是

$$G \cong S_3.$$

17

工作示例: 四面体群

使用双生成元四面体展示

$$G = \langle x, y \mid x^3, y^3, xyxy \rangle .$$

取 $H = \langle x \rangle$. 一次 Todd–Coxeter 枚举给出四个陪集及其生成元作用:

Table 2: 四面体展示的陪集表

陪集	x	y
1	1	2
2	3	3
3	4	1
4	2	4

于是

$$x = (234), \qquad y = (123).$$

这些置换满足

$$x^3 = 1, \qquad y^3 = 1, \qquad (xy)^2 = 1.$$

由于 x 在标号 $2, 3, 4$ 上作为 3-轮换作用, x 在展示群中的阶为 3, 故 $|H| = 3$. 表有四个陪集, 所以

$$|G| = |H|[G : H] = 3 \cdot 4 = 12.$$

正四面体的旋转对称群也阶为 12 且满足同样的关系, 因此展示完备. 所示置换生成 A_4, 故四面体旋转群同构于 A_4.

18

一个崩塌的例子

关系的小改动可以剧烈地改变一个群.考虑

$$G = \langle x, y \mid x^3, y^3, yxyxy \rangle$$

并取 $H = \langle y \rangle$. 与四面体关系 $xyxy = 1$ 相比, 关系 $yxyxy = 1$ 在陪集表中强制强烈的重合, 枚举崩塌为单个陪集, 所以 $H = G$.

由于 G 由 y 生成且 $y^3 = 1$, 群的阶至多为 3. 它并不被迫为平凡群: 存在满同态

$$G \to C_3, \qquad x \mapsto 1, \quad y \mapsto \bar{y},$$

其中 $\bar{y}$ 是 C_3 的生成元. 事实上关系子 $yxyxy$ 映到 $\bar{y}^3 = 1$. 因此

$$G \cong C_3.$$

19

为什么 Todd--Coxeter 能证明有限展示

设一个展示满射到已知的有限群 K. 要证明展示完备, 只需证明展示群至多有 $|K|$ 个元素. 陪集枚举通过找到一个子群 H 与指数 $[G:H]$ 做到这一点; 若同一张表还确定了 H 的阶, 则

$$|G| = |H|[G:H].$$

在四面体例子中, $H = \langle x \rangle$ 的阶为 3, 枚举给出指数 4, 故 $|G| = 12$. 由于实际四面体旋转群阶为 12 且由满足关系的元素生成, 从展示群到四面体群的满射必为同构.

警告 3: 终止性

Todd–Coxeter 强大但并非万能. 对某些展示或子群选择, 手算枚举可能非常长, 而对无限指数的子群, 枚举不会以有限表终止. 完备的有限表就是证书.

20

实用清单

Meth. 1　手算 Todd–Coxeter 的步骤

1. 选择阶容易控制的子群 H, 通常由一个生成元生成.
2. 第 1 行以所有子群生成元字固定第 1 行开始.
3. 仅当生成元把已知行送到未知处时, 才添加新的陪集名.
4. 从每一行正反两个方向读取每个关系子.
5. 每当两个标号被强制相等, 处处合并它们.
6. 表完备后, 把生成元列翻译为置换.
7. 当 H 的阶已知时, 用 $|G| = |H|[G : H]$.

Part IV

总结与练习

Summary and Practice

内容概要

- 三个主题的内容总结.
- 概念要点: 展示的两阶段构造.
- 五个练习及解答.

21

内容总结

Table 3: 三个主题的总结

主题	主要思想
自由群	元素是约化字,唯一的约化是相邻逆对, 映射性质说生成元到群的任何赋值都唯一地延拓为同态
关系	展示是自由群对关系子正规闭包的商, 所列关系子变为真, 且其全部共轭自动变为真
完备性	展示群满射到任何其生成元满足关系子的具体群, 关系完备当且仅当该映射单射
Todd–Coxeter	用关系子枚举子群的陪集, 完备的陪集表给出生成元置换, 并常常算出群的阶

22

概念要点

展示的两阶段构造

展示是一个两阶段对象:

$$\text{符号} \longrightarrow \text{自由群} \longrightarrow \text{按关系取商}.$$

自由群阶段在约化强制相等之前记住每一个字;商阶段恰好施加所列出的关系及其正规推论; Todd–Coxeter 则在能够完成可管理的陪集表时, 把抽象商转化为有限的置换计算.

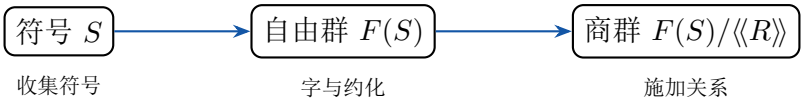


图 2: 展示的两阶段构造: 从符号到自由群再到商群.

23

练习

1. 证明 $\langle a, b \mid a^2, b^2, abab\rangle \cong C_2 \times C_2$. 提示: 关系 $abab = 1$ 说明, 在 $a^2 = b^2 = 1$ 时 $ab = (ab)^{-1} = ba$.
2. 证明 $\langle r, s \mid r^4, s^2, srsr\rangle$ 恰好有八个元素, 并把它等同于正方形的对称群.
3. 在 $F(a, b)$ 中约化字

$$aba^{-1}ab^{-1}, \qquad ab^{-1}ba^{-1}, \qquad aba^{-1}b^{-1}.$$

   其中哪些约化为空字?
4. 设 $G = \langle x, y \mid x^2, y^3, (xy)^2\rangle$. 用代换 $s = x$, $r = xy$ 把它与 S_3 的通常展示比较.
5. 对 $G = \langle x, y \mid x^3, y^3, xyxy\rangle$, 直接从置换表 $x = (234)$, $y = (123)$ 验证每个关系子平凡作用.

24

练习解答

练习 1. 设 $G = \langle a, b \mid a^2, b^2, abab \rangle$. 由 $a^2 = b^2 = 1$ 得 $a^{-1} = a$, $b^{-1} = b$, 而 $abab = 1$ 蕴含 $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$, 故 G 是 Abel 群, 每个元素形如 $a^i b^j$, $i, j \in \{0, 1\}$, 至多四个元素. 映射

$$\varphi : \left\langle a, b \mid a^2, b^2, abab \right\rangle \to C_2 \times C_2, \qquad a \mapsto (\bar{a}, 1), \quad b \mapsto (1, \bar{b})$$

良定义且满, 定义域至多四个元素, 故为同构. □

练习 2. 关系 $srsr = 1$ 等价于 $sr = r^{-1}s$, 故每个字可化为 $r^i s^j$ 的形式, $0 \le i < 4$, $j \in \{0, 1\}$, 至多八个元素. 正方形的对称群 D_4 (即 D_n 中 $n = 4$ 的情形) 由例 4 的展示给出, 阶为 8, 故该展示恰好定义八个元素, 即正方形的对称群. □

练习 3. 第一个字:

$$aba^{-1}ab^{-1} \longrightarrow ab(a^{-1}a)b^{-1} \longrightarrow abb^{-1} \longrightarrow a,$$

不为空字. 第二个字:

$$ab^{-1}ba^{-1} \longrightarrow a(b^{-1}b)a^{-1} \longrightarrow aa^{-1} \longrightarrow 1,$$

