Matemática Universitária N. 7, Junho de 1988, 77 - 120.

Alguns Procedimentos Computacionais Para Grupos Dados Por Uma Apresentação Finita

Joachim Neubüser
Lehrstuhl D für Mathematik
RWTH Aachen, 5100 Aachen
Alemanha Ocidental

Said Sidki
Departamento de Matemática
Universidade de Brasília
70919 - Brasília DF
Brasil

0. Introdução

Um título alternativo para este artigo poderia ser: "Qual é a natureza desse grupo?". Nosso interesse principal é em grupos que nos são apresentados como gerados por um conjunto de poucos elementos e por algumas das relações que entre eles valem. Em alguns casos trata-se das permutações dos vértices de um grafo, em outros das matrizes que descrevem os automorfismos de códigos lineares, em outros ainda das classes de homotopias de um nó (veja, por exemplo, [Hac 87]).

Apesar da simplicidade dos axiomas que definem a noção de grupo e da abundância de informações sobre grandes classes de grupos, é freqüente a frustração causada pela escassez de métodos que lidam com grupos descritos por um pequeno conjunto de geradores e por algumas relações existentes entre eles. O que falta nos textos de maior uso em álgebra clássica e teoria dos grupos é o análogo dos métodos numéricos em equações diferenciais. Todavia, esses métodos computacionais na teoria dos grupos foram desenvolvidos ao longo dos anos sob influência de problemas externos e também internos, especialmente pela necessidade de classificar

grupos finitos simples e pelo problema dos grupos de Burnside.

Devemos ressaltar que os métodos computacionais presentes neste artigo se baseiam numa análise cuidadosa dos aspectos algorítmicos das teorias conhecidas. Além disso, é preciso assinalar que a implementação desses algoritmos tornou-se possível de uma forma significativa graças ao advento da tecnologia dos computadores.

Vamos apresentar neste artigo alguns métodos computacionais conhecidos para investigar os grupos dados por geradores e relações, comentaremos suas bases teóricas e os ilustraremos com exemplos.

Fizemos um esforço para reduzir os requisitos ao mínimo, e desenvolvemos alguns dos cálculos detalhadamente. O leitor que quiser estudar este tópico a fundo poderá conhecer a situação atual do assunto em [Atk 84].

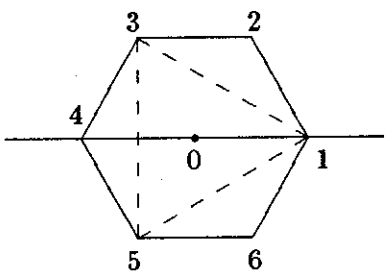
O primeiro autor expressa seus agradecimentos às instituições brasileiras, particularmente à Universidade de Brasília, pelo acolhimento quando proferiu, a convite do CNPq, conferências sobre tópicos relacionados aos que estão aqui expostos.

Índice

1. Grupos Livres e Apresentações

A identificação de um grupo através de seus geradores e relações se assemelha a uma história de detetive, onde as pistas disponíveis são poucas mas suficientes para identificar o culpado.

Como exemplo, consideremos D_{12} e D_6, os grupos das simetrias euclidianas do hexágono regular 123456, e do triângulo 135.



Por contagem direta, sabemos que D_{12} tem doze elementos e D_6 tem seis elementos. Chamemos de A a rotação anti-horária de $\frac{2\pi}{6}$ ao redor de 0, de A_2 a rotação A^2 e de B a reflexão sobre a linha 14. Então A e B são simetrias do hexágono, e A_2, B são simetrias do triângulo. Observemos que

$$A^6 = 1, \qquad B^2 = 1, \qquad B^{-1}AB = A^{-1},$$

e

$$A_2^3 = 1, \qquad B^2 = 1, \qquad B^{-1}A_2B = A_2^{-1}.$$

De $A_2^3 = 1$, segue $(A_2^3)^2 = A_2^6 = 1$.

A relação $B^{-1}AB = A^{-1}$ implica, para quaisquer inteiros $i, j \geq 0$ que

$$B^{-j}AB^j = B^{-1}(\cdots B^{-1}(B^{-1}AB)B\cdots)B = A^{(-1)^j},$$

e

$$B^{-j}A^iB^j = (B^{-j}AB^j)^i = A^{(-1)^j \cdot i},$$

quer dizer,

$$A^iB^j = B^jA^{(-1)^j \cdot i},$$

o que permite o transporte de B^j da direita para a esquerda de A^i. Os elementos do subgrupo H de D_{12} gerado por A e B têm a forma B^jA^i com $0 < i \leq 6$, $0 \leq j < 2$, e pode–se ver facilmente que essa forma é única; isto é, temos uma *forma normal* para os elementos de H.. Decorre que H tem doze elementos e portanto $H = D_{12}$. Da mesma forma mostramos que D_6 é gerado por A_2 e B.

Suponhamos agora que a informação que temos sobre um determinado grupo é de que ele é gerado por dois elementos a e b sujeitos às relações

$$a^6 = 1, \quad b^2 = 1, \quad b^{-1}ab = a^{-1}.$$

Este grupo pode ser um dos suspeitos D_{12} ou D_6 disfarçado. Pode–se identificà-lo, a menos de um isomorfismo, com D_{12}? Ou talvez D_6? Responder a esse tipo de pergunta requer uma introdução formal do conceito de *grupos livres* e de *apresentação de um grupo.*

Seja $X = \{x_1, \ldots, x_n, x_1^{-1} \cdots x_n^{-1}\}$ um conjunto de $2n$ elementos diferentes. Uma sequência finita $(y_1, \ldots, y_k)$ com $y_i \in X$ tal que dois elementos consecutivos não sejam da forma x_i, x_i^{-1} ou x_i^{-1}, x_i, assim como a sequência vazia ( ), é chamada uma "palavras reduzida" $w(x_i)$. Pode–se provar que o conjunto de todas as palavras reduzidas é um grupo, se definimos a "multiplicação" de duas sequências pela sua concatenação:

$$(y_1, \ldots, y_k)(y_{k+1}, \ldots, y_\ell) = (y_1, \ldots, y_k, y_{k+1}, \ldots, y_\ell)$$

após a remoção de todos os pares consecutivos da forma x_i, x_i^{-1} e x_i^{-1}, x_i. A parte mais importante dessa demonstração é mostrar que se chega ao mesmo resultado qualquer que seja a ordem

na qual as remoções são feitas. A sequência vazia é obviamente o elemento neutro desse grupo e o inverso de uma sequência se constrói invertendo-a e substituindo x_i por x_i^{-1}, e x_i^{-1} por x_i. Esse grupo é gerado pelas sequências (x_i), $i = 1, \ldots, n$. Escreveremos apenas o "produto formal" $y_1 y_2 \cdots y_k$ para indicar a sequência $(y_1, \ldots, y_k)$ com $y_i \in X$, e 1 para indicar a sequência vazia ( ). Esse grupo é chamado o *grupo livre* F_n de posto n, gerado livremete por $x_1, \ldots, x_n$.

Seja agora G um grupo qualquer gerado pelo conjunto $\{g_1, \ldots, g_n\}$. O fato de cada elemento de F_n ter uma única forma reduzida nos geradores $x_1, \ldots, x_n$, nos permite estender unicamente a função $\phi : x_i \mapsto g_i$ a um epimorfismo ϕ de F_n para G. Então pelo teorema geral dos homomorfismos, G é isomorfo ao grupo quociente de F_n pelo núcleo de ϕ. O núcleo $\ker \phi$ é formado pelas palavras $r(x_i)$ que, ao substituirmos suas "variáveis" x_i pelos g_i resultam nos "valores" $\phi(r(x_i)) = 1$, o elemento neutro de G. Dizemos então, que os elementos $r(x_i)$ são os "relatores" correspondentes às relações $r(g_i) = 1$ para o conjunto de geradores $\{g_i\}$ de G.

Qualquer subconjunto $R = \{r_j(x_i)\}$ de $\ker \phi$ cujo fecho normal (o menor subgrupo normal que contém R) em F_n é $\ker \phi$ é chamado um *conjunto definidor de relatores* de G com respeito ao conjunto gerator $\{g_i\}$, e o correspondente conjunto de relações $\{r_j(g_i) = 1\}$ é um *conjunto definidor de relações.*

Um conjunto de geradores juntamente com um conjunto definidor de relações (relatores) é chamado uma *apresentação* de um grupo G. Este grupo se diz *finitamente apresentado,* se tanto o conjunto dos geradores quanto o conjunto definidor de relações são finitos.

Voltemos agora a questão de saber se os geradores a e b junto com suas relações definidoras $a^6 = 1$, $b^2 = 1$, $b^{-1}ab = a^{-1}$ formam ou não uma apresentação para D_{12}. Em outras palavras, o grupo quociente do grupo livre F_2 pelo fecho normal N de $\{x_1^6, x_2^2, x_2^{-1}x_1x_2x_1\}$ é isomorfo a D_{12}? O núcleo do epimorfismo $\phi : F_2 \to D_{12}$ definido por $\phi : x_1 \mapsto A$, $x_2 \mapsto B$ contém x_1^6, x_2^2 ,$x_2^{-1}x_1x_2x_1$. Será que N é igual a $\ker \phi$? Aqui repetimos os cálculos feitos para a forma normal dos elementos em D_{12} no

caso de F_2/N o grupo gerado por Nx_1 e Nx_2 e chegamos a conclusão que F_2/N tem no máximo 12 elementos. Como, por outro lado, $N \subseteq \ker\phi$, o número de elementos de F_2/N é múltiplo de 12. Segue-se portanto que $N = \ker\phi$.

Antes de continuar, façamos duas observação:

(i) Um grupo não trivial tem muitos conjuntos de geradores e a cada um desses podem corresponder muitos conjuntos definidores de relação diferentes.

(ii) Podemos inverter o processo descrito acima. Seja $W = \{w_j(x_i)\}$ um conjunto arbitrário de elementos de F_n e N o fecho normal de W. Então $\{w_j(x_i)\}$ é um conjunto definidor de relatores para F_n/N. Portanto qualquer apresentação define (a menos de um isomorfismo) algum grupo. Tais apresentações são de fato usadas frequentemente em alguns ramos da Matemática, como na Topologia (ver [Hac 87]), para descrever grupos que de outra forma seriam pouco accessíveis.

Este era o caso, por exemplo, da seguinte classe de apresentações:

$$C_q = \langle a, b \mid aba^{-2}bab^{-1} = 1,\ a(b^{-1}a^3b^{-1}a^{-3})^q = 1\rangle,$$

que foi enviada a um de nós em novembro de 1984 por A. Cavicchioli. Apesar da questão original (se os C_q e $C_{q'}$ não são isomorfos para $q \neq q'$) já ter sido respondida por meios diferentes (ver [Cav 86]) tem-se aqui um bom exemplo para ilustrar os métodos computacionais.

Essa solicitação sobre a classe dos C_q se encaixa nos problemas colocados por Max Dehn em 1911 [Deh 11] sobre a existência de um algoritmo universal que pudesse responder a três questões sobre a classe FP dos grupos finitamente apresentados. Sejam G_1 e G_2 grupos FP e $\phi_i : F_{n_i} \to G_i$ $(i = 1, 2)$ os epimorfismos que fornecem apresentações finitas para esses grupos,

1. **(O Problema de Palavra).** dado $w \in F_{n_1}$, decidir se w pertence ou não ao $\ker\phi_1$,

2. **(O Problema de Conjugação).** dados $u, v \in F_{n_1}$, decidir

se $\phi_1(u)$ e $\phi_1(v)$ são ou não conjugados em G_1 (isto é, se existe $g \in G_1$ tal que $\phi(u) = g^{-1}\phi(v)g$),

3. **(O Problema do Isomorfismo).** decidir se G_1 e G_2 são ou não isomorfos.

