Solvable Group Generation

Max Horn

Joint work with Bettina Eick

23. Mai 2013

JUSTUS-LIEBIG-
UNIVERSITÄT
GIESSEN

Overview

Groups of a given order

All groups in this talk are finite.

- Constructing all groups of a given order is an old and fundamental topic in finite group theory.
- Goal: Compute a list of groups of order o such that every group of order o is isomorphic to exactly one group in the list.
- In the early history these are based on hand calculations; in more recent years algorithms have been developed for this purpose.
- There exist extensive amounts of literature on the subject.

The naive approach

- Suppose $o \in \mathbb{N}$ and we have constructed all groups of order $< o$.
- Any non-simple G of order o must fit into an exact sequence

$$1 \to N \to G \to H \to 1$$

  where H and N have order $< o$, so are already known.

- Construct all extensions of pairs N, H with $|N| \cdot |H| = o$:
  1. Determine possible actions of H on N
     $\rightsquigarrow$ find coupling homomorphisms $\chi : H \mapsto \mathrm{Out}(N)$.
  2. Compute extensions w.r.t. χ (typically using group cohomology)

Pitfalls

- Problem: The resulting list will contain many isomorphic groups.
- Extensions of group N by H can be isomorphic to extensions of different groups N', H'.
- Dealing with that is the primary bottleneck of this approach.
- Our approach completely avoids this problem, at least in the class of solvable groups.

p-groups

- Suppose G is p-group. The p-central series of G is

$$G = \mu_0(G) \rhd \mu_1(G) \rhd \ldots \rhd \mu_c(G) = 1$$

  where $\mu_0(G) := G$ and $\mu_{i+1}(G) := [G, \mu_i(G)]\mu_i(G)^p$ for $i \geq 0$.
- This series has some nice properties:
  - The $\mu_i(G)$ are characteristic in G
  - $\mu_i(G)/\mu_{i+1}(G)$ is elementary abelian (= $\mathbb{F}_p$-vectorspace).
  - G acts trivially on $\mu_i(G)/\mu_{i+1}(G)$ (= the series is centralized by G).
- The p-class of G is the length c of the p-central series.
- $G/\mu_{c-1}(G)$ has p-class $c-1$ is called (immediate) ancestor of G.
- G is an (immediate) descendant of $G/\mu_{c-1}(G)$.

The p-group generation algorithm

- The p-group generation algorithm [Newman, O'Brien] constructs groups of order $o = p^n$ up to isomorphism.
- Take group G of order p^m, $m < n$, and trivial $\mathbb{F}_p G$-module M.
- Find extensions E of G over M such that M embeds into E as last term of the p-central series of $G \implies E$ is a descendant of G.
- p-covering group G^*: an extension of G over a module M^* such that all descendants of G are quotients of G^*
- G, H p-groups with isomorphic descendants $\implies G \cong H$.
- Isomorphism problem for descendants of G is effectively solved by computing orbits of $\mathrm{Aut}(G)$ on submodules of M^*.

The F-central series

- We generalize p-group generation to all finite (solvable) groups.
- Fitting subgroup $F(G)$: maximal nilpotent normal subgroup of G.
- G solvable $\implies$ $F(G)$ is non-trivial.
- Suppose $|F(G)| = p_1^{e_1} \cdots p_r^{e_r}$ is the unique prime factorization. Then the F-exponent of G is $k := p_1 \cdots p_r$ and $i \geq 0$.
- The F-central series of G is the series

$$G \trianglerighteq \nu_0(G) \rhd \nu_1(G) \rhd \ldots \rhd \nu_c(G) = 1,$$

  $\nu_0(G) := F(G)$ and $\nu_{i+1}(G) := [F(G), \nu_i(G)]\, \nu_i(G)^k$ for $i \geq 0$.
- If G is a p-group, this recovers the p-central series.
- The groups in this series are characteristic.

F-class and F-rank

Lemma

For $i \geq 0$, the group $\nu_{i+1}(G)$ is minimal with regard to the properties

1. $\nu_{i+1}(G) \trianglelefteq \nu_i(G)$,
2. $\nu_i(G)/\nu_{i+1}(G)$ *is a direct product of elementary abelian groups,*
3. $\nu_i(G)/\nu_{i+1}(G)$ *is centralized by $F(G)$.*

- Since $F(G)$ is nilpotent, there is $c \geq 0$ such that $\nu_c(G) = \{1\}$.
- The order of the quotient $\nu_0(G)/\nu_1(G)$ is the F-rank of G.
- The smallest such integer c is the F-class of G.
- If G is solvable, $F(G) \neq \{1\}$, hence F-class $c \geq 1$.

Descendants and ancestors

- Suppose G has F-class c (that is, $\nu_c(G) = \{1\} \neq \nu_{c-1}(G)$).
- A group H of F-class $c+1$ with $H/\nu_c(H) \cong G$ is a descendant of G, and G the ancestor of H.

Lemma

$\nu_j(G/\nu_i(G)) = \nu_j(G)/\nu_i(G)$ *for each* $i \geq j \geq 0$.