约化为空字. 第三个字 $aba^{-1}b^{-1}$ 已约化, 不为空字. □

练习 4. 令 $s = x$, $r = xy$. 则 $x = s$, $y = s^{-1}r = sr$ (因 $s^2 = 1$). 关系变为

$$s^2 = 1, \qquad (sr)^3 = y^3 = 1, \qquad r^2 = (xy)^2 = 1.$$

故 $G \cong \langle s, r \mid s^2, r^2, (sr)^3 \rangle$. 这是 S_3 的经典展示 (两个对换生成, 其乘积为三轮换): 例如 $s = (12)$, $r = (23)$ 时 $sr = (123)$. 因此 $G \cong S_3$. □

练习 5. 在 $\{1, 2, 3, 4\}$ 上计算: $x^3 = (234)^3 = 1$; $y^3 = (123)^3 = 1$; 而

$$xy = (234)(123) = (13)(24),$$

故 $(xy)^2 = 1$. 三个关系子都平凡作用. □

A

课件英文原文

本附录逐节收录课件《Free Groups, Presentations, and the Todd–Coxeter Algorithm》(作者 Jiarui Fei) 的英文原文, 供对照阅读.

Roadmap and guiding problem

Purpose. These notes explain how to build groups from symbols. Section 7.9 constructs the free group: the group whose elements are reduced words in an alphabet and its formal inverses. Section 7.10 adds relations by quotienting the free group by a normal subgroup. Section 7.11 gives a practical finite-group test: enumerate cosets using the Todd–Coxeter method.

The guiding problem. Suppose a group is described by

$$G = \langle x_1, \dots, x_n \mid r_1 = 1, \dots, r_k = 1 \rangle.$$

What are its elements? Is it finite? Is it a familiar group? Can we decide whether two words in the generators represent the same element? The free group answers the first question before relations are imposed; quotient groups encode the relations; coset enumeration often answers the finite case.

Outline.

1. Free groups
2. Presentations
3. Todd–Coxeter enumeration
4. Summary and practice

1. Words and reduction

Let S be a set of symbols. For each $s \in S$, introduce a formal inverse symbol s^{-1}. Let

$$S^{\pm} = S \cup S^{-1}.$$

A word is a finite string $w = x_1 x_2 \cdots x_m$ with each $x_i \in S^{\pm}$. The empty word is denoted by 1. The length of w is m.

A cancellation is the deletion of adjacent symbols ss^{-1} or $s^{-1}s$. A word is reduced if no cancellation is possible. For example, with $S = \{a, b, c\}$,

$$w = abb^{-1}c^{-1}ca^{-1}b \quad \rightsquigarrow \quad aa^{-1}b \quad \rightsquigarrow \quad b.$$

The reduced word is b. In contrast, $aba^{-1}b^{-1}$ is already reduced. It is not the identity in the free group, though it becomes the identity after imposing the commutativity relation $aba^{-1}b^{-1} = 1$.

Warning 1. A word such as $aba^{-1}b^{-1}$ looks algebraically familiar, but at this stage the symbols do not commute. In a free group, the only cancellations are adjacent inverse cancellations.

1. Words and reduction continued

Example 1 (Two different-looking reductions). The word

$$w = abb^{-1}c^{-1}cb$$

can first cancel bb^{-1} or first cancel $c^{-1}c$. Either way, after all possible cancellations, the result is ab. This illustrates the key theorem: the final reduced word is independent of the choices made during cancellation.

2. Uniqueness of reduced form

Theorem 2 (Uniqueness of reduced form). Every word has a unique reduced form.

Proof. Existence is immediate because every cancellation shortens the word by two letters, so a sequence of cancellations must terminate. Termination gives at least one reduced word.

For uniqueness, use induction on the length m of the original word. If w is already reduced, there is nothing to prove. Otherwise choose an adjacent cancellable pair in w, say

$$w = \cdots xx^{-1} \cdots .$$

Let w_0 be any reduced word obtained from w by some sequence of cancellations. We show that this same w_0 can be obtained by first cancelling the displayed pair xx^{-1}.

If the displayed pair is eventually cancelled as a pair in the given reduction sequence, then we may commute that cancellation to the front of the sequence: cancellations before it occur away from the two letters or shorten unrelated parts of the word, and the same final result is obtained after cancelling xx^{-1} first.

If the two letters are not cancelled as a pair, then since w_0 is reduced, at least one of them must eventually cancel with a neighboring inverse. The first cancellation involving either of these two letters must occur inside a three-letter block of one of the forms

$$x^{-1}xx^{-1} \quad \text{or} \quad xx^{-1}x.$$

In either case, cancelling the neighboring pair gives exactly the same intermediate word as cancelling the original middle pair. For example,

$$x^{-1}xx^{-1} \longrightarrow x^{-1}$$

whether one cancels the first two letters or the last two letters. Thus the reduction sequence can again be modified so that the chosen pair xx^{-1} is cancelled first.

After this first cancellation, the word has length $m-2$. By the induction hypothesis, the shorter word has a unique reduced form. Hence all reduced forms of w agree. □

3. Equivalence of words

Define two words u and v to be equivalent, written $u \sim v$, if they have the same reduced form. This is an equivalence relation. The equivalence class of a word w will be denoted $[w]$.

Proposition 1 (Compatibility with multiplication). If $u \sim u'$ and $v \sim v'$, then $uv \sim u'v'$.

Proof. Reduce u and v separately to reduced words u_0 and v_0. Then the product uv reduces first to u_0v_0, and after that only cancellations crossing the boundary between u_0 and v_0 remain. The same process applied to $u'v'$ reaches the same intermediate word u_0v_0, because u' and v' have the same reduced forms as u and v. Hence uv and $u'v'$ have the same reduced form. □

4. The free group

Definition 3. The free group on S, denoted $F(S)$, is the set of equivalence classes of words in $S^{\pm}$, with multiplication

$$[u][v] = [uv].$$

The previous proposition says that this operation is well defined.

Theorem 4. $F(S)$ is a group. Its identity is the class of the empty word, and

$$[x_1x_2\cdots x_m]^{-1} = [x_m^{-1}\cdots x_2^{-1}x_1^{-1}].$$

Proof. Associativity follows from associativity of concatenation of words:

$$([u][v])[w] = [uv][w] = [(uv)w] = [u(vw)] = [u][vw] = [u]([v][w]).$$

The empty word acts as an identity because concatenating it changes nothing. Finally,

$$(x_1\cdots x_m)(x_m^{-1}\cdots x_1^{-1})$$

reduces completely to the empty word by cancelling from the middle outward; the reverse product reduces similarly. Thus the displayed reverse word represents the inverse. □

Example 5 (Free group on one generator). Let $S = \{a\}$. Every reduced word is a^n for a unique integer n. Therefore

$$F(a) \cong (\mathbb{Z}, +), \qquad a^n \longleftrightarrow n.$$

This is the only free group that is abelian, apart from the trivial free group.

4. The free group continued

Example 6 (Free group on two generators). In $F(a, b)$, the words ab and ba are distinct because both are reduced and unequal as strings. Thus $F(a, b)$ is nonabelian. The words

$$aba^{-1}, \qquad b^{-1}a^2b, \qquad [a, b] = aba^{-1}b^{-1}$$

are all reduced. No one of these is automatically equal to 1.