2. Grupos Abelianos e o Algoritmo dos Divisores Elementares

2.1. A decomposição canônica de grupos abelianos finitamente apresentados tem uma demonstração algorítmica que permite uma fácil implementação e leva a uma resposta positiva aos problemas de Dehn da palavra e do isomorfismo, para esta classe específica de grupos, (aqui, obviamente, o problema da conjugação e da palavra são equivalentes).

Seja A um grupo abeliano gerado pelo conjunto $\{a_1, a_2, \ldots, a_n\}$ satisfazendo um conjunto definidor de relações $\{r_i(a_j) = 1 \mid 1 \leq i \leq q\}$ que pode ou não ser vazio. Quer dizer, A admite a apresentação

$$\langle a_1, a_2, \ldots, a_n \mid [a_i, a_j] = 1 \ (1 \leq i < j \leq n), r_i(a_j) = 1 \ (1 \leq i \leq m)\rangle$$

onde o símbolo $[a_i, a_j]$ denote o comutador $a_i^{-1}a_j^{-1}a_ia_j$. O núcleo K do epimorfismo $\phi : F_n \to A$ definido por $\phi : x_i \mapsto a_i$ contém o subgrupo derivado F_n' que é o fecho normal do conjunto $\{[x_i, x_j] \mid (1 \leq i < j \leq n)\}$. Então, ϕ induz um epimorfismo $\overline{\phi} : \overline{F}_n \to A$ onde $\overline{F}_n = F_n/F_n'$ é por definição um ***grupo abeliano livre*** de posto n.

Se reescrevermos a operação do grupo aditivamente, então veremos que $\overline{K}$ é gerado por

$$r_i(\overline{x}_j) = \sum_{i=1}^{n} m_{ij}\overline{x}_j \quad (1 \leq i \leq m)$$

onde os m_{ij} são inteiros. Podemos aplicar à matriz $n \times m$, $M = (m_{ij})$ as transformações elementares interas com exceção da multiplicação de linhas ou colunas por inteiros $\neq \pm 1$. Essas operações

produzem novas bases para $\overline{F}_n$ e produzem novos conjuntos geradores para $\overline{K}$.

Seguindo o procedimento que será descrito abaixo, M poderá ser transformada em sua forma normal

$$\left[\begin{array}{ccc|c} d_1 & & & \\ & d_2 & & 0 \\ & & \ddots & \\ & & & d_k \\ \hline & 0 & & 0 \end{array}\right]$$

onde o conjunto de inteiros positivos $\{d_1, d_2, \ldots, d_k\}$, quando não vazio, terá a propriedade da divisão $d_1 \mid d_2 \mid \cdots \mid d_k$; os d_i's são chamados os *divisores elementares* de A.

A matriz em sua forma normal nos fornece a base $\overline{y}_1, \ldots, \overline{y}_n$ de $\overline{F}_n$ tal que $r'_1(\overline{y}_i) = d_1\overline{y}_1, \ldots, r'_k(\overline{y}_i) = d_k\overline{y}_k$ é uma base de $\overline{K}$, e assim,

$$A \cong \overline{F}_n/\overline{K} = \langle \overline{K} + \overline{y}_1 \rangle \oplus \cdots \oplus \langle \overline{K} + \overline{y}_n \rangle$$

onde

$$\begin{array}{rll} \langle \overline{K} + \overline{y}_i \rangle \cong \mathbb{Z}_{d_i} & (\text{cíclico de ordem } d_i) & \text{para} \quad 1 \leq i \leq k, \\ \cong \mathbb{Z} & (\text{cíclico infinito}) & \text{para} \quad k+1 \leq i \leq n. \end{array}$$

Assim chegamos a uma apresentação de A da forma

$$\langle z_1, \ldots, z_n \mid [z_i, z_j] = 1 \ (1 \leq i < j \leq n), z_1^{d_1} = \cdots = z_k^{d_k} = 1$$
$$(\text{para algum } d_i \geq 1 e \ d_1 \mid d_2 \mid \cdots \mid d_k) \rangle.$$

Se $d_1 = d_2 = \cdots = d_\ell = 1$ e $d_{\ell+1} \neq 1$ então A tem uma decomposição canônica

$$A \cong \mathbb{Z}_{d_{\ell+1}} \oplus \cdots \oplus \mathbb{Z}_{d_k} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-k}$$

e $\{d_{\ell+1}, \ldots, d_k; \ n-k\}$ é o conjunto dos invariantes de A.

2.2. Para demonstrar o algoritmo é suficiente transformar M numa matriz da forma

$$\left[\begin{array}{c|c} x & 0 \\ \hline 0 & M' \end{array}\right]$$

onde $x \mid m'_{ij}$ para todas as entradas m'_{ij} de M'.

Isso é feito como segue, para $M \neq 0$.

1. Escolha $m_{ij} \in M$ com $0 \neq |m_{ij}| \leq |m_{rs}|$ para todo $0 \neq m_{rs} \in M$.

2. Troque as linhas R_i e R_1;
   troque as colunas C_j e C_1;
   (agora $0 \neq |m_{11}| \leq |m_{rs}|$ para todo $0 \neq m_{rs} \in M$)
   multiplique R_1 por ± 1 para fazer $m_{11} > 0$.

3. Para $j = 2, \ldots, n$
   escreva $m_{1j} = c_j m_{11} + r_j$ com $0 \leq r_j < m_{11}$;
   se $c_j \neq 0$,
   subtraia $c_j C_1$ de C_j (agora $0 \leq m_{1j} < m_{11}$ para $j = 2, \ldots n$).

4. Se existe $m_{1j} \neq 0$ para $j \neq 1$,
   troque C_1 por C_j;
   volte para 3.
   (Este passo pára quando $R_1 = (m_{11}, 0, \ldots, 0)$).

5. Se m_{11} não dividir todas as entradas de M,
   escolha m_{ij} , tal que $m_{11} \nmid m_{ij}$;
   some C_1 a C_j (se $j \neq 1$);
   escreva $m_{ij} = d_{ij} m_{11} + r_{ij}$ com $0 < r_{ij} < m_{11}$;
   subtraia $d_{ij} R_i$ de R_j;
   (agora temos $0 < m_{ij} < m_{11}$)
   volte para 1.
   (Tendo em vista que obtemos valores sucessivamente menores para m_{11} chegaremos a um ponto quando $m_{11} \mid m_{ij}$ para todo i, j, e passaremos à etapa 6).

6. Para $i = 2, \ldots, m$,
   escreva $m_{i1} = d_i m_{11}$;
   se $d_i \neq 0$
   subtraia $d_i R_1$ de R_i.

As vantagens didáticas e práticas dessa demonstração construtiva são claras e por isso a recomendamos ao invés das outras

que dependem de argumentos de existência.

2.3. Dado o bom domínio que adquirimos em grupos abelianos finitamente apresentados, um dos primeiros métodos que aplicamos a um grupo G finitamente apresentado por

$$\langle g_1, \ldots, g_n \,|\, r_1(g_i) = \cdots = r_m(g_i) = 1 \rangle$$

é o estudo de sua *abelianização* $\overline{G} := G/G'$ que tem a apresentação

$$\langle a_1, \ldots, a_n \mid [a_i, a_j] = 1 \ (1 \leq i < j \leq n),\ r_1(a_i) = \cdots = r_m(a_i) = 1 \rangle.$$

Por exemplo, para C_q:

$$\overline{C}_q = \langle a, b \,|\, [a, b] = 1,\ \ aba^{-2}bab^{-1} = 1,\ \ a(b^{-1}a^3b^{-1}a^{-3})^q = 1 \rangle.$$

Como a e b comutam em $\overline{C}_q$, a segunda e terceira relações podem ser reescritas como

$$1 = aa^{-2}abbb^{-1} = b \qquad 1 = ab^{-q}a^{3q}b^{-q}a^{-3q} = ab^{-2q},$$

ou como

$$b = 1, \qquad a = b^{2q},$$

e então

$$a = b = 1 \qquad \text{em} \qquad \overline{C}_q.$$

Logo, $\overline{C}_q$ é trivial, ou seja, C_q é um grupo perfeito. Uma consequência imediata é que os quocientes finitos minimais não triviais de C_q são grupos simples não cíclicos.

3. O Teorema de Novikov e o Método de Todd–Coxeter

Na última seção vimos que os problemas de Dehn têm uma solução muito elegante para grupos abelianos finitamente apresentados. Entretanto em 1955 P. S. Novikov [Nov 55] publicou uma demonstração da não solubilidade do Problema da Palavra de Dehn. De fato, ele provou a existência de um grupo finitamente apresentado G, que derrota qualquer algoritmo proposto com a finalidade de decidir em um número finito de passos, se uma dada

palavra nos geradores de G representa ou não a identidade. Logo depois, foi provado que os outros problemas de Dehn também não eram algoritmicamente solúveis. Outras perguntas também tiveram respostas negativas, por exemplo, decidir se um grupo dado por uma de suas apresentações é finito ou não [Rab 58]. Esses resultados deixam espaço apenas para projetos mais modestos do que a solução dos problemas de Dehn. Uma proposta foi apresentada já em 1936 por J. Todd e H. S. M. Coxeter [ToC 36].

O método deles pode ser melhor caracterizado como um "método de verificação". Se um grupo descrito por uma apresentação finita fôr de fato finito, o método aplicado ao grupo, depois de um certo número finito de passos, para, tendo verificado a finitude do grupo. Porém, através da apresentação desse grupo finito é impossivel adivinhar o número de passos necessários para a conclusão do trabalho. Então, se o método não tiver sucesso depois de um certo tempo, não se pode chegar a nenhuma conclusão sobre a finitude do grupo; quer dizer, esse método **não** é um algoritmo de decisão.

O método de Todd–Coxeter lida na verdade com uma situação um pouco mais geral. Dada uma apresentação finita

$$G = \langle g_1, \ldots, g_n \,|\, r_1(g_i) = 1, \ldots, r_m(g_i) = 1 \rangle$$

e um conjunto finito de palavras

$$\{s_1(g_i), \ldots, s_p(g_i)\}$$

procura–se determinar o índice do subgrupo $U = \langle s_1(g_i), \ldots, s_p(g_i) \rangle$ em G construindo a representação permutacional de G no conjunto das classes lateriais à direita de U em G:

$$\phi_U : g \mapsto \begin{bmatrix} Uh \\ Uhg \end{bmatrix} \quad \text{para todo} \quad g, h \in G.$$

Naturalmente, basta encontrar a representação permutacional dos geradores de G, o que é feito por meio de tentativa–e–erro: as classes laterais de U serão enumeradas por $1, 2, 3, \ldots$ começando com $1 := U$, mas somente se o método for bem sucedido será certo que números diferentes representam classes diferentes. Acontece que durante o processo alguns números poderão corresponder inadvertidamente à mesma classe.

São montado três tipos de tabelas, uma "tabela de subgrupo" para cada gerador $s_j(g_i)$ do subgrupo U, uma "tabela de relações" para cada relação $r_j(g_i)$ de G, e uma "tabela de classes laterais" que controla o fluxo das definições, como explicamos a seguir.

Para cada gerador $s_j(g_i) = g_{i_1} \cdots g_{i_e}$, do subgrupo U, com $g_{i_j} \in \{g_1, \ldots, g_n, g_1^{-1}, \ldots, g_n^{-1}\} =: E$, a "tabela de subgrupo" é de uma linha

	g_{i_1}	g_{i_2}	$\cdots$	g_{i_e}
1				1

expressando o fato que $Us(g_i) = U$. Do mesmo modo, para cada relação $r(g_i) = g_{i_1} \cdots g_{i_t} = 1$ montamos uma "tabela de relações"

	g_{i_1}	g_{i_2}	$\cdots$	g_{i_t}
1				1
2				2
$\vdots$				$\vdots$
k				k
$\vdots$				$\vdots$

com uma linha para cada número de classe definido durante o processo, refletindo o fato de que para cada classe $k =: Uh$ temos $k \cdot r(g_i) = k$.

