Konstruktive Aspekte in der Gruppentheorie

Merseburg, Oktober 2004

Methoden eine Gruppe konstruktiv darzustellen

1. Als Permutations- oder Matrixgruppe

   Beispiele: $G := \langle\, (1,2),\, (2,3,4) \,\rangle$

   $$G := \left\langle \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle.$$

2. Als endliche Präsentation

   Beispiel: $G := \langle\, x, y \mid x^2,\, y^3,\, (xy)^4 \,\rangle$.

3. Als PC-Präsentation

   Beispiel: $G := \langle\, w, x, y, z \mid$

   $w^2 = 1,\, x^3 = 1,\, y^2 = 1,\, z^2 = 1,$

   $w^{-1}xw = x^{-1},\, w^{-1}yw = y,\, x^{-1}yx = z,$

   $w^{-1}zw = yz,\, x^{-1}zx = yz,\, y^{-1}zy = z \;\; \rangle$.

Berechnung mit Permutationsgruppen

Ansatz von Charles Sims (1970) mit der BSGS Datenstruktur.

Sei $G := \langle x_1, \ldots, x_r \rangle \leq \mathrm{Sym}(n)$ gegeben.

Polynomiale Algorithmen:

- Finde $|G|$
- Entscheide ob $g \in G$ für $g \in \mathrm{Sym}(n)$
- Berechne $[G, G]$, $\mathrm{Z}(G)$, $\mathrm{O}_p(G)$, $\mathrm{O}\infty(G), \ldots$

Nichtpolynomiale Algorithmen:

- Berechne $C_G(g)$ für $g \in \mathrm{Sym}(n)$
- $g, h \in \mathrm{Sym}(n)$: $\exists x \in G$ mit $x^{-1}gx = h$?
- Berechne $G \cap H$ für $H \leq \mathrm{Sym}(n)$
- Berechne G_Δ für $\Delta \subseteq [1..n]$

Liften durch elementaren Schichten

Sei G eine endliche Gruppe mit $N, M \trianglelefteq G$, und M/N eine elementar-abelsche p-Gruppe.

Für viele Probleme ist es möglich eine Lösung in G/M zu einer Lösung in G/N zu liften, mit Techniken der Linearen Algebra.

Zum Beispiel:

- Finde Vertreter der Konjugiertenklassen von G/N
- Finde die (maximale) Untergruppen von G/N
- Berechne Aut(G/N)

Man betrachtet M/N als $F(G/M)$-Modul, wobei F der endliche Körper der Ordnung p ist.

Eine endliche Präsentation von G/M ist erforderlich, um (zum Beispiel) $H^1(G/M, M/N)$ zu berechnen.

Für eine endliche auflösbare Gruppe G haben wir eine Untergruppenreihe:

$$G = N_0 \geq N_1 \geq \cdots \geq N_{r-1} \geq N_r = 1$$

mit $N_i \trianglelefteq G$ und N_{i-1}/N_i elementar-abelsch, und wir können solche Problem induktiv lösen.

Im allgemeinen, sei $R := \mathrm{O}_\infty(G)$ das *auflösbare Radikal* von G. Dann haben wir eine Reihe:

$$R = N_0 \geq N_1 \geq \cdots \geq N_{r-1} \geq N_r = 1$$

mit $N_i \trianglelefteq G$ und N_{i-1}/N_i elementar-abelsch.

Wenn wir ein Problem dieses Typs in der *Radikal-freie* Gruppe G/R lösen können, dann können wir es auch in G lösen.

Radikalfreie Gruppen

Der *Sockel* S einer radikalfreien Gruppe G ist ein direktes Produkt

$$S = S_1 \times S_2 \times \cdots \times S_k$$

nichtabelschen einfachen Gruppen S_i, wobei die Gruppen S_i unter der Konjugationswirkung von G vertauscht werden.

