ClassTwoAlg

A package to enumerate class two algebras over finite fields

Version 1.0

18 October 2017

Bettina Eick
Morten Wesche

Bettina Eick Email: beick@tu-bs.de
Homepage: http://www.icm.tu-bs.de/~beick/

Morten Wesche Email: m.wesche@tu-bs.de
Homepage: http://www.icm.tu-bs.de/~morwesch/

Copyright

Acknowledgements

We appreciate very much all past and future comments, suggestions and contributions to this package and its documentation provided by GAP users and developers.

Contents

Chapter 1

Introduction

This package provides some functions for GAP [GAP17] to compute PORC functions $N_{d,r}(q)$ giving the number of isomorphism classes of associative algebras of class two, rank r and dimension d.

Let $\mathbb{F}$ be a field and let V be a vector space over $\mathbb{F}$. An algebra $\mathscr{A}$ over $\mathbb{F}$ is a vector space over $\mathbb{F}$ equipped with a bilinear mapping

$$\cdot : \mathscr{A} \times \mathscr{A} \to \mathscr{A}, (x,y) \mapsto x \cdot y =: xy$$

called multiplication.

An algebra is called associative if its multiplication is associative; It is called commutative if the multiplication is commutative. If there exists an element $1 \in \mathscr{A}$ such that $1 \cdot x = x = x \cdot 1$ holds for all elements $x \in \mathscr{A}$ the algebra is said to be an algebra with one.

An algebra $\mathscr{A}$ is said to be nilpotent if the power ideal series

$$\mathscr{A} > \mathscr{A}^2 > \ldots > \mathscr{A}^k > \ldots$$

terminates in the trivial algebra, hence there is a $k \in \mathbb{N}$ such that

$$\mathscr{A} > \mathscr{A}^2 > \ldots > \mathscr{A}^k = \{0\}.$$

The smallest $l \in \mathbb{N}$ with $\mathscr{A}^l \neq \{0\}$ and $\mathscr{A}^{l+1} = \{0\}$ is called the nilpotency class or just class of $\mathscr{A}$ denoted by $\mathrm{cl}(\mathscr{A})$.

The dimension of the algebra $\mathscr{A}$ denoted by $\dim_{\mathbb{F}}(\mathscr{A}) = \dim(\mathscr{A})$ is the dimension of $\mathscr{A}$ considered as vector space. The rank of $\mathscr{A}$ denoted by $\mathrm{rk}(\mathscr{A})$ is the minimal number of generators of $\mathscr{A}$. It is $\mathrm{rk}(\mathscr{A}) = \dim(\mathscr{A}/\mathscr{A}^2)$.

Let $q \in \mathbb{N}$ be a prime or a power of a prime. Then $N_{d,r}(q)$ denotes the number of isomorphism classes of nilpotent algebras of class two of dimension d and rank r over the finite field with q elements.

A function f on an infinite subset S of the natural numbers is called Polynomial on Residue Classes (PORC) if there exists a natural number m and associated polynomials $g_0, \ldots, g_{m-1} \in \mathbb{Q}[x]$ so that $f(s) = g_a(s)$ for all $s \in S$ with $s \equiv a \bmod m$. This notation was introduced by Higman.

It can be shown (see [EW17]) that the number $N_{d,r}(q)$, considered as a function in q, is PORC.

Chapter 2

Main function

The most important feature of this package is to determine the number $N_{d,r}(q)$ for a given integer r and all d. Within the output the size of the field q is kept variable and is handled as an indeterminate. Hence, the PORC function $N_{d,r}(q)$ is given as a multivariate polynomial where every gcd is treated as an indeterminate, too.

It is useful to introduce the codimension $k := d - r$ as there are some symmetries that can be used.

2.1 Defining indeterminates and PORC functions

Within the ClassTwoAlg PORC functions are considered as multivariate polynomials. To avoid problems with different indeterminates not coming from this package, an `OFFSET_VARS` for the internal numbering of the indeterminates of this package was used. Its default value is 1000. All indeterminates of this package are polynomials over the rationals.