Uma única "tabela de classes" é usada para contabilizer as definições, feitas recursivamente, explicando o significado dos números correspondentes às classes:

	g_1	$\cdots$	g_n	g_1^{-1}	$\cdots$	g_n^{-1}
1						
2						
$\vdots$						
k						
$\vdots$						

O método prossegue definindo novos números de classes por equações da forma $\ell := k \cdot g$, onde k é um número de classe previamente definido, g é um gerador ou seu inverso e o lugar para essa definição na tabela das classes ainda não está preenchido. Juntamente com $\ell := kg$, a entrada $k = \ell g^{-1}$ é escrita na tabela de classes, de tal forma que ambas as definições são inseridas em todas as tabelas de subgrupo e de relações. Sempre que uma linha se completa em uma tabela de subgrupo ou de relações, ela nos fornece uma informação do tipo $kg = \ell$, chamada uma "consequência". Comparando isso com a configuração das tabelas de classes, um dos três casos seguintes pode ocorrer:

(i) ambas as entradas para kg e para ℓg^{-1} na tabela de classes continuam vazias. Então essa nova informação é introduzida em ambos os lugares da tabela de classes e é usada da mesma forma como na definições acima;

(ii) esses lugares já contém essa informação, neste caso não é necessário fazer nada;

(iii) um dos lugares tem uma informação diferente, digamos, $kg = \ell' \neq \ell$. Então sabemos que os *números de classe* ℓ e ℓ' denotam a mesma classe (dizemos que ℓ e ℓ' coincidem) e eliminamos um (o maior) deles. Fazendo isso, podemos, de fato, encontrar outras "coincidências".

Vamos expor o começo do método para o primeiro grupo de Cavicchioli. Escrevemos sua apresentação na forma equivalente

$$C_1 = \langle a, b \mid a^{-2}bab^{-1}ab = 1,\ \ a^3b^{-1}a^{-2}b^{-1} = 1 \rangle$$

e tentamos enumerar as classes laterais de $U := \langle a \rangle$. Então temos uma tabela de subgrupo

$$\begin{array}{c|c} & a \\ \hline 1 & 1 \end{array}$$

que nos diz imediatamente que $1a = 1$ e $(1a^{-1} = 1)$. Introduzindo essas definições e uma primeira definição $1b =: 2$ (e $2b^{-1} = 1$) nas tabelas, temos

Tabelas de relações:

a^{-1}	a^{-1}	b	a	b^{-1}	a	b	
1	1	1	2				1
2				2	1	1	2

a	a	a	b^{-1}	a^{-1}	a^{-1}	b^{-1}
1	1	1	1			2	1
2							2

Tabela de classes laterais:

	a	b	a^{-1}	b^{-1}
1	1	2	1	
2				1

Seguidas das definições $1b^{-1} =: 3$ e $2a =: 4$, a primeira linha da segunda tabela de relações se completa

a	a	a	b^{-1}	a^{-1}	a^{-1}	b^{-1}
1	1	1	1	3	4	2	1
·	·	·	·	·	·	·	·

e nos fornece como primeira "consequência" $3a^{-1} = 4$ que juntamente com $4a = 3$, são introduzidas na tabela de relações.

A sequência completa de definições, consequências e eliminações, juntamente com as tabelas podem ser encontradas no Apêndice. Nós só destacamos dois pontos dessa enumeração: depois da 9ª definição (do número de classe 10) encontramos a coincidência onde 9 e 8 definem a mesma classe. O número 9 é então eliminado. Ao invés de reenumerar, deixamos essa lacuna e continuamos com a definição do número de classe 11.

Depois da definição do número de classe 13, todas as tabelas são preenchidas sem nenhuma outra "coincidência" de números de classes pendente. A essa altura não é possível fazer nenhuma nova definição satisfazendo a restrição original.

Pode-se concluir de uma discussão mais geral deste procedimento (por exemplo, veja [Neu 82]) que toda vez que essa situação do fechamento das tabelas é alcançada, as colunas da tabela de classes laterais fornecem a representação de cada gerador do grupo como uma permutação das classes laterais de U através da multiplicação a direita dessas classes pelo referido gerador. A atribuição de permutações aos geradores do grupo G, que é finitamente

apresentado, define a representação permutacional ϕ_U. O núcleo é

$$\ker \phi_U = \{g \mid g \in G, \quad Uh = Uhg, \quad \forall\, h \in G\} = \bigcap_{h \in G} h^{-1}Uh.$$

Em particular, $\ker \phi_U \leq U$. Logo, do teorema do homomorfismo, $\phi_U(G) \cong G/\ker \phi_U$, segue a igualdade dos índices $[G : U] = [\phi_U(G) : \phi_U(U)]$, e portanto

$$|\phi_U(G)| = [G : \ker \phi_U] = [G : U] \,|\, \phi_U(U)|.$$

No caso do grupo de Cavicchioli C_1, as permutações obtidas dos geradores são

$$a \mapsto A = (2\ 4\ 3\ 7\ 6)(5\ 8\ 11\ 13\ 10)$$

$$b \mapsto B = (1\ 2\ 5\ 8\ 3)(6\ 10\ 12\ 11\ 7)$$

(lembramos que as permutações são definidas sobre a sequência $1, \ldots 13$ excetuando o número 9).

Dados os fatos $[C_1 : \langle a \rangle] = 12$ e $|\langle A \rangle| = 5$, temos que

$$[C_1 : \ker \phi_U] = 12 \cdot 5 = 60 = |\langle A,\, B \rangle|.$$

Naturalmente, se tivessemos tentado a enumeração das classes laterais do grupo trivial, com sorte poderiamos ter obtido a ordem de C_1; entretanto, como veremos mais adiante, essa enumeração teria requirido um espaço bastante maior. Ao invés disso, determinaremos a ordem de C_1 por uma variação do método de enumeração já exposto. Antes de chegar lá, abordaremos nas próximas duas seções o grupo C_2. Concluímos esta seção observando que N. Mendelsohn mostrou por uma análise mais cuidadosa que o procedimento de Todd–Coxeter possui de fato a propriedade de ser um método de verificação (por exemplo, veja [Neu 82]).

4. C_2 e o Método do "Baixo Indice"

Se quisermos estudar

$$C_2 = \langle a,\, b \,|\, aba^{-2}bab^{-1} = 1, \quad a(b^{-1}a^3b^{-1}a^{-3})^2 = 1 \rangle$$

tentando enumerar as classes laterais de $\langle a \rangle$, mesmo com a ajuda de um computador teremos uma decepção: depois de definir alguns milhares de números de classes, o espaço do computador estará totalmente esgotado antes do método chegar ao fim, e portanto nada poderá se concluir a respeito de C_2.

É claro que tentar novamente essa enumeração, escolhendo outros conjuntos de palávras como geradores de subgrupo, não seria nada satisfatório. Ao invés disso, é preferível um método que procure sistematicamente *todos* os subgrupos até um índice no máximo k, onde k é pequeno e préfixado.Tal método foi proposto por C. Sims fazendo uso da ideia de tabela de classe. Vamos descrevê–lo em linha gerais para um grupo finitamente apresentado

$$G = \langle g_1, \ldots, g_n \mid r_1(g_i) = 1, \ldots, r_m(g_i) = 1 \rangle.$$

Ele começa com a enumeração de Todd–Coxeter sem especificar geradores de subgrupos; se essa enumeração produzir mais que k classes laterais, e se além do mais essas forem classes laterais de algum subgrupo U de índice $\leq k$, então naturalmente, pelo menos dois desses números de classes deverão corresponder a mesma classe lateral. Pois bem, dizer que os números de classes x e y, representando classes laterais, definidos recursivamente no processo pelos representantes $t_x(g_1)$ e $t_y(g_i)$, de fato definem a mesma classe lateral, equivale a dizer que $t_x(g_i)\ t_y(g_i)^{-1} \in U$. No algorítmo de Sims, tais "coincidências forçadas" são estudadas numa certa ordem lexicográfica, assegurando–se, por uma busca retroativa, que cada subgrupo de índice $\leq k$ seja encontrado somente uma vez. Um refinamento adicional fornece apenas um representante de cada classe de conjugação de subgrupos. (Para maiores detalhes, veja de novo [Neu 82]).

Assim, para cada classe de conjugação de subgrupos, produz–se o número dos subgrupos que constitui essa classe. Para um representante U dessa classe, produz–se um conjunto de geradores de U expressos como palavras nos geradores de G, isto além da tabela de classe de U. A última por sua vez nos fornece as imagens $\phi_U(g_1), \ldots, \phi_U(g_n)$ dos geradores $g_1, \ldots, g_n$ de G, via a representação permutacional ϕ_U de G definida sobre o conjunto

das classes laterais de U em G.

Usando um computador no caso do grupo C_2, e fixando 15 como uma cota máxima para os índices dos subgrupos procurados, o método gera:

10 classes de conjugação de subgrupos de índice 11,

8 classes de conjugação de subgrupos de índice 12,

6 classes de conjugação de subgrupos de índice 13.

5. O Algoritmo de Schreier–Sims para Grupos de Permutações

As informações que obtivemos até agora sobre o grupo C_2 podem não parecer muito fortes. Porém, como foi visto no final da seção 3, devido ao fato

$$G/\ker \phi_U \cong \phi_U(G),$$

podemos encontrar tais grupos quocientes através das imagens permutacionais dos geradores de G que são fornecidas pelo algoritmo do "baixo índice". No caso de C_1, foi fácil encontrar a ordem de $\phi_U(G)$ já que $\phi_U(U)$ era cíclico. Na maioria dos casos, temos que gerar o grupo das permutações $\phi_U(G)$ através de seus geradores. A seguir, apresentaremos a idéia básica do método de Schreier–Sims para lidar com esta tarefa; o leitor interessado em detalhes técnicos e numa organização prática do método (indispensáveis para qualquer implementação eficiente) deve consultar [Leo 80a,b].

Seja H um grupo de permutações do conjunto $\Omega = \{1, 2, \ldots, z\}$. Definimos a "cadeia estabilizadora"

$$H^0 := H, \quad H^i := \mathrm{Stab}_{H_{i-1}}(i) = \{h \mid h \in H^{i-1}, \quad h : i \mapsto i\}.$$

Então,

$$H = H^0 \geq H^1 \geq \cdots \geq H^{z-1} = \langle 1 \rangle.$$

Devemos primeiro usar a correspondência biunívoca natural entre as classes laterais de H^i em H^{i-1} e os pontos de órbita

$$i^{H^{i-1}} = \{j \in \Omega \mid \exists h \in H^{i-1} \quad \text{com} \quad h : i \mapsto j\}$$

do ponto i sob a ação de H^{i-1}.

Começando com H podemos obter a órbita de 1 pela ação de H aplicando os geradores de H em 1 e depois nas imagens de 1 até que nenhuma outra imagem seja encontrada. Se anotarmos ao lado de cada ponto da órbita o gerador do grupo que o produziu, como imagem de um ponto já conhecido, obteremos simultaneamente representantes das classes laterais na forma de produto de esses geradores.

Vamos ilustrar o método de Schreier–Sims usando as informações sobre um subgrupo particular de C_2, digamos S, de índice 12, fornecidas pelo método de "baixo índice". Por essas informações os geradores a, b de C_2 são representados por

$$\phi_S(a) = A = (2\ 4\ 8\ 11\ 12\ 10\ 9\ 5\ 3\ 7\ 6)$$

$$\phi_S(b) = B = (1\ 2\ 5\ 4\ 3)(6\ 10\ 12\ 11\ 7)$$

e que o subgrupo S é gerado por a^{-1}, b^2ab, bab^2, e $b^{-1}a^3b^{-1}$.

