Cubefree

Construction Algorithm for Cubefree Groups

A GAP4 Package

by

Heiko Dietrich

Institut Computational Mathematics

TU Braunschweig

Pockelsstr. 14
D-38106 Braunschweig

email: h.dietrich@tu-bs.de

May 2007

Contents

1 Introduction

1.1 Overview and Background

This manual describes the Cubefree package, a GAP 4 package for constructing groups of cubefree order; i.e., groups whose order is not divisible by any third power of a prime.

The groups of squarefree order are known for a long time: Hoelder [Hoe95] investigated them at the end of the 19th century. Taunt [Tau55] has considered solvable groups of cubefree order, since he examined solvable groups with abelian Sylow subgroups. Cubefree groups in general are investigated firstly in [Die05] and [DE05], and this package contains the implementation of the algorithms described there.

Some general approaches to construct groups of an arbitrarily given order are described in [BE99a], [BE99b], and [BEO02].

The main function of this package is a method to construct all groups of a given cubefree order up to isomorphism. The algorithm behind this function is described completely in [Die05] and [DE05]. It is a refinement of the methods of the GrpConst package which are described in [BE99c].

This main function needs a method to construct up to conjugacy the solvable cubefree subgroups of $\mathrm{GL}(2,p)$ coprime to p. We split this construction into the construction of reducible and irreducible subgroups of $\mathrm{GL}(2,p)$. To determine the irreducible subgroups we use the method described in [FO05] for which this package also contains an implementation. Alternatively, the Irredsol package [Hoe00] could be used for primes $p \leq 251$.

The algorithm of [FO05] requires a method to rewrite a matrix representation. We use and implement the method of [GH97] for this purpose.

One can modify the construction algorithm for cubefree groups to a very efficient algorithm to construct groups of squarefree order. This is already done in the GrpConst package. Thus for the construction of groups of squarefree order it is more practical to use `AllSmallGroups` of the GrpConst package.

A more detailed description of the implemented methods can be found in Chapter 2.

Chapter 3 explains how to install and load the Cubefree package.

2 Functionality of the Cubefree package

This chapter describes the methods available from the Cubefree package.

2.1 New methods

This section lists the implemented functions.

1 ► `ConstructAllCFGroups(` *order* `)` F

The input *order* has to be a positive cubefree integer. The output is a complete and irredundant list of isomorphism type representatives of groups of this size. If possible, the groups are given as pc groups and as permutations groups otherwise.

2 ► `ConstructAllCFSolvableGroups(` *order* `)` F

The input *order* has to be a positive cubefree integer. The output is a complete and irredundant list of isomorphism type representatives of solvable groups of this size. The groups are given as pc groups.

3 ► `ConstructAllCFNilpotentGroups(` *order* `)` F

The input *order* has to be a positive cubefree integer. The output is a complete and irredundant list of isomorphism type representatives of nilpotent groups of this size. The groups are given as pc groups.

4 ► `ConstructAllCFSimpleGroups(` *order* `)` F

The input *order* has to be a positive cubefree integer. The output is a complete and irredundant list of isomorphism type representatives of simple groups of this size. In particular, there exists either none or exactly one simple group of the given order.

5 ► `ConstructAllCFFrattiniFreeGroups(` *order* `)` F

The input *order* has to be a positive cubefree integer. The output is a complete and irredundant list of isomorphism type representatives of Frattini-free groups of this size.

6 ► `NumberCFGroups(` *n*`[,` *bool* `] )` F

The input n has to be a positive cubefree integer and the output is the number of all cubefree groups of order n. The SmallGroups library is used whenever possible, i.e. when $n \leq 50000$. Only if *bool* is set to false, then only the numbers of squarefree groups are taken from the SmallGroups library.

7 ► `NumberCFSolvableGroups(` *n*`[,` *bool* `] )` F

The input n has to be a positive cubefree integer and the output is the number of all cubefree solvable groups of order n. The SmallGroups library is used whenever possible, i.e. when $n \leq 50000$. Only if *bool* is set to false, then only the numbers of squarefree groups are taken from the SmallGroups library.

8 ► `CountAllCFGroupsUpTo(` *n*`[,` *bool* `])` F

The input is a positive integer n and the output is a list L of size n such that $L[i]$ contains the number of isomorphism types of groups of order i if i is cubefree and $L[i]$ is not bound, otherwise, $1 \leq i \leq n$. The

SmallGroups library is used whenever possible, i.e. when $n \leq 50000$. Only if *bool* is set to false, then only the numbers of squarefree groups are taken from the SmallGroups library.

9 ► `IsCubeFreeInt(` n `)` P

The output is *true* if n is a cubefree integer and *false* otherwise.

10 ► `IsSquareFreeInt(` n `)` P

The output is *true* if n is a squarefree integer and *false* otherwise.

11 ► `IrreducibleSubgroupsOfGL(` n, q `)` O

The current version of this function allows only n=2. The input q has to be a prime-power $q = p^r$ with $p \geq 5$ a prime. The output is a list of all irreducible subgroups of $\mathrm{GL}(2, q)$ up to conjugacy.

12 ► `RewriteAbsolutelyIrreducibleMatrixGroup(` G `)`

The input G has to be an absolutely irreducible matrix group over a finite field $\mathrm{GF}(q)$. If possible, the output is G rewritten over the subfield of $\mathrm{GF}(q)$ generated by the traces of the elements of G. If no rewriting is possible, then the input G is returned.