5. Why the word "free"?

The free group has no relations except those forced by the group axioms. The precise statement is a universal property.

Theorem 7 (Mapping property of free groups). Let $F(S)$ be the free group on S. For every group G and every function $f : S \to G$, there is a unique group homomorphism

$$\varphi : F(S) \to G$$

such that $\varphi(s) = f(s)$ for all $s \in S$.

6. Proof of the mapping property

Proof. Extend f to formal inverse letters by setting

$$f(s^{-1}) = f(s)^{-1}.$$

For a word $w = x_1 \cdots x_m$, define

$$\Phi(w) = f(x_1)f(x_2)\cdots f(x_m) \in G.$$

If a word is changed by one cancellation, say ss^{-1} is deleted, then Φ does not change because

$$f(s)f(s)^{-1} = 1.$$

Similarly $s^{-1}s$ maps to 1. Therefore equivalent words have the same image under Φ, so Φ descends to a well-defined map on equivalence classes:

$$\varphi([w]) = \Phi(w).$$

It is a homomorphism because

$$\varphi([u][v]) = \varphi([uv]) = \Phi(uv) = \Phi(u)\Phi(v) = \varphi([u])\varphi([v]).$$

It sends each generator s to $f(s)$ by construction. For uniqueness, every element of $F(S)$ is represented by a word in elements of S and their inverses. A homomorphism is forced to send

$$s_1^{\varepsilon_1} \cdots s_m^{\varepsilon_m} \quad \text{to} \quad f(s_1)^{\varepsilon_1} \cdots f(s_m)^{\varepsilon_m},$$

where $\varepsilon_i = \pm 1$. Hence no other homomorphism can have the same values on S. □

6. Proof of the mapping property continued

Example 8 (Evaluation into a concrete group). Let $F(a, b)$ be free on a, b, and let $G = S_3$. Choose

$$f(a) = (123), \qquad f(b) = (12).$$

Then the universal property gives a homomorphism $\varphi : F(a, b) \to S_3$. For instance,

$$\varphi(aba^{-1}b^{-1}) = (123)(12)(132)(12).$$

This is the commutator of (123) and (12) in S_3. Thus free groups allow us to evaluate formal words in any group once we assign values to the generators.

7. Relations as a normal subgroup

A relation is a word that we want to become the identity. If $R \subseteq F(S)$ is a set of words, define its normal closure

$$\langle\langle R \rangle\rangle = \bigcap \{N \triangleleft F(S) : R \subseteq N\}.$$

It is the smallest normal subgroup of $F(S)$ containing R. Equivalently, it is generated by all conjugates

$$grg^{-1}, \quad g \in F(S), \quad r \in R.$$

Normality is essential: if $r = 1$ in a quotient group, then every conjugate grg^{-1} must also be 1.

8. Presentations

Definition 9. Let $S = \{x_1, \ldots, x_n\}$ and let $R = \{r_1, \ldots, r_k\} \subseteq F(S)$. The group generated by S with relations $r_1 = 1, \ldots, r_k = 1$ is

$$\langle x_1, \ldots, x_n \mid r_1, \ldots, r_k \rangle = F(S)/\langle\langle r_1, \ldots, r_k \rangle\rangle.$$

A word represents the identity in this presented group exactly when it lies in the normal closure of the relators.

Example 10 (Cyclic groups).

$$C_n \cong \langle a \mid a^n \rangle.$$

Indeed, $F(a) \cong \mathbb{Z}$, and quotienting by the normal subgroup generated by a^n identifies exponents modulo n. Every element has the form a^i with $0 \leqslant i < n$.

8. Presentations continued

Example 11 (The infinite cyclic group).

$$\langle a \mid \rangle \cong \mathbb{Z}.$$

There are no relators, so the normal closure is trivial and the group is just $F(a)$.

Example 12 (The free abelian group of rank two).

$$\langle a, b \mid aba^{-1}b^{-1} \rangle \cong \mathbb{Z}^2.$$

The relation $aba^{-1}b^{-1} = 1$ is equivalent to $ab = ba$. Once a and b commute, every word can be rearranged to $a^m b^n$. Define

$$\theta : \langle a, b \mid [a, b] \rangle \to \mathbb{Z}^2, \qquad \theta(a) = (1, 0), \quad \theta(b) = (0, 1).$$

The map is surjective. The inverse sends (m, n) to $a^m b^n$, and this is well defined because the group is abelian after imposing the relation. Hence the two groups are isomorphic.

8. Presentations continued

Example 13 (Dihedral group). The symmetry group of a regular n-gon has presentation

$$D_n \cong \langle r, s \mid r^n, s^2, srsr \rangle.$$

The relation $srsr = 1$ is equivalent to $srs = r^{-1}$, or $sr = r^{-1}s$. Therefore every word can be rewritten with all s's on the right:

$$r^i \quad \text{or} \quad r^i s, \qquad 0 \leqslant i < n.$$

So the presented group has at most $2n$ elements. The actual rotations and reflections of a regular n-gon satisfy the three relations and form a group of order $2n$, so the presentation is complete.

9. Mapping property of quotient groups

Theorem 14 (Quotient mapping property). Let $\pi : G' \to G'/N$ be the quotient map, where $N \triangleleft G'$. If $\varphi : G' \to G$ is a homomorphism and $N \subseteq \ker \varphi$, then there is a unique homomorphism

$$\bar{\varphi} : G'/N \to G$$

such that $\bar{\varphi} \circ \pi = \varphi$.

Proof. Define

$$\bar{\varphi}(gN) = \varphi(g).$$

This is well defined: if $gN = hN$, then $h^{-1}g \in N \subseteq \ker \varphi$, hence $\varphi(h^{-1}g) = 1$, so $\varphi(g) = \varphi(h)$. It is a homomorphism because

$$\bar{\varphi}(gN \cdot hN) = \bar{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = \bar{\varphi}(gN)\bar{\varphi}(hN).$$

Uniqueness follows because every coset has the form $\pi(g) = gN$, and the condition $\bar{\varphi} \circ \pi = \varphi$ forces $\bar{\varphi}(gN) = \varphi(g)$. □

10. Presentations map to groups

Proposition 2 (Canonical map from a presentation). Let G be a group containing elements $x_1, \ldots, x_n$, and suppose the words $r_1, \ldots, r_k$ become the identity when evaluated at these elements. Then there is a canonical homomorphism

$$\psi : \langle x_1, \ldots, x_n \mid r_1, \ldots, r_k \rangle \longrightarrow G$$

sending the abstract generator x_i to the concrete element $x_i \in G$. It is surjective exactly when the concrete elements generate G.

Proof. By the mapping property of the free group, the assignment of the abstract generators to the concrete elements extends to a homomorphism $F(x_1, \ldots, x_n) \to G$. Each relator maps to 1, so the normal closure of the relators lies in the kernel. The quotient mapping property gives the desired map from the presented group. Its image is precisely the subgroup of G generated by the concrete elements. □

10. Presentations map to groups continued

If ψ is also injective, the displayed relations are called a complete set of relations. Equivalently, every relation among the chosen elements of G follows from the listed relators.