O conhecimento do índice $[C_2 : S] = [\langle A, B\rangle : \phi_S(S)] = 12$ é o suficiente para encontrar a ordem de $S^* := \phi_S(S)$ que é o grupo gerado por

$$\phi_S(a^{-1}) = A^{-1}, \ldots, \phi_S(b^{-1}a^3b^{-1}) = B^{-1}A^3B^{-1}.$$

Computamos então esses produtos de permutações:

$$\begin{array}{lcl} A^{-1} & = & (2\ 6\ 7\ 3\ 5\ 9\ 10\ 12\ 11\ 8\ 4) \\ B^2AB & = & (2\ 8\ 7\ 9\ 4)(5\ 6\ 12\ 10\ 11) \\ BAB^2 & = & (3\ 5\ 8\ 6\ 9)(4\ 10\ 11\ 12\ 7) \\ B^{-1}A^3B^{-1} & = & (2\ 3\ 10\ 8\ 6\ 5\ 12\ 4\ 7\ 9\ 11). \end{array}$$

Notamos que $B^{-1}A^3B^{-1} = A^{-3}$, e portanto S^* é gerado por $X := A^{-1}$, $Y := B^2AB$ e $Z := BAB^2$. Com X, Y e Z obtemos a órbita de 2 (cada primeira ocorrência de um ponto da órbita é sublinhado):

$$
\begin{array}{lllllllllllll}
2X = \underline{6} & 6X = & \underline{7} & 8X = \underline{4} & 7X = \underline{3} & 12X = \underline{11} & 9X = & 10 & 4X = & 2 & 3X = \underline{5} \\
2Y = \underline{8} & 6Y = & \underline{12} & 8Y = 7 & 7Y = 9 & 12Y = \underline{10} & 9Y = & 4 & 4Y = & 2 & 3Y = 3 \\
2Z = 2 & 6Z = & \underline{9} & 8Z = 6 & 7Z = 4 & 12Z = & 7 & 9Z = & 3 & 4Z = & 10 & 3Z = 5
\end{array}
$$

A essa altura em nosso cálculo observamos que o grupo S^* permuta transitivamente os 11 pontos $2, \ldots 12$ e que dessa computação obtemos os representantes $T_2, \ldots, T_{12}$ do $\mathrm{Stab}_{S^*}(2)$ que listamos paralelamente aos pontos da órbita.

$$
\begin{array}{rcllcrcll}
2 & = & 2id & & \Rightarrow & T_2 & = & id & \\
3 & = & 7X = 2X^3 & & \Rightarrow & T_3 & = & X^3 & = (2\,3\,10\,8\,6\,5\,12\,4\,7\,9\,11) \\
4 & = & 8X = 2YX & & \Rightarrow & T_4 & = & YX & = (2\,4\,6\,11\,9)(3\,5\,7\,10\,8) \\
5 & = & 3X = 2X^4 & & \Rightarrow & T_5 & = & X^4 & = (2\,5\,11\,6\,9\,8\,7\,10\,4\,3\,12) \\
6 & = & 2X & & \Rightarrow & T_6 & = & X & = (2\,6\,7\,3\,5\,9\,10\,12\,11\,8\,4) \\
7 & = & 6X = 2X^2 & & \Rightarrow & T_7 & = & X^2 & = (2\,7\,5\,10\,11\,4\,6\,3\,9\,12\,8) \\
8 & = & 2Y & & \Rightarrow & T_8 & = & Y & = (2\,8\,7\,9\,4)(5\,6\,12\,10\,11) \\
9 & = & 6Z = 2XZ & & \Rightarrow & T_9 & = & XZ & = (2\,9\,11\,6\,4)(3\,8\,10\,7\,5) \\
10 & = & 12Y = 2XY^2 & & \Rightarrow & T_{10} & = & XY^2 & = (2\,10\,11\,9\,5)(3\,12\,6\,4\,7) \\
11 & = & 12X = 2XYX & & \Rightarrow & T_{11} & = & XYX & = (2\,11\,3\,7\,5)(6\,10\,12\,9\,8) \\
12 & = & 6Y = 2XY & & \Rightarrow & T_{12} & = & XY & = (2\,12\,5\,4\,8)(3\,6\,9\,11\,7)
\end{array}
$$

Tendo encontrado representantes das classes do $\mathrm{Stab}_{S^*}(2)$ em S^*, podemos então apelar a um teorema clássico de O. Schreier:

Teorema. Seja G um grupo gerador por $E := \{g_1, \ldots, g_n\}$, seja U um subgrupo de G, e $T = \{t_1, \ldots, t_x\}$ um conjunto de representantes de classes (um "transversal") de U em G. Então U é gerado pelo conjunto dos "geradores de Schreier"

$$\{s_{t,g} \mid s_{t,g} = tg\,\overline{tg}^{-1}, \quad t \in T, \quad g \in E\}$$

onde $\overline{tg}$ denota o representante da classe lateral de U em T; que contém o produto tg.

No nosso exemplo, podemos obviamente calcular esses geradores de Schreier; ilustrando, obtemos para o primeiro gerador X

a seguinte listagem:

$$
\begin{array}{llll}
S_{2,X} & = T_2 X \overline{T_2 X}^{-1} & = T_2 X T_6^{-1} & = id \\
S_{3,X} & = T_3 X \overline{T_3 X}^{-1} & = T_3 X T_5^{-1} & = id \\
S_{4,X} & = T_4 X \overline{T_4 X}^{-1} & = T_4 X T_2^{-1} & = (3\ 9\ 6\ 8\ 5)(4\ 7\ 12\ 11\ 10) \\
S_{5,X} & = T_5 X \overline{T_5 X}^{-1} & = T_5 X T_9^{-1} & = (3\ 9\ 6\ 8\ 5)(4\ 7\ 12\ 11\ 10) \\
S_{6,X} & = T_6 X \overline{T_6 X}^{-1} & = T_6 X T_7^{-1} & = id \\
S_{7,X} & = T_7 X \overline{T_7 X}^{-1} & = T_7 X T_3^{-1} & = id \\
S_{8,X} & = T_8 X \overline{T_8 X}^{-1} & = T_8 X T_4^{-1} & = id \\
S_{9,X} & = T_9 X \overline{T_9 X}^{-1} & = T_9 X T_{10}^{-1} & = (3\ 6\ 5\ 9\ 8)(4\ 12\ 10\ 7\ 11) \\
S_{10,X} & = T_{10} X \overline{T_{10} X}^{-1} & = T_{10} X T_{12}^{-1} & = (3\ 9\ 6\ 8\ 5)(4\ 7\ 12\ 11\ 10) \\
S_{11,X} & = T_{11} X \overline{T_{11} X}^{-1} & = T_{11} X T_8^{-1} & = id \\
S_{12,X} & = T_{12} X \overline{T_{12} X}^{-1} & = T_{12} X T_{11}^{-1} & = id.
\end{array}
$$

Dessa listagem, observamos que todos os geradores de Schreier $S_{i,x}$ são potencias do elemento (3 9 6 8 5)(4 7 12 11 10), e efetuando multiplicações de permutações, o leitor poderá verificar que os geradores de Schreier restantes $S_{i,Y}$ e $S_{i,Z}$ são também potencias desse mesmo elemento. Concluímos então que o subgrupo $\mathrm{Stab}_{S^*}(2)$ é cíclico de ordem 5, que $|S^*| = 11 \cdot 5 = 55$, e que $|\langle A, B\rangle = 12 \cdot 55 = 660$. Além do mais, o grupo $\langle A, B\rangle$ é duplamente transitivo. Os últimos dois fatos são suficientes para garantir que $\langle A, B\rangle$ seja isomorfo com $PSL(2, 11)$.

No exemplo já exposto, o fato que $\mathrm{Stab}_{S^*}(2)$ era cíclico facilitou nosso trabalho, o que não é regra. De fato o aumento dos geradores de Schreier de um passo para outro é algo problemático.

Essa dificuldade é superada pela seguinte observação: suponhamos que em alguma etapa é obtido um gerador s de Schreier que fixe $1, 2, \ldots, i-1$ e leve i em j diferente de i. Então $s \in H^{i-1}$ está na classe lateral de H^i que corresponde a j. Se já tivermos listado um representante r da mesma classe de H^i em H^{i-1} previamente como um gerador de Schreier, então ao invés de guardar s podemos guardar sr^{-1}, pois s e r geram o mesmo subgrupo que sr^{-1} e r. Contudo, sr^{-1} fixará também i, e então estará contido num subgrupo "mais abaixo" na cadeia estabilizadora. Dessa observação vemos que não guardaremos para um subgrupo H^i mais geradores do que o número máximo de possíveis classes em todos os passos da cadeia estabilizadora; quer dizer, no máximo

$z + (z-1) + \cdots + 1 = \frac{z(z+1)}{2}$. A implementação prática é ainda mais eficiente do que acabamos de descrever.

Vejamos agora o que uma implementação do método de Schreier–Sims nos diz sobre o grupo de Cavicchioli C_2. Como foi explicado na seção 4, foram obtidos as permutações $\phi_U(a)$, $\phi_U(b)$ onde U percorre os subgrupos representantes das 24 classes de conjugação de subgrupo de C_2 encontrados pelo método de "baixo índice". As ordens dos grupos de permutações

$$\langle \phi_U(a), \phi_U(b) \rangle \cong C_2 / \bigcap_{g \in G} U^g$$

encontrados pelo algoritmo de Schreier–Sims são listadas na segunda linha da seguinte tabela:

$C_2 : U$	11	12	12	11	12	13
$C_2 : \cap_{g \in G}\ U^g$	660	660	95040	11! / 2	12! / 2	13! / 2
No. de classes	2	1	4	8	3	6
No. de núcleos	1		2	8	3	6

Já que C_2 é igual a seu grupo comutador, seus grupos quocientes $C_2 / \bigcap_{g \in G} U^g$ também gozam da mesma propriedade. Uma comparação com a lista dos grupos finitos simples nos mostra que esses quocientes são de fato simples; em poucos casos foi verificado que o mesmo subgrupo normal de C_2 é encontrado como a interseção de diferentes classes de subgrupos conjugados de C_2, o que explica a última linha da tabela. O que resta são os seguintes grupos quocientes diferentes: uma vez $PSL(2,11)$, duas vezes o grupo de Mathieu M_{12}, 8 vezes A_{11}, 3 vezes A_{12}, 6 vezes A_{13}.

Agora, se $S_i = G/N_i$, $i = 1, \ldots, k$ são grupos quocientes simples não–abelianos de um grupo G com $N_i \neq N_j$ para $i \neq j$ então $G / \bigcap_{i-1}^{k} N_i$ é isomorfo ao produto direto $\mathsf{X}_{i=1}^{k} S_i$. Então podemos conlcuir que C_2 tem um grupo quociente isomorfo a

$$PSL(2,11) \times M_{12}^{\times 2} \times A_{11}^{\times 8} \times A_{12}^{\times 3} \times A_{13}^{\times 6} \text{ de ordem } \sim 1.9 \cdot 10^{153},$$

um resultado que não esperaríamos a primeira vista, pela aparência magra da lista de subgrupos obtidos no final da seção 4.

Fechamos esta seção observando que C. Sims usou refinamentos deste procedimento para construir alguns dos grupos simples esporádicos como grupos de permutações. Seu resultado mais espetacular nesse campo foi a construção do "Baby-Monster" como um grupo de permutações de grau 13 571 955 000 que obiamente envolveu muito mais teoria e uma programação bem especial.