The function `NameToIndet` (2.1.1) creates, depending on the given input, the indeterminates for the PORC functions. If the input is the string `"q"` then the indeterminate q is created having the GAP internal number `OFFSET_VAR`. If a list `[n,k]` is given then the indeterminate is displayed as $(q-k,n)$ and is used for the greatest common divisor of $q-k$ and n.

2.1.1 NameToIndet

▷ `NameToIndet(name)` (function)

Returns an indeterminate over the rationals which is displayed as desired. If *name* is given as string `"q"`, the indeterminate will be displayed as `q`. Internally, this indeterminate has got number `OFFSET_VARS`. If *name* is given as pair $[n,k]$, the ineterminate will be displayed as `(q-k,n)`. The internal number is `OFFSET_VARS`$+n\cdot(n-1)/2+(k \bmod n)$

Example

```
gap> NameToIndet("q");
q
gap> NameToIndet([5,3]);
(q-3,5)
gap> IndeterminateName(FamilyObj(NameToIndet("q")),1000);
"q"
gap> IndeterminateName(FamilyObj(NameToIndet("q")),1013);
"(q-3,5)"
gap> FieldOfPolynomial(NameToIndet("q")); FieldOfPolynomial(NameToIndet([3,2]));
```

```
Rationals
Rationals
```

2.1.2 ValueOfPorcPoly

▷ ValueOfPorcPoly(*f*, *q*) (function)

Given a PORC function *f*, this function evaluates *f* at *q*.

Example
```
gap> f := 3*NameToIndet("q") + NameToIndet("q")*NameToIndet([5,2])
> - 3*NameToIndet([3,1]);
q*(q-2,5)+3*q-3*(q-1,3)
gap> ValueOfPorcPoly(f,7);
47
```

In case of a function being the quotient of two PORC functions an extension of the previous function is implemented.

2.1.3 ValueOfPorcRatFun

▷ ValueOfPorcRatFun(*f*, *q*) (function)

Given a PORC function *f*, this function evaluates *f* at *q*.

Example
```
gap> g := 3*NameToIndet("q") + 2*NameToIndet("q")*NameToIndet([5,3])
>  - 4*NameToIndet([3,2]);;
gap> h := f/g;
(q*(q-2,5)+3*q-3*(q-1,3))/(2*q*(q-3,5)+3*q-4*(q-2,3))
gap> ValueOfPorcRatFun(h, 7);
47/31
gap> ValueOfPorcPoly(f,7)/ValueOfPorcPoly(g,7);
47/31
```

2.2 Computing the number isomorphism types

2.2.1 NumberOfClassTwoAlgebras

▷ NumberOfClassTwoAlgebras(*r*, *action*[, *k*]) (function)

Given a natural number *r* the function computes PORC functions in the indeterminate q whose values, evaluated at q, yield the number of isomorphism classes of certain algebras depending on the given action.

If *k* is not given, then all PORC functions will be computed simultaneously and the output is a list of PORC functions such that the i-th function belongs to the codimension i. Note that there is a symmetry between those functions, such that the latter half of functions is not printed (see section 3.1).

If the codimension k is given, only the PORC function giving the number of isomorphism classes of codimension $k = d - r$ is computed.

So far the following actions are implemented:

Kronecker: Yields the number of isomorphism classes of nilpotent algebras of class two.

Example
```
gap> NumberOfClassTwoAlgebras(2,Kronecker);
[ q-(q-0,2)+5, 3*q-(q-0,2)+6 ]
gap>
gap> NumberOfClassTwoAlgebras(2,Kronecker,1);
q-(q-0,2)+5
gap>
gap> N := NumberOfClassTwoAlgebras(3,Kronecker,2);;
gap> ValueOfPorcPoly(N, 91);
574319955425
```

2.3 Import and export of PORC functions

It might be useful to save the computed PORC functions in a separate file that can be imported to another GAP sesscion. For this purpose the functions `PorcToExt` (2.3.1) and `PorcByExt` (2.3.2) can be used. The PORC function is then converted into the GAP external representation of polynomials.