Sei K der Kern der entsprechenden Permutationsdarstellung von G auf $\{S_1, S_2, \ldots, S_k\}$, und sei $S_i \leq A_i$ mit $A_i \cong \mathrm{Aut}(S_i)$.

Dann haben wir $S \trianglelefteq K \trianglelefteq G$, wobei $G/K \lesssim \mathrm{Sym}(k)$, und

$$K/S \lesssim A_1/S_1 \times A_2/S_2 \times \cdots \times A_k/S_k.$$

Gewisse Probleme können in G gelöst werden, falls sie in den Gruppen T_i mit $S_i \leq T_i \leq A_i$ gelöst werden können, wobei $T_i \cong \mathbf{N}_G(S_i)/\mathbf{C}_G(S_i)$.

Zum Beispiel:

- Berechne Aut(G)
- Finde die maximale Untergruppen von G (Kovács (1986), Aschbacher/Scott)
- Finde Vertreter der Konjugiertenklassen von G

We können deshalb auf den Fall wenn G *fast-einfach* ist reduzieren.

Das heißt $S \leq G \leq A \cong$ Aut(S) für eine nicht-abelsche einfache Gruppe S.

Die endlichen einfachen Gruppen sind zirka 1980 klassifiziert worden, und viele ihrer grundlegenden Eigenschaften sind nun bekannt oder wohlverstanden.

Zum Beispiel:

- Automorphismengruppen sind alle bekannt
- Maximale Untergruppen sind wohlverstanden, und sind alle bekannt für die (fast)einfachen Gruppen im Bereich der Berechenbarkeit.
- Konjugiertenklassen sind für die kleineren Gruppen und die sporadischen Gruppen bekannt und für Gruppen vom Lie Typ wohlverstanden.
- Sylowgruppen sind bekannt.
- Vieles ist über ihre Charaktere bekannt.

Standarddarstellungen

Für jeden Isomorphietyp von fasteinfachen Gruppen wählen wir eine *Standarddarstellung*.

Daß soll eine bestimmte Permutations- oder Matrixdarstellung der Gruppe A mit kleinstmöglichem Grad sein. Es kann auch eine projektive Matrixdarstellung sein.

Zum Beispiel:

- $G \cong \mathrm{Alt}(n)$, $\mathrm{Sym}(n)$: wir nehmen die natürliche Darstellung auf der Menge $\{1, 2, \ldots, n\}$.
- $G \cong \mathrm{PSL}(n, q)$, $\mathrm{PGL}(n, q)$: wir wählen die projektive Darstellung auf $\mathrm{SL}(n, q)$ oder $\mathrm{GL}(n, q)$.
- Für sporadische Gruppen ist es nicht klar, ob eine Permutationsdarstellung oder eine Matrixdarstellung am zweckmäßigsten ist:

  $M_{24} \leq \mathrm{Sym}(24)$

  $3.J_1 \lesssim \mathrm{GL}(7, 11)$ oder $J_1 \lesssim \mathrm{Sym}(266)$

Identifikation von fasteinfachen Gruppen

Sei A eine vorgegebene fasteinfache Gruppe mit einfachem Sockel S.

Wir machen mit den folgenden Schritten weiter:

S1. Den Isomorphietyp von S und von A erkennen.

S2. Eine Standarddarstellung $\phi : A \to \hat{A}$ von A berechnen.

S3. Das Problem in $\hat{A}$ lösen.

S4. Die Lösung des Problems in A als Urbild unter ϕ finden.

S1: Den Isomorphietyp von S, A erkennen

Für Permutationsgruppen und für kleinere Matrixgruppen können wir $|S|$ und $|A|$ berechnen, und dann ist S1 leicht durchzuführen.

Für größere Matrixgruppen kann es schwer sein $|S|$ ohne weiteres zu berechnen - in solchen Fällen kennen wir $|S|$ erst nachdem wir S1 und S2 durchgeführt haben.