6. O Teorema de Reidemeister, um Método Modificado de Todd-Coxeter, e mais sobre C_1 e C_2

Na seção anterir exibimos grupos quocientes de C_1 e C_2 que sugeriam que C_1 poderia ser finito enquanto C_2 talvez não fosse. Para mostrar isso, voltemos ao teorema de Schreier que fornece geradores para um subgrupo U de G. Dado que nas aplicações temos trabalhado com permutações, o referido teorema foi satisfatório. Porém, se trabalharmos com geradores abstratos, para proceder da forma análoga torna-se necessário determinar um conjunto definidor de relações para os geradores de Schreier. É esse o conteudo do teorema de Reidemeisater:

Teorema. Seja G um grupo com apresentação finita

$$G = \langle g_1, \ldots, g_n \,|\, r_1(g_i) = 1, \ldots, r_m(g_i) = 1 \rangle,$$

seja $U \leq G$ e $T = \{t_1, \ldots, t_x\}$ um transversal de U em G. Então U tem a seguinte apresentação com relação ao conjunto $\{s_{t,g}\}$ dos geradores de Schreier.

$$U = \langle s_{t_\ell, g_i} \,|\, \tau(t_\ell r_j t_\ell^{-1}) = 1, \;\; s_{t_\ell g_i} = \tau(t_\ell g_i \overline{tg_i}^{-1}) \rangle$$

onde $j = 1, \ldots, m$; $\ell = 1, \ldots, x$; $i = 1, \ldots n$, e onde τ é a "reescrita de Reidemeister". Esse τ reescreve o produto dos geradores g_i que estão em U como um produto dos geradores de Schreier do U seguindo a seguinte regra:

se

$$u = g_{i_1}^{\varepsilon_1} \cdots g_{i_r}^{\varepsilon_r} \in U \quad \text{com} \quad \varepsilon_j = \pm 1,$$

então

$$\tau(u) = s_{p_1,g_{i_1}}^{\varepsilon_1} \cdots s_{p_r,g_{i_r}}^{\varepsilon_r}$$

onde

$$p_j = \overline{g_{i_1} \cdots g_{i_{j-1}}} \quad \text{se} \quad \varepsilon_j = 1$$

e

$$p_j = \overline{g_{i_1} \cdots g_{i_j}} \quad \text{se} \quad \varepsilon_j = -1.$$

Podemos ver facilmente que esta reescrita está correta simplesmente inserindo a definição dos geradores de Schreier no resultado anunciado acima: o leitor poderá encontrar a demonstação do teorema em [Joh 80]. Para nossos objetivos é essencial notar que a reescrita de Reidemeister de uma dada palavra pode ser efetuada se há uma tabela de classes para as classes com representantes t_ℓ. Já que

$$\overline{g_{i_1} \cdots g_{i_j}} = \overline{\overline{g_{i_1} \cdots g_{i_{j-1}}} g_{i_j}},$$

os representantes que precisamos para tais produtos podem ser procurados recursivamente na tabela de classes: se $\overline{g_{i_1} \cdots g_{i_{j-1}}}$ é o representante de uma classe de número c, então o nmero da classe tendo $\overline{g_{i_1} \cdots g_{i_j}}$ como representante é encontrado na coluna do gerador g_{i_j} na linha número c.

Baseado nessa observação, G. Havas implementou um programa que determina a apresentação de Reidemeister de um subgrupo U pela tabela de classes em G. É claro que o número de geradores de (Schreier) e de relações (de Reidemeister) assim obtidos será grande (dependendo do índice de U). O programa de Havas possui um programa heurístico para eliminar o maior número possível desses geradores.

Usando o programa de Havas para o subgrupo S de C_2, de índice 12, já considerado na seção 5, chega-se no final à seguinte apresentação em 4 geradores deste subgrupo:

$$\begin{aligned} S = \langle t_1, t_2, t_3, t_4 \,|\, & t_1 t_2 t_1^{-1} t_2^{-1} = 1, \\ & t_1^5 t_2^{-2} = 1, \quad t_1^2 t_3 t_1^{-2} t_4 t_3^{-1} t_1 t_4^{-1} = 1, \\ & t_1 t_2 t_4 t_1^{-1} t_3 t_4^{-1} t_2^{-1} t_1^{-1} t_3^{-1} = 1, \\ & t_1^3 t_2 t_4 t_1^{-3} t_2^{-1} t_4^{-1} = 1 \rangle. \end{aligned}$$

Se *abelianizarmos* S, a primeira e a última relação ficam triviais e conseguimos a seguinte matriz de relações do grupo abelianizado S/S' de S:

$$\begin{bmatrix} \bar{t}_1 & \bar{t}_2 & \bar{t}_3 & \bar{t}_4 \\ 0 & 0 & 0 & 0 \\ 5 & -2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

O algoritmo dos divisores elementares transforma essa matriz em:

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 5 & -2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 5 & -2 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Então vemos que S/S' é isomorfo a um produto direto de um grupo cíclico de ordem 2 com dois grupos cíclocos infinitos: $S/S' \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$: portanto, ele é infinito, assim como C_2.

Podemos usar o mesmo programa em C_1 e no seu subgrupo $\langle a \rangle$ de índice 12. De antemão o número dos geradores de Schreier para o subgrupo será 24. Contudo, usando uma versão especial do teorema de Reidemeister, esse número se reduz a 13, o que é bem inadequado já que sabemos que $\langle a \rangle$ é cíclico! É então desejável ter um algoritmo que nos dê a apresentação para um subgrupo com respeito aos geradores dados. De fato, uma versão modificada do método de Todd–Coxeter fará isso. Se introduzirmos os números $1, 2 \cdots$ não para indicar as classes laterais mas os representantes das classes, com o elemento neutro sendo o representante de U, veremos que ao se fechar a primeira tabela de subgrupo para um gerador

$$h = h(g_i) = g_{i_1} \cdots g_{i_x} \cdots g_{i_r}$$

do subgrupo U, teremos uma consequência da forma $kg_{i_x} = h\ell$ (ao invés de $kg_{i_x} = \ell$ como originalmente), para os números de classe k e ℓ:

g_{i_1}	$\cdots$	g_{i_x}	$\cdots$	g_{i_r}
1	$\ldots$ k	hl	$\ldots$	$h1$

Introduzindo as consequências desse tipo que completam uma tabela de subgrupo, tanto na tabela de classes quanto nas outras tabelas de subgrupos, assim como nas tabelas de relações, veremos que as entradas também se modificarão por produto dos geradores préfixados dos subgrupos. Agora considerando os três casos possíveis quando se coloca uma consequência numa tabela de classes (ver seção 3), vemos que no caso (ii) podemos ter o mesmo número de classe, mas palavras diferentes w_1 e w_2 nos geradores do subgrupo, da nova consequência e da tabela de classes. Nesse caso $w_1(h_j)\ell = w_2(h_j)\ell$, e concluimos que $w_1(h_j)w_2(h_j)^{-1} = 1$ é uma relação que vale para os geradores préfixados do subgrupo. Pode-se provar (por exemplo, veja [Neu, 82] e os artigos na sua bibliografia) que o conjunto de todas as relações que surgem nessa forma é um conjunto definidor de relações para U com respeito aos geradores dados. Os cálculos são feitos para C_1 no apêndice; a $13^{\underline{a}}$ e $14^{\underline{a}}$ consequência nesse sentido nos fornece $h^{10} = 1$, e disso se obtém que o subgrupo $\langle a \rangle$ de C_1 é de ordem 10. Já que o índice $[C_1 : \langle a \rangle] = 12$, o grupo C_1 tem ordem 120 e pode então ser identificado como sendo isomorfo a $SL(2,5)$. Deve-se mencionar que a implementação do método de Todd-Coxeter modificado precisa de mais considerações para que o comprimento crescente das palavras nos geradores de subgrupo seja controlado, no caso de haver mais de um gerador (veja [ARo 84]).

7. Usando as Representações em $SL(2, \cdot)$

O estudo das representações complexas de um grupo por matrizes é um procedimento essencial na teoria dos grupos finitos. Aqui os problemas de representação se traduzem eficientemente em problemas sobre traços de matrizes e entram no domínio da teoria dos caracteres.

Dado um grupo finitamente apresentado

$$G = \langle g_1, \ldots, g_n \mid r_1(g_s), \ldots, r_m(g_s) \rangle,$$

uma representação $\phi : G \to SL(d, \mathbb{F})$ é determinada por

$$\phi(g_s) = X_s = (x_{ij}^{(s)}) \quad (1 \leq s \leq n)$$

onde as entradas são soluções do conjunto de equações polinomiais em várias variáveis

$$\det(X_s) = 1 \ \ (1 \leq s \leq n), \quad r_i(X_s) = 0 \ \ (1 \leq i \leq m)$$

para alguma dimensão d e algum corpo $\mathbb{F}$.

W. Magnus promove em [Mag 81] o uso de representações em $SL(2,\mathbb{C})$ como uma ferramenta na teoria combinatória dos grupos e expõe os métodos e resultados conhecidos. Em particular expõe algumas fórmulas de traço que contudo não alcançam a dimensão da teoria geral dos caracteres.

Aparesentamos abaixo alguns exemplos onde um cálculo direto de representações produz resultados precisos para os grupos em questão.

Definimos três classes de grupos. Cada grupo da segunda classe será um grupo quociente de um grupo da primeira classe, e como mostraremos em (3) mais a frente, cada grupo na terceira classe será um grupo quociente de um grupo na segunda, o que nos leva aos grupos de Cavicchioli. Para i, j, k, ℓ, q, inteiros diferentes de zero, sejam

$$\begin{aligned} G(i,j,k) &= \langle a, b \,|\, a^i b a^j b a^k b^{-1} \rangle, \\ G(i,j,k,\ell) &= \langle a, b \,|\, a^i b a^j b a^k b^{-1}, \ [a, b a^\ell b] \rangle, \\ G(i,j,k,\ell,q) &= \langle a, b \,|\, a^i b a^j b a^k b^{-1}, \ \ a(b^{-1}a^{-\ell}b^{-1}a^{\ell})^q \rangle. \end{aligned}$$

Então, claramente, $C_q = G(1, -2, 1, -3, q)$.

I. Suponha $\mathbb{F}$ um corpo e

$$\phi : G(i,j,k) \to SL(2, \mathbb{F})$$

uma representação tal que no grupo imagem

$$\phi(a) = A = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}, \quad \phi(b) = B = \begin{bmatrix} \beta_{11} & \beta_{12} \\ \beta_{21} & \beta_{22} \end{bmatrix}$$

onde $\beta_{12}\beta_{21} \neq 0$. Então, podemos tornar $\beta_{21} = 1$ conjugando o grupo imagem por

$$M = \begin{bmatrix} 1 & 0 \\ 0 & \beta_{21} \end{bmatrix}.$$

Devemos notar que em geral $\phi(a)$ tem uma das formas canônicas de Jordan

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix} \quad \text{ou} \quad \begin{bmatrix} \pm 1 & 0 \\ 1 & \pm 1 \end{bmatrix}$$

em alguma extensão de $\mathbb{F}$. Escolhemos a primeira forma para facilitar os cálculos.