Example 15 (Tetrahedral setup). The rotational symmetry group T of a regular tetrahedron is generated by rotations x, y, z satisfying

$$x^3 = 1, \quad y^3 = 1, \quad z^2 = 1, \quad xyz = 1.$$

The presentation

$$\langle x, y, z \mid x^3, y^3, z^2, xyz \rangle$$

therefore maps onto T. To prove that it is exactly T, one must prove no additional hidden relations are present. Todd–Coxeter enumeration supplies this proof.

11. Changing presentations without changing the group

Some transformations of presentations are safe. The most useful for computations is eliminating a generator that is explicitly determined by the others.

Example 16 (Eliminating z in the tetrahedral presentation). Start with

$$\langle x, y, z \mid x^3, y^3, z^2, xyz \rangle.$$

The relation $xyz = 1$ implies $z = (xy)^{-1} = y^{-1}x^{-1}$. Since $z^2 = 1$, it is also common in this example to write $z = xy$ after using $z^{-1} = z$ and $xyz = 1$. Substituting $z = xy$ into $z^2 = 1$ gives

$$(xy)^2 = xyxy = 1.$$

Thus the tetrahedral presentation is equivalent to

$$\langle x, y \mid x^3, y^3, xyxy \rangle.$$

This two-generator presentation is much easier to use in coset enumeration.

11. Changing presentations without changing the group continued

Example 17 (A presentation for S_3). Let $x = (123)$ and $y = (12)$ in S_3. Then

$$x^3 = 1, \quad y^2 = 1, \quad yxy = x^{-1}.$$

The third relation is equivalent to $yxyx = 1$. Hence

$$S_3 \cong \langle x, y \mid x^3, y^2, yxyx \rangle.$$

To see this, the relations imply $yx = x^{-1}y = x^2y$, so every word reduces to one of

$$1,\ x,\ x^2,\ y,\ xy,\ x^2y.$$

Thus the presented group has at most six elements. Since the concrete permutations above satisfy the relations and generate a six-element group, the presentation is complete.

12. The word problem

For a presentation $G = \langle S \mid R \rangle$, the word problem asks whether a given word $w \in F(S)$ represents the identity in G, i.e. whether

$$w \in \langle\langle R \rangle\rangle.$$

If we can solve the word problem, then we can decide equality of arbitrary words because

$$w_1 = w_2 \text{ in } G \iff w_1 w_2^{-1} = 1 \text{ in } G.$$

For small finite presentations, Todd–Coxeter enumeration is one of the most useful practical tools.

13. Coset tables and the Todd--Coxeter idea

Let

$$G = \langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle$$

and let $H \leqslant G$ be generated by some words. The Todd–Coxeter algorithm tries to enumerate the right cosets

$$H,\ Hg_2,\ Hg_3, \dots$$

by assigning them labels $1, 2, 3, \dots$. A table records right multiplication by generators:

$$\text{entry } (i, x) = j \iff (Hg_i)x = Hg_j.$$

When inverse columns are included, the table must satisfy inverse consistency:

$$i^x = j \iff j^{x^{-1}} = i.$$

Each relator must trace a closed path from every row. If $r = x_{i_1} \cdots x_{i_m}$, then

$$i^r = i \quad \text{for every row } i.$$

13. Coset tables and the Todd--Coxeter idea continued

If h is a subgroup generator for H, then row 1 must satisfy

$$1^h = 1,$$

because $Hh = H$.

14. How entries are forced

Suppose the relation $r = xyxy = 1$ is being read from row i. If the table already tells us

$$i^x = a, \quad a^y = b, \quad i^{(xyxy)} = i,$$

then the remaining letters force b^x and $(b^x)^y$ in a way compatible with returning to i. In practice one works from both ends of a relation. For instance, if

$$i^x = a, \quad j^{y^{-1}} = i,$$

then the partial path may force an unknown middle entry to be j. If two different deductions force the same coset label to equal two labels, one merges the labels. Such a merge is called a coincidence.

Warning 2 (The main computational danger). A single wrong entry can make the table collapse incorrectly. In hand computations, every forced entry should be checked against inverse columns and every relator should be read from every row.

14. How entries are forced continued

Proposition 3 (What a completed table gives). A completed coset table gives permutations of the set of coset labels, one permutation for each generator. If every relator acts as the identity permutation and every subgroup generator fixes row 1, then the table defines a permutation representation of the presented group.

15. Worked example: the S3 presentation

Consider

$$G = \langle x, y \mid x^3, y^2, yxyx \rangle$$

and let $H = \langle y \rangle$. Since $y^2 = 1$, the subgroup H has order at most 2. We enumerate right cosets of H. Row 1 represents H itself, so $1^y = 1$. The relation $x^3 = 1$ suggests a cycle under x. The completed table is

coset	x	y
1	2	1
2	3	3
3	1	2

The corresponding permutations on $\{1, 2, 3\}$ are

$$x = (123), \qquad y = (23).$$

Check the relations:

$$x^3 = 1, \qquad y^2 = 1, \qquad yxyx = (23)(123)(23)(123) = 1.$$

Thus the table is compatible with the presentation.

Because y acts nontrivially on the cosets, $y \neq 1$ in G, so H has order 2. The table has three cosets, so

$$|G| = |H|[G : H] = 2 \cdot 3 = 6.$$

The concrete permutations $x = (123)$ and $y = (23)$ generate S_3, so

$$G \cong S_3.$$

16. Worked example: tetrahedral group

Use the two-generator tetrahedral presentation

$$G = \langle x, y \mid x^3, y^3, xyxy \rangle.$$

Let $H = \langle x \rangle$. A Todd–Coxeter enumeration gives four cosets with generator action

coset	x	y
1	1	2
2	3	3
3	4	1
4	2	4

Thus

$$x = (234), \qquad y = (123).$$

These permutations satisfy

$$x^3 = 1, \qquad y^3 = 1, \qquad (xy)^2 = 1.$$

Since x acts as a 3-cycle on the labels $2, 3, 4$, x has order 3 in the presented group. Hence $|H| = 3$. The table has four cosets, so

$$|G| = |H|[G : H] = 3 \cdot 4 = 12.$$

The rotational symmetry group of a tetrahedron also has order 12 and satisfies the same relations, so this proves that the presentation is complete. The displayed permutations generate A_4, so this also identifies the tetrahedral rotation group with A_4.

17. A collapse example

Small changes in relations can change a group dramatically. Consider

$$G = \langle x, y \mid x^3, y^3, yxyxy \rangle$$

and let $H = \langle y \rangle$. Compare this with the tetrahedral relation $xyxy = 1$. The relation $yxyxy = 1$ forces strong coincidences in the coset table. The enumeration collapses to a single coset, so $H = G$.