As the main algorithm `NumberOfClassTwoAlgebras` (2.2.1) produces (depending on the input) PORC functions or lists of PORC functions, the functions `PorcToExt` (2.3.1) and `PorcByExt` (2.3.2) are designed so that they can interpret both: a single function or a list of functions.

2.3.1 PorcToExt

▷ `PorcToExt(`*porc*`[, `*file*`])` (function)

Given a PORC function *porc* the external representation of *porc* is returned. If the second argument *file* is given and if it is a writable file then the output is directly printed into that file.

Instead of a single PORC function *porc* can also be a list of PORC function or even a matrix of PORC function. The nesting depth must not be greater than two.

Example
```
gap> N := NumberOfClassTwoAlgebras(3,Kronecker,3);;
gap> e := PorcToExt(N);
[ [ [  ], 173/2, [ 1007, 1 ], 1, [ 1004, 1 ], 1, [ 1003, 1 ], -1/2, [ 1001, 1 ],
       -20, [ 1000, 1 ], 223/2, [ 1000, 1, 1007, 1 ], 2, [ 1000, 1, 1004, 1 ], 4,
       [ 1000, 1, 1003, 1 ], -1/2, [ 1000, 1, 1001, 1 ], -22, [ 1000, 2 ], 177/2,
       [ 1000, 2, 1007, 1 ], 1, [ 1000, 2, 1004, 1 ], 2, [ 1000, 2, 1003, 1 ],
       -1/2, [ 1000, 2, 1001, 1 ], -15, [ 1000, 3 ], 48, [ 1000, 3, 1001, 1 ],
       -6, [ 1000, 4 ], 29, [ 1000, 4, 1001, 1 ], -2, [ 1000, 5 ], 13,
       [ 1000, 6 ], 8, [ 1000, 7 ], 5, [ 1000, 8 ], 3, [ 1000, 9 ], 1,
       [ 1000, 10 ], 1 ], [ [  ], 1 ] ]
gap>
gap> M := NumberOfClassTwoAlgebras(2,Kronecker);
[ q-(q-0,2)+5, 3*q-(q-0,2)+6 ]
gap> f := PorcToExt(M);
[ [ [ [  ], 5, [ 1001, 1 ], -1, [ 1000, 1 ], 1 ], [ [  ], 1 ] ], [ [ [  ], 6,
```

```
[ 1001, 1 ], -1, [ 1000, 1 ], 3 ], [ [  ], 1 ] ] ]
```

2.3.2 PorcByExt

▷ PorcByExt(*ext*[, *depth*]) (function)

Given a PORC function by an external GAP representation *ext* a multivariate polynomial is returned.

It is also possible to give a list *ext* of external representations or a matrix of such representations. The second argument *depth* stands for the nesting depth of the input. If only a single representation *ext* is given, it need not be given.

Example

```
gap> N2 := PorcByExt(e);;
gap> N = N2;
true
gap>
gap> M2 := PorcByExt(f,1);
[ q-(q-0,2)+5, 3*q-(q-0,2)+6 ]
gap> M2=M;
true
```

Chapter 3

Actions and classes of algebras whose isomorphism types can be enumerated

Here it is briefly introduced which actions are implemented and which classes of algebras can be enumerated.

When one follows [Eic08] one gets the relation between the desired class of algebras that shall be enumerated and the action that has to be used.

3.1 Kronecker Action - Associative algebras

In the case of class-2 nilpotent associative algebras of rank r one obtains that the general linear group $\mathrm{GL}(r,q)$ operates on the set of subspaces of the r^2 dimensional vector space $M = \mathbb{F}_q^r \otimes_{\mathbb{F}_q} \mathbb{F}_q^r$ via the Kronecker product.