Os segauintes cálculos são diretos:

$$A^i B = \begin{bmatrix} \alpha^i \beta_{11} & \alpha^i \beta_{12} \\ \alpha^{-i} & \alpha^{-i} \beta_{22} \end{bmatrix} \quad BA^{-k} = \begin{bmatrix} \beta_{11}\alpha^{-k} & \beta_{12}\alpha^k \\ \alpha^{-k} & \beta_{22}\alpha^k \end{bmatrix}$$

$$A^i B A^j B = \begin{bmatrix} \alpha^{i+j}\beta_{11}^2 + \alpha^{i-j}\beta_{12} & \alpha^{i+j}\beta_{11}\beta_{12} + \alpha^{i-j}\beta_{12}\beta_{22} \\ \alpha^{-i+j}\beta_{11} + \alpha^{-i-j}\beta_{22} & \alpha^{-i+j}\beta_{12} + \alpha^{-i-j}\beta_{22}^2 \end{bmatrix}$$

A relação

$$A^i B A^j B = B A^{-k}$$

equivale as equações seguintes

$$(11) \qquad \alpha^{i+j}\beta_{11}^2 + a^{i-j}\beta_{12} = \beta_{11}\alpha^{-k}$$

$$(12) \qquad \alpha^{i+j}\beta_{11}\beta_{12} + \alpha^{i-j}\beta_{12}\beta_{22} = \beta_{12}\alpha^k$$

$$(21) \qquad \alpha^{-i+j}\beta_{11} + \alpha^{-i-j}\beta_{22} = \alpha^{-k}$$

$$(22) \qquad \alpha^{-i+j}\beta_{12} + \alpha^{-i-j}\beta_{22}^2 = \beta_{22}\alpha^k.$$

De (12), como $\beta_{12} \neq 0$ temos

$$(12)' \qquad \alpha^{i+j}\beta_{11} + \alpha^{i-j}\beta_{22} = \alpha^k$$

que juntamente com (21) nos dá:

$$(21)' \qquad \alpha^{2(i-k)} = 1.$$

Agora

$$(11)' \qquad \beta_{12} = \alpha^{-i+j-k}\beta_{11} - \alpha^{2j}\beta_{11}^2$$

$$(12)'' \qquad \beta_{22} = \alpha^{-i+j+k} - \alpha^{2j}\beta_{11},$$

que substituido em (22), nos dá

$$\begin{aligned} & \alpha^{-i+j}(\alpha^{-i+j-k}\beta_{11} - \alpha^{2j}\beta_{11}^2) + \alpha^{i-j}(\alpha^{-i+j+k} - \alpha^{2j}\beta_{11})^2 \\ = \; & (\alpha^{-i+j+k} - \alpha^{2j}\beta_{11})\alpha^k, \end{aligned}$$

e isso por sua vez nos leva a

$$\alpha^{j+k}(\alpha^{-4k} - 2\alpha^{-2k} + \alpha^{2i-2k})\beta_{11} = \alpha^i - \alpha^{-i}.$$

Já que $\alpha^{2i} = \alpha^{2k}$, temos

$$\alpha^{j+k}(\alpha^{-2i} - 1)^2\beta_{11} = \alpha^i(1 - \alpha^{-2i});$$

então, usando novamente $\alpha^{2i} = \alpha^{2k}$,

$$(22)' \qquad \alpha^{2i} = 1 \quad \text{ou} \quad \beta_{11} = \frac{\alpha^{i-j+k}}{\alpha^{2i}-1}.$$

Usando (12)", (11)' na equação do determinante

$$\beta_{12} = \beta_{11}\beta_{22} - 1$$

chegamos ao mesmo resultado que (22)'.

Suponhamos $\alpha^{2i} \neq 1$. Então, por $(11)'$ temos

$$(11)'' \qquad \beta_{12} = \frac{\alpha^{4i}-\alpha^{2i}+1}{(\alpha^{2i}-1)^2}$$

e por $(12)''$ conseguimos

$$(12)''' \qquad \beta_{22} = \frac{\alpha^{-i+j+k}}{\alpha^{2i}-1};$$

observe que $\beta_{22} = -\alpha^{-2i+2j}\beta_{11}$.

Então, *para qualquer escolha de* $\alpha \in \mathbb{F}$ *tal que*

$$\alpha^{2(i-k)} = 1 \neq \alpha^{2i}$$

a função

$$\phi(a) = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}, \quad \phi(b) = \begin{bmatrix} \frac{\alpha^{i-j+k}}{\alpha^{2i}-1} & -\frac{\alpha^{4i}-\alpha^{2i}+1}{(\alpha^{2i}-1)^2} \\ 1 & -\frac{\alpha^{-i+j+k}}{\alpha^{2i}-1} \end{bmatrix}$$

se extende a uma representação de $G(i,j,k)$ em $SL(2,\mathbb{F})$.

Seja $C = A^j B$. Então $\det(C) = 1$, e

$$\text{traço}(C) = \frac{\alpha^{i+k} - \alpha^{-i+k}}{\alpha^{2i} - 1} = \alpha^{-i+k} = \pm 1.$$

Portanto, o polinômio característico de C é

$$x^2 - \text{traço}(C)x + \det C = x^2 \mp x + 1 \quad (\text{um fator de } x^3 \mp 1).$$

Pelo teorema de Cayley–Hamilton, C satisfaz seu polinômio característico, então $C^3 = \mp I$ e então C tem ordem 6 ou 3.

II. Propomos agora obter uma representação

$$\overline{\phi} : G(i,j,k,\ell) \to SL(2,\mathbb{F})$$

do ϕ da seção anterior. Para tal finalidade, A tem que comutar com $BA^\ell B$. Como A é uma matriz diagonal não–central, $BA^\ell B$ também é uma matriz diagonal. Por um cálculo direto, obtemos que $\alpha^{2(\ell+i-j)} = 1$. Portanto, $\overline{\phi}$ é uma representação para qualquer escolha de α que obedeça

$$\alpha^{2i} \neq 1 = \alpha^{2(i-k)} = \alpha^{2(\ell+i-j)}.$$

Usando esses fatos junto com $\alpha^{2k} = \alpha^{2i}$, temos

$$BA^\ell B = \begin{bmatrix} -\alpha^\ell & 0 \\ 0 & -\alpha^\ell \end{bmatrix} = -A^{-\ell}, \quad (A^\ell B)^2 = -I.$$

III. Seja $G := G(i,j,k,\ell,q)$.

Então a última relação $(b^{-1}a^{-\ell}b^{-1}a^\ell)^q = a^{-1}$ implica que a comuta com $b^{-1}a^{-\ell}b^{-1}$, já que a é uma potência de $b^{-1}a^{-\ell}b^{-1}a^\ell$, e isso mostra que G é um grupo quociente de $G(i,j,k,\ell)$. Substituindo A, B na última relação de G, concluimos que $\overline{\phi}$ induz uma

representação $\overline{\overline{\phi}} : G \to SL(2, \mathbb{F})$ se e só se, além das condições impostas anteriormente sobre α, tivermos:

$$\alpha^{2q\ell+1} = (-1)^q.$$

Portanto, temos acumulado as seguintes relações de torção:

$$A^{2q\ell+1} = (-1)^q I, \quad (A^j B)^3 = \pm I \quad (A^\ell B)^2 = -I,$$

que constituem um conjunto forte de relações. É bem sabido por exemplo que

$$\langle x, y \,|\, x^5, y^3, (xy)^2 \rangle \text{ é uma apresentação para } A_5$$

e daí concluimos facilmente que a imagem de C_1 por $\overline{\overline{\phi}}$ é isomorfa a $PSL(2,5)$ ou $SL(2,5)$.

IV. Para ilustrar uma linha que poderá ser seguida no estudo de $\overline{\overline{G}} := \overline{\overline{\phi}}(G)$, vamos restringir nossas considerações a corpos finitos $\mathbb{F}$ e chegaremos à conclusão que se $3 \,|\, q\ell$ e $|2q\ell + 1| > 5$ então $\overline{\overline{G}}$ tem um número infinito de grupos quocientes não-isomorfos do tipo $PSL(2, p^s)$ e obtemos como corolário que $\overline{\overline{G}}$ é um grupo infinito. Come $C_q = G(1, -2, 1, -3, q)$, o que dizemos acima vale em particular para C_q se $q > 1$.

Para conseguirmos um entendimento tão profundo não é de surpreender que tenhamos de recorrer à classificação da estrutura dos subgrupos de $PSL(2, p^s)$ por L. E. Dickson (veja [Hup, 67], vol. I, p. 213), que afirma que os subgrupos não solúveis de $PSL(2, p^s)$ são isomorfos a $PSL(2, p^{s'})$ onde $s' \,|\, s$, a $PGL(2, p^{s'})$ onde $2s' | s$, ou A_5 se $p = 5$ ou $p^s \equiv \pm 1 \pmod{10}$.

Ao exigirmos que $3 | q\ell$, as ordens de A, $A^j B$, $A^\ell B$ ficam relativamente primas entre si em $SL(2\mathbb{F})$ módulo seu centro $\langle -I \rangle$. Portanto, por abelianização, $\overline{\overline{G}}$ é um grupo perfeito.

Como podemos escolher corpos finitos $\mathbb{F}$ que satisfaçam essas finalidades?

Fixe (i, j, k, ℓ, q) de forma que $i\,j\,k\,\ell\,q \neq 0$, $3 \,|\, q\ell$ e para $N = 2\,q\,\ell + 1$,

$$i \not\equiv 0 \pmod{N}, \quad k \equiv i \pmod{N}, \quad j \equiv i + \ell \pmod{N}.$$

Para todo primo p não divisor de N seja $m(p,N)$, abreviado por m, o menor número natural tal que $p^m \equiv 1 \pmod{N}$ e seja $\mathbb{F}_p$ o corpo finito $GF(p^m)$. Então, $\mathbb{F}_p$ contém um elemento tendo a ordem multiplicativa $|N|$.

Para toda escolha de $\mathbb{F}_p$ desse tipo, a imagem $\overline{\overline{G}}$ de

$$\overline{\overline{\phi}} : G(i,j,k,\ell,q) \to SL(2,\mathbb{F}_p)$$

é isomorfa a $SL(2,\mathbb{F}_p)$. Aplicando o teorema do Dickson, temos que $G(i,j,k,\ell,q)$ tem um grupo quociente infinito isomorfo a

$$\mathsf{X}_{p\,\not|\,N} PSL(2,\mathbb{F}_p)$$

para $|N| > 5$. Isso nos leva ao fim da linha e em particular á infinitude dos grupos de Cavicchioli, C_q $(q > 1)$.

8. Outro Exemplo, o Algoritmo do Quociente Nilpotente

Uma mistura dos diferentes métodos esboçados no exemplo dos grupos de Cavicchioli foi aplicada com sucesso na investigação de diversas apresentações. Mencionaremos um deles no qual tivemos que usar um algoritmo bem poderoso.

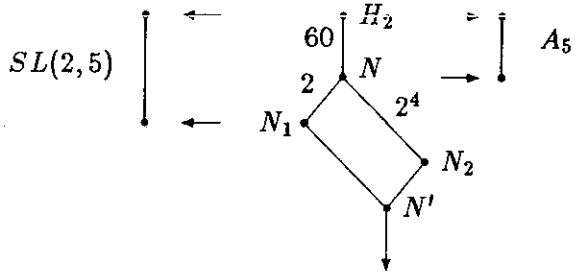
H. Heineken propôs numa comunicação particular o problema de investigar os grupos

$$H_1 = \langle a,b,c \,|\, [a,b]=c,\ \ [b,c]=a,\ \ [c,a]=b\rangle \quad e$$

$$H_2 = \langle a,b,c, \,|\, [a,\,[a,b]]=c,\ \ [b,\,[b,c]]=a,\ \ [c,\,[c,a]]=b\rangle.$$

Ambos são obviamente iguais aos seus grupos de comutadores. Usando o método de Todd–Coxeter pudemos mostrar que H_1 é um grupo trivial (apesar de mais de 100 números de classe serem definidos no decorrer do processo, antes de se chegar a essa conclusão). Tentativas de conseguir uma ordem finita para H_2 via o método de Todd–Coxeter novamente falharam. O método do "Índice Baixo" produziu uma classe de subgrupos de índice 5 e o algoritmo de Scheier–Sims mostrou que o grupo quociente de G por N (a intersecção desses subgrupos de índece 5) é isomorfo a

A_5. O método de Reidemeister–Scheier produz uma apresentação bem complicada para N; abelianizando, vemos que N/N' é isomorfo ao produto direto de 5 cópias do grupo cíclico de ordem 2. Agora temos um grupo quociente H_2/N' de ordem $60 \cdot 2^5$. Pode–se mostrar que N/N' sob a ação de H_2 é o produto direto de um fator principal N_2/N' de ordem 2 e um fator principal N_1/N' de ordem 2^4 e que H_2/N_1 é isomorfo a $SL(2,5)$. O métod das representações em $SL(2,\cdot)$, usando o sistema de manipulação de formulas $MAPLE$, nos mostra que esse é de fato o único grupo quociente de tipo $SL(2,\cdot)$ de H_2.



A tentativa de mostrar que H_2 é infinito exibindo um grupo quociente abeliano livre de um subgrupo de índice pequeno, falhou. Perguntamos então, se podemos encontrar outros grupos quocientes de N. Se esses forem nilpotentes então pelo teorema da Base de Burnside eles devem ser grupos de ordem de potência de 2 que poderão ser gerados por 5 geradores.