Since G is generated by y and $y^3 = 1$, the group has order at most 3. It is not forced to be trivial: there is a surjective homomorphism

$$G \to C_3, \qquad x \mapsto 1, \quad y \mapsto \bar{y},$$

where $\bar{y}$ is a generator of C_3. Indeed, the relator $yxyxy$ maps to $\bar{y}^3 = 1$. Therefore

$$G \cong C_3.$$

18. Why Todd--Coxeter proves finite presentations

Suppose a presentation maps onto a known finite group K. To prove the presentation is complete, it is enough to prove the presented group has at most $|K|$ elements. Coset enumeration does this by finding a subgroup H and an index $[G : H]$. If the same table also proves the order of H, then

$$|G| = |H|[G : H].$$

In the tetrahedral example, $H = \langle x \rangle$ has order 3 and the enumeration gives index 4, hence $|G| = 12$. Since the actual tetrahedral rotation group has order 12 and is generated by elements satisfying the relations, the surjection from the presented group to the tetrahedral group must be an isomorphism.

Warning 3 (Termination). Todd–Coxeter is powerful but not magic. For some presentations or subgroup choices, a hand enumeration may be very long, and for infinite-index subgroups it will not terminate with a finite table. The completed finite table is the certificate.

19. Practical checklist

When doing a Todd–Coxeter computation by hand:

1. Choose a subgroup H whose order is easy to control, often generated by one generator.
2. Start row 1 with all subgroup-generator words fixing row 1.
3. Add new coset names only when a generator sends a known row somewhere unknown.
4. Read every relator from every row, both forwards and backwards.
5. Whenever two labels are forced equal, merge them everywhere.
6. When the table is complete, translate generator columns into permutations.
7. Use $|G| = |H|[G : H]$ when H has known order.

20. Summary of the three sections

Topic	Main idea
Free group	Elements are reduced words. The only cancellations are adjacent inverse pairs. The mapping property says that any assignment of generators to a group extends uniquely to a homomorphism.
Relations	A presentation is a quotient of a free group by the normal closure of the relators. Listed relators become true, and all their conjugates become true automatically.
Completeness	A presented group maps onto any concrete group whose generators satisfy the relators. The relations are complete exactly when this map is injective.
Todd–Coxeter	Enumerate cosets of a subgroup using the relators. A completed coset table gives generator permutations and often computes the order of the group.

21. Further examples for practice

1. Prove that
$$\langle a, b \mid a^2, b^2, abab \rangle \cong C_2 \times C_2.$$
Hint: The relation $abab = 1$ says $ab = (ab)^{-1} = ba$ once $a^2 = b^2 = 1$.
2. Show that
$$\langle r, s \mid r^4, s^2, srsr \rangle$$
has exactly eight elements and identify it with the symmetry group of a square.
3. In $F(a, b)$, reduce the words
$$aba^{-1}ab^{-1}, \qquad ab^{-1}ba^{-1}, \qquad aba^{-1}b^{-1}.$$
Which of these reduce to the empty word?
4. Let
$$G = \langle x, y \mid x^2, y^3, (xy)^2 \rangle.$$
Use the substitution $s = x$, $r = xy$ to compare this with the usual presentation of S_3.

21. Further examples for practice continued

5. For
$$G = \langle x, y \mid x^3, y^3, xyxy \rangle,$$
verify directly from the permutation table $x = (234)$, $y = (123)$ that each relator acts trivially.

22. Conceptual takeaway

A presentation is a two-stage object:

$$\text{symbols} \longrightarrow \text{free group} \longrightarrow \text{quotient by relations.}$$

The free group stage remembers every word distinctly unless cancellation forces equality. The quotient stage imposes exactly the listed relations and their normal consequences. Todd–Coxeter then turns the abstract quotient into a finite permutation calculation whenever a manageable coset table can be completed.

B

课件中文翻译

本附录给出上述课件的全文中文翻译.翻译力求流畅可读而保持严谨; 数学名词按规范翻译, 首次出现的概念以括号标注英文; 课件中的人名 (如 Jiarui Fei, Todd–Coxeter) 一律保留英文.

路线图与引导问题

目的. 这些笔记解释如何从符号构造群. 第 7.9 节构造自由群 (free group): 其元素是字母表及其形式逆上的约化字 (reduced word). 第 7.10 节通过用正规子群 (normal subgroup) 对自由群取商来添加关系 (relation). 第 7.11 节给出一个实用的有限群检验: 用 Todd–Coxeter 方法枚举陪集 (coset).

引导问题. 设一个群由

$$G = \langle x_1, \dots, x_n \mid r_1 = 1, \dots, r_k = 1 \rangle$$

描述. 它的元素是什么? 它有限吗? 它是一个熟悉的群吗? 我们能否判定生成元中的两个字是否表示同一个元素? 自由群在施加关系之前回答了第一个问题; 商群编码了这些关系; 陪集枚举常常能回答有限的情形.

大纲.

1. 自由群
2. 群的展示 (presentation)
3. Todd–Coxeter 枚举
4. 总结与练习

1. 字与约化

设 S 是一个符号集合. 对每个 $s \in S$, 引入一个形式逆符号 (formal inverse symbol) s^{-1}. 令

$$S^{\pm} = S \cup S^{-1}.$$

一个字 (word) 是有限串 $w = x_1 x_2 \cdots x_m$, 其中每个 $x_i \in S^{\pm}$. 空字 (empty word) 记为 1. w 的长度 (length) 为 m.

约化 (cancellation) 是删除相邻符号 ss^{-1} 或 $s^{-1}s$. 若一个字不可能再约化, 则称其为约化字 (reduced word). 例如, 取 $S = \{a, b, c\}$,

$$w = abb^{-1}c^{-1}ca^{-1}b \quad \rightsquigarrow \quad aa^{-1}b \quad \rightsquigarrow \quad b.$$

约化字为 b. 相反, $aba^{-1}b^{-1}$ 已经是约化字. 它在自由群中不是单位元 (identity), 尽管在施加交换关系 (commutativity relation) $aba^{-1}b^{-1} = 1$ 之后它成为单位元.

警告 1. 像 $aba^{-1}b^{-1}$ 这样的字看起来在代数上很熟悉, 但现阶段符号并不交换. 在自由群中, 唯一的约化是相邻逆对的约化.

1. 字与约化 (续)

例 1 (两种看似不同的约化). 字

$$w = abb^{-1}c^{-1}cb$$

可以先约化 bb^{-1}, 也可以先约化 $c^{-1}c$. 无论哪种方式, 在所有可能的约化之后, 结果都是 ab. 这说明了关键定理: 最终的约化字与约化过程中所做的选择无关.

2. 约化形式的唯一性

定理 2 (约化形式的唯一性). 每个字都有唯一的约化形式.

证明. 存在性是显然的, 因为每次约化使字缩短两个字母, 所以约化序列必然终止. 终止给出至少一个约化字.

唯一性: 对原字的长度 m 归纳. 若 w 已约化, 则无事可证. 否则在 w 中选取一个相邻可约对, 设

$$w = \cdots xx^{-1} \cdots .$$

设 w_0 是从 w 经某个约化序列得到的任意约化字. 我们证明, 这个 w_0 可以先约化所显示的 xx^{-1} 对而得到.

若所显示的这一对在给定约化序列中最终是作为一对被约化的, 则可以把这次约化交换到序列最前: 它之前的约化都发生在这两个字母之外, 或缩短字的无关部分, 先约化 xx^{-1} 之后仍得到相同的最终结果.