2.2 Comments on the implementation

This section provides some useful information about the implementations.

ConstructAllCFGroups

The function `ConstructAllCFGroups` constructs all groups of a given cubefree order up to isomorphism using the Frattini Extension Method as described in [Die05], [DE05], [BE99a], and [BE99b]. One step in the Frattini Extension Method is to compute Frattini extensions and for this purpose some already implemented methods of the required GAP package GrpConst are used.

Since `ConstructAllCFGroups` requires only some special types of irreducible subgroups of $\mathrm{GL}(2, p)$ (e.g. of cubefree order), it contains a modified internal version of `IrreducibleSubgroupsOfGL`. This means that the latter is not called explicitely by `ConstructAllCFGroups`.

To reduce runtime, the generators of the reducible subgroups of $\mathrm{GL}(2, p)$, $2 \leq p \leq 100$ a prime, are stored in the file 'diagonalMatrices.dat'.

ConstructAllCFSimpleGroups and ConstructAllCFNilpotentGroups

The construction of simple or nilpotent groups of cubefree order is rather easy, see [Die05] or [DE05]. In particular, the methods used in these cases are independent from the methods used in the general cubefree case.

CountAllCFGroupsUpTo

As described in [Die05] and [DE05], every cubefree group G has the form $G = A \times I$ where A is trivial or non-abelian simple and I is solvable. Further, there is a one-to-one correspondence between the solvable cubefree groups and *some* solvable Frattini-free groups. This one-to-one correspondence allows to count the number of groups of a given cubefree order without computing any Frattini extension. To reduce runtime, the computed irreducible and reducible subgroups of the general linear groups $\mathrm{GL}(2, p)$ and also the number of the computed solvable Frattini-free groups are stored during the whole computation. This is very memory consuming but reduces the runtime significantly. The alternative is to run a loop over `NumberCFGroups`.

IrreducibleSubgroupsOfGL

If the input is a matrix group over $\mathrm{GF}(q)$, then the algorithm needs to construct $\mathrm{GF}(q^3)$ internally.

RewriteAbsolutelyIrreducibleMatrixGroup

The function `RewriteAbsolutelyIrreducibleMatrixGroup` as described algorithmically in [GH97] is probabilistic. If the input is $G \leq \mathrm{GL}(d, p^r)$, then the expected runtime is $O(rd^3)$.

2.3 Accuracy check

We have compared the results of `ConstructAllCFGroups` with the library of cubefree groups of GrpConst. Further, we compared the number and size of the solvable groups constructed by `IrreducibleSubgroupsOfGL` with the library of Irredsol.

3 Installing and loading the Cubefree package

3.1 Installing the Cubefree package

The installation of the Cubefree package follows standard GAP rules. So the standard method is to unpack the package into the `pkg` directory of your GAP distribution. This will create an `cubefree` subdirectory.

3.2 Loading the Cubefree package

To use the Cubefree Package you have to request it explicitly. This is done by calling `RequirePackage` like this:

```
gap> RequirePackage("Cubefree");
Loading Cubefree 1.05 ...

   -- Construction Algorithm for Cubefree Groups, 1.05 --
   -------- Heiko Dietrich, H.Dietrich@tu-bs.de ---------
true
```

Bibliography

[BE99a] H. U. Besche and B. Eick. Construction of finite groups. *J. Symb. Comput.*, 27:387–404, 1999.

[BE99b] H. U. Besche and B. Eick. The groups of order at most 1000 except 512 and 768. *J. Symb. Comput.*, 27:405–413, 1999.

[BE99c] H. U. Besche and B. Eick. *GrpConst*, 1999. A GAP 4 package, see [GAP4].

[BEO02] H. U. Besche, B. Eick, and E. A. O'Brien. A Millennium Project: Constructing small groups. *Intern. J. Alg. and Comput.*, 12:623–644, 2002.

[DE05] H. Dietrich and B. Eick. On the groups of cube-free order. *J. Algebra*, 292:122–137, 2005.

[Die05] H. Dietrich. On the groups of cube-free order. Diploma thesis, TU Braunschweig, 2005.

[FO05] D. L. Flannery and E. A. O'Brien. Linear groups of small degree over finite fields. *Intern. J. Alg. Comput.*, 15:467–502, 2005.

[GH97] S. P. Glasby and R. B. Howlett. Writing representations over minimal fields. *Comm. Alg.*, 25:1703–1711, 1997.

[Hoe95] O. Hoelder. Die Gruppen mit quadratfreier Ordnung. *Nachr. Koenigl. Ges. Wiss. Goettingen Math.-Phys. K*, 1:211–229, 1895.

[Hoe00] B. Hoefling. *Irredsol*, 2000. A GAP 4 package, see [GAP4].

[Tau55] D. R. Taunt. Remarks on the Isomorphism Problem in Theories of Construction of finite Groups. *Proc. Cambridge Philos. Soc.*, 51:16–24, 1955.

Index

This index covers only this manual. A page number in *italics* refers to a whole section which is devoted to the indexed subject. Keywords are sorted with case and spaces ignored, e.g., "`PermutationCharacter`" comes before "permutation group".