Um método para encontar esses grupos é o algoritmo do quociente nilpotente de I. D. MacDonald [Mac 74]. Esse algoritmo constrói indutivamente, para um grupo G dado pela apresentação finita

$$G = \langle g_1, \ldots, g_n \mid R \rangle$$

(onde R é um conjunto finito definidor de relações para G) e para um dado primo p, os fatores da "cadeia p–central descendente" definida por

$$G_0 := G, \quad G_i := [G_{i-1}, G] \cdot G_{i-1}^p$$

Aqui o grupo comutador relativo $[U, V]$ de dois subgrupos U e V de G é o fecho normal do conjunto de todos os comutadores $[u, v]$, $u \in U$ e $v \in V$, e U^p é o fecho normal do conjunto de p–potências dos elementos de U. Se $G_k = \langle 1 \rangle$ mas $G_{k-1} \neq \langle 1 \rangle$, dizemos que G é de p–classe k. Para cada grupo quociente G/G_i, construiremos um tipo especial de apresentação que será exposto a seguir.

Seja P um p–grupo e

$$P_0 := P > P_1 > \cdots > P_r = \langle 1 \rangle$$

uma série de subgrupos normais $P_i \lhd P$ tal que P_{i-1}/P_i é de ordem p e está contido no centro de G/P_i. Essa série será chamada uma *série central com degraus tipo p* de G. Escolhendo para cada $i = 1, \ldots, r$ um elemento a_i tal que $\langle P_i a_i \rangle = P_{i-1}/P_i$, obtemos um conjunto gerador $\{a_1, \ldots, a_r\}$ de P para o qual as relações definidoras são da forma

$$a_i^r = a_{i+1}^{\nu_{i,i+1}} \cdots a_r^{\nu_{i,r}} \qquad \text{para} \qquad i = 1, \ldots, r$$

$$(*) \qquad [a_j, a_i] = a_{j+1}^{\nu_{j,i,i+1}} \cdots a_r^{\nu_{j,i,r}} \quad \text{para} \quad j > i$$

podem ser encontradas. Cada elemento em P pode ser escrito na forma

$$a_1^{\alpha_1} \cdots a_r^{\alpha_r} \quad \text{com} \quad 0 \leq \alpha_i < p,$$

e a multiplicação de dois elementos nessa forma pode ser feita "coletando" o produto usando as relações, de maneira similar à explicada na seção 2 para os grupos diedrais.

Agora, qualquer conjunto de relações da forma (*) claramente define um p–grupo de ordem $\leq p^r$. Podemos ver no exemplo da apresentação

$$\langle a_1, a_2, a_3 \quad | \quad a_1^2 = a_2, \ \ a_2^2 = a_3, \ \ a_3^2 = 1, \\ [a_2, a_1] = a_3, \ \ [a_3, a_1 = 1, \ \ [a_3, a_2] = 1 \rangle$$

que a ordem não precisa ser exatamente p^r. O grupo assim definido não é de ordem 2^3 mas de ordem 2^2, e isso é visto de forma sistemática calculando a_1^3 de *duas maneiras*:

$$a_1 a_2 = a_1 a_1^2 = a_1^3 = a_1^2 a_1 = a_2 a_1 = a_1 a_2 \, [a_2, a_1] = a_1 a_2 a_3,$$

e portanto $a_3 = 1$.

Dizemos que uma apresentação do tipo (*) é *consistente* se ela define um grupo de ordem exatamente p^r, onde r é comprimento da sua serie central com degraus de tipo p. É possível checar a constência de uma apresentação do tipo (*), verificando "de duas maneiras" um número finito de palavras–testes da forma

$$a_i^{p+1}, \quad a_i a_j^p, \quad a_i^p a_j, \quad a_i a_j a_k$$

com $i > j > k$ (ver [New 76] para detalhes). Tendo definido esses termos, podemos agora afirmar que o algoritmo do quociente nilpotente determina recursivamente uma apresentação consistente da forma (*) para cada grupo quociente G/G_i da série p–central descendente.

Consideremos de novo um grupo

$$G = \langle g_1, \ldots, g_n \mid R \rangle$$

finitamente apresentado. Então o gruppo G/G_1 é o maior p–grupo quociente abeliano elementar de G, e por esse fato ele pode ser calculado efetuando o algoritmo dos divisores elementares módulo p. Isso nos leva à apresentação

(1) $$G/G_1 = \langle a_1, \ldots, a_d \mid a_i^p = 1, \ [a_j, a_i] = 1 \rangle$$

onde os a_i's podem ser escolhidos das classes $\overline{g}_i = G_1 g_i$. Note que pelo Teorema de Base de Burnside o número de geradores de qualquer grupo p–quociente de G pode ser no máximo d.

G/G_1 também tem a apresentação

(2) $$G/G_1 = \langle \quad g_1, \ldots, g_n, \ a_1, \ldots a_d \mid R, \ g_i = \Pi\, a_k^{\nu_k}, \ a_k^p = 1, \ [a_j, a_k] = 1 \rangle$$

na qual para cada a_k haverá uma relação $a_k = g_{i_k}$; essas serão chamadas as "definições" de a_k e não serão mudadas no decorrer do trabalho.

Os cálculos de G/G_2 a partir de G/G_1 (e analogamente, G/G_i de G/G_{i-1}) são agora feitos em três etapas.

(i) Na primeira etapa definimos um *p–recobrimento* $C(H)$ de um p–grupo H de p–classe b como sendo um p–grupo K de p–classe

$b+1$ com $K/K_b \cong H$ que é maximal tendo essa propriedade.

Uma apresentaão para o p–recobrimento $C(G/G_i)$ é obtida modificando todas as relações em (1) que não são definições, em congruências modulo novos geradores centrais a_k de ordem p.

(ii) A apresentação de $C(G/G_1)$, assim obtida, é da forma (*) mas pode não ser consistente. Avaliando as palavras testes, conseguimos um número finito de equações entre os geradores recém introduzidos. Como todos são centrais de ordem p, nós então temos que resolver um sistema de equações lineares homogêneas sobre o corpo de p elementos para eliminar os geradores redundantes e para ter uma apresentação consistente do tipo (*) para $C(G/G_1)$.

(iii) No terceiro passo, as relações em (2) que expressam os g_i em termos dos a_k, e que não são proibidas por serem definições dos a_k, são também modificadas pelos novos geradores (que são forçados a serem centrais de ordem p). Essas expressões dos g_i's são usadas para escrever as relações R em termos dos a_k. Essas relações são então coletadas e possivelmente nos levarão a outras equações lineares homogêneas entre os geradores recém introduzidos e portanto a novas eliminações.

Depois desses três passos, chegamos a uma apresentaçào consistente para G/G_2 do tipo (*) e podemos começar a construção de G/G_3, e assim por diante.

O algoritmo do quociente nilpotente teve uma de suas aplicações mais interessantes nos grupos de Burnside. Ele foi usado por M. F. Newman e G. Havas para mostrar que o grupo de Burnside restrito $\overline{B}(4,4)$ (o maior grupo nilpotente de 4 geradores, tendo expoente 4) tem ordem 2^{422}. Veja [HaN 80] para um relato dessas aplicações e para uma boa descrição do método.

Aplicando o algoritmo do quociente nilpotente na apresentação do subgrupo normal N do grupo de Heineken H_2, obtemos que N tem um grupo 2–quociente maximal de ordem 2^{24}; assim, obtemos um grupo–quociente de H_2 de ordem $60 \cdot 2^{24}$. Nesse ponto chegamos ao fim do que já foi explorado até o momento sobre H_2. Algumas tentativas de investigar a apresentação de outros subgrupos não trouxeram nenhuma outra informação. Parece estarmos no limite das possibilidades computacionais atuais, sem podermos

determinar se H_2 tem realmente ordem $60 \cdot 2^{24}$ ou se é infinito.

Novos métodos para encontrar quocientes solúveis, propostos recentemente e no momento sendo implementados, podem talvez permitir que saibamos mais sobre esse e outros grupos. Este exemplo então serve para mostrar que os "métodos computacionais de grupos" obviamente tem seus limites mas também é um assunto em desenvolvimento e aberto a novas idéias.

9. Implementações e Computadores

Todos os métodos que foram mencionados neste artigo foram implementados, na maioria dos casos, com muitos aperfeiçoamentos e refinamentos técnicos demais para serem aqui descritos. O programa mais abrangente em teoria dos grupos é o CAYLEY [Can 84]; ele é montado sobre um sistema gerencial de armazenamento chamado STACKHANDLER e possui sua própria linguagem, orientada para a formulaçào de problemas, que pode ser usada para combinar algoritmos implementados no sistema. O CAYLEY foi originalmente escrito em FORTRAN; uma mudança para *C* é também disponível. Outros sistemas mais especializados são: CAS, [NPP 84], para o trabalho de interação com caracteres; SOGOS, [LNS 84], para trabalhar com grupos solúveis; CAMAC para a aplicação de teoria dos Grupos em Combinatória e na Teoria de Codificação.

Endereços para contato:

CAYLEY: J. Cannon, Departament of Pure Mathematics, Universty of Sydney, Sydney, NSW 2006, Australia.

CAS, SOGOS: J. Neubüser, Lehrstuhl D für Mathematik, RWTH, 5100 Aachen, West Germany.

CAMAC: J. Leon, Department of Mathematics, University of Illinois at Chicago Box 4348, Chicago, Illinois 606380, USA.

Além desses há os sistemas menores e as implementações individuais de apenas um algoritmo. Além dos endereços dados acima, um bom endereço (por exemplo para Todd–Coxeter, Quociente

Nilpotente, etc.) é:

G. Havas: Division of Computing Research, CSIRO.
P. O. Box 1800, Canberra, ACT 2601, Australia.

Todos esses programas rodam muito bem em mini–computadores do tipo "workstation" tendo em torno de 2 Mbyte RAM, um disco rígido com $\geq$ 40 MByte gerenciado através de memória virtual e uma CPU baseada em algo equivalente ao chip Motorola 68020. Para muitos programas, menos que isso é suficiente, por exemplo Motorola 68010. A preferência dos sistemas operacionais parece tender hoje em dia para o UNIX, embora existem implementações de CAYLEY, CAS e SOGOS para alguns computadores, por exemplo para o VAX, usando o sistema VMS.

10. Um Epílogo

Os métodos de "Teoria computacional de grupos", que pudemos esboçar neste artigo, como também a álgebra computacional que lida com a aritmética polinomial, e integração de funções e equações diferenciais na sua forma fechada, se tornaram poderosas ferramentas na pesquisa. Por isso eles precisam encontrar seu espaço no ensino.

Isso não significa necessariamente a introdução de novos cursos. A discussão desses métodos pode ser integrada nos cursos já existentes, enriquecendo–os com os aspectos algorítmicos. Além do mais, os estudantes de pós–graduação podem aprender a implementar e usar tais métodos no contexto de suas teses de mestrado.

No Brasil, as universidades logo terão que enfrentar o problema de preparar a maioria de seus alunos de mestrado para trabalhar nas indústrias, como já acontece em países industrializados. Se os matemáticos puros forem tomar parte desse processo, o método ideal de formação dos alunos será a dosagem adequada de treinamento algorítmico e computacional com a habilidade e a arte de descobrir e demonstrar fatos matemáticos.

11. Apêndice

O apêndice contém os cálculos da tabela modificada de classes para o grupo C_1 com relação ao subgrupo $U = \langle a \rangle$.

As definições, suas consequências, a eliminação do número de classe 9, e a determinação das relações que o gerador do subgrupo satisfaz, são listadas num protocolo na ordem em que elas ocorreram. Definições e consequências são enumeradas separadamentes por $D_1, \ldots,$ e $C_1, \ldots$ respectivamente.

Nas tabelas de relações, lugares que poduzem consequências são sublinhadas. Cada nova consequência é marcada com seu número no protocolo, o qual é fixada no final, debaixo do subtraço. A duplicação de consequências já conhecidas são sublinhadas com linhas tracejadas. As consequências que produzem as relações definidoras para o gerador do subgrupo são sublinhados com linhas pontilhadas.

Na tabela de classe, as definições são sublinhadas. As entradas que são consequências são marcadas com o número da respectiva consequência no protocolo.