- Hence descendants of G have the same F-rank ℓ as G.
- G solvable $\implies$ descendants of G are solvable.
- We can construct all (solvable) groups of order o if we have algorithms doing the following (up to isomorphism):
  1. Given an integer ℓ, determine all groups of F-rank ℓ and F-class 1.
  2. Given a (solvable) group G, constructs all descendants of G.

Finite solvable groups of F-class 1

- From now on: G non-trivial finite solvable group.

Lemma

Let G be a solvable group of F-class 1 and F-rank ℓ.

1. *$F(G)$ is a direct product of elementary abelian groups of order ℓ.*
2. *$F(G)$ is self-centralizing in G, i.e. $C_G(F(G)) = F(G)$.*

- If $\ell = p_1^{e_1} \cdots p_r^{e_r}$ then $F(G)$ is a direct product of elementary abelian groups and $\mathrm{Aut}(F(G)) = \mathrm{GL}_{e_1}(p_1) \times \cdots \times \mathrm{GL}_{e_r}(p_r)$.
- $G/F(G)$ embeds into $\mathrm{Aut}(F(G))$.
- Idea:
  - Let $A := C_{p_1}^{e_1} \times \cdots \times C_{p_r}^{e_r}$ (our model for $F(G)$).
  - Determine up to conjugacy all solvable subgroups U of $\mathrm{Aut}(A)$ so that there exists an extension G of A by U with $F(G) \cong A$.

F-relevant subgroups

Recall: $A = C_{p_1}^{e_1} \times \cdots \times C_{p_r}^{e_r}$, $\mathrm{Aut}(A) = \mathrm{GL}_{e_1}(p_1) \times \cdots \times \mathrm{GL}_{e_r}(p_r)$.

Definition

$U \leq \mathrm{Aut}(A)$ is *F-relevant* if there exists an extension G of A by U with $F(G) \cong A$.

Lemma

Let $U \leq \mathrm{Aut}(A)$. Then the following are equivalent:

1. *U is F-relevant.*
2. *Every extension G of A by U satisfies that $F(G) \cong A$.*
3. *No non-trivial normal subgroup of U centralizes a series through A.*

Finding F-relevant subgroups

Recall: $A = C_{p_1}^{e_1} \times \cdots \times C_{p_r}^{e_r}$, $\mathrm{Aut}(A) = \mathrm{GL}_{e_1}(p_1) \times \cdots \times \mathrm{GL}_{e_r}(p_r)$.

Algorithm (`RelevantSolvableSubgroups`)

Input: List $p_1, e_1, p_2, e_2, \ldots, p_r, e_r$

1. For $1 \leq i \leq r$ determine up to conjugacy all solvable subgroups P_i of $\mathrm{GL}_{e_i}(p_i)$ together with their normalizers $R_i = N_{\mathrm{GL}_{e_i}(p_i)}(P_i)$.
2. For each combination $P = P_1 \times \cdots \times P_r$ with normalizer $R = R_1 \times \cdots \times R_r$ determine up to conjugacy all subdirect products U in P together with their normalizers $N_R(U)$.
3. Discard those subdirect products U which are not F-relevant

Output: list of F-relevant subgroups U with their normalizers $N_R(U)$.

Solving the isomorphism problem

- $A = C_{p_1}^{e_1} \times \cdots \times C_{p_r}^{e_r}$, $U \leq \mathrm{Aut}(A) = \mathrm{GL}_{e_1}(p_1) \times \cdots \times \mathrm{GL}_{e_r}(p_r)$.
- Extensions of A by U are parametrized by $H^2(U, A) = Z^2(U, A)/B^2(U, A)$.
- The normalizer $N(U)$ in $\mathrm{Aut}(A)$ acts on $H^2(U, A)$.
- For $\lambda \in Z^2(U, A)$ write $[\lambda] = \lambda + B^2(U, A) \in H^2(U, A)$ and denote the corresponding extension by G_λ.

Theorem

Let U be an F-relevant subgroup of $\mathrm{Aut}(A)$ and let $\delta, \lambda \in Z^2(U, A)$. Then $G_\delta \cong G_\lambda$ if and only if there exists $g \in N(U)$ with $g([\delta]) = [\lambda]$.

- Putting everything together, we can now find the isomorphism classes of groups with F-rank $\ell = |A| = p_1^{e_1} \cdots p_r^{e_r}$ and F-class 1 .

Computing descendants

- Goal: Compute descendants of G up to isomorphism (i.e. all H of F-class $c+1$ with $H/\nu_c(H) \cong G$).
- Choose $1 \to R \to \mathcal{F} \xrightarrow{\mu} G \to 1$ where $\mathcal{F}$ is a free group.
- Let L be the full preimage of $F(G)$ under μ.
- Define F-covering group $G^* := F/[R,L]R^k$ and
  F-multiplicator $M := R/[R,L]R^k$.

Theorem

The isomorphism type of G^* depends only on G and the rank of $\mathcal{F}$.