若这两个字母不是作为一对被约化, 则由于 w_0 是约化字, 它们中至少有一个最终必须与相邻的逆元约化. 涉及这两个字母中任意一个的第一次约化, 必然发生在下列两种三字母块之一中:

$$x^{-1}xx^{-1} \quad \text{或} \quad xx^{-1}x.$$

无论哪种情形, 约化相邻对与约化原来的中间对给出完全相同的中间字. 例如,

$$x^{-1}xx^{-1} \longrightarrow x^{-1},$$

无论先约化前两个字母还是后两个字母. 于是约化序列可以再次修改, 使所选的对 xx^{-1} 先被约化.

在这次首次约化之后, 字的长度为 $m-2$. 由归纳假设, 较短的字有唯一的约化形式. 因此 w 的所有约化形式一致. □

3. 字的等价

定义两个字 u 与 v 等价 (equivalent), 记作 $u \sim v$, 若它们有相同的约化形式. 这是一个等价关系 (equivalence relation). 字 w 的等价类 (equivalence class) 记为 $[w]$.

命题 1 (与乘法的相容性). 若 $u \sim u'$ 且 $v \sim v'$, 则 $uv \sim u'v'$.

证明. 把 u 与 v 分别约化为约化字 u_0 与 v_0. 于是乘积 uv 先约化为 u_0v_0, 之后只剩下跨越 u_0 与 v_0 边界的约化. 对 $u'v'$ 施加同样的过程, 会到达相同的中间字 u_0v_0, 因为 u' 与 v' 和 u 与 v 有相同的约化形式. 因此 uv 与 $u'v'$ 有相同的约化形式. □

4. 自由群

定义 3. S 上的自由群, 记作 $F(S)$, 是 $S^{\pm}$ 中字的等价类之集, 乘法为

$$[u][v] = [uv].$$

前一命题说明这个运算是良定义的 (well defined).

定理 4. $F(S)$ 是一个群. 其单位元是空字的等价类, 且

$$[x_1 x_2 \cdots x_m]^{-1} = [x_m^{-1} \cdots x_2^{-1} x_1^{-1}].$$

证明. 结合律来自字拼接的结合律:

$$([u][v])[w] = [uv][w] = [(uv)w] = [u(vw)] = [u][vw] = [u]([v][w]).$$

空字充当单位元, 因为拼接它不改变任何东西. 最后,

$$(x_1 \cdots x_m)(x_m^{-1} \cdots x_1^{-1})$$

从中间向外约化, 完全约化为空字; 逆序乘积类似地约化. 因此所显示的逆序字代表逆元. □

例 5 (单生成元上的自由群). 设 $S = \{a\}$. 每个约化字都是 a^n, 其中 n 是唯一的整数. 因此

$$F(a) \cong (\mathbb{Z}, +), \qquad a^n \longleftrightarrow n.$$

这是除平凡自由群之外唯一可交换的自由群.

4. 自由群 (续)

例 6 (双生成元上的自由群). 在 $F(a, b)$ 中, 字 ab 与 ba 不同, 因为二者都已约化且作为字符串不相等. 因此 $F(a, b)$ 是非 Abel 群 (nonabelian). 字

$$aba^{-1}, \qquad b^{-1}a^2b, \qquad [a, b] = aba^{-1}b^{-1}$$

都已约化. 它们中没有一个自动等于 1.

5. 为什么称为" 自由"?

自由群除了群公理所强制的那些关系之外没有其他关系. 精确的表述是一个泛性质 (universal property).

定理 7 (自由群的映射性质). 设 $F(S)$ 是 S 上的自由群. 对每个群 G 与每个函数 $f : S \to G$, 存在唯一的群同态 (homomorphism)

$$\varphi : F(S) \to G$$

使得对所有 $s \in S$ 都有 $\varphi(s) = f(s)$.

6. 映射性质的证明

证明. 把 f 延拓到形式逆字母, 令

$$f(s^{-1}) = f(s)^{-1}.$$

对字 $w = x_1 \cdots x_m$, 定义

$$\Phi(w) = f(x_1)f(x_2)\cdots f(x_m) \in G.$$

若一个字因一次约化而改变, 例如删去 ss^{-1}, 则 Φ 不变, 因为

$$f(s)f(s)^{-1} = 1.$$

类似地, $s^{-1}s$ 映到 1. 因此等价字在 Φ 下有相同的像, 于是 Φ 下降到等价类上的良定义映射:

$$\varphi([w]) = \Phi(w).$$

它是同态, 因为

$$\varphi([u][v]) = \varphi([uv]) = \Phi(uv) = \Phi(u)\Phi(v) = \varphi([u])\varphi([v]).$$

按构造, 它把每个生成元 s 送到 $f(s)$. 唯一性: $F(S)$ 的每个元素都由 S 的元素及其逆组成的字表示. 一个同态被迫把

$$s_1^{\varepsilon_1}\cdots s_m^{\varepsilon_m} \quad \text{送到} \quad f(s_1)^{\varepsilon_1}\cdots f(s_m)^{\varepsilon_m},$$

其中 $\varepsilon_i = \pm 1$. 因此不可能有其他同态在 S 上取相同的值. □

6. 映射性质的证明 (续)

例 8 (在具体群中求值). 设 $F(a,b)$ 在 a,b 上自由, 并设 $G = S_3$. 取

$$f(a) = (123), \qquad f(b) = (12).$$

于是泛性质给出同态 $\varphi : F(a,b) \to S_3$. 例如,

$$\varphi(aba^{-1}b^{-1}) = (123)(12)(132)(12).$$

这是 (123) 与 (12) 在 S_3 中的换位子 (commutator). 因此, 一旦给生成元赋值, 自由群就允许我们在任意群中求形式字的值.

7. 关系作为正规子群

关系 (relation) 是我们希望其成为单位元的字. 若 $R \subseteq F(S)$ 是字的集合, 定义其正规闭包 (normal closure)

$$\langle\langle R \rangle\rangle = \bigcap \{ N \triangleleft F(S) : R \subseteq N \}.$$

它是 $F(S)$ 中包含 R 的最小的正规子群. 等价地, 它由所有共轭 (conjugate)

$$grg^{-1}, \quad g \in F(S), \quad r \in R$$

生成. 正规性是本质的: 若在商群 (quotient group) 中 $r = 1$, 则每个共轭 grg^{-1} 也必须是 1.

8. 群的展示

定义 9. 设 $S = \{x_1, \dots, x_n\}$, $R = \{r_1, \dots, r_k\} \subseteq F(S)$. 由生成元 S 与关系 $r_1 = 1, \dots, r_k = 1$ 生成的群是

$$\langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle = F(S)/\langle\langle r_1, \dots, r_k \rangle\rangle.$$

一个字在这个展示群 (presented group) 中表示单位元, 当且仅当它位于关系子 (relator) 的正规闭包中.

例 10 (循环群).

$$C_n \cong \langle a \mid a^n \rangle.$$

事实上, $F(a) \cong \mathbb{Z}$, 对由 a^n 生成的正规子群取商, 指数模 n 相等. 每个元素都具有 a^i 的形式, 其中 $0 \leqslant i < n$.

8. 群的展示 (续)

例 11 (无限循环群).

$$\langle a \mid \rangle \cong \mathbb{Z}.$$

没有关系子, 所以正规闭包平凡, 群就是 $F(a)$.