To obtain the number of class-2 nilpotent algebras of rank r and dimension d over the field with q elements one hast to call the function `NumberOfClassTwoAlgebras` (2.2.1) wth the second argument *`Kronecker`*.

The algorithm uses some important properties arising from the action. Further, symmetries amongst the codimensions k are used:

$$N_{d,r}(q) = 0 \; if \; d \notin \{r+1,\ldots,r^2\} \; and \; N_{r+r^2,r}(q) = 1.$$

$$For \; all \; k \in \{1,\ldots,r^2\} \; holds \; N_{r+k,r}(q) = N_{r+r^2,r}(q) = 1.$$

A proof can be found in [EW17].

Especially the second equation is used for the output of `NumberOfClassTwoAlgebras` (2.2.1) when called with the second argument *`Kronecker`*: For a better reading, it will be returned a list of length $\lceil \frac{r^2}{2} + 1 \rceil$, only. The latter half would be just symmetric to the printed functions.

3.2 More actions

In the future hopefully more actions will be implemented.

Chapter 4

About the Info Class

4.1 The Info Class `InfoCountAlg`

An info class `InfoCountAlg` for this package is provided. Depending on the chosen level the function `NumberOfClassTwoAlgebras` (2.2.1) gives information on the progress of the computation.

The default value is 2.

If the info class is chosen to be 0 no intermediate data is printed.

Example
```
gap> SetInfoLevel(InfoCountAlg,0);
gap> NumberOfClassTwoAlgebras(2,Kronecker);
[ q-(q-0,2)+5, 3*q-(q-0,2)+6 ]
```

If the info class is chosen to be 1 it is just printed at what stage the algorithm is.

Example
```
gap> SetInfoLevel(InfoCountAlg,1);
gap> NumberOfClassTwoAlgebras(2,Kronecker);
#I  Determine exceptional chars
#I  Determine or catch extension dimensions
#I  Determine jnf types in GL
#I  Determine equations for 4 types
#I  Apply action to 4 types
#I  Determine fixed points in dims: [ 1 .. 2 ]
#I  Determine PORC poly in dims: [ 1 .. 2 ]
#I  Simplify PORC polys
[ q-(q-0,2)+5, 3*q-(q-0,2)+6 ]
```

If the info class is chosen to be 2 details are given while the types of matrices are considered. Note that not all types are considered. There are symmetries used such that some types are skipped.

Example
```
gap> SetInfoLevel(InfoCountAlg,2);
gap> NumberOfClassTwoAlgebras(2,Kronecker);
#I  Determine exceptional chars
#I  Determine or catch extension dimensions
#I  Determine jnf types in GL
#I  Determine equations for 4 types
#I    Consider type 1
#I      Got field description
#I      Got 0 elementary equations
```

```
#I      Got acting group of size 1
#I      Start inclusion-exclusion
#I      Done
#I    Consider type 3
#I      Got field description
#I      Got 1 elementary equations
#I      Got acting group of size 1
#I      Start inclusion-exclusion
#I      Done
#I    Consider type 4
#I      Got field description
#I      Got 1 elementary equations
#I      Got acting group of size 1
#I      Start inclusion-exclusion
#I      Done
#I  Apply action to 4 types
#I  Determine fixed points in dims: [ 1 .. 2 ]
#I  Determine PORC poly in dims: [ 1 .. 2 ]
#I  Simplify PORC polys
[ q-(q-0,2)+5, 3*q-(q-0,2)+6 ]
```

References

[Eic08] B. Eick. *Computing automorphism groups and testing isomorphism for modular group algebras*. Number 11. 2008. 9

[EW17] B. Eick and M. Wesche. *Enumeration of nilpotent associative algebras of class 2 over arbitrary finite fields*. 2017. 4, 9

[GAP17] The GAP Group, Aachen, St Andrews. *GAP – Groups, Algorithms, and Programming, Version 4.8.8*, 2017. `http://www.gap-system.org`. 4

Index