Allowable subgroups

- Let G be of F-class c with covering group G^* and multiplicator M.
- G^* is a finite group of F-class c or $c+1$.
- M is a direct product of elementary abelian groups.
- $N := \nu_c(G^*)$ is the nucleus of G.
- An allowable subgroup U of G^* is a proper subgroup of M which is normal in G^* and satisfies $M = NU$.

Theorem

Every descendant of H of G^* is isomorphic to G^*/U for some allowable subgroup U, and vice versa.

Solving the isomorphism problem

- Let $\mathrm{Aut}_M(G^*)$ denote the group of automorphisms of G^* which leaves M setwise invariant.

Theorem

Let U_1, U_2 be two allowable subgroups of G^*. Then $G^*/U_1 \cong G^*/U_2$ if and only if there exists $\alpha \in \mathrm{Aut}_M(G^*)$ which maps U_1 onto U_2.

- We only need the subgroup Γ of $\mathrm{Aut}(M)$ induced by $\mathrm{Aut}_M(G^*)$.
- Finding Γ involves lifting automorphisms from $\mathrm{Aut}(G)$ to $\mathrm{Aut}_M(G^*)$, then pushing them down to $\mathrm{Aut}(M)$.

The algorithm

Algorithm (`Descendants`)

Input: G

- Determine G^* with multiplicator M and nucleus N.
- If $|N| = 1$, then return an empty list.
- Determine $\mathrm{Aut}_M(G^*)$ (or rather: Γ) from $\mathrm{Aut}(G)$.
- Determine the set $\mathcal{L}$ of G^*-invariant supplements to N in M.
- Determine orbits and stabilizers for the action of $\mathrm{Aut}_M(G^*)$ on $\mathcal{L}$.
- For each orbit representative U determine $H = G^*/U$ and $\mathrm{Aut}(H)$.

Output: A list of descendants H and their automorphism groups.

Various improvements are possible and in fact necessary to make this effective.

The Small Groups Library

- The Small Groups Library [Besche, Eick, O'Brien] is a database of groups shipped with GAP and Magma. Among its contents are all groups of order at most 2000, except those of order 1024.
- Two applications of our new algorithm to the Small Groups Library are in progress:
  1. Verification of the existing content (for the first time with a completely different algorithm).
  2. Extension to groups up to order 10,000 but excluding multiples of $2^{10} = 1024$ and $3^7 = 2187$.

Groups of order 2304

- As a first step we have deteremined (for the first time) the groups of order $2304 = 2^8 \cdot 3^2$.
- Every group of order 2304 is solvable by Burnside's pq-Theorem.
- Nilpotent groups of order 2304 can be obtained via direct products of p-groups $\rightsquigarrow$ focus on solvable non-nilpotent groups of order 2304.

Groups of order 2304: F-central class 1

- The table lists possible F-ranks ℓ and for each ℓ the number of solvable groups of order 2304 and F-class 1 and F-rank ℓ.
- Missing divisors ℓ do not lead to any groups.
- There are 1953 groups of order 2304 and F-class 1.

ℓ	# of grps
$32 = 2^5$	8
$64 = 2^6$	37
$128 = 2^7$	28
$144 = 2^4 \cdot 3^2$	193
$192 = 2^6 \cdot 3$	208
$256 = 2^8$	9
$288 = 2^5 \cdot 3^2$	834
$384 = 2^7 \cdot 3$	54
$576 = 2^6 \cdot 3^2$	558
$768 = 2^8 \cdot 3$	8
$1134 = 2^7 \cdot 3^2$	16

Groups of order 2304: Descendants and final tally

order	# groups	# non-nilpotent	# grps w/ descendants	# descendants
6	2	1	0	0
12	5	3	0	0
18	5	3	0	0
24	15	10	0	0
36	14	10	0	0
48	52	38	4	34 210
72	50	40	2	6
96	231	180	5	728 926
144	197	169	21	68 945
192	1 543	1 276	6	24 889
288	1 045	943	116	10 835 672
384	20 169	17 841	7	426
576	8 681	8 147	865	1 980 937
768	1 090 235	1 034 143	8	8
1152	157 877	153 221	47 848	1 967 974
	1 280 121	1 216 025	48 882	15 641 993

Total: $112\,184 + 1\,953 + 15\,641\,757 = 15\,755\,894$ groups of order 2304.

Groups of order 2304: Some interesting observations

- The top ten groups according to the number of descendants of order 2304 are shown on the right.
- The descendants of the top group make up 57% of the total.
- The top ten together have almost 80% of the total.
- All have F-central class 1.

	order	group	# desc.
1.	288	1040	8,937,790
2.	576	8590	707,578
3.	96	230	696,554
3.	288	1043	696,554
3.	288	1044	696,554
6.	576	8588	203,006
7.	288	976	160,928
8.	576	8582	131,664
9.	576	8675	120,310
10.	576	8589	110,292

Concluding remarks

- Our result provides a new effective method for determining all solvable groups of a given order.
- The algorithm can also compute the automorphism groups of the computed extensions.
- Implemented as a package for the GAP computer algebra system, uses several other GAP packages: AutPGroup, FGA, genss, Polycyclic.