例 12 (秩二自由 Abel 群).

$$\langle a, b \mid aba^{-1}b^{-1} \rangle \cong \mathbb{Z}^2.$$

关系 $aba^{-1}b^{-1} = 1$ 等价于 $ab = ba$. 一旦 a 与 b 交换, 每个字都可以重排为 $a^m b^n$. 定义

$$\theta : \langle a, b \mid [a, b] \rangle \to \mathbb{Z}^2, \qquad \theta(a) = (1, 0), \quad \theta(b) = (0, 1).$$

该映射是满射. 逆映射把 (m, n) 送到 $a^m b^n$, 由于施加关系后群是 Abel 群, 这是良定义的. 因此两个群同构.

8. 群的展示 (续)

例 13 (二面体群). 正 n 边形的对称群有展示

$$D_n \cong \langle r, s \mid r^n, s^2, srsr \rangle.$$

关系 $srsr = 1$ 等价于 $srs = r^{-1}$, 或 $sr = r^{-1}s$. 因此每个字都可以重写, 使所有 s 都在右边:

$$r^i \quad \text{或} \quad r^i s, \qquad 0 \leqslant i < n.$$

所以展示群至多有 $2n$ 个元素. 正 n 边形的实际旋转与反射满足这三个关系, 并构成一个 $2n$ 阶群, 因此展示是完备的.

9. 商群的映射性质

定理 14 (商映射性质). 设 $\pi : G' \to G'/N$ 是商映射, 其中 $N \triangleleft G'$. 若 $\varphi : G' \to G$ 是同态且 $N \subseteq \ker \varphi$, 则存在唯一的同态

$$\bar{\varphi} : G'/N \to G$$

使得 $\bar{\varphi} \circ \pi = \varphi$.

证明. 定义

$$\bar{\varphi}(gN) = \varphi(g).$$

这是良定义的: 若 $gN = hN$, 则 $h^{-1}g \in N \subseteq \ker \varphi$, 因此 $\varphi(h^{-1}g) = 1$, 故 $\varphi(g) = \varphi(h)$. 它是同态, 因为

$$\bar{\varphi}(gN \cdot hN) = \bar{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = \bar{\varphi}(gN)\bar{\varphi}(hN).$$

唯一性: 每个陪集 (coset) 都具有形式 $\pi(g) = gN$, 条件 $\bar{\varphi} \circ \pi = \varphi$ 迫使 $\bar{\varphi}(gN) = \varphi(g)$. □

10. 展示映射到群

命题 2 (展示的典范映射). 设 G 是含元素 $x_1, \dots, x_n$ 的群, 并假设字 $r_1, \dots, r_k$ 在这些元素处求值时成为单位元. 则存在典范同态 (canonical homomorphism)

$$\psi : \langle x_1, \dots, x_n \mid r_1, \dots, r_k \rangle \longrightarrow G$$

把抽象生成元 x_i 送到具体元素 $x_i \in G$. 当且仅当这些具体元素生成 G 时它是满射.

证明. 由自由群的映射性质, 把抽象生成元赋给具体元素的指派延拓为从 $F(x_1, \dots, x_n)$ 到 G 的同态. 每个关系子映到 1, 所以关系子的正规闭包位于核 (kernel) 中. 商映射性质给出从展示群出发的所求映射. 其像恰为具体元素生成的 G 的子群. □

10. 展示映射到群 (续)

若 ψ 还是单射, 则所列关系称为完备关系组 (complete set of relations). 等价地, G 的所选元素之间成立的每个关系都可以从所列关系子推出.

例 15 (四面体的设置). 正四面体的旋转对称群 T 由旋转 x, y, z 生成, 满足

$$x^3 = 1, \quad y^3 = 1, \quad z^2 = 1, \quad xyz = 1.$$

因此展示

$$\langle x, y, z \mid x^3, y^3, z^2, xyz \rangle$$

满射到 T. 要证明它恰好是 T, 必须证明不存在额外的隐藏关系. Todd–Coxeter 枚举提供了这个证明.

11. 不改变群地改变展示

展示的某些变换是安全的. 对计算最有用的是消去一个由其他生成元明确确定的生成元.

例 16 (在四面体展示中消去 z). 从

$$\langle x, y, z \mid x^3, y^3, z^2, xyz \rangle$$

出发. 关系 $xyz = 1$ 蕴含 $z = (xy)^{-1} = y^{-1}x^{-1}$. 由于 $z^2 = 1$, 本例中也常利用 $z^{-1} = z$ 与 $xyz = 1$ 写 $z = xy$. 把 $z = xy$ 代入 $z^2 = 1$, 得到

$$(xy)^2 = xyxy = 1.$$

因此四面体展示等价于

$$\langle x, y \mid x^3, y^3, xyxy \rangle.$$

这个双生成元展示在陪集枚举中更容易使用.

11. 不改变群地改变展示 (续)

例 17 (S_3 的一个展示). 设 $x = (123), y = (12) \in S_3$. 则

$$x^3 = 1, \quad y^2 = 1, \quad yxy = x^{-1}.$$

第三个关系等价于 $yxyx = 1$. 因此

$$S_3 \cong \langle x, y \mid x^3, y^2, yxyx \rangle.$$

要看出这一点, 关系蕴含 $yx = x^{-1}y = x^2y$, 所以每个字都约化为

$$1,\ x,\ x^2,\ y,\ xy,\ x^2y$$

之一. 因此展示群至多有六个元素. 由于上面的具体置换满足这些关系并生成一个六元群, 展示是完备的.

12. 字问题

对展示 $G = \langle S \mid R \rangle$, 字问题 (word problem) 询问: 给定的字 $w \in F(S)$ 是否表示 G 中的单位元, 即是否

$$w \in \langle\langle R \rangle\rangle.$$

若我们能解字问题, 则能判定任意字的相等性, 因为

$$w_1 = w_2 \text{ in } G \iff w_1 w_2^{-1} = 1 \text{ in } G.$$

对小的有限展示, Todd–Coxeter 枚举是最有用的实用工具之一.

13. 陪集表与 Todd--Coxeter 思想

设

$$G = \langle x_1, \ldots, x_n \mid r_1, \ldots, r_k \rangle$$

并设 $H \leqslant G$ 由某些字生成. Todd–Coxeter 算法试图通过给它们编号 $1, 2, 3, \ldots$ 来枚举右陪集

$$H,\ Hg_2,\ Hg_3, \ldots$$

一张表记录乘以生成元的右乘:

$$\text{表项}(i, x) = j \iff (Hg_i)x = Hg_j.$$

当包含逆列时, 表必须满足逆一致性 (inverse consistency):

$$i^x = j \iff j^{x^{-1}} = i.$$

每个关系子必须从每一行追踪一条闭合路径. 若 $r = x_{i_1} \cdots x_{i_m}$, 则

$$i^r = i \quad \text{对每一行} i.$$

13. 陪集表与 Todd--Coxeter 思想 (续)

若 h 是 H 的子群生成元, 则第 1 行必须满足

$$1^h = 1,$$

因为 $Hh = H$.