Wir können aber mit Hilfe einer Methode von C.R. Leedham-Green und F.Celler die Ordnung einer großen Matrix über einem endlichen Körper (ungefähr) berechnen.

Wir können auch Zufallselemente aus A wählen.

Es ist möglich, den Isomorphietyp von S von den Ordnungen von 100 (?) Zufallselementen aus S mit sehr hoher Wahrscheinlichkeit zu erraten.

Die Durchführung von S2 wird diese Vermutung definitiv bestätigen.

S2. Eine Standarddarstellung $\phi : A \to \widehat{A}$ von A berechnen

Für diesen Schritt werden sogenannte *Standarderzueger* der (fast)einfachen Gruppen verwendet.

Solche Erzeuger sind für viele Beispiele von R.A. Wilson und anderen berechnet worden.

Beispiel: $S = A \cong \mathrm{PSp}(6,5)$

1. Wähle Zufallselemente $g \in A$ bis $o := |g| = 4, 8, 12, 20, 24, 26, 30, 40, 52, 60, 78, 120$ oder 130.
2. Sei $x := g^{o/2}$. (Dann ist $|x| = 2$.)
3. Wähle Zufallselemente $g \in A$ bis $o := |g| = 40$ oder 120.
4. Sei $t := g^{o/8}$. (Dann ist $|t| = 8$.)
5. Wähle Zufallskonjugierte $y := t^g$ von t bis $|xy| = 9$ und $|xyxyxyyxyy| = 15$.

Man wähle auf ähnliche Weise $\widehat{x}$ und $\widehat{y}$ aus dem Bild der Standarddarstellung $\widehat{A}$ von A.

(Vorsicht: $\widehat{A} = \mathrm{Sp}(6,5)$, und wir müssen "Ordnung" als "projektive Ordnung" verstehen.)

Dann ist die gesuchte Standarddarstellung mit $x \mapsto \widehat{x}$, $y \mapsto \widehat{y}$ definiert.

Ein Schwerpunkt der gegenwärtigen Forschung ist allgemeine Verfahren zu entwickeln, wodurch man Standarddarstellungen von ganzen Klassen von Gruppen vom Lie Typ, wie $\mathrm{PSL}(n,q)$, konstruieren kann.

Zur Zeit sind solche Verfahren aber nur teilweise implementiert worden, und ihre Leistungsverhalten ist hinreichend nur für Gruppen mit kleinem grad.

S3. Das Problem in $\widehat{A}$ lösen

Für kleinere Gruppen A können die nötigen Daten in Datenbanken gespeichert werden.

Zum Beispiel: Standarderzeuger; Erzeuger von Repräsentanten der Klassen (maximaler) Untergruppen; Vertreter der Konjugiertenklassen; Präsentationen; Charaktertafeln, ...

Wie früher, braucht man allgemeine Verfahren für die Gruppen vom Lie Typ.

Häufig sind die gewünschten Daten im Prinzip bekannt; man muß aber das abstrakte Wissen ins Konkrete übersetzen.

Übersicht des Ansatzes

Sei G eine endliche Gruppe.

1. Berechne $R := \mathsf{O}_\infty(G)$; sei $\overline{G} := G/R$.
2. Berechne $S := \mathsf{Soc}(\overline{G}) = S_1 \times S_2 \times \cdots \times S_k$.
3. Finde $T_i \cong \mathbf{N}_{\overline{G}}(S_i)/\mathbf{C}_{\overline{G}}(S_i)$ mit $S_i \leq T_i \leq \mathsf{Aut}(S_i)$.
4. Identifiziere die Isomorphietypen von S_i, T_i, und konstruiere die Standarddarstellungen $T_i \to \widehat{T}_i$.
5. Das Problem in den Gruppen $\widehat{T}_i$ lösen.
6. Das Problem in der radikalfreien Gruppe $\overline{G}$ lösen.
7. Das Problem in G lösen, durch Liften durch elementar-abelsche Schichten von R.