Anterior à eliminação do número 9, este ocorreu em diversos lugares nas tabelas de relações. Nesses lugares o número 9 é cortado e seu substituto é colocado junto com ele.

Se em todas as entradas as potências de h são eliminadas, então o procedimento original de Todd–Coxeter será recuperado.

$$C_1 = \langle\, a, b \mid a^{-2}bab^{-1}ab = 1,\ a^3b^{-1}a^{-2}b^{-1} = 1 \,\rangle,$$

$$U = \langle a \rangle, \quad h := a$$

Tabela de Subgrupo

a
$1 \mid h1$

Tabela da Primeira Relação

a^{-1}	a^{-1} b	a	b^{-1} a	b	
1	$h^{-1}1$	$h^{-2}1$	$h^{-2}2$	$h^{-2}4$ $h^{-3}4$	3 1
2	6	$h^{-2}7$	$h^{-1}6$	$h^{-1}2$ $h^{-1}1$ [2]	1 2
3	$h^{-3}4$	$h^{-3}2$	$h^{-3}5$ [4]	$h^{-3}9$ $h8$ $h^{-4}5$	8 3
4	2	6	$h^{-1}10$	$h^{-1}5$ $h^{-1}2$ [7]	$h^{-1}4$ 4
5	10	13	$h^{-1}13$ [5]	$h^{-1}10$ 6	2 5
6	$h^{-2}7$	$h^{-2}3$	$h^{-2}1$ [11]	$h^{-1}1$ $h^{-1}3$	$h^{-1}7$ 6
7	3	$h^{-3}4$	$h^{-2}4$	$h3$ $h8$	11 7
8	$h^{-4}5$	$h^{-4}10$	$h^{-4}12$	$h^{-5}12$ [9] $h^{-5}10$	$h^{-5}5$ [8] 8
9	5	10			9
10	13	$h^{-2}11$	$h^{-2}7$	6 $h^{-1}7$	$h6$ 10
11	$h8$	$h^{-3}5$ [12]	$h^{2}8$	$h11$ $h^{-4}12$	$h^{-5}12$ 11
12	$h12$	$h^{2}12$	$h^{7}11$	$h^{9}13$ $h^{10}13$	10 12
13	$h^{-2}11$	$h^{-1}8$	$h^{-1}3$	$h^{-1}7$ $h^{-1}11$	$h13$ [13] 13

Tabela da Segunda Relação

a	a	a	b^{-1}	a^{-1}	a^{-1}	b^{-1}	
1	$h1$	$h^2 1$	$h^3 1$	$h^3 1$	4	2	1
2	4	$h^3 3$	$h^3 7$	$h^3 11$	$9\ h^4 8$ [1]	5	2
3	7	$h^2 6$	$h^2 2$	$h^2 1$	$h1$	1	3
4	$h^3 3$	$h^3 7$ [3]	$h^5 6$	$h^4 7$	$h^4 3$	$h4$	4
5	$9\ h^4 8$	$h^3 11$	$h^5 13$	$h^6 13$	$h^4 11$	$h^5 8$	5
6	2	4	$h^3 3$	$h^3 8$	$h^{-1} 5$	$h^{-1} 10$	6
7	$h^2 6$	$h^2 2$	$h^2 4$	$h4$	$h2$ [6]	$h6$	7
8	$h^{-1} 11$	$h13$	$h10$	$h^2 6$	7	3	8
9							9
10	5	$h^4 8$	$h^3 11$	$h^{-2} 12$	$h^{-1} 12$	12	10
11	$h^2 13$	$h^2 10$	$h^2 5$	$h^2 2$ [10]	$h^2 6$	7	11
12	$h^{-1} 12$	$h^{-2} 12$	$h^{-3} 12$	$h^{-3} 10$	$h^{-3} 13$	$h^5 11$ [14]	12
13	10	5	$h^4 8$	$h^{-1} 5$	$h^{-1} 10$	$h^{-1} 13$	13

Tabela de Classes Laterais

	a	b	a^{-1}	b^{-1}
1	$h\mathbf{1}_0$	$\underline{\mathbf{2}}$	$h^{-1}\mathbf{1}_0$	$\underline{\mathbf{3}}$
2	$\underline{\mathbf{4}}$	$\underline{\mathbf{5}}$	$\underline{\mathbf{6}}$	$\underline{\mathbf{1}}$
3	$\underline{\mathbf{7}}$	$\underline{\mathbf{1}}$	$h^{-3}\mathbf{4}_1$	$\underline{\mathbf{8}}$
4	$h^3\mathbf{3}_1$	$h\mathbf{4}_2$	$\underline{\mathbf{2}}$	$h^{-1}\mathbf{4}_2$
5	$\not{\mathbf{9}}\ h^4\mathbf{8}_6$	$h^5\mathbf{8}_7$	$\underline{\mathbf{10}}$	$\underline{\mathbf{2}}$
6	$\underline{\mathbf{2}}$	$h^{-1}\mathbf{10}_5$	$h^{-2}\mathbf{7}_3$	$h^{-1}\mathbf{7}_4$
7	$h^2\mathbf{6}_3$	$h\mathbf{6}_4$	$\underline{\mathbf{3}}$	$\underline{\mathbf{11}}$
8	$h^{-1}\mathbf{11}_8$	$\underline{\mathbf{3}}$	$h^{-4}\mathbf{5}_6$	$h^{-5}\mathbf{5}_7$
$\not{\mathbf{9}}$			$\underline{\not{\mathbf{5}}}$	
10	$\underline{\mathbf{5}}$	$\underline{\mathbf{12}}$	$\underline{\mathbf{13}}$	$h\mathbf{6}_5$
11	$h^2\mathbf{13}_{12}$	$\underline{\mathbf{7}}$	$h\mathbf{8}_8$	$h^{-5}\mathbf{12}_{10}$
12	$h^{-1}\mathbf{12}_9$	$h^5\mathbf{11}_{10}$	$h\mathbf{12}_9$	$\underline{\mathbf{10}}$
13	$\underline{\mathbf{10}}$	$h^{-1}\mathbf{13}_{11}$	$h^{-2}\mathbf{11}_{12}$	$h\mathbf{13}_{11}$

Protocolo (D=Definição, C=Consequência)

$C0$ $\quad 1a = h1, \quad 1a^{-1} = h^{-1}1$

$D1$ $\quad 1b =: 2$

$D2$ $\quad 1b^{-1} =: 3$

$D3$ $\quad 2a =: 4$

$C1$ $\quad 3a^{-1} = h^{-3}4, \quad 4a = h^{3}3$

$C2$ $\quad 4b^{-1} = h^{-1}4, \quad 4b = h4$

$D4$ $\quad 2b =: 5$

$D5$ $\quad 2a^{-1} =: 6$

$D6$ $\quad 3a =: 7$

$C3$ $\quad 7a = h^{2}6, \quad 6a^{-1} = h^{-2}7$

$C4$ $\quad 7b = h6, \quad 6b^{-1} = h^{-1}7$

$D7$ $\quad 3b^{-1} =: 8$

$D8$ $\quad 5a =: 9$

$D9$ $\quad 5a^{-1} =: 10$

$C5$ $\quad 6b = h^{-1}10, \quad 10b^{-1} = h6$

$C6$ $\quad 8a^{-1} = h^{-4}5, \quad 5a = h^{4}8$
de tabela de classe $\quad 5a = 9$ $\Rightarrow 9 = h^{4}8$

$C7$ $\quad 8b^{-1} = h^{-5}5, \quad 5b = h^{5}8$

$D10$ $\quad 7b^{-1} =: 11$

$C8$ $\quad 11a^{-1} = h8, \quad 8a = h^{-1}11$

$D11$ $\quad 10b =: 12$

$C9$ $\quad 12a = h^{-1}12, \quad 12a^{-1} = h12$

$C10$ $\quad 11b^{-1} = h^{-5}12, \quad 12b = h^{5}11$

$D12$ $\quad 10a^{-1} =: 13$

$C11$ $\quad 13b = h^{-1}13, \quad 13b^{-1} = h13$

$C12$ $\quad 13a^{-1} = h^{-2}11, \quad 11a = h^{2}13$

$C13$ $\quad h^{10}13a = 10$
de tabela de classe $\quad 13a = 10$ $\Rightarrow \underline{h^{10} = 1}$

$C14$ $\quad h^{-3}13a^{-1} = h^{5}11$
de tabela de classe $\quad h^{-3}13a^{-1} = h^{-5}11$ $\Rightarrow \underline{h^{10} = 1}$

12. Bibliografia

[Atk 84] M.D. Atkinson, ed., Computational group theory. Academic Press, London (1984).

[ARo 84] D.G. Arrell, E.F. Robertson, A modified Todd-Coxeter Algorithm. pp. 27-32 em [Atk 84].

[Can 84] J.J. Cannon, An introduction to the group theory language, Cayley. pp. 145-183 em [Atk 84].

[Cav 86] A. Cavicchioli, A countable class of non-homeomorphic homology spheres with Heegard genus 2. Geom. Dedicata 20 (1986) 345-348.

[Deh 11] M. Dehn, Über unendliche diskontinuierliche Gruppen. Math. Annalen 71 (1911) 116-144.

[Hac 86] D. Hacon, O invariante de Jones e outros invariantes de nos. Matematica Universitaria No 3 (1986) 61-83.

[HaN 80] G. Havas, M.F. Newman, Application of computers to questions like those of Burnside. Lecture Notes in Math. 806, Springer, Berlin (1980) 211-230.

[Hup 67] B. Huppert, Endliche Gruppen I. Springer-Verlag (1967).

[Joh 80] D.L. Johnson, Topics in the theory of group presentations. LMS Lecture Notes Series 42, Cambridge U.P. (1980).

[Leo 80a] J.S. Leon, Finding the order of a permutation group. pp. 511-517 em: B. Cooperstein, G. Mason, eds.: Proc. Symp. Pure Math. 37, AMS (1980).

[Leo 80b] J.S. Leon, On an algorithm for finding a base and a strong generating set for a group given by generating permutations. Math. Comp. 35 (1980) 941-974.

[LNS 84] R. Laue, J. Neubüser, U. Schoenwaelder, Algorithms for finite soluble groups and the SOGOS system. pp. 105-135 em [Atk 84].

[Mac 74] I.D. Macdonald, A computer application to finite p-groups. J. Austral. Math. Soc. 17 (1974) 102-112.

[Mag 81] W. Magnus, The uses of 2 by 2 matrices in combinatorial group theory. A survey. Resul. der Mat. 4 (1981) 171 - 192.

[MAP 85] B.W. Char, K.O. Geddes, G.H. Gonnet, S.M. Watt, MAPLE Reference Manual. Symbolic Computation Group, Department of Computer Science, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1 (1985).

[Neu 82] J. Neubüser, An elementary introduction to coset table methods in computational group theory. pp. 1-45 em: C. Campbell, E. Robertson, eds.: Groups St. Andrews 81, LMS Lecture Note Series 71, Cambridge U.P. (1982).

[New 76] M.F. Newman, Calculating presentations for certain kinds of quotient groups, pp. 2-8 em: R.D. Jenks, ed.: SYMSAC 76, Assoc. Comp. Mach., New York, (1976).

[NPP 84] J. Neubüser, H. Pahlings, W. Plesken, CAS; Design and use of a system for the handling of characters of finite groups. pp. 195-247 em [Atk 84].

[Nov 55] P.S. Novikov, On the algorithmic unsolvability of the word problem in group theory. Trudy Mat. Inst. im Steklov 44 (1955) 143pp; AMS Translations, ser. 2, 9 (1958) 1-122.

[Rab 58] M.O. Rabin, Recursive unsolvability of group theoretic problems. Ann. of Math., 67 (1958) 172-194.

[ToC 36] J.A. Todd, H.S.M. Coxeter, A practical method for enumerating cosets of a finite abstract group. Proc. Edinburgh Math. Soc. 5 (1936) 26-34.