14. 条目如何被强制

假设正在从第 i 行读取关系 $r = xyxy = 1$. 若表已经告诉我们

$$i^x = a, \quad a^y = b, \quad i^{(xyxy)} = i,$$

则剩余字母以与回到 i 相容的方式强制 b^x 与 $(b^x)^y$ 的值. 实践中从关系的两端同时工作. 例如, 若

$$i^x = a, \quad j^{y^{-1}} = i,$$

则部分路径可能强制某个未知的中间条目等于 j. 若两个不同的推导强制同一个陪集标号等于两个标号, 则合并这两个标号. 这样的合并称为重合 (coincidence).

警告 2 (主要的计算危险). 单个错误的条目可能使表错误地崩塌. 手算中, 每个被强制的条目都应检查逆列, 每个关系子都应从每一行读取.

14. 条目如何被强制 (续)

命题 3 (完备的表给出什么). 一张完备的陪集表给出陪集标号集合上的置换 (permutation), 每个生成元一个. 若每个关系子都作为恒等置换作用, 且每个子群生成元都固定第 1 行, 则这张表定义了展示群的一个置换表示 (permutation representation).

15. 工作示例: S3 的展示

考虑

$$G = \langle x, y \mid x^3, y^2, yxyx \rangle$$

并设 $H = \langle y \rangle$. 由于 $y^2 = 1$, 子群 H 的阶至多为 2. 我们枚举 H 的右陪集. 第 1 行代表 H 本身, 所以 $1^y = 1$. 关系 $x^3 = 1$ 提示在 x 下有一个轮换. 完备的表是

陪集	x	y
1	2	1
2	3	3
3	1	2

相应的置换为

$$x = (123), \qquad y = (23).$$

检验关系:

$$x^3 = 1, \qquad y^2 = 1, \qquad yxyx = (23)(123)(23)(123) = 1.$$

因此该表与展示相容.

因为 y 在陪集上非平凡地作用, G 中 $y \neq 1$, 所以 H 的阶为 2. 表有三个陪集, 所以

$$|G| = |H|[G : H] = 2 \cdot 3 = 6.$$

具体置换 $x = (123)$ 与 $y = (23)$ 生成 S_3, 所以

$$G \cong S_3.$$

16. 工作示例: 四面体群

使用双生成元四面体展示

$$G = \langle x, y \mid x^3, y^3, xyxy \rangle.$$

设 $H = \langle x \rangle$. 一次 Todd–Coxeter 枚举给出四个陪集及生成元作用

陪集	x	y
1	1	2
2	3	3
3	4	1
4	2	4

于是

$$x = (234), \qquad y = (123).$$

这些置换满足

$$x^3 = 1, \qquad y^3 = 1, \qquad (xy)^2 = 1.$$

由于 x 在标号 $2, 3, 4$ 上作为 3-轮换作用, x 在展示群中的阶为 3. 因此 $|H| = 3$. 表有四个陪集, 所以

$$|G| = |H|[G : H] = 3 \cdot 4 = 12.$$

正四面体的旋转对称群也阶为 12 并满足同样的关系, 因此这证明展示是完备的. 所示的置换生成 A_4, 因此这也把四面体旋转群等同于 A_4.

17. 一个崩塌的例子

关系的小改动可以剧烈地改变一个群. 考虑

$$G = \langle x, y \mid x^3, y^3, yxyxy \rangle$$

并设 $H = \langle y \rangle$. 把它与四面体关系 $xyxy = 1$ 比较. 关系 $yxyxy = 1$ 在陪集表中强制强烈的重合. 枚举崩塌为单个陪集, 所以 $H = G$.

由于 G 由 y 生成且 $y^3 = 1$, 群的阶至多为 3. 它并不被迫为平凡群: 存在满射同态

$$G \to C_3, \qquad x \mapsto 1, \quad y \mapsto \bar{y},$$

其中 $\bar{y}$ 是 C_3 的生成元. 事实上, 关系子 $yxyxy$ 映到 $\bar{y}^3 = 1$. 因此

$$G \cong C_3.$$

18. 为什么 Todd--Coxeter 能证明有限展示

假设一个展示满射到已知的有限群 K. 要证明展示完备, 只需证明展示群至多有 $|K|$ 个元素. 陪集枚举通过找到子群 H 与指数 $[G:H]$ 做到这一点. 若同一张表还证明了 H 的阶, 则

$$|G| = |H|[G:H].$$

在四面体例子中, $H = \langle x \rangle$ 的阶为 3, 枚举给出指数 4, 因此 $|G| = 12$. 由于实际四面体旋转群的阶为 12 且由满足关系的元素生成, 从展示群到四面体群的满射必为同构.

警告 3 (终止性). Todd–Coxeter 强大但并非魔术. 对某些展示或子群选择, 手算枚举可能非常长, 而对无限指数的子群, 它不会以有限表终止. 完备的有限表就是证书.

19. 实用清单

手算 Todd–Coxeter 计算时:

1. 选择阶容易控制的子群 H, 通常由一个生成元生成.
2. 第 1 行以所有子群生成元字固定第 1 行开始.
3. 仅当生成元把已知行送到未知处时, 才添加新的陪集名.
4. 从每一行正反两个方向读取每个关系子.
5. 每当两个标号被强制相等, 处处合并它们.
6. 表完备后, 把生成元列翻译为置换.
7. 当 H 的阶已知时, 使用 $|G| = |H|[G:H]$.

20. 三节内容总结

主题	主要思想
自由群	元素是约化字. 唯一的约化是相邻逆对. 映射性质说, 生成元到群的任何赋值都唯一地延拓为同态.
关系	展示是自由群对关系子正规闭包的商. 所列关系子变为真, 且其全部共轭自动变为真.
完备性	展示群满射到任何其生成元满足关系子的具体群. 当且仅当该映射单射时关系完备.
Todd–Coxeter	用关系子枚举子群的陪集. 完备的陪集表给出生成元置换, 并常常算出群的阶.

21. 供练习的更多例子

1. 证明
$$\langle a, b \mid a^2, b^2, abab \rangle \cong C_2 \times C_2.$$
提示:关系 $abab = 1$ 说明, 一旦 $a^2 = b^2 = 1$, 就有 $ab = (ab)^{-1} = ba$.

2. 证明
$$\langle r, s \mid r^4, s^2, srsr\rangle$$
恰好有八个元素,并将其等同于正方形的对称群.
3. 在 $F(a,b)$ 中约化字
$$aba^{-1}ab^{-1}, \qquad ab^{-1}ba^{-1}, \qquad aba^{-1}b^{-1}.$$
其中哪些约化为空字?
4. 设
$$G = \langle x, y \mid x^2, y^3, (xy)^2\rangle.$$
用代换 $s = x$, $r = xy$ 把它与 S_3 的通常展示比较.

21. 供练习的更多例子 (续)

5. 对
$$G = \langle x, y \mid x^3, y^3, xyxy\rangle,$$
直接从置换表 $x = (234)$, $y = (123)$ 验证每个关系子平凡作用.

22. 概念要点

展示是一个两阶段对象:

$$\text{符号} \longrightarrow \text{自由群} \longrightarrow \text{按关系取商}.$$

自由群阶段在约化强制相等之前记住每一个字. 商阶段恰好施加所列出的关系及其正规推论. 每当能够完成一张可管理的陪集表时, Todd–Coxeter 就把抽象商转化为有限的置换计算.